

# **Oracle® Enterprise Manager Ops Center**

Feature Reference Guide

12c Release 1 (12.1.1.0.0)

**E27511-04**

August 2012

E27511-04

Copyright © 2007, 2012, Oracle and/or its affiliates. All rights reserved.

Primary Authors: Barbara Higgins, Laura Hartman, Shanthi Srinivasan, Owen Allen, Uma Shankar, Richa Agarwala, Luis Ramos Veja, Karen Orozco Sanchez

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

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

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

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

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

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

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

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

---

---

# Contents

<b>Preface</b> .....	xxvii
Audience .....	xxvii
Documentation Accessibility .....	xxvii
Related Documents .....	xxvii
Conventions .....	xxvii
<b>Part I Getting Started</b>	
<b>1 Introduction</b>	
<b>Oracle Enterprise Manager Ops Center in the Data Center</b> .....	1-1
<b>Roles and Connection Modes</b> .....	1-1
<b>User Preferences and Roles</b> .....	1-2
Start In and Start Page Preferences .....	1-2
User Interface Preferences .....	1-2
Membership Graph Preferences .....	1-2
User Preferences Summary .....	1-2
Role Preferences .....	1-3
<b>How To Use This Collection</b> .....	1-3
<b>2 Asset Management</b>	
<b>Introduction to Asset Management</b> .....	2-1
<b>Roles for Asset Management</b> .....	2-1
<b>Actions for Asset Management</b> .....	2-2
<b>Location of Asset Management Information in the User Interface</b> .....	2-2
<b>Discovering and Managing Assets</b> .....	2-3
Declaring Servers for OS Provisioning .....	2-4
Declaring Servers for Service Processor Configuration .....	2-5
Adding Assets Using a Discovery Profile .....	2-6
Finding Assets .....	2-7
Creating a Discovery Profile .....	2-7
Editing a Discovery Profile .....	2-8
Copying a Discovery Profile .....	2-9
Deleting a Discovery Profile .....	2-9
Installing Agent Controllers From the Command Line .....	2-9
Using Management Credentials .....	2-16

Upgrading Management Credentials From a Prior Version .....	2-16
Updating Management Credentials .....	2-16
Creating Management Credentials .....	2-17
Using Custom SSH Keys for OS Discovery .....	2-17
Editing Management Credentials.....	2-18
Copying Management Credentials .....	2-18
Deleting Management Credentials.....	2-18
Editing Asset Attributes .....	2-18
Using Access Points .....	2-19
Deleting Assets .....	2-19
Special Discovery and Management Procedures .....	2-20
Windows Systems.....	2-20
Servers .....	2-21
Storage .....	2-22
Oracle Solaris Cluster .....	2-24
<b>Using Tags .....</b>	<b>2-24</b>
Adding Tags.....	2-24
Viewing Tags .....	2-24
Grouping Assets Using Tags .....	2-25
Deleting Tags .....	2-25
<b>Using Groups .....</b>	<b>2-25</b>
System Groups and User-Defined Groups.....	2-25
System Groups .....	2-25
User-Defined Groups .....	2-26
Viewing Group Data.....	2-26
Creating a Group.....	2-26
Editing a Group .....	2-27
Adding Assets to a Group .....	2-28
Removing Assets from a Group.....	2-28
Moving Assets to a Group .....	2-28
Moving a Group .....	2-29
Deleting a Group .....	2-29
<b>Related Resources for Asset Management .....</b>	<b>2-29</b>

### 3 Jobs

<b>Introduction to Jobs .....</b>	<b>3-1</b>
<b>Roles for Job Management .....</b>	<b>3-3</b>
<b>Job Management.....</b>	<b>3-4</b>
<b>Viewing Jobs .....</b>	<b>3-4</b>
Viewing All Jobs and Jobs With Specific Status .....	3-4
Viewing Job Details.....	3-5
Monitoring Jobs for an Asset.....	3-7
Search for Jobs .....	3-7
<b>Taking Actions on a Job .....</b>	<b>3-8</b>
Answering Questions .....	3-8
Stopping a Job.....	3-8
Re-running a Completed Job .....	3-9

Re-running a Job on Failed Targets .....	3-9
Copying a Job.....	3-9
Deleting a Job.....	3-9
Debugging a Job Using the OCDoctor.....	3-9
<b>Changing the Job Properties .....</b>	<b>3-10</b>
<b>Events for Job Management .....</b>	<b>3-10</b>
<b>Related Resources for Job Management.....</b>	<b>3-10</b>

## Part II Configure

### 4 Monitoring Rules and Policies

<b>Introduction to Monitoring .....</b>	<b>4-1</b>
<b>Monitoring Roles.....</b>	<b>4-1</b>
<b>Location of Monitoring Rules and Policies in the User Interface .....</b>	<b>4-2</b>
<b>Monitoring Rules .....</b>	<b>4-2</b>
System-Defined and User-Defined Rules.....	4-3
User-Defined Rule Parameters.....	4-3
Enabled and Active Rules .....	4-4
Edit Monitoring Rules .....	4-5
Use Historical Data to Determine Threshold Limits for a Specific Asset .....	4-6
Add Monitoring Rules.....	4-6
<b>Monitoring Policies.....</b>	<b>4-7</b>
Default Monitoring Policies.....	4-8
Available Monitoring Policies .....	4-8
Monitoring Policy Details .....	4-9
Apply a Monitoring Policy to a Group .....	4-11
Edit the Monitoring Configuration of an Asset Bound to a Monitoring Policy .....	4-12
Create a Group of Assets According to Monitoring Policy .....	4-12
Extract a Monitoring Policy .....	4-12
Add or Copy a Monitoring Policy .....	4-13
Delete a Monitoring Policy .....	4-14
<b>Related Resources for Monitoring Rules and Policies .....</b>	<b>4-14</b>

### 5 Software Libraries

<b>Introduction to Software Libraries and Repositories.....</b>	<b>5-1</b>
<b>Roles for Software Libraries .....</b>	<b>5-2</b>
<b>Actions for Software Libraries.....</b>	<b>5-2</b>
<b>Location of Software Library Information in the User Interface.....</b>	<b>5-2</b>
<b>Knowledge Base and Parent Repository.....</b>	<b>5-3</b>
EC Library .....	5-3
Publishers and Parent of the Oracle Solaris 11 Repository.....	5-4
<b>Using Software Libraries .....</b>	<b>5-4</b>
Viewing the Contents of a Software Library.....	5-4
Creating a Software Library .....	5-5
Maintaining the Knowledge Base and Updates .....	5-6
<b>Libraries for Oracle Solaris 11 .....</b>	<b>5-6</b>

Oracle Solaris 11 Software Update Library .....	5-6
Oracle Solaris 11 Software Update Library Summary Tab .....	5-7
Oracle Solaris 11 Software Update Library Content Tab .....	5-8
Actions for Oracle Solaris 11 Libraries .....	5-8
Configure Parent Repositories .....	5-8
Add Content .....	5-9
Delete Oracle Solaris 11 Software Update Library .....	5-9
<b>Libraries for Oracle Solaris 10, 9, 8 and Linux</b> .....	5-9
<b>Images</b> .....	5-9
Images for OS Provisioning .....	5-10
Images for Firmware Updates .....	5-11
Uploading or Importing ISO Images .....	5-12
Working with Firmware for Power Distribution Units .....	5-12
<b>Local Content</b> .....	5-13
Local Action .....	5-13
Local Package .....	5-14
Local Configuration Files .....	5-15
Local Categories .....	5-16
Editing a Local Component File .....	5-17
Deleting a Local Component .....	5-17
Uploading Local Software in Bulk .....	5-18
Viewing Bulk Upload Results .....	5-19
<b>Backing Up Images and Local Content</b> .....	5-19
<b>Related Resources for Software Libraries</b> .....	5-19

## 6 Storage Libraries

<b>Introduction to Storage Management</b> .....	6-1
<b>Roles for Storage Management</b> .....	6-1
<b>Actions for Storage Management</b> .....	6-2
<b>Location of Storage Information in the User Interface</b> .....	6-2
<b>Storage Libraries</b> .....	6-3
Network Attached Storage (NAS) Storage Libraries .....	6-5
Block Storage .....	6-5
Dynamic Block Storage .....	6-6
Static Block Storage .....	6-6
Storage Libraries for a Virtual Datacenter .....	6-6
Storage Libraries for Oracle Solaris Zones .....	6-7
Storage Libraries and Repositories for Oracle VM Server .....	6-7
<b>Types of Storage for Libraries</b> .....	6-7
File Systems Libraries .....	6-7
Viewing Local Libraries .....	6-7
Editing the Attributes of a Local Library .....	6-8
Creating a Local Library .....	6-8
Deleting a Local Library .....	6-9
Block Storage .....	6-9
Select LUNs For the Block Storage Library .....	6-9
Add Capacity to Dynamic Block Storage Libraries .....	6-10

<b>Oracle VM Storage Connect Plug-ins</b> .....	6-11
<b>Storage Hardware</b> .....	6-12
RAID Controller .....	6-12
NAS Storage Appliance.....	6-12
To Set Up a Share on the NFS Server .....	6-12
To Set Up an NFS Client .....	6-13
To Create a NAS Storage Library .....	6-14
File Server .....	6-15
Storage Array .....	6-15
Storage Server: Sun ZFS Storage Appliance.....	6-15
Managing a Sun ZFS Storage Appliance .....	6-15
Provisioning and Updating a Sun ZFS Storage Appliance.....	6-15
Exadata Storage Server.....	6-16
<b>Storage Profiles</b> .....	6-16
<b>High Availability for Storage Resources</b> .....	6-16
<b>Related Resources for Storage Management</b> .....	6-17

## 7 Networks

<b>Introduction to Network Management</b> .....	7-1
<b>Roles Required for Network Management</b> .....	7-2
<b>Actions for a Network and Network Domain</b> .....	7-2
<b>Location of Network Information in the User Interface</b> .....	7-3
<b>Network Domains</b> .....	7-3
Default Network Domain .....	7-4
User-Defined Network Domains .....	7-4
Editing Attributes of a User-Defined Network Domain .....	7-5
<b>Networks</b> .....	7-5
Requirements for a Network .....	7-6
Public Networks and Private Networks .....	7-6
Networks for Server Pools .....	7-7
Networks for Oracle Solaris Zones.....	7-7
Networks for Oracle VM Servers.....	7-8
Networks for Virtual Datacenters.....	7-8
Bandwidth Management.....	7-8
IP Multipathing Groups .....	7-9
Link Aggregation or Bond .....	7-10
<b>Properties of a Network</b> .....	7-10
IPv4 and IPv6 Protocols .....	7-11
Routing Mode .....	7-11
Static Route for the Network .....	7-11
Address Allocation Method .....	7-11
Maximum Transmission Unit (MTU) .....	7-12
VLAN and VLAN Tags .....	7-12
<b>Network Utilization</b> .....	7-12
<b>Network Connectivity</b> .....	7-12
<b>Network Hardware</b> .....	7-13
Network Interface Card (NIC) .....	7-13

Network Switches .....	7-13
<b>Network Profiles</b> .....	7-13
<b>Oracle Enterprise Manager Ops Center's Networks</b> .....	7-14
Network Switch Configuration.....	7-14
Separate Management, Provisioning, and Data Networks.....	7-14
Combined Management and Provisioning Network and a Separate Data Network .....	7-16
Combined Provisioning and Data Network and a Separate Management Network .....	7-18
Combined Provisioning, Data, and Management Network.....	7-19
Firewall Rules .....	7-21
Network Port Requirements and Protocols .....	7-21
<b>Related Resources for Networks</b> .....	7-24

## 8 Plans and Profiles

<b>Introduction to Plans and Profiles</b> .....	8-1
Version Control .....	8-2
<b>Roles for Plans and Profiles</b> .....	8-2
<b>Operational Profiles and Plans</b> .....	8-3
Actions for Operational Profiles and Plans .....	8-4
Create an Operational Profile and Plan .....	8-4
Edit an Operational Profile or Plan .....	8-5
Copy an Operational Profile.....	8-5
Copy an Operational Plan.....	8-5
Delete an Operational Profile or Plan .....	8-5
<b>Profiles and Policies</b> .....	8-6
Policies .....	8-6
Profiles .....	8-6
<b>Deployment Plans</b> .....	8-7
Simple Deployment Plans.....	8-8
Multi-Step Deployment Plans .....	8-9
Complex Deployment Plans.....	8-9
<b>Actions for Deployment Plans</b> .....	8-10
Edit a Profile.....	8-10
Edit a Deployment Plan .....	8-10
Copy a Deployment Plan .....	8-11
Deploy a Plan.....	8-12
Delete a Deployment Plan .....	8-12
<b>Location of Profiles and Plans in the User Interface</b> .....	8-12
<b>Related Resources for Plan Management</b> .....	8-13

## Part III Operate and Maintain

### 9 Incidents

<b>Introduction to Incident Lifecycle Management</b> .....	9-1
<b>Roles for Incident Management</b> .....	9-2
<b>Actions for Incident Management</b> .....	9-3
Actions for Incidents.....	9-3



Actions for Service Requests .....	9-3
Actions for Incidents Knowledge Base .....	9-4
<b>Location of Incident and Service Request Information in the User Interface .....</b>	<b>9-4</b>
<b>Incidents .....</b>	<b>9-5</b>
Incident Severity Badges .....	9-5
<b>Message Center .....</b>	<b>9-6</b>
Incidents Dashboards in the Message Center .....	9-8
<b>Annotations .....</b>	<b>9-10</b>
Annotation Views .....	9-11
<b>Incidents Knowledge Base .....</b>	<b>9-12</b>
<b>Oracle Services and Service Requests .....</b>	<b>9-13</b>
Requirements for Oracle Services .....	9-13
View Contract and Warranty Information .....	9-14
View Service Requests .....	9-14
File a Service Request .....	9-15
Automated Service Requests .....	9-15
<b>Incident Lifecycle Management .....</b>	<b>9-16</b>
Methods of Incident Management .....	9-16
View Unresolved Incidents .....	9-17
View Incident Details .....	9-17
Assign an Incident .....	9-18
Acknowledge Incidents .....	9-18
Add an Annotation .....	9-19
Display Annotations .....	9-20
View Comments .....	9-20
Take Action on a Incident .....	9-20
Maintenance Mode .....	9-21
Mark an Incident Repaired .....	9-21
Close an Incident .....	9-22
<b>Annotations .....</b>	<b>9-23</b>
<b>Related Resources for Incident Management .....</b>	<b>9-24</b>

## 10 Reports

<b>Introduction to Reports .....</b>	<b>10-1</b>
<b>Roles for Reports .....</b>	<b>10-2</b>
<b>Actions for Reports .....</b>	<b>10-2</b>
Manage Report Templates .....	10-2
Generate a Report from a Report Template .....	10-3
Edit a Report Template .....	10-3
Delete a Report Template .....	10-3
View and Export Report Results .....	10-3
View the Report Result .....	10-3
Save the Report Result .....	10-4
<b>Location of Report Information in the User Interface .....</b>	<b>10-4</b>
<b>Firmware Reports .....</b>	<b>10-5</b>
<b>Operating System Reports .....</b>	<b>10-6</b>
Update Compliance Reports .....	10-7

Linux and Oracle Solaris OS Update Reports.....	10-7
Change History Report.....	10-8
Baseline Analysis Report.....	10-9
Profile Analysis Report .....	10-13
Recommended Software Configuration Report .....	10-15
Oracle Solaris Update Compliance Report.....	10-16
Incident Compliance Report.....	10-17
Incident Compliance Report for Oracle Solaris or Linux.....	10-17
Incident Compliance Report for Microsoft Windows .....	10-19
Host Compliance Report.....	10-20
Host Compliance Report for Oracle Solaris or Linux.....	10-20
Host Compliance Report for Microsoft Windows .....	10-21
Common Vulnerability and Exposure (CVE) Report .....	10-22
System Catalog Report .....	10-23
<b>Additional Operating System Reports</b> .....	10-24
Distribution Update Report.....	10-24
Service Pack Compliance Report .....	10-24
Package Compliance Report.....	10-25
<b>Incident Reports</b> .....	10-26
<b>System Information Reports</b> .....	10-27
<b>Exalogic Reports</b> .....	10-28
<b>Related Resources for Reports</b> .....	10-29

## 11 Hardware

<b>Introduction to Managing Hardware Assets</b> .....	11-1
Configuring Hardware Assets .....	11-1
Monitoring Hardware Assets.....	11-2
Maintaining Hardware Assets .....	11-2
<b>Roles for Hardware Management</b> .....	11-2
<b>Actions for Hardware Management</b> .....	11-3
<b>Location of Hardware Information in the User Interface</b> .....	11-4
<b>Profiles for Hardware Management</b> .....	11-4
Hardware Resource Profiles .....	11-5
Firmware Provisioning Profiles .....	11-5
<b>Configuring the Service Processor</b> .....	11-5
Create Service Processor Configuration Profile and Plan .....	11-5
Create BIOS Configuration Profile and Plan.....	11-6
Create a Snapshot of a Service Processor Configuration .....	11-7
Apply a Snapshot of a Server Processor Configuration .....	11-8
<b>Configuring a RAID Controller</b> .....	11-9
<b>Configuring a Dynamic System Domain</b> .....	11-9
<b>Configuring a Rack and Placing Components</b> .....	11-9
<b>Hardware Monitoring</b> .....	11-11
Hardware Status.....	11-11
Monitoring a Group of Hardware Assets.....	11-11
Connectivity Status .....	11-11
Service Processor Details.....	11-11

RAID Controller Details.....	11-12
Sun ZFS Storage Appliance Details.....	11-12
Server Details.....	11-12
Chassis Details.....	11-13
M-Series Details.....	11-14
Switch Details.....	11-15
Rack Details.....	11-16
PDU Details.....	11-17
Oracle Solaris Cluster Details.....	11-17
Oracle Exalogic Details.....	11-17
<b>Monitoring Power Utilization.....</b>	<b>11-18</b>
Energy Tab.....	11-18
Charts Tab.....	11-19
<b>Maintaining Hardware Assets.....</b>	<b>11-20</b>
Setting and Changing the Power Policy.....	11-20
Replacing a Failed Power Distribution Unit in a Rack.....	11-21
Installing and Upgrading Oracle Solaris Cluster.....	11-22
<b>Firmware Provisioning.....</b>	<b>11-22</b>
Firmware Profiles.....	11-22
Firmware Compliance Reports.....	11-22
Updating Firmware.....	11-23
<b>Related Resources for Hardware Management.....</b>	<b>11-24</b>

## 12 Operating Systems

Introduction to Operating Systems.....	12-1
Roles for Operating Systems.....	12-3
Actions for Operating Systems.....	12-4
Location of Operating System Information in the User Interface.....	12-4
Operating System Profiles.....	12-6
Agent-Managed and Agentlessly-Managed Operating Systems.....	12-6
Monitoring Operating Systems.....	12-9
<b>Analytics.....</b>	<b>12-10</b>
Displaying Analytics Information.....	12-10
Analytics Views.....	12-11
Customize the View.....	12-12
Analytics Summary View.....	12-12
Processes View.....	12-13
Services View.....	12-14
Thresholds.....	12-14
History.....	12-15
Metrics.....	12-16
Virtualization Analytics View.....	12-18
Charts and Group Charts.....	12-19
Creating Charts.....	12-21
<b>Provisioning Operating Systems.....</b>	<b>12-22</b>
DHCP.....	12-22
WAN Boot.....	12-23

WAN Boot Connection Requirements .....	12-23
Checking Your Client OBP for WAN Boot Support .....	12-24
Setting Up a WAN Boot Connection.....	12-24
Disabling and Enabling WAN Boot .....	12-25
Importing Images .....	12-25
OS Provisioning Profiles .....	12-25
Common Linux Parameters.....	12-25
Oracle Solaris or Linux OS Provisioning Profile .....	12-26
Oracle VM Server for SPARC OS Provisioning Profile.....	12-27
JumpStart Enterprise Toolkit (JET) for Oracle Solaris .....	12-27
Provisioning Plans .....	12-28
Deployment Plans That Provision an Operating System.....	12-29
Provisioning Linux and Oracle Solaris 8, 9, and 10.....	12-29
Provisioning Oracle Solaris 11.....	12-30
Oracle Solaris 11 Provisioning Profiles .....	12-31
Steps for Oracle Solaris 11 Provisioning Plan.....	12-31
<b>Oracle Solaris Boot Environments</b> .....	12-32
Differences Between Oracle Solaris 11 and Oracle Solaris 10 Boot Environments.....	12-32
Boot Environment Monitoring.....	12-33
View Boot Environments .....	12-33
Manage Boot Environments .....	12-35
Activate and Reboot a Boot Environment .....	12-35
To Delete a Boot Environment .....	12-35
<b>Oracle Solaris 11 Boot Environments</b> .....	12-36
Boot Environment Details for Oracle Solaris 11 .....	12-36
Total ZPools Utilization for Oracle Solaris 11 Boot Environments .....	12-37
Boot Environments for Oracle Solaris 11.....	12-37
Snapshots for Oracle Solaris 11 Boot Environments.....	12-38
File Systems for Oracle Solaris 11 Boot Environments.....	12-38
Associated Zone Boot Environments .....	12-38
Boot Environment Profiles and Plans for Oracle Solaris 11 .....	12-39
Create an Oracle Solaris 11 Boot Environment.....	12-40
<b>Oracle Solaris 10 and Earlier Boot Environments</b> .....	12-40
Support for Oracle Solaris 10 Live Upgrade and Oracle Solaris Zones .....	12-42
Boot Environment Details for Oracle Solaris 10 and Previous Versions .....	12-42
Total ZPools Utilization for Oracle Solaris 10 and Earlier Boot Environments.....	12-43
Boot Environments for Oracle Solaris 10 and Earlier .....	12-43
File Systems for Oracle Solaris 10 and Earlier Boot Environments .....	12-43
Boot Environments Profiles and Plans for Oracle Solaris 10 and Earlier .....	12-44
Determine Your Boot Environment Policy .....	12-44
Determine Your Live Upgrade Feature Requirements and Options .....	12-45
Overview of Boot Environments Profiles and Plans .....	12-45
Create an Oracle Solaris 8, 9, or 10 Boot Environment .....	12-45
Deployment Options for Oracle Solaris 8, 9, or 10 .....	12-46
Create an Oracle Solaris 8, 9, or 10 Boot Environments From a Deployment Plan.....	12-47
Create an Oracle Solaris 8, 9, or 10 Boot Environments from an Operational Plan .....	12-47
Create an Update Profile for Oracle Solaris 8, 9, or 10 Boot Environment .....	12-48

Create an Oracle Solaris 8, 9, or 10 Boot Environment From an Update Profile .....	12-48
Create an Oracle Solaris 8, 9, or 10 Boot Environment With an OS Update Job.....	12-49
Synchronize Oracle Solaris 10 Boot Environments .....	12-50
<b>Related Resources</b> .....	12-51

## 13 Operating System Updates

<b>Introduction to Operating System Updates</b> .....	13-1
Operating System Update Requirements .....	13-3
Methods of Running an Update Job .....	13-4
Options Available When Running an Update Job .....	13-4
<b>Roles for Operating System Updates</b> .....	13-4
<b>Actions for Operating System Updates</b> .....	13-5
<b>Location of Operating System Update Information in the User Interface</b> .....	13-5
<b>Agent Managed Operating Systems</b> .....	13-6
<b>System Catalogs</b> .....	13-6
View and Modify a Catalog.....	13-6
Compare System Catalogs .....	13-6
<b>Operating System Update Reports</b> .....	13-7
<b>Update Policies</b> .....	13-7
<b>Update Profiles</b> .....	13-9
<b>Operating System Updates for Oracle Solaris 8, 9, and 10 and Linux</b> .....	13-11
Update an Operating System From a Deployment Plan.....	13-12
Operating System Update Job.....	13-12
Update an Operating System by Modifying a System Catalog .....	13-13
Update From an Operating System Report Result .....	13-13
Use a System Catalog .....	13-14
<b>Operating System Updates for Oracle Solaris 11</b> .....	13-14
Update Oracle Solaris 11 .....	13-15
Oracle Solaris 11 Update Deployment Plan.....	13-15
<b>Update an Oracle Solaris Boot Environment</b> .....	13-16
Update a Boot Environment Using an Update Profile .....	13-16
<b>Operating System Updates for Microsoft Windows</b> .....	13-19
Update Job.....	13-19
Modify the Registry .....	13-20
Configure Oracle Enterprise Manager Ops Center for Updating the Windows Operating System	13-20
Create an Update Job for the Windows Operating System .....	13-21
<b>Related Resources</b> .....	13-21

## Part IV Virtualize and Cloud Management

### 14 Oracle Solaris Zones

<b>Introduction to Oracle Solaris Zones</b> .....	14-1
Global and Non-global Zones .....	14-2
Types of Non-Global Zones.....	14-2
<b>Roles for Zone Management</b> .....	14-2

<b>Zone Management Functions</b> .....	14-3
<b>Prepare Your Global Zone</b> .....	14-3
Associate Storage Libraries.....	14-4
Manage Global Zone Networks.....	14-4
Create IPMP Groups.....	14-7
Create Link Aggregation.....	14-9
Modify and Detach Network from Global Zone.....	14-10
<b>Discover and Manage Existing Zones</b> .....	14-11
Delete or Unmanage Global Zone.....	14-12
Unmanaged Zone Storage Information.....	14-12
<b>Outline of Zone Creation</b> .....	14-13
<b>Zone Requirements</b> .....	14-13
Requirements for Zones on Oracle Solaris 10 OS.....	14-14
Requirements for Zones on Oracle Solaris 11 OS.....	14-15
<b>Zone Configuration Parameters</b> .....	14-15
<b>Create Zone Profile</b> .....	14-16
<b>Deployment of Zone Plans</b> .....	14-19
Apply Zone Deployment Plans.....	14-20
Zpool and File System of Zones.....	14-21
Modify Zone Configuration.....	14-21
<b>Zone Management</b> .....	14-22
Zone Replication.....	14-24
Add Storage to Zones.....	14-25
Move Storage.....	14-26
Add File Systems to Zones.....	14-28
Connect and Disconnect Networks.....	14-28
Automatic Recovery.....	14-28
<b>Zone Migration</b> .....	14-28
Migrating a Physical Oracle Solaris System into a Zone.....	14-29
Migrating Zones to a Different Machine.....	14-30
Script to Migrate a Zone With Dependencies.....	14-34
Script Requirements.....	14-35
<b>Recovering Zones</b> .....	14-37
<b>Zones Server Pool</b> .....	14-38
<b>Update Zones</b> .....	14-38
Installing Packages and Patches on Zones.....	14-39
Configuring patchadd and pkgadd Commands.....	14-39
Editing the .uce.rc File.....	14-39
Updating a Global Zone.....	14-40
Updating Non-Global Zones.....	14-40
Zone Parallel Patching.....	14-41
<b>Other Functions</b> .....	14-42
<b>Related Resources</b> .....	14-42

## 15 Oracle VM Server for SPARC

Introduction to Oracle VM Server for SPARC.....	15-1
Roles for Managing Oracle VM Server for SPARC.....	15-2

<b>Available Management Features</b> .....	15-2
<b>Preparing Your Control Domain</b> .....	15-3
<b>Recommended Minimum Configuration</b> .....	15-3
CPU Threads.....	15-3
Crypto Units.....	15-4
RAM.....	15-4
<b>Create OS Provisioning Profile</b> .....	15-4
Create Link Aggregation in Oracle VM Server for SPARC.....	15-9
Create and Apply Deployment Plan for Oracle VM Server for SPARC.....	15-9
<b>Installation of Oracle VM Server for SPARC</b> .....	15-10
Provisioning the Required Oracle VM Server Version.....	15-12
Important Notes for Installation.....	15-12
Initiating Manual Net Boot.....	15-12
Additional Configurations.....	15-12
<b>Oracle VM Server for SPARC Management</b> .....	15-13
Edit Configuration and Tags.....	15-13
Associate Storage Libraries.....	15-13
Attach Networks.....	15-13
Reboot Oracle VM Server.....	15-15
Performance Management.....	15-15
<b>Server Pools</b> .....	15-17
<b>About Logical Domains</b> .....	15-17
<b>Create Logical Domain Profile</b> .....	15-17
<b>Create and Apply Logical Domain Plan</b> .....	15-19
Apply Logical Domain Deployment Plan.....	15-20
OS Provisioning on Logical Domains.....	15-21
Complex Plan.....	15-21
<b>Management of Logical Domains</b> .....	15-21
Edit Logical Domain Configuration.....	15-22
Shut Down a Logical Domain.....	15-22
Start Logical Domain.....	15-22
Add Storage to Logical Domain.....	15-23
Managing Logical Domain Networks.....	15-23
Migrating a Logical Domain.....	15-23
Enabling Automatic Recovery of Logical Domains.....	15-25
Recovering Logical Domains.....	15-26
Deleting a Logical Domain.....	15-26
Using the Logical Domain Console.....	15-26
<b>Managing Existing Oracle VM Server for SPARC Environments</b> .....	15-26
<b>Related Resources</b> .....	15-28

## 16 Oracle VM Server for x86

<b>Introduction to Oracle VM Server for x86</b> .....	16-1
<b>Roles for Oracle VM Server for x86 Management</b> .....	16-2
<b>Integration of Oracle VM Server for x86 with Oracle Enterprise Manager Ops Center</b> .....	16-2
<b>Installing Oracle VM Manager</b> .....	16-3
<b>Discover Oracle VM Manager</b> .....	16-3

<b>Discover Oracle VM Servers</b> .....	16-6
Discovery Profile for Oracle VM Server .....	16-6
SSH Discovery of Oracle VM Servers .....	16-6
<b>Installing Oracle VM Servers</b> .....	16-7
OS Provisioning Profile for Oracle VM Server .....	16-7
Apply Deployment Plan for Oracle VM Server.....	16-9
<b>Administration of Oracle VM Manager</b> .....	16-10
Manage Ownership of Oracle VM Servers.....	16-10
<b>Discover Storage Resources</b> .....	16-11
<b>Manage Storage Resources</b> .....	16-12
<b>Manage Networks</b> .....	16-13
Attach Networks .....	16-14
<b>Manage Oracle VM Servers</b> .....	16-14
Edit Oracle VM Server Information .....	16-15
Edit IPMI Configuration .....	16-15
Place Oracle VM Server in Maintenance Mode .....	16-15
Update Oracle VM Server.....	16-16
<b>Create Server Pool</b> .....	16-17
Server Pool Policies.....	16-17
Create Oracle VM Server for x86 Server Pools .....	16-18
<b>Create Virtual Machines</b> .....	16-20
Virtualization Types .....	16-21
Create Virtual Machine Profile.....	16-21
<b>Create and Deploy Virtual Machine Plan</b> .....	16-24
<b>Provisioning OS on Virtual Machines</b> .....	16-25
<b>Manage Virtual Machines</b> .....	16-25
Edit Boot Order.....	16-26
Automatic Recovery .....	16-27
<b>Related Resources</b> .....	16-27

## 17 Server Pools

<b>Introduction to Server Pools</b> .....	17-1
<b>Roles for Server Pool Management</b> .....	17-2
<b>Server Pool Policies</b> .....	17-2
Placement Policy .....	17-3
Minimize Power Consumption Policy .....	17-3
Automatic Load Balancing Policy .....	17-3
<b>Automatic Recovery</b> .....	17-4
<b>Server Pool Libraries</b> .....	17-5
<b>Server Pool Networks</b> .....	17-5
<b>Oracle VM Server for SPARC Server Pool</b> .....	17-5
Server Pool Policies.....	17-6
Automatic Recovery .....	17-6
Create an Oracle VM Server for SPARC Server Pool.....	17-8
<b>Oracle Solaris Zones Server Pool</b> .....	17-11
IP Stack in Server Pool.....	17-11
Server Pool Policies.....	17-12



Create a Zones Server Pool .....	17-12
<b>Oracle VM Server for x86 Server Pool</b> .....	17-15
Server Pool Policies .....	17-16
Create Oracle VM Server for x86 Server Pools .....	17-16
<b>Manage Server Pools</b> .....	17-19
Edit Server Pool Parameters .....	17-19
Add Virtualization Hosts .....	17-20
Associate Network Domains .....	17-21
Attach Networks .....	17-22
Associate Libraries .....	17-24
Create Guests .....	17-24
Migrate Multiple Guests .....	17-25
Migrate Zones .....	17-25
Migrate Logical Domains.....	17-26
Migrate Virtual Machines .....	17-26
Balancing Resources .....	17-26
Delete Server Pool .....	17-27
<b>Related Resources</b> .....	17-27

## 18 Virtual Datacenters

<b>Introduction to Cloud Management</b> .....	18-1
Oracle Engineered Systems .....	18-2
<b>Overview of Virtual Datacenter</b> .....	18-3
<b>Roles for Managing Virtual Datacenter</b> .....	18-3
Required User Role .....	18-3
<b>Actions Available in vDC Management</b> .....	18-3
<b>Virtual Datacenter Creation</b> .....	18-4
Server Pool Setup .....	18-4
Storage Setup .....	18-5
Network Setup.....	18-5
Create Virtual Datacenter .....	18-7
<b>vDC Management</b> .....	18-9
Update vDC Configuration .....	18-9
Resource Management .....	18-9
Delete vDC .....	18-11
<b>Account Creation</b> .....	18-12
Create Account .....	18-12
<b>Account Management</b> .....	18-13
Update Account Configuration.....	18-13
Manage Cloud Users to an Account.....	18-13
Maintaining OS Images.....	18-14
Delete an Account .....	18-14
<b>Create and Manage vServer Types</b> .....	18-14
<b>Overview of Cloud Users</b> .....	18-16
<b>Roles for Cloud User Tasks</b> .....	18-17
<b>Actions Available for a Cloud User</b> .....	18-17
<b>View Account Quotas and Virtual Resources</b> .....	18-19

<b>Create and Manage vServers</b> .....	18-20
Before You Begin.....	18-20
Create vServers.....	18-22
vServer Management.....	18-23
<b>vNets Creation</b> .....	18-24
Create a Private vNet.....	18-25
<b>vNets Management</b> .....	18-25
<b>Manage Server Templates</b> .....	18-26
Upload Server Templates.....	18-26
Create Server Templates .....	18-27
Server Template Management .....	18-28
<b>Volume Creation</b> .....	18-28
Create a Volume .....	18-28
Volume Management .....	18-30
<b>Snapshot Creation</b> .....	18-30
Snapshot Management .....	18-31
<b>Distribution Group Creation</b> .....	18-31
Distribution Group Management .....	18-32
<b>Related Resources</b> .....	18-32

## Part V Command Line Interface

### 19 Command Line Interface

<b>CLI Features</b> .....	19-1
Asset Discovery, Management, and Grouping.....	19-1
Operating System Provisioning and Patching.....	19-2
Firmware Provisioning.....	19-3
Administration .....	19-3
<b>Starting the CLI</b> .....	19-3
Invoking the Command Line Interface.....	19-3
To Connect From the Enterprise Controller.....	19-4
To Connect From a Remote System.....	19-4
CLI Usage .....	19-4
User Variables.....	19-5
CLI One-Liner .....	19-5
<b>General Commands</b> .....	19-5
Checking Connectivity .....	19-5
Displaying User Configuration.....	19-5
Setting the User Environment .....	19-6
Recording Console Input and Output.....	19-6
Using a Source File.....	19-7
Viewing the Version .....	19-7
Waiting for a Job to Complete.....	19-7
Viewing Help.....	19-8
Reviewing Commands .....	19-8
Displaying a Man Page.....	19-8
Ending a Mode .....	19-8

Disconnecting from Oracle Enterprise Manager Ops Center .....	19-9
Exiting the CLI.....	19-9
<b>Universal Output Filters .....</b>	<b>19-9</b>
<b>Command Scripts .....</b>	<b>19-9</b>
<b>Commands for Administrative Shell .....</b>	<b>19-10</b>
ecadm.....	19-10
Synopsis.....	19-10
Options .....	19-10
Subcommands .....	19-10
Subcommand options.....	19-12
Exit status .....	19-15
proxyadm .....	19-16
Synopsis.....	19-16
Options .....	19-16
Subcommands .....	19-16
Subcommand options.....	19-17
Exit status .....	19-18
agentadm.....	19-18
Synopsis.....	19-18
Usage.....	19-18
Options .....	19-18
Subcommands .....	19-19
Subcommand options.....	19-19
<b>Mode Commands .....</b>	<b>19-20</b>
User .....	19-20
Starting User Mode.....	19-21
Viewing Users .....	19-21
Viewing Role Types.....	19-21
Viewing User Roles.....	19-21
Adding a User to the Enterprise Controller.....	19-21
Granting Roles to a User .....	19-21
Replicating User Roles .....	19-21
Removing Roles From a User.....	19-22
Adding a Directory Server.....	19-22
Viewing Directory Servers.....	19-22
Viewing Remote Users.....	19-22
Synchronizing All Remote Users.....	19-22
Synchronizing a Single User.....	19-23
Removing a Directory Server.....	19-23
Deleting a User .....	19-23
Incidents .....	19-23
Starting Incidents Mode.....	19-23
Viewing Incidents .....	19-23
Viewing Incident Details .....	19-23
Acknowledging an Incident .....	19-23
Adding an Annotation to One or More Incidents.....	19-23
Assigning Incidents .....	19-24

Closing Incident .....	19-24
Discover .....	19-24
Starting Discover Mode .....	19-24
Creating a Discovery Job .....	19-24
Discovering an OS.....	19-24
Discovering an ILOM Service Processor .....	19-25
Discovering an ALOM Service Processor.....	19-26
Viewing Discovery Profiles .....	19-27
Viewing Discovery Ranges.....	19-27
Viewing Driver Credentials.....	19-27
Viewing Discovery Profile Credentials .....	19-27
Viewing Discovery Ranges.....	19-27
Viewing Networks.....	19-27
Executing Discovery Profiles .....	19-27
Gear .....	19-28
Starting Gear Mode.....	19-28
Viewing Assets .....	19-28
Updating Asset Information .....	19-29
Viewing Jobs Associated With Assets.....	19-29
Managing an Asset .....	19-29
Unmanaging an Asset .....	19-30
Deleting an Asset .....	19-30
Reinstalling an Agent Controller on an Operating System .....	19-31
Rebooting an Operating System .....	19-31
Updating Firmware .....	19-31
Checking Firmware Compliance .....	19-32
Provisioning an OS .....	19-32
Changing Locator Lights .....	19-32
Enabling or Disabling Notifications.....	19-33
Powering Off a Server or Chassis.....	19-33
Powering On a Server or Chassis .....	19-33
Resetting a Server or Chassis.....	19-34
Refreshing a Server .....	19-34
Groups .....	19-35
Starting Groups Mode.....	19-35
Viewing Groups .....	19-35
Viewing Members of a Group.....	19-35
Viewing Group Memberships.....	19-35
Creating a Group .....	19-35
Updating Group Attributes.....	19-35
Adding an Asset To a Group .....	19-35
Removing an Asset From a Group .....	19-36
Moving an Asset From One Group To Another Group.....	19-36
Deleting a Group.....	19-36
Powering On the Assets in a Group.....	19-36
Powering Off the Assets in a Group .....	19-36
Reset Servers in a Group.....	19-36

Jobs .....	19-37
Starting Jobs Mode.....	19-37
Viewing Jobs.....	19-37
Starting a Job.....	19-37
Repeating a Job on Failed Targets .....	19-38
Deleting a Job.....	19-38
Stopping a Job.....	19-38
Stats .....	19-38
Starting Stats Mode.....	19-38
Viewing Statistics.....	19-38
Notifications.....	19-38
Starting Notifications Mode .....	19-38
Viewing Notifications.....	19-39
Deleting a Notification .....	19-39
Update .....	19-39
Starting Update Mode.....	19-39
Viewing OS Update Policies.....	19-40
Viewing OS Update Profiles.....	19-40
Viewing OS Distributions.....	19-40
Viewing Snapshots .....	19-40
Searching Inventory.....	19-40
Checking Inventory .....	19-41
Checking Connectivity to the Knowledge Base .....	19-41
Querying Job History .....	19-41
Querying Job Status.....	19-42
Uploading a Knowledge Base Bundle .....	19-42
Checking the Connection Mode .....	19-42
Changing to Connected Mode .....	19-42
Changing to Disconnected Mode .....	19-42
Modifying an OS Asset .....	19-42
Applying an Update Profile to an OS Asset .....	19-43
Creating a Historical Snapshot .....	19-44
Deleting a Snapshot.....	19-44
Creating a Profile .....	19-44
Creating a Profile From Inventory .....	19-45
Deleting a Profile.....	19-45
Adding a File to a Distribution .....	19-45
Uploading Local Software in Bulk From a Directory .....	19-45
Adding a Local Action .....	19-46
Adding a Local Category.....	19-46
Deleting a Component .....	19-46
Adding a Configuration File .....	19-46
Setting a Component File.....	19-46
Finding Nodes .....	19-46
OSImage .....	19-47
Starting OS Image Mode.....	19-47
Viewing OS Images .....	19-47

Importing an OS Image.....	19-47
Deleting an OS Image.....	19-47
OSProfile.....	19-48
Starting OS Profile Mode .....	19-48
Viewing OS Profiles.....	19-48
Importing a JET Template .....	19-48
Importing an OS Profile.....	19-48
Exporting an OS Profile .....	19-48
Copying an OS Profile.....	19-48
Deleting an OS Profile.....	19-48
FWImage .....	19-48
Starting Fwimage Mode.....	19-49
Viewing Firmware Images .....	19-49
Creating a Firmware Image.....	19-49
Updating a Firmware Image .....	19-49
Deleting a Firmware Image.....	19-50
FWProfile.....	19-50
Starting FW Profile Mode .....	19-50
Viewing Firmware Profiles.....	19-50
Checking the Status of a Firmware Profile.....	19-50
Creating a Firmware Profile .....	19-50
Updating a Firmware Profile .....	19-51
Deleting a Firmware Profile .....	19-51
Virtualization .....	19-51
Starting Virtualization Mode .....	19-51
Viewing Hosts .....	19-51
Viewing Guests .....	19-51
Migrating a Non-Global Zone.....	19-51
Deploy-Setup .....	19-52
Starting Deploy-Setup Mode.....	19-52
Selecting a Deployment Plan.....	19-52
Selecting a Target Asset .....	19-52
Deploy.....	19-53
Viewing the Plan.....	19-53
Setting the Attributes of a Deployment Plan .....	19-54
Adding Attributes to a Deployment Plan .....	19-56
Testing a Deployment Plan .....	19-57
Applying a Deployment Plan .....	19-57

## Part VI Engineered Systems

### 20 Oracle Engineered Systems

Introduction to Oracle Engineered Systems .....	20-1
Datacenter Management .....	20-2
Finding Assets .....	20-2
Creating a Discovery Profile .....	20-3
Adding Assets Using a Discovery Profile .....	20-4

Viewing the Asset Content Pane .....	20-5
Relayed Incidents.....	20-6
Relayed Service Requests.....	20-6
Baseline Check .....	20-6
<b>Oracle Exalogic Elastic Cloud .....</b>	<b>20-6</b>
Oracle Enterprise Manager Ops Center Configuration.....	20-7
Understanding User Roles.....	20-7
Exalogic System Admin Role .....	20-8
Cloud Administrator .....	20-8
Cloud User .....	20-8
Adding a User.....	20-8
Navigation.....	20-8
Viewing the Exalogic System .....	20-9
Dashboard Tab .....	20-10
Details Tab .....	20-11
Controls Tab.....	20-12
Networks Tab .....	20-12
Incidents Tab .....	20-13
Permitted Actions in the Exalogic System View .....	20-14
Viewing the Exalogic System Rack.....	20-14
Photorealistic View of the Rack .....	20-15
Permitted Actions in Rack View .....	20-16
Creating and Viewing Reports.....	20-17
Viewing the Exalogic System Report .....	20-17
<b>SPARC SuperCluster T4-4.....</b>	<b>20-19</b>
SPARC SuperCluster Configuration .....	20-19
Understanding User Roles.....	20-20
SuperCluster System Admin Role.....	20-20
Navigation.....	20-20
Viewing the SPARC SuperCluster System.....	20-21
Dashboard Tab .....	20-22
Details Tab .....	20-24
Networks Tab .....	20-25
Incidents Tab .....	20-25
Permitted Actions in the SPARC SuperCluster System View.....	20-26
Viewing the SPARC SuperCluster System Rack.....	20-26
Photorealistic View of the SPARC SuperCluster System Rack .....	20-27
Viewing the Exadata Storage Server .....	20-28
Discovering a SPARC SuperCluster Component.....	20-29
Add Assets to the SPARC SuperCluster Rack.....	20-29
Creating and Viewing Reports.....	20-30
Viewing the SPARC SuperCluster System Report.....	20-30

## Part VII Reference

<b>A</b>	<b>Asset Attributes</b>	
	Monitoring Attributes .....	A-1
	Grouping Attributes .....	A-1
	Time Zone Values .....	A-10
<b>B</b>	<b>Oracle Solaris Cluster</b>	
	Upgrading an Oracle Solaris Cluster.....	B-1
	Cluster Profiles .....	B-1
	Obtaining the Cluster Profiles and Scripts .....	B-2
	Uploading the Cluster Profiles and Scripts .....	B-3
	Importing Cluster Profiles and Scripts .....	B-4
	Editing the Core Profile for Provisioning.....	B-4
<b>C</b>	<b>Logs and Directories</b>	
	Installation.....	C-1
	General Events .....	C-1
	High Availability.....	C-2
	Software Updates .....	C-2
	Agents .....	C-2
	Local Database .....	C-2
	Upgrade .....	C-3
	Event Logs for Jobs .....	C-3
	To Control the Number of Common Agent Container Log Files .....	C-3
<b>D</b>	<b>JumpStart Enterprise Toolkit</b>	
	JumpStart Enterprise Toolkit Configuration File Location .....	D-1
	SUNWjet Parameters .....	D-1
<b>E</b>	<b>Icons</b>	
	Administration Icons.....	E-1
	Badges.....	E-3
	Boot Environment Icons.....	E-3
	Connectivity Icons.....	E-4
	Group Icons .....	E-5
	Hardware Icons .....	E-6
	Incident Icons .....	E-8
	Job Icons .....	E-9
	Kernel Icons.....	E-10
	Library Icons.....	E-10
	Message Center Icons .....	E-11
	Monitoring Icons .....	E-11
	Network Icons .....	E-13
	Operating System Icons .....	E-13
	Oracle VM Server Icons .....	E-14
	Process Icons.....	E-15



Report Icons.....	E-15
SuperCluster Icons.....	E-17
Switch Icons .....	E-18
Universal Icons .....	E-19
Update Policy Icons .....	E-20
Update Profile Icons .....	E-20

## **F Oracle Enterprise Manager Ops Center API**

List of Public APIs.....	F-4
Public API Access.....	F-7
JMX.....	F-7
WS-Management.....	F-7
Public API Access Through JMX-Remoting.....	F-7
Public API Access Through WS-Management .....	F-8
Virtualization Management Stack.....	F-8
Presentation Tier .....	F-8
Service Tier.....	F-8
Domain Model.....	F-8

## **Glossary**

## **Index**



---

---

# Preface

The Oracle® Oracle Enterprise Manager Ops Center Feature Reference Guide describes all features of the Oracle Enterprise Manager Ops Center software.

## Audience

This document is intended for users who require a detailed description of Oracle Enterprise Manager Ops Center features and functionality.

## 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 [Oracle Enterprise Manager Ops Center documentation library](#).

Oracle Enterprise Manager Ops Center provides online Help. Click Help at the top-right corner of any page in the user interface to display the online help window.

For the latest releases of these and other Oracle documentation, check the Oracle Technology Network at: <http://www.oracle.com/technetwork/documentation/index.html#em>

## Conventions

The following text conventions are used in this document:

Convention	Meaning
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

---

<b>Convention</b>	<b>Meaning</b>
monospace	Monospace type indicates commands within a paragraph, code in examples, text that appears on the screen, or text that you enter.

---

# Part I

---

## Getting Started

Part I contains the following chapters:

- [Chapter 1, "Introduction"](#)
- [Chapter 2, "Asset Management"](#)
- [Chapter 3, "Jobs"](#)



---

---

# Introduction

Oracle Enterprise Manager Ops Center is Oracle's comprehensive solution for managing the assets in your data center: operating system, firmware, and BIOS configuration, bare metal and virtual machine provisioning, hardware monitoring, automatic My Oracle Support service request generation, and performance and energy management.

## Oracle Enterprise Manager Ops Center in the Data Center

After the assets have been discovered and brought under the management of the software as described in the *Oracle Enterprise Manager Ops Center Administration Guide*, you can monitor, configure, provision, and update the assets throughout their lifecycle from a single console, regardless of where the asset is located. You can see the status of all assets and you can drill down to see details of a specific asset. You can track an individual asset's status right now and you can view the history of all the assets of that type. If an asset reports an incident, you can track the progress of any investigation or service requests. You can deploy new assets in a manner consistent with the existing assets because you use profiles to set the attributes and plans to deploy the profiles to one target or many targets.

## Roles and Connection Modes

Your ability to perform an operation is affected by the role assigned to your user account and by the connection mode of the product software:

- All the actions that are included in your role are available in the Actions pane. When you must accomplish a task and a necessary action is not available, your administrator can add the role to your user account. When you log in again, the action is available.

The required roles for using a feature are listed in its chapter. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

- When the software is in Connected mode, any deployment plan and profile that relies on images and packages uses the current images and packages downloaded from Oracle and vendor sites to the Enterprise Controller. If your site uses the product software in Disconnected mode, the images and packages in your local knowledge base do not change until your site acquires them.

Changing the connection mode can be done easily and temporarily. See the *Oracle Enterprise Manager Ops Center Administration Guide* for the procedure for changing the connection mode.

## User Preferences and Roles

Oracle Enterprise Manager Ops Center enables you to customize the user interface by setting your own user preferences.

### Start In and Start Page Preferences

Oracle Enterprise Manager Ops Center caters to select any drawer of the Navigation pane to be displayed as the default view upon your log in. At the next login through your user name, the home page displays the details of the drawer of Navigation pane that you have selected as your default view. For example, when you select assets from the Navigation pane, then you can also select the sub-option for assets to be displayed as the default view on start up. Your personal preferences overrides the preferences that were previously set for your role.

### User Interface Preferences

Oracle Enterprise Manager Ops Center enables you to use Display preferences to display any specific drawer from the Navigation pane at your start up view of the user interface. When you log into the user interface, the selected drawer and sub-option are displayed. By default, the Assets and Administration drawers cannot be hidden. When you select Assets for display, then you can also choose a default tab to display.

Time interval lets you define a definite length of time marked off by two instants. Time interval has the following options:

- Session timeout – This option lets you set the timeout for your user interface session. The default value is 30 minutes. You can set the value for session timeout anything in the range in between 5 to 120 minutes.
- Console timeout – This option lets you set the timeout for the serial console of managed assets. The default value is 120 minutes. You can set the value for console timeout anything in the range in between 5 to 120 minutes.
- Connectivity check interval – This option lets you determine how often the software checks access to the Internet, Knowledge Base, and My Oracle Support Services. The default value is 15 minutes and the minimum value is 1 minute.
- Table refresh frequency – This option determines how often the tables in the user interface refresh their data. The default value is 30 seconds and the minimum value is 10 seconds.
- Job status popup duration – This option determines after how long the job completion popup is displayed when a job is completed. The default value is 5 seconds.

### Membership Graph Preferences

As a user, you can also select the default display preferences for Membership Graph. You can set the display preferences for the orientation as left, right, top, and bottom. You can choose the icon size as small or large and the level of depth for the assets to be displayed in Membership Graph.

### User Preferences Summary

The User Preferences Summary displays a summarized history of the preferences that you have selected for your user preferences. You can view your set preferences for the start page, time intervals, asset default tab, and the Membership Graph.



## Role Preferences

Oracle Enterprise Manager Ops Center lets you set preferences for a role. On the start up of the user interface, you can set the display preferences, time interval settings, and an asset to be displayed for a defined role.

You can also set the preferences of the membership graph through selecting the depth, icon size, and orientation for the selected role.

## How To Use This Collection

All the documentation for the Oracle Enterprise Manager Ops Center 12c Release 1 software is located at this site: <http://www.oracle.com/pls/topic/lookup?ctx=oc121> including end-to-end examples located on the How to tab.

This document is divided into parts, not all of which will be relevant to your site's activities or your role in the data center. Within each part, this document describes the capabilities of the product software, organized by feature. Where it is practical, all information about a feature is discussed in the same chapter. To avoid repetition, links have been added to other chapters in the document and to the How To library.

When you open a document from the [Oracle Technical Network web site](#), you can use the site's Search feature to search the entire library of product documents or this specific document. The site can also convert the documents to PDF, EPUB, and Mobipocket file formats for download.



---

---

## Asset Management

Asset management is the process through which you discover your assets and organize them using groups and tags.

The following features and topics are covered in this chapter:

- [Introduction to Asset Management](#)
- [Roles for Asset Management](#)
- [Actions for Asset Management](#)
- [Location of Asset Management Information in the User Interface](#)
- [Discovering and Managing Assets](#)
- [Using Tags](#)
- [Using Groups](#)
- [Related Resources for Asset Management](#)

### Introduction to Asset Management

Asset management is the process through which Oracle Enterprise Manager Ops Center begins to manage and monitor your assets, which includes server hardware, chassis, racks, network equipment, operating systems, virtualization software and clustering software. Discovering and managing your assets is a prerequisite for almost every action in the software.

### Roles for Asset Management

[Table 2–1](#) lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task. See *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 2–1** *Asset Management Roles and Permissions*

Task	Role
View Assets	Read
Add Assets	Asset Admin
Find Assets	Asset Admin
Create Discovery Profile	Asset Admin
Update Management Credentials	Security Admin

**Table 2–1 (Cont.) Asset Management Roles and Permissions**

<b>Task</b>	<b>Role</b>
Edit Asset Attributes	Asset Admin
Edit Access Points	Security Admin
Delete Assets	Asset Admin
Edit Tags	Asset Management
Create Group	Asset Admin
	Exalogic Admin
Edit Group	Asset Admin
	Exalogic Admin
Move Group	Asset Admin
	Exalogic Admin
Add or Remove Assets From a Group	Asset Admin
	Exalogic Admin
Delete Group	Asset Admin
	Exalogic Admin

## Actions for Asset Management

You can perform a variety of asset management actions, depending on the needs of your environment:

- Add Assets by Declaring Servers for OS Provisioning
- Add Assets by Declaring Servers for Service Processor Configuration
- Add Assets Using a Discovery Profile
- Find Assets
- Create a Discovery Profile
- Edit a Discovery Profile
- Copy a Discovery Profile
- Delete a Discovery Profile
- Install Agent Controllers From the Command Line
- Update Management Credentials
- Edit Asset Attributes
- Delete Assets
- Use Access Points

## Location of Asset Management Information in the User Interface

Asset Management actions and information are located in several sections of the user interface.

**Table 2–2 Location of Asset Management Information in the BUI**

To Display:	Select:
Asset Discovery and Management actions	Expand Assets in the Navigation pane.
Discovery Profiles	Expand Plan Management in the Navigation pane, then select Discovery in the Profiles and Policies section.

## Discovering and Managing Assets

Assets that have been discovered and managed by Oracle Enterprise Manager Ops Center can be monitored and targeted with jobs. You can discover assets by using specific discovery criteria, by running a search for service tags, or by specifying server information.

After assets have been discovered, they are automatically managed, giving Oracle Enterprise Manager Ops Center full access to the assets and enabling you to monitor, update, and provision them. For an asset to be managed, it must be accessible on a network that is associated with a Proxy Controller.

Hardware assets are managed using a set of credentials. Operating systems and virtualization software can be managed using an Agent Controller installed on the system or using only a set of credentials.

Some features are not available when the operating system is managed agentlessly. [Table 2–3](#) shows the information that are available for each management type.

**Table 2–3 Information Available for Agent Managed and Agentlessly Managed Assets**

Tab or Feature	Agent Managed	Agentlessly Managed
Dashboard	Yes	Yes
Summary	Yes	Yes
Libraries	Yes	No
Storage	Yes	No
Utilization	Yes	Yes
Analytics	Yes	Limited
Virtualization Analytics for Oracle VM Server	Yes, if the guest is agent-managed	No
Virtualization Analytics for Oracle Solaris 10 Zones	Yes, if the global zone is agent-managed or if the non-global zone is agent-managed.	No
Networks	Yes	No
Incidents	Yes	Yes
Monitoring	Yes	Yes
Charts	Yes	Yes
Terminal	Yes	No
Jobs	Yes	Yes
Configuration	Yes	Yes

## Declaring Servers for OS Provisioning

The Declare Server option lets you declare one or more bare metal systems in preparation for OS provisioning, even if the systems have no service processor.

You can declare a single server by entering the server information directly into the wizard, or declare multiple servers using a discovery file containing the information for all of the servers.

To declare a single server for OS Provisioning, select All Assets in the Navigation pane, then click Add Assets in the Actions pane. Select Manually Declare a Server to be a Target of OS provisioning, then select Declare a Single Server. Enter the server information, then click Declare Asset.

- Server Name – Name of the server in the UI.
- IP Address – Specify an IP address to route the discovery to the correct Proxy Controller. You do not need to use a server's actual IP address. You can use an IP address that is on the same subnet as that of the server to be discovered.
- Model Category – Select the category in which the asset model appears.
- Model – The model of the asset.
- MAC Address and Port combination – Used to connect to the server once it is available on the network. Click the Add or Edit icons to add or edit a MAC Address/Port combination, then select the combination.

Enter a logical port name for each network interface. One of these logical port names must be GB\_0. Available logical port names are GB\_0 through GB\_11. You can also use mgmt as a management port. These logical port names will be mapped to network interfaces after the asset has been provisioned, according to the MAC addresses that you specify. If the server has only one network interface, use GB\_0.

Enter the MAC addresses of the network interfaces in the server that you want to declare.

To declare multiple servers for OS Provisioning, perform the following steps:

Create a discovery file using the format in the example below.

1. Select All Assets in the Navigation pane, then click Add Assets in the Actions pane.
2. Select Manually Declare a Server to be a Target of OS Provisioning, then select Declare All Servers.
3. Enter the location of the discovery file, then click Declare Asset.

### Example Discovery File

Here is an example of a discovery file.

```
<?xml version='1.0' encoding='utf-8'?>
<servers>
<server name="T5440" model="Sun SPARC Enterprise T5440 Server"
      guid="12345678"
      proxyHostname="server-13"
      ipAddress="10.167.46.22" >
<ethernetPort name="GB_0" mac="00:14:4F:A1:51:7F"/>
</server>
</servers>
```

The following variables can be used:

- **server name** – The name that the server has in the UI
- **model** – Must be a model supported by Oracle Enterprise Manager Ops Center
- **guid** – A unique identifier for the server
- **proxyHostname** – The Proxy Controller to be used to connect to the server
- **ipAddress** – The IP address for the server
- **netmask** – (Optional) The netmask for the server
- **gateway** – (Optional) The gateway for the server
- **unconfigured** – (Optional) Specifies that the server is unconfigured when set to true.
- **ethernetPort** – Used to connect to the server once it is available on the network. You can specify multiple ethernet ports. Includes:
  - **Ethernet port name** – The name of the ethernet port
  - **Ethernet Port mac** – The MAC address for the ethernet port

## Declaring Servers for Service Processor Configuration

The Declare Servers for Service Processor Configuration option lets you declare one or more bare metal systems in preparation for service processor configuration.

The assets being declared do not need to be physically connected to the network at the time of the discovery, because the assets produced by an asset declaration are skeletal representations of the real assets. These assets can then be targeted with service processor configuration jobs. Once the real assets are connected to the network, provisioned and discovered, they are correlated with the declared version into complete assets.

To declare unconfigured assets for service processor configuration, perform the following steps:

1. Select All Assets in the Navigation pane, then click Add Assets in the Actions pane.
2. Select Declare an Unconfigured Hardware Asset, then enter data for the servers to be declared:

**Figure 2–1 Declare Unconfigured Hardware Assets**

**Declare Unconfigured Hardware Assets** \* Indicates Required Field

You can declare one or more unconfigured hardware assets, which can then be targeted with Configure Service Processor deployment plans. Unconfigured assets are assets without set network parameters.

\* Number Of Servers:

\* Model Categories:

\* Model:

\* Server Names: Automatic Naming, Prefix:  Starting Number:  Suffix:

\* Network:

\* IP Addresses:  Enter comma-separated IP addresses and/or an IP range for the servers

\* MAC Addresses:  Enter comma-separated MAC addresses for the servers

- Number of Servers – The total number of servers to be discovered.
  - Model Categories – The model category of the servers.
  - Model – The specific model of the servers.
  - Server Names – The names of the servers, including:
    - Prefix – A prefix that appears before each server name. This field is required.
    - Starting Number – The number of the first server. The number is increased by one for each additional server. This field is required.
    - Suffix – A suffix that appears after each server name.
  - Network – The network on which the server or servers is added.
  - IP addresses – The IP addresses to be used for the servers.
  - MAC Addresses – The MAC Addresses of the servers.
3. Click Declare Asset.

## Adding Assets Using a Discovery Profile

After you have created a discovery profile, you can run it to discover and manage assets. This lets you discover assets using a pre-existing set of protocols and credentials, and manage assets consistently.

To declare unconfigured assets for service processor configuration, perform the following steps:

1. In the Navigation pane, select All Assets.
2. In the Actions pane, click Add Assets.



3. Select Add and Manage Various Types of Assets via Discovery Probes, then select a discovery profile.
4. Add or edit the IP addresses, hostnames, and credentials for the targets, then click Add Now.
  - Any hostnames must be resolvable from the Enterprise Controller to be discovered.

## Finding Assets

Service tags are small XML files containing product information. Many Oracle systems come equipped with service tags. If you have hardware assets equipped with service tags, you can discover them using the Find Assets wizard. This method lets you discover large numbers of assets quickly.

The Find Assets wizard searches known networks for service tags, then uses credentials that you specify to manage the discovered assets.

Products without service tags cannot be discovered using this method.

To find assets, perform the following steps:

1. In the Navigation pane, select All Assets.
2. In the Actions pane, click Find Assets.
3. Select Run Discovery Now.
4. When the initial discovery is complete, select the assets in each category (hardware, operating systems, and engineered systems) that you want to manage and provide credentials for them, then click Finish.

## Creating a Discovery Profile

You can create a discovery profile and then discover the assets that comply with the profile.

To create a discovery profile, perform the following steps:

1. In the Navigation pane, click Plan Management.
2. Under Profiles and Policies, click Discovery.
3. In the Actions pane, click Create Profile.

**Figure 2–2 Create Discovery Profile**

4. Enter a name for the discovery profile and select a type of asset to discover.  
If the service tag parameters have been modified for the target assets, enter the Service Tag parameters
  - Service tag passphrase - Necessary if a service tag has been configured to be encrypted.
  - Service tag port - Necessary if a service tag has been configured to use a port other than the default of 6481.
  - Service tag timeout - The default value is 20 seconds.
5. Enter the information for the target assets:
  - Hostnames or IPs - Enter a comma-separated list of hostnames or IP addresses. If you want to target an IP range, use the IP Ranges field instead.
  - Network - The managed network with which the hostnames or IP addresses are associated. This is used to route the discovery to the correct Proxy Controller. Select Automatic to route the job to the most appropriate Proxy Controller. The IP address of a target must resolve to only one known network for automatic routing to succeed.
  - IP ranges - Click the plus icon to add one or more IP ranges. Enter a name, optional description, network, and IP range for each. If you want to target specific hostnames or IP addresses, you must enter them when you run the discovery profile.
6. Enter credentials for each selected discovery profile, then view the summary and click Finish to create the discovery profile.

## Editing a Discovery Profile

You can edit an existing discovery profile.

To edit a discovery profile, perform the following steps:

1. In the Navigation pane, click Plan Management.
2. Under Profiles and Policies, click Discovery.
3. Select the profile and click the Edit Profile icon.
4. Edit any of the information in the discovery profile, then click Finish to save your changes.

## Copying a Discovery Profile

You can copy an existing discovery profile.

To copy a discovery profile, perform the following steps:

1. In the Navigation pane, click Plan Management.
2. Under Profiles and Policies, click Discovery.
3. Select the profile and click the Copy Profile icon.
4. Edit any of the information in the discovery profile, then click Finish to save the new discovery profile.

## Deleting a Discovery Profile

You can delete an existing discovery profile.

To delete a discovery profile, perform the following steps:

1. In the Navigation pane, click Plan Management.
2. Under Profiles and Policies, click Discovery.
3. Select the profile and click the Delete Profile icon. The discovery profile is deleted.

## Installing Agent Controllers From the Command Line

Use these procedures to install an Agent Controller and to register the target system.

### Before You Begin

To use the `agentadm` command, you need the following information:

- Administrative user name on the Enterprise Controller - Configuring an Agent Controller using user credentials requires using an administrative user account that exists on the Enterprise Controller. This user account provides authentication that supports Agent Controller registration. Use this user name as the argument for the `agentadm -u` option.
- Password for the administrative user name on the Enterprise Controller - If you use user credentials to configure your Agent Controller, use this password to populate the `/var/tmp/OC/mypasswd` file. Then use this file name as the argument for the `agentadm -p` option.
- The auto-reg-token registration token from the `/var/opt/sun/xvm/persistence/scn-proxy/connection.properties` file on the appropriate Proxy Controller - If you decide not to use user credentials to configure your Agent Controller software, use this token to populate the `/var/tmp/OC/mytoken` file. Then use this file name as the argument for the `agentadm -t` option.
- IP address or host name of the Proxy Controller with which you will associate the Agent Controller - Use this IP address or host name as the argument for the

agentadm -x option. Typically, you would associate the Agent Controller with the Proxy Controller that is connected to the same subnet as the target system.

- The IP address of the network interface that the Agent Controller will use for registration - Use this IP address as the argument for the agentadm -a option.

Some example agentadm commands in this procedure use the alternative administrative user name droot. In these examples, the droot user exists on the Enterprise Controller.

When you install an Agent Controller on a global zone, the Agent Controller installation installs, or upgrades to, Java Runtime Environment (JRE) 1.6.0\_21. Later versions of JRE are not affected.

### To Manually Install and Configure an Agent Controller Using User Credentials

This procedure creates a file that holds the password of the administrative user for your Oracle Enterprise Manager Ops Center installation.

1. On the Enterprise Controller, change to the `/var/opt/sun/xvm/images/agent/` directory, and list the files that it contains. This directory contains the Agent Controller installation archives. For example:

```
# cd /var/opt/sun/xvm/images/agent/
# ls
OpsCenterAgent.Linux.i686.12.1.0.zip
OpsCenterAgent.Linux.i686.12.1.0.zip.sig
OpsCenterAgent.SunOS.i386.12.1.0.zip
OpsCenterAgent.SunOS.i386.12.1.0.zip.sig
OpsCenterAgent.SunOS.sparc.12.1.0.zip
OpsCenterAgent.SunOS.sparc.12.1.0.zip.sig
#
```

2. Identify the Agent Controller archive that is appropriate for the system where you intend to install the Agent Controller.
3. On the system where you want to install the Agent Controller (the target system), create a directory named `/var/tmp/OC`.

```
# mkdir /var/tmp/OC
```

4. Use scp or ftp to transfer the correct Agent Controller archive from the Enterprise Controller to the `/var/tmp/OC` directory on the target system. Respond to any authentication or confirmation prompts that are displayed. For example:

```
# scp OpsCenterAgent.SunOS.sparc.12.1.0.zip root@10.5.241.74:/var/tmp/OC
Password:
OpsCenterAgent.S 100%
|*****| 34695
KB 00:32
#
```

5. On the target system, change to the `/var/tmp/OC` directory.

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

6. Use the unzip command to uncompress the Agent Controller archive. For example:

```
# unzip OpsCenterAgent.SunOS.sparc.12.1.0.zip
(output omitted)
```

7. Run the `install -a` script in the `OpsCenterAgent` directory. For example:

```
# OpsCenterAgent/install -a
Installing Ops Center Agent Controller.
No need to install 120900-04.
No need to install 121133-02.
No need to install 119254-63.
No need to install 119042-09.
No need to install 121901-02.
No need to install 137321-01.
Installed SUNWjdmk-runtime.
Installed SUNWjdmk-runtime-jmx.
(output omitted)
6 patches skipped.
19 packages installed.
Installation complete.
Detailed installation log is at /var/scn/install/log.
Uninstall using /var/scn/install/uninstall.
#
```

8. Create an empty file named `/var/tmp/OC/mypasswd`, and set its permission mode to 400. For example:

```
# touch /var/tmp/OC/mypasswd
# chmod 400 /var/tmp/OC/mypasswd
```

9. Edit the `/var/tmp/OC/mypasswd` file so that it contains the password for the administrative user that exists on the Enterprise Controller to which the Proxy Controller is connected. The following `echo` command appends the password to the `/var/tmp/OC/mypasswd` file. Replace password with the correct password. For example:

```
# echo 'password' > /var/tmp/OC/mypasswd
```

10. Use the `agentadm` command to associate the Agent Controller with the Proxy Controller.

- Oracle Solaris OS – Use the `/opt/SUNWxvmoc/bin/agentadm` command.
- Linux OS – Use the `/opt/sun/xvmoc/bin/agentadm` command. The example commands below use the following options:
- `configure` – Causes an Agent Controller configuration operation to take place.
- `-u` – Specifies the administrative user that exists on the Enterprise Controller to which the Proxy Controller is connected. Be certain that the password that you specified in the `/var/tmp/OC/mypasswd` file is correct for the user that you specify for this option.

---

**Note:** The example below uses *droot* as the administrative user.

---

- `-p` – Specifies the absolute path name of the file that contains the password for the user that you specified with the `-u` option.
- `-x` – Specifies the IP address or host name of the Proxy Controller to which this Agent Controller will connect.
- `-a` – Specifies the IP address to use during Agent Controller registration. This selects the network interface that the Agent Controller will use for registration. Accept the server's certificate when prompted. For example:

```
# /opt/SUNWxvmoc/bin/agentadm configure -u droot -p /var/tmp/OC/mypasswd -x
172.20.26.218
agentadm: Version 1.0.3 launched with args: configure -u droot -p
/var/tmp/OC/mypasswd -x 172.20.26.218
workaround configuration done.
Certificate:
Serial Number: 947973225
Version: 3
Issuer: CN=flyfishing_scn-proxy_ca
Subject: CN=flyfishing_scn-proxy_Agent Controller
Not valid before: Thu Jun 19 15:36:59 MDT 1969
Not valid after: Thu Apr 19 15:36:59 MDT 2029
Certificate:
Serial Number: 1176469424
Version: 3
Issuer: CN=flyfishing_scn-proxy_ca
Subject: CN=flyfishing_scn-proxy_ca
Not valid before: Thu Jun 19 15:36:56 MDT 1969
Not valid after: Thu Apr 19 15:36:56 MDT 2029
Accept server's certificate? (y|n)
Y
Connection registered successfully.
scn-Agent Controller configuration done.
Checking if UCE Agent Controller process is still running, it may take a
couple of minutes ...
Process is no longer running
UCE Agent Controller is stopped.
UCE Agent Controller is in [online] state.
Checking if UCE Agent Controller process is up and running ...
The process is up and running.
UCE Agent Controller is started.
Added the zone configuration automation successfully.
Added the service tags recreate script successfully.
#
```

Error messages similar to *Connection cannot be registered* in the following example typically indicate problems with the user credentials that you specified in the `agentadm` command. In this example, the user `droot` was not authenticated on the Enterprise Controller. If you see an error like this, check that the user name that you supplied for the `agentadm -u` option, and the password in the file that you specified for the `agentadm -p` option, match an existing administrative user on the Enterprise Controller.

```
Accept server's certificate? (y|n)
Y
Error with connection to CRS: com.sun.scn.connmgt.SCNRegClientException:
droot, Code: 4, Code: 4
ERROR : Connection cannot be registered.
Code--2
sc-console registration failed on [2].
sc-console : User authentication error.
Error executing step : sc_console
```

If the system where you are installing the Agent Controller has multiple active network interfaces, you can use the `-a` option to specify the IP address of the interface that you want to use for Agent Controller registration. For example:

```
# /opt/SUNWxvmoc/bin/agentadm configure -u droot -p /var/tmp/OC/mypasswd -x
172.20.26.218 -a 172.20.26.128
(output omitted)
```

11. If you encountered a *Connection cannot be registered* error message from the `agentadm` command, use `agentadm` to unconfigure the Agent Controller. For example:

```
# /opt/SUNWxvmoc/bin/agentadm unconfigure
agentadm: Version 1.0.3 launched with args: unconfigure
verified sc_console command is OK
End of validation
{output omitted}
End of configuration.
```

After the Agent Controller has been unconfigured, correct the problem that was indicated by the error message, and re-run the `agentadm configure` command.

12. Use the `sc-console` command to list the Agent Controller connection. For example:

```
# sc-console list-connections
scn-Agent Controller https://172.20.26.218:21165
urn:scn:clregid:a860a6d4-6899-4bcc-9ac7-a6ebaf71c1f5:20090420171121805
#
```

### To Manually Install and Configure an Agent Controller Using a Token

This procedure uses a token to configure your Agent Controller software.

1. On the Enterprise Controller, change to the `/var/opt/sun/xvm/images/agent/` directory, and list the files that it contains. This directory contains the Agent Controller installation archives. For example:

```
# cd /var/opt/sun/xvm/images/agent/
# ls
OpsCenterAgent.Linux.i686.12.1.0.zip
OpsCenterAgent.Linux.i686.12.1.0.zip.sig
OpsCenterAgent.SunOS.i386.12.1.0.zip
OpsCenterAgent.SunOS.i386.12.1.0.zip.sig
OpsCenterAgent.SunOS.sparc.12.1.0.zip
OpsCenterAgent.SunOS.sparc.12.1.0.zip.sig
#
```

2. Identify the Agent Controller archive that is appropriate for the system where you intend to install the Agent Controller.
3. On the system where you want to install the Agent Controller (the target system), create a directory named `/var/tmp/OC`.

```
# mkdir /var/tmp/OC
```

4. Use `scp` or `ftp` to transfer the correct Agent Controller archive from the Enterprise Controller to the `/var/tmp/OC` directory on the target system. Respond to any authentication or confirmation prompts that are displayed. For example:

```
# scp OpsCenterAgent.SunOS.sparc.12.1.0.zip root@10.5.241.74:/var/tmp/OC
Password:
OpsCenterAgent.S 100%
|*****| 34695
KB 00:32
#
```

5. On the target system, change to the `/var/tmp/OC` directory.

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

```
#
```

6. Use the `unzip` command to uncompress the Agent Controller archive. For example:

```
# unzip OpsCenterAgent.SunOS.sparc.12.1.0.zip
(output omitted)
```

7. Run the `install -a` script in the `OpsCenterAgent` directory. For example:

```
# OpsCenterAgent/install -a
Installing Ops Center Agent Controller.
No need to install 120900-04.
No need to install 121133-02.
No need to install 119254-63.
No need to install 119042-09.
No need to install 121901-02.
No need to install 137321-01.
Installed SUNWjdmk-runtime.
Installed SUNWjdmk-runtime-jmx.
(output omitted)
6 patches skipped.
19 packages installed.
Installation complete.
Detailed installation log is at /var/scn/install/log.
Uninstall using /var/scn/install/uninstall.
#
```

8. On the Proxy Controller that will communicate with this Agent Controller instance, examine the `/var/opt/sun/xvm/persistence/scn-proxy/connection.properties` file. The last line in this file contains the `auto-reg-token` that is required for Agent Controller registration. For example:

```
# cat /var/opt/sun/xvm/persistence/scn-proxy/connection.properties
#Generated by a program. Do not edit. All manual changes subject to deletion.

(output omitted)

trust-store=/var/opt/sun/xvm/security/jsse/scn-proxy/truststore
auto-reg-token=5b51bd9f-1700-450d-b038-ece0f9482474\ :1271743200000\ :T
#
```

9. On the system where you have installed the Agent Controller software, create an empty file named `/var/tmp/OC/mytoken`, and set its permission mode to 400. For example:

```
# touch /var/tmp/OC/mytoken
# chmod 400 /var/tmp/OC/mytoken
```

10. Edit the `/var/tmp/OC/mytoken` file so that it contains the `auto-reg-token` string from Proxy Controller with the following changes:

- Remove the `auto-reg-token=`.
- Remove any backslash characters from the token string. For example:

```
5b51bd9f-1700-450d-b038-ece0f9482474:1271743200000:T
```

11. Use the `agentadm` command to associate the Agent Controller with the a Proxy Controller.



- Oracle Solaris OS – Use the `/opt/SUNWxvmoc/bin/agentadm` command.
- Linux OS – Use the `/opt/sun/xvmoc/bin/agentadm` command. The example commands below use the following options:
- `configure` – Causes an Agent Controller configuration operation to take place.
- `-t` – Specifies the absolute path name of the file that contains the registration token.
- `-x` – Specifies the IP address or host name of the Proxy Controller to which this Agent Controller will connect.
- `-a` – Specifies the IP address to use during Agent Controller registration. This selects the network interface that the Agent Controller will use for registration. Accept the server's certificate when prompted. For example:

```
# /opt/SUNWxvmoc/bin/agentadm configure -t /var/tmp/OC/mytoken -x
172.20.26.218
agentadm: Version 1.0.3 launched with args: configure -t
/var/tmp/OC/mytoken -x 172.20.26.218
workaround configuration done.
```

```
Certificate:
Serial Number: 947973225
Version: 3
Issuer: CN=flyfishing_scn-proxy_ca
Subject: CN=flyfishing_scn-proxy_Agent Controller
Not valid before: Thu Jun 19 15:36:59 MDT 1969
Not valid after: Thu Apr 19 15:36:59 MDT 2029
```

```
Certificate:
Serial Number: 1176469424
Version: 3
Issuer: CN=flyfishing_scn-proxy_ca
Subject: CN=flyfishing_scn-proxy_ca
Not valid before: Thu Jun 19 15:36:56 MDT 1969
Not valid after: Thu Apr 19 15:36:56 MDT 2029
```

```
Accept server's certificate? (y|n)
y
Connection registered successfully.
scn-Agent Controller configuration done.
Checking if UCE Agent Controller process is still running, it may take a
couple of minutes ...
Process is no longer running
UCE Agent Controller is stopped.
UCE Agent Controller is in [online] state.
Checking if UCE Agent Controller process is up and running ...
The process is up and running.
UCE Agent Controller is started.
Added the zone configuration automation successfully.
Added the service tags recreate script successfully.
#
```

If the system where you are installing the Agent Controller has multiple active network interfaces, you can use the `-a` option to specify the IP address of the interface that you want to use for Agent Controller registration. For example:

```
# /opt/SUNWxvmoc/bin/agentadm configure -t /var/tmp/OC/mytoken -x
172.20.26.218 -a 172.20.26.128
(output omitted)
```

12. If you encountered a *Connection cannot be registered* error message from the `agentadm` command, use `agentadm` to unconfigure the Agent Controller. For example:

```
# /opt/SUNWxvmoc/bin/agentadm unconfigure
agentadm: Version 1.0.3 launched with args: unconfigure
verified sc_console command is OK
End of validation

{output omitted}
End of configuration.
```

After the Agent Controller has been unconfigured, correct the problem that was indicated by the error message, and re-run the `agentadm configure` command.

13. Use the `sc-console` command to list the Agent Controller connection. For example:

```
# sc-console list-connections
scn-Agent Controller https://172.20.26.218:21165
urn:scn:clregid:a860a6d4-6899-4bcc-9ac7-a6ebaf71c1f5:20090420171121805
#
```

## Using Management Credentials

Oracle Enterprise Manager Ops Center stores the credentials that are used to manage each asset. You can update, edit, and delete these credentials.

### Upgrading Management Credentials From a Prior Version

Assets that were discovered and managed in prior versions of Oracle Enterprise Manager Ops Center might not have management credentials associated with them. You can associate new or existing sets of credentials with these assets.

If a discovered asset is blacklisted, the same can be removed by updating the management credentials.

To upgrade management credentials, perform the following steps:

1. On the Navigation pane, select All Assets.
2. In the Actions pane, click Upgrade Management Credentials.
3. Select an asset category (operating systems; servers; or chassis, m-series, and switches).
4. Select one or more assets of that category.
  - To assign an existing set of credentials, select Assign existing set and then select an existing set of credentials.
  - To assign a new set of credentials, select Create and assign new set and then enter a protocol, name, and credential information.

### Updating Management Credentials

You can change the set of management credentials used by an asset or group of assets.

To update management credentials, perform the following steps:

1. On the Navigation pane, select an asset or group.
2. In the Actions pane, click Update Management Credentials.

3. Click Select to select an existing set of credentials, or click New to create a new set.

### Creating Management Credentials

You can create a new set of management credentials. These credentials can then be used to discover and manage new assets or to manage existing assets.

To create management credentials, perform the following steps:

1. On the Navigation pane, under Administration, select Credentials.
2. In the Actions pane, click Create Credentials.
3. Select a protocol, then enter a name for the set of credentials and the information required by the protocol.
4. Click Create to create the management credentials.

### Using Custom SSH Keys for OS Discovery

You can use SSH keys as an option when performing the OS discovery.

You must create SSH keys on each PC that might access the target asset and also add the SSH public key to the `~/.ssh/authorized_keys` location on the remote OS or use the hardware's web interface to upload the public keys.

1. On the Navigation pane, under Administration, click Credentials.
2. In the Actions pane, click Create Credentials.

**Figure 2–3 Create Credentials**

Oracle Enterprise Manager Ops Center - Create Credentials

Create Credentials ? ORACLE

\* Indicates Required Field

\* Name: priv

Description:

SSH

\* Authentication Type:  Password  Custom SSH Key

\* Login User: root

\* Private Key File on Proxy Controller(s): ~/.ssh/id\_rsa

Passphrase: \*\*\*\*\*

Confirm Passphrase: \*\*\*\*\*

Privileged Role: |

Role Password:

Confirm Password:

\* SSH Port: 22

Create Cancel

3. In the Name field, enter a name for the credential.
4. In the Description field, enter a description for the credential.

5. In the SSH section, select Custom SSH Key as Authentication Type.
6. In the Login User field, enter the login credential.
7. In the Private Key File on Proxy Controller(s) field, the location is set by default; change this value if you want to reference other keys.
8. In the Passphrase field, enter the passphrase that was set when the key was originally created and if it was specified.
9. In the Confirm Passphrase field, enter the passphrase again.
10. In the SSH Port field, enter the SSH port number, the default is 22.
11. Click Create.

For a nonprivileged user, enter the Privileged User role credentials in the Privileged Role and Role Password fields respectively.

### **Editing Management Credentials**

You can edit an existing set of management credentials to reflect changes to the managed assets.

To edit management credentials, perform the following steps:

1. On the Navigation pane, under Administration, select Credentials.
2. In the center pane, select a set of credentials and click the Edit Credentials icon.
3. Edit the description and the information required by the protocol, then click Update to save the changes.

### **Copying Management Credentials**

You can copy an existing set of management credentials to create a new set.

To copy management credentials, perform the following steps:

1. On the Navigation pane, under Administration, select Credentials.
2. In the center pane, select a set of credentials and click the Copy Credentials icon.
3. Edit the name, description, and the information required by the protocol, then click Copy to save the new set of credentials.

### **Deleting Management Credentials**

You can delete an existing set of management credentials. Discovery profiles that use the credentials might no longer function, and Agentless assets that are managed using the credentials must be given a new set.

To delete management credentials, perform the following steps:

1. On the Navigation pane, under Administration, select Credentials.
2. In the center pane, select a set of credentials and click the Delete Credentials icon.
3. Click OK to delete the credentials.

## **Editing Asset Attributes**

All assets have a description and a set of tags that can be edited.

The description field can be used for descriptive information about a system.

Tags can be used to categorize assets and simplify later searches. Each tag consists of a tag name and a value.

To edit asset attributes, perform the following steps:

1. On the Navigation pane, under Assets, select an asset.
2. In the Actions pane, click Edit Asset.
3. Edit the name, description, and tags, then click Save.

## Using Access Points

An asset's access points show how Oracle Enterprise Manager Ops Center connects to the asset.

The following are possible access points:

- The discovery credentials used to discover the asset.
- The discovery credentials used to discover a related asset. For example, an access point for a service processor is the discovery credentials of its operating system.
- Agent Controller installed on the asset.
- A virtual asset's virtualization host.

To view access points, select an asset and click the Configuration tab.

To delete an access point, perform the following steps:

1. On the Navigation pane, under Assets, select an asset and click the Configuration tab.
2. Select one or more access points, then click Delete Access Point.

## Deleting Assets

The Delete Asset option uninstalls Agent Controller software if it is present, removing the asset from Oracle Enterprise Manager Ops Center. All data for the asset is removed. You delete assets to stop managing them with Oracle Enterprise Manager Ops Center.

The operating systems that support the Enterprise Controller and Proxy Controllers cannot be deleted or removed.

---

---

**Note:** Deleting a global zone also deletes its non-global zones. However, if a global zone is managed with an Agent Controller, its non-global zones continue to be managed agentlessly even if their Agent Controllers are removed.

---

---

### To Delete Assets

1. Click All Assets in the Assets section of the Navigation pane.
2. Select the asset or assets that you want to delete from the Managed Assets or Unprocessed Assets tabs.
3. Click Delete Asset.
4. If the assets do not have Agent Controllers, a confirmation window is displayed. Click Delete. A job is launched to delete the assets.

5. If the assets have Agent Controllers, the Management Credentials page is displayed. Provide management credentials using one of the following methods:
  - Click New to create a new set of credentials. Enter a name and the credential information, then click Ok.
  - Click Select to select an existing set of credentials. Select an existing set of credentials, then click Ok.
6. Click Next.  
The Summary page is displayed.
7. Review the summary, then click Finish.

## Special Discovery and Management Procedures

Most assets can be discovered and managed using the procedures in [Discovering and Managing Assets](#). However, some types of assets must be discovered or managed using special procedures. Use these procedures when any of the following asset types is discovered or managed.

- Oracle Solaris 11 – You can discover and manage Oracle Solaris 11 operating systems only if the Enterprise Controller and Proxy Controller are installed on Oracle Solaris 11 and the Oracle Solaris 11 Update Library is configured.
- Microsoft Windows – You must enable Windows Management Instrumentation (WMI) on Microsoft Windows systems before discovering them. Once WMI is enabled, they can be discovered normally.
- Sun SPARC Enterprise M-Series Servers: – You must ensure that user privileges and the status of each dynamic system domain are correct before discovering a Sun SPARC Enterprise M-Series server.
- Sun ZFS Storage Appliances: – You must discover both the storage appliance and its service processor, and follow special procedures to manage them.
- Oracle Solaris Clusters:– You must discover and manage Oracle Solaris Clusters in a specific order so that Oracle Enterprise Manager Ops Center can manage the entire cluster.

### Windows Systems

Microsoft Windows systems can be discovered and managed using normal discovery and management procedures. However, before the system can be discovered, the Windows Management Instrumentation (WMI) utility must be configured and have access through the Windows Firewall or Internet Connection Firewall.

#### To Enable WMI

This procedure allows the Enterprise Controller or a Proxy Controller to connect to the target system.

1. Log in to the WMI on the target host.
2. Click Administrative Tools, then click Computer Management.
3. Expand Services and Applications.
4. On WMI Control, right click Properties.
5. Click the Security tab.
6. Click the Security button.

7. Add the monitoring user (if needed).
8. Click the checkbox to allow Remote Enable.

### To Allow WMI Through the Windows Firewall

This procedure allows WMI to send data through the target system's firewall.

1. Go to the command prompt on the target system.
2. Use the `netsh` command to allow WMI to send data through the firewall.

- On Windows Server 2008 R2, use the following command:

```
netsh advfirewall firewall set rule group="remote administration" new
enable=yes
```

- On other Windows systems, use the following command:

```
netsh firewall set service RemoteAdmin enable
```

## Servers

Most servers can be discovered using the normal discovery and management procedures. However, certain servers must be properly configured before they can be discovered and managed.

**Discovering a M-Series Server** To discover, manage, provision, and update a Sun or Fujitsu SPARC Enterprise® M3000, M4000, M5000, M8000, or M9000 server (SPARC Enterprise M-series servers), you monitor its XSCF service processor and its dynamic system domains.

The SPARC Enterprise M-series servers have a dedicated processor for system control that is independent of the system processor. A SPARC Enterprise M3000, M4000, and M5000 server has one service processor. The SPARC Enterprise M8000 and M9000 servers, each have two service processors; however, only one service processor is active at a time. The eXtended System Control Facility (XSCF) firmware runs on the dedicated service processor. The firmware manages hardware configuration, monitors cooling system (fan units), domain status, and error status, and can power on and power off peripheral devices.

The XSCF firmware also has the ability to create dynamic system domains. Each domain is a logical unit that can function as a system. An Oracle Solaris OS can operate in each domain.

### To Discover a SPARC Enterprise M-Series Server

To discover a Sun or Fujitsu SPARC Enterprise® M3000, M4000, M5000, M8000, or M9000 server, run an Add Assets Using Discovery Profile job for the XSCF service processor. The discovery job discovers the XSCF service processor and its dynamic system domains.

Perform the following tasks to discover this type of asset:

1. In the XSCF service processor, create a user account with `platadm` privilege if one does not exist.
2. Ensure that user privileges and the status of each dynamic system domain are correct.
3. Check the status of each dynamic system domain, using the `showdomainstatus -a` command. Oracle Enterprise Manager Ops Center can only discover domains that do not have a "-" status.

4. Log in to the XSCF shell from an XSCF-LAN port or from the serial port.
5. Discover the system using the Add Assets Using a Discovery Profile procedure.

A Discovery job is launched. Dynamic system domains and the XSCF service processor are discovered at the same time.

When the job is complete, the domains and the XSCF service processor are displayed in the Managed Assets tab. The XSCF service processor is listed as a chassis and the dynamic system domains are listed as blade servers under the chassis.

## Storage

The Sun ZFS Storage Appliance family of products provides rich and efficient data services for file and block storage formats. Each appliance has the Analytics feature for observing the condition and behavior of the appliance in real time and the ZFS Hybrid Storage Pool that uses Flash-memory devices, high-capacity disks, and DRAM memory within a data hierarchy. The hybrid storage pool provides solid-state response time with spinning disk capacity.

When you use Sun ZFS Storage Appliances within the Oracle Enterprise Manager Ops Center environment, you not only manage the appliance as one of the assets in the data center, but you also can make use of the storage provided by these appliances as a backing storage for storage libraries and software libraries.

To manage a Sun ZFS storage appliance, you must prepare the appliance and discover both the storage appliance and its service processor.

1. Create a user account on the appliance with the username *ocuser* with the basic administration role and the following permissions and characteristics:
  - Permission to configure alert filters and thresholds
  - Permission to administer the Phone Home Service. If the user account does not have this permission, it is not possible to use the Enable Appliance Phone Home or Disable Appliance Phone Home actions.
  - Permission to power off the appliance. If the user account does not have this permission, it is not possible to power off the storage appliance remotely.
  - Permission to administer, configure and restart the SNMP service (required).

A sample user account is shown in the following figure:



Figure 2-4 Sun ZFS Storage Appliance Support

OBJECT	PERMISSIONS
alert	configure
appliance.*	powerOff
svc.scrk	administer
svc.snmp	administer, configure, restart

- User account must not be a kiosk type.
  - User account must not require session annotation.
2. Configure the Sun ZFS Storage Appliance.
  3. Configure the storage pool on the appliance.
  4. Discover both the service processor and the storage appliance using the Adding Assets Using a Discovery Profile procedure.

See the Sun ZFS Storage Appliance documentation for more information about creating user accounts.

**Discovering a Sun ZFS Storage Appliance** Because the storage appliance contains a service processor, it is possible to discover the service processor but not the appliance, discover the appliance but not the service processor, or to discover both. The recommended procedure is to discover both aspects of the Sun ZFS Storage Appliance, using either Find Assets or Discovery Profiles.

- Use Find Assets. Each storage appliance is discovered as two assets: a service processor and a storage appliance. Select both the appliance and its service processor and enter the user credentials. Oracle Enterprise Manager Ops Center displays the asset in the Storage section.
- Use Discovery Profiles to discover the storage appliance first and then discover its service processor. When you discover the storage appliance, Oracle Enterprise Manager Ops Center displays the device in the Storage section of the Assets tree. When you discover the service processor, its information is mapped to the already-discovered appliance.

---

**Note:** If you change the order of discovery, the result is the same. However, Oracle Enterprise Manager Ops Center displays a generic asset in the Server section of the Asset tree. When the appliance discovery succeeds, Oracle Enterprise Manager Ops Center removes the generic server from the Servers section and displays a new asset in the Storage section.

---

See the Sun ZFS Storage Appliance documentation for creating user accounts. To view the Sun ZFS Storage 7000 System Administration Guide, log in to the Unified Storage System software interface and click Help in the top right corner of any screen.

### Oracle Solaris Cluster

Discovering and managing an Oracle Solaris Cluster has some specific requirements. The discovery and management must be performed in the correct order.

---

**Note:** Do not configure a new zone cluster or add a new global node during the discovery and management process.

---

#### To Discover an Oracle Solaris Cluster

1. Verify that all global nodes in the cluster are in cluster mode.
2. Discover all of the cluster's global nodes using a discovery profile. You must provide both ssh credentials and JMX credentials for each global node.
3. Discover the cluster using a discovery profile.

## Using Tags

A tag is a set of information attached to an asset. Each tag consists of a tag name, which is drawn from a list of values appropriate for each asset, and a tag value, which can be any text string. For example, an asset could have a tag with a tag name of `oracle.cloud.resource.creation.time` and a value of 12 June.

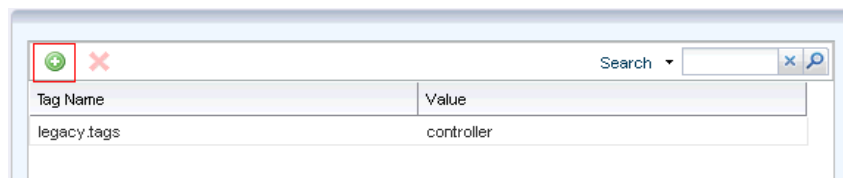
Tags can be used to associate information with assets, and to group assets based on tags or tag values. You can add tags to assets during or after discovery.

### Adding Tags

To add tags to one or more assets, perform the following steps:

1. On the Navigation pane, select an asset or group.
2. In the Actions pane, click Edit Tags.

**Figure 2–5 Add Tags**



3. Click the add icon and select a tag name from the drop-down list. Enter a tag value, then click Save.

### Viewing Tags

Tags are displayed in the dashboard tab for managed assets. Select an asset, then mouseover the tags icon in the center pane to display the tags.

## Grouping Assets Using Tags

To add assets to a group using tags, create a new group or edit an existing group using the procedures described in the [Using Groups](#) section, and create one or more rules that add assets based on tags.

## Deleting Tags

To delete tags, perform the following steps:

1. On the Navigation pane, select an asset or group.
2. In the Actions pane, click Edit Tags.
3. Select a tag, then click the Delete icon.
4. Click Save. The tag is deleted.

## Using Groups

Assets are automatically placed into system groups based on asset type. You can also create your own groups and add assets to them, either by manually adding assets or by creating rules that add assets automatically based on asset characteristics.

## System Groups and User-Defined Groups

There are two types of group. System groups are automatically generated for each category of asset. User-defined groups can contain any assets, and can be configured with rules to add assets that meet the rule criteria.

You can take any action on a group that is applicable to the assets in the group. For example, you can update Automated Service Request (ASR) contacts for all assets in a group, or target a group containing operating systems with an OS update job.

### System Groups

Oracle Enterprise Manager Ops Center automatically creates groups of major asset types called system groups. Within these system groups, a subgroup is created for each type of asset that Oracle Enterprise Manager Ops Center is managing. You can use System Groups to locate and view assets of a specific type. You can also act on System Groups, such as changing monitoring thresholds and updating management credentials.

You can view system groups by selecting them from the drop-down list at the top of the Assets section in the Navigation panel.

Oracle Enterprise Manager Ops Center creates these system groups:

- All Assets – Contains all discovered and managed assets. This is the default view of the assets section.
- Operating Systems – Contains all operating systems with subgroups for each type of operating system such as Oracle Solaris OS, Oracle Linux, Red Hat Enterprise Linux, and SUSE Linux. The subgroups are further organized by version, such as Oracle Solaris 9 and Oracle Solaris 10 software.
- Servers – Contains all hardware that can receive OS provisioning.
- Chassis – Contains all hardware that can receive firmware updates but not OS provisioning.
- Server Pools – Contains all server pools.

- Storage – Contains all storage systems.
- Racks – Contains all racks.
- Oracle Engineered Systems – Contains all Oracle Engineered Systems.
- Oracle Solaris Clusters – Contains all Oracle Solaris Clusters.

### User-Defined Groups

User-defined groups can contain any type of asset and can be organized by any criteria. You can configure rules for user-defined groups that automatically add assets with specific characteristics to the group.

You can specify the following characteristics for a user-defined group:

- **Group Name**
- **Description**
- **Group Location**
- **Group Rules** – Group rules add any assets to the group that match the attributes and rules.
- **Subgroups** – Groups can be organized hierarchically.

### Viewing Group Data

Each group can list all the assets in the group and can display data about their assets. Chassis and hardware groups display power usage information, and operating system groups display CPU, network, memory, and system load information.

You can select a group to see a dashboard page with information about the group, including:

- A group summary that shows the group's name, description, tags, location, and number of members.
- A membership graph showing the group's assets, any child groups, and any parent groups.
- A status summary showing the problems of the assets within the group.
- An asset summary showing basic data about the assets within the group.

### Creating a Group

You can organize your assets into groups to aid in management and inventory.

To create a group, click Create Group in the Actions pane, then enter the group information:

- **Group Name** - This name is displayed in the User-Defined Groups of the Navigation pane.
- **Description (optional)** – This is a description of the group that is displayed in the group's dashboard.
- **Group Location** – A group's position within the tree. You can create a group at the top level (root) or as a child of an existing user-defined group.
- **Configure Group Rules** – Use this option to specify the membership rules. Any assets that match the rules are added to the group.

- **Configure Subgroups** – Use this option to specify any existing user-defined group as a child of this group.
- **Preview Group Before Creation** – If you are configuring group rules or subgroups, select this option to see the assets and subgroups that will be added to the new group before it is created.

If you are creating a rules-based group, provide the rule information:

- **Matching Policy** – A rule can contain one or more attributes. For each rule, specify whether an asset must match all of the rule's attributes or any of the rule's attributes.
- **Asset Type** – Select the asset type that uses the rule.
- **Attribute** – Select an attribute to be considered by the rule. For example, if you select Name, the rule compares the asset's name to a given value. The available attributes vary depending on the selected asset type. You can add additional attributes to a rule using the Add Attribute icon.
- **Condition** – Select a condition for the rule. For example, if you select Contains for the Name attribute, the rule includes assets if their name contains a given value.
- **Value** – Enter a value to be used by the rule. For example, if you select Name as an Attribute, Contains as a condition, and Pod3 as a value, any asset of the specified type with Pod3 in its name is added to the group.

If you are adding subgroups, drag and drop one or more groups from the available groups list to the selected groups list.

If you chose to preview the group, view the assets and subgroups that will be added to the group. If necessary, go back and change the group rules or the list of subgroups.

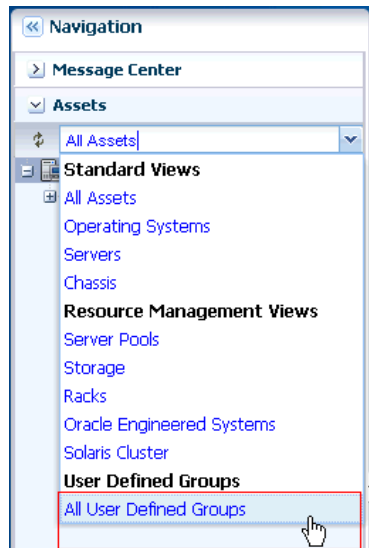
See [Appendix A](#) for a list of the asset attributes that can be used in group rules.

## Editing a Group

You can change the attributes of an existing group, including its name, description, rules, subgroups, and parent group. If you change or remove the rules of an existing group, assets added by those rules are removed if they do not match the new rules. However, assets that were added manually can only be removed manually.

To edit a group, perform the following steps:

1. On the Navigation pane, select All User Defined Groups from the Assets drop-down list.

**Figure 2–6 All User Defined Groups**

2. In the Actions pane, click Edit Group.
  - You can edit any of the group's characteristics. If you edit a group's rules, assets that were added by group rules will be removed if they do not meet the new rules, but assets that were manually added will not be affected.

See [Appendix A](#) for a list of the asset attributes that can be used in group rules.

## Adding Assets to a Group

You can place assets into user-defined groups to organize them. When an asset is added to a group, it continues to be displayed in the All Assets section. Assets can be added to any number of groups.

To add assets to a user-defined group, select the assets in either the managed assets tab of the center pane or the Assets section of the Navigation pane. Click Add Asset to Group, select the destination group, and click Add Assets to Group.

## Removing Assets from a Group

You can remove assets from any user-defined group. The assets remain in any other groups.

---



---

**Note:** If an asset was added to a group by the group's rules, it cannot be manually removed.

---



---

To remove an asset from a group, select the group. Select the asset and click Remove Asset from Group.

## Moving Assets to a Group

When you move assets to a new user-defined group, the assets are removed from the current group and added to the new group.

---

---

**Note:** If the current group has rules that match the asset you want to move, the asset is not removed from the original group.

---

---

To move assets to a new group, perform the following steps:

1. On the Navigation pane, under Assets, select All User Defined Groups.
2. Select the group that currently contains the assets.
3. Select one or more assets and click Move Asset to Group.
4. Select the destination group and click Move Assets to Group/Subgroup.

## Moving a Group

You can move a user-defined group within the hierarchy of groups, making it a child of a different user-defined group or placing it at the top level.

To move a group, select the group and click Move Group. Select a destination group and click Move Group.

## Deleting a Group

Deleting a user-defined group removes the group and all of its subgroups from the user-defined group hierarchy. It does not delete any of the assets.

To delete a group, select a group and click Delete Group in the Actions pane.

## Related Resources for Asset Management

For instructions in performing actions or to learn more about the role of this feature, go to one of the following resources:

- [Chapter 4, "Monitoring Rules and Policies"](#)
- *Oracle Enterprise Manager Ops Center Administration Guide*





This chapter describes in detail about jobs, the different roles for managing jobs, viewing jobs, and the different actions that can be performed on jobs.

The following information is included:

- [Introduction to Jobs](#)
- [Roles for Job Management](#)
- [Job Management](#)
- [Viewing Jobs](#)
- [Taking Actions on a Job](#)
- [Changing the Job Properties](#)
- [Events for Job Management](#)
- [Related Resources for Job Management](#)

## Introduction to Jobs

Any action performed by Oracle Enterprise Manager Ops Center creates a job. This job is either run on the Enterprise Controller system or picked up by a Proxy Controller to be run on a Proxy Controller or a managed asset. The progress of the job is tracked and displayed in the user interface. Each job is made up of one or more tasks, and has one or more targets; information on the job's progress on any task or target can be viewed.

The Jobs pane is located at the bottom of the user interface and displays a list of all current and historical jobs. From the Jobs pane, you can monitor the progress of current jobs and can also review historical jobs. You can view the status of all jobs, view detailed information about specific jobs, and take actions on jobs.

To view the details of the job, double-click the job in the Job Summary table. The Job Details view displays the targets of the job, and also the following information:

- Job status:
  - Running – The job is in progress.
  - Waiting for User Input – The job has started, but needs information from a user before it can be completed.
  - Failed – The job was not successful.
  - Partially Successful – Some of the job's tasks were completed successfully. This could be a job with multiple tasks, in which some tasks completed but others

failed, or a job with multiple targets, in which the job was successful for only some targets.

- Stopped – The job was stopped by the user.
- Scheduled – The job has been scheduled to run at a specific time. It might be a one-time job or a recurring job.
- Successful – The job has completed. All of its tasks were completed successfully.
- Job ID – A unique identification number for the job.
- Type of job – For example, the discovery custom type identifies a job as a result of a custom discovery action.
- Name of job – A name for the job.
- Run ID – If a job has been run multiple times, each run of the job will have a separate run ID.
- Mode of job – Simulated or Actual Run. Some jobs can be simulated. Simulated jobs verify that the necessary permissions, images, space, and other job requirements are satisfied. To perform an actual run of a simulated job, you must create a new job.
- Owner of job – The user who launched the job.
- Start / Scheduled Date – The date and time when the job was started or is scheduled to start.
- Elapsed time – The amount of time the job has been running, if the job is running. The amount of time it took for the job to complete, if the job has completed.
- Description – Description of the job.
- Failure policy – The failure policy of the job, can be one of the following:
  - Continue on Failure - if a task fails, continue to run other tasks.
  - Abort on Failure - if a task fails, all remaining tasks are aborted.
  - Rollback on Failure - if a task fails, abort all remaining tasks, and run the rollback method on the failed task and all previous successful tasks.
- Next Scheduled Time (For recurring scheduled jobs) – This option is available only in the job summary table. It displays the time when the job started. If it is scheduled to run in the future, then it displays the next run time.
- Next Scheduled Date – The next date that the job will run, or null if the job will not run again.
- Start Date – The date/time that the run of this job started.
- Creation Date – The date/time that the job was first created.
- Task Execution Order:
  - Sequential - the tasks are run one after another.
  - Parallel - all the tasks run at the same time.
  - Sequential\_on\_task - this applies to tasks that target more than one target. The task must complete on all targets before the next task will begin.
- List of tasks – This option is available on the job target details view. It displays the following:

- the task target
- the last log entry for the task, or the result of the task if the task is completed.
- the elapsed time - the amount of time that this task has been running.
- Task execution order – The execution order of the task.
- Task progress/results – Progress or result of the task.
- Event logs - Event logs are generated by tasks as they progress.

You can perform the following actions on jobs:

- View details about the job, including the status of all tasks.
- Respond to prompts during a job.
- Interrupt or stop a running job. You can re-run the job later.
- Remove a job from the history.
- Re-run a job that had partial success, failed, or was stopped.
- Create a new job with a new Job ID based on a previous job; for example, to repeat a successful complex multi-step job on another target.

## Roles for Job Management

A cloud user can only view or act on jobs that were created by the user. The cloud user cannot view jobs that were created by another user.

The following table lists the tasks that are discussed in this section and the role required to complete the task. An administrator with the appropriate role can restrict privileges to specific targets or groups of targets. Contact your administrator if you do not have the necessary role or privilege to complete a task. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 3–1 Job Management Tasks and Roles**

Task	Role
Viewing Job Status	The same as the role required to launch the job.
Viewing Job Details	The same as the role required to launch the job.
Monitoring Jobs for an Asset	The same as the role required to launch the job.
Answering Questions	The same as the role required to launch the job.
Stopping a Job	The same as the role required to launch the job.
Re-running a Job	The same as the role required to launch the job.
Copying a Job	The same as the role required to launch the job.
Deleting a Job	The same as the role required to launch the job or Job Management.
Changing the Maximum Time for a Job	Root access on Enterprise Controller system.

**Note:** If a job has multiple targets, you can only see the targets for which you have the correct role. If you do not have the role for any of the targets, the job is not displayed.

## Job Management

The job management service is responsible for managing the execution of jobs and monitoring them. The job manager communicates instructions in the task to one or more agents in the order specified by the task. The job manager monitors the state of execution, logs each successful or unsuccessful operation, and maintains the information state that will enable the job manager to report success or failure.

Within job management, you can perform the following actions, depending on what jobs have been launched and their status:

- View all jobs
- View all jobs with a specific status
- View details for a job
- Monitor jobs for an asset
- Search for jobs
- Answer questions for a job
- Stop a job
- Re-run a job
- Re-run a job on failed targets
- Copy a job
- Delete a job
- Debug a job using the OCDoctor
- Change the job properties

## Viewing Jobs

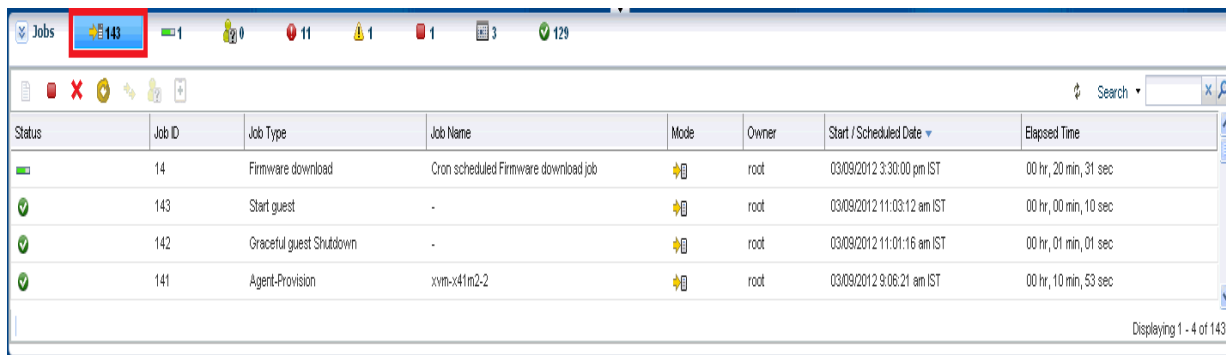
You can view jobs in different ways. The Jobs pane displays all current and past jobs that have not been deleted. You can also view the details of a specific job, and view all jobs with a specific status or for a specific asset.

### Viewing All Jobs and Jobs With Specific Status

You can view a list of all jobs run by Oracle Enterprise Manager Ops Center.

To view all jobs, perform the following steps:

1. Click and expand the Jobs pane at the bottom of the UI.
  - The Jobs pane is displayed as shown in the following figure.

**Figure 3–1 Jobs pane**

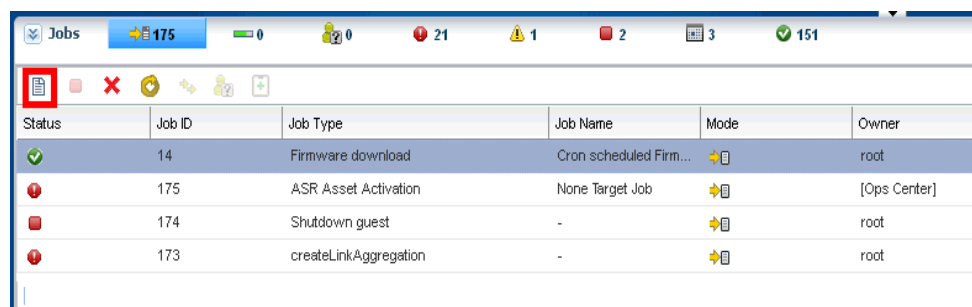
2. In the Jobs pane, click the All Jobs icon (highlighted in the previous figure).
  - All the jobs including jobs in progress, jobs waiting for user input, failed jobs, partially successful jobs, stopped jobs, scheduled jobs, and successful jobs are displayed.
3. To view jobs with a specific status (such as jobs in progress, jobs waiting for user input, failed jobs, partially successful jobs, stopped jobs, scheduled jobs, and successful jobs), click the respective job status icon. The jobs with the selected status are displayed.

## Viewing Job Details

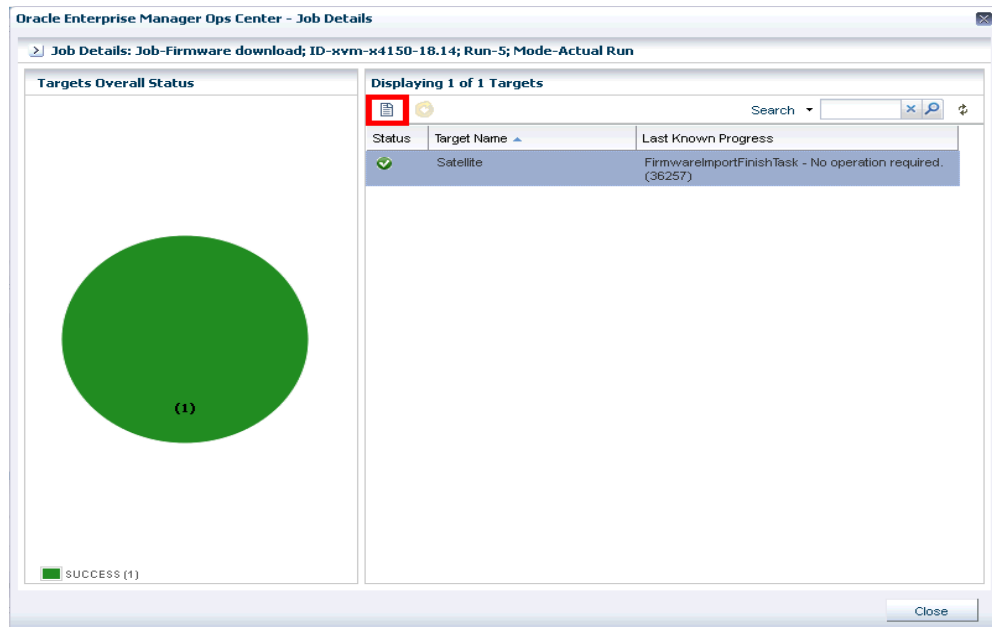
You can view detailed information about a job, including the status of the tasks that make up the job.

To view job details, perform the following steps:

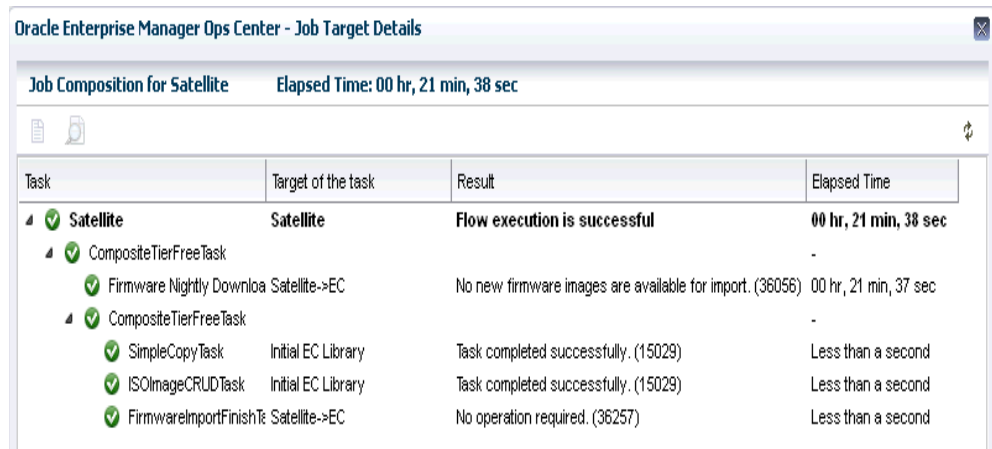
1. Select a job in the Jobs pane.

**Figure 3–2 View Job Details**

2. Click the View Job Details icon (highlighted in the above figure) or double-click the job. The Job Details window is displayed.

**Figure 3–3 Job Details Window**

- The overall status of the target is displayed on the left. On the right, a table lists all the targets.
3. Select a target and click Display Selected Target Details icon (highlighted in the previous figure). You can also double-click the target to display the target details.
    - The Job Target Details window is displayed.

**Figure 3–4 Job Target Details Window**

4. Double click a task to view the logs. The event logs and task properties are displayed.
  - The View Target Logs window displays all the task logs in a text area that can be copied from.
5. Click Export Logs to save the log as a text file.
  - Select Selected Task Target Log and click Save to save the log as a text file.
  - Select Full Job Log and click Save to save the log as a text file.

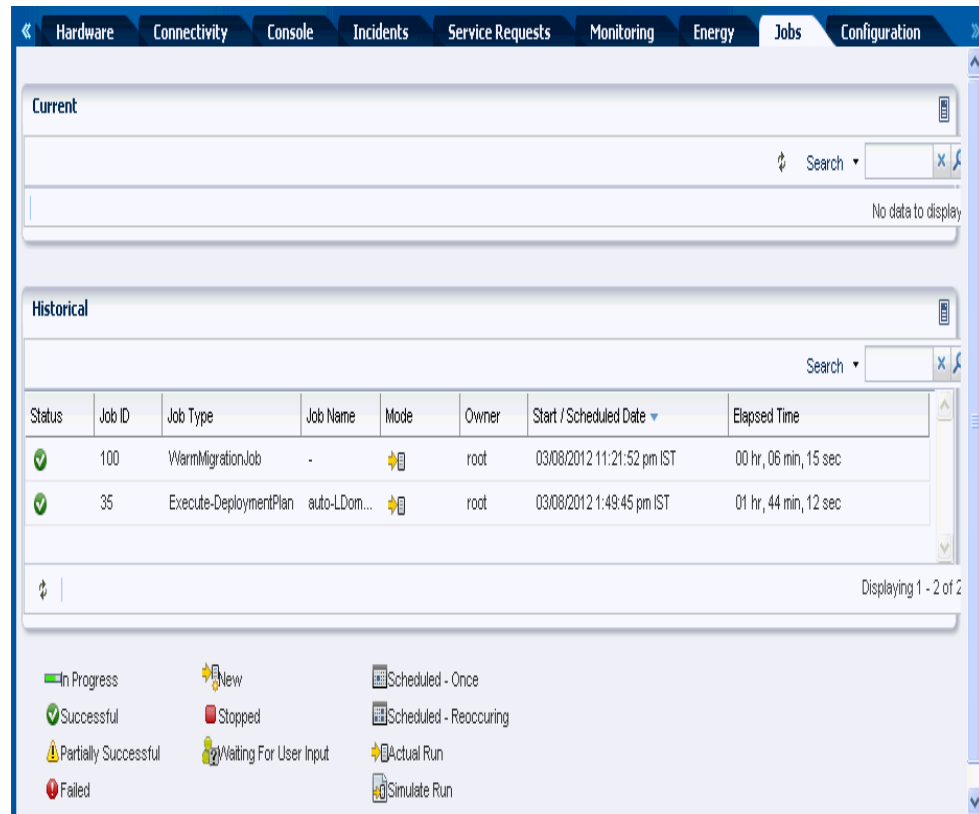
## Monitoring Jobs for an Asset

You can view jobs for a particular asset, both running jobs and jobs that have been completed.

To view only those jobs for a particular asset, perform the following steps:

1. On the Navigation pane, under Assets, select an asset.
2. Click the Jobs tab on the center pane.
  - The Current and Historical jobs are listed.

**Figure 3–5** Jobs pane in Assets View



3. Select a job and double click to view the details of the job.

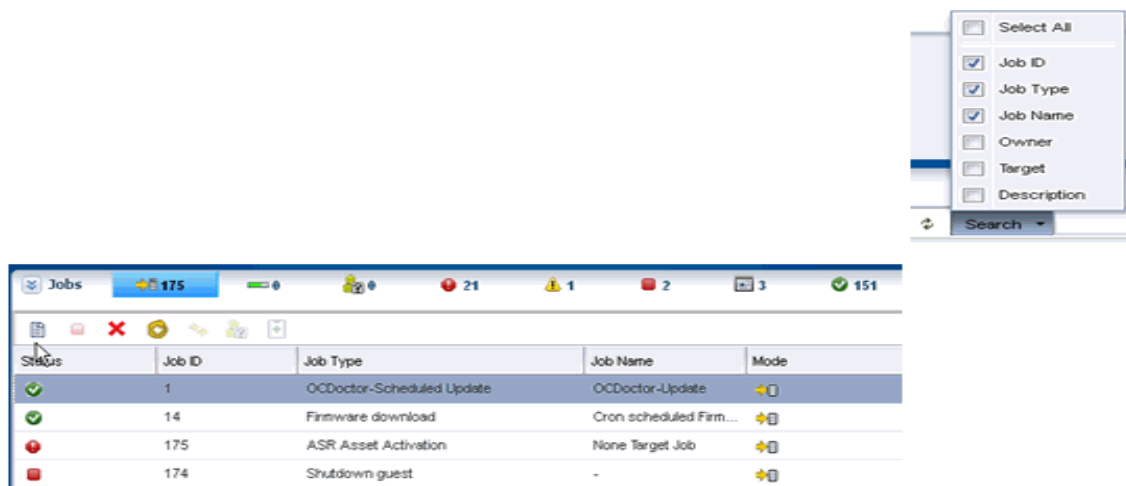
## Search for Jobs

You can search for specific jobs in any state.

To search for a particular job, perform the following steps:

1. Click Search in the upper right corner of the Jobs pane.

Figure 3-6 Jobs Search



2. Select one or more job characteristics to search, then enter a search term and click the search icon.
  - Jobs for which the selected characteristics matches or includes the search term are displayed.

## Taking Actions on a Job

You can take actions on jobs that have been launched. These actions vary depending on the current status of the job. If a job has stopped and is waiting for user input, you can answer questions and resume the job. If a job is running, you can stop it. If a job has completed, you can re-run it entirely, re-run it only on failed targets, copy it to create a new job, or delete it.

## Answering Questions

Some jobs require user input to complete. A job that requires a response has the status of Waiting for User Input. To provide user input, perform the following steps:

1. Select a job with the Waiting for User Input status.
2. Click the Answer Questions icon.
3. Select Yes or No for each question, or click Yes to All or No to All.
4. When you have answered each question, click Submit to resubmit the job using the same Job ID and Run ID.

## Stopping a Job

You can stop a job that is running. All tasks in progress are interrupted and tasks that have not yet started are aborted. The completion status of the job depends on the number of tasks that have completed, been interrupted, and not started.

To stop a job, perform the following steps:

1. Select a job that is running.
2. Click Stop Selected Jobs.
3. Click Stop Job to confirm.



## Re-running a Completed Job

If a job is completed, you can repeat the job with a new Run ID.

To re-run a job, perform the following steps:

1. Click and expand the Jobs pane at the bottom of the UI.
2. Select the failed job to be re-run.
3. Click Re-Run Selected Jobs.
4. Click Run Job.

The job is re-run with a new Run ID.

## Re-running a Job on Failed Targets

If a job is partially completed, failed, or stopped, you can repeat the job on failed or incomplete targets.

To re-run a job on failed targets, perform the following steps:

1. Select the job and view the job details.
2. Select one or more failed targets from the list of targets and click Re-Run Selected Failed Targets, then click OK.

The job is re-run with the same Run ID on the failed targets.

## Copying a Job

You can copy an OS or firmware update job, using an old job as a template for a new job.

To copy a job, perform the following steps:

1. Select the job that you want to copy and click Copy Job.

A new job wizard is displayed, using the information from the existing job.

2. Modify the job information, select a schedule, and click Submit Job.

The new job is submitted with a new Job ID.

## Deleting a Job

Deleting a job removes it from the queue entirely. It cannot be re-run or resumed, and its job details are not available.

To delete a job, perform the following steps:

1. Select the job that you want to delete.
2. Click Delete Selected Jobs, then click Delete Jobs to confirm.

---

---

**Note:** You cannot delete jobs that are running. You must first stop the job that is running and then delete it.

---

---

## Debugging a Job Using the OCDoctor

You can debug a job that has been run on a managed asset. This action runs a self-diagnosis using the OCDoctor's `--troubleshoot` option on the asset.

To debug a job, perform the following steps:

1. Select the job and click the Debug Job Using OCDoctor icon.
2. Select either Run New Self Diagnosis to run a new self diagnosis or Work on Previous Self Diagnosis to view the results of a prior self diagnosis. If you select Work on Previous Self Diagnosis, the results of the prior self-diagnosis are displayed, and you can re-run the self diagnosis.
3. Attempt to fix issues by selecting Attempt to Fix Issues, or select Collect Logs to collect log files from the target.
4. Review the summary information and click Finish to launch the self-diagnosis job.
5. Review the job details or rerun the wizard and select Work on Previous Self Diagnosis to view the data gathered by the self diagnosis.

## Changing the Job Properties

The Enterprise Controller sets several variables for job management, including the time-out values for jobs and tasks. You can modify the values to improve performance. The following are the time-out values for jobs and tasks:

- `jobtypeweight.FirmwareProvisioningJob` - This value sets the relative weight of firmware provisioning jobs. Do not modify this value unless directed by Oracle Support.
- `taskTimeOut` - This value sets the time, in minutes, after which a task will time out and fail.
- `tierTimeOut` - This value sets the time, in minutes, after which a job that has not been picked up by a Proxy Controller will fail.
- `totalAllowedWeight` - Do not modify this value unless directed by Oracle Support.
- `totalDispatchWeight` - This value sets the total weight of jobs that can be performed in parallel. Increase this value if your Enterprise Controller system can handle additional jobs.

To modify the Job Manager values, perform the following steps:

1. In the Navigation pane, select Administration, then select the Enterprise Controller and click the Configuration tab.
2. In the drop-down menu, select Job Manager properties.
3. Edit the values, then click Save.

## Events for Job Management

To follow the progress of a job, view the Job Details. If a job does not complete successfully, you can examine the following log file on Oracle Solaris system:  
`/var/cacao/instances/oem-ec/logs/cacao.*`

## Related Resources for Job Management

For instructions on performing actions or to learn more about the role of this feature, refer to the following:

- *Oracle Enterprise Manager Ops Center Administration Guide*

# Part II

---

## Configure

Part II contains the following chapters:

- [Chapter 4, "Monitoring Rules and Policies"](#)
- [Chapter 5, "Software Libraries"](#)
- [Chapter 6, "Storage Libraries"](#)
- [Chapter 7, "Networks"](#)
- [Chapter 8, "Plans and Profiles"](#)



---

---

## Monitoring Rules and Policies

This chapter discusses the types of monitoring rules and how the software uses monitoring rules and policies to generate alerts and incidents in the user interface.

The following information is included:

- [Introduction to Monitoring](#)
- [Monitoring Roles](#)
- [Monitoring Rules](#)
- [Monitoring Policies](#)
- [Location of Monitoring Rules and Policies in the User Interface](#)
- [Related Resources for Monitoring Rules and Policies](#)

### Introduction to Monitoring

Monitoring detects components or attributes of a managed resource that are not operating within specified parameters. A resource is a generic term for an asset (such as hardware or operating system), a group, a network, or a library that is managed by Oracle Enterprise Manager Ops Center.

Monitoring rules and policies define the monitoring parameters and are the main components of a complete monitoring configuration. They are defined as follows:

- **Monitoring Rules** – Define alerting conditions. You can apply one or more rules to an asset to monitor the asset and raise an alert when the an asset is operating outside the defined parameter.
- **Monitoring Policies** – A set of monitoring rules targeted to a specific asset type. Default monitoring policies contain a set of rules that are automatically applied to monitored resources. You can create your own policies and define the rules for the policy.

Monitoring typically uses the Agent Controller to gather information. When an operating system is an agentless managed system, the software monitors it remotely.

### Monitoring Roles

[Table 4–1](#) lists the roles required to complete monitoring tasks. You can restrict privileges to specific targets or groups of targets. Contact your administrator if you do not have the necessary role or privilege to complete a task. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 4–1 Monitoring Tasks and Roles**

<b>Task</b>	<b>Role</b>
View a monitoring rule	Read Policy / Plan Administrator
View a monitoring policy	Read Policy / Plan Administrator
View the association of an asset and a monitoring policy	Read Asset Administrator Policy / Plan Administrator
View the historical data of a threshold rule	Read Asset Administrator
Create, edit, or delete a monitoring rule	Fault Administrator
Create, copy, extract, edit, and apply a monitoring policy	Policy / Plan Administrator
Modify the monitoring configuration of an asset	Fault Administrator
Delete a monitoring policy	Policy / Plan Administrator
Group assets by monitoring policy	Asset Administrator
Apply a monitoring policy to an asset	Fault Administrator
Apply a monitoring policy to a group	Asset Administrator and Fault Administrator

## Location of Monitoring Rules and Policies in the User Interface

**Table 4–2 Location of Monitoring Rules and Policies in the UI**

<b>Object</b>	<b>Location</b>
Monitoring policies	Expand Plan Management in the Navigation pane, then click Monitoring Policies.
Monitoring rules	Expand Plan Management in the Navigation pane, then click Monitoring Policies. Open a policy to see the rules.
Asset-specific monitoring rules	Select an asset from the Asset view, then click the Monitoring tab.

## Monitoring Rules

Monitoring rules state the values and boundaries for an asset's activity. The set of rules is called a monitoring policy. When a monitoring policy is applied to all the assets, it enforces consistency. Each monitoring policy contains rules for threshold levels. Default policies for monitoring hardware, operating systems, and Oracle Solaris Clusters are included in the software. You can use the default policies, but you cannot edit them. To edit or add monitoring rules to a monitoring policy, you must make a copy.

Monitoring rules define the alerting conditions. Rules are associated with, and determined by, the type of managed resource. You can apply a generic monitoring rule to many different attributes, but other monitoring rules are attribute-specific, hard-coded into drivers and cannot be moved or reconfigured.

When you set a threshold, the UI displays the existing historical data for an attribute. The software might propose some default threshold values based on the analysis of

historical data, and display existing thresholds as a bar on that historical data. You can enter any threshold value.

Each managed resource has a Monitoring tab. You can add, edit, enable, disable, and remove resource monitoring rules. You can tune the rules for a specific managed resource. However, tuning the rules for a specific managed resource detaches the resource from the monitoring policy, keeping only a copy of the rules. When you modify rules in the policy, the change is not made to the rules that are associated with the resource.

Rules have Info, Warning, and Critical severity levels. Default values and severity levels are provided at installation, but you can edit the rules for your organization. For user-defined rules, you can define the time between when the alerting condition occurs and when the software generates an alert or incident. You can configure the software to send an e-mail or pager message when it identifies a Warning or Critical incident.

Rules for a specific asset are located in the Monitoring tab for the asset. This is the asset view. To display the tab, click the asset in the Assets drawer, then scroll over to the Monitoring tab in the center pane. The name of the monitoring policy applied to the asset appears at the top of the monitoring rule grid, next to the number of rules.

Rules for a specific policy are located under Monitoring Policies in the Operational Plans section of the Plan Management drawer. This is the policy view.

## System-Defined and User-Defined Rules

There are two categories of monitoring rules:

- System-defined rules – These are attribute-specific and are hard-coded into drivers. You can disable a system-defined rule, but you cannot edit, move, or reconfigure these types of rules.
- User-defined rules – These are associated with, and determined by, the type of managed resource. You can apply a user-defined rule to many different attributes.

## User-Defined Rule Parameters

The following types of editable user-defined rule parameters, also known as rule types, are available:

- Threshold – Sets an upper or lower monitoring threshold for the monitored attribute.
- Boolean Control – Sets a logical operator of true or false for the monitored attribute.
- Enumerated Control – A series of values that defines a subset of specific values among the possible values of the monitored attribute. An alert occurs when the attribute matches one of those specific values.
- Expression – Defines the variables, literals, and operators for an attribute. An expression is an instruction to execute something that returns a value.

You cannot modify all rule parameters, but most rules include some parameters that you can tune, or edit, to meet your organization's requirements.

The following are some examples of editable parameters:

- Severity level of the alert. You can define the parameters for informational, warning, and critical alerts.

- Raising and clearing values. These are threshold settings that determine when an alert is raised and cleared. These two values are always the same. For example, you can configure the software to raise an alert when a value reaches 90% and clear the alert when the value falls below 90%.
- Monitor for alert limits at specific time – Defines when you want monitoring to occur, or to not occur. You might use this parameter when a daily maintenance procedure causes an attribute to operate outside of the normal monitoring threshold, but you do not want to raise an alert. You can define a period of time when the monitors are disabled and you can perform maintenance.
- Generate alert after – Defines how long an issue occurs before an alert is generated. The number defines the time between when a threshold is exceeded and when an alert is generated. The alert is not triggered immediately. An alert is generated when the monitored attribute value is outside the threshold after the specified delay. You might use this parameter to limit false positive alerts due to a temporary condition.

## Enabled and Active Rules

Monitoring rules have two types of states:

- Enabled or Disabled – Disabling a rule removes that attribute from monitoring. You can disable and enable rules on a per asset or group basis.
- Active or Inactive – Reflects the system's state and indicates whether the software is monitoring the asset or group. When a rule is not enabled, monitoring is not active.

By default, all monitoring rules are enabled. The status appears on the Alert Monitoring Rules page, which you can access from the Monitoring tab. When Yes is in the Enabled and Active fields, the rule is enabled and active. When “No” appears in the corresponding field, a rule is disabled or inactive. [Figure 4-1](#) shows the DHCP status as enabled, but inactive.

**Figure 4-1 Enabled and Active Monitoring Rules**

Alert Monitoring Rules	Alert Limits	Enabled ?	Active ?
<b>Reachability Monitoring Rules (1)</b>			
Operating System Reachability Immediate Action: N/A		Yes	Yes
<b>ServiceAlertMonitor Monitoring Rules (1)</b>			
Service Alert Monitor Immediate Action: N/A		Yes	No
<b>Threshold Monitoring Rules (16)</b>			
Boot Env Usage Percent in a ZPool Immediate Action: N/A	Critical: 75.0 Warning: 50.0	Yes	Yes

An Enabled field appears in the list of monitoring rules for an asset. You can disable one or more rules for a specific asset. When No appears in the Enabled column, the rule is disabled.



When a rule is enabled, the active state reflects the system's actual state and indicates whether the software is using the rule. The following are some of the reasons that an enabled rule might be inactive:

- When a specific attribute is not hard-coded into the driver, monitoring is not possible for that attribute.
- The software cannot reach the resource or the attribute cannot be refreshed.
- Some type of misconfiguration, such as a missing mandatory parameter or an illegal value for a parameter.
- An internal error specific to the monitor, particularly in the case of driver-specific monitors.

You can view the rules for a specific asset or you can view the rules for a policy that is associated with one or more assets.

## Edit Monitoring Rules

Monitoring rules have pre-defined parameters. You can change the parameters, including the threshold values and the monitoring level, to meet your data center guidelines. You can define the parameters for an individual asset or for a group of assets.

You can create separate monitoring groups to consistently and efficiently define the parameters for all systems in each group. For example, you can create a group for a set of high priority systems. You edit one set of specific threshold values for all members of that group and apply a monitoring policy to the group. All members of the group are now monitored in the same way for the same values.

You can edit a monitoring rule for a specific asset or the monitoring rule for a monitoring policy. Editing the monitoring rule parameters for an individual system might be useful when a particular system is on a critical path. For example, you might consider the systems that you have the Enterprise Controller and Proxy Controllers on critical path systems, you can monitor the system continuously and create more stringent monitoring thresholds for those systems.

---

---

**Note:** When you update a monitoring rule in a policy, the monitoring configuration of all assets that are associated with the policy are updated to reflect the revised rule.

---

---

You can perform the following tasks:

- Change the values for the Warning and Critical thresholds.
- Change file system thresholds.
- Change the thresholds by system or by group.
- Set specific threshold values for different operating systems.

For example, you can create a threshold on the Enterprise Controller system that sends a warning when the file system use exceeds 90%. This alerts you when the Enterprise Controller file system is almost full.

For a threshold alert, you can change how often and for how long the software monitors the resource. You can change the threshold values.

- Alert window – Enables you to specify a period of the day when the monitoring rule is enabled. For example, when a daily maintenance operation causes a

monitored attribute to exceed a threshold, you can exclude monitoring for that time to disable monitoring for that maintenance window.

- **Generate alert after** – Enables you to configure monitoring to ignore a monitored attribute that is outside the defined monitoring parameters for a short period of time. Specifying a delay means that the software generates an alert only when the value remains above the specified limit for a given duration. It does not generate an alert when the value goes above the limit once and then immediately goes back to normal.

### To Edit a Monitoring Rule

1. Determine whether to edit a rule for a policy or for an individual asset:
  - For a policy – From the Plan Management section of the Navigation pane, click Monitoring Policies, then click a policy.
  - For an asset – From the Assets section of the Navigation pane, select an asset, then click the Monitoring tab.
2. Click the Edit Alert Monitoring Rule Parameters icon.
3. Click the entry in the Value column and type the new value. For a threshold alert, you can change how often and for how long the value is monitored, and you can change the threshold values.
4. Click Apply to submit the changes.

See [Appendix A, "Asset Attributes"](#) for more about the attributes that you can use in monitoring rules.

## Use Historical Data to Determine Threshold Limits for a Specific Asset

The software maintains a history of each monitored asset's performance against its assigned threshold rules. When you add a new threshold-type monitoring rule or modify a threshold configuration for a specific asset, it does not impact the asset's attribute history.

The asset's attribute history, which is maintained by the software, is not specifically tied to the threshold rules. It only records statistical values of the asset attributes over time. However, the threshold wizard can leverage the history to suggest meaningful threshold values. When there is historical data for the monitored attribute, a graphical representation of the historical data appears along with a proposed default threshold value based on the analysis of the data.

When modifying a threshold configuration for a specific asset, you can choose the time frame from a list of options, from one day up to six months, to display a graphical representation of the historical data. You can use this information to tune the threshold rules.

---

---

**Note:** When you edit the threshold limit for a specific asset, the software disassociates the asset from the default monitoring policy and creates a new monitoring policy for the asset.

---

---

## Add Monitoring Rules

Each monitoring policy contains a default set of rules. See [Monitoring Policies](#) for information on policies. The rule set and default parameters depend on the managed asset subtype. See [Monitoring Rules](#) for a definition of type.

When specifying an Expression monitoring rule, you use a specific language to write a logical expression that defines the alerting condition for one or more resource attributes. The logical expression includes attribute names, operators, and literal values.

When adding a Threshold, Enumerated, or Boolean monitoring rule, you must define the monitored attribute. You are not required to define the attribute for the Expression rule type. The following are some examples of monitored attributes:

- `CpuUsage.usagePercentage`
- `ProcessUsage.topMemoryProcesses.pid=*.physicalMemoryUsage`
- `DiskUsageSet.name=*.busyPercentage.`

Monitored attributes are available in the Javadoc that is in the Oracle Enterprise Manager Ops Center Software Developer's Kit (SDK). Go to the `dvd/platform/Product/components/packages` directory and install the `SUNWxvmoc-sdk.pkg` package.

Browse the available attributes and names for the monitoring framework. Attributes always start with an upper case letter, such as `SystemUpTime`, and fields always start with a lower-case letter.

For example, when you want to list the valid monitored attributes for an operating system, go to the `com.sun.hss.type.os.OperatingSystem` Javadoc page. This page displays all of the attributes of an `OperatingSystem`

Each of these attributes is either a simple type, a structure or struct-like type, or a collection type. The following are examples of the different types of attributes:

- Simple – You can use the name, such as `SystemUpTime`
- Struct-like – You can drill-down into a field of the structure type. The fields always start with a lower-case letter, such as `SystemLoad.average1Minute`
- Collection – You can drill-down into a member of the collection. For Maps you do this by specifying the appropriate 'key'. When you set the key, specify the value for the 'name' field, to get the value of a single member. For example, use the following to check the 'enabled' value of the interface named 'eth0':  
`InterfaceInfos.name=eth0.enabled`

---

**Note:** Structures are sometimes nested. For example, a struct-like attribute can contain another struct-like field, or a collection. Collections typically contain struct-like values. To drill down, continue to append the appropriate field names.

---

You can perform a query which scans across all members of a collection by specifying the '\*' wildcard value for the key or name. When you do, you must use one of the 'max', 'min' or 'like' operators. The `DomainQuery` Java class's Javadoc defines the query syntax to use. See [Appendix A, "Asset Attributes"](#) for details.

## Monitoring Policies

A monitoring policy contains the information needed to monitor a managed asset with user-defined alert configurations, including defined thresholds and alert monitors.

A policy is for a specific type of resource, such as operating systems. A more specific policy might apply to a subset of operating systems, such as all Oracle Solaris operating systems. Each monitoring policy contains a number of alert monitors for a

specific type of resource. Alert monitors watch the state of managed resources and their attributes and raise an alert when the state is outside the pre-defined thresholds.

Each Monitoring policy contains a default set of rules. The default rule set and parameters depend on the managed asset subtype. You can apply any monitoring policy to a managed asset or group of assets to change the monitoring configuration on the subset of those resources of a compatible type.

For example, you can highlight a Oracle Solaris operating system and extract a monitoring policy for an operating system. You can specify one of the following as the OS subtype for the new policy:

- Oracle Solaris 10 – Any supported Oracle Solaris 10 operating system.
- Oracle Solaris 10 Operating System – Any supported Oracle Solaris operating system, beginning with Oracle Solaris10 8/07 (update 4). You might use this subtype when you use the Oracle Solaris Zones policy.
- Oracle Solaris – Any supported Oracle Solaris operating system release.
- Operating System – Any supported Oracle Solaris, Linux, or Windows operating system.

You can use the following methods to create a policy:

- Create a new policy, then edit the policy to add rules
- Copy an existing policy and then edit it, as needed, to modify the rules
- Extract an existing policy from an asset and modify it.

You can view a policy from the asset view or the policy view. The asset view is

Extracting a Monitoring Policy is similar to copying a policy. You perform the copy policy action from the policy view and the extract policy action from the asset view. By extracting a policy from the asset view, you can be sure that the subtypes are valid for that asset type. You can change the target subtype to a more specific or a more generic eligible target type. To be eligible, the policy must be a member of a more general policy for the specified target.

## Default Monitoring Policies

When you discover and add an asset, the software applies the default monitoring policy for the asset's type immediately.

Some monitoring policies install probes or agents on managed resources, while other policies are designed to invoke arbitrary actions or scripts against the managed resource.

## Available Monitoring Policies

A monitoring policy is a collection of rules that are associated with each type of monitored asset. The policy defines the resources monitored and the rules for that asset type. You can add and edit policies and select the default policy for a specific asset type.

Go to the Plan Management section of the UI for a list of available monitoring policies. Click Monitoring Policies to display a list of all policies, the default status of the policy, and the intended asset or target type. The following types of monitoring policies are available:

- User-Defined Policies – Typically use generic rules and contain monitoring thresholds. A Operating System policy is an example of a user-defined policy that

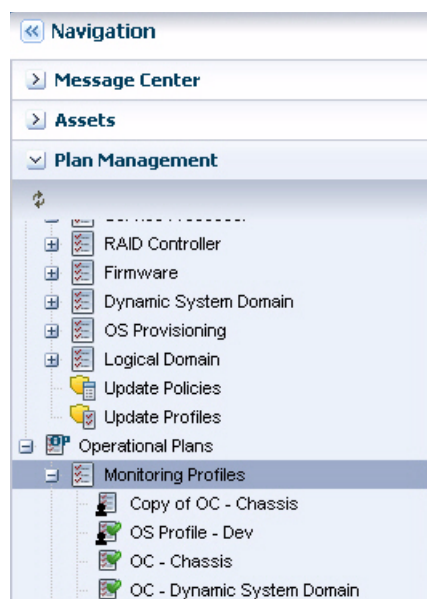
monitors the following generic operating system parameters: CPU usage, disk IO queue length and utilization percentage, file system usage, memory usage, network bandwidth utilization, and swap usage, and system load.

- System Defined Policies – A system-defined policy is read-only, you cannot disable or modify the rules defined in the policy. Typically use asset specific rules. The monitored details are determined by what is implemented on the specific asset. An example of a system-defined policy is the MSeriesChassis policy that monitors the Xsb Mode of a SPARC M-series chassis. The naming convention for system-defined policies is that the name always begins with the letters OC.

You cannot configure this type of rule, you can only turn the rule off and on.

The Navigation pane and center pane both display user-defined policies followed by system-defined policies. The icons and naming convention help to identify the type of policy in the Navigation pane. The system-defined profiles are prepended with OC. For example, in [Figure 4–2](#) Copy of OC - Chassis and OS Profile - Dev are user-defined profiles and OC - Chassis is a system-defined profile. The policies appear in different sections in the center pane.

**Figure 4–2 List of Monitoring Policies**



## Monitoring Policy Details

Each asset has a Monitoring tab. The tab displays monitoring configuration details, such as the associated monitoring policy.

When an asset is managed, the software automatically assigns a default monitoring policy to the asset. The name of the associated monitoring policy appears above the Monitoring Rules table. The field is empty when an asset is not associated with a policy. If you associate the asset with a user-defined monitoring policy and then later delete that policy, the asset might not have an associated monitoring policy.

Monitoring policy details vary, depending on the asset and associated resources being monitored. [Figure 4–3](#) is an example of a system-defined operating system monitoring policy, including the Policy Details. The Details section of the page contains information about the policy, including the name, description, and the type of policy. The policy details also describes the applicable types of assets or targets, whether the

policy is a sub-type of another policy, when the policy was last modified, and whether the policy is the default policy for the target types.

**Figure 4–3 System-Defined Operating System Monitoring Policy**

<b>Name:</b> OC - Operating System	<b>Subtype:</b> Operating System	
<b>Description:</b> Generic Operating System	<b>Nature:</b> System defined	
<b>Target Type:</b> Operating Systems	<b>Last Modified:</b> 03/19/2012 11:24:01 pm MDT	
<input checked="" type="checkbox"/> Default monitoring policy for assets matching subtype and target type		
<b>Policy Details</b>		
Alert Monitoring Rules	Alert Limits	Enabled ?
<b>BooleanControl Monitoring Rules (1)</b>		
<b>File System Reachability</b>	Critical: false	Yes
Immediate Action: N/A		
<b>Reachability Monitoring Rules (1)</b>		
<b>Operating System Reachability</b>		Yes

The following system-defined and generic monitoring policies are available:

- OC – Chassis: Monitors the chassis fan and power supply
- OC – CiscoSwitch: Monitors an Ethernet switch's power status, switch port status, and switch status.
- OC – Dynamic System Domain: Monitors the state and status of the dynamic system domains on eligible servers. Server reachability is monitored. Informational alerts are available for the power state, either on or off, and the operating system state, either running or not. The Server Port Status generates a Warning alert when the server port is disabled or down.
- OC – File Server: Monitors the file server reachability, backing devices usage percentage, storage allocation percentage, and storage usage percentage of generic file servers.
- OC – Global Zone: Monitors the DHCP status, appliance health, CPU usage, disk IO, file system usage, memory usage, network bandwidth, Swap usage, and system load of a global zone.
- OC – iSCSI Storage Array: Monitors the iSCSI storage array reachability, storage allocation percentage, storage usage percentage, volume group allocated space percentage, and volume group used space percentage.
- OC – Local Library: Monitors the storage library usage percentage for a local storage library.
- OC – Logical Domain: Monitors Oracle VM Server for SPARC guest status, including the migration status, running or not, and whether the guest is powered on.
- OC – M-Series: Monitors the Xsb Mode of a SPARC M-series chassis
- OC – NAS Library: Monitors the storage library status and storage library usage percentage of network attached storage (NAS) libraries.
- OC – Non-global Zone: Monitors CPU usage, disk IO queue length and utilization percentage, memory usage, network bandwidth utilization, and swap usage for non-global zones.
- OC – Operating System: Monitors the following generic operating system parameters: CPU usage, disk IO queue length and utilization percentage, file

system usage, memory usage, network bandwidth utilization, and swap usage, and system load.

- OC – Oracle VM Server for SPARC: Monitors Oracle VM Server for SPARC status, including the DHCP client, appliance health, and free virtual CPU (VCPU) usage.
- OC – Oracle VM Server for x86: Monitors Oracle VM Server for x86 status, including the DHCP client, appliance health, and free virtual CPU (VCPU) usage.
- OC - Power Distribution Unit: Monitors Ampere levels of rack Power Distribution Units.
- OC – Remote Oracle Engineered System: monitors remote Oracle engineered systems.
- OC – SAN Library: Monitors the status of the storage area network (SAN) libraries.
- OC – SAN Storage Array: Monitors the SAN storage array reachability and usage. The usage includes the storage allocation percentage, storage usage percentage, volume group allocated percentage, and volume group used space percentage.
- OC – Server: Monitors the following parameters on a generic server: Power status, server port status, CPU, NIC, fan, fan tray, memory, and power supply.
- OC – Server Pool: Monitors the total CPU allocation percentage, total cryptographic units allocation percentage, and the total memory usage percentage.
- OC – Solaris Cluster: Monitors the Oracle Solaris cluster install mode, reachability, and monitor.
- OC – Solaris Cluster Node: Monitors the online status, scalert.node reachability, and scalert.node alert monitor.
- OC – Solaris Cluster Zone Cluster Group: Monitors the scalert.zone cluster alert monitor.
- OC – Solaris Cluster Zone Cluster Node: Monitors the scalert.zone Cluster Node Alert Monitor
- OC – Storage: Monitors the following parameters for a generic storage device: operating system status, power status, server port status, and storage alert.
- OC – Switch: Monitors an Ethernet switch's power status, switch port status, and switch status.
- OC – Virtual Machine: Monitors the reachability of the virtual machine, if the operating system is running, and the migration status of a virtual machine.

## Apply a Monitoring Policy to a Group

### See CR 7102610 - Moved to Delta 1

You can apply, or associate, a monitoring policy with a user-defined group. When you apply a monitoring policy to a group, all applicable members of the group are associated with the policy. The policy associated with an asset appears next to the asset in the wizard. When you apply a policy to all assets in a group, the software disassociates the asset from the assigned policy and associates it with the policy that is assigned to the group.

When you remove the asset from the user-defined group, the asset is associated with the group's monitoring policy until you move it to another user-defined group that

has a different policy or you manually associate the asset with a different monitoring policy.

## Edit the Monitoring Configuration of an Asset Bound to a Monitoring Policy

Monitoring configurations contain monitoring policies and are associated with an asset type, such as an operating system. You can edit specific rules and parameters, but you cannot edit general monitoring policy properties, such as name and description after you create the policy. Editing a policy changes the monitoring configuration for all associated assets.

You can modify the monitoring configuration of an individual asset. When you create a monitoring configuration, the asset is no longer associated with the monitoring configuration and policies for that asset type. Instead, it has its own independent monitoring configuration.

When you modify a monitoring configuration for an asset, you create a policy and the asset is associated with the new created policy.

## Create a Group of Assets According to Monitoring Policy

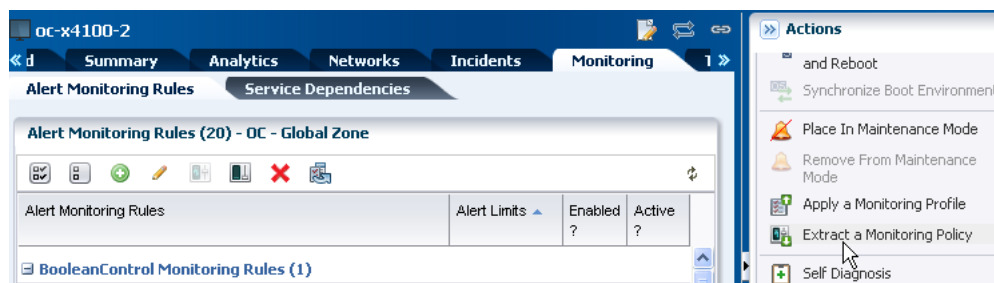
When you create a user-defined group, you can specify a rule that filters out the assets based on the name of the associated monitoring policy. You can use this to group all the assets associated with a given monitoring policy or to find assets that are not associated with a specific policy.

When viewing the monitoring configuration of an asset, you can navigate to the definition of the monitoring policy bound to the asset.

## Extract a Monitoring Policy

Extracting a monitoring policy is similar to copying a policy. Copying a policy is performed from the policy view, while extracting a policy is performed from the asset view, as shown in [Figure 4-4](#).

**Figure 4-4** Extract a Monitoring Policy Action



By extracting a policy from the asset view, you filter the possible subtypes to only those that are valid. You can change the target subtype to a more specific or a more generic eligible target type. To be eligible, the policy must be a member of a more general policy for the specified target. If a list of valid target types does not display, then the target type cannot be changed.

You can specify one of the following as the OS subtype for the new policy:

- Oracle Solaris 10 – Any Oracle Solaris 10 operating system.



- Oracle Solaris 10 Operating System – Any Oracle Solaris 10 8/07 (update 4) or higher operating system. You might use this subtype if you was to use the policy for zones.
- Oracle Solaris – Any supported Oracle Solaris operating system release.
- Operating System – Any supported Oracle Solaris, Linux, or Windows operating system.

### Extract a Monitoring Policy

1. Expand Assets in the Navigation pane, then click an asset type, such as operating system.
2. Click the Monitoring tab, then click Extract Monitoring Policy in the Action pane.
3. Enter a name and description for the new policy, then select the subtype and target type. Click Next.

**Figure 4–5 Extract Monitoring Policy**

The screenshot shows a web-based interface for creating a monitoring policy. The title is 'Extract Policy - Monitoring'. On the left, there are two tabs: 'Steps' and 'Help'. Under 'Steps', there are two items: '1. Identify Policy' (active) and '2. Summary'. The main area is titled 'Identify Policy' and contains several input fields and dropdown menus:

- Name:** A text input field containing 'S10 zone monitoring'.
- Description:** A text input field containing 'Use this policy to monitor Oracle Solaris 10 zones.'
- Subtype:** A dropdown menu with 'Subtype' as the current selection and 'Global Zone' as the selected option.
- Target Type:** A dropdown menu with 'Target Type' as the current selection and 'Operating Systems' as the selected option.

4. Click Finish to add the policy to the list of available policies.
5. To see the new policy, expand Plan Management and click Monitoring Policies. Click the policy to display details.
  - To add or remove rules or change monitoring parameters, double-click the policy in the center pane
  - To view all assets that are monitored with this policy, click View Associated Assets
  - To make this policy the default monitoring policy, click the Set as Default Policy icon

## Add or Copy a Monitoring Policy

You can add a new monitoring policy or copy an existing monitoring policy.

### Add or Copy a Monitoring Policy

1. Expand Plan Management in the Navigation pane, then click Monitoring Policies.
2. Click Copy Policy or Create Policy in the Action pane
3. Enter a name and description for the new policy, then select the subtype and target type.

4. Click Next, then click Finish to add the policy to the list of available policies.
5. To see the new policy, expand Plan Management and click Monitoring Policies. Click the policy to display details.
  - To add or remove rules or change monitoring parameters, double-click the policy in the center content pane
  - To view all assets that are monitored with this policy, click View Associated Assets
  - To make this policy the default monitoring policy, click the Set as Default Policy icon

## Delete a Monitoring Policy

You can delete user-defined monitoring policies in the Plan Management section. Resources are associated with a monitoring policy. When you delete a user-defined monitoring policy, any asset or group associated with that policy is automatically detached from the policy. However, the asset does retain the monitoring configuration that was defined by the policy.

You cannot delete system-defined policies.

## Related Resources for Monitoring Rules and Policies

For instructions in performing actions or to learn more about the role of this feature, go to one of the following resources:

- [Chapter 9, "Incidents"](#)
- [Appendix A, "Asset Attributes"](#)
- For end-to-end examples, see the How To library at <http://www.oracle.com/pls/topic/lookup?ctx=oc121&id=howto>

---

---

## Software Libraries

The following information is included:

- [Introduction to Software Libraries and Repositories](#)
- [Roles for Software Libraries](#)
- [Actions for Software Libraries](#)
- [Location of Software Library Information in the User Interface](#)
- [Knowledge Base and Parent Repository](#)
- [Using Software Libraries](#)
- [Libraries for Oracle Solaris 11](#)
- [Libraries for Oracle Solaris 10, 9, 8 and Linux](#)
- [Images](#)
- [Local Content](#)
- [Backing Up Images and Local Content](#)
- [Related Resources for Software Libraries](#)

### Introduction to Software Libraries and Repositories

Oracle Enterprise Manager Ops Center uses libraries to store and manage cached data, images, packages, and metadata. A library that stores images for provisioning operations is called a Software Library, or in the case of Oracle Solaris 11, the Oracle Solaris 11 Software Update Library. At least one software library always exists on the Enterprise Controller.

A Software Library accepts the following types of images:

- OS images that install an operating system
- Branded images that install a specialized version of an operating system
- Firmware images and the supporting metadata to update existing firmware on service processors, RAID controllers, and disks

Another type of library is a storage library. See [Chapter 6, "Storage Libraries"](#) for information about this type of library.

## Roles for Software Libraries

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 5–1 Software Libraries Roles and Permissions**

Task	Role
Set Enterprise Controller Storage Library	Oracle Enterprise Manager Ops Center Admin
Create Library	Storage Admin
Delete Library	Storage Admin
Associate Library	Storage Admin
Import image	Storage Admin
Upload image	Storage Admin
View details of an image	Storage Admin
Moving an image	Storage Admin
Edit Attributes	Storage Admin
Associate Library to Server Pool	Cloud Admin

## Actions for Software Libraries

You can perform the following actions, depending on the requirements:

- Designate a default software library
- View details of an image
- Create Library
- Delete Library
- Associate Library
- Import Image
- Upload Image
- Moving an image
- Edit Attributes
- Create Update Library

## Location of Software Library Information in the User Interface

**Table 5–2 Location of Library Information in the BUI**

Object	Location
To see the software libraries	Expand Libraries in the Navigation pane, then expand Software Libraries.
To see firmware profiles	Expand Plan Management in the Navigation pane, then click Profiles and Policies.

## Knowledge Base and Parent Repository

By default, Oracle Enterprise Manager Ops Center is configured in Connected mode. In this mode, the Enterprise Controller uses the Internet to download images and metadata from the Oracle Knowledge Base, and the Oracle Solaris 11 Package Repository. The Oracle Knowledge Base (KB) contains metadata for Oracle Solaris 10, 9, and 8 as well as Oracle Linux OS components. The Oracle Solaris 11 Package Repository includes packages of images. In both cases, the metadata is information about patch dependencies, standard patch compatibilities, withdrawn updates, downloads, and deployment rules. In addition, the KB includes URLs for each supported operating system and downloads the components from the appropriate vendor download site.

If it is necessary to use the Oracle Enterprise Manager Ops Center software in Disconnected mode, that is, without Internet access, your site can create a local version of the Knowledge Base or Repository on your site's network. In this case, the Enterprise Controller connects to the local network location to get the latest information.

## EC Library

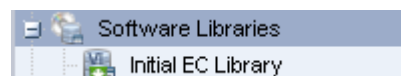
The Enterprise Controller must have at least one Software Library to store the new versions of images that are downloaded from the Oracle Knowledge Base automatically. This default EC Library is updated at the following maximum intervals between updates:

- New Oracle Solaris updates – 1 day (including security updates, Oracle Solaris Cluster updates, and standard updates)
- Oracle Solaris updates — 3 weeks
- Oracle Solaris EIS Baseline — 7 days
- Oracle Solaris Freeware Package — 3 days
- Linux Software Update (RPM) — 1 day
- Linux Service Pack — 3 weeks
- Linux Distribution New Version — 30 days

In addition to the routine download operations, you can create jobs to update assets. When you submit an update job for specific target assets, the Agent Controllers on the targets send a request to the KB through the Enterprise Controller to download the latest information.

The Initial EC Library is created when the product software is installed. At any time, you can specify a different software library to accept the automatic download operations from the Knowledge Base. The current active library is identified by its badge, a white down arrow on a green background, as shown in [Figure 5-1](#).

**Figure 5-1** Badge Identifying the Current Default Library



### To Change EC Software Libraries

To specify a different software library as the default software library:

1. Expand Administration in the Navigation pane.

2. Click Set Enterprise Controller Storage Library in the Action pane. The window lists all libraries with the current library highlighted.
3. Click the library you want to store the images from the automatic download operations.
4. Click Apply.

When the job is completed, the Library section of the Navigation pane shows the software library you selected as the default library.

## Publishers and Parent of the Oracle Solaris 11 Repository

Beginning with Oracle Solaris 11, updates are delivered in packages. With Oracle Enterprise Manager Ops Center, you do not need to create an Image Packaging System (IPS) repository.

The Oracle Solaris 11 Package Repository resides at the Oracle site: <http://pkg.oracle.com/solaris/release/>. This repository has the role of Publisher and Parent. The Oracle Solaris 11 Package repository is similar to the Knowledge Base but is only for Oracle Solaris 11 images and updates. As with the Knowledge Base, you can create a local repository.

A component of an Oracle Solaris 11 update package is the IPS Package Manifest. The manifest is the metadata for the package (such as name, description, version, and category), what files and directories are included, and the package dependencies. Packages might specify what services to restart in order to refresh some configuration on the system, specify what aliases to update for a given hardware driver, or what users and groups to create as part of the package installation process.

## Using Software Libraries

In addition to the default EC Library, you can create more Software Libraries and organize their content, according to your site's purposes. You can use a file system on the Enterprise Controller's system or a shared file system on an NFS server that the Enterprise Controller mounts. The file system on the Enterprise Controller is called a local software library. The file system on the NFS server is called a NAS software library. See [Types of Storage for Libraries](#).

When Oracle Enterprise Manager Ops Center provisions target systems with an operating system or firmware, it copies the images files from the designated Software Library to each Proxy Controller. The Proxy Controllers handle the provisioning operations. When Oracle Enterprise Manager Ops Center provisions target systems with an update to an operating system, it uses the software library named Linux and Oracle Solaris 8-10 Software Update Library or the Oracle Solaris 11 Software Update Library.

## Viewing the Contents of a Software Library

You can display the contents of the software library, its associations, and details about the disks in the software library. You can also see how the library is being monitored and any problems.

### To View the Contents of a NAS Software Library

1. Expand Libraries in the Navigation pane.
2. Click NAS Storage in Software Libraries.
3. Click a software library.

The details of the selected NAS library are displayed in the center pane in a set of tabs. The Summary tab displays information about the entire software library:

- URL — NFS
  - Size — Total storage capacity of the library
  - Used Space — Space assigned to guests and zones
  - State — State of the library
  - Access — Read-Write
  - The Library Contents table lists all the images in the library, organized by type, and includes the size and date the image was modified.
4. The Disks tab lists all disks in the library by name and description and shows the current use of each one by allocation and size.

**Figure 5–2 Disks Tab**

The following tables list all disks in the library and their current use.

Disk Name	Description	Allocated to	Size (GB)
<b>Storage Type: filesystem (5 Items)</b>			
zone_vdisk	/filesystem	ZonedOut_Clone	4.00
zone_vdisk	/filesystem	ZonedIn	4.00
zone_vdisk	/filesystem	AreWeAllZones	4.00
zone_vdisk	/filesystem	testZone1	4.00
zone_vdisk	/filesystem	ZonedOut	4.00
<b>Storage Type: raw (6 Items)</b>			
AreWeAllZone-disk-0		AreWeAllZones	6.00
ZonedIn-disk-0		ZonedIn	6.00
ZonedOut-disk-0		ZonedOut	6.00
ZonedOut_Clo-disk-0		ZonedOut_Clone	6.00
nasguest1-vdisk0	nasguest1-vdisk0	nasguest1	20.00
testZone1-disk-0		testZone1	6.00

5. To see the results of monitoring the software library, click the Incidents tab.
6. To see the attributes and values that are being monitored, click the Monitoring tab.

## Creating a Software Library

You can create a software library that uses space on a file system on the Enterprise Controller's system. This is called an Local Library. You can also create a software library that uses space on a shared file system on an NFS server. This is called a NAS Library.

---

**Note:** When you use both local and NAS software libraries, do not use the same name for the library.

---

### To Create a Local Software Library

1. Expand Libraries in the Navigation pane. The current active library is identified by its badge.
2. Click New EC Local Library in the Action pane.
3. Enter a unique name and description.
4. In the URL field, enter the location of the file system.
5. Click Create.

**To Create a NAS Software Library**

1. Expand Libraries in the Navigation pane. The current active library is identified by its badge.
2. Click New EC NAS Library in the Action pane.
3. Enter a unique name and a description.
4. Choose the type of service:
  - a. To use a unified storage appliance, select an appliance and specify the exported share to use.
  - b. To use an NFS server, enter the hostname and path for the NAS appliance.
5. Click Create.

**Maintaining the Knowledge Base and Updates**

In Connected mode, the Linux and Oracle Solaris 8-10 Software Update Library is updated on the schedule described in [EC Library](#).

**Libraries for Oracle Solaris 11**

The Oracle Solaris 11 Image Packaging System (IPS) contains the packages that you need to install, provision, and update your Oracle Solaris 11 operating system. Each IPS package has an associated manifest that describes how the package is put together. The package manifest provides basic metadata about the package (such as name, description, version, and category), what files and directories are included, and the package dependencies. Packages might specify what services to restart in order to refresh some configuration on the system, specify what aliases to update for a given hardware driver, or what users and groups to create as part of the package installation process. All software packages are hosted by a package repository and systems must connect to the repository to install software updates.

**Oracle Solaris 11 Software Update Library**

Oracle Enterprise Manager Ops Center incorporates and simplifies the IPS. The software provides a local IPS repository on the Enterprise Controller, called the Oracle Solaris 11 Software Update Library, and provides package lifecycle management. The Oracle Solaris 11 Software Update Library enables you to interact with the IPS. You can assign storage to the Oracle Solaris 11 Software Update Library, and then populate it with a local copy of the IPS.

---

---

**Note:** The host system for the Enterprise Controller must have the Oracle Solaris 11 operating system. It is not possible to initialize an Oracle Solaris 11 Software Update Library on a different Oracle Solaris operating system.

---

---

You can configure the Oracle Solaris 11 Software Update Library when you install and configure Oracle Enterprise Manager Ops Center, or you can configure the Oracle Solaris 11 Software Update Library after installation using the Create Update Library action.

The Oracle Solaris 11 Software Update Library has the following states:

- Unconfigured – Oracle Solaris 11 Software Update Library was not configured when you installed and configured Oracle Enterprise Manager Ops Center.



- Configuring – The Oracle Solaris 11 Software Update Library is in the process of being configured.
- Syncing – The Oracle Solaris 11 Software Update Library is in the process of updating and synchronizing with the IPS or is in the process of being reconfigured. The Oracle Solaris 11 Software Update Library is locked and unavailable for use when in this state.
- Ready – The Oracle Solaris 11 Software Update Library is ready to use.

If the Oracle Solaris 11 Software Update Library is in an unconfigured state, use the Initialize Oracle Solaris 11 Software Update Library action to define the port that the repository uses, assign at least 10 gigabytes (GB) of storage, and create a Local EC Library to populate the library with a local copy of the IPS. When complete, the new library appears in the Libraries section and contains three sections: Summary, Boot Image, and Packages.

---



---

**Note:** The process of initializing the library takes several hours.

---



---

To obtain updated packages for the Oracle Solaris 11 Software Update Library, synchronize with the remote parent IPS repository. The Oracle Solaris 11 Software Update Library is locked during the process and you cannot perform OS provisioning or OS update tasks.

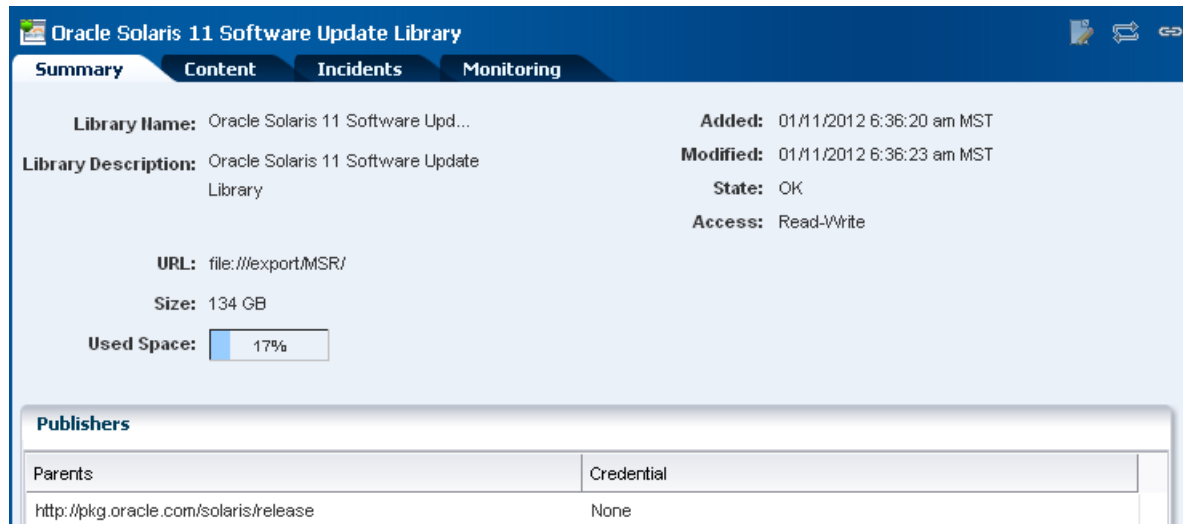
Parent repositories are the URLs of Oracle Solaris 11 content that you use to update, or sync, your local Oracle Solaris 11 Software Update Library. Other parent repositories, such as Oracle Solaris Cluster, are available. You can configure more than one parent repository and provide their credentials. For a list of all available Oracle repositories, go to [pkg-register.oracle.com](http://pkg-register.oracle.com)

A child repository is a subset, such as the release and branch for an Oracle Solaris 11 update release.

## Oracle Solaris 11 Software Update Library Summary Tab

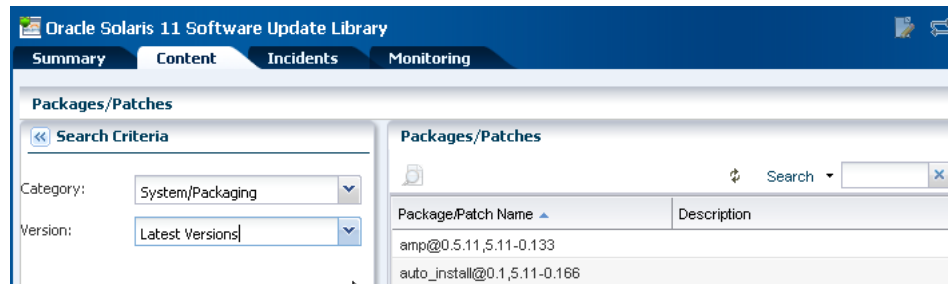
The Oracle Solaris 11 Software Update Library Summary is available after the library is configured. The summary provides an overview of the health, status, and last update. The URL listed on the Summary is the location of the Oracle Solaris 11 Software Update Library. The size is the amount of space allocated to the file system, and the used space shows how much space is used by the packages that are located in the library.

The Publisher table shows the Parents and the associated credentials. Parents are the URLs for Oracle Solaris 11 packages and content located in the Image Packaging System (IPS). These URLs are used to synchronize the information in your Oracle Solaris 11 Software Update Library with the Image Packaging System. The Parent list is created when you use the Create Parent Repositories wizard. If your site has its own local repository for Oracle Solaris 11 packages, you can update Oracle Enterprise Manager Ops Center's library from that location.

**Figure 5–3 Oracle Solaris 11 Software Update Library Summary**

## Oracle Solaris 11 Software Update Library Content Tab

The Content tab displays a list of the packages in the Oracle Solaris 11 Software Update Library with a brief description of each package. You can search for a specific package, or you can refine the search by category and version.

**Figure 5–4 Oracle Solaris 11 Software Update Library Content**

## Actions for Oracle Solaris 11 Libraries

You can perform the following actions from the Content tab:

- [Configure Parent Repositories](#)
- [Add Content](#)
- [Delete Oracle Solaris 11 Software Update Library](#)

## Configure Parent Repositories

You can manage publishers for the parent repository and synchronize the Oracle Solaris 11 Software Update Library with the parent. You can manually synchronize the repositories at any time, or you can create a recurring synchronization schedule to automatically synchronize the Oracle Solaris 11 Software Update Library during non-peak hours. In the Configure Parent Repositories wizard, you create a list of parent repositories and associated credentials that you use to update the Oracle Solaris 11 Software Update Library. You can update the Oracle Solaris 11 Software Update Library manually, or schedule updates during off peak hours.

## Add Content

You can define a parent repository and add content to the Oracle Solaris 11 Software Update Library manually by using the Add Content action. The parent repository URL and credentials are not saved when you use this action. To save a list of repositories, use the Configure Parent Repository action.

## Delete Oracle Solaris 11 Software Update Library

You can delete the library from the UI and keep its packages and content, or you can delete the library and all of its contents.

## Libraries for Oracle Solaris 10, 9, 8 and Linux

Update Profiles and any profiles you create that provision an OS or firmware image rely on the contents of a software library. For Oracle Solaris 10, 9, and 8 and for Oracle Linux, a dedicated software library called Linux, Solaris 8-10 Software Update Library contains the packages, updates, and site-specific scripts and configuration files for these operating systems. For each OS, this software library organizes its contents in the following categories:

- Clusters (groups of Oracle Solaris packages)
- Configuration files
- Hardware
- Local
- Local Packages
- Local RPMs
- Notifications
- Packages
- Patches
- Post-actions
- Pre-actions
- Probes
- Recommended Software Configurations
- Oracle Solaris Baselines

You can change the display of the contents of the library according to the OS distribution, the category, the type of view, and the version.

See [Images](#) for information about managing the content in the library.

See [Local Content](#) for information about managing the content of the local categories.

## Images

In most cases, all the images you need are downloaded from the Oracle Knowledge Base. However, you can also create images within Oracle Enterprise Manager Ops Center or obtain them from a location external to Oracle Enterprise Manager Ops Center and then import or upload them into Oracle Enterprise Manager Ops Center.

Oracle Enterprise Manager Ops Center manages the following categories of images:

- Firmware image - In Oracle Enterprise Manager Ops Center, a firmware image consists of the hardware's firmware, the instructions to use the firmware, its platform, and its software dependencies. These images are stored in the Software Libraries. The following firmware types are supported:
  - Service Processor firmware
  - Chassis firmware
  - Power distribution unit firmware
  - Storage Component firmware updates firmware on RAID Controllers, Expanders and Disks. The maximum size of a firmware image is 20 MB.
- OS image – An OS image contains an entire operating system. A subset of OS images are branded images, which install an operating system that is optimized for a specific purpose and can also install applications. For example, a branded image for Oracle Solaris 9 can be installed in a nonglobal zone of a system running Oracle Solaris 10. The maximum size of an OS image is 2 GB. These images are stored in the Software Libraries.
- ISO image – The image, also called a disk image, contains uncompressed directories and files of any type. This is the image that resides on removable media. It can be an application or data or both. While the firmware and OS images are stored in one of the dedicated update libraries, these images can be stored in other software libraries. When you create a profile for these images, you specify the software library where it is located. The maximum size of an ISO image that you can transfer using browser operations is 2 GB. If the image is larger than 2 GB, move the file manually to the Enterprise Controller's system and then import it.

---

---

**Note:** Another type of image is guest metadata. These images are stored in the Storage Libraries and have a different purpose. This image contains the configuration information for a virtualization host's guest, its operating system, and the applications used by a virtualization host's guest, either a logical domain or a nonglobal zones, depending on the type of virtualization host.

---

---

## Images for OS Provisioning

OS images provision both hardware servers and virtualization hosts with an operating system. In addition to being grouped as packages, updates, Oracle Solaris OS images are also grouped into baselines. You import OS images from existing ISO files. OS images for virtualization hosts are provided as ISO files that you import in the same manner as Oracle Solaris or Linux OS images.

### Requirements for OS Images

- An OS image must be in an image file that has the ISO format. If the image is not in an ISO file, create the file. For example, on an Oracle Solaris system, the following command collects all OS component files on the auto-mounted file system into an ISO file.

```
# mkisofs -o <name_of_OS.iso> -J -R /cdrom/<name_of_OS>
```

- The Oracle Enterprise Manager Ops Center software loads one ISO file per operation. If an ISO file spans more than one CD, combine the content on one DVD.
- An ISO file cannot be made from Oracle Solaris installation CDs.

**Table 5–3 Types of Images for Each Operating System**

Operating System	Location of Images
Oracle Solaris 11	Oracle Solaris 11 Software Update Library
Oracle Solaris 10, 9, 8	Linux and Oracle Solaris 8-10 Software Update Library
Oracle Linux	Linux and Oracle Solaris 8-10 Software Update Library
JumpStart Enterprise Toolkit	JumpStart Enterprise Toolkit (JET) is available for Oracle Solaris 8, 9, and 10.

## Images for Firmware Updates

Firmware images provision hardware assets and are grouped as packages or updates. They are created by their manufacturers and must be downloaded from vendor web sites or uploaded from their media. A firmware image is a copy of the vendor's firmware file and metadata for the firmware, such as the platform it is used on and any software dependencies.

When you import a firmware image, you might be required to provide metadata to complete the image file. You can usually find the information in the image's README file. You must provide the firmware type, the systems that the firmware supports, the version of the firmware, and any other firmware images that this firmware image depends on.

### Example 5–1 Example of Firmware Metadata

The following is an example of a README file for ALOM-CMT firmware, where a single binary is deployed to the Service Processor.

- To determine the type and version of the firmware update:

```
Latest Sun System Firmware(6.1.2):
-----
System Firmware 6.1.2 Sun Fire[TM] T2000 2006/01/20 18:19
ALOM-CMT v1.1.2 Jan 20 2006 18:06:10
VBSC 1.1.1 Jan 20 2006 17:56:19
Reset V1.0.0
Hypervisor 1.1.0 2005/12/15 11:10
OBP 4.20.0 2005/12/15 16:48
Sun Fire[TM] T2000 POST 4.20.0 2005/12/15 17:19
```

- To determine the models supported:

```
This README is intended for users who wish to
upgrade the firmware in their Sun Fire T2000.
```

- To determine if the system needs to be powered off before updating the firmware:

```
a)To update the Sun System Firmware, the system must be powered off (i.e. in
standby mode).
```

From this README file, you can identify the following metadata:

- Available platforms - Sun Fire T2000
- Type - VBSC
- Version - 1.1.1
- Require power off - Yes

For this example, the VBSB firmware subcomponent/type with version 1.1.1 was used. You can use any of the other types such as ALOM-CMT:1.1.2 or OBP:4.20.0. However, you must ensure that the version specified is always the firmware subcomponent/type.

## Uploading or Importing ISO Images

To provision firmware or an OS, you use a deployment plan to direct Oracle Enterprise Manager Ops Center to retrieve the images from the appropriate software library and install them on the targeted assets. Each time you import an image, a profile is also created with the same name. This default profile can be used in deployment plans but, as a good practice, rename a copy of this profile for use in deployment plans and leave the original profile with its original name in the library.

To use an image in a deployment plan, the image must be in one of the Oracle Enterprise Manager Ops Center's software libraries. You upload an image or import an image, depending on where the image resides. In both cases, you are moving the image from a location external to Oracle Enterprise Manager Ops Center's management into one of its libraries.

- If the image resides on the Enterprise Controller's system, import the image.
- If the image does not reside on the Enterprise Controller's system, upload the image.

See the procedures in Keeping Your Firmware Up-to-Date in the [How To library](#)

## Working with Firmware for Power Distribution Units

The firmware for a PDU consists of two files, one for the firmware and one for the management software of the PDU. Each firmware image must be imported or uploaded and then a profile created that includes both images. The firmware images must have metadata, which is not always included in the image. In that case, you specify the metadata during the import or upload operation.

### Uploading Firmware With Metadata

Use the procedures in Keeping Your Firmware Up-to-Date in the [How To library](#) to upload firmware. At the step for Select Firmware Components, select both firmware components:

- `MKAPP_Vfirmware_version.DL`
- `HTML_Vfirmware_version.DL`

### Uploading Firmware Without Metadata

Use the procedures in Keeping Your Firmware Up-to-Date in the [How To library](#) to upload firmware. At the step for Select Firmware Components, select one firmware component, `MKAPP_Vfirmware_version.DL` and click Upload. To define the metadata for the firmware:

1. For the target type click PDU.
2. For the platform, click Sun Rack II PDU.
3. Type the version of the firmware.
4. Choose Depends On None and accept the remaining default options.

After the job is completed, repeat the procedure with the other firmware image, `HTML_Vfirmware_version.DL` with one difference: At Step 4, specify that this firmware image depends on the `MKAPP_Vfirmware_version.DL` image.

### Creating a Firmware Profile for PDU Firmware Updates

1. Expand Plan Management in the Navigation pane.
2. Click Create Firmware Profile in the Actions pane.
3. Type a name and description for the profile.
4. For subtype, click Power Distribution Units.
5. For target type, click Power Distribution Units. Click Next.
6. For Firmware Configuration, accept the default options and values. Click Next.
7. Select both images: MKAPP\_V*firmware\_version*.DL and dHTML\_V*firmware\_version*.DL. Click Next.
8. Review the summary of the new profile and click Finish to submit the job.

## Local Content

The Linux and Oracle Solaris 8-10 Software Update Library software library also stores and gives access to site-specific configuration files, and scripts used in deployment plans. Other local content your site requires can be data files, executable files, or binary files. For example, you might develop a script to test servers before running a provisioning job.

The Local categories of the Updates Library have no connection to the Knowledge Base. You upload files to the software update library, directed into one of the categories, and then maintain them throughout their life cycle. You can create subcategories of any category to organize the files.

You can view details about a component such as distribution, version, release, group, size URL, when the file was added or edited, any summary and description information, host, RPM, and vendor.

## Local Action

An action is a script, binary file, or executable file that makes changes to the managed host. After you upload the script or file to the appropriate category, you create a profile for the type of script or files and then include the profile in the deployment plan that installs or upgrades the OS or firmware. The following actions are available:

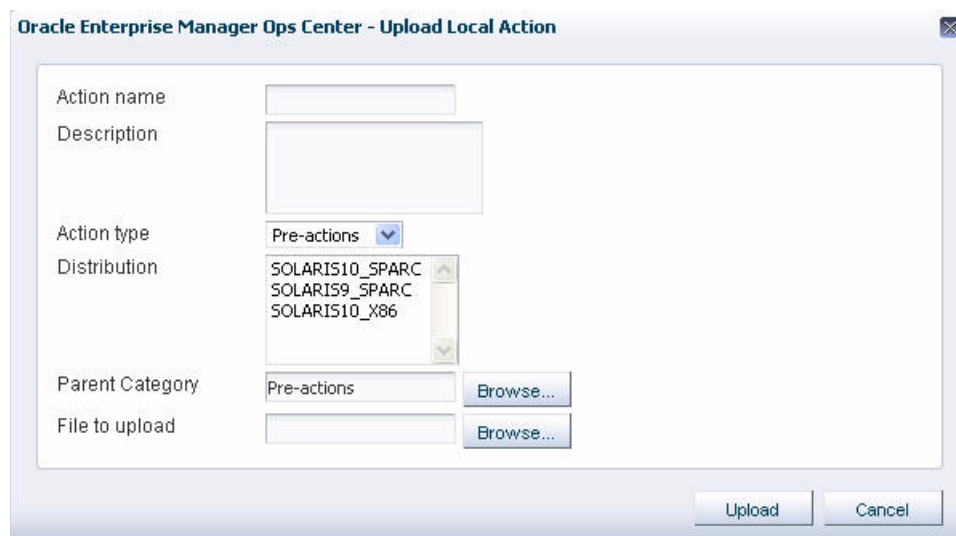
- Pre-Actions – Script that runs on a managed host before the provisioning step starts. When you create the deployment plan, you select the Execute Pre-Install step and then select the profile that includes the script.
- Post-Actions – Script that runs on a managed host after a job is completed. When you create the deployment plan, you select the Execute Post-Install step and then select the profile that includes the script.
- Probes – Script that runs on a managed host to verify that a job can be performed.
- Macros – Script that modifies a generic configuration file to make it appropriate for a managed host. The script outputs a single line that replaces a macro sign in a configuration file. Use macros to apply a single configuration file across multiple hosts by customizing the configuration file for each host's environment.

### To Upload a Local Action

1. Expand Libraries in the Navigation pane.
2. Click Linux and Oracle Solaris 8-10 Software Update Library.

3. Click Upload Local Action in the Actions pane.  
The Upload Local Action window is displayed.

**Figure 5–5 Local Upload Action**



4. Enter a name for the action.
5. Enter text to describe the purpose of the script or executable file.
6. Select the type of action such as Pre-Action, Post-action, Macros, or Probes.
7. Click the name of the distribution that is appropriate for the script or executable file.
8. The Parent Category field shows the category you specified as the type of Action. If your site uses subcategories, click the Browse button to navigate to the specific subcategory.
9. Click Browse to locate and select the script or executable file.
10. Click Upload. The file is uploaded to the Linux, Solaris 8-10 Software Update Library in the category you specified.

You can now create a profile for the script and then use the profile in a deployment plan.

## Local Package

You can upload software in the following formats:

- pkg
- rpm
- tar
- zip
- gzip
- compress

If the file is in compressed format, the file is uncompressed after it is uploaded.



**To Upload a Local Software Package**

1. Expand Libraries in the Navigation pane.
2. Click the operating system's Software Update Library.
3. Click Upload Local Software Packages in the Actions pane.
4. Select Yes if the package is a security fix for a previous version of the software. Otherwise, select No.
5. Click the name of the distribution to which you want to add this package.
6. In the Parent Category section, click Local PKGs or click Browse to locate a subcategory.
7. In the Files section, click Add to see the list of files. Select at least one software package.
8. Click Upload. The file is uploaded to the Linux, Solaris 8-10 Software Update Library in the category you specified.

You can now include the package or RPM in an provisioning profile.

**Local Configuration Files**

A configuration file is a text file, binary file, or non-RPM application that contains the settings and values for an asset type. A profile or deployment plan then uses the configuration file on all of the assets defined for it.

**To Upload a Local Configuration File**

1. Expand Libraries in the Navigation pane.
2. Click Linux and Oracle Solaris 8-10 Software Update Library.
3. Click Upload Local Configuration File in the Actions pane.  
The Upload Local Configuration File window is displayed.

**Figure 5-6 Upload Local Configuration File**

4. In Target path on server, type the full path to the configuration file.
5. In Version, type a character string to identify this version of the file. The string is appended to the file name when it is displayed in a Components list.
6. Type a brief description of the file.
7. Select the Distribution to which this file is applied. You can choose multiple distributions.
8. In Parent Category, accept the Configuration Files category or click Browse to locate a subcategory.
9. Click Browse to locate and select the configuration file.
10. Click Upload. The file is uploaded to the Linux, Solaris 8-10 Software Update Library in the category you specified.

## Local Categories

Your site's local content is organized into the following default categories: local RPMs or PKGs, configuration files, macros, pre-actions, post-actions, and probes. You can create subcategories to further organize your local content. The type of local content allowed in a subcategory depends on its parent category.

### To Add a Local Category

1. Expand Libraries in the Navigation pane.
2. Click Linux and Oracle Solaris 8-10 Software Update Library.
3. Click Add Local Category in the Actions pane.
4. Enter a name for the new subcategory.
5. Enter a brief description for the new subcategory such as its purpose.

6. Click Distribution to assign to the subcategory.
7. Click Parent Category to select one of the system-defined categories for the subcategory.
8. Click Apply. The new subcategory is created under the selected default category. You can now upload software packages and files into the new subcategory.

## Editing a Local Component File

You can edit the contents of a local component file. For example, if you uploaded a system file that contained IP addresses and determined that there was an incorrect IP address in the file, you can edit the file to correct the IP address. You can also use this procedure to replace the file with a corrected file.

### To Edit Local Component Files

1. Expand Libraries in the Navigation pane.
2. Click Linux and Oracle Solaris 8-10 Software Update Library.
3. Click Edit Local Component File in the Actions pane.
4. To specify the file, type its name or click the Browse button to navigate to the file. If the file is not found, click Distribution to select the correct distribution. Only files in the selected distribution are displayed.
5. Select either Edit existing file or Replace existing file.
  - If you choose to edit the file, make changes to the file and click Save.
  - If you choose to replace the file, browse for the replacement file and click Upload.

## Deleting a Local Component

You can remove your site's local content but you cannot remove the default categories.

---

---

**Note:** Deleting content does not require confirmation and cannot be undone. Verify you are deleting the correct local component.

---

---

### To Delete a Local Component File

1. Expand Libraries in the Navigation pane.
2. Click Linux and Oracle Solaris 8-10 Software Update Library.
3. Click Delete Local Component in the Actions pane.
4. Expand the category to display the component you want to delete. To change the distribution that is displayed, click Distribution.
5. Select the component or a subcategory to delete.
6. Click Delete.

To remove a subcategory and its components, do not attempt to remove each component and then remove the subcategory. When there are no components in a subcategory, the subcategory creates a placeholder component, which you cannot delete. Repeat the procedure and select the subcategory itself to delete. The placeholder component is also removed.

## Uploading Local Software in Bulk

You can upload multiple files or an entire directory in one operation. For example, you can upload the contents of a DVD or you can specify a directory. All components in the directory and subdirectories are uploaded.

The files must be in the following formats:

- pkg
- rpm (for Linux RPMs)
- tar
- zip
- gzip
- compress

If files are compressed, the software extracts the files after it uploads them.

### Before You Begin

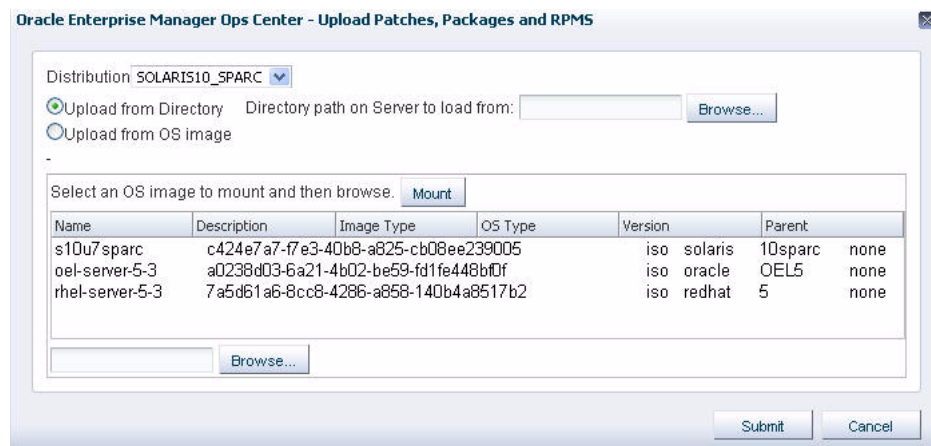
- Verify that the files have the supported file types.
- Verify that the file size does not exceed 2 GB. If the file is larger than 2 GB, copy the file manually to a file system on the Enterprise Controller's system.
- If you are uploading from removable media, insert the media.

### To Upload Local Software in Bulk

1. Expand Libraries in the Navigation pane.
2. Click Linux and Oracle Solaris 8-10 Software Update Library
3. Click Bulk Upload Packages and Patches in the Actions pane.

The Upload Packages, Patches, and RPMS window is displayed

**Figure 5–7 Local Software Upload**



4. Click Distribution to select the distribution that applies to these files.
5. Select either Upload from OS Image or Upload from Directory.
6. Specify the path to the OS image or directory or click Browse to locate and select it. If you specify a directory, all files in the directory and its subdirectories are

uploaded. If you specify an OS image, you must mount the OS image and select the files.

- a. Click one of the OS images and click Mount.
  - b. Click Browse to locate and select the files.
7. Click Submit. The upload job is created.

To view the status of the upload job, select Bulk Upload Results.

To view the certified packages in the software update library, click the Content tab in the center pane and select Patches in the Category list. To view non-certified packages, click Local PKGs or Local RPMs in the Category list.

## Viewing Bulk Upload Results

You can view a detailed history of all the local components that were uploaded in bulk.

### To View Bulk Upload Results

1. Expand Libraries in the Navigation pane.
2. Click Linux and Oracle Solaris 8-10 Software Update Library.
3. Click Bulk Upload Results in the Actions pane. The uploaded components list displays the name, description, status, and date for each component.
4. Select a component and click View Results. The details of the uploaded components are displayed.

## Backing Up Images and Local Content

The `ecadm backup` command does not back up the software libraries. It is a good practice to create the software library for OS images on networked storage (NAS) and include the network storage device in your site's backup plan. As an alternative, back up the Enterprise Controller's directory manually.

### To Back Up Images and Local Content

1. Move the archive to another server, file-share facility, or a location outside of the `/var/opt/sun` directory, according to your site's disaster recovery plan.
2. If it is necessary to rebuild the Enterprise Controller, restore the Enterprise Controller and then restore the `/var/opt/sun/xvm/images/os` hierarchy.

## Related Resources for Software Libraries

For instructions in performing actions or to learn more about the role of this feature, see the following resources in the How To library:

<http://www.oracle.com/pls/topic/lookup?ctx=oc121&id=howto>.

- Configuring and Managing Software Libraries on the Enterprise Controller
- Keeping Your Firmware Up-to-Date



---

---

## Storage Libraries

The following information is included:

- [Introduction to Storage Management](#)
- [Roles for Storage Management](#)
- [Actions for Storage Management](#)
- [Location of Storage Information in the User Interface](#)
- [Storage Libraries](#)
- [Types of Storage for Libraries](#)
- [Storage Hardware](#)
- [Storage Profiles](#)
- [High Availability for Storage Resources](#)
- [Related Resources for Storage Management](#)

### Introduction to Storage Management

Oracle Enterprise Manager Ops Center manages and monitors storage servers and appliances, discovers and provisions storage capacity on these appliances through Storage Connect plug-in software, and then makes the storage available to virtual assets through its storage libraries.

Storage libraries are the storage resources for Oracle Solaris Zones, Oracle VM Servers for SPARC, Oracle VM Servers for x86, their server pools, and virtual datacenters. These virtualization hosts and server pools store their metadata and their operational data in storage libraries. The metadata and data for Oracle Solaris zones are stored in a storage library associated with the global zone or server pool. A storage library that supports an Oracle VM Server is an Oracle VM Storage Repository.

### Roles for Storage Management

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 6–1 Storage Roles and Permissions**

Task	Role
Create a new storage library	Storage Admin
Remove a storage library	Storage Admin
Edit attributes of a storage library	Storage Admin
Add storage capacity	Storage Admin
Update a storage appliance	Update Admin

## Actions for Storage Management

You can perform the following actions, depending on the requirements.

- Create new storage libraries, either as a file system or as block storage.
- Modify existing storage libraries by changing their attributes or adding LUNs.
- Update storage appliances.

The set of available actions depends on what you have selected:

- When a physical asset is selected, you can launch the asset’s user interface and view information about the hardware’s state and configuration.
- When you choose an asset in the File Server group, the Filesystems tab in the center pane lists all of the file systems with the Add a Backing Device icon, the Edit icon, and the Delete icon.
- When you choose an asset in the Storage Array Group, the Logical Units tab gives you access to the Create Logical Unit icon, the Resize LUN icon, the Delete LUN icon, and the Clone LUN icon.

## Location of Storage Information in the User Interface

**Table 6–2 Location of Library Information in the BUI**

Object	Location
To see the storage libraries	Expand Libraries in the Navigation pane, then expand Storage Libraries.
To see storage hardware information	Expand All Assets in the Navigation pane, then scroll to the Storage section. Select a physical asset to see information about it in the center pane.
To see groups of storage arrays or file servers	Expand All Assets in the Navigation pane, then Storage in the Resource Management Views section.
To see storage profiles	Expand Plan Management in the Navigation pane, then click Profiles and Policies. The Discovery, RAID Controller, and Update Storage Appliance categories contain profiles.
To see the virtual host that is using a LUN	Expand Libraries in the Navigation pane, then expand Storage Libraries. Select the storage library to view the LUNs table in the center pane. The Allocated To field displays the virtual host’s identifier.
To see the virtualization host that is using a storage library	Expand Libraries in the Navigation pane, then expand Storage Libraries. Select the storage library to view the Summary tab in the center pane. The IP address of the virtualization host is in the Allocated To field.



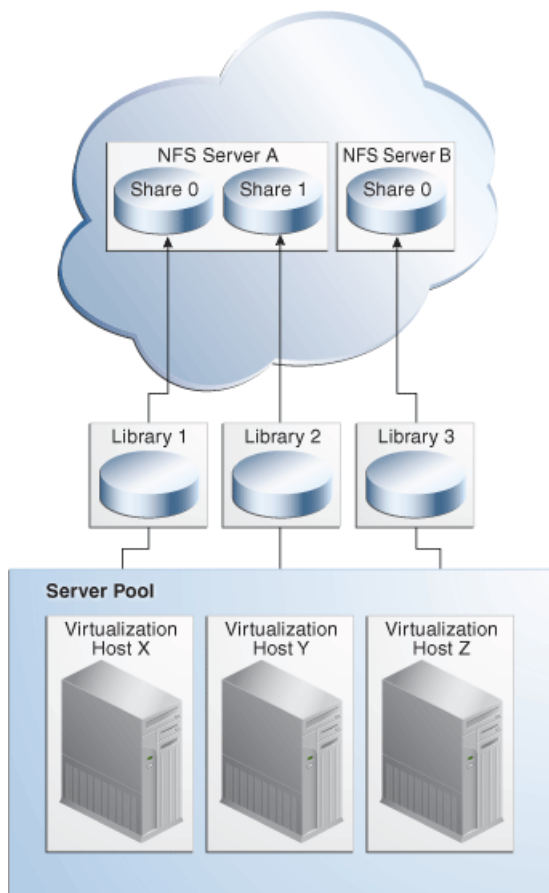
## Storage Libraries

A storage library stores metadata for each virtualization host in the server pool that is associated with the storage library. Metadata is a virtualization host's image or identity: the configuration for its operating system, CPU, memory, and network. The virtualization host's data, which results from its use, can reside in the same storage library or in a different storage library.

A storage library can be a local, that is, a file system on the virtualization host's server or it can be accessed through an NFS server or SAN network. When you create a virtualization host, you assign it to one of the storage libraries associated with its virtualization host so that its metadata can be stored.

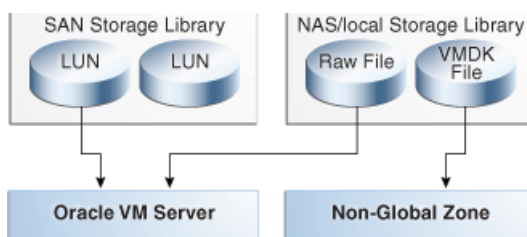
- For the metadata of its local virtual hosts, virtualization hosts (Oracle VM Server for SPARC, Oracle VM Server for x86, and global zones) can use a local storage library.
- For metadata of all virtual hosts, virtualization hosts must use a Network Attached Storage (NAS) storage library.
- For data, Oracle VM Server for SPARC and Oracle VM Server for x86 can use either NAS shares or SAN LUNs for itself and for its virtual hosts. A global zone can use SAN LUNs for itself and for its non-global zones. The storage library must be associated with the virtualization host.
- A server pool must use a NAS storage library.

You can group virtualization hosts with the same processor architecture to create a server pool. The virtualization hosts share all the storage and networks associated with the server pool. If you add a virtualization host to a server pool, the libraries associated with that virtualization host become available to all the other hosts in the server pool. [Figure 6-1](#) shows how virtualization hosts in a server pool get access to storage resources through the storage libraries.

**Figure 6–1 External Storage**

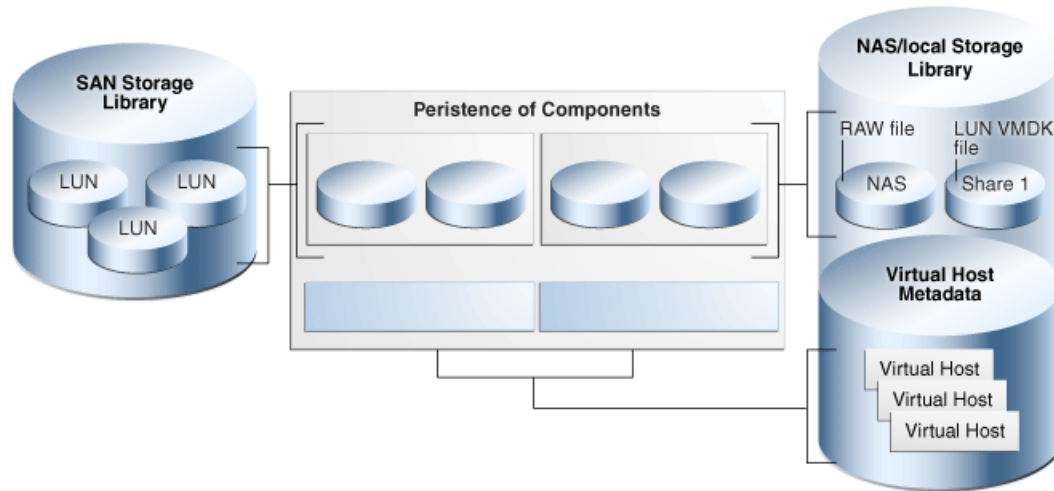
The diagram in [Figure 6–2](#) shows how the NAS and SAN storage libraries and virtualization hosts interact with LUNs.

- SAN storage libraries expose data as virtual disks (LUNs), identified by their LUN GUIDs. A control domain makes raw partitions available to its logical domains using Fibre Channel or iSCSI, as described in [Block Storage](#)
- NAS storage libraries expose data as raw files and files in VMDK format. All types of virtualization hosts store metadata using NFS services, as described in [Network Attached Storage \(NAS\) Storage Libraries](#)

**Figure 6–2 SAN and NAS Storage Libraries**

The LUNs, raw files, and raw volumes store data and metadata for the virtual hosts. [Figure 6–3](#) expands [Figure 6–2](#) to show that the metadata for NAS virtual disks are stored in the NAS storage library. Metadata for SAN virtual disks is persisted in the SAN Storage Library.

Figure 6-3 Storage Library Metadata



## Network Attached Storage (NAS) Storage Libraries

Network-attached-storage (NAS) libraries are storage libraries for NFS storage device mount points. The virtualization hosts use NFS services to attach to the storage libraries and get access to the data and metadata.

You can store metadata for all virtual hosts in one NAS storage library or you can create separate storage libraries for each virtual host. The benefit of using separate storage libraries is to increase ease of access, to increase capacity, and to increase performance.

If a NAS storage library becomes unavailable, the virtual hosts associated with the library are affected in the following ways:

- If the storage library is used for the virtual hosts' metadata, a virtual host continues to function but Oracle Enterprise Manager Ops Center can no longer manage the virtual host. Because Oracle Enterprise Manager Ops Center relies on its interaction with the metadata in the storage library, jobs that must read or modify the metadata fail. You must manage the virtual host manually.
- If the storage library is used for NFS large files that support virtual disks, the virtual host does not function.
- If the boot disk is on the NFS share, the virtual host cannot be rebooted.
- The virtual host cannot be migrated.

## Block Storage

You can associate block storage libraries with server pools, Oracle VM Servers, or global zones to store their data. A block storage library consists of groups of LUNs. A LUN (Logical Unit Number) is a slice of a storage volume, which is a collection of disks.

- Disk — Physical storage media. A set of disks is a disk array.
- Volume — An aggregation of storage space provided by several disks.
- Slice — A partition of a volume that is exposed to the servers connected to the disk array.
- LUN (Logical Unit Number) — The representation of a slice.

- GUID — The Global Unique Identifier for a LUN.

A storage library can use block storage or file system storage. Block storage is backed by Fibre Channel disks or iSCSI disks in the form of Logical Units or LUNs. Block storage can be static or dynamic.

### Dynamic Block Storage

When Oracle Enterprise Manager Ops Center can create, resize, delete, and clone LUNs, the block storage library is dynamic. When you add more virtual hosts to a server pool, you can add more LUNs to the storage library in the same action. In this release, a dynamic block storage library is created when a storage device with iSCSI LUNs is discovered.

### Static Block Storage

When Oracle Enterprise Manager Ops Center manages a storage device with existing LUNs, it can use the LUNs but cannot change or delete them, or create new LUNs. This can be done through the storage device's own user interface. A static block storage library supports storage devices that were discovered and configured in previous product software versions. Each LUN is for the exclusive use of its assigned virtual host. Because a LUN has a fixed size and cannot be shared, you must plan how to optimize the available storage in the storage library and assign a LUN of the appropriate size.

Table [Table 6–3](#) compares static block storage libraries and dynamic block storage libraries.

**Table 6–3 Comparison of Static and Dynamic Libraries**

	Dynamic Block Storage Library	Static Block Storage Library
Protocol	iSCSI	iSCSI Fibre Channel
To create a storage library	The storage library is created implicitly when you discover storage hardware and its target groups.	You create LUNs and then create the storage library. You assign existing LUNs to the library.
To manage a storage library	When you add a virtual host, you can create a LUN for it. When a virtual host needs more storage, you can increase the size of the LUN.  Any changes made through the storage server's user interface are reflected in the Oracle Enterprise Manager Ops Center's user interface.	The number of virtual hosts that can use the storage library is set by the number of LUNs in the storage library.  Changes made through the storage server's user interface are not updated in the Oracle Enterprise Manager Ops Center's user interface. Some information, such as a LUN's GUID can be obtained only from the storage server's user interface.
Add LUN icon	Create a new LUN.	Select an existing LUN or enter the GUID of an existing LUN.
Edit LUN Details icon	Increase the size of the LUN.	Renames the LUN in Oracle Enterprise Manager Ops Center
Delete LUN icon	Deletes the LUN and deletes the data. You are deleting the LUN on the storage server.	Deletes the LUN from the library but does not delete data.

## Storage Libraries for a Virtual Datacenter

The vDC inherits the storage resources allocated for the server pool. See [Storage Setup](#) in [Chapter 18](#).

## Storage Libraries for Oracle Solaris Zones

To use storage resources, an Oracle Solaris Zone must be associated with the storage library. See [Associate Storage Libraries](#) in [Chapter 14](#).

## Storage Libraries and Repositories for Oracle VM Server

Oracle Enterprise Manager Ops Center provides option to create Oracle VM Storage Repositories. The Oracle VM storage repositories are storage libraries that are used to store virtual machine metadata, ISO images and virtual disk images. If the storage repository is created on a NFS file server, it is a NFS based storage repository. If the storage repository is created on a LUN, it is a block- based repository. You create storage repositories on these file servers to be used by Oracle VM Servers to store resources. The resources include virtual machine metadata, templates, assemblies, ISO images and virtual disks.

### To Create an Oracle VM Storage Repository

1. Expand Libraries in the Navigation pane.
2. Select Storage Libraries.
3. Click New Oracle VM Storage Repository.
4. Type a name and description for the repository and choose either the NFS or OCFS protocol. Click Next.
5. From the drop-down lists, choose the Oracle VM Manager and the Oracle VM Server that will use the storage repository, and the NFS File Server that supports the storage repository.
6. Choose the file system on the NFS file server for the storage repository and specify the share name. Click Next.
7. Choose the server pool to associate with the storage repository. Click Next.
8. Review the configuration and then click Finish to submit the job.

## Types of Storage for Libraries

- [File Systems Libraries](#)
- [Block Storage](#)

### File Systems Libraries

Each virtual host has a default local library named `/guests` where data and metadata for the host's guests are stored. For the purposes of storage efficiency and your site's organization, you can create and maintain other local libraries by specifying a file system as a library.

If the storage library becomes unavailable, the local library remains available. However, any guest with metadata in a local library cannot be migrated.

### Viewing Local Libraries

Use this procedure to see the local libraries for a virtual host and the contents of a library. You can also see details of the local disks that support the local libraries.

### To View a Virtual Host's Local Libraries

1. Expand Assets in the Navigation pane.

2. Select the virtual host.
3. Click the Libraries tab in the center pane. The Associated Libraries table's Type column identifies the libraries of the Local type.
4. Select a library of the Local type. The Usage table shows all the guests that use that local library.
5. In the Usage table, select a guest.
6. Click the Contents tab to see the Library Contents table with all of the images, sorted by type.
7. To see details of the local disks, return to the Associated Libraries table and click Local Devices. The select the local device library.

### **Editing the Attributes of a Local Library**

You can rename a local library and you can change its description. You cannot change the file system defined for the local library.

#### **To Edit a Local Library**

1. Expand Assets in the Navigation pane.
2. Select the asset.
3. Click the Libraries tab in the center pane. The asset's associated libraries and the guests that are stored in the libraries are listed.
4. Click the Edit Local Library icon.
5. In the Edit Local Library pane, enter the new name or description for the library.
6. Click the Update button. When the job is completed, the edited local library is listed in the Associated Libraries table.

### **Creating a Local Library**

Each virtual host has a local library, located at `file:///guests`. In addition to the default local library, you can create other local libraries to use your storage resources efficiently or organize your images.

#### **To Add a Local Library**

1. Create a file system with read/write permissions for only the root user.
2. Expand Assets in the Navigation pane.
3. Select the asset.
4. Click the Libraries tab in the center pane. The asset's associated libraries and the guests that are stored in the libraries are listed.
5. Click the New Local Library icon.
6. In the Create Local Library pane, type a name and description for the library.
7. In the URL field, enter the directory name for the location where you want to store images and metadata.
8. Click the Create Local Library button. When the job is completed, the new local library is listed in the Associated Libraries table.

## Deleting a Local Library

You can delete a local library that was added to a virtual host. After the deletion, the virtual host does not have any access to either the directory defined for the local library or any of its contents. The default local library, /guests, cannot be deleted. You have the option of deleting the library and all of its contents or to delete the library but keep the contents in the directory of the storage resource. In either case, the directory is not deleted.

When the job is completed, the local library is removed from the Associated Libraries table. If you chose to keep the local library's content, you can create a local library with the same content by specifying the same URL for the new library.

## Block Storage

The block storage libraries are used in SAN networks and are based on either Fibre Channel LUNs or iSCSI LUNs, depending on the storage array that backs the LUNs. The LUNs can provide static or dynamic storage, depending on whether the storage array is a managed asset.

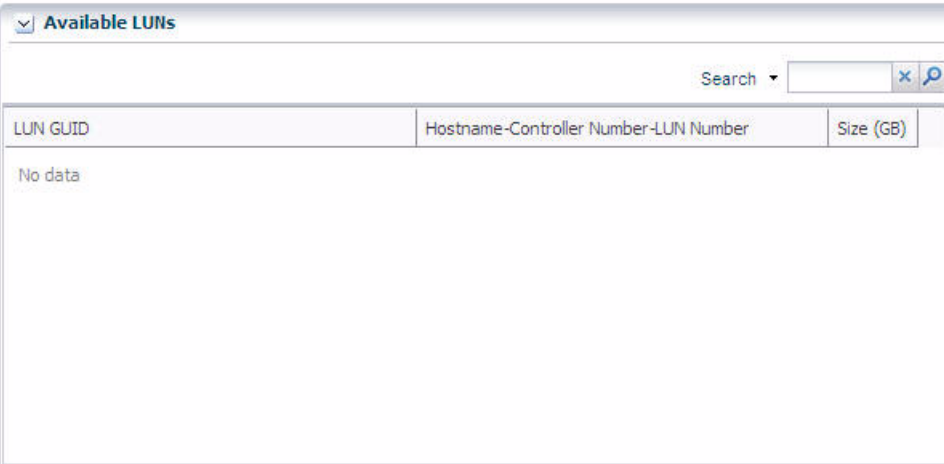
### Select LUNs For the Block Storage Library

You use this procedure in the following situations:

- You are creating a new SAN storage library and have associated the new library with a virtual host or server pool immediately.
- You are increasing the storage capacity of an existing SAN storage library and chose to select LUNs from the available LUNs.

The Available LUNs table shows all of the LUNs that are accessible from either the associated library or from the pools, hosts, or zones you selected.

**Figure 6–4 Available LUNs**



LUN GUID	Hostname-Controller Number-LUN Number	Size (GB)
No data		

For each LUN, the following information is displayed to help you identify the ones you want to add to the library.

- LUN GUID - The unique 32-digit identifier for the LUN.
- Host information for the LUN:
  - Hostname - Name or IP address of the host that can access the LUN.

- Controller Number - The host's identifier for the HBA port, which is the physical interface to the Fibre Channel disk array.
  - LUN Number - The host's identifier for the LUN.
  - Size (GB) - Size of each LUN in Gigabytes. Use the Search box to locate a specific LUN.
1. Click one or more LUNs. When you finished, click Next or Add LUN.
  2. If you are adding a LUN to an existing storage library, a new job starts. If you are creating a SAN storage library, review the details of the LUNs you have configured in the Summary pane.
  3. Click Finish to close the library.

## Add Capacity to Dynamic Block Storage Libraries

If the block storage library is not associated with a server pool or virtual host, you can add storage capacity by specifying new LUNs by name. If the storage library is associated, you can also select new LUNs from a list of the LUNs available to the server pool or virtual host.

### To Add LUNs to a Block Storage Library

1. Expand Libraries in the Navigation pane.
2. Click Block Storage in Storage Libraries.
3. Click one of the available storage libraries.
4. Click Add LUN in the Actions pane.
5. Choose the method for adding LUNs:
  - To add LUNs to the library manually, accept the default option: Manually enter the GUID/WWN of the LUNs to be added. See [To Add LUNs to a Block Storage Library Manually](#) to complete the procedure.
  - To select LUNs from the available LUNs, click the Select from available LUNs option. See [Select LUNs For the Block Storage Library](#) to complete the procedure.

### To Add LUNs to a Block Storage Library Manually

You use this procedure in the following situations:

- You are creating a new SAN storage library and have accepted the default action of adding LUNs later. You are required to add at least one LUN to create the storage library.
- You are adding a LUN to an existing SAN storage library. You selected the library and then the Add LUN action. The default option is specify each new LUN by name.

After you have accepted the default option to add the LUNs by name, the following table is displayed:



**Figure 6–5 Manually Adding LUNs**

Library Name : **FCLib-11102010-153513**

Description :

**NOTE:** You can only select from available LUNs if the Fibre Channel library is already associated with one or more virtual pools, global containers or virtual servers.

Manually enter the GUID/WWN of the LUNs to be added

Add one or more LUNs to the library. Use Ctrl+Click and Shift+Click to select multiple LUNs

**LUNs to be added to the library**

LUN GUID	LUN Name
	FCLib-11102010-153513-LUN1

Add LUNs    Cancel

1. Click the icon to create an entry for the LUN.
2. Click in the GUID/WWN field and type the GUID or WWN for the LUN. The GUID is the Global Unique Identifier associated with each LUN, which is a hexadecimal number of 32 digits. If your site uses SCSI initiators and targets, you can enter the WWN for the LUN. You can edit the default name for each LUN. Click Next or Add LUN.
3. If you are creating the storage library, review the details in the Summary pane.
4. Click Finish to close the Fibre Channel library.

## Oracle VM Storage Connect Plug-ins

Oracle Enterprise Manager Ops Center shares the capability of Oracle VM Manager to manage storage devices of various vendors. Oracle VM Storage Connect is an application programming interface (API) that exposes the storage device's features and attributes to Oracle Enterprise Manager Ops Center. When a storage vendor creates an Oracle VM Storage Connect plug-in, you install the plug-in so that you can manage the vendor's storage products. The storage devices are managed through the Oracle Enterprise Manager Ops Center's user interface. The plug-in software is available from the vendor.

Use the following procedure to see the plug-ins that have been installed:

1. Expand Administration in the Assets pane.
2. Select Enterprise Controller.
3. Click the Proxy Controller tab in the center pane.

The Installed StorageConnect Plugins section of the center pane lists the plug-in software and its details.

## Storage Hardware

The storage features are supported by various types of storage devices. The tabs in the center pane contain specific information about each type.

### RAID Controller

RAID Controllers embedded in other types of storage report the following in addition to the hardware information:

- RAID Volumes
- RAID Levels
- Stripe size
- Number of disks

### NAS Storage Appliance

Software and Storage Libraries can reside on the shares of an NFS server. These libraries can be created by one of the following methods:

- Create the library, attach the virtual host to the Oracle Enterprise Manager Ops Centersoftware, and then associate the library with the virtual host's server pool.
- Use the Oracle Enterprise Manager Ops Center software to create a library and add it to a virtual host's server pool.

---

---

**Note:** NFS protocol requires agreement on the Domain Name System (DNS) that the NFS server and NFS clients use. The server and a client must agree on the identity of the authorized users accessing the share.

---

---

Because the Enterprise Controller does not mount the NFS share, install the NFS server on a system that is close to the systems where the NFS share must be used, that is, the systems that host Oracle VM Server for SPARC and Oracle VM Server for x86.

#### To Set Up a Share on the NFS Server

1. On the NFS server, edit the `/etc/default/nfs` file.
2. Locate the `NFSMAPID_DOMAIN` variable and change the variable value to the domain name.
3. Define a group and user account that are common to both the NFS server and the NFS clients. Create the group account with GID 60, and the user account with UID 60. For example, use the following commands to create a group and a user named `opsctr`: Create the `opsctr` group:

```
# groupadd -g 60 opsctr
```

Create the `opsctr` user:

```
# useradd -u 60 -g 60 -d / -c 'Ops Center user' -s /bin/true opsctr
```

4. Create the directory to share, and set its ownership and permission modes. For example:

```
# mkdir -p /export/lib/libX
# chown opsctr:opsctr /export/lib/libX
# chmod 777 /export/lib/libX
```

5. Edit the `/etc/dfs/dfstab` file on the NFS server.
6. Add an entry to share the directory with the correct share options. For example, to share a directory named `/export/lib/libX`, create the following entry:

```
share -F nfs -o rw,root=<domain name>,anon=60 -d "Share 0" /export/lib/libX
```

where *<domain name>* is the domain name that you specified in the `/etc/default/nfs` file. If you want the NFS share to be accessible outside the domain, use the `rw` option to specify the optional domain list.

```
share -F nfs -o rw=<domain name 1>,<domain name 2>,anon=60 -d "Share 0"
/path/to/share
```

Replace the *<domain name n>* entries with the correct domain names.

7. Share the directory and verify that the directory is shared. For example:

```
# shareall
# share
-                /export/lib/libX  rw,root=_<domain>_,anon=60  "Share 0"
```

The share now allows the `opsctr` user account and root user on the NFS clients to have write privileges. The special options set the directory to allow write access, the domain to allow access as the root user, and specifies that the anonymous user is seen on the clients as the user account with UID 60 (`opsctr`).

---

**Note:** Add the domain name to the `/etc/nsswitch.conf` file so that `root=<domain name>` is effective. If possible, use DNS instead of Network Information Service (NIS). DNS maps the host names to the IP addresses. Change the host line to DNS in the `/etc/nsswitch.conf` file.

---

After setting up a share on the NFS server, the NFS client has to be prepared to mount the share.

### To Set Up an NFS Client

1. On each NFS client, edit the `/etc/default/nfs` file.
2. Locate the `NFSMAPID_DOMAIN` variable and change the variable value to the domain name.
3. Verify that the `opsctr` user account has been created.

```
# grep opsctr /etc/passwd
```

A successful result is similar to the following:

```
opsctr:x:60:60:opsctr user:/:
```

4. Verify the NFS share is visible on the client.

```
# showmount -e <server-name>
export list for <server-name>:
/export/virtlib/lib0 (everyone)
```

## To Create a NAS Storage Library

A NAS Storage Library is the same as a NAS Software Library but its purpose is different. The software library holds images for provisioning. The storage library holds metadata and data.

### To Create a NAS Storage Library

1. Expand Libraries in the Navigation pane.
2. Click Storage Libraries
3. Click New NAS Storage in the Action pane.

The Create New NAS library window is displayed.

**Figure 6–6** Create New NAS Library

**Oracle Enterprise Manager Ops Center - Create New NAS Library**

**New NAS Library**

Library Name:

Library Description:

Server Pool Association: **Select the server pool you want to be associated with this library. Use Ctrl+Click and Shift+Click to select multiple server pools.**

Name	Description
NORM-VirtPool-0	
NORM-VirtPool-1	

Select the type of service:

Exported share on a managed asset

Select a storage asset and then select the share that provides storage.

Asset:

Share:

Other

Replace hostname, port, and path with the values for the storage resource.

URL:

4. Enter a name for the library and a description.
5. Select the server pool to be associated with this library.
6. For the Type, you have a choice of either entering the path of a shared directory or, if Oracle Enterprise Manager Ops Center is managing a unified storage asset, selecting the asset and specifying the exported share to use.
7. Click the New NAS Library button to create the library.

## File Server

For file-based storage devices such as NAS appliances and other NFS devices, Oracle Enterprise Manager Ops Center reports the following in addition to hardware information:

- File systems - The location in the file system hierarchy that is presented as a physical device. For example, an NAS share.
- Backing Devices - The physical device that supports a file system. For example, a RAID disk.

## Storage Array

For block-based storage such as iSCSI SAN and Fibre Channel SAN devices, the storage array assets include the following tabs in the center pane:

- Volume Groups - Indicates a collection of physical disks or portions of physical disks.
- Logical Units (LUN) - Virtual disks created from the volume groups.

## Storage Server: Sun ZFS Storage Appliance

See the Sun ZFS Storage Appliance documentation for specific information about the storage appliance. To view the Sun ZFS Storage 7000 System Administration Guide, log in to the Unified Storage System software interface and click Help in the top right corner of any screen.

This type of storage appliance contains a service processor, which must also be discovered. See [Discovering a Sun ZFS Storage Appliance](#) for this procedure.

### Managing a Sun ZFS Storage Appliance

After the storage appliance is discovered, you can manage it as you do other assets with the additional capabilities that the Sun ZFS Storage Appliance provides. From the Oracle Enterprise Manager Ops Center UI, you can launch the storage appliance's UI. Use the following commands in the Action pane, to launch a specific page of the appliance's user interface. For each one, enter the credentials for the appliance and then perform the appliance tasks.

- Launch Appliance UI opens a new browser window or tab for the main page.
- Launch Detailed Dashboard opens a new browser window or tab for the status page.
- Launch Analytics opens a new browser window or tab for the dynamic analysis page.
- Manage Shares opens a new browser window or tab for the share configuration page.
- Manage Services opens a new browser window or tab for the data services configuration page.

### Provisioning and Updating a Sun ZFS Storage Appliance

---

---

**Note:** Starting with this version of the product software, you can update the storage appliance using provisioning profile and deployment plan.

---

---

1. Download the appliance update from My Oracle Support and uncompress the file to obtain the image for the appliance update.
2. Upload/import the appliance update image into a software library and accept the default action of creating a profile for this image.
3. Create a plan from the Update Storage Appliances plan template. Select the software library and then select the profile for the image.
4. To apply the deployment plan, select the plan and then select the storage appliances to update.

If it is necessary to downgrade a storage appliance, use the following procedure:

1. Expand Assets and then Storage in the Navigation pane.
2. Select the storage appliance.
3. Click the System Details tab in the center pane.
4. In the Appliance Updates table, select the update to remove.
5. Click the Rollback Appliance Software icon.
6. Confirm the action to submit the job.

## Exadata Storage Server

The Oracle Exadata Storage Server is a fast, high capacity storage server. Each server comes has 12 disks connected to a storage controller. Exadata has three disk groups that span all of the disks so that each physical disk is in each disk group. Having all physical disks participating in data retrieval and storage maximizes performance.

Oracle Enterprise Manager Ops Center discovers the Exadata Storage Server and its disks when it manages a SuperCluster Engineered System. See [Chapter 20, "Oracle Engineered Systems"](#) for more information.

## Storage Profiles

Oracle Enterprise Manager Ops Center provides default profiles for the following operations:

- Configuring RAID Controllers
- Updating the Sun ZFS Storage Appliance

## High Availability for Storage Resources

Storage devices for an HA configuration must meet these requirements:

- Storage must be transferable between the primary and secondary Enterprise Controller systems. Do not attempt to use local file systems for high-availability storage.
- Storage must offer data redundancy capability, such as mirroring or RAID 5.
- Storage must offer performance that is sufficient to support operations.
- Storage must have the capacity to hold the data that the Oracle Enterprise Manager Ops Center software stores in the `/var/opt/sun/xvm` directory structure.

A variety of storage solutions meet these criteria, including NAS appliances, hardware RAID arrays and external JBODs. Storage can be attached directly to the Enterprise Controllers or through Storage Area Networks.

You must determine what storage solution offers the required capacity, performance, connectivity, and redundancy capabilities. Configuration procedures vary greatly among the available storage solutions, and among operating systems.

You must determine the specific failover procedures to use for the HA storage solution. Contact My Oracle Support to determine the procedures to use for your particular installation.

## Related Resources for Storage Management

For instructions in performing actions or to learn more about the role of this feature, go to one of the following resources.

- For end-to-end examples, see the How To library at <http://www.oracle.com/pls/topic/lookup?ctx=oc121&id=howto>
- For information about storage hardware, see [Chapter 11](#).
- To view the Sun ZFS Storage 7000 System Administration Guide, log in to the Unified Storage System software interface and click Help in the top right corner of any screen. You can also access this guide at the hostname or IP address of the storage system:
  - <https://hostname:215/wiki>
  - <https://ipaddress:215/wiki>

See the Sun ZFS Storage Appliance Software product information page for links to more information.





The following information is included:

- [Introduction to Network Management](#)
- [Roles Required for Network Management](#)
- [Actions for a Network and Network Domain](#)
- [Location of Network Information in the User Interface](#)
- [Network Domains](#)
- [Networks](#)
- [Properties of a Network](#)
- [Network Utilization](#)
- [Network Connectivity](#)
- [Network Hardware](#)
- [Network Profiles](#)
- [Oracle Enterprise Manager Ops Center's Networks](#)
- [Related Resources for Networks](#)

## Introduction to Network Management

Oracle Enterprise Manager Ops Center supports Ethernet and InfiniBand network protocols. While the Ethernet interconnect is the established and common interconnect, InfiniBand is popular in high-performance computing environments because it maximizes the speed of transactions using the short, multiple connections found in clusters and data centers.

- For an Ethernet network, both tagged and untagged VLANs are supported.
- For an InfiniBand network, partitions are supported.

---

---

**Note:** If you use an InfiniBand switch in an Ethernet network, the ports on the switch have Ethernet names.

---

---

When you use Oracle Enterprise Manager Ops Center to discover a physical switch, all the fabrics that the switch supports are also discovered. One physical fabric supports many fabrics. Each port on an Ethernet switch can support 128 fabrics through its VLAN ID. Each partition on an InfiniBand switch can support 32000 partition keys.

The members of a partition are identified by partition keys or "P-keys," which act like Ethernet's VLAN tags. For example, if a server has two P-Keys, it participates in two different partitions.

---

**Note:** For an Oracle Exalogic server that has Oracle Enterprise Manager Ops Center installed, all physical and logical fabrics are discovered. For an Exalogic server that does not have Oracle Enterprise Manager Ops Center installed but resides in a data center that uses Oracle Enterprise Manager Ops Center, the Exalogic server is discovered as a server and then all of its fabrics are discovered.

---

## Roles Required for Network Management

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 7-1 Network Roles and Permissions**

Task	Role
Edit Network Domain	Network Admin
Edit Network Attributes	Network Admin
Edit Network Services	Network Admin
Aggregate Links	Network Admin
Create IPMP Groups	Network Admin
Attach Network to Server Pool	Cloud Admin
Create Network Domain	Network Admin
Create Network	Network Admin
Delete Network Domain	Network Admin
Delete Network	Network Admin
Manage Fabric	Network Admin
Delete Fabric	Network Admin
Assign Network	Network Admin
Connect Guests	Network Admin
Discover and Manage the Switches	Network Admin
Configure Network for Server Deployment	Server Deployment Admin

## Actions for a Network and Network Domain

After a network is created, you can perform the following actions, depending on the requirements.

- Edit Network Attributes
- Edit Network Services
- Aggregate Links
- Create IPMP Groups

- Attach Network to Server Pool
- Create Network (manage network)
- Delete Network
- Assign Network
- Connect Guests
- Discover and manage the switches

## Location of Network Information in the User Interface

**Table 7–2** Location of Network Information in the BUI

Object	Location
Fabric	Expand Networks in the Assets pane. Then select Fabrics.
Physical Fabric	Expand Networks in the Assets pane. Then select Fabrics and then select Network Switches.
Network	To see all networks, regardless of type, expand Networks in the Assets pane. Then select Network Domains.
Services of a Network	Network Services tab: time server, WINS, DNS, and NIS. To modify these services, edit the network services. You cannot change the network's IP address or name.
Network Domain	Expand Networks in the Assets pane. For the Default Network Domain, select first item in the hierarchy
Physical switch	Expand Assets and expand Network Switches. To see each port, click the Connectivity tab.

## Network Domains

A network domain is a container for managed networks and handles the relationship between the physical fabrics that support the networks and the virtualization hosts or server pools that use the networks. The fabrics provide network resources such as links and IP subnets to the network domain. Within the network domain, networks that have been discovered or specified are available for assignment. These are called public networks. Their network resources have been defined. Another type of network is dynamic, that is, the network is created when it is needed, using an IP address space available to the network domain. Because they exist only for a specific purpose and only within a specific network domain, they are called private networks.

In Oracle Enterprise Manager Ops Center, networks become part of a network domain in the following ways:

- An asset that has a network is discovered.
- A user creates a network.
- A network is created when it is required. This is a dynamic network.

Oracle Enterprise Manager Ops Center operates on more than one layer of the Open Systems Interconnection model. All of the elements at all layers are managed in a network domain. [Table 7–3](#) shows the physical to logical stack.

**Table 7-3 Elements of a Network Domain**

Layer	Asset	What Is Managed	Capability
Layer 3 Network: IP address	For Ethernet: fabric networks For InfiniBand: non-fabric networks	IP subnet and mask IP address range VLAN or Partition Services Routing	The network provides connectivity.
Layer 2 Data links	For a tagged Ethernet: VLAN For an untagged Ethernet: portID For InfiniBand: partition	VLAN IDs Partition keys (P-key)	A virtual host uses the virtual NIC and a virtual switch in a VLAN or partition.
Layer 1 Physical: switches, ports, host bus adapters	Fabrics	\	\
/	Fully-managed switched fabric	The switch is a managed asset.	Can create a dynamic private network for each VLAN ID or partition key.
/	Host-managed fabric	The host of the switch is a managed asset.	Can create a dynamic private network for each VLAN ID or partition key when you enable the VLAN IDs or partition keys on the switch ports connected to the host.
/	Unmanaged fabric	The switch is discovered or declared during the discovery of another asset but is not managed.	Cannot create dynamic private networks because the VLAN IDs or partition keys are not available. The networks you create on an unmanaged fabric are static private networks.

## Default Network Domain

The Oracle Enterprise Manager Ops Center software always has a Default Network Domain and all public networks are members of it. If you have upgraded your product software, the existing managed networks are now in the Default Network Domain. A new public network becomes a member of the default network domain. If you direct the new network to a user-defined network domain, the network is also a member of that network domain. Like the default network domain, a user-defined network domain provides network resources to a server pool or virtualization host.

## User-Defined Network Domains

You create a network domain to support the use of virtualization hosts, server pools, or a virtual datacenter. For example, a virtual datacenter uses server, storage, and network resources in a dynamic way, allocating and releasing resources whenever necessary. The network domain provides the network resources to the virtual datacenter.

When you create a network domain, you can set a limit on the number of networks that can be created in the network domain. Increase the number of networks when accounts in a virtual datacenter are not able to create vnets.

## Editing Attributes of a User-Defined Network Domain

You can change the name and description of the network domain and you can change the number of dynamic networks that are in use simultaneously.

### To Edit Attributes of a Network Domain

1. Expand Libraries in the Navigation pane.
2. Expand Networks in the Navigation pane.
3. Select the network domain.
4. Click Edit Attributes in the Actions pane.

The Details tab is displayed in the center pane. The Name Description, and Number of Networks fields are now editable.

5. Edit the name or description or increase the number of networks.
6. Click Save.

## Networks

In Oracle Enterprise Manager Ops Center, networks are the discovered and managed IP subnets. Oracle Enterprise Manager Ops Center manages network resources for its virtualization hosts.

---

---

**Note:** A network is defined only within Oracle Enterprise Manager Ops Center. These networks are not the network connections for servers and chassis.

---

---

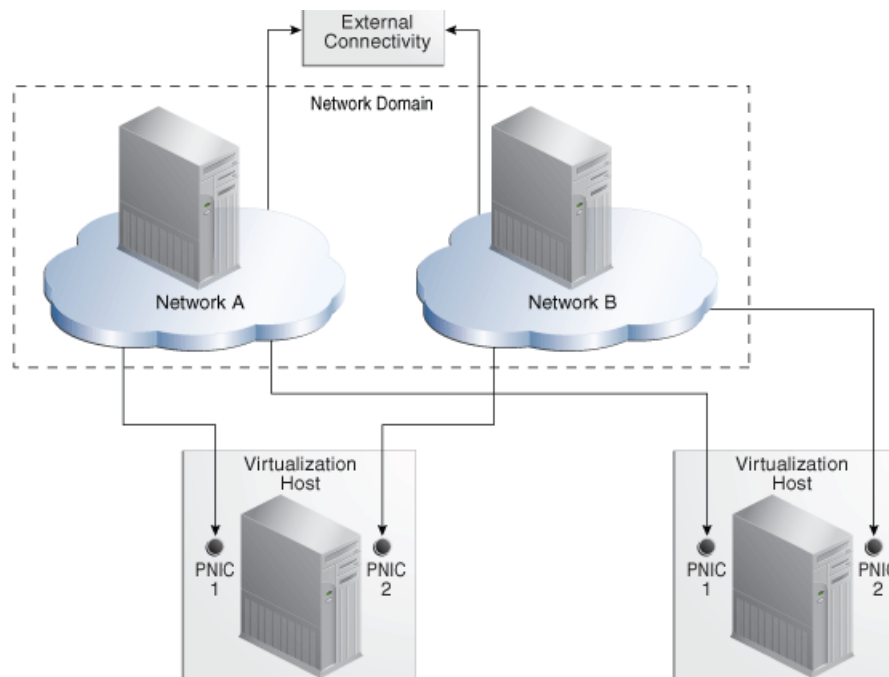
Networks are associated with server pools, which contain virtualization hosts, or standalone virtualization hosts. When you assign a network to a server pool, the network is accessible from each virtualization hosts in the pool and every guest of each virtualization host.

You can use networks to do the following:

- Manage individual virtualization hosts
- Connect virtualization hosts to the Proxy Controller
- Allow guests to communicate with each other or with the Internet
- Connect remote JMX with the public API

A network depends on the physical network interface card (PNIC) that is available to the host. You can create one network for each physical network interface card. If one host has two PNICs, it is a good practice to create two networks: a management network and a data network. Then place all guests on the data network, keeping them separate from the management network. The management network is dedicated to giving access to internal resources of the data center.

The following configuration shows how two virtualization hosts participate in two networks. The actual network connection is made to the PNICs in the virtualization host. Network A is connected to PNIC 1 of both hosts and Network B is connected to PNIC 2 of the hosts.

**Figure 7-1 Network with Virtual Hosts**

## Requirements for a Network

A network requires a physical network interface or a link aggregation and the following mandatory specifications:

- IP address of the network
- Netmask
- If you use static IP addressing, the IP address of the management interface  
If you use dynamic IP addressing, the range of allowed IP addresses and the gateway address

## Public Networks and Private Networks

Oracle Enterprise Manager Ops Center creates virtual networks and provides them to a virtual datacenter. These networks are created from the resources of the network domain as needed. These networks are displayed in the vDC Management section of the Navigation pane.

A virtual network defines a virtual IP subnet that is divided into public external networks and private external networks. You specify the size of the virtual network, which sets the maximum number of IP addresses for a public external network.

The public external network can be shared among the accounts in a virtual datacenter. You can attach virtual servers from different accounts in a single public external network. When you create a virtual server, you specify the number of public external networks to which it can be associated.

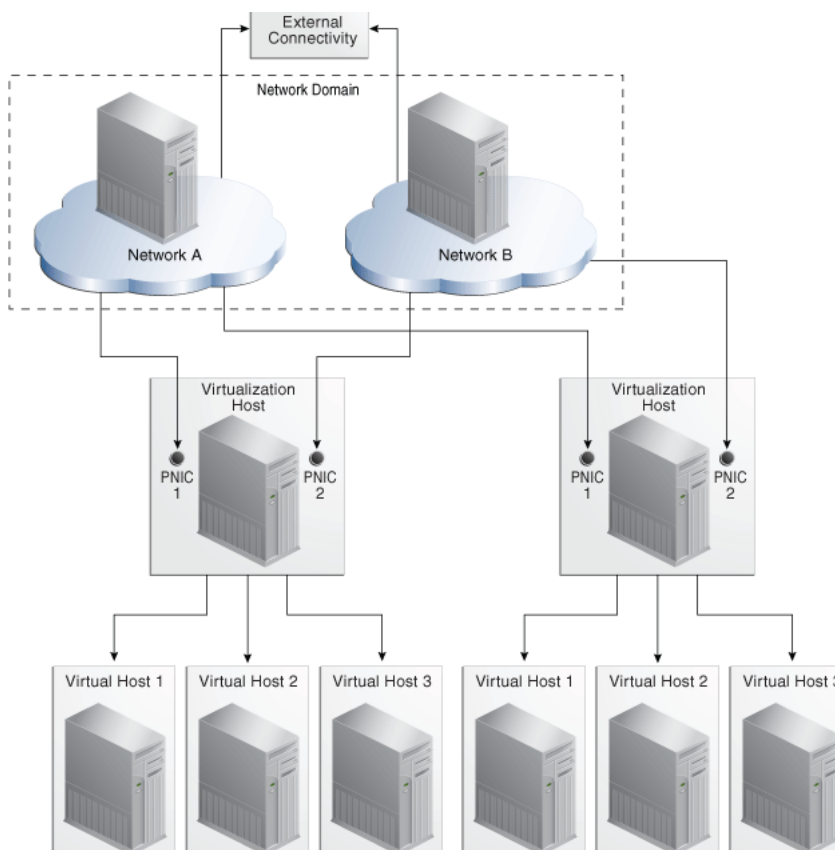
You can reserve the IP address in a public external network for an account use only. When you create a virtual server, you can provide the reserved IP address. Otherwise, the virtual server is allocated the IP address from the server pool.

## Networks for Server Pools

A server pool must have at least one network. When a server pool has more than one network, all virtualization hosts in the server pool are associated with the same set of networks. When you add a virtualization host to a server pool, the virtualization host has access to all the networks defined for the pool and can be an active member of the pool. This ensures that all virtual hosts have network access, even when you migrate a virtual host from one virtualization host to another one within the pool.

The following figure illustrates an example of network connections to two virtualization hosts in a server pool. This server pool has two virtualization hosts and two network associations.

**Figure 7-2 Network Connections for a Server Pool**



## Networks for Oracle Solaris Zones

You specify the networks that support a global zone. The network attached to a global zone also supports its non-global zones. You can attach one or more networks to a global zone using the Attach Networks action.

Although the fabric that supports the network does not change, you can specify the way the network works differently for each type of zone. A network that is assigned as shared on a global zone can be assigned as exclusive on another global zone.

- In Shared IP mode, the network interface is used by more than one zone. You define the network interface when you assign the global zone to the network.

- In Exclusive IP mode, the network interface is dedicated to the zone. An exclusive network must be declared for the global zone when you assign network to the global zone. Then you configure the IP configuration for the non-global zone.

For a complete description, see [Manage Global Zone Networks](#) in [Chapter 14](#).

## Networks for Oracle VM Servers

The Oracle VM Server Control Domain's network support is specified when the Oracle VM Server software is installed to provide networking facilities for the logical domains. For each network connection, a virtual switch is created.

For a complete description of networks for Oracle VM Server for SPARC, see [Attach Networks](#) in [Chapter 15](#).

For a complete description of networks for Oracle VM Server for x86, see [Manage Networks](#) in [Chapter 16](#).

## Networks for Virtual Datacenters

Each virtual datacenter uses server, storage, and network resources in a dynamic way, allocating and releasing resources when necessary.

The virtual datacenter inherits its network resources from the network domain that supports the server pool. These networks form the public external networks for the virtual datacenter. These networks can then be assigned to the accounts in the virtual datacenter. When the user of an account create a private vNet, either a dynamic private network is created or the static private network is made available for use in that account.

For a complete description of networks for virtual datacenters, see [vNets Creation and Network Setup](#) in [Chapter 18](#).

## Bandwidth Management

Bandwidth management for data links is available for Oracle Solaris 11 operating system. A data link is a physical NIC, an aggregated link, or a virtual NIC. You define the flow on the data link, prioritizing the network traffic on the link and setting the maximum bandwidth limit.

When a new data link is created, its default bandwidth flow is created by Oracle Solaris 11 operating system. You cannot remove this flow. The flow is removed only when the physical link is removed. However, you can create new flows for the data link. The flow for a network interface is specified by its local and the remote IP address, Internet Protocol, and the type of service.

To create a new flow for a data link, specify a name for the flow and the physical network interface. Then set the new bandwidth properties:

- Priority – Set the priority of the network traffic on the link as high, medium or low.
- Bandwidth Limit – Enable the bandwidth limit to allocate guaranteed bandwidth to the specified link. Enter the maximum value for bandwidth limit in Kbps, Mbps or Gbps
- Set attributes for the data flow to identify its network traffic:
  - Local and Remote IP - The source and destination IP address
  - Transport – The Internet Protocol used such as TCP, UDP, SCTP, ICMP.
  - Ports – The source and destination ports for TCP, UDP, and SCTP.



- DS Field – The type of service field in the IP packets' header.

### To View the Flows for a Data Link

1. Expand Assets in the Navigation pane.
2. Select an Oracle Solaris 11 operating system.
3. Click the Networks tab in the center pane.
4. Click the Bandwidth Management subtab in the center pane.

To modify a flow, click the Modify icon. To create a new link, click the Add icon.

## IP Multipathing Groups

Using IP Multipathing (IPMP), two or more physical network interface cards (NIC) form a group that use one IP address. If one NIC fails, the other NIC in the group maintains network access.

When you create a network, you define its network interface. The interface can be a physical network interface card (NIC) or, in the case of an Oracle Solaris OS asset, it can be an IPMP group or link aggregation. You can implement both methods on the same network because they work at different layers of the network stack. See the Oracle Solaris 11 documentation at [http://docs.oracle.com/cd/E23824\\_01/index.html](http://docs.oracle.com/cd/E23824_01/index.html) and Oracle Solaris 10 documentation at <http://www.oracle.com/technetwork/documentation/solaris-10-192992.html> for information about these services and how to implement IPMP.

---



---

**Note:** IPMP groups are supported only for IPv4 protocol.

---



---

IPMP provides increased reliability, availability, and network performance for systems with multiple physical interfaces. It provides physical interface failure detection and transparent network access failover.

Occasionally, a physical interface or the networking hardware attached to that interface might fail or require maintenance. By using IPMP, you can configure one or more physical interfaces into an IPMP group. After configuring the IPMP group, the system monitors the interfaces in the IPMP group for failure. If an interface in the group fails or is removed for maintenance, IPMP migrates, or fails over, the failed interface's IP addresses. The failover feature of IPMP preserves connectivity and prevents disruption of any existing connections.

The association between an IPMP group and a network must be unique; an IPMP group can be associated with only one network and a network can be associated with only one IPMP group or individual NICs.

In an IPMP group, you define whether each interface is a failover or a standby one. The actions of each type differ if the current network interface fails:

- Network access changes from the failed interface to the failover interface in the IPMP group and uses the failover interface data address. You must provide the data address for an interface that is defined as failover.
- Network access changes from the failed interface to the standby interface in the IPMP group but does not change its data address. The data address of the failed interface migrates to the standby interface.

Link-based failure detection in an IPMP group is always enabled if your interface supports this type of failure detection. You can also set for probe-based failure detection by providing a test address for each interface in the group.

You can create a single IPMP group while provisioning an operating system. If you create IPMP groups manually, Oracle Enterprise Manager Ops Center identifies and displays the groups on the UI.

## Link Aggregation or Bond

In an aggregated link, two or more NICs form a group and all members of the link aggregation provide network access at the same time. In addition to the high availability and load balancing that an IPMP group provides, an aggregated link can also provide increased throughput if the network ports are also aggregated.

When you create a network, you define its network interface. The interface can be a physical network interface card (NIC) or, in the case of an Oracle Solaris OS asset, it can be an IPMP group or link aggregation. You can implement both methods on the same network because they work at different layers of the network stack. See the Oracle Solaris 11 documentation at [http://docs.oracle.com/cd/E23824\\_01/index.html](http://docs.oracle.com/cd/E23824_01/index.html) and Oracle Solaris 10 documentation at <http://www.oracle.com/technetwork/documentation/solaris-10-192992.html> for information about these services and how to implement link aggregation.

Link aggregation is a standard defined in IEEE802.3ad. An aggregated link consists of several interfaces on a system configured as a single, logical unit. Link aggregation increases the speed and high availability of a connection between a server and a switch. The most common protocol used to manage link aggregation is LACP (Linked Aggregation Control Protocol).

You can create one link aggregation while provisioning an OS. You can configure the interfaces together as a logical unit and define the link aggregation information if the following conditions are met:

- All the members of the aggregated link are connected to the same switch.
- The members of the aggregated link are of the same type. For example, NICs with the `e1000g` interface cannot be mixed with NICs that use the `bge` interface.
- For Oracle Solaris OS, the required driver is `GLDv3`.

When interfaces have been aggregated, they are treated as a single network interface. Oracle Enterprise Manager Ops Center displays the link aggregation in the list of available NICs as if it were an individual interface. When you assign a network with a link aggregation to an Oracle VM Server, logical domain, global zone, or a non-global zone, select the link aggregation from the NIC list. You can view the link aggregation details on the Oracle VM Server's or global zone's Network tab.

## Properties of a Network

The characteristics of a network are displayed in its Network Details tab. You can edit the network name and description, MTU size, assignable IP range, and default gateway. The network IP address, netmask, and its network type cannot be changed. You can also enable and disable DHCP service, VLAN tagging, and manage the static routes of the network. To change the MTU size, see the instructions in [Maximum Transmission Unit \(MTU\)](#).

## IPv4 and IPv6 Protocols

Some environments have a mix of IPv4 and IPv6. Oracle Enterprise Manager Ops Center is "IPv6-aware." If an asset has an IPv6 network interface, Oracle Enterprise Manager Ops Center can read it and displays its information, but it cannot provision an IPv6 network or use IPv6 networks to discover, monitor, or provision assets.

## Routing Mode

A virtual host uses the network assigned to it according to the host's routing mode. You specify a virtual host's routing mode during its initial configuration if you do not accept the default mode, Automatic Routing. Oracle Enterprise Manager Ops Center supports the following routing modes:

- Automatic Routing – This is the default routing mode. Applying the static routes depends on the following conditions:
  - If your site defined a default gateway or static route or retrieved one from the DHCP server, this route is used and dynamic routing is disabled.
  - If no default gateway or static route is available, dynamic routing is enabled.
- Dynamic Routing Off – The virtual host uses the default gateway and any static routes configured for the network. The default gateway is retrieved from the DHCP server.
- Dynamic Routing On – The virtual host uses routes provided by the dynamic routing service. The default gateway and any static routes configured for the network are ignored.

## Static Route for the Network

Static routes specify the route for external access. Although you define a default gateway for a network, it might not reach a particular subnet. In this case, you must also provide a static route for the subnet.

When you create a network, you can specify the static route. To add static routes after the network has been created, use the following procedure.

### To Add a Static Route for the Network

1. Click Managed Networks in the Navigation pane.
2. Select a network from the list of networks.
3. Click Edit Network Attributes in the Actions pane.
4. Click the Add icon in the Static Routes table. A row is added to the table.
5. Type the values for destination IP, netmask, and gateway.
6. Click Finish.

You can delete a static route and change the order of the routes using the icons in the Static Routes table.

## Address Allocation Method

When you create a network, you specify how its IP address is assigned:

- Static IP: A specific IP address is assigned to the network
- Automatic: An available IP address is assigned to the network.

## Maximum Transmission Unit (MTU)

The default size for the network's Maximum Transmission Unit (MTU) is 1500 bytes. If your network interface card is one of the following types, you can change the size of the MTU to a size between 576 and 9216 bytes. However, to assign the network to a logical domain, the minimum MTU size is 1500 bytes.

- nxge
- ixgbe
- hxge
- e1000g
- ce
- bge
- ipge

When you specify a size greater than 1500 bytes, Oracle Enterprise Manager Ops Center modifies the network interface card's MTU size. For other types of network interface cards, the MTU is changed when the card's driver firmware is updated to support the new MTU size. However, to change the MTU value for an IPMP group, you must edit the MTU value manually.

---

---

**Note:** When you provision an operating system, the MTU size resets to the default value. You must change the MTU again after you provision the system.

---

---

## VLAN and VLAN Tags

For fabrics based on Ethernet protocol, the ability to use VLAN tags is an attribute of each network. Use the Edit Network Attributes action to add or change the VLAN capability.

## Network Utilization

Oracle Enterprise Manager Ops Center collects information every five minutes on every managed asset and displays the last hour of data on the asset. To see utilization data for a network over longer periods of time, up to six months, create a Network Utilization chart, which includes operating system, operating system for a virtual machine, virtual host, and server pool. You can also create a network utilization chart for an OS group or host group.

## Network Connectivity

Connectivity is the network interface of the system. You can view information about a hardware asset's Network Interface Card (NIC) on the Connectivity tab of the asset's dashboard, including name, connection status, MAC address, and the corresponding IP address.

For switch hardware, the Connectivity tab shows information about each port.

For an Oracle Solaris OS, the Connectivity tab includes IPMP groups and aggregated links.

- The IPMP Groups subtab shows the group's name, its assigned network, and the type of failure detection, either link-based, probe-based, or both. For each IPMP

group, the details include the state of the connection for each NIC, whether it is in standby mode or failover mode, and the IP address the NIC supports.

- The Link Aggregation sub tab shows the aggregation's name, its MAC address, and its attributes. For each aggregated link, shows the state of the connection for each NIC, whether it is in standby mode or failover mode, and the IP address the NIC supports.

## Network Hardware

Oracle Enterprise Manager Ops Center can manage Sun Ethernet 10GbE Fabric switches and Sun Datacenter InfiniBand switches. These switches reside in the system or blade system and provide the switch fabric.

The InfiniBand Gateway switch can expose the ports of a server that resides on an InfiniBand partition to an Ethernet network. To create an Ethernet on InfiniBand (EoIB) interface on the switch, you associate the switch's external port (eport) with the InfiniBand partition where the server resides, creating a virtual NIC (vNIC). The server's ports are displayed on the Switch Connectivity tab in the center pane.

For more information about these switches, see [Switch Details](#) or see [Related Resources for Networks](#) for links to the switch documentation.

## Network Interface Card (NIC)

The Network Interface Card (NIC) is the physical connection to a network. To see the NICs for a server, select the server and then click the Connectivity tab. The Server Processor Connectivity table lists all of the NICs.

## Network Switches

Oracle Enterprise Manager Ops Center can manage Sun Ethernet 10GbE Fabric switches and Sun Datacenter InfiniBand switches. These switches reside in the system or blade system and provide the switch fabric.

For the Ethernet switches, both tagged and untagged VLANs are supported.

If you use an InfiniBand switch in an Ethernet network, the ports on the switch have Ethernet names.

For more information about these switches, see the product documentation:

- For the Sun Ethernet 10GbE Fabric switch, see <http://docs.oracle.com/cd/E19934-01/index.html>
- For Sun Datacenter InfiniBand switch, see <http://docs.oracle.com/cd/E19654-01/index.html>

## Network Profiles

Oracle Enterprise Manager Ops Center provides default profiles for the following operations:

- Deploy a network – Create a network.
- Monitor a network – Monitor for changes in membership and attributes, and any problems in the physical fabric, such as a change in port or link status.
- Monitor Network hardware – Reports Cisco switch's connection to assets on the Switch Connectivity tab.

- Discover a switch – Use a discovery profile with Cisco iOS credentials.

## Oracle Enterprise Manager Ops Center's Networks

This section describes the requirements for the networks that Oracle Enterprise Manager Ops Center uses. This section does not discuss the networks that support virtual hosts and server pools.

You can implement Oracle Enterprise Manager Ops Center's network connections using any combination of VLANs and switches. However, each network, whether management, provisioning, or data, must be assigned to separate VLANs.

### Network Switch Configuration

Use these guidelines to configure a network switch for a system running the Oracle Enterprise Manager Ops Center software.

- Use an Virtual LAN (VLAN)-capable switch.
- Discover and manage the switch.
- Create a separate VLAN for Oracle Enterprise Manager Ops Center management and provisioning networks.

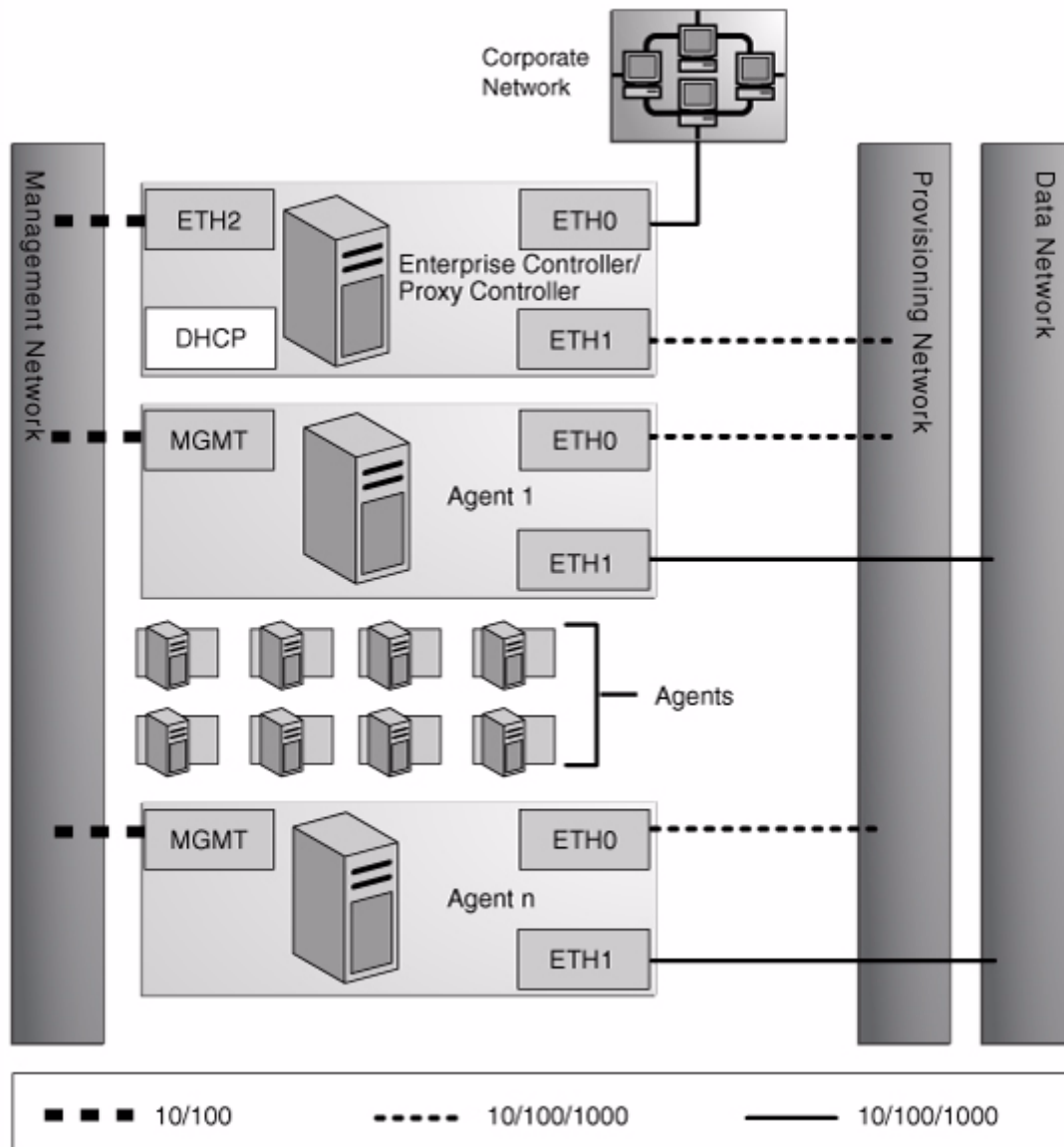
For Ethernet connectivity:

- The management network must be a 10/100 connection.
- The provisioning and data networks must be at least a 10/100/1000 (1 GB) connection.

### Separate Management, Provisioning, and Data Networks

- Separate networks provide the highest security and the lowest number of points of failure.
- Additional NICs are needed to support this configuration.

Figure 7-3 Separate Management, Provisioning, and Data Networks



A configuration with separate management, provisioning, and data networks has these requirements:

- Enterprise Controller/Proxy Controller
  - ETH0 connects the Enterprise Controller/Proxy Controller to the corporate network for external access. Configure the ETH0 IP address, netmask, and gateway to meet corporate connectivity requirements.
  - ETH1 connects the Enterprise Controller/Proxy Controller to the provisioning network and must be on the same network as the ETH0 connections of the Agent Controllers. Only the Enterprise Controller/Proxy Controller and the Agent Controllers must reside on the provisioning network. ETH1 must be a 1 Gb NIC interface.
  - ETH2 connects the Enterprise Controller/Proxy Controller to the management network and must be on the same network as the management port connections of the Agent Controllers. Configure the ETH2 IP address,

netmask, and gateway to enable connectivity to the Agent Controllers' management port IP addresses. ETH2 must be a 100 Mb NIC interface.

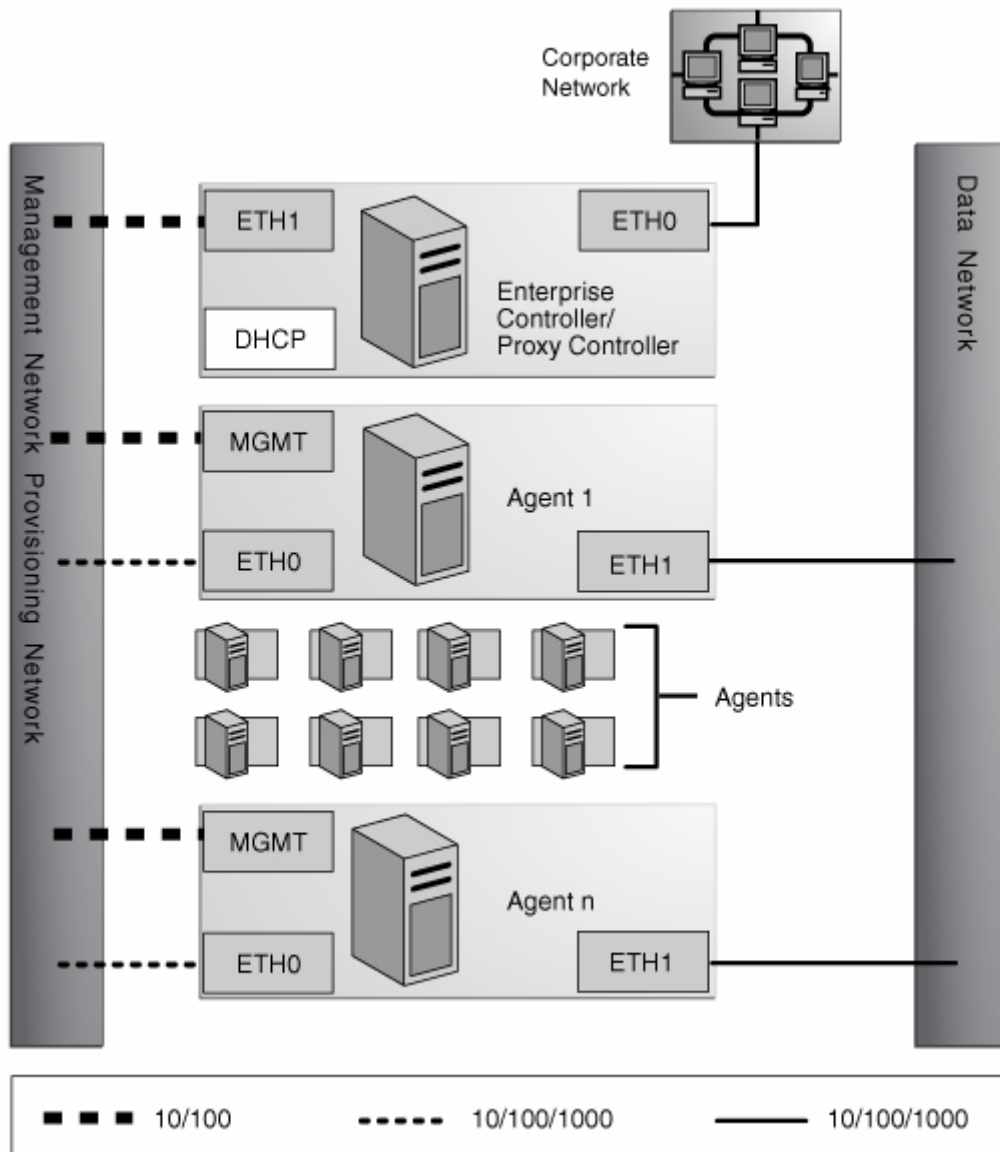
- The DHCP service allocates IP addresses to the Agent Controllers for provisioning operating systems.
- Agent Controllers
  - Each Agent Controller's management port connects the Agent Controller to the management network and must be on the same network as the ETH2 connection of the Enterprise Controller/Proxy Controller. The management port must be a 100 Mb connection.
  - ETH0 connects the Agent Controller to the provisioning network and must be on the same network as the ETH1 connection of the Enterprise Controller/Proxy Controller. ETH0 must be a 1 GB connection.
  - ETH1 connects the Agent Controller to the data network through the switch to provide corporate network access to the Agent Controller. ETH1 must be a 1 GB connection.

### **Combined Management and Provisioning Network and a Separate Data Network**

- Reduced system and network security.
- No additional NIC is needed on the Enterprise Controller or Proxy Controller.



Figure 7-4 Combined Management and Provisioning Network and a Separate Data Network

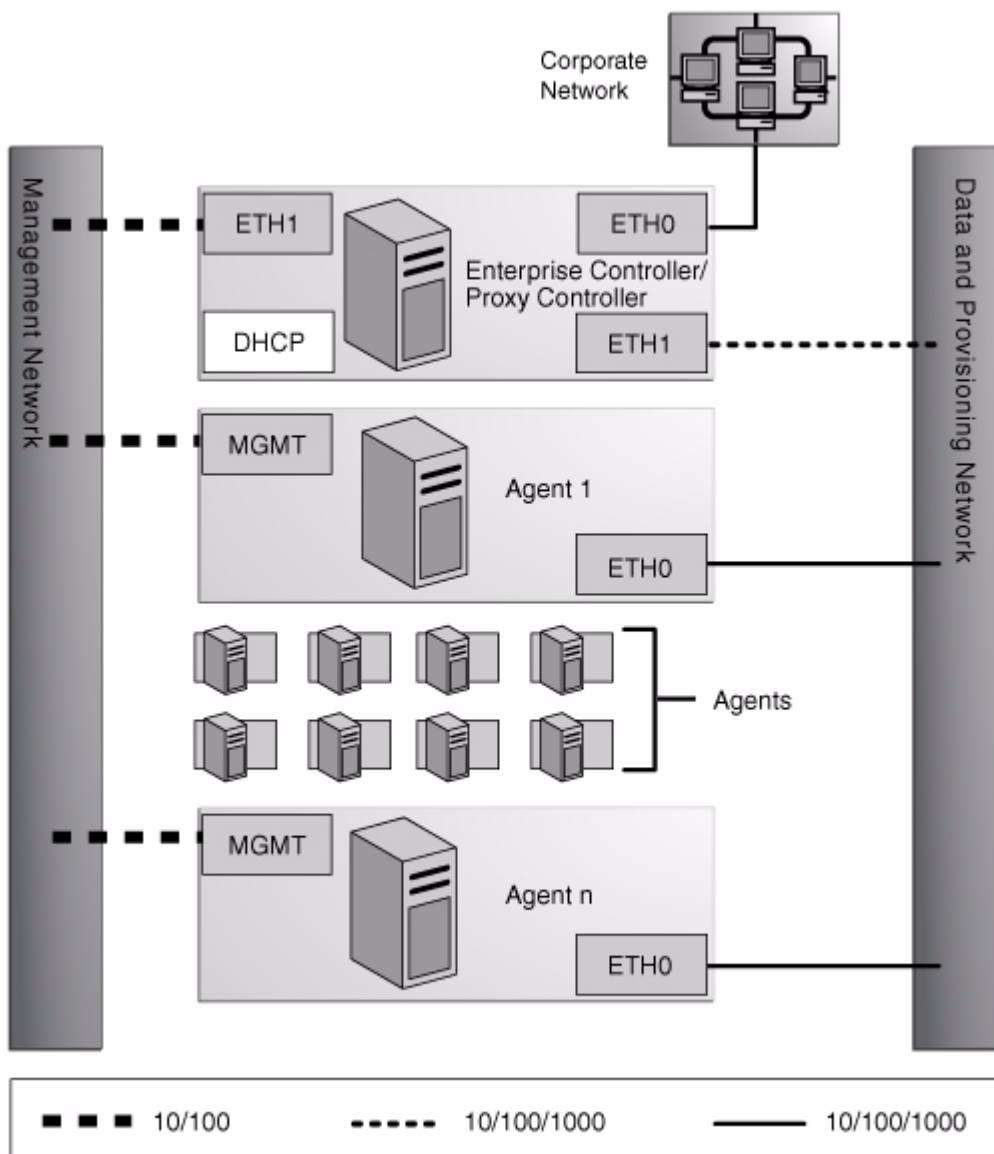


- Enterprise Controller/Proxy Controller
  - ETH0 connects the Enterprise Controller/Proxy Controller to the corporate network to provide external access. Configure the ETH0 IP address, netmask, and gateway to meet corporate connectivity requirements.
  - ETH1 connects the Enterprise Controller/Proxy Controller to the management and provisioning network and must be on the same network as the MGMT and ETH0 connections of the Agent Controllers. Only the Enterprise Controller/Proxy Controller and the Agent Controllers must reside on the management and provisioning network. The ETH1 IP address, netmask, and gateway must be configured to enable connectivity to the Agent Controller's management port IP addresses. ETH1 must be a 1 Gb NIC interface.
  - The DHCP service allocates IP addresses to the Agent Controllers for provisioning operating systems.
- Agent Controllers

- Each Agent Controller's management port connects the Agent Controller to the management and provisioning network and must be on the same network as the ETH1 connection of the Enterprise Controller/Proxy Controller. The management port must be a 100 Mb connection.
- ETH0 connects the Agent Controller to the management and provisioning network and must be on the same network as the ETH1 connection of the Enterprise Controller/Proxy Controller. ETH0 must be a 1 GB connection.
- ETH1 connects the Agent Controller to the data network through the switch to provide corporate network access to the Agent Controller. ETH1 must be a 1-GB connection.

## Combined Provisioning and Data Network and a Separate Management Network

Figure 7-5 Combined Provisioning and Data Network and a Separate Management Network



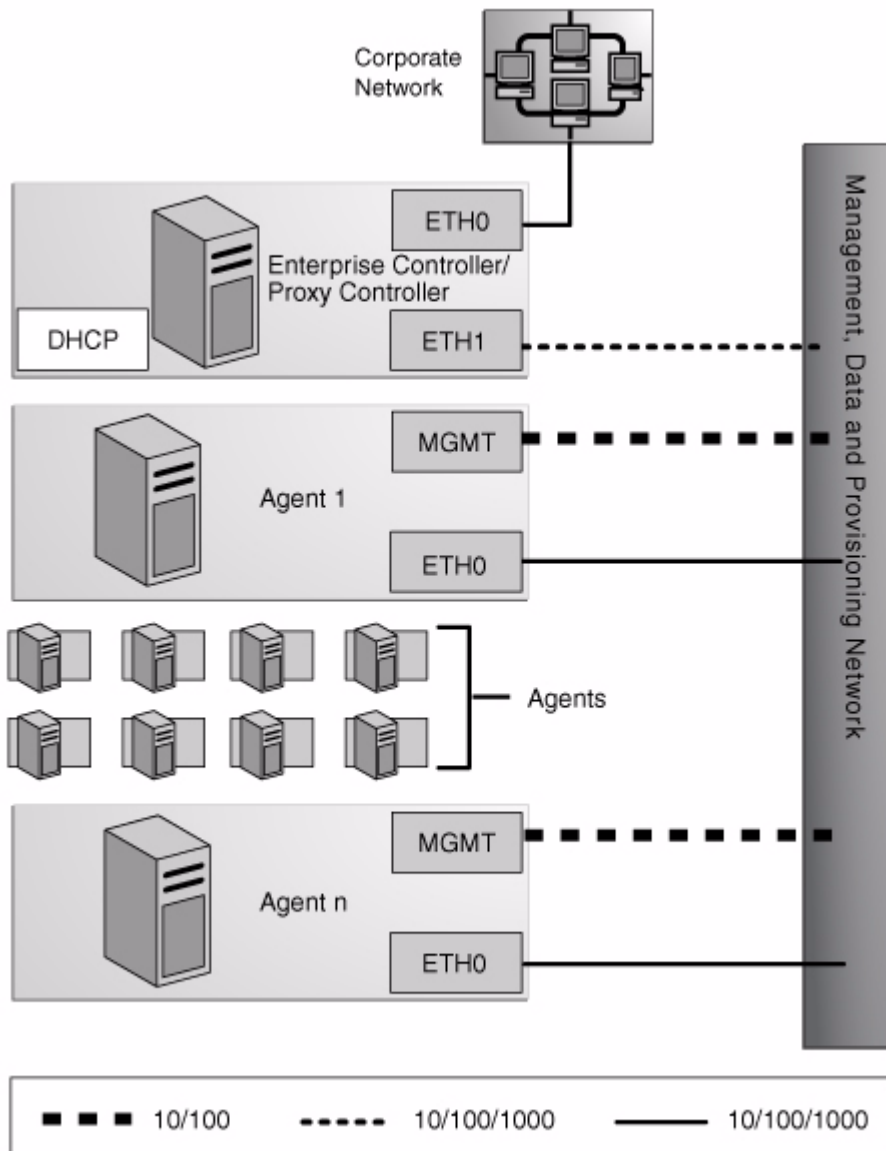
- Enterprise Controller/Proxy Controller

- ETH0 connects the Enterprise Controller/Proxy Controller to the corporate network to provide external access. Configure the ETH0 IP address, netmask, and gateway to meet corporate connectivity requirements.
- ETH1 connects the Enterprise Controller/Proxy Controller to the provisioning and data network and must be on the same network as the ETH0 connections of the Agent Controllers. Only the Enterprise Controller/Proxy Controller and the Agent Controllers must reside on the data and provisioning network. ETH1 must be a 1 Gb NIC interface.
- ETH2 connects the Enterprise Controller/Proxy Controller to the management network and must be on the same network as the management port connections of the Agent Controllers. Configure the ETH2 IP address, netmask, and gateway to enable connectivity to the Agent Controller's management port IP addresses. ETH2 must be a 100 Mb NIC interface.
- The DHCP service allocates IP addresses to the Agent Controllers for provisioning operating systems.
- Agent Controllers
  - The management port connects the Agent Controller to the management network and must be on the same network as the ETH2 connection of the Enterprise Controller/Proxy Controller. The management port must be a 100 Mb connection.
  - ETH0 connects the Agent Controller to the data and provisioning network to provide corporate network access to the Agent Controller. ETH0 connection must be on the same network as the ETH1 connection of the Enterprise Controller/Proxy Controller. ETH0 must be a 1 GB connection.

### **Combined Provisioning, Data, and Management Network**

- Least secure system and network
- No additional NIC is needed for the Enterprise Controller/Proxy Controller.

**Figure 7–6 Combined Provisioning, Data, and Management Network**



- Enterprise Controller/Proxy Controller
  - ETH0 connects the Enterprise Controller/Proxy Controller to the corporate network to provide external access. Configure the ETH0 IP address, netmask, and gateway to meet corporate connectivity requirements.
  - ETH1 connects the Enterprise Controller/Proxy Controller to the combined management, provisioning, and data network and must be on the same network as the MGMT and ETH0 connections of the Agent Controllers. Only the Enterprise Controller/Proxy Controller and the Agent Controllers must reside on the combined network. ETH1 must be a 1 GB NIC interface.
  - The DHCP service allocates IP addresses to the Agent Controllers for provisioning operating systems.
- Agent Controllers

- Each Agent Controller's management port connects the Agent Controller to the management, provisioning, and data network and must be on the same network as the ETH1 connection of the Enterprise Controller/Proxy Controller. The management port must be a 100 MB connection.
- ETH0 connects the Agent Controller to the management, provisioning, and data network, and must be on the same network as the ETH1 connection of the Enterprise Controller/Proxy Controller. ETH0 also connects the Agent Controller to the data network through the switch to provide external corporate network access to the Agent Controller. ETH0 must be a 1 GB connection.

## Firewall Rules

The Enterprise Controller must reach some external sites. If you have explicit firewall rules enabled to allow access to these services from your Enterprise Controller, you must update these rules to allow access to the following addresses:

**Table 7-4 IP Address and Port Requirements**

Site	IP Address	Port	Purpose
java.net	-	Port 80 and Port 443	Updates to OCDoctor utility Access to Oracle Solaris Cluster profiles and scripts.
login.oracle.com getupdates.oracle.com	192.18.110.9	Port 443	Access to Oracle Knowledge Base for OS updates
inv-cs.oracle.com	192.18.110.10	Port 443	Product registration
hs-ws1.oracle.com	192.18.110.11	Port 443	Product registration
support.oracle.com	141.146.54.16	Port 443	My Oracle Support
www.oracle.com	96.17.111.33 and 96.17.111.49	Port 80	-

## Network Port Requirements and Protocols

This section lists the ports and protocols used by Oracle Enterprise Manager Ops Center.

The Enterprise Controller's default port is 443. If port 443 is in use, the Enterprise Controller uses Port 11165. The following table describes the required ports and their protocols.

**Table 7-5 Required Ports and Protocols**

Communication Direction	Protocol and Port	Purpose
Enterprise Controller	Port 8005	Enterprise Controller in Disconnected mode
Enterprise Controller	Port 443, then Port 11165	Enterprise Controller in Connected mode
OCDoctor to java.net	HTTPS, TCP: Port 443	To acquire updates.
Browser to Enterprise Controller	HTTP, TCP: Port 80	Redirects to port 9443
Browser to Enterprise Controller	HTTPS, TCP: Port 9443	Web interface

**Table 7-5 (Cont.) Required Ports and Protocols**

Communication Direction	Protocol and Port	Purpose
Enterprise Controller to Database	Port 11176	Oracle Listener port for local database
Enterprise Controller to Proxy Controller	SSH, TCP: Port 22 ICMP ping: Type 8 Code 0 (echo request)	Enterprise Controller installs or upgrades a Proxy Controller through the UI.
Proxy Controllers to Enterprise Controller	HTTP: Port 8004 HTTPS, TCP: Port 443 ICMP ping: Type 0 Code 0 (echo reply)	WAN boot traffic Proxy Controller pushes data about assets to Enterprise Controller. Proxy Controller pulls data for jobs, updates, Agent Controllers, and OS images from the Enterprise Controller. Proxy Controllers use ICMP ping during upgrades.
Proxy Controller to Targets	FTP <sup>1</sup> , TCP: Port 21 SSH, TCP: Port 22 Telnet <sup>2</sup> , TCP: Port 23 DHCP: Port 67 SNMP, UDP: Port 161 IPMI, TCP+UDP: Port 623 Service Tags, TCP: Port 6481 ICMP ping: Type 8 Code 0 (echo request)	Proxy Controller discovers, manages, and monitors assets Proxy Controller performs bare-metal provisioning DHCP is used for OS provisioning.
Target to Proxy Controller	DHCP: Port 68 SNMP, UDP: Port 162 ICMP ping: Type 0 (echo reply)	Asset reports status on update operation. Proxy Controller receives ICMP ping Type 3 (destination unreachable) for failed connection.
Agent Controller to Proxy Controller	HTTPS, TCP: Port 21165	Agent Controllers push asset data to Proxy Controller. Agent Controllers pull data for jobs.
Agent Controller to Proxy Controller	HTTPS, TCP: Port 8002	Agent Controllers pull updates from Proxy Controller.
Agent Controller on Oracle Solaris OS and hardware to Proxy Controller	SNMP: Port 1162, then ports 1100 through 1200	For monitoring, Agent Controller sends trap notifications and fault management (FMA)
Proxy Controller to OS Host	SSH, TCP: Port 22 Telnet <sup>2</sup> , TCP: Port 23 TCP: Port 6481 (discovery, monitoring by service tags) DHCP, UDP: Ports 67, 68 ICMP, Type 0 Code 0 (echo reply)	Proxy Controller discovers, manages, and monitors asset. Proxy Controller performs bare-metal OS provisioning

**Table 7–5 (Cont.) Required Ports and Protocols**

<b>Communication Direction</b>	<b>Protocol and Port</b>	<b>Purpose</b>
OS Host to Proxy Controller	HTTP, TCP: Port 8004 Oracle Solaris 11 Automated Installer: Port 5555	OS Host reports status of OS provisioning and status of Agent Controller installation.  OS Host downloads Agent Controller archive file.  The Automated Installer Web Server for Oracle Solaris 11 opens Port 5555 to accept requests from the OS Hosts during Oracle Solaris 11 provisioning. For provisioning handled by DHCP, the open port is on the Proxy Controller. For provisioning handled by WAN boot, the open port is on the Enterprise Controller or a Proxy Controller.
OS Host to Proxy Controller	DHCP, UDP: Ports 67, 68 TFTP, UDP: Port 69 TCP+UDP: Port 37 ICMP ping, Type 8 Code 0 (echo request)	OS Host responds to Proxy Controller inquiries during bare-metal OS provisioning
Java client to public APIs	Transport Layer Security (TLS): Port 11172	JMX access from clients
WMI client to Agent Controller	Port 11162	WMI client resides on the Proxy Controller and communicates with the WMI server on the Agent Controller.  The Proxy Controller uses the DCOM protocol to monitor a Windows system. The Proxy Controller opens a TCP connection to the Windows DCOM registry port, TCP 135, which provides a lookup service to the WMI scripting DCOM object. The Proxy Controller connects to the DCOM object. The port number for this connection is allocated by the Windows system.
Proxy Controller to NFS server	Use an NFS server that is on the same side of the firewall as the Proxy Controller.  Refer to your OS documentation to set up the NFS server.	Proxy Controller pulls provisioning images from NAS Library
Global Zones or Oracle VM Servers to NFS server	Use an NFS server that is on the same side of the firewall as the Proxy Controller.  Refer to your OS documentation to set up the NFS server.	Global Zones and Oracle VM Servers push their metadata and virtual host images to NAS Library
Proxy Controller to Service Processors	SSH, TCP: Port 22 Telnet <sup>2</sup> , TCP: Port 23 IPMI, TCP, UDP: Port 623 TCP: Port 6481 (discovery by service tags)	Proxy Controller discovers, manages, and monitors asset.  Proxy Controller performs bare-metal OS provisioning and firmware provisioning.

**Table 7–5 (Cont.) Required Ports and Protocols**

Communication Direction	Protocol and Port	Purpose
Proxy Controller to Service Processors	SNMP, UDP: Port 161 TCP: Port 6481 by service tags	Proxy Controller sends inquiries to service processors.
Service Processors to Proxy Controller	FTP <sup>1</sup> , TCP: Port 21 TFTP, UDP: Port 69	Service processors report status of firmware provisioning.
Service Processors to Proxy Controller	SNMP, UDP: Port 162	Service processors report status.

<sup>1</sup> The FTP protocol is used only by servers with the ALOM service processor or by SPARC Enterprise M-Series servers.

<sup>2</sup> The telnet protocol is used only by servers with the ALOM service processor.

## Related Resources for Networks

For instructions in performing actions or to learn more about the role of this feature, go to one of the following resources.

- For the Sun Ethernet 10GbE Fabric switch, see <http://docs.oracle.com/cd/E19934-01/index.html>
- For Sun Datacenter InfiniBand switch and gateway, see <http://docs.oracle.com/cd/E19654-01/index.html>



---

---

## Plans and Profiles

This chapter provides an overview of the concepts of profiles, policies, and plans. Detailed information is covered in the corresponding feature chapters.

The following information is included:

- [Introduction to Plans and Profiles](#)
- [Roles for Plans and Profiles](#)
- [Operational Profiles and Plans](#)
- [Profiles and Policies](#)
- [Deployment Plans](#)
- [Actions for Deployment Plans](#)
- [Location of Profiles and Plans in the User Interface](#)
- [Related Resources for Plan Management](#)

### Introduction to Plans and Profiles

Oracle Enterprise Manager Ops Center uses a combination of profiles and plans to reduce complexity and increase consistency when you perform standard management and operational activities. Templates are available in the Plan Management section of the UI. You use templates to create customized profiles and plans for your environment.

The software uses profiles and plans to create a reusable set of procedures to perform tasks, such as provisioning and updating. You create, manage, and access all profiles and plans in the Plan Management section of the user interface.

A profile defines how a task is performed and enables you to define what is allowed, and not allowed, to be installed on a system. A plan provides the steps to complete an operation, defines the targets upon which the tasks are performed, and enables you to deploy the profile to the targets. Together, plans and the associated profiles enable you to define operations. You create your own profiles and plans from a set of templates.

Plan Management contains three basic components:

- **Operational Profiles and Plans** – Perform one or more operational activities, such as scripts and utilities to fix common problems, monitoring rule configurations and thresholds, and a knowledge base that you can create based on the incidents that occur in your environment.
- **Profiles and Policies** – Profiles define the configuration of components for a specific type of system and task, such as the naming schema and configuration

options to use when creating a new Oracle Solaris 10 zone. Update policies define the level of interaction you want when applying patches and packages.

- Deployment Plans – Perform standard management activities, such as provisioning and creating Oracle Solaris Zones.

To see all profiles and plans, expand Plan Management in the Navigation pane. Select the profile or plan to see the available actions. For each plan, you can define the course of action to take when a step cannot be completed on a target. You can choose to stop the job at the first failure, or attempt to complete as much as possible.

Deployment plans are all based on a set of pre-defined templates. You can use the available templates to create customized profiles and plans for your data center. Some templates are designed for simple tasks and other, more complex plans, are designed to perform a series of functions. You can build complex plans by combining existing plans, for example, adding an operational profile and plan to the end of a deployment plan.

## Version Control

Profiles and plans versions are numbered sequentially. When you create a profile or plan, the version number is one. When you edit a profile or plan, you create a version that is referenced by a new number.

When you create a version, you have the option to automatically change the related plan during the update. When you do not choose that option, the operational and deployment plans that are using the profile are not updated with the new version. For example, you have a firmware profile that is using firmware image A, the profile version is one. You want to update the profile to use the latest firmware image, B. When you update the profile to change the image to B, version two of the profile is created. When you have five plans that are using version one of the firmware profile, all of those plans continue to use version one and image A. When you want the plans to use image B, you must manually update the plans to reference version two of the profile.

The same is true for plans. When you edit a deployment plan that is referred to by another plan in a complex plan, the referring plan is not automatically updated to refer to the edited plan's version unless you choose the option when you edit the plan.

You can view version details by highlighting the plan, then clicking the View Version Details icon. Use the arrows to view the different versions. When you want a plan to use the new version of the profile, edit the plan and associate it with the correct version of the profile. You can edit the following fields in an Operational Plan: Description, Failure Policy, and Associated Profile. You cannot edit the name of a profile or plan. When you want a different name, you must copy or create a profile and plan.

You can delete a version of a profile or plan. When you delete a version and more than one version exists, the previous version becomes the default. When only one version of the plan exists, both the profile and plan are deleted. When the plan is used in other plans, then the Delete Deployment Plan option is not enabled.

## Roles for Plans and Profiles

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 8–1 Plan Management Roles and Permissions**

<b>Task</b>	<b>Role</b>
View a profile or plan	Read
Create a profile or plan	Profile Plan Administrator
Edit a profile or plan	Profile Plan Administrator
Copy a profile or plan	Profile Plan Administrator
Delete a profile or plan	Profile Plan Administrator
Create a profile or plan	Profile Plan Administrator

## Operational Profiles and Plans

Operational profiles are designed to assist you in the day-to-day operation of your data center.

An Operational Profile performs one or more tasks needed to operate your environment. The profile contains a single shell script and can include asset attributes as environmental variables. For each profile, you can choose one of the following types of shell scripts:

- **EC Shell** – The script runs only on the Enterprise Controller. It is executed with the logged-in user's credentials.
- **Remote Shell** – The script can run on any managed system that contains a remote agent. It is executed with root permissions.

You have the option of adding two types of variables to operational profiles:

- **System defined variables** – Use these variables to define specific information in the script. The following are software-specific variables:
  - \$OC\_TARGET\_NAME
  - \$OC\_JOB\_ID
  - \$OC\_SASL\_FILE
  - \$OC\_UFN
  - \$OC\_TARGET\_TYPE
- **Additional Variables** – Use these variables to add information to the script and enable users to change that information when they execute the operational plan. Additional variables are user-defined.

A list of supported asset attributes is available in [Appendix A, "Asset Attributes"](#).

An Operational Plan is required to execute an Operational Profile and is created by default when you create an Operational Profile. You can use the plan to execute the profile on a managed resource or group of resources, such as performing state changing actions.

You can create a simple plan, such as disabling print capabilities, and deploy the plan across a group of resources in your data center. A more sophisticated example is to create several Operational Plans and add them as steps in a complex type Deployment Plan. For example, you can create an Operational Plan to shut down all logical domains and another Operational Plan to shut down an Oracle VM Server for SPARC. You can then add these plans as steps in a complex Deployment Plan.

## Actions for Operational Profiles and Plans

You can perform the following actions, depending on the role:

- [Create an Operational Profile and Plan](#)
- [Edit an Operational Profile or Plan](#)
- [Copy an Operational Profile](#)
- [Delete an Operational Profile or Plan](#)

## Create an Operational Profile and Plan

An Operational Plan defines how an Operational Profile is deployed, and against which targets. By default, creating a profile also creates an Operational Plan.

You can save a shell script on the Enterprise Controller and download it into the plan, or you can enter the script in a text field when you create the plan. Both types of shell scripts are executed by the user. They differ in the location, either on the Enterprise Controller or on the remote Agent, and the user credentials needed to execute the profile.

An operational plan defines the targets and failure policy for an operational profile. The profile defines one or more operations that are to be performed on a managed resource or group of resources. For example, deploying thresholds onto a managed resource, or performing state changing actions such as shutting down all logical domains and then shutting down an Oracle VM Server for SPARC.

The profile uses a shell script to define the operations. When you do not have an operational profile, you can create a profile when you create the plan. When you create the profile, either download a shell script that is on the Enterprise Controller (EC Shell script), or enter the shell script (Remote Shell script) in the profile. The EC Shell and Remote Shell are both shell scripts that are executed by the user. They differ in the location (on the Enterprise Controller or on the remote Agent) and manner (user credentials) of the execution. The EC Shell is executed with the credentials of the user that is logged in. The Remote Shell can run on any managed system that contains a remote agent and is executed with root permissions.

1. Expand Plan Management in the Navigation pane, then click Operational Profiles.
2. Click Create Profile.
3. Name the new profile and add a description. Select a subtype from the list to identify the type of target for this profile. Click Next.
4. Define the script, then click Next.
  - a. Define the type, either EC Shell or Remote Shell.
  - b. Define the time out parameters.
  - c. Type the script in the Script field, or click Load if you are loading an EC Shell script that is saved on the Enterprise Controller. Click View System Variables to see the available software-specific variables.
5. (Optional) Add user-defined variables in the Specify Additional Variables page. Click Next.
6. Review, then click Finish.

## Edit an Operational Profile or Plan

When you edit a profile or plan, you create a version. When you create a version, you have the option to automatically change the related plans during the update. See [Version Control](#) for how versions are maintained.

You can view version details by highlighting the plan, then clicking the View Version Details icon. Use the arrows to view the different versions. When you want a plan to use the new version of the profile, edit the plan and associate it with the correct version of the profile. You can edit the following fields in an Operational Plan: Description, Failure Policy, and Associated Profile. You cannot edit the name of an Operational profile or plan. When you want a different name, you must copy or create a Operational Profile and Plan.

## Copy an Operational Profile

You can copy an existing operational profile, rename it, and create a new profile and plan.

1. Expand Plan Management in the Navigation pane, then click Operational Profiles.
2. Select the profile in the center pane that you want to copy, then click the Copy Profile icon. Or you can double-click the profile in the center pane to display actions in the Actions pane.
3. Rename the new profile you are creating and revise the description, then click Next.
4. (Optional) Edit the script. Click Next.
5. (Optional) Edit the variables in the Specify Additional Variables page. Click Next.
6. Review, then click Finish.

## Copy an Operational Plan

You can copy an existing operational plan, rename it, and create a new profile and plan.

1. Expand Plan Management in the Navigation pane, then click Operational Plans.
2. Select the plan in the center pane that you want to copy, then click the Copy Plan icon. Or you can double-click the plan in the center pane to display actions in the Actions pane.
3. Rename the new plan you are creating and revise the description. You can choose to change the Failure Policy for the new plan and change the Operational Plan steps. You can change the associated profile or plan for each step. To change the profile or plan, click the associated profile or plan to select from a list of available options. To add additional steps, click the Replicate Step icon, then select the profile or plan from the list to associate with that step. Click Save.
4. (Optional) Edit the script. Click Next.
5. (Optional) Edit the variables in the Specify Additional Variables page. Click Next.
6. Review, then click Finish.

## Delete an Operational Profile or Plan

You can delete a version of a profile, or you can delete all versions of the profile and the associated plan.

You cannot delete a version of an operational plan version unless you created the version. Deleting a version of a plan might impact the Incident Knowledge Base or deployment plans that reference the version. Before deleting a version, verify that the version is not being used.

---

---

**Note:** When you delete a version and more than one version exists, the previous version becomes the default. When only one version of the plan exists, the operational profile and plan are deleted.

---

---

## Profiles and Policies

Profiles and policies define how a job is performed and the level of interaction.

### Policies

Policies are lists of actions that are explicitly approved or denied. Policies are specific to OS update and define the amount of user interaction you want when applying OS patches and packages. For example, you might want to automate applying fixes without user interaction, but you might want to pause a job and require user approval before performing a downgrade or uninstall. You can also deny certain actions, such as installing uncertified patches or packages.

Policy settings are hierarchical. When you have not defined a policy for a component, the policy for that component's parent applies. For example, it is possible to create a policy that allows the system to install a given component, but prohibits installing specific versions of that component.

Update policies are discussed in detail in [Chapter 13, "Operating System Updates"](#).

### Profiles

Profiles define how a standard management tasks are performed. With the help of wizards, you create a customized set of profiles. Once created, authorized users can use the profiles to perform tasks, such as discovery and provisioning. The software has pre-defined profiles for some common OS tasks, such as reboot and check for installed security patches. You can choose to use the pre-defined profiles for those actions or create your own.

Profiles are organized in the UI by category. The profiles are discussed in more detail in various sections of the documentation. The following are the profile categories and where you can find more specific information about that task and profile:

- Discovery – See [Chapter 2, "Asset Management"](#)
- Service Processor – See [Chapter 11, "Hardware"](#)
- RAID Controller – See [Chapter 11, "Hardware"](#)
- Firmware – See [Chapter 11, "Hardware"](#)
- Dynamic System Domain – See [Chapter 11, "Hardware"](#)
- OS Provisioning – See [Chapter 12, "Operating Systems"](#)
- Logical Domain – See [Chapter 15, "Oracle VM Server for SPARC"](#)
- Solaris Zone – See [Chapter 14, "Oracle Solaris Zones"](#)
- Virtual Machine – See [Chapter 16, "Oracle VM Server for x86"](#)
- BIOS Configuration – See [Chapter 11, "Hardware"](#)

- Boot Environment – See [Chapter 12, "Operating Systems"](#)
- Storage Appliance Update – See [Chapter 11, "Hardware"](#)
- Update Policies – See [Chapter 13, "Operating System Updates"](#)
- Update Profiles – See [Chapter 13, "Operating System Updates"](#)

With the exception of the Discovery profile, these types of management profiles require a deployment plan to execute the tasks on specific targets. When you create a profile, the default setting is to create a corresponding deployment plan. See [Deployment Plans](#) for more information on these types of plans.

## Deployment Plans

Deployment Plans use profiles to perform standard management activities in a consistent and repeatable manner. A deployment plan defines the sequence of operations or steps that must be carried out on an asset to deploy it together with the specification or profile that each step applies and the resources that are required to apply it such as network addresses and system names.

A comprehensive set of deployment templates is available for you to use to create a variety of deployment plans. Each template is an unbound deployment plan which defines the steps of execution, but not the profiles and assets. A deployment template enable you to define a task and the associated resources (such as images and network addresses), that are needed to complete the task.

The software provides several plans that contain more than one step. In some cases, you can associate steps in a plan with another plan. The associated plan is referred to as a nested plan. You can use nested plans as shared building blocks, much in the same way as profiles are used. Configuring a single nested plan once and reusing it in many other plans reduces the number of individual operations that you must complete in the UI. The templates appear in the user interface in alphabetical order, not by type. However, it is useful to categorize the plans as simple, multi-step, and complex. See the different categories for a description of the plans. The following lists the plans that are located in each category:

- [Simple Deployment Plans](#)
  - Configure RAID
  - Configure Service Processor
  - Provision OS
  - Update Firmware
  - Update BIOS Configuration
  - Update Storage Appliances
  - Create Oracle Solaris Zones
  - Create Virtual Machines
- [Multi-Step Deployment Plans](#)
  - Install Server
  - Create Dynamic System Domain
  - Create Logical Domains
  - Software Deployment/Update

- Update Solaris 11 OS
- Create Boot Environment
- Update Firmware and Install Oracle VM Server for SPARC
- **Complex Deployment Plans**
  - Configure M-Series Hardware, Create, and Install Domain
  - Configure Server Hardware and Install OS
  - Configure and Install Dynamic System Domain
  - Configure and Install Logical Domains
  - Configure and Install Oracle Solaris Zones
  - Configure and Install Virtual Machines

You can use the templates to create your own deployment plans and configure the plans using profiles. The settings and values in the profiles bound to each step are defaults. You can modify the plan is actually applied. You can further constrain the profile settings and values by the target systems to which the plan is applied.

With the exception of complex plans, the templates do not allow you to add steps to a plan. You can use only those steps that are defined in the template from which the plan is derived. Complex plans enable you to add one or more deployment and operational plans inside a complex type plan.

## Simple Deployment Plans

The software provides you with the ability to create, configure, manage and execute deployment plans which drive the hardware, firmware and software provisioning activities in a repeatable fashion.

You create plans from defined templates. Each plan defines the sequence of steps that must be carried out for configuration or provisioning of a system. Plans might contain a single step or a sequence of multi-steps. Each step in the plan is configured by associating a profile or another plan.

A simple plan contains a single step with a single image. You can define the image used by the plan, but you cannot add more than one image or add steps.

The following plans are simple deployment plans:

- **Configure RAID** – Use this plan to configure the RAID controller on a server. See [Configuring a RAID Controller](#) for how to use the profile and plan.
- **Configure Service Processor** – Use this plan to configure the service processor on a chassis. See [Configuring the Service Processor](#) for how to use the profile and plan.
- **Provision OS** – Use this plan to provision an operating system. See [Provisioning Operating Systems](#) for how to use the profile and plan.
- **Update Firmware** – Use this plan to update firmware. See [Firmware Provisioning](#) for how to use the profile and plan.
- **Update BIOS Configuration** – Use this plan to update the BIOS configuration of servers. See [Create BIOS Configuration Profile and Plan](#) for how to use the profile and plan.
- **Update Storage Appliances** – Use this plan to update storage appliance software. See [Storage Libraries](#) for how to use the profile and plan.



- Create Oracle Solaris Zones – Use this plan to create zones. See [Create Zone Profile](#) and [Deployment of Zone Plans](#) for how to use the profile and plan.
- Create Virtual Machines – Use this plan to create virtual machines for Oracle VM Server for x86. See [Create Virtual Machines](#) and [Create and Deploy Virtual Machine Plan](#) for how to use the profile and plan.
- Create Dynamic System Domain – Use this plan to create dynamic system domains. See [Configuring a Dynamic System Domain](#) for how to use the profile and plan.
- Create Logical Domains – Use this plan to create logical domains. See [Create Logical Domain Profile](#) for how to use the profile and plan.

In most cases, when you create a profile, the default action also creates a simple deployment plan.

## Multi-Step Deployment Plans

Several deployment templates with multi-step sequences are available. These plans are designed to provide you with a customized and repeatable way to perform common operations with a single click.

The following plans are multi-step deployment plans:

- Install Server – Use this plan to provision the server and update the OS.
- Software Deployment and Update – Use this plan to apply script based update profiles. See [Update an Operating System From a Deployment Plan](#) for how to use the profile and plan.
- Update Solaris 11 OS – Use this plan to update Oracle Solaris 11 operating systems. See [Update Oracle Solaris 11](#) for how to use the profile and plan.
- Create Boot Environment – Use this plan to create Oracle Solaris boot environments. See [Create an Oracle Solaris 11 Boot Environment](#) and [Create an Oracle Solaris 8, 9, or 10 Boot Environment](#) for how to use the profile and plan.
- Update Firmware and Install Oracle VM Server for SPARC – Use this plan to update firmware and then install Oracle VM Server for SPARC on the system. See [Installation of Oracle VM Server for SPARC](#) for how to use the profile and plan.

The steps in a multi-step plan are defined in the template. You cannot skip steps or add steps.

## Complex Deployment Plans

You can use a combination of profiles, deployment plans, and operational plans to create a complex deployment plan that enables you to automate a variety of detailed workflows into a single plan. Complex plans provide flexibility to structure plans that meet your local requirements, increasing consistency and allowing for a greater level of automation.

When you create complex deployment plans, you can choose to skip a step in the plan. Skipped steps are not processed when the plan is applied. You can replicate certain steps to perform the same operation but using a different profile or plan. You can also add one or more deployment plans and operational plans.

The following plans are complex deployment plans:

- Configure M-Series Hardware, Create and Install Domain – Use this plan to configure an M-Series server, create dynamic system domains, provision OS on the domains, and update the domains.
- Configure Server Hardware and Install OS – Use this plan to configure a service processor or a chassis, provision OS and update the OS.
- Configure and Install Dynamic System Domain – Use this plan to create dynamic system domains, provision and update OS on the domains.
- Configure and Install Logical Domains – Use this plan to create logical domains and provision OS on the logical domains.

## Actions for Deployment Plans

After you create a profile and plan, you can perform the following actions:

- [Edit a Profile](#)
- [Edit a Deployment Plan](#)
- [Copy a Deployment Plan](#)
- [Deploy a Plan](#)
- [Delete a Deployment Plan](#)

### Edit a Profile

Editing a profile enables you to change the profile configuration. Changing values other than the name or description will create a new version. When a profile is referenced by one or more deployment plans, the default action is to update the referring plans to the new version.

#### To Edit a Profile

1. Expand Plan Management in the Navigation pane.
2. Select a profile from the Profiles and Policies tree.
3. Click Edit Profile.
4. Complete the changes, then click Finish.

### Edit a Deployment Plan

You can edit the deployment plan details, alter the plan configuration by skipping steps in the plan, change the profile or plan bound to each step, or save the plan under a different name to create a new plan.

---

**Note:** When you edit a deployment plan that is referred to by another plan, for example, in a nested plan, the referring plan is not automatically updated to refer to the edited plan's version. You must manually modify the referring plan if you want it to use the modified version.

---

#### To Edit a Deployment Plan

1. Select Plan Management from the Navigation pane.
2. You can use either of the way to select Edit Deployment Plan option:

- Method 1 – Select the deployment type from the tree and select a plan from the list. The Edit Deployment Plan icon is enabled. Click the Edit Deployment Plan icon.
  - Method 2 – Expand the selected deployment type and select a plan from the list. The plan details are displayed. Select Edit Deployment Plan from the Actions pane. The Edit Deployment Plan window is displayed.
3. Edit the following details of the plan:
    - Plan Name – When you can modify the name of the plan, a new plan is created. Edit the name to create a new plan.
    - Description – Provide a description of the plan.
    - Failure Policy – Select whether you want the plan execution to stop at failure or complete as much as possible.
  4. You can configure a step of the plan by setting or changing the associated profile, or by creating a new profile.
  5. You can edit the plan by replicating the steps and associate targets depending on the type of plan selected, if any.
  6. Click Save to save any changes made to the plan. When you have changed the name, a new plan is saved with the version v1.

## Copy a Deployment Plan

You can copy an existing deployment plan, rename it, and create a new plan.

### To Copy a Deployment Plan

1. Select Plan Management from the Navigation pane.
2. You can use either of the way to select Copy Deployment Plan:
  - Method 1 – Select the deployment type from the tree and select a plan from the list. The Copy Deployment Plan icon is enabled. Click the Copy Deployment Plan icon.
  - Method 2 – Expand the selected deployment type and select a plan from the list. The plan details are displayed. Select Copy Deployment Plan from the Actions pane. The Create a Deployment Plan window is displayed.
3. Edit the following details of the plan:
  - Description – Provide a description of the plan.
  - Plan Name – By default, the plan name is Copy of *<plan name>*. For example, Copy of Firmware Update. You can modify the name.
  - Failure Policy – Select whether the plan execution is to stop at failure or complete as much as possible.
4. You can configure a step of the plan by setting or changing the associated profile, or by creating a new profile.
5. You can edit the plan by replicating the steps and associate targets, depending on the type of plan selected.
6. Click Save the new plan. A new plan is saved with the version v1.

## Deploy a Plan

When you deploy a plan, you select the target assets against which the plan is executed. After you select the targets, you have the option to temporarily override the profile configuration for specific assets before you deploy the plan.

Many actions use deployment plans. See the How To tab in the documentation library at <http://www.oracle.com/pls/topic/lookup?ctx=oc121&id=howto> for a list of end-to-end examples that use profiles and plans.

## Delete a Deployment Plan

You can delete a deployment plan or only a version of the plan. When the selected deployment plan is not referenced by any other plans, you can confirm deleting the plan or its version. When the plan is used in other plans, the Delete Deployment Plan option is not be enabled.

### To Delete a Deployment Plan

1. Select Plan Management from the Navigation pane.
2. You can use either of the way to select Delete Deployment Plan option:
  - Method 1 – Select the deployment type from the tree. The plans of that type are listed in the center pane. Select a plan from the list. The Delete Deployment Plan and Delete Version icon is enabled. Click Delete Deployment Plan or Delete Version icon accordingly.
  - Method 2 – Expand the selected deployment type and select a plan from the list. The plan details are displayed. Select Delete Deployment Plan or Delete Version from the Actions pane. The Delete Plan window is displayed.
3. Click Delete to confirm the delete action.

## Location of Profiles and Plans in the User Interface

**Table 8–2** Location of Profile and Plan Information in the UI

Object	Location
Operational Plans	Expand the Plan Management section of the Navigation pane, then scroll down to Operational Plans.
Operational Profiles	Expand the Plan Management section of the Navigation pane, then scroll down to Operational Plans. Operational Profiles are in the Operational Plans section. Click Operational Profiles for a list of available profiles.
Deployment Plans	Expand the Plan Management section of the Navigation pane, then scroll down to Deployment Plans. Click Deployment Plans for a list of existing plans. To locate a specific plan, expand the folder for the plan you want, such as Configure RAID.
Profiles	Expand the Plan Management section of the Navigation pane, then scroll down to Profiles and Policies. Click Profiles and Policies for a list of existing profiles. Expand the folder for the type of profile you want, such as RAID Controller.

## Related Resources for Plan Management

For profile and plan details, and how to use individual profiles and plans, go to one of the following resources.

- [Chapter 2, "Asset Management"](#)
- [Chapter 12, "Operating Systems"](#)
- [Chapter 11, "Hardware"](#)
- [Chapter 13, "Operating System Updates"](#)
- [Chapter 14, "Oracle Solaris Zones"](#)
- [Chapter 15, "Oracle VM Server for SPARC"](#)
- For end-to-end examples, see the How To library at <http://www.oracle.com/pls/topic/lookup?ctx=oc121&id=howto>



# Part III

---

## Operate and Maintain

Part III contains the following chapters:

- [Chapter 9, "Incidents"](#)
- [Chapter 10, "Reports"](#)
- [Chapter 11, "Hardware"](#)
- [Chapter 12, "Operating Systems"](#)
- [Chapter 13, "Operating System Updates"](#)





This chapter describes how you can use the software to identify, assign, and resolve incidents.

The following information is included:

- [Introduction to Incident Lifecycle Management](#)
- [Roles for Incident Management](#)
- [Actions for Incident Management](#)
- [Location of Incident and Service Request Information in the User Interface](#)
- [Incidents](#)
- [Message Center](#)
- [Annotations](#)
- [Incidents Knowledge Base](#)
- [Oracle Services and Service Requests](#)
- [Incident Lifecycle Management](#)
- [Annotations](#)
- [Related Resources for Incident Management](#)

## Introduction to Incident Lifecycle Management

When an asset is not operating within the parameters defined in the monitoring rules and policies, Oracle Enterprise Manager Ops Center generates an alert and an incident.

An alert indicates that a monitored asset is not performing as expected. The monitoring rule parameters determine when an alert is triggered and the severity: Informational (info), Warning, or Critical.

An incident is raised when the monitoring rule is asserted by the raising of one or more alerts that the monitoring rule requires. New alerts will update an open incident. One or more subsequent alerts trigger the monitoring rule, which notifies the incident management system. The incident management system detects that there is already an open incident for the monitoring rule for that asset and correlates the alerts under the open incident and the worst severity level is associated with the incident. For example, when the incident is at a Critical severity level and a new Warning alert is added to the incident, the incident severity remains at the Critical level.

Oracle Enterprise Manager Ops Center uses a help desk approach to manage the incidents in your data center. All open incidents appear in the Message Center. You can assign incidents to others for resolution, add comments, provide a list of possible causes and impacts, provide recommendations, add utilities or scripts to resolve an issue, view progress, and open a service desk ticket.

The following are the main components that help you to track and manage known issues on your monitored assets:

- [Message Center](#) – Central location for details on incidents, notifications, and service requests.
- [Annotations](#) – Comments, suggested actions, and operational plans that enable you to effectively manage an incident.
- [Incidents Knowledge Base](#) – Database of your annotations and actions for specific types of incidents and severity levels.
- [Oracle Services and Service Requests](#) – Service request details on all requests submitted to My Oracle Support through Automated Service Request or the Oracle Enterprise Manager Ops Center UI. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about Automated Service Requests and how to enable them.

When an incident appears, you can assign it to a user for resolution and use annotations to add comments and suggested actions. You can build an Incident Knowledge Base that contains your annotations from specific incidents, or add suggested fixes or automated fixes for a specific type of incident.

If you cannot resolve an incident, you can open a service request with My Oracle Support inside the Oracle Enterprise Manager Ops Center UI. The information gathered by the software is automatically populated into the service request. You can track the status of any service request opened from within Oracle Enterprise Manager Ops Center, whether they belong to you or one of your co-workers.

## Roles for Incident Management

The following table lists the tasks that are discussed in this section and the role required to complete the task. You can restrict privileges to specific targets or groups of targets. Contact your administrator when you do not have the necessary role or privilege to complete a task. Contact your administrator if you do not have the necessary role or privilege to complete a task. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 9–1 Incident Management Tasks and Roles**

Task	Role
View Incidents	All
Assign Incidents	Fault Administrator
Add Annotation to incidents	Fault Administrator
Acknowledge incidents	Fault Administrator
Take Actions on Incidents	Fault Administrator
Mark Incidents as Repaired	Fault Administrator

**Table 9–1 (Cont.) Incident Management Tasks and Roles**

<b>Task</b>	<b>Role</b>
Close Incidents	Fault Administrator
Take Actions on Notification	Fault Administrator
Delete Notifications	Fault Administrator

## Actions for Incident Management

Incident management is automatically enabled after an asset is discovered and managed. Alerts and incidents are generated based on the monitoring profiles and policies.

### Actions for Incidents

You can perform the following actions for a specific incident:

- View Alerts – View all alerts that are generated when the state is outside the defined monitoring parameters.
- View Annotations – View the scripts or suggested actions that you or others in your organization have associated with an incident.
- View Possible Impacts and Causes – View the possible impacts and causes for an incident.
- View Comments – View comments that you or others in your organization have associated with an incident.
- View Suggested Actions – View suggested actions that you or others in your organization have associated with an incident.
- Add Annotation to the Incident – Add a script, suggested action, or comment to a specific incident.
- Assign the Incident – Assign an incident to a user.
- Acknowledge the Incident – Acknowledge, or accept, an incident that has been assigned to you.
- Take Actions on the Incident – Take action to resolve an incident. Options include executing a suggested action, executing a script that is part of an operational profile, executing a command, or executing a script.
- Mark Incident as Repaired – Identifies the incident as being fixed.
- Close the Incident – Closes the incident and removes it from the Message Center.
- Open a Service Request – Open a service request for the incident with My Oracle Support.

### Actions for Service Requests

When the Enterprise Controller is connected to My Oracle Support and service requests are enabled, you can perform the following service request actions:

- View all open service requests – View all open service requests that were filed with the Oracle Enterprise Manager Ops Center software.
- View your service requests – View open service requests that you filed with the Oracle Enterprise Manager Ops Center software.

## Actions for Incidents Knowledge Base

The Incidents Knowledge Base is located in the Operational Plans section of the Plan Management drawer. You can perform the following actions for the Incidents Knowledge Base:

- View and sort the annotations by type – The Incident Knowledge Base appears as a table with the name, description, subtype, target type, version and date the annotation was last updated.
- Add an annotation for an Incident type – Add a comment, suggested action, or automated action for a type of incident and monitored attribute. You define the severity levels that the annotation is applicable.
- Edit an annotation for an incident type – Edit an annotation for a type of incident.
- Delete an annotation for an incident type – Delete an annotation for a type of incident.

## Location of Incident and Service Request Information in the User Interface

Incident and service request information is available in the Message Center in the Navigation pane. Use the Message Center to view and manage view notifications, service requests and warranty information for an asset. You can also view incident details by expanding the asset and clicking the Incident tab.

**Table 9–2** Location of Incidents and Service Request Information in the UI

Object	Location
Unassigned Incidents	Expand the Message Center in the Navigation pane, then click Unassigned Incidents. Or, click the asset in the Assets section, then click the Incidents tab.
My Incidents	Expand the Message Center in the Navigation pane., then click My Incidents. Or, click the asset in the Assets section, then click the Incidents tab.
Incidents Assigned to Others	Expand the Message Center in the Navigation pane, then click Incidents Assigned to Others. Or, click the asset in the Assets section, then click the Incidents tab.
Open Service Requests	Expand the Message Center in the Navigation pane, then click Open Service Requests.
My Service Requests	Expand the Message Center in the Navigation pane., then click My Service Requests.
Notifications	Expand the Message Center in the Navigation pane, then click Notifications.
Relayed Incidents	Expand the Message Center in the Navigation pane, then click Relayed Incidents.
Relayed Service Requests	Expand the Message Center in the Navigation pane, then click Relayed Incident Requests.
Incident Knowledge Base	Expand Plan Management in the Navigation pane, then click Incident Knowledge Base.

## Incidents

Each time a monitored attribute does not meet its monitoring rule, a new alert is generated. The first alert raises an incident, which appears in the Message Center. Subsequent alerts for the same rule and asset are correlated with the same open incident.

When a value for an attribute exceeds its monitoring rule and then later meets the rule, the alert is cleared automatically. The change in the attribute value does not automatically clear the incident. When an attribute's value is moving in and out of its monitoring rule's parameters, alerts are generated and cleared continuously. A new incident is only generated when the original incident is closed. When an incident is not yet closed, the new alerts are aggregated into the existing incident. You must close an incident to clear it from the user interface.

### Incident Severity Badges

Incident severity badges are an option that you can enable to display an incident severity badge next to an asset show the incident status. Badges also appear in the dashboard membership graph to show the status of an asset. See [Badges](#) in [Appendix E](#) for a description of each badge.

---

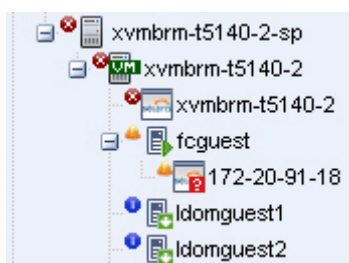
**Note:** The badges are disabled by default. To display the badges in the Navigation pane, click Setup, My Preferences, then click User Interface Preferences. Click the check box to make the badges visible in the user interface.

---

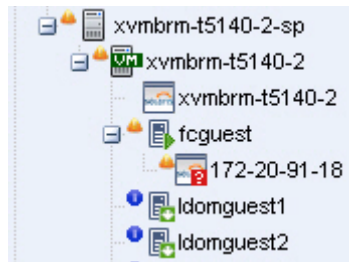
Incident severity badges are an option that you can enable to display an incident severity badge to show the status of an asset. You can configure the severity badges in User Interface Preferences.

When an asset has an incident, the severity badge appears next to the asset icon in the Asset hierarchy. When it is the highest severity incident in the membership of a group, the severity badge also appears next to the parent assets. In [Figure 9-1](#), the operating system for xvmbrrm-t5140-2 has a critical incident. The critical incident badge also appears on the system and service processor. Any group that this OS is a member of, such as All Assets and Operating Systems, also display the badge.

**Figure 9-1 Critical Incident Badge**



When the incident is the only critical incident, the badge is removed when the incident is acknowledged, marked repaired, or closed. When open incidents are still present, the next highest severity badge displays. For example, when both a Critical and a Warning incident is detected and the Critical incident is acknowledged, the Critical badge is replaced with the Warning badge because that is now the highest level unacknowledged incident.

**Figure 9–2 Warning Incident Badge**

After the incident is closed, its severity badge is not displayed in the asset hierarchy.

See [Chapter 4, "Monitoring Rules and Policies"](#) for more information about creating and maintaining monitoring rules and profiles.

An incident is one or more alerts on the same monitored attribute and asset. A ticker at the top of the UI contains the number of unassigned critical incidents, unassigned Warning incidents, number of relayed incidents, the number of critical incidents and the number of warning that are assigned to you. You can click an icon to display the incidents dashboard for that category.

**Figure 9–3 Incidents Ticker**

## Message Center

Incidents, notifications, and service requests that are generated by managed assets appear in the Message Center. Your assigned user role determines the actions that you can perform in the Message Center.

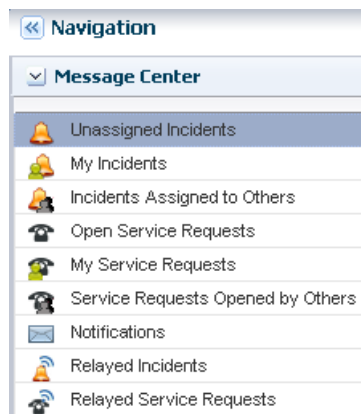
Incidents, notifications and service requests appear in the following categories in the Message Center:

- Unassigned Incidents – Newly created incidents and those that have not been assigned an owner.
- My Incidents – All incidents that are assigned to you. You can perform additional actions to these incidents to manage their status, such as: Take Action, mark as being repaired, acknowledge, and open a service request for the incident.
- Incidents Assigned to Others – Incidents that are currently assigned to other users. You can view these incidents, but you cannot perform specific actions on them.
- Open Service Requests – All Service Requests that have been filed on assets that are submitted through Oracle Enterprise Manager Ops Center.
- My Service Requests – All Service Requests that you submitted on assets that are managed by Oracle Enterprise Manager Ops Center.
- Service Requests Opened by Others – All Service Requests that have been submitted on assets that are managed by Oracle Enterprise Manager Ops Center.
- Notifications – Information that is automatically generated by services running in the backend while monitoring the assets. Typically, notifications are less important than incidents.

- Relayed Incidents – All incidents reported from any discovered Oracle Engineered System. You must log into the Oracle Enterprise Manager Ops Center instance that manages each Oracle Engineered system to fix any incidents related to its assets.
- Relayed Service Requests – All open Service Requests for any discovered Oracle Engineered System.

Closed incidents and service requests do not appear in the Message Center.

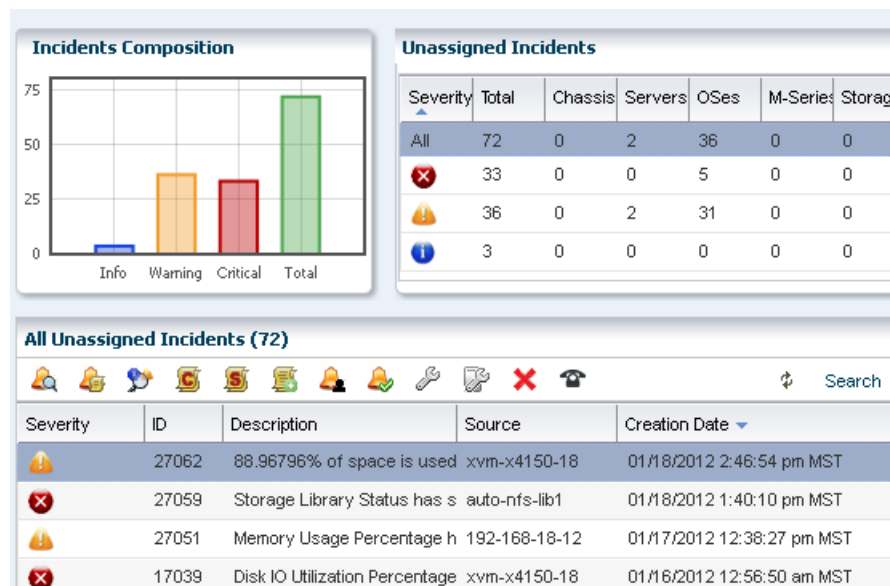
**Figure 9–4 Message Center**



A bar chart on the page visually displays the number of new incidents by severity and the total number of unassigned incidents. The page also contains a table that categorizes the incidents by severity and asset type. Select a row in the table to display all unassigned incidents for the selected severity category. A third table, at the bottom of the dashboard provides details and action icons.

The All Unassigned Incidents table shows all open unassigned incidents. Each incident receives an ID to help you to track the issue. The table includes a description, source, Creation Date, and URL field for each incident. Hover over the URL icon for an incident to display a pop-up window. The default sort is by the creation date; however, you can sort by any column.

**Figure 9–5 Unassigned Incidents Dashboard**



The following information is available in the Unassigned Incidents table:

- Severity – The severity icon shows the severity level, either informational (info), warning, or critical.
- ID – A generated ID assigned to the incident to help track the issue.
- Description – A brief description of the incident.
- Source – The asset that is generating the incident.
- Creation Date – The date and time that the incident generated.
- URL – Contains incident details. Hover over the URL icon to display the duration of the incident, when the incident was assigned, and to whom, any suggested actions, the source and a larger description field.

A row of icons at the top of the Unassigned Incidents table provides actions that are available to you, based on your user role. The following action icons are available for incidents, the actions are in the order that the icons appear in [Figure 9-6](#):

- View Alerts
- View Annotations
- View Possible Impacts and Causes
- View Comments
- View Suggested Actions
- Add Annotation to Incident(s)
- Assign Incident(s)
- Acknowledge Incident(s)
- Take Action(s) on Incident
- Mark Incident(s) as Repaired
- Close Incident(s)

**Figure 9-6 Incident Actions**



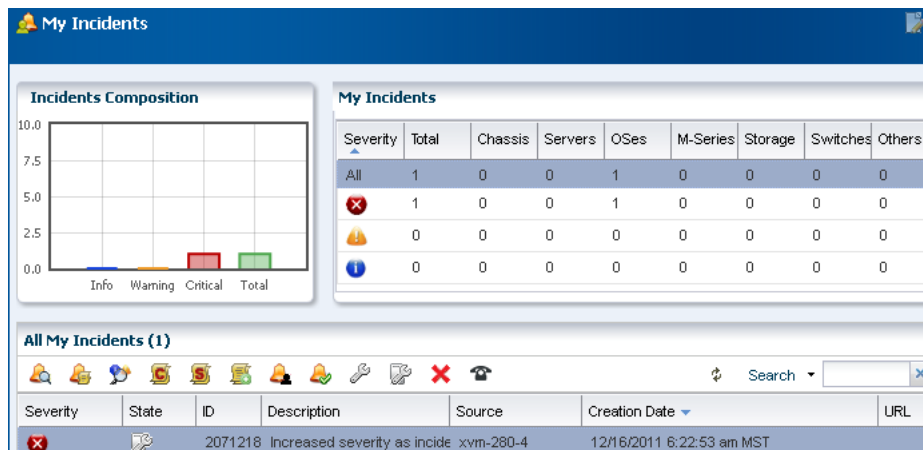
## Incidents Dashboards in the Message Center

Incidents assigned to you appear in the My Incidents dashboard in the Message Center. Anybody with the appropriate permission level can see the incidents in your queue, can reassign incidents to another user, and can assign you new incidents. Unassigned Incidents and Incidents assigned to others have their own categories in the Message Center. Each Incident dashboard is laid out the same.

A bar chart on the page visually displays the number of new incidents by severity. The page also contains a table that categorizes the incidents by severity and asset type.

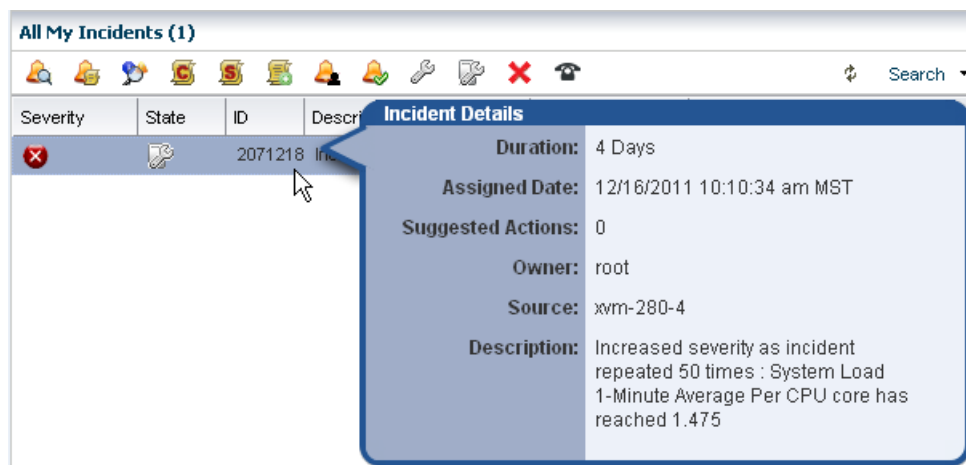


**Figure 9-7 My Incidents**



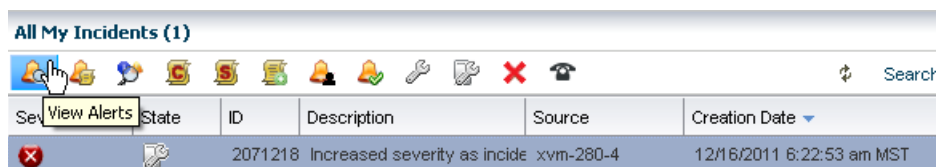
Select a row in the table to display all incidents for the selected severity category and to drill down for more details. The software assigns each incident an ID for tracking purposes. Hovering your mouse over any field in the incident row displays details.

**Figure 9-8 Incident Details**



The icons in the center pane enable you to perform actions on a specific incident or view the alerts that make up an incident in the center pane. Each icon has hover text to define the action.

**Figure 9-9 Incident Icons**



The following actions, as described in [Actions for Incident Management](#), are available:

- View Alerts
- View Annotations
- View Possible Impacts and Causes

- View Comments
- View Suggested Actions
- Add Annotation to Incident(s)
- Assign Incident(s)
- Acknowledge Incident(s)
- Take Action(s) on Incident
- Mark Incident(s) as Repaired
- Close Incident(s)
- Open a Service Request

You can configure the software to send you e-mail or pager notification of incidents for critical assets or severity levels. The Notifications appear in the Message Center.

## Annotations

Annotations are comments, suggestions, or automated operations with associated scripts that you can use to document an incident. They are defined by an asset type, asset resource type, an attribute, or an incident type.

Annotations are as powerful as you want to make them. You can View Annotations, View Possible Impacts and Causes, View Comments, View Suggested Actions, and Add Annotations that are associated with an incident in the Message Center or from the Incidents tab in the Asset view, as shown in [Figure 9–10](#).


**Figure 9–10 Annotation Icons**



You can add informational comments and notes to an issue while you are working on a resolution, when you mark an incident as fixed, and when you close an incident.

**Figure 9–11 Add Comment Type Annotation**

Add Annotation

Severity	ID	Description	Source
	1653	Memory Usage Percentage has reached 82.60498	ocbrm-ippgs13

\* Annotation Type:

Associated Operational Plan:

\* Synopsis:

Note: Investigating why memory usage percentage is high. |

Save this annotation in the Incidents Knowledge Base to associate the annotation with all incidents of this type and severity.

You can associate annotations with an incident instance or an asset type. The Incidents Knowledge Base contains your annotations, by asset type, and stores the information on the Enterprise Controller. You can view this annotation by browsing the Incidents Knowledge Base.

For more robust incident management, associate an annotation with an incident and store the annotation in the Incidents Knowledge Base to provide an automated solution or a suggested action when a similar incident is detected. To provide an automated solution, create an operational plan that contains a shell script. When a specific incident occurs, the script is executed automatically. To provide a suggested fix or course of action for a specific incident, you can create a text only annotation that provides a suggested course of action, or you can include a shell script.

When a rule is triggered, and an alert or incident is identified, the software checks the Incidents Knowledge Base and Incident Profiles for the Incident Type and any associated annotations. It generates an incident of the defined type and severity level and attaches any annotations. When an automated operation annotation is associated with the incident, the script is executed. When a suggested action annotation is associated with the incident, the text and script (when available) appear in the incident details.

## Annotation Views

Annotations are available from several different views within the UI:

- In the Message Center, when an annotation is associated with an incident
- In the Asset view, when an annotation is associated with an incident
- In the Incident Knowledge Base (in the Plan Management drawer), when an annotation is associated with an asset type

When an annotation is associated with an incident, you can click the View Annotations icon to see the associated annotation.

You can create annotations by an asset type, asset resource type, an attribute, or an incident type. The annotations are located in the Incidents Knowledge Base (KB). Annotations are automated operations with associated operational profile, suggested fixes or actions, or text only comments. You can associate Automated Action and Suggested Action annotations with an operational profile, which can contain a script.

You can also add an annotation to the Incidents KB when you add an annotation to a specific incident.

A comment is a type of annotation. You can add informational comments and notes to an issue while you are working on a resolution, when you mark an incident as fixed, and when you close an incident. You can also use annotations to build a Incidents Knowledge Base that contains a mixture of comments, suggested actions, and automated actions. To add a comment, see [Add an Annotation](#).

Annotations in the Incidents Knowledge Base (KB) are associated with types of incidents. You can delete an annotation in the Plan Management section of the UI.

## Incidents Knowledge Base

Annotations enable you to build a Incidents Knowledge Base that contains a mixture of comments, suggested actions, and automated actions.

You can use your annotations to build an Incidents Knowledge Base that is based on your company policies, procedures, and incidents.

You can add annotations to the Incidents Knowledge Base in Plan Management or from a specific incident. Either way, annotations enable you to provide solutions or recommended actions for specific incidents.

The following types of Annotations are available:

- Automated Operation – You can create an annotation that references an Operational Profile and automatically executes the profile when a specific incident occurs.
- Suggested Action – You can provide a suggested fix or course of action for a specific incident. The suggested course of action can be text only, or you can reference an Operational Profile.
- Comment – You can write notes about the situation, such as the current status of an incident. This is a text only field.

You can build an Incident Knowledge Base that contains your annotations from specific incidents, or add suggested fixes or automated fixes for a specific type of incident. You can add possible causes and impacts or you can add an annotation. An annotation is either a comment or a suggested action. Annotations enable you to associate an operational plan that contains a utility or script to correct a specific issue. You can choose to associate the annotation with all incidents of the same type and severity and save it in the Incidents Knowledge Base. The next time the incident occurs, you can access the possible causes and impacts and annotations identified in the previous incident and resolve the issue more quickly.

When an incident is detected, Oracle Enterprise Manager Ops Center checks the Incidents Knowledge Base and Incident Profiles for the asset type and corresponding incident type. Any associated annotations are added to the Incident and Operational Profiles referenced in Automated Operation annotations are executed against the asset on which this incident was open. You can create, update, and delete annotations in the Incidents Knowledge Base.

## Oracle Services and Service Requests

Oracle Services provides integrated methods for maintaining and displaying current contracts, warranty information, contract dates, and service requests for managed assets.

Use the Oracle Services feature to view the contract or warranty information and any service requests for a specific asset. You can also view service requests that were the result of an alert or incident in Oracle Enterprise Manager Ops Center, view service request details, and file a service request.

- **Contracts and Warranties**

Maintaining a valid inventory of the assets in your data center, including contracts and warranties, can be a time-consuming and labor-intensive process. Use Oracle Enterprise Manager Ops Center to display current contract and warranty information for a specific asset, or view the entitlements associated with your Oracle online account. When a contract or warranty is about to expire, Enterprise Manager Ops Center generates an alert.

- **Service Request**

You can create new service requests, review your requests, and review the requests of other users.

You can file requests manually, or you can provide credentials and contact information for assets and configure Oracle Enterprise Manager Ops Center to generate service requests. When an incident occurs with an asset, a service request is automatically created using the credentials and contact information that you provided.

---

---

**Note:** You cannot display service requests created outside of Oracle Enterprise Manager Ops Center. To see the status of any service requests filed outside of Enterprise Manager Ops Center, go to the Service Requests Home page on My Oracle Support.

---

---

## Requirements for Oracle Services

To use these Oracle Services, you must take the following actions:

- Register your assets with My Oracle Support.
- Register your user account as a My Oracle Support user so that you can get access to the My Oracle Support database.
- Run Enterprise Manager Ops Center in Connected Mode.

To access the My Oracle Support database, your user must be registered as a My Oracle Support user. This is the same account that is used to access My Oracle Support at

To determine if you are running in Connected Mode and have access to My Oracle Support, check the icons in the upper right corner of the UI, as shown in [Figure 9-12](#). If an icon does not contain color, you are not connected.

- The World icon indicates the status of the Internet connection.
- The Shield icon indicates the status of the connection to the Oracle Knowledge Base.
- The Phone icon indicates the status of the connection to My Oracle Support Services.

**Figure 9–12 Connection Icons**

## View Contract and Warranty Information

You can display contract information by asset, or you can obtain entitlements associated with all contracts that are associated with a user. Contract and warranty information is available for managed servers that have a serial number associated with a contract in the My Oracle Support database.

The contract and warranty information in Enterprise Manager Ops Center is updated each week so contract changes or new contracts might take up to seven days to appear in the user interface. When a contract or warranty is about to expire, an alert is displayed as an Incident in the Message Center and the contract details are displayed in orange text in the asset's Summary tab.

---

---

**Note:** Updating contract and warranty information requires running the product software in Connected mode. If you change to Disconnected Mode, the contract information becomes outdated.

---

---

### To View Contract and Warranty Information For an Asset

1. Select a hardware asset in the Navigation pane, from either the All Asset list or from a group.
2. Click the Summary tab. If Enterprise Manager Ops Center is in Connected Mode and the serial number of the selected asset is associated with a contract, a Support row is added to the summary. The Support field contains the contract ID and an expiration date.
  - If the contract is within 90 days of expiration, the information is displayed in an orange font.
  - If the contract has expired, the information is displayed in a red font.

### To View All Contracts Associated with a My Oracle Support Account

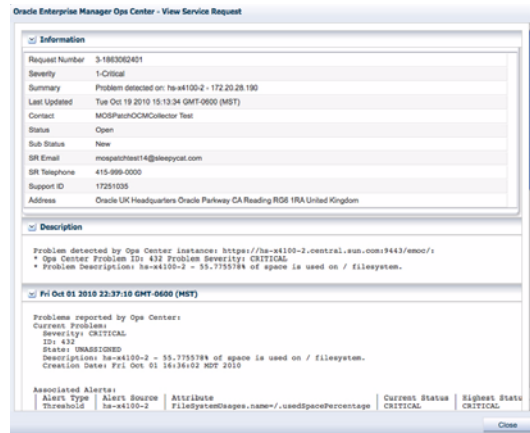
1. Click the Enterprise Controller in the Administration section of the Navigation pane.
2. Click Edit Authentications in the Actions pane. The Edit Authentications window is displayed with online user names and associated contracts.

## View Service Requests

You can see all the current and completed service requests.

### To View Service Requests

1. Click Message Center in the Navigation pane.
2. Click Open Service Requests, My Service Requests, or Service Requests Opened by Others to display a list of requests.
3. To view details of a particular service request, highlight a row, then click the View Service Request icon.

**Figure 9–13 View Service Request**

4. Click Close.

## File a Service Request

When your assets are associated with a contract and registered in the Oracle database, you can create a service request from an incident or from an asset. See [Requirements for Oracle Services](#) for requirements that must be met before successfully filing a service request ticket. For example, if the asset is not registered in My Oracle Support, the service request job fails. If the Open Service Request action is disabled, there is no connection to My Oracle Support.

### To File a Service Request From an Incident

1. Click Message Center in the Navigation pane.
2. Click My Incidents or Unassigned Incidents
3. Select the incident, then click the Open Service Request icon in the center pane.

### To File a Service Request From an Asset

1. Click the hardware in the Assets section of the Navigation pane.
2. Click Open Service Request in the Actions pane.

## Automated Service Requests

Instead of manually filing a service request, you can configure Oracle Enterprise Manager Ops Center to automatically create service requests for known issues. When Automated Service Requests (ASRs) are enabled, Oracle Enterprise Manager Ops Center automatically generates service requests based on critical incidents. Contact information for the ASR is taken either from Oracle Enterprise Manager Ops Center or from the Customer Service Identifier (CSI) associated with the asset. Annotations are added to the incident to indicate the status of the ASR creation. Once they are created, ASRs are identical to other service requests and can be viewed and managed using the same processes and tools.

A user with the Ops Center Admin role must enable the ASR feature. See the *Oracle Enterprise Manager Ops Center Administration Guide* for how to configure and use automated service requests.

## Incident Lifecycle Management

Incident management in Oracle Enterprise Manager Ops Center consists of several components that are designed to work together to simplify managing incidents for a large number of assets. The components include monitoring rules, suggested actions, and methods for automating incident identification and resolution.

Monitoring includes a standard set of monitoring rules, consisting of an asset's attribute and the threshold value for that attribute. When Oracle Enterprise Manager Ops Center performs monitoring, it generates alerts, which connect to both the incident management and notification features.

When an asset is not operating within the parameters defined in the monitoring rules and policies, Oracle Enterprise Manager Ops Center generates an incident and displays the information in the Unassigned Incidents section. Incidents appear as Informational (Info), Warning, or Critical severity. All incidents appear in the Message Center. When an incident is first detected, it appears in the Unassigned category. When you assign an incident to yourself, it moves from the Unassigned Incidents to My Incidents. When an incident is assigned to someone else, it appears in Assigned Incidents.

For example, the CPU usage on a Sun Fire x4150 host is exceeded and an incident is generated. You assign the incident to Bob. Bob is concerned because these systems are often used to host Oracle Solaris Zones.

Bob reviews the incident and adds the following comment to the incident: This asset is not powerful enough and cannot cope with the load. Bob also wants to associate an annotation with the Global Zone asset type. He wants to add a recommended action annotation to the asset type to check for processes that are consuming excessive CPU usage on the Global Zone. He adds the following annotation to the asset type: Run the 'prstat 1 1' command to check which processes are taking CPU. The annotation is saved in the Incidents Knowledge Base and displays the next time CPU usage is exceeded on a global zone asset type.

## Methods of Incident Management

Oracle Enterprise Manager Ops Center uses a help desk approach to managing incidents. The following are the key tools available for taking action on an incident:

- Message Center – View the status of incidents and assign incidents.
- Annotations – Add notes and change status. Use annotation options to provide recommended actions or fixes, or add custom scripts to provide an automated response to an incident.
- Operational Plans – Deploy a shell script against a specific asset, or asset sub-type to automate incident resolution.
- Incidents Knowledge Base – Collect comments and suggested actions for known issues for future use.

When you want to receive e-mail or pager notification each time an incident is reported in the Message Center, you can create notification rules to send a message advising you of a new critical or warning incident.

The Message Center contains a detailed list of unassigned incidents, incidents assigned to you, and incidents assigned to other users.

You can manage incidents from either the Message Center or from the Asset view. You can view and add comments and annotations, take action on an incident, and close incidents.



- The Message Center provides a list of all incidents. Select an incident to see its details and activity.
- From the Asset tree in the Navigation pane, select the asset and then click the Incidents tab to see a list of incidents for that asset.

When you have the Manage or Admin role for the asset, you can take action on the incident. The person assigned to the incident must also have the Manage or Admin role. When the icon is not active, you do not have the appropriate role.

## View Unresolved Incidents

You can view unresolved incidents for a specific asset or by incident:

- To view unresolved incidents for a specific asset, click the asset in the Navigation pane, then click the Incidents tab in the center pane.
- To view unresolved incidents from the Message Center, click one of the following:
  - Unassigned Incidents
  - My Incidents
  - Incidents Assigned to Others

The number of unresolved incidents for an asset appears in a bar chart and in a summary by severity. All Unresolved incidents appear in a table.

View high-level details by hovering your mouse over the incident or clicking the incident in the Unresolved Incidents table. You can drill down to view the alerts that make up the incident by clicking the incident, then clicking the Alerts icon in the center pane.

## View Incident Details

A incident consists of one or more alerts. You can view incident details, including the individual alerts that are part of the incident. The following incident details are available:

- How long the incident has been open, or the duration
- When the incident was assigned
- The number of suggested actions for the incident
- Who is assigned to the incident
- Which resource is affected, or the cause
- A description of the incident

Perform the following steps to view incident details:

1. Select Assets in the Navigation pane.
2. Select an asset that has an incident badge next to the icon. The Dashboard page displays with the status of the asset.
3. Click the Incidents tab.
4. Hover over the incident to display the incident details.
5. To display the alerts that are associated with the incident, click the Alerts sub-tab or click the Alerts icon in the center pane. The alerts that make up the incident are displayed, including the current and highest alert status, and the alert history.

## Assign an Incident

You can assign an incident to a user who has Manage or Admin role for the asset.

Assigning an incident might affect the asset's Incident severity badge. When an incident was previously acknowledged or marked as being repaired, its severity was not propagated up to antecedent assets in the navigation pane. After assigning an incident (to a user or to no one), the severity is propagated up again to antecedent assets in the navigation pane.

1. To display an incident from the Message Center, click Message Center, then click Unassigned Incidents in the navigation pane.

To display an incident from the asset view, click the asset in the Navigation pane, then click the Incidents tab.

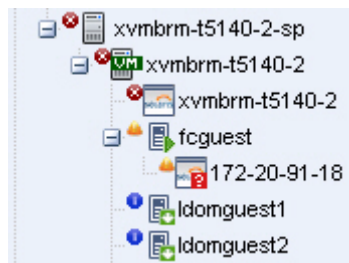
2. Select one or more incidents in the center pane, then click the Assign Incident(s) icon.
3. Select a user name from the Assign To list, which is the list of users who have either the Manage or Admin role for the asset. To move an assigned incident back to the Unassigned Incidents queue, select No One from the list.
4. (Optional) Add a note in the text field.
5. Click Assign Incidents.

## Acknowledge Incidents

Acknowledging an incident indicates that you are investigating the issue. You can acknowledge an incident when you have the Admin or Manage role for the asset on which the incident is identified.

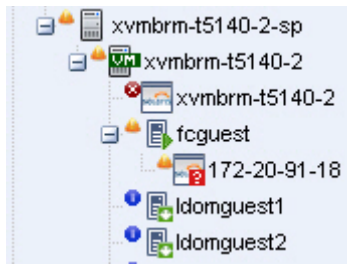
When severity badges are enabled and an incident occurs on an asset, a severity badge appears next to the asset in the Asset hierarchy. When it is the highest severity incident in the membership, it also appears next to the parent assets. In [Figure 9-14](#), the operating system for xvmbrrm-t5140-2 has a critical incident. The critical incident badge also appears on the system and service processor. The badge appears on any group that this operating system is a member of, such as All Assets and Operating Systems.

**Figure 9-14 Critical Incident Badge on Asset and Parent Assets**



When the incident was previously in an Unassigned state or was assigned to someone else, the severity was taken into account in the computation of the highest severity to propagate up to antecedent assets in the navigation pane. When you acknowledge an incident, it is moved into your queue in the Message Center and the severity is no longer propagated up to antecedent assets in the navigation pane.

When you acknowledge the Critical incident, the badge is replaced with the Warning badge because that is now the highest level unacknowledged incident.

**Figure 9–15 Effect of Acknowledging a Critical Incident**

1. Open the incident from the Message Center or Assets view.
  - Message Center View – Click Message Center, then click an Incident category: Unassigned Incidents, My Incidents, or Incidents Assigned to Others
  - Assets View – Click the asset in the Assets section of the Navigation pane, then click the Incidents tab in the center pane.
2. Select one or more incidents, then click the Acknowledge Incidents icon in the center pane.

## Add an Annotation

Annotations are defined by the asset type. Annotations are comments, a suggested action, or a reference to an operational profile. Any user can add an annotation to a Incident. To add an entry to the Incidents Knowledge Base requires Oracle Enterprise Manager Ops Center Admin permissions.

1. Open the incident from the Message Center or Assets view.
  - Message Center View – Click Message Center, then click an Incident category: Unassigned Incidents, My Incidents, or Incidents Assigned to Others
  - Assets View – Click the asset in the Assets section of the Navigation pane, then click the Incidents tab in the center pane.
2. Select the incident, then click the Add Annotations icon in the center pane.
3. Select one of the following types from the Annotation Type from the drop-down list:
  - Comment – Text only option that is designed to be used to add a note or editorial comment.
  - Suggested Action – Text required and a script is optional.
4. Select an operational plan from the drop-down list of operational profiles defined for the type of asset on which this Incident is open.
5. The Synopsis field is completed based on the annotation type. Edit the synopsis, as needed. There is no character limit in the UI, but the API allows for 80 characters.

---

**Note:** When you enter more than 80 characters, the synopsis is truncated to the first 80 characters when viewed in the annotation.

---

6. Type a description or instructions in the Note field. There is no character limit.
7. To add the annotation to the Incidents Knowledge Base and include the annotation for every incident of this type and severity, click the check box.

---

---

**Note:** You must have the Oracle Enterprise Manager Ops Center Admin role to complete this operation.

---

---

8. Click Save and Execute or click Save.

## Display Annotations

You can display annotations for an asset type in the Incidents Knowledge Base.

1. Click Plan Management.
2. Expand Incidents Knowledge Base in the Navigation pane, then select the asset type. The annotations associated with the asset type are displayed in the center pane.

## View Comments

A comment is a type of annotation. You can add informational comments and notes to an issue while you are working on a resolution, when you mark an incident as fixed, or when you close an incident. You can also use annotations to build a Incidents Knowledge Base that contains a mixture of comments, suggested actions, and automated actions. To add a comment, see [Add an Annotation](#).

1. Expand the Message Center, then click one of the following:
  - Unassigned Incidents
  - My Incidents
  - Incidents Assigned to Others
2. Click the incident in the center pane, then click the View Comments icon.

## Take Action on a Incident

When you have the Manage or Administration role for an asset that has an Open Incident, you can correct some incidents by using a script or command. In these situations, you might want to associate an automated action with some known issues. For other incidents, you might want to review the issue before deciding on the appropriate action.

The incident management functionality provides varying levels of control. You can build the Incidents Knowledge Base with annotations that contain a combination of automated actions, suggested actions, and comments. You can execute one or more of the suggested actions associated with the Incident or use an operational plan to correct the incident. When an action is not available in a suggested action or Operational Profile, you can execute a command or a custom script that is stored on the managed asset or on the Enterprise Controller.

See [Add an Annotation](#) for information on adding a suggested action to a Incident.

See [Incidents Knowledge Base](#) to add a suggested action or automated action in the Incidents Knowledge Base. See [Create an Operational Profile and Plan](#) for information about creating an operational profile.

1. Open the incident from the Message Center or Assets view.
  - Message Center View – Click Message Center, then click an Incident category: Unassigned Incidents, My Incidents, or Incidents Assigned to Others

- Assets View – Click the asset in the Assets section of the Navigation pane, then click the Incidents tab in the center pane.
2. Select the incident.
3. Click the Take Action(s) on a Incident icon in the center pane.
4. Select the action to perform:
  - When the Incidents Knowledge Base has provided a suggested action for the incident, select Execute the Selected Suggested Action option and then select the action from the table.
  - When an operational plan has a suggested action, select the Execute an Operational Plan option, then select the plan from the drop-down list.
  - To run a script or command that is not part of a suggested action or operational plan, select the Execute a Command or Script File option.
    - To execute a command, type the command in the field.
    - To browse for a script, click Browse and then select the script from the File Chooser popup.
5. Select where to run the script, on the managed asset where the incident is open, or on the Enterprise Controller.
6. Define the time out period for the action, in minutes, hours, or days.
7. (Optional) Add a note describing the action taken.
8. Click Execute Selected Action.

## Maintenance Mode

Maintenance mode is designed to disable assets from generating incidents temporarily. This mode is useful when you plan to power off a hardware asset or reconfigure a system manually, and you do not want incidents to appear in the UI.

---

---

**Note:** Alerts are still generated when the asset is in maintenance mode. View alerts by selecting the Alerts tab, which is a subtab of the Incidents tab.

---

---

When an asset is placed in maintenance mode, the severity badge of unassigned and assigned incidents affecting the asset and its children is not propagated up the asset membership hierarchy in the navigation pane.

When the maintenance operations are completed, use the Remove From Maintenance action to begin monitoring the asset. When the asset is removed from maintenance mode, the severity badge appears in the asset membership hierarchy in the navigation pane.

1. To remove an asset from monitoring, highlight the asset in the Navigation pane, then click Place in Maintenance in the Actions pane.
2. To begin monitoring the asset, highlight the asset in the Navigation pane, then click Remove From Maintenance in the Actions pane.

## Mark an Incident Repaired

The software cannot determine when an incident is repaired. However, you can open a known incident and manually add a note with the repair details and mark the incident

as repaired. You must have the Manage or Admin role for the asset to perform this task.

When the incident was previously in an Unassigned state or Assigned to someone, the severity was taken into account in the computation of the highest severity to propagate up to antecedent assets in the navigation pane. After marking this incident as repaired, its severity badge does not appear in the assets list in the navigation pane.

1. From the Message Center, click Message Center, then click one of the following:
  - Unassigned Incidents
  - My Incidents
  - Incidents Assigned to Others

or

From the asset view, click the asset in the Assets section of the Navigation pane, then click the Incidents tab.

2. Select one or more incidents, then click the Mark Incident(s) as Repaired icon in the center pane.
3. (Optional) Select the incident, then add a Note.
4. Click Tag Incidents as Being Repaired.

## Close an Incident

The incident stays open until you close it, even if the alerting condition is cleared. To remove an incident from the Message Center and the asset view, you must close the incident or take no action on it for seven (7) days. When any action is taken on an incident, such as adding an annotation, the counter is reset.

---

---

**Note:** Incidents with no activity for seven (7) days are closed automatically by Oracle Enterprise Manager Ops Center, and do not appear in the UI. You can edit this value in the public API.

---

---

When an incident is closed, its status changes to Closed, the incident is deleted from the list of active incidents, and the incident is no longer displayed in the UI. You can retrieve information about a closed incident for 60 days by using the public API. After 60 days, closed incidents are permanently deleted. To edit the time limit, you must edit the value in the public API. You can disable the time limit by setting the value for the number of days to 0.

---

---

**Note:** When the monitoring condition is still true after the incident is closed, a new alert is raised and a new incident is created.

---

---

### To Close an Incident

You can close an incident from the asset view or from the following categories in the Message Center:

- Unassigned Incidents
- My Incidents
- Incidents Assigned to Others

Perform the following steps to close an incident from the asset view:

1. Click the asset in the Assets section of the Navigation pane, then click the Incidents tab.
2. Select one or more incidents, then click the Close Incident(s) icon in the center pane.
3. (Optional) Select the incident, then add a Note.
4. (Optional) To temporarily disable the monitoring rule that identified the incident, click the Action check box, then define when to enable the monitors.

This action does not disable the monitoring rule for all assets. It only disables the monitoring rule for the assets that were related to the incident in order to avoid raising a similar incident on the same assets.

5. Click Close Incidents.

## Annotations

For more robust incident management, you can associate an annotation with a rule and store the annotation in the Incidents Knowledge Base to provide an automated solution or a suggested action when a specific incident is detected. To provide an automated solution, create an operational plan that contains a shell script. When a specific incident occurs, the script is executed automatically. To provide a suggested fix or course of action for a specific incident, you can create a text only annotation that provides a suggested course of action, or you can include a shell script.

When a rule is triggered, and an alert or incident is identified, the software checks the Incidents Knowledge Base and Incident Profiles for the Incident Type and any associated annotations. It generates an incident of the defined type and severity level and attaches any annotations. When an automated operation annotation is associated with the incident, the script is executed. When a suggested action annotation is associated with the incident, the text and script (when available) appear in the incident details.

Annotations are automated operations with associated scripts, suggested fixes or actions, or text-only comments. You can associate annotations with an incident instance or an asset type. The Incidents Knowledge Base contains your annotations, by asset type, and stores the information on the Enterprise Controller. This annotation can be viewed by browsing the Incidents Knowledge Base.

1. Open the incident from the Message Center or Assets view.
  - Message Center View – Click Message Center, then click an Incident category: Unassigned Incidents, My Incidents, or Incidents Assigned to Others
  - Assets View – Click the asset in the Assets section of the Navigation pane, then click the Incidents tab in the center pane.
2. Click the incident in the center pane.
3. Click the View Annotations icon.

### **Example 9–1 Example of Using Annotations**

The CPU usage on a Sun Fire x4150 host is exceeded and an incident is generated. You assign the incident to Lee. Lee is concerned because these systems are often used to host Oracle Solaris Zones. Lee adds the following comment to the incident: "This asset is not powerful enough and cannot cope with the load". Lee also wants to associate an annotation with the Global Zone asset type to recommend checking for processes that are consuming excessive CPU usage on the Global Zone. Lee adds the following annotation to the asset type: "Run the 'prstat 1 1' command to check

which processes are taking CPU." The annotation is saved in the Incidents Knowledge Base and appears the next time CPU usage is exceeded on a global zone asset type.

## Related Resources for Incident Management

For instructions in performing actions or to learn more about the role of this feature, go to one of the following resources.

- [Chapter 4, "Monitoring Rules and Policies"](#)
- [Appendix E, "Icons"](#)
- For end-to-end examples, see the How To library at <http://www.oracle.com/pls/topic/lookup?ctx=oc121&id=howto>



This chapter includes the following information:

- [Introduction to Reports](#)
- [Roles for Reports](#)
- [Actions for Reports](#)
- [Location of Report Information in the User Interface](#)
- [Firmware Reports](#)
- [Operating System Reports](#)
- [Additional Operating System Reports](#)
- [Incident Reports](#)
- [System Information Reports](#)
- [Exalogic Reports](#)
- [Related Resources for Reports](#)

## Introduction to Reports

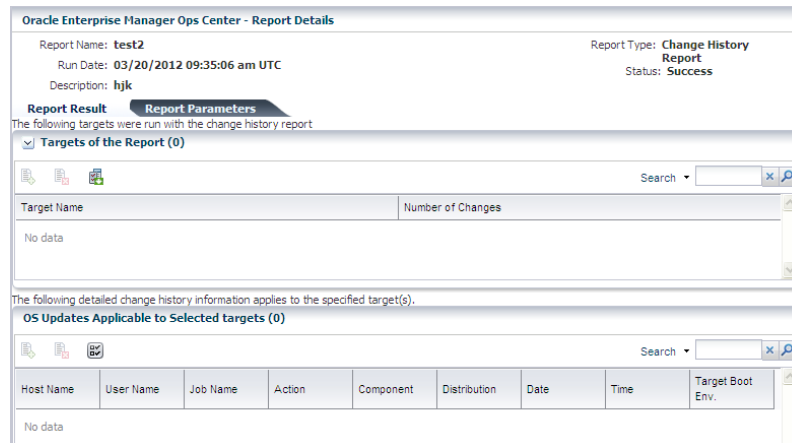
The Reports of Oracle Enterprise Manager Ops Center provides information about assets, such as job history, firmware, operating system updates, and incidents. Reports are exported or used to start jobs on targeted assets. You can schedule to run the report using any of the following parameters:

- **Now** – Select the current date and time to generate the report.
- **At a later date/time** – Select a date and time to generate the report.
- **On a Recurring Schedule** – Select the month and day when you want to generate the report. Select the Start Time, End Time, and Number of Hours between runs. This is to set the number of times the report is generated between the specified start and end time. For example, when you set the start time at 6.00 a.m, end time at 12.00 a.m, and the number of hours between runs as 2, then the report is run at 6.00 a.m, 8.00 a.m, 10.00 a.m, and 12.00 a.m.

After the report is generated, the Report Results pane lets you to export the report result in CSV and PDF formats, view the report interactively, and delete the report. View Interactive option helps you to view the generated report in detail. Report result displays the Report name, Report type, Run Date, Targets of the Report, OS updates applicable to selected targets. Report parameters show the target name, product name, description. You can save the report as a template and also rerun the report.

Figure 10–1 displays an Interactive view of Report Result.

**Figure 10–1 Interactive View of Report Result**



## Roles for Reports

The following table lists the tasks and the role required to complete the task. Contact your administrator when you do not have the necessary role or privilege to complete a task. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant. Table 10–1 illustrates the roles and permissions for reports.

**Table 10–1 Reports Roles and Permissions**

Task	Role
View Reports	All
Create Reports	Asset Administrator

## Actions for Reports

You can perform the following actions in the reports section.

- [Manage Report Templates](#)
- [View and Export Report Results](#)

## Manage Report Templates

A report template is a file that serves as a starting point to create a new report. When you open a report template, it is pre-formatted in some way. When you save a file created with a template, you are usually prompted to save a copy of the file, so that you don't override the template. Templates are provided within a software or a program or it is created by the user. Most major software support templates. If you want to create a similar document or report over and over again, it is a good idea to save one of them as a template. You can open the report template and start creating reports from there. Parameters in the report template are specified when the report is created or run. You can save the criteria as a template, after creating the report criteria. The saved report template enables us to:

- [Generate a Report from a Report Template](#)
- [Edit a Report Template](#)

- [Delete a Report Template](#)

### **Generate a Report from a Report Template**

To generate a report from the report template, do the following:

1. Select Reports from the Navigation pane.
2. Select a saved report template from the center pane.
3. Click the Generate Report icon to run the report. The corresponding report is generated and the results are displayed under Report Results.

### **Edit a Report Template**

To edit a report from the report template, do the following:

1. Select Reports from the Navigation pane.
2. Select a saved report template to edit from the center pane.
3. Click the Edit View icon to edit the selected report template. The corresponding report wizard is displayed.
4. Edit the report parameters as required in the wizard.
5. Click Run and Close to run the report or click Save Template and Close to save the report template. When you click Run and Close, the report is generated but the edits for the report are not saved.

### **Delete a Report Template**

To delete a report from the report template, do the following:

1. Select Reports from the Navigation pane.
2. Select a saved report template to delete from the center pane.
3. Click the Delete icon to delete the report template.
4. Click Ok to confirm the delete action. The selected report template is deleted.

## **View and Export Report Results**

Oracle Enterprise Manager Ops Center provides an interactive result viewer to view the results. The generated report results are displayed under the Report Results in the All Reports page. You can select a report result from the Report Results pane to view the report interactively. You can rerun the report, delete the report, view, export, and save the output of report in the format of CSV and PDF.

You can do the following:

- [View the Report Result](#)
- [Save the Report Result](#)

### **View the Report Result**

To view the report result, do the following:

1. Select Reports in the Navigation pane. The All Reports page in the center pane displays all the report templates and report results.
2. Select a report result under the Report Result section in the center pane.

3. Click the Interactive icon to view the report result. The Interactive Result viewer opens the report result and displays the following information.
  - Report detail – It displays the name, type, run time, and the status of the report.
  - Report Result – It displays the targets on which the report is run and the corresponding operating system updates that are applicable.
  - Report Parameters – It displays the parameters that are used to generate the report.

### Save the Report Result

To save the report result, do the following:

1. Select Reports in the Navigation pane. The All Reports page in the center pane displays all the report templates and report results.
2. Select a report result under the Report Result section in the center pane.
3. Click the View CSV or View PDF icon. You can save or open the report in CSV or PDF formats.

Figure 10–2 illustrates the report output in PDF format.

**Figure 10–2 Exporting a Report Result in PDF**

Report Name:	test1
Description:	test1
Run Date:	Mon Mar 19 20:40:17 MDT 2012
Report Type:	Change History Report

Target Name	Number of Changes
-------------	-------------------

## Location of Report Information in the User Interface

To see report information, expand Reports in the Navigation pane. It displays OS reports, System Information reports, Incident reports, and Firmware reports. Click OS reports to view the various types of OS reports that run on Oracle Solaris/Linux OS updates and Windows OS updates. Click Incident reports to view the different types of incident reports. Table 10–2 illustrates the location of reports in the user interface.

**Table 10–2 Location of Report Information in the UI**

<b>Object</b>	<b>Location</b>
OS Reports	Expand the Reports drawer in the Navigation pane. Click OS Reports to view the various reports that run on Oracle Solaris/Linux OS updates and Windows OS updates.
System Information Reports	Expand the Reports drawer in the Navigation pane. Click System Information Reports. It displays the Create System Information Report wizard in the Actions pane.
Incident Reports	Expand the Reports drawer in the Navigation pane. Click Incident Reports. It displays the types of incident reports.
Firmware Reports	Expand the Reports drawer in the Navigation pane. Click Firmware Reports. It displays the Create Firmware Report wizard in the Actions pane.
Exalogic Reports	Expand the Reports drawer in the Navigation pane. Click Exalogic Reports. It displays the Create Exalogic Report wizard in the Actions pane.

## Firmware Reports

Firmware Compliance Reports enables us to maintain consistent firmware versions across the datacenter. The Firmware Report feature compares the firmware images specified in a firmware profile to the firmware images installed on hardware assets. The report indicates whether the firmware on the asset complies with the profile's specifications. You can update the firmware on any non-compliant asset by clicking the Make Targets Compliant button in the Interactive report.

### To Create a Firmware Report

1. Select Reports in the Navigation pane.
2. Select Firmware Reports.
3. Select Create Firmware Report from the Actions pane. The Create Firmware Report wizard is displayed.
4. Define the report parameters, including:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Schedule – If you do not plan to create this report routinely, clear the Create Schedule check box.
  - Output Format – Select the output format of the report result. CSV and PDF formats are available.
  - Profile – Select the firmware profile for a service processor or for a storage component, such as a RAID controller, expander, or disk.
5. Click Next to display the Select Targets.
6. Select the targets you want to test against the profile. Select the asset from the Available Items hierarchy and click Add to Target List. When you have selected all the targets, click Next to display the Schedule page.
7. Select a desired schedule to run and generate the report.

8. Click Next to display the Summary.
9. Review the summary and click Run Report to create the report job.

The report job starts at the time you specified and compares the values in the profile to the existing values on the targets you selected. The report displays whether a target asset is compliant, not compliant, or not applicable:

- A compliant asset has the firmware images specified in the profile.
- A non-compliant asset does not have the same firmware images as specified in the profile. You can update the firmware on the asset by either clicking the Make Targets Compliant button in the Interactive report or using the procedure in Updating Firmware.
- A non-applicable asset indicates that a firmware image in the profile does not match the model of service processor in the asset. This condition can occur when either the profile does not recognize the model that the service processor is reporting or the profile includes firmware images that are not designed for the service processor.
  - a. Compare the model of the service processor displayed in the asset's Summary tab with the model of the service processor included in the profile. If they are different, add the name in the profile to the asset's data.  
 See *Oracle Enterprise Manager Ops Center Administration Guide* for information about adding a product alias.
  - b. When the firmware profile was created, only images that matched the service processor could be included. However, if the service processor did not report all the firmware types it supported, an image that did not match the service processor could have been included in the profile. To update the software with all the service processor's supported firmware types, use the Refresh action to update the information about the service processor. When the job is completed, view the service processor's Summary tab to see all firmware types.
  - c. Repeat the procedure to create a firmware report.

## Operating System Reports

Use Operating System update reports to check for new software updates and security advisories. For auditing purposes, create a change history report. Various types of update reports are available for Linux, Oracle Solaris, and Windows operating systems. You can export report results to CSV or PDF format.

Use operating system reports to obtain information about managed Oracle Solaris, Linux, and Windows operating systems.

[Table 10-3](#) illustrates the various reports that are run in Oracle Enterprise Manager Ops Center and displays the type of report that are supported and run on an operating system.

**Table 10-3** Compatibility of Reports on Operating System

Report Name	Linux OS	Oracle Solaris 8, 9, and 10	Oracle Solaris 11	Microsoft Windows
Change History Report	Yes	Yes	Yes	No
CVE Compliance Report	Yes	Yes	Yes	No
RSC Report	Yes	Yes	Yes	No

**Table 10–3 (Cont.) Compatibility of Reports on Operating System**

<b>Report Name</b>	<b>Linux OS</b>	<b>Oracle Solaris 8, 9, and 10</b>	<b>Oracle Solaris 11</b>	<b>Microsoft Windows</b>
System Catalog Report	Yes	Yes	Yes	No
Oracle Solaris Update Compliance Report	No	Yes	Yes	No
Baseline Analysis Report	No	Yes	Yes	No
Update Compliance Report	Yes	Yes	Yes	Yes
Incident Compliance Report	Yes	Yes	Yes	Yes
Host Compliance Report	Yes	Yes	Yes	Yes
Distribution Update Report	Yes	Yes	Yes	No
Service Pack Compliance Report	Yes	Yes	Yes	No
Package Compliance Report	Yes	Yes	Yes	No

## Update Compliance Reports

The following reports are available for Linux, Oracle Solaris, and Windows operating systems:

- Host Compliance – Provides information on whether your system is compliant with security and bug fixes incidents.
- Incidence Compliance – Provides information about the number of systems to which the selected operating system updates apply.

## Linux and Oracle Solaris OS Update Reports

In addition to the reports created for all types of operating systems, the following reports are available for Linux and Oracle Solaris operating systems:

- Change History – Provides a history of Operating System update, install, and uninstall jobs completed on managed systems.
- CVE Compliance – Provides information on incidents that are related to specific Common Vulnerability and Exposure Identifiers (CVE IDs) and the systems that have these incidents installed. CVE IDs are unique, common identifiers for publicly known security vulnerabilities.
- Distribution Update – Provides a mapping between selected updates, CVE's, and selected distributions to find out whether the updates are installed.
- Package Compliance – Provides the details of the selected packages on managed system that are compliant or not compliant with the latest recommended version available.
- RSC – Recommended Software Configuration – Provides information about the system compliance for installing a specific application, such as the Oracle 11g Database, on an Oracle Solaris, or Linux Operating System.
- Service Pack Compliance (Linux only) – Provides information on incidents created by the publication and release of a service pack by a vendor. This helps in determining whether the system has the latest service packs released by the vendor.

- Oracle Solaris Update Compliance (Oracle Solaris Operating System only) – Provides information on whether an Oracle Solaris system is compliant with a specific update.
- Baseline Analysis (Oracle Solaris Operating System only) – It helps to check the compliance of systems against newly released Oracle Solaris baselines.

## Change History Report

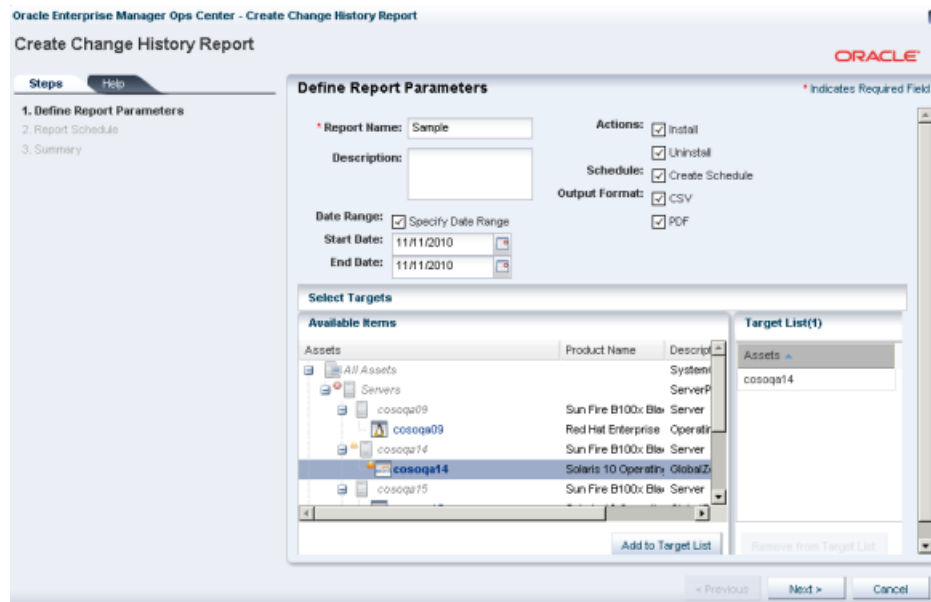
The Change History Report provides a history of operating system update install and uninstall jobs completed on managed Oracle Solaris or Linux systems. The report also displays the deployments made by the specific user, enabling you to track a team of operators.

### To Create a Change History Report

1. Select Reports from the Navigation pane.
2. Select Oracle Solaris/Linux OS Updates from the Reports section.
3. Select Create Change History Report from the Actions pane.

The Create Change History Report wizard is displayed.

**Figure 10–3 Defining Report Parameters for Change History Report**



4. Define the report parameters:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Date Range – Specify the start date and end date between which the report will cover.
  - Actions – Select the actions to be reported. You can select Install, Uninstall or both.
  - Schedule – Select Create Schedule to schedule the report.



- Output Format – Select the output format of the report result. CSV and PDF formats are available.
  - Select Targets – Add the targets by selecting them from the list of Available Items by clicking Add to Target List.
5. Click Next to schedule the report.
  6. Select a desired schedule to run and generate the report.
  7. Click Next to display the Summary.
  8. Review the report parameters and select one of the options as required:
    - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
    - Run and Close – Runs the report and closes the wizard window.

The report results are displayed under the Report Results in the center pane.

See [View and Export Report Results](#) for more information about viewing a report result.

## Baseline Analysis Report

An Oracle Solaris baseline is a dated collection of Oracle Solaris updates, update metadata, and tools. Oracle releases Oracle Solaris baselines on a monthly basis. A Baseline Analysis Report checks the compliance of Oracle Solaris systems against newly released Oracle Solaris baseline. When you install the updates of a baseline on a host, that system is considered to be compliant with that baseline.

Each dated baseline contains these update sets:

- Full – Includes all Oracle Solaris updates
- Recommended – Includes Oracle Solaris recommended updates and security updates
- Security – Includes only Oracle Solaris security updates

All baselines include updates for a specific time frame. However, the Full baseline often contains Oracle Solaris operating system updates that are not included in the Recommended baseline. The Full baseline includes additional updates based on feedback from various customer support groups within Oracle. Recommended baseline does not includes these updates.

To install the Recommended and Security baselines, you must either deploy two jobs or have a job that includes multiple tasks. This might result in multiple reboots, for example, if both tasks (baselines) include updates that have Single User mode requirements.

Oracle Enterprise Manager Ops Center's Knowledge Base (KB) is updated with the information about the baselines. This is done a few days after the official release of baselines by Oracle.

---

---

**Note:** The Oracle Solaris 8 Operating System was placed into End of Service Live (EOSL) on March 31, 2009. Oracle Solaris 8 Operating System baselines are available through March 2009. The KB might contain artificial baselines after that date. Do not use baselines dated after March 2009.

---

---

Oracle Solaris baselines enables you to easily identify the update level of your hosts. For example, install some test hosts with a particular baseline. Test these hosts for a period to see whether the updates in this baseline are stable enough to be used on production hosts. When the testing reveals that this baseline is stable, install the same baseline on production hosts.

Oracle Solaris baselines are available as a component in the recommended component list. It contains a list of dated baselines.

The Baseline Analysis report helps to verify the compliance of your system against the newly-released baselines (as and when they are available in Knowledge Base).

The Baseline Analysis Report (BAR) enables you to determine whether the managed system is compliant with recently released Oracle Solaris baselines. Baselines pertain only to Oracle Solaris systems. This section describes Oracle Solaris baselines, white list, black list, and how to run a Baseline Analysis report in connected and disconnected mode of the Enterprise Controller.

The Baseline Analysis Report (BAR) describes how to generate a BAR. The report gives the compliance status of the managed system with the selected Oracle Solaris baseline that was released.

You can generate two types of BARs:

- Agent-based BAR
- Database-based BAR

In an agent-based BAR, a simulated job is run against the managed hosts. This type of report takes time to complete because it checks for dependent components and missing dependencies, and then downloads the updates that must be installed. When you run a compliance job from this report result, the job is completed quickly because the updates are downloaded. However, to improve the report performance of a BAR, skip the downloads in a simulated job by clearing the check box that is provided for this purpose.

In a database-based BAR, the report is run against the database of the management server, the selected baselines are broken down into individual update IDs, and then formed into an incidents list. The report is generated based on the information that are available on the database. Based on the report result, run a compliance job.

### **White List**

A white list is the list of updates that is required to install in addition to the updates in the baseline. To establish a white list, create a profile using the Required setting. You can also specify a white list when generating a Baseline Analysis Report. Select the white list either from the created profile or enter the update IDs separated by new lines.

For example, baseline B includes updates X, Y, and Z, and the white list has updates U, V, and W. When the Baseline Analysis report is created, the host is marked compliant only when all six updates X, Y, Z, U, V, and W are present.

### **Black List**

A black list is a list of updates that you do not want to install. Create a black list by creating a policy with the specified action for the updates. Select a black list option while creating a Baseline Analysis Report. Select the black list either from the created policy or enter the update IDs separated by new lines.

If a particular update in the profile is set with the policy component setting as Never for an install action, then the update is not installed. If the update is installed, it will not be uninstalled or removed.

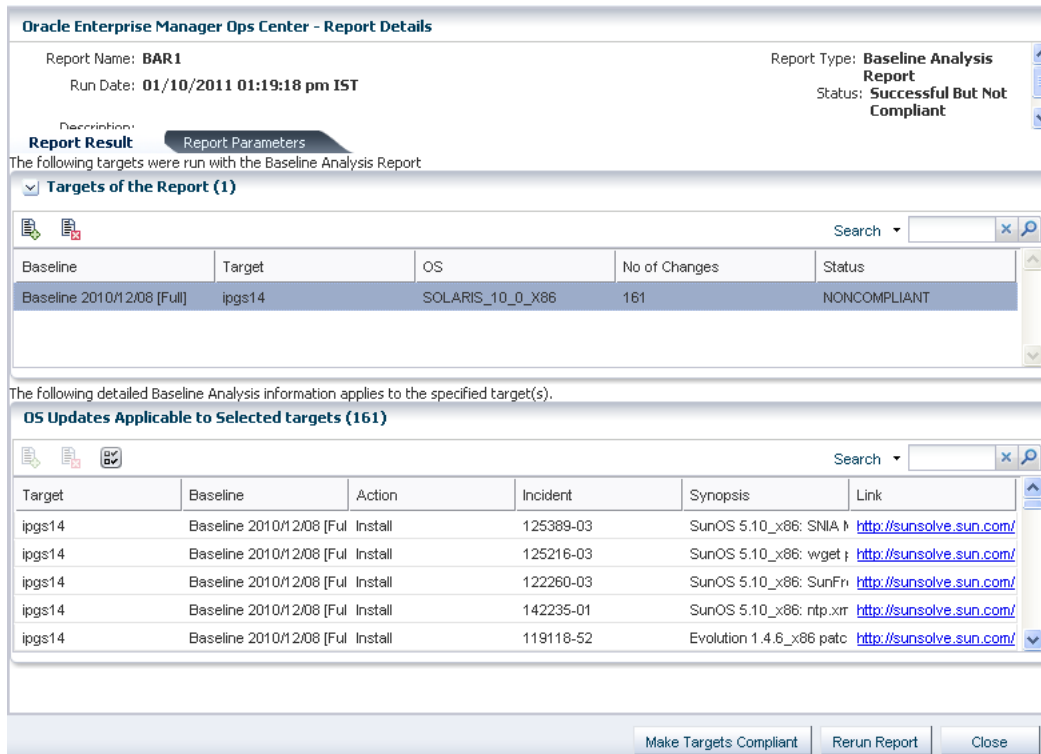
For example, if baseline A has updates X, Y, and Z, and the black list specifies only Y and Z, the system is compliant if X is installed. If the updates Y and Z are installed, they will not get uninstalled if you run a compliance job from the report results. If Y and Z are not installed, they are not listed in the non compliant result and are not added in the compliance job.

### **To Create a Baseline Analysis Report**

This report provides information about the hosts that are compliant with a baseline operating system.

1. Select Reports from the Navigation pane.
2. Select Oracle Solaris/Linux OS Updates from the Reports section.
3. Select Create Baseline Report from the Actions pane. The Create Baseline Analysis Report wizard is displayed.
4. Define the report parameters:
  - Report Name – Name of the report.
  - Description – The description of the report.
  - Schedule – Select Create Schedule to schedule the report.
  - Output Format – Select the output format of the report result. CSV and PDF formats are available.
  - Select Targets – Add the targets by selecting them from the list of Available Items by clicking Add to Target List.
5. Click Next to select the Oracle Solaris baselines.
6. In Select Baseline(s), select the following options:

**Figure 10–4 Selecting Baselines for Baseline Analysis Report**



- Run Against Database or Run Report Against Agent.  
When you select Run Report Against Agent, check the Download check box to download the updates that are installed on the target.
- Select the distribution type and select the baselines from the list. You can select targets of multiple distribution. For each distribution, select the corresponding baselines. A warning message is displayed when the baselines are not selected for a distribution.

---

**Note:** If you have multiple distributions, then you must select baselines for at least one distribution to continue further in the wizard. If you have not selected baselines for a distribution, then the targets of that distribution are not in the report result.

---

- Click Add or Add All to select all the baselines.
7. Click Next to modify the update lists that are applied to the report.
  8. Select any of the following White List options:
    - None – No white list.
    - Manual Input – Enter a list of updates.
    - Specify with Profile – Select a profile to import as a white list.
  9. Select any of the following Black List options:
    - None – No black list.
    - Manual Input – Enter a list of updates.

- Specify with Policy – Select a policy to import as a black list.
10. Click Next to schedule the report.
  11. Select a desired schedule to run and generate the report.
  12. Click Next to display the Summary.
  13. Review the report parameters and select one of the options as required:
    - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate reports later.
    - Run and Close – Runs the report and closes the wizard window.

The report result displays under the Report Results in the center pane.

See [View and Export Report Results](#) for more information about viewing a report result and generating a compliance job from the result.

## Profile Analysis Report

A Profile Analysis Report provides information about Oracle Solaris or Linux systems' compliance with the Operating System Update Profiles that you define in Oracle Enterprise Manager Ops Center. The update profiles include both the system-defined and user-defined profiles in Oracle Enterprise Manager Ops Center.

---

---

**Note:** Avoid running reports for system-defined profiles like Perform Reboot+Reconfigure and Perform Reboot as these profiles do not contain any updates.

---

---

### Before You Begin

You can modify the update list that is applied to generate the report by selecting a white list and a black list.

A white list is the list of updates to install. To establish a white list, create a profile using the required setting. Select the white list either from the created profile or enter the update IDs separated by new lines.

For example, baseline B includes updates X, Y, and Z, and the white list has updates U, V, and W. When the Baseline Analysis Report is created, the host is marked compliant only when all six updates (X, Y, Z, U, V, and W) are present.

A black list is a list of updates that you do not want them to be installed. You create a black list by creating a policy with the specified action for the updates. Select the black list either from the created policy or enter the update IDs separated by new lines.

When a particular update in the profile is set with the policy component setting as Never for the install action, then the update is not installed. When the update is installed, it is not uninstalled or removed.

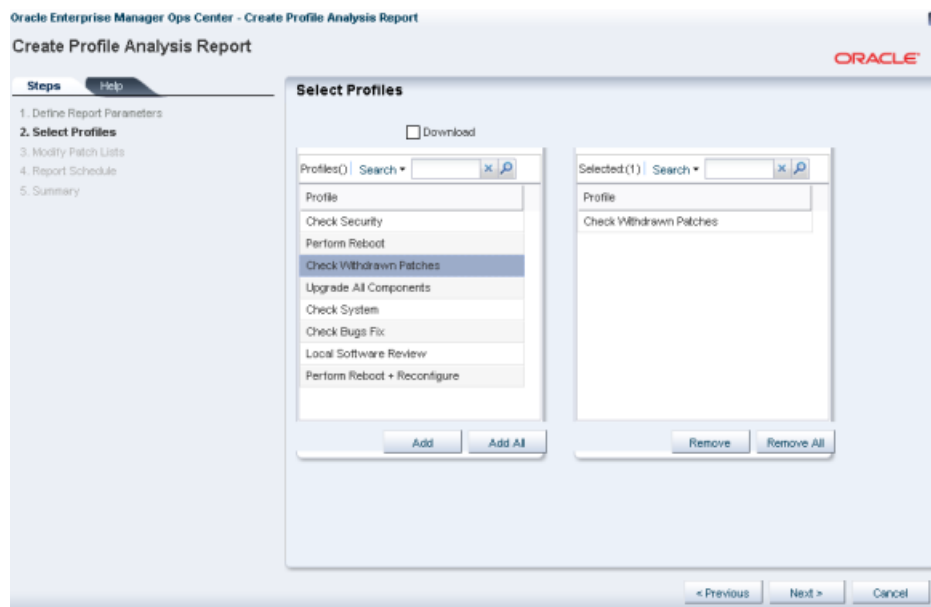
For example, when baseline A has updates X, Y, and Z, and the black list specifies only Y and Z, the system is compliant when X is installed. Even if the updates Y and Z are installed, they are not uninstalled when you run a compliance job from the report results.

### To Create a Profile Analysis Report

1. Select Reports from the Navigation pane.
2. Select Oracle Solaris/Linux OS Updates from the Reports section.

3. Select Create Profile Report from the Actions pane. The Create Profile Report wizard is displayed.
4. Define the report parameters:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Schedule – Select Create Schedule to schedule the report.
  - Output Format – Select the output format of the report result. CSV and PDF formats are available.
  - Select Targets – Add the targets by selecting them from the list of Available Items by clicking Add to Target List.
5. Click Next to select the profiles.
6. Select the profiles from the list and click Add or Add All to select all the available profiles.

**Figure 10–5 Selecting Profiles for Profile Analysis Report**



7. Check the Download check box to download the updates that must be installed for the system compliance.
8. Click Next to modify the update lists that are applied to the report.
9. Select any of the following White List options:
  - None – No white list.
  - Manual Input – Enter a list of updates.
  - Specify with Profile – Select a profile to import as a white list.
10. Select any of the following black list options:
  - None – No black list.
  - Manual Input – Enter a list of updates.
  - Specify with Policy – Select a policy to import as a black list.

11. Click Next to schedule the report.
12. Select a desired schedule to run and generate the report.
13. Click Next to display the Summary.
14. Review the report parameters and select one of the options as required:
  - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
  - Run and Close – Runs the report and closes the wizard window.

The report result displays under the Report Results in the center pane.

See [View and Export Report Results](#) for more information about viewing a report result and generating a compliance job from the result.

## Recommended Software Configuration Report

A Recommended Software Configuration provides information about the system compliance for installing a specific application, such as the Oracle 11g Database, on an Oracle Solaris or Linux operating system.

The Knowledge Base provides a list of application configuration requirements with which you can check your system compliance status.

For example, you can check the system compliance status of Oracle Solaris operating system for installing Oracle 11g Database. The report provides information about the updates that must be installed, uninstalled, or upgraded for installing the Oracle database.

For an Oracle Solaris operating system, you cannot upgrade a update component from the existing lower version to the recommended higher version. Such instances will be marked as Error in the RSC report result. In such scenarios, you cannot make the target system fully compliant with the recommended software components by the report.

### Before You Begin

You can generate different types of RSCs:

- Agent-based RSC
- Database-based RSC

In an agent-based RSC, the report is generated based on the information from the target system. The dependencies for the updates are checked and downloaded when required. This report takes time to generate because it checks dependencies and downloads updates that must be installed.

In a database-based RSC, the report is generated based on the target system information that is available on the database of the Enterprise Controller. The dependencies are not checked and required updates are not downloaded. This type of report is generated quickly.

### To Create a Recommended Software Configuration Report

1. Select Reports from the Navigation pane.
2. Select Oracle Solaris/Linux OS Updates from the Reports section.
3. Select Create Recommended Software Configuration Report from the Actions pane. The Create Recommended Software Configuration Report wizard is displayed.

4. Define the report parameters:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Schedule – Select Create Schedule to schedule the report.
  - Output Format – Select the output format of the report result. CSV and PDF formats are available.
  - Select Targets – Add the targets by selecting them from the list of Available Items by clicking Add to Target List.
5. Click Next to select the recommended software configurations.
6. In Select Recommended Software Configurations, select any of the following options:
  - Run Against Database or Run Report Against Agent.  
When you select Run Report Against Agent, then click the Download check box to download the updates that must be installed on the target.
  - Select the Distribution type.
  - Select the recommended software component from the list and select the required configuration. The recommended configuration describes the prerequisite list of updates for the selected application. You can select targets of multiple distribution. For each distribution, select the corresponding RSCs. A warning message is displayed when you have not selected RSCs for a distribution.

---



---

**Note:** When you have multiple distributions, then you must select RSCs for at least one distribution to continue further in the wizard. When you have not selected RSCs for a distribution, then the targets of that distribution are not in the report result.

---



---

7. Click Next to schedule the report.
8. Select a desired schedule to run and generate the report.
9. Click Next to display the Summary.
10. Review the report parameters and select one of the option as required:
  - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
  - Run and Close – Runs the report and closes the wizard window.

The report result displays under the Report Results in the center pane.

See [View and Export Report Results](#) for more information about viewing a report result and generating a compliance job from the result.

## Oracle Solaris Update Compliance Report

The Oracle Solaris Update Compliance report determines whether a specific Oracle Solaris system is compliant with a particular released Update.

### To Create an Oracle Solaris Update Compliance Report

1. Select Reports from the Navigation pane.



2. Select Additional Reports from the Reports section.
3. Select Solaris Update Compliance from the Actions pane. The Solaris Update Compliance Report wizard is displayed.
4. Specify the report parameters:
  - Name – The name of the report.
  - Description – A description of the report.
  - Schedule – Select Create Schedule to schedule the report.
  - Output Format – Select the output format of the report result. CSV and PDF formats are available.
  - Select Targets – Add the targets by selecting them from the list of Available Items by clicking Add to Target List.
5. Click Next to select the target asset.  
The Select Targets page is displayed.
6. Add the targets by selecting them from the list on the left by clicking Add to Target List. Click Next to display the Summary page.
7. Click Save Report to save the report for future use. This returns you to the Reports tab, where you can run the report by selecting it from the Saved Reports section and clicking Re-run Report.
8. Click Run Report to run and display the report.
9. Click Export to CSV to export the report result.
10. Click Done to close the report.

## Incident Compliance Report

Incidents are the updates that are available for an application or feature. Incidents apply to one or more packages or RPMs. You can run an incident compliance report to determine whether the incidents on the managed hosts are compliant with the latest released version.

### Incident Compliance Report for Oracle Solaris or Linux

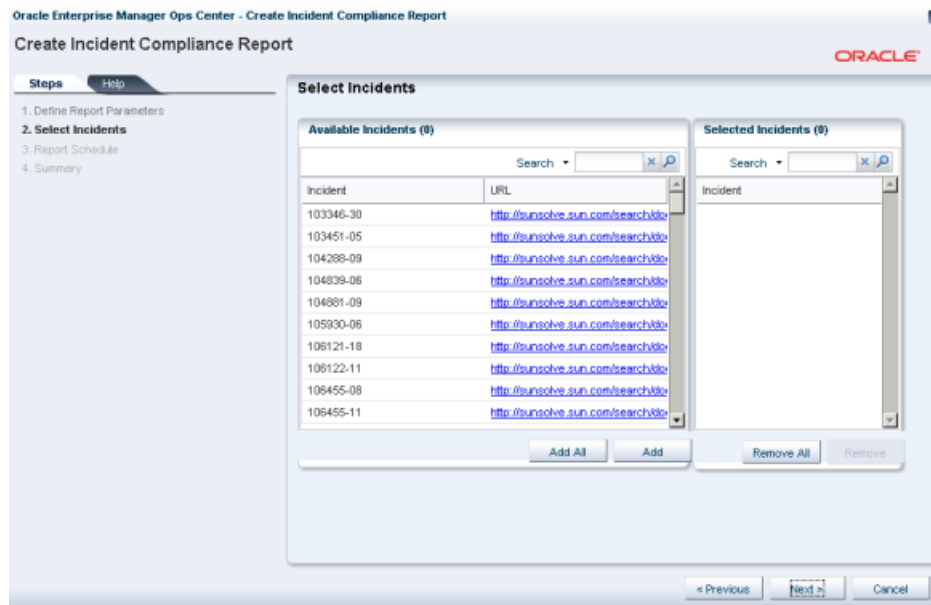
You can run an incident compliance report to determine whether the incidents on the managed hosts are compliant with the latest released version.

#### To Create an Incident Compliance Report for Oracle Solaris or Linux

1. Select Reports from the Navigation pane.
2. Select Oracle Solaris/Linux OS Updates from the Reports section.
3. Select Create Incident Report from the Actions pane. The Create Incident Compliance Report wizard is displayed.
4. Define the report parameters:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Criteria – You can select either Select Updates or Filter Updates, for selecting the updates that are used as a comparison. Depending on the selection of criteria the wizard steps vary.

- Compliant – Select either Compliant or Non-compliant for compliance status.
  - Schedule – Select Create Schedule to schedule the report.
  - Output Format – Select the output format of the report result. CSV and PDF formats are available.
  - Select Targets – Add the targets by selecting them from the list of Available Items by clicking Add to Target List.
5. Click Next to select the updates.
  6. When you have selected Select Updates in the previous step, the list of available incidents is displayed.

**Figure 10–6 Selecting Incidents for Incident Compliance Report**



7. Select the incidents and click Add or Add All to select all the listed incidents.
8. If you have selected Filter Updates in the first step, then select the following:
  - Select Packages – You can select the updates based on the category, update type and releases date. Select the packages and click Add or Add All to select all the packages in the Available Packages list. Click Next to select the CAN IDs.
  - Select CAN IDs – Select from the list of Available CAN IDs. Click Add or Add All as required.
9. Click Next to schedule the report.
10. Select a desired schedule to run and generate the report.
11. Click Next to display the Summary.
12. Review the report parameters and select one of the options as required:
  - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
  - Run and Close – Runs the report and closes the wizard window.

The report result displays under the Report Results in the center pane.

See [View and Export Report Results](#) for more information about viewing a report result and generating a compliance job from the result.

### Incident Compliance Report for Microsoft Windows

You can run an incident compliance report to determine whether the incidents on the managed hosts are compliant with the latest released version.

The Incident Compliance Report provides information about whether your systems are compliant with the Windows updates incidents. This report displays the number of systems to which the selected Windows updates apply, how many systems have the updates installed, and how many systems require the updates to be installed to make the systems compliant. You can create a Windows update job based on the results of an Incident Compliance Report.

#### To Create an Incident Compliance Report for Windows

1. Select Reports from the Navigation pane.
2. Select Windows Incident Compliance Report from the Actions pane. The Windows Incident Compliance Report wizard is displayed.
3. Specify the report parameters. They include:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Specify the Windows OS updates on which to run the report – You can specify filter criteria such as Category, Severity, Superseded, and Release Date for Windows OS updates, or you can select specific Windows OS updates to run the report.  
Click Next.
4. Based on your selection in Step 3, either the Define Updates Filter window is displayed or the Select Updates window is displayed. When the Define Updates Filter window is displayed, go to Step 6. When the Select Updates window is displayed, go to Step 7.
5. Make your selections in the Define Updates Filter screen. They include:
  - Category – Includes Application, Critical Updates, Definition Updates, Drivers, Service Packs, Security Updates, Tools, Update Rollups, and WSUS Infrastructure Updates. You can select either All available updates under all category or Selected categories only. Use the Control key on the keyboard to select multiple items in the list under Selected category only.
  - Severity – Includes Critical, Important, Moderate, Low, and Default. You can select either All updates with any severity or Selected severities only. Use the Ctrl key on the keyboard to select multiple items in the list under Severity.
  - Superseded – Enables you to select all or just the most recent updates.
  - Release Date – Refers to the date that the update updates were released. You can select the range of release dates to include in your report by filling in the From and To fields. Click Next. Go to Step 8.
6. Make your selections in the Select Updates window. Under Search, Select All enables you to include a bulletin ID, article ID, and title in your search, or you can select specific fields to narrow your search. Use the Control key on the keyboard to make multiple selections in the list under Available Windows Software Updates.  
Click Add to Updates List, and then click Next to select the targets.

7. Add the targets by selecting them in the list of Available Items, by clicking Add to Target List.

Click Next to display the Summary page.

8. Click Finish to run the report.

The results of the report are displayed under the Report Results list.

## Host Compliance Report

You can run a host compliance report to determine whether the hosts are compliant with security and bug fix incidents. This report displays the number of updates that are applicable to each system, and whether the updates are installed or must be installed to make the system compliant. You can also create an update job based on the results of a Host Compliance Report.

### Host Compliance Report for Oracle Solaris or Linux

The Host Compliance Report provides information if your systems are compliant with update incidents.

#### To Create a Host Compliance Report for Oracle Solaris or Linux

1. Select Reports from the Navigation pane.
2. Select Oracle Solaris/Linux OS Updates from the Reports section.
3. Select Create Host Compliance Report from the Actions pane.  
The Create Host Compliance Report wizard is displayed.
4. Define the report parameters:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Update Level – Select whether you want the compliant status for Security and Bug Fixes or for only Security Updates.
  - Compliance – Select either Compliant or Non-Compliant.
  - Schedule – Select Create Schedule to schedule the report.
  - Output Format – Select the output format of the report result. CSV and PDF formats are available.
  - Select Targets – Add the targets by selecting them in the list of Available Items by clicking Add to Target List.
5. Click Next to schedule the report.
6. Select a desired schedule to run and generate the report.
7. Click Next to display the Summary.
8. Review the report parameters and select one of the options as required:
  - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
  - Run and Close – Runs the report and closes the wizard window.

The report result displays under the Report Results in the center pane.

See [View and Export Report Results](#) for more information about viewing a report result and generating a compliance job from the result.

### Host Compliance Report for Microsoft Windows

The Host Compliance Report for Windows provides information if your systems are compliant with the Windows updates incidents. This report displays the number of Windows updates that are applicable to each system, and whether the updates are installed or must be installed to make the system compliant. You can also create a Windows update job based on the results of a Host Compliance Report.

#### To Create a Host Compliance Report for Windows

1. Select Reports from the Navigation pane.
2. Select Windows Host Compliance Report from the Actions pane. The Windows Host Compliance Report wizard is displayed.
3. Specify the report parameters. They include:
  - Report Name – A name for the report.
  - Description – A description of the report.
  - Specify the Windows OS updates on which to run the report. You can specify filter criteria such as Category, Severity, Superseded, and Release Date for Windows OS updates, or you can select specific Windows OS updates to run the report.
4. Click Next. Based on your selection in Step 3, either the Define Updates Filter window is displayed or the Select Updates window is displayed. When the Define Updates Filter window is displayed, go to Step 5. When the Select Updates window is displayed, proceed to Step 6.
5. Make your selections in the Define Updates Filter screen. They include:
  - Category – Includes Application, Critical Updates, Definition Updates, Drivers, Service Packs, Security Updates, Tools, Update Rollups, and WSUS Infrastructure Updates. You can select either All available updates under all category or Selected categories only. Use the Control key on the keyboard to select multiple items in the list under Selected category only.
  - Severity – Includes Critical, Important, Moderate, Low, and Default. You can select either All updates with any severity or Selected severities only. Use the Ctrl key on the keyboard to select multiple items in the list under Severity.
  - Superseded – Enables you to select all or just the most recent updates.
  - Release Date – Refers to the date that the updates were released. You can select the range of release dates to include in your report by filling in the From and To fields. Click Next. Go to Step 8.
6. Make your selections in the Select Updates window. Under Search, Select All enables you to include a bulletin ID, article ID, and title in your search, or you can select specific fields to narrow your search. Use the Control key on the keyboard to make multiple selections in the list under Available Windows Software Updates. Click Add to Updates List. Click Next.
7. Add the targets by selecting them from the list of Available Items. Click Add to Target List. Click Next to display the Summary page.
8. Click Finish to run the report.

The results of the report are displayed under Report Results list.

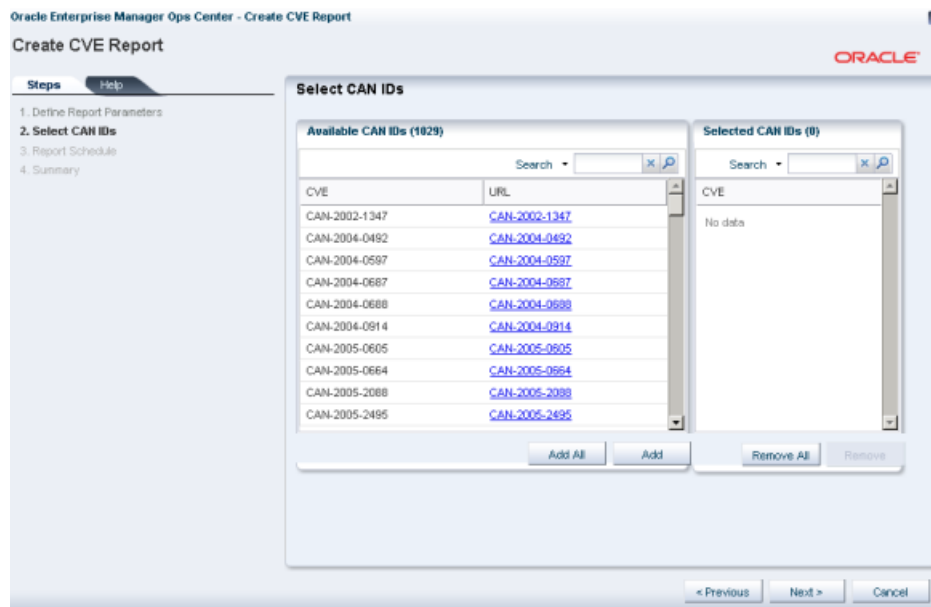
## Common Vulnerability and Exposure (CVE) Report

The CVE report provides information about incidents that are related to specific Common Vulnerability and Exposure Identifiers (CVE IDs) and the systems that must have these incidents installed. CVE IDs are unique, common identifiers for publicly known security vulnerabilities. The updates from a list of vendors are published as common vulnerabilities and security exposure incidents. CVEs are identified by a candidate ID (CAN ID).

### To Create a CVE Report

1. Select Reports from the Navigation pane.
2. Select Oracle Solaris/Linux OS Updates from the Reports section.
3. Select Create CVE Report from the Actions pane. The Create CVE Report wizard is displayed.
4. Define the report parameters. They include:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Compliance – Select either compliant or non-compliant report.
  - Schedule – Select Create Schedule to schedule the report.
  - Output Format – Select the output format of the report result. CSV and PDF formats are available.
  - Select Targets – Add the targets by selecting them from the list of Available Items by clicking Add to Target List.
5. Click Next to select the CAN IDs.
6. Select one or more CAN IDs and click Add or Add All to select all the available CAN IDs.

**Figure 10–7** Selecting CAN IDs in CVE Report



7. Click Next to schedule the report.

8. Select a desired schedule to run and generate the report.
9. Click Next to display the Summary.
10. Review the report parameters and select one of the options as required:
  - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
  - Run and Close – Runs the report and closes the wizard window.

The report result is displayed under the Report Results in the center pane.

See [View and Export Report Results](#) for more information about viewing a report result and generating a compliance job from the result.

## System Catalog Report

A System Catalog Report lists the current catalog of one or more systems. A system catalog contains a list of operating system software components that are installed on a managed system. Catalogs provide the capability to directly manipulate the installed software components on a single operating system or a group of operating systems.

After an operating system is available and selected, you can view and modify the catalogs, and create historical catalogs. Historical catalogs are snapshots of the system. The software automatically takes a snapshot of the operating system after running a job on the operating system, including when you discover and manage the operating system. A snapshot is stored as a catalog with the time stamp and job details after every update job that you run on a system.

You can create a new catalog at any time and use it to record the state of a system. Catalogs enables us to rollback our system to any previous configuration or to create a profile that is used to apply a consistent configuration throughout our datacenter.

See [Chapter 13, "Operating System Updates"](#) for more information on System Catalogs.

### To Create a System Catalog Report

1. Select Reports from the Navigation pane.
2. Select System Catalog Report from the Actions pane.

The System Catalog Report wizard is displayed.
3. Define the report parameters, including:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Schedule – Select Create Schedule to schedule the report.
  - Output Format – Select the output format of the report result. CSV and PDF formats are available.
  - Select Targets – Add one or more targets by selecting them in the list of Available Items by clicking Add to Target List.
4. Click Next to display the Schedule.
5. Select a desired schedule to run and generate the report.
6. Click Next to display the Summary.
7. Review the Summary, then click Run and Close.

The report result is displayed under the Report Results in the center pane.

See [View and Export Report Results](#) for more information about viewing a report result and generating a compliance job from the result.

## Additional Operating System Reports

Use Additional Operating System Reports to obtain information from Service Pack Compliance Report, Distribution Update Report, and Package Compliance Report. You can export report results to CSV format.

### Distribution Update Report

A Distribution Update Report provides a mapping between selected updates, and CVEs and selected distributions to find out whether the updates are installed. This report determines whether a specific distribution (E.G. SOLARIS10\_SPARC) has been updated with specific updates, or CVEs.

#### To Create a Distribution Update Report

1. Select Reports from the Navigation pane.
2. Select Oracle Solaris/Linux OS Updates from the Reports section.
3. Select Distribution Update Report from the Actions pane. The Distribution Update Report wizard is displayed.
4. Define the report parameters. They include:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Category – Select the required categories.
  - Type – Select required types. Package and Update types are available.
  - Released – Mention the start date and the end date.
5. Click Next to display the Distributions.
6. Select the required Distribution and click Add or Add All to add distributions. You might click Remove or Remove All when you do not require any distribution.
7. Click Next to select the updates.
8. Click Next to select the packages.
9. Click Next to select the CVEs. You might click Add or Add All to add CVEs and Remove or Remove All when you do not require any CVE.
10. Click Next to display the Summary.
11. Review the Summary and select one of the options as required:
  - Save Report – Saves the report as a template and closes the wizard.
  - Run Report – Runs the report and closes the wizard window.

The report result is displayed under the Report Results in the center pane.

### Service Pack Compliance Report

A Service Pack Compliance Report provides information on updates created by the publication and release of a service pack by a vendor. This report enables you to



determine whether the target system has the latest service package installed that is provided by the vendors.

### **To Create a Service Pack Compliance Report**

1. Select Reports from the Navigation pane.
2. Select Oracle Solaris/Linux OS Updates from the Reports section.
3. Select Service Pack Compliance Report Creation Wizard from the Actions pane. The Service Pack Compliance Report Creation wizard is displayed.
4. Define the report parameters. They include:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Status – Select the compliant or non compliant status.
  - Services – Select the required services.
5. Click Next to select the Targets. Add the targets by selecting them from the list of Available Items by clicking Add to Target List.
6. Click Next to display the summary.
7. Review the Summary and select one of the options as required:
  - Save Report – Saves the report as a template and closes the wizard.
  - Run Report – Runs the report and closes the wizard window.The report result is displayed under the Report Results in the center pane.

## **Package Compliance Report**

A Package Compliance Report provides a mapping between the selected packages and the selected target systems to find out the installed packages.

### **To Create a Package Compliance Report**

1. Select Reports from the Navigation pane.
2. Select Oracle Solaris/Linux OS Updates from the Reports section.
3. Select Package Compliance Report Creation Wizard from the Actions pane. The Package Compliance Report Creation wizard is displayed.
4. Define the report parameters. They include:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Status – Select the compliant or non compliant status.
  - Level – Select security updates or security and bug updates.
5. Click Next to select the Targets. Add the targets by selecting them from the list of Available Items by clicking Add to Target List.
6. Click Next to select the Packages.
7. Click Next to display the summary.
8. Review the Summary and select one of the options as required:
  - Save Report – Saves the report as a template and closes the wizard.

- Run Report – Runs the report and closes the wizard window.

The report result is displayed under the Report Results in the center pane.

## Incident Reports

You can create incident reports to obtain information about incidents.

The following types of incident reports are available:

- The Incident Summary Report – It is a historical report that summarizes information about all alerts and incidents for a specified category, such as alarm state, alarm owner, asset type, date range, severity levels, and affected asset groups.
- The Incident Detail Report – It contains detailed information about one or more incidents. In addition to a summary, the report includes an audit trail consisting of state-change annotations, alert annotations, suggested-fix annotations, comment annotations, operation annotations.

Each incident has four pages, after the summary page. They are:

- Details of the incident
- Suggested actions, if any
- Alerts History
- Any annotations that are associated with the incident

When you create a report, you can save the report as a template, or you can generate the report. After a report is created, you can view the report, re-run the report to get updated information, or save it as a template.

### To Create an Incident Summary Report

1. Select Reports in the Navigation pane.
2. Select Incident Reports, and then click Incident Summary Report.
3. Select Create Incident Summary Report from the Actions pane.
4. Define the report parameters:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Schedule – Select Create Schedule to schedule the report.
  - Output Format – Select the output format of the report result. CSV and PDF formats are available.
  - Select Assets – Select either all assets or specific assets.
5. Click Next to specify the Incident Parameters.
6. Define the incident parameters by providing the following information:
  - To create a historical report of all incidents and the date that each incident was detected, select All Creation Dates.
  - To create a summary report for incidents detected during a specific date range, select Range of Creation Dates, then enter the beginning date in the From field and the ending date in the To field.

- To filter by severity level, owner, or state, highlight the fields to include in the report. Use Ctrl+Enter to select multiple options.
  - To filter by one or more criteria, add the criterion in the Description Contains field. Use a comma-delimited list for multiple criteria. For example, FileSystemUsage or FileSystemUsage,SwapUsage.
7. Click Next to display the Schedule.
  8. Select a desired schedule to run and generate the report.
  9. Click Next to display the Summary.
  10. Review the summary and select one of the options as required:
    - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
    - Run and Close – Runs the report and closes the wizard window.
- The report results are displayed under the Report Results in the center pane.

#### To Create an Incident Detail Report

1. Select Reports in the Navigation pane.
2. Select Incident Reports, and then click Incident Detail Report.
3. Select Create Incident Detail Report from the Actions pane.
4. Define the report parameters:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Output Format – Select the output format of the report result. CSV and PDF formats are available.
5. Click Next to display the Summary.
6. Review the summary and select Save Template and Close. It saves the report as a template and closes the wizard. You can use the report template to generate the report later.

The report results are displayed under the Report Results in the center pane.

---



---

**Note:** The Incident Compliance Report refers to the Microsoft Windows operating system incidents, while Incident Summary Report and Incident Detail Report refers to alerts and alarms that are raised by Oracle Enterprise Manager Ops Center incidents.

---



---

## System Information Reports

Create a system information report to obtain the information on assets such as operating systems, servers, chassis, logical domains, global zones, non-global zones, and M-Series servers.

#### To Create a System Information Report

1. Select Reports from the Navigation pane.
2. Select System Information Reports from the Reports section.

3. Select Create System Information Report from the Actions pane. The Create System Information Report wizard is displayed.
4. Define the report parameters, including:
  - Report Name – The name of the report.
  - Description – A description of the report.
  - Schedule – Select Create Schedule to schedule the report.
  - Output Format – Select the output format of the report result. CSV and PDF formats are available.
  - Select Targets – Add one or more targets by selecting them in the list of Available Items by clicking Add to Target List.
5. Click Next to display the Attribute Selection.
6. Select one or more attributes from the list and click Add or Add All to choose all the attributes.  
Click Next to display the Attribute Filters.
7. To set a filter for an attribute, select the attribute and specify its condition. Click the Add icon to set filters for other attributes.  
Click Next to display the Schedule, when you are finished setting the filters.
8. Select a desired schedule to run and generate the report.
9. Click Next to display the Summary.
10. Review the report parameters and select one of the options as required:
  - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
  - Run and Close – Runs the report and closes the wizard window.The report results are displayed under the Report Results in the center pane.

To view the report, select it from the Reports Results section and then click one of the icons to choose the format: View interactively, View CSV, or View PDF.

See [View and Export Report Results](#) for more information about generating a compliance job from the result.

## Exalogic Reports

The Exalogic report is all about viewing the rack setup for each of the rack within the system including the asset details related to the firmware. Exalogic Report parameters display the name and model of the Exalogic system. It also displays the number of assets in the rack by their types, such as compute nodes, switches, and storage nodes in the system.

### To Create an Exalogic Report

1. Select Reports from the Navigation pane.
2. Select Exalogic Reports from the Reports section.
3. Select Create Exalogic System Report from the Actions pane. The Create Exalogic System Report wizard is displayed.
4. Define the report parameters, including:

- Report Name – The name of the report.
  - Description – A description of the report.
  - Schedule – Select Create Schedule to schedule the report.
  - Output Format – Select the output format of the report result. CSV and PDF formats are available.
5. Click Next to display the Schedule.
  6. Select a desired schedule to run and generate the report.
  7. Click Next to display the Summary.
  8. Review the report parameters and select one of the options as required:
    - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
    - Run and Close – Runs the report and closes the wizard window.The report results are displayed under the Report Results in the center pane.
  9. Once the report is run successfully, select the report in the Reports Results section and click the PDF or CSV icon to open the report.

## Related Resources for Reports

For instructions in performing actions or to learn more about the role of this feature, see Oracle Enterprise Manager Ops Center Library at <http://www.oracle.com/pls/topic/lookup?ctx=oc121&id=howto>



This chapter describes hardware management features that are available in Oracle Enterprise Manager Ops Center:

- [Introduction to Managing Hardware Assets](#)
- [Roles for Hardware Management](#)
- [Actions for Hardware Management](#)
- [Location of Hardware Information in the User Interface](#)
- [Profiles for Hardware Management](#)
- [Configuring the Service Processor](#)
- [Configuring a RAID Controller](#)
- [Configuring a Dynamic System Domain](#)
- [Configuring a Rack and Placing Components](#)
- [Hardware Monitoring](#)
- [Monitoring Power Utilization](#)
- [Maintaining Hardware Assets](#)
- [Firmware Provisioning](#)
- [Related Resources for Hardware Management](#)

## **Introduction to Managing Hardware Assets**

Oracle Enterprise Manager Ops Center provides comprehensive lifecycle management for the hardware assets in your data center. The hardware assets can be handled individually or as a group. After the discovery and management of the hardware assets, as described in [Asset Management](#), you can configure and then monitor them to gather the information to maintain them.

### **Configuring Hardware Assets**

Use these deployment plans:

- Install Server
- Update BIOS Configuration
- Configure Service Processor
- Configure Server Hardware and Install OS

- Configure RAID
- Configure M-Series Hardware, Create and Install Domain
- Configure and Install Dynamic System Domain

All the plans are based on hardware resource profiles. See [Hardware Resource Profiles](#)

## Monitoring Hardware Assets

As soon as a hardware asset is managed, Oracle Enterprise Manager Ops Center starts to monitor it, according to the asset type's monitoring profile. The center pane displays information for a selected asset in a series of tabbed windows. The tabs and the type of information is specific for the asset type but, in general, Oracle Enterprise Manager Ops Center reports the following:

- Health status
- Power state
- Power usage
- Hardware variables and connectivity

You can change the monitoring thresholds in the standard profile to specify the conditions that generate an alert. You can also create custom profiles with different rule sets and alert parameters and apply the profile to a specific system, a group of homogeneous systems, or a group that you define.

For more information about monitoring policies and rules, see [Chapter 4](#).

For information about monitoring power consumption, see [Energy Tab](#).

## Maintaining Hardware Assets

Based on your observations, you can control your hardware assets and do the following actions:

- Update management credentials. See [Asset Management](#)
- [Setting and Changing the Power Policy](#)
- Power systems on and off
- Place in maintenance mode
- Reset a server
- Get access to the serial console
- Use locator lights to identify a specific asset
- Check firmware compliance and update firmware

Use these deployment plans or customize them:

- Update Firmware
- Update Storage Appliances
- Update BIOS Configuration

## Roles for Hardware Management

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



task. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 11–1 Hardware Roles and Permissions**

<b>Task</b>	<b>Role</b>
Configure and Deploy Server	Server Deploy Admin
Install Server	Server Deploy Admin
Configure RAID	Server Deploy Admin
Update Management Credentials	Security Admin
Importing and uploading firmware images	Storage Admin
Edit Attributes	Asset Admin
Power On, Power Off, Power on with Net Boot	Asset Admin
Set Power Policy	Asset Admin
Reset Servers, Reset Service Processors, Refresh	Asset Admin
Locator Light On/Off,	Asset Admin
Snapshot BIOS Configuration, Update BIOS Configuration	Asset Admin
Update Firmware	Update Admin
Simulate a firmware update	Update Admin Update Sim Admin
Launch LOM Controller	Asset Admin
Edit Tags	Asset Admin

## Actions for Hardware Management

After you manage your assets, you can perform the following actions:

- Use a resource profile to configure a hardware asset
- View utilization of systems
- Modify energy consumption
- Reset a server
- Power systems on and off
- Place in maintenance mode
- Get access to the serial console
- Use locator lights to identify a specific asset
- Check firmware compliance
- Update firmware
- Use a provisioning profile to update firmware

## Location of Hardware Information in the User Interface

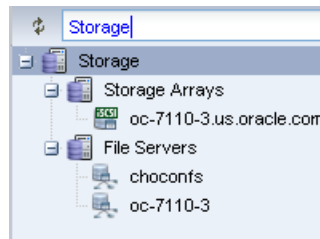
Hardware assets are visible in the All Assets section of the user interface. For assets with a service processor, both the service processor and the system are included, as shown in [Figure 11-1](#).

**Figure 11-1 Managed System**



Each type of hardware is also added to the appropriate group in the Resource Management view, as shown in [Figure 11-2](#).

**Figure 11-2 Example of Resource Management View**



**Table 11-2 Location of Hardware Information in the BUI**

To See	Location
All servers	Expand Servers in the Assets pane. The center pane lists up to 50 servers.
Details for a specific server	Expand Servers in the Assets pane. Then select one of the servers. The center pane includes a series of tabbed displays.
Monitoring Rules for a specific server	Expand Servers in the Assets pane. Then select one of the servers. Then select the Monitoring tab.
Monitoring rules for a hardware type	Expand Plans and then Operational Plans and then Monitoring Policies. Select a type. The center pane shows all of the rules and thresholds.
Current firmware version	Expand Servers in the Assets pane. Then select one of the servers. Then select either the Summary tab or the Hardware tab. Each one includes the Firmware table.
A report of all attributes	Expand Reports and then select System Information Report.

## Profiles for Hardware Management

The work flow of an asset deployment can be captured and enacted in a repeatable fashion using plans and the profiles included in the plans. Oracle Enterprise Manager Ops Center provides default profiles for configuring hardware asset types consistently. You can use the default profiles, make copies of the profile to edit, or create new ones.

Deployment proceeds from configuring the hardware, installing the correct firmware, provisioning the OS, and applying the required updates. The deployment is not only

for servers with an OS installed but also for chassis, racks, power distribution units, and M-Series servers.

## Hardware Resource Profiles

Use hardware resource profiles in a deployment plan to configure, install, or update systems. The Oracle Enterprise Manager Ops Center software provides the following hardware resource profiles:

- [Configuring the Service Processor](#)
- [Configuring a RAID Controller](#)
- [Configuring a Dynamic System Domain](#)
- [Configuring a Rack and Placing Components](#)

You can use the default profiles, make copies of the profile to edit, or create new ones. Use the profiles in a deployment plan to configure your hardware assets.

## Firmware Provisioning Profiles

Hardware depends on firmware to perform operations. Part of monitoring and managing a hardware asset is to make sure that it has the appropriate version of firmware. Oracle Enterprise Manager Ops Center uses firmware profiles to provision, or update, firmware on each type of asset.

A firmware profile is a set of actions and values that define how to provision one or more assets and specifies one or more firmware images. A firmware profile updates existing firmware assets completely and consistently. When you apply a deployment plan that contains a firmware profile, Oracle Enterprise Manager Ops Center compares the versions of each firmware image specified in the profile with the versions of the existing firmware on the asset. It then takes the action you specify in the profile.

See [Firmware Compliance Reports](#) and [Firmware Provisioning](#).

## Configuring the Service Processor

The Declare Unconfigured Asset action includes the service processor in the Oracle Enterprise Manager Ops Center environment. You can configure only unconfigured service processors, that is, a processor in its factory default state. Use a deployment plan to configure the service processor:

- Configure Service Processor
- Update BIOS Configuration
- Configure and Deploy Server
- Install Server

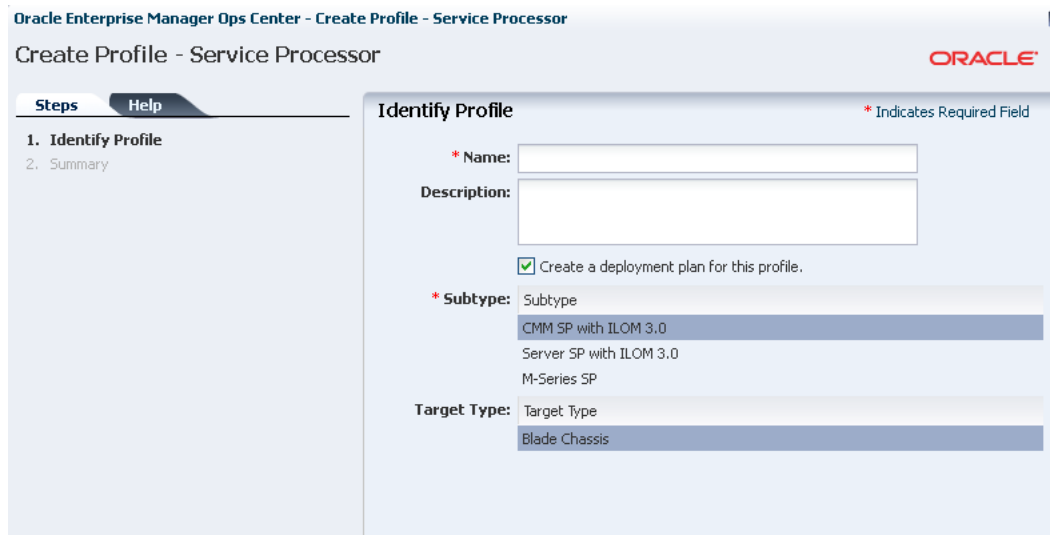
An alternative to specifying the configuration in the profile, is to duplicate an existing configuration. You can create a snapshot of the BIOS of a working service processor, which creates also creates profile. You then apply the profile to an unconfigured service processor.

## Create Service Processor Configuration Profile and Plan

1. Expand Plans in the Navigation pane and the select Profiles and Policies.
2. Expand Service Processors.

3. Click Create Profile. The first step of the wizard is displayed. Depending on the subtype and target you select, more steps are added.

**Figure 11–3 Create Profile - Service Processor**

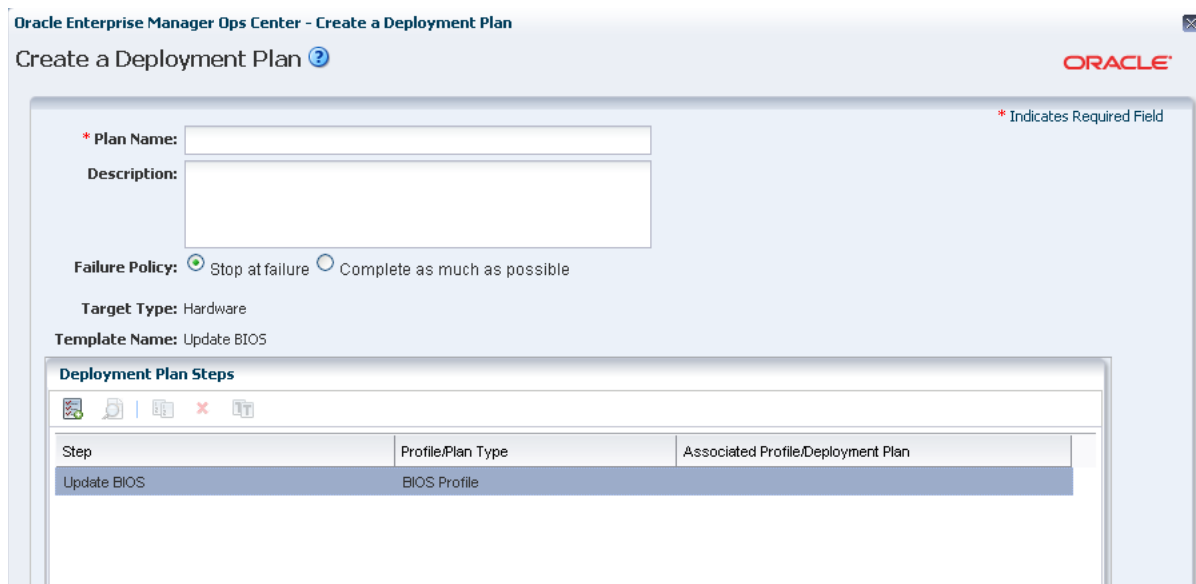


4. Complete the specification of the service processor and click Finish. The new profile and plan are available from the Assets pane.

## Create BIOS Configuration Profile and Plan

1. Expand Plans in the Navigation pane and the select Plans.
2. Expand Update BIOS Configurations.
3. Click Create Plan from Template. The first step of the wizard is displayed, which includes the Update BIOS profile.

**Figure 11–4 Create Plan - BIOS**



4. Click on Update BIOS profile.
5. Click the Create Profile icon.

**Figure 11–5 Create Profile-BIOS Configuration**

6. Click Next to review and then click Finish to submit the job.
7. When the job is completed, return to the Create a Deployment Plan window.
8. Specify a name for the plan and select the new profile.
9. Click Save to submit the job.

The new profile and plan are available from the Assets pane.

## Create a Snapshot of a Service Processor Configuration

1. Expand Assets in the Navigation pane and select Servers.
2. Select the configured server.
3. Click the Hardware tab in the center pane.
4. In the Component Navigation section, select Service Processor. The Service Processor Configuration section displays the configuration attributes and values.
5. In the Service Processor Snapshots section, click the Create Snapshot icon to display the following window:

**Figure 11–6 Create Service Processor Configuration Snapshot**


---

**Note:** An alternative method of displaying this window if you are familiar with the current configuration is to select the server and then choose Snapshot BIOS Configuration in the Actions pane.

---

6. Specify a name for this snapshot and accept the default of creating a profile from the snapshot.
7. Click Create Snapshot to submit the job.
8. When the job completes, the snapshot is located in the EC local library.

## Apply a Snapshot of a Server Processor Configuration

This procedure applies a snapshot of one server's service processor to another, unconfigured service processor. You can apply the snapshot to one server by using the Update BIOS Configuration action or you can use the snapshot profile as a step in the Install Server deployment plan.

### View a Service Processor Snapshot

To verify the snapshot configuration before you attempt to configure a new server, view the snapshot.

1. Expand Libraries in the Navigation pane and then select the current EC local library.
2. In the center pane, scroll down to the BIOS Configuration section of the library.
3. Select the snapshot and then select the View Snapshot icon.
4. You can apply the snapshot directly to a server or you can use a deployment plan.

### Apply a Service Processor Snapshot to a Server

1. Expand Assets in the Navigation pane and then select Servers.
2. Select the unconfigured server.
3. Click Update Service Processor in the Action pane. The following one-step wizard is displayed, including the list of snapshots in the EC local library that are appropriate for the selected server.

4. Select the snapshot from the list.
5. Click Next to review the Summary and then click Finish to submit the job.

When the service processor is configured, the server reboots.

#### **Apply a Service Processor Snapshot Profile to a Server**

1. Expand Plans in the Navigation pane and then select Profiles.
2. Expand Update BIOS Configuration and select the profile for the snapshot.
3. Review the profile in the center pane. To modify the profile, click the Edit Profile icon.
4. Create a plan that includes this profile as its only step or edit an existing deployment plan to include this profile.

## **Configuring a RAID Controller**

Oracle Enterprise Manager Ops Center provides a default profile for configuring RAID controllers. You can configure and update the hardware devices that can be done only through the host OS. This profile provisions a reduced OS image along with the management pack on the target to configure RAID.

---

---

**Caution:** When you reconfigure an existing RAID controller, all the data on the disk is lost.

---

---

## **Configuring a Dynamic System Domain**

You can create domains on a M-series server.

- Verify that a user account with `platadm` privilege exists on the XSCF processor and is included in the profile. Disable the audit policy for this user account, using the following command:

```
setaudit -a opsadm=disable
```

- Verify that you can use `ssh` to log into the XSCF processor.

To configure a Dynamic System Domain, you apply a deployment plan to an M-Series server, as described in [Chapter 8](#). The plan includes the profile for the Dynamic System Domain.

## **Configuring a Rack and Placing Components**

The rack asset is a group that includes the other managed assets installed in the physical rack, such as servers or compute nodes, storage arrays or appliances, switches, and power distribution units (PDU). After you create the rack, you put assets in the rack so that Oracle Enterprise Manager Ops Center can present them and manage them as if it were a physical asset.

#### **Creating a Rack**

1. Expand Assets in the Navigation pane and select Racks.
2. Click Create Rack in the Action pane.
3. Enter the name for the rack.

4. For a rack containing an Oracle Engineered System, specify the serial number of the rack.
5. Enter the total number of slots in the rack. A full rack has 42 slots. Default to 42.
6. You have the option to place assets into the rack immediately after this procedure ends or to perform this task at a later time.
7. Enter a description for this rack.
8. Add semantic tags that are appropriate for this rack.
9. Click Create Rack to submit the job.

Use the Place/Remove Assets in Rack action and the Place/Remove PDU in Rack action to specify each asset in the physical rack and its location in the rack so that Oracle Enterprise Manager Ops Center can represent the physical rack accurately to remote users.

### **Placing Assets in a Rack**

The rack asset is a group that includes the managed assets installed in the physical rack, such as servers or compute nodes, storage arrays or appliances, switches, and power distribution units (PDU).

Use the Place/Remove Assets in Rack action and the Place/Remove PDU in Rack action to specify each asset in the physical rack and its location in the rack so that Oracle Enterprise Manager Ops Center can represent the physical rack accurately to users who cannot examine the rack. Update the type and location of the assets in the rack asset when the configuration of the physical rack changes.

### **Placing a Power Distribution Unit in a Rack**

1. Expand Assets in the Navigation pane and select Racks from the Resource Management Views.
2. Select the rack.
3. Click Place/Remove Assets in Rack in the Actions pane or click the Details tab to navigate to the icon. The Place Assets in <name> Rack window opens. All managed assets in the physical rack are listed. You can filter the list by type or attribute.
4. Click an asset and then enter its slot number.
5. Click Place Asset in Rack button. The Assets in the Rack pane is updated to show the location.
6. Continue to select assets and place them in the rack.
7. To change an asset's slot, select it and click Edit Placement. Enter a new slot number.
8. To remove an asset, select it and click Remove Asset. The asset is deleted from the Assets in the Rack pane and is available to be placed.
9. When you are satisfied with the configuration displayed in the Assets in the Rack pane, click Submit.

To add PDUs to the rack asset, use the Place/Remove PDUs action in the same way. Select the rack and the action. The assets you have placed in the rack are shown in the Assets in Rack pane. Add each PDU.



## Hardware Monitoring

The Oracle Hardware Management Agents use Simple Network Management Protocol (SNMP) to monitor your Oracle hardware and storage devices. The software uses the Intelligent Platform Management Interface (IPMI) protocol to access the Oracle ILOM service processors.

A monitoring policy is a set of rules applied to an asset. If a status changes or a threshold is crossed, an alert is created. Oracle Enterprise Manager Ops Center provides default policies for each asset type. You can create new policies or modify existing policies.

### Hardware Status

If a hardware asset can report a value for a hardware variable, Oracle Enterprise Manager Ops Center reports its current state and compares it to the threshold value.

- Good – The hardware asset is working properly.
- Unknown – Oracle Enterprise Manager Ops Center is unable to retrieve information from the sensor. The hardware asset is connected but is not reporting information.
- Unreachable – The hardware asset cannot be contacted. This state indicates a network problem.
- Warning Failure – Oracle Enterprise Manager Ops Center has detected a potential or impending fault condition. Take action to prevent the problem.
- Critical Failure – A fault condition has occurred. Take corrective action.
- Nonrecoverable Failure – The hardware asset has failed. Recovery is not possible.
- Faulted – The hardware asset reports a fault. Contact service personnel to repair.

### Monitoring a Group of Hardware Assets

Oracle Enterprise Manager Ops Center monitors hardware assets according to the monitoring profile for that type of asset. To see the default profile for monitoring a hardware type, see [Hardware Monitoring](#).

To change a threshold value, see [Edit Monitoring Rules](#) in [Chapter 4](#).

### Connectivity Status

Connectivity is the network interface of the system. You can view information about a hardware asset's Network Interface Card (NIC).

### Service Processor Details

Use the Hardware tab to view information about each component of the system:

- Name and SNMP Community
- Whether Auto DNS through DHCP is in use, and any DNS Servers
- Search Path, if any
- Time Zone
- Whether an NTP server is in use and its identifier

## RAID Controller Details

- RAID volume name
- RAID level
- Number of disks
- Stripe zone
- RAID Controller ID

## Sun ZFS Storage Appliance Details

The Sun ZFS Storage Appliance support both file storage and application use.

The Dashboard tab reports the following hardware information:

- Name
- Description
- Current Alert Status
- Model
- Serial Number
- Management IP
- Memory
- Power
- Locator Light
- Appliance Kit Version
- Running Time
- Processor

The Hardware tab displays the appliance's firmware version and the following information for each component:

- CPU: Name, Model, Architecture, Speed, Manufacturer
- Memory: Name, Type, Size in bytes, Manufacturer, Part number, Serial number
- Network Adapters: Name or each, MAC Address, Description, Manufacturer, Part number, Serial number
- Disks: Name, Size in bytes, Manufacturer, Part number, Serial number
- Power Supply: Name, Manufacturer, Part number, Serial Number
- Fan Tray: Name, Manufacturer, Part number, Serial number

See [Discovering a Sun ZFS Storage Appliance](#) in [Chapter 2](#) for discovery requirements.

## Server Details

For server hardware, the Summary page displays:

- Name
- Description and Tags
- Current Alert Status

- Model
- Serial Number
- Management Interface IP
- MAC Address
- Processor
- Memory
- Power state
  - On – The server is powered on and running.
  - Standby – The server is powered off but responds to commands.
  - Unknown – An error occurred while attempting to retrieve the power status of the hardware. The server is connected but is not returning any information on power status.
  - Unreachable – The server cannot be contacted for information about its power state. This indicates a network problem or that the server is in standby mode.
- Locator Lights state
- Notification

Use the Hardware tab to view information about each component of the system:

- System: Description, type, and version of all firmware installed except for disk firmware. See the Disk tab for firmware version.
- CPU: Name, Model, Architecture, Speed, Manufacturer
- Memory: Name, Type, Size in bytes, Manufacturer, Part number, Serial number
- Network Adaptors: Name or each, MAC Address, Manufacturer, Part number, Serial Number
- Disks: Name of each, Model, Size in bytes, Slot ID, Node ID, Firmware Version, Manufacturer, Root Disk, RAID Disk
- Power Supply: Name, Manufacturer, Part number, Serial number
- Disk Controller: Name, Model Number, Firmware Version, BIOS Version, PCI Address, PCI Version ID
- Disk Expander: Name, Manufacturer, Version, Model Number, Firmware Version, Chassis ID
- Fan Tray: Name, Manufacturer, Part number, Serial number
- Fans: Name, Speed

## Chassis Details

For chassis hardware as a group, the Summary page shows:

- The five largest consumers of CPU
- The five largest consumers of memory
- The five largest consumers of the network

For chassis hardware, the Summary page displays:

- Group Name

- Description
- Location
- Type

## M-Series Details

The hardware resources in a SPARC Enterprise M-Series Server are divided into one or more logical units, called dynamic system domains. Oracle Enterprise Manager Ops Center can monitor each domain, in addition to the server hardware.

For an M-Series server, the Dashboard tab displays:

- Number of Dynamic System Domains it is supporting
- Model
- Product Serial Number
- Description
- Support contract
- XCP Firmware version
- OBP Firmware version
- XSCF Firmware version
- Operator Panel Switch Status: Locked
- Current Alert Status

The Summary tab adds details to the information in the Dashboard tab. For the Power status, the reported status is for the server's domains. When any domain is powered on, the status is reported as powered on. When all domains are powered off, the Summary tab shows a status of Powered Off; the M-Series server itself remains powered on.

- Name
- Model
- Product Serial Number
- Management IP
- MAC Address
- Current Alert Status
- Power
- Locator Light
- Notification
- All firmware versions
- For each domain: Name, Model, Health, Power, Locator Light, Notification

The Hardware tab shows the state of the server or, if a Dynamic System Domain is selected, the state of that domain. The Hardware tab reports the following:

- Model
- Serial Number
- State

- Power
- Locator Light
- Notification
- Operator Panel Switch State

At the System level, the hardware tab includes:

- The Unallocated Resources table lists all the physical system boards and their status: PSD ID, Assignment Status, Power Status, Connection Status, Diagnostics Status, and Operational Status
- The Allocated Resources table lists all domains that are using the physical system boards and their status: Domain ID, PSB ID, XSB ID, LSB ID, Assignment Status, Power Status, Connection Status, Diagnostics Status, and Operational Status
- The Dynamic System Domain table lists all the domains and their details: Domain ID, MAC Address, Autoboot Policy, Secure Mode Policy, CPU Mode, Diagnostics Level, Domain Degradation Policy, and Operational Status

You change the display to show information about each component of the system:

- CPU: Name, Architecture, Type, Manufacturer, Speed, Core Count, Thread Count, Serial Number, Part Number, Version, Status For Sensors: Name, Description, Type, Value
- Memory: Name, Type, Size in bytes, Serial number, Part number, Status For Sensors: Name, Description, Type, Value
- Board: Name, Serial number, Part number, Memory mirrored, Version, Status
- Power Supply: Name, Serial number, Part Number, Status For Sensors: Name, Description, Type, Value
- Board: Name, XSB Mode, Memory Mirrored, Serial Number, Part Number, Version, Status For Sensors: Name, Description, Type, Value
- IO Unit: Name, Serial Number, Part Number Version, Status For Sensors: Name, Description, Type, Value
- XSCF: Name, Host Name, Serial Number, Part Number, Version, Status
- Fan Tray: Name, Manufacturer, Part number, Serial number
- Fans: Name, Speed For Sensors: Name, Description, Type, Value

Oracle Enterprise Manager Ops Center monitors the voltage for the Board and IO Unit components and the speed for the Fan components. Click the Monitoring tab to see the actual value and the threshold values.

See [Discovering a M-Series Server](#) in [Chapter 2](#) for discovery requirements.

## Switch Details

Oracle Enterprise Manager Ops Center can manage Sun Ethernet 10GbE Fabric switches and Sun Datacenter InfiniBand switches. These switches reside in the system or blade system and provide the switch fabric.

For more information about these switches, see the product documentation:

- For the Sun Ethernet 10GbE Fabric switch, see <http://docs.oracle.com/cd/E19934-01/index.html>

- For Sun Datacenter InfiniBand switch, see <http://docs.oracle.com/cd/E19654-01/index.html>

Oracle Enterprise Manager Ops Center reports hardware information on the Summary tab:

- Name
- Model
- Port count
- Serial number
- Management Interface IP
- MAC Address
- Fabric Manager: true or false
- Fabric Manager Address
- Power state
- Locator lights state
- Notification state
- Current Alert Status
- Firmware types and versions

At the System level, the Hardware tab includes:

- Model
- Server Name
- Serial Number
- State
- Power
- Firmware versions
- Sensors: temperature and voltage

You change the display to show information about each component of the switch:

- Network Adaptors: Name or each, MAC Address, IP Address, Description
- Power Supply: Name, Manufacturer, Part number, Serial Number For Sensors: Description, Type, Status
- Fan Sensors: Description, Type, Value, Status, Warning Threshold (Lower), Warning Threshold (Upper), Critical Threshold (Lower), Critical Threshold (Upper), Non-Recoverable Threshold (Lower), Non-Recoverable Threshold (Upper)

## Rack Details

The rack's Dashboard displays the following information:

- Name
- Rack ID
- Description

- Number of Slots
- Tags
- Support

The Details tab shows the configuration of each slot in the rack. For each component in the rack, this tab displays the position, name, description, type, model and health status. The Power Distribution Units are included and their current status is displayed.

The Firmware tab displays the name, description, and version of the firmware for each component and the slot for each component:

- Compute Nodes
- Switches
- Storage Appliances
- Power Distribution Units

The rack's Charts tab displays the following plots, as described in [Charts Tab](#):

- Aggregate Power Usage
- Power Usage
- Average Fan Speed

The rack's Energy tab displays the information described in [Energy Tab](#)

## PDU Details

The Dashboard tab shows:

- Name, description
- Model and serial number
- Management IP address and MAC address, if any

The Details tab reports the same information and adds whether SNMP and HTTP is enabled and the version of the firmware.

## Oracle Solaris Cluster Details

The Dashboard tab shows:

- Name, description, and ID
- Number of possible quorum votes and the current quorum votes

The Network tab shows the public and private interconnects used by the cluster.

The Quorum tab shows the status of each member of the quorum and the number of quorum votes for each member.

## Oracle Exalogic Details

Oracle Enterprise Manager Ops Center supports bare metal provisioning, discovery of hardware assets, and firmware upgrade for the hardware components of an Exalogic machine. The Oracle Exalogic architecture includes InfiniBand and Ethernet switches and the Sun ZFS Storage 7320 Appliance. Using Oracle Enterprise Manager Ops Center, you can manage these components individually and as a group, as well as get access to the browser user interface to the storage appliance and serial console access to the compute nodes and switches.

For detailed information about how to use Oracle Enterprise Manager Ops Center with Oracle Exalogic, see the Oracle Exalogic documentation:  
[http://docs.oracle.com/cd/E18476\\_01/doc.220/e18478/toc.htm](http://docs.oracle.com/cd/E18476_01/doc.220/e18478/toc.htm)

## Monitoring Power Utilization

Input power is the power pulled into a power supply from an external resource. The power consumption of a hardware asset is the sum of the input power consumed by each power supply of the asset. Output power is the amount of power provided from the power supply to the system components, measured at the power supply output. Input power is calculated from output power by applying an efficiency function to the output power from each power supply.

Calculating power compensation for the blades is difficult because the power supplies are shared. Each blade gives a report based on the power consumption of the local components, but this is not an accurate power consumption value for an individual blade.

To measure the input power, the interfaces must be exposed and the service processors must be able to retrieve and report data with one-minute accuracy. Servers that can report power usage have a Charts tab. Use the following procedure to check whether any hardware asset can report its power utilization.

You can see current power usage and change the display of power graphs using the controls on the Energy tab and the Charts tab.

## Energy Tab

The asset's Energy tab reports power consumption as the current value and for a period of time, as well as attributes of the fan and power supplies. The current values are reported for the following attributes:

- Wattage
- System Load for an OS
- Utilization Per Cent for an Oracle VM Server for SPARC
- Incoming air temperature and outgoing air temperature
- Power Policy
- Cost Per KiloWatt-hour
- Currency units used to compute cost. The price per currency unit is set by the Edit Energy Cost action in the Administration section of the Navigation pane. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information.
- Total Power Cost for one day

The data over time is represented in the following graphs:

- Power Consumption and Utilization: By default, the graph shows the power consumed in the last day in watts. If the server is shut down, the graph shows any existing historical data.
- Temperature and Fan Speed: By default, the graph shows the incoming air temperature and the outgoing air temperature in Fahrenheit, and the average fan speed in RPM. Click on any point on the graph to see that data for that point in time.



By default, the graphs are in Live mode, which reports new information every five seconds. Click the Live button in the graph's toolbar to make the information static so that you can set the period of the graphs to one of the following:

- One hour (1H) – One point for every five minutes
- One day (1D) – One point for every five minutes
- Five days (5D) – One point for every five minutes
- Three weeks (3W) – One point every hour
- Six weeks (6W) – One point every 12 hours
- Six months (6M) – One point for every day

To make a graph with the minimum of two points, a hardware asset must have been managed for at least 10 minutes to view a one-hour graph and for at least two days to view the six-months graph.

The data for these time periods is stored separately. For example, if a server has been managed for two hours and you select the 6W view, the graph cannot be displayed because only one point of data of that type has been stored; the second point has not yet occurred. If you then select the 1D view, the graph can display 24 points of data (120 minutes at 5-minute intervals). However, the graph displays these points over a 24-hour period and not over the actual two-hour period. For the most accurate representation of the data, choose a time period that is less than or equal to the time that the hardware asset has been managed.

You can export the data for either the current view or all available data to a file in either CSV or XML format. Use the Export Chart Data toolbar icon to choose options for exporting the data.

If the graph is blank, one of the following conditions has occurred:

- The server does not have the appropriate ILOM version.
- The server has not been discovered through the ILOM driver.
- The server is unreachable.

## Charts Tab

The Chart tab provides more ways to display the power utilization data. You can change the graphed data to a bar chart or an area chart. You can also export the data for either the current view or all available data to a file in either CSV or XML format. Use the Export Chart Data button to choose options for exporting the data.

For groups and virtual pools, the following options are available:

- Select Order: The five highest or five lowest historical power utilization.
- Select Resource: Select the Power or Aggregate Power option for a homogeneous or heterogeneous group of servers.
  - The Power option displays power utilization for the five highest or lowest power consumers in the group or virtual pool.
  - The Aggregate Power option displays the power utilization, using the sum of all members that report power consumption. The number of systems in the aggregate is included. For heterogeneous group, the Chart tab includes a table of all systems in the group and their various power attributes for the selected time period. From this table, you can power off and power on selected servers to conserve power.

## Maintaining Hardware Assets

- Update management credentials. See [Updating Management Credentials in Chapter 2](#)
- Set power policy
- Power systems on and off
- Place in maintenance mode
- Reset a server
- Get access to the serial console
- Enable and disable ports
- Use locator lights to identify a specific asset
- Check firmware compliance and update firmware. See [Firmware Provisioning](#)

## Setting and Changing the Power Policy

An asset's use of power can be optimized for performance or for conservation:

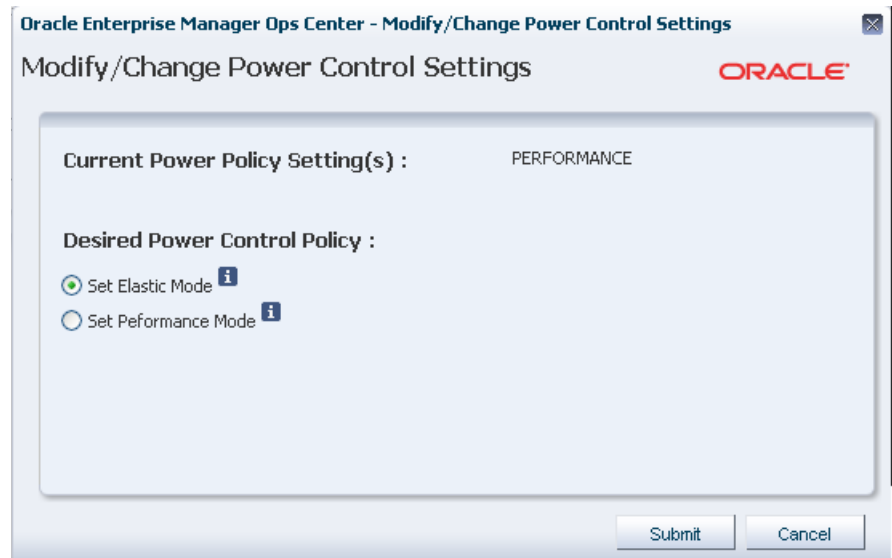
- Performance - Disable CPU power management to use of more power.
- Elastic - Enable CPU power management to conserve power.

### View an Asset's Power Policy

1. Expand the Assets in the Navigation pane.
2. Select a hardware asset.
3. Click the Energy tab in the center pane.

### Changing an Asset's Power Policy

1. Expand the Assets in the Navigation pane.
2. Select a hardware asset.
3. Click Set Power Policy in the center pane.

**Figure 11–7 Set Power Policy**

4. The current power policy is displayed. Choose the alternative policy.
5. Click Submit to create a job that sets the power policy.

## Replacing a Failed Power Distribution Unit in a Rack

1. Expand Assets in the Navigation pane and then expand Racks.
2. Navigate to the rack type and expand to show its components. Expand Power Distribution Units.
3. Select the failed power distribution unit.
4. Click Place in Maintenance Mode in the Action pane.
5. Go to the rack's location and remove the failed PDU.

Install the new PDU and connect it to the network, according to the procedures in the [Power Distribution Units User's Guide](#).

6. Verify that the new PDU has the same IP address as the failed PDU.
7. Use the PDU's web interface to configure the administrator user account, according to the procedure in the [Power Distribution Units User's Guide](#).
8. Return to the Oracle Enterprise Manager Ops Center user interface and navigate to the same rack and the new PDU. Select the PDU.
9. Click Remove From Maintenance Mode in the Action pane.
10. To update the credentials for the administrator user, click Update Management Credentials in the Action pane. The wizard opens.
11. On Management Type step, select HTTP credentials and then select the Create a new set of credentials option. Click Next.
12. Enter new credentials for the administrator user.
13. Click Apply to update credentials.
14. To create new SNMP credentials, click Update Management Credentials in the Actions pane again.

15. Select SNMP credentials and Create a new set of credentials.  
Specify a community string that is different than the previous community string.
16. Press Apply to update credentials.

## Installing and Upgrading Oracle Solaris Cluster

You use cluster profiles in a deployment plan to perform the following operations:

- Install Oracle Solaris Cluster software
- Upgrade Oracle Solaris Cluster software

See [Appendix B](#) for instructions on obtaining the current profiles and supporting scripts.

## Firmware Provisioning

The Oracle Enterprise Manager Ops Center provisioning feature installs firmware on the managed hardware assets. You initiate the installations from the UI, rather than from the asset itself.

Oracle Enterprise Manager Ops Center provides default profiles for configuring firmware for servers and for disk storage. An alternate procedure is to create a Firmware Report. You then use the report results to update the firmware.

The benefit of using a profile to install firmware is that the firmware is installed consistently, no matter how many assets you provision. The benefit of using the Firmware Compliance Report is to identify the firmware on a specific asset or set of assets.

## Firmware Profiles

The general procedure for provisioning firmware has the following steps:

1. Import a file with the firmware and the associated metadata into a software library, according to the procedure in Keeping Your Firmware Up-to-Date in the [How To library](#).
2. Create a firmware profile, based on one or more firmware images, according to the procedures in Keeping Your Firmware Up-to-Date in the [How To library](#).
3. Shut down the server gracefully. Most firmware requires that the server is not running when the firmware is updated. Most firmware images include a power-off command for a running server, which causes a hard shutdown of the server.
4. Apply the firmware profile.

## Firmware Compliance Reports

The Firmware Report feature compares the firmware images specified in a firmware profile to the firmware images installed on one or more hardware assets. You have the option of updating the firmware on any non-compliant assets by clicking the Make Targets Compliant button in the Interactive report.

The report shows whether a target asset is compliant, not compliant, or not applicable:

- A compliant asset has the firmware images specified in the profile.

- A non-compliant asset does not have the same firmware images as specified in the profile. Update the firmware by either clicking the Make Targets Compliant button in the Interactive report or using the procedure in [Updating Firmware](#).
- A non-applicable asset indicates that a firmware image in the profile does not match the model of service processor in the asset. This condition can occur when either the profile does not recognize the model of the service processor or the profile includes firmware images that are not designed for the service processor.
  1. Compare the model of the service processor displayed in the asset's Summary tab with the model of the service processor included in the profile. If they are different, add the name in the profile to the asset's data.
  2. When the firmware profile was created, only images that matched the service processor could be included. However, if the service processor did not report all the firmware types it supported, an image that did not match the service processor could have been included in the profile. To update the Oracle Enterprise Manager Ops Center software with all the service processor's supported firmware types, use the Refresh action. When the job is completed, view the service processor's Summary tab to see all firmware types.
  3. Create a new firmware compliance report.

See [Firmware Reports](#) for the procedure to create the report.

## Updating Firmware

To update the firmware on one or many assets, you apply a firmware profile for the type of asset. For a server, the profile updates the firmware on a service processor. For storage components, profiles update firmware on a RAID controller, an expander, or disk. You apply the firmware profile through a deployment plan.

To see the deployment plans that update firmware, expand the Deployment Plans section of the Navigation pane and then click Firmware. A list of existing plans is displayed. In addition, a plan and profile is created for each firmware image when the image is imported into a software library.

When you are updating the firmware of one asset, an alternative to a deployment plan is to use the Update Firmware action. Select the asset from the Asset section of the Navigation pane and then click Update Firmware in the Actions pane.

### Before You Begin

The software library must contain the images that provision the firmware. Perform the Uploading a Firmware Image procedure in the Keeping Your Firmware Up-to-Date document in the [How To library](#).

If you are updating the firmware on a server, shut down the server before you update the firmware. A firmware update to a server's service processor usually requires that the server is not running. If you start to update the firmware on a running server's service processor, the firmware image performs a hard shutdown of the server.

The firmware provisioning process for M-Series servers and servers that have ALOM service processors relies on a temporary account that performs an FTP operation. If your site does not allow this type of account, use the following procedure to prepare for the provisioning operation:

1. On the Enterprise Controller, open the `/var/opt/sun/xvm/hal.properties` in an editor.
2. Add the following properties to the file:

```
ftp.user.name=username  
ftp.user.password=password
```

3. Restrict access to the file to root user:

```
chmod 600 /var/opt/sun/xvm/hal.properties
```

4. On the Proxy Controller that provisions the firmware, enable the FTP service on Oracle Solaris or the vsftpd service for Oracle Linux systems.

You can now apply the firmware provisioning deployment plan. The FTP operation retrieves the credentials from the file.

---

---

**Note:** Advanced Lights Out Management (ALOM) is a Sun Microsystems standard for these systems: SunFire V125/V210/V215/V240/V245/V250/V440/T1000 and Sun Netra 210/240/440.

---

---

If a network failure occurs while updating the firmware, repeat the firmware update procedure. If you do not repeat the procedure, the firmware inventory list might be incomplete.

#### **Post-Provisioning Tasks for Exalogic Compute Nodes**

When the ILOM firmware on an Exalogic compute node is upgraded or downgraded, the BIOS setting for SR-IOV is reset to the default value, disabled. You must set the SR-IOV value again manually. In the BIOS, select Advanced, then I/O Virtualization, and then SR-IOV Supported. Edit the value to change it to enabled

## **Related Resources for Hardware Management**

For instructions in performing actions or to learn more about the role of this feature, go to one of the following resources.

- Configuring and Managing Software Libraries on the Enterprise Controller Guide in the [How To library](#)
- For the Sun Ethernet 10GbE Fabric switch, see <http://docs.oracle.com/cd/E19934-01/index.html>
- For Sun Datacenter InfiniBand switch, see <http://docs.oracle.com/cd/E19654-01/index.html>
- [Power Distribution Units User's Guide](#)

---

---

## Operating Systems

This chapter provides an overview of the operating system (OS) management features that are available in Oracle Enterprise Manager Ops Center.

The following information is included:

- [Introduction to Operating Systems](#)
- [Roles for Operating Systems](#)
- [Actions for Operating Systems](#)
- [Location of Operating System Information in the User Interface](#)
- [Operating System Profiles](#)
- [Agent-Managed and Agentlessly-Managed Operating Systems](#)
- [Monitoring Operating Systems](#)
- [Analytics](#)
- [Provisioning Operating Systems](#)
- [Oracle Solaris Boot Environments](#)
- [Oracle Solaris 11 Boot Environments](#)
- [Oracle Solaris 10 and Earlier Boot Environments](#)
- [Related Resources](#)

See [Chapter 13, "Operating System Updates"](#) for information about patching and updating your operating systems.

### Introduction to Operating Systems

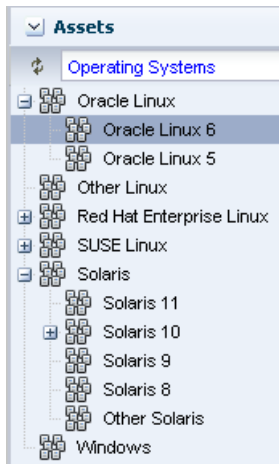
Oracle Enterprise Manager Ops Center provides comprehensive lifecycle management for Oracle Solaris, Oracle Linux, SUSE Linux, Red Hat Linux, and Microsoft Windows operating systems in your datacenter.

The discovery feature makes adding operating systems and other assets quick and easy. After the operating systems are added, they are considered managed and you can begin using the monitoring, analytics, OS provisioning, and update features to gather information and perform tasks.

Your managed operating systems are visible in the All Assets section of the user interface. The operating system appears under the service processor and hardware, as shown in [Figure 12-1](#).

**Figure 12–1 Managed System and Operating System**

The OS is also added to the appropriate platform-specific group in the Operating Systems view, as shown in [Figure 12–2](#).

**Figure 12–2 Operating Systems View**

You can create user-defined groups and subgroups to refine your administration tasks. For example, you might want to create groups for Critical Systems, Training, Region 1 and Region 2. This is useful when you want to organize the systems to apply different monitoring standards, implement update requirements, or job scheduling times. You can create rules for your groups to automatically add existing and newly managed operating systems to the correct group or subgroup. See [Chapter 2, "Asset Management"](#) for details on using the discovery feature to add assets and for more information on creating user-defined groups.

The monitoring feature provides extensive monitoring capabilities that are enabled as soon as you begin managing an operating system. A series of three escalating status levels notifies you when something is not operating as expected. The first level is informational, then warning, and finally a critical status. A set of default monitoring attributes and alert triggers are included with the software. You can tune the monitoring thresholds and triggers to define what you want to generate an alert and when. You can create custom monitoring rule sets and alert parameters and apply the customized monitoring rules to a specific operating system, a group of homogeneous operating systems, or a group that you define, such as critical systems or regional systems.

The Analytics feature provides extensive information about a specific operating system in one location so that you can maximize performance and utilization. The Analytics information includes process details, defined monitoring thresholds for operating systems, metrics and historical information on the top consumers, and an extensive list of metrics data. The Summary contains details on the top five consumers for CPU, memory, network, and I/O utilization. Use the graphical representation to quickly view utilization trends and high resource consumers. You can drill down to get detailed utilization and process information, and kill a process that is consuming too many resources.

The following features are available for operating systems:



- Monitoring – A series of monitoring rules and parameters monitor your managed assets. Alerts and incidents are raised for components that are not performing as expected.
- Performance – Analytics provides you with a detailed view into OS performance.
  - System resource graphs, processes information, and a view of the top consumers
  - Resource usage of virtualized OS instances
- Provisioning – Install Oracle Solaris or Linux operating systems onto your systems, making it easy to install one system or many servers simultaneously.
- Manage Oracle Solaris Boot Environments – Create and manage Oracle Solaris boot environments in a repeatable and consistent manner from a single user console.
- OS Updates – Apply update packages to keep your operating systems up-to-date. See [Chapter 13, "Operating System Updates"](#) for information.
- Reports and Snapshots – A variety of reports are available for your operating systems. See [Chapter 10, "Reports"](#) for OS reports. See [Chapter 13, "Operating System Updates"](#) for information on how to use the System Catalogs to maintain snapshots of your operating system.

Two types of OS management are available: agent managed and agentlessly managed. In some cases, the features and actions that you can perform on an operating system are determined by how the OS is managed.

## Roles for Operating Systems

[Table 12-1](#) lists the tasks that are discussed in this section and the role required to complete the task. An administrator with the appropriate role can restrict privileges to specific targets or groups of targets. Contact your administrator if you do not have the necessary role or privilege to complete a task. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 12-1 OS Management Roles and Permissions**

Task	Role
Reboot an OS	Asset Admin
Charts and Utilization	Asset Admin Cloud Admin
Analytics	Read Asset Admin
Kill action in Analytics	Operating System Management
Update Management Credentials	Security Admin
Any Actions related to changing credentials	Security Admin
Import image	Storage Admin
Upload image	Storage Admin
Unconfigure, SCCM Configuration	Oracle Enterprise Manager Ops Center Admin

**Table 12–1 (Cont.) OS Management Roles and Permissions**

<b>Task</b>	<b>Role</b>
Reboot, upgrade Agent Controller	Asset Admin
Edit Tags	Asset Admin
Edit Attributes	Asset Admin
View Boot Environment	Read Asset Admin Update Admin
Create Boot Environment	Asset Admin Update Admin
Update an Alternate Boot Environment	Update Admin
Activate and Reboot a Boot Environment	Asset Admin Update Admin
Synchronize Boot Environments	Asset Admin Update Admin
Delete an Alternate Boot Environment	Asset Admin Update Admin
Monitor Boot Environment Attributes	Asset Admin

## Actions for Operating Systems

You can manage an operating system in one of two modes: agent managed or agentless managed. The management mode determines the features that are enabled for your operating system.

The more robust management mode is agent managed because the Agent enables a greater level of communication with the Proxy Controller and Enterprise Controller than the agentless managed operating systems. You can use the features and perform the actions described in this chapter with an agentless managed operating system, but OS update functionality requires an agent managed operating system. You can manage your operating systems by installing an Agent Controller on the OS or by using SSH to perform tasks. See [Agent-Managed and Agentlessly-Managed Operating Systems](#) for more details.

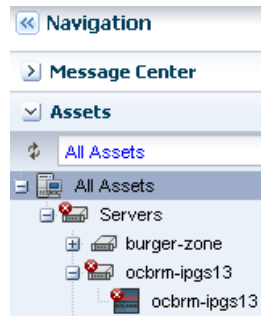
See [Chapter 2, "Asset Management"](#) for details on using the discovery feature to add assets and for more information on creating user-defined groups.

After you manage your assets, you can perform the following actions:

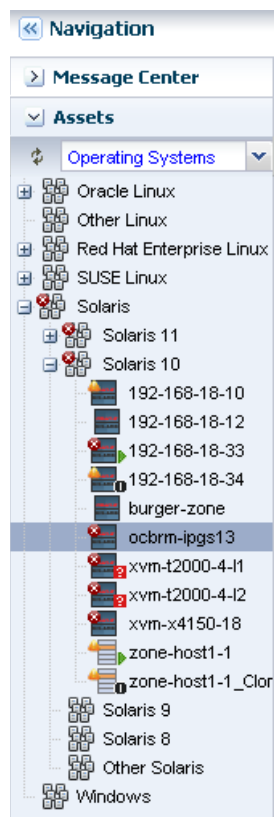
- Monitor your physical and virtual operating systems
- View OS utilization for Oracle Solaris and Linux operating systems
- Provision Oracle Solaris and Linux operating systems
- Manage Oracle Solaris boot environments

## Location of Operating System Information in the User Interface

When you manage a physical or virtual operating system, it appears under the associated server in the All Assets view, as shown in [Figure 12–3](#) and it appears in a special pre-defined operating system group, as shown in [Figure 12–4](#).

**Figure 12–3 All Assets View**

Operating systems are automatically added to a homogenous group of operating systems. The group contains directories for each release. In [Figure 12–4](#), the list of Oracle Solaris 10 operating systems includes physical operating systems, virtual hosts, and zones. You can add user-defined groups and create rules to automatically add newly discovered assets to that group, or you can manually add them at any time. See [Using Groups](#) for details.

**Figure 12–4 Operating Systems View**

To view information about a specific OS, select the OS from the Assets pane. OS details appear in the tabs across the center pane.

**Table 12–2 Location of Operating System Information in the UI**

<b>To Display:</b>	<b>Select:</b>
Managed operating systems	Expand the Assets pane. Each operating system appears in the Assets tree under the system on which it is installed. To only view operating systems, click the drop-down next to All Assets and select Operating Systems. The systems are grouped by platform.
Operating system details for a specific operating system	Select an operating system in the Assets pane, then click the Summary tab.
Operating system details for a group of operating systems	Select an operating system in the Assets pane, then click the drop-down next to All Assets and select Operating Systems. Select a group, then click the Summary tab.
Unresolved incidents and alerts for a specific operating system	Select an operating system in the Assets pane, then click the Incidents tab. The details are in the Unresolved Incidents and Alert subtabs.
Unresolved incidents and alerts for a group of operating systems	Expand the Assets pane, then click the drop-down next to All Assets and select Operating Systems. Select a group, then click the Incidents tab. The details are in the Unresolved Incidents and Alert subtabs.
Monitoring Rules for a specific operating system	Select an operating system in the Assets pane, then click the Monitoring tab.
Monitoring Rules for a group of operating systems	Select an operating system in the Assets pane, then click the drop-down next to All Assets and select Operating Systems. Select a group, then click the Monitoring tab.
Analytics	Select an operating system in the Assets pane, then click the Analytics tab.
OS Provisioning	Select a Provision OS plan in Plan Management.
Boot environments	Select an operating system in the Assets pane, then click the Boot Environments tab.

## Operating System Profiles

The following categories of OS Management profiles are available:

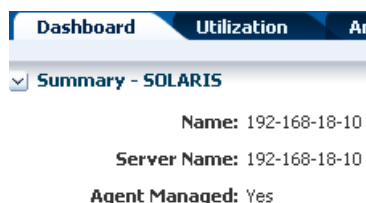
- OS Provisioning
- Monitoring Profile
- Oracle Solaris Zone
- Boot Environments

## Agent-Managed and Agentlessly-Managed Operating Systems

Two management modes are available, agent-managed and agentlessly-managed. An agent managed operating system has an Agent Controller installed to gather information for the Enterprise Controller and is required for some OS-specific features. When you do not want an Agent Controller installed, you can agentlessly manage your operating systems. To gather information on an agentlessly managed operating system, the Proxy Controller uses SSH to perform certain tasks and periodically check on the operating system.

The current management mode of an operating system appears on the Dashboard for the operating system, as shown in [Figure 12-5](#) and [Figure 12-6](#).

**Figure 12-5 Agent Managed**



When you install the Agent Controller on the operating system, the following actions occur:

- The Agent Controller is registered with the Enterprise Controller. It takes at least five (5) minutes for the software to register the Agent Controller. After registered, you can update the operating system.
- The software sends you a notification when it has enabled the update function for the operating system.
- The Agent Controller checks the inventory of patches and packages and creates the System Catalog. The catalog lists the patches and packages, and the versions that are currently installed on the operating system.

Some features are not available when the operating system is managed agentlessly. [Table 12-3](#) shows the information that are available for each management type.

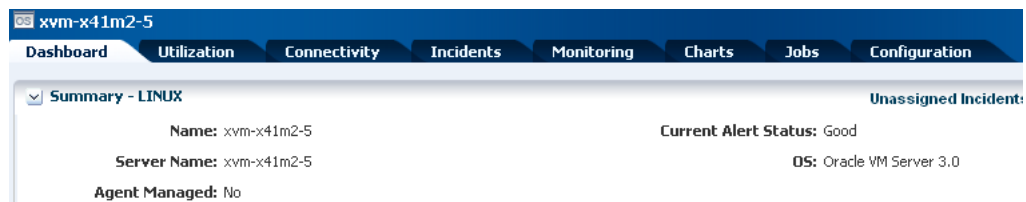
**Table 12-3 Information Available for Agent Managed and Agentlessly Managed Assets**

Tab or Feature	Agent Managed	Agentlessly Managed
Dashboard	Yes	Yes
Summary	Yes	Yes
Libraries	Yes	No
Storage	Yes	No
Utilization	Yes	Yes
Analytics	Yes	Limited
Virtualization Analytics for Oracle VM Server	Yes, if the guest is agent-managed	No
Virtualization Analytics for Oracle Solaris 10 Zones	Yes, if the global zone is agent-managed or if the non-global zone is agent-managed.	No
Networks	Yes	No
Incidents	Yes	Yes
Monitoring	Yes	Yes
Charts	Yes	Yes
Reports	Yes	No

See [Chapter 10, "Reports"](#)

**Table 12–3 (Cont.) Information Available for Agent Managed and Agentlessly Managed**

Tab or Feature	Agent Managed	Agentlessly Managed
System Catalogs	Yes	Oracle Solaris 11 – Yes Oracle Solaris 8-10, Linux, Windows – No
Terminal	Yes	No
Jobs	Yes	Yes
Configuration	Yes	Yes
OS update	Yes	Oracle Solaris 11, Windows – Yes Oracle Solaris 8-10, Linux – No
OS provisioning	Yes	No
Zone management, including create, read, update, and delete zones	Yes	No

**Figure 12–6 Agentlessly Managed**

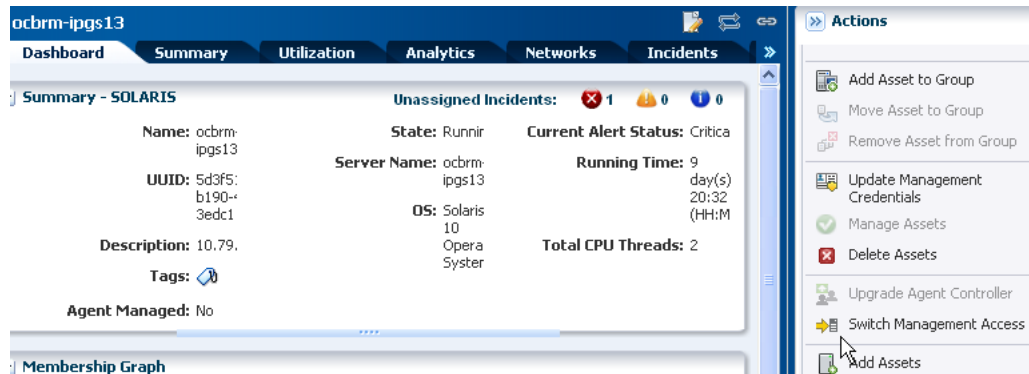
You can change the agent management mode:

- Unmanage the agent, then rediscover the operating system using a profile with the alternative mode.
- Use the Switch Management Access feature.

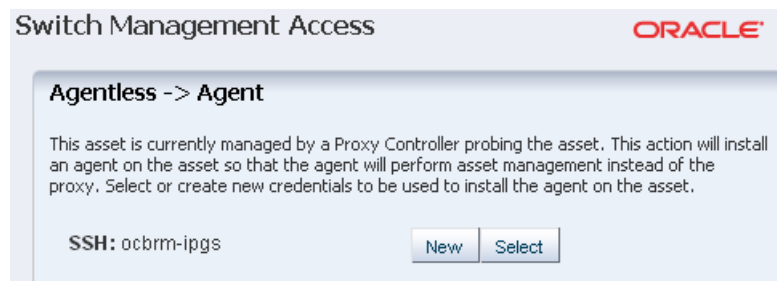
The Switch Management feature enables you to move back and forth from agentlessly managed to agent managed. When the operating system is agent managed and you use this action, the agent is removed and the operating system is managed agentlessly. Select or create new credentials for the Proxy Controller to use to obtain information from the asset.

#### To Use Switch Management Access

1. Select the operating system from the Assets drawer. You can view the current management status in the Dashboard tab.
2. Click Switch Management Access in the Actions pane.

**Figure 12–7 Switch Management Access**

3. Add or select the credentials for the system, then click Finish.
  - To create a new set of credentials, click New and complete the Create Credentials wizard, then click OK.
  - To select from a list of existing credentials, click Select, highlight the credentials from the list of available credentials, then click OK.

**Figure 12–8 Switch Management Access Credentials**

## Monitoring Operating Systems

The software monitors the status of your operating systems as soon as the asset is managed, using the default rules and thresholds. Monitoring rules state the values and boundaries for an asset's activity. A monitoring policy is a set of rules. You can change the rules or thresholds to adjust the type and level of monitoring you want. Analytics provides details on operating system activity and utilization.

A monitoring policy defines alert configurations to be performed on one or more managed resources. A policy is for a specific type of resource, such as operating systems. A more specific policy might apply to all Oracle Solaris operating systems. Each monitoring policy contains several alert monitors for a specific type of resource. Alert monitors watch the state of managed resources and their attributes and raise an alert when the state is outside the pre-defined thresholds.

Applying a monitoring policy to all the assets enforces consistency. Each monitoring policy contains rules for threshold levels. Default policies for monitoring hardware, operating systems, and Oracle Solaris Clusters are included in the software. You can use the default policies, but you cannot edit them. To edit or add monitoring rules to a monitoring policy, you must make a copy. Modifying a monitoring rule for a specific asset creates a custom set of monitoring rules for the asset.

See [Chapter 4, "Monitoring Rules and Policies"](#) for information about how to change the threshold limits and how to change the deactivate or activate the auto delete

policy. See [Chapter 9, "Incidents"](#) for details about how incidents are generated, severity badges, how to assign and close an incident.

## Analytics

The Analytics feature provides a view into operating system performance and status. The charts, reports, and utilization data provide details of an individual eligible OS. You can use the information to analyze the behavior of an OS to aid in peak performance and to diagnose and correct incidents.

The OS Analytics view provides information for the following agent-managed platforms:

- Linux
- Oracle Solaris 11 and 10 OS
- Oracle Solaris 10 non-global zone, when the global zone or non-global zone is agent-managed
- Oracle Solaris 11 non-global zone, when the global zone is agent-managed

When your operating system is agentlessly-managed, information is not available for zones and less information is available for Linux and Oracle Solaris 10 and 11 operating systems. [Table 12-4](#) shows a list of features and whether the feature is supported on an agent managed or agentlessly managed asset.

**Table 12-4 Supported Analytics Information**

Feature	Supported on Agent Managed OS	Supported on an Agentlessly Managed OS
Summary	Yes	Yes
Virtualization Analytics for Oracle VM Server	Yes, if the guest is agent-managed	No
Virtualization Analytics for Oracle Solaris 10 Zones	Yes, if the global zone is agent-managed or if the non-global zone is agent-managed.	No
Services	Yes	Yes
Processes	Yes, if the guest, global zone, or non-global zone is agent-managed	No
Threshold	Yes	Yes
History	Yes, if the guest, global zone, or non-global zone is agent-managed	No
Metrics	Yes	Yes

The current management mode appears in the Dashboard Summary page for the operating system. See [Agent-Managed and Agentlessly-Managed Operating Systems](#) for details and for the steps to switch the management mode.

## Displaying Analytics Information

For each operating system, the information appears in the Analytics tab in the center pane. The information appears in several views.



---



---

**Note:** Monitoring uses the Agent Controller to gather information. When an operating system is an agentless managed system or Microsoft Windows, the software uses an SSH connection from a Proxy Controller to perform remote monitoring. Remote monitoring over an SSH connection limits the available metric information. The Summary view, Process view, Historical view and Virtualization Analytics are not available for these operating systems.

---



---

The following sections discuss the diagnostic pages for an agent-managed operating system:

- Analytics view
  - System resource graphs
  - Top-consumers views
  - Processes information
  - View historical data and set thresholds
- Virtualization Analytics view
  - Virtualized OS instance
  - Breakdown of resource usage of the physical server
  - Running OS instance
  - View historical data and set thresholds

## Analytics Views

The Analytics view contains current and historical information about an operating system's use of resources, including CPU, Network, disk I/O, memory, alert history, and total thread and process counts. Information presented in this section assumes that the operating system is agent managed. See [Table 12-4](#) for the list of supported features for an agentlessly managed OS.

The information appears in a series of charts in the following subtabs:

- Summary – View a high-level overview of the top consumers, by process, for the CPU, memory, network, and disk I/O resources
- Processes – View process-specific details
- Services – View and monitor Oracle Solaris 10 and 11 SMF services
- Thresholds – View and edit the threshold limits for a selected monitored attribute
- History – View a history for the top consumers
- Metrics – View specific details an operating system element, such as the percentage of memory used
- Charts – You can create a variety of utilization charts, define the coordinates, and export the chart data to CSV or XML output

You can view analytics information for all supported and managed operating systems, both physical and virtual. The information presented varies, depending on the data available for the OS. For example, when the System Tap is not installed on a Linux operating system, information about the top network and I/O consumers might not be

available. Also, the top consumers for I/O data might not be available with some versions of the Linux kernel.

When an agent-managed operating system is on a virtualization platform, you can view the information in the Analytics view of the virtualization platform. See [Virtualization Analytics View](#) for information about analytics for virtualized platforms.

### Customize the View

The default display is the resource usage data. You can change the display settings for each view and choose which system resource graphs and details to display. The changes made on a given analytics screen affects the views of all analytics screens for the same OS or virtualized OS.

To change the analytics information displayed on the page, click the Settings Menu icon in the center pane.

### Analytics Summary View

The Summary view provides details for an individual operating system. The Summary provides a graphical representation and a list of the top five (5) resource usage consumers, by process, for the CPU, memory, network, and disk I/O resources. The following details appear in the Summary view:

- CPU Utilization – A graph of the percentage of CPU Utilization over time and a detailed list of the top five (5) CPU processes. The list includes the process identification number (PID), name, and CPU Usage %. Click the View icon for a row to display process details.
- Memory Utilization – A graph of the top 5 memory processes, including the PID, the process name, and the percentage of memory used.
- Network Utilization– A graph of the top 5 network processes, including the PID, the process name, and the network usage in Kilobytes (KB) per second.
- I/O Utilization– A graph of the top 5 I/O processes, including the PID, the process name, and the I/O usage per second.

The information is refreshed every five (5) seconds. Each list has an icon before the PID column for each process. Click an icon to view details of the process. The type of resource determines the available details.

- Process Details – Includes the contract ID, Service FMRI, creator, elapsed time, project name, project ID, and a process tree.
- Thread Information – Includes the thread's light-weight process (LWP) ID, the number of threads (NLWP), the user, the priority, the state (such as sleeping), the percentage of CPU used, the CPU time, the percentage of memory used, how much memory the process has marked for allocation (VSZ memory), the processors, and the command.
- Handles – Includes the port details, such as the family, local address, local port, the protocol, remote address, remote port, device, and node.
- Process Environment – Includes details about the environment, such as the arguments, data model, and flags.
- Memory Information – Includes physical, virtual, and anonymous memory and dirty page details. Details include the virtual address and the number of KB in the virtual mapping size, the resident physical memory, the anonymous memory, and

the dirty pages. The lock status, permissions, and mapping name details are displayed, when available.

### CPU Utilization Details

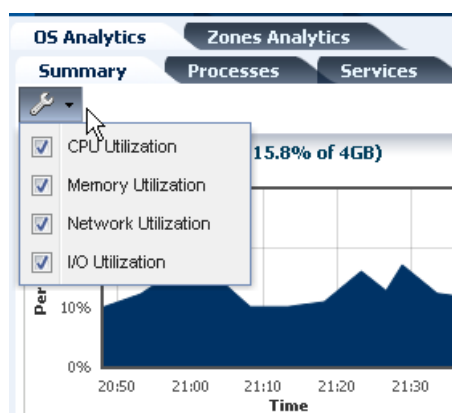
Process Details, Thread Information, Handles (port bindings and file descriptors), Process Environment, and Memory Information.

### Configure Graphs

When the icon that looks like a wrench appears on a page with graphs, you can click the icon to configure the graphs or change the graphs that appear on the page.

Figure 12–9 shows an example where you can choose the system resource graphs that display on the Summary page.

**Figure 12–9** Configure Graphs Menu



### Processes View

You can drill down to display process-specific data, based on current data from the operating system. Some data, such as CPU usage, might also be available in the History view.

The following details are available in the Process view:

- Process ID (PID)
- Process Name
- User
- State
- CPU Usage %
- Memory Usage %
- Physical Memory size in MB
- Virtual memory size
- Target

When you click a process in the Processes table, two icons are enabled in the center pane, one to view more details and the other to kill the process. Figure 12–9 shows an example where you can click check boxes to select or deselect system resource graphs from displaying on the Summary page.

When the software is configured to work with Oracle Enterprise Manager Cloud Control, information about available Oracle Enterprise Manager Cloud Control targets appears in the Process view.

### Services View

The Services tab provides a view of Oracle Solaris 10 and 11 Service Management Facility (SMF) services. The Oracle Solaris SMF feature defines the relationships between applications, or services, and is a method of managing them by providing a framework for startup scripts, `init` run levels, and configuration files. Each service is identified by a Fault Managed Resource Identifier (FMRI).

The Services tab contains SMF service instances, state, dependencies, and severity information. You can drill down to see specific service details, including the configuration, dependencies, and the processes that are in the service contract.

You can perform the following actions in the Services tab:

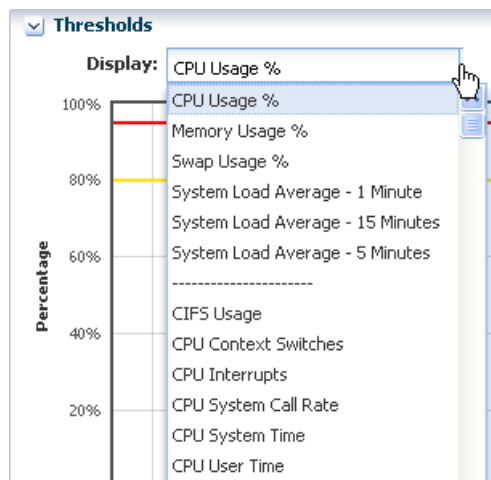
- View a list of services currently installed and their states
- View a list of dependencies and dependents for FMRI
- View the relationship between services and processes
- View details about why a service is not available
- Obtain logs for debugging
- Clear faults for FMRI
- Invoke the disable, enable, and restart actions on FMRI
- Read configuration files

Services information is available for agent managed and agentlessly managed Oracle Solaris 10 and 11 operating systems, including global and non-global zones.

### Thresholds

The Thresholds tab contains information about all monitored attributes for the selected operating system, including per-instance attributes such as File System Usage for each file-system on the asset. [Figure 12-10](#) shows a partial list of the monitored attributes available for display.

**Figure 12-10** Thresholds Display Options



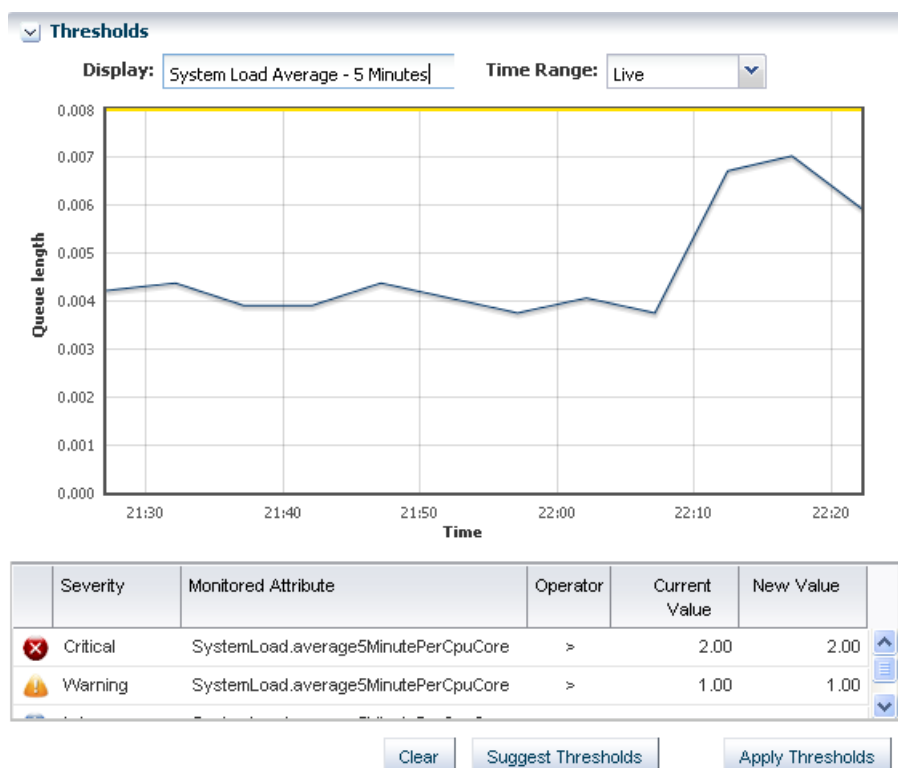
Charts for the historical data of those attributes show the alert monitor threshold levels, if configured, for that attribute. [Figure 12-11](#) shows the chart for the System Load Average - 5 minutes. The time frame selected is Live. Under the chart are the severity levels for this monitored attribute (SystemLoad.average15MinutePerCpuCore), the operator, and the threshold values. Instead of editing the thresholds in the Monitoring tab, you change the values on this page. You can either add values in the New Value column or click Suggest Thresholds to populate the fields with suggested values. Click Apply Thresholds to change the existing thresholds.

---

**Note:** When the threshold monitor is modified, the asset is removed from the default monitoring profile and a custom profile created.

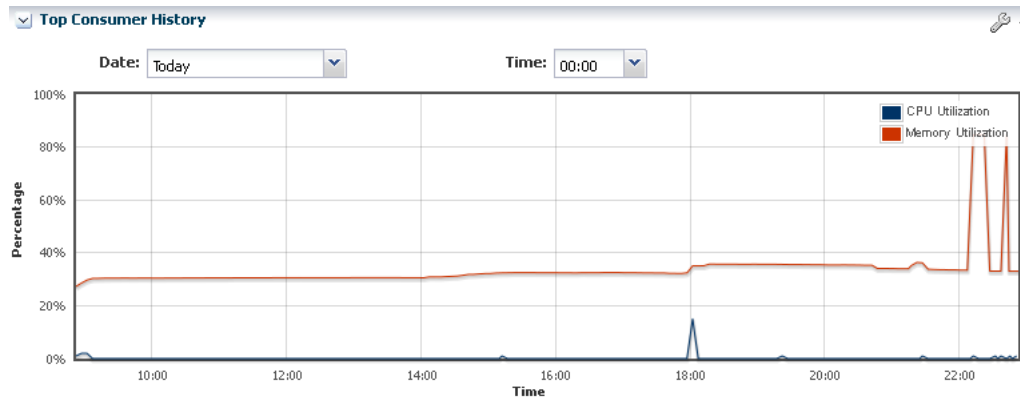
---

**Figure 12-11** Thresholds Chart



### History

The History tab contains the history for the top consumers. By default, the current date displays. The time selection box is used to select a time of day for which the top consumer processes are listed. It does not affect the chart, which can only show discrete intervals of 1 hour, 1 day, 5 days, 3 weeks, 6 weeks, and 6 months. The history chart displays the most applicable chart interval for the selected date and time. [Figure 12-12](#) is an example of a Top Consumer History chart. Click the wrench icon to select from a list of options to chart.

**Figure 12–12 Top Consumer History**

## Metrics

The Metrics tab provides you with specific details about various operating system statistics, such as the percentage of memory used, and view graphs. When monitoring thresholds are enabled for an element, you can reset the thresholds. When an element does not have a monitoring threshold, you can configure a new monitoring threshold.

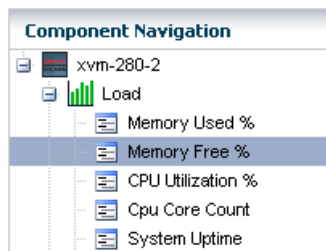
Click the Metrics tab to see OS-specific components. The following list are the categories of component details available for an agent-managed Oracle Solaris OS:

- Load
- File Systems
- Networks
- Users
- Buffer Activity
- Disk Usage
- Paging Activity
- Message Activity
- Tables Status
- TTY Activity
- Kernel Memory
- DNLC
- IPC Message Queue
- IPC Shared Memory
- IPC Semaphore Usage
- CPU Detail
- File Access
- Disk Errors
- Memory Utilization

Expand a component to view the available elements. Click an element to view the details. In [Figure 12–13](#), the Load component is expanded and the elements, such as percentage of memory used, CPU utilization percentage, CPU core count, and system

update options are available in the Load list. Memory Used % is selected and the details and a graph are visible.

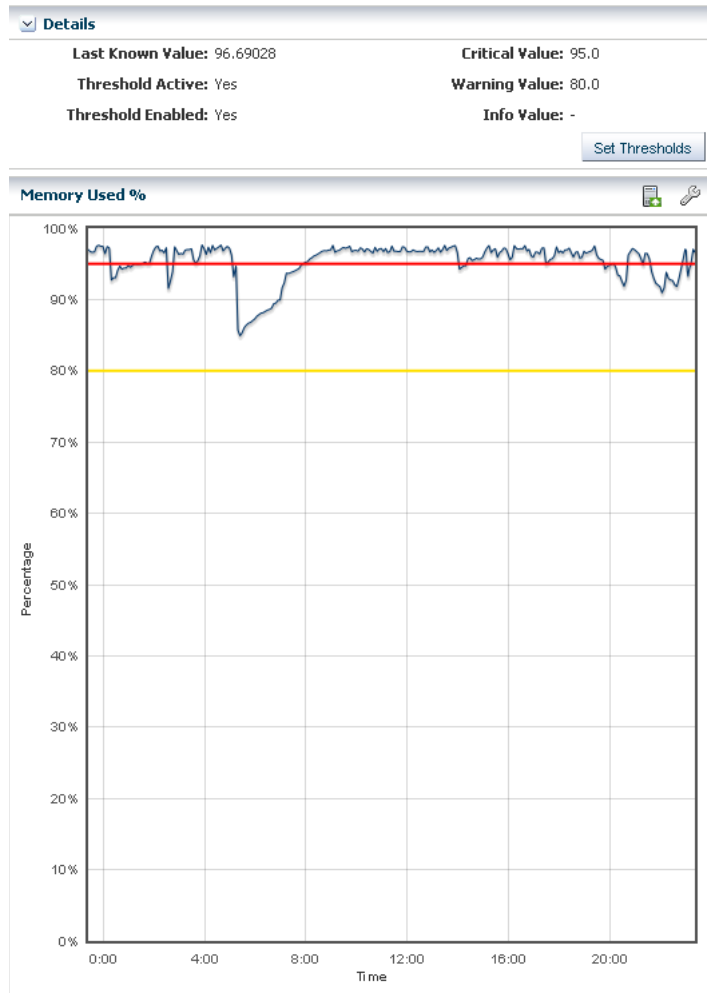
**Figure 12–13 Component Navigation**



The type of resource determines the available details. [Figure 12–14](#) is an example of the details and graph for the Memory Used % element. This example shows a system in trouble. The Details shows the last known value memory usage at 95.59111 percent and the established monitoring parameters. A warning incident is generated at 80 percent and a critical incident is generated when the used memory reaches 95 percent.

View the bar graph to see how the memory usage has trended over the selected time period. The yellow and red horizontal lines indicate the warning and critical thresholds.

**Figure 12-14 Memory Used % Details and Graph**



The wrench icon appears above the graph. For this graph, you can click the icon to change the graph style to line, bar, or area. You can also change the definition of the X axis from 1 day to 1 hour, 5 days, 3 weeks, 6 weeks, or 6 months. The export icon enables you to export the graph to file in CSV or XML format.

You have the opportunity to reset the threshold values for the monitoring rule from this page, or to view recommended threshold values based on past performance. When you click the Set Thresholds button, you are taken to the Thresholds tab, where you can enter new threshold values. When the Thresholds tab appears, the drop-down menu contains the name of the monitored attribute from the metrics view, and the associated chart is displayed. Editing a threshold value will create a custom set of monitoring rules for the asset. See [Chapter 4, "Monitoring Rules and Policies"](#) for more information about editing individual monitoring rule parameters and creating a custom monitoring policy.

## Virtualization Analytics View

The Virtualization Analytics view displays resource usage of the physical server for each running operating system instance, showing the physical resources consumed by the control domain (global zone or Oracle VM Server), and each non-global zone or guest. Metrics for Oracle VM Server for x86 are available through the Oracle VM Manager.



- Virtualization Analytics Summary
- Virtualization Analytics Zones or Virtualization Analytics Guests
- Virtualization Analytics History

The information is refreshed every 20 seconds for a guest running on a virtualization server container, including global zones, Oracle VM Server for SPARC, and Oracle VM Server for x86.

## Charts and Group Charts

Oracle Enterprise Manager Ops Center collects information every five minutes on every managed asset and displays the last hour of data on the asset's Summary tab and OS Details page. Use the following charts to see utilization data over longer periods of time, up to six months:

- Power Utilization: Servers, chassis
- CPU Utilization: Operating system, operating system for a virtualization host, virtual host, server pool
- Memory Utilization: Operating system, virtual host, server pool
- Network Utilization: Operating system, operating system for a virtual machine, virtualization host, server pool
- File System Utilization: Oracle Solaris OS and Linux OS
- System Load: Oracle Solaris OS and Linux OS

For the first five days of operation, the software collects data every five minutes. After the fifth day, the reported data is an average, according to the following:

- Five days to three weeks: Average for each hour
- Three weeks to six weeks: Average for each 12-hour period
- Six weeks to six months: Average for each 24-hour period

The data is automatically deleted after six months.

The following figure is a sample chart for a managed OS asset.

Figure 12–15 Sample Chart for an Managed OS



### Group Charts

In addition to displaying charts for individual assets, you can see charts for a group of assets: the five most-utilized assets and the five least-utilized assets in the group. In the Summary page of a group, hourly usage appears in a bar chart. You can create the following charts for the managed groups:

- Server Group
  - Power
- Chassis Group
- OS Group
  - CPU Utilization

- Network Utilization
- System Load
- Memory Utilization
- Host Group
  - CPU Utilization
  - Network Utilization
  - Allocated Memory
  - Power

## Creating Charts

You can create charts 24 hours after you first manage the asset. The asset must be operating and the Enterprise Controller must be able to get access to the asset. You can use the default format or change the charts to use a line, bar, or area format or to use different time intervals.

By default, the graphs show one day of data. Click the Live button in the graph's toolbar to change to Live mode, which reports new information every 5 seconds. You can also change the graph to one of the following periods:

- One hour (1H) – One point for every 5 minutes
- One day (1D) – One point for every 5 minutes
- Five days (5D) – One point for every 5 minutes
- Three weeks (3W) – One point every hour
- Six weeks (6W) – One point every 12 hours
- Six months (6M) – One point for every day To make a graph with the minimum of two points, a system must have been managed for at least 10 minutes to view a one-hour graph and for at least two days to view the six-months graph.

The software stores the data for these time periods separately. For example, when a server is managed for two hours and you select the 6W view, the graph does not display because only one point of data of that type is available; the second point has not yet occurred. When you select the 1D view, the graph displays 24 points of data (120 minutes in 5-minute intervals). However, the graph displays these points over a 24-hour period and not over the actual two-hour period. For the most accurate representation of the data, choose a time period that is less than or equal to the time that the selected server has been managed.

You can export the data for either the current view or all available data to a file in either CSV or XML format. Use the Export Chart Data tool bar icon to choose options for exporting the data.

When the graph is blank for a server, one of the following conditions has occurred:

- Server does not have the appropriate ILOM version.
- Server has not been discovered through the ILOM driver.
- Server is unreachable.

## Provisioning Operating Systems

The provisioning feature provides a method of automatically and consistently installing operating systems on managed systems from the Oracle Enterprise Manager Ops Center user interface.

You can provision the following operating systems:

- Oracle, SuSE, and Red Hat Linux
- Oracle Solaris (SPARC or x86)
- Oracle VM Server for SPARC
- Oracle VM Server for x86
- Oracle Solaris Clusters

---

---

**Note:** To provision Oracle Solaris 11, both the Enterprise Controller and Proxy Controller must be installed on a system that is running Oracle Solaris 11.

To provision Oracle Solaris 9 and 10, you can use a Proxy Controller that is installed on a system that is running either Oracle Solaris or Linux.

---

---

Automated OS provisioning is performed through a managed service processor. You can provision the OS on a single system, one or more groups of systems, or a combination of systems that are attached to your network.

OS provisioning is handled by a profile and an associated deployment plan. The profile defines the image and the plan defines the tasks to perform and the targets to provision. Some plans are simple single step plans, others are multi-step plans where OS provisioning is a step in a larger plan.

You have many options available when you provision an operating system. The following steps are needed to complete a basic provisioning job:

1. Determine how you will import the OS image files, with either Dynamic Host Configuration Protocol (DHCP) or a WAN boot.
2. Import a file with the OS image into a Software Library. A provisioning profile is automatically created when you import the OS image. You can use this profile, edit the profile, or create a new profile. See [Images](#) and [Images for OS Provisioning](#) for details on importing images. See [OS Provisioning Profiles](#) for the types of profiles you can create.
3. Create or configure a deployment plan that includes your profile.
4. Manage the service processor for one or more systems to provision. See [Discovering and Managing Assets](#) for details.
5. Apply the deployment plan on the targets. When you choose a group as a target, it must be an homogeneous group where all members are the same.

After you import the OS images and create the OS profiles, you can reuse the profiles in a variety of plans that have OS provisioning as a step.

### DHCP

DHCP dynamically assigns IP addresses to devices on a network. A typical OS provisioning job requires an installation server and a DHCP server on the same subnet

as that of the client systems. A JumpStart boot server must be on the same subnet as that of the client systems.

Before you can provision, you must configure DHCP services on the Proxy Controllers. You can use basic DHCP services, with or without defined subnets, or an external DHCP server. See the *Administration Guide* for information about how to configure DHCP and subnets for OS provisioning.

## WAN Boot

The WAN boot installation method enables you to boot and install software over a wide area network (WAN) by using HTTP. By using WAN boot, you can install the Solaris OS on SPARC based systems over a large public network where the network infrastructure might be untrustworthy. You can use WAN boot with security features to protect data confidentiality and installation image integrity.

WAN boot is the default connection for Oracle Solaris 11 provisioning. Oracle Solaris 11 provisioning does not use a Flash Archive (FLAR) image.

Oracle Solaris 10 provisioning can use a WAN boot or DHCP connection. With a WAN boot connection, Oracle Solaris 10 provisioning enables you to provision a FLAR image on a SPARC system using an HTTP web server. WAN boot installation is useful when DHCP does not meet your organization's security policies or you have SPARC-based systems that are located in geographically remote areas and you need to install servers or clients that are accessible only over a public network. Because WAN boot uses an HTTP server, it will work across your corporate firewall and does not require DHCP or a JumpStart boot server to be on the same network as the client systems.

The WAN boot installation method uses port 5555 and HTTP to boot and install software on SPARC-based ILOM, ALOM, or M-series systems over a wide area network (WAN). The WAN boot security features protect data confidentiality and installation image integrity over a large public network where the network infrastructure might be untrustworthy. You can use private keys to authenticate and encrypt data. You can also transmit your installation data and files over a secure HTTP connection by configuring your systems to use digital certificates. See "[Security Configurations Supported by WAN Boot](#)" in the *Oracle Solaris 10 10/09 Installation Guide: Network-Based Installations* document for more information about secure WAN boot installation configuration.

### WAN Boot Connection Requirements

The following are required to use WAN boot with Oracle Enterprise Manager Ops Center:

- Oracle Solaris 11
  - The target is a SPARC ALOM-CMT, ILOM-SPARC or M-Series platform that has a supported OBP or XCP. See [Checking Your Client OBP for WAN Boot Support](#) for how to check your client OBP. For M-Series, the XCP version should be at least version 1082.
  - The Enterprise Controller is installed on an Oracle Solaris operating system. You can use a SPARC or x86 platform for the Enterprise Controller.
  - WAN boot is enabled for Oracle Solaris 11 in Administration. See [Disabling and Enabling WAN Boot](#).

---

---

**Note:** When the target does not have the required OBP firmware version, Oracle Solaris 11 provisioning is disabled.

---

---

- Oracle Solaris 10
  - The target is a SPARC (ALOM-CMT, ILOM-SPARC or M-Series) and has the minimum OBP or XCP version
  - A FLAR image is used
  - The Enterprise Controller is installed on an Oracle Solaris operating system. You can use a SPARC or x86 platform for the Enterprise Controller.
- WAN boot is enabled for Oracle Solaris 10 in Administration. See [Disabling and Enabling WAN Boot](#).

---

---

**Note:** When the target does not have the required OBP firmware version, Oracle Solaris 10 provisioning will revert to a DHCP connection.

---

---

To determine if your client system has a WAN boot-enabled PROM, see [Checking Your Client OBP for WAN Boot Support](#).

### Checking Your Client OBP for WAN Boot Support

To determine if your client system has a WAN boot-enabled PROM, perform the following to check the client Open Boot PROM (OBP) for WAN boot support.

1. Log into a terminal window as root.
2. Type the following to check the OBP configuration variables for WAN boot support:

```
# eeprom | grep network-boot-arguments
```
3. The OBP supports WAN boot installations when the variable `network-boot-arguments` is displayed, or when the command returns the output `network-boot-arguments: data not available`. For example:

```
# eeprom | grep network-boot-arguments
network-boot-arguments: data not available
```
4. If the command in Step 2 does not return any output, the OBP does not support WAN boot installations. See your system documentation for information about how to update the OBP.

### Setting Up a WAN Boot Connection

When Oracle Enterprise Manager Ops Center is installed on an Oracle Solaris operating system, the Enterprise Controller is automatically configured to be a WAN boot server.

Oracle Solaris 11 uses WAN boot. For earlier versions of Oracle Solaris, WAN boot is the default connection for provisioning when the requirements are met and you choose to use a FLAR image. When you launch an OS provisioning on an eligible SPARC-based system and you choose a FLAR image, the software automatically uses WAN boot. If you have a group of systems to provision, the software determines whether to use WAN boot or DHCP for each system.

## Disabling and Enabling WAN Boot

WAN boot is automatically installed and enabled when the Enterprise Controller is running on an Oracle Solaris operating system. You can check the status, disable, or enable WAN boot in the Enterprise Controller configuration file. WAN boot is enabled when the value for the property is set to true in the Enterprise Controller configuration file. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about how to check the status, disable or enable the WAN boot connection.

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 disable WAN boot, change the value for the property to false.
5. To enable WAN boot, change the value for the property to true.

## Importing Images

Import your OS images into the Software Library before you can start a provisioning job. You can save the images in a Local Software Library on the Enterprise Controller or in a Network Attached Storage (NAS) Software Library that is created on an NFS server that the Enterprise Controller can access. See [Creating a Software Library](#) for details.

## OS Provisioning Profiles

The provisioning profiles collects all the information such as type of target, OS image, time zone and language setup, required JET modules, disk partitions, naming services and network details. Depending on the type of operating system you are provisioning, include its parameters in the profile that installs the operating system.

### Common Linux Parameters

Specify the following parameters:

- Installation number – The number that enables you to install all of the Linux software that is included in your subscription.
- Partition action – Use this parameter when you want to change the disk partition of the system.
  - You can opt to remove all the existing Linux partitions and retain the non-Linux partitions. You can provide specification for the new partitions.
  - You can opt to preserve all the existing partitions. You must define new partitions, outside of the partitions that exist, in which to install the OS.
  - You can opt to remove all the existing partitions. Define specification for the new partitions.
- Install protocol – Specify HTTP or NFS as the install protocol.
- Kernel parameters – Enter kernel parameters for the GRUB menu of the target system, when needed.
- MD5 Checksum – Select this option to use MD5 encryption for user passwords.

- Reboot action – Select whether you want to reboot the target system after OS installation.
- Disk label initialization – Select this option to initialize labels on new disks. This option creates labels that are appropriate for the target system architecture.
- Shadow passwords – Select this option to use an `/etc/shadow` file to store passwords on the target system.
- Clear master boot record – Select this option to clear all invalid partition tables.
- Linux packages – You can specify the Linux packages to include or exclude during provisioning. To include a package, enter the package name in a line. To exclude any package, enter the package name preceded by a dash (-).

### **SuSE Parameters**

To create a profile that installs the SuSE Linux OS, specify the following parameters:

- FTP proxy server – Enter the name of the FTP proxy server to support FTP services.
- HTTP proxy server – Enter the name of the HTTP proxy server to support HTTP services.
- Install protocol – Specify HTTP or NFS as the install protocol.
- Enable proxy servers – Select this option to enable the FTP and HTTP proxy servers that you specified in the FTP Proxy Server and HTTP Proxy Server fields.
- Kernel parameters – Enter kernel parameters for the GRUB menu of the target system, when necessary.
- Reboot action – Select whether you want to reboot the target system after OS installation.
- Linux packages – You can specify the Linux packages to include or exclude during provisioning. To include a package, enter the package name in a line. To exclude any package, enter the package name preceded by a dash (-).

### **Oracle Solaris or Linux OS Provisioning Profile**

Each profile is defined by the OS image that is either in the Software Library, or is imported into the Software Library. When you import an OS image into the software library, a default provisioning profile is automatically created. You can edit the default profile or you can create a new profile.

For each profile, you specify the setup parameters, file system parameters, the management mode, and the naming service for the operating system. For Oracle Solaris only, you can optionally use JET Modules to specify additional Installation Parameters. To learn more about JET and how to use JET in a profile, see [JumpStart Enterprise Toolkit \(JET\) for Oracle Solaris](#).

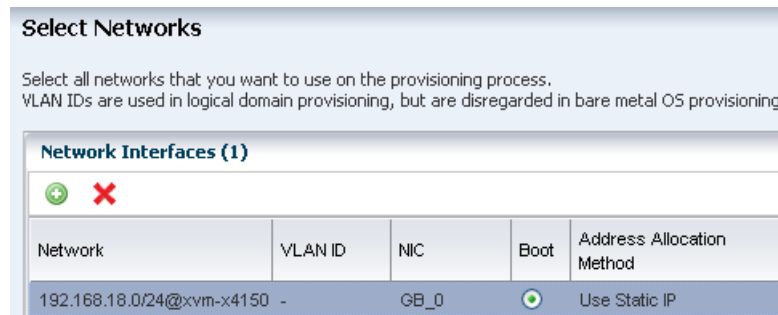
When you choose the agent managed mode, you can perform software updates and create operating system reports. When you choose agentlessly managed, SSH credentials are required to monitor the operating system. You can change the management mode after the OS is provisioned.

A provisioning profile, requires a DHCP-enabled network interface for the boot interface. You can add multiple networks, as long as the networks are available and defined in the Enterprise Controller. You can select a NIC from the list of available logical interfaces for each network or, as shown in [Figure 12-16](#), you can use the Address Allocation Method for the selected networks. You cannot use the Address



Allocation method for the boot interface. When you use a static IP address, you must provide the IP address when you apply a deployment plan that uses the profile. The IP address is assigned to the target system after provisioning.

**Figure 12–16 Select Networks**



By default, the profile reboots the OS. You can choose the Manual Net Boot option to enable manual control of network boot operations for the target system.

---

**Note:** The Enterprise Controller cannot remotely control the network boot process on systems that do not have a service processor. When your target system does not have a service processor, you must select the Manual Net Boot option.

---

### Oracle VM Server for SPARC OS Provisioning Profile

To create a profile that installs an Oracle VM Server Control Domain, define the following parameters:

- CPU Threads
- Memory
- Crypto Units
- Virtual Console Port Range
- Enable JASS

Enabling JASS results in installation of SUNWJass package to harden the system when installing Oracle VM Server 1.2 or lower versions. JASS is not supported for Oracle VM Server for SPARC 1.3 or higher versions. When you select Enable JASS in the profile that is installing Oracle VM Server for SPARC version 1.3 or 2.0, the software disregards this option and JASS is not enabled.

- Enable Multiplexed I/O

Enabling multiplexed I/O on a system used for storage enables the Fibre Channel ports on the system.

### JumpStart Enterprise Toolkit (JET) for Oracle Solaris

JumpStart Enterprise Toolkit (JET) provides a framework to simplify and extend the JumpStart functionality provided within the Oracle Solaris operating system. The SUNWjet and JetFLASH packages are installed on the Proxy Controller during installation.

Using JET provides more options for defining the Jumpstart parameters. When you install JET on a JumpStart server, you have the following advantages:

- Install multiple versions of Oracle Solaris
- Deploy flash archives
- Utilize multiple boot methods
- Install recommended patches
- Configure all your network interfaces

---

**Note:** You cannot define IPMP groups or link aggregation for a JET template profile.

---

Table 12–5 describes the JET modules that are installed on the Proxy Controller.

**Table 12–5 JET Modules and Associated Packages**

JET Module Name	JET Package	Description
base_config	SUNWjet	Provides the standard installation configuration for the client, including the information required to set up the JumpStart server to allow the client to boot and build.
custom	SUNWjet	Adds functionality to the JumpStart framework to handle packages, patches, scripts, and files.
flash	JetFLASH	Adds the ability for the JumpStart server to deliver Solaris images in Solaris Flash format.

See [Appendix D, "JumpStart Enterprise Toolkit"](#) for a list of SUNWjet parameters.

### To Create a JET Template

To create a profile that uses the JumpStart Enterprise Toolkit (JET), select a JET template that defines all the parameters for OS provisioning.

Place the JET template on a directory that the Enterprise Controller can access. You can also create a JET template on the Enterprise Controller in the directory `/opt/SUNWjet/Templates`, using the following command:

```
./make_template template_name
```

A sample template is provided. You can make a copy and change the values in the JET template as required. During provisioning, the OS provisioning parameters are read from the template. After you create the JET templates you want and save them on the Enterprise Controller, you can use them in your Oracle Solaris provisioning profiles.

## Provisioning Plans

When you create a profile, the default action creates a deployment plan and associates the plan with the profile. To provision an OS, you must have an OS image. Importing OS images and creating OS profiles are one-time tasks for each OS-target combination. After an OS image and an associated OS profile are created, you can use deployment

plan to provision the operating system onto one or more managed systems at the same time.

---

---

**Note:** It is a good practice to place the systems that you are going to provision in Maintenance Mode so that you can take the system offline without generating alerts and incidents.

---

---

The following is the general workflow for provisioning an OS:

1. Import a file with the OS image into a Software Library. The import process creates a profile that specifies the name and location of the OS image.
2. Use a deployment plan that includes the profile, either the default one, or one that you create.
3. Apply the deployment plan on the targets. Oracle Enterprise Manager Ops Center enables OS provisioning on single systems, groups of systems, a combination of the single systems and groups, or Oracle Solaris Clusters. OS provisioning for groups of systems requires using homogeneous groups.

To provision an operating system on an Oracle Solaris Cluster, you provision the same operating system on all nodes of a cluster. The Cluster OS Profile profile handles the pre-action and post-action operations. See the Oracle Solaris Cluster documentation and [Appendix B, "Oracle Solaris Cluster"](#) for how to install a new Oracle Solaris Cluster and to maintain existing Oracle Solaris Clusters.

## Deployment Plans That Provision an Operating System

Using the provisioning profiles created for different targets, create a deployment plan with the associated profile. Several multi-step and complex plans use an OS provisioning profile and plan as a step in the larger plan. Provisioning an Oracle Solaris 11 operating system is a different procedure from provisioning earlier versions.

The following deployment plans include a step to provision an operating system:

- Provision an Oracle Solaris or Linux OS
- Provision an Oracle Solaris 11 OS
- Provision and Update Logical Domains
- Provision an OS on an Oracle Solaris Cluster

## Provisioning Linux and Oracle Solaris 8, 9, and 10

You can create OS profiles for provisioning Linux OS on x86 systems or Oracle Solaris on x86 or SPARC systems. See [Provisioning Oracle Solaris 11](#) for details on provisioning Oracle Solaris 11.

### Planning

Perform the following before you provision the operating system:

- Import the OS image. A default OS provisioning profile for the image is automatically created. Uploading the packages from Oracle to the library can take several hours.
- (Optional) Edit an existing OS provisioning profile or create a new profile.
- Discover the service processors of the target systems.

- Verify that the Dynamic Host Configuration Protocol (DHCP) services are enabled on Proxy Controllers. You cannot create a profile or assign any network if the DHCP services are not enabled. The Install Server option to provision OS on a server is not enabled if the DHCP is not enabled on any of the interfaces.
- Verify that any scripts the profile uses are in a directory that the Enterprise Controller can access. You can save scripts in a local directory of the Enterprise Controller, or in a directory that the Enterprise Controller mounts using NFS.
- When you are provisioning a dynamic system domain of an M-Series server, the domain must have an IP address.
- Disable monitoring for the target systems to prevent events related to a system going offline. See [Maintenance Mode](#) for more information.

Complete the following steps to provision an operating system:

1. Verify that the OS image and profile are available and configured with the parameters you want to use.
2. Discover the service processors of the target systems.
3. Place the asset in [Maintenance Mode](#) to prevent events related to a system going offline
4. Select the OS Provisioning plan, or a plan that uses OS Provisioning as a step.
5. Define the targets for the plan, make any last minute changes in the plan, then submit the job.

## Provisioning Oracle Solaris 11

Oracle Solaris 11 uses a new OS provisioning technology, called the Automated Installer. This feature replaces the older JumpStart Enterprise Toolkit technology that Oracle Enterprise Manager Ops Center uses to provision earlier versions of Oracle Solaris.

Oracle Enterprise Manager Ops Center reduces the complexity by using a local copy of the Oracle Solaris 11 Software Library on the Enterprise Controller and creating an Automated Installer server on the Proxy Controller for your use.

---

---

**Note:** To provision an Oracle Solaris 11 operating system, the Enterprise Controller and Proxy Controller must both be running on an Oracle Solaris 11 operating system. The repository resides on the Enterprise Controller and the Automated Installer server resides on the Proxy Controller. When the Enterprise Controller and Proxy Controller are not running on Oracle Solaris 11, the Oracle Solaris 11 library and OS provisioning actions are not available.

---

---

Oracle Solaris 11 uses the following components for provisioning an operating system:

- Oracle Solaris 11 Software Library – A local version of the software package repository. You can update the Oracle Solaris 11 Software Library, as needed, and then provision multiple systems without using a network connection to Oracle for each provisioning job. See [Chapter 5, "Software Libraries"](#) for more information about adding content to libraries.
- Installation manifest – Defines the system configuration, including what software to install and details on the virtualized environments to provision. A default manifest is included with each Image Packaging System (IPS) software repository.

- DHCP or WAN boot connection
  - x86 client – Requires a DHCP connection.
  - SPARC client – Requires a DHCP or WAN boot connection. Oracle Enterprise Manager Ops Center automatically sets up WAN boot connection.

---

**Note:** Oracle Solaris 11 only supports a ISC DHCP Server. Oracle Solaris DHCP Server is not supported.

---

You can provision Oracle Solaris 11 zones as part of the OS installation. After a system is bootstrapped with a minimized operating system, the operating system is installed from the Oracle Solaris 11 Software Update Library in Oracle Enterprise Manager Ops Center. The zones are provisioned during the initial system reboot after the base operating system is installed.

### Oracle Solaris 11 Provisioning Profiles

You can create multiple profiles to respond to subtle variations in hardware attributes, software profiles, or your organization's requirements.

Before you can create provisioning profiles, verify that the Oracle Solaris 11 Software Library is configured on the Enterprise Controller and the package you want is available in the library.

When you create an Oracle Solaris 11 OS provisioning profile, you select the architecture, either SPARC or x86, to display the boot image and distribution for your architecture. You must provide non-root user credentials and root user credentials. You can only use non-root user credentials to login or SSH to the client after install.

The boot image has several associated software groups. You must select one of the following software groups:

- large-server
- small-server
- desktop

The boot image might have additional Software groups that you can select, such as storage-server and NAS attached. You can select one or more of these groups. Each group has a tool tip that provides a description of the group.

To install the OS to an iSCSI disk, select the Use iSCSI Disk option when you create the profile, then specify the iSCSI disk settings. When you use this option, you must provide the following parameters when you deploy the OS Provisioning plan:

- Storage server IP
- SCSI disk LUN

### Steps for Oracle Solaris 11 Provisioning Plan

The following are the main steps to provision an Oracle Solaris 11 operating system:

1. Create an Oracle Solaris 11 OS provisioning profile.
2. From the Library section, initialize the Oracle Solaris 11 Software Update Library.
3. From the Plan Management section, create a Solaris 11 x86 or SPARC profile (the Solaris 11 images are pre-imported as part of MSR creation).
4. Target the plan to an x86 server or WAN boot-capable SPARC server.

## Oracle Solaris Boot Environments

Boot environments are a feature of Oracle Solaris. A boot environment is an instance of a bootable Oracle Solaris image plus additional software packages that are installed onto the image, and the set of all file systems and devices (disk slices and mount points) that are required to operate an Oracle Solaris OS instance. You can have disk slices, also known as partitions, on the same disk or distributed across several disks.

A dual boot environment consists of a live, or active, boot environment (BE) and one or more inactive alternate boot environments (ABE). A system can have only one active boot environment, which is the booted environment. An alternate boot environment is an inactive environment that is not currently booted. A system can have many inactive boot environments. You can activate an alternate boot environment at any time.

You can use a dual boot environment within Oracle Enterprise Manager Ops Center to manage your Oracle Solaris software. A dual boot environment is often used to manage updates because it can significantly reduce the service outage time that is usually associated with patching. Maintaining multiple boot environments also enables quick and easy rollback to a version before the patches were applied, if needed. The boot environment technology enables you to duplicate a boot environment and perform the following tasks without affecting the currently running system:

- Run an Oracle Solaris software update simulation on the inactive boot environment. You can run the simulation with or without downloading the patches.
- Update your Oracle Solaris OS on the inactive boot environment and test the update before deploying it as your active environment.
- Maintain multiple boot environments with different images. For example, you can create one boot environment that contains all current patches and another that contains only security patches.

## Differences Between Oracle Solaris 11 and Oracle Solaris 10 Boot Environments

The boot environment feature changed beginning with Oracle Solaris 11, including the supported file systems, file system requirements, zone support, and how boot environments are created.

Oracle Solaris 11 Boot Environments use the `beadm` utility and ZFS file systems to create and manage boot environments. You do not need to create boot environments ahead of time. The software creates them automatically. You can use an agent-managed or agentless-managed operating system with the Oracle Solaris 11 Boot Environments feature.

Oracle Solaris 10 and earlier use the Live Upgrade feature with `lucreate` scripts and ZFS or UDFS file systems to create alternate boot environments. You must use an agent-managed operating system with the Oracle Solaris Live Upgrade feature.

The Boot Environments profile defines the boot environment for the OS update deployment plans. The Oracle Solaris release determines how the profile is used:

- Oracle Solaris 11 – The profile indicates the policy that is used when an OS update plan is executed. Use this profile to define the creation policies and as a step in an OS update deployment plan.
- Oracle Solaris 8, 9, and 10 – The profile defines the `lucreate` script that is used to create your alternate boot environments. Use this profile to specify how to create

alternate boot environments for the eligible operating systems in your data center, create alternate boot environments, synchronize and activate boot environments, and as a step in an OS update deployment plan.

The user interface assists you in easily navigating the differences in the boot environments features and provides a unified view whenever possible. See [Oracle Solaris 11 Boot Environments](#) and [Oracle Solaris 10 and Earlier Boot Environments](#) for detailed version-specific information.

## Boot Environment Monitoring

Monitoring rules and thresholds are defined in the Monitoring tab. The following rules apply to boot environments:

- Number of Boot Environments – Defines the number of boot environments in the selected zone.
- Boot Env Usage Percent in a ZPool – Defines the percentage disk utilization on the boot environments in any of the zpools.

Each rule has two defined thresholds:

- Warning – Generates a warning alert and displays the yellow warning badge in the asset tree. A warning alert contains a suggested action.
- Critical – Generates a critical alert and displays the red critical badge in the asset tree. By default, a critical alert contains an automated action.

See [Monitoring Operating Systems](#) for more information.

### To Clear a Boot Environment Incident

Perform the following steps to manually clear the disk space and close the incident:

1. Click an OS in the Asset tree to view the Boot Environment in the center pane, then click the Incidents tab.
2. Delete one or more boot environments to clear the disk space.
3. Select one or more incidents, then click the Close Incident(s) icon in the center pane.

See [Chapter 4, "Monitoring Rules and Policies"](#) for details on how monitoring rules and policies work in the software and see [Chapter 9, "Incidents"](#) for information on how to manage and close an incident.

## View Boot Environments

The active boot environment is identified in the Boot Environments tab and in the Summary tab. Inactive boot environments appear in the Boot Environments tab for each operating system. For global zones, the Boot Environments tab displays the relationship between the associated zones and existing boot environments.

---

---

**Note:** If there are no alternate boot environments, the Boot Environments tab is not displayed in the center pane.

---

---

Boot environment support for Oracle Zones is available beginning with Oracle Solaris 11, enabling boot environments from the non-global zone to appear in the asset tree.

The Summary tab provides the name of the active boot environment, the zpool utilization of all zpools for the selected OS and the amount of zpool utilization

attributed to the boot environments. Details are available in the Boot Environments tab.

1. Click an OS or zone in the Asset tree. Details about the active boot environment appear in the Summary tab.

Non-bootable snapshots are available beginning with Oracle Solaris 11. When a boot environment has one or more associated non-bootable snapshots, the snapshots appear in the Snapshots subtab, as shown in [Figure 12–17](#).

**Figure 12–17 Boot Environment Tab and Snapshots Subtab**

The screenshot displays two panels. The top panel, titled 'Boot Environments', contains a table with the following data:

Active	BE Name	Size	Description	Created/Last Synchronized on
	solaris	19.14 GB		11/15/2011 6:58:06
	B1	165.00 KB		11/16/2011 9:46:29
	solaris-backup-1	242.00 KB		02/27/2012 4:36:59
	solaris-backup-2	576.00 KB		02/28/2012 3:57:07

Below this table are three subtabs: 'Snapshots', 'File Systems', and 'Associated Zone BEs'. The 'Snapshots' subtab is active, showing 'Snapshots of selected BE: solaris'. It contains a table with the following data:

Name	Size	Created on
solaris@2012-02-28-10:57:06	357.00 KB	02/28/2012 3:57:06 am MST
solaris@2012-02-27-11:36:58	7.91 MB	02/27/2012 4:36:58 am MST

2. Click the Boot Environments tab in the center pane to see details about the associated alternate boot environments.  
If the tab is disabled, no alternate boot environments exist for that OS in the zone or non-global zone.
3. To display file system details, click the boot environment in the table, then click the File Systems subtab:
  - Oracle Solaris 11 – Mount point information, boot environment file systems, zone boot environment information, and non-global zones in the selected boot environment. When a global zone boot environment is selected, the zone boot environment details are listed separately, a zone per row. You can expand all rows to display a complete view of all zone boot environments under the selected global zone boot environment.
  - Oracle Solaris 10 – Mount point information and boot environment file systems.
4. To display associated zone boot environment details, click the boot environment in the table, then click the Associated Zone BEs subtab:
  - Oracle Solaris 11 – Mount point information, boot environment file systems, zone boot environment information, and non-global zones in the selected boot environment. When a global zone boot environment is selected, the zone boot environment details are listed separately, a zone per row. You can expand all rows to display a complete view of all zone boot environments under the selected global zone boot environment.



- Oracle Solaris 10 – Mount point information and boot environment file systems.

Monitoring rules and thresholds are defined in the Monitoring tab.

## Manage Boot Environments

You can view all available boot environments for a system, and choose to activate an alternate boot environment or delete inactive environments.

### Activate and Reboot a Boot Environment

Activating a boot environment makes an inactive or alternate boot environment the active boot environment. You can activate a single boot environment, or you can select an OS group and activate an alternate boot environment for each operating system.

#### To Activate a Single Boot Environment

Information about boot environments appears in the Boot Environments tab for each operating system.

Perform the following steps to activate a single boot environment:

1. Click an Oracle Solaris 11 global or non-global zone or an Oracle Solaris 10 global zone in the Asset tree.
2. Click the Boot Environments tab.

Existing boot environments for the OS appear in the center pane.

#### To Activate Boot Environments for All Members of a Group

You can activate an alternate boot environment for all members of a group. If each OS in the group has a single alternate boot environment, all operating systems are booted into the alternate boot environment. When some systems have more than one alternate boot environment, you are prompted to select the alternate boot environment.

Perform the following steps to activate boot environments for all members of an operating system group:

1. Select an Oracle Solaris 11 or an Oracle Solaris 10 Operating system group from the Assets section in the Navigation pane.
2. Click Activate Boot Environment and Reboot in the Actions pane.
3. For systems with multiple alternate boot environments, select the one that you want to boot into. A Filter ABE by name option is available to identify similarly named alternate boot environments across multiple targets.

#### To Delete a Boot Environment

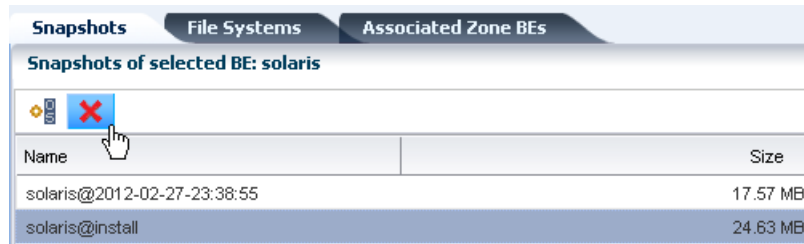
When you delete a boot environment, you delete all associated snapshots and unshared file systems. A snapshot is a non-bootable copy of a boot environment. If there are non-global zone boot environments associated with the global zone boot environment, they are deleted too. Shared file systems are not deleted.

You cannot delete the active boot environment.

1. Click an Oracle Solaris 11 global or non-global zone, or an Oracle Solaris 10 global zone in the Asset tree.
2. Click the Boot Environments tab.

3. Select one or more boot environments or snapshots that you want to remove, then click the Delete icon. [Figure 12–18](#) shows a snapshot selected for deletion.

**Figure 12–18 Delete an Oracle Solaris 11 Snapshot**



## Oracle Solaris 11 Boot Environments

Oracle Solaris 11 uses ZFS file systems, where the swap and dump volumes are shared within the pool. For unshared file systems, ZFS is the only supported file system for boot environments on Oracle Solaris 11. With the ZFS-based boot environment, the boot environments are clones of the existing ZFS partitions. This saves disk space and you do not need to reserve disk partitions for additional boot environments. The create and activate boot environment functionality is much faster than in previous versions.

Oracle Solaris 11 boot environments are managed through the `beadm` utility. A new boot environment is created whenever the kernel or system packages are installed or updated. This can result in high disk space utilization levels. By default, Oracle Enterprise Manager Ops Center monitors the disk (zpool) utilization of boot environments. If the utilization levels exceed defined thresholds, you can delete unwanted boot environments.

When a boot environment is created in the global zone, the following occurs:

- A Boot Environment of the source boot environment is created (the boot environment from which it is cloned).
- The currently active boot environment in all of the non-global zones is cloned and it is associated with the global zone boot environment that was just created.

When a global zone boot environment is activated, the active boot environment data set that is associated with that boot environment in each non-global zone is mounted and activated. Only one non-global zone boot environment that is associated with a global zone boot environment can be active.

When a global zone boot environment is deleted, all corresponding zone-specific boot environments are also deleted.

When a non-global zone is deleted, all corresponding boot environments are deleted. The boot environments for other zones are not deleted.

## Boot Environment Details for Oracle Solaris 11

The Oracle Solaris 11 Boot Environments tab provides you with a large amount of information about the boot environments that are associated with the selected physical or virtual Oracle Solaris 11 operating system. This is particularly valuable since Oracle Solaris 11 boot environments are automatically created and they can quickly consume valuable resources. The following information is available:

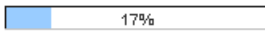
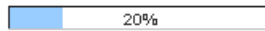
- [Total ZPools Utilization for Oracle Solaris 11 Boot Environments](#)
- [Boot Environments for Oracle Solaris 11](#)

- [Snapshots for Oracle Solaris 11 Boot Environments](#)
- [File Systems for Oracle Solaris 11 Boot Environments](#)
- [Associated Zone Boot Environments](#)

### Total ZPools Utilization for Oracle Solaris 11 Boot Environments

The first section in the Boot Environments tab is Total ZPools Utilization. It is compressed by default. Use the arrow to expand the table. The amount of resources used by the zpool appears in this section, as shown in [Figure 12-19](#).





**Figure 12-19 Oracle Solaris 11 Total ZPools Utilization**

Total ZPools Utilization			
ZPool Name ▲	% Space used by all Boot Environments	% Total Space Used	Total Space
rpool	 17%	 20%	72.80 GB

### Boot Environments for Oracle Solaris 11

All boot environments that are associated with the physical or virtual operating system that is selected in the Asset tree appear in the Boot Environments table. As shown in [Figure 12-20](#), the active status, size, and when the boot environment was created appear in this section. A green check mark icon next to the boot environment name identifies the boot environment as active. A green check mark with a green circle and white x indicates that this is the boot environment that is active upon reboot. When you see two green check marks in the Active column, the boot environment is active and is the active boot environment upon reboot.

**Figure 12-20 Oracle Solaris 11 Boot Environments Tab**

Boot Environments				
Active	BE Name	Size	Description	Created/Last Synchronized on
	solaris	19.14 GB		11/15/2011 6:58:06
	B1	165.00 KB		11/16/2011 9:46:29
	solaris-backup-1	242.00 KB		02/27/2012 4:36:59
	solaris-backup-2	576.00 KB		02/28/2012 3:57:07

Snapshots of selected BE: solaris		
Name	Size	Created on ▼
solaris@2012-02-28-10:57:06	357.00 KB	02/28/2012 3:57:06 am MST
solaris@2012-02-27-11:36:58	7.91 MB	02/27/2012 4:36:58 am MST

The lower section of the page has three tabs that provide details about the boot environment that you select in the Boot Environments table.

## Snapshots for Oracle Solaris 11 Boot Environments

A snapshot is a point-in-time image of a Volume. It is a non-bootable copy of a boot environment that uses much less disk space than a boot environment. You can create a boot environment from a snapshot.

Non-bootable snapshots are available beginning with Oracle Solaris 11. Select a boot environment in the Boot Environments table to see all associated non-bootable snapshots in the Snapshots tab. You can select a snapshot in this tab and click the icon to create a boot environment from the snapshot.

**Figure 12–21 Oracle Solaris 11 Boot Environment Snapshots**

Name	Size	Created on
solaris@2012-02-22-19:45:03	21.12 MB	02/22/2012 12:45:03 pm MST
solaris@2012-01-27-23:41:50	195.01 MB	01/27/2012 4:41:50 pm MST

## File Systems for Oracle Solaris 11 Boot Environments

The File Systems tab provides file system details for the boot environment, or alternate boot environment, that you select in the Boot Environments tab. As shown in [Figure 12–22](#), the file system name, type, size and mount location appear in this table. You can also see if the file system is shared or not.

**Figure 12–22 Oracle Solaris 11 Boot Environments File Systems**

Name	Type	Size	Mounted on	Shared
rpool	ZFS	13.80 GB	/rpool	true
rpool/ROOT/solaris	ZFS	11.73 GB	/	false

## Associated Zone Boot Environments

The Associated Zone BEs tab is populated with the boot environment details for a selected zone's boot environment. The zone might have multiple boot environments. The table shows whether the boot environment selected is active. You can see the boot environment name, the zone name, the size and when the boot environment was created. As shown in [Figure 12–23](#), when you select an operating system that is not a zone, No Data appears in the table.

**Figure 12–23 Oracle Solaris 11 Boot Environments Associated Zone BEs**

Active	BE name	Zone Name	Size	Creation Date
No data				

## Boot Environment Profiles and Plans for Oracle Solaris 11

A Boot Environments plan and profile for Oracle Solaris 11 operating systems identifies and defines how the boot environment is updated and activated. You can use an agent-managed or agentless-managed operating system.

Use the profile for Oracle Solaris 11 to perform the following tasks:

- Create a Boot Environments profile that defines the creation policies
- Create an OS update deployment plan, specifying a Boot Environments profile and an OS update profile

You can create profiles with different policy options. The following options are available for Oracle Solaris 11:

- Create a new boot environment only when needed, such as when the OS update operation requires a reboot.
- Always create a new boot environment
- Never create a new boot environment
- Activate and reboot

### To Create a Boot Environments Profile for Oracle Solaris 11

1. Click Plan Management in the Navigation pane, then scroll down to the Profiles and Policies directory and click Boot Environments.

The Boot Environments Profiles page appears in the center pane.

2. Click Create Profile in the Actions pane.
3. Identify the profile by typing a unique profile name, provide a description, and select the Oracle Solaris 11 subtype.
4. Choose the boot environment policy for this profile:
  - Create a new boot environment when needed
  - Always create a new boot environment
  - Never create a new boot environment
5. Click the check box to activate boot environment and reboot when the job is completed.
6. Choose to have the software automatically create a unique name or enter a specific boot environment name in the field provided, then click Finish.

### To Copy an Oracle Solaris 11 Boot Environments Profile

Copying a boot environment profile makes a copy of an existing profile.

1. Click Plan Management in the Navigation pane, then scroll down to the Profiles and Policies directory and click Boot Environments.

The Boot Environments Profiles page appears in the center pane.

2. Select the profile to copy, then click the Copy Profile icon in the center pane.
3. Identify the profile by typing a unique profile name and description.
4. Change the boot environment parameters, as needed, then click Finish.

## Create an Oracle Solaris 11 Boot Environment

A new alternate boot environment is automatically created when you install or update the operating system's kernel or system packages.

You can create a bootable or non-bootable copy of an existing boot environment. A non-bootable copy is called a snapshot. You can create a boot environment from a snapshot.

### To Create an Oracle Solaris 11 Boot Environment

You can create a bootable or non-bootable (snapshot) copy of an Oracle Solaris 11 boot environment.

1. Click an Oracle Solaris 11 OS, a global or non-global zone, in the Asset tree, then click the Boot Environments tab.
2. Select the boot environment to copy, then click the Create icon.
3. Select the option, either the Create a Snapshot or Create a BE option, and select the boot environment to use as the source. Type a unique name for the boot environment and provide a description that includes the purpose of the boot environment and the name of the source boot environment, then click Create.

**Figure 12–24 Create Boot Environment for Oracle Solaris 11**

Create Boot Environment(BE)

Create a snapshot from

Create a BE from

\* Name:

Description:

4. When the job finishes, refresh the Boot Environment table to see the new boot environment.

If you have a group that contains only Oracle Solaris 11 operating systems and you select the OS group as the target, a new boot environment is created for every active boot environment in the group. You can assign a common name for all of the boot environments. If you do not assign a common name, default names are assigned.

## Oracle Solaris 10 and Earlier Boot Environments

Boot environments in Oracle Solaris 8, 9, and 10 are managed through the Live Upgrade feature. A boot environment is created by using a script that contains the `lucreate` command and options.

The Live Upgrade feature is available on the following operating systems:

- Oracle Solaris 10 OS for x86 platform versions through Oracle Solaris 10 5/09 – Update alternate boot environments for physical systems.

- Oracle Solaris 10 OS for SPARC through Oracle Solaris 10 5/09 – Update alternate boot environments for physical and virtual machines, including Oracle Solaris Zones and Oracle VM Server for SPARC (formerly known as Logical Domains).
- Oracle Solaris 9 OS SPARC – Update alternate boot environments for physical machines using a UFS file system.
- Oracle Solaris 8 OS SPARC – Update alternate boot environments for physical machines using a UFS file system.

---

---

**Note:** Do not use Oracle Solaris Live Upgrade on your Enterprise Controller or Proxy Controllers. It does not synchronize all of the files that are required for these Oracle Enterprise Manager Ops Center components.

---

---

To create and update alternate boot environments, install the latest Oracle Solaris Live Upgrade packages and patches. This ensures that you have all the latest bug fixes and features. In addition, verify that the disk space and format are sufficient for an alternate boot environment.

Live Upgrade packages and patches are available for each Oracle Solaris software release beginning with Oracle Solaris 9 OS. Use the packages and patches that are appropriate for your software instance. To use Live Upgrade with Oracle Solaris 8 OS, follow the special patching instructions.

If you installed Oracle Solaris 10 using any of the following software groups, have the required packages:

- Entire Oracle Solaris Software Group Plus OEM Support
- Entire Oracle Solaris Software Group
- Developer Oracle Solaris Software Group
- End User Oracle Solaris Software Group

When you install one of these Software Groups, verify that you have all of the required packages:

- Core System Support Software Group
- Reduced Network Support Software Group

For detailed requirements to install and use the Live Upgrade feature, see the [Oracle Solaris 10 Installation Guide: Solaris Live Upgrade and Upgrade Planning](#). For information on other releases, see the [Oracle Solaris Documentation Library](#). Review and verify that all the packages and patches that are relevant to your system are installed and that the disk is formatted properly before creating a new boot environment.

For Oracle Solaris 9 and 10 alternate boot environments, file systems are categorized into the following types:

- Critical File Systems – Non-shareable file systems that are required by the Oracle Solaris OS, such as root (/), /usr, /var, and /opt. These file systems are separate mount points in the `vfstab` of the active and inactive boot environments and are always copied from the source to the inactive boot environment.
- Shareable File Systems – User-defined files, such as /export, that contain the same mount point in the `vfstab` in both the active and inactive boot environments. Updating shared files in the active boot environment also updates data in the

inactive boot environment. When you create a boot environment, shareable file systems are shared by default. If you specify a destination slice, also known as a partition, the file systems are copied.

- Swap – Depends on the type of file system:
  - For UFS file systems, swap is a special shareable volume. Like a shareable file system, all swap slices are shared by default. If you specify a destination directory for swap, the swap slice is copied.
  - For ZFS file systems, swap and dump volumes are shared within the pool.

When creating a new boot environment in Oracle Solaris 9 or 10, the entire contents of a slice is copied to the designated new boot environment slice. You might want some large file systems on that slice to be shared between boot environments rather than copied to conserve space and copying time. File systems that are critical to the OS such as root (/) and /var must be copied. File systems such as /home are not critical file systems and could be shared between boot environments. Shareable file systems must be user-defined file systems and on separate swap slices on both the active and new boot environments. You can reconfigure the disk several ways, depending your needs.

You can reslice, or partition, the disk before creating the new boot environment and put the shareable file system on its own slice. For example, if the root (/) file systems, /var, and /home are on the same slice, reconfigure the disk and put /home on its own slice. When you create any new boot environments, /home is shared with the new boot environment by default. To share a directory, the directory must be split off to its own slice.

## Support for Oracle Solaris 10 Live Upgrade and Oracle Solaris Zones

The following requirements are needed to use the Live Upgrade feature with zones:

- Agent managed operating system
- At least Oracle Solaris 10 5/09 (update 7) operating system
- Storage library used to house the zones cannot be part of the root pool; you must create a separate pool on a shared file system
- You cannot use the `-p` option to create alternate boot environments

The `-p` option, which copies between two root pools on ZFS configuration, is not supported with the `lucreate` command.

---

---

**Note:** If you plan to use alternate boot environments with zones, you must designate sufficient zone storage space. When you create the zones and configure the zone storage, specify twice the size of the zone file system for the root file system of the zone. For example if your zone root file system was configured as 8 GB, the storage used to back up the zone must be at least 16 GB.

---

---

See [Update Zones](#) for how to update Oracle Solaris Zones without using a dual boot environment.

## Boot Environment Details for Oracle Solaris 10 and Previous Versions

The Oracle Solaris 10 Boot Environments tab provides you with a large amount of information about the boot environments that are associated with the selected Oracle





Solaris operating system. A Boot Environments tab is not available for Oracle Solaris 10 non-global zones. The following information is available:

- [Total ZPools Utilization for Oracle Solaris 10 and Earlier Boot Environments](#)
- [Boot Environments for Oracle Solaris 11](#)
- [File Systems for Oracle Solaris 10 and Earlier Boot Environments](#)

### Total ZPools Utilization for Oracle Solaris 10 and Earlier Boot Environments

The first section in the Boot Environments tab is Total ZPools Utilization. It is compressed by default, use the arrow to expand the table. The amount of resources used by the zpool appears in this section, as shown in [Figure 12–25](#).



**Figure 12–25 Oracle Solaris 10 and Earlier Total ZPools Utilization**

Total ZPools Utilization			
ZPool Name ▲	% Space used by all Boot Environments	% Total Space Used	Total Space
rpool	 17%	 20%	72.80 GB

### Boot Environments for Oracle Solaris 10 and Earlier

All boot environments that are associated with the physical or virtual operating system that is selected in the Asset tree appear in the Boot Environments table. As shown in [Figure 12–26](#), the active status, size, description, and when the boot environment was created or synchronized appear in this section. A green check mark icon next to the boot environment name identifies the boot environment as active. A green check mark with a green circle and white x indicates that this is the boot environment that is active upon reboot. When you see two green check marks in the Active column, the boot environment is active and is the active boot environment upon reboot.

**Figure 12–26 Boot Environments for Oracle Solaris 10 and Earlier**

Boot Environments				
Active	BE Name	Size ▼	Description	Created/Last Synchronized on
	newbemythilis	150.82 GB		-
	cherokeeBE	123.97 GB		-

The lower section of the page the File Systems tab that provide details about the boot environment that you select in the Boot Environments table.

### File Systems for Oracle Solaris 10 and Earlier Boot Environments

The File Systems tab provides file system details for the boot environment, or alternate boot environment, that you select in the Boot Environments tab. As shown in [Figure 12–27](#), the file system name, type, size and mount location appear in this table. You can also see if the file system is shared or not.

**Figure 12–27 Oracle Solaris 10 Boot Environments File Systems**

File Systems				
File Systems of selected BE: EranSol10ABE				
Name	Type	Size ▲	Mounted on	Shared
shripool/ROOT/EranSol10ABE	zfs	15.57 MB	/	false
/dev/zvol/dsk/shripool/swap	swap	4.00 GB	-	false

## Boot Environments Profiles and Plans for Oracle Solaris 10 and Earlier

You can use an alternate boot environment that was created outside of Oracle Enterprise Manager Ops Center; however, the preferred method is to create a Boot Environment profile and use the associated plan to create a boot environment. In either case, the operating system must be an agent-managed asset in the Oracle Enterprise Manager Ops Center software.

Use the profile for Oracle Solaris 10 and earlier releases to perform the following tasks:

1. Create a Boot Environments profile to specify how to create boot environments across all your managed system, using `lucreate` scripts
2. Create your boot environments using the action in the action panel for your assets. This is typically a one time operation, as you'll probably reuse the alternate boot environment.
3. Create a Boot Environments profile to always sync (and possibly) activate. Use this profile for OS update deployment plans.
4. Create an OS update deployment plan specifying the boot environment in step 3 and any OS update profile

Depending on the Oracle Solaris version that you are using, several methods are available for creating alternate boot environments. The Oracle Enterprise Manager Ops Center software uses Boot Environments profiles to help standardize and simplify the process.

Perform the following tasks before creating a Boot Environments profile:

1. [Determine Your Boot Environment Policy](#)
2. [Determine Your Live Upgrade Feature Requirements and Options](#)

### Determine Your Boot Environment Policy

Each Boot Environments profile can have a different boot environment policy. The following options are available:

- For Oracle Solaris 11
  - Create a new boot environment, as needed
  - Always create a new boot environment
  - Never create a new boot environment
  - Activate and reboot the boot environment
- For Oracle Solaris 8, 9, or 10
  - Activate Boot Environment and reboot on job completion
  - Synchronize existing Boot Environment before submitting a job

## Determine Your Live Upgrade Feature Requirements and Options

For Oracle Solaris 8, 9 and 10 only, determine the file system and swap requirements and the `lucreate` command options that you want to use. If you are using ZFS, create a zpool. See the Oracle Solaris documentation for more information about the requirements and command options for the Live Upgrade feature.

You can create an operational plan that includes your script, or you can enter the `lucreate` options directly in the Boot Environments profile without creating a script.

## Overview of Boot Environments Profiles and Plans

The following is a high-level overview of how to create an alternate boot environment for Oracle Solaris 10 and earlier releases.

### 1. Create an Boot Environments profile.

The profile identifies and defines how the boot environment is created and activated, including defining the target type, the options used to create the boot environment, and the activation parameters. Review the Oracle Solaris 10 Live Upgrade documentation for more details on the requirements:

- Define your file system and swap requirements.
- Determine the `lucreate` command options. You can enter the options in the Boot Environments profile, or you can create an operational profile that contains a script with the `lucreate` command and options. If you are specifying a variable boot environment name in the script passed to the operational profile, make sure the variable is called `BENAME`. If you use this as the variable name, the operational plan will pass on the BE name entered during plan execution to the `lucreate` script.
- Determine your boot environment policies

### 2. Create a deployment plan.

The Boot Environment deployment plan defines the failure policy and is associated with a single Boot Environments profile. You can add a Boot Environments profile as a task, or step, within a complex deployment plan. See Plan Management for information about complex plans.

### 3. Execute the deployment plan.

After the deployment plans are created, a user with the appropriate role and privileges can choose from a list of plans to quickly and consistently create an alternate boot environment.

### 4. Create and deploy an OS Update plan to update the inactive boot environment.

See [Update an Oracle Solaris Boot Environment](#) for the steps to create and deploy the OS Update plan.

For information about system administration tasks such as managing file systems, mounting, booting, and managing swap space, see the *Oracle Solaris System Administration Guide: Devices and File Systems* in the Oracle Solaris 10 Documentation Library.

## Create an Oracle Solaris 8, 9, or 10 Boot Environment

Oracle Solaris Live Upgrade scripts are used to create an alternate boot environment. To create a replica of your boot environment, run the script in Oracle Enterprise Manager Ops Center.

The following methods are available to create the alternate boot environment:

- Copy an existing boot environment.
- Execute a Boot Environments deployment plan.  
The deployment plan must reference an Boot Environments profile.
- Run an operational plan that contains the lucreate script.
- Upload an Oracle Solaris Live Upgrade script as Local Content in Enterprise Manager Ops Center.
  - Run an OS update job and specify a pre-action which runs the script. You can select multiple compatible targets and create an alternate boot environment for each target using the same script at the same time.
  - Create an OS profile, and then run an OS Update job. The profile enables you to define the components and the actions to be performed every time you use the profile to create an alternate boot environment.
- Run an Oracle Solaris Live Upgrade script from the command line. With this method, you must log in to each agent and then run the script to create the boot environment.

When you create the alternate boot environment with an OS Update job, you can choose to run the job immediately, or you can schedule the job to run during your maintenance window. In all methods, the new boot environment is automatically discovered and a new Boot Environments tab appears in the center pane for OS management.

This task describes how to run a New OS Update job to create the alternate boot environment. Although it is a New OS Update job, the sole purpose of the job is to create an alternate boot environment. The job uses the Live Upgrade script that you uploaded to Local Content to create a duplicate of your boot environment.

### Deployment Options for Oracle Solaris 8, 9, or 10

To create boot environments for Oracle Solaris 10, you can define the options in an Boot Environments profile or you can add a script to an operational profile. The software enables you to store the scripts and parameters and provides a couple of methods of deploying the scripts.

- As a profile
- As part of a plan
- As part of an update job

The scripts use the `lucreate` command to create an alternate boot environment. To see a complete list of options, see the Oracle Solaris 10 OS Live Upgrade `lucreate(1M)` documentation. The following are some commonly used options:

- `-m` option to create a boot environment and split a directory off to its own slice.  
To share a directory, the directory must be split off to its own slice. The directory is then a file system that can be shared with another boot environment. You can use the `lucreate` command with the `-m` option to create a boot environment and split a directory off to its own slice. But, the new file system cannot yet be shared with the original boot environment. You must run the `lucreate` command with the `-m` option again to create another boot environment. The two new boot environments can then share the directory.
- `-s` option to force a synchronization.
- `-p` specifies the ZFS pool in which a new boot environment will reside.

This option is not required if the source and target boot environments are within the same pool. This option does not support the splitting and merging of file systems in a target boot environment that is supported by the `-m` option.

Existing boot environments appear in the hierarchy in the Boot Environments tab for a global zone. You can create the boot environment with Oracle Enterprise Manager Ops Center or outside of the software.

### Create an Oracle Solaris 8, 9, or 10 Boot Environments From a Deployment Plan

You can only create a boot environment from a global zone in Oracle Solaris 10. The boot environments on Oracle Solaris non-global zones are tightly coupled with the corresponding boot environment on the global zone and cannot be managed independently.

For Oracle Solaris 10, the boot environment is created from the default alternate boot environment profile. You can override the applicable parameters in the profile.

1. Click an Oracle Solaris 10 OS global zone in the Asset tree to view the Boot Environment in the center pane.
2. Click the Boot Environment tab.

Existing boot environments for the OS appear in the center pane.

3. To create a copy, or clone, of the existing active boot environment, click the Create icon.

The plan for execution that uses the default Boot Environments profile for Oracle Solaris 10 is launched.

4. Type a unique name for the boot environment and provide a description. The text describes what the boot environment and from what source it was created. Edit the applicable parameters in the Alternate Boot Environment profile, then click Confirm.
5. When the job finishes, refresh the Boot Environment table to see the new boot environment.

### Create an Oracle Solaris 8, 9, or 10 Boot Environments from an Operational Plan

An operational profile contains a single script and can define variables. The profile is launched by an associated plan. An operational plan is associated with a specific version of an operational profile. By default, creating a profile also creates an operational plan.

You can create the boot environments using this script from a few different contexts:

- Simple BE Operational profile
- Boot Environments profile using BE Operational profile from the plan context
- Create Boot Environment from the asset context

You can save a shell script on the Enterprise Controller and download it into the plan, or you can enter the script in a text field when you create the plan. Both types of shell scripts are executed by the user. They differ in the location, either on the Enterprise Controller or on the remote Agent, and the user credentials needed to execute the profile. See [Operational Profiles and Plans](#) for more information about operational profiles and plans and the variables you can use.

1. Click Plan Management in the Navigation pane, then click Operational Profiles. The Operational Profiles appear in the center pane.

2. Click Create Operational Profile. The Create Profile - Operation page appears.
3. Type a name for the new plan and a description of its purpose or role.
4. Select an asset type from the Subtype list.
5. Click Next.
6. Select the Operation Type from the drop-down menu, either EC Shell or Remote Shell.
  - If you selected EC Shell, browse to the location of the script in the Script File field, then click Load Script.
  - If you selected Remote Shell, type your script in the Script field.
7. Enter a numeric value in the Timeout field, then select Minutes or Seconds. The default is 60 minutes.
8. (Optional) Click View System Variables to view the default variables.
9. Click Next.
10. (Optional) Specify Additional Variables. You can specify any variable you want. For example, add Alarm\_ID\$ to add the incident identifier number for easier incident management.

### **Create an Update Profile for Oracle Solaris 8, 9, or 10 Boot Environment**

You can use an Update profile to create and update a boot environment.

1. Expand Plan Management, then click Update Profiles in the Navigation pane.
2. Click New Profile in the Actions pane.
3. Provide a name and description for the profile.
4. Select Script from the Type drop-down menu.
5. Select an OS channel from the Distribution drop-down menu.
6. Select Local from the Category drop-down menu.
7. Choose the options that you want from the View and the Version drop-down menus.
8. Highlight Local RPMs in the Available Packages / Patches table, click the Apply to all applicable distributions check box.
9. Click Profile Contents and select an item, then click Create OS Update Profile.

### **Create an Oracle Solaris 8, 9, or 10 Boot Environment From an Update Profile**

You can use an Update profile to create and update a boot environment.

1. Click an Oracle Solaris 10 OS global zone in the Asset tree to view the Boot Environment in the center pane.
2. Click the Boot Environment tab.

Existing boot environments for the OS appear in the center pane.
3. To create a copy, or clone, of the existing active boot environment, click the Create icon.

The plan for execution that uses the default Boot Environments profile for Oracle Solaris 10 is launched.

4. Type a unique name for the boot environment and provide a description. The text describes what the boot environment and from what source it was created. Edit the applicable parameters in the Alternate Boot Environment profile, then click Confirm.
5. When the job finishes, refresh the Boot Environment table to see the new boot environment.

### **Create an Oracle Solaris 8, 9, or 10 Boot Environment With an OS Update Job**

Oracle Solaris Live Upgrade contains a suite of script commands. To create an alternate boot environment with Enterprise Manager Ops Center, use the `lucreate` command to write one or more Oracle Solaris Live Upgrade scripts, add the scripts to the Local Content library in Enterprise Manager Ops Center, then run an OS Update job and select the ABE options.

When you use Enterprise Manager Ops Center to create the alternate boot environment, the scripts must meet the following requirements:

- The script cannot contain parameters.
- The alternate boot environment name must be hard-coded into the script itself or otherwise be provided outside of Enterprise Manager Ops Center.
- The alternate boot environment name defined in the script must match the alternate boot environment name that you use when you run the update job to create the alternate boot environment.
- The script must return 0 on success and non-zero on failure.

For detailed instructions and examples for using the `lucreate` command to create a boot environment, see *Oracle Solaris 10 9/10 Installation Guide: Solaris Live Upgrade and Upgrade Planning* available at:

<http://www.oracle.com/technetwork/indexes/documentation/index.html>

1. Expand Libraries in the Navigation pane.
2. Click Local Content in the Solaris/Linux OS Updates library.
3. Click Upload Local Action in the Actions pane.
4. Type a name for the file.
5. Enter a brief description of the purpose of the action.
6. In the Action list, click the Pre-action type of action to run the script on the managed host before job tasks are carried out.
7. Click the name of the distribution that uses the action in the Distribution list. The Parent field shows the category, based on the type of Action.
8. Click Browse to locate and select the file.
9. Click Upload. The file is uploaded to the selected distribution.

### **To Create a Boot Environment With an OS Update Job**

1. Click the OS in the Assets section of the Navigation pane.
2. Click New Update OS Job in the Update section of the Actions pane. The New Update OS Job wizard is displayed.
3. Complete the following Job Information parameters:
  - Type a job name.

- Select Actual Run, which creates the alternate boot environment when you specify in Step 5.
  - Select the Sequential task execution order.
  - Select the Target Setting: Use the same Targets for all tasks in the job.
  - Select a Task Failure Policy:
    - Complete as much of the job as possible
    - Stop at failure and notify
  - Click the Boot Environment Type check box.
  - Click the Run ABE Pre-action Script check box.
4. (Optional) To add tasks to the job, click the Add Task icon. To edit, click the Profile and Policy fields. Click Next.
  5. Type the name of the alternate boot environment, as defined in the script. Select a script, then click Next.
  6. (Optional) Complete the Boot Environment Workflow, then click Next.
    - To synchronize the alternate boot environment with the current boot environment before the alternate boot environment is mounted, click the Sync ABE check box.
    - To edit the description to describe the state of the Boot Environment, click Modify Current BE, and add text to the Description field.
    - To edit the description to describe the state of the alternate boot environment, click Modify Alternate BE, and add text to the Description field.
    - To switch boot environments after update, click the Activate and Reboot ABE check box.
  7. Schedule the job, then click Next.
    - Run Now starts the job immediately after you click Finish in the Job Summary.
    - Start Date enables you to select a date and time to start the job.
    - On a recurring schedule enables you to run the same job on a monthly or daily scheduled time.
  8. Review the Job Summary, then click Finish to run the job as scheduled in the previous step.

When the job completes, the alternate boot environment is created and associated with the OS. To verify that the alternate boot environment is created, click the OS in the Assets pane. The Boot Environments tab appears in the center pane. Click the Boot Environments tab to display the new boot environment, as specified in the Live Upgrade script. An OS can have several associated alternate boot environments.

---

---

**Note:** The Boot Environments tab is only displayed if there is at least one alternate boot environment associated with the OS.

---

---

## Synchronize Oracle Solaris 10 Boot Environments

You can synchronize, or sync, an active Oracle Solaris 10 global zone boot environment with an inactive boot environment on the same system. Synchronizing boot



environments makes the inactive boot environment the same as the currently running boot environment.

## Related Resources

For instructions in performing actions or to learn more about the role of this feature, go to one of the following resources.

- For end-to-end examples, see the How To library at <http://www.oracle.com/pls/topic/lookup?ctx=oc121&id=howto>
- See [Operating System Updates](#) for information about patching, or updating, your operating systems.
- See [Oracle Solaris Zones](#) for information about zones and how you can use Oracle Enterprise Manager Ops Center to efficiently manage all phases of zones lifecycle.
- See [Monitoring Rules and Policies](#) for information on how monitoring rules and policies work in the software.

For in-depth information about these products, see the following Oracle documentation:

- Oracle Linux at <http://www.oracle.com/us/technologies/linux/index.html>
- Oracle Solaris 11 at <http://www.oracle.com/technetwork/documentation/solaris-11-192991.html>
- Oracle Solaris 10 at <http://www.oracle.com/technetwork/documentation/solaris-10-192992.html>
- Oracle Solaris 8 and 9 at <http://www.oracle.com/technetwork/documentation/legacy-solaris-192993.html>
- For more information about JET resources and documentation, see *Solaris 10 10/09 Installation Guide: Custom JumpStart and Advanced Installations* available at <http://www.oracle.com/technetwork/indexes/documentation/index.html>



---

---

## Operating System Updates

This chapter describes the operating system update features that are available in the software.

The following information is included:

- [Introduction to Operating System Updates](#)
- [Roles for Operating System Updates](#)
- [Actions for Operating System Updates](#)
- [Agent Managed Operating Systems](#)
- [System Catalogs](#)
- [Operating System Update Reports](#)
- [Update Policies](#)
- [Update Profiles](#)
- [Operating System Updates for Oracle Solaris 8, 9, and 10 and Linux](#)
- [Operating System Updates for Oracle Solaris 11](#)
- [Update an Oracle Solaris Boot Environment](#)
- [Operating System Updates for Microsoft Windows](#)
- [Location of Operating System Update Information in the User Interface](#)
- [Related Resources](#)

### Introduction to Operating System Updates

Oracle Enterprise Manager Ops Center reduces the complexity of updating a large number of systems, standardizes the update installation process, minimizes downtime, and enables you to choose the level of automation.

You can maintain your Oracle Solaris, Linux, and Microsoft Windows operating systems to the recommended and latest updates and perform complex update tasks in a consistent manner. For most platforms, the update features help you to perform the following tasks:

- Manage different operating system update conditions that exist for installing an update
- Identify dependencies
- Download update packages or updates from the appropriate vendor sites

- Run an update simulation to test the update in your environment
- Rollback your systems to a previous state if an update is not stable in your environment
- Maintain consistent component configuration of your systems to the latest security updates

The list of supported operating system releases and functionality is available in the *Oracle Enterprise Manager Ops Center Certified Systems Matrix Guide*.

The update features include:

- Catalogs
- Reports
- Update Profiles
- Update Policies
- Deployment Plans

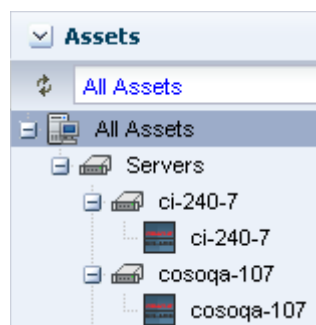
Oracle Enterprise Manager Ops Center provides one stop solution for all the requirements for updating your operating systems. You can use Update Profiles and Plans to define which components must be installed and the level of automation during the installation.

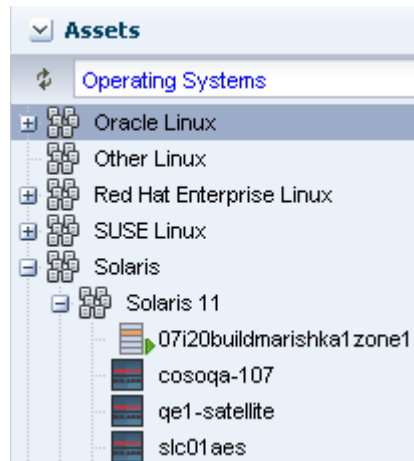
You create update jobs with operating system update profiles and policies to update an operating system. OS update profiles and policies define which updates to install, and how the update job proceeds after determining the update dependencies and user interaction. A set of system-defined update profiles is available in the UI. You can copy the profiles and edit them to create your own customized profiles.

A variety of operating system reports are available to give you insight into the operating system compliance status, the state of your operating system update levels, and provide information about the recommended updates and packages.

You can view your managed operating systems with the All Assets view or the Operating Systems view, as shown in [Figure 13-1](#) and [Figure 13-2](#).

**Figure 13-1 All Assets View**



**Figure 13–2 Operating Systems View**

## Operating System Update Requirements

The Enterprise Controller obtains information about latest updates from the Knowledge Base, Oracle Solaris 11 parent repositories on Oracle.com, and vendor sites. It requires an Internet connection to obtain the updates and packages from the various locations. In the absence of an Internet connection to the Enterprise Controller, you can get the latest updates by using a special script, called the harvester, to create local versions of the Knowledge Base and Oracle Solaris 11 Software Update Library. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about connection modes and how to use the harvester script.

The operating system update feature has the following requirements

- Agent managed – Linux and Oracle Solaris 8, 9, and 10 operating system must be agent-managed to perform most operating system update tasks. You can update Oracle Solaris 11 and Microsoft Windows with an agentlessly managed operating system. See [Agent-Managed and Agentlessly-Managed Operating Systems](#) for details and how to switch management modes.
- Access to updates – The software is designed to use a secure Internet connection to obtain operating system updates as they become available. If you cannot use an Internet connection from within your datacenter, you can run the software in disconnected mode and download the latest updates to an external storage device and use that to update the software libraries.
- Established Software Update Library – For Linux or Oracle Solaris, you must create an update library to store the update information. See [Chapter 5, "Software Libraries"](#) for information on establishing and using software update libraries.
- Compatible configuration for Oracle Solaris 11 – To update an Oracle Solaris 11 operating system, the Enterprise Controller and the Proxy Controller must be running on an Oracle Solaris 11 operating system.
- Valid update credentials – You must have update credentials for each platform vendor. You must provide a valid My Oracle Support (MOS) account for Oracle Linux and Oracle Solaris. Valid vendor credentials are required for SuSE Linux, and Red Hat Linux and Microsoft Windows. Typically, you supply the credentials when you install Oracle Enterprise Manager Ops Center. See [Authentications](#) in the *Oracle Enterprise Manager Ops Center Administration Guide* for how to add or edit your update credentials.

Manage the operating systems with an agent for the most robust feature set, including reports, monitoring, and analytics. See [Discovering and Managing Assets](#) for more about the discovery and management process. See [Agent-Managed and Agentlessly-Managed Operating Systems](#) for the differences between the two modes and how to change the agent management mode.

## Methods of Running an Update Job

You can use the following methods to run an update job:

- OS Update deployment plan that uses the update profiles and policies
- System catalogs
- Reports
- Update profile

## Options Available When Running an Update Job

You have the following options available when running an update job:

- Select update profiles and policies.
- Select different targets for each task in the job.
- Select job simulation mode. Simulating a patching job helps to estimate the time required to run the job, to know the patch dependencies and the expected job result. In the simulation mode, you can select to download the required updates.
- Failure policy to determine the action when a task fails.

## Roles for Operating System Updates

[Table 13–1](#) lists the tasks that are discussed in this section and the role required to complete the task. An administrator with the appropriate role can restrict privileges to specific targets or groups of targets. Contact your administrator when you do not have the necessary role or privilege to complete a task.

See [Asset Management](#) for details on using the discovery feature to add assets and for more information on creating user-defined groups. Contact your administrator if you do not have the necessary role or privilege to complete a task. See the *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 13–1** *Operating System Management Roles and Permissions*

Task	Role
New Update OS Job	Update Admin
Deploy or Update Software	Update Admin
Simulate an OS Update	Update Admin OR Update Sim Admin
Compare System Catalog	Update Admin
Create Catalog Snapshot	Update Admin
View and Modify Catalog	Update Admin
Update Management Credentials	Security Admin

**Table 13–1 (Cont.) Operating System Management Roles and Permissions**

Task	Role
Any Actions related to changing credentials	Security Admin
Import image	Storage Admin
Upload image	Storage Admin
Upload image	Storage Admin
Unconfigure, SCCM Configuration	Ops Center Admin
Reboot, upgrade Agent Controller	Asset Admin
Edit Tags	Asset Admin
Edit Attributes	Asset Admin

## Actions for Operating System Updates

You can manage your operating systems by installing an Agent Controller on the OS or by using SSH to perform tasks. You must have an Agent managed operating system to use the OS Update features, including the system catalogs, OS update jobs, and reports. See [Agent-Managed and Agentlessly-Managed Operating Systems](#) for more details and how to switch management modes.

After you manage your assets, you can perform the following actions:

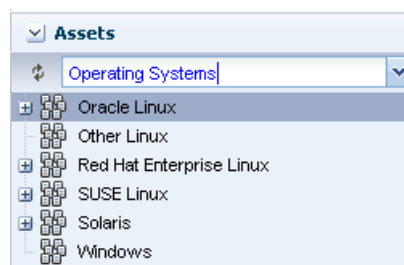
- Monitor your physical and virtual operating systems
- View OS utilization for Oracle Solaris and Linux operating systems
- Provision Oracle Solaris and Linux operating systems
- Manage Oracle Solaris boot environments

After you manage your assets, you can perform the following actions:

- Create a System Catalog
- Create an OS Report
- Update Oracle Solaris and Linux operating systems
- Update Microsoft Windows operating systems

## Location of Operating System Update Information in the User Interface

To see operating system information, expand Assets in the Navigation pane, then select the operating system. You can use the Operating Systems filter to just display the operating systems, as shown in [Figure 13–3](#).

**Figure 13–3 Operating System Filter**

## Agent Managed Operating Systems

Two management modes are available, agent managed and agentlessly managed. To perform updates to your Linux or Oracle Solaris 8, 9, or 10 operating system, the operating system must be a managed asset. Oracle Solaris 11 and Microsoft Windows do not require an agent-managed operating system.

See [Agent-Managed and Agentlessly-Managed Operating Systems](#) for details about the different management mode, how to determine the management mode, and how to change the management mode.

## System Catalogs

The software automatically takes a snapshot of the OS after executing any job on the OS, including when you discover and manage the OS. A snapshot is stored as a catalog with the time stamp and job details after every update job that you run on a system.

You can create a new catalog at any time and use it to record the state of a system. Catalogs enable you to rollback your system to any previous configuration or to create a profile that you can use to apply a consistent configuration throughout your data center.

The Catalog List contains all of the snapshots. When you create a historical catalog, the current state of the selected system is identified and stored as the previous catalog of the system. The saved previous catalog is the most recent system catalog

---

---

**Note:** You can create a historical catalog only for the current state of the system.

---

---

The catalog list always provides the listing of the most recent catalog. The software updates the catalog list whenever you update a system or create an historical catalog. You can identify the current catalog by the time stamp. You can use an historical catalog to create a profile and apply it to configure other systems.

## View and Modify a Catalog

When you are using dual boot environments for Oracle Solaris Live Upgrade (Oracle Solaris 10), the catalog displays the inventory of the active boot environment of the operating system. To view the catalog of an alternate boot environment (ABE), you must first activate the ABE from the UI, and then wait for the job to finish. The software updates the current catalog and contains the ABE catalog information and OS software components. This automatically updates the catalog of any zones.

When you have an alternate boot environment, you cannot create and compare catalogs until you activate the ABE. By default, only the catalogs of the active boot environment are compared.

## Compare System Catalogs

You can compare two managed systems or two system catalogs for differences in the installed update components. You can also compare the current system catalog and saved snapshots of the same managed system to examine the differences in the components that were installed and uninstalled after executing a job.



Use the Compare Catalogs option to change the software components of a particular operating system to that of the source system.

The following options are available when you compare catalogs:

- Differences Between Systems – Displays the difference between the source and the target systems update components. The difference appears in the Compare Catalog window.
- Tasks to Make Target Like Source – Creates the list of components that must be installed on the target system. Select Include for the components to install on the target system.

## Operating System Update Reports

To ensure that your managed systems are up-to-date, you must determine which updates (packages and patches) and actions to apply to your system. The OS update reports help you to determine the updates that are applicable to your systems and how many of the applicable updates are compliant or not compliant for the selected systems.

The OS Update reports enable you to check for new updates and update your systems. You can get a general report, or test a system for available fixes.

When you create a report, you select the criteria that are relevant to you, such as a list of hosts that have a specific patch or a list of hosts that do not have a specific patch. See [Operating System Reports](#) in [Chapter 10](#) for detailed information about these reports.

**Table 13–2 Compatibility of Reports on Operating System**

Report Name	Linux OS	Oracle Solaris 8, 9, and 10	Oracle Solaris 11	Microsoft Windows
CVE Compliance Report	Yes	Yes	Yes	No
Recommended Software Configuration Report (RSC) Report	Yes	Yes	Yes	No
Oracle Solaris Update Compliance Report	No	Yes	Yes	No
Baseline Analysis Report	No	Yes	Yes	No
Incident Compliance Report	Yes	Yes	Yes	Yes
Host Compliance Report	Yes	Yes	Yes	Yes
Profile Analysis Report	Yes	Yes	Yes	No
Package Compliance Report	Yes	Yes	Yes	No

## Update Policies

An Update policy defines the level of interaction required during an OS update job for Oracle Solaris and Linux operating systems. Policies define how to answer any questions that are raised during installation, uninstallation, or upgrade of Oracle Solaris and Linux updates.

The following system-defined policies are available in the software:

- Ask for All – The software stops the update job for each action and consults you on all action to take.
- No to All – The software denies all actions.
- Yes to All – The software confirms all actions.

---

**Note:** All operating system update plans use the "yes to all" policy by default.

---

You can create customized policies that answer differently depending on the specific OS update component. For example, when you want to review the questions and manually supply answers for patch 121288, which is part of the Oracle Solaris 10 Recommended updates from February 23, 2012, you can choose to set a specific policy for that patch, as shown in [Figure 13–4](#).

**Figure 13–4 OS Update Policies and User Defined Policy Details**

The screenshot shows the 'OS Update Policies' interface. At the top, there is a search bar and a table with the following data:

Policy Name	Description	Defined By
121288 Update Policy	Use this policy when updating 121288	User-defined Policies
Ask For All	System policy that consults the user on all actions	System-defined Policies
No To All	System policy that denies all actions	System-defined Policies
Yes To All	System policy that confirms all actions	System-defined Policies

Below the table is the 'User-defined Policy Detail' section for the '121288 Update Policy':

- Reboot Policy:** Do not ignore patches that require reboot
- Default Answer to Questions:** Ask me

There is also an 'Exceptions to the Default Answer to questions' table:

Component	Description	Attribute	Distribution	Answer
10 Recommended [Feb/23/12]	10 Recommended [Feb/23/12]		SOLARIS_10_0_SPARC	Ask me

Policy settings are hierarchical. When there is not a policy setting for a component, the policy for that component's parent applies. For example, it is possible to create a policy that allows the system to install a given component but prohibits installation of certain specific versions of that component.

---

**Note:** The policy only applies to actions that are implicitly generated by the dependency resolver. If a conflict occurs between a profile and policy, the profile overrides the policy.

The update policy is not applicable when updating Microsoft Windows operating systems.

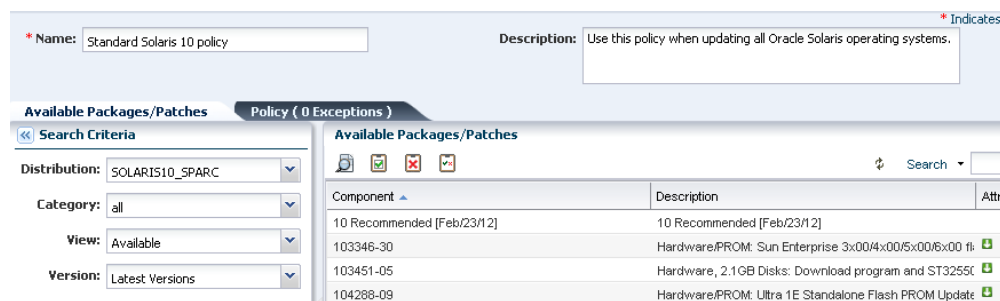
---

### Create a User-Defined Policy

1. Expand Plan Management, then click Update Policies in the Navigation pane.
2. Click Create Policy in the Actions pane.
3. Identify the policy by providing a name and description.

4. Click the Available Packages / Patches tab to view all available packages and updates. Use the search criteria to refine the list:
  - Distribution – The operating system distribution, such as Oracle Solaris 9 for SPARC, Oracle Solaris 10 for SPARC, or Oracle Solaris 10 for x86
  - Category – Package category, such as Cluster, Recommended Software Configuration, or Hardware
  - View – You can view all, available, withdrawn, modified packages/updates, or reboot
  - Version– You can view All Versions or filter for the Latest Versions

**Figure 13–5 Create OS Update Policy**



5. Select the component, then click an icon for the type of policy you want for the component, either Answer Questions Yes, Answer Questions No, or Answer Questions Ask User. To view details of the component, click the View icon.
6. Click Create OS Update Policy.

## Update Profiles

An update profile defines the component configuration of the systems that you want to manage. Update profiles specify which components are to be installed and which are prohibited, and any additional actions to be performed on an Oracle Solaris or Linux OS.

Use profiles to accomplish the following:

- Manage multiple systems in a consistent manner.
- Automate repetitive administration jobs.
- Record the requirements of your enterprise.
- Automatically configure servers and workstations.
- Manage dependencies and ensure consistency.

The profile settings Required, Not Allowed, and Upgrade affect a managed host only during the actual deployment of that profile. At any time, you can run a job that contradicts the settings of a previously used profile; therefore you must understand your system settings and requirements thoroughly.

Predefined profiles are provided to perform common system-wide checks and to automate the operating system updates. These profiles cannot be edited or deleted.

You can identify the profile type when you create the profile. The profile type is a tag that is used to filter the required profiles when you create a deployment plan. The following are profile types:

- Install – Indicates that new components are added, or installed.
- Upgrade – Indicates that existing components are upgraded.
- Script – Indicates that action scripts are executed.

---

**Note:** It is possible to create profiles that perform all of the actions for the profile type, or to tag a profile with a type inconsistent with its actions. The tag is used for filtering the required profiles in deployment plans. See [Complex Deployment Plans](#) for more information.

---

### To Create a New Profile

1. Expand Plan Management, then click Update Profiles in the Navigation pane.
2. Click Create New Profile in the Actions pane.
3. Enter a profile name and brief description of the profile.
  - a. Type a name and Description for the profile.
  - b. Select a Profile Type tag, either Upgrade, Install, or Script. This is used to categorize and filter the profiles later.
  - c. Select a distribution from the drop-down list. For example, SOLARIS10\_SPARC
  - d. You can further define the criteria by choosing a category, view, and version from the drop-down lists.

**Figure 13–6 OS Update Profile Search Criteria**

The screenshot shows a 'Search Criteria' dialog box with the following settings:

- Distribution: SOLARIS10\_SPARC
- Category: all
- View: Available
- Version: Latest Versions

**Figure 13–7 Create an OS Update Profile**

The screenshot shows the 'Create an OS Update Profile' form with the following details:

- Name:** S10 - Recommended Feb 27, 2009
- Type:** Install
- Description:** Solaris 10 SPARC recommended package from February 27, 2009

Below the form, the 'Available Packages/Patches' section shows a table of components:

Component	Description
10 Recommended [Feb/27/09]	10 Recommended [Feb/27/09]
10 Recommended [Feb/20/09]	10 Recommended [Feb/20/09]
10 Recommended [Feb/23/09]	10 Recommended [Feb/23/09]

4. Locate and select a Component from the Component tree.

5. If required, select the check box to specify that the component is added to all applicable distributions.

---

**Note:** This only applies to distributions that are active at the time the profile is created. As new distributions are activated you must edit the profile to explicitly add any components for those distributions.

---

6. Specify whether the action is Required, Upgrade, or Uninstall.

---

**Note:** Some actions might not apply. For example, a component cannot be Required if the system does not have the information about how to obtain the component.

---

7. (Optional) You can repeat the preceding actions to select multiple components for the same or different operating systems.
8. When you are finished, click Save as Named Profile. If a profile of that name exists you will be asked to confirm that it is to be replaced.

---

**Note:** You cannot replace system-defined profiles.

---

## Operating System Updates for Oracle Solaris 8, 9, and 10 and Linux

You will use a similar methodology and set of procedures to update your Linux and Oracle Solaris 8, 9, and 10 operating systems.

You can use the following update methods and options to update these operating systems:

- Use predefined or custom profiles and associated deployment plans to update a system or group of systems.
- Use a system catalog to create a simple update job without creating a profile. Use this method to apply a single patch quickly.
- Use the compliance reports output to update your OS. Use this method to make your systems compliant with newly released updates.
- Use compare catalogs to roll a system back to its previous state.

**Table 13–3** *Methods of Creating an Operating System Update Job*

Update Method	Oracle Solaris 8, 9, and 10	Linux
Create and deploy an Update Plan	Yes	Yes
Create a new Update OS Job	Yes	Yes
Create Update Profile and Policy	Yes	Yes

**Table 13–3 (Cont.) Methods of Creating an Operating System Update Job**

Update Method	Oracle Solaris 8, 9, and 10	Linux
Modify or compare a System Catalog	Yes	No
Create an Oracle Solaris Update Compliance report	Yes	No
Create a Compliance Report	Yes	No

In addition to the methods described previously, you can use Live Upgrade and alternate boot environments to update your Oracle Solaris OS with a minimum of downtime.

## Update an Operating System From a Deployment Plan

Deployment plans enable you to control how the update is performed and apply updates consistently across many systems. With this method, you can use custom or predefined profiles to perform complex update scenarios or to apply updates consistently across many systems.

You can use the following deployment plan templates to update a supported operating system:

- Software Deployment/Update – Use this plan to apply script based update profiles.
- Configure Server Hardware and Install OS – Use this plan to configure a service processor or a chassis, provision OS and update the OS.
- Configure and Install Dynamic System Domain – Use this plan to create dynamic system domains, provision and update OS on the domains.
- Install Server – Use this plan to provision and update the OS.

You will complete the following actions to use plans to update your Oracle Solaris or Linux operating system:

1. Create an OS update profile.
2. Optionally, create operational profiles that contain scripts to perform preinstall and postinstall actions.
3. Create a deployment plan.
4. Complete the plan, select the target asset, then select the Deploy/Update Software action.

The settings and values in the profiles bound to each step are defaults. You can modify the settings and values when you apply the plan. The profile settings and values can be constrained by the target systems to which the plan is applied. All update plans use "yes to all" policy.

### Operating System Update Job

Creating a new update job enables you to use custom or predefined profiles. Use this method for complex update scenarios or to apply updates consistently across many systems. You can run the OS update plan in simulate or deploy mode. In simulate mode, you can choose whether to download the updates.

The New Update OS Job option enables you to create customized update jobs. When creating a job, you define how the software performs the job, set the automation level of the job, and select a policy from the list of available policies. You can run the job in simulation mode or run the actual job. Simulation mode determines the actions and results of a job, and estimates the amount of time required to complete the job. You can use a job simulation to determine if your job can succeed based on your policy and profile responses. You can run a simulation with or without downloading updates

---

---

**Note:** To use an alternate boot environment (ABE) and run ABE pre-action scripts for Solaris OS, see the procedures in Oracle Solaris Boot Environments.

---

---

### Update an Operating System by Modifying a System Catalog

A system catalog contains a list of operating system software components that are installed on a managed system. Catalogs provide the capability to directly manipulate the installed software components on a single operating system or a group of operating systems.

Updating an operating system by modifying a system catalog provides the following advantages:

- Enables you to create a quick ad hoc job
- Provides an easy method of applying a single patch, baseline, or package
- Enables you to update an operating system without creating a profile for a one-time job

### Update From an Operating System Report Result

You can generate compliance reports for an operating system from which you can create an operating system update job.

The Oracle Solaris Update Compliance report is similar to a Recommended Software Configuration report. It uses the Oracle Solaris update patch bundles as the recommended software configurations. You can use this report to check how compliant a system is with a particular Oracle Solaris update and bring the operating system into compliance.

See [Chapter 10, "Reports"](#) for information about generating these reports. You can generate these reports for non-compliant components. The report result appears with the option to install the updates, packages, updates, and incidents.

The report results are stored in the database associated with the Enterprise Controller. The software maintains a history of the reports for analysis purposes.

From the report result, you can initiate a job to install the non-compliant component updates. The New Update OS Job wizard starts, enabling you to enter job information and to schedule the job. The required data for profiles, policies, and targets are automatically pre-populated in the job wizard.

---

---

**Note:** Updating a version of Oracle Solaris is not the same as upgrading to a new version.

---

---

For example, you can run the Oracle Solaris Update Compliance reports for Oracle Solaris update releases and bring systems into compliance with those bundles. Oracle Solaris update release bundles contain the equivalent set of updates to the

corresponding update. You can use them to bring pre-existing packages up to the same software level as the corresponding update. However, this feature will not perform a full Oracle Solaris upgrade from one release to another. The update release bundles do not contain additional packages that are in the update releases and they do not change the first line of `/etc/release` to specify an upgrade has taken place, although they do append a line at the end of `/etc/release` to specify that the update bundle is applied.

### **Use a System Catalog**

A system catalog is a list of operating system software components that are installed on a particular managed system. An initial catalog is created after the system is discovered and managed.

After an operating system is available and selected, you can view and modify the catalogs and create historical catalogs (snapshots of the system).

Modifying a catalog is an alternate way to run an operating system update job to install, uninstall, or upgrade a component. Modifying a catalog does not require an update profile to run the update job. It is a quick way of changing the component configuration of a system.

You can compare the system catalogs of two managed systems, view the summary of the comparison, and you can choose to make the target system the same as the source system.

Catalogs provide the capability to directly manipulate the installed software components on a single operating system or a group of operating systems. Alternatively, a catalog can be saved as a profile, and then an operating system update job can be run using this profile.

You can run an operating system update job, or you can use the simulate feature to run an update simulation before you apply updates.

### **Create an Update Profile From a System Catalog**

You can save the catalog of a system as a profile. Using this profile, you can create the systems with the required configuration in your data center.

## **Operating System Updates for Oracle Solaris 11**

Oracle Solaris 11 uses a different update mechanism than earlier versions of the operating system. Oracle Solaris 11 uses packages to update the operating system and any non-global zones. The packages are part of an Image Packaging System (IPS) that is integrated with the ZFS file system.

When you install Oracle Enterprise Manager Ops Center on an Oracle Solaris 11 operating system, you create a local software package repository. The repository, called the Oracle Solaris 11 Software Update Library, is either on a file system on the same system as the Enterprise Controller, or on an NFS server share that the Enterprise Controller can access. You will populate the local library with packages from the parent repository instead of the Knowledge Base.

---

---

**Note:** To update an Oracle Solaris 11 operating system, the Enterprise Controller and Proxy Controller must be running on an Oracle Solaris 11 operating system. When Oracle Enterprise Manager Ops Center is not running on Oracle Solaris 11, the Oracle Solaris 11 update actions are not available.

---

---



The ZFS integration automatically creates an alternate boot environment every time an operating system is installed or updated. You can quickly and easily create an alternate boot environment when needed, and manage existing boot environments. Using an alternate boot environment provides a safe method of testing an update before deploying it to your live environment.

## Update Oracle Solaris 11

Unlike earlier versions of Oracle Solaris, you cannot run an ad-hoc operating system update job or browse package contents for Oracle Solaris 11. The best method of updating an Oracle Solaris 11 operating system is with a deployment plan.

To upgrade the operating system to the latest version of the Oracle Solaris 11 package, choose Upgrade all components.

Before you run an update job, verify that the Oracle Solaris 11 Software Update Library contains the package, or latest version of the package, that you want to use. See [Libraries for Oracle Solaris 11](#) for more information.

You will complete the following actions to update your Oracle Solaris 11 operating system:

1. Create an Oracle Solaris 11 update profile.
2. Optionally, create operational profiles that contain scripts to perform preinstall and postinstall actions.
3. Create an Oracle Solaris 11 update plan.
4. Select the target asset, then select the Deploy/Update Software action.

All update plans use the "yes to all" policy by default. If you do not want to automate the update by answering yes to all questions, you can create one or more customized update policies.

Create an update profile to define the images to use. After you have created the profile, you can create a deployment plan and choose the update and operational profiles to perform the tasks that you want for that plan. You can copy and edit plans to create customized plans for different purposes or targets.

### Oracle Solaris 11 Update Deployment Plan

An Oracle Solaris 11 update deployment plan provides a framework of steps and actions that you can perform to update your Oracle Solaris 11 operating systems.

The Oracle Solaris 11 Update deployment plan is a multi-step plan. The Update OS step is required, all other steps are optional. You cannot add steps to this type of plan.

**Figure 13–8 Oracle Solaris 11 Deployment Template**

Solaris 11 Update		
<b>Target Type:</b> Solaris 11	<b>Version:</b> 1	
<b>Template Name:</b> Update Solaris 11 OS	<b>Release Date:</b> 03/22/2012 9:54:24 am MDT	
<b>Description:</b> Updates a Solaris 11 OS		
Deployment Template Composition		
Step	Required Input	Required Profile/Plan
Update Configuration	Not Required	Not Required
Execute Pre-Install script	profile	Operational Profile
Create a Boot Environment	profile	Boot Environment Profile
Update OS	profile	Software Update Profile
Execute PostInstall script	profile	Operational Profile
Monitoring	profile	Monitoring Policy

The Oracle Solaris 11 Update deployment plan includes the following steps:

1. Update Configuration – There is no profile attached to this step. The configuration is not required. At runtime, you can choose the type of update job, either an update simulation or an actual job.
2. Preinstall script – Optionally, you can associate an operational profile that contains a script that performs an action before you apply the update.
3. Create an alternate boot environment – You can create an alternate boot environment before the update job. This is optional.
4. Update the operating system – The profile that applies the update packages.
5. Post install script – Optionally, you can associate an operational profile that contains a script that performs an action after you apply the update.
6. Monitoring – Optionally, you can enable monitoring.

You can choose a failure policy for the plan, either to stop the update when a failure occurs, or to complete as many of the steps as possible.

## Update an Oracle Solaris Boot Environment

Updating an alternate boot environment is performed by deploying a Software Deployment / Update deployment plan and selecting the alternate boot environment as the target. Before you update an alternate boot environment, you must have a Software Deployment / Update plan. You can also update a boot environment from an Update Profile.

### Update a Boot Environment Using an Update Profile

You can create a customized update job, including the option to use an alternate boot environment (ABE) to perform a live upgrade of your Oracle Solaris 10 operating system. With Live Upgrade, you create an inactive ABE, update and patch the ABE, synchronize the ABE and BE, and then switch boot environments. When you switch boot environments, the patched and tested ABE becomes the active boot environment.

---

---

**Note:** Do not use Live Upgrade on your Enterprise Controller or Proxy Controllers. Live Upgrade does not synchronize all of the files that are required for these components.

---

---

You must run a separate update job for systems that use an ABE from those that do not use an ABE. When creating a job, you must define the following job parameters:

- Name and description of the update job.
- Alternate Boot Environment.
- Profile – Defines what updates are to be installed, uninstalled, or updated on an operating system. Select a profile from the list of predefined and customized profiles.
- Policy – Defines how a job is performed and sets the automation level of the job. Select a policy from the list of available policies. You can also create your own policies.
- Target Settings – Defines whether the target is different or similar for each task in the job.
- Actual Run – Defines whether this job is in simulation mode. You can choose to deploy the job, or to run a job simulation. A job simulation determines the actions and results of a job, and estimates how much time is required to complete the job. A job simulation also indicates whether your policy and profile responses will enable the job to succeed.
- Task Execution Order – Specifies whether the tasks is run in parallel or sequentially.
- Task Failure Policy – Specifies the action to take if a task fails.
- Targets – Select one or more target hosts for this job.

To create an ABE as part of this job, you must write at least one script that uses the `lucreate` command and then upload the script to the Local Content.

---

---

**Note:** The ABE name defined in the script must match the ABE name that you use when you run the update job to create the ABE.

---

---

Perform the following steps to update a boot environment:

1. Click Assets in the Navigation pane.
2. Expand All Assets, or use the All Assets filter to locate the Oracle Solaris 10 operating system instance.
3. Click New Update OS Job from the Actions pane. The New Update OS Job wizard is displayed. The Job Information window is displayed first.
4. Complete the following Job parameters:
  - Type a job name.
  - Select the Run Type:
    - Simulation. To download the required updates as part of the simulation, click the Download check box.
    - Actual Run.

- Select the task execution order:
  - Sequential
  - Parallel
- Choose the Target Setting:
  - Use the same Targets for all tasks in the job
  - Use different Targets for each task in the job
- Choose the Task Failure Policy:
  - Complete as much of the job as possible
  - Stop at failure and notify
- Click the ABE check box.
- (optional) To create an alternate boot environment during this job by running an ABE Pre-Action Script, click the Enable check box.

---

---

**Note:** You must have created the script and uploaded it to the Library for this option.

---

---

5. You can define the profile, policy and target for each task, or edit the profile and policy.
6. To edit the profile or policy of the default task, click the Profile or Policy cell for the task to display a drop-down menu. Select the profile or policy from the menu.
7. To add a new task, click the plus (+) icon.
  - A second row will appear. Click the Profile cell for that row to display a drop-down menu. Select the new profile that you want to add.
  - To change the policy for the new profile, click the Policy cell and select a new policy from the drop-down menu.
  - If you chose the parameter to use a different target for each task, click the Targets cell to display the Select Targets page. Select one or more target from the list of Available Items, then click Select to include the asset in the Target List. Click Add to Target List to close the page.
  - Click Next.
8. If you selected chose to create an ABE as part of the job, the Create ABE page appears.
9. When you have only one ABE, the Boot Environment Workflow page appears, go to step 10. When you have multiple alternate boot environments, the ABE Selection page appears.
  - One or more of the targets has more than one possible associated ABE. Select the ABE from the drop-down menu for each of the Targets. You can use the Select ABE field to filter for the ABE name.
  - Click Next. The Boot Environment Workflow page is displayed.
10. If you selected Simulation in the job parameters, the boot environment workflow cannot be edited. Skip to step 12.
11. If you selected Actual Run in the job parameters, you can edit the pre-actions and post-actions in the workflow.

- Pre-actions by default will unmount and then mount the ABE. To synch the ABE with the BE before mounting, click the Sync ABE check box.
  - Post-Actions by default will unmount the ABE.
    - Click Modify Current BE to edit the description of the current boot environment. You might use this to describe the state of the current BE. For example, Boot environment running Oracle Solaris 10 5/08 operating system before applying the Oracle Solaris 10 operating system September baseline.
    - Click Modify Alternate BE to edit the description of the ABE. You might use this to describe the state of the ABE. For example, Boot environment running Oracle Solaris 10 5/08 operating system after applying the Oracle Solaris 10 operating system September baseline.
  - Click Activate and Reboot ABE to switch boot environments after update.
12. Schedule the job, then click Next.
- Run Now starts the job immediately after you click Finish in the Job Summary.
  - Start Date enables you to select a date and time to start the job.
  - On a recurring schedule enables you to run the same job on a monthly or daily scheduled time.
13. Review the Job Summary, then click Finish to run the job as scheduled in the previous step.

## Operating System Updates for Microsoft Windows

You can update your managed Microsoft Windows operating systems by using the Microsoft System Center Configuration Manager (SCCM) and Windows Management Instrumentation (WMI) software.

Oracle Enterprise Manager Ops Center uses the Microsoft SCCM 2007 and WMI software to update your managed Windows operating systems. The Windows Update function depends on the SCCM's agent installed on the managed systems. You can configure SCCM to install agents on your managed Windows systems either automatically or through a manual process.

You must have access to SCCM software that is configured for software updates. The Enterprise Controller connects to the SCCM software to get the latest updates and packages. The SCCM software connects to the Microsoft web site through the Internet and downloads the metadata that is used for compliance analysis. You can connect Oracle Enterprise Manager Ops Center to the Microsoft web site to download updates that are then handled by SCCM for installation.

You do not need any authentication to access the Microsoft Web site. However, you must provide authentication information to access the SCCM server.

### Update Job

Oracle Enterprise Manager Ops Center contains the following options in an update job to maintain control and consistency across your data center:

- Groups – Help you to organize your assets in the user interface and act as targets for many types of jobs.
- Roles – Determine the tasks that you can perform on a specific piece of an asset or a group of assets.

- Reports – Enable you to run compliance reports and create update jobs from the compliance reports.

You can define the following job parameters while creating a windows update job:

- Name and Description – Identify the name of the report against which you want to create a Windows operating system update job. Provide a detailed description that clearly identifies the job in the historical record.
- Reboot behavior – Enables you to select the reboot behavior when a reboot is required after running the new update job. You can choose to reboot the system immediately following the update operation or to reboot the system at the default setting of the SCCM server.
- License Terms – Enables you to review the license terms and either accept or decline them. The License Terms window appears only when the updates in the report require you to review the License Terms.
- Schedule – Enables you to schedule when the update job runs.

## Modify the Registry

Due to some changes that Microsoft introduced for registry key ownership, you must manually modify the registry and change the ownership permissions for the Administrators group.

---

---

**Note:** You must modify the registry on a Windows Server 2008 R2. Other Windows servers, such as 2008 Server SP2, do not require you to modify the registry.

---

---

## Configure Oracle Enterprise Manager Ops Center for Updating the Windows Operating System

Oracle Enterprise Manager Ops Center uses the `j-Interop` command to access the Windows Management Instrumentation (WMI) and get Windows update information. It uses the software update capability of the Microsoft System Center Configuration Manager (SCCM) to update any managed Windows operating systems.

Before you can use the software to update your Windows systems, configure it to interact with the identified Microsoft System Center Configuration Manager (SCCM). In addition, you might need to modify the WMI registry.

To configure Oracle Enterprise Manager Ops Center to interact with the identified SCCM, you must have the following credentials:

- SCCM Server
  - Server Name
  - Domain Name
  - Site Name
  - User Name
  - Password
- SCCM Share
  - URL
  - Domain Name

- User Name
- Password

The configuration information appears in the Configuration tab of the Windows Update window.

---

**Note:** Oracle Enterprise Manager Ops Center uses the same SCCM credentials to access the SCCM server and enable the SCCM share. Use the <domain> format for the Domain Name field. Do not use the <domain>\<username> format. Entering an incorrect format for the Domain Name field returns a configuration task. In this case, unconfigure the SCCM and configure the SCCM again with the correct format for the credentials.

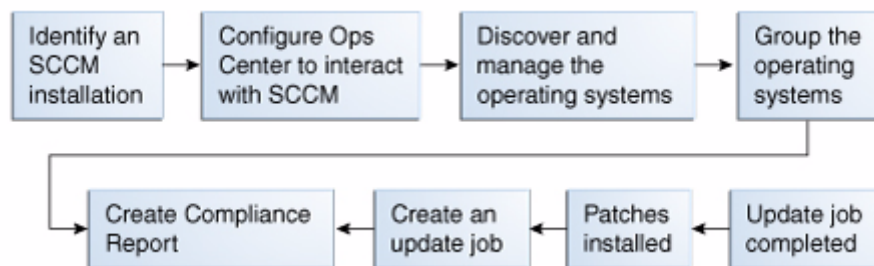
---

## Create an Update Job for the Windows Operating System

You can use the output from compliance reports to update your Windows operating system to comply with the newly released updates.

From the results of the Windows Host Compliance Report and the Windows Incident Compliance Report, you can make your systems compliant by initiating an update job for the Windows operating system.

**Figure 13–9 Process for Updating Windows Operating System**



The Create New Windows Update Job wizard enables you to create an update job. When creating a new update job, you must define the following job parameters:

- Name and Description for the new Windows software update job.
- Reboot behavior – Lets you select whether you want the system to reboot immediately following the update operation or at the default setting of the SCCM server.
- License Terms – Lets you review the license terms and either accept or decline them. The License Terms window appears only when the updates in the report require license terms that must be reviewed.
- Schedule – Lets you decide how you want to schedule the execution of the new update job.

## Related Resources

For instructions in performing actions or to learn more about the role of this feature, go to one of the following resources.

- [Chapter 5, "Software Libraries"](#) for how to add and update operating system packages and images.
- [Chapter 12, "Operating Systems"](#) for details on managing operating systems, including [Agent-Managed and Agentlessly-Managed Operating Systems](#), [Oracle Solaris Boot Environments](#), [Oracle Solaris 11 Boot Environments](#), and [Oracle Solaris 10 and Earlier Boot Environments](#).
- [Chapter 10, "Reports"](#) for details on the operating system Update reports.
- See [Chapter 14, "Oracle Solaris Zones"](#) for information about zones and how you can use Oracle Enterprise Manager Ops Center to efficiently manage all phases of zones lifecycle.
- For end-to-end examples, see the How To library at <http://www.oracle.com/pls/topic/lookup?ctx=oc121&id=howto>

For in-depth information about these products, see the following Oracle documentation:

- Oracle Linux at <http://www.oracle.com/us/technologies/linux/index.html>
- Transitioning From Oracle Solaris 10 to Oracle Solaris 11 Guide at [http://docs.oracle.com/cd/E23824\\_01/html/E24456/docinfo.html](http://docs.oracle.com/cd/E23824_01/html/E24456/docinfo.html)
- Oracle Solaris 11 Information Library at [http://docs.oracle.com/cd/E23824\\_01/index.html](http://docs.oracle.com/cd/E23824_01/index.html)
- Oracle Solaris 10 documentation at <http://www.oracle.com/technetwork/documentation/solaris-10-192992.html>
- Oracle Solaris 8 and 9 documentation at <http://www.oracle.com/technetwork/documentation/legacy-solaris-192993.html>



# Part IV

---

## Virtualize and Cloud Management

Part IV contains the following chapters:

- [Chapter 14, "Oracle Solaris Zones"](#)
- [Chapter 15, "Oracle VM Server for SPARC"](#)
- [Chapter 16, "Oracle VM Server for x86"](#)
- [Chapter 17, "Server Pools"](#)
- [Chapter 18, "Virtual Datacenters"](#)



---

---

## Oracle Solaris Zones

This chapter includes the following information:

- [Introduction to Oracle Solaris Zones](#)
- [Roles for Zone Management](#)
- [Zone Management Functions](#)
- [Prepare Your Global Zone](#)
- [Discover and Manage Existing Zones](#)
- [Outline of Zone Creation](#)
- [Zone Requirements](#)
- [Zone Configuration Parameters](#)
- [Create Zone Profile](#)
- [Deployment of Zone Plans](#)
- [Zone Management](#)
- [Zone Migration](#)
- [Recovering Zones](#)
- [Zones Server Pool](#)
- [Update Zones](#)
- [Other Functions](#)
- [Related Resources](#)

### Introduction to Oracle Solaris Zones

Oracle Solaris Zones, also known as Oracle Solaris Containers, is used to virtualize operating systems and provide an isolated and secure environment for running software applications. A zone is a virtualized operating system environment created within a single instance of the Oracle Solaris operating system.

You can think of a zone as a box with flexible, software-defined walls. One or more applications can run in this box without interacting with the rest of the system. Because zones isolate software applications or services, applications that are running in the same instance of the Oracle Solaris OS can be managed independently of each other. For example, different versions of the same application can be run in separate zones.

Zones can be used on machine that is running Oracle Solaris 10 or later release.

## Global and Non-global Zones

The global zone is the default operating system and has control over all the processes. A global zone always exists even when no other zones are configured. The global zone is used for system-wide administrative control.

Non-global zones, or simply zones, are configured inside the global zone. Zones are isolated from the physical hardware by the virtual platform layer. A zone cannot detect the existence of other zones.

## Types of Non-Global Zones

You can create different types of non-global zone for different purposes.

- Sparse Root Zone** – Contains a read/write copy of a portion of the file system that exists on the global zone. Other file systems are mounted read-only from the global zone as loop-back virtual file systems. When a sparse root zone is created, the global administrator selects which file systems to share with the sparse root zone in addition to the default read-only file systems: `/usr`, `/lib`, `/sbin`, and `/platform`. All packages that are installed on the global zone are available to the sparse root zone; a package database is created and all files in the mounted file system are shared with the zone.

---



---

**Note:** Sparse root zone is not available from Oracle Solaris 11 onwards. You can create sparse root zones only in Oracle Solaris 10.

---



---

- Whole Root Zone** – Contains a read/write copy of the entire file system that exists on the global zone. When a whole root zone is created, all packages that are installed on the global zone are available to the whole root zone; a package database is created and all files are copied onto the whole root zone for the dedicated and independent use of the zone.
- Branded Zone** – The non-global zone runs the same operating system software on the global zone. The branded zone facility is used to create non-global branded zones that contain operating environments different from that of the global zone. For example, you can install Oracle Solaris 8, 9, or 10 in a branded zone.

## Roles for Zone Management

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task. See *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 14–1 Oracle Solaris Zones Roles and Permissions**

Task	Role
Create, manage, update, and delete zones	Virtualization admin
Provision and manage virtualization host	Virtualization admin
Discover and manage virtualization hosts	Asset admin
Create and manage zone profiles and plans	Profile and plan admin

**Table 14–1 (Cont.) Oracle Solaris Zones Roles and Permissions**

Task	Role
Create and manage IPMP groups	Network admin
Create and manage Link Aggregation	Network admin
Set monitor thresholds	Asset admin

## Zone Management Functions

Oracle Enterprise Manager Ops Center provides the following solution for managing your zones environment in a data center:

- Create zones using profiles and deployment plan.
- Discover and manage existing zone environments.
- Perform zones functions such as booting, rebooting, shutting down, cloning, migrating and delete zones from the software UI.
- Manage zone configuration such as file systems, storage, and networks from the UI.
- Aggregate your NICs or create IPMP groups.
- Create zones server pool for balancing available resources and provide the infrastructure support for virtual datacenter creation.
- Use UI and native CLI interchangeably to create and manage zones.
- Complete support for managing Oracle Solaris 11 zones.
- Options to upload scripts to manage the unmanaged file system and zone dependencies.

## Prepare Your Global Zone

The global zone is the default operating system installed on a system. The OS can be Oracle Solaris 10 or 11 version. When you have provisioned systems, you can discover in Oracle Enterprise Manager Ops Center using Add Assets or find Assets option. When you want to provision the system with Oracle Solaris OS, refer to [Chapter 12, "Operating Systems"](#) for detailed procedures.

You must prepare your global zones with the required network and storage resources that need to be used for the zones. You must associate the required storage libraries with the global zone. You must also attach networks to the global zone. You can also aggregate the interfaces or create IPMP groups in the global zone before you connect them to the zones. The use of IPMP and link aggregated interfaces results in enhanced network availability for the zones.

This section covers the following topics:

- [Associate Storage Libraries](#)
- [Manage Global Zone Networks](#)
- [Create IPMP Groups](#)
- [Create Link Aggregation](#)
- [Modify and Detach Network from Global Zone](#)

## Associate Storage Libraries

You can associate or disassociate libraries from a global zone. When you associate a library with the global zone, the libraries are available to all the zones in the hierarchy of the global zone.

You can associate the following types of storage libraries to a global zone:

- Filesystem storage – NAS libraries
- Block storage – SAN and Dynamic storage libraries

For the zones, all the libraries associated with the global zone are available for association.

### To Associate a Library With the Global Zone

1. Select the global zone in the Assets tree.
2. Click Associate Libraries in the Actions pane.

The Associate Library window lists the libraries that are not associated with the global zone.

3. Select one or more libraries to add.
4. Click Associate Libraries.

A job is submitted to associate the libraries with the global zone.

When you disassociate a library from global zone:

- The libraries are disassociated from the global zone.
- The libraries are not available to new zones.
- The libraries remain associated to existing non-global zones in that global zone.

### To Disassociate Libraries From Global Zone

1. Select the global zone in the Assets tree.
2. Select the Libraries tab in the center pane.

The associated libraries with the global zone are listed.

3. Select a library from the list.

The Disassociate Library icon is enabled.

4. Click the Disassociate Library icon. The Disassociate Library window is displayed.
5. Click Disassociate Library to confirm unmounting the library.

## Manage Global Zone Networks

You can attach one or more networks to global zone using the option Attach Networks. When your networks are grouped as network domains in Oracle Enterprise Manager Ops Center, then select the domain and choose the corresponding networks to be attached.

When you assign a network to a stand-alone global zone, you must define the mode of the network, either Shared IP or Exclusive IP:

- In Shared IP mode, the global zone shares its network interface with one or more zone. You must define the network interface when you assign the network to the global zone.

- In Exclusive IP mode, a dedicated network interface is allocated to the zone. You can choose the network interface when you assign the network to a zone.

A network that is assigned as shared on a global zone can be assigned as exclusive on another global zone. For a global zone, a network has only one mode. For non-global zones, a network that is used in a shared mode for one zone cannot be used in exclusive mode for another zone.

While you attach networks to a global zone, you can deploy IP Multipathing (IPMP) to obtain better network performance or link aggregation to provide increased reliability, availability, and network performance for systems with multiple physical interfaces.

For stand-alone global zones with Oracle Solaris 10 OS, network can be attached in shared or exclusive IP mode. Whereas with Oracle Solaris 11 OS, the network is always attached in exclusive IP mode. This is because a virtual NIC or VNIC is created when the zone boots and deleted when the zone is halted.

This scenario is different for attaching networks to global zones that are in a server pool. See [Attach Networks](#) for more information about attaching networks in a zones server pool.

### IPMP Groups

Oracle Enterprise Manager Ops Center provides the option to configure one or more physical interfaces into an IP multipathing group, or IPMP group. You can configure IPMP in the global zone and extend the functionality to the non-global zone.

You can create IPMP groups on Oracle Solaris 10 and 11 OS. When you attach network in exclusive IP mode, you can create IPMP groups. Whereas, you cannot create IPMP groups for shared IP mode networks.

When you attach networks to a global zone in a shared IP mode, you can select to create an IPMP group. Define the number of members for the IPMP group. Select the NICs that are part of the IPMP group. The NICs selected are placed in the IPMP group. You can select the standby interface, and provide the test address when you want probe-based detection. For the active interface, provide the data address and choose whether failover must be enabled for the interface for uninterrupted access to the network. This is applicable for Oracle Solaris 10 OS. It is inherent in Oracle Solaris 11 OS.

When you create a zone or connect a network to a zone, the IPMP group is displayed in the NIC list. Select the IPMP group from the list to connect to the selected network. The IPMP group can be used by multiple shared IP zones.

### Link Aggregation

Several interfaces in a system can be aggregated into a single logical link. The aggregation is done as per the standard defined in IEEE802.3ad. When interfaces have been aggregated, they are treated as a single network interface. Oracle Enterprise Manager Ops Center displays the link aggregation in the list of available NICs as if it were an individual interface. You can assign a network with a link aggregation to a non-global zone, and select the link aggregation from the NIC list.

When you attach a network to a global zone, you can aggregate the physical interfaces and attach to the network. Link aggregation is available for both shared and exclusive IP network stack.

**To Attach a Network to Global Zone**

When you attach a network to a global zone, you can choose to create IPMP group or aggregate link. As per the selection, you are taken through the required steps to provide the information.

Follow the given procedure to attach a network to a stand-alone global zone:

1. Select the global zone in the Assets tree.
2. Click Attach Network in the Actions pane.

The Attach Network wizard displays.

3. Select the network domain and the corresponding networks that are not yet connected to the asset are displayed in the network list. Select a network from the list.

You can attach one or more networks to the global zone. Click Next to configure the networks.

4. For each selected network, select the following information:

- Select the IP stack as shared or exclusive.

The global zone shares the network interface with the zones that uses shared IP network. For zones that use exclusive IP network, has a dedicated network interface. For networks defined as shared, you must configure the network interfaces of the global zone. The networks defined as exclusive, you can configure the interfaces later when you connect a zone to the exclusive network.

- Select the network configuration as IPMP, Link Aggregation or None. For exclusive IP stack, only Link Aggregation network configuration is available.
  - When you select None, you are taken to Step 8 to configure the network interfaces for shared IP stack or to the summary step.
  - When you select IPMP network configuration, you are taken through the steps for IPMP configuration.
  - When you select Link Aggregation configuration, you are taken through the steps to configure the aggregation.
- Enter the number of connections for each network.

The number of connections depend on the Oracle Solaris OS version. For Oracle Solaris 10 OS, you cannot make multiple connections. For Oracle Solaris 11 OS, you can make multiple network connections.

Click Next to specify the link aggregation.

5. Provide the following information for link aggregation:

- The link aggregation name.
- Select the load balancing policy.

Click Next to configure the link aggregation.

6. Specify the following information for link aggregation:

- LACP mode and timer
- MAC address policy and the MAC address if required.

7. Specify the IPMP group details.

- IPMP group name



- Number of members of the IPMP group
- Select whether the probe-based failure detection must be enabled.

Click Next to configure the interfaces.

8. For IPMP group, provide the following information:

- The NICs that are member of the group.
- Select the interfaces that will be standby interface. You must have at least one active interface.

Click Next to specify the data addresses.

Configure the interfaces for networks that do not have network configuration:

- Specify the NIC and the IP address for the network connection.
- You can select System Allocated for the NIC and Assign by DHCP for the system to take care of the NIC and IP address allocation.
- You can select Do Not Allocate IP for the IP address, when you do not want to allocate IP address for the network connection.

9. Enter the data addresses that must be used for the active network interfaces. Also, specify whether failover must be enabled for the interface. You must have more than one interface to allow failover.

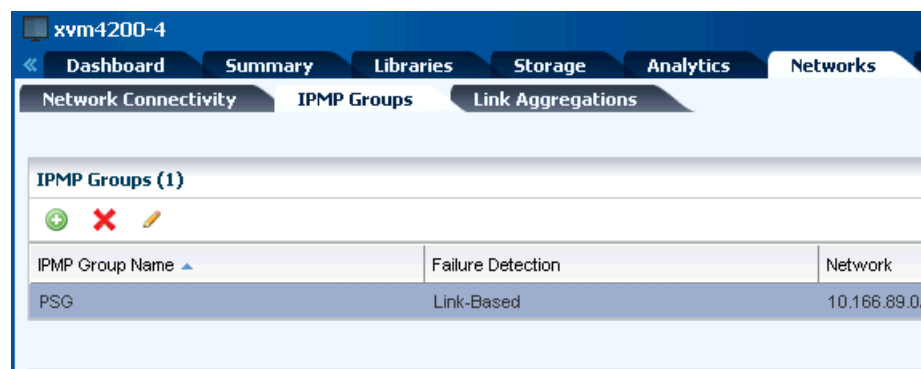
10. Review the information provided for attaching a network to the global zone and click Finish to attach the network.

You must ensure that you enter the correct information for different versions of Oracle Solaris OS. Otherwise, the attach network job fails.

## Create IPMP Groups

You can also directly create IPMP groups on the global zone without using the attach network option. From the network tabs, you have the option to create and manage the IPMP groups in the selected Oracle Solaris OS.

**Figure 14–1 IPMP Group Option**



IPMP provides physical interface failure detection, transparent network access failover, and packet load spreading for systems with multiple interfaces. Oracle Enterprise Manager Ops Center provides option to create IPMP groups. One or more interfaces can be configured into an IPMP group. The group functions like an IP interface with data addresses to send and receive network traffic. When an underlying interface in the group fails, the data addresses are redistributed among the remaining

underlying active interfaces in the group. Thus, the group maintains network connectivity despite an interface failure. With IPMP, network connectivity is always available, provided that a minimum of one interface is usable for the group. It also provides load spreading for the outbound network traffic across the network interfaces in the group.

To create an IPMP group, you must define the parameters for the group like:

- The active and the standby interfaces of the group. By default, an interface added to an IPMP group is active. You can configure as many standby interfaces as you want for the group.
- The link-based failure detection is enabled by default. You must select whether you want to enable Probe-Based failure detection. For probe-based failure detection, you must provide the test address to track the interface status.
- You must assign the data addresses for the physical interfaces in the IPMP group. Data traffic flow uses the data addresses that are hosted on the IPMP interface and flow through the active interfaces of that group.

#### **To Create an IPMP Group**

1. Select the Oracle Solaris OS in the Assets tree.
2. Select the Network tab in the center pane.
3. Select IPMP Groups subtab in the pane.  
Existing IPMP groups in the OS are listed.
4. Click the Create IPMP Group icon to create an IPMP group.  
The Create IPMP Group wizard displays.
5. Enter the following details for the IPMP group:
  - Provide a name for the IPMP group.
  - Select a network from the list.  
The list of available network interfaces in the global zone are displayed.
  - The Link-Based failure detection is always enabled by default. Select whether you want to enable Probe-Based failure detection.
  - Select the interfaces that are part of the IPMP group.

**Figure 14–2 Specify IPMP Group Details**

Click Next to specify the NIC settings.

6. When you have enabled probe-based failure detection, then enter the test address for the NICs in the group.
7. Select the interfaces that are in standby mode.  
You must have at least one active interface in the group. Click Next to specify the data address.
8. Enter the data address that will be used on the active interfaces of the group and select whether the interface has a failover.  
Click Next to view the summary.
9. Review the information and click Finish to create the IPMP group.

---

**Note:** For Oracle Solaris 11 OS, you cannot create IPMP groups. Instead, you can aggregate the links.

---

## Create Link Aggregation

You can also create link aggregation directly on the Oracle Solaris OS. To create link aggregation, you must define the following details:

- Load balancing policy
- LACP mode and timer
- MAC address policy and if required, the MAC address

### To Create a Link Aggregation

1. Select the global zone in the Assets tree.
2. Select the Network tab.
3. Select the subtab Link Aggregation.
4. Click the Create Link Aggregation icon.

The Create Link Aggregation wizard displays.

5. Enter the name of the link aggregation.  
The name starts with "aggr" by default. Append a number to make the name unique.
6. Select the NICs that will be part of the link aggregation.  
Click Next to configure the link aggregation.
7. Specify the following information for link aggregation:
  - Select the load balancing policy.
  - LACP mode and timer.
  - MAC address policy and MAC address if required.
 Click Next to view the summary.
8. Review the information and click Finish to create the link aggregation.

## Modify and Detach Network from Global Zone

You can modify the network connection that are attached to the network except for the management network. The modify and unbind network options are available in the Network tab.

**Figure 14–3 Network Options**

Network Interface Connectivity			
Network Name	VLAN ID	IP Mode	NIC
10.137.247.0/24	-	Shared	igb1
192.168.3.0/24	-	Shared	igb0

### Modify Physical Connectivity

Select the Network tab of the selected global zone in the Assets section. Click the Modify Physical Connectivity icon.

**Figure 14–4 Modify Physical Connectivity**

The screenshot shows a dialog box titled "Oracle Enterprise Manager Ops Center - Change Virtual Host Network/NIC Connection". Inside the dialog, there is a section titled "Change Network-NIC Connection on". Below this title are several input fields: "Network Name" with the value "192.168.3.0/24.1", "Physical NIC" with a dropdown menu showing "igb0", "IP Address Allocation Method" with a dropdown menu showing "Use Static IP", "IP Address" with the value "192.168.3.58", and "DHCP ID" which is currently empty. At the bottom right of the dialog, there are two buttons: "Submit" and "Cancel".

You can change the permanent IP address or change the allocation method.

---

**Note:** When the network interface is an IPMP group, you cannot modify the network interface.

---

### Unbind Network connection

When you unbind a network from a global zone, the global zone's non-global zones are also disconnected from the network. Select the global zone and click the Unbind Network icon to remove the network.

## Discover and Manage Existing Zones

When you discover a global zone which has already zones in it, then the zones are also automatically discovered and displayed on the UI. The option to deploy the agent on the global zone is inherited to the zones.

The following steps provide an outline of the procedure to discover and manage existing zones:

1. Use the option Add Assets to discover a global zone.
2. In the Add Assets wizard, select whether you want to deploy the agent on the global zone or you want agentless management.
3. All the non-global zones in the selected global zone are automatically discovered.
4. When you want to deploy the agent on the global zone, the agent is installed on all the zones that are in running state. When you want to deploy the agent for the zones in shutdown state, boot them and use the option Switch Management Access. Using this option you can change the state from agentless management to managed by agent mode.
5. You can always use the option Switch Management Access to switch between managed by agent and agentless management mode.

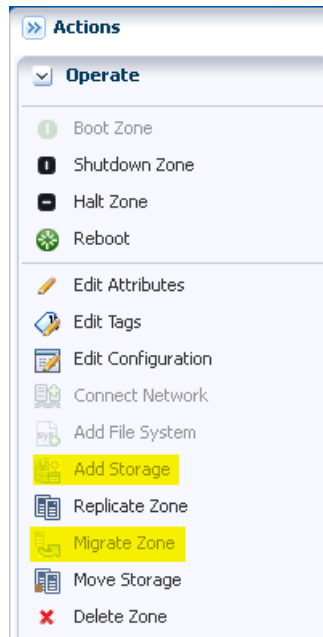
You cannot create zones on a global zone that is managed agentless. For an agentless managed zone, you can boot, shutdown, halt and delete the zone. Agent is required on the zone when you want to use the full range of OS update actions on the OS.

When you use the native CLI to create a zone, the new zone is automatically reflected in the UI. You can interchangeably use the CLI and the UI to perform zone functions. The UI reflects the change in the zone configuration and state.

You can also use other options like Find Asset to discover an asset with Service Tags. See [Chapter 2, "Asset Management"](#) for more information about discovering and managing an asset in Oracle Enterprise Manager Ops Center.

The discovered zones are displayed in the UI and the following actions are enabled for the zone.

**Figure 14–5 Enabled Actions**



You can see that the options Migrate Zone and Add Storage options are not enabled as the zone storage source is unmanaged. To have these actions enabled, you must move the storage source to managed using the option Move Storage.

Refer to the section for [Zone Management Functions](#) for more information about performing zone management operations.

## Delete or Unmanage Global Zone

When you delete or unmanage the global zone, all the non-global zones under it are also automatically unmanaged.

You need not require to unmanage the non-global zones first and then the global zone. See [Chapter 2, "Asset Management"](#) for more information about deleting an asset.

## Unmanaged Zone Storage Information

When you discover and manage existing zones, Oracle Enterprise Manager Ops Center handles the zone metadata and networks except for the zone storage. The metadata of the existing zones is stored in the local storage of the global zone. Whereas, the zone's storage is considered to be unmanaged storage source.

Even for the zones that were created using Oracle Enterprise Manager Ops Center, when you add a storage or file system manually using the native CLI, then it becomes an unmanaged storage or file system.

See [Move Storage](#) for more information about how to move the unmanaged storage to managed storage.

## Outline of Zone Creation

Using Oracle Enterprise Manager Ops Center, you create zone profiles that captures the zone configuration. Use the profile in a deployment plan to create one or more zones simultaneously. The benefit of using a profile is that you can create multiple zones with consistent configuration.

---



---

**Note:** When you create or migrate a zone using Oracle Enterprise Manager Ops Center, you cannot use Oracle Solaris Live Upgrade and an alternate boot environment (ABE) to update the zone.

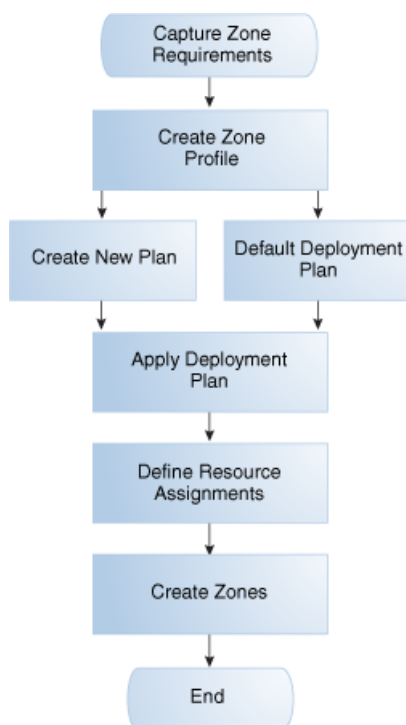
---



---

Create a zone profile that captures all the zone configurations. Then, create a deployment plan with the zone profile. The deployment plan is a single step plan which covers only the zone profile. During the application of the deployment plan, select the number of zones to create. In the plan deployment, you can correct the storage and network details as required.

**Figure 14–6 Zone Creation Process**



## Zone Requirements

Before you create a zone profile, determine the requirements for the zone. The requirements varies according to the Oracle Solaris OS version and the type of zone.

Refer to the following section according to the Oracle Solaris OS version on which you create the zones:

- [Requirements for Zones on Oracle Solaris 10 OS](#)
- [Requirements for Zones on Oracle Solaris 11 OS](#)

## Requirements for Zones on Oracle Solaris 10 OS

You can create sparse root, whole root, and branded zones on Oracle Solaris 10 OS. While creating the zone profile, select the appropriate options and provide the required resources for a successful zone creation.

### Requirements for a Whole Root Zone

A whole root zone contains a read/write copy of the global zone's file system and has the following requirements:

- Minimum size of the file system is 5 GB.
- Minimum size of the virtual disk for the storage library is 6 GB.

### Requirements for a Sparse Root Zone

A sparse root zone contains a read/write copy of a portion of the global zone's file system and shares the global zone's `/usr`, `/lib`, `/sbin`, and `/platform` directories in read-only mode. A sparse root zone has the following requirements:

- Minimum size of the file system is 1 GB.
- Minimum size of the virtual disk for the storage library is 1 GB.

### Requirements for a Branded Zone

A branded zone emulates the user environment of earlier versions of Oracle Solaris. For example, you can create a branded zone to run Oracle Solaris 8 applications on your Oracle Solaris 10 system. Use the following procedure to prepare to create a branded zone:

1. Download the images for the operating system, as shown in [Table 14-2](#).
2. Import the images into one of the software libraries associated with the global zone.

During the process of creating a branded zone, you install the images in the global zone. For instructions, see the README files in the Oracle Solaris 8 or 9 Containers bundle.

**Table 14-2 Packages for Branded Zones**

Global Zone OS	Branded Non-Global Zone
Oracle Solaris 10 10/08 OS or later:	For Oracle Solaris 8, install SUNWs8brandk from Oracle Solaris 8 Containers 1.0.1. For Oracle Solaris 9, install SUNWs9brandk from Oracle Solaris 9 Containers 1.0.1.
A version of Oracle Solaris before Oracle Solaris 10 10/08 OS:	For Oracle Solaris 8, install SUNWs8brandr and SUNWs8brandu from Oracle Solaris 8 Containers 1.0.1. For Oracle Solaris 9, install SUNWs9brandr, SUNWs9brandu, and SUNWs9brandk from Oracle Solaris 9 Containers 1.0.1.



## Requirements for Zones on Oracle Solaris 11 OS

You can install zones in Oracle Solaris 11 OS either using the IPS packages in the default Oracle Solaris 11 Package Repository or using an image of an installed system running the Oracle Solaris release.

To install zones using images, you must have an Oracle Solaris 10 image in flash archive format or from an existing Oracle Solaris 11 OS image in gzip format. See <http://www.oracle.com/technetwork/documentation/solaris-11-192991.html> for how to prepare your installed Oracle Solaris 10 or 11 systems, and create the `flar` or `gzip` image. Upload these images to the storage libraries and install branded zones in Oracle Solaris 11 OS.

### Requirements for Installing Zones Using Repository

To install zones from the repository, configure your Oracle Solaris 11 Software Update Library in the Enterprise Controller to synchronize with the Oracle Solaris 11 Package Repository. When you install from repository, the default software group, `solaris-small-server` group is used. This occupies less space. The zones are whole root type only.

### Requirements for Oracle Solaris 10 Branded Zone

You can migrate an Oracle Solaris 10 OS into an Oracle Solaris 11 environment. Create an archive of the Oracle Solaris 10 instance that you would like to migrate. In the Enterprise Controller software library, import an ISO image of Oracle Solaris 10 OS that has the same architecture of the instance to be migrated, for example, SPARC or x86 architecture. Then, import the `flar` archive with the parent as the ISO image imported previously.

For Oracle Solaris 11 OS, create an archive in the format of `gzip` file using `cpio` command. Import the archive into Enterprise Controller software library with the reference to the parent ISO image.

You can migrate only systems that have Oracle Solaris 10 10/09 or later versions. To migrate earlier versions, install the kernel patch 141444-09 (SPARC) or 141445-09 (x86/x64), or later version, on the original system.

Since zones do not nest, existing zones in the original system is detected and a warning is issued that nested zones are not usable and that the disk space can be recovered.

To use the Oracle Solaris 10 package and patch tools in your Oracle Solaris 10 Container, install patches 119254-75 (SPARC) and 119255-75 (x86/x64) on your source system before the image is created. The P2V process works without the patches, but the package and patch tools do not work properly within the `solaris10` branded zone.

To use Oracle Solaris 10 zones on your system, the `system/zones/brand/s10` package must be installed on the system running Oracle Solaris 11 OS.

## Zone Configuration Parameters

When you create a zone profile, you can provide zone configuration details such as CPU model, memory caps, priority value, network mode, and storage resources for the zone.

- **Zone name** – Specify a unique name for the zone. Do not use names that start with `global` or `SUNW`.
- **Autoboot** – Specify whether the zone must boot immediately after you create it and whenever the global zone boots.

- **Shared CPU** – A zone with a shared CPU gets its CPU resources by the number of shares you allocate to it from the resource pool, which is also used by other zones. The new zone is added to the Fair Share Scheduling automatically. You have the option to set a maximum value for the CPU resources. The CPU cap limits the amount of CPU resources that can be used by one zone. For example, a CPU cap value of 1 means 100% of a CPU.
- **Dedicated CPU** – A zone with a dedicated CPU gets exclusive use of the available CPU resources. You specify the minimum and maximum number of CPUs available to the new zone. A temporary resource pool is created and dedicated to the zone.

**Importance** – This parameter is available when you select dedicated CPU. Set the priority of the zone. Assign an importance value for the zone so that when there are not enough CPU resources to satisfy all zones, the zone with the greater importance value receives a larger share of the available CPU resources.

- **Priority of recovery** – When you enable automatic recovery for the zone, the priority of recovery value decides which zone must be migrated first during a global zone failure in a server pool. Set the priority of recovery between 0 to 100.
- **Memory Caps** – Set the maximum value for physical, swap and lock memory resources.
- **Naming Service** – Specify the name service that the zone uses to communicate with network objects. You can select the DNS, NIS, NIS+ or LDAP naming service. To specify the name service, you require the domain name and the IP address of the name server.
- **Shared IP Address or Exclusive IP Address**
  - A zone with a shared IP address uses its global zone's IP layer configuration and state. The zone has a logical network interface to the IP address.
  - A zone with an exclusive IP has its own dedicated IP layer configuration and state. The zone has its own set of network interfaces. You must configure the network interfaces using the same network configuration methods applied to all Oracle Solaris OS configurations.

For Oracle Solaris 11 OS, only exclusive IP mode is supported for the network.

## Create Zone Profile

Oracle Enterprise Manager Ops Center provides option to create profile that captures the zone configuration. Use the zone profile in a deployment plan and apply to create one or more zones simultaneously.

### To Create a Zone Profile

1. Select Plan Management section in the UI.
2. Click Oracle Solaris Zone in the Profiles and Policies tree.
3. Click Create Profile in the Actions pane.

The Create Profile – Oracle Solaris Zone wizard displays.

4. Enter a name and description for the profile identification.

Select whether you want to create a deployment plan automatically using this profile.

5. Select the OS version of the zone.

You must ensure that you apply the plan on correct target to create the zone. See [Table 14-3](#) for more information.

**Table 14-3 Oracle Solaris Zones Targets**

Zone OS Version	As	On Target
Oracle Solaris 10	Whole root zone Sparse root zone	Oracle Solaris 10
Oracle Solaris 10	Branded zone	Oracle Solaris 11
Oracle Solaris 11	Whole root zone	Oracle Solaris 11
Oracle Solaris 8	Branded zone	Oracle Solaris 10
Oracle Solaris 9	Branded zone	Oracle Solaris 10

Click Next to specify the zone identity.

6. You can create one or more zones using the profile. To identify the zones, provide a zone prefix name and a number to start the series.

Each zone created uses the prefix name appended with the number that will be incremented. For example, if the prefix name is Myzone and the number to start from is 1, then the zones will be created with names Myzone1, Myzone2, and Myzone3.

Enter the description and tags for the zones. This is common for all the zones created using this profile.

Click Next to specify the zone installation source.

7. According to the OS version selected, the page displays the following information:

- Oracle Solaris 10

Select whether you want to create whole root, sparse root, or branded zone. For branded zone, provide the following information:

- Select the architecture as x86 or SPARC
- Select the branded zone image. You must have created a flash archive image of an installed Oracle Solaris 10 OS and uploaded to the software library in Oracle Enterprise Manager Ops Center. These images are listed in the Branded Zone Image list.
- Enter the prefix for the Host ID and the starting number.
- Select the machine type as sun4u or sun4v.

- Oracle Solaris 11

You must select the installation source for installing Oracle Solaris 11 zones. You have the following options to select:

- Install from repository. You must have configured your Oracle Solaris 11 Software Update Library in Oracle Enterprise Manager Ops Center in synchronization with the Oracle Solaris 11 Package Repository. This option installs the `solaris-small-server` software group by default. This is also referred to as the whole root zone for Oracle Solaris 11 OS.
- Install from selected image. You must have created `gzip` archive image of an installed Oracle Solaris 11 OS and uploaded to software libraries in Oracle Enterprise Manager Ops Center. Select an image from the list. The `gzip` archive formats can be created using `cpio` or `zfs` command options.

- Oracle Solaris 8 and 9

You can install Oracle Solaris 8 and 9 as branded zones on Oracle Solaris 10 OS only.

Download the images of Oracle Solaris 8 or 9 and upload them to a software library. Refer to [Requirements for Zones on Oracle Solaris 10 OS](#) for more information about requirements for branded zones.

Click Next to specify the zone configuration details.

8. Specify the CPU type and memory thresholds. The CPU type can be either Shared or Dedicated. Set the memory thresholds and verify that the locked memory threshold value is less than or equal to the physical memory threshold.

You can enable automatic recovery option for the zone. Set the priority of recovery value between 0 to 100. This value decides which zone must be recovered first when the global zone fails.

Click Next to specify the zone file system.

9. The zone is created with a default root file system which is the zone path. You cannot delete this file system or change its read and write access. You can add more file systems from original zone's list of file systems. Set the size and access to the file system.

For each file system added, specify whether it is managed or unmanaged. When it is unmanaged, enter the mount point for the file system.

The Reserved size is the size of the file system that the user can reserve. The Quota size is the maximum size that the file system can utilize.

Click Next to configure the zone's storage.

10. Select the storage library for the zone and its metadata.

You can store the zone metadata in the local or NAS library only. To migrate a zone, it is required that you store the zone metadata in a NAS storage library.

All the libraries that are available in the Oracle Enterprise Manager Ops Center are listed. Select the library type and the corresponding libraries are listed. Select the library and the virtual disk for the zone. You can select library types such as NAS, SAN, Local, Local Devices, and Dynamic Storage.

---

---

**Note:** When you specify a local storage library, you cannot migrate the zone in the future.

---

---

---

---

**Caution:** An Oracle Solaris Zone running with a zone path on a NFS share is not a supported configuration. When you specify this type of storage, do not use the zone for production or non-experimental workload.

---

---

11. When the library is local or NAS storage, specify the virtual disk name and size of the disk. For SAN library, select a LUN from the available list. You cannot change the size of the LUN and the size of the local devices.

For Dynamic Storage, select the Dynamic library that is available for the discovered storage servers in Oracle Enterprise Manager Ops Center. You can select the existing LUNs or create new LUN. Select Create LUN in the drop-down

list of the column LUN/Virtual Disk Name and select the volume group. The size of the volume group is automatically displayed.

Click Next to specify the zone networks.

12. Select the networks that you want to connect to the zone. Also, specify the number of connections to the zone for each network. The actual binding of the networks takes place during deployment of a plan with this profile.

Click Next to specify the zone setup parameters.

13. Specify the following setup parameters:

- Language, time zone, terminal-type and root password for the zone.
- Provide a domain name for the NFSv4 Domain Name or accept the default value dynamic to allow the naming service that you specify in Step 14 to determine the NFSv4 domain at run time.
- Set the boot properties for the zone. You can set the zone to boot after it is created or whenever the global zone boots.
- For Oracle Solaris 10 version, you can select whether to install the agent on the zone or not. When the agent is not installed, the global zone access the zone through zlogin.

Click Next to specify the naming services.

14. Specify the naming service for the zone: DNS, NIS, NIS+ or LDAP naming service. You can also choose not to specify a naming service.

- **DNS** – Enter the domain name of the DNS server and the IP address of the DNS server. You can enter up to three IP addresses in the Name Server field. To specify additional domains to search, enter up to six domain names for the Domain Name Search List. The total length of each entry cannot exceed 250 characters.
- **NIS and NIS+** – Enter the domain name of the NIS or NIS+ server. When you know the NIS server details, choose the Specify an NIS Server option to provide the NIS server host name and its IP address. When you do not have the NIS server information, select the Find an NIS Server option.
- **LDAP** – Enter the domain name of the LDAP server. Specify the name of the LDAP Profile. Enter the IP address of the LDAP Profile Server. You can also provide the Proxy Bind Distinguished Name and Password.
- **NONE** – Select this option so that no name server is configured.

Click Next to view the summary of the selected parameters for creating a zone profile.

15. Review the information and click Finish to create the zone profile.

The zone profile is created with version 1 and a corresponding deployment plan also with version 1. Apply the deployment plan to create one or more zones of consistent configuration.

## Deployment of Zone Plans

Apply the zone deployment plans on the required number of targets. When you apply the deployment plan, you are required to provide the resource assignments for storage and network. When there are resources that are provided from the profile are not

available or not accessible, it is flagged in red and you must re-assign the resources to continue further.

Use zone deployment plans to modify the parameters such as storage, networks, and zone name. The zone deployment plan is a single step plan which collects details of the number of zones to be created. You can also create your own zone deployment plans.

### **To Create a Zone Deployment Plan**

1. In the Plan Management section, expand Deployment Plans and select Oracle Solaris Zone.
2. Click Create Plan from Template in the Actions pane.
3. Enter a name and description for the plan.
4. Select the failure policy.
5. In the Deployment Plan Steps, select the Oracle Solaris Zone profile.
6. Enter the number of zones to create.
7. Click Save to save the deployment plan.

When you modify the zone profile, you can choose to update the deployment plan with the correct version of the zone profile.

## **Apply Zone Deployment Plans**

Zone deployment allows you modify the parameters such as storage, networks, and zone name. When you apply the zone deployment plan, resource assignments that are not available is marked in red and it must be corrected.

### **To Apply Zone Deployment Plan**

1. Select the zone deployment plan and click Apply Deployment Plan in the Actions pane.
2. Select the target asset from the list and click Add to Target List.

You can add more than one asset to the list.

3. Select how to apply the plan.

You can either apply the plan with minimal interaction or override the profile values. When you select to override the profile values, you are taken through each step of the profile. Otherwise, you will be directed to provide only the required resource assignments. In this procedure the minimal interaction is taken into consideration. Click Next.

4. In the Specify Storage Step, correct the storage resources defined in the profile if required.

For example, when the selected storage libraries in the profile are not associated with the target global zone., then you must modify the storage resources accordingly.

Click Next to specify the zone networks.

5. The IP stack for the zone can be Shared or Exclusive. Select the IP stack and the network list are updated accordingly.

For Shared IP network:

- Select a network from the list.

- The address allocation method is Use Static IP only. This is fixed for shared IP networks.
- Enter the IP address. When you create more than one zone, enter the IP addresses either in the form of range, separated by comma or both. For example, 192.168.1.2 - 192.168.1.5, or 192.168.1.10, 192.168.1.210, 192.168.1.167.

For Exclusive IP network:

- Select a network from the list.
- Enter the number of times that the zone will be connected to the network. This is applicable only for exclusive IP networks.

---

**Note:** For Oracle Solaris 11 OS, you can connect to networks configured as exclusive IP stack only.

---

- Select the type of address allocation. Use static IP or DHCP allocated.
- When the allocation is static, then the IP range for the zones is proposed. The range depends on the number of zone and number of connections for each zone. You can modify the IP range as required.

Click Next to define the network resource assignment.

6. Modify zone host name and network assignment as required. You can also add or remove the network assignment to a zone.

For each network connection of the zone, the NIC and the individual IP address is displayed. Each zone's host name is also editable. Modify the zone resource assignment as required.

Click Next to schedule the job.

7. Select either to run the zone creation job now or schedule to a later time.

Click Next to view the summary.

8. Review the information provided for creating zones. Click Apply to start the zone creation tasks.

## Zpool and File System of Zones

Creating zones with Oracle Enterprise Manager Ops Center results in the following operations which run automatically in the background:

- The file systems of the zones are implemented as ZFS file systems.
- A zpool is created for each zone with the name of the zone metadata.
- The storage that is allocated to the zone is pooled in a zpool and used by all the file systems.

## Modify Zone Configuration

You can modify the configuration of a zone to change the CPU or memory resources, scheduler, and the identity of the zone. When you modify the CPU and memory configuration, you must reboot the zone for the changes to take effect.

You can modify the following properties of a zone:

- CPU Model – The CPU model can be shared or dedicated. For a shared CPU, you can modify the number of CPU shares allocated to the zone. For a dedicated CPU,

you can edit the minimum and maximum dedicated CPU numbers. You can also set the relative importance of the zone compared to other zones when contending for CPUs.

- Memory Caps – You can specify caps on various aspects of memory used by the zone. You can modify the caps set for physical, swap, and locked memory.
- Scheduler – For shared CPU model, the scheduler is assigned to Fair Share Scheduler (FSS). For a dedicated CPU model, you can set the following scheduler attributes:
  - Fair Share Scheduler (FSS)
  - Fixed Priority (FX)
  - Interactive (IA)
  - Real-time (RT)
  - Timer Sharing (TS)
- LightWeight Processes (LWP) – You can set the maximum number of LWPs simultaneously available to a zone.
  - Message IDs – Set the maximum number of message queue IDs.
  - Semaphore IDs – Set the maximum number of semaphore IDs.
  - Shared Memory IDs – Set the maximum number of shared memory IDs.
  - Shared Memory – Set the maximum amount of shared memory.
- Automatic Recovery – Set the value of priority of recovery. Zone with highest priority will be recovered first when the server fails.

### Modify Zone Attributes

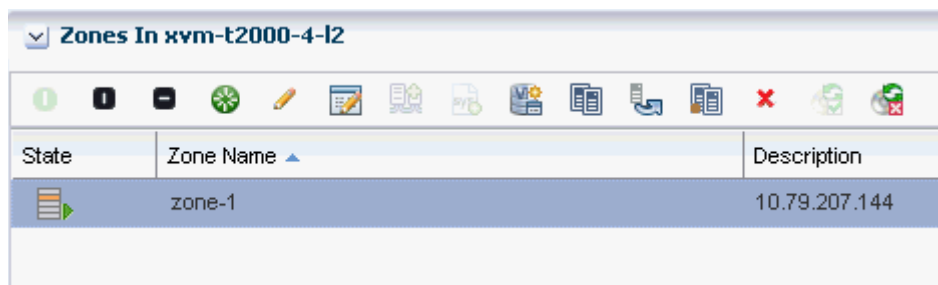
Use the option Edit Attributes to modify the description and tags of the zone. You can also add new tags to the zone.

## Zone Management

After creating the zones, you can perform various operations such as boot, reboot, shut down, and halt on the zone. Oracle Enterprise Manager Ops Center provides all these options to be performed from the UI. The UI updates the status of the zone when you perform these operations from the CLI.

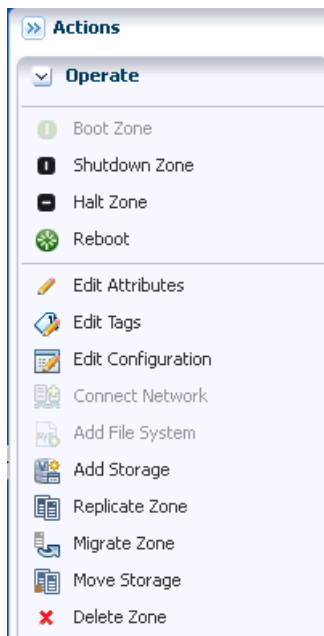
Select the global zone Summary tab in the center pane. The actions available for the zone are displayed as in [Figure 14–7](#).

**Figure 14–7 Zone Management Functions**



The same actions are available in the Actions pane when you select the zone.



**Figure 14–8 Zone Actions Pane View**

Simple zone operations that can be performed from the UI are as follows:

### Boot Zone

Booting a zone places the zone in the running state, using the current configuration. This option is enabled only when the zone is in the ready or installed state. The zone boots whenever the global zone boots depending on the autoboot properties set during zone creation.

### Reboot Zone

You can reboot a zone that is in the running state. The zone is shut down and then booted. This is different from the `zoneadm reboot` command in which the zone is first halted and then booted.

### Halt Zone

When you halt a zone, it removes both the application environment and the virtual platform of the zone. Halting a zone changes the zone's state to Installed, all processes are killed, devices are unconfigured, network interfaces are unplumbed, file systems are unmounted, and the kernel data structures are destroyed.

### Shutdown Zone

Shut a zone down in a graceful manner so that it is in a state that can be restarted.

### Delete Zone

When you delete a running zone, the zone is halted, uninstalled, then deleted from the global zone. The following changes are also made:

- Zone root file system is deleted.
- Other file systems that were added to the zone are deleted.
- Zone metadata is deleted from the storage library.
- The zpool for the zone is deleted and the storage is made available.

- Exclusive IPs that were assigned to the zone are available for re-use.

## Zone Replication

Use this option to copy an existing zone so that you can provision a new zone on the same system efficiently. The process of cloning a zone is similar to the process of creating a zone because you can accept each of the original zone's specification or change it before you create the copied zone.

### To Clone a Zone

1. Select the zone that you want to clone in the Assets tree.
2. Click Replicate Zone in the Actions pane.  
The Replicate Zone wizard displays.
3. Enter a different zone name and description for the zone.
4. Select a library from the list of libraries that are associated with the global zone to store the cloned zone's image and metadata.  
Click Next.
5. The CPU shares that are allocated in the original zone are displayed. You can edit the changes for the cloned zone.  
Click Next.
6. Accept or change the attributes of the original zone: language, timezone, terminal type, host name and root password.  
Click Next.
7. Set the boot properties for the cloned zone. You can set the properties so that the new zone boots after it is created and whenever the global zone boots.  
Click Next.
8. Configure the file systems for the cloned zone. The new zone has a default root file system which is the zone path. You cannot delete this file system or change its read and write access. You can add more file systems from original zone's list of file systems. Accept or change the size and access to the file system. The Reserved size is the size of the file system that the user can reserve. The Quota size is the maximum size that the file system can utilize.  
Click Next.  

---

---

**Note:** Make sure that the cloned zone has the same or more size for its file system than the size of the original zone's file system. When the cloned zone's file system is smaller than the original zone's file system, the clone operation cannot complete and the job fails. Do not modify the root file system of the new zone to a size less than the source zone root file system. Do not modify the system file system if it is defined in the source zone.

---

---
9. Accept or change the storage library. The library can be either a NAS storage or Fibre Channel library. When the library is NAS storage, specify the virtual disk name and size of the disk. For SAN library, select a LUN from the available list of LUNs in the library. The size of the selected LUN is displayed. You cannot change the size of the LUN.

10. The accumulated size of the storage is displayed as Currently Accumulated Storage. The required storage is displayed as Recommended Storage Size. Click the Add icon to configure more storage resources to the zone if the Currently Accumulated Storage is less than the Recommended Storage Size. When you have defined the Currently Accumulated Storage size as at least equal to the Recommended Storage size, click Next.
11. Assign at least one network to the zone. Select the zone IP type as Shared or Exclusive.
  - For Shared IP networks:
    - a. Select a network from the list of networks that use the Shared IP mode and are assigned to the global zone.
    - b. Select a NIC from the list of shared Network Interface Cards (NIC).
    - c. Specify the management interface for the NIC. When the network has a defined IP range, the Auto Allocate IP option is displayed with the zone's IP address from the range. When the network does not have a defined IP range, the Use Static IP option is displayed. Type an IP address for the zone in the Zone IP field.
  - For Exclusive IP networks
    - a. Select a network from the list of networks that are assigned to the global zone and are not used by other zones.
    - b. Select a NIC from the list of the selected network's NICs that are not bound or assigned to other networks.
    - c. Specify the management interface for the NIC. When the selected network has a defined IP range, the Auto Allocate IP option is displayed in the Management Interface and the zone's IP address is populated with an IP address from the defined range.  
  
When the network does not have a defined IP range, you must either provide the IP address or specify a DHCP server to provide one. To provide an IP address, select the Static IP option and type the IP address in the Zone IP field. To designate a DHCP server, select the Assigned by ext. DHCP option. The Zone IP field contains the Automatically Allocated value.

Click Next.
12. Click Finish to launch the job for replicating a zone.

## Add Storage to Zones

You can add storage to zones dynamically. The storage is added to the zpool that is created for the zone. You cannot delete the storage from the zpool.

The storage libraries that are associated with the global zone are available for the zone. The libraries can be of the type file system storage or block storage. The filesystem storage that can be assigned to a zone are NAS libraries. The block storage that can be assigned to a zone are SAN, and Dynamic storage libraries.

Apart from these storage libraries, you can also add the local storage on the global zone and local devices that are attached to the system.

See [Chapter 6, "Storage Libraries"](#) and [Chapter 5, "Software Libraries"](#) for more information about setting up your storage servers and software libraries.

**To Add Storage to Zones**

1. Select the zone in the Assets tree.
2. Click Add Storage in the Actions pane. As an alternative, select the Storage tab and click the Add Storage to Zone icon under Zpool and Storage.

The Add Storage to the Zone window displays.

3. Click the Add icon to add storage.

The storage libraries associated with the global zone are displayed in the Library list. The library can be a local storage, NAS, local device, Dynamic Storage, or SAN library.

4. Select a library from the list.
5. The selection of virtual disks varies according to the library selected.
  - Local and NAS library – Enter a virtual disk name and specify the size of the disk.
  - For SAN and iSCSI libraries – Select a LUN from the list. The size of the LUN displays automatically.
  - For Dynamic Storage Library – Either select a LUN from the list or create new LUN. When you create a new LUN, select the volume group from the list and specify the size of the new LUN.

The Additional Storage Specified shows the additional storage added to the zone.

6. Click Add Storage to add the specified storage to the zone.

The specified storage is added to the zone.

**Move Storage**

Some of the management and monitoring functions of the zone might be disabled depending on the managed resources of the zone. For example, the zone migration option is disabled when the zone file system is not on a shared storage.

To enable the storage management and monitoring functions of the zone, you must move the zone's existing storage to a shared storage. This provides the following options to you to manage the storage and zpools:

- Convert the local storage to shared storage so that you can migrate zones.
- Convert the experimental NFS file systems into local or shared storage.
- Combine small ZFS pools per zone into a single ZFS pool.
- Split a single ZFS pool hosting zones into ZFS pools dedicated to each zone.

Oracle Enterprise Manager Ops Center provides the option Move Storage to convert the storage of the zones. You can use this option to manage your unmanaged storage resources of the zone. However, you cannot move a managed storage to unmanaged storage. You also cannot alter the root file system of the zone.

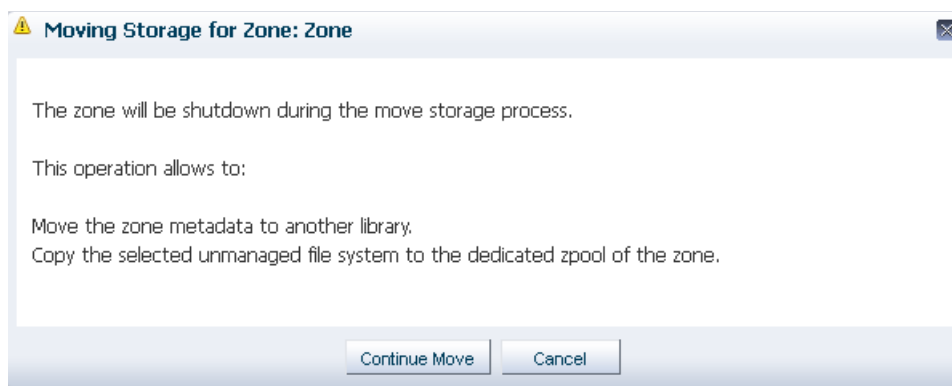
When you discover and manage existing zone environments in Oracle Enterprise Manager Ops Center, the storage is considered to be unmanaged. You can move this storage from unmanaged state to managed using this option.

**To Move Zone Storage**

1. Select the zone for which you want to move the storage.
2. Click Move Storage in the Actions pane.

A warning message displays that the zone will be shutdown during this process and you can use this option to move the zone metadata to a shared storage and unmanaged file systems to the dedicated zpool of the zone.

**Figure 14–9 Warning Message for Move Storage**



3. Click Continue Move to proceed with the move storage process.  
The Move Storage wizard displays. The zone details are displayed.
4. You can edit the description and tags of the zone.
5. If required, you can change the library in which you have stored the zone metadata. All the libraries associated with the global zone are listed. Select the library from the list.  
Click Next.
6. Select the file systems that you want to be managed.
  - When there are unmanaged file systems in the zone, you can select the option Managed and provide the Reserved and Quota size of the file system. These are added as new ZFS file systems on the existing zpool for the zone.
  - When you want to move the root file system to a managed storage, a dedicated zpool is created for the zone and you must proceed to configure the virtual disks for the file systems.
  - You can also modify the size of the file systems except for the root file system.
  - You can leave some of the unmanaged file systems as such and move only those you require.
  - You cannot move a managed storage to unmanaged storage.

Click Next to configure the virtual disk storage when you move the root file system from unmanaged to managed state.
7. Select the library and the virtual disk for the zone's storage.  
The libraries associated with the global zone are listed. You can select NAS, SAN and Dynamic Storage library from the list.  
For NAS library, provide a virtual disk name and enter the size of the disk.  
For SAN, select a LUN from the list.  
For Dynamic Storage library, either select a LUN or create new LUN from the list. When you create a new LUN, select the volume group and enter the size of the LUN.

Click Next to view the summary.

8. Review the information and click Finish to move the zone storage from unmanaged to managed.

## Add File Systems to Zones

You can add file systems to zones. The zone must be in shut down state to add file systems. The storage source for the file system can be either managed or unmanaged storage source. For unmanaged storage source, you must provide the mount point of the storage.

Provide the Reserved and Quota size for the file system. Boot the zone for the changes to take effect. The file system is added to the existing zpool of the zone.

### To Add a File System to a Zone

1. Select the zone in the Assets tree.
2. Click Add File Systems in the Actions pane.  
The Add File Systems window displays.
3. Click the Add icon to add file system.
4. Enter the file system.
5. Select whether the storage is managed or unmanaged.  
When it is not managed, enter the mount point of the storage source.
6. Enter the Reserved and Quota size for the new file system.
7. Click Add File Systems.
8. Boot the zone for the changes to take effect.

## Connect and Disconnect Networks

You can connect and disconnect networks from non-global zones. The networks attached to the corresponding global zone are available for the zones. The shared IP zones can connect to only networks that are specified for shared IP mode. The exclusive IP zones can connect to only exclusive IP networks.

Select the network and click the connect or disconnect icon as required.

## Automatic Recovery

Use the options Enable Automatic Recovery and Disable Automatic Recovery to set the recovery option of created zones. To set automatic recovery for the zone, select the option Enable Automatic Recover. Edit the zone configuration to set the priority of recovery. The zone with highest value will be recovered first. See [Recovering Zones](#) to manually recover the zones.

## Zone Migration

In Oracle Enterprise Manager Ops Center, zone migration is a cold migration because the zone is shut down, all applications are stopped, the migration occurs, and then the zone is restarted.

To enable migration action for a zone, the zone storage must be on a shared storage. When a zone uses local storage, use the [Move Storage](#) option to change the storage from local to shared.

This section describes the procedure for the following types of migration:

- Migrating an Oracle Solaris system into a new non-global zone. This is referred to as physical to virtual (P2V) conversion. See [Migrating a Physical Oracle Solaris System into a Zone](#)
- Migrating a non-global zone from one global zone to another global zone, when all components are managed by Oracle Enterprise Manager Ops Center. See [Migrating Zones to a Different Machine](#)
- Migrating a non-global zone that has dependencies that are not managed by Oracle Enterprise Manager Ops Center. This process uses a script to perform the migration. To migrate unmanaged file systems, see [Script to Migrate a Zone With Dependencies](#)

---

**Note:** When you migrate a zone, the Alternate Boot Environment (ABE) is not supported.

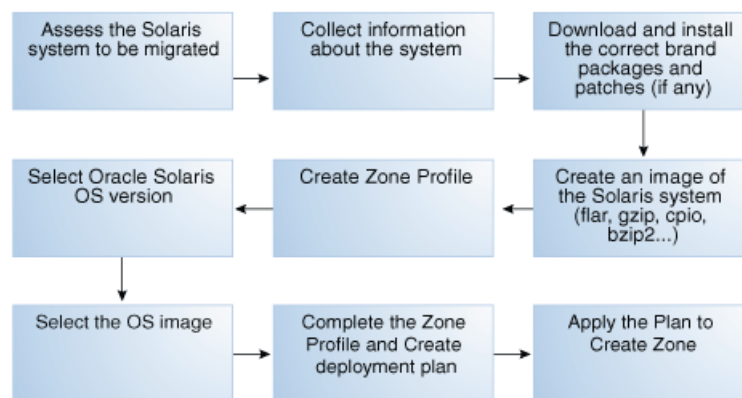
---

## Migrating a Physical Oracle Solaris System into a Zone

A "physical to virtual" (P2V) conversion moves an existing Oracle Solaris system into a new non-global zone on the target system's global zone.

Figure 13–3 diagrams the steps for a P2V conversion.

**Figure 14–10 Workflow for Migrating an Existing Oracle Solaris System Into a Zone**



Ensure the following before migrating the zone:

- Assess the system to be migrated and collect information.  
See <http://docs.oracle.com/cd/E19683-01/817-1592/> for information about collecting information about the source system.
- The system image to be installed in the non-global zone must not be newer than the target global zones's operating system release or the installation fails.
- The destination global zone must be running at least Oracle Solaris 10 8/07 OS.
- The supported branded zones are Oracle Solaris 8 and 9. For the branded zones to be supported on the destination global zone, remove the following brand packages from the global zone:

- SUNWs8brandu
- SUNWs8brandr
- SUNWs9brandu
- SUNWs9brandr

For instructions to download and install the correct brand packages, refer [http://docs.oracle.com/cd/E22645\\_01/index.html](http://docs.oracle.com/cd/E22645_01/index.html)

## Migrating Zones to a Different Machine

Using Oracle Enterprise Manager Ops Center you can migrate one or more zones simultaneously. You can either migrate the zone to an individual global zone or to a zones server pool. When you migrate zones to a server pool, the target global zone depends on the server pool placement policy.

When you migrate a zone, perform a trial run before submitting the migration job to verify that the target global zone has the correct configuration to host the non-global zones.

The target global zone must have same or later versions of the following operating system packages and patches that are installed on the non-global zone.

- Packages that deliver files under an `inherit-pkg-dir` resource
- Packages where `SUNW_PKG_ALLZONES=true`

Other packages and patches, such as those for third-party products, can be different.

When the source and target global zone do not have the same patches and packages during migration, then you can either update the zones patches and packages to match the target global zone or migrate without updating the zone patches and packages.

When the target global zone has later versions of the zone-dependent packages or patches, update those packages in the non-global zone before the migration to match the target global zone. When the target global zone supports the update on attach capability, it checks the non-global zone for packages that must be updated and only those packages are updated. The rest of the packages, and their associated patches, can vary from zone to zone.

You cannot downgrade the patches and packages of the zones to a lower version. In such cases, the update option fails.

The patches that must be backed out of the zone before the update are also listed. You must remove the patches manually and run the migration job again.

You can change the Name, Description, Tags, and NIC details of the non-global zone but, when you change other configuration, a warning message indicating that to change the zone configuration you must execute the `sys-unconfigure` command on the zone.

After you migrate a zone, you cannot use an alternate boot environment (ABE) to upgrade the zone.

### Compatible Global Zones for Migration

When you click the Migrate Zone option in the Actions pane, Oracle Enterprise Manager Ops Center checks all global zones for compatibility with the source global zone. When there are compatible global zones, the Migrate Zone wizard displays.

Otherwise, the following pop-up window displays.



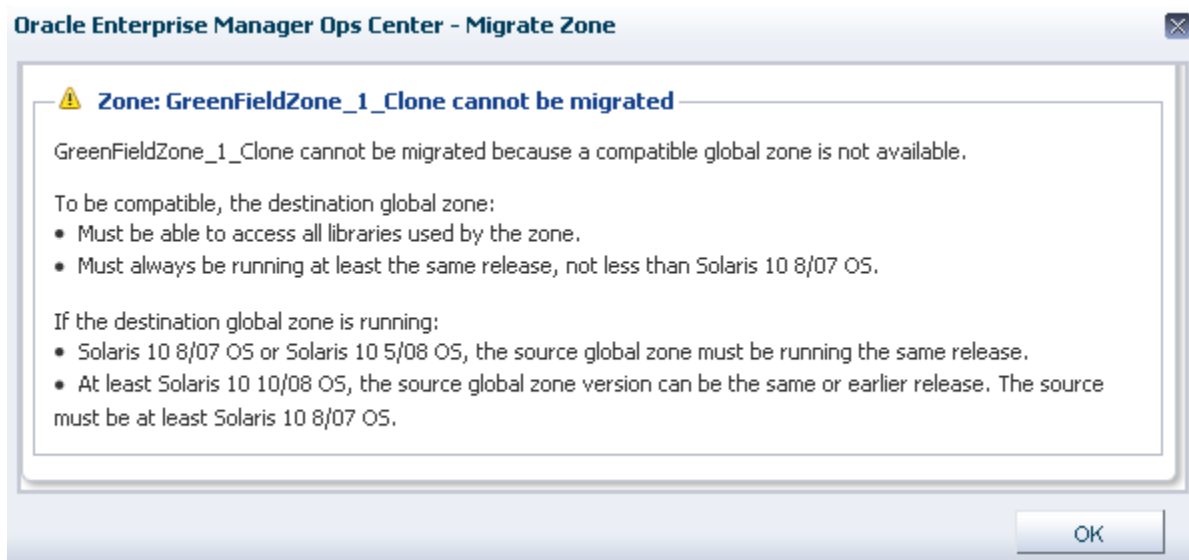
**Figure 14–11** Message Displayed When No Global Zones are Compatible

Table 14–4 shows the compatible global zones, depending on the operating system release.

**Table 14–4** Compatible Global Zones

Source Global Zone	Compatible Target Global Zone
Oracle Solaris 10 8/07	Oracle Solaris 10 8/07 Oracle Solaris 10 10/08 Oracle Solaris 10 5/09 Oracle Solaris 10 10/09 Oracle Solaris 10 9/10 Oracle Solaris 10 8/11
Oracle Solaris 10 5/08	Oracle Solaris 10 5/08 Oracle Solaris 10 10/08 Oracle Solaris 10 5/09 Oracle Solaris 10 10/09 Oracle Solaris 10 9/10 Oracle Solaris 10 8/11
Oracle Solaris 10 10/08	Oracle Solaris 10 10/08 Oracle Solaris 10 5/09 Oracle Solaris 10 10/09 Oracle Solaris 10 9/10 Oracle Solaris 10 8/11
Oracle Solaris 10 5/09	Oracle Solaris 10 5/09 Oracle Solaris 10 10/09 Oracle Solaris 10 9/10 Oracle Solaris 10 8/11

**Table 14–4 (Cont.) Compatible Global Zones**

Source Global Zone	Compatible Target Global Zone
Oracle Solaris 10 10/09	Oracle Solaris 10 10/09 Oracle Solaris 10 9/10 Oracle Solaris 10 8/11
Oracle Solaris 10 9/10	Oracle Solaris 10 9/10 Oracle Solaris 10 8/11
Oracle Solaris 10 8/11	Oracle Solaris 10 8/11
Oracle Solaris 11	Oracle Solaris 11 Oracle Solaris 11 Update 1
Oracle Solaris 11 Update 1	Oracle Solaris 11 Update 1

Verify the following conditions

- The source and target global zones are compatible.
- The source and target global zones have access to all the libraries associated with the non-global zone.
- The non-global zone's metadata is not stored in the source global zone's local library.
- The non-global zone's data is not stored in the source global zone's local library. The zone must use a shared storage library.
- The non-global zone is in the running state.
- For a server pool, it must have at least one compatible global zone for migration.
- When you migrate the zone, a warning message indicates that when you change the zone configuration except for Name, Description, Tags, and NIC details, you must execute the `sys-unconfigure` command on the zone. Also, when the NIC names are changed for a zone that uses exclusive IP mode, the `/etc/hostname.itf` and `/etc/dhcp.itf` file are renamed accordingly.

When the target global zone does not support backout on attach capability, you must remove or downgrade the patches and packages manually before you can continue with the migration. Create an update profile that includes the patches that must be removed. Run an update job with this update profile. Repeat the migration job on the zone after the removal of the patches and packages.

### To Migrate a Zone

1. Select the zone in the Assets tree.
2. Click Migrate Zone in the Actions pane.

A warning message indicating that when you change the zone configuration except for Name, Description, Tags, and NIC details, you must execute the `sys-unconfigure` command on the zone. Also, when the NIC names are changed for a zone that uses exclusive IP mode, the `/etc/hostname.itf` and `/etc/dhcp.itf` file are renamed accordingly.

3. Click Continue Migration.  
The Migrate Zone wizard displays.
4. Select an individual global zone or server pool as the target.

The compatible global zones list the number of zones that are already running, total CPUs, and available dedicated CPUs. The server pools list the average usage of CPU and memory.

Click Next. The zone migration test starts.

5. Review the migration test result. Select an update option to continue the migration on the target global zone or server pool:
  - Update the patches and packages of the zone to match the target and then migrate the zone.
  - Migrate the zone without updating its patches and packages.

Click Save Test Result As to save the migration test result. When you want to change the target, click Previous and select another target to run the migration test.

Click Next to review the zone identification.

6. When the zone name already exists in the target global zone, you must change the zone name.

Click Next to specify the zone setup.

7. Select the language, timezone, and terminal type for the zone. The host name is the zone name as defined.

The dynamic value for NFSv4 domain name enables the domain name to be derived dynamically from the naming service configuration. To hard code the value for NFSv4 domain, provide a domain name.

Leave the password fields empty to use the existing password. Click Next to define the network interfaces.

8. You must have at least one network interface for the migration to continue. The network interfaces that are not accessible to the target global zone are displayed in yellow. Specify a new network interface for the inaccessible networks or select Do Not Connect to that network.
  - a. Select the network which is marked in yellow color. The network interface details are displayed under Network Interface.
  - b. Select a new network interface from the Network list or select Do Not Connect. The selected network can be either shared or dedicated. Enter the required network interface information for the selected network.

Click Next to specify the naming service.

9. Specify the naming service for the zone: DNS, NIS, NIS+ or LDAP naming service. You can also choose not to specify a naming service.
  - **DNS** – Enter the domain name of the DNS server and the IP address of the DNS server. You can enter up to three IP addresses in the Name Server field. To specify additional domains to search, enter up to six domain names for the Domain Name Search List. The total length of each entry cannot exceed 250 characters.
  - **NIS and NIS+** – Enter the domain name of the NIS or NIS+ server. When you know the NIS server details, choose the Specify an NIS Server option to provide the NIS server host name and its IP address. When you do not have the NIS server information, select the Find an NIS Server option.

- **LDAP** – Enter the domain name of the LDAP server. Specify the name of the LDAP Profile. Enter the IP address of the LDAP Profile Server. You can also provide the Proxy Bind Distinguished Name and Password.
- **NONE** – Select this option so that no name server is configured.

Click Next.

10. Review the summary of the migration job. When there are no patches and packages to be backed out, continue with the migration. When there are patches or patches that must be removed, a warning is displayed.
  - When the target global zone supports backout on attach capability, a warning is displayed that the a list of patches have been removed or downgraded.
  - When the target global zone does not support backout on attach, the patches and packages on the zone must be removed or downgraded manually so that the source zone matches the destination global zone. Cancel the migration or select a new target global zone.
11. Click Finish to submit the migration job.

### To Migrate Multiple Zones

1. Select the global zone from which you want to migrate the zones.
2. Click Migrate Zones in the Actions pane.

The Migrate Zones wizard displays. The list includes the zones running in the global zone.

3. Select one or more zones from the list. Click Next.
4. Select an individual global zone or server pool to which you can migrate the zones.

The table displays the list of eligible global zones and server pool to which you can migrate the zones. The target global zone in the server pool depends on the server pool placement policy.

5. Select an update option to continue with migration.

The source and the target global zones might not be in the same patch level. Either you can select to update the patches and packages of zone to match the target global zone or continue migration without updating the zone.

6. Review the details and click Finish to migrate the zones.

## Script to Migrate a Zone With Dependencies

You can migrate zones even when the zone has dependencies that are not managed by Oracle Enterprise Manager Ops Center, for example, when the zone uses storage that is not part of the zpool. You can use scripts to extend the zone migration feature to include the migration of the dependencies such as storage or other resources that is not managed by Oracle Enterprise Manager Ops Center.

You can lose the additional unmanaged file systems of a zone during migration. To avoid this, use this script to migrate the file systems.

You can also develop your own scripts to migrate the dependencies and place it on the source and target global zone before migration.

The script for migrating the dependencies is executed in the following way:

- The migration job checks for a script placed on both the source and target global zones. The migration job is aborted when the script is found only on one of the global zone.
- When you create zones server pool, ensure that you upload the script to handle the unmanaged storage. The script is placed in all the global zones in the server pool and thus the migration of zone dependencies are taken care.
- The job checks whether the script has zero on exit. A non-zero exit is a failure and the migration job fails.
- The script is called on the global zone six times when the migration job is executed.

**Table 14-5 Script Call to Environmental Variables**

Call to the Script	Environmental Variables
On the source global zone, to verify the script existence and user dependencies	OEMOC_ZONENAME=source zonename OEMOC_PHASE=VERIFY OEMOC_OPERATION=MIGRATION
On the target global zone, to verify the script existence and user dependencies	OEMOC_ZONENAME=destination zonename OEMOC_PHASE=VERIFY OEMOC_OPERATION=MIGRATION
On the source global zone, before the zone is shutdown	OEMOC_ZONENAME=source zonename OEMOC_PHASE=PREOPERATION_RUNNING OEMOC_OPERATION=MIGRATION
On the source global zone, after the zone is shutdown.	OEMOC_ZONENAME=source zonename OEMOC_PHASE=PREOPERATION_NOTRUNNING OEMOC_OPERATION=MIGRATION
On the target global zone, before the zone is started.	OEMOC_ZONENAME=source zonename OEMOC_PHASE=POSTOPERATION_NOTRUNNING OEMOC_OPERATION=MIGRATION
On the target global zone, after the zone is started	OEMOC_ZONENAME=source zonename OEMOC_PHASE=POSTOPERATION_RUNNING OEMOC_OPERATION=MIGRATION

During rollback phase, the same sequence is executed in reverse order. The environment variables values change accordingly:

- PREOPERATION becomes PREROLLBACK
- POSTOPERATION becomes POSTROLLBACK

## Script Requirements

The script must be executable and follow these conventions:

- Good error checking and clean-up within the script
- Standard exit code conventions
- Non-zero exit indicates that an error has occurred
- Informational messages are in stdout

- Error messages are in stderr
- The script must be named as `guest-operations` and placed in the `/var/opt/sun/oc/public` directory on both the source and target global zone.

See the [Sample Script](#) for migrating the additional inherited file systems of an adopted zone. The sample script is based on the assumption that `/opt/` file system is the additional inherited file system. The script re-configures `/opt/` file system on the target global zone before rebooting the zone. The script reconfigures the user-inherited file systems during `POSTOPERATION_NOTRUNNING` phase

#### **Example 14–1 Sample Script**

```
#!/bin/sh

do_migration_action() {

    echo "executing migration action for zone ${OEMOC_ZONENAME}"

    if [ ${OEMOC_PHASE} != "POSTOPERATION_NOTRUNNING" ]; then
        exit 0
    fi

    #
    # for migration action, before starting the zone on the target GZ
    # add to /opt inherited filesystem.

    /usr/sbin/zoneadm -z ${OEMOC_ZONENAME} detach >/dev/null 2>&1
    if [ $? -ne 0 ] ;then
        echo "unable to detach ${OEMOC_ZONENAME}"
        exit 1
    fi

    echo "add inherit-pkg-dir" >/tmp/tmp-$$ .txt
    echo "set dir=/opt" >>/tmp/tmp-$$ .txt
    echo "end" >>/tmp/tmp-$$ .txt

    /usr/sbin/zonecfg -z ${OEMOC_ZONENAME} -f /tmp/tmp-$$ .txt >/dev/null 2>&1
    if [ $? -ne 0 ] ;then
        echo "unable to add inherit filesystem for ${OEMOC_ZONENAME}"
        exit 1
    fi

    /usr/sbin/zoneadm -z ${OEMOC_ZONENAME} attach -u >/dev/null 2>&1
    if [ $? -ne 0 ] ;then
        echo "unable to attach ${OEMOC_ZONENAME}"
        exit 1
    fi
}

echo ${OEMOC_ZONENAME}
echo ${OEMOC_PHASE}
echo ${OEMOC_OPERATION}

if [ ${OEMOC_OPERATION} = "MIGRATION" ] ;then
    do_migration_action
fi
exit 0
```

## Recovering Zones

When the global zone crashes or must be halted, its non-global zones can be migrated to another global zone. However, this zone recovery procedure is not the same as zone migration because Oracle Enterprise Manager Ops Center cannot get access to the information in the global zone and therefore cannot perform compatibility checks. The procedure to move non-global zones from the source global zone to the target global zone is a forced attachment of the non-global zone.

The zone recovery procedure uses the Command Line Interface for the Oracle Enterprise Manager Ops Center.

See the [Chapter 19, "Command Line Interface"](#) for instructions on getting access to the CLI and the available CLI commands.

### Before You Begin

- Verify that the zone metadata is on the NAS storage library.
- Verify that both the source and target global zones have the same network connectivity.
- Verify that the source and the target global zones have the shared storage.
- Verify that the target global zone has access to the same libraries associated with the non-global zone.
- Verify that the non-global zone's metadata and operational data is not stored in a local library.
- Verify that JDK version 6 is used. In the Enterprise Controller command prompt, enter the following command:

```
export JAVA_HOME=/usr/jdk/latest
```

### To Recover Zones

1. Connect to the Oracle Enterprise Manager Ops Center CLI using the following command:

```
/opt/SUNWoccli/bin/oc
```

2. Connect to the local Enterprise Controller.

```
xvmSh > connect
```

```
localhost >
```

3. Enter the virtualization mode.

```
localhost > virtualization
localhost [virtualization] >
```

4. List the available global zones.

```
localhost [virtualization] >list_hosts
```

Name	Type	Health	Reachable
gzhost36	zone	OK	False
com.sun.hss.domain:type=xVMserver,name=NORM-NORM-localhost			

```
gzhost44          zone          OK          True
com.sun.hss.domain:type=xVMServer,name=NORM-NORM-localhost-4
```

- List the zones that are running in the source global zone. For example, when the source global zone is gzhost36, then enter the following command.

---



---

**Note:** Do not use the user-friendly name of the zone in the commands.

---



---

```
localhost [virtualization] >list_hosts -C
com.sun.hss.domain:type=xVMServer,name=NORM-NORM-localhost
```

Name ObjectName	Type	State	Migratable
--------------------	------	-------	------------

```
-----
test          ZONE          RUNNING      True
com.sun.hss.domain:type=Server,name=NORM-07e91405-8313-43ec-9671-dc320989866e
```

- Select the destination global zone and start the zone on it. For example, when the destination global zone is gzhost44, execute then execute the following command to start the test zone on it.

```
localhost [virtualization] >startup -Z <source global zone> -D <target global zone>
```

```
localhost [virtualization] >startup -Z
com.sun.hss.domain:type=Server,name=NORM-07e91405-8313-43ec-9671-dc320989866e
-D com.sun.hss.domain:type=xVMServer,name=NORM-NORM-localhost-4
```

```
submitted job : <Ecname>-1.17
```

A job is submitted. You can view the status of the job in the Jobs pane.

After the zone is migrated to the target global zone, the zone is a managed zone of the target global zone. The zone might continue to be displayed under source global zone. This is because the status of the source global zone is not updated. After the source global zone is rebooted, the zone does not appear as one of its managed zones.

## Zones Server Pool

You can create server pool for zones in Oracle Enterprise Manager Ops Center. Pooling your virtualization hosts provides the capability for load balancing the virtualization servers, high availability and minimize power consumption.

All the information about creating and managing zones server pools are described in [Chapter 17, "Server Pools"](#).

## Update Zones

Oracle Enterprise Manager Ops Center enables you to update the global and non-global zones. You can also patch zones that are running on a supported configuration. The installation of the patches on the zones depend on the package parameters and the attribute set for the patch commands. This section describes the parameters for installation of the packages and patches. The concepts involved in updating global and non-global zones, and the procedures to update the zones are described in this section.



---



---

**Note:** When you use Oracle Solaris Live Upgrade to update the OS in a zone, you cannot use Oracle Enterprise Manager Ops Center to manage the zone. Alternate Boot Environment (ABE) is not supported for zones that were created using Oracle Enterprise Manager Ops Center.

---



---

## Installing Packages and Patches on Zones

A patch is a collection of files and directories that replace existing files and directories that are preventing proper execution of the software.

You can install packages and patches on a zone. The `patchadd` and `pkgadd` commands operate in the background to install a patch and package respectively. However, the installation of packages on zones also depends on the parameters `SUNW_PKG_ALLZONES`, `SUNW_PKG_HOLLOW`, and `SUNW_PKG_THISZONE`. These parameters control whether a package can be installed on global zones or non-global zones. The actions for the parameters are as follows:

- **SUNW\_PKG\_ALLZONES** – If the value is true, the package is installed on all zones, both global and non-global.
- **SUNW\_PKG\_HOLLOW** – If the value is true, the package information is propagated to the non-global zones, but the package is not installed.
- **SUNW\_PKG\_THISZONE** – If the value is true, the package is installed only in that zone.

## Configuring `patchadd` and `pkgadd` Commands

In Oracle Enterprise Manager Ops Center, the `patchadd`, `pkgadd`, `patchrm`, and `pkgrm` commands are implemented without the `-G` switch by default. To install updates or packages only on the current zone, enable the `-G` switch by editing the `.uce.rc` file.

---



---

**Note:** There is a `uce.rc` file and a `.uce.rc` file. The `uce.rc` file is the default file and must not be edited. Verify that you are editing the `.uce.rc` file.

---



---

## Editing the `.uce.rc` File

1. Open the `.uce.rc` file in the `/SUNWuce/agent/bin` directory in the managed system.
2. Add the following lines to the `.uce.rc` file:
 

```
( all ) (invisible.__is_patchadd_g_specified, false)
( all ) (invisible.__is_patchremove_g_specified, false)
( all ) ( invisible.__is_pkgadd_g_specified, false)
```
3. Set the `-G` parameter to true for the action that you want to perform.
4. Save and close the file.
5. For this change to take effect, restart the services using the following commands:
 

```
svcadm disable -s update-agent
svcadm enable -s update-agent
```

## Updating a Global Zone

In Oracle Enterprise Manager Ops Center, when a package or patch is installed, the `patchadd` and `pkgadd` commands are implemented in the background as shown in the following example:

```
patchadd <patchid>
pkgadd <pkgname>
```

You can change the way that these commands are implemented by enabling the `-G` switch. You can enable the `-G` switch to cause the patch or package to be installed to the target zone only if the package parameter `SUNW_PKG_THISZONE` is set to true. See [Installing Packages and Patches on Zones](#) for information about configuring the `patchadd` and `pkgadd` commands on the managed systems.

See the following scenarios when you are updating a global zone. The result for each scenario determines whether the update job is successful, depending on the package information.

**Table 14–6** Updating a Global Zone Scenarios

SUNW_PKG_ALLZONES	SUNW_PKG_THISZONE	SUNW_PKG_HOLLOW	Impact	Impact with -G Configuration
False	False	False	The package will be installed on the global zone, and all the non-global zones	The package is installed only on the global zone.
True	False	False	The package is installed on the global zone and all the non-global zones.	The <code>-G</code> switch cannot override the <code>SUNW_PKG_ALLZONES</code> parameter, and the package is installed on all the zones.
True	False	True	The package is installed on the global zone and the package information is made available on all the non-global zones.	The <code>-G</code> switch cannot override the <code>SUNW_PKG_ALLZONES</code> parameter, and the package is installed on all the zones.
False	True	False	The package is installed only on the global zone.	The package is installed only on the global zone.

Patches are sets of updates to packages. When you install a patch, the patch is installed on the global zone and the non-global zones, depending on the package parameters as shown in the previous table.

---

**Note:** Use caution while enabling the `-G` option on a host with sparse zones. Packages that are inherited from the global zone that are not `SUNW_ALL_ZONES` cannot be patched within a sparse zone.

---

## Updating Non-Global Zones

As a virtualization administrator, you can install packages and patches on non-global zones. The `patchadd` and `pkgadd` command must be used without options. Do not configure the `-G` switch to the commands while updating the non-global zones.

See the following scenarios when you are updating a non-global zone. The results of each scenario determine whether the update job is successful, depending on the package information.

---



---

**Note:** The `-G` switch does not have effect on installing packages or patches in a non-global zone.

---



---

**Table 14-7** *Updating Non-Global Zones Scenarios*

<b>SUNW_PKG_ALLZONES</b>	<b>SUNW_PKG_THISZONE</b>	<b>SUNW_PKG_HOLLOW</b>	<b>Impact</b>
False	False	False	The package is installed only on the target non-global zone.
True	False	False	The package installation fails.
True	False	True	The package installation fails.
False	True	False	The package is installed only on the target non-global zone.

---



---

**Note:** When the patch is installed only on the non-global zone, ensure that `autoboot` property is set to `true` for the zone. Otherwise, single user mode patches fail to apply as the zone does not come up after the reboot.

---



---

Patches are sets of packages that must be installed. When one of the packages has the `SUNW_PKG_ALLZONES` parameter set to `true`, then the patch installation fails. For a successful patch installation, ensure that none of the packages have `SUNW_PKG_ALLZONES` parameter set to `true`.

---



---

**Note:** Packages that deliver to read-only inherit directories do not install on sparse root zones. These packages must be installed from the global zone with the `-G` switch disabled. When a package has the parameter `SUNW_PKG_THISZONE=true`, it does not appear as installed from the sparse zone and the software might not function correctly. In this case, a whole root zone must be used. Packages with `SUNW_PKG_THISZONE=true` must not deliver to read-only inherit directories.

---



---

## Zone Parallel Patching

The number of zones that can be patched in parallel when you patch a global zone can be viewed from the Summary page of a global zone. When the agent is installed on the Oracle Solaris OS, the number of zones that can be patched in parallel is calculated as 1.5 times the number of CPU cores in the server. For example, if you have a 2 CPU core machine, then the number of zones that can be patched in parallel are 3. This is set and displayed on the UI.

Oracle Solaris 10 and 11 OS version displays this information in the Summary page. When the update capability is not enabled on the OS, then the zone parallel patching is also not enabled.

## Other Functions

You can refer to the following chapters in this guide for other operations that are common for many resources:

- See [Chapter 6, "Storage Libraries"](#) for setting up your storage resources.  
See [Chapter 7, "Networks"](#) for setting up your network infrastructure.
- See [Chapter 8, "Plans and Profiles"](#) for managing your zone profiles and deployment plans.
- See [Chapter 12, "Operating Systems"](#) for monitoring your resources and setting up boot environments.  
See [Chapter 2, "Asset Management"](#) for managing your discoveries and registering your assets.  
See [Chapter 17, "Server Pools"](#) for creating and managing zones server pools.

## Related Resources

For instructions in performing actions or to learn more about the role of this feature, go to one of the following resources:

- [Chapter 17, "Server Pools"](#)
- [Chapter 7, "Networks"](#)
- [Chapter 6, "Storage Libraries"](#)
- *Oracle Enterprise Manager Ops Center Administration Guide*
- See <http://docs.oracle.com/cd/E19044-01/sol.containers/817-1592/> for Oracle Solaris Resource Management and Oracle Solaris Zones documentation.
- Complete Oracle Solaris 10 documentation set at <http://docs.oracle.com/cd/E19253-01/index.html>.
- See [http://docs.oracle.com/cd/E23824\\_01/html/E24456/transzone-1.html](http://docs.oracle.com/cd/E23824_01/html/E24456/transzone-1.html) for creating flar images of Oracle Solaris 10 OS.
- See <http://docs.oracle.com/cd/E19082-01/819-6990/index.html> for administration of your network interfaces.

---

---

## Oracle VM Server for SPARC

The following information includes:

- [Introduction to Oracle VM Server for SPARC](#)
- [Roles for Managing Oracle VM Server for SPARC](#)
- [Available Management Features](#)
- [Preparing Your Control Domain](#)
- [Recommended Minimum Configuration](#)
- [Create OS Provisioning Profile](#)
- [Installation of Oracle VM Server for SPARC](#)
- [Oracle VM Server for SPARC Management](#)
- [Server Pools](#)
- [About Logical Domains](#)
- [Create Logical Domain Profile](#)
- [Create and Apply Logical Domain Plan](#)
- [Management of Logical Domains](#)
- [Managing Existing Oracle VM Server for SPARC Environments](#)
- [Related Resources](#)

### Introduction to Oracle VM Server for SPARC

Oracle VM Server for SPARC technology enables server virtualization on SPARC platforms. You can create and manage multiple virtual machine instances simultaneously on a single SPARC machine. Each virtual machine, or guest, can run a different operating system.

Oracle VM Server for SPARC technology is virtualization of SPARC servers. This technology is part of a suite of methodologies for consolidation and resource management for SPARC Chip Multi Threading (CMT) systems. Using this technology, you can allocate the various resources of the system such as memory, CPU threads, and devices, into logical groupings and create multiple discrete systems. These discrete systems have their own operating system, resources, and identity within a single system. By careful architecture, an Oracle VM Server for SPARC environment can help you achieve greater resource usage, better scaling, and increased security and isolation.

When Oracle VM Server for SPARC software is installed, a domain called the control domain is created. From this control domain, you create virtual machines called logical domains that each run an independent OS. A logical domain is a virtual machine with resources, such as a boot environment, CPU threads, memory, I/O devices, and its own operating system. The control domain manages the logical domains. Each logical domain can be created, destroyed, reconfigured, and rebooted independently of other logical domains.

For more information about Oracle VM Server for SPARC, refer to <http://www.oracle.com/technetwork/documentation/vm-sparc-194287.html>.

## Roles for Managing Oracle VM Server for SPARC

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task. See *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 15–1 Oracle VM Server for SPARC Roles and Permissions**

Task	Role
Provision and manage virtualization host	Virtualization admin
Create, manage, update, and delete guests	Virtualization admin
Discover and manage virtualization hosts	Asset admin
Create and manage profiles and plans	Profile and plan admin
Create and manage IPMP groups	Network admin
Create and manage Link Aggregation	Network admin
Set monitor threshold	Asset admin

## Available Management Features

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

- Provision Oracle VM Server for SPARC
- Manage Oracle VM Server, including, rebooting, shutting down, changing name servers and NFS4 domains.
- Monitor the performance of Oracle VM Server
- Create and provision logical domains
- Manage logical domains, including editing, migrating, starting, rebooting, and shutting down domains
- Monitor the performance of logical domains
- Discover and manage existing Oracle VM Server for SPARC systems and logical domains
- Create server pools to maximize capacity and for automatic load balancing
- Migrate logical domains

## Preparing Your Control Domain

You can provision Oracle VM Server for SPARC using Oracle Enterprise Manager Ops Center. You can provision the following versions:

- 1.2
- 1.3
- 2.0
- 2.1
- 2.2

The Oracle VM Server must meet specific hardware, OS, and firmware requirements.

### Operating System

You require Oracle Solaris 10 9/10 OS or later release to provision 1.2, 1.3, 2.0, and 2.1 version.

For 2.2 version, you require Oracle Solaris 10 8/11 OS or Oracle Solaris 11 OS. The minimum version of Oracle Solaris 11 OS for all domain type is Oracle Solaris 11 Support Repository Update 8 (SRU 8).

Refer to the Oracle VM Server for SPARC 2.2 Release Notes at [http://docs.oracle.com/cd/E35434\\_01/pdf/E23810.pdf](http://docs.oracle.com/cd/E35434_01/pdf/E23810.pdf) for more information about required patches for using OS version older than Oracle Solaris 10 8/11 OS.

### Hardware and Firmware

Refer to the Oracle VM Server for SPARC Release Notes in <http://www.oracle.com/technetwork/documentation/vm-sparc-194287.html> for the supported platforms to install different versions of Oracle VM Server for SPARC.

Ensure that you install the correct system firmware. You can update the firmware using Oracle Enterprise Manager Ops Center. See [Chapter 11, "Hardware"](#) for downloading and updating the required firmware version.

When you use Oracle Enterprise Manager Ops Center to provision the Oracle VM Server for SPARC software, it installs the Oracle Solaris OS, the Control Domain, and an agent on the target system. This provisioning action removes existing virtualization software, including any previous logical domains installed on the service processor.

To install Oracle VM Server for SPARC software, apply a profile that specifies the values for resources such as CPU threads, crypto units, and memory as described in [Create OS Provisioning Profile](#).

When you have existing Oracle VM Server for SPARC environment that you want to discover and manage in Oracle Enterprise Manager, refer to the section [Managing Existing Oracle VM Server for SPARC Environments](#) for more information.

## Recommended Minimum Configuration

The recommended minimum configurations for the Control Domain are described in the following sections.

### CPU Threads

The number of system CPUs determines the number of Control Domain CPU threads:

- For less than 16 system CPUs, set the Control Domain CPU Threads to 2.

- For between 16 and 64 system CPUs, set the Control Domain CPU Threads to 4.
- For more than 64 system CPUs, set the Control Domain CPU Threads to 8.

## Crypto Units

Crypto units are the resources on the supported platforms that provide high-performance, dedicated cryptographic engines. These can be used for tasks such as encrypting and decrypting network traffic between a Secure Socket Layer (SSL) web server and an application server.

Each CPU core has one crypto unit and four or eight CPU threads. Because the crypto unit is part of a core, the crypto unit is bound only to domains that contain at least one thread from the parent core. Crypto units cannot be split as CPU threads are split. For example, you have assigned the crypto unit for the first CPU core to the control domain. When a new logical domain is assigned a thread from the first CPU core and the crypto unit for that core is already assigned, the Control Domain cannot assign that crypto unit to the new logical domain. Allocation of crypto units might not succeed, especially when a core is split between domains. An Oracle VM Server might allocate fewer crypto units or none at all.

You must assign at least one crypto unit to the Control Domain because the crypto unit enables domain migration.

The use of Crypto Units is not mandatory although it might speed the logical domain migration. Allocation of Crypto Units might not be available in all the hardware supported. See the corresponding hardware data sheet and documentation for more information before planning for Crypto Units.

### **Example 15–1 Example of Crypto Unit Assignments**

In UltraSPARC T1 based servers, one core is four CPU threads. Therefore, assign one crypto unit and four CPU threads to the Control Domain. These values are set in the OS profile for Oracle VM Server for SPARC.

In UltraSPARC T2 and T2 Plus based servers, one core is eight CPU threads. Therefore, assign one crypto unit and eight CPU threads to the Control Domain.

## RAM

The amount of RAM for the Control Domain depends on the size of the system RAM:

- For system RAM less than 8 GB, set the Control Domain's RAM to 1 GB.
- For system RAM between 8 GB to 16 GB, set the Control Domain's RAM to 2 GB.
- For system RAM greater than 16 GB, set the Control Domain's RAM to 8 GB.

---

---

**Note:** See Oracle VM Server for SPARC 2.1 Administration Guide at [http://docs.oracle.com/cd/E23120\\_01/html/821-2854/index.html](http://docs.oracle.com/cd/E23120_01/html/821-2854/index.html) for more information about allocating memory size.

---

---

## Create OS Provisioning Profile

Create an OS provisioning profile to install the Oracle VM Server for SPARC software, the OS, and to set the parameters for the Control Domain. The profile collects details such as type of target, OS image, time zone and language setup, required JET modules, disk partitions, naming services and network details.



Upload the required Oracle Solaris OS image to the software library in Oracle Enterprise Manager Ops Center. See [Chapter 5, "Software Libraries"](#) for more information about uploading OS images.

### **Oracle VM Server for SPARC Parameters**

You can select the following parameters while creating the profile:

- Oracle VM Server for SPARC version - 1.2, 1.3, 2.0, 2.1, and 2.2.
- Software groups
- CPU Threads
- Memory
- Crypto Units
- Virtual Console Port Range
- Enable Multiplexed I/O
  - Enabling multiplexed I/O results in enabling the Fibre Channel ports on the system that is configured for storage.
- Name service
- NFS Domain value
- Manual netboot option

### **To Create Oracle VM Server for SPARC Provisioning Profile**

1. Select the Plan Management section and expand Profiles and Policies.
2. Choose OS Provisioning and click Create Profile in the Actions pane.
3. Enter the following details to identify the profile:
  - Name and description of the profile.
  - Select Oracle VM Server for SPARC as the Subtype.
  - Select the option Create a deployment plan for this profile.

**Figure 15–1 Profile Identification**

**Identify Profile** \* Indicates Required

\* **Name:** myldom21

**Description:**

Create a deployment plan for this profile.

\* **Subtype:** Subtype  
 Oracle VM Server for SPARC  
 Oracle Linux  
 Oracle VM Server for x86  
 Red Hat Linux  
 SUSE Linux  
 JET Template  
 Solaris SPARC  
 Solaris x86

**Target Type:** Target Type  
 V class (sun4v)

Click Next to select the OS image and distribution.

4. Select the following parameters in the Specify OSP Parameters step:
  - You can select 1.0, 1.2, 1.3, 2.0, or 2.1 and only Oracle Solaris 10 OS is used for these versions. Select Oracle Solaris 10 9/10 OS or a later release.
  - For 2.2 version, the OS can be Oracle Solaris 10 or Oracle Solaris 11 OS. You must have Oracle Solaris 10 8/11 OS or later release for Oracle Solaris 10 OS. For Oracle Solaris 11, you must synchronize your Oracle Solaris 11 Software Update Library with the parent repository for SRU 8 to get the 2.2 version OS image.
  - For Oracle Solaris 10 OS, select Full Distribution for the Software Group.

Click Next to specify the OS setup.
5. Specify the following OS setup parameters:
  - Select a language from the list.
  - Specify the time zone.
  - Specify a terminal type.
  - To monitor the installation using a serial connection, select the console serial port device and the baud rate.
  - Enter the NFS4 domain name that the target system will use. A dynamic NFSv4 domain name enables the name to be derived at run time, based on the naming service configuration. You can also enter a static domain name.
  - Enter the root password for the root user on systems provisioned using this profile. Re-enter the password for confirmation.

- Select the Manual Net Boot option to enable manual control of network boot operations for the target system. You must select this option for a target system that does not have a service processor because Oracle Enterprise Manager Ops Center cannot control the network boot process remotely on these systems.
- 6. Click Next.
 

If it is Oracle Solaris 11 OS, then you will be directed to Step 7 to create a user account to log in.

Otherwise, to Step 8 for Oracle Solaris 10 OS.
- 7. For Oracle Solaris 11 OS, root login to the system is not enabled. Create a user account through which you can SSH to the OS after provisioning. Enter the username and password for the user account.
 

Click Next and you will be directed to Step 9 to specify the Control Domain parameters.
- 8. JET modules can be used to provision an OS. The base\_config, custom, and flash JET modules are always installed. To specify additional JET modules that you have installed on the Proxy Controller to perform OS provisioning operations, enter a comma-separated list of the JET modules.
  - a. Click the Add icon to add JET name-value pairs. The JET parameters customize how this profile provisions the target systems.
  - b. Enter the name of the JET parameter that you want to add in the Name field.
  - c. Enter the value that you want to assign to the JET parameter in the Value field.

Click Next to specify the Oracle VM Server Control Domain parameters.
- 9. Specify the resources that you want to assign to the Control Domain. The remaining resources are available for the logical domains.
  - CPU Threads – Specify the number of CPU threads that you want to assign to the Control Domain.
  - Memory – Specify the amount of memory that you want to assign to the Control Domain.
  - Requested Crypto Units – Specify the number of crypto units that you want to assign to the Control Domain.
  - Virtual Console Port Range – Specify the minimum port and maximum port of the virtual console of the Control Domain. The default port range for virtual console is 5000 to 6000.
  - Enable Multiplexed I/O (MPxIO) – Select this option to enable SAN library connectivity for the control domain. This action enables the Fibre Channel ports on the system that is configured for storage.

---

**Note:** For Oracle VM Server for SPARC 1.2 version, you can select to install SUNWJass package to harden the system.

---

Click Next to specify the file system layout.

- 10. Specify the disk partitions and file systems that you want to create on the target system. The root (/) and a swap file system are defined by default. Click the Add

icon to define a new partition. For each partition that you define, provide the following information:

- **File System Type** – Select a file system type, either ufs, unnamed, zfs, or swap.
- **Mount Point** – Enter a directory to use as a mount point for partitions.
- **Device** – Enter the rootdisk keyword and a slice value to describe a partition on the target system's boot disk, for example, rootdisk.s0, or enter the logical device name, for example, c1t0d0s0, of the partition that you want to create.
- **Size (MB)** – Enter the size that you want to assign to the partition, expressed in MB. Do not enter any value for the size when you want to allocate the remaining unused disk space to a file system.

Click Next to specify the name service.

11. Specify the name service, domain name and the corresponding name server. You can select one of the following name services:

- **DNS** – Enter the domain name of the DNS server and enter the IP address of the DNS server in the Name Server field. You can enter up to three IP addresses as the value for the Name Server. Provide the additional domains to search for name service information in the Domain Name Search List. You can specify up to six domain names to search. The maximum length of each search entry is 250 characters.
- **NIS or NIS+** – Enter the domain name of the NIS or NIS+ server. When you know the NIS server details, choose the option Specify an NIS Server and enter the NIS server host name and the IP address.
- **LDAP** – Enter the domain name of the LDAP server. Specify the name of the LDAP Profile you want to use to configure the system. Enter the IP address of the LDAP Profile Server. You can also provide the Proxy Bind Distinguished Name and Password.
- **None** – Select None when there is no naming service configured.

Click Next to specify the network information.

12. Select one of the network options for the target system:

- When you select Use Link Aggregation, refer to the section [Create Link Aggregation in Oracle VM Server for SPARC](#) to define the parameters for Link Aggregation.
- When you select None, you will be forwarded to the next step to define the network interfaces and IP address allocation for the selected networks.

---

---

**Note:** You can create Link Aggregation only with Oracle Solaris 10 OS. It is not applicable for Oracle Solaris 11 OS.

---

---

Select an option and click Next to continue.

13. Select a DHCP-enabled network interface for the boot interface from the list of all managed networks. Click the Add icon to add more networks.

Select the Address Allocation Method for each network except the boot interface.

- When you select Use Static IP, you must provide the IP address when you apply the profile so that the IP address can be assigned to the target system after provisioning.

- When you select Assign By DHCP, the IP address is automatically assigned from the designated DHCP server.

Click Next to go to the Summary step.

14. Review the Summary of your selections. Click Finish to create the profile.

## Create Link Aggregation in Oracle VM Server for SPARC

While creating the profile for installing Oracle VM Server for SPARC, follow the procedure to create link aggregation:

1. Select Link Aggregation in the Specify Networks step of the profile.
2. Specify and configure the Link Aggregation details:
  - a. **Link Aggregation Name** – The name of the Link Aggregation is set to "aggr". Add an integer to make the name unique.
  - b. **Network** – Select a network from the list.
  - c. **NICs** – List the physical interfaces of the selected network that must be configured as a single unit. For example, GB\_1, and GB\_2.

Click Next to configure the IEEE 802.3ad Link Aggregation.

3. Define the following parameters for IEEE 802.3ad link aggregation standard:
  - **Load Balancing Policy** – Define the policy for outgoing traffic.
  - **Aggregation Mode and Switches** – When the aggregation topology connects through a switch, determine whether the switch supports the Link Aggregation Control Protocol (LACP). When the switch supports LACP, you must configure LACP for the switch and the aggregation. Define one of the modes in which LACP must operate.
  - **MAC Address Policy** – Define whether the MAC address of the NICs are fixed.

Click Next to continue.

4. Continue to complete the profile.

## Create and Apply Deployment Plan for Oracle VM Server for SPARC

When you create a profile, you can select to create a deployment plan with the profile automatically. You can also create your own deployment plan. Oracle Enterprise Manager Ops Center provides two different types of deployment plan to provision Oracle VM Server for SPARC:

- **Single Step Deployment Plan**

You have the Provision OS deployment plan to provision Oracle VM Server for SPARC. This requires the profile to install Oracle VM Server for SPARC.

- **Multi-Step Deployment Plan**

- **Install Server**

This multi-step deployment comprises the steps to provision Oracle VM Server for SPARC, install updates or software, apply monitoring profiles, and create logical domains.

- **Update Firmware and Install Oracle VM Server for SPARC**

This multi-step deployment plan comprises the steps to update the firmware of the hardware and then install the required version of Oracle VM Server for SPARC.

Select the required method and create the plan. All the plans described here require the OS provisioning profile for Oracle VM Server for SPARC. You can see [Plans and Profiles](#) for more information about creating and managing the profiles and plans.

### Apply a Deployment Plan for Oracle VM Server for SPARC

When you apply a deployment plan to provision Oracle VM Server for SPARC, you will be required to provide the IP address for the OS to be provisioned. You can also select the Oracle VM Server for SPARC to be placed in a server pool after provisioning. You have options to create a new server pool or place the server in an existing server pool.

**Figure 15–2 Placing Oracle VM Server for SPARC in Server Pool**

The screenshot shows a configuration window titled "Server Pool" with a sub-header "\* Indicates Required Field". The main text reads: "The server that will be installed can be assigned to an Oracle VM Server SPARC Server Pool. Select an assignment choice:". There are three radio button options:

- Do not assign to a Server Pool. The new server will execute in stand-alone mode. You may add the server to a pool at a later time.
- Assign to one of these compatible Server Pools:
- Create a new Server Pool based on the attributes of the new server and assign the server, using default pool settings. The pool settings can be changed later after it has been created.

Under the second option, there is a table with two columns: "Server Pool" and "Current Members".

Server Pool	Current Members
MyVPool	xvmt5120-2,xvmt5120-1

Under the third option, there is a text input field for "\* Server Pool Name:". Below it is a table with three columns: "Storage Library", "Type", and "Description".

Storage Library	Type	Description
LDomNAS	NAS	nfs://10.166.74.193/xVMShares/LDom
MyFCLib	SAN	fc://cdab12aa-181c-4a1f-8ebd-281c
MyNas7onnelib	NAS	nfs://10.166.88.16/xVMShares/7one

Read through the following sections to provision Oracle VM Server for SPARC in your environment.

## Installation of Oracle VM Server for SPARC

You can install the software on bare-metal or on systems that is configured with logical domains. When you provision Oracle VM Server through Oracle Enterprise Manager Ops Center, previous configuration is removed from the service processor by resetting the service processor to its factory defaults.

When you provision Oracle VM Server for SPARC, the instance of the Oracle Solaris OS becomes the Control Domain which is the first domain to be created. The virtualization host on which this instance of Oracle Solaris OS runs is called the Oracle VM Server Host or simply, Oracle VM Server. The Logical Domains Manager runs in the Control Domain to create and manage logical domains. You can have only one Control Domain per server. You cannot change the name or destroy the Control Domain.

This section describes how to install the Oracle VM Server for SPARC software on a service processor:

1. The Oracle VM Server for SPARC software depends on particular Oracle Solaris OS versions, required software patches, and particular versions of system firmware. See [Provisioning the Required Oracle VM Server Version](#).
2. Discover the target system on which you want to install Oracle VM Server for SPARC software.
3. Configure DHCP services on Proxy Controllers.
4. Create a profile for provisioning Oracle VM Server for SPARC. See [Create OS Provisioning Profile](#).
5. Create a deployment plan with the profile created for provisioning Oracle VM Server for SPARC.
6. (Optional) Adjust the amount of time allowed for the provisioning job. The default time is three hours or 180 minutes. You can edit the default\_timeout value for OS provisioning in the Enterprise Controller Configuration in the Administration section.

**Figure 15–3 Default Timeout Settings**

The screenshot shows the Oracle Enterprise Manager interface. The left navigation pane is expanded to 'Administration' > 'Enterprise Controller'. The main content area shows the 'Configuration Management' section for the 'OS Provisioning' subsystem. A table lists various properties and their values, with 'default\_timeout' highlighted.

Property	Value
default_password	admin
default_timeout	180
id.satellite_base_dir	/var/opt/sun/xvm
ldom.pis_key.1.2	LDOM_VERSION_12_FW
ldom.pis_key.1.3	LDOM_VERSION_13_FW
ldom.pis_key.2.0	LDOM_VERSION_20_FW_REC
ldom.pis_key.2.1	LDOM_VERSION_21_FW_REC
ldom.pis_key.2.2	LDOM_VERSION_22_FW_REC
ldom.update_version.1.2	7
ldom.update_version.1.3	7

The Oracle VM Server for SPARC provisioning job performs the following major tasks:

- Downloads the appropriate OS image.
- Initiates a net boot action on the Service Processor.
- Configures DHCP and installs the OS.
- Installs the Oracle VM Server Host.
- Configures Oracle VM Server Host according to the values set in the profile such as memory, CPU threads, Crypto units, and virtual console port range.
- When selected, installs the SUNWjass package to harden the system. For example, you can install the SUN Wjass package for version 1.2.
- Enables the Fibre Channel ports on the system that is configured for storage.
- Installs and configures the Agent Controller. Do not install the Agent Controller manually on the Oracle VM Server host.

## Provisioning the Required Oracle VM Server Version

Verify that the target system has the correct hardware and firmware configuration to support the installation of selected version of Oracle VM Server for SPARC.

When the supported hardware and firmware versions are not there, the provisioning job might fail. You cannot force set the version of the software to be installed. For the complete list of supported hardware, firmware version, and the supported Oracle VM Server for SPARC version, refer to the Release Notes in the library

<http://www.oracle.com/technetwork/documentation/vm-sparc-194287.html> for more information.

## Important Notes for Installation

Some important notes for installing Oracle VM Server for SPARC in Oracle Enterprise Manager Ops Center:

- The OS in the Control Domain must have the default locale set to C. The Control Domain provisioning is supported on Oracle Solaris SPARC or x86 Proxy Controllers, but not on Linux Proxy Controllers.
- To provision the Oracle VM Server for SPARC software, the proper system model name must be populated on the service processor. The model name is not available on the service processor of the Sun Blade T6320 hardware.
- Oracle Enterprise Manager Ops Center does not support use of the LDOMs configuration manager in LDOMs 1.2.
- Do not attempt to reconfigure the Control Domain and logical domains using the native CLI.
- You must not unconfigure and reconfigure the agent installed on the Control Domain.

## Initiating Manual Net Boot

A target system requires a manual net boot operation when Oracle Enterprise Manager Ops Center cannot perform a remote network boot process. Profiles that provision this type of system contain the Manual Net Boot option enabled. You must initiate the net boot operation when the Oracle VM Server provisioning job completes on the UI.

1. Log in to the service processor of the target system.
2. When the target system is running, enter `halt`.
3. Enter the following command

```
boot net:dhcp - install
```

## Additional Configurations

The following configuration for the Control Domain is performed during installation of Oracle VM Server for SPARC and is not required to be included in the profile:

- A virtual network switch for each subnet named *subnet-address\_prefix-length*, for example, *10.17.7.0\_24*
- A virtual disk server named *primary-vds0*
- A virtual console concentrator is named *primary-vcc0*



## Oracle VM Server for SPARC Management

After you have provisioned or discovered the Oracle VM Server for SPARC, you can dynamically manage the Oracle VM Server Control Domain resource configurations such as CPU Threads, Crypto Units, and memory. You can associate storage libraries and attach networks with Oracle VM Server for SPARC, create logical domains, and monitor the performance of logical domains.

You can also create server pools for Oracle VM Server for SPARC for an efficient management of your resources. For creating server pools, see [Chapter 17, "Server Pools"](#).

The following actions are available for managing the Oracle VM Server:

- [Edit Configuration and Tags](#)
- [Associate Storage Libraries](#)
- [Attach Networks](#)

### Edit Configuration and Tags

You can modify the Control Domain configuration that includes CPU Threads, Crypto Units, and memory. You can also modify the Name and Description of the Control Domain. Use the Edit Attributes option to modify the configuration.

The Oracle VM Server must have Oracle Solaris 10 10/09 OS or higher version to edit the attributes. When you modify the memory size, Oracle VM Server is rebooted unless it is running Oracle VM Server for SPARC 2.0 or higher version. Use Edit Tags to modify the existing tags and add new tags.

### Associate Storage Libraries

Storage libraries are required for storing logical domain metadata, ISO images and to provide virtual disks for logical domain storage. You must first associate the storage library to the Oracle VM Server and then it is made available for all the logical domains under it.

You can associate the following libraries for Oracle VM Server:

- Filesystem storage – This includes the NAS storage libraries.
- Block storage – This includes the Static and Dynamic Storage libraries. The Static Storage library includes the exported LUNs of SAN and iSCSI storage servers that are not managed by Oracle Enterprise Manager Ops Center. The LUNs of storage servers managed in Oracle Enterprise Manager Ops Center are available through Dynamic Storage library. This library provide option to create new LUN when you add storage to the logical domains.

Select the option Associate Library to associate libraries with the selected Oracle VM Server for SPARC.

### Attach Networks

Attach networks to Oracle VM Server to provide networking facilities for the logical domains. You can make multiple connections to a network in the Oracle VM Server Control Domain. For each network connection, a virtual switch is created. There is a naming pattern for the switch. For an example network 1.1.1.0/24, the name of the virtual switches will be 1.1.1.0\_24, 1.1.1.0\_24\_1, 1.1.1.0\_24\_2 and 1.1.1.0\_24\_3. This ensures that the switches have a unique name. When a network connection is made to the server, the virtual switch created is incremented. When you create and start a

logical domain, you define the virtual switch that will be connected to the logical domain. Each virtual switch must be connected to a NIC.

When you migrate logical domains, the switch name must be identical in the source and the target Oracle VM Server for SPARC.

See [Migrating a Logical Domain](#) for more information about migrating the logical domains.

You can create IPMP groups and aggregate links in the Control Domain. Navigate to the Oracle Solaris OS of the Control Domain and create IPMP groups or Link Aggregation. Refer to [Chapter 7, "Networks"](#) for more information about creating IPMP groups and Link Aggregations in an Oracle Solaris OS.

### To Attach Networks to Oracle VM Server

This procedure to attach networks is applicable for Oracle VM Server for SPARC in stand-alone mode.

1. Select the Oracle VM Server for SPARC in the Assets tree.
2. Click Attach Networks in the Actions pane.

The list of available networks in Oracle Enterprise Manager Ops Center are displayed. The list also displays the existing number of connections with the server.

3. Select one or more networks from the list. You can make multiple connections to a network.

Click Next.

4. Specify the number of connections for the selected networks. Increment the total number of connections.

---

---

**Note:** The number of connections does not limit the number of logical domains that can be connected to this network.

---

---

5. Specify the NIC and IP address for each network connection.

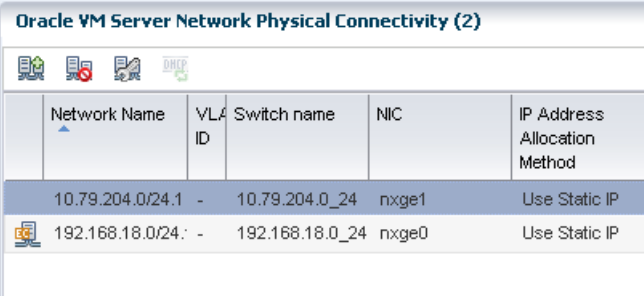
For each network connection, you must provide a NIC as a virtual switch is created for each connection. The virtual switch requires a physical interface to allow communication between the logical domains and external network. Follow these rules while assigning the NIC and IP address:

- You can specify the same NIC to different network when the network has different VLAN ID. Otherwise, you cannot assign the same NIC to different networks.
- When supported by the network, select System Allocated to enable the system to allocate the NIC and IP address.
- You can select Do Not Allocate IP for IP address when you do not want to assign IP address to the selected network interface.

Click Next.

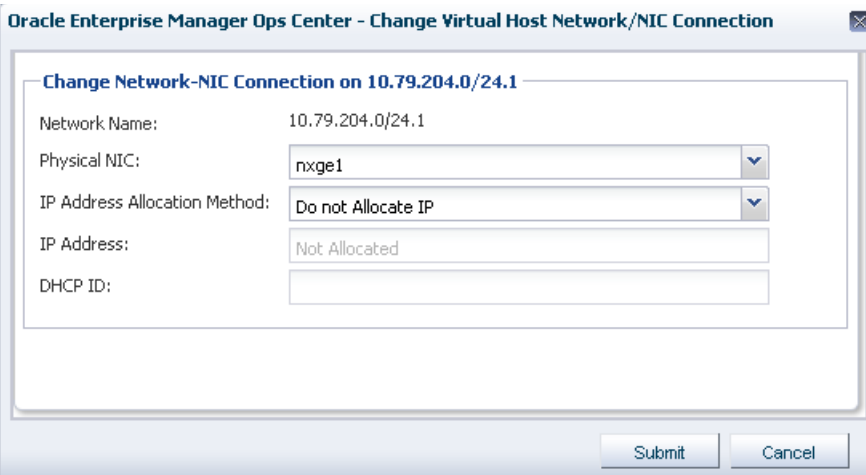
6. Review the summary and click Finish to attach the selected network to the Oracle VM Server.

In the Network tab of the Oracle VM Server for SPARC, you have the following options to manage the networks:

**Figure 15–4 Network Options**


Network Name	VLAN ID	Switch name	NIC	IP Address Allocation Method
10.79.204.0/24.1	-	10.79.204.0_24	nxge1	Use Static IP
192.168.18.0/24.1	-	192.168.18.0_24	nxge0	Use Static IP

- Unbind networks – Disconnects the selected network from Oracle VM Server.
- Modify physical connectivity – Allows to edit the connectivity attributes of the selected network.

**Figure 15–5 Modify Physical connectivity**


**Change Network-NIC Connection on 10.79.204.0/24.1**

Network Name: 10.79.204.0/24.1

Physical NIC:

IP Address Allocation Method:

IP Address:

DHCP ID:

- Refresh DHCP connectivity – Allows to re-connect to the DHCP server.

## Reboot Oracle VM Server

You can reboot the Control Domain regardless of the state of the logical domains in it. During the reboot, the logical domains might suspend temporarily but keep their current states.

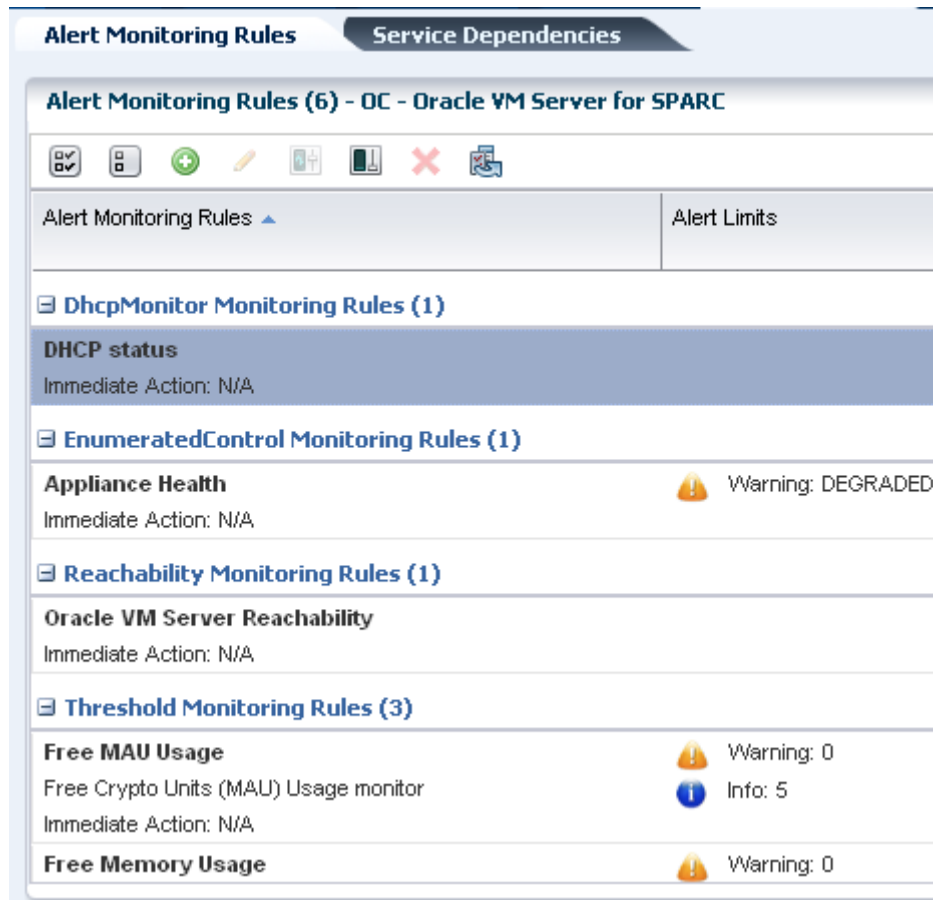
## Performance Management

You can view the following information about Oracle VM Server performance on the UI:

- The Summary tab displays the Oracle VM Server for SPARC configuration information, and its health status.
- The Dashboard displays the general information about the selected Oracle VM Server for SPARC. A graphical representation of the group members and its relationship is displayed. The unassigned incidents and the list of recent incidents are also displayed.

- The Analytics displays the CPU, memory and network utilization by the logical domains in the Oracle VM Server. The consumption is represented in the form of charts.
- The Incidents tab lists the incidents that are reported for the Oracle VM Server. It provides the list of unresolved incidents and a graphical representation of the problem composition.  
To see the corresponding alerts for each incident, see [Chapter 9, "Incidents"](#) for more detailed information.
- The Monitoring tab shows the monitoring values and boundaries that are set for Oracle VM Server activity. You can review the rules, monitoring attributes, specific time period for monitoring, and the level of severity for monitoring the activity of Oracle VM Server. To change these values, see [Chapter 4, "Monitoring Rules and Policies"](#).

**Figure 15–6 Oracle VM Server for SPARC Monitoring Options**



- The Configuration tab displays information such as remote logging, routing, NFS domain name, and name service information for the Oracle VM Server.
- The Charts tab displays the CPU, memory and network utilization of the Oracle VM Server. The data is collected in five-minute intervals and is displayed graphically. The utilization data is provided for different time intervals. See [Chapter 12, "Operating Systems"](#) for more information about reading charts.

## Server Pools

You can create server pools of your Oracle VM Server for SPARC systems in Oracle Enterprise Manager Ops Center. An Oracle VM Server must not have logical domains in running, shutdown, or suspended states when you want to add it to a server pool.

The detailed description and procedure for creating server pools are described in [Chapter 17, "Server Pools"](#).

## About Logical Domains

A logical domain is a virtual machine that has its own operating system and identity within a single server. Each logical domain can be created, destroyed, reconfigured, and rebooted independently, without requiring the server to be powered off. You can run a variety of applications in different logical domains to keep them independent for performance and security purposes.

Using Oracle Enterprise Manager Ops Center, you can create logical domains and install Oracle Solaris OS on them. Using profiles and deployment plans, you can create more than one logical domain simultaneously and then save the configuration for future use.

You can use one of the following methods to create logical domains:

- **Create Logical Domain Profile and Plan**
  1. Create a profile which defines the configuration of the logical domain.
  2. Using the profile, create a deployment plan.
  3. Apply the plan on an Oracle VM Server to create logical domains.
  4. The logical domains do not have the OS installed. You must select each logical domain and apply an OS provisioning plan to install the OS. See [OS Provisioning on Logical Domains](#) for provisioning OS on the logical domains.
- **Configure and Install Logical Domains**

This is a complex plan which contains deployment plans that create logical domains and install Oracle Solaris OS on them. You must have the required profiles and deployment plans available to create the complex plan. The outline to create a plan is as follows:

  1. Create a logical domain profile.
  2. Create an OS provisioning profile to install the OS.
  3. Create a deployment plan to install the OS and other updates if any.
  4. Create the Configure and Install Logical Domains plan.

You can now manage logical domains that were created manually using the native CLI in Oracle Enterprise Manager Ops Center. See [Managing Existing Oracle VM Server for SPARC Environments](#) for more information.

## Create Logical Domain Profile

A logical domain profile contains the requirements and configuration for an entire logical domain, including the CPU Threads, memory, storage, and network details. When a deployment plan applies the profile, you create a logical domain. You must provision Oracle Solaris OS on each domain separately. As an alternative, you can

include the logical domain profile along with an OS provisioning profile in a complex plan.

Ensure that you have the following information before you create a profile:

- **CPU and memory requirements**

The physical CPUs of the Oracle VM Server for SPARC are shared among the CPU threads of all the logical domains. Each logical domain requires:

- At least one GB of memory.
- At least one CPU thread.

Each CPU thread can be allocated independently to logical domain. The CPU threads are grouped into cores. For example, there are 4 Threads per core in the Oracle Sun Fire and SPARC Enterprise T1000 CMT processors. Some hardware resources are provided on a per-core basis and therefore, shared between the threads in the core. When the threads in a core are allocated to two or more separate logical domains, it can lead to suboptimal performance of those threads. To get the best performance, it is best to avoid allocating the threads of a core to many logical domains. The best approach would be create large logical domains first, the logical domains with complete cores, and then the smaller logical domains.

Crypto units are assigned based on CPU thread assignments. You can request the number of crypto units to be assigned to the logical domain. However, the number of crypto units assigned might be different than the amount requested because we can only allocate a crypto unit for every given number of CPU thread allocation, depending on the server hardware. After the creation of logical domain, view the job notification to see the actual number of Crypto Units assigned to the logical domain. You can also edit the logical domain configuration, storage, and network resource configuration later.

- **Storage resources**

The libraries for virtual disk can be local, local device, NAS, SAN, or Dynamic Storage libraries.

- **Network resources and number of connections for a network**

You can connect to a network multiple times to the logical domain. When you create a logical domain, the number of connections for a network translate to the number of virtual network devices created for the logical domain. The number of virtual network devices created depends on the number of virtual switches present in the Control Domain.

When you start a logical domain, you have to define the virtual switches through which you connect the logical domain to the external network.

### **To Create a Logical Domain Profile**

1. Select the Plan section from the Navigation pane.
2. Select Logical Domain from the Profile tree.
3. Click Create Profile from the Actions pane.

The Create Logical Domain Profile wizard displays.

4. Provide a name and description to identify the profile.
5. Select Create a deployment plan for this profile to automatically create a plan using this profile.

6. Click Next and provide a name and the starting number for the logical domain.

Using this profile, you can create more than one logical domain. For unique identification of the domains to be created, provide a prefix start name and starting number. For example, assume that the Start Name is TestDomain and the starting number is 10. If you create three logical domains, then the name of the logical domains will be TestDomain10, TestDomain11, and TestDomain12.

7. Click Next to configure the CPU Threads and memory.

The physical CPUs of the Oracle VM Server for SPARC are shared among the CPU threads of all the logical domains. Each logical domain requires:

- At least one Gigabyte of memory.
- At least one CPU thread.

If required, enable the automatic recovery option and then enter the value for priority of recovery. The value must be between 0 and 100. A logical domain with a higher value will be recovered first.

8. Click Next to specify the library for storing the domain metadata and storage disks for the logical domain.

9. Select a library to store the logical domain metadata.

You can select only the local or NAS library to store the domain metadata.

10. Select one or more libraries that form the logical domain storage disks.

The libraries for virtual disk can be local, local device, NAS, SAN, or Dynamic Storage libraries.

11. Click Next to specify the networks for the domains.

12. Select at least one network from the list of networks identified by Oracle Enterprise Manager Ops Center. You can associate a logical domain with more than one network.

13. Enter the number of connections for each network.

You can connect to a network multiple times to the logical domain. When you create a logical domain, the number of connections for a network translate to the number of virtual network devices created for the logical domain. The number of virtual network devices created depends on the number of virtual switches present in the Control Domain.

When you start a logical domain, you have to define the virtual switches through which you connect the logical domain to the external network.

14. Click Next to view the summary of the details selected for creating a logical domain.

15. Review the information and click Finish to save the profile.

When you want to create a deployment plan with this profile in the first step, then a corresponding logical domain plan is also created.

## Create and Apply Logical Domain Plan

When you create a logical domain profile, you can select to create a deployment plan with that profile. You can also create logical domain plans. You can either create a simple plan to install only the logical domains or a complex plan to create the logical domains and provision OS on it. The following procedure describes how to create a

simple plan to install the logical domains only. You require to have created a logical domain profile to select in the plan.

#### **To Create a Logical Domain Plan**

1. Select Create Logical Domains plan under Deployment Plans tree in the Plan Management section.
2. Click Create Plan from Template in the Actions pane.  
Create a Deployment Plan window displays.
3. Enter a name and description for the plan.
4. Select the failure policy.
5. Select the logical domain profile in the Create Logical Domain step.

This is a simple single step plan to select the logical domain profile. The logical domain profiles that are available are listed in the drop-down list of Associated Profile/Deployment Plan.

6. Enter the number of logical domains to be created.
7. Click Save to create the deployment plan.

The deployment plan will be created with the associated profile. Now, apply the plan on a suitable target to create the logical domains.

### **Apply Logical Domain Deployment Plan**

Apply the created logical domain deployment plan on the target server and create the logical domains.

1. Select the created logical domain deployment plan in the Deployment Plans tree.
2. Click Apply Deployment Plan in the Actions pane.  
The Select Target Assets window displays.
3. Select the target server from the list.  
You can select one or more targets to apply the plan.
4. Click Add to Target List option to add the selected targets on which you want to apply the plan.
5. Select whether you want to run the plan with minimal interaction or you want to override the profile values.
6. Click Next to specify the resource assignments in the profile.
7. If required, modify the name of the logical domains starting name and the number appended to it.  
Click Next to specify the storage resource assignments.
8. When the storage resources from the profile are not available for the selected target, it is flagged in red color. Modify the storage resources accordingly.  
Click Next to specify the network resource assignments.
9. When the network resource assignments from the profile are not available for the selected target, then it is flagged in red color. Modify the network resources accordingly.  
Click Next to schedule the job.



10. Schedule the job to run now or at a later time. Click Next.
11. Review the summary and click Apply to execute the deployment plan on the selected targets.

## OS Provisioning on Logical Domains

The Oracle OS version that is provisioned on the logical domains is independent of the OS version on the Oracle VM Server for SPARC Control Domain. You can provision Oracle Solaris 10 or Oracle Solaris 11 OS on the logical domains irrespective of the Oracle Solaris OS version of the Control Domain.

After you create a logical domain, you must provision an OS on it.

- Ensure that you have imported the appropriate ISO image into the library. If it is Oracle Solaris 10, then it must be at least Oracle Solaris 10 8/07.
- Create or identify an OS provisioning profile for SPARC. See [Provisioning Operating Systems](#) for more information.
- Create or identify a deployment plan with the OS provisioning profile and apply the deployment plan.

---

---

**Note:** When you want to monitor the OS provisioning on the logical domains, you must first enable the logical domain console. See [Using the Logical Domain Console](#) for enabling the console.

---

---

## Complex Plan

You have the Configure and Install Logical Domains deployment plan that comprises the step to create logical domains and provision OS on them. This complex plan steps are:

- Create Logical Domains Profile – See [Create Logical Domain Profile](#) for creating the logical domain profile.
- Install and Update OS Plan – See [Multi-Step Deployment Plans](#) for creating the plan.

Create the required profile and plan to create this complex plan.

## Management of Logical Domains

The following operations are available for managing the logical domains that were created using Oracle Enterprise Manager Ops Center:

- Edit logical domain attributes
- Start a logical domain
- Shut down a logical domain
- Reboot a logical domain
- Migrate logical domains
- Add storage to logical domains
- Connect networks to logical domains
- Automatic recovery of logical domains

## Edit Logical Domain Configuration

Use the option Edit Attributes in the Actions pane of a selected logical domain. You can edit the name, description, CPU Threads, memory, Crypto Units and automatic recovery priority value.

Use the option Edit Tags to modify the tag values or to add new tags.

## Shut Down a Logical Domain

When you shut down a logical domain, it is disconnected from its networks, disassociated from the Oracle VM Server Control Domain, and all the associated resources are released. You can restart the logical domain with the same configuration that is maintained in its storage library on the same Oracle VM Server or on a different target server.

## Start Logical Domain

You can start a logical domain from a shut down state. When you start a logical domain, you can select to start the logical domain on the same target or on a different target server. Depending on the number of network connections to an Oracle VM Server for SPARC, you have that many virtual switches created for an Oracle VM Server for SPARC.

You must select the virtual switch that it will connect to the logical domain MAC address. A virtual switch can be connected to only one MAC address. You can also select not to connect to network for a virtual switch.

### To Start a Logical Domain

1. Select the shutdown logical domain.
2. Click Start in the Actions pane.

The Start Logical Domain wizard displays.

3. Select the server pool in which you want to start the logical domain.

When you shutdown a logical domain, the logical domain is disassociated from the Control Domain and it can be started on a server.

When you have networks attached to a logical domain and is not available in the selected server pool, then that network will not be available when the logical domain starts.

4. Select the Oracle VM Server for SPARC in which you want to start the logical domain. You can select the same Oracle VM Server in which the logical domain was running already. Otherwise, select an Oracle VM Server for SPARC from the list.

The current load for all the Oracle VM Server for SPARC are displayed. Use this information to place your logical domain.

Click Next to specify the network interfaces.

5. Select the virtual switch that must be associated with the logical domain MAC address.

The number of virtual switched displayed depends on the number of network connections for the server pool. For each network connection, you have a virtual switch created. You can associate a virtual switch with only one MAC address.

6. Select Do Not Connect when you do not want the virtual switch to connect to MAC address.

Click Next to schedule the job.

7. Schedule the job to run now or at a later time.
8. Review the properties and click Start to run the logical domain.

## Add Storage to Logical Domain

You can add virtual disks to a logical domain. The associated libraries to the Oracle VM Server for SPARC are available to be added as additional storage to logical domains. The logical domain must be shut down to enable the option Add Storage in the Actions pane.

You can add virtual disks from the following type of storage libraries:

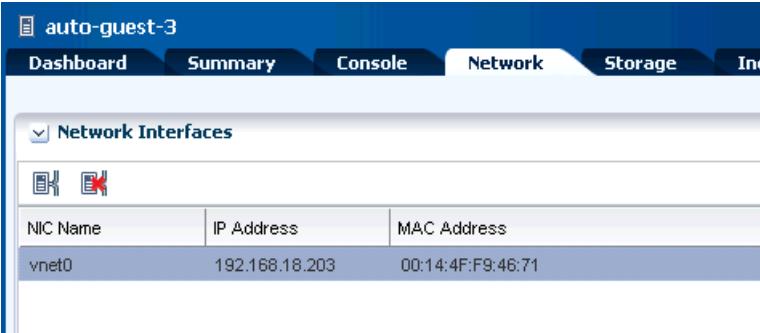
- File system storage – NAS libraries. Specify a virtual disk name and size of the disk.
- Static block storage – Select LUNs from SAN or iSCSI storage servers. The LUNs sizes are fixed.
- Dynamic block storage – Add LUNs from SAN or iSCSI storage servers discovered and managed in Oracle Enterprise Manager Ops Center. You can also create LUNs by selecting a volume group and specifying the size of the LUN.

## Managing Logical Domain Networks

The logical domain must be shut down state to connect or disconnect from a network. Use the option Connect Network to connect to a network. You can connect to a network multiple times.

Use the icons Connect and Disconnect Network icon in the Networks tab to connect or disconnect a network from a logical domain.

**Figure 15–7 Logical Domain Network Options**



NIC Name	IP Address	MAC Address
vnet0	192.168.18.203	00:14:4F:F9:46:71

You can create IPMP groups or aggregate the NICs allocated to the logical domain. See [Chapter 7, "Networks"](#) for more information about creating IPMP groups and link aggregation.

## Migrating a Logical Domain

You can migrate a logical domain from an Oracle VM Server to another Oracle VM Server. The type of migration is warm migration. The logical domain is shut down or suspended and then its static configuration is moved to the target host. The logical

domain is then restarted on the target host using the same virtual image. Warm migration does not maintain the live run state of the operating system, that is, going through a save-to-disk cycle during the migration. To migrate domains, shared storage resources is required.

For Oracle VM Server for SPARC 1.2 version, you can migrate with only 1 MAU.

For Oracle VM Server for SPARC 1.3 and later versions, you can migrate with any number of MAUs.

From Oracle VM Server for SPARC 2.1 version, live migration of the logical domains is supported.

---

---

**Note:** For Oracle VM Server for SPARC 2.1, you cannot migrate a logical domain to a previous version of the server such as 2.0, 1.3, or 1.2. You can migrate only within the same version of Oracle VM Server for SPARC.

---

---

### To Migrate a Logical Domain

1. Select the logical domain to be migrated in the Assets tree.
2. Click Migrate in the Actions pane.

The Migrate Logical Domain wizard displays.

3. The eligible Oracle VM Servers are displayed in the decreasing order of preference. Select an Oracle VM Server from the list.

Click Next.

4. Review the information and click Finish to migrate the logical domain.

This migration is initiated from the logical domain and it results in migration of single logical domain. When the Oracle VM Server is placed in a server pool and there are more than one logical domain in the host, you can use Migrate Logical Domains to migrate more than one logical domain from the host.

### To Migrate Multiple Logical Domains

1. Select an Oracle VM Server that is placed in a server pool.
2. Click Migrate Logical Domains in the Actions pane.

The Migrate Logical Domains wizard displays.

3. The list of logical domains running in the Oracle VM Server are listed. Select one or more logical domains from the list.

Click Next.

4. The eligible Oracle VM Servers in the same server pool that have the required resources to host all the logical domains are listed in the decreasing order of preference. Select an Oracle VM Server from the list.

Click Next.

5. Review the summary and click Finish to migrate logical domains.

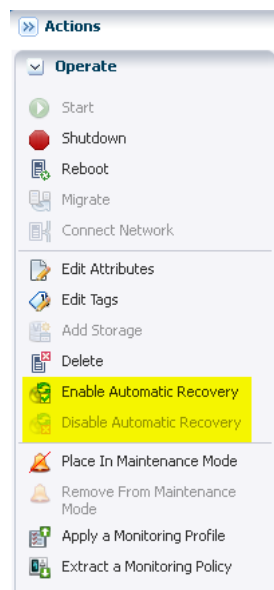
## Enabling Automatic Recovery of Logical Domains

You can enable automatic recovery of logical domains. This ensures that when the Oracle VM Server for SPARC placed in a server pool fails, the logical domains are recovered and restarted on another server in the server pool.

You can set the priority of recovery value for the logical domain that decides the order of recovery of the logical domains in the Oracle VM Server for SPARC. The priority of recovery value can be set between 0 to 100. For example, if the priority of recovery value set for logical domain A is 12 and logical domain B is 15, then the logical domain B will be recovered first.

Use the options Enable Automatic Recovery and Disable Automatic Recovery to set the automatic recovery for a logical domain. If you have disabled the automatic recovery of a logical domain, then it will not be migrated to other servers in the pool when the underlying virtualization host fails. Instead, it will be listed under Shutdown Guests in the Server Pool. You can restart them on other servers as required.

**Figure 15–8 Enable and Disable Automatic Recovery**



When you edit the attributes of a logical domain, you can edit the priority of recovery value.

If there are no resources available to recover the logical domains in the server pool, then the automatic recovery of logical domains is not possible and you must follow the recovery procedure as described in [Recovering Logical Domains](#).

When a logical domain is configured for automatic recovery, the auto boot value for the logical domain is set to false. The auto boot value is controlled by Oracle Enterprise Manager Ops Center. This is because, when the failed server is repaired and restarted, the logical domains are not started automatically. Oracle Enterprise Manager Ops Center will check whether the logical domains are recovered and running on other servers. If the logical domains are not recovered, then the logical domains are started. If the logical domains are recovered on other servers, then Oracle Enterprise Manager Ops Center will cleanup those logical domains on the server.

When you perform shut down and start operations using the UI for a logical domain that is configured to automatically recover, the operating system is also booted automatically by Oracle Enterprise Manager Ops Center.

When you perform the shut down and start operations using the CLI for a logical domain that is configured to automatically recover, you must boot the OS separately. It is not automatically done by Oracle Enterprise Manager Ops Center.

See [Chapter 17, "Server Pools"](#) and [Automatic Recovery](#) of Oracle VM Server for SPARC in a server pool for more information.

## Recovering Logical Domains

The following procedure describes the actions that must be performed to recover the attached logical domains when an Oracle VM Server for SPARC server in a server pool has failed.

1. Isolate the failed server.  
Log into the ALOM or ILOM of the physical server and shut down the server.
2. Power-off the failed server.
3. In the Oracle Enterprise Manager Ops Center UI, select the server pool in which the failed server is the member. Check whether the server is flagged as unavailable. This status is updated within 5 minutes approximately.
4. Select the Control Domain of the server in the UI and click Delete Asset in the Actions pane.
5. Select the server pool in which the failed server was a member and expand the Shutdown Guests list.
6. The attached logical domains of the failed server are listed. Select the logical domains and click Start to start the logical domains in the desired server in the server pool.

## Deleting a Logical Domain

When you delete a logical domain, it is disconnected from the associated networks and is disassociated from the Oracle VM Server. All the associated resources are released and the domain configuration is removed from the library. All the references to the logical domain, including its disk image and snapshots are removed from the system. However, the logical domain profile and plan remain unaffected.

When you delete a logical domain manually, that is using the native CLI, then the UI reflects the removal of the logical domain.

## Using the Logical Domain Console

You can attach to the logical domain console within the Oracle Enterprise Manager Ops Center UI. You enable the console connection and then you connect to the console.

---

---

**Note:** When the logical domain is not in view in the Assets tree, the console is logged out automatically but the connection exists until the connection time expires. You must log in again.

---

---

## Managing Existing Oracle VM Server for SPARC Environments

You can now manage existing Oracle VM Server for SPARC environments in Oracle Enterprise Manager Ops Center.

You can discover and manage Oracle VM Server for SPARC that has been provisioned manually. The underlying logical domains are automatically discovered and managed in Oracle Enterprise Manager Ops Center. In the Assets tree, the discovered logical domains are displayed in order and grouped under the Control Domain.

Logical domains that are created manually for an Oracle VM Server for SPARC provisioned through the UI are also automatically discovered and managed on the UI.

You can also provision OS on the manually created logical domains using the OS provisioning profile and plans in Oracle Enterprise Manager Ops Center.

You can perform the following functions on the UI for an existing logical domains:

- Start
- Shut down
- Reboot
- Modify the attributes of Logical Domain
- Delete Logical Domains

### Limitations

The following are the limitations for managing such logical domains in Oracle Enterprise Manager Ops Center:

- Storage and network resources of the logical domains cannot be managed.
- Cannot be part of server pools.
- Cannot migrate the logical domains as it is not part of a server pool.

[Table 15-2](#) shows the options for managing existing logical domains as compared to managing new logical domains.

**Table 15-2 Management Options for Oracle VM Server**

Options	New Oracle VM Server for SPARC	New Logical Domain	Existing Oracle VM Server for SPARC	Existing Logical Domain
Modify attributes for Oracle VM Server	Yes	N/A	Yes	N/A
Reboot Oracle VM Server	Yes	N/A	Yes	N/A
Manage Networks	Yes (stand-alone)	Yes	No	No
Manage Storage	Yes (stand-alone)	Yes	No	No
Start Logical Domain	N/A	Yes	N/A	Yes
Shutdown Logical Domain	N/A	Yes	N/A	Yes
Reboot Logical Domain	N/A	Yes	N/A	Yes
Delete Logical Domain	N/A	Yes	N/A	Yes

**Table 15–2 (Cont.) Management Options for Oracle VM Server**

<b>Options</b>	<b>New Oracle VM Server for SPARC</b>	<b>New Logical Domain</b>	<b>Existing Oracle VM Server for SPARC</b>	<b>Existing Logical Domain</b>
Install Server Deployment Plan	Yes	Yes	No	Yes
Enable Console	N/A	Yes	N/A	Yes

## Related Resources

For instructions in performing actions or to learn more about the role of this feature, go to one of the following resources.

- <http://www.oracle.com/technetwork/documentation/vm-sparc-194287.html>
- Chapter 2, "Asset Management"
- Chapter 17, "Server Pools"
- Chapter 7, "Networks"
- Chapter 6, "Storage Libraries"
- *Oracle Enterprise Manager Ops Center Administration Guide*
- *Oracle Enterprise Manager Ops Center Deploying and Configuring Oracle VM Server for SPARC Guide*



---

---

## Oracle VM Server for x86

The following information includes:

- [Introduction to Oracle VM Server for x86](#)
- [Roles for Oracle VM Server for x86 Management](#)
- [Integration of Oracle VM Server for x86 with Oracle Enterprise Manager Ops Center](#)
- [Installing Oracle VM Manager](#)
- [Discover Oracle VM Manager](#)
- [Discover Oracle VM Servers](#)
- [Installing Oracle VM Servers](#)
- [Administration of Oracle VM Manager](#)
- [Discover Storage Resources](#)
- [Manage Storage Resources](#)
- [Manage Networks](#)
- [Manage Oracle VM Servers](#)
- [Create Server Pool](#)
- [Create Virtual Machines](#)
- [Create and Deploy Virtual Machine Plan](#)
- [Provisioning OS on Virtual Machines](#)
- [Manage Virtual Machines](#)
- [Related Resources](#)

### Introduction to Oracle VM Server for x86

Oracle VM Server for x86 is a platform that provides a fully equipped environment to leverage the benefits of x86 virtualization technology. Oracle VM Server enables you to deploy operating systems and application software within a supported virtualization environment.

Oracle VM Server for x86 is a Xen-based server virtualization technology which supports Linux, Oracle Solaris, and Windows guests, and provide features to manage guests lifecycle operations, allocate and monitor guest resource consumption. The components of Oracle VM are:

- Oracle VM Manager – Provides the user interface to manage Oracle VM Servers, virtual machines, and resources.
- Oracle VM Server – A self-contained environment that is designed to produce a lightweight, secure server-based platform for running virtual machines. The Oracle VM Server can perform one or more of the following functions:
  - Server Pool Master – It is the core of the server pool operations. It acts as the contact point for the server pool to Oracle VM Manager, and also as the dispatcher to other Oracle VM Servers in the server pool.
  - Utility Server – Its function focuses on the creation and removal operations of virtual machines, Oracle VM Servers, and server pools.
  - Virtual Machine Server – The primary function of virtual machine server is to run virtual machines.

## Roles for Oracle VM Server for x86 Management

Table 16–1 lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task. See *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 16–1 Oracle VM Server for x86 Roles and Permissions**

Task	Role
Discover Oracle VM Manager and Oracle VM Server	Virtualization admin
Provision Oracle VM Manager	Ops Center admin
Manage Oracle VM Manager	Virtualization admin
Create Link Aggregation	Network admin
Create, manage, update, and delete virtual machines	Virtualization admin
Set monitor threshold	Asset admin
Manage storage resources	Storage admin
Create and manage profiles and plans	Profile and plan admin

## Integration of Oracle VM Server for x86 with Oracle Enterprise Manager Ops Center

The integration of Oracle VM Server for x86 with Oracle Enterprise Manager Ops Center provides the platform to manage Oracle VM Manager, Oracle VM Servers, server pools, and the virtual machines through Oracle Enterprise Manager Ops Center UI.

You can do the following operations through Oracle Enterprise Manager Ops Center to manage Oracle VM Server for x86 deployments:

- Discover deployed Oracle VM Managers
- Provision Oracle VM Servers
- Discover existing Oracle VM Servers
- Launch Oracle VM Manager UI

- Create virtual machines
- Provision OS on virtual machines
- Create server pools
- Connect to Oracle VM Manager console
- Manage storage repositories of Oracle VM Server for x86
- Perform management operations on Oracle VM Servers and virtual machines

## Installing Oracle VM Manager

Installation of Oracle VM Manager is outside the scope of this document. For detailed instructions about how to install the Oracle VM Manager, see *Oracle VM Installation and Upgrade Guide for x86*.

You can discover the Oracle VM Manager in Oracle Enterprise Manager Ops Center and launch the console to access it.

## Discover Oracle VM Manager

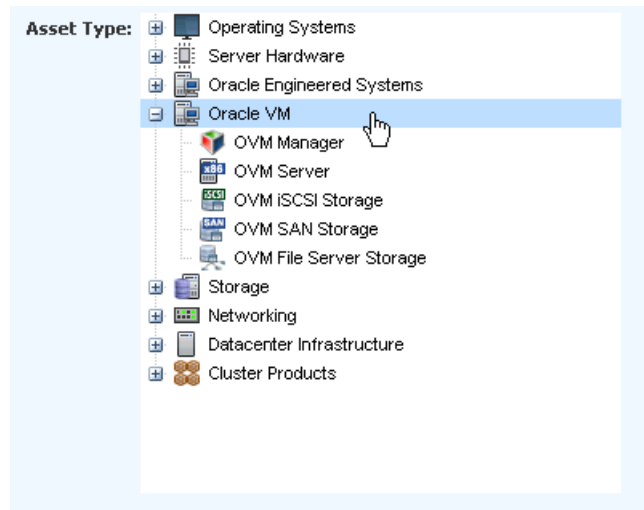
You can discover the deployed Oracle VM Manager in Oracle Enterprise Manager Ops Center. When you discover the Oracle VM Manager, the following Oracle VM resources are automatically discovered and populated in the UI:

- Oracle VM Servers
- Server pools
- Virtual machines
- Storage servers
- Storage repositories
- Networks

To discover an existing Oracle VM Manager, you must have the following information:

- Discovery profile for Oracle VM Manager
- Credentials for Oracle VM Manager access

You must create a discovery profile for discovering the installed Oracle VM Manager. The discovery profile provides options to create the discovery profiles for all the components related to Oracle VM Server for x86.

**Figure 16–1 Discovery Asset Type**

### To Create a Discovery Profile for Oracle VM Manager

The following procedure outlines the steps to create a discovery profile for Oracle VM Manager:

1. Select Discovery from the Plan Management section.
2. Click Create Profile in the Actions pane.  
The Create Profile-Discovery wizard displays.
3. Enter a name and description for the discovery profile.
4. Select the Asset Type as Oracle VM Manager from the list.  
Click Next to define the tags.
5. It is optional to define the tags for the asset to be discovered. Tags help to group the assets.  
Click Next to enter the IP range.
6. It is optional to enter the IP address of the Oracle VM Manager to be discovered. You can enter the host name or IP Address when you execute the profile.  
Click Next to select the credentials of the Oracle VM Manager.
7. When you have the credentials of the Oracle VM Manager, click Select and the list of saved credentials are displayed. Select the appropriate credential from the list.  
Click New to display the Create Credentials window. Enter the following information:
  - Name and description for the credential.
  - Enter the username and password of the Oracle VM Manager. Re-enter the password to confirm.
  - Select the protocol and enter the port number.
 Click Ok to create the credential and click Next to review the summary of the Oracle VM Manager discovery parameters.
8. Click Finish to create the profile.

After creating the profile, execute the profile to discover the Oracle VM Manager. The following procedure describes how to execute the profile:

1. Select the discovery profile created for Oracle VM Manager.
2. Click the Add Assets Using Profile icon to launch the Add Assets wizard.
3. When you have not provided the details of the IP address or hostname in the profile, you must enter the details of the IP address or host name of the Oracle VM Manager.
4. Click Add Now to initiate the discovery job.

The Oracle VM Manager is considered an independent entity with which Oracle Enterprise Manager Ops Center integrates. The Oracle VM Manager appears in the Administration section of the UI, not as an asset in the Assets tree.

Figure 16–2 shows the Oracle VM Managers displayed in the Administration section of the UI.

**Figure 16–2 Oracle VM Manager**



When you discover an Oracle VM Manager, all of the Oracle VM Servers managed in it are also discovered and displayed in the Assets section. Existing server pools in the Oracle VM Manager are also displayed in the Server Pools view of the UI.

## Discover Oracle VM Servers

When you discover and manage an Oracle VM Manager, all of the known Oracle VM Servers to the manager are also discovered and displayed in the software UI. When you have manually installed Oracle VM Servers and not discovered in the Oracle VM Manager, you can still discover the Oracle VM Server in the Oracle Enterprise Manager Ops Center UI.

When you create a discovery profile for Oracle VM Server, you must define the Oracle VM Manager to which it can be associated. This makes the Oracle VM Server known to the Oracle VM Manager.

You must use SSH discovery of the Oracle VM Server when you want access to the serial console and perform advanced configuration in the Control Domain. For example, in Oracle Exalogic systems, you must use SSH discovery of the Oracle VM Server to support the use of InfiniBand switches.

### Discovery Profile for Oracle VM Server

The creation of discovery profiles is similar to Oracle VM Manager except for selecting the Discovery Type as Oracle VM Server. When you provide the Oracle VM Server host name or IP address, select the Oracle VM Manager with which you want to associate the Oracle VM Server.

**Figure 16–3** Select Oracle VM Manager

Execute the profile and discover the Oracle VM Server. This is a very basic discovery of the server. The storage and network configuration of the server are not populated in the UI and only basic information is displayed in the UI.

### SSH Discovery of Oracle VM Servers

Use this method when you want to access the serial console of the Oracle VM Server and perform advanced configuration.

To use SSH for discovery, define the credentials for the Oracle VM Server as explained in this procedure:

1. Select Credentials from the Plan Management section.
2. Click Create Credentials in the Actions pane.

The Create Credentials window displays.

3. Select the protocol SSH from the list.
4. Provide a name and description for the credential.
5. Select Password for Authentication Type.
6. Enter the root user and the password.
7. Click Ok to save the credential.

Create a discovery profile for the Oracle VM Server and select the credential created for ssh discovery. Discover the Oracle VM Server using the profile. Since the discovery of the Oracle VM Server is through the SSH discovery, the network and storage configuration of the server is populated in the UI.

## Installing Oracle VM Servers

You can provision Oracle VM Servers using Oracle Enterprise Manager Ops Center. You can download an Oracle VM Server image into the storage libraries, create OS provisioning profiles and then deploy a plan with the profile on the selected target. When you import an image into Oracle Enterprise Manager Ops Center, a default profile and plan are created automatically. See [Uploading or Importing ISO Images](#) to upload or import image into the software library.

### Hardware and Software Requirements

Oracle VM Server is a managed virtualization environment based upon the Xen hypervisor technology and includes a small Linux-based management operating system. For hardware and software requirements for installing Oracle VM Server, see *Oracle VM Installation and Upgrade Guide for x86*.

### Oracle VM Agent Installation

When you install Oracle VM Server through Oracle Enterprise Manager Ops Center, the Oracle VM Server is installed without Agent Controller. The Oracle VM Agent is installed automatically when you install Oracle VM Server. The Oracle VM Agent enables communication between the Oracle VM Manager and Oracle VM Server for all management tasks.

### Oracle VM Server Password Management

The provisioning profile of installing Oracle VM Server is similar to installing a Linux OS profile with additional steps to provide the Oracle VM Server password and the management interface. The Oracle VM Server password is different from the root password. This password is used by the Oracle VM Manager to manage and monitor the Oracle VM Server and the virtual machines running in it. You must use this password while discovering the Oracle VM Server from Oracle VM Manager.

## OS Provisioning Profile for Oracle VM Server

You can create OS provisioning profile for provisioning Oracle VM Servers.

### To Create a Provisioning Profile for Oracle VM Server

1. Select OS Provisioning profile in the Plan Management section.
2. Click Create Profile to create a new profile.
3. Provide a name and description for the profile.
4. Select Oracle VM Server for x86 in the subtype.

Click Next to specify the OSP parameters.

5. Select the Oracle VM Server from the list.

There are no specific software groups for Oracle VM Server. Click Next to specify the OS setup.

Optionally, you can select Include Custom Scripts to add some scripts to the installation. You will be directed to select the scripts in the subsequent steps.

6. Specify the time zone, language, terminal type and the root password for the OS. Also, specify the console baud rate and the serial port.

Click Next to specify the installation parameters.

7. Specify the following parameters for the Linux OS:

- Installation number – You can enter the installation number that is used to allow installation of all of the software that is included in your subscription.
- Partition action – Select whether you want to change the disk partition of the system.
- Install protocol – Specify HTTP or NFS as the install protocol.
- Kernel parameters – If necessary, enter kernel parameters for the GRUB menu of the target system.
- Linux packages – You can specify the Linux packages to include or exclude during provisioning. To include a package, enter the package name in a line. To exclude a package, enter the package name preceded by a dash (-).

The options MD5 Checksum, Reboot action, Initialize Disk label, Use Shadow passwords, and Clear master boot record are enabled by default.

Click Next to specify the volume groups when you are using Logical Volume Manager.

8. Select Use Logical Volume Manager when you want to specify the volume groups in the Logical Volume Manager for the hard disk drives.

Click Next to specify the disk partitions and file systems.

9. Specify the disk partitions and file systems that you want to create on the target system. For the file system device, you can also select the logical device name.

Click Next to specify the naming service.

10. Specify the name service, domain name and the corresponding name server. You can select the following name service:

- **DNS** – Enter the domain name of the DNS server. Provide the IP address of the DNS server in the Name Server field. You can enter up to three IP addresses as the value for the Name Server. Provide the additional domains to search for name service information in the Domain Name Search List. You can specify up to six domain names to search. The total length of each search entry cannot exceed 250 characters.
- **NIS or NIS+** – Enter the domain name of the NIS or NIS+ server. When you know the NIS server details, choose the option Specify an NIS Server and provide the NIS server host name and the IP address.
- **LDAP** – Enter the domain name of the LDAP server. Specify the name of the LDAP Profile you want to use to configure the system. Enter the IP address of the LDAP Profile Server. You can also optionally provide the Proxy Bind Distinguished Name and Password.



- **None** – Select None when there is no naming service configured.

Click Next to specify the network.

**11.** Select None to continue to specify the networks.

You can bond the interfaces after provisioning the Oracle VM Server. Select the Linux OS and aggregate the links.

**12.** Click the Add icon to add multiple networks.

All of the networks that are defined in Oracle Enterprise Manager Ops Center are displayed in the Network list. Enter the following information for each selected network:

- Select a NIC from the list of available logical interfaces for each network.
- Select the Address Allocation Method for the selected networks except the boot interface.

When you have selected Use Static IP for Address Allocation Method, then you must provide the IP address when you apply a plan with this profile. The specific IP address is assigned to the target system after provisioning.

Click Next to specify the Oracle VM Server parameters.

**13.** Enter the password to be used by the Oracle VM Agent. This password is used by the Oracle VM Manager to manage and monitor the Oracle VM Server. Re-enter the password to confirm it.

**Figure 16–4 Oracle VM Server Password**

The screenshot shows a configuration window titled "Specify Oracle VM Server Parameters". At the top right, there is a legend: "\* Indicates Required Field". Below this, the text reads "Specify the setup configuration for the Oracle VM Server." There are three input fields:
 

- The first field is labeled "\* Oracle VM Server Password:" and is empty.
- The second field is labeled "\* Oracle VM Server Password Confirm:" and is empty.
- The third field is labeled "Oracle VM Server Management Interface:" and contains the text "GB\_0".

**14.** Specify the management interface, then click Next.

**15.** Review the information in the Summary, then click Finish to create the profile.

## Apply Deployment Plan for Oracle VM Server

When you create a profile for provisioning Oracle VM Server, you can select the option to create a deployment plan with the profile. Either apply the created plan or create your own deployment plan.

### To Apply a Deployment Plan for Oracle VM Server for x86

1. Select the plan created for provisioning Oracle VM Server in the Plan Management section.
2. Click Apply Deployment Plan in the Actions pane.
3. Specify the network resources defined in the profile. Provide the IP address for the boot interface.

4. It is optional to provide a host name for the Oracle VM Server.  
Click Next to select the Oracle VM Manager.
5. It is optional to select an Oracle VM Manager from the list to discover and manage the Oracle VM Server. You can select None when you do not want to associate with an Oracle VM Manager.  
  
You can also place the Oracle VM Server in one of the server pools of the selected Oracle VM Manager. After provisioning, a separate job is initiated to add the Oracle VM Server to the server pool.  
  
Click Next to schedule the job.
6. Schedule the provisioning job to run now or at a later time.
7. Review the summary and click Apply to launch the provisioning job.

## Administration of Oracle VM Manager

The list of Oracle VM Managers discovered and managed in Oracle Enterprise Manager Ops Center are displayed in the Administration section.

Select an Oracle VM Manager and the following information is displayed as shown in [Figure 16–5](#).

**Figure 16–5 Oracle VM Manager View**

The screenshot displays the 'Summary' page for an Oracle VM Manager. The page is titled 'xvm-vhost18.fr.oracle.com' and has tabs for 'Summary', 'Storage', 'Networks', and 'Incidents'. The main content area shows the following information:

- Oracle VM Manager Name: xvm-vhost18.fr.oracle.com
- Oracle VM Manager UUID: 0004fb0000010000224378d24d7bc8a
- Description: 10.166.88.178
- Oracle VM Manager Version: 3.0.3.126
- Server Pools: 1
- Servers: 2
- Virtual Machines: 3
- Storage Servers: 2
- Storage Repositories: 1
- Networks: 1

Additional information on the right side includes:

- Reachable: Yes
- YUM Repository Name: -
- YUM Repository URL: -
- YUM GPG Key: -

There is a 'Tags' section with a table for Tag Name and Value.

At the bottom, there is a table for 'Server Pools (1)':

Server Pool Name	Description	Oracle VM Servers	Virtual Machines
OvmPool	0		

The Summary page displays information about the Oracle VM Manager, the list of server pools, the discovered Oracle VM Servers, and the virtual machines that are created in the corresponding Oracle VM Servers.

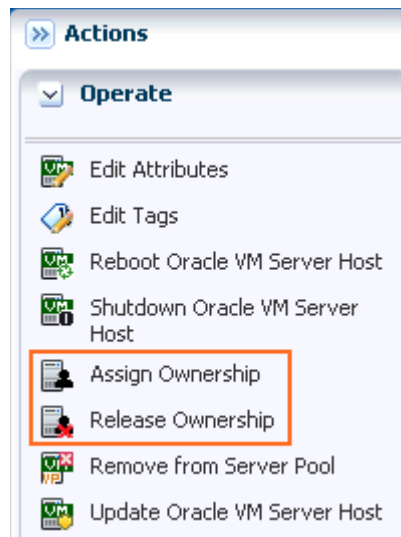
## Manage Ownership of Oracle VM Servers

To use the Oracle VM Servers in the server pool and create virtual machines, it is required that you take ownership of the Oracle VM Server from the Oracle VM Manager.

Oracle VM Manager must take ownership of the Oracle VM Servers. You can either assign ownership from the Oracle VM Server or take ownership through the Oracle VM Manager.

When you select an Oracle VM Server in the Assets section, the Assign Ownership and Release Ownership actions are available in the Actions pane.

**Figure 16–6 Assign and Release Ownership From Oracle VM Server**



When you select the Oracle VM Manager from the Administration section, the Take Ownership and Release Ownership options are available in the Actions pane.

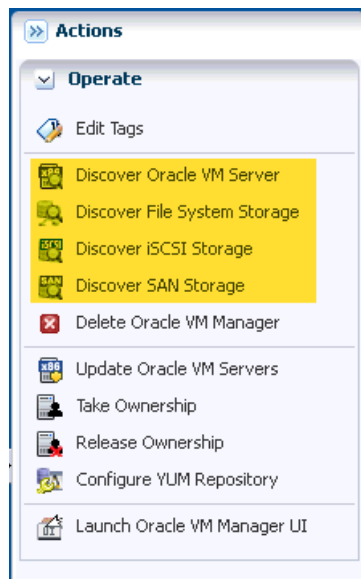
When you take ownership of the Oracle VM Servers, you can add them to server pools and create virtual machines in them.

## Discover Storage Resources

When you discover an Oracle VM Manager, Oracle Enterprise Manager Ops Center provides the option to discover the storage servers attached to it.

The following discovery options are available from the Oracle VM Manager:

- File system storage
- iSCSI storage
- SAN storage

**Figure 16–7 Discover Storage Resources from Oracle VM Manager**

Create discovery profiles for the storage servers and save them.

When you select to discover a storage server, existing discovery profiles are searched for the selected storage type. You can select from an available profile. When there are no profiles available, then the wizard to discover the corresponding storage server appears.

When you discover a storage resource, existing resources such as virtual disks, templates, ISO images, and virtual machine metadata are also discovered and displayed.

See [Chapter 6, "Storage Libraries"](#) for more information about the storage servers and the discovering them in Oracle Enterprise Manager Ops Center.

## Manage Storage Resources

You can have the following type of libraries setup for storage of Oracle VM resources:

- **Filesystem Storage Libraries**

Oracle Enterprise Manager Ops Center provides an option to create Oracle VM Storage Repositories. A storage repository is a logical disk space made available through a file system on top of physical storage hardware. The supported types of file system are NFS and OCFS. When the storage repository is created on an NFS file server, it is a NFS based storage repository. The NFS file server consists of NFS file systems. When the storage repository is created on a LUN, it is a LUN-based repository. The OCFS file system is created on the storage server. You can create storage repositories on these file servers to be used by Oracle VM Servers to store resources. The resources include virtual machine metadata, templates, assemblies, ISO images and virtual disks.

To create Oracle VM storage repositories, you must have an Oracle VM Server discovered. Only NFS-based repositories can be shared by multiple server pools.

- **Static Block Storage Libraries**

The LUNs from the storage arrays that are not managed by Oracle Enterprise Manager Ops Center form the static storage libraries. The LUNs are addressed by

iSCSI or Fibre Channel protocols. This forms the iSCSI and SAN static storage libraries. You can also add LUNs exported from managed storage arrays. The LUNs can belong to one library at a time.

- **Dynamic Block Storage Libraries**

The storage servers that are discovered and managed in Oracle Enterprise Manager Ops Center are presented under dynamic block storage libraries. The dynamic block storage libraries contains the exported LUNs from the storage array servers.

See [Chapter 6, "Storage Libraries"](#) for more information about discovering your storage servers, storage connect plug-ins, creating storage libraries and managing the libraries.

## Manage Networks

During the installation of Oracle VM Server, the network interface used for the management is configured as a bonded interface. The bond is created with one interface and named as `bond0`. You can create additional bonds to add redundancy and load balancing of your network environment.

You can attach networks to the Oracle VM Server or to the server pool that consists of a group of Oracle VM Servers on an Oracle VM Manager. Configure the network interfaces or the bonds to the network to be attached. You can assign different roles or functions to the networks attached to the Oracle VM Server.

The following are the network roles available for an Oracle VM Server:

- **Server Management**– Manages the Oracle VM Servers in a server pool. There is only one Server Management network per Oracle VM Manager.
- **Live Migrate** – This is used to migrate the virtual machines from one Oracle VM Server to another in the server pool, without changing the state of the virtual machine.
- **Cluster Heartbeat** – This is used to check whether all the Oracle VM Servers in the server pool are up and running.
- **Virtual Machine** – This is used for the network traffic between the different virtual machines in a server pool.
- **Storage** – This is used for all storage transport in a server pool. It is used by the virtual machines to connect to the virtual disks.

The management network created during the installation of Oracle VM Server has the following roles:

- Server Management
- Cluster Heartbeat
- Live Migrate

You can add and remove the roles of this management network, except for the Server Management role.

Depending on the available network interfaces on the Oracle VM Server, you can attach networks to Oracle VM Server and assign different roles to the networks. For example, you can attach the network in which your storage servers are placed and assign the Storage role to that network. You can assign a network with Live Migrate to be used only for migration.

For more information about setting different roles for network, refer to the *Oracle VM User's Guide* .

## Attach Networks

You can attach networks to the Oracle VM Server using the option Attach Network. When the Oracle VM Server is placed in a server pool and the server pool is associated with an user-defined network domain, you must add the network to the network domain.

1. Select the Oracle VM Server or the server pool.
2. Select Attach Networks from the Actions pane.

The Attach Network wizard displays. The list of available networks in the network domain are displayed with the current connection to the Oracle VM Server.

3. Select one or more networks that you want to attach to the Oracle VM Server or the server pool.

---

---

**Note:** You cannot make multiple connections to the same network. You can connect to a network only once.

---

---

Click Next to configure the networks.

4. You cannot make more than one connection to the network. Do not increment the number of connections.

Click Next to configure the interfaces to the network.

5. For each selected network, select the NIC and the IP address.
  - **NIC**– You can select an available NIC from the list. When the networks have different VLAN IDs, then you can assign the same NIC to another network. Otherwise, you cannot assign the same NIC to different network connection. When supported by the network, you can also select System Allocated for the system to take care of the NIC allocation.
  - **IP Address** – Select Use Static IP to provide the IP address manually or select Use System Allocated IP Address for the system to take care of the IP address allocation.

Click Next to view the summary of the selected information.

6. Review the information provided and click Finish to attach the networks to the Oracle VM Server or the server pool.

## Manage Oracle VM Servers

When you install or discover the Oracle VM Server through the Oracle Enterprise Manager Ops Center UI, take ownership of the server from the Oracle VM Manager. This helps to place the Oracle VM Servers in the server pool. These are some of the management functions available for managing Oracle VM Servers:

- Edit Oracle VM Server information
- Reboot the server
- Shutdown the server

- Update the server
- Edit IPMI configuration

## Edit Oracle VM Server Information

Select the Oracle VM Server and click Edit Attributes in the Actions pane. You can edit the following Oracle VM Server information:

- Name
- Description
- Tags

## Edit IPMI Configuration

Intelligent Platform Management Interface (IPMI) allows you to remotely power off an Oracle VM Server, and to send a Wake-on-LAN message to power on an Oracle VM Server without having to physically press the power button. You can edit the IPMI configuration in the following method:

1. Select the Oracle VM Server and click Edit IPMI Configuration in the Actions pane.

The Edit IPMI Configuration window displays.

**Figure 16–8 IPMI Configuration**

The screenshot shows a dialog box titled "Oracle Enterprise Manager Ops Center - Edit IPMI Configuration". Inside the dialog, there is a section titled "Edit IPMI Configuration" with the Oracle logo. Below this, there are four input fields, each preceded by an asterisk and the text "\* Indicates Required Field". The fields are:
 

- \* Username: [text input field]
- \* Password: [password input field]
- \* Confirm Password: [password input field]
- \* IP Address: [text input field]

 At the bottom right of the dialog box, there are two buttons: "OK" and "Cancel".

2. Enter the following information for IPMI configuration:
  - Username for the IPMI
  - Password for the IPMI
  - IP address of the IPMI
3. Click Ok to enter the IPMI configuration.

## Place Oracle VM Server in Maintenance Mode

To perform hardware or software maintenance, an Oracle VM Server can be placed in maintenance mode. When an Oracle VM Server is placed in maintenance mode, all of the virtual machines running on the Oracle VM Server are automatically migrated to other Oracle VM Servers in the server pool, if they are available, otherwise they are

stopped. When the Oracle VM Server is the master Oracle VM Server in the server pool, this role is moved to another Oracle VM Server in the server pool, if available.

1. Select the Oracle VM Server and click Place in Maintenance Mode in the Actions pane.
2. Click Place to confirm the action.

The Oracle VM Server is placed in maintenance mode.

When you have finished with the maintenance on the Oracle VM Server and you are ready for it to rejoin the server pool, select the option Remove From Maintenance Mode.

## Update Oracle VM Server

Using a YUM repository, update or upgrade Oracle VM Servers. To access patch updates for Oracle VM, contact Oracle to purchase an Oracle VM Support contract and gain access to the Unbreakable Linux Network (ULN) which contains updates for Oracle VM. When you have access to ULN, you can use this to set up your own Yum repository to use when updating your Oracle VM Servers.

### Configure YUM Repository

A YUM repository is required to update or upgrade Oracle VM Servers that are attached to an Oracle VM Manager. Set up a YUM repository and configure for automatic updates of the Oracle VM Servers managed by an Oracle VM Manager. Setting up a YUM repository is beyond the scope of this document.

After you set up a YUM repository, select the Oracle VM Manager and click Configure YUM Repository in the Actions pane. Enter the following details of the repository to configure it.

- Yum Repository Name – A name for the Yum repository.
- YUM Base URL – The URL to access the Yum repository, for example, the Oracle public YUM repository is at:  
<http://public-yum.oracle.com/>
- Enable GPG Key – Select whether to use the GPG Key for the Yum repository. The GPG key or GnuPG key is the GNU project's implementation of the OpenPGP key management standard.
- Yum GPG Key – This field is enabled when you select Enable GPG Key. Enter the GPG key for the Yum repository, for example:

`http://public-yum.oracle.com/RPM-GPG-KEY-oracle-e15`

The GPG key must be available through HTTP, FTP, or HTTPS protocols. The GPG key for Oracle-signed updates from ULN is pre-installed on the Oracle VM Server at `/etc/pki/rpm-gpg/RPM-GPG-KEY-oracle`. When you want to use this GPG key, enter as:

`file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle`

### To Update Oracle VM Server

1. Configure the Yum repository.
2. Select the Oracle VM Server and click Update Oracle VM Server Host in the Actions pane.



When you update the Oracle VM Server, the server is placed into maintenance mode and then the update is performed. When there are virtual machines in the Oracle VM Server, they are migrated to other Oracle VM Servers in the server pool, if they are available, otherwise they are stopped. After the update, the Oracle VM Server remains in maintenance mode. Select the option Remove From Maintenance Mode.

## Create Server Pool

You can group one or more Oracle VM Servers in an Oracle VM Manager and create server pools. You must create server pools before you start creating virtual machines. You can apply the virtual machines plans only on Oracle VM Servers that are in a server pool.

This section describes only how to create server pools using Oracle Enterprise Manager Ops Center. For more information about server pool policies, and managing server pools, see [Chapter 17, "Server Pools"](#).

When you create a server pool for Oracle VM Server for x86 systems, you must have the following information defined:

- Cluster file system
- Server pool master
- Virtual IP address for the server pool master

### Cluster File System

Shared access to the server pool resources is a must for providing for high availability for the virtual machines running in the Oracle VM Servers of the server pool. This is achieved by cluster file system OCFS2 which allows multiple Oracle VM Servers to access the same disk at the same time. OCFS2 ensures that the Oracle VM Servers in a server pool can access and modify resources in the shared repositories in a controlled manner.

When you create a server pool, you must specify the server pool file system for the cluster heartbeat and other cluster information. The file system can be NFS shares or LUNs of iSCSI or SAN-based storage servers. Oracle VM formats the server pool file system as OCFS2 file system.

In Oracle Enterprise Manager Ops Center, the cluster is always enabled by default. The cluster configuration is pushed out to all the Oracle VM Servers in the server pool and the cluster heartbeat starts when the server pool is created. You can set a separate network for this cluster heartbeat. See [Manage Networks](#) for more information about setting up the networks and its role for an Oracle VM Server.

### Server Pool Master

An Oracle VM Server is internally elected as Server Pool Master. You cannot set the role for an Oracle VM Server. When the elected Oracle VM Server fails, the role is set for another Oracle VM Server in the server pool. The virtual IP address provided while creating the server pool is assigned to the Oracle VM Server that has been elected as server pool master.

## Server Pool Policies

The server pool policies that are applicable for Oracle VM Server for x86 are as follows:

- Set the CPU utilization threshold. Places the virtual machines on the Oracle VM Server that has the lowest relative load.

- Set the CPU utilization threshold. Places the virtual machines on minimum number of Oracle VM servers to minimize the power consumption.
- You can select the automatic load balancing so that the virtual machines can be migrated automatically in the server pool whenever the thresholds are exceeded.

When you enable automatic load balancing for Oracle VM Server for x86 server pool, the server pool is checked continuously for the selected placement policy. When the threshold exceeds, the virtual machines are migrated from one Oracle VM Server to another.

When you have selected power minimization and automatic load balancing policy, and the servers in the server pool are not over loaded, then some of the Oracle VM Server host servers are freed up from the logical domains and powered off to minimize power consumption.

When the servers are overloaded and there are no other servers in the pool to host the virtual machines, then the policy will start a powered-off server using its Wake-on-LAN capability and live migrate the virtual machines to take up the load. It is necessary that the Wake-on-LAN capability must be enabled on the BIOS of the Oracle VM Server.

- When an Oracle VM Server fails, the virtual machines are migrated to another Oracle VM Server in the server pool, when you have selected Enable High Availability while creating the virtual machine.

## Create Oracle VM Server for x86 Server Pools

The following procedure describes the steps in the wizard to create an Oracle VM Server for x86 server pool.

1. Select Server Pool in the Systems Group list on the Navigation pane.
2. Click Create Server Pool in the Actions pane.

The Create Server Pool wizard displays.

3. In the Identify Server Pool step, enter the following information:

- Name and description of the server pool.
- Enter tags for categorizing your server pool.
- Select Oracle VM Server for x86 from the Virtualization Technology.

Click Next to define the server pool configuration.

4. Define the following configuration details:

- Select the Oracle VM Manager in which the Oracle VM Servers are discovered and owned.
- Select the network domain.
- Select a network from the list of networks available in the network domain.
- Enter the virtual IP address that is assigned to the server pool master. When the server pool master changes, the IP address is assigned to the new Oracle VM Server.
- Select the server pool file system to store cluster heartbeat and other cluster information. The file system can be either NFS shares on a NFS file servers or LUNs of SAN and iSCSI based storages. The NFS file servers and the storage servers are known and reachable to the selected Oracle VM Manager.

Click Next to select the members of the pool.

5. Select one or more Oracle VM Servers to add to the server pool.

The list of Oracle VM Servers displayed have the following characteristics:

- Owned by the Oracle VM Manager. Refer to [Manage Ownership of Oracle VM Servers](#) to own an Oracle VM Server.
- Not associated with server pool.
- In a healthy state.
- Not placed in maintenance mode.
- Do not have virtual machines in running, shutdown or suspended state.

Select Oracle VM Servers that are compatible for migration of virtual machines. To migrate virtual machines within a server pool, the Oracle VM Servers systems must be identical in model.

Click Next to associate the network domain.

6. Select the network domain to associate with the server pool.

- When you have selected default network domain, then go to Step 7.
- For a user-defined network domain, select the physical interfaces of each selected servers to connect to each fabric in the network domain. You cannot bond the interfaces in Oracle VM Server for x86. Bonding can be done in only individual OS of the Oracle VM Server.

Click next to select the networks and associate with the server pool.

7. For default network domain, all the networks that are declared and managed in Oracle Enterprise Manager Ops Center are listed. For an user-defined network domain, only the networks assigned to it are listed.

Select the networks that you want to associate with all the servers in the server pool. You cannot make multiple connections to a network. Limit the number of connections to 1.

Click Next to configure the interfaces of the servers.

8. For each network connection, specify the following details:

- Specify the NIC and IP address for each network connection. When a selected server is connected to the network, then no rows are displayed for that server.
- You can assign the same NIC to different network connection when the networks have different VLAN IDs.
- When supported by the network, you can select System Allocated for the NIC and IP address to be automatically allocated by the system.

Click Next to associate the storage libraries.

9. The storage libraries that are reachable from the selected members of the pool are displayed. The storage libraries are required to store virtual machine metadata, ISO images, and for virtual disks of virtual machine.

You can select the following type of storage libraries:

- **Filesystem Storage Libraries** – This includes the Oracle VM storage repositories. It is recommended to have at least one Oracle VM storage repository associated with the server pool.

- **Block Storage Libraries** – This includes the Static Block Storage and Dynamic Block Storage. Static block storage libraries comprises the exported LUNs of storage arrays that are not managed by Oracle Enterprise Manager Ops Center. Dynamic block storage libraries comprises the exported LUNs of storage array servers that are discovered and managed in Oracle Enterprise Manager Ops Center.

Select the storage libraries from the list that you want to associate with all the virtualization hosts in the server pool.

Click Next to select the server pool policies.

10. You must select the following policies in the server pool to manage the under utilized and overutilized servers in the pool:

- **Placement Policy** – This policy decides the preferred virtualization host in the server pool to place the logical domains.
- **Auto Balancing Policy** – This policy will perform load balancing of the server pool automatically at set intervals.

11. Select one of the following placement policies:

- **Lowest relative load** – The recent lowest memory and CPU utilization for the Oracle VM Servers in the server pool are calculated. Based on this, the server with the lowest relative load is considered to place a virtual machine. Provide the threshold for CPU utilization above which the server is considered to be over-utilized and virtual machines are migrated to server with lowest relative load.
- **Minimize power consumption** – The virtual machines running in a server pool are placed on the minimum number of Oracle VM Servers so that the unused Oracle VM Servers can be powered off. The threshold value set for the server over-utilization will ensure that the servers are not over-loaded. Otherwise, the powered off Oracle VM Servers can be powered on to host the virtual machines.

12. Select the automatic load balancing policies:

- Select automatic load balancing and set the interval in which the server pool must be checked for resource balancing. You can set the approval to migrate the virtual machines automatically. Or send notifications about the approval.
- You cannot manually balance the resources.

Click Next to view the summary of the server pool details.

13. Review the information to create a server pool for Oracle VM Server for x86. Click Finish to create the server pool.

## Create Virtual Machines

A virtual machine comprises configurable set of resources and its own operating system. The resources include virtual CPU, memory, network, and virtual disk. You can start, stop, and restart each virtual machine independently. You can create virtual machines using one of the following installation sources:

- Templates
- Existing virtual machines
- ISO images in storage libraries

- Mounted ISO images on NFS, HTTP or FTP server
- Netboot

The operating system provisioned on the virtual machines can be hardware virtualized, paravirtualized and, hardware virtualized with paravirtualized drivers. Based on these virtualization types, you select the appropriate option to create the virtual machines.

---

---

**Note:** You can create virtual machines only in an Oracle VM Server for x86 server pools.

---

---

## Virtualization Types

The following virtualization types are available for a virtual machine:

- **HVM**  
Hardware virtualization or fully virtualized. For HVM, select an ISO image from the storage library and create a virtual machine. You must activate the hardware virtualization in the BIOS of the Oracle VM Server in which you want to create the virtual machine. The OS might be completely unmodified.
- **PVM**  
Paravirtualized. You must use an ISO file mounted from an NFS share, HTTP, or FTP server. The OS is modified and recompiled to be made aware of the virtual environment. The paravirtualized guests run at near native speed, since most memory, disk and network accesses are optimized for maximum performance.
- **PVHVM or HVM with PV Drivers**  
Hardware assisted virtualization with a paravirtualized driver. Install paravirtualized drivers on the hardware virtualized machines for optimized performance. This is mainly used for running Microsoft Windows guest operating systems.

## Create Virtual Machine Profile

You can capture the virtual machine requirements in the form of profile in Oracle Enterprise Manager Ops Center. Create a deployment plan with this profile and apply it on the selected targets. You can use these profiles and plans to create more than one virtual machine at a time.

### To Create a Virtual Machine

1. Select Virtual Machine under Profiles and Policies in Plan Management section.
2. Click Create Profile in the Actions pane.  
The Create Profile - Virtual Machine wizard displays.
3. Enter the name and description of the profile.  
Select Create a deployment plan for this profile to automatically create a plan using this profile. Click Next to specify the installation source of the virtual machine.
4. Select an installation source for creating the virtual machine. You have the following options to select from:

- **Templates** – Templates are pre-configured, pre-installed virtual machine. You must upload the templates into Oracle VM Storage Repositories. In the profile, the available storage repositories and the corresponding available templates are listed. Select a storage library and template.
- **Existing Virtual Machine** – When there are existing virtual machines, select the storage repository and the virtual machine image stored in it.
- **Install from ISO image (HVM)** – You must have imported ISO images into the storage repository. Select the library and an ISO image from the list.
- **Install from mounted ISO image (PVM)** – Mount the required ISO files to a NFS share, HTTP or FTP server and it must be accessible from the Enterprise Controller. Provide the network path of the mounted ISO file. For example, an ISO image accessed through HTTP server is represented like this.

`http://example.com/Enterprise-R5-U6-Server-x86_64-dvd.iso/`

- **Install from Network (Netboot)** – Use this option only to create the virtual machine with Network as the boot order. You must provision the OS separately on it.

Select an option for the installation source and click Next to identify the virtual machines created.

5. Provide a name for the virtual machine and the number to be appended to the name. You can create one or more virtual machines simultaneously using this profile. To provide unique name for the virtual machines, enter the prefix name and the number to start the series.

For example, if the prefix name is VMachine, the number to start from is 10 and the number of virtual machines to be created is 3, then the virtual machines are created with the name VMachine10, VMachine11, and VMachine12.

6. Provide the description and tags for the virtual machine. All the virtual machines created with this profile carry the same description and tags. Use the tags to group the virtual machines based on the role.

Click Next to specify the configuration of the virtual machine.

7. When you have the installation source selected as templates or existing virtual machine, the values for all the parameters are set from the template. Otherwise, you must provide the following parameters:
  - **VM Type** – Based on the installation source, select the type as HVM, PVM or HVM with PV Drivers. For HVM, you must have the ISO image in the storage library. For PVM, you must use mounted ISO images.
  - **OS** – Select the OS from the list that will be installed on the virtual machine.
  - **Enable High Availability** – High availability is to ensure the uninterrupted availability of a virtual machine. When an Oracle VM Server shuts down or fails in a server pool, all the virtual machines will be migrated to other Oracle VM Servers in the server pool. High availability is implemented only in server pool.
  - **CPU Threads** – The number of CPU threads to be used by the virtual machine.
  - **CPU Priority** – The CPU priority of the virtual machine. You can select a high (100), intermediate (50), or low (1) priority for the virtual CPUs. The higher the priority more number of physical CPU cycles are allocated to the virtual machine.

- **CPU Cap** – This parameter defines the maximum percentage to which the virtual CPUs can receive scheduled time. Set this option to keep the low priority virtual machines from using too many CPU cycles.
- **Memory** – The size of the memory the virtual machine is allocated to use when starting it.
- **Boot Property** – Select whether you want to start the virtual machine after creation.

Set these parameters and click Next to specify the boot configuration.

8. Select the boot media and order for the virtual machine. The boot options are set according to the installation source.

The default boot order for different installation source are:

- Templates – Disk
- Existing Virtual Machines – Disk
- HVM using ISO image – CDROM and Disk
- PVM using mounted ISO image – Network and Disk
- Netboot – Network

Select the correct order when you want to modify the boot order. Click Next to select the storage resources for virtual machine.

9. Select the storage resources to store the virtual machine configuration, also known as virtual machine metadata, and the virtual disks.

Use the following libraries for the virtual machine:

- **Oracle VM Storage Repositories** – The Oracle VM storage repositories are NFS file servers that are used to store virtual machine metadata, ISO images and virtual disk images. You can store the virtual machine metadata only in Oracle VM storage repositories. When you use the storage repository for virtual disk storage, you can either create a virtual disk or select existing virtual disks that are unshared and unused. You can also select ISO images to a virtual machine for HVM and PVHVM types.
  - **Static Block Storage Libraries** – These are the storage array servers that are not managed by Oracle Enterprise Manager Ops Center but reachable to the Oracle VM Servers in the Oracle VM Manager. Select the LUNs that are exported as iSCSI and SAN storage types.
  - **Dynamic Block Storage Libraries** – The exported LUNs that are available from the storage servers that are managed by Oracle Enterprise Manager Ops Center. Select the existing LUNs that are available from the storage servers. You can also create LUNs by specifying the volume group and the size of the LUN.
10. When you select to create virtual machines from existing virtual machines or templates, you are required to select the clone type for the virtual disks. You can select the following clone types:
    - **Sparse type** – This clone type is a disk image file of a physical disk, taking up only the amount of space actually in use; not the full specified disk size.
    - **Non-sparse type** – This clone type is a disk image file of a physical disk, taking up the space equivalent to the full specified disk size, including empty blocks.

Select the appropriate storage library, specify the virtual disks, disk size, and click Next to select the networks.

11. Select the network domain, and the networks that must be attached to the virtual machine.

You can connect to one or more networks. The number of connection to a network is limited to 1.

Click Next to view the summary.

12. Review the information provided to create a virtual machine profile. Click Finish to create the profile.

Create a deployment plan with this profile and apply the plan to create virtual machines. Except for the installation source Netboot, all the other source types results in creating a virtual machine with the OS installed. For virtual machine created with Netboot installation source, you must provision the OS on it separately using an OS provisioning plan.

The next section describes the different methods of deployment of virtual machine plans to create virtual machines.

## Create and Deploy Virtual Machine Plan

This section describes how to create virtual machines and provision OS in an Oracle VM Server using Oracle Enterprise Manager Ops Center.

There are two new deployments plans for provisioning and creating multiple virtual machines:

- Single step deployment plan to create only virtual machines
- Multi-step deployment plan to create virtual machine, provision OS, and install other applications.

In the single step deployment plan, the virtual machine can be created using Oracle VM templates or ISO images stored in Oracle VM repositories. Or only a virtual machine is created with ready to be booted using a separate OS provision plan.

In the complex deployment plan, you can configure and install the virtual machine, provision the OS, install software applications, apply monitoring profiles, and operational plans.

### To Apply a Create Virtual Machine Plan

This is a single step virtual machine plan that will create a virtual machine and the OS will be installed depending on the installation source selection. When you create HVM or PVHVM type virtual machines, select the ISO image that will be used to create the virtual machine. You can select only one ISO image and multiple ISO files are not supported. While selecting the virtual disks, you have the option to select the ISO image. The following procedure describes how to apply the plan for creating a virtual machine:

1. Select the Virtual Machine plan in the Plan Management section.
2. Click Apply Deployment Plan in the Actions pane.
3. Select the targets on which you want to apply the plan. Click Add Targets to List.

You can apply the plan only on the Oracle VM Server for x86 server pools. You cannot create virtual machines on Oracle VM Servers that are not part of a server pool.



4. Select to apply the plan with minimal interaction when you do not want to modify the parameters in the profile.

Click Next.

5. You can modify the virtual machine identification, if required.

Click Next to specify the storage resource assignments.

6. The storage resources from the profile are populated. When the storage libraries are not available for a selected target, it is flagged in red. Modify the storage resources accordingly.

7. For the selected storage library, define the virtual disks.

- For Oracle VM Storage repositories, you can create new virtual disks, select existing disks, or select ISO images. Select ISO image option is available only for HVMM and PVHVM type virtual machines. Provide a disk name, select an existing disk or an ISO image.
- For Static Block Storage, select an available LUN from the list.
- For Dynamic Block Storage, either select an available LUN from the list or create a new LUN. When you create a new LUN, select the volume group and enter the size of the LUN.

Click Next to provide the network resources.

8. The network selected in the profile is populated. When the network is not available for a selected target, it is flagged in red. Modify the network resource.

9. Specify the network resource and the IP address for the virtual machine.

Click Next to view the summary.

10. Review the information provided and click Apply to apply the plan on the selected targets.

Except for the virtual machine created with Netboot as the installation source, all the other virtual machines are installed and provisioned with the OS.

Use the complex plan [Configure and Install Virtual Machines](#) to install the virtual machine and provision the OS on it. See [Chapter 8, "Plans and Profiles"](#) for more information about complex plans.

## Provisioning OS on Virtual Machines

You can install OS on the virtual machines created on the Oracle VM Server. OS provisioning profiles to install OS can be used to provision the OS on the virtual machines. You can refer to [Chapter 12, "Operating Systems"](#) for more information about creating provisioning profiles and plans to install an OS.

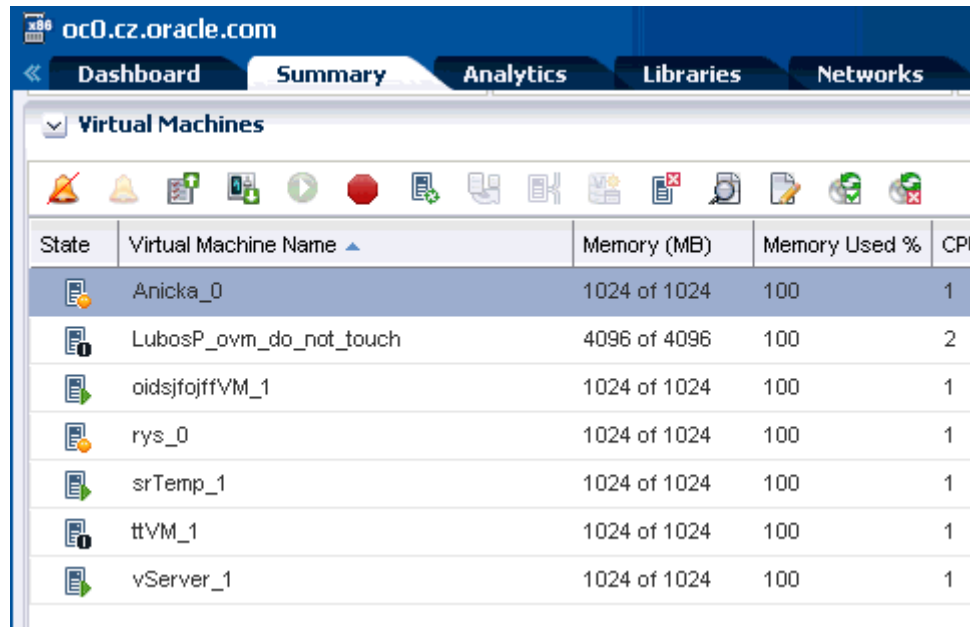
## Manage Virtual Machines

Oracle Enterprise Manager Ops Center provides options to manage the lifecycle operations of virtual machines. You can start, suspend, resume, shut down, and delete virtual machines on the UI.

When you select the Oracle VM Server in the Assets section, the Summary tab in the center pane lists all the virtual machines that are currently running. All the options required to manage a virtual machine is available on the UI.

[Figure 16–9](#) shows the actions available for a virtual machine from Oracle VM Server.

Figure 16–9 Action Icons for Virtual Machines



State	Virtual Machine Name	Memory (MB)	Memory Used %	CPU
	Anicka_0	1024 of 1024	100	1
	LubosP_ovm_do_not_touch	4096 of 4096	100	2
	oidsjfojffVM_1	1024 of 1024	100	1
	rys_0	1024 of 1024	100	1
	srTemp_1	1024 of 1024	100	1
	ttVM_1	1024 of 1024	100	1
	vServer_1	1024 of 1024	100	1

### Starting a Virtual Machine

Select the virtual machine and click the Start Selected Guest icon. The job is initiated to start the virtual machine.

### Suspending a Virtual Machine

Select the virtual machine and click the Suspend Selected Guest icon. When you suspend a virtual machine, you cannot use the virtual machine. Click Ok to confirm the suspend action.

### Rebooting a Virtual Machine

Select the virtual machine in the running state and click the Reboot Selected Guest icon. Click Reboot Guest to confirm the action.

### Shutting Down a Virtual Machine

Select the virtual machine and click the Shut Down Guest icon. When you shut down a virtual machine, it is disconnected from its network. Click Ok to shut down the virtual machine.

### Deleting a Virtual Machine

Select the virtual machine and click the Delete Selected Guest icon. Click Ok to confirm deleting the virtual machine. When you delete a virtual machine, all the references to the virtual machine such as the metadata and disk images are deleted from the system.

All these options are also available in the Actions pane when you select the virtual machine in the Assets section.

## Edit Boot Order

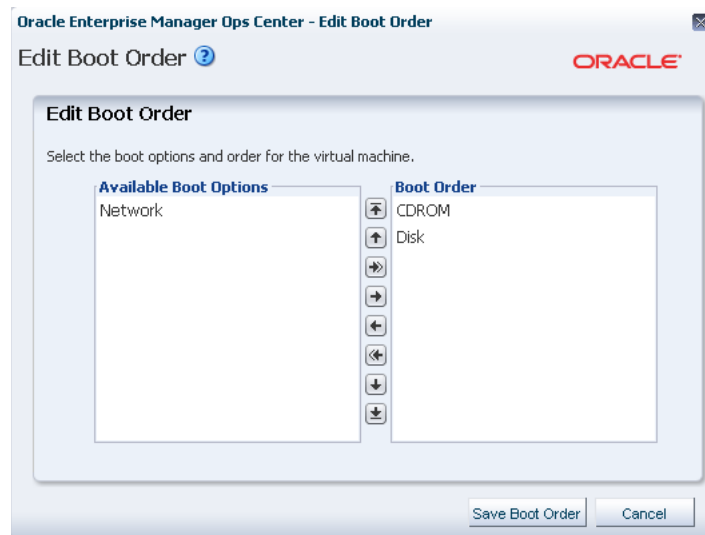
The boot order that you have set during virtual machine installation is displayed. You can modify the boot order. You must specify the appropriate boot order depending on the installation source of the virtual machine. The following list shows the preferred boot options for different installation source:

- Hardware Virtualized Machine (HVM) – CDROM and Disk
- Paravirtualized Virtual Machine (PVM) – Network and Disk
- Templates and existing virtual machines – Disk
- Netboot – Network

If the virtual machine is in running state, then the modified boot order takes effect on the next reboot. Ensure to select the correct boot order for the virtual machine.

The Edit Boot Order option is available in the Actions pane of a selected virtual machine appears as shown in the figure:

**Figure 16–10**



Modify the boot order and click Save Boot Order to save the changes.

## Automatic Recovery

You can enable high availability for a virtual machine while creating a virtual machine profile. When the virtual machines are selected to be highly available and the Oracle VM Server shuts down or fails, the virtual machine will be restarted on another available Oracle VM Server in the server pool.

You can also use the options Enable Automatic Discovery and Disable Automatic Discovery for a virtual machine to manage the high availability.

## Related Resources

For instructions in performing actions or to learn more about the role of this feature, go to one of the following resources:

- [Chapter 2, "Asset Management"](#)
- [Chapter 17, "Server Pools"](#)
- [Chapter 7, "Networks"](#)
- [Chapter 6, "Storage Libraries"](#)
- *Oracle VM Installation and Upgrade Guide for x86*

- *Oracle VM User's Guide*
- *Oracle Enterprise Manager Ops Center Administration Guide*

This chapter includes the following information:

- [Introduction to Server Pools](#)
- [Roles for Server Pool Management](#)
- [Server Pool Policies](#)
- [Automatic Recovery](#)
- [Server Pool Libraries](#)
- [Server Pool Networks](#)
- [Oracle VM Server for SPARC Server Pool](#)
- [Oracle Solaris Zones Server Pool](#)
- [Oracle VM Server for x86 Server Pool](#)
- [Manage Server Pools](#)
- [Related Resources](#)

## Introduction to Server Pools

A server pool is a group of one or more virtualization hosts with the same processor architecture that have access to the same virtual and physical networks, and storage resources. Server pools provide load balancing, high availability capabilities, and sharing of some resources for all members of the pool.

You can create server pools for the following types of virtualization servers:

- Oracle VM Server for SPARC
- Oracle VM Server for x86
- Oracle Solaris Zones

A virtualization host can refer to Oracle VM Server for SPARC, Oracle Solaris Zones, or Oracle VM Server for x86 that are managed through Oracle Enterprise Manager Ops Center. A virtual host or guest in a server pool refers to a non-global zone, logical domain or virtual machine running on the virtualization host.

Server pools are resource pools of virtualization hosts that share compatible chip architecture, which facilitates actions such as moving guests between hosts. You can also apply resource configurations and policies to them. The policies that you establish for a server pool manage many of the CPU utilization and resource balancing functions. Operations to the server pool are delegated to the individual virtualization hosts in the server pool.

To manage the guests within a server pool, you can perform warm and live guest migration and you can balance all of the guests' load among the members of the server pool. You can configure a policy to balance the load automatically, based on a schedule that you determine, or you can balance the load manually. When a virtualization host system shuts down, such as a hardware failure, you can start the guests on another host in the same pool.

Virtualization hosts in a server pool share network and storage libraries and several server pools can share the same networks and storage resources.

Server pools form a key concept for virtual datacenter management. Pooling your virtualization supported systems plays an important role and requires proper understanding of your requirements in your environment.

All the requirements, procedures, and different functions available for a server pool depend on the type of virtualization technology selected. See the appropriate sections to create a server pool for different virtualization technology.

- [Oracle VM Server for SPARC Server Pool](#)
- [Oracle Solaris Zones Server Pool](#)
- [Oracle VM Server for x86 Server Pool](#)

When you create a server pool, you must plan the storage and network resources such that they are accessible for all the members of the server pool.

You must set the policies to place the guests on the virtualization hosts and choose how you want to do the load balancing of the server pool. To understand more on this, refer to [Server Pool Policies](#).

## Roles for Server Pool Management

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task. See [User and Role Management](#) in the *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 17-1 Server Pool Roles and Permissions**

Task	Role
Create, manage, update, and delete server pools	Virtualization Admin
Provision and manage virtualization host	Virtualization Admin
Create, manage, update, and delete guests	Virtualization Admin

## Server Pool Policies

When you create a server pool, you define guest placement, and automatic load balancing policies. When you create guests, you define the guest resource consumption, including physical and virtual CPUs. You can edit the policies of a server pool.

## Placement Policy

The Placement Policy determines the preferred virtualization host for new guests within the server pool and how the server pool is balanced. The placement policy is defined when a server pool is created. The following are the placement policy options:

- Place the guest on the virtualization host with the lowest relative load, based on the lowest memory and CPU utilization. The calculation is based on a combination of the average load during one hour, one day and three weeks.
- Place the guest on the virtualization host with the lowest allocated CPU and memory, that is, the total static resource allocation across all guests on the host. The resource allocation is the sum of the number of vCPUs and virtual memory specified for each guest.
- Place the guest on minimum number of virtualization host and thereby consume less power.

You can modify the placement policy of a server pool. Following is an example of how the placement policy is worked upon a server pool.

### **Example 17–1 Example of Least Allocated Virtualization Host**

A server pool has two virtualization hosts with different CPU and memory allocations. Host A has 8 available CPUs and 16 GB of memory. Host B has 4 available CPUs and 8 GB of memory.

Host A has three guests:

- Guest X has one vCPU and 1024 MB of memory.
- Guest Y has two vCPUs and 2048 MB of memory.
- Guest Z has one vCPU and 1024 MB of memory.

Host A's total static allocation is 4 vCPUs and 4 GB of memory.

Host B has one guest:

- Guest W has 3 vCPU and 4096 MB of memory.

Host B's total static allocation is 3 vCPUs and 4 GB of memory.

The allocation percentage for Host A is: CPU allocation is 4 vCPUs/8 physical CPUs, or 50%. Memory allocation is 4 GB/16 GB or 25%.

The allocation percentage for Host B is: CPU allocation is 3 vCPUs/4 physical CPUs or 75%. Memory allocation is 4 GB/8 GB or 50%

Therefore, Host A is the less or least allocated of the virtualization hosts.

## Minimize Power Consumption Policy

The policy to minimize power consumption places the guests on minimum number of virtualization hosts and powers off the idle servers. The idle virtualization hosts are powered off or set to low-power mode on explicit approval.

## Automatic Load Balancing Policy

Scheduling the automatic balancing is applicable only for Oracle VM Server for SPARC and Oracle Solaris Zones server pool.

Use the Automatic Load Balancing Policy to schedule load balancing within a server pool. You can schedule the automatic balancing to occur weekly, daily, or hourly on a

specific day and time of the week. The default is to balance the load on the servers in the server pool every Saturday at midnight according to the defined placement policy.

---

---

**Note:** The day and time are in the Enterprise Controller's time zone.

---

---

When you do not want to balance the server pool's load automatically, schedule a reminder to balance the server pool's load manually.

### **Maintenance Mode**

Automatic load balancing policy does not consider the virtualization hosts that are placed in maintenance mode as a target in the server pool for migrating the guests. When you place a virtualization host in maintenance mode, then all the migratable guests in it are migrated to other servers in the server pool. This action is triggered automatically.

### **Resource Balancing Enhancements**

You can define the resource usage threshold for the servers in the server pool. The resource usage is defined on the CPU utilization. When the CPU utilization exceeds the set threshold value, the server is considered to be loaded heavily.

When a virtualization host in the server pool exceeds the threshold for the specified time, the automatic balancing policy tries to migrate some of its guests to other virtualization hosts in the same server pool.

When the virtualization hosts are well within the threshold and power minimization policy is selected, the automatic balancing policy attempts to free a virtualization host from its guest so that the administrator can power off the server.

## **Automatic Recovery**

The automatic recovery option is available for all types of supported virtualization technology. You can enable or disable the automatic recovery of zones, logical domains, and the virtual machines.

This feature provides the option to recover the guests that are attached to a failed server. The recovered guests are restarted on other servers in the server pool.

The automatic recovery for virtual machines is managed by Oracle VM Manager. For logical domains and zones, the automatic recovery is managed by Oracle Enterprise Manager Ops Center.

### **Recovery Process**

Oracle Enterprise Manager Ops Center monitors the managed assets by checking the connection between the agent deployed on the assets and the Proxy Controller. To detect the unreachability of the assets, it takes about 5 minutes approximately. The unreachability detection steps are as follows:

1. A heartbeat time-out of 3 minutes will allow the Proxy Controller to detect that the connection is down.
2. A re-connection attempt is made for every 30 seconds for four times.

When the connection cannot be re-established, the asset is seen as unreachable from Oracle Enterprise Manager Ops Center.

An automatic recovery job is initiated when the global zone or Oracle VM Server for SPARC is:



- Identified as unreachable by Oracle Enterprise Manager Ops Center, and its attached zones or logical domains are also seen as unreachable.
- Placed in a server pool.
- Has at least a zone or logical domain that is configured to recover automatically.

You can also manually recover the zones and logical domains if the automatic recovery fails. See [Recovering Zones](#) for more information about manual recovery.

See the sections [Oracle Solaris Zones Server Pool](#), [Oracle VM Server for SPARC Server Pool](#), and [Oracle VM Server for x86 Server Pool](#) for more information about automatic recovery options.

## Server Pool Libraries

Oracle Enterprise Manager Ops Center uses software libraries to store ISO images and guest metadata. Storage libraries are also used to provide storage disks for the guest operating systems and for guests' data.

The virtualization hosts in a server pool share the libraries associated with the server pool. The type of library you can associate with the server pool depends on type of virtualization hosts in the server pool and on whether all members of the server pool can get access to the storage resource.

See [Chapter 6, "Storage Libraries"](#) and [Chapter 5, "Software Libraries"](#) for more information about setting up these libraries.

## Server Pool Networks

Oracle Enterprise Manager Ops Center provides groups related networking components such as fabrics and networks as network domains. All the managed and declared networks in Oracle Enterprise Manager Ops Center are available contained in the default network domain. Associating a virtualization host or a server pool with the default network domain does not require fabric connection. All the networks in the default network domain are available to be attached to the server pool.

You can also create network domains. Associating a server pool with a user-defined network domain requires connection between the physical interface of each server in the pool and each fabric in the network domain. Only networks assigned to the new network domain are available to be attached to the server pool.

Plan your networks and network domains that you must attach to the server pool. See [Chapter 7, "Networks"](#) for more information about creating network domains and managed networks.

## Oracle VM Server for SPARC Server Pool

You can pool the Oracle VM Server for SPARC resources and manage your logical domains. Oracle VM Servers for SPARC must meet the following requirements to be added to a server pool:

- Must have the same chip architecture as the other virtualization hosts in the server pool to support load balancing and guest migration. Oracle Enterprise Manager Ops Center and Oracle VM Server for SPARC support SPARC T-Series chip architectures.

Overview of the type of Oracle VM Servers present. It is essential that you group your servers that have the same CPU architecture and frequency. This enables

migration of logical domains within the server pool. For example, you cannot migrate a logical domain of Oracle VM Server for SPARC 2.1 version to a server lower than this version. So, plan your servers that must be pooled.

- Must be running at least Oracle VM Server for SPARC 1.2 version.
- Must be running on at least the Solaris 10 10/09 OS and must meet specific patch and firmware requirements.
- Plan the network that must be attached to the server pool. Either place those networks in the user-defined network domain or use the default network domain. You can connect to a network multiple times. For each network connection, a virtual switch is created. For each network connection, you must define the NIC and IP address in each of the Oracle VM Servers in the server pool. Select the virtual switches when you start a logical domain. The multiple network connection allows you to create IPMP or aggregate the links in the logical domain.
- The storage libraries must be associated with the server pool to store logical domain metadata, ISO images, and for virtual disk storage of logical domains. You can associate file system and block storage libraries with the server pool. Filesystem storage includes the NAS storage libraries. Block storage includes the SAN, iSCSI, and Dynamic Storage libraries. Ensure that you have at least one NAS storage library assigned to the server pool. For using migration capabilities, the server pool must be on shared storage facility.
- Logical domain in the virtualization host must be created using Oracle Enterprise Manager Ops Center.
- Do not have logical domains in running, shutdown, or suspended state.

## Server Pool Policies

The server pool policies that are applicable for Oracle VM Server for SPARC are as follows:

- **Placement Policy**

Set the CPU utilization threshold. Place the logical domains on the Oracle VM Server for SPARC that has the lowest relative load.

Set the CPU and memory allocation threshold. Place the logical domains on the Oracle VM Server for SPARC allocated with lowest CPU and memory resources.

Set the CPU utilization threshold. Place the logical domains on the minimum number of Oracle VM Servers to minimize the power consumption.

- **Automatic Balancing**

Set the automatic load balancing. Logical domains are migrated automatically in the server pool whenever the thresholds are exceeded. Schedule the automatic load balancing to take place at definite time interval.

When you have selected power minimization and automatic load balancing policy, and the servers in the server pool are not overloaded, then some of the Oracle VM Server host servers are freed up from the logical domains and powered off to minimize power consumption.

Set whether administrator approval is required for migrating the logical domains.

## Automatic Recovery

You can enable automatic recovery for a logical domain in the following scenarios:

- During logical domain creation, you can enable automatic recovery option and set the value for priority of recovery. See [Create Logical Domain Profile](#) for more information about setting the priority of recovery while creating a logical domain profile.
- For an already created logical domain, use the options Enable Automatic Recovery and Disable Automatic Recovery to set the automatic recovery. Also, you can edit the attributes of a logical domain to set the value for priority of recovery. See [Enabling Automatic Recovery of Logical Domains](#) for more information.

In an Oracle VM Server for SPARC server pool, the option to power-off the failed server and recover the logical domains is enabled by default. When a server fails, Oracle Enterprise Manager Ops Center tries to power-off the failed server, ensure that it is stopped and then initiates the automatic recovery of the logical domains. The logical domains that are configured for automatic recovery will be recovered and restarted on other servers in the server pool.

When the option to power-off the failed server is enabled and Oracle Enterprise Manager Ops Center cannot power-off the failed server, that is the Service Processor is also unreachable, the automatic recovery of the logical domains will not take place. This is to avoid any potential data corruption during the recovery process of the logical domains.

When Oracle Enterprise Manager Ops Center detects that the failed server is unreachable, the logical domain that were running in the server will disappear from the Navigation pane in the UI until they are recovered to other servers in the server pool.

The metadata of disappeared logical domains will still be available in the storage libraries. The logical domains that are not configured for automatic recovery or the logical domains that cannot be recovered will re-appear in the UI in the following scenario:

- When the failed server is restarted, the logical domains will be booted and attached to the server again.
- When you have followed the manual recovery procedure and deleted the failed server from Oracle Enterprise Manager Ops Center, the logical domains will re-appear in the list of Shutdown Guests in the Server Pool. You can start them on other server in the server pool. See [Recovering Logical Domains](#) for the logical domains recovery.

The following table provides a quick view of different conditions that exist for recovering a logical domain.

**Table 17–2 Recovery of Logical Domains**

	Conditions	Result
Logical domains	<ul style="list-style-type: none"> <li>■ Failed Oracle VM Server for SPARC</li> <li>■ The server pool option to power-off the failed server on automatic recovery is enabled</li> <li>■ Oracle Enterprise Manager Ops Center can power-off the failed server</li> <li>■ Automatic recovery is enabled for the logical domain</li> </ul>	<p>The logical domain is restarted and placed in another server in the server pool.</p> <p>If there are no server available in the server pool, then you must manually recover the logical domains.</p> <p>See <a href="#">Recovering Logical Domains</a> for more information.</p>
Logical domains	<ul style="list-style-type: none"> <li>■ Failed Oracle VM Server for SPARC</li> <li>■ The server pool option to power-off the failed server on automatic recovery is enabled</li> <li>■ Oracle Enterprise Manager Ops Center cannot power-off the failed server</li> <li>■ Automatic recovery is enabled for the logical domain</li> </ul>	<p>The automatic recovery of the logical domain will not take place.</p> <p>This is to avoid any data corruption during the recovery procedure.</p> <p>You must manually recover the logical domains.</p>
Logical domains	<ul style="list-style-type: none"> <li>■ Failed Oracle VM Server for SPARC</li> <li>■ The server pool option to power-off the failed server on automatic recovery is not enabled</li> </ul>	<p>Oracle Enterprise Manager Ops Center will proceed to recover the logical domains configured to automatically recover without trying to power-off the failed server from its processor.</p> <p>This can lead to data corruption if the failed server is just isolated from the network point of view, and has still logical domains writing to disks.</p>
Logical domains	<ul style="list-style-type: none"> <li>■ Failed Oracle VM Server for SPARC</li> <li>■ Automatic recovery is not enabled for the logical domain</li> </ul>	<p>Follow the procedure in <a href="#">Recovering Logical Domains</a> to recover the logical domains.</p> <p>Only after this the logical domains will appear in the Shutdown Guests list in the UI. You can restart them on the available server in the server pool.</p>

## Create an Oracle VM Server for SPARC Server Pool

Oracle Enterprise Manager Ops Center launches a wizard that collects information about the servers, storage and network resources, and placement policies to create a server pool.

### To Create a Server Pool for Oracle VM Server for SPARC

1. Select Server Pools in the Systems Group list on the Navigation pane.
2. Click Create Server Pool in the Actions pane.

The Create Server Pool wizard displays.

3. In the Identify Server Pool step, enter the following information:
  - Name and description of the server pool.
  - Enter tags for categorizing your server pool.
  - Select Oracle VM Server for SPARC from the Virtualization Technology.Click Next to select the members of the server pool.
4. Select one or more Oracle VM Servers to add to the server pool.

The list of Oracle VM Servers displayed have the following characteristics:

  - Not associated with a server pool.
  - In a healthy state.
  - Not placed in maintenance mode.
  - Have no logical domains in the running, shutdown or suspended state.

The list displays the details of CPU frequency, type, and architecture of Oracle VM Servers. Select Oracle VM Servers that are compatible for migration of logical domains.

Click Next to associate the network domain.
5. Select the network domain to associate with the server pool.
  - When you have selected default network domain, then go to Step 8.
  - For a user-defined network domain, select the physical interfaces of each server to connect to each fabric in the network domain. When you do not want to bond the interfaces, go to Step 8.
6. You can bond the interfaces of the servers into a single logical link. The aggregation is done according to the standard IEEE 802.3ad Link Aggregation. Select Bond Interface in the Physical Interface column. A Bond ID is provided. Select the physical interfaces for the aggregation.

Click Next to configure the bonding parameters.
7. In the Configure Bonding step, specify the following parameters for Link Aggregation:
  - Load balancing policy.
  - LACP mode. If the Ethernet switch to which the physical interface connects to supports aggregation, then specify the LACP mode.
  - LACP timer.
  - MAC address policy and provide the MAC address.Click next to select the networks and associate with the server pool.
8. For default network domain, all the networks that are declared and managed in Oracle Enterprise Manager Ops Center are listed. For an user-defined network domain, only the networks assigned to it are listed.

Select the networks that you want to associate with all the servers in the server pool. You can make multiple connections to a network. Enter the total number of connections. For each network connection, a virtual switch is created. Choose the networks that you want to use for migration of logical domains.

Click Next to configure the interfaces of the servers.
9. For each network connection, provide the connection details:

- Specify the NIC and IP address for each network connection. When a selected server is connected to the network, then no rows are displayed for that server.

You can assign the same NIC to different network connection when the networks have different VLAN IDs.

- You can select System Allocated for the NIC and IP address to be automatically allocated by the system.
- You can select Do Not Allocate IP to allocate no IP address for the network connection.

Click Next to associate the storage libraries.

10. The storage libraries that are reachable from the selected members of the pool are displayed. The storage libraries are required to store logical domain metadata, ISO images, and for virtual disks of logical domain.

You can select the following types of storage libraries:

- Filesystem Storage Libraries - This includes the NAS storage libraries. It is recommended to have at least one NAS storage library to store the logical domain metadata.
- Block Storage Libraries - This includes the Static Block Storage and Dynamic Block Storage. Static block storage libraries comprises the exported LUNs of storage arrays that are not managed by Oracle Enterprise Manager Ops Center. Dynamic block storage libraries comprises the exported LUNs of storage array servers that are discovered and managed in Oracle Enterprise Manager Ops Center.

Select the storage libraries from the list that you want to associate with all the virtualization hosts in the server pool.

Click Next to select the server pool policies.

11. Select the following policies in the server pool to manage the under utilized and overutilized servers in the pool:
  - Placement Policy – This policy decides the preferred virtualization host in the server pool to place the logical domains.
  - Auto Balancing Policy – This policy will perform load balancing of the server pool automatically at set intervals.
12. Select one of the following placement policies:
  - Lowest relative load – The recent lowest memory and CPU utilization for the Oracle VM Servers in the server pool are calculated. Based on this, the server with the lowest relative load is considered to place a logical domain. Provide the threshold for CPU utilization above which the server is considered to be over-utilized and logical domains are migrated to server with lowest relative load.
  - Lowest allocated CPU and memory resources – The total number of virtual CPU and memory resources allocated for all the logical domains in an Oracle VM Server are calculated. The server with the lowest allocated resources is considered to place a logical domain in the pool. Provide the threshold values for CPU and memory allocation. When the allocation is exceeded, the server is considered to be over-allocated and logical domains are migrated to server with lowest allocated CPU and memory resources.
  - Minimize power consumption – The logical domains running in a server pool are placed on the minimum number of Oracle VM Servers and the unused

Oracle VM Servers are powered off. The threshold value set for the server over-utilization ensures that the servers are not overloaded.

13. Select the automatic load balancing policies:
  - Select automatic load balancing and set the interval in which the server pool must be checked for resource balancing. You can set the approval to migrate the logical domains automatically. Or send notifications about the approval.
  - You can also select to manually balance the resources. See [Balancing Resources](#) for more information.
14. For Automatic Recovery, you can specify whether an attempt to power-off the failed server must be performed before initiating the automatic recovery of the logical domains.
 

When Oracle Enterprise Manager Ops Center has the capability to power-off the Service Processor of a failed server and you have selected the automatic recovery option, the failed server is powered off and then the logical domain recovery is started.

If Oracle Enterprise Manager Ops Center cannot power-off the failed server, the recovery of the attached logical domains will not take place. This is to avoid any data corruption during the recovery process.

Click Next to view the summary of the server pool details.
15. Review the information to create a server pool for Oracle VM Server for SPARC. Click Finish to create the server pool.

## Oracle Solaris Zones Server Pool

You can now pool Oracle Solaris Zones resources and manage your zones. Oracle Solaris Zones must meet the following requirements to be added to a server pool:

- All the assets in the pool must have compatible architecture for supporting guest migration. For a global zone to be added to the server pool, it must have the same release or must be at least Oracle Solaris 10 10/08 version. This ensures that the zones can be migrated to a global zone in the server pool.
- The global zones must be in healthy state.
- The global zones must not be associated with a server pool already.
- The global zones must not be placed in maintenance mode.

## IP Stack in Server Pool

The network deployment for zones server pool vary depending on the Oracle Solaris OS version.

For a stand-alone Oracle Solaris 10 OS, the network can be attached to in either shared IP or exclusive IP mode. Whereas, in a server pool, you can attach a network only in shared IP mode for Oracle Solaris 10 OS. You cannot make multiple connections to a network.

For Oracle Solaris 11 OS, the network is always attached to in exclusive IP mode. In a server pool also, the network for Oracle Solaris 11 OS is always deployed in exclusive IP mode. You can make multiple connections to a network.

When you want to have a server pool with mixture of Oracle Solaris 10 and 11 OS, then you cannot make multiple connections to a network. So, plan your server pools with compatible Oracle Solaris OS versions.

## Server Pool Policies

The server pool policies that are applicable for Oracle Solaris Zones are as follows:

### ■ Placement Policy

Place the zones on the global zone that has the lowest relative load. Set the CPU utilization threshold.

Place the zones on the global zone allocated with lowest CPU and memory resources. Set the CPU and memory allocation threshold.

Place zones on minimum number of global zones to minimize the power consumption. Set the CPU utilization threshold.

### ■ Automatic Balancing

You can select the automatic load balancing so that the zones can be migrated automatically in the server pool whenever the thresholds are exceeded. You can schedule the automatic load balancing to take place at definite time interval.

When you have selected power minimization and automatic load balancing policy, and the servers in the server pool are not over loaded, then some of the servers are freed up from the zones and powered off to minimize power consumption.

You can set whether the approval is required from the administrator for migrating the zones.

### ■ Automatic Recovery

You can set the automatic recovery for the zones in the following scenarios:

- During zone creation, you can enable automatic recovery of the zones. You can set the value for priority of recovery. Zone with a highest priority is migrated first.
- For already created zones, use the option Enable Automatic Recovery and Disable Automatic Recovery to set the automatic recovery. You can edit the zone configuration to modify the value for priority of recovery.

In an Oracle Solaris Zones server pool, you can specify that the automatic recovery of a failed server must start first with an attempt to power off the failed server, ensure that it is stopped and then initiate the automatic recovery of the zones.

## Create a Zones Server Pool

Oracle Enterprise Manager Ops Center takes you through a series of steps to collect information for creating a zones server pool.

1. Select Server Pool in the Systems Group list on the Navigation pane.
2. Click Create Server Pool in the Actions pane.  
The Create Server Pool wizard displays.
3. In the Identify Server Pool step, enter the following information:
  - Name and description of the server pool.
  - Enter tags for categorizing your server pool.



- Select Oracle Solaris Zones – SPARC or x86 from the Virtualization Technology.

You cannot have a zones server pool with a mixture of SPARC or x86 architecture.

Click Next to select the members of the server pool.

4. Select one or more global zones to add to the server pool.

The list of global zones displayed have the following characteristics:

- The same architecture – SPARC or x86
- Oracle Solaris 10 10/08 OS or higher version
- Not associated with a server pool
- In a healthy state
- Not placed in maintenance mode

The list displays the details of global zones such as CPU architecture and OS version. Select global zones that are compatible for migration of zones within the pool.

Click Next to associate the network domain.

5. Select the network domain to associate with the server pool.

- When you have selected default network domain, go to Step 8.
- For a user-defined network domain, select the physical interfaces of each selected servers to connect to each fabric in the network domain. When you do not want to bond the interfaces, go to Step 8.

6. You can bond the interfaces of the servers into a single logical link. The aggregation is done according to the standard IEEE 802.3ad Link Aggregation. Select Bond Interface in the Physical Interface column. A Bond ID is provided. Select the physical interfaces for the aggregation.

Click Next to configure the bonding parameters.

7. In the Configure Bonding step, specify the following parameters for Link Aggregation:

- Load balancing policy.
- LACP mode. If the Ethernet switch to which the physical interface connects to supports aggregation, then specify the LACP mode.
- LACP timer.
- MAC address policy and provide the MAC address.

Click next to select the networks and associate with the server pool.

8. For default network domain, all the networks that are declared and managed in Oracle Enterprise Manager Ops Center are listed. For an user-defined network domain, only the networks assigned to it are listed.

Select the networks that you want to associate with all the global zones in the server pool. Depending on the Oracle Solaris OS versions selected for the server pool, you can make multiple connections to a network. See [IP Stack in Server Pool](#) for more information about IP stack mode for networks in the zones server pool.

Enter the total number of connections and click Next to configure the interfaces of the servers.

9. For each network connection, provide the connection details:
  - Specify the NIC and IP address for each network connection. When a selected server is connected to the network, no rows are displayed for that server.  
You can assign the same NIC to different network connection when the networks have different VLAN IDs.
  - When supported by the network, you can select System Allocated for the NIC and IP address to be automatically allocated by the system.
  - You can select Do Not Allocate IP to allocate no IP address for the network connection.

Click Next to associate the storage libraries.

10. The storage libraries that are reachable from the selected members of the pool are displayed. The storage libraries are required to store zone metadata, ISO images, and for virtual disks of zones.

You can select the following type of storage libraries:

- Filesystem Storage Libraries – This includes the NAS storage libraries. It is recommended to have at least one NAS storage library to store the zone metadata.
- Block Storage Libraries – This includes the Static Block Storage and Dynamic Block Storage. Static block storage libraries comprises the exported LUNs of storage arrays that are not managed by Oracle Enterprise Manager Ops Center. Dynamic block storage libraries comprises the exported LUNs of storage array servers that are discovered and managed in Oracle Enterprise Manager Ops Center.

Select the storage libraries from the list that you want to associate with all the virtualization hosts in the server pool.

---

---

**Note:** When you have unmanaged storage attached to the non-global zones, then upload the script to be placed in all the global zones in the server pool. See [Script to Migrate a Zone With Dependencies](#) for more information about migrating zone with unmanaged storage.

---

---

Click Next to select the server pool policies.

11. You must select the following policies in the server pool to manage the under utilized and overutilized servers in the pool:
  - Placement Policy – This policy decides the preferred virtualization host in the server pool to place the zones.
  - Auto Balancing Policy – This policy will perform load balancing of the server pool automatically at set intervals.
12. Select one of the following placement policies:
  - Lowest relative load – The recent lowest memory and CPU utilization for the global zones in the server pool are calculated. Based on this, the server with the lowest relative load is considered to place the zone. Provide the threshold for CPU utilization above which the server is considered to be over-utilized and zones are migrated to server with lowest relative load.
  - Lowest allocated CPU and memory resources – The total number of virtual CPU and memory resources allocated for all the zones in an Oracle VM Server

are calculated. The server with the lowest allocated resources is considered to place a zone in the pool. Provide the threshold values for CPU and memory allocation. When the allocation is exceeded, the server is considered to be over-allocated and zones are migrated to server with lowest allocated CPU and memory resources.

- Minimize power consumption – The zones running in the server pool are placed on the minimum number of global zone and the unused servers are powered off. The threshold value set for the server over-utilization ensures that the servers are not overloaded. Otherwise, the powered off servers can be powered on to host the zones.

**13. Select the automatic load balancing policies:**

- Select automatic load balancing and set the interval in which the server pool must be checked for resource balancing. You can set the approval to migrate the zones automatically. Or send notifications for the approval.
- You can also select to manually balance the resources. See [Balancing Resources](#) for more information.

**14. For Automatic Recovery, you can specify whether an attempt to power-off the failed server must be performed before initiating the automatic recovery of the zones.**

When Oracle Enterprise Manager Ops Center has the capability to power-off the Service Processor of a failed server and you have selected the automatic recovery option, the failed server is powered off and then the zone recovery is started.

Click Next to view the summary of the server pool details.

**15. Review the information to create a server pool for Oracle Solaris Zones. Click Finish to create the server pool.**

## Oracle VM Server for x86 Server Pool

You can group one or more Oracle VM Servers in an Oracle VM Manager and create server pools. When you create a server pool for Oracle VM Server for x86 systems, you must have the following information defined:

- Cluster file system
- Server pool master
- Virtual IP address for the server pool master

### Cluster File System

Shared access to the server pool resources is a must for providing for high availability for the virtual machines running in the Oracle VM Servers of the server pool. This is achieved by cluster file system OCFS2 which allows multiple Oracle VM Servers to access the same disk at the same time. OCFS2 ensures that the Oracle VM Servers in a server pool can access and modify resources in the shared repositories in a controlled manner.

When you create a server pool, you must specify the server pool file system for the cluster heartbeat and other cluster information. The file system can be NFS shares or LUNs of iSCSI or SAN based storage servers. Oracle VM formats the server pool file system as OCFS2 file system.

In Oracle Enterprise Manager Ops Center, the cluster is always enabled by default. The cluster configuration is pushed out to all the Oracle VM Servers in the server pool and

the cluster heartbeat starts when the server pool is created. You can set a separate network for this cluster heartbeat. See [Manage Networks](#) for more information about setting up the networks and their role for an Oracle VM Server.

### **Server Pool Master**

An Oracle VM Server is internally elected as server pool master. You cannot set the role for an Oracle VM Server. When the elected Oracle VM Server fails, the role is set for another Oracle VM Server in the server pool. The virtual IP address provided while creating the server pool is assigned to the Oracle VM Server that has been elected as server pool master.

## **Server Pool Policies**

The server pool policies that are applicable for Oracle VM Server for x86 are as follows:

### ■ **Placement Policy**

Places the virtual machines on the Oracle VM Server that has the lowest relative load. Set the CPU utilization threshold.

Places the virtual machines on minimum number of Oracle VM servers to minimize the power consumption. Set the CPU utilization threshold.

### ■ **Automatic Balancing**

You can select the automatic load balancing so that the virtual machines can be migrated automatically in the server pool whenever the thresholds are exceeded.

When you enable automatic load balancing for Oracle VM Server for x86 server pool, the server pool is checked continuously for the selected placement policy. When the threshold exceeds, the virtual machines are migrated from one Oracle VM Server to another.

When you have selected power minimization and automatic load balancing policy, and the servers in the server pool are not over loaded, then some of the Oracle VM Server host servers are freed up from the logical domains and powered off to minimize power consumption.

When the servers are overloaded and there are no other servers in the pool to host the virtual machines, then the policy will start a powered-off server using its Wake-on-LAN capability and live migrate the virtual machines to take up the load. It is necessary that the Wake-on-LAN capability must be enabled on the BIOS of the Oracle VM Server.

### ■ **Automatic Recovery**

When an Oracle VM Server fails, the virtual machines are migrated to another Oracle VM Server in the server pool. The automatic recovery for a virtual machine is set in the following scenarios:

- During virtual machine creation, select the option Enable High Availability. This ensures that the virtual machines are migrated when an Oracle VM Server fails.
- For an already created virtual machine, use the option Enable or Disable Automatic Recovery to set the automatic recovery.

## **Create Oracle VM Server for x86 Server Pools**

The following procedure describes the steps in the wizard that is launched to create an Oracle VM Server for x86 server pool.

1. Select Server Pool in the Systems Group list on the Navigation pane.
2. Click Create Server Pool in the Actions pane.  
The Create Server Pool wizard displays.
3. In the Identify Server Pool step, enter the following information:
  - Name and description of the server pool.
  - Enter tags for categorizing your server pool.
  - Select Oracle VM Server for x86 from the Virtualization Technology.Click Next to define the server pool configuration.
4. Define the following configuration details:
  - Select the Oracle VM Manager in which the Oracle VM Servers are discovered and owned.
  - Select the network domain.
  - Select a network from the list of networks available in the network domain.
  - Enter the virtual IP address that is assigned to the server pool master. When the server pool master changes, the IP address is assigned to the new Oracle VM Server.
  - Select the server pool file system to store cluster heartbeat and other cluster information. The file system can be either NFS shares on a NFS file servers or LUNs of SAN and iSCSI based storages. The NFS file servers and the storage servers are known and reachable to the selected Oracle VM Manager.Click Next to select the members of the pool.
5. Select one or more Oracle VM Servers to add to the server pool.  
The list of Oracle VM Servers displayed have the following characteristics:
  - Owned by the Oracle VM Manager. Refer to [Manage Ownership of Oracle VM Servers](#) to own an Oracle VM Server.
  - Not associated with a server pool.
  - In a healthy state.
  - Not placed in maintenance mode.
  - Have no virtual machines in the running, shutdown or suspended state.Select Oracle VM Servers that are compatible for migration of virtual machines. To migrate virtual machines within a server pool, the Oracle VM Servers systems must be identical in model.  
Click Next to associate the network domain.
6. Select the network domain to associate with the server pool.
  - When you have selected default network domain, go to Step 7.
  - For a user-defined network domain, select the physical interfaces of each selected servers to connect to each fabric in the network domain. You cannot bond the interfaces in Oracle VM Server for x86. Bonding can be done in only individual OS of the Oracle VM Server.Click next to select the networks and associate with the server pool.

7. For default network domain, all the networks that are declared and managed in Oracle Enterprise Manager Ops Center are listed. For a user-defined network domain, only the networks assigned to it are listed.

Select the networks that you want to associate with all the servers in the server pool. You cannot make multiple connections to a network. Limit the number of connections to 1.

Click Next to configure the interfaces of the servers.

8. For each network connection, specify the following details:
  - Specify the NIC and IP address for each network connection. When a selected server is connected to the network, no rows are displayed for that server.
  - You can assign the same NIC to different network connection when the networks have different VLAN IDs.
  - You can select System Allocated for the NIC and IP address to be automatically allocated by the system.

Click Next to associate the storage libraries.

9. The storage libraries that are reachable from the selected members of the pool are displayed. The storage libraries are required to store virtual machine metadata, ISO images, and for virtual disks of virtual machine.

You can select the following type of storage libraries:

- Filesystem Storage Libraries – This includes the Oracle VM storage repositories. It is recommended to have at least one Oracle VM storage repository associated with the server pool.
- Block Storage Libraries – This includes the Static Block Storage and Dynamic Block Storage. Static block storage libraries comprises the exported LUNs of storage arrays that are not managed by Oracle Enterprise Manager Ops Center. Dynamic block storage libraries comprises the exported LUNs of storage array servers that are discovered and managed in Oracle Enterprise Manager Ops Center.

Select the storage libraries from the list that you want to associate with all the virtualization hosts in the server pool.

Click Next to select the server pool policies.

10. You must select the following policies in the server pool to manage the under utilized and overutilized servers in the pool:
  - Placement Policy – This policy decides the preferred virtualization host in the server pool to place the logical domains.
  - Auto Balancing Policy – This policy will perform load balancing of the server pool automatically at set intervals.
11. Select one of the following placement policies:
  - Lowest relative load – The recent lowest memory and CPU utilization for the Oracle VM Servers in the server pool are calculated. Based on this, the server with the lowest relative load is considered to place a virtual machine. Provide the threshold for CPU utilization above which the server is considered to be over-utilized and virtual machines are migrated to server with lowest relative load.
  - Minimize power consumption – The virtual machines running in a server pool are placed on the minimum number of Oracle VM Servers and the unused

Oracle VM Servers are powered off. The threshold value set for the server over-utilization ensures that the servers are not overloaded. Otherwise, the powered off Oracle VM Servers can be powered on to host the virtual machines.

**12.** Select the automatic load balancing policies:

- Select automatic load balancing and set the interval in which the server pool must be checked for resource balancing. You can set the approval to migrate the virtual machines automatically. Or send notifications about the approval.
- You can also select to manually balance the resources. See [Balancing Resources](#) for more information.

Click Next to view the summary of the server pool details.

**13.** Review the information to create a server pool for Oracle VM Server for x86. Click Finish to create the server pool.

## Manage Server Pools

You must monitor the requirements of the server pool so that there are resources to host the guests and run them efficiently. Also, the server pools gives the infrastructure support for the virtual datacenters. You might need to add storage and network resources to run the guests. Oracle Enterprise Manager Ops Center provides the following management functions to manage the resources in the server pool:

- [Edit Server Pool Parameters](#)
- [Add Virtualization Hosts](#)
- [Associate Network Domains](#)
- [Attach Networks](#)
- [Associate Libraries](#)
- [Create Guests](#)
- [Migrate Multiple Guests](#)
- [Migrate Zones](#)
- [Migrate Logical Domains](#)
- [Migrate Virtual Machines](#)
- [Balancing Resources](#)
- [Delete Server Pool](#)

## Edit Server Pool Parameters

You can modify the parameters set during the creation of a server pool. Click Edit Attributes in the Actions pane and you can edit the following parameters of a server pool:

- Name
- Description
- Change the placement policy
- Change the auto balancing policy

To add, remove or modify the tags added to the server pool, use the option Edit Tags in the Actions pane.

For Oracle Solaris Zones and Oracle VM Server for SPARC server pool, you can edit the following additional parameters:

- Enable or disable automatic recovery option.
- Upload scripts to manage the file systems on unmanaged storage. See Step 10 in [Oracle Solaris Zones Server Pool](#) for more information.

## Add Virtualization Hosts

You can add more virtualization hosts to a server pool when you require more CPU and memory resources to take up the load in the server pool. Depending on the virtualization type, you can add global zones, and Oracle VM Servers of x86 and SPARC architecture.

### Oracle Solaris Zones

The list of global zones that are displayed to be added to the server pool has the following characteristics:

- Same release as the existing global zones in the pool or at least Oracle Solaris 10 10/08 OS or higher version.
- Not associated with a server pool
- In a healthy state and not placed in maintenance mode

When the server pool has Oracle Solaris 11 OS and multiple network connections, then the list of available global zones is limited to only Oracle Solaris 11 OS. You cannot add Oracle Solaris 10 OS as you cannot make multiple network connections to it.

Load balancing in the server pool requires the zones to be migrated within the pool. Therefore, ensure compatibility for migration within the pool when you select the members.

### Oracle VM Server for SPARC

The list of Oracle VM Servers displayed to be added to the server pool have the following characteristics:

- Compatible architecture with the other members of the server pool
- Not associated with a server pool
- In a healthy state and not placed in maintenance mode
- Have no logical domains in the running, shutdown or suspended states

### Oracle VM Server for x86

The list of Oracle VM Servers displayed to be added to the server pool have the following characteristics:

- Owned by the Oracle VM Manager
- Not associated with a server pool
- In a healthy state and not placed in maintenance mode
- Have no virtual machines in the running, shutdown or suspended states



### To Add Virtualization Hosts to the Server Pool

1. Select the server pool and click Add Global Zones or Add Oracle VM Servers in the Actions pane.

The Add Virtualization Host to Server Pool wizard displays.

2. Select one or more virtualization hosts to be added to the server pool.

When the server pool is associated with the default network domain, you must proceed to configure the interfaces. Otherwise, you must associate the network domain with the selected assets.

3. For a user-defined network domain, select the physical interfaces of each selected servers to connect to each fabric in the network domain. When you do not want to bond the interfaces, go to Step 6. For Oracle VM Server for x86, you cannot bond the interfaces and go to Step 6.

4. You can bond the interfaces of the servers into a single logical link. The aggregation is done according to the standard IEEE 802.3ad Link Aggregation. Select Bond Interface in the Physical Interface column. A Bond ID is provided. Select the physical interfaces for the aggregation.

Click Next to configure the bonding parameters.

5. In the Configure Bonding step, specify the following parameters for Link Aggregation:

- Load balancing policy.
- LACP mode. If the Ethernet switch to which the physical interface connects supports aggregation, then specify the LACP mode.
- LACP timer.
- MAC address policy and provide the MAC address.

Click next to define the network connection.

6. For each network connection, specify the following details:

- Specify the NIC and IP address for each network connection. When a selected server is connected to the network, no rows are displayed for that server.

You can assign the same NIC to different network connection when the networks have different VLAN IDs.

- You can select System Allocated for the NIC and IP address to be automatically allocated by the system.

Click Next to view the summary.

7. Review the information provided and click Finish to add the selected assets to the server pool.

## Associate Network Domains

All networks in a network domain that is associated with a server pool are available to the members of the server pool. To associate a user-defined network domain with a server pool, there must be a connection between the virtualization servers and the fabrics in the network domain. The fabric connection is not required for the default network domain.

The default network domain includes all the networks in Oracle Enterprise Manager Ops Center. When you associate a server pool with the default network domain, all the

networks in Oracle Enterprise Manager Ops Center are available for attaching with the server pool.

For a user-defined network domain, you must define the physical interfaces of each virtualization server in the server pool to connect to each fabric in the network domain. You can also bond the interfaces of the virtualization servers.

---

---

**Note:** You cannot bond the interfaces of Oracle VM Server for x86 servers.

---

---

### To Associate the Network Domain to a Server Pool

1. Select the server pool.
2. Click Associate Network Domain in the Actions pane.  
The Associate Network Domain wizard displays.
3. Select the network domain from the list.
4. For a user-defined network domain, select the physical interfaces of each selected servers to connect to each fabric in the network domain. When you do not want to bond the interfaces, go to Step 7. For Oracle VM Server for x86, you cannot bond the interfaces and go to Step 7.

For default network domain, you will be taken to the Summary step.

5. You can bond the interfaces of the servers into a single logical link. The aggregation is done according to the standard IEEE 802.3ad Link Aggregation. Select Bond Interface in the Physical Interface column. A Bond ID is provided. Select the physical interfaces for the aggregation.

Click Next to configure the bonding.

6. In the Configure Bonding step, specify the following parameters for Link Aggregation:
  - Load balancing policy.
  - LACP mode. If the Ethernet switch to which the physical interface connects to supports aggregation, then specify the LACP mode.
  - LACP timer.
  - MAC address policy and provide the MAC address.

Click next to view the summary.

7. Review the information and click Finish to associate the network domain with the server pool.

When you associate with a user-defined network domain, only the assigned networks in the network domain are available for attaching with the server pool. Therefore, ensure that you assign the required networks to the domain to attach to the server pool.

## Attach Networks

After the network domain is associated with a server pool, you can attach the networks in the network domain. Depending on the type of virtualization, the multiple connection to a network is allowed.

For Oracle VM Server for SPARC, you can make multiple connections to a network. Refer to the [Chapter 16, "Oracle VM Server for x86"](#) for more information.

For Oracle Solaris Zones, you can make multiple connections to a network when the server pool contains only Oracle Solaris 11 OS. For Oracle Solaris 10 OS, you can make only one connection. Also, when the server pool has mixture of Oracle Solaris 10 and 11 OS, then also you can make only single connection.

### To Attach Networks to Server Pool

1. Select the server pool.
2. Click Attach Networks in the Action pane.

The Attach Network wizard displays. All the networks assigned to the network domains are listed. For default network domain, all the networks are listed. The table also displays existing number of connections to the server pool.

3. Select one or more networks to attach to the server pool.

Click Next to specify the number of connections.

4. Enter the total number of connections required as per the virtualization type:
  - For Oracle VM Server for SPARC, you can enter multiple connections. For each network connection, a virtual switch is created. You must physical interface for each virtual switch. You assign these virtual switches to the logical domains.
  - For Oracle VM Server for x86, you can enter only one connection per network. You cannot make multiple connections.
  - For Oracle Solaris Zones, the Oracle Solaris OS version plays an important role. For Oracle Solaris 10 OS, the network is always deployed in shared IP mode. You cannot make multiple connections. For Oracle Solaris 11 OS, the network is always deployed in exclusive IP mode. You can make multiple connections to the network. For each network connection, a VNIC is created when you boot the zone. For a server pool of mixture of Oracle Solaris 10 and 11 OS, the network connection is limited to single connection.

---



---

**Note:** The number of connections do not limit the number of guests to be connected to be network.

---



---

Click Next to configure the interfaces.

5. When one of the virtualization hosts are connected to the network, the corresponding rows for network configuration for that hosts are not displayed. If not, specify the information for each connection:
  - Specify the NIC and IP address for each connection.  
You can assign the same NIC to different network connection when the VLAN IDS are different for the networks.
  - Use System Allocated for the system to take care of the NIC and IP address allocation.
  - Use Do Not Allocate IP which is available for zones and Oracle VM Server for SPARC. You can connect to the network without specifying the IP address.

Click Next to view the summary of the information.

6. Review the information provided and click Finish to attach the networks to the server pool.

Ensure that you have provided correct information. Otherwise, the network attach job fails.

## Associate Libraries

You can associate the following types of storage libraries to the server pool:

**Table 17-3 Supported Libraries**

	Oracle VM Storage Repositories	NAS Libraries	SAN Fibre Channel Libraries	SAN iSCSI Libraries
Oracle VM Server for SPARC	No	Yes	Yes	Yes
Oracle VM Server for x86	Yes	Yes	Yes	Yes
Oracle Solaris Zones	No	Yes	Yes	Yes

When you associate libraries with the server pool, only the libraries that are reachable from the virtualization hosts in the server pool are listed. Depending on the type of library, you either provide virtual disks or LUNs to the guests' storage.

### To Associate a Storage Library

1. Select the server pool.
2. Click Associate Libraries from the Actions pane.  
The Associate Library window displays.
3. The storage libraries that are accessible from the virtualization hosts in the server pool are listed. Select the libraries that you want to associate with the server pool. You can one or more storage libraries from the list.
4. Click Associate Libraries to associate the selected libraries with the server pool.

## Create Guests

The guests refer to the logical domains, zones or the virtual machines that can be created in the virtualization hosts. According to the virtualization type of the server pool, you have the following options:

- Oracle VM Server for SPARC – Create Logical Domains
- Oracle Solaris Zones – Create Zones
- Oracle VM Server for x86 – Create Virtual Machines

These options trigger the deployment plans for the corresponding guests. Refer to the following chapters to refer to the profile and plan creation for the guests:

- [Chapter 14, "Oracle Solaris Zones"](#)
- [Chapter 15, "Oracle VM Server for SPARC"](#)
- [Chapter 16, "Oracle VM Server for x86"](#)

## Migrate Multiple Guests

When you place a virtualization host in a server pool, the option to migrate one or more guests is enabled. The following options become available for the virtualization hosts:

- Oracle Solaris Zones – [Migrate Zones](#)
- Oracle VM Server for SPARC - [Migrate Logical Domains](#)
- Oracle VM Server for x86 – [Migrate Virtual Machines](#)

## Migrate Zones

You can migrate multiple zones from a global zone which is in a server pool. You can migrate the zones to an individual global zone or other zones server pool. When you migrate zones, the source and the target global zone must be compatible. The target global zones must have the following characteristics:

- Running at least Oracle Solaris 10 8/07 OS.
- Can access all the storage libraries associated with the zone.

Apart from compatibility, the target and the source global zone might have differences in the patches and packages installed on them. You can choose to update the zone to match the patches and packages of the target global zone.

---

---

**Note:** You cannot downgrade the patches and packages of the zone. The migration fails in such scenario.

---

---

You can also force the migration of the zone without updating the patches and packages. Select the update options while migrating the zone.

### To Migrate Multiple Zones

1. Select the global zone from which you want to migrate the zones.
2. Click Migrate Zones in the Actions pane.

The Migrate Zones wizard displays.

3. The list includes the zones running in the global zone. Select one or more zones from the list.

Click Next.

4. Select an individual global zone or server pool to which you can migrate the zones.

The table displays the list of eligible global zones and server pool to which you can migrate the zones. The target global zone in the server pool depends on the server pool placement policy.

5. Select an update option to continue with migration.

The source and the target global zones might not be in the same patch level. Either you can select to update the patches and packages of zone to match the target global zone or continue migration without updating the zone.

6. Review the details and click Finish to migrate the zones.

## Migrate Logical Domains

Migrate multiple logical domains from an Oracle VM Server to another Oracle VM Server in the same server pool. You cannot do cross server pool migration.

Only from Oracle VM Server for SPARC 2.1 version, live migration of logical domains is supported. For earlier releases, it is warm migration. The logical domains are shut down and then restarted on the target server.

### To Migrate Logical Domains

1. Select the Oracle VM Server in a server pool.
2. Click Migrate Logical Domains in the Actions pane.
3. The list of logical domains running in the Oracle VM Server are listed. Select one or more logical domains from the list.
4. Select an Oracle VM Server from the list.

The table lists the Oracle VM Servers that have enough resources to host the logical domains in the same server pool. The Oracle VM Server are listed in the decreasing order of preference.

5. Review the information and click Finish to migrate the logical domains.

## Migrate Virtual Machines

For Oracle VM Server for x86 systems, you can migrate virtual machines only within a server pool. Live migration of virtual machines is supported. The eligible Oracle VM Servers have the following characteristics:

- Owned by the Oracle VM Manager.
- Placed in the same server pool as the source Oracle VM Server.
- Have required resources to host the virtual machines.
- Identical in machine make and model of the source Oracle VM Server.

### To Migrate Virtual Machines

1. Select the Oracle VM Server in the server pool.
2. Click Migrate Virtual Machines in the Actions pane.
3. Select the virtual machines that you want to migrate.
4. Select the Oracle VM Server to which you want to migrate the virtual machines.

The table lists the Oracle VM Servers that are eligible to host the virtual machines.

5. Review the summary and click Finish to migrate the virtual machines.

## Balancing Resources

When you have selected to balance server pool resource manually, use the Balance Resources action to check for the under-utilization or over-utilization of resources. Select a server pool and click Balance Resources in the Actions pane to display the current utilization of the virtualization hosts in the server pool. When balancing is required according to the placement policy, Oracle Enterprise Manager Ops Center displays a list of target server that can accept migrated guests. Click Balance Resources button to start the migration job.

## Delete Server Pool

Use the option Delete Server Pool to release the virtualization hosts back to stand-alone state. The type of server pool imposes some limitations to delete a server pool.

### Oracle VM Server for SPARC

When you want to delete an Oracle VM Server for SPARC server pool, shut down the logical domains running in the server pool. Only when the logical domains are detached, you can delete the server pool.

### Oracle Solaris Zones

For a zones server pool, you can delete the server pool and the zones continue to be attached to the global zone. There are no restrictions to shut down the zones before deleting a zones server pool.

### Oracle VM Server for x86

Shut down all the virtual machines and remove all Oracle VM Servers except for the Master Oracle VM Server before deleting the server pool. The virtual machine metadata and virtual disks are stored in the storage library. The virtual machine details are not lost and you can start the virtual machine.

## Related Resources

For instructions in performing actions or to learn more about the role of this feature, go to one of the following resources:

- [Chapter 16, "Oracle VM Server for x86"](#)
- [Chapter 15, "Oracle VM Server for SPARC"](#)
- [Chapter 14, "Oracle Solaris Zones"](#)
- [Chapter 7, "Networks"](#)
- [Chapter 2, "Asset Management"](#)
- [Chapter 6, "Storage Libraries"](#)
- [Chapter 18, "Virtual Datacenters"](#)
- *Oracle Enterprise Manager Ops Center Administration Guide*





---

---

## Virtual Datacenters

This chapter includes the following information:

- [Introduction to Cloud Management](#)
- [Overview of Virtual Datacenter](#)
- [Roles for Managing Virtual Datacenter](#)
- [Actions Available in vDC Management](#)
- [Virtual Datacenter Creation](#)
- [vDC Management](#)
- [Account Creation](#)
- [Account Management](#)
- [Create and Manage vServer Types](#)
- [Overview of Cloud Users](#)
- [Roles for Cloud User Tasks](#)
- [Actions Available for a Cloud User](#)
- [View Account Quotas and Virtual Resources](#)
- [Create and Manage vServers](#)
- [vNets Creation](#)
- [vNets Management](#)
- [Manage Server Templates](#)
- [Volume Creation](#)
- [Snapshot Creation](#)
- [Distribution Group Creation](#)
- [Related Resources](#)

### Introduction to Cloud Management

Oracle Enterprise Manager Ops Center provides the platform to consolidate the physical resources in your data center, and to build and operate your cloud services. The physical resources such as virtualization servers, storage, and network are pooled which are accessed by users to build their applications.

Oracle Enterprise Manager Ops Center provides comprehensive management solution to deploy, configure, and manage the virtualization servers, storage resources, and network fabrics. You can also pool the virtualization resources that share the storage and network resources. All these features are leveraged and can be deployed as Infrastructure-as-a-Service (IaaS) cloud platform service model in Oracle Enterprise Manager Ops Center.

In Oracle Enterprise Manager Ops Center, the provision to setup the IaaS cloud platform service is available as vDC Management. Virtual Datacenter or vDC is a collection of the server pools that share the common storage and network resources. A cloud administrator sets up the infrastructure and provide access to cloud users. The cloud users use the allocated resources to create guest and install an OS of different flavours, deploy applications, monitor, and manage the applications. The cloud user is provided the access to Oracle Enterprise Manager Ops Center UI to view and manage their applications.

Oracle Enterprise Manager exposes APIs and Command Line Interface (CLI) to enable the access to a subset of the Virtual Datacenter functionality. The cloud user can also manage the allocated resources programmatically by calling the IaaS web services directly.

The features accessible through the Cloud Infrastructure API and CLI are available for a Cloud User. The features that are restricted to the Cloud Administrator, such as infrastructure configuration and setup are not available through the Cloud Infrastructure API and CLI except for listing the accessible accounts and to create key based access to cloud users who have access to the accounts already. All the functions that are available for a Cloud User are also available for the Cloud Administrator.

When you log into Oracle Enterprise Manager Ops Center, the views and access for different sections of the UI are different for a cloud administrator and a cloud user.

### **Cloud User**

If you are a cloud user looking for more information about creating and managing virtual servers, then go to the section [Overview of Cloud Users](#).

See *Oracle Enterprise Manager Ops Center Cloud Infrastructure API and CLI Reference Guide* for more information about using Cloud Web Service and Cloud Infrastructure API and CLI.

### **Cloud Administrator**

If you are a cloud administrator, continue with the following sections that describe to create and manage the virtual datacenters in Oracle Enterprise Manager Ops Center.

## **Oracle Engineered Systems**

When Oracle Enterprise Manager Ops Center is installed on Oracle Engineered systems and you want to create and manage a virtual datacenter built upon on the engineered systems, then the procedures described here for setting up the infrastructure and the virtual datacenter might not be suitable.

The infrastructure setup is different and a default virtual datacenter is configured during installation and configuration of Oracle Engineered systems. Refer to the [Chapter 20, "Oracle Engineered Systems"](#) for more information.

## Overview of Virtual Datacenter

In Oracle Enterprise Manager Ops Center, you can consolidate the virtualization servers, storage, and network resources, and enable those resources to be utilized optimally and securely for mixed and dynamic workloads. This optimization of your resources is done by creating a Virtual Datacenter (vDC) in Oracle Enterprise Manager Ops Center.

The physical resources allocated of a vDC are entitled to accounts as virtual resources under quotas set by the cloud administrator. Accounts provide the required capabilities to manage the allocated resources. An account entitles designated cloud users the right to use its virtual computing, network, and storage resources.

A cloud user with access to different accounts can create virtual servers, known as vServers, and host or access applications.

A cloud administrator is involved in setting up the infrastructure for the vDC, creating and managing vDCs, creating and managing accounts, and managing access to cloud users.

## Roles for Managing Virtual Datacenter

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task. See *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 18–1 Virtual Datacenter Roles and Permissions**

Task	Role
Create and Manage Virtual Datacenters	Cloud Administrator
Create and Manage Accounts	Cloud Administrator
Create and Manage vServer Types	Cloud Administrator
Add and Manage Cloud Users	Cloud Administrator

### Required User Role

A cloud administrator can create and manage the virtual datacenters, accounts, and cloud users. The cloud administrator has the role of Asset Admin and Network Admin to setup and manage the virtual datacenter infrastructure.

#### Specify Privileges

To access an already created vDC as a cloud administrator, you must have the proper privileges set to view and manage it. Creating only the cloud admin role is not enough, you must have the privileges for the vDCs to be managed. Contact the Ops Center administrator for more information.

## Actions Available in vDC Management

The virtual datacenter configuration involves the setup of the infrastructure, managing the resource workloads, and understanding cloud user requirements. The user with the cloud administrator role has the following actions:

- Create and manage virtual datacenters
- Create and manage accounts

- Manage access to accounts
- Manage physical resources of virtual datacenter
- Create and manage vServer types

## Virtual Datacenter Creation

Virtual datacenter (vDC) is a consolidation of your physical resources that share the network and storage resources. The physical resources that form a virtual datacenter are:

- **Homogenous server pools**

The server pools are groups of virtualization supported servers that share compatible chip architecture. The supported virtualization types are:

- Oracle Solaris Zones
- Oracle VM Server for x86
- Oracle VM Server for SPARC

In a vDC, you cannot have mixture of server pools that have different virtualization technology. A vDC is based on any one of the supported virtualization technology. This infrastructure difference brings in some major differences in using the vDC. The cloud user might not be aware of the background infrastructure but the cloud administrator ensures that the vDC resources are always highly available to a cloud user. See [Server Pool Setup](#) for more information about the server pool setup required for virtual datacenter.

- **Storage**

The storage is inherited from the server pools. The storage is used for storing rootdisk of the virtual server created in the accounts, virtual server configuration data, templates, ISO images, FLAR images, and also used as volumes. While creating a vDC, you can allocate some storage resources that are used only for volumes. Volumes are used to attach to the vServers. See [Storage Setup](#) for more information about the storage resources required for virtual datacenter.

- **Networks**

Plan the network requirements and attach the network to the server pools. vDC inherits the network resources from the server pools. See [Network Setup](#) for more information about setting up your network resources for virtual datacenter.

## Server Pool Setup

You can create vDC with server pools based on the following types of virtualization technology:

- Oracle VM Server for x86
- Oracle Solaris Zones
- Oracle VM Server for SPARC

See [Chapter 17, "Server Pools"](#) for more information about how to create server pools.

Ensure all the required networks are assigned to the user-defined network domain that is associated with the server pool. The vDC creation wizard displays the list of available server pools in Oracle Enterprise Manager Ops Center. The list includes the server pools that conform to the following characteristics:

- There are virtualization servers in the server pool and the server pool is not empty.
- The server pool is associated with a user-defined network domain.
- Server pools of supported virtualization technology.
- There are compatible storage resources to be used as root disk and volumes for the vServers.
- There are compatible storage resources for saving vServer metadata.

For Oracle Solaris Zones server pool, the pool members must not be a mixture of Oracle Solaris 10 and 11 operating system.

## Storage Setup

The vDC inherits the storage resources allocated for the server pool. The virtualization type of the server pool defines all the possible types of storage resources available for the vDC. Oracle VM Server for x86 based server pools can have the following type of storage resources:

- Oracle VM Storage Repositories
- LUNs allocated from Static Block Storage libraries
- LUNs from Dynamic Block Storage libraries

For Oracle VM Server for x86 server pools, the Oracle VM Storage repositories must be associated with the server pool.

The Oracle Solaris Zones server pools can have the following types of storage resources:

- NAS libraries
- LUNs allocated from Static Block Storage libraries
- LUNs from Dynamic Block Storage libraries

The Oracle VM Server for SPARC server pools can have the following types of storage:

- NAS libraries
- LUNs allocated from Static Block Storage libraries
- LUNs from Dynamic Block Storage libraries

You require the Oracle Solaris Zones and Oracle VM Server for SPARC server pool to be associated with NAS libraries if they are associated only with Block Storage libraries. NAS libraries are required for storing guest metadata details.

### Volume Storage

When you create a vDC, you allocate the storage resources to be used for all the accounts created in the vDC. The allocated storage resources are used as root disks of the vServers and volumes. Volumes are additional storages that you can attach to the vServers. For volumes, the storage is allocated from the storage libraries that are associated with the server pools. A cloud user can also import external volumes into the account.

## Network Setup

Oracle Enterprise Manager Ops Center provides comprehensive network management options that enables secure management of the virtual datacenter.

The server pools must be associated with user-defined network domain to be added to the vDC.

### **Understanding Network Domain Implementation**

The network domain is a logical grouping of related networking components in Oracle Enterprise Manager Ops Center. You can build the network on the following type of fabrics:

- **Fully-managed switched fabrics**

The switches and the fabrics they support are discovered and managed in Oracle Enterprise Manager Ops Center and you can create VLANs or InfiniBand partitions. The network domain created from fully-managed fabrics provides the option to create dynamic private networks.

- **Host-managed fabrics**

Set VLAN IDs to unmanaged Ethernet fabrics and make it host-managed fabrics. Though the switches are not managed in Oracle Enterprise Manager Ops Center, you can assign VLAN IDs to the Ethernet fabrics. You have to manually enable the VLAN IDs on the switch ports connected to the hosts in that fabric. Host-managed fabrics allow you to create dynamic private networks.

Oracle Enterprise Manager Ops Center uses the VLAN IDs set for the creation of dynamic private networks.

- **Unmanaged fabrics**

Neither the switches are managed nor the VLAN IDs are available in Oracle Enterprise Manager Ops Center to create the network. The networks are declared or discovered while discovering an asset in Oracle Enterprise Manager Ops Center. The network domain created out of these networks does not provide the option to create dynamic private networks. You can set aside the networks created on the unmanaged fabrics as private while creating a network domain.

You must ensure that these networks assigned as private are not in use and there is no routing between the selected networks and other networks. These private networks are defined as static private networks. For vDC, a network domain only with unmanaged fabrics can be assigned to a server pool if there are static private networks in it.

### **Dynamic Private Networks**

Each dynamic private network created is allocated a subnet address according to the standards specified in IETF RFC1918. While creating network domains, you can select the option to select the fabric on which you want to create the network, limit the number of networks to be created on the fabric, and the network addresses to be excluded from use.

The number of private networks that you can create on a fully-managed fabric depends on the type of physical fabric. Each port on an Ethernet switch can support 128 logical fabrics. Each partition on an InfiniBand switch can support 32000 logical fabrics. The number of logical fabrics determines how many private networks you can create. For an InfiniBand fabric, each P-key can support a private network. For an Ethernet fabric, each VLAN ID can support a private network.

When you create a network domain, you can set the network creation limit for each selected fabric. This determines how many private vNets that can be created in an account. You can spread the number of private networks across all of the accounts in the vDC.

## Plan Your Network Domains

The network setup must be implemented in such a way that the cloud user has the required network resources available to allocate to the virtual servers created in the accounts. The cloud user must be able to create private networks. The networks must be created upon either fully-managed switched fabrics, host-managed fabrics or unmanaged fabrics.

Create a network domain, assign the managed networks, and associate it with the server pool which must be added to the vDC. The vDC inherits the network domain from the server pool. From the available networks in the network domain, attach the required networks to the server pool. These managed networks form the public external networks for the vDC. You can assign these networks to the accounts created in vDC.

The vDC enables cloud users to create virtual machines and run applications. The cloud user provides networking to its virtual machines from the public networks that are allocated to each account or by creating private networks. The cloud user can use the public networks, or create a private vNet for use in the account. When the cloud users create a private vNet, either a dynamic private network is created or the static private network is available for use in that account.

You must allocate the IP addresses in the public networks and static private networks. This will enable the cloud users to use the allocated IP addresses.

---

---

**Note:** All the server pools in the vDC must be associated with the same user-defined network domain.

---

---

When the cloud user creates a private vNet, it is listed under the network domain of the vDC.

See [Chapter 7, "Networks"](#) for more information about managing fabrics, creating network domains, and private networks.

## Create Virtual Datacenter

Before you create the vDC, it is important to have your server pools, network, and storage set up. When they are set up properly, you can select the required resources for the vDC.

### To Create a Virtual Datacenter

1. Select vDC Management in the Navigation pane.
2. Click Create Virtual Datacenter in the Actions pane.

The Create Virtual Datacenter wizard displays.

3. The first step provides an introduction to the vDC and the prerequisites for creating a vDC.

You can select to skip this step in the future when you create a vDC again. Click Next to specify identification details for the vDC.

4. In the Specify Virtual Datacenter Details, enter the following information:
  - Provide a name and description for the vDC.
  - Enter tags for better identification and classification of the vDC in Oracle Enterprise Manager Ops Center.

Click Next to select the server pools.

5. Select a server pool from the list.
6. Select whether you want to add more compatible server pools as that of the selected server pool.
7. Select the compatible server pools that you want to assign to the vDC.

Click Next to configure the volume storage.

8. Designate some of the storage resources to be used for volumes. You can designate the following storage resources as volume:
  - Oracle VM Server for x86 based vDC
    - Oracle VM Storage Repositories
    - Dynamic Block Storage Libraries
  - Oracle Solaris Zone based vDC
    - NAS Libraries
    - Block Storage Libraries that include both Dynamic and Static
  - Oracle VM Server for SPARC based vDC
    - NAS Libraries
    - Block Storage Libraries that include both Dynamic and Static

Click Next to specify the vCPU sizing.

9. Select the minimum and maximum share of the physical CPU threads that are available for each vCPU.

The virtual datacenter resources are allocated to the accounts. Each account has a quota defined for the usage of vCPU, memory and storage resources. You must specify the share of the physical CPU that each vCPU must receive. Through timesharing of the CPU cycles, you can allocate more vCPUs than the existing physical CPU threads.

For zone based vDCs, you can set the minimum and maximum share of the physical CPU threads. When vServers (zones) are created, the Fair Share Scheduler is the default scheduler. The physical CPU allocation for each vServer is provided by the Fair Share Scheduler.

This option will not be available for Oracle VM Server for SPARC based vDCs as there is one to one relationship between the vCPU and the physical CPU thread.

Click Next to view the summary.

10. The summary lists the total resources that are allocated for the vDC. The summary lists the following:
  - Virtualization type – The virtualization technology of the server pool.
  - Total CPUs – The physical CPU threads available from all the virtualization servers in the selected server pools of the vDC.
  - Total memory – The total RAM allocated to the management domains of the selected server pool. For example, Oracle Solaris Zones based vDC, it is the total memory of the global zones in the server pool. For Oracle VM Server for x86 based server pools, it is the total memory of the Oracle VM Servers in which the virtual machines run.



- Total disk space – The sum of all the disk spaces allocated from the storage libraries associated with the selected server pools.
- vCPU sizing cap values – The minimum and maximum share of the physical CPU for each vCPU must receive.

Confirm the vDC configuration and click Finish to create the vDC.

## vDC Management

You can perform the following actions for managing the vDC:

- [Update vDC Configuration](#)
- [Resource Management](#)
- [Delete vDC](#)

## Update vDC Configuration

You can update the following details of vDC:

- vDC identification and tags.
- Assign more server pools or remove server pools that are not used.
- Assign more storage for volume. You cannot remove the storage already assigned for volume.
- Modify the vCPU sizing.

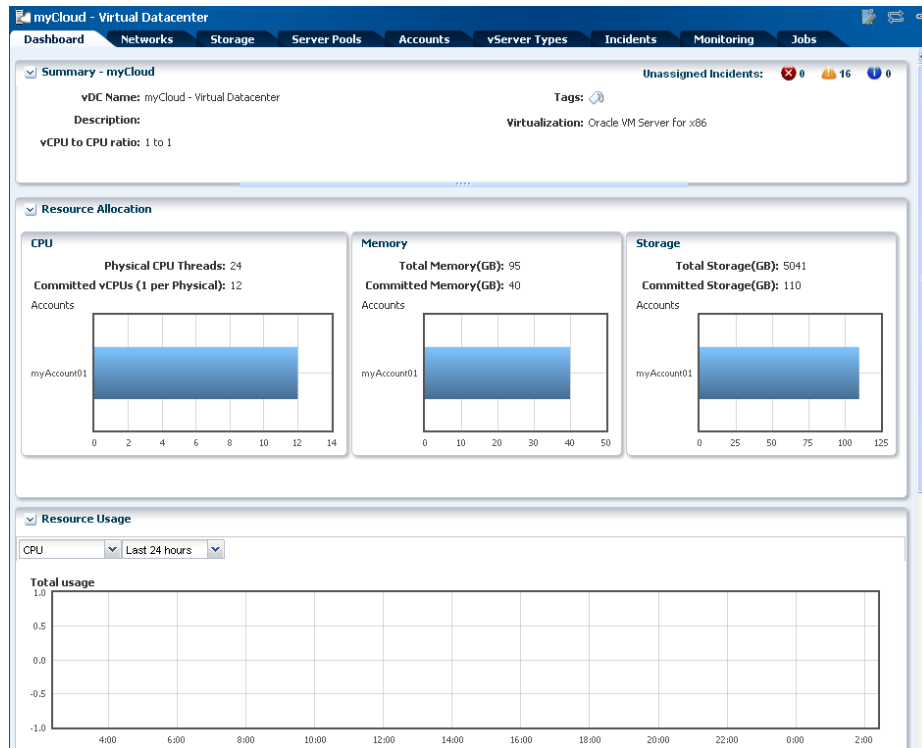
Select a vDC and click the Update Virtual Datacenter option in the Actions pane. Modify the required attributes and complete the wizard.

## Resource Management

Oracle Enterprise Manager provides a complete view of the resources in the vDC and monitors the utilization of the virtualization servers, network, and storage. The cloud administrator gets a good picture of the utilization of the resources which helps to manage the under-utilized and over-utilized resources.

The following figure shows the Dashboard view when you select a vDC.

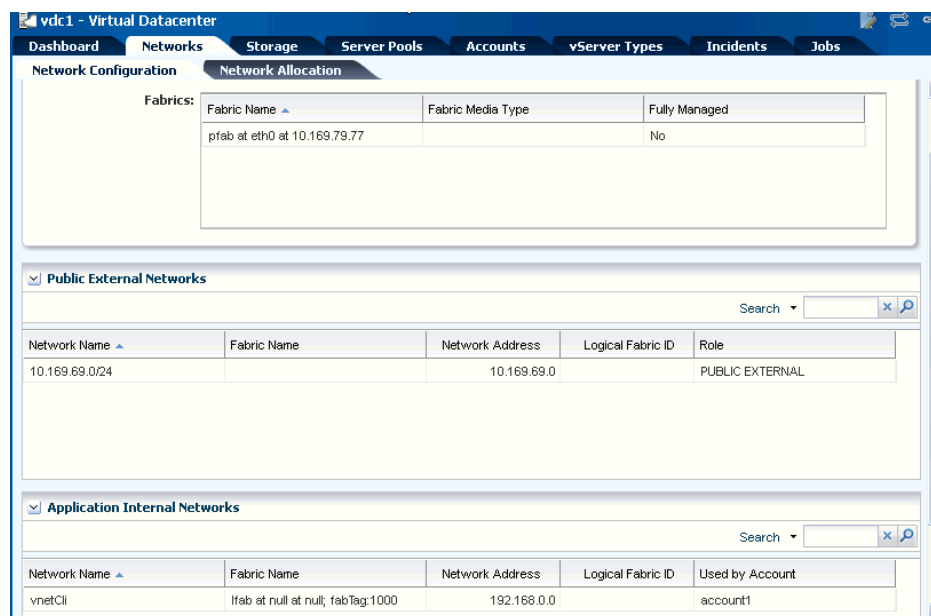
Figure 18–1 Virtual Datacenter Dashboard



The Dashboard shows the total resources available for a vDC and the amount allocated for different accounts. The committed resources indicate the total resources entitled to all the accounts in the vDC.

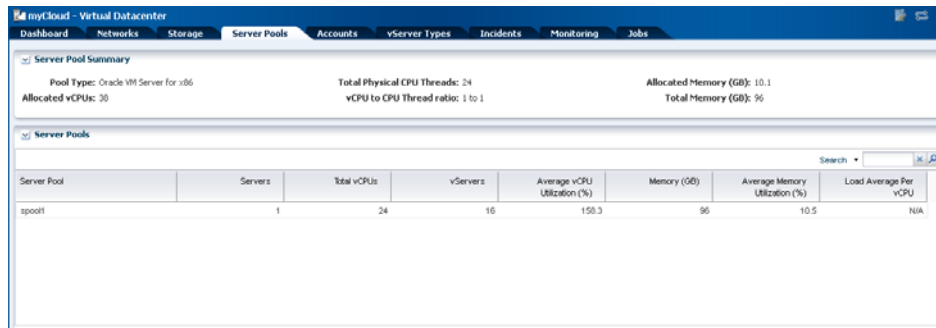
The Network tab displays detailed network usage in the vDC. It lists the fabric and public networks of the vDC, and all of the private networks created by the cloud user. You can see on which fabric the private vNets are created.

Figure 18–2 Network Usage in a vDC



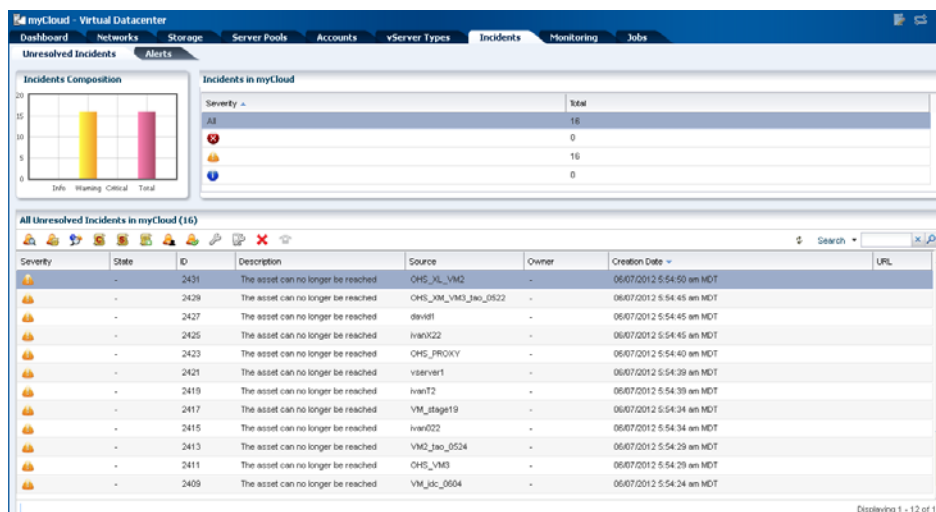
The Server Pools tab shows the usage of the server pool resources. This lists the server pools that are in the vDC. The total and committed resources of vCPU, memory and storage are displayed. This helps you to plan whether you must add more resources to the vDC.

**Figure 18–3 vDC Server Pool Usage**



The Incident tab lists all the incidents reported from all the infrastructure components in the vDC. For each incident, view the source of the incident which will help you to identify the component and the source of the problem. The incidents also covers the warnings issued when the vDC resources are over-utilized.

**Figure 18–4 vDc Incidents Tab**



## Delete vDC

You can delete a virtual datacenter and release all of the resources attached to it. To delete a virtual datacenter, ensure the following conditions:

- No vServers are in the running state in the virtual datacenter.
- Shut down all the vServers in the virtual datacenter.

When you delete a virtual datacenter, all of the suspended or shut down vServers are deleted and the resources are released.

## Account Creation

An account entitles designated cloud users the right to use computing, network, and storage resources of vDC. The account provides the required capabilities to manage these resources.

The prerequisites for creating an account are:

- Estimate the resource quotas to be allocated for the account
- Identify the cloud users to be assigned to the account

The quota for vCPU, memory and storage resources are defined during account creation. The Resource Quota Information display in the account wizard creation indicates how much of the corresponding vDC resources are used. It also displays whether the vDC resources are oversubscribed or undersubscribed.

You can create a maximum of 4096 private vNets in an account. You can set the limit of number of private vNets that can be created in an account.

During account creation, the public networks that are available in the vDC are listed. You can set the number of public IP addresses allocated to the account from the resource. A cloud user can assign the public IP address to a vServer, as needed.

Assign the cloud users to the account during account creation or separately. Cloud users have access to only specific accounts. As a cloud administrator, you can manage the access of the cloud users to all the accounts.

## Create Account

You provide an entitlement to the virtual resources for an account. You allocate the resources from the vDC to an account. The resource allocation for all the accounts in a vDC can be more than the actual resources in a vDC. This oversubscription of the resources must be identified and planned for a vDC. You must configure the virtual resources for an account properly and update the resource configuration when the requirement increases. When an account does not have enough resources, the cloud user receives notifications that they cannot create vServers due to unavailability of resources.

As a cloud administrator watch the resource usage and properly configure the resources for an account.

### To Create an Account

1. Select the vDC in which you want to create the account.
2. Click Create Accounts in the Actions pane.  
The Create Account wizard displays.
3. The first step provides a introduction to accounts and the prerequisites for creating an account.

You can skip this step in the future when you create an account again. Click Next to specify identification details for the account.

4. Enter the name and description for the account.  
Add tags for categorizing and identifying the account. Click Next.
5. Specify the resource quotas for vCPU, memory and storage to the account.

The available resources from vDC are allocated to the vDC. You can over-subscribe the resources. The Resource Quota Information displays whether the vDC

resources are undersubscribed or oversubscribed. This gives a complete picture of the vDC resource usage.

6. Select the number of private vNets a cloud user can create in an account.  
The maximum number of private vNets that you can create in an account is 4096.
7. Select the public networks from the vDC that you can allocate to the account.  
For each network, the available number of IP addresses is displayed. Enter the number of IP addresses that will be allocated to the account. Click Next.
8. Select the cloud users who can access the account. You must assign a cloud user while creating the account. Thereafter, use Add Users option to add more users.
9. Review the account information and click Finish to create the account.

## Account Management

You have the following options to manage the account configuration in a vDC:

- Update account resource configuration
- Assign cloud users to accounts
- Delete an account

### Update Account Configuration

As a cloud administrator, you can modify the identification, and resources allocated to an account. When you want to increase the resources allocated to an account, you can modify by selecting an account and click Update Account in the Actions pane. Modify the resources and complete the wizard.

You cannot remove the resources allocated to an account. Also, you cannot remove the public network or reduce the limit of public addresses assigned to an account.

### Manage Cloud Users to an Account

You can add cloud users to the account and give them the right to use the resources allocated to an account. You can add the cloud users while you create an account or using the option Add Users.

#### To Add a Cloud User

1. Select the account and click Add Users in the Actions pane.  
The Add Users wizard displays.
2. The list of available cloud users and already assigned cloud users to the account are displayed. Select the users to whom you want to assign to the account and move it to the Assigned Users.  
Click Next to view the summary.
3. View the summary and click Finish to add the user to the account.

#### To Remove a Cloud User

1. Select the account.
2. Select the Users tab in the center pane.  
The list of users assigned to the account are displayed.

3. Select the cloud user whom you want to remove.
4. Click the Delete icon.
5. Click Remove to confirm the action.

## Maintaining OS Images

For vDCs based on Oracle VM Server for SPARC virtualization technology, you must manage OS provisioning profiles that the cloud user can use for creating vServers in their environment. The Oracle Solaris 10 ISO or FLAR images must be imported in the NAS libraries associated with the server pools placed in the vDCs.

Configure your Oracle Solaris 11 Software Update Library in the Enterprise Controller to synchronize with the Oracle Solaris 11 Package Repository. The cloud user can use all the profiles for Oracle Solaris 11 OS.

Ensure to configure DHCP in your environment so that the cloud user can install Oracle Solaris 10 ISO image.

OS provisioning profiles that are based on Oracle Solaris 10 FLAR images and Oracle Solaris 11 OS, use WAN boot and do not require DHCP configuration.

See [Chapter 5, "Software Libraries"](#) for more information.

## Delete an Account

Ensure that you do not have running virtual servers in the account. Shut down all the virtual servers in the account. Use the option Delete Account to remove the account.

When there are vServers in running state, the following message displays:

**Figure 18–5 Delete Account**



## Create and Manage vServer Types

vServer Type are profiles of virtual machines that defines the computing resources such as virtual CPU, memory, and storage size. A cloud user can use this to implement and create vServers.

---

**Note:** For vDCs based on Oracle VM Server for x86, the storage size defined in the vServer type does not limit the vServer storage. Instead, the storage size is defined from the server template of the vServer.

---

A vServer type created is available for all the accounts in a virtual datacenter.

As a cloud administrator, you can capture the user requirements and create different vServer Types. Cloud users can use this to create vServers. By default, there are three system-defined vServer types that define the computing resources.

### System-Defined vServer Types

There are three system-defined vServer types provided for all vDCs. The three vServer types are:

- Extra Large
- Large
- Small

The vServer type configuration varies depending on the virtualization technology on which the vDC is constructed.

**Figure 18–6 vServer Types**

Name	Description	Memory Size(GB)	Storage Size(GB)	Number of vCPUs	User Defined
EXTRA_LARGE	Virtual Machine extra-large instan	16	16	4	No
LARGE	Virtual Machine large instance typ	8	8	2	No
SMALL	Virtual Machine small instance typ	4	4	1	No

### To Create a vServer Type

When you create a vServer type, the VM hosting details display the following information in the wizard based on the resources defined:

- The number of virtualization servers in the vDC that have sufficient physical resources to host a vServer with the selected resources.
- An estimation of number of vServers that can be hosted with the total number of physical resources of the vDC.
- A warning when the current value of the memory size exceeds the selected storage size.

The procedure to create a vServer type is as follows:

1. Select the vDC and click Create vServer Type in the Actions pane.

The Create vServer Type wizard displays.

2. Enter the name and description for the vServer type.

Add tags for identification and classification of the vServer type. Click Next.

3. Specify the vCPU, memory and storage resources for the vServer type.

As you enter the values, the VM Hosting displays the following information:

- The number of virtualization servers that have sufficient resources in the vDC to host a vServer of this type.
- The number of vServers that the vDC can host with the total number of physical resources of the vDC.

A warning message is displayed when the current memory size is more than the storage size. The existing vServer types are displayed with the configuration details. You can avoid creating duplicate vServer types.

Provide the values for the resources and click Next.

4. Review the information provided and click Finish to create the vServer type.

### **Update vServer Type**

You can modify the following details of a vServer type:

- Name and description
- Modify, or add new tags
- Modify the resource configuration

Use the option Update vServer Type to launch the Update vServer Type wizard. Modify the configuration and complete the wizard.

### **Delete vServer Type**

You cannot delete the system-defined vServer types. You can delete only the vServer types that you have created.

## **Overview of Cloud Users**

A cloud user with access to an account is entitled to manage and use computing, network, and storage resources allocated in a vDC within the limits of the account quotas.

Cloud users can create and manage the life cycle of vServers for their applications. Creation and management of vServers involve the setup of virtual resources, the management of virtual resource workloads, and understanding application requirements.

Cloud Users can manage the following virtual resources:

- Virtual Networks (vNets) – Used to connect and restrict network access of vServers.
- Server Templates – Provide pre-built images for creating vServers.
- Virtual Storage – Includes volumes that you can attach to vServers, and snapshots to capture the current state of a volume for different purposes.
- vServers – An entity that provides the outward interface of a stand-alone operating system. A vServer has its own identity, local storage, interfaces, and configuration that exist for the full lifetime of the vServer.

Availability and management of some of these virtual resources vary depending on the virtualization technology of the vDC or resource type supported by the vDC.

Oracle Enterprise Manager Ops Center offers to cloud users the option to perform their tasks using its browser interface or through:

- APIs – A Web service API and a Java API to programmatically manage the allocated resources in a vDC account for automation or integration purposes.



- CLI – To manage allocated resources in a vDC account from a text-based console that can be also used for automation or integration purposes.

The following sections in this guide describe the tasks a cloud user can perform in Oracle Enterprise Manager Ops Center using the UI. For more information about the use of APIs and CLI, refer to *Oracle Enterprise Manager Ops Center Cloud Infrastructure API and CLI Reference Guide*.

## Roles for Cloud User Tasks

Table 18–2 lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task. See *Oracle Enterprise Manager Ops Center Administration Guide* for information about the different roles and the permissions they grant.

**Table 18–2 Cloud User Tasks and Roles**

Task	Role
View Account Quotas and Virtual Resources	Cloud User
Create and Manage vServers	Cloud User
Create and Manage Virtual Networks	Cloud User
Create and Manage Volumes	Cloud User
Create and Manage Snapshots	Cloud User
Create and Manage Server Templates	Cloud User

## Actions Available for a Cloud User

A cloud user can perform different actions to use and manage the allocated resources in a vDC account. This section lists the actions a cloud user can perform for each type of resource. It also indicates if the action is available for the different vDC account types.

- View account quotas and virtual resources
- Create and manage vServers
- Create and manage virtual networks
- Create and manage volumes
- Create and manage snapshots
- Create and manage server templates

Based on the virtualization technology on which the vDC and its accounts are created, there might be differences in the availability of the options in the cloud user view. The following tables provide a detailed list of options that are available for a cloud user when the vDC is based on different virtualization technology.

### Account

Action	Oracle VM Server for x86 based vDC	Oracle VM Server for SPARC based vDC	Oracle Solaris Zones based vDC
View account quotas and resources	Yes	Yes	Yes

<b>Action</b>	<b>Oracle VM Server for x86 based vDC</b>	<b>Oracle VM Server for SPARC based vDC</b>	<b>Oracle Solaris Zones based vDC</b>
View account Incidents	Yes	Yes	Yes
View Account Jobs	Yes	Yes	Yes

**vServers**

<b>Action</b>	<b>Oracle VM Server for x86 based vDC</b>	<b>Oracle VM Server for SPARC based vDC</b>	<b>Oracle Solaris Zones based vDC</b>
Create vServer	Yes	Yes	Yes
Stop and start vServer	Yes	Yes	Yes
Pause and Resume vServer	Yes	No	No
Update vServer	Yes	Yes	Yes
Launch Virtual Console	Yes	No	No
Shutdown All vServers	Yes	Yes	Yes
Attach and Detach Volume	Yes	Yes	Yes
Delete vServer	Yes	Yes	Yes

**Networks**

<b>Action</b>	<b>Oracle VM Server for x86 based vDC</b>	<b>Oracle VM Server for SPARC based vDC</b>	<b>Oracle Solaris Zones based vDC</b>
Create private vNet	Yes	Yes	Yes
Update private vNet	Yes	Yes	Yes
Delete private vNet	Yes	Yes	Yes
Allocate vIP	Yes	Yes	Yes
Deallocate vIP	Yes	Yes	Yes
View allocated vIPs	Yes	Yes	Yes

**Volumes and Snapshots**

<b>Action</b>	<b>Oracle VM Server for x86 based vDC</b>	<b>Oracle VM Server for SPARC based vDC</b>	<b>Oracle Solaris Zones based vDC</b>
Create Volume	Yes	Yes	Yes
Create Volume from Snapshot	Yes	No	No
Import Volume	Yes	No	No
Update Volume	Yes	Yes	Yes
Delete Volume	Yes	Yes	Yes
Create Snapshot	Yes	No	No

## Server Templates

Action	Oracle VM Server for x86 based vDC	Oracle VM Server for SPARC based vDC	Oracle Solaris Zones based vDC
Upload Server Template	Yes	No	No
Create Server Template	No	Yes	No
Update Server Template	Yes	Yes	No
Delete Server Template	Yes	Yes	No
Register and Unregister Server Template	Yes	Yes	No

## Distribution Groups

Action	Oracle VM Server for x86 based vDC	Oracle VM Server for SPARC based vDC	Oracle Solaris Zones based vDC
Create Distribution Group	No	Yes	No
Update Distribution Group	No	Yes	No
Delete Distribution Group	No	Yes	No

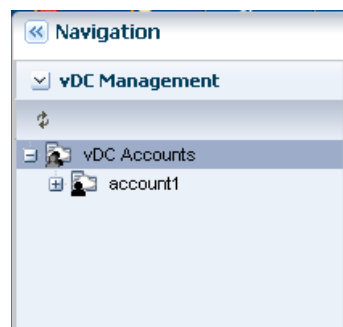
## View Account Quotas and Virtual Resources

Account quotas limit the creation of new virtual resources in the account. A cloud user must be aware of the account quotas and manage the workloads of the virtual resources.

To see the quotas and virtual resources of an account, expand vDC Management in the Navigation pane.

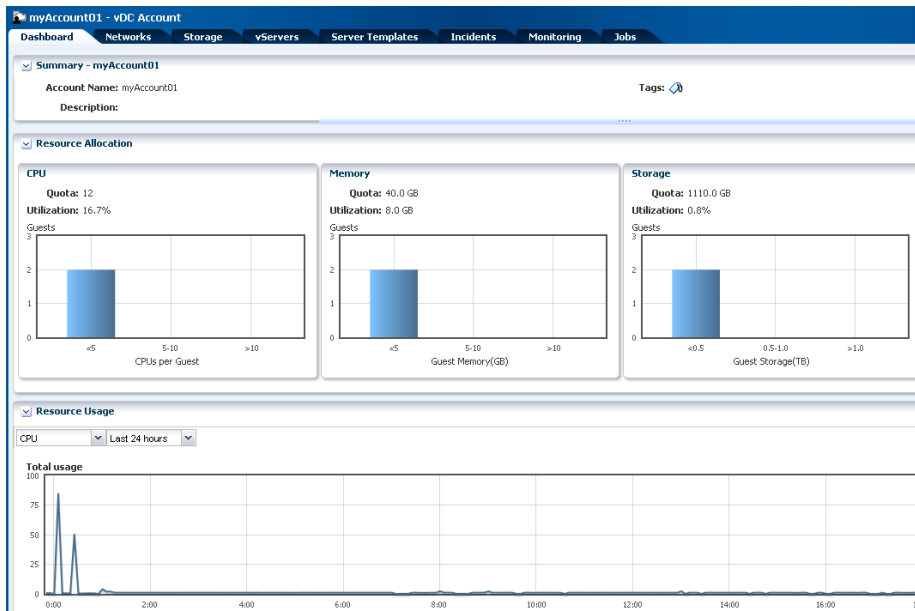
This lists all the accounts to which a cloud user has access under vDC Accounts.

**Figure 18–7 vDC Management**



You can select a listed account to display general account information and quotas in the Dashboard tab of the center pane. The Dashboard tab displays general information about the selected account and a summary of the virtual resources status and usage.

Figure 18–8 vDC Account Center Pane



Virtual resources details appear in the other tabs across the center pane:

- **Networks** – Shows the vNets quotas. Lists and displays information for each private vNet and public network available for the account. Also displays the actions bar for the actions that you can perform for a vNet.
- **Storage** – Shows the storage quotas. Lists and displays information for each vServer root disk, volume, and snapshot available for the account. Also displays the actions bar for the actions that you can perform for a storage resource.
- **vServers** – Shows the CPU quotas. Lists and displays information for each vServer available for the account. Also displays the actions bar for the actions that you can perform for a vServer.
- **Server Templates** – Lists and displays information for each server template available for the account. Also displays the actions bar for the actions that you can perform for a server template.

## Create and Manage vServers

A vServer is an entity that provides the outward interface of a stand-alone operating system that consumes CPU, storage, and memory resources. A vServer has its own identity, local storage, interfaces, and configuration that exist for the full lifetime of the vServer.

You determine the creation of new vServers according to the account quota limits and applications requirements.

### Before You Begin

You must complete the following tasks as prerequisites for creating vServers:

- **Define the memory, storage, and number of CPUs required for the vServers**  
After memory, storage, and number of CPUs are defined, you can select the best suitable vServer type from those available for the account. vServer types are

visible to cloud users during the vServer creation process. Contact your cloud administrator when you require a vServer type.

- **Define the operating system and configuration for the vServers**

You must define the OS and configuration for the vServers. Based on that, you can choose the correct server template. The proper server template must exist before creating a vServer. You can either select a server template from those that exist for the account or create a new server template. Actions to use or create server templates vary based on the virtualization technology used in the vDC. For more information about server templates, see [Manage Server Templates](#)

- **Define the virtual networks to attach to vServers for connectivity**

Plan the network connectivity of the vServers. vServers are only assigned to virtual networks at vServer creation time. You must choose one or more vNets from the available vNets or create new ones before creating a vServer. For more information about vNets, see [vNets Creation](#)

- **Define the IP address assignment method**

You can choose from two different methods for IP address assignment to vServers:

- Static method – Used to assign a specific IP address to a vServer. When using this method you must allocate in advance an IP address from the selected virtual networks. You must consider using this method when creating a single vServer at a time.
- Automatic method – This method dynamically assign an IP address from each selected virtual network. When creating a multiple vServer at a time, only the use of the automatic IP address assignment method is allowed.

- **Define the number of vServers to create**

You can create single or multiple vServers at a time. When creating multiple vServers at a time, vServers are created with the same configuration and a suffix is added to each vServer's name. You must also consider the IP address assignment method when defining the number of vServers.

- **Define the use of the high availability support option for vServers**

Choose to use the high availability support option for vServers. When a high availability is enabled, the vServer is available uninterruptedly. The vServer is not shutdown when the backend infrastructure fails and it is migrated to another server and started. When high availability is not enabled, the vServer starts only after the backend infrastructure is available. Cloud administrator takes care of server pool settings to provide high availability feature in a vDC.

- **Determine the use of the vServers access control mechanism**

You must determine the access mechanism to log into your systems. An option available as an alternative secure method is to use a public key to authenticate SSH root access to the vServer without the use of a password. This option is available to all cloud users, other options to create local user account or provide password for remote SSH access might be present based on the virtualization technology of the vDC.

- **Determine the use of distribution groups for vServers**

You can determine if a vServer needs to be added to a distribution group. This feature is available for vDCs based on Oracle VM Server for SPARC virtualization technology and Oracle Exalogic systems. Distribution group ensures that two vServers are not running in the same Oracle VM Server. If you choose to assign a

vServer to a distribution group, the distribution group must exist before creating the vServer. For more information about distribution group, see [Distribution Group Creation](#).

Some of the other additional tasks that you can perform before or after creating a vServer:

- **Define the use of additional storage for vServers**

When you require additional storage for vServers, attach volumes to vServers. You might attach volumes to vServers at vServers creation time, in that case, volumes must exist before creating the vServers. For more information about creating volume, see [Volume Creation](#).

You can skip this option at vServer creation time, you can also attach volumes at a later time.

## Create vServers

Oracle Enterprise Manager Ops Center provides a wizard that walks you through a series of steps to collect information and resources to create vServers. It is important to have your planning tasks completed before running the wizard.

### To Create vServers

1. Expand vDC Management in the Navigation pane.
2. Select the account from the vDC Accounts list.
3. Click Create vServer in the Actions pane.

The Create vServer wizard displays.

4. Enter the following information in the vServer Details step:
  - Name and description for the vServer.
  - Tags for better identification and classification of the vServer.
  - Number of vServers to create.
  - Check the High Availability Support option if required.

Click Next to select a server template.

5. Select a server template from the list.  
Click Next to select a vServer type.
6. Select a vServer type from the list and click Next.
7. Select one or more volumes from the Available Volumes list. Use the arrow keys to move the selected volumes to the Attached Volumes list.

You can skip this step as the volumes can also be attached after creating a vServer. Click Next to continue.

8. Select one or more vNets from the list.  
Click Next to select the IP address assignment method.
9. Select the IP address assignment method for each vNet and click Next.  
When the static method is selected, choose an IP address from the list.

10. When the Distribution Group Selection step is present, select a distribution group from the list if required.

You can skip this step. Click Next to provide a public key.

**11.** In the vServer Access step, you can choose from one of the available options to get remote SSH access to the vServer:

- Provide a public key to authenticate the SSH root access to the vServer. You can use either of the following options to register the public key:
  - Check the Upload Local Key option to upload the public key from a local file, then click Next to view the Summary.
  - Paste the public key directly into the Public Key text area, then click Next to view the Summary.
- Provide login credentials to authenticate the SSH access to the vServer. This is only available for cloud users using Zones or Oracle OVM for SPARC as virtualization technology in the vDC. You can use one or both of the following options:

- Check the option to supply the password for the remote SSH root access, and click Next.

You will be directed to the Login Credentials step. Enter the password and confirm it, then click Next to view the Summary.

- Check the option to create a local user account and password for remote SSH access, then click Next.

You will be directed to the Login Credentials step. Enter the local user name and the password, then click Next to view the Summary.

You can also skip this step and click Next to view the summary.

**12.** Confirm the vServer information provided in the Summary and click Finish to create the vServer.

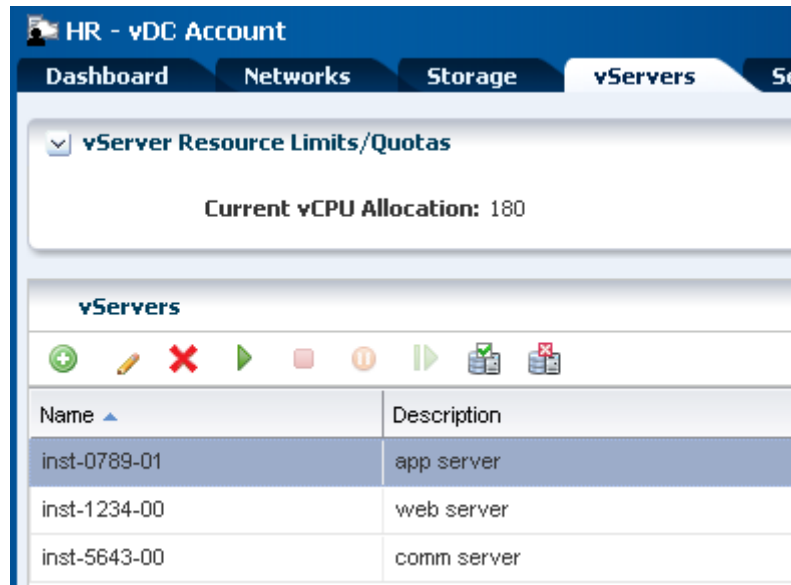
## vServer Management

After creating a vServer, you can manage the vServer life cycle by executing the available actions for vServer management.

To locate all the actions available for managing a vServer:

1. Expand vDC Management in the Navigation pane.
2. Select the account from the vDC Accounts list.
3. Select the vServer tab in the Center Pane.
4. You can then select a vServer from the vServers list and then choose one of the actions displayed.

Figure 18–9 vServer Management Options



Cloud users can perform the following actions to manage a vServer life cycle. The availability of some of the actions depends on the cloud infrastructure. See [Actions Available for a Cloud User](#) for available actions under different cloud infrastructure:

- Update a vServer – To modify the current name or description of a vServer. This action also allows the creation or deletion of vServer tags.
- Stop a vServer – To stop a running vServer. When a vServer is stopped, the guest operating system is shutdown. A stopped vServer can be started later.
- Start a vServer – To start a stopped or shutdown vServer. The restarted vServer might not get the same IP address as the original vServer.
- Pause a vServer – To suspend a running vServer.
- Resume vServer – To start a suspended vServer.
- Shutdown all vServers – To shutdown all vServers listed for an account. This action is only available in the Actions pane.
- Attach vServer volumes – To attach one or more new volumes to a vServer. You must stop the vServer before executing this action.
- Detach vServer volumes – To detach one or more volumes from a vServer. You must stop the vServer before executing this action.
- Delete a vServer – To delete a vServer from a vDC account. Deleting a vServer results in shutting down the vServer followed by the deletion of the vServer.

## vNets Creation

vServers are bound to one or more vNets to restrict network connectivity. There are different types of vNets a cloud user can use:

- Public networks – Created by cloud administrators. Cloud users cannot create, update, or delete this type of vNet. Cloud administrators can also share this type of vNet among a number of accounts in a vDC. vServers that are members of public vNets have also external communication beyond vDCs. You can also use the vServer to host public services.



- Private vNets – Created by cloud users according to their requirements and within the limits of the account quota. A private vNet is created based on the private network from the network domain of the vDC. Private vNets are only accessible within an account. All vServers that have membership to a private vNet in common can communicate freely through that subnet.

Cloud users define which vNets are associated with a vServer. You can specify the membership of a vServer to one or more vNets when you create a vServer. Once a vNet is associated with a vServer, the association persists until the vServer is deleted.

A cloud user can release a reserved IP address that is not allocated to a vServer. Allocated IP addresses are only released when the vServer is deleted.

### Before You Begin

Cloud users can create private vNets. To create a private vNet, you must:

- Plan vServers connectivity.
- Define the number of vServer that can be part of a Private vNet.

## Create a Private vNet

Private vNet is a private virtual network set up exclusively for an account. The vServers associated with this vNet have private virtual IP address for internal communication.

### To Create a Private vNet

1. Expand vDC Management in the Navigation pane.
2. Select the account from the vDC Accounts list.
3. Click Create Private vNet in the Actions pane.

The Create Private vNet wizard displays.

4. Enter the following information in the Private vNet Details step:
  - Name and description for the private vNet.
  - Tags for better identification and classification of the private vNet.

Click Next to configure the private vNet.

5. Select the number of elements for the private vNet.

This is the maximum number of vServers that can be part of this vNet. Use the slide bar to set the value. The values entered are rounded to the next value of 2, 6, 14, 30, 62, 126, 254, 510, 1022, 2046, 4094, and 8190.

Click Next to view the summary.

6. Confirm the private vNet information and click Finish to create the private vNet.

## vNets Management

Virtual network management involves the necessary actions to connect and restrict network access to vServers. After a vNet is created, cloud users can perform the following actions for virtual networks management:

- Allocate vIP – To allocate one or more IP addresses from a private or public vNet. IP addresses are dynamically allocated from those available IP addresses that have

not been assigned to a vServer or allocated previously. You can use allocated vIP addresses for static assignment to vServers.

- View allocated IP addresses – To see a complete list of the allocated IP addresses from a public or private vNet. This list includes all allocated IP addresses that are not assigned to a vServer.
- Deallocate vIP – To release an IP address that was previously allocated from a public or private vNet. IP addresses assigned to a vServer are not listed and they cannot be deallocated. Once an IP address is deallocated, the IP address is available to the account.
- Update a private vNet – To modify the name or description of a private vNet. This action also allows the creation or deletion of vNet tags.
- Delete private vNets – To delete a private vNet. You cannot delete vNets associated with a vServer.

## Manage Server Templates

Server templates designate the operating system and how it will be installed while creating a vServer. Server templates are specific to processor architecture of the server pool and virtualization type and can be pre-built images or identifies the OS distribution.

Server templates are loaded into the storage libraries associated with the vDC and cannot be changed later. By default, a server template is bound to a specific account.

The proper server template must exist before creating vServers. Depending on the virtualization type of the vDC account, cloud users can have the following options:

- Use a default server template provided by the system for creating vServers. This is available only for Zones based cloud infrastructure.
- Upload a new server template to be used for creating vServers. This is available only for Oracle VM Server for x86 based cloud infrastructure.
- Create a new server template for installing vServers. This is available only for Oracle VM Server for SPARC based cloud infrastructure.

## Upload Server Templates

To upload a server template, you can choose from two different server templates sub types:

- Template – Single virtual machine template that is ready to be deployed into virtualized platforms. Templates can be of format `.tgz`, `.tar` or other file types.
- Assembly – Collection of interrelated software appliances that can include a configuration of multiple virtual machines with their virtual disks and their inter connectivity. An assembly is contained in a single `.ova` (Open Virtualization Format Archive) file. When uploading an assembly, you can also create snapshots.

You can either select the server templates stored in the local host machines or from other locations that you can access. Use FTP, HTTP, or HTTPS protocols to upload the server templates from other locations.

Before uploading a server template, you must:

- Decide on a suitable server template sub type.
- Make sure the file for the server template is of the correct format.

- Check whether the file is accessible when uploading the server template from a file in other location.

### To Upload a Server Template

1. Expand vDC Management in the Navigation pane.
2. Select the account from the vDC Accounts list.
3. Click Upload Server Template in the Actions pane.  
The Upload Server Template wizard displays.
4. Enter the following information in the Identify Server Template step:
  - Name and description for the server template.
  - Tags for better identification and classification of the server template.
 Click Next to specify server template details.
5. Choose a server template sub type.
6. Choose an option to upload the server template file.  
When the URL option is selected, enter the complete URL.  
Click Next to view the summary.
7. Confirm the server template information and click Finish to create the server template.

## Create Server Templates

The option to create a server template is available only when the vDC is built on Oracle VM Server for SPARC virtualization technology. You can create server templates from existing OS provisioning profiles. The list of profiles is filtered to display only the distribution which are available to vDC. If a required profile is not available, contact your cloud administrator for required OS provisioning profiles to install your vServers. The OS profiles that have been created for a selected ISO image is made available to create the server template.

### To Create a Server Template

1. Select the Account in the vDC Management section.
2. Click Create Server Template in the Actions pane.  
The Create Server Template wizard is displayed.
3. Skip the introduction and click Next.
4. Enter the name and description for the server template.  
If required, enter tags for easy classification and categorization.  
Click Next.
5. Select a profile that provisions Oracle Solaris OS.  
You can install Oracle Solaris 10 or Oracle Solaris 11 OS on the vServer. Click Next.
6. Review the information and click Finish to create the server template.  
The new template will be created and will be available to be used to create a vServer.

## Server Template Management

You can perform the following actions for server templates management:

- Update Server Template – To modify the name or description of a server template. This action also allows the creation or deletion of server template tags.
- Register Server Template – To register a server template for public use. Registering a server template make the server template available to other accounts in the vDC.
- Unregister Server Template – To unregister a server template is accessible for public use. Unregistering a server template make the server template available to only to the vDC account from which the server template was created.
- Delete Server Template – To delete a registered or unregistered server template. Deletion of a server template does not influence a vServer that was created based on the server template.

These options are disabled when the vDC is built on Zones virtualization technology.

## Volume Creation

A volume is a virtual block storage device that you can attach or detach from vServers. Volumes are bound to an account. Storage space for volumes is limited by the account's quota.

You can attach one or more volumes to a vServer at vServer creation time or at a later time.

To create a volume, you can:

- Create a new empty volume specifying only the size.
- Create a volume from a snapshot. A volume created from a snapshot can be empty or not. The size of the volume is defined by the snapshot. Availability of this action depends of the virtualization type of the vDC account. This action might be disabled for some cloud users.
- Import volume from another location. Volumes must be contained in a file of the format `.img`. Volume files must be accessible by the Enterprise Controller, using HTTP, HTTPS or FTP protocols. This action is available only when the vDC is built on Oracle VM Server for x86 based virtualization technology.

Volumes can be shared at volume's creation time. When a volume is shared, the volume is available for all the cloud users of the account.

### Before You Begin

Before creating a volume a cloud user must:

- Verify the storage space available for the account and plan accordingly.
- Decide for a suitable option to create the volume.  
When importing a volume, check for file accessibility and format.
- Define whether the volume must be shared.

## Create a Volume

You can create or import volumes. The procedures to create and import volumes are described in this section.

**To Create an Empty Volume**

1. Expand vDC Management in the Navigation pane.
2. Select the account from the vDC Accounts list.
3. Click Create Volume in the Actions pane.  
The Create Volume wizard displays.
4. Enter the following information in the Volume Details step:
  - Name and description for the volume.
  - Tags for better identification and classification of the volume.Click Next to configure the volume.
5. Check the Shared option if required.
6. Enter the size of the volume.  
Click Next to view the summary.
7. Confirm the volume information and click Finish to create the volume.

**To Create a Volume from a Snapshot**

1. Expand vDC Management in the Navigation pane.
2. Select the account from the vDC Accounts list.
3. Select the Storage tab in the center pane.
4. Select the Snapshot sub tab in the center pane.
5. Select a Snapshot for the Snapshots list.
6. Click the Create Volume from Snapshot action.  
The Create Volume From Snapshot wizard displays.
7. Enter the following information in the Volume Details step:
  - Name and description for the volume.
  - Tags for better identification and classification of the volume.
8. Check the Shared option if required.
9. Click Create to create the volume.

**To Import a Volume**

1. Expand vDC Management in the Navigation pane.
2. Select the account from the vDC Accounts list.
3. Click Import Volume in the Action action.  
The Import Volume wizard displays.
4. Enter the following information in the Volume Details step:
  - Name and description for the volume.
  - Tags for better identification and classification of the volume.
5. Enter the URL in which the external volume resides.
6. Check the Shared option if required.
7. Click Import to import the volume.

## Volume Management

After a volume is created, you can perform the following actions for volume management.

- **Update Volume** – To modify the name or description of a volume. This action also allows the creation or deletion of volume tags.
- **Delete Volume** – To delete a volume from a vDC account. Only volumes that are not currently attached to a vServer can be deleted. Deleting a volume results in releasing storage space. The process of deletion of a volume does not influence a snapshot that has been created previously based on that volume.

## Snapshot Creation

A snapshot is an image of a volume at a given time. A snapshot captures the current state of the volume and is immutable. You can create snapshots for the following purposes:

- Backup of data stored on a volume
- Creation of new volumes based on a snapshot.

Snapshots availability and management are possible only when supported by the storage of the vDC. Contact a cloud administrator for verification.

You can create a snapshot from:

- An existing volume.
- Uploading an assembly. See [Manage Server Templates](#).

There are four types of exposed disks in an assembly's template. Three of them are presented to cloud users as snapshots, this allows cloud users to optionally create a shared volume from the snapshot. The types of disk created as snapshots are:

- **Public Populated** – Extra disk with already present data.
- **Private Raw** – Dynamically created as empty disk, no disk data, just a size.
- **Shared Raw** – Dynamically created as empty disk, no disk data, just a size.

You can create a volume from a snapshot and attach those volumes to vServers.

### Before You Begin

Before creating a volume, you must:

- Verify the storage space available for the account and plan accordingly.
- Decide for a suitable option to create the snapshot: from a volume or from an assembly.

### To Create a Snapshot from Volume

1. Expand vDC Management in the Navigation pane.
2. Select the account from the vDC Accounts list.
3. Click Create Snapshot in the Actions pane.  
The Create Snapshot wizard displays.
4. Enter the following information in the Snapshot Details step:
  - Name and description for the snapshot.

- Tags for better identification and classification of the snapshot.
- Click Next to select a volume.
5. Select a volume from the list.
 

Click Next to view the summary.
  6. Confirm the snapshot information and click Finish.

## Snapshot Management

You can perform the following actions for storage management

- Update Snapshot – To modify the name or description of a snapshot. This action also allows the creation or deletion of snapshot tags.
- Create Volume from a Snapshot – To create a volume base on a snapshot, see [Volume Creation](#)
- Delete Snapshot – To delete a snapshot from a vDC account. Deleting a snapshot does not affect volumes, snapshots exist independently of the volume.

## Distribution Group Creation

Distribution groups are necessary for properties similar to anti-affinity scaling. Distribution groups are available for vDCs based on Oracle VM Server for SPARC virtualization technology and Oracle Exalogic systems. The action to create a distribution group might be disabled to some cloud users.

Distribution groups are bound to a specific account. You can only assign a vServer to a distribution group when you create the vServer. All vServers that are created within a distribution group are placed on a separate server of the server pool the account uses. When a spare server is not available, the create vServer task fails.

The size of the distribution group define the maximum number of vServers that you can associate with a distribution group. The size of the distribution group is limited by the actual number of Oracle VM Servers available in the server pools of the vDC.

### Before You Begin

Before creating a distribution group, you must:

- Be aware of the size limit for creating a distribution groups. Contact a cloud administrator to verify it.
- Plan the creation and vServers distribution for the distribution groups.

### To Create a Distribution Group

1. Expand vDC Management in the Navigation pane.
2. Select the account from the vDC Accounts list.
3. Click Create Distribution Group in the Actions pane.
 

The Create Distribution Group wizard displays
4. Enter the following information in the Distribution Group Details step:
  - Name and description for the distribution group.
  - Tags for better identification and classification of the distribution group.

Click Next to configure the distribution group.

5. Define the size of the distribution group.  
Click Next to view the summary.
6. Confirm the distribution group information and click Finish.

## Distribution Group Management

You can perform the following actions for distribution groups management:

- Update a distribution group – To modify the name or description of a distribution group. This action also allows the creation or deletion of distribution group tags.
- Delete a distribution group.

## Related Resources

For instructions in performing actions or to learn more about the role of this feature, go to one of the following resources:

- [Chapter 17, "Server Pools"](#)
- [Chapter 16, "Oracle VM Server for x86"](#)
- [Chapter 14, "Oracle Solaris Zones"](#)
- [Chapter 7, "Networks"](#)
- [Chapter 6, "Storage Libraries"](#)
- *Oracle Enterprise Manager Ops Center Cloud Infrastructure API and CLI Reference Guide*
- *Oracle Enterprise Manager Ops Center Administration Guide*



# Part V

---

## Command Line Interface

Part V contains the following chapters:

- [Chapter 19, "Command Line Interface"](#)



---



---

## Command Line Interface

The Oracle Enterprise Manager Ops Center Command Line Interface (CLI) is an alternative to the browser user interface for Oracle Enterprise Manager Ops Center.

This chapter explains how to use the Oracle Enterprise Ops Center CLI and all the commands included within this tool.

The following information is included:

- [CLI Features](#)
- [Starting the CLI](#)
- [General Commands](#)
- [Universal Output Filters](#)
- [Command Scripts](#)
- [Commands for Administrative Shell](#)
- [Mode Commands](#)

### CLI Features

The Oracle Enterprise Manager Ops Center CLI can perform many, but not all, functions of Oracle Enterprise Manager Ops Center. The following charts show the available features.

### Asset Discovery, Management, and Grouping

[Table 19–1](#) shows the functions that the CLI can perform for asset discovery, management, and grouping.

**Table 19–1** *Asset Discovery, Management, and Grouping*

Function	Possible with CLI	Mode
Find asset	Yes	Discover
Execute discovery profiles	Yes	Discover
Add asset	No	n/a
Declare asset	No	n/a
Manage asset	Yes	Gear
Unmanage asset	Yes	Gear
Register asset	Yes	Gear

**Table 19–1 (Cont.) Asset Discovery, Management, and Grouping**

Function	Possible with CLI	Mode
View asset data	Yes	Gear
Update asset data	Yes	Gear
Reset a server	Yes	Gear
Refresh a server	Yes	Gear
Manage locator lights	Yes	Gear
Manage power settings	Yes	Gear
Reboot an OS	Yes	Gear
Reinstall an asset on an OS	Yes	Gear
Create a group	Yes	Groups
Add asset to a group	Yes	Groups
Move assets between groups	Yes	Group
Manage power settings of an asset in a group	Yes	Group
Delete a group	Yes	Group
Delete an asset	Yes	Gear

## Operating System Provisioning and Patching

Table 19–2 shows the functions that the CLI can perform for operating system provisioning and patching.

**Table 19–2 Operating System Provisioning and Patching**

Function	Possible with CLI	Mode
Import an OS image	Yes	OSImage
Delete an OS image	Yes	OSImage
Create an OS profile	No	n/a
Import an OS profile	Yes	OSProfile
Export an OS profile	Yes	OSProfile
Clone an OS profile	Yes	OSProfile
Delete an OS profile	Yes	OSProfile
Import a JET template	Yes	OSProfile
Provision an OS	Yes	Gear
Check inventory	Yes	Update
Upload a knowledge base bundle	Yes	Update
Update operating systems	Yes	Update
Create OS update profiles	Yes	Update
Apply OS update profiles	Yes	Update
Add a configuration file	Yes	Update
Add a file to a distribution	Yes	Update

**Table 19–2 (Cont.) Operating System Provisioning and Patching**

Function	Possible with CLI	Mode
Run OS update profiles	No	n/a

## Firmware Provisioning

Table 19–3 shows the functions that the CLI can perform for firmware provisioning.

**Table 19–3 Firmware Provisioning**

Function	Possible with CLI	Mode
Create a firmware image	Yes	FWImage
Update a firmware image	Yes	FWImage
Delete a firmware image	Yes	FWImage
Create a firmware profile	Yes	FWProfile
Update a firmware profile	Yes	FWProfile
Delete a firmware profile	Yes	FWProfile
Update firmware	Yes	Gear
Check firmware compliance	Yes	Gear
Run firmware reports	No	n/a

## Administration

Table 19–4 shows the functions that the CLI can perform for administration.

**Table 19–4 Administration**

Function	Possible with CLI	Mode
Change connection mode	Yes	Update
Deploy a Proxy Controller	No	n/a
Manage users and roles	Yes	User
View roles	Yes	Jobs
Manage jobs	Yes	Jobs
View notifications	Yes	Notifications
Delete notifications	Yes	Notifications
Manage incidents	Yes	Incidents

## Starting the CLI

The CLI must share information with the Enterprise Controller, therefore you must connect the CLI to the Enterprise Controller.

When the CLI runs on a system other than the Enterprise Controller, it needs credentials to connect to the Enterprise Controller. When the CLI runs on the same system as the Enterprise Controller, the CLI does not need credentials.

## Invoking the Command Line Interface

You get access to the command line interface from the following locations:

- Oracle Solaris: `/opt/SUNWoccli/bin/oc`
- Linux: `/opt/sun/xvmoc/bin/oc`

## To Connect From the Enterprise Controller

1. Enter the `oc` command.

```
# ./oc
xvmSh>
```

You can also add some options. For more information about the options for the `oc` command, see [CLI Usage](#).

2. Enter the `connect` command.

```
xvmSh > connect
EnterpriseController >
```

The CLI is connected to the Enterprise Controller.

## To Connect From a Remote System

1. Enter the `oc` command.

```
# ./oc
xvmSh>
```

You can also add some options. For more information about the options for the `oc` command, see [CLI Usage](#).

2. Enter the `connect` command with the `-h <enterprise controller>`, `-u <username>`, and `-p <password>` | `-p@<filename for password>` options.

Examples:

```
xvmSh > connect -h EnterpriseController -u root -p rootpass
EnterpriseController >
```

```
xvmSh > connect -h EnterpriseController -u root -p@/tmp/pwd
EnterpriseController >
```

The CLI is connected to the Enterprise Controller.

---

---

**Note:** If you do not use the `-h`, `-u`, and `-p` options, you are prompted for the Enterprise Controller name, username, and password.

---

---

## CLI Usage

The CLI is accessed with the `oc` command. The `oc` command can be run with the following options:

- Use `-V` | `--version` to show the CLI version and exit.
- Use `-h` | `--help` to show the CLI help and exit.
- Use `-q` | `--quiet` to be as quiet as possible.
- Use `-d` | `--debug <debug level>` to specify a debug logging level. Debug logging levels are `DEBUG`, `FINEDEBUG`, `CMDSTAT`, `INFO`, `WARNING`, `ERROR`, `CRITICAL`, `OFF`, and `ALL`.

- Use `-c | --cmdfile <file>` to execute the `<file>` command file.
- Use `-e | --eval <command>` for one-line execution. The `<command>` command is the only command to be executed. This option can be run with onliners. For more information about one-liners see [CLI One-Liner](#).
- Use `-o | --outfile <file>` to write the output to the `<file>` file.

Examples:

```
#!/oc -V
OpsCenter Command Line Interface 12.1.0

#!/oc -e history
495 connect
496 version
```

## User Variables

Variables can be defined and then used within any command.

- Enter `set <variable name>=<value>`.

Example:

```
#!/oc
#set JOBID=foo.3
#connect
#localhost> jobs.list -x $JOBID
```

## CLI One-Liner

The CLI accepts a list of commands as an argument.

- Enter `./oc -e 'list commands separated by a semicolon'`.

Example:

```
#!/oc -e 'connect ; jobs.list | grep FAILED'
```

## General Commands

The following are general commands used either for CLI execution or as universal commands.

---



---

**Note:** You can use the Tab key to see a list of the available commands or as a completion key when typing a command.

---



---

## Checking Connectivity

The `ping` command checks connectivity to the Enterprise Controller.

- Enter `ping`.

```
EnterpriseController > ping
EMEC None is alive, version : 12.1.0.1848
```

## Displaying User Configuration

The `printenv` command displays the current user configuration. The variables included in the user configuration are:

- `Output_format`: Format for the command output.
- `Parsable_text_separator`: Text separator for parsable command output.
- `Log_level`: Logging level.
- `History_length`: Number of commands saved in the history.
- `Debug`: Debug logging.
- `Pager`: Pager for long output.
- `Continue_on_error`: Continue when a command fails.
- `Text_wrap_width`: Maximum width, in characters, to be displayed in a line.
- `Enter printenv`.

```
EnterpriseController > printenv
output_format=text
parsable_text_separator=
log_level=OFF
history_length=500
debug=false
pager=false
continue_on_error=false
text_wrap_width=-1
```

The user configuration can be changed using the `setenv` command.

## Setting the User Environment

The `setenv` command sets the user environment in the following ways:

```
output_format=text|parsable
parsable_text_separator=integer
log_level=OFF|ON
history_length=integer
debug=true|false
pager=true|false
continue_on_error=true|false
text_wrap_width=integer
```

- `Enter setenv <variable>=<value>`

Example:

```
EnterpriseController > setenv pager=true
```

---

---

**Note:** You must set the pager variable to true before running some commands, such as the `man` command.

---

---

## Recording Console Input and Output

The `record` command copies all console inputs and outputs to a text file. You can save the resulting file in the directory you prefer. Issue the command without a file name to stop the recording.

- `Enter record <filename>`.

```
EnterpriseController > record foo.file
```



---

---

**Note:** You can use the Tab key for filename completion.

---

---

## Using a Source File

The `source` command uses command script files to source commands as if they were entered at the prompt. For more information about command scripts, see [Command Scripts](#). This command is also used to specify a file as the source of an operation when executing other commands. This file can be used for information that is shared by more than one script, or to keep secure information separate.

- Enter `source <filename>`.

```
EnterpriseController > source /tmp/cmds
```

## Viewing the Version

The `version` command displays the version of the CLI, the Oracle Enterprise Manager Ops Center software, the Java SE Runtime Environment, and the Java HotSpot Server VM software.

- Enter `version`.

```
EnterpriseController > version
CLI version: 12.1.0
OpsCenter version: 12.1.0.1848
Platform: Java-1.6.0_21-Java_HotSpot-TM-Server_VM,_17.0-b16,_Sun_Microsystems_
Inc.-on-SunOS-5.10-x86
Jython Version: 2.5.1
```

## Waiting for a Job to Complete

You can set the CLI to wait until either the most recent job or a specific job finishes before launching a new job, using the `wait` command. This can be useful if one job, such as a discovery, is a requirement for another job, such as grouping or managing discovered assets. You can identify a job by its jobID or by its runID.

The `wait` command is used in command scripts where many commands are run almost at the same time, and it is necessary to wait for a job launched by a command to be completed before running the next command. For more information about command scripts, see [Command Scripts](#). This command can be used from within any mode at any time or from the main command line.

- Enter `wait`.

Use the `-i | --jobid <job ID>` option to specify a job ID. The CLI waits for that job to complete.

Use the `-r | --runid <run ID>` option to specify a job runID. The CLI waits for that job to complete. Default is to wait for the last job.

Use the `-a | --all` option to wait for all jobs.

Use the `-n | --maxwait <maximum wait time>` to specify a timeout, a maximum number of seconds to wait for a job to complete.

---

---

**Note:** To interrupt a wait operation during interactive session, press Ctrl+C.

---

---

## Viewing Help

You can use the `help` command to show the available commands. This command can be used from within any mode at any time or from the main command line.

- Enter `help`.

The available commands for the current mode are displayed.

Use the `-l` option to include detailed usage information.

## Reviewing Commands

The `history` command shows recent commands. This command can be used from within any mode at any time or from the main command line.

- Enter `history`.

The recent commands are displayed.

Use the `-n <number of commands>` option to limit the history list.

```
EnterpriseController > history -n 3
```

The history includes a command number for the sequence. To repeat a command in the history enter the `!` character with the command number and press the `Tab` key, as shown in the following example:

```
EnterpriseController > history -n 3
495 connect
496 version
498 history -n 3
#!496 <TAB>
#version
```

## Displaying a Man Page

You can display the man page for a specific mode, using the `man` command. The syntax usage and description for all mode subcommands are included in the man page. This command can be used from within any mode at any time or from the main command line.

- Enter `man <mode name>`.

```
EnterpriseController > man gear
```

If no mode name is given, the CLI man page is displayed.

To see a list of man pages, enter the command and press the `Tab` key.

---

---

**Note:** The `man` command requires the `pager` environment variable to be set to `true` for multipage output before being run. For more information about how to set the `pager` variable to `true`, see [Setting the User Environment](#).

---

---

## Ending a Mode

You can exit a mode and return to the initial CLI prompt, using the `end` command. This command can be used from within any mode at any time or from the main command line.

- Enter `end`.

```
EnterpriseController/gear > end
EnterpriseController >
```

## Disconnecting from Oracle Enterprise Manager Ops Center

The `disconnect` command closes the connection between the Oracle Enterprise Manager Ops Center Command Line Interface and the Enterprise Controller.

- Enter `disconnect`.

```
EnterpriseController > disconnect
xvmSh >
```

## Exiting the CLI

You can exit the CLI from any mode, using the `exit` command. This command can be used from within any mode at any time or from the main command line.

- Enter `exit`.

```
EnterpriseController > exit
#
```

## Universal Output Filters

For any main or mode command, you can constrain the output by appending one of the following filters to the command:

- `|grep regexp` to filter by the regular expression
- `|count integer` to display only the number of output lines
- `|tee filename` to write the output to a file

Example:

```
EnterpriseController/jobs > list | tee /var/tmp/todays_jobs.txt
```

---



---

**Note:** For better results with `grep` and `count` filters, activate parsable output, using the `setenv` command.

---



---

## Command Scripts

The CLI can also be used in a non-interactive way, using command scripts. The following example shows a script named `update.xvm` that writes the inventory of a server to a file:

```
connect finance_svr -u zz3282134 -p b@seball
update
csv_inventory -h finance_svr -f ~/inventory_latest.csv
wait
end
```

To create the file at any time, issue the following command:

```
oc --cmdfile update.xvm
```

To run a command script use the `source` command.

Example:

```
xvmSh > source update.xvm
```

## Commands for Administrative Shell

The following commands are described in this section:

- [ecadm](#)
- [proxyadm](#)
- [agentadm](#)

### 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, it must have the same hostname 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 username and password. It 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 `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 database properties. The default location of `db.properties` file is `/var/opt/sun/xvm/db.properties`

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

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

### **ha-status**

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



-d | --as\_read\_only\_user: Displays full High Availability status info.

### ha-configure-primary

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

### ha-configure-standby

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

-p | --credentialsfilename<credentials-file>: Specifies the file containing the username and password for privileged access. The first line of the file must contain the username 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 username and password for privileged access. The first line of the file must contain the username 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. It 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

## 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 <username> ] [ -p | --passwordfile ] [ -t | --tokenfile <password-file> ] [ -x | --proxy <hostname>[:<port>] ] [ -U | --proxy-user <proxyusername> ] [ -P | --proxy-passwordfile <password-file> ] [ -a | --proxy-ip ]`.

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

The following parameters are optional for registering the Proxy Controller with the Enterprise Controller:

- t | --tokenfile <autoregistration\_tokenfile>: Specifies an autoregistration token stored in a file. This is used as an alternative for Enterprise Controller administrator username and password.
- x | --proxy <hostname>[:<port>]: If an HTTPS proxy is required to reach the Enterprise Controller, specify the <hostname> for that proxy. Specifying the IP port is optional. The default proxy port is 8080.
- U | --proxy-user <proxyusername>: If a proxy requires a username for authentication, use <proxyusername>.
- P | --proxy-passwordfile <password-file>: Uses the password in <password-file> for proxy authentication.
- 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

## **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 <username> ] [ -p | --passwordfile<password-file> ] [ -a | --agent-ip <IP address> ] [ -t | --token <tokenfilename> ] [ -x | --proxy <URI> ] [ -I | --non-interactive ] [ -k | --keep-connection ]

-u | --user <username>: 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 already exists.

### **unconfigure**

Enter `agentadm unconfigure`

## Mode Commands

The commands in this section start a mode that includes a set of subcommands. Use the `man` command to display the man page for each mode.

- **User** - Use user mode to create, view and manage users and roles.
- **Incidents** - Use incidents mode to view and manage incidents.
- **Discover** - Use discovery mode to discover gear (assets).
- **Gear** - Use gear mode to view and manage gear (assets) and provision operating systems and firmware.
- **Groups** - Use groups mode to view, create, and manage groups.
- **Jobs** - Use jobs mode to view and manage jobs.
- **Stats** - Use stats mode to view statistics about the Enterprise Controller.
- **Notifications** - Use notifications mode to view notifications and change notification settings.
- **Update** - Use update mode to view and manage OS update profiles, policies, snapshots, and distributions, and view and change the connection mode.
- **OSImage** - Use osimage mode to view, manage, and install OS images.
- **OSProfile** - Use opsprofile mode to view, manage, and import OS profiles.
- **FWImage** - Use fwimage mode to create, view, and manage firmware images.
- **FWProfile** - Use fwprofile mode to create, view, and manage firmware profiles.
- **Virtualization** - Use virtualization mode to view, and manage virtual hosts and virtual machines.
- **Deploy-Setup** - Use deploy-setup mode to set up the plan and target to deploy an asset.
- **Deploy** - Use deploy mode to deploy an asset.

Unlike the `ecadm` and `proxyadm` commands, which are used for administering the Enterprise Controller and its Proxy Controllers, the CLI operates on the assets of the data center.

To execute a subcommand within a mode:

- Enter the mode, then enter the subcommand.
- Enter `<mode name>.<subcommand name>`.

Example:

```
EnterpriseController > jobs.list
```

## User

User mode allows you to view and manage local and remote users and their roles.

## Starting User Mode

You must switch to user mode to run these commands.

- Enter user in the CLI prompt.

```
EnterpriseController > user
EnterpriseController/user >
```

## Viewing Users

You can view the existing users in the Enterprise Controller.

- Enter show\_local\_users.

A list of users is shown.

Use the `-r | --roles <role name>` option to view users with `<role name>` role. A list of users and their roles are shown.

## Viewing Role Types

You can view the available role types in the Enterprise Controller.

- Enter show\_all\_local\_roles.

## Viewing User Roles

You can view the roles assigned to a specific user in the Enterprise Controller.

- Enter show\_local\_user\_roles `-u | --user <username>`.

## Adding a User to the Enterprise Controller

You can add a user to the Enterprise Controller and grant a role to the new user. The user must already exist in the host where the Enterprise Controller is installed.

- Enter add\_local\_user `-u | --user <username> -r | --role <role or comma-separated roles list>`.

For information about the available role types you can grant to a user, see [Viewing Role Types](#).

## Granting Roles to a User

You can grant a user role to a user of the Enterprise Controller.

- Enter grant\_local\_role `-u | --user <username> -r | --role <role or comma-separated roles list>`.

For information about the available role types you can grant to a user, see [Viewing Role Types](#).

## Replicating User Roles

You can replicate the roles from a source user to a recipient user. The current roles and privileges of the recipient users are overwritten with the roles and privileges of the source user.

- Enter replicate\_user\_roles `-u | --user <source user> -r | --role <recipient user>`.

## Removing Roles From a User

You can remove a role from a user of the Enterprise Controller. For more information about how to see the roles of a user, see [Viewing User Roles](#).

- Enter `revoke_local_role -u | --user <username> -r | --role <role or list of comma-separated roles to remove>`.

## Adding a Directory Server

You can add a directory server.

1. Enter `configureds`.

```
EnterpriseController/user > configureds
EnterpriseController/user/configureds >
```

2. Enter `set name=<name>` to set the directory server name.
3. Enter `set hostname=<hostname>` to set a fully qualified host name.
4. Enter `set use_ssl=<false|true>` if you want to enable or disable SSL. Default is `false`.
5. Enter `set port=<port>` to set a port.
6. Enter `set user=<username>` to set a username to connect with.
7. Enter `set password=<password>` to set a password.
8. Enter `set root_suffix=<root suffix>` to set the root suffix.
9. Enter `set user_dn=<user DN>` to set the user search DN.
10. Enter `set user_scope=<user scope>` to set the user search scope.
11. Enter `set search_filter=<search filter>` to set the user search filter.
12. (Optional) Use the `show` command to show the values of all directory server properties. If necessary, use the `unset <property>` command to unset a property or the `reset` command to reset all properties.
13. Use the `commit` command to finish configuring the directory server.

## Viewing Directory Servers

You can view a list of directory servers and their IDs.

- Enter `get_directory_servers`.  
Use the `-d | --details` option to show directory server details.

## Viewing Remote Users

You can get a list of directory server users and their roles.

- Enter `get_ds_users -d | --directory <directory server name>`.  
Use the `-r | --roles <role>` option to filter users with `<role>` role.

## Synchronizing All Remote Users

You can synchronize all directory server users and their roles with the cache on the Enterprise Controller.

- Enter `sync_all_ds_users -d | --directory <directory server name>`.



### Synchronizing a Single User

You can synchronize a specific user on the directory server with the cache on the Enterprise Controller.

- Enter `sync_ds_users -d| --directory <directory server name> -u| --user <user>`.

### Removing a Directory Server

You can remove a directory server from the Enterprise Controller.

- Enter `remove_directory_service -d| --directory <directory server name>`.

### Deleting a User

You can delete a local user in the Enterprise Controller.

- Enter `delete_local_user -u| --user <username>`.

## Incidents

Incidents mode allows you to view and manage existing incidents.

### Starting Incidents Mode

You must switch to incidents mode to run incidents commands.

- Enter incidents in the CLI prompt.

```
EnterpriseController > incidents
EnterpriseController/incidents >
```

### Viewing Incidents

You can view a list of existing incidents.

- Enter `list`.  
Use the `-l| --details` option to display detailed incidents information.  
Use the `-s| --state <state>` option to filter incidents by `<state>`.  
Use the `-u| --user <owner>` to filter incidents by `<owner>`.

### Viewing Incident Details

You can view details of the existing incidents or a specific incident.

- Enter `show --i| --incidents <incident ID or comma-separated incident IDs list>`.

### Acknowledging an Incident

You can indicate that you are investigating one or more incidents.

- Enter `acknowledge -i| --incidents <comma-separated incident IDs list>`  
Use the `-n| --note <note>` option to add a note.

### Adding an Annotation to One or More Incidents

You can add an annotation to one or more incidents.

- Enter `annotate -i| --incidents <comma-separated incident IDs list>`

Use the `-t | --type <annotation type>` option to specify an annotation type. Annotation types are `comment` or `suggested_action`.

Use the `-s | --synopsis <synopsis>` option to specify an annotation synopsis.

Use the `-n | --note <note>` option to add a note.

### Assigning Incidents

You can assign one or more incidents to a user.

- Enter `assign -i | --incidents <comma-separated incident IDs list> -u | --user <user>`.

Use the `-n | --note <note>` option to add a note.

### Closing Incident

You can close one or more incidents.

- Enter `close -i | --incidents <comma-separated incident IDs list>`.

Use the `-d | --disable-delay <disable delay>` option to disable the incident monitoring conditions, and reactivate the monitors after `<disable delay>` minutes.

Use the `-n | --note <note>` option to add a note.

## Discover

Discover mode allows you to set up and run discovery jobs. You can create a discovery job or use a discovery profile to discover an asset. You can also execute an existing discovery profile.

### Starting Discover Mode

You must switch to discover mode to run discovery commands.

- Enter `discover` in the CLI prompt.

```
EnterpriseController > discover
EnterpriseController/discover >
```

### Creating a Discovery Job

The `create` submode is used to create and launch new discovery jobs. This submode has its own set of commands.

1. Enter `create`.

```
EnterpriseController/discover > create
EnterpriseController/discover/create >
```

2. Set the type of discovery job, for example, OS, ILOM, ALOM.

### Discovering an OS

1. Enter `set type=os`.

2. Enter the discovery credentials.

- Enter `set ssh_user=<user>` to set the login user name.
- Enter `set ssh_password=<password>` to set the login password.

- (Optional) If the login user name is not the root user, enter `set ssh_root_user=<root user>` to set the root user name.
  - (Optional) If the login user name is not the root user, enter `set ssh_root_password=<root password>` to set the root password.
3. Enter `set ipaddrs=<IP address or addresses>` to specify the target IP address or addresses. The following formats can be used:
    - A single IP address.
    - A comma-separated list of IP addresses enclosed in parentheses. Example: (192.168.1.1, 192.168.1.2).
    - An IP range in Classless Inter-Domain Routing (CIDR) subnet notation. Example: 192.168.1.0/24.
    - An IP range in hyphen notation. Example: 192.168.1.1 - 192.168.1.10.
  4. (Optional) Enter `set ssh_port=<port>` to specify a port.
  5. (Optional) Enter `set use_default=true|false` to specify if the factory default credentials are used or not for the discovery job.
  6. (Optional) Enter the `show` command to display all discovery information. If necessary, use the `unset <parameter>` command to unset a discovery parameter or `clear` to reset and revert to default values all configuration data.
  7. Enter `commit` to start the configured discovery job.

The job is launched, and the job ID is displayed.

Example of OS discovery:

```
EnterpriseController/discover > create
EnterpriseController/discover/create > set type=os
EnterpriseController/discover/create > set ssh_user=sysmgmt
EnterpriseController/discover/create > set ssh_password=l0ckit
EnterpriseController/discover/create > set ipaddrs=172.20.28.202
EnterpriseController/discover/create > show
discovery type: Solaris, Linux OS
use_default=False
ipaddrs=172.20.28.202
ssh_user=sysmgmt
ssh_password=l0ckit
ssh_root_user=
ssh_root_password=
ssh_port=
EnterpriseController/discover/create > commit
```

### Discovering an ILOM Service Processor

ILOM is the service processor used in some Oracle Sun servers. An ILOM discovery also discovers operating systems.

1. Enter `set type=ilom`.
2. Enter the discovery credentials.
  - Enter `set ssh_user=<user>` to set the login user name.
  - Enter `set ssh_password=<password>` to set the login password.
  - (Optional) If the login user name is not the root user, enter `set ssh_root_user=<root user>` to set the root user name.

- (Optional) If the login user name is not the root user, enter `set ssh_root_password=<root password>` to set the root password.
3. Enter `set ipaddrs=<IP address or addresses>` to specify the target IP address or addresses. The following formats can be used:
  - A single IP address.
  - A comma-separated list of IP addresses enclosed in parentheses. Example: `(192.168.1.1, 192.168.1.2)`.
  - An IP range in CIDR subnet notation. Example: `192.168.1.0/24`.
  - An IP range in hyphen notation. Example: `192.168.1.1 - 192.168.1.10`.
4. Enter `set ipmi_user=<IPMI user name>`.
5. Enter `set ipmi_password=<IPMI user password>`.
6. (Optional) Enter the `show` command to display all discovery information. If necessary, use the `unset <parameter>` command to unset a discovery parameter or `clear` to reset and revert to default values all configuration data.
7. Enter `commit` to start the configured discovery job.

The job is launched, and the job ID is displayed.

### Discovering an ALOM Service Processor

ALOM is the service processor used in some Oracle Sun servers. An ALOM discovery also discovers operating systems and systems with ILOM service processors.

1. Enter `set type=alom`.
2. Enter the discovery credentials.
  - Enter `set ssh_user=<user>` to set the login user name.
  - Enter `set ssh_password=<password>` to set the login password.
  - (Optional) If the login user name is not the root user, enter `set ssh_root_user=<root user>` to set the root user name.
  - (Optional) If the login user name is not the root user, enter `set ssh_root_password=<root password>` to set the root password.
3. Enter `set ipaddrs=<IP address or addresses>` to specify the target IP address or addresses. The following formats can be used:
  - A single IP address.
  - A comma-separated list of IP addresses enclosed in parentheses. Example: `(192.168.1.1, 192.168.1.2)`.
  - An IP range in CIDR subnet notation. Example: `192.168.1.0/24`.
  - An IP range in hyphen notation. Example: `192.168.1.1 - 192.168.1.10`.
4. Enter `set telnet_user=<telnet user name>`.
5. Enter `set ipmi_password=<password for telnet user name>`.
6. (Optional) Enter the `show` command to display all discovery information. If necessary, use the `unset <parameter>` command to unset a discovery parameter or `clear` to reset and revert to default values all configuration data.
7. Enter `commit` to start the configured discovery job.

The job is launched, and the job ID is displayed.

### Viewing Discovery Profiles

You can list all discovery profiles that can be used to discover systems.

- Enter `list_profiles`.  
Use the `-i | --ids <IDs>` option to give a list of discovery profile IDs to be displayed. IDs must be separated by a comma.

### Viewing Discovery Ranges

You can list all the existing discovery ranges that can be used to discover systems.

- Enter `list_ranges`.  
Use the `-i | --ids <IDs>` option to give a list of discovery ranges IDs to be displayed. IDs must be separated by a comma.

### Viewing Driver Credentials

You can list all driver credentials that can be used to discover systems with.

- Enter `list_credentials`.  
Use the `-i | --ids <IDs>` option to give a list of driver credentials IDs. IDs must be separated by a comma.

### Viewing Discovery Profile Credentials

You can list all driver credentials for a discovery profile that can be used to discover systems with.

- Enter `list_profile_credentials -i | --id <discovery profile iD>`.

### Viewing Discovery Ranges

You can list all driver ranges for a discovery profile that can be used to discover systems with.

- Enter `list_profile_ranges -i | --id <discovery profile iD>`.

### Viewing Networks

You can list all proxy networks that can be used to discover systems with.

- Enter `list_networks`.

### Executing Discovery Profiles

You can execute a discovery profile to discover systems.

- Enter `execute -i | --id <discovery profile id> -t | --targets <target friendly names>`.  
Use `-i | --id <ID>` to execute the discovery profile with ID `<ID>`.  
Use `-t | --targets <target friendly names>` to give a list of target friendly names. Target names must be separated by a comma.  
Use the `-n | --networkuuid <network UUID>` option to give a network UUID.  
Use the `-c | --credentials <discovery credentials IDs>` option to give a list of discovery credentials IDs. IDs must be separated by a comma.  
Use the `-m | --management <management credential ID>` option to give a management credential ID.

Use the `-s | --serviceTag <servicetag credential ID>` option to give a service tag credential ID.

Use the `-a | --agentLess` option to set agentless deployment on.

Use the `-r | --ranges <discovery ranges IDs>` option to give a list of discovery ranges IDs. IDs must be separated by a comma.

## Gear

Use gear mode to view and manage all assets, including operating systems, hardware, and chassis. Although the term for objects that the Enterprise Manager Ops Center software manages is "asset," the CLI uses the term "gear."

### Starting Gear Mode

You must switch to gear mode before using other gear subcommands.

- Enter gear in the CLI prompt.

```
EnterpriseController > gear
EnterpriseController/gear >
```

### Viewing Assets

You can list the assets managed by Oracle Enterprise Manager Ops Center

- Enter list.

```
EnterpriseController/gear > list
Registered Gear:
UFN |Manage state|Description |Asset Type|                UUID                |
-----|-----|-----|-----|-----|
v64v|  MANAGED  |10.79.103.14|  Server  | 6f1f1dg9-f8sc-8b1b-9c81-ddaab86a261d
c4pr|  MANAGED  |10.68.102.26|  Server  | 5a5fff44-d17c-4ca3-8282-ef8cb8aed88d
```

Use the `-l` option to show asset details.

#### Example

```
EnterpriseController/gear > list -l
Registered Gear:
-----
Name : v64v
  Description : 10.79.103.14
  Managed State : MANAGED
  Status : OK
  Lock Info : None
  Is a Zone : False
  Public UUID : 6f1f1dg9-f8sc-8b1b-9c81-ddaab86a261d
  Asset Type : Server
Name : c4pr
  Description : 10.68.102.26
  Managed State : MANAGED
  Status : OK
  Lock Info : None
  Is a Zone : False
  Public UUID : 5a5fff44-d17c-4ca3-8282-ef8cb8aed88d
  Asset Type : Server
```

Use the `f | --filter <filter term>` option to filter the assets list.

### Example

```
EnterpriseController/gear > list --filter v64v
Registered Gear:
UFN |Manage state|Description |Asset Type|                UUID                |
-----|-----|-----|-----|-----|
v64v|  MANAGED  |10.79.103.14|  Server  | 6f1f1dg9-f8sc-8b1b-9c81-ddaab86a261d
```

## Updating Asset Information

You can update the name of any asset, including the Enterprise Controller. You can also update an asset's description and associated tags.

- Enter `update -g | --gear <asset name>`.

Use the `-U | --UUID <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

Use the `--attributes <attribute list>` option to give a list of asset attributes instead of the asset name. This is useful when assets might have the same name. The asset attributes that can be used are the `type`, `UUID`, `UFN`, and `ip`. Attributes must be separated by a comma. The `type` attribute must be `os`, `server` or `chassis`, and the `ip` attribute must be a valid IPv4 address.

Examples:

```
--attributes=ip=192.168.1.1,type='server'
```

```
--attributes=type='server',UFN='foo'
```

Use the `-n | --name <new name>` option to give the asset a new name.

Use the `-d | --description <description>` option to update the asset's description.

Use the `-t | --tags <space-separated list of tags>` option to update the asset's tags.

## Viewing Jobs Associated With Assets

You can view current and historical jobs associated with an OS, server, or chassis.

- Enter `show_jobs -g | --gear <asset name>`.

Use the `-U | --UUID <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

Use the `--attributes <attribute list>` option to give a list of asset attributes instead of the asset name. This is useful when assets might have the same name. The asset attributes that can be used are the `type`, `UUID`, `UFN`, and `ip`. Attributes must be separated by a comma. The `type` attribute must be `os`, `server` or `chassis`, and the `ip` attribute must be a valid IPv4 address.

Examples:

```
--attributes=ip=192.168.1.1,type='server'
```

```
--attributes=type='server',UFN='foo'
```

## Managing an Asset

You can manage discovered assets.

- Enter `manage -g | --gear <asset name> -u | --user <user name with access to asset> -p | --password <username's password>`.

Use the `-U | --UUID <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

Use the `--attributes <attribute list>` option to give a list of asset attributes instead of the asset name. This is useful when assets might have the same name. The asset attributes that can be used are the `type`, `UUID`, `UFN`, and `ip`. Attributes must be separated by a comma. The `type` attribute must be `os`, `server` or `chassis`, and the `ip` attribute must be a valid IPv4 address.

Examples:

```
--attributes=ip=192.168.1.1,type='server'
```

```
--attributes=type='server',UFN='foo'
```

Use the `-t | --type <type>` option to give the asset type. This is useful when assets might have the same name.

### Unmanaging an Asset

You can unmanage a managed asset, removing the asset from the managed asset list and removing any agent.

- Enter `unmanage -g | --gear <asset name>`.

Use the `-U | --UUID <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

Use the `--attributes <attribute list>` option to give a list of asset attributes instead of the asset name. This is useful when assets might have the same name. The asset attributes that can be used are the `type`, `UUID`, `UFN`, and `ip`. Attributes must be separated by a comma. The `type` attribute must be `os`, `server` or `chassis`, and the `ip` attribute must be a valid IPv4 address.

Examples:

```
--attributes=ip=192.168.1.1,type='server'
```

```
--attributes=type='server',UFN='foo'
```

Use the `-u | --user <user>` option to give the user name to be used for unmanage action.

Use the `-p | --password <password>` option to give the user name's password.

Use the `-t | --type <type>` option to give the asset type. This is useful when assets might have the same name.

### Deleting an Asset

You can delete discovered assets to remove it from Oracle Enterprise Manager Ops Center.

- Enter `delete -g | --gear <asset name>`.

Use the `-U | --UUID <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

Use the `--attributes <attribute list>` option to give a list of asset attributes instead of the asset name. This is useful when assets might have the same name. The asset attributes that can be used are the `type`, `UUID`, `UFN`, and `ip`. Attributes



must be separated by a comma. The `type` attribute must be `os`, `server` or `chassis`, and the `ip` attribute must be a valid IPv4 address.

Examples:

```
--attributes=ip=192.168.1.1,type='server'
```

```
--attributes=type='server',UFN='foo'
```

## Reinstalling an Agent Controller on an Operating System

You can reinstall an agent on one or more managed operating systems.

- Enter `reinstall_agent -g | --gear <comma-separated asset list> -v | --version <Agent version to install> -u | --user <user name> -p | --password <password>`.

Use the `-U | --UUID <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

Use the `--attributes <attribute list>` option to give a list of asset attributes instead of the asset name. This is useful when assets might have the same name. The asset attributes that can be used are the `type`, `UUID`, `UFN`, and `ip`. Attributes must be separated by a comma. The `type` attribute must be `os`, `server` or `chassis`, and the `ip` attribute must be a valid IPv4 address.

Examples:

```
--attributes=ip=192.168.1.1,type='server'
```

```
--attributes=type='server',UFN='foo'
```

## Rebooting an Operating System

You can reboot a managed operating system.

- Enter `reboot -g | --gear <OS asset name>`.

Use the `-U | --UUID <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

Use the `--attributes <attribute list>` option to give a list of asset attributes instead of the asset name. This is useful when assets might have the same name. The asset attributes that can be used are the `type`, `UUID`, `UFN`, and `ip`. Attributes must be separated by a comma. The `type` attribute must be `os`, `server` or `chassis`, and the `ip` attribute must be a valid IPv4 address.

Examples:

```
--attributes=ip=192.168.1.1,type='server'
```

```
--attributes=type='server',UFN='foo'
```

## Updating Firmware

You can provision updated firmware on one or more systems using an existing firmware profile.

- Enter `apply_firmware -g | --gear <comma-separated asset list> -p | --profile <firmware profile>`.

Use the `-U | --UUID <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

### Checking Firmware Compliance

You can compare the firmware for a list of assets to a firmware profile.

- Enter `fwprofile_compliance -g | --gear <comma-separated asset list> -p | --profile <firmware profile>`.

### Provisioning an OS

You can provision a new operating system to a managed system. The `provision_os` command starts a submode with its own set of subcommands.

1. Enter `provision_os -g | --gear <asset name> -p | --profile <profile>`.  

```
EnterpriseController/gear > provision_os -g targetsystem -p S10
EnterpriseController/gear/provision_os# >
```
2. Use the `set` command to set the provisioning properties. The properties are:
  - `profile` – The OS profile to use for the provisioning job. Required.
  - `register` – Specifies whether the new OS will be registered. Values are true or false.
  - `manualnetboot` – Values are true or false.
  - `system_type` – The OS that is provisioned. Values are redhat, suse or solaris.
  - `server_name` – The name of the target system. Required.
  - `hostname` – The new host name. Required.
  - `domain`
  - `netmask`
  - `gateway`
  - `nameserver`
  - `ip_address` – The IP address for the OS. Required.
  - `boot_path`
  - `boot_device`
  - `console_baud`
  - `console`
3. (Optional) Use the `show` command to show the values of all provisioning properties. If necessary, use the `unset <property>` command to unset a property or the `reset` command to reset all properties.
4. Use the `commit` command to launch the OS provisioning job.

### Changing Locator Lights

You can activate or deactivate locator lights.

- Enter `set -g | --gear <asset name> -l | --locator <on|off>`.

Use the `-U | --UUID <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

Use the `--attributes <attribute list>` option to give a list of asset attributes instead of the asset name. This is useful when assets might have the same name. The asset attributes that can be used are the `type`, `UUID`, `UFN`, and `ip`. Attributes must be separated by a comma. The `type` attribute must be `os`, `server` or `chassis`, and the `ip` attribute must be a valid IPv4 address.

Examples:

```
--attributes=ip=192.168.1.1,type='server'
--attributes=type='server',UFN='foo'
```

### Enabling or Disabling Notifications

You can enable or disable notifications for a specific OS, server, or chassis.

- Enter `set -g| --gear <asset name> -n| --notifications <on|off>`.

Use the `-U| --UUID <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

Use the `--attributes <attribute list>` option to give a list of asset attributes instead of the asset name. This is useful when assets might have the same name. The asset attributes that can be used are the `type`, `UUID`, `UFN`, and `ip`. Attributes must be separated by a comma. The `type` attribute must be `os`, `server` or `chassis`, and the `ip` attribute must be a valid IPv4 address.

Examples:

```
--attributes=ip=192.168.1.1,type='server'
--attributes=type='server',UFN='foo'
```

### Powering Off a Server or Chassis

You can deactivate a managed server or a chassis.

- Enter `poweroff -g| --gear <asset name>`.

Use the `-U| --UUID <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

Use the `--attributes <attribute list>` option to give a list of asset attributes instead of the asset name. This is useful when assets might have the same name. The asset attributes that can be used are the `type`, `UUID`, `UFN`, and `ip`. Attributes must be separated by a comma. The `type` attribute must be `os`, `server` or `chassis`, and the `ip` attribute must be a valid IPv4 address.

Examples:

```
--attributes=ip=192.168.1.1,type='server'
--attributes=type='server',UFN='foo'
```

Use the `-f| --force` option to force the server or chassis to power off.

### Powering On a Server or Chassis

You can activate a managed server or a chassis.

- Enter `poweron -g| --gear <asset name>`.

Use the `-U | --UUID <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

Use the `--attributes <attribute list>` option to give a list of asset attributes instead of the asset name. This is useful when assets might have the same name. The asset attributes that can be used are the `type`, `UUID`, `UFN`, and `ip`. Attributes must be separated by a comma. The `type` attribute must be `os`, `server` or `chassis`, and the `ip` attribute must be a valid IPv4 address.

Examples:

```
--attributes=ip=192.168.1.1,type='server'
```

```
--attributes=type='server',UFN='foo'
```

## Resetting a Server or Chassis

You can reset a managed server or chassis.

- Enter `reset -g | --gear <server or chassis name>`.

Use the `-U | --UUID <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

Use the `--attributes <attribute list>` option to give a list of asset attributes instead of the asset name. This is useful when assets might have the same name. The asset attributes that can be used are the `type`, `UUID`, `UFN`, and `ip`. Attributes must be separated by a comma. The `type` attribute must be `os`, `server` or `chassis`, and the `ip` attribute must be a valid IPv4 address.

Examples:

```
--attributes=ip=192.168.1.1,type='server'
```

```
--attributes=type='server',UFN='foo'
```

Use `-n | --netboot` to cause each server to do a netboot instead of booting from disk.

Use the `-f | --force` option to force the server or chassis to power off.

## Refreshing a Server

You can refresh the data for a server.

- Enter `refresh -g | --gear <server name>`.

Use the `-U | --UUID <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

Use the `--attributes <attribute list>` option to give a list of asset attributes instead of the asset name. This is useful when assets might have the same name. The asset attributes that can be used are the `type`, `UUID`, `UFN`, and `ip`. Attributes must be separated by a comma. The `type` attribute must be `os`, `server` or `chassis`, and the `ip` attribute must be a valid IPv4 address.

Examples:

```
--attributes=ip=192.168.1.1,type='server'
```

```
--attributes=type='server',UFN='foo'
```

## Groups

Groups mode allows you to view and manage groups.

### Starting Groups Mode

You must change to groups mode to run these commands.

- Enter `groups` in the CLI prompt.

```
EnterpriseController > groups
EnterpriseController/groups >
```

### Viewing Groups

You can view the list of existing groups.

- Enter `list`.
  - Use the `-l | --detail` option to view a list showing group details.
  - Use the `-b | --brief` option to limit the output to group names.

### Viewing Members of a Group

You can view the members of a group.

- Enter `list_members -g | --group <group name>`.

### Viewing Group Memberships

You can view the groups to which an asset belongs.

- Enter `list_membership -n | --gear <asset name>`.
  - Use the `-U | --uuid <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

### Creating a Group

You can create a group.

- Enter `create -g | --group <group> -d | --description <description> -p | --parent <parent group>`.

The parent group must already exist.

### Updating Group Attributes

You can change the name, description, and parent group of a group.

- Enter `update -g | --group <group>`.
  - Use the `-n | --name <new name>` option to rename the group.
  - Use the `-d | --description <new description>` option to give the group a new description.
  - Use the `-p | --parent <new description>` option to give the group a new parent group.

### Adding an Asset To a Group

You can add an asset to a group.

- Enter `attach -n | --gear <asset name> -g | --group <group>`.

Use the `-U | --uuid <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

### Removing an Asset From a Group

You can remove an asset from a group.

- Enter `detach -n | --gear <asset name> -g | --group <group>`.

Use the `-U | --uuid <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

### Moving an Asset From One Group To Another Group

You can move an asset from one group to another group.

- Enter `move -n | --gear <name of gear> -f | --from_group <current group> -g | --group <destination group>`.

Use the `-U | --uuid <UUID>` option to give the asset public UUID instead of the asset name. This is useful when assets might have the same name.

### Deleting a Group

You can delete a group. Deleting a group does not affect the assets within the group.

- Enter `delete -g | --group <group>`.

Use the `-c | --child` option to indicate if sub-groups under the specified group must be also deleted.

### Powering On the Assets in a Group

You can power on assets within a group.

- Enter `poweron -g | --group <group name>`.

Use the `-n | --netboot` option to cause each server to do a netboot instead of booting from disk.

Deactivated hardware within the group is powered on.

### Powering Off the Assets in a Group

You can power off assets within a group.

- Enter `poweroff -g | --group <group name>`.

Use the `-f | --force` option to force the hardware to power off.

Activated hardware within the group is powered off.

### Reset Servers in a Group

You can reset servers inside a group.

- Enter `reset -g | --group <group>`

Use the `-f | --force` option to force the operation.

Use the `-n | --netboot` option to cause each server to do a netboot instead of booting from disk.

## Jobs

Use the jobs mode to view existing jobs.

### Starting Jobs Mode

You must change to jobs mode to run job commands.

- Enter jobs in the CLI prompt.

```
EnterpriseController > jobs
EnterpriseController/jobs >
```

### Viewing Jobs

You can view a list of jobs.

- Enter list.

The list of current and historical jobs is displayed.

```
EnterpriseController/jobs > list
Job ID           Status           Owner           Job Type
-----
amritsar.5      SUCCESS         root           UpdateGearJob
amritsar.4      SUCCESS         root           DeleteAssetJob
amritsar.3      SUCCESS         root           AgentProvisioningJob
amritsar.2      SUCCESS         root           AgentProvisioningJob
amritsar.1      PARTIALLYSUCCESSFUL root           DeleteAssetJob
```

Use the `-l` | `--detail` option to view detailed job information.

Use the `-f` | `--filter <term>` option to filter the job list.

Use the `-o` | `--owner <job_owner>` option to list jobs owned by `job_owner`.

Use the `-s` | `--status <job_status>` option to list jobs with status `job_status`.

Use the `-t` | `--type <job_type>` option to list jobs with job type `job_type`.

Use the `-x` | `--id <job_id>` option to list jobs with job id `job_id`.

Use the `-m` | `--matchAll` option to list jobs that match all of the criteria indicated; default is for any search criteria to match.

Use the `-r` | `--runid <run ID>` option to retrieve information of a job with a specific `runID`.

Use the `-C` | `--limit <limit>` option to limit the number of jobs returned.

Use the `-A` | `--ascend` option to sort results ascending; default is descending.

Use the `-S` | `--sort <job_attribute>` option to sort results on `<job_attribute>`; default is to sort on job id.

Use the `-L` | `--nologdetails` option to not include log details in detailed listing of jobs.

### Starting a Job

You can run an existing job using its job ID.

- Enter `run -x` | `--id <Job ID>`.

Use the `--simulate` option to run the job in simulation mode.

### Repeating a Job on Failed Targets

You can re-run a partially successful job on its failed targets.

- Enter `rerun_on_failed -x| --id <Job ID>`.

### Deleting a Job

Deleting a job removes the job information from Oracle Enterprise Manager Ops Center. You can only delete jobs that are stopped or completed.

- Enter `delete -x| --id <Job ID>`.

### Stopping a Job

Stopping a job ends progress on the job.

- Enter `stop -x| --id <Job ID>`.  
Use the `-f| --force` option to force the operation.

## Stats

In stats mode, you view statistics about the Enterprise Controller:

- Percentage of memory used
- Free memory (MB)
- Average load (15 min)
- CPU utilization percentage

### Starting Stats Mode

You must switch to stats mode to run stats commands.

- Enter `stats` in the CLI prompt.

```
EnterpriseController > stats
EnterpriseController/stats >
```

### Viewing Statistics

You can view statistics about the Enterprise Controller.

- Enter `show`.

Name	Used Mem %	Free Mem (MB)	Avg Load 15min	CPU Util %
EnterpriseController	34.28	6646	1.74	75.00
EnterpriseController	34.28	6646	1.74	75.00
EnterpriseController	34.28	6646	1.74	75.00

Use the `-i| --interval <interval>` option to specify a repeat interval in seconds.

## Notifications

Notifications mode allows you to view notifications.

### Starting Notifications Mode

You must switch to notifications mode to run notifications commands.



- Enter notifications in the CLI prompt.

```
EnterpriseController > notifications
EnterpriseController/notifications >
```

## Viewing Notifications

You can view all current notifications.

- Enter list.

A list of notifications is displayed.

```
EnterpriseController/notifications > list
ID   Severity  Type    Message
-----
1    MEDIUM   INFO    Enterprise Controller registered with Sun. (70002)
2    MEDIUM   INFO    Proxy Controller proxyone (172.20.27.185) has b...
3    MEDIUM   INFO    Proxy Controller proxytwo (172.20.26.218) has b...
```

Use the `-l` | `--detail` option to display a detailed list.

Use the `-f` | `--filter` `<filter term>` option to filter the notifications.

Use the `-s` | `--severity` `<severity>` option to display only notifications of given severity [HIGH|MEDIUM|LOW].

Use the `-c` | `--count` `<max>` option to specify a maximum count of notifications to display.

Use the `-u` | `--username` `<user>` option to display only notifications belonging to a user.

Use the `-i` | `--notification_id` `<ID>` option to display notifications of a specific ID.

Use the `-r` | `--status` `<status>` option to display only notifications according to their status [READ|UNREAD]. Default is to display both.

## Deleting a Notification

You can delete a notification using its ID number.

- Enter delete `-i` | `notification_id` `<notification ID number>`.

```
EnterpriseController > delete -i 43
Successfully deleted notification
```

Use the `-u` | `--username` `<user>` option to delete notifications belonging to a user.

## Update

Update mode allows you to view and manage policies, profiles, and snapshots for OS updates.

### Starting Update Mode

You must change to update mode to run these commands.

- Enter update in the CLI prompt.

```
EnterpriseController > update
EnterpriseController/update >
```

### Viewing OS Update Policies

You can view the available OS update policies.

1. Enter `list_policies`.  
Use the `-l | --detail` option to display a detailed list.

### Viewing OS Update Profiles

You can view the available OS update profiles.

- Enter `list_profiles`.  
Use the `-l | --detail` option to display a detailed list.  
Use the `-p | --profile_name <profile_name>` option to display profiles with a specific profile name.

### Viewing OS Distributions

You can view the available distributions. By default, this command shows only active distributions.

- Enter `list_distros`.  
Use the `-a | --all` option to display inactive and active distributions.

### Viewing Snapshots

You can view the snapshots for a specific asset.

- Enter `list_snapshots -g | --gear <asset name>`.  
The list of snapshots is displayed.

### Searching Inventory

You can search an OS asset or all assets for inventory whose name matches a search string. The search string used for this command must be a regular expression. For a summary of regular expression constructs, visit <http://docs.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html#sum>

- Enter `search_inventory -s | --search_string <search string>`.  
Enter the `-g | --gear <asset name>` option to search a specific asset, or use the `-a | --allgear` option to search all gear. You must use one of these two options.  
Use the `-t | --snapshot <snapshot name>` option to search for a specific snapshot. This option can only be used with the `-g` option.  
Use the `-n | --description_string` option to search descriptions.  
Use the `-c | --csv` option to output to comma-separated values (CSV).  
Use the `-f | --filename <filename>` option to specify a filename for CSV output.  
Use the `-d | --delimiter <delimiter>` option to specify a delimiter character. The default is the pipe (|) character.  
Use the `-e | --enclosure <enclosure>` option to specify an enclosure character. The default is the quote (") character.  
Use the `-p | --append` option to append the data to an existing file.  
Use the `-l | --detail` option to display detailed data.

## Checking Inventory

You can check an OS asset to see if inventory is available for it.

- Enter `check_inventory`.

Enter the `-g | --gear <asset name>` option to check a specific asset, or use the `-a | --allgear` option to check all assets. You must use one of these two options.

Use the `-t | --snapshot <snapshot name>` option to check a specific snapshot. This option can only be used with the `-g` option.

Use the `-c | --csv` option to output to comma-separated values (CSV).

Use the `-f | --filename <filename>` option to specify a filename for CSV output.

Use the `-d | --delimiter <delimiter>` option to specify a delimiter character. The default is the pipe (|) character.

Use the `-e | --enclosure <enclosure>` option to specify an enclosure character. The default is the quote (") character.

Use the `-r | --header` option to include a header line.

Use the `-p | --append` option to append the asset data to an existing file.

## Checking Connectivity to the Knowledge Base

You can check the connectivity to the knowledge base.

- Enter `check_guus`.

Use the `-u | --user <user name>` option to specify a user name.

Use the `-p | --password <password>` option to specify a password.

Use the `--proxy <proxy hostname>` option to specify a proxy.

Use the `--port <proxy port>` option to specify a proxy port.

Use the `--proxyuser <proxy user name>` option to specify a proxy user name.

Use the `--proxypass <proxy password>` option to specify a proxy password.

## Querying Job History

You can view the job history for a specific OS asset.

- Enter `job_history -g | --gear <asset list>`.

Use the `-f | --fromdate <from date YYYYMMDD>` option to specify a from date. The default is seven days ago.

Use the `-t | --todate <to date YYYYMMDD>` option to specify an end date. The default is today.

Use the `-i | --jobids <ID>` option to query a specific job or jobs, you must still supply the asset name.

Use the `-l | --log` option to print logs.

Use the `--fail` option to query failed status.

Use the `--ok` option to query ok status.

Use the `--warning` option to query warning status.

Use the `--nostatus` option to query nostatus status.

Use the `--install` option to query install action.

Use the `--upgrade` option to query upgrade action.

Use the `--uninstall` option to query uninstall action.

Use the `--downgrade` option to query downgrade action.

Use the `--detail` option to show a detailed listing.

### Querying Job Status

You can query job status.

- Enter `get_job_status`.

Enter the `-i | --jobids <job id>` option to query specific jobs, or use the `-a | --alljobs` option to query all jobs. You must use one of these two options.

Use the `-l | --detail` option to print out detail, including logs if available.

Use the `-c | --csv` option to output to comma-separated values (CSV).

Use the `-f | --filename <filename>` option to specify a filename for CSV output.

Use the `-d | --delimiter <delimiter>` option to specify a delimiter character. The default is the pipe (`|`) character.

Use the `-e | --enclosure <enclosure>` option to specify an enclosure character. The default is the quote (`"`) character.

Use the `-r | --header` option to include a header line.

Use the `-p | --append` option to append the asset data to an existing file.

### Uploading a Knowledge Base Bundle

Knowledge base bundles contain current patch data. A knowledge base bundle must be moved to the system running the Enterprise Controller before it can be uploaded.

- Enter `load_kb_bundle -f <path to KB bundle>`.

### Checking the Connection Mode

You can check the connection mode.

- Enter `check_disconnected`.

### Changing to Connected Mode

You can change the Enterprise Controller from disconnected to connected mode.

- Enter `set_connected_mode -c | --connected`.

### Changing to Disconnected Mode

You can change the Enterprise Controller from connected to disconnected mode.

- Enter `set_connected_mode -d | --disconnected`.

### Modifying an OS Asset

You can update a specific OS asset by installing, upgrading, and uninstalling specific packages and patches.

- Enter `modify_gear -g | --gear <assetname> -y | --policy <policy name> -a | --actual`.

Omit the `-a` option to run the job as a simulation.

Use the `--si <search string>` option to specify a search term to add to the install list.

Use the `--sisubstring <search string>` option to make the `--si` search a substring search.

Use the `--su <search string>` option to specify a search term to add to the upgrade list.

Use the `--susubstring` option to make the `--su` search a substring search.

Use the `--sr <search string>` option to specify a search term to add to the uninstall list.

Use the `--srsubstring <search string>` option to make the `--sr` search a substring search.

The search strings used for this command must be regular expressions. For a summary of regular expression constructs, visit

<http://docs.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html#sum>

Use the `--ni <node ids to install>` option to specify node IDs for install.

Use the `--nu <node ids to upgrade>` option to specify node IDs for upgrade.

Use the `--nr <node ids to uninstall>` option to specify node IDs for uninstall.

Use the `-j | --jobname <job name>` option to specify a job name.

Use the `-e | --job-desc <job description>` option to specify a job description.

Use the `-k | --taskname <taskname>` option to specify a task name.

Use the `-f | --profile <profile name>` option to specify a profile name.

Use the `-l | --profiledesc <profile description>` option to specify a profile description.

Use the `-r | --failure_policy <failure policy>` option to specify a failure policy.

Use the `-x | --execution_policy <execution policy>` option to specify an execution policy.

Use the `-n <creator name>` option to specify a creator name.

Use the `-o | --seconds <number of seconds>` option to wait a specified number of seconds before running the job.

Use the `-c | --case` option to run a case sensitive search.

Use the `-d | --desc` option to search the description.

Example:

```
EnterpriseController/update > modify_gear -g "foo.us.oracle.com" --sr SUNWbzip
-y "Yes To All" -a
```

### Applying an Update Profile to an OS Asset

You can apply a profile to an asset, updating all packages and patches to match the profile.

- Enter `apply_profile_to_gear -g | --gear <assetname> -y | --policy <policy name> -f | --profile_name <profile name> -a | --acutal`

Omit the `-a` option to run the job as a simulation.

Use the `-j | --jobname <job name>` option to specify a job name.

Use the `-e | --job-desc <job description>` option to specify a job description.

Use the `-k | --taskname <taskname>` option to specify a task name.

Use the `-f | --profile <profile name>` option to specify a profile name.

Use the `-r | --failure_policy <failure policy>` option to specify a failure policy.

Use the `-x | --execution_policy <execution policy>` option to specify an execution policy.

Use the `-o | --seconds <number of seconds>` option to wait a specified number of seconds before running the job.

The following is an example of a CLI command to deploy a profile job to one or more hosts:

```
EnterpriseController/update > apply_profile_to_gear -g <space separated list of hostnames> -y "Yes To All" -f <profile name>
```

### Creating a Historical Snapshot

You can create a historical snapshot.

- Enter `create_historical_snapshot -g | --gear <asset name> -s | --snapshot <snapshot name> -d | --description <snapshot description>`.

### Deleting a Snapshot

You can delete an existing snapshot of an asset.

- Enter `delete_snapshots -g | --gear <asset name> -s | --snapshot <snapshot name>`.

### Creating a Profile

You can create a new profile by specifying packages and patches to install, upgrade, and uninstall.

- Enter `create_profile`.

You must supply a search string or node id. The search string used for this command must be a regular expression. For a summary of regular expression constructs, visit

<http://docs.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html#sum>

Use the `--si <search string>` option to specify a search term to add to the install list.

Use the `--sisubstring <search string>` option to make the `--si` search a substring search.

Use the `--su <search string>` option to specify a search term to add to the upgrade list.

Use the `--susubstring` option to make the `--su` search a substring search.

Use the `--sr <search string>` option to specify a search term to add to the uninstall list.

Use the `--srsubstring <search string>` option to make the `--sr` search a substring search.

Use the `--ni <node ids to install>` option to specify node IDs for install.

Use the `--nu <node ids to upgrade>` option to specify node IDs for upgrade.

Use the `--nr <node ids to uninstall>` option to specify node IDs for uninstall.

Use the `-f | --profile <distribution name>` option to specify a profile name.

Use the `-o | --distro <profile name>` option to limit by distro name.

Use the `-l | --profiledesc <profile description>` option to specify a profile description.

Use the `-a | --all` option to include all matched packages/patches.

Use the `-c | --case` option to run a case sensitive search.

Use the `-d | --desc` option to search the description.

Use the `-r | --replace` option to replace an existing profile if the names are the same.

### Creating a Profile From Inventory

You can create a new OS profile based on an existing system.

- Enter `create_profile_from_inventory -g | --gear <gear name>`.  
Use the `-t | --snapshot <snapshot name>` option to search for a specific snapshot. This option can only be used with the `-g` option.  
Use the `-f | --profile_name <profile name>` option to specify a profile name.  
Use the `-l | --profile_desc <profile description>` option to specify a profile description.  
Use the `-r | --include_removes` option to include removed packages.

### Deleting a Profile

You can delete a profile.

- Enter `delete_profiles -p | --profilename <profile name>`.

### Adding a File to a Distribution

You can add a file stored on the Enterprise Controller to a distribution.

- Enter `add_file_to_distro -f | --file_path <full path to distribution> -o | --distro_name <distro name> -a | --category_name <category name>`.  
Use the `-s | --security` option to mark the distribution as security.

### Uploading Local Software in Bulk From a Directory

You can upload the content from a directory and its subdirectories to the Updates software library.

- Enter `bulk_upload_directory -D | --distribution <distribution name of uploaded files> -d | --directory <full path to the source directory>`.

---

**Note:** For more information about how to view the available distributions, see [Viewing OS Distributions](#)

---

## Adding a Local Action

You can add a local action.

- Enter `add_local_action -a | --actionname <action name> -f | --filename <file name> -p | --parentname <parent category name> -d | --description <description> -c | --channelname <channel name> -t | --actiontype <action type>`.

The action type must be macro, postaction, preaction, or probe.

## Adding a Local Category

You can add a local category.

- Enter `add_local_category -c | --category_name <category name> -p | --parent_name <parent name> -d | --description <description> -o | --distro <distribution name>`.

Use the `-r | --refresh` option to refresh the hierarchy.

## Deleting a Component

You can delete a component.

- Enter `delete_component -i | --nodeid <node id> -d | --distro <distro>`.

Use the `-k | --donotcheckforinstall` option to refrain from checking for install.

## Adding a Configuration File

You can add a configuration file.

- Enter `add_configuration_file -f | --filename <filename> -p | --pathname <pathname to file> -v | --version <version> -c | --categoryname <category name> -d | --description <description> -c | --channelname <channel name>`.

## Setting a Component File

You can set a component file.

- Enter `set_component_file -n | --componentname <component name> -d | --distro <distribution> -f | --filename <filename>`.

## Finding Nodes

You can find nodes whose names match a search string. The search string used for this command must be a regular expression. For a summary of regular expression constructs, visit

<http://docs.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html#sum>

- Enter `find_nodes -s | --search_string <search string>`.

Use the `-a | --all` option to list all nodes.

Use the `-l | --detail` option to print details.

Use the `-c | --case` option to specify a case-sensitive search.

Use the `-d | --desc` option to search descriptions.

As the following examples shows, when regular expressions are not used correctly, any node is listed as a result:

```
EnterpriseController/update > find_nodes -s SMCcurl-7.21* -a
```



```

Name                               Node id   Distro     Available Certified
-----
EnterpriseController/update > find_nodes -s SMCcurl-7.21.2-0 [1/1/2012] -a
Name                               Node id   Distro     Available Certified
-----

```

#### Correct examples:

```

EnterpriseController/update > find_nodes -s SMCcurl-7.21.* -a
Name                               Node id   Distro     Available Certified
-----
SMCcurl-7.21.0-0 [1/1/2012]        41025315  SOLARIS10_SPARC  True      True
SMCcurl-7.21.1-0 [1/1/2012]        41125695  SOLARIS10_SPARC  True      True
SMCcurl-7.21.2-0 [1/1/2012]        42327548  SOLARIS10_SPARC  True      True

EnterpriseController/update > find_nodes -s SMCcurl-* -a
Name                               Node id   Distro     Available Certified
-----
SMCcurl                            41002397  SOLARIS10_SPARC  False     True
SMCcurl                            46108251  SOLARIS9_SPARC   False     True
SMCcurl                            52104822  SOLARIS10_X86    False     True

```

## OSImage

OS image mode allows you to view and manage OS images.

### Starting OS Image Mode

You must switch to OS image mode to run OS image commands.

- Enter `osimage` in the CLI prompt.

```

EnterpriseController > osimage
EnterpriseController/osimage >

```

### Viewing OS Images

You can view OS images.

- Enter `list`.  
Use the `-l | --detail` option to view a detailed list.

### Importing an OS Image

You can import an OS image when it is located to the Enterprise Controller's local file system.

- Enter `import -f | --filename <image file name and location> -d | --description <description> -n | --name <image name>`.

```

EnterpriseController/osimage > import -f folder/location/image.iso -d Solaris
10 -n Solaris 10
JobId = EnterpriseController.47

```

### Deleting an OS Image

You can delete OS images.

- Enter `delete -n | --name <image name>`.

## OSProfile

OS profile mode allows you to view, import, and export operating system profiles.

### Starting OS Profile Mode

You must switch to OS profile mode to run OS profile commands.

- Enter `osprofile` in the CLI prompt.

```
EnterpriseController > osprofile
EnterpriseController/osprofile >
```

### Viewing OS Profiles

You can view OS profiles.

- Enter `list`.

Use the `-l | --detail` option to view a detailed list.

```
EnterpriseController/osprofile > list
Profile Name: sles10Jeff1
Description: sles10Jeff1
Distro Name: sles10
OS Version: SUSE-Linux-Enterprise-Server-SP2-10.2-0
Platform: x86
```

### Importing a JET Template

You can import a JET template.

- Enter `import_jet_template -p | --profile <profile name> -i | --image <OS image> -t | --template <local template path>`.

### Importing an OS Profile

You can import an OS profile file. If you are importing a profile that you have previously exported, change the 'Name' and 'Payload\_Name' fields before importing.

- Enter `import -f | --file <profile name>`

### Exporting an OS Profile

You can export an OS profile to a designated file.

- Enter `export -p | --profile <profile name> -f | --file <file name.prof>`.

### Copying an OS Profile

You can make a new profile by copying an existing profile.

- Enter `clone -p | --profile <original profile name> -n | --name <new profile name>`.

### Deleting an OS Profile

You can delete an existing profile.

- Enter `delete -p | --profile <profile name>`.

## FWImage

Fwimage mode allows you to view and delete firmware images.

## Starting Fwimage Mode

You must switch to fwimage mode to run firmware image commands.

- Enter `fwimage` in the CLI prompt.

```
EnterpriseController > fwimage
EnterpriseController/fwimage >
```

## Viewing Firmware Images

You can view a list of available firmware images.

- Enter `list`.  
Use the `-l | --detail` option to display a detailed list.

## Creating a Firmware Image

You can create a firmware image.

1. Enter `create`.

The image creation submode is launched.

2. Enter `add_device -v | --vendor <vendor> -m | --model <model>` to add a device for the firmware image.

Use the `-v | --validated` option to specify a validated image.

3. Enter the criteria for the image using the `set` command.
  - Enter `set name=<name>` to set the firmware image name.
  - Enter `set version=<version>` to set the firmware version.
  - Enter `set type=<type>`.
  - Enter `set make=<make>`.
  - (Optional) Enter `set description=<description>`.
  - (Optional) Enter `set size=<size>`.
  - (Optional) Enter `set powerOffRequired=<True|False>`. This criteria is set to `False` by default.
  - (Optional) Enter `set dependeeFirmwarePackageName=<dependencies>`. This criteria is set to `None` by default.
  - (Optional) Enter `set updateCount=<update count>`.
4. (Optional) Use the `show` command to show the current criteria. If necessary, use the `unset <property>` command to unset a property, or use the `reset` command to clear all criteria.
5. Enter `commit` to create the new image using your criteria.

## Updating a Firmware Image

You can update an existing firmware image.

1. Enter `update -i | --image <image name>`.

The image update submode is launched.

2. Enter the new criteria for the image using the `set` command.
  - Enter `set version=<version>` to set the firmware version.

- Enter `set type=<type>` to set the firmware type.
3. Enter `commit` to update the firmware image.

```
EnterpriseController/fwimage > update -i myimage
EnterpriseController/fwimage/update > set version=1.1
EnterpriseController/fwimage/update > set type=ALOM-CMT
EnterpriseController/fwimage/update > commit
Firmware image updated successfully
```

### Deleting a Firmware Image

You can delete any firmware image.

- Enter `delete -i | --image <firmware image name>`.  
The firmware image is deleted.

## FWProfile

Fwprofile mode allows you to view and delete firmware profiles.

### Starting FW Profile Mode

You must switch to fwprofile mode to run firmware profile commands.

- Enter `fwprofile` in the CLI prompt.

```
EnterpriseController > fwprofile
EnterpriseController/fwprofile >
```

### Viewing Firmware Profiles

You can view the existing firmware profiles.

- Enter `list`.  
Use the `-l | --detail` option to display a detailed list.  
A list of firmware profiles is displayed.

### Checking the Status of a Firmware Profile

You can check the status of a firmware profile.

- Enter `status -p | --profile <profile name>`.  
The firmware profile status is displayed.

### Creating a Firmware Profile

You can create a firmware profile using one or more existing firmware images.

- Enter `create -p | --profile <firmware profile name> -i | --images <list of images separated by comma>`.  
Use the `-d | --description <description>` option to add a description to the profile.  
Use the `-r | --reinstall` option to force a reinstall when provisioning the firmware.  
Use the `-g | --downgrade` option to force a downgrade when provisioning the firmware.  
The firmware profile is created.

## Updating a Firmware Profile

You can update an existing firmware profile.

- Enter `update -p | --profile <firmware profile name> -i | --images <list of images separated by comma>`.

Use the `-d | --description <description>` option to add a description to the profile.

Use the `-r | --reinstall` option to force a reinstall when provisioning the firmware.

Use the `-g | --downgrade` option to force a downgrade when provisioning the firmware.

The firmware profile is updated.

## Deleting a Firmware Profile

You can delete a firmware profile.

- Enter `delete -p | --profile <firmware profile name>`.

The firmware profile is deleted.

## Virtualization

The virtualization mode manages virtual hosts and virtual machines (Oracle Solaris zones only).

### Starting Virtualization Mode

You must switch to `virtualization` mode to run virtualization commands.

- Enter `virtualization` in the CLI prompt.

```
EnterpriseController > virtualization
EnterpriseController/virtualization >
```

### Viewing Hosts

You can view the list of guest containers (global zones).

- Enter `list_hosts`.

### Viewing Guests

You can view the list of non-global zones for a specific global zone.

- Enter `list_guests -c | --container <global zone name>`.

### Migrating a Non-Global Zone

You can detach a non-global zone from its non-functioning global zone and attach the non-global zone to a different global zone.

- Enter `startup (-z zonename -S ObjectName | -Z ObjectName) -D ObjectName`.

Use the `-z | --zonename` option to specify a guest (non-global zone). If you select this option you must specify a source global zone object name.

Use the `-S | --source-on` option if you specify a `zonename` before. Using this option you specify a source global zone object name.

Use the `-z | --zone-on` option in case you did not select the `-z | --zonename` option. Using this option you indicate the host (global zone) object name.

Use the `-D | --destination` option to indicate the destination (global zone).

## Deploy-Setup

Deploy-setup mode allows you to specify a deployment plan and its target. The deployment plan must exist already and the asset must be already a managed asset.

### Starting Deploy-Setup Mode

You must switch to deploy-setup mode to run commands for deploying assets. To start the deploy-setup mode, enter the deploy mode, which redirects you to the deploy-setup mode.

- Enter `deploy` in the CLI prompt.

```
EnterpriseController > deploy
EnterpriseController/deploy-setup >
```

### Selecting a Deployment Plan

You must select an existing deployment plan.

- Enter `plan <plan name>`

Use the `-v | --version` option to specify a version of a plan.

```
EnterpriseController/deploy-setup > plan plan-fw
Plan "plan-fw" selected: version 1, description "None"
```

### Selecting a Target Asset

You must select an asset as the target of the deployment plan. You must always indicate an asset name or public UUID. In case of ambiguity, where multiple assets have the same user friendly name, the user is informed to use UUID instead.

- Enter `target <asset name or public UUID>`

You can also add some other options:

Use the `-a | --add` option to add assets to current set of targets.

Use the `-d | --delete` option to delete assets from the current set of targets.

Use the `-g | --gear <asset name>` option to give an asset name or a list of asset names, separated by comma.

Use the `-U | --UUID <public UUID>` option to give an asset UUID or a list of asset UUIDs, separated by comma.

Example using an asset's friendly user name:

```
EnterpriseController/deploy-setup > target foo.us.oracle.com
```

Example using an asset public UUID:

```
EnterpriseController/deploy-setup > target 53f6e87f-3582-4cda-9c63-9121a3a8beb3
```

After you specify the plan and target, the mode changes from the deploy-setup mode to the deploy mode. This is reflected at the command prompt as follows:

```
EnterpriseController/deploy>
```

## Deploy

Deploy mode allows you to deploy an asset.

### Viewing the Plan

You can view the attributes of the deployment plan or the deployment plan structure.

To view the attributes of a deployment plan:

- Enter show plan.

```
EnterpriseController/deploy > show plan
Target: foo.us.oracle.com
```

---

```
Step: Update Firmware
```

---

```
Associated Profile:
{
firmwarePackages:
[
ILOM-3_0_3_31_a-Sun_Fire_X4600M2
]
dryRun: False
subType: Server
resetSP: False
profileDescription:
forceDowngrade: False
forceReinstall: False
profileName: fwp-profile
network: None
ip: None

}
```

If you wish to view the structure of a plan:

- Enter show.

```
EnterpriseController/deploy > show
Step: Update Firmware
```

---

```
{
isDryRun: Dry run?
type: boolean

firmwarePackages: Firmware Packages
type: array of [
type:java.lang.String
]

resetSP: Reset SP?
type: boolean

forceDowngrade: Force Downgrade?
type: boolean

forceReinstall: Force Reinstall?
type: boolean

ip: IP Address
type: java.lang.String
```

```

network: Network Information
{
gateway: Gateway IP Address
type: java.lang.String

objectName: Object Name
type: java.lang.String

userFriendlyName: User Friendly Name
type: java.lang.String

netmask: Network Address Mask
type: java.lang.String

ip: IP Address
type: java.lang.String

}
}

```

There are deployment plans that have results, if you wish to view these results:

- Enter `show results`.

Example:

```

EnterpriseController/deploy > show results
Step: Provision OS
Operating-System-1

```

### Setting the Attributes of a Deployment Plan

You can modify the value of the attributes of a deployment plan. Some deployment plans require specific information during the deployment. See [Table 19–5](#) for the names of the attributes you must set before applying the plan.

**Table 19–5** *Deployment Plans and Attributes*

Deployment Plan	Attributes
Configure M-Series Hardware, Create and Install Domain	No per-target attribute collection required.
Configure RAID	No per-target attribute collection required.
Configure Server Hardware and Install OS	No per-target attribute collection required.
Configure Service Processor	No per-target attribute collection required.
Configure and Install Dynamic System Domain	No per-target attribute collection required.
Configure and Install Logical Domains	No per-target attribute collection required.
Configure and Install Virtual Machines	No per-target attribute collection required.
Create Boot Environment	No per-target attribute collection required.
Create Dynamic System Domain	No per-target attribute collection required.



**Table 19–5 (Cont.) Deployment Plans and Attributes**

Deployment Plan	Attributes
Create Logical Domains	<p>guestName: name of the new logical domain. This is just the name of the virtual server guest.</p> <p>(optional) prime: set to true to set the resource plan data so that the already set profile data on the logical domain step are used to prime the resource data.</p> <p>Logical domains creation requires the setting of resource plan structures per each logical domain to create.</p>
Create Solaris Zones	<p>ipAddress: IP for the new zone, if mode is static.</p> <p>ipMode: IP address assignment mode. Value = static or dynamic.</p> <p>ifName: network interface name to identify NIC to assign to zone.</p> <p>hostName: hostname of the new zone.</p> <p>(optional) prime: set to true to set the resource plan data so that the already set profile data on the zone step are used to prime the resource data.</p> <p>Solaris zones creation requires the setting of resource plan structures per each logical domain to create.</p>
Configure and Install Solaris Zones	The only parameters that must be set are the same as those used in creating an Oracle Solaris zones deployment plan.
Create Virtual Machines	No per-target attribute collection required.
Provision Network	No per-target attribute collection required.
Provision OS	<p>ip: set this attribute if networking option selected in the OS provision profile was None or Link Aggregation.</p> <p>dataIp: set this attribute if networking option selected in the OS provision profile was IPMP.</p>
Install Server	The only parameters that must be set are the same than in provision OS.
Software Deployment / Update	No per-target attribute collection required.
Update Solaris 11 OS	No per-target attribute collection required.
Update BIOS Configuration	No per-target attribute collection required.
Update Firmware	No per-target attribute collection required.
Update Firmware and Install Oracle VM Server for SPARC	No per-target attribute collection required.

Use the following syntax to set an attribute or list of attributes of a deployment plan:

- For simple types:

```
Enter set "<attribute-name> = <'string-value'>" |<int>|<>true|false>
```

Examples:

```
EnterpriseController/deploy > set "forceReinstall = false"
EnterpriseController/deploy > set "ip = '213.123.123.23'"
```

- For attributes that are backed by other struct-like value objects, use the following syntax:

```
Enter set "<attribute-name> = list or nested object"
```

```
set "network={gateway='213.123.123.111', userFriendlyName='ip address',
ip='213.123.123.4'}"
```

- If you use JavaScript Object Notation (JSON) format, use the following syntax:

```
set
"{'resourcePlans': [{'hostName': 'myhostname', 'networks': [{'networkBindings': [{'i
pAddress': '123.123.123.1'}]}]}]"
```

Or

```
set
"resourcePlans=[{hostName='myhostname', networks=[{networkBindings=[{ipAddress='
123.123.123.1'}]}]}]"
```

Or

```
set "<json-string> "
```

- For deployment plans on multiple targets that require unique values for each target, use the `set` command as follows:

```
EnterpriseController/deploy > set "@<target-uuid or
dynamic-target>:<key>=<'string-value'>" |<int>|<>true|false>|list of nested
objects"
set "@<target-uuid or dynamic-target>:<json-string>"
```

Example:

```
EnterpriseController/deploy > set
@<target-UUID>:"network={gateway='213.123.123.111', userFriendlyName='ip
address', ip='213.123.123.4'}"
```

### Adding Attributes to a Deployment Plan

You can add attributes to a deployment plan. The syntax for adding attributes is similar to the syntax for setting attributes. However, in the case of arrays, the `add` command appends an element to the array while the `set` command modifies the attribute of an existing element within the array.

Use the following syntax to add attributes to a deployment plan:

- For simple types:

```
Enter add "<attribute-name> = {'string-value'}" |<int>|<>true|false>}
```

Examples:

```
EnterpriseController/deploy > add "forceReinstall = false"
EnterpriseController/deploy > add "ip = '213.123.123.23'"
```

- For attributes that are backed by other struct-like value objects, use the following syntax:

```
Enter add"<attribute-name> = list or nested object"
```

```
EnterpriseController/deploy > add "network={gateway='213.123.123.111',
userFriendlyName='ip address', ip='213.123.123.4'}"
```

- If you use JavaScript Object Notation (JSON) format, use the following syntax:

```
"{'resourcePlans': [{'hostName': 'myhostname', 'networks': [{'networkBindings': [{'i
pAddress': '123.123.123.1'}]}]}]"
```

Or

```
add
"resourcePlans=[{hostName='myhostname',networks=[{networkBindings=[{ipAddress='
123.123.123.1'}}]}]}]"
```

Or

```
add "<json-string> "
```

- For deployment plans on multiple targets that require unique values for each target, use the `set` command as follows:

```
add "@<target-uuid or
dynamic-target>:<key>=<'string-value'>"|<int>|<>true|false>|list of nested
objects"
add "@<target-uuid or dynamic-target>:<json-string>"
```

Example:

```
EnterpriseController/deploy > add
@<target-UUID>:"network={gateway='213.123.123.111', userFriendlyName='ip
address', ip='213.123.123.4'}"
```

### Testing a Deployment Plan

To test a deployment plan, use the `dryrun` command to create the tasks without committing the job, this ensures no errors with data.

To dry run a deployment plan:

- Enter `dryrun`.

```
EnterpriseController/deploy > dryrun
```

### Applying a Deployment Plan

To execute a deployment plan, set the attributes if required and then apply the plan. Some deployment plans need to have their attributes set before applying the plan.

To apply a deployment plan to an asset:

- Enter `apply`.

```
EnterpriseController/deploy > apply
```



# Part VI

---

## Engineered Systems

Part VI contains the following chapters:

- [Chapter 20, "Oracle Engineered Systems"](#)



---

---

## Oracle Engineered Systems

The following information is included in this section:

- [Introduction to Oracle Engineered Systems](#)
- [Oracle Exalogic Elastic Cloud](#)
- [SPARC SuperCluster T4-4](#)

### Introduction to Oracle Engineered Systems

Traditionally, IT departments have been required to install and configure software that is hosted on hardware that was itself installed and configured separately. Oracle Engineered Systems relieve this burden from the IT department by providing a pre-defined combination of hardware and software. Oracle Engineered System is a complete set of integrated hardware and software designed to reach a predetermined level of capability, capacity, and scale. This relatively new concept of an integrated hardware and software solution dedicated to provide a specific service, changes the way one must think about architecture in IT environments.

In addition to removing the burden of installation and configuration, Oracle Engineered Systems provide significant cost savings, this is one of the many advantages delivered by Oracle Engineered Systems. An even larger advantage is the optimization that pre-defined hardware and software enables. As the hardware and software are engineered together to form a complete system, there are multiple opportunities to improve the overall system performance. The unified and integrated monitoring and management of the Engineered System also provides cost savings through simplification of the overall environment. Thus, Oracle engineered systems allow datacenter services to be delivered more efficiently via modular, dedicated systems. This greatly simplifies the entire purchase, deploy, configure, monitor, and manage lifecycle of the provided services.

The whole impetus for cloud computing is to provide specific services (whether IaaS, PaaS, or SaaS) as efficiently as possible; therefore, the increased efficiency delivered by Oracle Engineered Systems make them ideal candidates for the building blocks of a cloud computing environment.

In addition to creating a cloud computing environment, these building blocks can be used to address a variety of enterprise architecture requirements to provide a path for enterprise maturation alongside the move to cloud adoption. Each building block can be selected as needed to meet specific maturation needs, and thus ultimately they provide an increase in overall architectural flexibility. For example, an architect may choose to integrate an Exadata Storage Server and SPARC SuperCluster or Oracle VM Blade Cluster early on to begin the process of consolidation into a scalable architecture, and then expand the system later to meet future demand. Shifting the overall

environment into a standardized architecture opens possibilities for future shift into cloud adoption and/or continuation down the traditional enterprise computing maturation continuum while providing for future scale.

The Oracle Exalogic Elastic Cloud and SPARC SuperCluster T4-4 Engineered Systems are described in detail in the following sections.

### **Oracle Exalogic Elastic Cloud**

The Oracle Exalogic Elastic Cloud comprises of a complete stack of hardware and software, computing, storage, and network, all engineered to work optimally together to provide a private cloud leveraging fusion middleware. Oracle Enterprise Manager Ops Center is a key part of the Exalogic appliance control system and serves as the operating system of the Exalogic platform.

### **SPARC SuperCluster T4-4**

The SPARC SuperCluster T4-4 comprises of a complete stack of hardware and software, computing, storage, and network, all engineered to work optimally together to provide a consolidated platform for running database, middleware, or third party applications. Oracle Enterprise Manager Ops Center is closely integrated with SPARC SuperCluster and provides hardware management, provisioning, and virtualization management.

## **Datacenter Management**

Using Oracle Enterprise Manager Ops Center, you can discover and manage Oracle Engineered Systems. You can view and access multiple Engineered Systems from a single datacenter through Oracle Enterprise Manager Ops Center. You can also view the Engineered System's assets, incidents reported from the Engineered Systems, and Service Requests from the same UI. You can generate reports for all datacenter assets, including Engineered Systems.

The discovery and management process is performed using one of the following methods:

- [Finding Assets](#)
- [Adding Assets Using a Discovery Profile](#)

### **Finding Assets**

You can find assets using their service tags. Service tags are small XML files containing product information. Many Oracle systems come equipped with service tags. If you have hardware assets equipped with service tags, you can discover them using the Find Assets wizard. This method lets you discover large numbers of assets quickly.

The Find Assets wizard searches IP ranges or networks for service tags, then uses credentials that you specify to discover and manage the discovered assets.

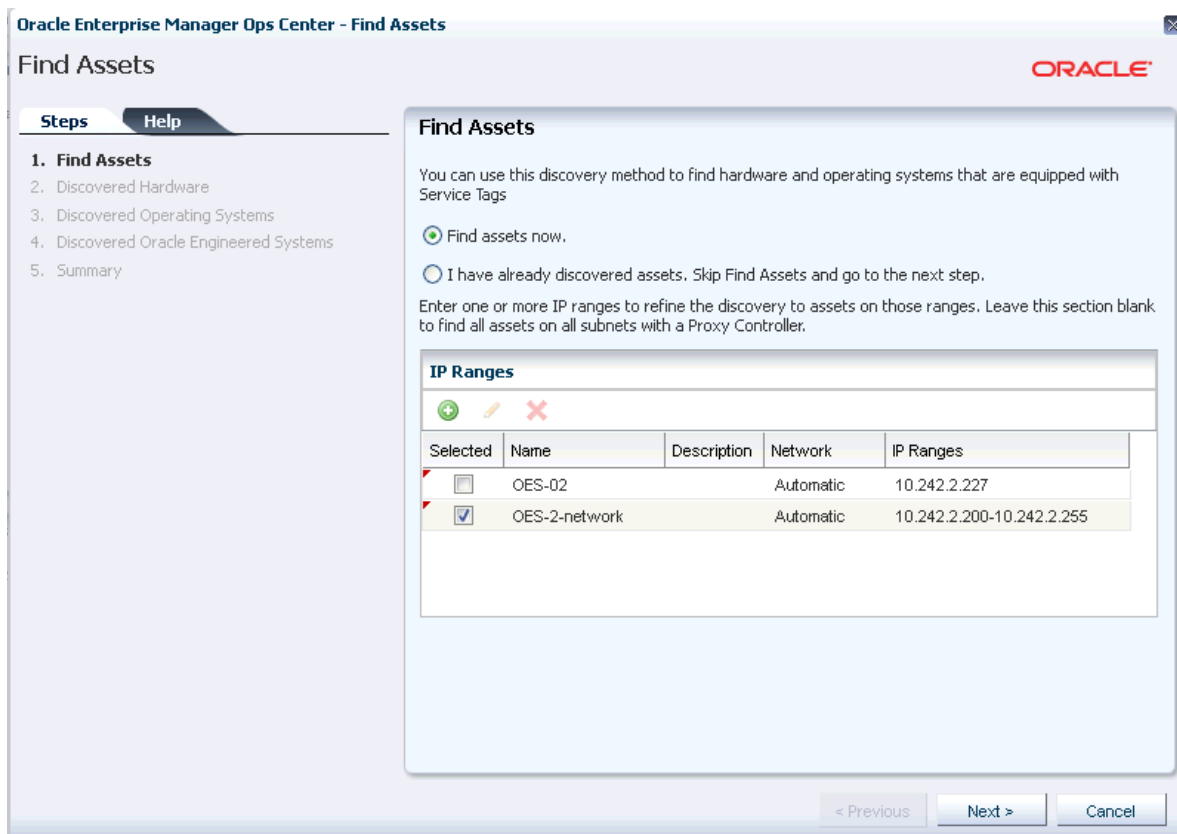
Products without service tags cannot be discovered using this method.

To find assets, perform the following steps:

1. On the Navigation pane, under Assets, select All Assets.
2. In the Actions pane, click Find Assets. The Find Assets wizard opens.



Figure 20–1 Find Assets



3. Select Find Assets Now and click Next.

When the initial discovery is complete, select the assets in each category (hardware, operating systems, and engineered systems) that you want to manage and provide necessary credentials.

---

**Note:** When adding a network range, enter the values without any space between the IP addresses. Use the format *start\_ip-end\_ip*.

---

4. Click Finish. The manage asset job is launched.

See [Discovering and Managing Assets](#) for more information.

### Creating a Discovery Profile

To discover an asset, a discovery profile has to be created. After it has been created, you run a discovery job using the profile.

To create a discovery profile, perform the following steps:

1. On the Navigation pane, select Plan Management.
2. Under Profiles and Policies, select Discovery.
3. In the Actions pane, click Create Profile.
4. Enter a name for the discovery profile and select the type as Oracle Engineered Systems. Click Next.

5. If the service tag parameters have been modified for the target assets, enter the Service Tag parameters:
  - Service tag passphrase - Necessary if a service tag has been configured to be encrypted.
  - Service tag port - Necessary if a service tag has been configured to use a port other than the default of 6481.
  - Service tag timeout - The default value is 20 seconds.
6. Enter the information for the target assets.
  - Hostnames or IPs - Enter a comma-separated list of hostnames or IP addresses. If you want to target an IP range, use the IP Ranges field instead.
  - Network - The managed network with which the hostnames or IP addresses are associated. This is used to route the discovery to the correct Proxy Controller. Select Automatic to route the job to the most appropriate Proxy Controller. The IP address of a target must resolve to only one known network for automatic routing to succeed.
  - IP ranges - Click the plus icon to add one or more IP ranges. Enter a name, optional description, network, and IP range for each. If you want to target specific hostnames or IP addresses, you must enter them when you run the discovery profile.
7. Enter credentials for each selected discovery profile.
8. View the summary and click Finish to create the discovery profile.

### Adding Assets Using a Discovery Profile

After you have created a discovery profile, you run a discovery job and manage Engineered System's assets. This lets you discover assets using a pre-existing set of protocols and credentials, and manage assets consistently.

To declare unconfigured assets for service processor configuration, perform the following steps:

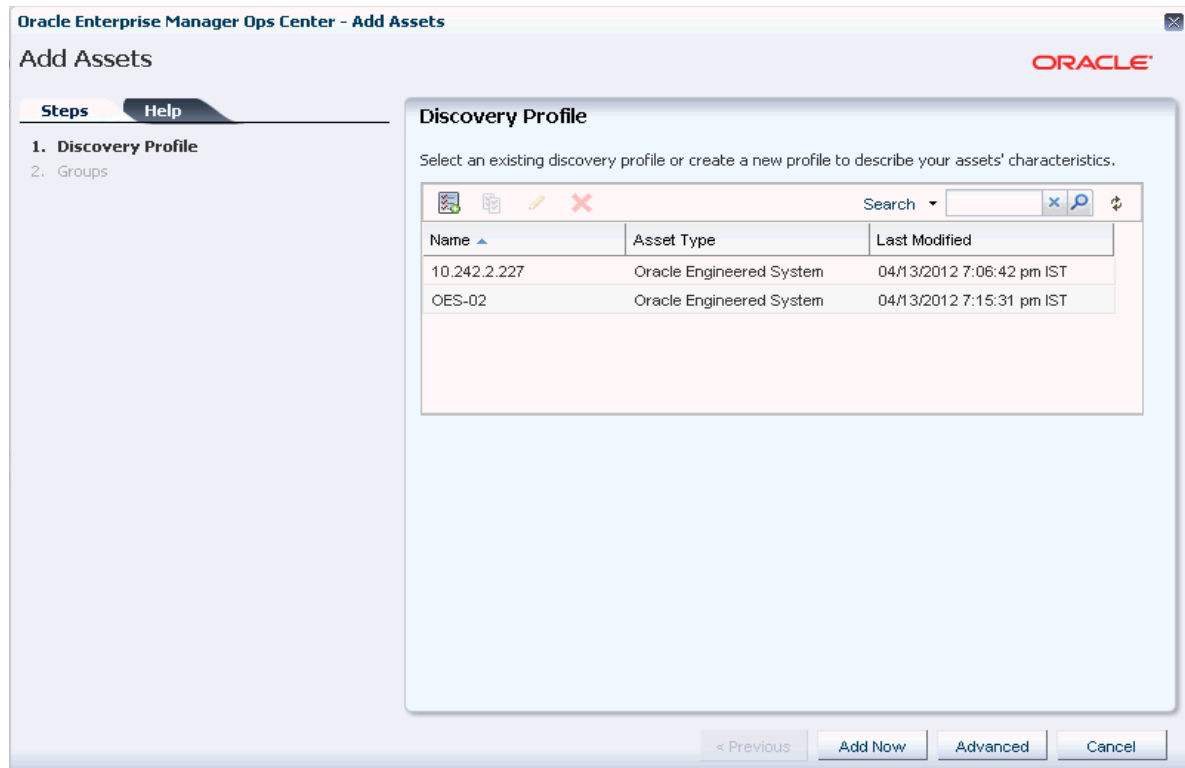
1. On the Navigation pane, under Assets, select All Assets.
2. In the Actions pane, click Add Assets. The Add Assets wizard opens.

**Figure 20–2 Add Assets**



3. Select the option, Add and manage various types of assets via discovery probes. The Discovery profile window opens.

**Figure 20–3 Select Discovery Profile**



4. Select a discovery profile.
5. Add or edit the IP addresses, hostnames, and credentials for the targets.
6. Click Add Now.

### Viewing the Asset Content Pane

You can view Engineered System's assets in the Datacenter Enterprise Controller BUI.

To view the Engineered System's assets in the Datacenter Enterprise Controller BUI, perform the following steps:

1. On the Navigation pane, under Assets, select Oracle Engineered Systems.
2. Select the Engineered System. The Dashboard, Details, Rack Info, Incidents, Service Request, and Monitoring tabs are displayed in the center pane.
  - Dashboard Tab – Displays the summary of the selected Engineered System, its membership graph, and the status of the system.
  - Details Tab – Displays the name of the selected Engineered System, description, master subnet manager address, number of racks, compute nodes, storage nodes, switches, and PDUs in the system.
  - Rack Info Tab – Displays a photorealistic view of the selected Engineered System.
  - Incidents Tab – Displays all incidents reported from the selected Engineered System.

- Service Request Tab – Displays the service request for the selected Engineered System.
- Monitoring Tab – Displays the alert monitoring rules and service dependencies of the selected Engineered System.

To perform active management actions on any asset of Engineered Systems, launch the web interface of the selected Engineered System by clicking Launch Web Interface on the Actions pane.

### Relayed Incidents

Relayed Incidents are datacenter incidents that are reported from Oracle Engineered Systems attached to Datacenter Enterprise Controller. You can only view and delete the relayed incidents. No actions can be performed on these incidents.

When you close the relayed incidents from the Datacenter Enterprise Controller, the incident is closed in the respective Engineered System as well.

To view all datacenter incidents, do the following:

- On the Navigation pane, under Message Center, select Relayed Incidents.  
All the relayed incidents are displayed.

See [Incidents](#) for more information.

### Relayed Service Requests

You can view the relayed service requests related to the Oracle Engineered Systems. You can also file service requests.

To view the relayed service requests, do the following:

- On the Navigation pane, under Message Center, select Relayed Service Requests.  
All the relayed service requests are displayed. Details such as summary of the request, SR number, serial number, severity, status, contact person, and last updated date are displayed.

See [Oracle Services and Service Requests](#) for more information.

## Baseline Check

Baseline Check is a feature in Oracle Enterprise Manager Ops Center Engineered Systems in which the factory default configuration of eighth, quarter, half, and full rack configurations are considered as a normal or baseline setup. When the assets are discovered and associated with the rack, this setup is compared with the default factory configuration. For any discrepancy, the baseline check reports a question mark at the slot in the rack where the local configuration differs from the factory default configuration.

Hover the cursor over the question mark to view details of the warning, for example, missing asset, asset mismatch, or unknown asset. Based on the warning, you can decide to adjust the assets.

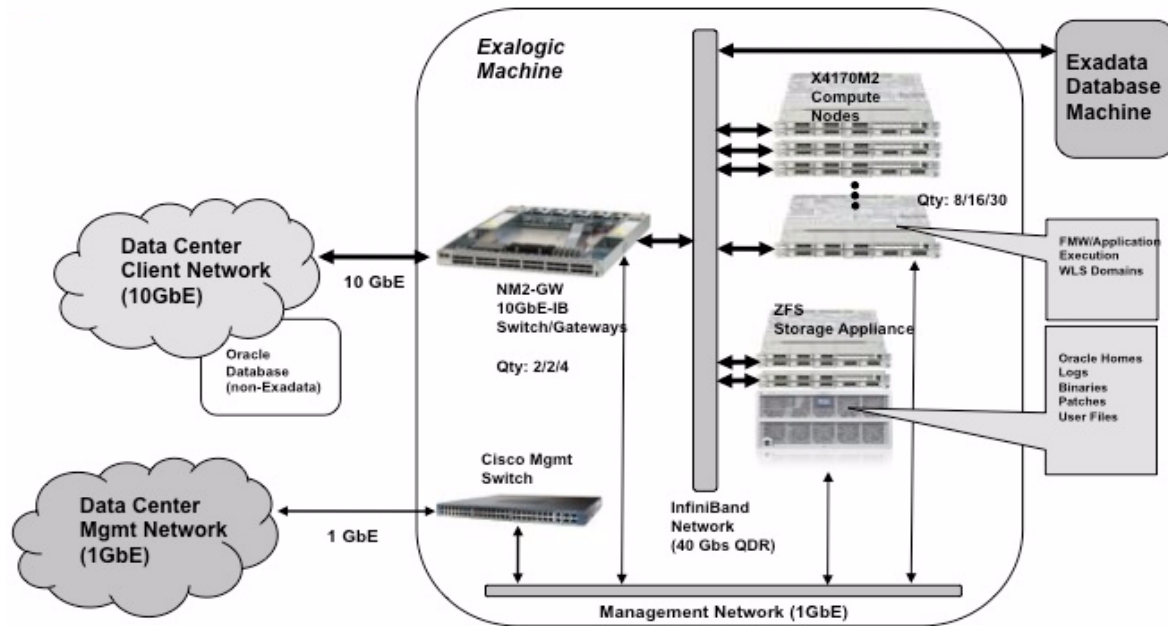
## Oracle Exalogic Elastic Cloud

The Oracle Exalogic Elastic Cloud Engineered System delivers a standalone Oracle Enterprise Manager Ops Center that is preinstalled on a factory packaged Exalogic system. The embedded Oracle Enterprise Manager Ops Center is an integral part of Exalogic Control software and offers full set of Oracle Enterprise Manager Ops Center

built-in functionality to provide Exalogic platform administration operations. It also provides features to view the Exalogic machine as an appliance, monitor and manage the Exalogic hardware, and cover the replacement part of the fault management lifecycle.

Figure 20–4 is a pictorial representation of the Exalogic System.

Figure 20–4 Exalogic System Overview



Note: Quantities are specified as Quarter/Half/Full rack configurations.

## Oracle Enterprise Manager Ops Center Configuration

The Exalogic Control software components are deployed in HA configuration to ensure that the platform management system is reliable and available.

To conserve the limited Exalogic resources and simplify the deployment model, Exalogic Control deploys a single database in HA configuration that is shared among other Exalogic Control software components such as Oracle Enterprise Manager Ops Center, Oracle VM Manager, and LDAP.

## Understanding User Roles

In Oracle Enterprise Manager Ops Center, users can be assigned several roles such as Asset Admin, Cloud Admin, Exalogic System Admin, and many more. Each role grants the user a set of permissions. A particular permission can be granted by more than one role such as Asset Management, Network Management, and so on.

You can add users to Oracle Enterprise Manager Ops Center from the local authentication subsystem of the Enterprise Controller's operating system. Each user can be given a different role which grants or denies access to the different functions of Oracle Enterprise Manager Ops Center. You can view the existing users from the Users tab of the Administration section.

### **Exalogic System Admin Role**

The Exalogic System Administrator is responsible for overall monitoring and management of the engineered system, including hardware subsystems, network management, and user management. The Exalogic System Administrator also has privileges to manage Oracle VM Servers.

The Exalogic System Admin role is a default role for the management of the Exalogic appliance and tasks related to the above functionality. As an Exalogic System Admin, you can perform most of the operations that are allowed in the context of the Exalogic system, except tasks related to cloud management.

For tasks related to cloud management, the Cloud Admin and Cloud User roles are available.

Prerequisites: The user must be familiar with the use of Oracle Enterprise Manager Ops Center and be familiar with hardware management and OS management.

### **Cloud Administrator**

The Cloud Administrator's responsibilities include setting up of infrastructure and resource allocation so that cloud users can deploy their application onto authorized accounts. They also manage the cloud users accessing the accounts and their authorization.

Prerequisites: The user must be trained on Oracle Enterprise Manager Ops Center, installation and configuration, and the continual maintenance of the product.

### **Cloud User**

Cloud users create virtual servers and deploy applications. Cloud users are restricted to virtual datacenter infrastructure activities and are presented only with the required options on the Oracle Enterprise Manager Ops Center UI.

Prerequisites: The user must be familiar with the use of Oracle Enterprise Manager Ops Center and be familiar with hardware management and OS management in general.

## **Adding a User**

Users with the User Admin role can add other users. New user information, such as passwords for new users are retrieved 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.

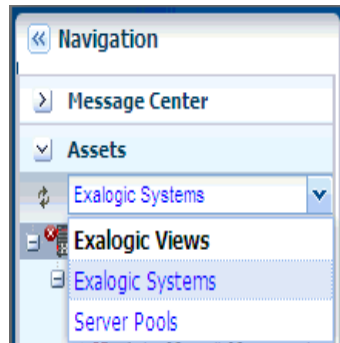
## **Navigation**

This section briefly describes the steps to navigate to Exalogic Systems from the Oracle Enterprise Manager Ops Center UI.

1. Log in to Oracle Enterprise Manager Ops Center using the Exalogic Admin Role.

2. On the Navigation pane, under Assets, select Exalogic Systems from the drop-down list.

**Figure 20–5** Navigation pane



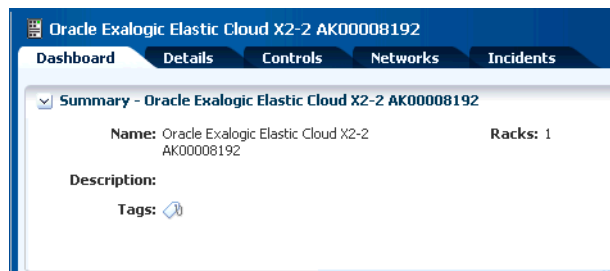
## Viewing the Exalogic System

Viewing the Exalogic system basically means how you view the virtual Exalogic system using the four tabs on the Center pane, namely Dashboard, Details, Controls, and Networks. You can also perform relative actions by clicking the respective actions on the Actions pane. The actions that are allowed to be performed from the Actions pane are context sensitive to the selected assets on the Navigation pane. The actions are also role based, not all users will be able to perform all actions. For more information on Roles, see [Understanding User Roles](#).

To view the Exalogic system, perform the following steps:

1. On the Navigation pane, under Assets, select Exalogic Systems from the drop-down list.
2. Select the Exalogic system that you want to view.
  - The Dashboard, Details, Controls, Networks, and Incidents tabs are displayed in the Center pane.

**Figure 20–6** Center Pane With Dashboard Tab Selected



3. Click on the respective tab on the Center pane to view more details.
  - **Dashboard Tab** displays the summary of the Exalogic system, its membership graph, and the status of the system.
  - **Details Tab** displays the name of the Exalogic system, description, master subnet manager address, number of racks, compute nodes, storage nodes, switches, and PDUs present in the system.

- **Controls Tab** displays the Exalogic Control Software details such as name of the software, version number, description, name of the virtual machine, and server name.
- **Networks Tab** displays the infrastructure network table and network connectivity table.
- **Incidents Tab** displays all the incidents and alerts reported in the Exalogic System.

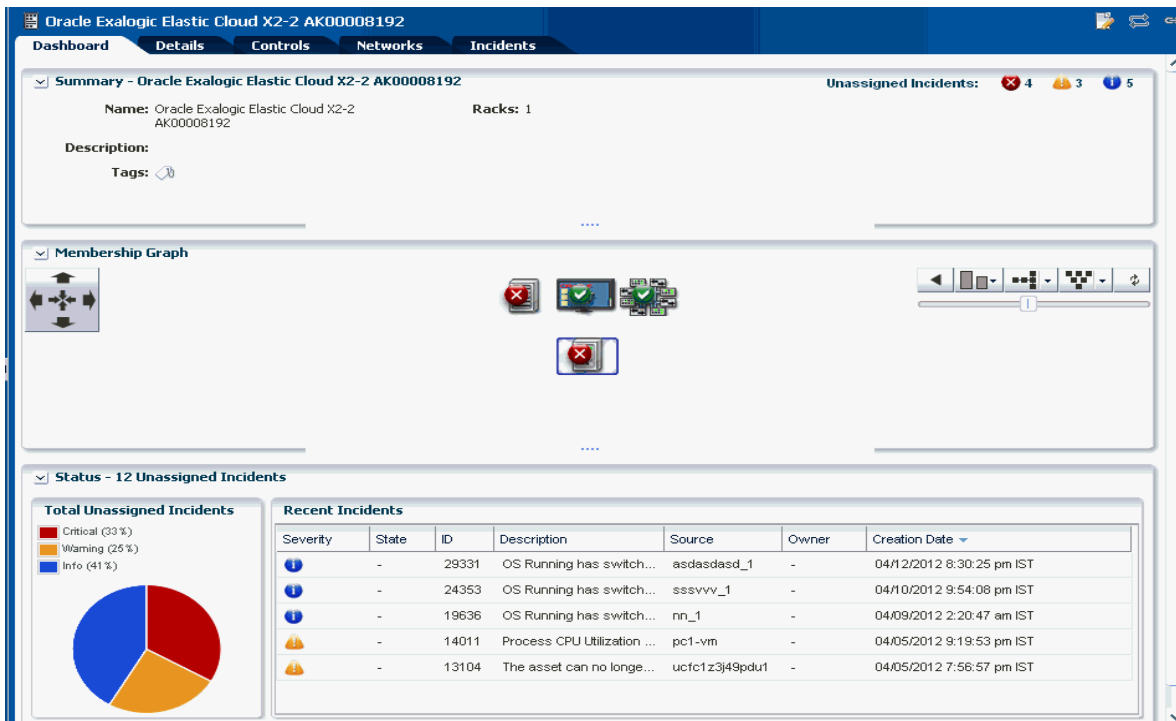
**Dashboard Tab**

The dashboard has three sections - Summary, Membership Graph, and Status.

In the Dashboard Tab, the following panes are displayed:

- **Summary Pane**
- **Membership Graph Pane**
- **Status Pane**

**Figure 20–7 Dashboard Tab**



\*\*\*\*\*

**Summary Pane** The Summary section displays the name of the Exalogic system, description or name of the system identifier, number of racks that are part of the system, and also the number of unassigned incidents. The Unassigned Incidents icon in the summary pane includes incidents resulting from hardware faults. The three icons depict Critical Incidents, Warnings, and Information Incidents respectively. These incidents are from the assets that belong to all Exalogic racks.



**Membership Graph Pane** The Membership Graph pane displays the Exalogic system as a hierarchy of its components. It shows the relationship between the Oracle VM Manager, physical InfiniBand fabric, and the hardware that is grouped in the rack. You can navigate to any asset by double-clicking on the asset in the membership graph.

Using the controls on the top right of the graphic pane, you can change the view of the graph to either a horizontal or a vertical orientation. You can also refresh the view by clicking the Refresh icon. You can also change the graph depths or size of the images.

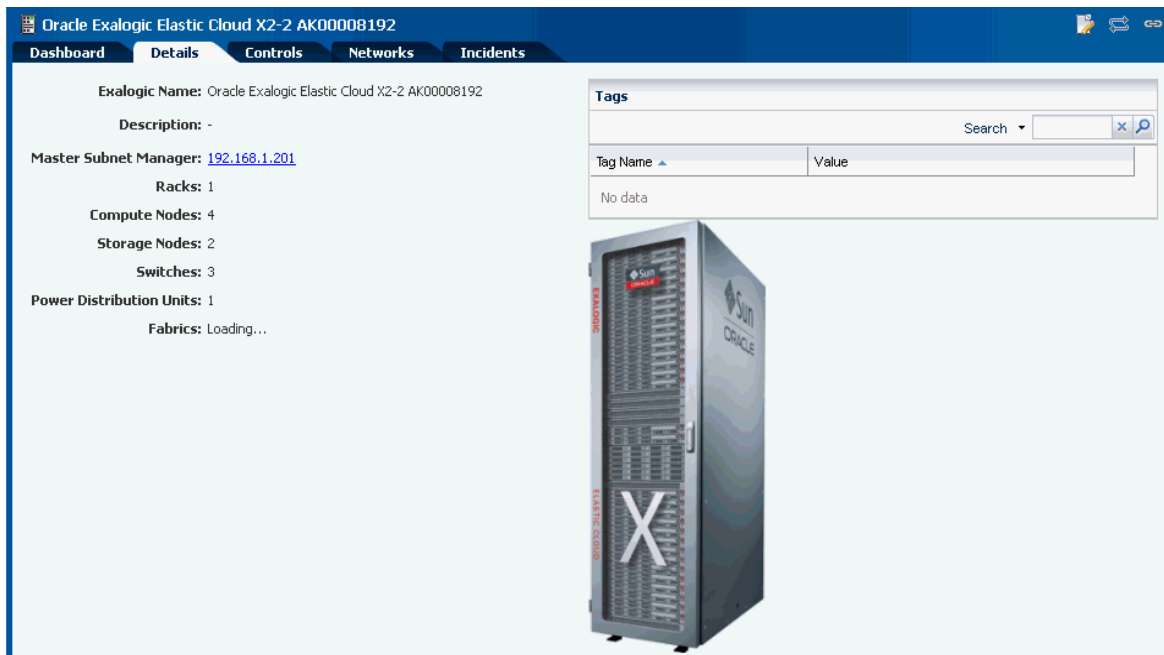
**Status Pane** The Status Pane displays the total unassigned incidents in chart format as well as the recent incidents encountered by the Exalogic system. In the Recent Incidents section, the following details are displayed:

- Severity – Displays the severity of the incident.
- State – Displays the state of the incident.
- ID – Displays the incident ID.
- Description – Displays the incident description.
- Source – Displays the source of the incident.
- Owner – Displays the name of the owner who reported the incident.
- Creation Date – Displays the date on which the incident was created.

### Details Tab

In the Details Tab, the following details are displayed:

**Figure 20–8 Details Tab**



- Exalogic Name
- Description
- Model
- Number of Racks

- Number of Compute Node
- Number of Storage Nodes
- Number of Switches

In the Tags pane, the tag names and their respective values are displayed. You can search for a particular tag using the Search feature.

### Controls Tab

The Controls tab displays the Exalogic Control Software details including the database, Oracle VM Manager, Proxy Controllers, and Enterprise Controller. The table displays the name of the control component, version number of the control component, description, virtual machine name, and server name.

**Figure 20–9 Controls Tab**

Software Name	Version	Description	Virtual Machine Name	Server Name
No data				

You can select a control component from the table and double-click it to view the Dashboard of the respective control component. The values in the table give an idea as to where the Exalogic control stack runs so that the user can quickly navigate to that compute node just by clicking on it.

Use the Refresh icon on the Exalogic Control Software pane to refresh the list as and when needed.

### Networks Tab

The Networks Tab displays the Infrastructure Networks table and Network Connectivity table.

Figure 20–10 Networks Tab

The screenshot shows the Oracle Exalogic Elastic Cloud interface with the 'Networks' tab selected. It displays two main sections: 'Infrastructure Networks' and 'Network Connectivity'.

**Infrastructure Networks Table:**

Network Name	Network CIDR	Partition Key	IP Range	Roles
EoIB-external-mgmt	10.242.0.0/21	32773	-	-
IPoIB-admin	192.168.20.0/24	32769	-	-
IPoIB-ovm-mgmt	192.168.23.0/24	32772	-	-
IPoIB-storage	192.168.21.0/24	32770	-	-
IPoIB-virt-admin	172.16.0.0/16	32771	-	-
el01-eth-admin	192.168.1.0/24	-	-	-

**Network Connectivity Table:**

Network Name	Asset Type	IPoIB-virt-admin	IPoIB-admin	IPoIB-ovm-mgmt	IPoIB-storage	EoIB-external-mgmt	el01-eth-admin
<b>Rack: Rack: Oracle Exalogic X2-2 AK00008192 (10)</b>							
192.168.1.115		-	192.168....	-	192.168.21.9	-	192.168.1.15,192.168...
192.168.1.116		-	192.168....	-	192.168.21.9	-	192.168.1.15,192.168...
192.168.1.200		-	-	-	-	-	192.168.1.200
192.168.1.201		-	-	-	-	-	192.168.1.201
192.168.1.202		-	-	-	-	-	192.168.1.202
el01 cn05.localdomain		172.16....	192.168....	192.168.23....	192.168.21.45	-	192.168.1.5
el01 cn06.localdomain		172.16....	192.168....	192.168.23.46	192.168.21.46	-	192.168.1.106,192.16...
el01 cn07.localdomain		172.16....	192.168....	192.168.23....	192.168.21.47	-	192.168.1.7,192.168....
el01 cn08.localdomain		172.16....	192.168....	192.168.23.48	192.168.21.48	-	192.168.1.8,192.168....
ucfc1z3j49pdu1		-	-	-	-	-	192.168.1.210

### Infrastructure Networks Table

The Infrastructure Networks table displays the infrastructure networks that are used inside the Exalogic system for communication between the Exalogic control components and cloud virtual machines.

- Network Name - displays the name of the managed network.
- Network CIDR - displays the type of the asset.
- Partition Key - displays the partition of the port.
- IP Range - specifies the minimum and maximum boundaries of the IP addresses assigned to the network.
- Roles - displays the role.

### Network Connectivity Table

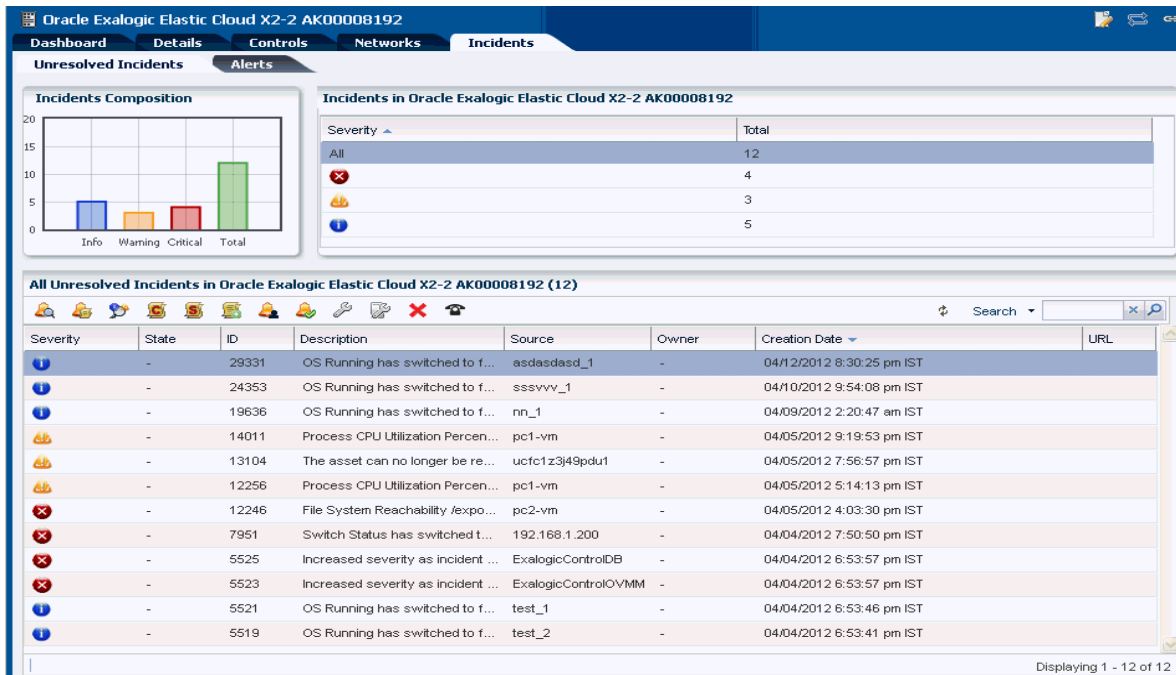
The Network Connectivity Table displays the infrastructure networks with IPs assigned to the individual hardware components of Exalogic system.

- Network Name
- Asset Type

### Incidents Tab

The Incidents Tab displays all the unassigned incidents and alerts reported in the Exalogic system.

Figure 20–11 Incidents Tab



### Permitted Actions in the Exalogic System View

The following are the permitted actions that can be performed in the Exalogic system view. Refer to *Oracle Enterprise Manager Ops Center Feature Reference Guide* for steps on how to perform these actions.

- Create Rack
- Edit Tags
- Add Assets
- Find Assets

### Viewing the Exalogic System Rack

This section describes how to view the Exalogic System rack, visualization of the rack physical layout, aggregated rack components, energy data, and other rack details. As an administrator, you can drill down to an asset contained in the rack (server, storage node, switch, PDU) or even further.

To view the Exalogic system rack, perform the following steps:

1. On the Navigation pane, under Assets, select Exalogic Systems.
2. Select a rack that you want to view.

The Dashboard, Details, Firmware, Incidents, Charts, Energy, and Jobs tabs are displayed in the center pane.

Figure 20–12 Tabs of the Exalogic System Rack



- Dashboard Tab – Displays the summary, membership graph, and status of the rack.
  - Details Tab – Displays the rack info with a photorealistic view of the rack.
  - Firmware Tab – Displays the name, description, and version of the firmware for each component and the slot for each component
  - Incidents Tab – Displays all unresolved incidents in the rack.
  - Charts Tab – Provides more ways to display the power utilization data. You can change the graphed data to a bar chart or an area chart. You can also export the data for either the current view or all available data to a file in either CSV or XML format.
  - Energy Tab – Reports power consumption as the current value and for a period of time, as well as attributes of the fan and power supplies.
  - Jobs Tab – Displays the current and historical jobs.
3. Select any of the tabs to view more details.

Refer To [Hardware Monitoring](#) section in the *Hardware Management Guide* for information on the Tabs and Views of the rack.

### Photorealistic View of the Rack

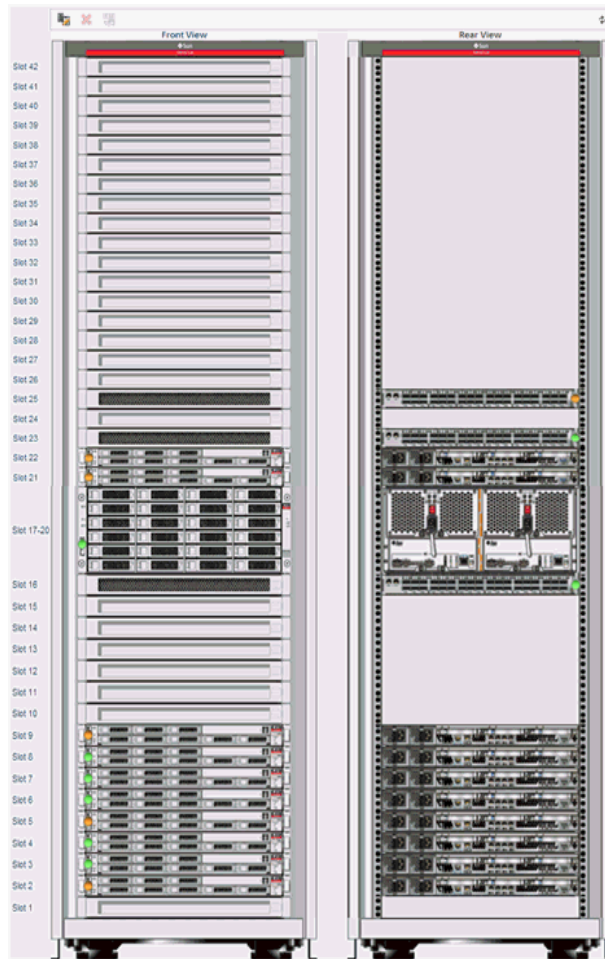
This view is a representation of the physical rack so that you can see the placement of the rack and its components.. The front and rear views of the rack are displayed in this view. All slots and the respective assets are displayed. Positions within the rack are displayed in a 3-dimensional view.

Each asset in the rack is represented by an image. The health status of assets such as OK, Warning, or Critical is displayed in the form of colored lights as seen on the physical rack itself. OK status is identified by the green color. Warning and critical status are identified by the yellow color. Hover the mouse over the slots in the rack and view details about the assets such as slot number, asset name and description, type of asset, model number of the asset, and its health status.

A question mark in any of the slots indicates a discrepancy from the baseline check. See [Baseline Check](#) for more information.

To see the photorealistic view of the rack, perform the following steps:

1. On the Navigation pane, under Assets, select Exalogic Systems.
2. Select a rack that you want to view.
3. In the Center pane, click the Details tab.
  - A photorealistic view of the rack is displayed.

**Figure 20–13 Photorealistic View of the Rack**

### Permitted Actions in Rack View

The following are the permitted actions that can be performed in the Exalogic system Rack view. Refer to *Oracle Enterprise Manager Ops Center Feature Reference Guide* for steps on how to perform these actions.

- Create Rack
- Delete Rack
- Power Off
- Reset
- Place/Remove Asset(s) in Rack
- Place/Remove PDU(s) in Rack
- Edit Tags
- Add Asset to Group
- Add Assets
- Find Assets

## Creating and Viewing Reports

In general, using reports, you can view the configuration for each rack, including the asset details related to the firmware. Reports provide information about your assets, such as job history, firmware, OS updates, and problems. Reports are created in PDF and CSV formats. Reports can be exported or used to launch jobs on targeted assets.

To create a Report, see [How to Create an Exalogic Report](#) in the [How To library](#).

### Viewing the Exalogic System Report

You can either view existing reports that have been created or you can create a new report for yourself and view it.

In this section, the Exalogic System Report is described in detail. The following sections of the report are described below:

- [Report Parameters](#)
- [Summary Table](#)
- [System Control Software Table](#)
- [Compute Nodes Table](#)
- [Switches Table](#)
- [Storage Appliances Table](#)
- [Power Distribution Units Table](#)
- [Validation Table](#)

### Report Parameters

Report Parameters displays the name and model of the Exalogic system. It also displays the number of assets in the rack by their types, such as compute nodes, switches, and storage nodes in the system.

**Figure 20–14** *Report Parameters*

Report Name: SIR01-All  
 Description: All Assets  
 Run Date: Mon Apr 09 18:49:07 EDT 2012  
 Report Type: Exalogic System Report

#### Report Parameters

Exalogic Name	Oracle Exalogic Elastic Cloud X2-2 AK00008192
Model	2.0.1.0.0
Racks	1
Compute Nodes	4
Switches	3
Storage Nodes	2

### Summary Table

The Summary Table is a table of contents of all tables in the report. It displays the number of records for each table.

**Figure 20–15 Summary Table**

Name of Detailed Table	Records
Virtual Datacenter Status Report	4
Rack Oracle Exalogic X2-2 AK00008192 - Compute Nodes	4
Rack Oracle Exalogic X2-2 AK00008192 - Switches	3
Rack Oracle Exalogic X2-2 AK00008192 - Storage Appliances	2
Rack Oracle Exalogic X2-2 AK00008192 - Power Distribution Units	1
Rack Oracle Exalogic X2-2 AK00008192 - Validation Table	12

**System Control Software Table**

The System Control Software Table lists the name of the software (control components – Proxy Controller, Enterprise Controller, LDAP, Oracle VM Manager, and database), version, description, server name, and virtual machine name. These are the same attributes as seen on the UI of control components.

**Compute Nodes Table**

The Compute Nodes Table displays the setup of the racks such as the type of asset, name of the asset (compute node), firmware version (such as BIOS, service processor, and HCA adaptor), Oracle VM Server version, and the location of the asset in the rack with the slot number where it is placed.

**Switches Table**

The Switches Table displays the name of the switch node, type of switch, firmware version, and location of the switch in the rack with the slot number where it is placed.

**Storage Appliances Table**

The Storage Appliances Table displays the name of the compute node, version of the service processor firmware, and the location of the appliance with the slot number where it is placed in the rack.

**Power Distribution Units Table**

The Power Distribution Units Table displays the PDUs and their firmware version.

**Validation Table**

The Validation Table displays the validity result of the rack. A baseline check is performed against the known schema for the rack. See [Baseline Check](#) for more information. The Expected Component column in the table displays the expected component if the placed component in the slot does not match the schema when the baseline check is performed.



**Figure 20–16 Validation Table****Rack: Oracle Exalogic X2-2 AK00008192 - Validation Table**

Location	Type	Name	Validation Result	Expected Component
Slot 25	Switch	192.168.1.200	OK	
Slot 23	Switch	192.168.1.202	OK	
Slot 22	Storage	192.168.1.116	OK	
Slot 21	Storage	192.168.1.115	OK	
Slot 17	DiskShelf	192.168.1.15	OK	
Slot 16	Switch	192.168.1.201	OK	
Slot 5	Server	e101cn08.localdomain	OK	
Slot 4	Server	e101cn07.localdomain	OK	
Slot 3	Server	e101cn06.localdomain	OK	
Slot 2	Server	e101cn05.localdomain	OK	
-	PDU	ucfc1z3i49pdu1	OK	
-	-	-	MISSING	PDU, Oracle Rack Power Distribution Unit

## SPARC SuperCluster T4-4

SPARC SuperCluster is an Oracle Engineered System which integrates SPARC compute nodes, a Sun ZFS Storage Appliance, InfiniBand switches, PDUs, and Exadata Storage Servers into a multi-rack system.

The SPARC SuperCluster hardware comprises of two or four SPARC T4-4 servers, three Sun Datacenter InfiniBand Switch 36 switches as InfiniBand backplane, a Cisco 4948 48-port 1Gb Ethernet Switch for external connectivity, and a Sun Rack II.

SPARC SuperCluster is available in two configurations, half rack and full rack. The half rack includes three Exadata Storage Servers and the full rack includes six Exadata Storage Servers. In addition, for additional storage capacity, connecting to an Oracle Exadata Storage Expansion Rack is supported.

## SPARC SuperCluster Configuration

The SPARC SuperCluster uses logical domains (LDMs) so that you can create specialized virtual systems within a single hardware platform. The logical domains have direct access to storage and network resources..

LDM configurations supported on SPARC SuperCluster have the following types:

- 11gR2 Database (DB) Domains
- Oracle Solaris 10 General Purpose Domains
- Oracle Solaris 11 General Purpose Domains

There are nine basic configuration options to choose from for the SPARC SuperCluster (Configurations A - I), with each configuration option containing one or more of the LDM configurations listed above. Each configuration is based on a mirrored two-server model, so any one of the nine basic configuration options can be used in a SPARC SuperCluster Half Rack, with some restrictions. For a SPARC SuperCluster Full Rack, you can use different combinations of these nine basic configuration options, with some restrictions.

---

---

**Note:** In this document, it is assumed that the SPARC SuperCluster system is configured and discovered in Oracle Enterprise Manager Ops Center.

---

---

## Understanding User Roles

In Oracle Enterprise Manager Ops Center, users can be assigned several roles such as Asset Admin, Cloud Admin, SuperCluster System Admin, and many more. Each of such role grants the user a set of permissions; a particular permission can be granted by more than one role such as Asset Management, Network Management, and so on.

You can add users to Oracle Enterprise Manager Ops Center from the local authentication subsystem of the Enterprise Controller's operating system. Each user can be given a different role which grants or denies access to the different functions of Oracle Enterprise Manager Ops Center. You can view the existing Users from the Users tab of the Administration section.

### SuperCluster System Admin Role

The SuperCluster System Administrator is responsible for overall monitoring and management of the SPARC SuperCluster system. The SuperCluster System Administrator also has privileges to manage the Oracle Solaris Cluster, Virtual Pools, and Storages. As a SuperCluster System Administrator, you can perform most of the operations which are allowed in the context of the SPARC SuperCluster appliance system.

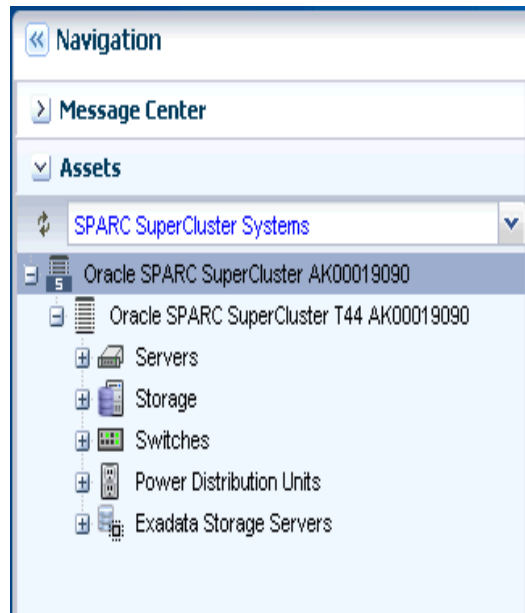
The SuperCluster System Administrator role is a default role highly recommended for the management of the SPARC SuperCluster appliance and tasks related to the above functionality.

**Prerequisites:** The user must be familiar with the use of Oracle Enterprise Manager Ops Center and be familiar with hardware management and OS management in general.

## Navigation

This section briefly describes the steps to navigate to SPARC SuperCluster from the Oracle Enterprise Manager Ops Center UI.

1. Login to Oracle Enterprise Manager Ops Center using the SuperCluster System Admin role.
2. On the Navigation pane, under Assets, select SuperCluster Systems from the drop-down list.

**Figure 20–17 Navigation**

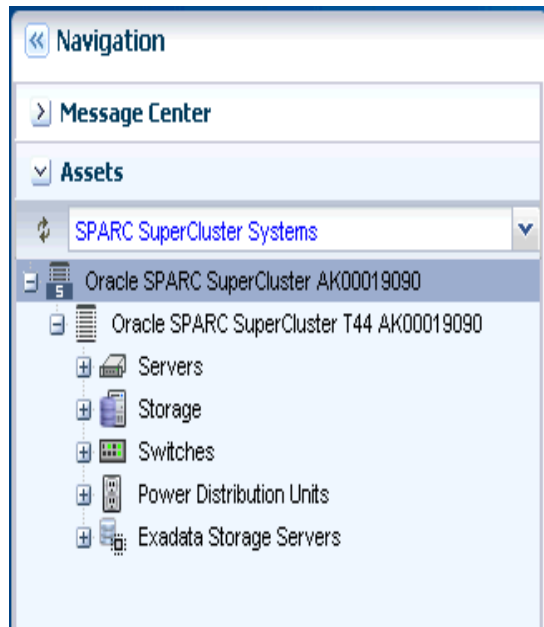
3. Select the Oracle SPARC SuperCluster system.

## Viewing the SPARC SuperCluster System

Viewing the SPARC SuperCluster system means how you view the virtual SPARC SuperCluster system using the tabs on the center pane, namely Dashboard, Details, Networks, and Incidents. You can also perform actions by clicking the respective actions on the Actions pane. The actions available on the Actions pane depend on the selected asset on the Navigation pane. The actions are also role based, not all users will be able to perform all actions. For more information on Roles, see [Understanding User Roles](#).

To view the SPARC SuperCluster system, perform the following steps:

1. On the Navigation pane, under Assets, select SuperCluster Systems from the drop-down list.

**Figure 20–18** Navigation pane

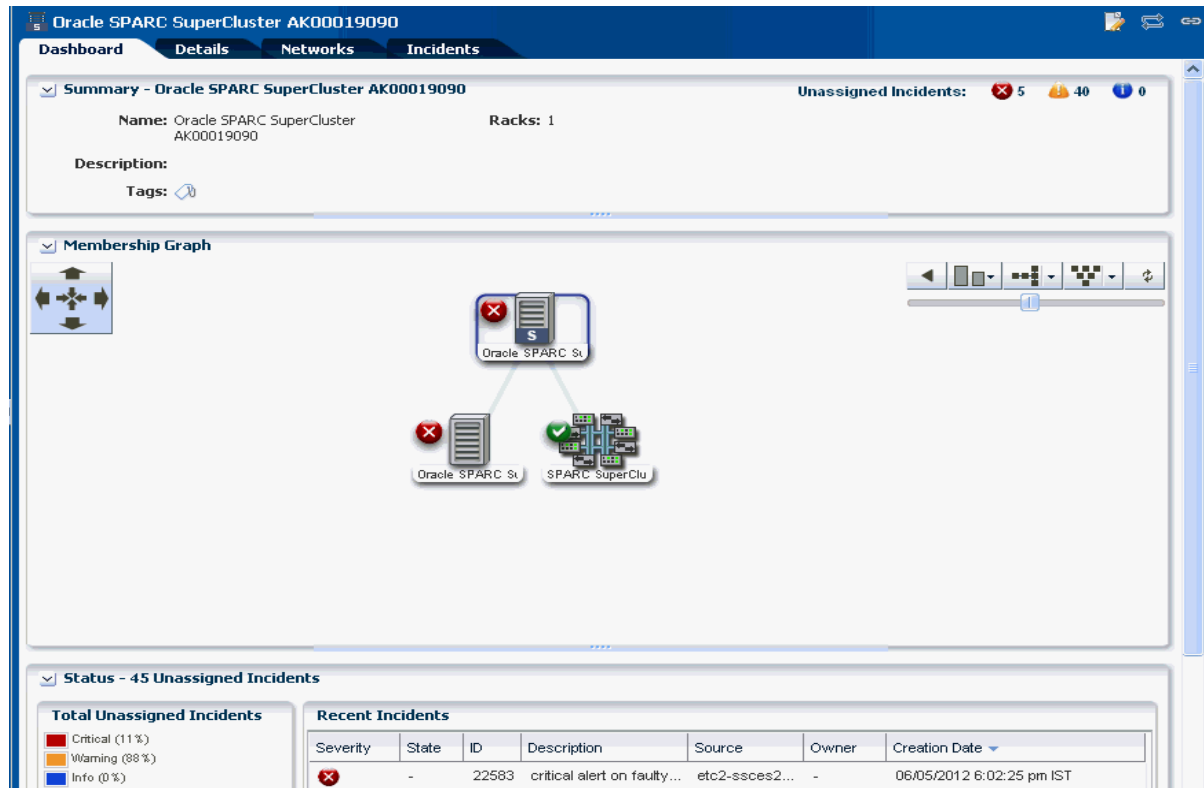
2. Select the Oracle SPARC SuperCluster system that you want to view.
  - The Dashboard, Details, Controls, Networks, and Incidents tabs are displayed in the center pane.
3. Click on a tab to view more details.
  - **Dashboard Tab** displays the summary of the SPARC SuperCluster system, membership graph, and the status of the system.
  - **Details Tab** displays the name of the SPARC SuperCluster system, description, master subnet manager address, number of racks, compute nodes, storage nodes, Exadata Storage Servers, switches, and PDUs in the rack.
  - **Networks Tab** displays the Infrastructure Network Table and Network Connectivity Table.
  - **Incidents Tab** displays all the incidents and alerts reported in the SPARC SuperCluster System.

### Dashboard Tab

The dashboard comprises of three sections - Summary, Membership Graph, and Status.

- **Summary Pane**
- **Membership Graph Pane**
- **Status Pane**

Figure 20–19 Dashboard Tab



**Summary Pane** The Summary section displays the name of the SPARC SuperCluster system, description or the name of the system identifier, number of racks that are part of the system, and the number of unassigned incidents. The Unassigned Incidents icon in the summary pane includes incidents resulting from hardware faults. The three icons depict Critical Incidents, Warnings, and Information Incidents respectively. These incidents are from the assets that belong to all SPARC SuperCluster systems.

### Membership Graph Pane

The Membership Graph pane displays the SPARC SuperCluster system as a hierarchy of its components. It shows the relationship between the SPARC SuperCluster system and fabrics that are grouped in the rack. You can instantly navigate to any asset by double-clicking on the asset in the membership graph.

Using the controls on the top right of the graphic pane, you can change the view of the graph to either a horizontal or a vertical orientation. You can also refresh the view by clicking the Refresh icon. You can also change the graph depths or size of the images.

### Status Pane

The Status Pane displays the total unassigned incidents in chart format as well as the recent incidents encountered by the SPARC SuperCluster system. In the Recent Incidents section, the following details are displayed:

- Severity - displays the severity of the incident.
- State - Displays the state of the incident.
- ID - Displays the incident ID.
- Description - Displays the incident description.

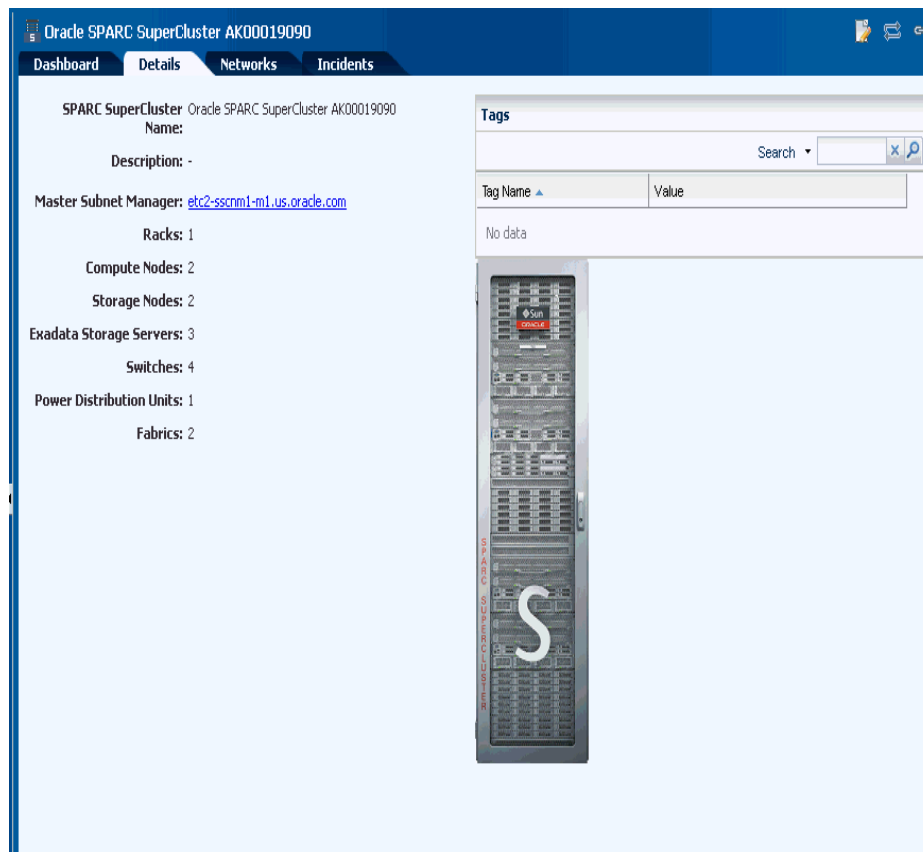
- Source – Displays the source of the incident.
- Owner – Displays the name of the owner who reported the incident.
- Creation Date – Displays the date on which the incident was created.

### Details Tab

In the Details Tab, the following details are displayed:

- SPARC SuperCluster System Name
- Description
- Master Subnet Manager
- Number of Racks
- Number of Compute Nodes
- Number of Storage Nodes
- Number of Exadata Storage Servers
- Number of Switches
- Number of PDUs

**Figure 20–20 Details Tab**



In the Tags pane, the tag names and their values are displayed. You can search for a particular tag using the Search feature.

## Networks Tab

The Networks Tab displays the Infrastructure Networks Table and Network Connectivity Table.

**Figure 20–21 Networks Tab**

The screenshot shows the Oracle SPARC SuperCluster AK00019090 interface. The 'Networks' tab is active, displaying two tables:

- Infrastructure Networks Table:** This table is currently empty, showing 'No data'. It has columns for Network Name, Network CIDR, Partition Key, IP Range, and Roles.
- Network Connectivity Table:** This table displays network assets for a rack. The header includes 'Network Name' and 'Asset Type'. The data rows are as follows:
 

Network Name	Asset Type
<b>Rack: Rack: Oracle SPARC SuperCluster T44 AK00019090 (12)</b>	
(S-002128469411a0a0)[S-002128469411a0a0]	[Icon]
(S-0021284698baa0a0)[S-0021284698baa0a0]	[Icon]
10.129.201.118	[Icon]
etc2-ssc4948-m1.us.oracle.com	[Icon]
etc2-ssccn1-10g1	[Icon]
etc2-ssccn2-10g1	[Icon]
etc2-ssces1-m1.us.oracle.com	[Icon]
etc2-ssces2-m1.us.oracle.com	[Icon]
etc2-ssces3-m1.us.oracle.com	[Icon]
etc2-sscnm1-m1.us.oracle.com	[Icon]
etc2-sscsn1-sp.us.oracle.com	[Icon]
etc2-sscsn2-sp.us.oracle.com	[Icon]

### Infrastructure Networks Table

The Infrastructure Networks Table displays the infrastructure networks that are defined and used inside the SPARC SuperCluster system for communication between the SPARC SuperCluster control components.

- Network Name - displays the name of the managed network.
- Network CIDR - displays the type of the asset.
- Partition Key - displays the partition of the port.
- IP Range - specifies the minimum and maximum boundaries of the IP addresses assigned to the network.
- Roles - displays the role.

### Network Connectivity Table

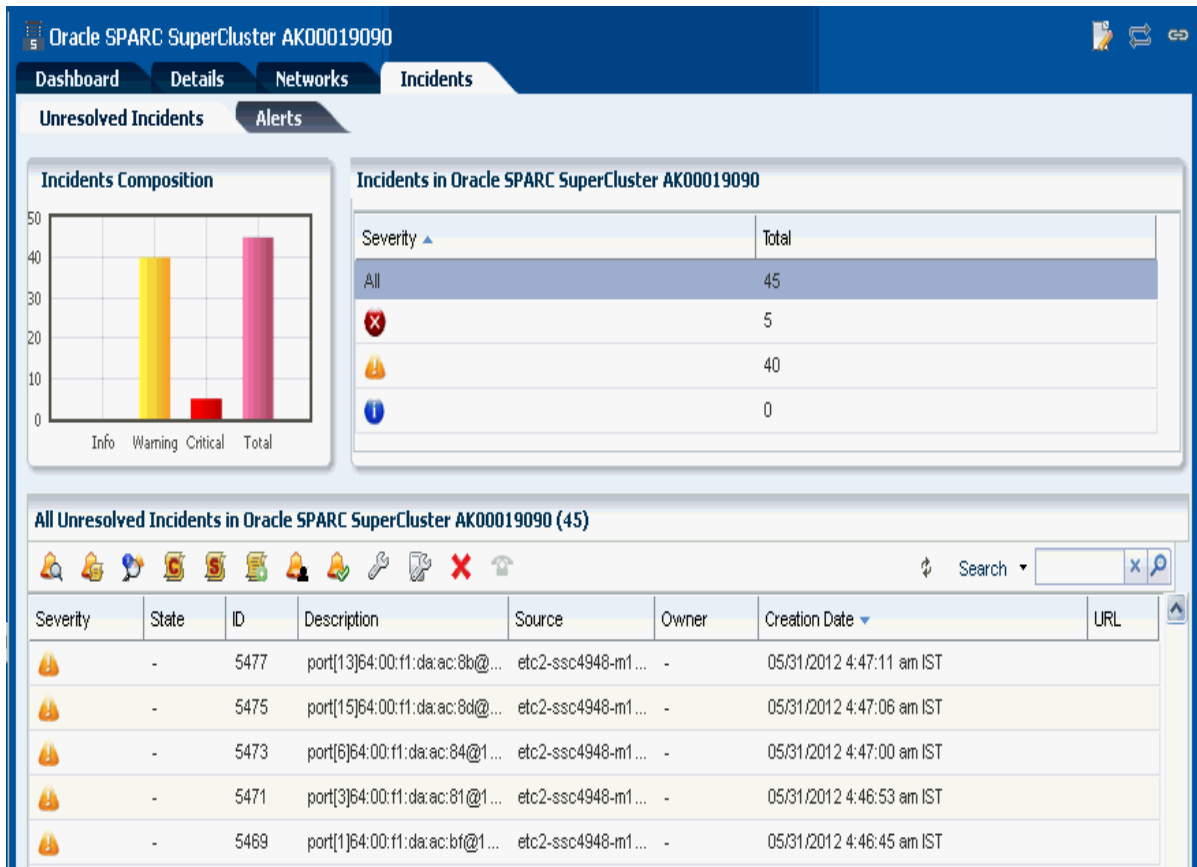
The Network Connectivity Table displays the infrastructure networks with IPs assigned to the individual hardware components of the SPARC SuperCluster system.

- Network Name
- Asset Type

### Incidents Tab

The Incidents Tab displays all the unresolved incidents and alerts reported in the SPARC SuperCluster System.

Figure 20–22 Incidents tab



### Permitted Actions in the SPARC SuperCluster System View

You can perform the following actions.

To see the procedures for completing these tasks, refer

*Oracle Enterprise Manager Ops Center Feature Reference Guide*

- Create Rack
- Edit Tags
- Add Assets
- Find Assets

### Viewing the SPARC SuperCluster System Rack

This section describes how to view the SPARC SuperCluster System rack, visualization of the rack physical layout, aggregated rack components, energy data, and other rack details. As an administrator, you can drill down to an asset contained in the rack (server, storage node, switch, Exadata Cells) or even further.

To view the SPARC SuperCluster System rack, perform the following steps:

1. On the Navigation pane, under Assets, select SuperCluster Systems.
2. Select a rack that you want to view.

The Dashboard, Details, Firmware, Incidents, Charts, Energy, and Jobs tabs are displayed in the center pane.



**Figure 20–23 Tabs of the SuperCluster System Rack**

- Dashboard Tab – Displays the summary, membership graph, and status of the rack.
  - Details Tab – Displays the rack info with a photorealistic view of the rack.
  - Firmware Tab – Displays the name, description, and version of the firmware for each component and the slot for each component
  - Incidents Tab – Displays all unresolved incidents in the rack.
  - Charts Tab – Provides more ways to display the power utilization data. You can change the graphed data to a bar chart or an area chart. You can also export the data for either the current view or all available data to a file in either CSV or XML format.
  - Energy Tab – Reports power consumption as the current value and for a period of time, as well as attributes of the fan and power supplies.
  - Jobs Tab – Displays the current and historical jobs.
3. Select any of the tabs to view more details of the rack.

Refer To [Hardware Monitoring](#) section in the *Hardware Management Guide* for information on the Tabs and Views of the rack.

## Photorealistic View of the SPARC SuperCluster System Rack

This view is a representation of the physical rack so that you can see the placement of the rack and its components.. The front and rear views of the rack are displayed in this view. All slots and the respective assets are displayed. Positions within the rack are displayed in a 3-dimensional view.

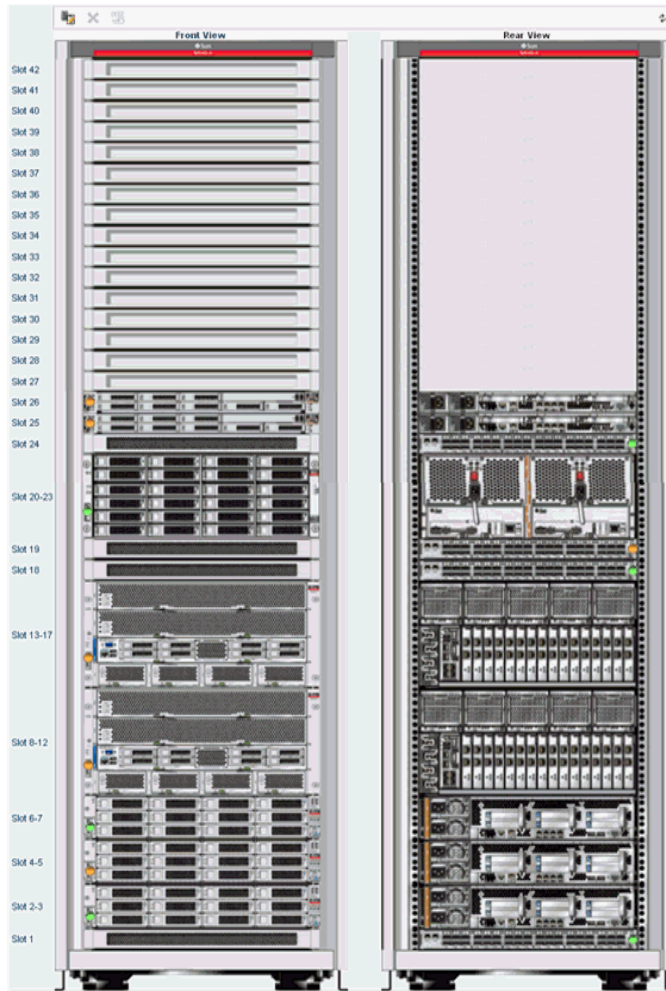
Each asset in the rack is represented by an image. The health status of assets such as OK, Warning, or Critical is displayed in the form of colored lights as seen on the physical rack itself. OK status is identified by the green color. Warning and critical status are identified by the yellow color. Hover the mouse over the slots in the rack and view details about the assets such as slot number, asset name and description, type of asset, model number of the asset, and its health status.

A question mark in any of the slots indicates a discrepancy from the baseline check. See [Baseline Check](#) for more information.

To see the photorealistic view of the rack, perform the following steps:

1. On the Navigation pane, under Assets, select SuperCluster Systems.
2. Select a rack that you want to view.
3. In the center pane, click the Details tab.

A photorealistic view of the SPARC SuperCluster System rack is displayed.

**Figure 20–24 Photorealistic view of SPARC SuperCluster**

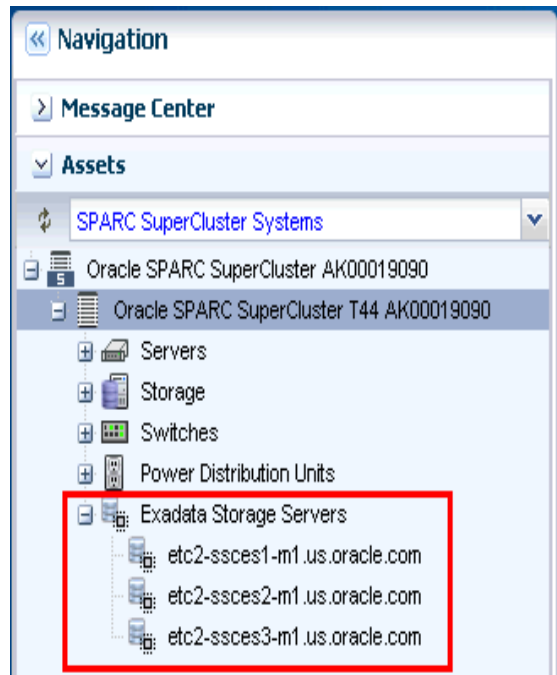
## Viewing the Exadata Storage Server

The Exadata Storage Server provides storage for the SPARC SuperCluster system. It is a sub-type of the Linux server installed to be a database node.

The Exadata Storage Servers are grouped together in the Navigation pane. In the same way that you view the SPARC SuperCluster system and its rack, you can also view the Exadata Storage Servers.

To view the Exadata Storage Server, do the following:

1. On the Navigation pane, under Assets, select SuperCluster Systems from the drop-down menu.

**Figure 20–25 Exadata Storage Server**

2. Expand Exadata Storage Servers, and select an Exadata Storage Server. The server details are displayed on the center pane. Select the respective tabs on the center pane to view or perform actions.

Refer To [Hardware Monitoring](#) section in the *Hardware Management Guide* for information on the different views and tasks that can be performed on the server cells.

## Discovering a SPARC SuperCluster Component

Manual discovery is necessary if a component has been replaced or some properties of a component has changed autonomously. The component can either be a compute node, storage, or switch.

To manually discover a SPARC SuperCluster component, do the following:

1. On the Navigation pane, select Plan Management.
2. Select Profiles and Policies, then select Discovery.  
The available discovery profiles are listed in the center pane.
3. Select the required stored discovery profile and edit the profile and metadata if required.
4. Click Finish. The job is run and the component is discovered.

### Add Assets to the SPARC SuperCluster Rack

After the asset is discovered, the new asset moves to the available asset poll. The asset must be added to the SPARC SuperCluster rack.

To add an asset to the SPARC SuperCluster rack, perform the following steps:

1. On the Navigation pane, under Assets, select SuperCluster Systems from the drop-down list.

2. Select the rack to which you want to add the asset.
3. On the center pane, click the Details tab. A photorealistic view of the rack is displayed.
4. Click the Add/Remove Asset in the rack.
5. Search for the right type of asset.
6. Assign or Remove the asset in the rack.
7. Save the rack changes. A rack modification job is created.

After the rack modification job is successful, the manually discovered asset appears in the SPARC SuperCluster rack.

## Creating and Viewing Reports

In general, using reports, you can view the rack setup for each of the rack within the system including the asset details related to the rack. Reports provide information about your assets, such as job history, firmware, OS updates, and incidents. Reports are created in PDF and CSV formats. You can export reports or use reports to launch jobs on targeted assets.

To create a Report, see the How To library at

<http://www.oracle.com/pls/topic/lookup?ctx=oc121&id=howto>

### Viewing the SPARC SuperCluster System Report

You can either view existing reports that have been created or you can create a new report for yourself and view it.

In this section, the SPARC SuperCluster System Report is described in detail. The following sections of the report are described below:

- [Report Parameters](#)
- [Summary Table](#)
- [Compute Nodes Table](#)
- [Switches Table](#)
- [Storage Appliances Table](#)
- [Exadata Storage Servers Table](#)
- [Power Distribution Units Table](#)
- [Validation Table](#)

#### Report Parameters

Report Parameters displays the name and model of the SPARC SuperCluster system. It also displays the number of assets in the rack by their types, such as compute nodes, switches, storage nodes, and Exadata Storage Servers present in the system.

#### Summary Table

The Summary Table is a table of contents of all tables in the report. It displays the number of records for each table.

#### Compute Nodes Table

The Compute Nodes Table displays the setup of the racks such as name of the asset (compute node), firmware version, hypervisor version, OBP version, LDOM manager

version, and the location of the asset in the rack with the slot number where it is placed.

**Switches Table**

The Switches Table displays the name of the switch node, type of switch (infiniband or ethernet), firmware version, and location of the switch in the rack with the slot number where it is placed.

**Storage Appliances Table**

The Storage Appliances Table displays the name of the compute node, version of the service processor firmware, and the location of the appliance with the slot number where it is placed in the rack.

**Exadata Storage Servers Table**

The Exadata Storage Servers table displays the name of the compute node, version of the service processor firmware, and the location of the appliance with the slot number where it is placed in the rack.

**Power Distribution Units Table**

The Power Distribution Units Table displays the name and firmware version of the PDUs.

**Validation Table**

The Validation Table displays the location, type, name, validation result, and expected components of the rack. A baseline check is performed against the known schema for the rack. See [Baseline Check](#) for more information. The expected component column in the table displays the expected component if the placed component in the slot does not match the schema when the baseline check was performed.



# Part VII

---

## Reference

Part VII contains the following chapters:

- [Appendix A, "Asset Attributes"](#)
- [Appendix B, "Oracle Solaris Cluster"](#)
- [Appendix C, "Logs and Directories"](#)
- [Appendix D, "JumpStart Enterprise Toolkit"](#)
- [Appendix E, "Icons"](#)
- [Appendix F, "Oracle Enterprise Manager Ops Center API"](#)
- [Glossary](#)





---



---

## Asset Attributes

Oracle Enterprise Manager Ops Center records the attributes of the assets it manages. You can use these attributes to administer groups. You can use the time zone values to adjust the reporting of assets.

### Monitoring Attributes

The attributes that can be used for asset monitoring vary across asset types. The full list of attributes for each asset are available in a set of Javadocs within the SDK package. This package is located in the following directory:

- Linux OS - <Installation directory>/xvmoc\_full\_bundle/Linux\_i686/Product/components/packages/sun-xvmoc-sdk-12.0.0.noarch.rpm
- Oracle Solaris OS for SPARC - <Installation directory>/xvmoc\_full\_bundle/SunOS\_sparc/Product/components/packages/SUNWxvmoc-sdk.pkg
- Oracle Solaris OS for x86 - <Installation directory>/xvmoc\_full\_bundle/SunOS\_i386/Product/components/packages/SUNWxvmoc-sdk.pkg

This package installs the Javadocs in the `/opt/sun/xvm/sdk/xvm_oc/doc/javadoc/` directory. Open the Javadoc for an asset type to view the attributes for that asset type.

### Grouping Attributes

[Table A-1](#) lists the attributes that you can use in group rules.

**Table A-1** Group Asset Attributes

Attribute	Supported Values
Appliance IP Address	Any IP address
Appliance Name	Any string
Architecture	
Asset Provisioning Supported	

**Table A-1 (Cont.) Group Asset Attributes**

<b>Attribute</b>	<b>Supported Values</b>
Asset Type	GlobalZone NonGlobalZone LDomHost LDomGuest OperatingSystem Server Network ServerContainer MSeriesChassis VirtualPool SolarisCluster SolarisClusterNode SolarisClusterZoneClusterGroup
Auto Boot	on off
Capability Entry	
Control Component Info Description	
Control Component Info Version	
Control Component Server Hostname	
Control Web Console URI	
CPU Architecture	POWER_PC SPARC SPARC-SUN4V X86
CPU Core Count	Any number
CPU Info Thread Count	Any number
CPU Mode	compatible auto
CPU Model	Any string
CPU Speed	Any number
CPU Type	Any string
Debug User SSH Access	TRUE FALSE
Description	Any string
Diag Level	max none min
DNS Configured	TRUE FALSE
DNS Domain Name	Any string

**Table A-1 (Cont.) Group Asset Attributes**

<b>Attribute</b>	<b>Supported Values</b>
Domain Degredation Policy	fru system xsb
Ethernet Port Fabric Tag	
Ethernet Port Info IP Address	Any IP address
Ethernet Port Infos Management	TRUE FALSE
Fabric Type	
Firmware Info Type	Any string
Firmware Description	Any string
FirmwareInfo Compliant	TRUE FALSE
FirmwareInfo Provider	Any string
Firmware Version	Any string
Hard Disk Size (Bytes)	Any number
Host ID	Any string
Hostname	Any string
HTTP Enabled	
IbP Key	
In Ucast Packets	
Interface Info Enabled	TRUE FALSE
Interface Info Fabric Tag	
Interface Info Subnet Mask	Any number
Interface Infos Mac Address	Any number
Interface IP Address	Any IP address
IP Address	Any IP address
IPSLicense	Any string
IPS Readme	Any string
Keep Alive Trap Time Seconds	
LDAP Profile Name	Any string
LDAP Proxy DN	Any string
LDAP Server	Any string
Local DNS Address	

**Table A-1 (Cont.) Group Asset Attributes**

<b>Attribute</b>	<b>Supported Values</b>
Locale	C POSIX en_CA en_CA.ISO8859-1 en_CA.UTF-8 en_US en_US.ISO8859-1 en_US.ISO8859-15 en_US.ISO8859-15@euro es es_MX es_MX.ISO8859-1 es_MX.UTF-8 fr fr_CA fr_CA.ISO8859-1 fr_CA.UTF-8 iso_8859_1
Location	
Locator Light On	TRUE FALSE
MAC Address	
Machine Hardware Class	InfiniBand Ethernet FibreChannel EthernetGateway InfiniBandGateway Unknown TOR NEM
Maintenance Mode	
Managed State	HIDDEN MANAGED MANAGED_OR_PROVISIONED PROVISIONING UNMANAGED UNMANAGED_OR_PROVISIONED
Management IP	
Manufactured Service Tag	
Manufacturer	Any string
MBean Interface Name	Any string

**Table A-1 (Cont.) Group Asset Attributes**

<b>Attribute</b>	<b>Supported Values</b>
Member Info Secure Mode	on off
Member Info Set Type	DOMAIN NEM SERVER
Memor Size	Any number
Memor Type	Any string
Model	Any string
Monitored	TRUE FALSE
Monitoring Policy	
MTU	
Multi Path Enabled	TRUE FALSE
Name	
Name Service Domain Name	Any string
Network CIDR	Any string
NFS Map ID Domain	Any string
NIS Name Server By IP Address	Any IP address
NIS Name Server By Name	Any string
Notifications Enabled	TRUE FALSE
Operator Panel Switch Status	Any string
Ops Center Version	
OSRunning	TRUE FALSE
Out Ucast Pkts	
PDU Modules	
Platform	
Port Info Address	Any string
Port Info Connected Peer	Any string
Port Connector Type	BOARD_INTERNAL CHASSIS_BLADE CHASSIS_FABRIC CXP QSFP SFP SFP_PLUS UNKNOWN

**Table A-1 (Cont.) Group Asset Attributes**

<b>Attribute</b>	<b>Supported Values</b>
Port Description	Any string
Port Fabric Tag	ETHERNET FIBRE_CHANNEL INFINIBAND UNKNOWN
Port Info In Discards	Any number
Port Info In Errors	Any number
PortInfos.inNUcastPkts	Any number
Port Info In Octets	Any number
Port Info Last Tick	Any number
Port Info Link Type	Any string
Port Info Local IP Address	Any string
Port Info Management	TRUE FALSE
Port Info MTU	Any number
Port Info Node Address	
Port Info Oper Status	Any string
Port Info Out Discards	Any number
Port Info Out Errors	Any number
Port Info Out NU CastPackets	Any number
Port Info Out Octets	Any number
Port Info Peer Address	Any number
Port Info Port Type	HOST ROUTER SWITCH TARGET
Port Info Remote DNS Address	Any string
Port Info Remote IP Address	Any string
Port Info Speed	Any string
Port Info Type	ETHERNET FIBRE_CHANNEL INFINIBAND POWER SERIAL VLAN UNKNOWN
Port Infos In Unknown Proto	
Port Infos NUcast Packets	

**Table A-1 (Cont.) Group Asset Attributes**

<b>Attribute</b>	<b>Supported Values</b>
PoweredOn	TRUE FALSE
Product Defined Instance ID	
Product Name	
Product URN	
Product Vendor	
Product Version	
Public UUID	
Rack ID	
Rack Info Asset Domain Type	
Rack Info Asset Gear Type	
Rack Info Asset ON	
Rack Info Asset Status	
Rack Info Asset User Friendly Name	
Rack Info Assets	
Rack Info Assets Model	
Rack Info Assets Occupancy	
Rack Info Position X	
Rack Info Position Y	
Rack Info Position Z	
Rack Info Assets User Friendly Name	
Rack Info Configuration	
Rack Info Number of Slots	
Rack Info Type	
Rcv Error Rate	Any string
RcvThroughput	Any string
Repeat Trap Number	
Repeat Trap Time Seconds	
Revision	
RoutingMode	DYN_OFF DYN_ON DYN_AUTO
Satellite	Any string
Semantic Tag Key	
Semantic Tag Key & Value	
Sensor Notification Enabled	TRUE FALSE

**Table A-1 (Cont.) Group Asset Attributes**

<b>Attribute</b>	<b>Supported Values</b>
Serial Console URL	Any string
Serial Number	
Service Tag Agent Version	Any string
Service Tag AssetLabel	Any string
Service Tag CPU Manufacturer	Any string
Service Tag Customer Asset Tag	Any string
Service Tag Host	Any string
Service Tag Instance URN	Any string
Service Tag IP Address	Any IP address
Service Tag Platform Architecture	Any string
Service Tag Port	Any number
Service Tag Product Hierarchy	Any string
Service Tag Release	Any string
Service Tag Serial Number	Any string
Service Tag Sub-Status	Any string
Service Tag Type	NATIVE NATIVE_NOT_FOUND MANUFACTURED
SNMP Enabled	
Solaris Non-global zone Exclusive	
Solaris Non-Global Zone.	
Static Route Info Set	
Status	FAULTED NON_RECOVERABLE MAINTENANCE DECONFIGURED DEGRADED CRITICAL WARNING INFO OK UNINITIALIZED UNKNOWN UNCONFIGURED NEEDS_POWERON
Subnet Manager	TRUE FALSE
Subnet Manager Address	Any string
Subnet Mask	Any string



**Table A-1 (Cont.) Group Asset Attributes**

<b>Attribute</b>	<b>Supported Values</b>
System Identifier	
System Name	
System Version	
Time Zone	See Time Zone Values list below
Total Rcv Errors	Any string
Total Rcv Octets	Any string
Total Xmit Errors	Any string
Total Xmit Octets	Any string
User Friendly Description	Any string
User Friendly Name	Any string
Version	
Virtualization Type	ldom xen zone
VLAN ID	Any string
Web Console URI	Any string
Web Console URL	Any string
Xmit Error Rate	Any string
Xmit Throughput	Any string
XSB Assignment Status	Assigned Available Unavailable
XSB Connection Status	y n
XSB Diag Status	Failed Passed Testing Unknown Unmount

**Table A-1 (Cont.) Group Asset Attributes**

<b>Attribute</b>	<b>Supported Values</b>
XSB Domain ID	00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 SP
XSB Dynamic Reconf Status	Any string
XSB ID	Any string
XSB Fault Status	Degraded Faulted Normal
XSB Info Set	
XSB Power Status	y n
XSB PSB ID	Any string
XSB Incorporation Status	y n
XVMServerVersion	Any string

## Time Zone Values

- Africa/Abidjan
- Africa/Accra
- Africa/Addis\_Ababa
- Africa/Algiers
- Africa/Asmara
- Africa/Asmera
- Africa/Bamako
- Africa/Bangui
- Africa/Banjul

- Africa/Bissau
- Africa/Blantyre
- Africa/Brazzaville
- Africa/Bujumbura
- Africa/Cairo
- Africa/Casablanca
- Africa/Ceuta
- Africa/Conakry
- Africa/Dakar
- Africa/Dar\_es\_Salaam
- Africa/Djibouti
- Africa/Douala
- Africa/El\_Aaiun
- Africa/Freetown
- Africa/Gaborone
- Africa/Harare
- Africa/Johannesburg
- Africa/Kampala
- Africa/Khartoum
- Africa/Kigali
- Africa/Kinshasa
- Africa/Lagos
- Africa/Libreville
- Africa/Lome
- Africa/Luanda
- Africa/Lubumbashi
- Africa/Lusaka
- Africa/Malabo
- Africa/Maputo
- Africa/Maseru
- Africa/Mbabane
- Africa/Mogadishu
- Africa/Monrovia
- Africa/Nairobi
- Africa/Ndjamena
- Africa/Niamey
- Africa/Nouakchott

- Africa/Ouagadougou
- Africa/Porto-Novo
- Africa/Sao\_Tome
- Africa/Timbuktu
- Africa/Tripoli
- Africa/Tunis
- Africa/Windhoek
- America/Adak
- America/Anchorage
- America/Anguilla
- America/Antigua
- America/Araguaina
- America/Argentina/Buenos\_Aires
- America/Argentina/Catamarca
- America/Argentina/ComodRivadavia
- America/Argentina/Cordoba
- America/Argentina/Jujuy
- America/Argentina/La\_Rioja
- America/Argentina/Mendoza
- America/Argentina/Rio\_Gallegos
- America/Argentina/Salta
- America/Argentina/San\_Juan
- America/Argentina/San\_Luis
- America/Argentina/Tucuman
- America/Argentina/Ushuaia
- America/Aruba
- America/Asuncion
- America/Atikokan
- America/Atka
- America/Bahia
- America/Bahia\_Banderas
- America/Barbados
- America/Belem
- America/Belize
- America/Blanc-Sablon
- America/Boa\_Vista
- America/Bogota

- America/Boise
- America/Buenos\_Aires
- America/Cambridge\_Bay
- America/Campo\_Grande
- America/Cancun
- America/Caracas
- America/Catamarca
- America/Cayenne
- America/Cayman
- America/Chicago
- America/Chihuahua
- America/Coral\_Harbour
- America/Cordoba
- America/Costa\_Rica
- America/Cuiaba
- America/Curacao
- America/Danmarkshavn
- America/Dawson
- America/Dawson\_Creek
- America/Denver
- America/Detroit
- America/Dominica
- America/Edmonton
- America/Eirunepe
- America/El\_Salvador
- America/Ensenada
- America/Fort\_Wayne
- America/Fortaleza
- America/Glace\_Bay
- America/Godthab
- America/Goose\_Bay
- America/Grand\_Turk
- America/Grenada
- America/Guadeloupe
- America/Guatemala
- America/Guayaquil
- America/Guyana

- America/Halifax
- America/Havana
- America/Hermosillo
- America/Indiana/Indianapolis
- America/Indiana/Knox
- America/Indiana/Marengo
- America/Indiana/Petersburg
- America/Indiana/Tell\_City
- America/Indiana/Vevay
- America/Indiana/Vincennes
- America/Indiana/Winamac
- America/Indianapolis
- America/Inuvik
- America/Iqaluit
- America/Jamaica
- America/Jujuy
- America/Juneau
- America/Kentucky/Louisville
- America/Kentucky/Monticello
- America/Knox\_IN
- America/La\_Paz
- America/Lima
- America/Los\_Angeles
- America/Louisville
- America/Maceio
- America/Managua
- America/Manaus
- America/Marigot
- America/Martinique
- America/Matamoros
- America/Mazatlan
- America/Mendoza
- America/Menominee
- America/Merida
- America/Mexico\_City
- America/Miquelon
- America/Moncton

- America/Monterrey
- America/Montevideo
- America/Montreal
- America/Montserrat
- America/Nassau
- America/New\_York
- America/Nipigon
- America/Nome
- America/Noronha
- America/North\_Dakota/Center
- America/North\_Dakota/New\_Salem
- America/Ojinaga
- America/Panama
- America/Pangnirtung
- America/Paramaribo
- America/Phoenix
- America/Port-au-Prince
- America/Port\_of\_Spain
- America/Porto\_Acre
- America/Porto\_Velho
- America/Puerto\_Rico
- America/Rainy\_River
- America/Rankin\_Inlet
- America/Recife
- America/Regina
- America/Resolute
- America/Rio\_Branco
- America/Rosario
- America/Santa\_Isabel
- America/Santarem
- America/Santiago
- America/Santo\_Domingo
- America/Sao\_Paulo
- America/Scoresbysund
- America/Shiprock
- America/St\_Barthlemy
- America/St\_Johns

- America/St\_Kitts
- America/St\_Lucia
- America/St\_Thomas
- America/St\_Vincent
- America/Swift\_Current
- America/Tegucigalpa
- America/Thule
- America/Thunder\_Bay
- America/Tijuana
- America/Toronto
- America/Tortola
- America/Vancouver
- America/Virgin
- America/Whitehorse
- America/Winnipeg
- America/Yakutat
- America/Yellowknife
- Antarctica/Casey
- Antarctica/Davis
- Antarctica/DumontDUrville
- Antarctica/Macquarie
- Antarctica/Mawson
- Antarctica/McMurdo
- Antarctica/Palmer
- Antarctica/Rothera
- Antarctica/South\_Pole
- Antarctica/Syowa
- Antarctica/Vostok
- Arctic/Longyearbyen
- Asia/Aden
- Asia/Almaty
- Asia/Amman
- Asia/Anadyr
- Asia/Aqtau
- Asia/Aqtobe
- Asia/Ashgabat
- Asia/Ashkhabad



- 
- Asia/Baghdad
  - Asia/Bahrain
  - Asia/Baku
  - Asia/Bangkok
  - Asia/Beirut
  - Asia/Bishkek
  - Asia/Brunei
  - Asia/Calcutta
  - Asia/Choibalsan
  - Asia/Chongqing
  - Asia/Chungking
  - Asia/Colombo
  - Asia/Dacca
  - Asia/Damascus
  - Asia/Dhaka
  - Asia/Dili
  - Asia/Dubai
  - Asia/Dushanbe
  - Asia/Gaza
  - Asia/Harbin
  - Asia/Ho\_Chi\_Minh
  - Asia/Hong\_Kong
  - Asia/Hovd
  - Asia/Irkutsk
  - Asia/Istanbul
  - Asia/Jakarta
  - Asia/Jayapura
  - Asia/Jerusalem
  - Asia/Kabul
  - Asia/Kamchatka
  - Asia/Karachi
  - Asia/Kashgar
  - Asia/Kathmandu
  - Asia/Katmandu
  - Asia/Kolkata
  - Asia/Krasnoyarsk
  - Asia/Kuala\_Lumpur

- Asia/Kuching
- Asia/Kuwait
- Asia/Macao
- Asia/Macau
- Asia/Magadan
- Asia/Makassar
- Asia/Manila
- Asia/Muscat
- Asia/Nicosia
- Asia/Novokuznetsk
- Asia/Novosibirsk
- Asia/Omsk
- Asia/Oral
- Asia/Phnom\_Penh
- Asia/Pontianak
- Asia/Pyongyang
- Asia/Qatar
- Asia/Qyzylorda
- Asia/Rangoon
- Asia/Riyadh
- Asia/Riyadh87
- Asia/Riyadh88
- Asia/Riyadh89
- Asia/Saigon
- Asia/Sakhalin
- Asia/Samarkand
- Asia/Seoul
- Asia/Shanghai
- Asia/Singapore
- Asia/Taipei
- Asia/Tashkent
- Asia/Tbilisi
- Asia/Tehran
- Asia/Tel\_Aviv
- Asia/Thimbu
- Asia/Thimphu
- Asia/Tokyo

- Asia/Ujung\_Pandang
- Asia/Ulaanbaatar
- Asia/Ulan\_Bator
- Asia/Urumqi
- Asia/Vientiane
- Asia/Vladivostok
- Asia/Yakutsk
- Asia/Yekaterinburg
- Asia/Yerevan
- Atlantic/Azores
- Atlantic/Bermuda
- Atlantic/Canary
- Atlantic/Cape\_Verde
- Atlantic/Faeroe
- Atlantic/Faroe
- Atlantic/Jan\_Mayen
- Atlantic/Madeira
- Atlantic/Reykjavik
- Atlantic/South\_Georgia
- Atlantic/St\_Helena
- Atlantic/Stanley
- Australia/ACT
- Australia/Adelaide
- Australia/Brisbane
- Australia/Broken\_Hill
- Australia/Canberra
- Australia/Currie
- Australia/Darwin
- Australia/Eucla
- Australia/Hobart
- Australia/LHI
- Australia/Lindeman
- Australia/Lord\_Howe
- Australia/Melbourne
- Australia/NSW
- Australia/North
- Australia/Perth

- Australia/Queensland
- Australia/South
- Australia/Sydney
- Australia/Tasmania
- Australia/Victoria
- Australia/West
- Australia/Yancowinna
- Brazil/Acre
- Brazil/DeNoronha
- Brazil/East
- Brazil/West
- CET
- CST6CDT
- Canada/Atlantic
- Canada/Central
- Canada/East-Saskatchewan
- Canada/Eastern
- Canada/Mountain
- Canada/Newfoundland
- Canada/Pacific
- Canada/Saskatchewan
- Canada/Yukon
- Chile/Continental
- Chile/EasterIsland
- Cuba
- EET
- EST
- EST5EDT
- Egypt
- Eire
- Etc/GMT
- Etc/GMT+0
- Etc/GMT+1
- Etc/GMT+10
- Etc/GMT+11
- Etc/GMT+12
- Etc/GMT+2

- Etc/GMT+3
- Etc/GMT+4
- Etc/GMT+5
- Etc/GMT+6
- Etc/GMT+7
- Etc/GMT+8
- Etc/GMT+9
- Etc/GMT-0
- Etc/GMT-1
- Etc/GMT-10
- Etc/GMT-11
- Etc/GMT-12
- Etc/GMT-13
- Etc/GMT-14
- Etc/GMT-2
- Etc/GMT-3
- Etc/GMT-4
- Etc/GMT-5
- Etc/GMT-6
- Etc/GMT-7
- Etc/GMT-8
- Etc/GMT-9
- Etc/GMT0
- Etc/Greenwich
- Etc/UCT
- Etc/UTC
- Etc/Universal
- Etc/Zulu
- Europe/Amsterdam
- Europe/Andorra
- Europe/Athens
- Europe/Belfast
- Europe/Belgrade
- Europe/Berlin
- Europe/Bratislava
- Europe/Brussels
- Europe/Bucharest

- Europe/Budapest
- Europe/Chisinau
- Europe/Copenhagen
- Europe/Dublin
- Europe/Gibraltar
- Europe/Guernsey
- Europe/Helsinki
- Europe/Isle\_of\_Man
- Europe/Istanbul
- Europe/Jersey
- Europe/Kaliningrad
- Europe/Kiev
- Europe/Lisbon
- Europe/Ljubljana
- Europe/London
- Europe/Luxembourg
- Europe/Madrid
- Europe/Malta
- Europe/Mariehamn
- Europe/Minsk
- Europe/Monaco
- Europe/Moscow
- Europe/Nicosia
- Europe/Oslo
- Europe/Paris
- Europe/Podgorica
- Europe/Prague
- Europe/Riga
- Europe/Rome
- Europe/Samara
- Europe/San\_Marino
- Europe/Sarajevo
- Europe/Simferopol
- Europe/Skopje
- Europe/Sofia
- Europe/Stockholm
- Europe/Tallinn

- 
- Europe/Tirane
  - Europe/Tiraspol
  - Europe/Uzhgorod
  - Europe/Vaduz
  - Europe/Vatican
  - Europe/Vienna
  - Europe/Vilnius
  - Europe/Volgograd
  - Europe/Warsaw
  - Europe/Zagreb
  - Europe/Zaporozhye
  - Europe/Zurich
  - Factory
  - GB
  - GB-Eire
  - GMT
  - GMT+0
  - GMT-0
  - GMT0
  - Greenwich
  - HST
  - Hongkong
  - Iceland
  - Indian/Antananarivo
  - Indian/Chagos
  - Indian/Christmas
  - Indian/Cocos
  - Indian/Comoro
  - Indian/Kerguelen
  - Indian/Mahe
  - Indian/Maldives
  - Indian/Mauritius
  - Indian/Mayotte
  - Indian/Reunion
  - Iran
  - Israel
  - Jamaica

- Japan
- Kwajalein
- Libya
- MET
- MST
- MST7MDT
- Mexico/BajaNorte
- Mexico/BajaSur
- Mexico/General
- Mideast/Riyadh87
- Mideast/Riyadh88
- Mideast/Riyadh89
- NZ
- NZ-CHAT
- Navajo
- PRC
- PST8PDT
- Pacific/Apia
- Pacific/Auckland
- Pacific/Chatham
- Pacific/Easter
- Pacific/Efate
- Pacific/Enderbury
- Pacific/Fakaofu
- Pacific/Fiji
- Pacific/Funafuti
- Pacific/Galapagos
- Pacific/Gambier
- Pacific/Guadalcanal
- Pacific/Guam
- Pacific/Honolulu
- Pacific/Johnston
- Pacific/Kiritimati
- Pacific/Kosrae
- Pacific/Kwajalein
- Pacific/Majuro
- Pacific/Marquesas



- Pacific/Midway
- Pacific/Nauru
- Pacific/Niue
- Pacific/Norfolk
- Pacific/Noumea
- Pacific/Pago\_Pago
- Pacific/Palau
- Pacific/Pitcairn
- Pacific/Ponape
- Pacific/Port\_Moresby
- Pacific/Rarotonga
- Pacific/Saipan
- Pacific/Samoa
- Pacific/Tahiti
- Pacific/Tarawa
- Pacific/Tongatapu
- Pacific/Truk
- Pacific/Wake
- Pacific/Wallis
- Pacific/Yap
- Poland
- Portugal
- ROK
- Singapore
- Turkey
- UCT
- US/Alaska
- US/Aleutian
- US/Arizona
- US/Central
- US/East-Indiana
- US/Eastern
- US/Hawaii
- US/Indiana-Starke
- US/Michigan
- US/Mountain
- US/Pacific

- US/Pacific-New
- US/Samoa
- UTC
- Universal
- W-SU
- WET
- Zulu

---

---

## Oracle Solaris Cluster

Use Oracle Enterprise Manager Ops Center to install a new Oracle Solaris Cluster and to maintain existing Oracle Solaris Clusters.

### Upgrading an Oracle Solaris Cluster

The cluster update procedures operate on complete clusters. It is not possible to upgrade only a cluster node.

To upgrade a cluster to a newer version of the Oracle Solaris Cluster software, use a profile that defines the new version. You can begin the procedure by either selecting the target cluster and then the deployment plan or selecting the deployment plan and then the target. In either case, you use the Solaris Cluster Upgrade Job wizard to specify how the deployment operates.

#### Before You Begin

Import the cluster profile.

See XREF or detailed procedure about importing a cluster profile.

#### To Upgrade the Cluster

1. Expand Plan Management in the Navigation pane.
2. In the Profiles and Policies section, click Update Profiles.
3. Select Oracle Solaris Upgrade Job in the Actions pane. The Oracle Solaris Upgrade Job wizard starts.
4. Enter a name for the upgrade job.
5. Click display the cluster targets.
6. Choose one or more clusters and click Select/Add to Target List.
7. Select Dual Partition Mode.
8. Select the policy to use if a task in the upgrade cannot be completed.
9. Select the profile that you imported.
10. Review the summary of the job and click Finish. The upgrade job is submitted. You can follow the progress of the job by clicking the View Job Details icon in the jobs pane.

### Cluster Profiles

You use cluster profiles in a deployment plan to perform the following operations:

- Install Oracle Solaris Cluster software
- Upgrade Oracle Solaris Cluster software

The profiles and deployment plans rely on pre-action and post-action scripts to suspend cluster operations and save configuration information during the update process.

The following cluster-specific profiles and scripts are located in Enterprise Manager Ops Center's Local Content software library. As the Oracle Solaris Cluster software is revised, new profiles are made available to you through the Java.net site's Ops Center Cluster Profiles project. You download these new profiles and scripts, then import them into the Local Content library. See [Obtaining the Cluster Profiles and Scripts](#) for instructions to get these files.

- Profiles for Provisioning Oracle Solaris Cluster Software version 3.2u3
  - SPARC
    - \* sc-3.2u3-core-sparc
    - \* sc-3.2u3-manager-sparc
    - \* sc-3.2u3-agents-sparc
  - x86
    - \* sc-3.2u3-core-x86
    - \* sc-3.2u3-manager-x86
    - \* sc-3.2u3-agents-x86
- Profiles for Upgrading Version 3.2u3 to Version 3.3 or for Provisioning an Oracle Solaris Cluster Software Version 3.3
  - SPARC
    - \* sc-3.3-core-sparc
    - \* sc-3.3-manager-sparc
    - \* sc-3.3-agents-sparc
  - x86
    - \* sc-3.3-core-x86
    - \* sc-3.3-manager-x86
    - \* sc-3.3-agents-x86
- Scripts for pre-action and post-action
  - Post-action script for provisioning either version 3.2 or 3.3: SolarisCluster-Post.ksh
  - Post-action script for upgrading version 3.2 to 3.3: SolarisCluster3.21109-Post
  - Pre-action script for upgrading version 3.2 to 3.3: SolarisCluster3.21109-Pre

## Obtaining the Cluster Profiles and Scripts

To obtain profiles and scripts for a new release of Oracle Solaris s Cluster software, download them to the system that is running the Enterprise Controller.

---

---

**Note:** When you download, transfer, upload, or import these files, do not change the file name. Keep the same name throughout the procedure.

---

---

### To Obtain the Cluster Profiles and Scripts

1. Go to <http://java.net/projects/oc-cluster-profiles>
2. Click the Downloads button.
3. Select the folder for the profiles you want:
  - To provision Oracle Solaris Cluster Software version 3.2u3, select the Version-3.2u3 folder.
  - To upgrade version 3.2u3 to version 3.3, select the Version-3.3 folder.
  - To provision Oracle Solaris Cluster Software version 3.3, select the Version-3.3 folder.
4. In the version folder, select the platform you want, either SPARC or x86.  
The platform folder contains three files: Agents, Core, and Manager. You need all three files to complete upgrade or provision operations.
5. Use the browser window's Save feature to save each file, keeping its file name.
6. Return to the home page for the project and select the Action-Scripts folder.
7. Select the scripts that complete the core profiles:
  - To upgrade version 3.2u3 to version 3.3, select the Pre-Upgrade and Post-Upgrade scripts.
  - To provision version 3.2u3 or version 3.3, select the Post-Provision script.
8. Upload the profiles and scripts, according to [Uploading the Cluster Profiles and Scripts](#).

## Uploading the Cluster Profiles and Scripts

The files containing the profiles and scripts must reside on the same system that is running the browser and they must reside in the same directory. This operation uploads all files in the selected directory.

1. Move the profiles and scripts to the appropriate system and directory.
2. Expand Libraries in the Navigation pane.
3. Click Local Content in the Solaris/Linux OS Updates library.
4. Click Bulk Upload Packages and Patches in the Actions pane.
5. Click Distribution to select the distribution that applies to these files.
6. Select Upload from Directory.
7. Specify the path to the directory or click Browse to locate and select it.  
All files in the directory and its subdirectories are uploaded.
8. Click Submit.
9. Import the profiles into Enterprise Manager Ops Center, according to [Importing Cluster Profiles and Scripts](#).

## Importing Cluster Profiles and Scripts

### Before You Begin

- To import profiles, use the browser on the same system or transfer the profiles to the system on which you are running the browser.
- To import scripts, transfer the files to the Enterprise Controller's system.

---

---

**Note:** When you download, transfer, upload, or import these files, do not change the file name. Keep the same name throughout the procedure.

---

---

### To Import a Cluster Profile

1. Expand Plan Management in the Navigation pane.
2. Click Update Profiles.
3. Click the Import Profile icon.
4. For each profile and script:
  - a. Enter the name of the file you downloaded. Do not change the name.
  - b. Click Import.
5. Expand Libraries in the Navigation pane.
6. Select Solaris/Linux OS Updates.
7. Select Local Content.
8. Click Upload Local Action.
9. For each profile:
  - a. Enter the name of the profile as you want it to be displayed in the Plan Management section.
  - b. Select the distribution of the OS that uses the profile.
  - c. Enter the name of the file that contains the profile. Do not change the name.
  - d. Click Upload.
10. For each script:
  - a. Select action type, the matching parent category, and the OS distribution.
  - b. Enter the name of the file that contains the script. Do not change the name.
  - c. Click Upload.
11. For provisioning profiles, edit the core profiles to include the Post-Provision scripts, according to [Editing the Core Profile for Provisioning](#)

To upgrade a cluster, no modification is needed because the scripts are available to the upgrade profile after the import operation.

## Editing the Core Profile for Provisioning

1. Expand Plan Management in the Navigation pane.
2. Click Update Profiles.
3. In the OS Update Profiles table, select the core profile.

4. Click the Edit Profile icon.
5. In the Edit OS Update Profile window, navigate from Local to either Post-actions or Pre-action.
6. Select the script and click Required. For example, to edit the core profile for provisioning, navigate to Post-actions, select SolarisCluster-Post.ksh, and click Required. The file is now listed in the Profile Contents section.
7. Click the Saved as Named Profile button.





---

---

## Logs and Directories

Each Enterprise Manager Ops Center component has some auditing capability. Follow audit advice in this document and regularly monitor audit records.

Enterprise Manager Ops Center performs each action as a job. The details of a job show the order of operations in the job and the managed assets that were targets of the job. You can view the details of a job from either the browser or the command-line interface. Each job is stored until it is deleted explicitly.

In addition to the jobs record, log files can be a source of activity records. Logs are written during operations and can provide additional detail about system activity. Log files are protected by file permissions and therefore requires a privileged user to access them.

### Installation

- Log of the most recent installation or uninstallation:  
`/var/tmp/installer.log.latest`
- Log of previous installation or uninstallation operations:  
`/var/tmp/installer.log.xxxx`
- Log of an agent installation: `/var/scn/install/log`

### General Events

- Messages: `/var/adm/messages*`
- BUI: `/var/opt/sun/xvm/logs/emoc.log`
- Actions of the BUI and remote clients on the Enterprise Controller:
  - On Oracle Solaris: `/var/cacao/instances/oem-ec/audits/`
  - On Linux: `/var/opt/sun/cacao/instances/oem-ec/audits/`
- Events between controllers and agents:
  - On an Oracle Solaris Enterprise Controller:  
`/var/cacao/instances/oem-ec/logs`
  - On a Linux Enterprise Controller:  
`/var/opt/sun/cacao/instances/oem-ec/logs`
  - On each Oracle Solaris Proxy Controller:  
`/var/cacao/instances/scn-proxy/logs/cacao.n`

- On each Linux Proxy Controller:  
`/var/opt/sun/cacao/instances/scn-proxy/logs/cacao.n`

## High Availability

When Oracle Enterprise Manager Ops Center is in a High Availability configuration, each Enterprise Controller is a Clusterware node. The Clusterware resource activity is logged and the following log file is updated each time the active Enterprise Controller's resource action script's check() function is executed. The default interval is 60 seconds.

- On Oracle Solaris: `/var/opt/sun/xvm/ha/EnterpriseController.log`

## Software Updates

The Software Update component has its own server with its own logs. The following logs provide information on the activity for this server:

- Audit Log
  - On Oracle Solaris: `/var/opt/sun/xvm/uce/var.opt/server/logs/audit.log`
  - On Linux: `/usr/local/uce/server/logs/audit.log`
- Errors
  - On Oracle Solaris: `/var/opt/sun/xvm/uce/var.opt/server/logs/error.log`
  - On Linux: `/usr/local/uce/server/logs/error.log`
  - Log of errors in download jobs: `/opt/SUNWuce/server/logs/SERVICE_CHANNEL/error.log`
- Job Log
  - On Oracle Solaris: `/var/opt/sun/xvm/uce/var.opt/server/logs/job.log`
  - On Linux: `/usr/local/uce/server/logs/job.log`

## Agents

- `/var/scn/update-agent/logs` directory.
- `/var/opt/sun/xvm/logs`

## Local Database

- On the Enterprise Controller:
  - For installation events:  
`/var/opt/sun/xvm/oracle/cfgtoollogs/dbca/OCDB/*`  
`/var/tmp/installer.log.latest`
  - For operational events, reported by the `ecadm sqlplus` utility:  
`/var/opt/sun/xvm/oracle/diag/rdbms/ocdb/OCDB/alert/log.xml.*`  
`/var/opt/sun/xvm/oracle/diag/rdbms/ocdb/OCDB/trace/alert_OCDB.log.*`  
`/var/opt/sun/xvm/oracle/diag/tnslsnr/<hostname>/oclistener/alert/log.xml.*`  
`/var/opt/sun/xvm/oracle/diag/tnslsnr/<hostname>/oclistener/trace/listener.log.*`

- For schema changes:
  - `/var/opt/sun/xvm/log/satadmsqlplus.log`
  - `/var/opt/sun/xvm/logs/alter_oracle_schema.out`
  - `/var/opt/sun/xvm/logs/alter_oracle_storage.out`
- For backup, restore, and migrate operations:
  - `/var/tmp/sat-backup-<`date +%F-%T`>.log`
  - `/var/tmp/sat-restore-<`date +%F-%T`>.log`
  - `/var/opt/sun/xvm/logs/migrate.log`
- On the Proxy Controller: `/var/opt/sun/xvm/proxydb/*`
- On each agent: `/var/opt/sun/xvm/agentdb/*`

## Upgrade

The log of upgrade actions for the Enterprise Controller and its co-located proxy controller is in the `/var/scn/update-saved-state/update_satellite_bundle_12.1.n.xxxx/updatelog.txt` file.

The log of upgrade actions for a Proxy Controller that is not co-located is in the `/var/scn/update-saved-state/update_proxy_bundle_12.1.n.xxxx/updatelog.txt` file.

After an upgrade, the state of the database is saved in the `/var/scn/update-saved-state/update_satellite_bundle_12.1.n.xxxx/dblogs` folder.

## Event Logs for Jobs

Event logs for jobs are generated by tasks as they progress. See [Viewing Jobs](#) for instructions on viewing job event logs.

## To Control the Number of Common Agent Container Log Files

The Common Agent Container cacao is a common Java container for JDMX/JMX management and handles the interactions between controllers and agents. All events are recorded in the cacao log files and events that are above the level of INFO are also logged in the syslog. You can view the contents of the current log file using the Ops Center BUI.

- On an Oracle Solaris Enterprise Controller:
  - `/var/cacao/instances/oem-ec/logs/cacao.n`
- On a Linux Enterprise Controller:
  - `/var/opt/sun/cacao/instances/oem-ec/logs/cacao.n`
- On each Oracle Solaris Proxy Controller:
  - `/var/cacao/instances/scn-proxy/logs/cacao.n`
- On each Linux Proxy Controller:
  - `/var/opt/sun/cacao/instances/scn-proxy/logs/cacao.n`

The maximum file size is 1 MB. When the limit is reached, the current log file is closed and a new one created. The default number of log files is three. You can change the

number of log files Ops Center retains, using the Common Agent Container's management utility, `cacaoadm`.

To view the current number of log files maintained for the Enterprise Controller, issue the following command on the system where the Enterprise software is running:

```
# cacaoadm get-param log-file-count -i oem-ec
log-file-count=3
```

To view the number of log files maintained for a Proxy Controller, issue the following command on the system where the proxy controller software is running:

```
# cacaoadm get-param log-file-count -i scn-proxy
log-file-count=3
```

To change the number of log files on the Enterprise Controller, a Proxy Controller, or both:

1. Verify that there are no active jobs.
2. Stop the Common Agent Container service on the Enterprise Controller.

- On Oracle Solaris:

```
# /opt/SUNWxvmoc/bin/satadm stop -w -v
```

- On Linux:

```
# /opt/sun/xvmoc/bin/satadm stop -w -v
```

Stop the Common Agent Container service on a Proxy Controller:

- On Oracle Solaris:

```
# /opt/SUNWxvmoc/bin/proxyadm stop -w -v
```

- On Linux:

```
# /opt/sun/xvmoc/bin/proxyadm stop -w -v
```

3. Specify the maximum number of log files to be retained in addition to the current log file. In the following example, the count of 10 specifies that nine log files of previous events are retained in addition to the log file for current events. On the Enterprise Controller:

```
# cacaoadm set-param log-file-count=10 -i default
```

On a Proxy Controller:

```
# cacaoadm set-param log-file-count=10 -i scn-proxy
```

4. Start the Enterprise Controller.

- On Oracle Solaris:

```
# /opt/SUNWxvmoc/bin/satadm start -w -v
```

- On Linux:

```
# /opt/sun/xvmoc/bin/satadm start -w -v
```

5. Verify that the Enterprise Controller has been restarted completely before attempting other operations. For example, if you have stopped both the Enterprise Controller and a Proxy Controller, wait for the Enterprise Controller to restart before restarting each Proxy Controller. On an Oracle Solaris Proxy Controller:

```
# /opt/SUNWxvmoc/bin/proxyadm start -w -v
```

**On a Linux Proxy Controller:**

```
# /opt/sun/xvmoc/bin/proxyadm start -w -v
```

- 6.** Verify that all controllers have restarted completely before attempting other operations.



---

---

## JumpStart Enterprise Toolkit

Use JumpStart Enterprise Toolkit (JET) to extend the JumpStart functionality provided within the Oracle Solaris operating system.

JumpStart Enterprise Toolkit (JET) provides a framework to simplify and extend the JumpStart functionality provided within the Oracle Solaris operating system. The SUNWjet and JetFLASH packages are installed on the Proxy Controller during installation.

### JumpStart Enterprise Toolkit Configuration File Location

The JET module parameters are available for use in OS profiles. See the `module.conf` configuration files that are associated with JET modules for information about parameters for specific JET modules. The configuration files are located in the `/opt/SUNWjet/Products` directory on the Proxy Controller. For example, the configuration files for the custom module is located in the following directory on the Proxy Controller: `/opt/SUNWjet/Products/custom/custom.conf`. You can review the parameters for these modules by looking at the `sample.template` file in the `/opt/SUNWjet/Templates` directory on a Proxy Controller.

### SUNWjet Parameters

When you specify JET parameters with an OS profile, the following parameters from the `base_config` JET module are automatically updated within the OS profile and must not be modified:

- `base_config_ClientArch`
- `base_config_ClientEther`
- `base_config_client_allocation`
- `base_config_sysidcfg_network_interface`
- `base_config_sysidcfg_ip_address`
- `base_config_sysidcfg_netmask`
- `base_config_sysidcfg_nameservice`
- `base_config_sysidcfg_system_locale`
- `base_config_sysidcfg_terminal`
- `base_config_sysidcfg_timeserve`
- `base_config_sysidcfg_timezone`

- `base_config_sysidcfg_root_password`
- `base_config_sysidcfg_security_policy`
- `base_config_sysidcfg_protocol_ipv6`

The following list describes the parameters that are associated with the `base_config` JET module. These parameters provide basic operating system configuration information. Values for many of these parameters use the term `targetableComponent` to represent the target system.

- `base_config_client_allocation` – The mechanism used to build this client. By default, the options listed in `/opt/SUNWjet/etc/jumpstart.conf` are used. Leave the value blank unless you need to do something different from the default for this specific client. If you are provisioning the Solaris 10 1/06 x86 release, set the value of this variable to GRUB to enable GRUB-based booting and installation.
- `base_config_ClientArch` – Kernel architecture, such as `sun4u` or `x86`. By default, this is set to the kernel architecture of the `targetableComponent`.
  - Default Value – `[targetableComponent:kernel_arch]`
- `base_config_ClientEther` – Ethernet MAC address. By default, this is set to the Ethernet MAC address of the `targetableComponent`.
  - Default Value – `[targetableComponent:ethernet_mac_address]`
- `base_config_ClientOS` – Version of the OS to be provisioned.
  - Example – `Solaris9_u7_sparc`
- `base_config_dedicated_dump_device` – If set, the `dumpadm` utility configures the partition as a Dedicated Dump Device. See `dumpadm(1M)` for supported Operating Environments.
- `base_config_defaultrouter` – Value to use for `/etc/defaultrouter`.
- `base_config_disable_sysid_probe` – If set, skip the `sysid` step on the first reboot. This can significantly increase provisioning efficiency on systems that have many unused network adapters.
  - Default Value – `yes`
- `base_config_dns_disableforbuild` – Delay DNS configuration until later. If DNS is not available in the build environment, set this variable to `yes`.
- `base_config_dns_domain` – DNS domain entry for the `/etc/resolv.conf` file.
- `base_config_dns_nameservers` – Space-separated list of IP addresses to use for DNS name server entries in the `/etc/resolv.conf` file.
- `base_config_dns_searchpath` – List of entries to go in the DNS search line in `/etc/resolv.conf` file.
- `base_config_dumpadm_minfree` – Set a limit so that crash dumps do not fill up the dump file system. See the `dumpadm(1M)` `-m` option for possible values.
  - Example – `20000k`
- `base_config_enable_altbreak` – If set, enable alternate break sequence.
- `base_config_enable_rootftp` – If set to any value, enable root FTP access.
- `base_config_enable_rootlogin` – If set to any value, enable network root login from telnet, rsh, and ssh.



- `base_config_enable_savecore` – If set to any value, enable save core for Solaris 2.6 systems.
  - Default Value – `yes`
- `base_config_grub_append` – For Solaris 10 1/06 x86 systems, specifies additional options or arguments to pass to the GRUB bootloader.
- `base_config_ipmp_networkifs` – Space-separated list of interfaces to be defined under IPMP control. For each interface listed, define sets of variables to provide the `netgroup`, `mode`, `test1`, `test2`, `netmask`, host name, `log-ip`, `hostname2`, and `log-ip2` for the interface.
  - Example – `qfe0_qfe4!database-net 1 10.0.0.1 10.0.0.2 24 oracle-db 10.0.0.3 apache 10.0.0.4`
- `base_config_networkifs` – Space-separated list of additional network interfaces to be defined. For logical interfaces, use underscores (`_`) rather than colons (`:`). Use the format `c_ntndn`. For each interface listed, define sets of variables to provide the `netname`, `netmask`, host name, and IP address for the interface.
  - Example – `le1!netB 255.255.255.0 myhost-netB 192.168.1.0`
- `base_config_nfs_mounts` – Space-separated list of remote NFS mount points. Use `?` to separate the mount source from the mount target, as shown in the example.
  - Example – `fs?1.1.1.1:/fs`
- `base_config_nfsv4_domain` – Set up the NFSv4 domain to prevent being prompted at first reboot. If not set, look first for the entry in `base_config_dns_domain`, and second for the domain value in `/etc/default/nfs`.
- `base_config_noautosshutdown` – If set to any value, disable power management.
  - Default Value – `pm_disabled`
- `base_config_nodename` – Value to use for `/etc/nodename` if not the default host name.
- `base_config_notrouter` – If set to `y`, then disable IPv4 forwarding and create the `/etc/notrouter` file.
- `base_config_ntp_servers` – Space-separated list of names or IP addresses for the NTP servers. The first server will be given a `prefer` tag. This section places lines of the form: `server [prefer]` into the `/etc/inet/ntp.conf` file. For additional NTP control, use the custom module to deploy your own custom `ntp.conf` file.
- `base_config_patchdir` – Path to the patches. If blank, use information from the `jumpstart.conf` file and the IP address of the JET server. If your patch files are not stored on the JET server, then provide an NFS-style path to the location of the patches.
- `base_config_poweroff_afterbuild` – If set, shut down the system once the build completes.
- `base_config_productdir` – Path to the products. If blank, use information from the `jumpstart.conf` file and the IP address of the JET server. If your package files are not stored on the JET server, then provide an NFS-style path to the location of the packages.
- `base_config_products` – JET modules to provision.
- `base_config_profile` – Create your own custom JumpStart profile. By default, if you leave this variable blank, the OS provisioning plug-in creates the `/opt/SUNWjet/Clients/hostname/profile` based on the other `base_config_profile`

variables. Alternatively, you can create your own custom JumpStart profile. To use the profile that you created manually, set the `base_config_profile` variable to the name of the created profile. By default, the OS provisioning plug-in looks for the profile in the `/opt/SUNWjet/Clients/hostname` directory. To direct the plug-in to a profile in another directory, provide an absolute path name in the `base_config_profile` variable.

---

---

**Note:** If you are provisioning the Solaris OS on x86 target hosts, you must create a custom JumpStart profile that deletes any existing partitions, and point to that profile in the `base_config_profile` variable.

---

---

- `base_config_profile_add_clusters` – Space-separated list of cluster packages to add.
- `base_config_profile_add_geos` – Comma-separated list of geographical regions to add.
  - Example – `N_Europe, C_Europe`
- `base_config_profile_add_locales` – Comma-separated list of locales to add.
  - Example – `fr_FR, ja_JP.UTF-8`
- `base_config_profile_add_packages` – Space-separated list of packages to add.
- `base_config_profile_additional_disks` – A list of disks to use and configure in addition to the boot disk. Use the format `cntndn`. For each disk listed, define sets of variables for each slice to identify the mount point and the size.
- `base_config_profile_cluster` – Solaris software group package.
  - Default Value – `SUNWCreq`
  - Example –  
`SUNWCreqSUNWCuserSUNWCprogSUNWCallsSUNWCXallSUNWCrnet`
- `base_config_profile_del_clusters` – Space-separated list of cluster packages to remove.
  - Example – `SUNWCpm SUNWCpmx SUNWCdial SUNWCdialx`
- `base_config_profile_del_geos` – Comma-separated list of geographical regions to delete.
- `base_config_profile_del_locales` – Comma-separated list of locales to delete.
- `base_config_profile_del_packages` – Space-separated list of packages to remove. To prevent interactive installations on Solaris x86 headless target hosts, set this value to `SUNWxwssu SUNWxwscf`.
- `base_config_profile_dontuse` – A comma-separated list of disks that must not be used. Use the format `cntndn`. This variable applies only if `base_config_profile_usedisk` is not set.
- `base_config_profile_root` – Root space (free, or size in Megabytes)
  - Default Value – `free`.
- `base_config_profile_s3_mtpt` – Mount path to slice 3.

---

---

**Note:** If you are using VxVM and you want your boot disk to look like the mirror, then leave slices 3 and 4 empty.

---

---

- `base_config_profile_s3_size` – Size of slice 3 (in Megabytes).
- `base_config_profile_s4_mtpt` – Mount path of slice 4.
- `base_config_profile_s4_size` – Size of slice 4 (in Megabytes).
- `base_config_profile_s5_mtpt` – Mount path of slice 5.
  - Default Value – `/var`
- `base_config_profile_s5_size` – Size of slice 5 (in Megabytes).
- `base_config_profile_s6_mtpt` – Mount path of slice 6.
  - Default Value – `/usr`
- `base_config_profile_s6_size` – Size of slice 6 (in Megabytes).
- `base_config_profile_s7_mtpt` – Mount path of slice 7.

---

**Note:** If you are using Solaris Volume Manager (SVM), the default behavior is to use slice 7 as a location for metastate databases. If you are using the SVM default configuration, do not use slice 7 for data.

---

- Default Value – `/opt`
- `base_config_profile_s7_size` – Size of slice 7 (in Megabytes).
- `base_config_profile_swap` – Swap space (in Megabytes).
  - Default Value – 256
- `base_config_profile_usedisk` – Defines the boot disk onto which the OS will be loaded. Use the format `cntndn` or the keyword `rootdisk`. If the value is `rootdisk`, then the current boot disk will be used.
  - Default Value – `rootdisk`
- `base_config_shutup_sendmail` – If set, create an alias host name to disable sendmail.
  - Default Value – `yes`
- `base_config_sysidcfg_default_route` – Router IP address to use during JumpStart for Solaris 9 or later environments. If blank, will try to use value from the `defaultrouter_base_config` variable. If that is also blank, or for another net interface, JumpStart `sysidcfg` will get a router IP from the JET server.
- `base_config_sysidcfg_ip_address` – IP address to use at initial boot. By default, this is set to the IP address of the targetable component.
  - Default Value – `[targetableComponent:ethernet_ip_address]`
- `base_config_sysidcfg_nameservice` – Name service to configure at initial boot.
  - Default Value – `NIS`
- `base_config_sysidcfg_netmask` – Netmask to use at initial boot. By default, this is set to the netmask of the targetable component.
  - Default Value – `[targetableComponent:ethernet_netmask]`
- `base_config_sysidcfg_network_interface` – Network interface to use at initial boot.
  - Default Value – `NONE`
- `base_config_sysidcfg_protocol_ipv6` – Whether to use IPv6 protocol at initial boot.

- Default Value – no
- `base_config_sysidcfg_root_password` – Encrypted root password.
- `base_config_sysidcfg_security_policy` – Kerberos security policy to use at initial boot.
  - Default Value – NONE
- `base_config_sysidcfg_system_locale` – System locale to use at initial boot.
  - Example – `en_US.ISO8859-1`
- `base_config_sysidcfg_terminal` – Terminal emulator to set at initial boot.
  - Default Value – `vt100`
- `base_config_sysidcfg_timeserver` – Where to get system time for initial boot. If blank, system time comes from the JET server. Alternatively, you can set this variable to `localhost` to get the system time from the hardware clock on the client.
- `base_config_sysidcfg_timezone` – System time zone to use for initial boot.
  - Example – `US/Pacific`
- `base_config_sysidcfg_x86_kdmfile` – For Solaris x86 systems, specifies the name of a keyboard, display, and mouse configuration file to append to the `sysidcfg` file.
  - Default Value – `/sysidcfg-addon-file`
- `base_config_ufs_logging_filesys` – For Solaris 7 and later systems, a space-separated list of mount points to use for logging. To enable logging on all UFS file systems, use the keyword `all`. Solaris 9 09/04 enables logging by default. To disable logging on a specific file system, add a hyphen in front of the mount point. To disable logging on all file systems, use the keyword `none`.

---

---

**Note:** You cannot mix keywords and mount points. You can specify the root file system (`/`), although the root file system is included as part of the `all` and `none` keywords.

---

---

- Default Value – `all`
- `base_config_update_terminal` – If set, put the `sysidcfg` terminal type into `inittab`.
  - Default Value – `yes`
- `base_config_x86_confflags` – For Solaris 9 x86 systems, specifies arguments to be used with the `confflags` attribute of the `add_install_client` command.
  - Example – `-f -P /boot/solaris/dca`
- `base_config_x86_console` – For x86 systems, set the console to the correct tty port if you are not going to connect a keyboard and monitor to the client. Setting this variable enables you to perform installs through the serial port. For `b1600`, `v20z`, and `v40z` systems, use `ttya`. For `lx50`, `v60x`, and `v65x` systems, use `ttyb`.
- `base_config_x86_disable_acpi` – For x86 systems, any value disables ACPI. Disabling ACPI might make the installation process proceed better due to how the interrupts are handled.
- `base_config_x86_disable_kdmconfig` – For Solaris x86 systems, disables the `kdmconfig` interactive utility for configuring the keyboard, display, and mouse of the target host. If you are installing a Solaris OS with the GRUB bootloader, set this variable value to `yes`.

- `base_config_x86_nowin` – For x86 systems, prevents Solaris from trying to run Windows during the install.
  - Default Value – yes
- `base_config_x86_safetoreboot` – For x86 systems, controls whether the system automatically reboots. If your PXE boot is a one-time option, and the next reboot will attempt to boot from disk, you must set this option to yes.



An icon is a small picture or symbol on a user interface (UI) that represents an action or a state.

Oracle Enterprise Manager Ops Center has a variety of icons to represent an asset, the current state of an asset, and actions. A tool tip appears when you place the mouse over an icon. Tool tips provide brief descriptions of the icons that appear in Oracle Enterprise Manager Ops Center.

When an icon is grayed out, it means that the feature is not functional for the current scenario or you have not been assigned the role to perform the action.

## Administration Icons

Oracle Enterprise Manager Ops Center provides you with a variety of tools for understanding and managing your datacenter. The Administration icons are associated with actions that you use to configure and manage Oracle Enterprise Manager Ops Center. You can only enter or edit the cost of power in Administration. Following are the icons that are associated with Administration.

**Figure E-1 Register Enterprise Controller**



**Figure E-2 Ops Center Downloads**



**Figure E-3 Set Enterprise Controller Storage Library**



**Figure E-4 Setup Connection Mode**



**Figure E-5 Edit Authentications**



**Figure E–6 Proxy Deployment Wizard**



**Figure E–7 Configure Local Agent**



**Figure E–8 Self Diagnosis**



**Figure E–9 Unconfigure Enterprise Controller**



**Figure E–10 Change HTTP Proxy**



**Figure E–11 Edit Energy Cost**



**Figure E–12 Add User**



**Figure E–13 DHCP Config**



**Figure E–14 Subnets**



**Figure E–15 External DHCP Server**



**Figure E–16 Navigate to Selected Oracle VM Manager**



**Figure E–17 Discover Oracle VM Managers**





**Figure E–18 Discover Oracle VM Server****Figure E–19 Discover File Server****Figure E–20 Discover iSCSI Storage**

## Badges

Badges are special types of icons that appear in the corner of asset icons to show the status of the assets.

**Figure E–21 Critical Badge****Figure E–22 Warning Badge****Figure E–23 Info Badge****Figure E–24 Configure Badge****Figure E–25 Shutdown Badge****Figure E–26 Update Badge****Figure E–27 Lock Badge****Figure E–28 Unreachable Badge**

## Boot Environment Icons

A boot environment is an instance of a bootable Oracle Solaris image plus additional software packages that are installed onto the image, and the set of all file systems and devices (disk slices and mount points) that are required to operate an Oracle Solaris OS instance.

Following are the icons that are associated with Boot Environment.

**Figure E–29 Create New Boot Environment**



**Figure E–30 Activate Boot Environment and Reboot**



**Figure E–31 Active Boot Environment**



**Figure E–32 Active Boot Environment Upon Reboot**



**Figure E–33 Delete New Boot Environment**



**Figure E–34 Synchronize Boot Environment**



## Connectivity Icons

Connectivity icons display the session mode and connectivity. To determine if you run in Connected Mode and have access to My Oracle Support Services, check the icons in the upper right corner of the UI. If an icon is not colored, you are not in connected mode. The icons indicate:

- Whether or not Oracle Enterprise Manager Ops Center is connected to the Internet.
- Whether or not Oracle Enterprise Manager Ops Center is connected to the Oracle Knowledge Base.
- Whether or not Oracle Enterprise Manager Ops Center is connected to My Oracle Support Services.

**Figure E–35 My Oracle Support Services Connected**



**Figure E–36 My Oracle Support Services Disconnected**



**Figure E–37 Internet Connected**



**Figure E–38 Internet Disconnected****Figure E–39 Knowledge Base Connected****Figure E–40 Knowledge Base Disconnected**

## Group Icons

Group icons are icons that are associated with administrative structures that organize assets so that you can locate an asset quickly or perform operations on all assets of the same type.

**Figure E–41 Create Group****Figure E–42 Add Assets to Groups****Figure E–43 Remove Asset From Group****Figure E–44 Move Assets to Group****Figure E–45 Add Attribute Icon****Figure E–46 Add Rule Icon****Figure E–47 Delete Attribute Icon****Figure E–48 Delete Rule Icon**

## Hardware Icons

Hardware icons represent the various types of hardware that is used to manage the datacenter.

**Figure E-49 Blade Icon**



**Figure E-50 Chassis Icon**



**Figure E-51 CPU Icon**



**Figure E-52 Disk Controller Icon**



**Figure E-53 Disk Expander**



**Figure E-54 Ethernet Port Icon**



**Figure E-55 Fan Icon**



**Figure E-56 Fan Tray Icon**



**Figure E-57 Generic Hardware Icon**



**Figure E-58 Hard Disk Icon**



**Figure E-59 I/O Board Icon**



**Figure E-60 I/O Module Icon**



**Figure E-61** *Memory Icon*



**Figure E-62** *Memory Board Icon*



**Figure E-63** *PCI Icon*



**Figure E-64** *Power Control Setting Icon*



**Figure E-65** *Power Supply Setting Icon*



**Figure E-66** *System Icon*



**Figure E-67** *Utilization CPU*



**Figure E-68** *Utilization File System*



**Figure E-69** *Utilization*



**Figure E-70** *Utilization IO*



**Figure E-71** *Utilization Memory*



**Figure E-72** *Utilization Network*



**Figure E-73** *Utilization Swap Icon*



**Figure E-74 Utilization System Load Icon**



**Figure E-75 XSCF Icon**



## Incident Icons

Incident icons are icons that reflect the current state of the incidents.

**Figure E-76 View Alerts**



**Figure E-77 View Annotations**



**Figure E-78 View Possible Impacts and Causes**



**Figure E-79 View Comments**



**Figure E-80 View Suggested Actions**



**Figure E-81 Add Annotations**



**Figure E-82 Assign Incidents**



**Figure E-83 Acknowledge Incident**



**Figure E-84 Take Action on Incidents**



**Figure E-85 Mark Incident as Repaired**



**Figure E-86 Close Incident**

## Job Icons

Every action creates a job. Many jobs can run at the same time and some jobs take longer than others to complete. To follow the progress of a particular job, you can display the job details.

**Figure E-87 All Jobs****Figure E-88 Jobs In Progress****Figure E-89 Jobs Waiting For User Input****Figure E-90 Jobs Stopped****Figure E-91 Jobs Scheduled****Figure E-92 Jobs Partially Successful****Figure E-93 Jobs Suspended****Figure E-94 Jobs Failed****Figure E-95 Jobs Successful****Figure E-96 View Job Details**

**Figure E-97 Re-run Selected Jobs****Figure E-98 Display Selected Target Details****Figure E-99 Debug Jobs Using OCDoctor****Figure E-100 Mode Actual****Figure E-101 Delete Selected Jobs**

## Kernel Icons

The kernel is a program that constitutes the central core of a computer operating system. It has complete control over everything that occurs in the system.

**Figure E-102 Tree Node Icon**

## Library Icons

Libraries store and manage cached data, images, packages, and metadata. A software library stores images for provisioning operations. A Storage Library is a file system on the virtual host's server or it can be accessed through an NFS server or SAN network. Guest configurations for its operating system, data, CPU, memory, and network as metadata are stored in the storage library associated with the virtual host.

**Figure E-103 New Local Software Library****Figure E-104 New NAS Software Library****Figure E-105 New SAN Storage Library**



**Figure E-106 Set Enterprise Controller Storage Library**

## Message Center Icons

You can create, view, and manage service requests from the Oracle Enterprise Manager Ops Center user interface.

**Figure E-107 Open Service Requests****Figure E-108 Service Request Opened By Others****Figure E-109 My Service Requests****Figure E-110 Notifications****Figure E-111 Delete All Notifications****Figure E-112 My Incidents****Figure E-113 Unassigned Incidents**

## Monitoring Icons

Monitoring rules and policies define the monitoring parameters. Monitoring rules define the alerting conditions. Rules are associated with, and determined by, the type of managed resource. Monitoring rules state the values and boundaries for an asset's activity. A monitoring policy defines alert configurations to be performed on one or more managed resources. It contains the information needed to monitor a managed asset with user-defined alert configurations, including defined thresholds and alert monitors.

Below are the icons that are associated with monitoring rules and policies.

**Figure E-114 Add Alert Monitoring Rule**

**Figure E–115 Deselect All Rules**



**Figure E–116 Select All Rules**



**Figure E–117 Edit Alert Monitoring Rule**



**Figure E–118 Disable Alert Monitoring Rule**



**Figure E–119 Delete Alert Monitoring Rule**



**Figure E–120 Navigate to Monitoring Policy**



**Figure E–121 Applying a Monitoring Policy**



**Figure E–122 Extract a Monitoring Policy**



**Figure E–123 Create a New Monitoring Policy**



**Figure E–124 Copy Monitoring Policy**



**Figure E–125 Delete Monitoring Policy**



**Figure E–126 Set as Default Policy**



**Figure E–127 View Associated Assets**



## Network Icons

Oracle Enterprise Manager Ops Center manages networks for its virtual hosts. Guests in the network communicate with each other or with the Internet through these virtual hosts. Use networks to:

- Manage individual hosts
- Connect hosts to the Proxy Controller
- Allow guests to communicate with each other or with the Internet
- Connect remote JMX with the public API

Below are the icons that are associated with Network.

**Figure E-128** *Create Network Domain*



**Figure E-129** *Delete Network Domain*



**Figure E-130** *Connect Guests*



**Figure E-131** *Create Public Network*



**Figure E-132** *Manage Network*



**Figure E-133** *Edit Attributes*



## Operating System Icons

Operating system icons are icons that depict the type of operating system and the actions that are associated with the operating system.

**Figure E-134** *Linux Operating System Icon*



**Figure E-135** *Oracle Solaris Icon*



**Figure E-136 Oracle Solaris Cluster Icon**



**Figure E-137 Microsoft Windows Icon**



**Figure E-138 New Update OS Job**



**Figure E-139 Deploy/Update Software**



**Figure E-140 Reboot**



**Figure E-141 Attach Network**



**Figure E-142 Place in Maintenance**



**Figure E-143 Update Operating System**



## Oracle VM Server Icons

These are icons that are related to the functions for Oracle VM Server.

**Figure E-144 Oracle VM Server Pool**



**Figure E-145 x86 Server Pool**



**Figure E-146 LDOM SPARC**



**Figure E-147 LDOM Server Pool**



**Figure E-148 LDOM SPARC Server Pool**



**Figure E-149 Global Zone**



## Process Icons

These are icons associated to the processes of Oracle Enterprise Manager Ops Center.

**Figure E-150 CPU Tree Node Icon**



**Figure E-151 Memory Tree Node Icon**



**Figure E-152 Tree Node Icon**



## Report Icons

Reports let you gather information about your assets, such as job history, firmware, operating system updates, and incidents. You can export reports or use them to start jobs on targeted assets.

**Figure E-153 Create Windows Host Compliance Report**



**Figure E-154 Create Windows Incident Compliance Report**



**Figure E-155 View Host Compliance Report Result**



**Figure E-156 Rerun Report**



**Figure E–157 Delete Incident Compliance Report**



**Figure E–158 Run Report Template**



**Figure E–159 Report Pending to Run**



**Figure E–160 Create System Information Report**



**Figure E–161 Create Incident Summary Report**



**Figure E–162 Create Incident Detail Report**



**Figure E–163 Create Firmware Report**



**Figure E–164 Create Change History Report**



**Figure E–165 Create Baseline Report**



**Figure E–166 Create System Catalog Report**



**Figure E–167 Create CVE report**



**Figure E–168 Create Recommended Software Configuration Report**



**Figure E-169 Create Solaris Update Compliance Report**



**Figure E-170 Create Profile Report**



**Figure E-171 Create Exalogic System Report**



**Figure E-172 Compare Catalog Report**



**Figure E-173 Distribution Update Report**



**Figure E-174 Package Compliance Report**



**Figure E-175 Service Pack Compliance Report**



**Figure E-176 View CSV Output Icon**



**Figure E-177 View Interactive Output Icon**



**Figure E-178 View PDF Output Icon**



## SuperCluster Icons

SPARC SuperCluster is an Oracle Engineered System, which integrates SPARC compute nodes, a ZFS storage appliance, InfiniBand switches, and Exadata database Cells into a multi-rack system. Below are the icons that are associated with SuperCluster.

**Figure E-179 SuperCluster**



**Figure E-180 SuperCluster Cluster**



**Figure E-181 SuperCluster Node**



**Figure E-182 SuperCluster Partnership**



**Figure E-183 SuperCluster Quorum**



**Figure E-184 SuperCluster Zone Cluster**



**Figure E-185 SuperCluster Zone Cluster Node**



**Figure E-186 Oracle Solaris Cluster Upgrade**



## Switch Icons

Switch icons represent the hardware devices that join multiple computers within one local area network (LAN).

**Figure E-187 General Switch**



**Figure E-188 InfiniBand Icon**





**Figure E-189 10 GIG E****Figure E-190 Switch Reset****Figure E-191 Launch Switch UI**

## Universal Icons

Universal icons are icons that are associated with the most common functions or actions that are performed in the application.

**Figure E-192 Add Icon****Figure E-193 Delete Icon****Figure E-194 Deselect All Icon****Figure E-195 Select All Icon****Figure E-196 Power Off Icon****Figure E-197 Refresh Icon****Figure E-198 Start Icon****Figure E-199 Suspend Icon**

**Figure E–200 View Details Icon****Figure E–201 Go To Icon****Figure E–202 Shutdown**

## Update Policy Icons

Policies are lists of actions that are explicitly approved or denied. Policies are specific to operating system update and define the amount of user interaction you want when applying operating system patches and packages. Update policies define the component configuration of the system you want to update.

**Figure E–203 New Policy****Figure E–204 Import Policy**

## Update Profile Icons

Update profile icons are icons that are associated to the update actions that are carried out on a profile in a defined order.

**Figure E–205 Copy Icon****Figure E–206 New Profile Icon****Figure E–207 Delete Icon****Figure E–208 Import Profile****Figure E–209 Profile Install Packages**

**Figure E-210 Profile Uninstall Packages**





---



---

## Oracle Enterprise Manager Ops Center API

Oracle Enterprise Manager Ops Center exposes certain APIs. These APIs allow external systems management solutions to integrate with Oracle Enterprise Manager Ops Center. The APIs are remotely available using TCP/IP, through one of two secure protocols: JMXRemoting over TLS and WS-Management over https.

The Oracle Enterprise Manager Ops Center Software Developer's Kit (SDK), that is shipped with the Oracle Enterprise Manager Ops Center software, includes some examples that show how to use the public APIs.

To use the examples included in the package:

1. Locate the `SUNWxvmoc-sdk.pkg` package in the `dvd/<platform>/Product/components/packages/` directory on the DVD/Install Media.
2. Install the `SUNWxvmoc-sdk.pkg` package.
3. Locate the example you want. [Table F-1](#) lists the examples in the package.
4. Compile the example.
5. Execute the example, using the appropriate shell script.

**Table F-1** *Examples Included in the SUNWxvmoc-sdk.pkg Package.*

Example	Description	Code
Basic client example using JMX	<p>This example demonstrates the JMX Messaging Protocol (JMXMP) connector with Java/JMX technology. This example does not require any external JARs except Java and JDMK. This example performs the following functions:</p> <ul style="list-style-type: none"> <li>▪ Configures the connection.</li> <li>▪ Performs security settings.</li> <li>▪ Opens the connection (locally or remotely).</li> <li>▪ Uses the connection with JMX basic requests.</li> <li>▪ Closes the connection.</li> </ul>	BasicClient.java

**Table F-1 (Cont.) Examples Included in the SUNWxvmoc-sdk.pkg Package.**

<b>Example</b>	<b>Description</b>	<b>Code</b>
Domain model client example using WS-MAN	<p>This example demonstrates direct access to the read-only copy of the domain model. This example performs the following functions:</p> <ul style="list-style-type: none"><li>■ Configures the connection.</li><li>■ Performs security settings.</li><li>■ Opens the connection (locally or remotely).</li><li>■ Queries the domain model for all the server objects and displays the value of their model attributes.</li><li>■ Queries the domain model for all the OperatingSystems objects and displays the value of their description attributes.</li><li>■ Queries the domain model for all the ZoneController objects and displays the value of their ZoneControllerType attributes.</li><li>■ Queries the domain model for all the ISOImage objects and displays the value of their DiskImagePath attributes.</li><li>■ Queries the domain model for all the VirtServerImage objects and displays the value of their DomainFilePath attributes.</li><li>■ Closes the connection.</li></ul>	DomainModelClient.java
Basic client example using WS-MAN	<p>This example performs the same functions as the basic client with JMX example. However, this example uses the WS-MAN connector with Java/JMX technology.</p>	SimpleClient.java
Server services access example using WS-MAN	<p>This example demonstrates the server public services. This example performs the following functions:</p> <ul style="list-style-type: none"><li>■ Configures the connection.</li><li>■ Performs the security settings.</li><li>■ Opens the connection (locally or remotely)</li><li>■ Creates a proxy for each xVM server service to verify everything is working.</li><li>■ Displays the attribute values.</li><li>■ Lists the service tags.</li><li>■ Lists the nodes and their names.</li><li>■ Lists the xVM servers and displays some information on each one including the list of guests.</li><li>■ Closes the connection.</li></ul>	ServerClient.java ServerClientServices.java

---

**Table F-1 (Cont.) Examples Included in the SUNWxvmoc-sdk.pkg Package.**

<b>Example</b>	<b>Description</b>	<b>Code</b>
Services access using WS-MAN	<p>This example demonstrates specific Oracle Enterprise Manager Ops Center public services. This example performs the following functions:</p> <ul style="list-style-type: none"><li>■ Configures the connection.</li><li>■ Performs security settings.</li><li>■ Opens the connection (locally or remotely).</li><li>■ Creates a proxy for each specific service to verify everything is working.</li><li>■ Closes the connection.</li></ul>	<p>OpsCenterClient.java OpsCenterClientServices.java</p>
Discovery and agent provisioning example using WS-MAN	<p>This example demonstrates some Oracle Enterprise Manager Ops Center public services. This example performs the following functions:</p> <ul style="list-style-type: none"><li>■ Configures the connection.</li><li>■ Performs security settings.</li><li>■ Opens the connection (locally or remotely) with the satellite.</li><li>■ Uses the discovery service to discover one machine.</li><li>■ Registers the server asset for this machine.</li><li>■ Provisions the agent on this machine.</li><li>■ Unprovisions the agent on this machine.</li><li>■ Deletes both the server and operating system asset created for this machine.</li><li>■ Closes the connection.</li></ul>	<p>OCProvisionClient.java Utils.java</p>
Server example using WS-MAN	<p>This example demonstrates some Oracle Enterprise Manager Ops Center public services. This example performs the following functions:</p> <ul style="list-style-type: none"><li>■ Configures the connection.</li><li>■ Performs some security settings.</li><li>■ Opens the connection (locally or remotely) with the satellite.</li><li>■ Unattaches the xVM server if it is already attached.</li><li>■ Deletes the asset associated with the xVM server.</li><li>■ Uses the discovery service to discover one xVM server.</li><li>■ Attaches the xVM server to the Oracle Enterprise Manager Ops Center.</li><li>■ Closes the connection.</li></ul>	<p>OCXVMServer.java Utils.java</p>

---

## List of Public APIs

Table F-2 provides a brief description of the public APIs exposed by Oracle Enterprise Manager Ops Center. For a complete list of packages, its classes, interfaces, and methods, refer to the javadoc that is included in the SDK.

**Table F-2 List of Public APIs**

Package	Description
com.oracle.sysman.services.bios	Provides BIOS configuration services.
com.oracle.sysman.services.bootenvironment	Provides parameters for ABE related operations.
com.oracle.sysman.services.cloudmgmt	Provides virtual datacenter (vDC) administration and vDC management services.
com.oracle.sysman.services.common	Provides common constants and utility classes.
com.oracle.sysman.services.discovery	Provides services to perform discovery and manage discovery profiles.
com.oracle.sysman.services.exadatacell	Provides the service interface for exadata cell management.
com.oracle.sysman.services.network	Provides network domain services.
com.oracle.sysman.services.ocdoctor	Provides services for OCDoctor functionality in Ops Center.
com.oracle.sysman.services.ops	Provides Oracle pre-engineered system management services.
om.oracle.sysman.services.osanalytics	Provides services for operating systems and virtual server container analytics.
com.oracle.sysman.services.ovm	Provides services to perform operations on OVM deployments through the OVM manager.
com.oracle.sysman.services.rack	Provides rack management services.
com.oracle.sysman.services.reset	Provides the reset service interface to handle resetting and refreshing the service processor.
com.sun.xvm.services.agentprov	Provides service for managing the provisioning of agents. This package provides services for the installation, configuration, and removal of agent software to remote operating systems.
com.sun.xvm.services.agentupgrade	Provides the service interface for agent upgrades.
com.sun.xvm.services.alarm	Provides services for alarm management.
com.sun.xvm.services.authorization	Provides the operations for authorization management.
com.sun.xvm.services.bootenvironment	Provides the interface for boot environment service.
com.sun.xvm.services.cachemanager	Provides the service interface for managing the cached view of the domain model.



**Table F-2 (Cont.) List of Public APIs**

<b>Package</b>	<b>Description</b>
com.sun.xvm.services.cluster	Provides the service interface for cluster management. This service is responsible for viewing and managing Solaris cluster instances and their nodes.
com.sun.xvm.services.common	Provides the service interfaces that are common to different public API services.
com.sun.xvm.services.componentmgmt	Provides the service interface for hardware components management.
com.sun.xvm.services.datamodel	Provides the service for accessing low-level data models.
com.sun.xvm.services.deleteasset	Provides the service interface to delete assets such as servers, operating systems, service tags, and chassis. The virtualization assets such as hosts, guests, virtual image libraries, and networks can be removed by calling the appropriate methods on their respective services.
com.sun.xvm.services.discovery	Provides services to discover assets. The interface for discovery service provides capability to initiate a discovery operation for a set of IP addresses.
com.sun.xvm.services.event	Provides the interface for event service. The interface for event service allows the client to subscribe to notifications emitted from the domain model.
com.sun.xvm.services.fabricmgmt	Provides service interfaces for fabric management.
com.sun.xvm.services.fwdeployment	Provides services for firmware deployment management. This package manages deployments of firmware updates to servers and chassis.
com.sun.xvm.services.gear	Provides service tag and general gear management interfaces.
com.sun.xvm.services.grouping	Provides asset group management services.
com.sun.xvm.services.guest	Provides service interfaces for guest management.
com.sun.xvm.services.guest.provision	Provides service interfaces for guest provisioning.
com.sun.xvm.services.jobmanager	Provides job management services for performing job actions, controlling job status, and retrieving information on job actions and job history.
com.sun.xvm.services.migration	Provides the service interface for migration service. This package provides the service for live, warm and cold migration of guest domains.
com.sun.xvm.services.mos	Provides the My Oracle Support services.
com.sun.xvm.services.network	Provides the network management services. This package provides services for managing networks for guests.
com.sun.xvm.services.notification	Provides notifications management services.

**Table F-2 (Cont.) List of Public APIs**

<b>Package</b>	<b>Description</b>
com.sun.xvm.services.oemgc	Provides the service interface for OEM Grid Control repository integration.
com.sun.xvm.services.operation	Provides services for operation profile functionality.
com.sun.xvm.services.opscenter	Provides the service interface for XMV Update Job Manager.
com.sun.xvm.services.osdeployment	Provides services and types to manage deployment of operating systems to servers. This package provides services to access aggregated and detailed information on installed operating systems, monitor OS activity, and provision OS. This package is available only in Enterprise Controllers.
com.sun.xvm.services.osmonitoring	Provides the parameters for OS monitoring profile value object creation.
com.sun.xvm.services.pis	Provides the product and asset information service and types interfaces, used to classify assets according to their product name and hierarchy.
com.sun.xvm.services.productupdate	Provides the service interface to download update catalog files and bundles.
com.sun.xvm.services.profile	Provides the profile services to create, delete, and update profiles.
com.sun.xvm.services.provisioning	Provides services for managing server provisioning.
com.sun.xvm.services.proxysservice	Provides service for managing the provisioning of proxys.
com.sun.xvm.services.report	Provides services and types for retrieving reports on utilization trend.
com.sun.xvm.services.reportsmanager	Provides services interfaces for the report manager.
com.sun.xvm.services.storageemgmt	Provides service interfaces for storage server management.
com.sun.xvm.services.svrmgmt	Provides service interfaces for server management.
com.sun.xvm.services.switchmgmt	Provides the physical and virtual switch management service interface.
com.sun.xvm.services.topology	Provides the topology service and types interfaces to get topology information of the managed resources. This package provides a tree-based navigation view of the Ops Center assets.
com.sun.xvm.services.user	Provides the services to manage user preferences.
com.sun.xvm.services.virtimagelib	Provides the services for virtual images library and virtual image management.

**Table F–2 (Cont.) List of Public APIs**

Package	Description
com.sun.xvm.services.virtpool	Provides the service for managing the life cycle of virtual pools sharing the same libraries or networks, and have the same processor architecture, integrating virtual pools with storage, networks, and virtualization hosts.
com.sun.xvm.services.virtservercontainer	Provides the service interface for managing virtualized server containers.
com.sun.xvm.services.win	Provides filters supported for Windows services.
com.sun.xvm.services.winpm	Provides service interfaces for Windows compliance reports and Windows software updates deployment.
com.sun.xvm.services.wme	Provides the service interface for Windows management extension administration.
com.sun.xvm.services.xvmserver	Provides the XVM server management service for managing the system level aspects of the XVM server.

## Public API Access

There are two ways of accessing public APIs:

- [Public API Access Through JMX-Remoting](#)
- [Public API Access Through WS-Management](#)

## JMX

Java Management Extensions (JMX) technology provides the tools for building distributed, modular, and dynamic solutions for managing and monitoring devices, applications, and networks. The JMX API defines the notion of MBeans, or manageable objects, which expose attributes and operations in a way that allows remote management applications to access them. An important new feature of the JMX API in the Java Platform, Standard Edition 7 (Java SE 7) is its ability to create MXBeans, a substantial improvement over Standard MBeans. For more information on JMX, visit the Java Management Extensions (JMX) Technology website at <http://www.oracle.com/technetwork/java/javase/tech/javamanagement-140525.html>.

## WS-Management

Web Services for Management (WS-MAN) is a specification for managing servers, devices, and applications using web services standards. It provides a common way for systems to access and exchange management information across the entire IT infrastructure. It is commonly used in the Windows management stacks, and is supported by Microsoft management tools, including the winrm command-line interface and COM objects that can be used from Visual Basic or from C#.

## Public API Access Through JMX-Remoting

The simplest and preferred way of interacting with the public APIs is using a Java client. This Java client communicates with the public APIs using a secure remote JMX

client. By using a remote JMX client, it is possible to directly interact with the Service MBeans in Java using the strongly-typed Java MBeans interface class library. The JMX MBean interfaces are documented in the javadoc that is included in the SDK. The following remote JMX management protocols are supported: JMXMP and WS-MAN.

## Public API Access Through WS-Management

The public API MBeans are exposed over WS-Management through JSR-262. This specification defines a way to use Web Services to access JMX instrumentation remotely. Clients do not have to be Java applications, but can be. This permits a generic WS-Management client to interact with the public APIs. The WS-Management mappings for each service tier API is documented in the javadoc that is included in the SDK.

## Virtualization Management Stack

The virtualization management stack is a three-tier management paradigm. The stack consists of presentation tier, service tier, and an underlying domain model.

### Presentation Tier

The presentation tier provides the user interface, displays the information provided by the service tier, and takes actions through the service tier.

### Service Tier

The service tier contains all the core management logic. This tier exposes the management functionality through a set of public APIs that are used by the presentation tier and external systems management solutions. These public APIs are the ideal integration points for third-party software to control or to monitor the Enterprise Manager Ops Center software.

The service tier exposes its management APIs as a series of Java Management Extensions (JMX) MBean interfaces. These interfaces are made accessible as public APIs through several remote protocols, including JMXRemoting (JSR 160) and WS-Management (JSR 262).

The services are identified by MBean ObjectName, and these are of the form:

```
com.sun.xvm.services:type=<service name>
```

The main entry point to the public APIs is the MBean interface defined in `com.sun.xvm.services`.

### Domain Model

The domain model provides the representation of underlying managed resources and associations between them. The domain model exposes a normalized data model of these managed resources as a collection of JMX MBeans. There is one MBean for each managed resource, and one for each association between these resources.

---

---

# Glossary

## **Account**

An account entitles designated cloud users the right to use computing, network, and storage resources of vDC. The account provides the required capabilities to manage these resources. It defines the amount of vCPU, memory and storage resources that can be used from the available vDC resources.

## **Action Pane**

The Actions pane is used to start jobs based on the current selection in the Navigation pane. Selections in the Navigation pane or center pane change the display of operations in the Actions pane. The Actions pane is subdivided into four sections – Operate, Organize, Deploy, and Update.

## **Active**

Reflects the state of system and indicates whether monitoring is actually being performed. The active state is not editable. When a rule is not enabled, monitoring is not active. The status is displayed on the Alert Monitoring Rules page, which is accessed from the Monitoring tab. Text in the Active field indicates whether the parameter is active.

## **Activate**

Changes an inactive Oracle Solaris boot environment to the new default boot environment on reboot.

## **Agent Controller**

The Agent Controller software communicates with the Enterprise Controller and is installed automatically when an asset is discovered to make the asset a managed asset. You can choose to manage resources remotely with proxy resources without putting an agent on the system. Some features of the product don't work without the agent, but discovery manages the assets without putting an agent on them.

## **Agentless**

A system that is managed with Oracle Enterprise Manager Ops Center without the Agent Controller software being installed.

## **Alert Monitor**

Monitors the state of managed resources and their attributes and raise an alert when the state is outside the pre-defined thresholds.

## **Alternate Boot Environment**

An alternate boot environment, or ABE, is an inactive Oracle Solaris boot environment.

**Annotations**

Annotations are scripts or comments that you can associate with a incident. Annotations can be automated operations to solve a incident, a suggested action, or a comment. You can associate an annotation with a specific incident. Annotations can be added to the Incidents Knowledge Base.

**Assemblies**

Assemblies are kind of infrastructure templates that contain a configuration of multiple virtual machines with their virtual disks and the inter connectivity between them. Assemblies can be created as a set of .ovf (Open Virtualization Format) and .img (disk image) files, or may all be contained in a single .ova (Open Virtualization Format Archive) file.

**Assets**

Assets are physical or virtual piece of hardware, storage device, or operating system that you can manage with Oracle Enterprise Manager Ops Center.

**Auto-Balancing Policy**

An auto-balancing policy determines if, and how, a server pool is automatically load balanced. By default, automatic balancing is not selected. When you designate the server pool for automatic balancing, the software reviews the load on the virtualization hosts for the interval and day that you request. The software then migrates the guests, as needed, to balance the load. You can require administrator approval before the guests are moved. Also see placement policy and policy.

**Bandwidth Flow**

Bandwidth flow is the speed of a connection, or the amount of data that flows from a site's server out to the viewer at any given time.

**Baseline**

A dated collection of Oracle Solaris patches, patch metadata, and tools. Oracle releases Solaris baselines on a monthly basis. You can use the black lists and the white lists to modify a baseline and create a custom patch set.

**Baseline Check**

Baseline check is a feature of Oracle Enterprise Manager Ops Center Engineered Systems where the factory setup of eighth, quarter, half, and full rack configurations are considered as a normal or ideal setup. When the assets are discovered and associated with the rack, this setup is compared with the normal factory setup.

**Black List**

A list of Oracle Solaris operating system patch IDs that you never want to apply to an asset. The black list is used when you are using a baseline to update an Oracle Solaris operating system.

**Block Storage**

A block storage library consists of LUNs (Logical Unit Number). Each LUN is a slice of a storage volume, which is storage space provided by a collection of disks.

**Boolean Control Parameter**

A monitoring rule that uses a true-false check.

**Boot Environment**

A collection of mandatory file systems (disk slices and mount points) that are critical to the operation of the Oracle Solaris operating system. These disk slices can be on the same disk or distributed across multiple disks.

**Branded Zone**

Zones that are capable of emulating user environments from operating systems other than Oracle Solaris 10. It supports different versions of Oracle Solaris operating system in the zones for running applications.

**Category**

For Oracle Enterprise Manager Ops Center's Local Content, a category is the type of software that is uploaded to Oracle Enterprise Manager Ops Center for use at a site. The parent category is one of the types defined in Oracle Enterprise Manager Ops Center. The local category is a category defined for the site, for example a script for a quarterly inventory.

**Channel**

An operating system distribution, such as Oracle Solaris 10 5/09 on x86 platform or Oracle Linux 5.5. A channel is also called a distribution.

**Cloud**

A cloud is a set of physical resources that can be divided and allocated to multiple users who can in turn create and use virtual resources as needed without impact to or awareness of the other users' resources. A cloud is implemented as a pool of servers sharing the same virtualization type, storage, networks and fabrics.

**Cluster Heartbeat**

Cluster heartbeat is used to verify if the Oracle VM Servers in a clustered server pool are up and running. The heartbeat function has a network component, where a TCP/IP communication channel is created with each Oracle VM Server. Each Oracle VM Server sends regular keep-active packets and these packets are used to determine if each Oracle VM Server is active.

**Connected Mode**

This is the default connection mode for Oracle Enterprise Manager Ops Center. With this mode, patch data is regularly downloaded from Knowledge Base through an Internet connection.

**Control Domain**

A domain that is created when Oracle VM Server for SPARC software is installed. The control domain contains the software packages for Oracle VM Server, including the domains manager application and the domains manager daemon (ldmd) process required for managing the logical domains. The interface to the hypervisor is through the domains manager. The control domain enables you to create, and manage logical domains and allocate virtual resources to the domains.

**Critical File System**

File systems that are required by the Oracle Solaris operating system. When you use Solaris Live Upgrade, these file systems are separate mount points in the `vfstab` file of the active and inactive boot environments. Example file systems are `root`, `/usr`, `/var`, and `/opt`. These file systems are copied from the source to the inactive boot environment.

### **Dashboard**

Displays a high-level overview of an asset or a group of assets on the user interface. The information of the selected asset or group is displayed in the Center Pane.

### **Deployment Plans**

Defines the sequence of steps that must be carried out on an asset to deploy. It also includes the specification or profile that each step should apply, and the resources that are required to apply it such as network addresses, host names and so on. Customized deployment plan enables you to perform hardware, firmware and operating system provisioning activities in a repeatable fashion.

### **Disconnected Mode**

This is the alternate connection mode for Oracle Enterprise Manager Ops Center. Instead of relying on an Internet connection for updates, patch data is acquired using the harvester script and moved to the Enterprise Controller.

### **Discovery**

This is the method for adding assets to Oracle Enterprise Manager Ops Center. Assets can be discovered using a variety of protocols, by their service tags, or by declaring hardware so that it can be configured and provisioned with an operating system.

### **Distribution**

For an operating system, a distribution is a specialized version of the operating system.

### **Distribution Groups**

Distribution groups are defined especially for Oracle Exalogic system based vDCs. Place your vServers in a distribution group and ensure that no two vServers run on the same Oracle VM Servers.

### **Domain Name Service (DNS)**

DNS is a network protocol that issues IP addresses within a specified range to devices on the network.

### **Dynamic System Domains**

In M-Series servers, you can partition the available hardware resources into smaller logical systems called as dynamic system domains. Dynamic System Domains run their own copies of the operating system and offer a very high level of isolation from other domains in the system because the partitioning occurs at the hardware level.

### **Dynamic Storage Library**

When the block storage library uses LUNs constructed from a storage array that is a managed asset, the block storage library is dynamic. You can add storage capacity as needed by adding LUNs supplied by the storage array.

When the block storage library relies on a storage array that is not a managed asset, the block storage library is static. Because Oracle Enterprise Manager Ops Center has less information about the storage array, you cannot increase the number of LUNs in the storage library.

### **Enabled**

A monitoring rule that is enabled is actively monitoring a parameter. By default, all rules are enabled. Users can disable and enable parameters on a per asset or group basis. The status is displayed on the Alert Monitoring Rules page, which is accessed



from the Monitoring tab. Text in the Enabled field indicates whether the parameter is enabled.

### **Enterprise Controller**

This is the central server for Oracle Enterprise Manager Ops Center software. The Enterprise Controller hosts the user interface and communicates with the Knowledge Base. It stores management information, such as firmware and operating system images, plans, profiles, and policies. It also stores the asset data and site customizations. All operations, or jobs, are initiated from the Enterprise Controller.

### **Enumerated Control Parameter**

A monitoring rule that uses a series of values.

### **Expression Parameter**

A monitoring rule that uses an instruction to execute something that returns a value.

### **/etc Directory**

The directory that contains critical system configuration files and maintenance commands.

### **/etc/netboot Directory**

The directory on a WANboot server that contains the client configuration information and security data that are required for a WANboot installation.

### **/export File System**

A file system on an operating system server that is shared with other systems on a network. For example, the /export file system can contain the root ( / ) file system and swap space for diskless clients and the home directories for users on the network. Diskless clients rely on the /export file system on an operating system server to boot and run.

### **Fabrics**

Fabrics are network topologies where network nodes connect with each other through one or more network switches. A true fabric provides a direct connection between any two ports, and supports single step/lookup-based processing. Regardless of its various components, a fabric appears on the outside as a single, logical device with a single, consistent state.

The term is popular in telecommunication, Fibre Channel storage area networks, and other high-speed networks, including InfiniBand.

### **Filesystem Storage**

A software or storage library that relies on a file system on the Enterprise Controller's system or a shared file system on an NFS server that the Enterprise Controller mounts.

### **Global Zone**

In Oracle Solaris Zones, the global zone is both the default zone for the system and the zone used for system-wide administrative control. The global zone is the only zone from which a non-global zone can be configured, installed, managed, or uninstalled. Administration of the system infrastructure, such as physical devices, routing, or dynamic reconfiguration (DR), is only possible in the global zone. Appropriately privileged processes running in the global zone can access objects associated with other zones.

### **Group**

A group is a user-defined set of assets. Assets can be added to groups based on asset attributes such as type or location. A group can include other groups. Assets can be manually added in addition to the rules based addition using attributes. Any type of asset that can be in a group can be added manually to any user-defined asset group.

### **Guest**

Guest refers to a virtual machine that is configured and installed in a virtualization host. For example, the logical domains in an Oracle VM Server host are referred to as guests in a server pool.

### **GUID**

Globally Unique Identifier. A pseudo-random 128-bit number that is computed by Windows to identify any component in the computer that requires a unique number. In Oracle Enterprise Manager Ops Center, GUIDs are used to identify LUNs.

### **Hardware Virtualization (HVM)**

Hardware virtualization is a technology that is used to create multiple virtual systems on a single piece of physical hardware. When you create a hardware virtualized (HVM) guest, you must supply an ISO file in a repository to create the virtual machine.

### **Hardware Virtualized with Paravirtualized Drivers (PVHVM)**

PVHVM is identical to HVM, but with additional paravirtualized drivers for improved performance of the virtual machine. This is used to run Microsoft Windows guest operating system with an acceptable performance level.

### **Host Name**

The name by which a system is known to other systems on a network. This name must be unique among all the systems within a particular domain (usually, this means within any single organization). A host name can be any combination of letters, numbers, and dashes ( - ), but it cannot begin or end with a dash.

### **Hypervisor**

A hypervisor is the software that enables multiple virtual machines to be multiplexed on a single physical machine. The hypervisor code runs at a higher privilege level than the supervisor code of its guest operating systems to manage use of the underlying hardware resources by multiple supervisor kernels.

### **Image Packaging System (IPS)**

Image Packaging System is an Oracle Solaris 11 package that contains operating system components and a manifest that provides basic metadata.

### **Incident**

An event that triggers an alert when a monitored attribute does not meet the monitoring parameters. A new incident is displayed in the Unassigned Incidents queue in the Message Center. From the Message Center you can view and act on incidents.

### **Incident Knowledge Base**

A custom database of annotations that are associated with known incidents.

**InfiniBand**

InfiniBand is a switched fabric communications link primarily used in high-performance computing. Its features include quality of service and failover, and it is designed to be scalable. The InfiniBand architecture specification defines a connection between processor nodes and high performance I/O nodes such as storage devices.

InfiniBand transmission rates begin at 2.5 GBps.

**IPMP**

IPMP (IP network multipathing) provides physical interface failure detection and transparent network access failover. You can configure one or more physical interfaces into an IP multipathing group, or IPMP group. After configuring IPMP, the system automatically monitors the interfaces in the IPMP group for failure.

**JET Templates**

JumpStart Enterprise Toolkit provides a framework to simplify and extend the JumpStart functionality provided within the Oracle Solaris operating system. You can use JET to install Oracle Solaris on the SPARC and x86/64 platforms. You create JET templates to customize the operating system configuration options as required.

**JMX**

Java Management Extensions (JMX) technology provides the tools for building distributed, modular, and dynamic solutions for managing and monitoring devices, applications, and networks. The JMX API defines the notion of MBeans, or manageable objects, which expose attributes and operations in a way that enables remote management applications to access them. The public API in Oracle Enterprise Manager Ops Center can be accessed through JMX-Remoting.

**Knowledge Base**

The Knowledge Base is the repository for metadata about Oracle Solaris and Linux operating system components. It stores information about patch dependencies, patch compatibilities, withdrawn patches, downloads, and deployment rules. It stores URL of operating system vendor download sites and downloads the components at set intervals. The Enterprise Controller must have Internet connection to connect to the Knowledge Base.

**Least Allocated**

Least allocated is a parameter in the server pool placement policy. The lowest allocated CPU and memory is the total static resource allocation across all guests on the virtualization host. The other placement policy parameter is relative load.

**Libraries**

A collection of virtual machine images and disk images that are located under the same file system. When a server pool is created, one or more libraries are assigned to the server pool. Server pools can share the same libraries.

**Link Aggregation**

Link aggregation is a standard defined in IEEE802.3ad. An aggregated link consists of several interfaces on a system configured as a single, logical unit. Link aggregation increases the speed and high availability of a connection between a server and a switch.

**LUN**

LUN stands for Logical Unit Number. In storage, a LUN is the number assigned to a SCSI protocol entity, that handles (I/O) operations. A SCSI target provides a LUN for each storage volume.

**Management**

An asset is managed when Oracle Enterprise Manager Ops Center can monitor it and target it with jobs. Operating systems can be managed with or without an Agent Controller, but operating system update functions are only available with an Agent Controller.

**Manifest**

Each Oracle Solaris 11 package has an associated manifest that describes how the package is put together. The package manifest provides basic metadata about the package (such as name, description, version, and category), what files and directories are included, and the package dependencies.

**Membership Graph**

Shows a graphical relationship between assets and status of the connection. A blue line shows the working connection and a red line represents the faulted or disconnected status. The membership graph is displayed in the Center Pane.

**Message Center**

Displays all incidents, alerts, and notifications. It helps you to view and manage incidents, notifications, and service request, and display warranty information.

**MTU**

MTU stands for Maximum Transmission Unit. MTU is the largest packet size, in bytes, that can be sent over a network.

**Monitoring Policy**

A set of monitoring rules that defines alert conditions. Policies are either system-defined, user-defined, or generic. Each monitoring policy contains one or more alert monitors for a specific type of resource. An alert is raised when the state is outside the pre-defined condition.

**Monitoring Rule**

Contains monitoring parameters that state the values and boundaries for an asset's activity. The set of rules is called a monitoring policy.

**MPxIO**

MPxIO provides a multipathing solution for storage devices accessible through multiple physical paths. MPxIO is included as a part of the distribution in Solaris 10 onwards.

**NAT**

NAT stands for Network Address Translation. NAT is a protocol that enables a network to use many internal-only IP addresses and a few Internet-facing IP addresses.

**Navigation Pane**

Navigation pane is an important part of the user interface of Oracle Enterprise Manager Ops Center. It contains Message Center, Assets, Plan Management,

---

Networks, Libraries, Reports, vDC Management, and Administration. The Assets section of the Navigation pane lists all the asset that are managed by Oracle Enterprise Manager Ops Center, grouped by its type and the required criteria.

**Network**

A network enables guests to communicate with each other or with the external world (that is, the Internet). When a server pool is created, one or more networks is assigned to the server pool. Server pools can share the same networks.

**Network Bonding**

Network bonding refers to the combination of network interfaces on one host for redundancy and/or increased throughput. Redundancy is the key factor you use to protect your virtualized environment from loss of service due to failure of a single physical link. This network bonding equals as the Linux network bonding. Using network bonding in Oracle VM might require some switch configuration.

**Network Domain**

A system of centralized network administration, in which the permissions that grant access to resources in the network are maintained in one or more servers. Network Domains use a hierarchical structure that enables you to assign permissions to collaborate with different departments in an organization.

A large network may have several domains based on the needs of each set of users.

**NIS**

NIS stands for Network Information System. NIS is a network naming and administration system for smaller networks. NIS is similar to the Internet's domain name system (DNS) but designed for a smaller network.

**Non-global Zone**

A virtualized operating system environment created within a single instance of the Oracle Solaris operating system. One or more applications can run in a non-global zone without interacting with the rest of the system. Non-global zones are also called zones.

**Non-Sparse Copy**

A clone of the type "non-sparse copy" is a disk image file of a physical disk, taking up the space equivalent to the full specified disk size, including empty blocks.

**Notifications**

An email, pager, or user interface message that is automatically sent by Oracle Enterprise Manager Ops Center when specified conditions are met. You can configure separate notification profiles for different assets and different users. You can configure the software to send notification for specific incidents, or when a critical or warning incident is detected.

**Opaque Data**

An opaque data is a data type that is incompletely defined in an interface, so that its values can only be manipulated by calling subroutines that have access to the missing information.

**/opt**

A file system that contains the mount points for third-party and unbundled software.

### **Oracle Enterprise Manager Cloud Control**

Oracle Enterprise Manager Cloud Control is a single, integrated solution for managing all aspects of the Oracle Cloud and the applications running on it. Oracle Enterprise Manager Cloud Control couples a potent, top-down monitoring approach to delivering the highest quality of service for applications with a cost-effective automated configuration management, provisioning, and administration solution.

### **Oracle Engineered System**

Oracle Engineered Systems are hardware and software integrated systems that are designed for a specific enterprise purpose. It helps in reducing the cost and complexity of the IT infrastructures, and increases the productivity and performance.

### **Oracle Services**

Provides integrated methods of maintaining and displaying current contracts, warranty information, contract dates, and service requests in Oracle Enterprise Manager Ops Center.

### **Oracle Solaris Clusters**

Oracle Solaris Clusters is a high availability software product for Solaris operating system. It is used to improve the availability of software services such as databases, file sharing on a network, electronic commerce web sites, or other applications. You can now manage Oracle Solaris Clusters as any other asset using Oracle Enterprise Manager Ops Center.

### **Oracle Solaris Zones**

Oracle Solaris Zones is a software partitioning technology used to virtualize operating system services, and provide an isolated and secure environment for running applications. When you create a non-global zone, you produce an application execution environment in which processes are isolated from all other zones. This isolation prevents processes that run in a zone from monitoring or affecting processes that run in any other zones. See also global zone and non-global zone.

### **Oracle Solaris 11 Software Update Library**

Oracle Solaris 11 Software Update Library repository is located on the Enterprise Controller. It contains the Oracle Solaris 11 packages that you need to install, provision, and update your Oracle Solaris 11 operating system.

### **Oracle VM Server for SPARC**

Oracle VM Server is a virtualization technology that enables the creation of multiple virtual systems by a hypervisor in the firmware layer, interposed between the operating system and the hardware platform. It is designed to abstract the hardware and can expose or hide various system resources, allowing for the creation of resource partitions that can operate as discrete systems, complete with virtual CPU, memory and I/O devices.

Oracle VM Server for SPARC was previously known as Logical Domains, It is a virtualization technology designed to run on CMT based servers.

### **Oracle VM Server for x86**

Oracle VM Server for x86 is a managed virtualization environment or part of such an environment, that is designed to provide a lightweight, secure, server-based platform for running virtual machines. Oracle VM Server for x86 is based upon an updated version of the underlying Xen hypervisor technology, and includes Oracle VM Agent.

**Oracle Solaris ZFS**

An Oracle Solaris operating system file system that uses storage pools to manage physical storage.

**Paravirtualization**

Paravirtualization enables you to select a location for the mounted ISO file from which you create the virtual machine. Before you create the virtual machine using the paravirtualized method, you must mount the ISO file on an NFS share, or HTTP or FTP server.

**Parent Repositories**

Any hosted Oracle repository that Oracle Solaris 11 Software Update Library can use to upload, or sync, content.

**Photorealistic View**

Photorealistic view displays the front and rear views of the rack. All slots and the respective assets are displayed. Positions within the rack are displayed in a 2-dimensional view. All assets in the rack have a specific image. The health status of assets such as OK, Warning, and Critical are displayed in the form of colored buttons.

**Placement Policy**

Determines whether the guest is placed on a virtualization host with the lowest relative load or the least allocated. By default, new guests are placed on the server with the lowest load and are automatically started. The placement policy is defined when a server pool is created. Server pools can have different placement policies.

**Policy**

Defines how a job is performed and sets the automation level of the job. A policy file is similar to a response file. If there is a conflict between a profile and policy, the profile overrides the policy.

**Private vNet**

vNet that is unique to a given account is called Private vNet.

**Profile**

Defines the configuration of components for a specific type of system. By using a profile, you can define what is enabled, and not enabled, to be installed on a system. If there is a conflict between a profile and policy, the profile overrides the policy.

**Proxy Controller**

Proxy Controllers link the managed assets to the Enterprise Controller and act as proxies for operations that must be located close to the managed assets, such as operating system provisioning. Proxy Controllers distribute the network load and provide for fan-out capabilities to minimize network load. Proxy Controllers perform management operations on assets and report the results to the Enterprise Controller. An Oracle Enterprise Manager Ops Center installation must have at least one functioning Proxy Controller.

**Relative Load**

Relative load is a parameter in the server pool placement policy. Lowest relative load is based on the lowest memory and CPU utilization for the virtualization host over the past three weeks. The other placement policy parameter is least allocated.

## **Repository**

A repository is a central place that stores an aggregation of data in an organized way, usually in a computer storage. Depending on how the term is used, a repository may be directly accessible to users or may be a place from which specific databases, files, or documents are obtained for further relocation or distribution in a network.

## **Root**

The top level of a hierarchy of items. `root` is the one item from which all other items are descended. See `root` directory or `root ( / )` file system.

## **Root Directory**

The top-level directory from which all other directories stem.

## **Root File System**

The top-level file system from which all other file systems stem. The `root ( / )` file system is the base on which all other file systems are mounted, and is never unmounted. The `root ( / )` file system contains the directories and files critical for system operation, such as the kernel, device drivers, and the programs that are used to boot a system.

## **RPM**

A package manager used by many versions of the Linux operating system.

## **Rule Parameters**

Define the monitoring parameters. The following types of rule parameters are available: Threshold, Boolean Control, Enumerated Control, and Expression. Some parameters are editable. All active parameters can be disabled.

## **SAN Storage Library**

Storage Attached Network (SAN) storage which is used for providing storage spaces for managed assets in Oracle Enterprise Manager Ops Center. The SAN storage library consists of groups of LUNs.

## **Script**

A command file that is associated with one of Oracle Enterprise Manager Ops Center's actions, either before the action occurs (pre-action script), or after the action completes (post-action script).

## **Security Group**

The organization of users and other domain objects into groups for easy administration of access permissions is known as a security group. A Security Group enables you to specify certain security settings on an instance specific basis. You have the ability to filter traffic based on IP's (a specific address or a subnet), packet types (TCP, UDP or ICMP), and ports (or a range of ports). You can also grant access to an entire security group. It enables your trusted computers to access each other without having to open ports to the public.

## **Server Management**

Server management is used to manage the physical Oracle VM Servers in a server pool, for example, to update the Oracle VM Agent on the different Oracle VM Servers.



**Server Pool**

A server pool is a resource pool of virtualization hosts that share compatible chip architecture, which facilitates actions such as moving guests between virtualization host instances. Members of the server pool have access to the same network and storage library resources. Guests can access the images contained in the server pool's library. Several server pools can share the same network and library storage resources.

**Server Templates**

Server templates provide pre-built images for creating vServers. They can be uploaded individually or as part of an Assembly. Server templates can be created from an existing vServer.

**Service Tag**

Service tags are XML files that identify assets uniquely. Assets with service tags can be discovered using the Find Assets wizard.

**Snapshot**

Snapshot is a point in time image of a Volume. It is a non-bootable copy of a boot environment that uses much less disk space than a boot environment. You can create a boot environment from a snapshot.

**Software Libraries**

A software library can be a local file system on the Enterprise Controller or a mount point on an NFS server. The software library is used to store the operating system images for provisioning, branded images, flars, firmwares, profiles, operating system updates, custom programs and scripts.

**Sparse Copy**

A clone of the type "sparse copy" is a disk image file of a physical disk, taking up only the amount of space actually in use; not the full specified disk size.

**Static Route**

Specifies the route taken by the network for external access. You define a default gateway for the network; however, this default gateway may not be reachable to a given subnet. In this case, you must add a static route for this specific subnet.

**Status Pane**

The Status pane in the Jobs section describes about the state of the incidents like jobs in progress, jobs failed, jobs partially successful, jobs stopped, jobs schedules, jobs successful and so on.

**SCCM**

Microsoft System Center Configuration Manager (SCCM), is used to update Windows operating systems.

**Syncing**

Syncing is the process of reconfiguring or updating the Oracle Solaris 11 Software Update Library with the Oracle Solaris 11 Image Packaging System (IPS).

**Synchronizing**

Updates an inactive boot environment to match an active boot environment.

### **System Groups**

Default asset groups that automatically organize your assets by type in the user interface.

### **System-defined Rules**

Attribute specific monitoring rules that are hard-coded into drivers. You can disable a system-defined rule, but cannot edit, move, or reconfigure these types of rules.

### **Thin Clone**

A thin clone is a clone of a physical disk that takes up only the amount of disk space actually in use; not the full specified disk size.

### **Threshold Parameters**

A monitoring rule that uses a numeric value above or below a defined level.

### **Time Server**

The network device that provides accurate time for synchronizing network activity.

### **Unmanaged Storage**

Unmanaged storage is the storage resource that is unknown to Oracle Enterprise Manager Ops Center. When you add storage to zones using the native CLI or manage existing zone environments, the zone's storage is not identified and termed as unmanaged.

### **User-defined Network Domain**

A network domain provides custom network resources from an Ethernet or InfiniBand fabric to virtualization hosts, server pools, or virtual datacenters so that new networks can be created as needed. A user-defined network domain supplements the Default Network Domain that is always available and cannot be deleted.

### **User-defined Rules**

Monitoring rules that are associated with, and determined by, the type of managed resource. You can apply a user-defined rule to many different attributes.

### **/usr File System**

A file system on a standalone system or server that contains many of the standard UNIX programs.

Sharing the large `/usr` file system with a server rather than maintaining a local copy minimizes the overall disk space that is required to install and run the Solaris software on a system.

### **/var File System**

A file system or directory (on standalone systems) that contains system files that are likely to change or grow over the life of the system. These files include system logs, vi files, mail files, and UUCP files.

### **vDC**

vDC is a collection of physical servers and storage that are placed on a common network. These physical resources are organized into a pool that are accessed by self-service users. It offers an access point through which you can allocate and control the resources inside. This is created during the set up phase. An example of a vDC is a single Exalogic system that might consist of multiple racks.

**vNets**

vNets are managed networks and their associated logical (L2) fabrics that can be associated with a vDC and its Accounts.

**vServer**

vServer is an entity that provides the outward interface of a standalone operating system. This may be a Virtual Machine (VM) or a Solaris Container or a similar construct. It consumes CPU and memory resources. It can be a member of one or multiple vNets.

**vServer Type**

vServer type is a profile for vServer creation that defines size of memory, size of disk and number of vCPUs to be used when creating a new vServer instance, that is used in combination with a Server Template.

**VID**

VLAN Identifier. Part of the VLAN tag inserted into Ethernet frame that specifies its VLAN.

**White List**

A list of Oracle Solaris operating system patch IDs that you always want to be applied to a host. The white list is used when you are using a baseline to update an Oracle Solaris operating system.

**Virtual Disk Image**

A virtual disk image is a representation of a virtual storage device that is associated with a virtual machine. Such storage can represent a virtual hard disk or a virtual CD/DVD.

**Virtualization Host**

Oracle VM Server that are managed by Oracle Enterprise Manager Ops Center is referred to as virtualization host. The virtualization host contains a hypervisor and its local resources and network connections.

**Virtual Machine**

A virtual machine is a software implementation of a computing environment in which an operating system or program is installed and run.

A virtual machine typically emulates a physical computing environment, requests for CPU, memory, hard disk, network, and other hardware resources that are managed by a virtualization layer which translates these requests to the underlying physical hardware.

**Virtual Machine Template**

A Virtual Machine Template provides a standardized group of hardware, and software settings that is used repeatedly to create virtual machines configured with those settings.

**Virtual Server Image**

A virtual server image is the persisted specification and state of a virtual machine. A virtual server is created when you create a guest. The virtual server image contains the general specification of the guest such as CPU, network, memory, and the type of physical storage that is backing the guest. A virtual server image is also referred to as a guest image.

### **Virtual Local Area Network (VLAN)**

VLAN is a group of network resources connected to different network segments that behave as if they were connected to a single network segment. All transmissions from the VLAN are identified by a unique VLAN tag.

### **Volume**

A volume is an identifiable unit of data storage that is sometimes physically removable from the computer or storage system. In tape storage systems, a volume may be a tape cartridge. In mainframe storage systems, a volume may be a removable hard disk. Each volume has a system-unique name or number that enables it to be specified by a user.

### **WINS**

WINS stands for Windows Internet Naming Service. The WINS server converts NetBIOS names to IP addresses.

### **WS-Man**

Web Services for Management (WS-MAN) is a specification for managing servers, devices, and applications using web services standards. It provides a common way for systems to access and exchange management information across the entire IT infrastructure. The public API in Oracle Enterprise Manager Ops Center can be accessed through WS-Management.

### **World Wide Name (WWN)**

WWN is a unique identifier in a Fibre Channel or Serial Attached SCSI storage network. Each WWN is an 8-byte number derived from an IEEE OUI and vendor information.

### **Zone**

Also called non-global zones, are a virtualized operating system environment created within a single instance of the Oracle Solaris operating system. One or more applications can run in a non-global zone without interacting with the rest of the system.

## A

---

- ABE See Boot environments, 12-32
- Access points, 2-19
- Accounts
  - private networks, 18-6, 18-12
  - quotas, 18-8, 18-12
  - vDC, 18-3, 18-12, 18-13, 18-14, 18-19
- Acknowledge Incident, 9-8, 9-10, 9-18
- Acting on an incident, 9-20
- Add Annotation to Incident, 9-8, 9-10
- Add Assets, 2-4, 2-6
- Add Assets to Group, 2-28
- Add Assets Using Profile, 16-5
- Add Content, 5-9
- Add File System, 14-28
- Add LUNs, 6-10
- Add monitoring rules, 4-6
- Add Storage, 14-25
  - logical domains, 15-23
  - Migrate Zone, 14-12
- Add Virtualization Host to Server Pool, 17-21
- Address Allocation Method, 7-11
  - Automatic, 18-21
  - static, 18-21
- Agent Controllers, 2-3
  - access point, 2-19
  - installing, 2-9, 2-10, 2-13
  - log file, C-2
  - monitoring, 4-1
  - operating systems, 12-6, 12-7
  - Oracle VM Server for x86, 16-7
  - uninstalling, 2-19
- agentadm, 19-10
  - requirements, 2-9
- Agentless assets, 2-3
- Agentless-managed operating systems, 12-6, 12-7, 12-10
  - changing mode, 12-8
- Agent-managed assets, 2-3
- Agent-managed operating systems, 12-6, 12-7, 12-10
  - changing mode, 12-8
  - updating, 13-3
- Aggregated link, 7-10
- Alert Monitoring Rules, 4-4
- Alert monitors, 4-8
- Alerts, 9-1
  - clearing, 9-5
- All Unassigned Incidents, 9-7
- Analytics
  - operating systems, 12-10, 12-11, 12-12, 12-13, 12-14, 12-15, 12-16, 12-18
  - Oracle VM Server for SPARC, 15-15
- Annotations, 9-16
  - Automated Operation, 9-12
  - Comment, 9-12
  - comment, 9-12
  - deleting, 9-12
  - incident, 9-10, 9-19
  - Suggested Action, 9-12
  - viewing, 9-11, 9-20, 9-23
- API for vDC, 18-16
- Asset attributes, 2-18, 2-24
  - adding, 2-24
  - deleting, 2-25
  - viewing, 2-24
- Asset management
  - access points, 2-19
  - adding assets to a group, 2-28
  - Agent Controller, 2-3
  - agentless, 2-3
  - agent-managed, 2-3
  - asset attributes, 2-18
  - changing groups, 2-28
  - credentials, 2-3, 2-16
    - copying, 2-18
    - creating, 2-17
    - deleting, 2-18
    - editing, 2-18
    - updatng, 2-16
    - upgrading, 2-16
  - deleting groups, 2-29
  - global zones, 14-11, 14-12
  - grouping, 2-25, 2-26, 2-27
  - incidents, 9-11
  - jobs, 3-7
  - logical domains, 15-26, 15-27
  - Move Storage, 14-26
  - moving groups, 2-29
  - Oracle Services, 9-14
  - Oracle Solaris 11, 2-20
  - Oracle Solaris Clusters, 2-20

- removing assets, 2-19
- removing assets from a group, 2-28
- roles, 2-1
- SPARC SuperCluster, 20-29
- Sun SPARC Enterprise M-Series Servers, 2-20, 2-21
- Sun ZFS Storage Appliances, 2-20, 2-22
- Windows, 2-20, 2-21
- Assign Incident, 9-8, 9-10, 9-18
- Assign Ownership, 16-11
- Associate Libraries, 17-24
- Associating network domains, 17-22
- Attach Networks, 7-7
  - Oracle VM Server for SPARC, 15-14
  - Oracle VM Server for x86, 16-14
  - server pools, 17-23
- Automated Operation, 9-12
- Automatic Load Balancing Policy, 17-3, 17-4
- Automatic method, 7-11
- Automatic Recovery, 17-4, 17-12
- Available LUNs, 6-9

## B

---

- Badges
  - incident severity, 9-5
- Balance resources
  - server pools, 17-26
- Bandwidth flow, 7-8
- Bandwidth management, 7-8
- Baseline Analysis Report, 10-9, 13-7
  - black list, 10-10
  - white list, 10-10
- Baseline Check, 20-6
- beadm, 12-32
- Black list, 10-10, 10-13
- Block storage, 6-5, 6-9
  - dynamic, 6-6
  - LUNs
    - selecting, 6-9
    - specifying, 6-10
  - static, 6-6
- Bonded interface, 16-13, 17-21
- Boolean Control, 4-3
- Boot environments, 12-32
  - activating, 12-35
  - active, 12-32
  - alternate, 12-32, 12-45
  - deleting, 12-35
  - dual, 12-32
  - icons, E-3
  - incidents, 12-33
  - Live Upgrade, 12-45
  - monitoring, 12-33
  - Oracle Solaris 10, 12-32
  - Oracle Solaris 10-8, 12-40, 12-42, 12-43, 12-44, 12-45, 12-46, 12-47, 12-48, 12-49
  - Oracle Solaris 11, 12-32, 12-36, 12-37, 12-38, 12-39, 12-40, 12-42
  - policy, 12-44

- profiles, 12-45
- requirements, 12-44, 12-45
- update profile, 13-16
- updating operating systems, 13-12, 13-16
- viewing, 12-33
- Boot interface, 12-26
- Boot Zone, 14-23
- Branded root zones, 14-2
  - packages, 14-14
  - requirements, 14-14, 14-15

## C

---

- Change History Report, 10-8
- Charts
  - creating, 12-21
  - groups, 12-20
  - operating systems, 12-15, 12-19, 12-20
- Chassis, 4-10
- Cisco switches, 4-10
- CLI
  - access, 19-3
  - administrative commands, 19-10
  - command scripts, 19-9
  - general commands, 19-5
  - modes, 19-20
- CLI for vDC, 18-17
- Close Incident, 9-8, 9-10
- Closing an incident, 9-22
- Cloud Admin, 20-8
  - prerequisites, 20-8
- Cloud User, 20-8
  - prerequisites, 20-8
- Cloud user, 18-16
- Cluster file system, 16-17, 17-15
- Cluster Heartbeat, 16-13
- Cluster profiles, B-1, B-2, B-3, B-4
- Command Line Interface
  - See CLI, 19-3
- Comment, 9-12, 9-20
- Common Vulnerability and Exposure
  - See CVE Report, 10-22
- Compare Catalogs, 13-6
- Compute Nodes, 20-18, 20-30, 20-31
- Compute nodes, 20-29
  - SPARC SuperCluster, 20-19
- Configuration
  - jobs, 3-10
- Configure Parent Repositories, 5-8
- Configure YUM Repository, 16-16
  - Oracle VM Manager, 16-16
- Connectivity
  - networks, 7-12
- connectivity check interval
  - user interface preferences, 1-2
- console timeout
  - user interface preferences, 1-2
- Consoles
  - logical domains, 15-26
  - Oracle VM Server for x86, 16-6

- Contracts, 9-13, 9-14
- Control domains, 15-10, 15-11, 15-12, 15-13
  - networks, 15-13
  - Oracle VM Server for SPARC, 15-2
  - reboot, 15-15
  - storage libraries, 15-13
- Copy Policy, 4-13
- Create Logical Domains, 17-24
- Create New NAS Library, 6-14
- Create Policy, 4-13
- Create Profile
  - Discovery, 16-4
- Create Update Library, 5-6
- Create Virtual Machines, 17-24
- Create Zones, 17-24
- Credentials
  - access points, 2-19
  - asset management, 2-3, 2-16
    - copying, 2-18
    - creating, 2-17
    - deleting, 2-18
    - editing, 2-18
    - upgrading, 2-16
  - ssh, 16-6
- Critical, 4-3, 9-16
- CSV reports, 10-1
- Custom content, 5-13
- CVE Report, 10-22, 13-7

## D

---

- Data link, 7-8
- Database
  - log file, C-2
  - Oracle Exalogic Elastic Cloud, 20-7
- Datacenter Enterprise Controller, 20-5
- Declaring servers, 2-4
  - operating systems, 2-4
  - service processors, 2-5
- Default network domain, 7-4
  - server pools, 17-5
- Default Policy icon, 4-13
- Delete Access Point, 2-19
- Delete Asset, 2-19
- Delete Group, 2-29
- Delete Local Component File, 5-17
- Delete Logical Domain, 15-26
- Delete Selected Guest, 16-26
- Delete Server Pool, 17-27
- Delete Zone, 14-23
- Deleting annotations, 9-12
- Deployment plans, 12-28, 12-29
  - boot environments, 12-47
  - Linux, 12-29
  - logical domains, 15-20, 15-21
  - non-global zones, 14-19, 14-20
  - operating systems, 12-29, 12-30
  - Oracle Solaris 11, 12-30
  - Oracle VM Server for SPARC, 15-9, 15-10
  - Oracle VM Server for x86, 16-9

- provisioning operating systems, 12-31
- updating operating systems, 13-12
- updating Oracle Solaris 11, 13-15
- virtual machine, 16-24
- DHCP, 12-22
- Discovering assets, 2-7
- Discovery
  - assets, 2-7
  - logical domains, 15-26
  - Oracle Solaris Clusters, 2-24
  - Oracle VM Manager, 16-3, 16-4
  - Oracle VM Server, 16-5, 16-6
  - Oracle VM Server for x86, 16-6, 16-7
    - requirements, 16-6
    - ssh, 16-6
  - servers, 2-4, 2-5, 2-6
  - SPARC SuperCluster, 20-29
  - storage servers, 16-11, 16-12
  - Sun SPARC Enterprise M-Series Servers, 2-21
  - Sun ZFS Storage Appliances, 2-23
- Discovery file, 2-4
- Discovery profile, 2-6
  - copying a profile, 2-9
  - creating a profile, 2-7
  - deleting a profile, 2-9
  - editing a profile, 2-8
- Disk image, 5-10
- Distribution Update Report, 10-24
- Dynamic block storage, 6-6
- Dynamic Host Configuration Protocol (DHCP), 12-30
- Dynamic private networks, 7-4, 18-6, 18-7
- Dynamic System Domains, 2-21, 4-10

## E

---

- EC Library, 5-3
  - changing, 5-3
  - Initial EC Library, 5-3
  - updating, 5-3
- ecadm, 19-10
- Edit Attributes, 16-15
- Edit Group, 2-27
- Edit IPMI Configuration, 16-15
- Edit Local Component File, 5-17
- Editing monitoring rules, 4-5, 4-6
- Engineered Systems
  - See Oracle Engineered Systems, 20-1
- Enterprise Controller
  - Oracle Engineered Systems, 20-5
- Enumerated Control, 4-3
- Ethernet network, 7-1
- Exadata Storage Servers, 20-28, 20-31
  - SPARC SuperCluster, 6-16, 20-19
- Exalogic, 20-6, 20-7
  - Cloud, 20-2
- Exalogic Control, 20-6, 20-7
  - Controls tab, 20-12
  - database, 20-7
  - Incidents tab

- Incidents
  - Oracle Exalogic Elastic Cloud, 20-13
  - Networks tab, 20-12, 20-13
- Exalogic Rack View, 20-14, 20-15
  - actions, 20-16
- Exalogic Report, 10-28
- Exalogic System Admin, 20-8
  - prerequisites, 20-8
- Exalogic System Report, 20-17
  - Baseline Check, 20-2, 20-18
  - Compute Nodes, 20-18
  - Power distribution units, 20-18
  - Report Parameters, 20-17
  - Storage Appliances, 20-18
  - Summary Table, 20-17
  - Switches, 20-18
  - System Control Software, 20-18
  - Validation, 20-2, 20-18
- Exalogic System View, 20-9, 20-10, 20-11, 20-12, 20-13
  - actions, 20-14
- Exclusive IP mode, 7-8, 14-5, 17-11
- Expression, 4-3
- eXtended System Control Facility
  - See XSCF, 2-21
- Extract a Monitor Policy, 4-12, 4-13

## F

---

- Fabrics
  - fully-managed, 7-4, 18-6
  - host-managed, 7-4
  - physical, 7-1
  - unmanaged, 7-4, 18-6
- Failure policy, 3-2
- Fibre Channel SAN, 6-15
- File servers, 4-10, 6-15
- File system libraries, 5-4
- File systems
  - boot environments, 12-38, 12-43
- Find Assets, 2-7
- Firewall, 7-21
- Firmware
  - power distribution units, 5-12
  - Profile for PDU, 5-13
- Firmware Compliance Report, 10-5, 11-22
- Firmware images, 5-10, 5-11
  - metadata, 5-11
  - PDU, 5-12
- Formatting reports, 10-1
- Fully-managed fabrics, 7-4, 18-6

## G

---

- Generate Report, 10-3
- Global zones, 14-2
  - Attach Network, 14-6
  - deleting, 14-12
  - discovering, 14-11

- IPMP groups, 14-6
- Link aggregation, 14-6
- monitoring policies, 4-10
- networks, 14-4, 14-10, 14-11
- requirements, 14-3
- storage libraries, 14-4, 14-12, 14-26
- updating operating systems, 14-40
- GnuPG key, 16-16
- Groups
  - adding assets, 2-28
  - attributes, A-1
  - changing groups, 2-28
  - changing position, 2-29
  - charts, 12-20
  - creating groups, 2-26
  - deleting, 2-29
  - editing, 2-27
  - icons, E-5
  - removing assets, 2-28
  - system groups, 2-25
  - tags, 2-25
  - user-defined, 2-25, 2-26
  - viewing data, 2-26
- Guest metadata, 5-10
- Guests
  - See virtual hosts, 17-1
- GUID
  - LUN, 6-11
  - WWN, 6-11

## H

---

- Halt Zone, 14-23
- Hardware
  - icons, E-6
- High Availability
  - storage, 6-16
- Historical data, 4-2, 4-6
- Host Compliance Report, 10-20, 10-21, 13-7
- Host-managed fabrics, 7-4

## I

---

- IaaS, 18-2
- Icons
  - Acknowledge Incident, 9-8, 9-10
  - Add Annotation to Incident, 9-8, 9-10
  - Add Assets Using Profile, 16-5
  - Add Content, 5-9
  - Administration, E-1
  - annotation, 9-10
  - Assign Incident, 9-8, 9-10
  - Boot Environment, E-3
  - Close Incident, 9-8, 9-10
  - Connectivity, E-4
  - Default Policy, 4-13
  - Edit View, 10-3
  - Generate Report, 10-3
  - Group, E-5
  - Hardware, E-6



- Incident, E-8
- Jobs, E-9
- Kernal, E-10
- Mark Incident as Repaired, 9-8, 9-10
- Message Center, E-11
- Monitoring, E-11
- Network, E-13
- Open Service Request, 9-10
- Operating System, E-13
- Processes, E-15
- Report, E-15
- Software Library, E-10
- SuperCluster, E-17
- Switch, E-18
- Take Action on Incident, 9-8, 9-10
- Unbind Network, 14-11
- Universal, E-19
- Update Policy, E-20
- Update Profiles, E-20
- URL, 9-7
- View Alerts, 9-8, 9-9
- View Annotations, 9-8, 9-9
- View Comments, 9-8, 9-10
- View Possible Impacts and Causes, 9-8, 9-9
- View Suggested Actions, 9-8, 9-10
- Virtualization, E-14
- wrench, 12-18
- Image Packaging System, 5-6
- Images
  - disk image, 5-10
  - HVM, 16-22
  - import, 5-12
  - ISO, 5-10
  - Oracle VM Server for x86, 16-7
  - OS, 5-10
  - PVM, 16-22
  - upload, 5-12
  - virtual machines, 16-22
- Import images, 5-12
- Incident Compliance Report, 10-17, 10-19, 13-7
- Incident Detail Report, 10-26
- Incident Severity Badges, 9-5
  - Asset icon, 9-5
  - enabling, 9-5
- Incident Summary Report, 10-26
- Incident tab for vDC, 18-11
- Incidents, 9-1
  - Acknowledge Incident, 9-8
  - acknowledging, 9-18
  - acting, 9-20
  - Add Annotation to Incident, 9-8
  - alerts, 9-5
  - annotating, 9-19
  - annotations, 9-10
  - Assign Incident, 9-8
  - Assigned to Others, 9-6
  - assigning, 9-18
  - boot environments, 12-33
  - Close Incident, 9-8
  - closing, 9-22, 20-6
  - comments, 9-20
  - Critical, 9-16
  - details, 9-17
  - icons, 9-6, E-8
  - ID, 9-7
  - Informational, 9-16
  - Mark Incident as Repaired, 9-8
  - Message Center, 9-6
  - monitoring rules, 9-16
  - My Incidents, 9-6
  - My Service Requests, 9-6
    - new, 9-7
  - Notifications, 9-6
  - Open Service Requests, 9-6
  - Oracle Engineered Systems, 20-6
  - Relayed, 9-7, 20-6
  - Relayed Service Requests, 9-7
  - repaired, 9-21
  - roles, 9-2
  - Service Requests Opened by Others, 9-6
  - SPARC SuperCluster, 20-25
  - Take Action on Incident, 9-8
  - unassigned, 9-6, 9-7
  - unresolved, 9-17
  - View Alerts, 9-8
  - View Annotations, 9-8
  - View Comments, 9-8
  - View Possible Impacts and Causes, 9-8
  - View Suggested Actions, 9-8
  - viewing, 20-6
  - viewing annotations, 9-20
  - Warning, 9-16
- Incidents Assigned to Others, 9-6
- Incidents Knowledge Base, 9-11, 9-12, 9-16
  - annotations, 9-11, 9-12
  - operational plans, 9-11, 9-12
- Incidents tab, 9-17
- InfiniBand network, 7-1
- Info, 4-3
- Informational, 9-16
- Infrastructure-as-a-Service, 18-2
- Initial EC Library, 5-3
- Initialize Oracle Solaris 11 Software Update Library, 5-7
- Installing operating system
  - See Provisioning, 12-22
- Intelligent Platform Management Interface
  - See IPMI, 16-15
- Interactive reports, 10-1
- Internet Connection Firewall., 2-20
- IP Multipathing, 7-9
- IPMI, 16-15
  - Wake-on-LAN, 16-15
- IPMP groups, 7-9, 14-5
  - creating, 14-7, 14-8
  - global zones, 14-6
  - Oracle VM Server for SPARC, 15-14
- IPS, 5-6
- IPv4, 7-11
- IPv6, 7-11

iSCSI storage arrays, 4-10  
ISO format, 5-10  
ISO image, 5-10

## J

---

JET  
    See JumpStart Enterprise Toolkit, 12-27  
JetFLASH, 12-27  
job status popup duration  
    user interface preferences, 1-2  
Jobs  
    actions, 3-8  
    Actual Run, 3-2  
    by asset, 3-7  
    configuring, 3-10  
    copying, 3-9  
    debugging, 3-9  
    deleting, 3-9  
    failure policy, 3-2  
    icons, E-9  
    order of tasks, 3-2  
    repeating, 3-9  
    roles, 3-3  
    Run ID, 3-2  
    searching, 3-7  
    Simulated, 3-2  
    status, 3-1  
    stopping, 3-8  
    Update Microsoft Windows, 13-19  
    updating operating systems, 13-12  
    viewing, 3-4, 3-5, 3-9  
Jobs pane, 3-1  
JumpStart Enterprise Toolkit, 12-27, 12-28, D-1  
    location, D-1  
    parameters, D-1  
    templates, 12-28

## K

---

Kernal  
    icons, E-10  
Knowledge Base, 5-3

## L

---

Launch Web Interface, 20-6  
LDAP, 20-7  
Libraries  
    images, 5-1  
    local content, 5-1  
    software, 5-1  
    storage libraries, 6-1  
Link aggregation, 7-10  
    Configure Bonding, 17-21  
    creating, 14-9  
    global zones, 14-6  
    Networks  
        Link aggregation, 14-5  
        Oracle VM Server for SPARC, 15-9, 15-14  
Linux and Oracle Solaris 8-10 Software Update  
    Library, 5-9  
    Linux provisioning parameters, 12-25  
    Linux SuSE provisioning parameters, 12-26  
    Live Migrate, 16-13  
    Live Upgrade, 12-40, 12-42, 12-45, 12-46  
        updated operating systems, 12-49  
        updating operating systems, 13-12  
Local actions, 5-13  
Local Categories, 5-16  
Local Component File, 5-17  
Local Configuration File, 5-15  
Local content, 5-13  
    actions, 5-13  
    categories, 5-16  
    changing, 5-17  
    configuration files, 5-15  
    editing, 5-17  
    packages, 5-14  
Local libraries, 5-4  
    monitoring policies, 4-10  
Local Packages, 5-14  
Local storage  
    File system storage, 6-7, 6-8, 6-9  
Logical domains  
    console, 15-26  
    deleting, 15-26  
    deployment plans, 15-20, 15-21  
    discovering, 15-26  
    migrating, 15-23, 15-24  
    modifying, 15-22  
    monitoring policies, 4-10  
    networks, 15-13, 15-23  
    operating systems, 15-21  
    Oracle Engineered Systems, 20-19  
    Oracle VM Server for SPARC, 15-2, 15-17, 15-18,  
        15-20, 15-21, 15-22, 15-23, 15-24, 15-26, 15-27  
    profiles, 15-17, 15-18  
    server pools, 17-24, 17-26  
    shutdown, 15-22  
    start, 15-22  
    storage libraries, 15-13, 15-23  
Logical Domains Manager, 15-10  
Logical Units  
    See LUNs, 6-15  
Logs  
    cacao, C-3  
    events, C-1  
    installation, C-1  
    upgrades, C-3  
Lowest allocated CPU and memory resources, 17-14  
Lowest relative load, 17-14  
lucreate, 12-32, 12-44  
LUNs, 6-4, 6-5  
    Add LUNs, 6-10  
    selecting, 6-9  
    specifying, 6-10  
    volume groups, 6-15

## M

- Maintenance mode
  - Incidents
    - disabling, 9-21
    - migrating virtual hosts, 17-4
- Managed networks
  - Subnets, 7-5
- Manual Net Boot, 12-27, 15-12
- Manually Adding LUNs, 6-10
- Mark an Incident as Repaired
  - Repaired incidents, 9-21
- Mark Incident as Repaired, 9-8, 9-10
- Maximum Transmission Unit, 7-12
- membership graph preferences
  - user preferences, 1-2
- Message Center, 9-2, 9-16
  - annotations, 9-11
  - icons, E-11
  - incidents, 9-6, 20-6
  - My Incidents, 9-8
  - Notifications, 9-10
  - relayed service requests, 20-6
- Metadata, 6-3
  - firmware, 5-11
  - guest, 5-10
- Microsoft System Center Configuration Manager, 13-19
- Microsoft Windows
  - registry, 13-20
  - update job, 13-21
  - updates, 13-19, 13-20
  - updating, 13-19
- Migrate Logical Domain, 15-23, 15-24
- Migrate Zones, 14-30
- Migrating logical domains
  - server pool, 17-26
- Migrating virtual machines
  - server pool, 17-26
- Migrating zones, 14-29, 14-30, 14-32, 14-34, 14-35
  - server pool, 17-25
- Minimize Power Consumption Policy, 17-3, 17-15
- Modify Physical Connectivity, 14-10
  - Networks
    - Oracle VM Server for SPARC, 15-15
- Monitored attributes, 4-7, A-1
  - collection, 4-7
  - simple, 4-7
  - struct-like, 4-7
  - structure, 4-7
- Monitoring
  - boot environments, 12-33
  - icons, E-11
  - operating systems, 12-9, 12-14, 12-18
  - Oracle VM Server for SPARC, 15-16
  - roles, 4-1
  - thresholds, 4-2
- Monitoring policies, 4-1, 4-2, 4-3, 4-7, 12-9
  - chassis, 4-10
  - Cisco switches, 4-10
  - copying, 4-13
  - creating, 4-8, 4-12, 4-13
  - default, 4-8, 4-13
  - deleting, 4-14
  - details, 4-9
  - Dynamic System Domains, 4-10
  - extracting, 4-8, 4-12, 4-13
  - file servers, 4-10
  - global zones, 4-10
  - groups of assets, 4-12
  - iSCSI storage arrays, 4-10
  - local libraries, 4-10
  - logical domains, 4-10
  - modifying, 4-12
  - M-Series servers, 4-10
  - NAS libraries, 4-10
  - non-global zones, 4-10
  - operating systems, 4-10
  - Oracle VM Server for SPARC, 4-11
  - Oracle VM Server for x86, 4-11
  - power distribution units, 4-11
  - Remote Oracle Engineered System, 4-11
  - rule set, 4-8
  - SAN libraries, 4-11
  - SAN storage arrays, 4-11
  - server pools, 4-11
  - Servers, 4-11
  - Solaris Cluster, 4-11
  - Solaris Cluster Node, 4-11
  - Solaris Cluster Zone Cluster Group, 4-11
  - Solaris Cluster Zone Cluster Node, 4-11
  - Storage, 4-11
  - switches, 4-11
  - system-defined, 4-9, 4-10
  - user-defined, 4-8
  - viewing assets, 4-13
  - Virtual machines, 4-11
- Monitoring rules, 4-1, 4-2, 12-9
  - active, 4-4, 4-5
  - adding, 4-6
  - Critical, 4-3
  - disabled, 4-4
  - editing, 4-5, 4-6
  - enabled, 4-4
  - inactive, 4-4
  - incidents, 9-16
  - Info, 4-3
  - state, 4-4
  - system-defined, 4-3
  - thresholds, 4-6
  - user-defined, 4-3
  - Warning, 4-3
- Monitoring tab, 4-3
  - details, 4-9
- Move Asset to Group, 2-28
- Move Group, 2-29
- Move Storage, 14-12, 14-26
- M-Series servers, 2-21
  - monitoring policies, 4-10
- My Incidents, 9-6, 9-8
  - Acknowledge Incident, 9-10

- Add Annotation to Incident, 9-10
- Assign Incident, 9-10
- Close Incident, 9-10
- Mark Incident as Repaired, 9-10
- new, 9-8
- Open Service Request, 9-10
- Take Action on Incident, 9-10
- unassigned, 9-8
- View Alerts, 9-9
- View Annotations, 9-9
- View Comments, 9-10
- View Possible Impacts and Causes, 9-9
- View Suggested Actions, 9-10
- My Oracle Support, 9-2
- My Service Requests, 9-6

## N

---

- NAS libraries, 17-24
- NAS software libraries, 5-4
- NAS storage
  - monitoring policies, 4-10
  - NFS, 6-5
- NAS Storage Appliances, 6-12
- NAS storage libraries, 6-5
  - creating, 6-14
- Netboot
  - virtual machines, 16-22
- Network domains, 7-3
  - default, 7-4
  - server pools, 17-21, 17-22
  - user-defined, 7-4
  - vDC, 18-7
  - virtual datacenter, 18-6
  - virtual machines, 16-24
- Network File Service, 6-5
- Network Interface Card, 7-13
- Network-attached storage
  - See NAS, 6-5
- Networks, 7-5
  - Connectivity, 7-12
  - exclusive IP mode, 14-5
  - firewall, 7-21
  - global zones, 14-4, 14-10, 14-11
  - icons, E-13
  - IPMP groups, 14-5
  - logical domains, 15-23
  - MTU, 7-12
  - non-global zones, 14-28
  - Oracle Enterprise Manager Ops Center
    - operations, 7-14
  - Oracle Solaris Zones, 7-7
  - Oracle VM Server for SPARC, 7-8, 15-13, 15-14
  - Oracle VM Server for x86, 7-8, 16-13, 16-14
    - roles, 16-13
  - ports, 7-21
  - profiles, 7-13
  - properties, 7-10
  - protocols, 7-21
  - requirements, 7-6

- roles, 7-2
- routing mode, 7-11
- server pools, 7-7, 17-5, 17-11, 17-22, 17-23
- shared IP mode, 14-4
- static route, 7-11
- switches, 7-13
- utilization, 7-12
- vDC, 7-8, 18-10, 18-20, 18-21
- virtual datacenter, 18-4
- VLAN, 7-12
- New Update OS Job, 13-13
- NFS Client, 6-13
- NFS Server, 6-12
- NIC See also PNIC, 7-13
- Non-global zones, 14-2
  - Add File System, 14-28
  - Add Storage, 14-25
  - Boot Zone, 14-23
  - branded root zones, 14-2
  - clones, 14-24
  - creating, 14-13
  - Delete Zone, 14-23
  - deleting, 14-12
  - deployment plans, 14-19, 14-20
  - file systems, 14-21
  - Halt Zone, 14-23
  - migrating, 14-28, 14-29, 14-30, 14-32, 14-34, 14-35
  - modifying, 14-21
  - monitoring policies, 4-10
  - networks, 14-28
  - Oracle Solaris 11 Software Update Library, 14-15
  - profiles, 14-13, 14-15, 14-16
  - Reboot Zone, 14-23
  - recovering, 14-37
  - Replicate Zone, 14-24
  - requirements, 14-13, 14-14, 14-15
  - server pools, 14-38, 17-24, 17-25
  - Shutdown Zone, 14-23
  - sparse root zones, 14-2
  - storage, 14-28
  - targets, 14-17
  - updating operating systems, 14-38, 14-40, 14-41
  - updating operating systems in parallel, 14-41
  - whole root zones, 14-2
  - zpool, 14-21
- Notifications, 9-6, 9-10

## O

---

- OCDoctor
  - debugging a job, 3-9
- Open Service Requests, 9-6, 9-10
- Operating system updates
  - roles, 13-4
- Operating systems
  - agentless-managed, 12-6, 12-7, 12-10
    - changing mode, 12-8
  - agent-managed, 12-6, 12-7, 12-10
    - changing mode, 12-8
  - Analytics, 12-10, 12-11

- charts, 12-15
  - custom, 12-12, 12-13
  - Summary, 12-12
- boot environments, 12-32, 12-33, 12-35, 12-36, 12-37, 12-38, 12-39, 12-40, 12-42, 12-43, 12-44, 12-45, 12-46, 12-47, 12-48, 12-49
- charts, 12-19, 12-20
- CPU Utilization, 12-13
- deployment plans, 12-29, 12-30, 12-31
- History, 12-15
- icons, E-13
- logical domains, 15-21
- Metrics, 12-16
- Microsoft Windows, 13-20, 13-21
- monitor thresholds, 12-14
- monitoring, 12-9
- monitoring policies, 4-10
- Oracle VM Server for x86, 16-7, 16-9
- parameters, 12-25, 12-26
- Processes, 12-13
- profiles, 12-6, 12-25, 12-26, 12-27, 12-31
- provisioning, 12-22, 12-29
- roles, 12-3
- Services, 12-14
- system catalog, 13-6
- threshold, 12-18
- update job, 13-12
- update policies, 13-7, 13-8
- update profiles, 13-9, 13-10
- updates, 13-11, 13-12, 13-13, 13-14, 13-15, 13-16, 13-19
  - requirements, 13-3
- vDC, 18-21
- Virtualization Analytics, 12-18
- zones, 14-38, 14-39, 14-40, 14-41
- Operational plans, 4-3, 9-16
  - boot environments, 12-47
  - incidents, 9-11, 9-12
- Oracle 8,9,10, 12-29
- Oracle Engineered Systems, 20-1
  - Baseline Check, 20-6
  - incidents, 20-6
  - Launch Web Interface, 20-6
  - logical domains, 20-19
  - monitoring policies, 4-11
- Oracle Exalogic Elastic Cloud, 20-2, 20-6, 20-7, 20-8, 20-9, 20-10, 20-14, 20-15, 20-16, 20-17, 20-18
- rack, 20-5
- service requests, 20-6
- SPARC SuperCluster, 20-19, 20-20
  - actions, 20-26
  - add assets, 20-29
  - Baseline Check, 20-31
  - compute nodes, 20-29, 20-30, 20-31
  - Dashboard, 20-22, 20-23
  - Details, 20-24
  - discovery, 20-29
  - Exadata Storage Server, 20-28
  - Incidents, 20-25
  - Infrastructure Networks, 20-25
  - Network Connectivity, 20-25
  - Networks, 20-25
  - power distribution units, 20-31
  - reports, 20-30
  - storage, 20-28, 20-29, 20-31
  - switches, 20-29, 20-31
  - validation, 20-31
  - viewing, 20-20, 20-21
  - viewing racks, 20-26, 20-27
- SPARC SuperCluster T4-4, 20-19
- status, 20-5
- Oracle Enterprise Manager Ops Center Software Developer's Kit (SDK), F-1
  - SUNWxvmoc-sdk.pkg, 4-7
- Oracle Exalogic Elastic Cloud, 20-2, 20-6, 20-7, 20-8
  - actions, 20-14
  - Baseline Check, 20-2, 20-18
  - compute nodes, 20-18
  - Controls, 20-12
  - Dashboard, 20-10
  - Details, 20-11
  - Incidents, 20-11, 20-13
  - Infrastructure Networks, 20-13
  - Membership Graph, 20-11
  - Network Connectivity Exalogic Control Networks tab, 20-13
  - Networks, 20-12
  - power distribution units, 20-18
  - reports, 20-17
  - software, 20-18
  - Status, 20-11
  - storage appliances, 20-18
  - Summary, 20-10
  - switches, 20-18
  - validation, 20-2, 20-18
  - viewing, 20-8, 20-9
  - viewing racks, 20-14, 20-15, 20-16
- Oracle Knowledge Base, 5-3
- Oracle Services, 9-13
  - contracts, 9-13, 9-14
  - icons, E-4
  - requirements, 9-13
  - service requests, 9-13, 9-14, 9-15
  - warranty, 9-13, 9-14
- Oracle Solaris 10
  - boot environments, 12-32
  - branded root zones, 14-14
  - non-global zones, 14-14
  - sparse root zones, 14-14
  - whole root zones, 14-14
- Oracle Solaris 10-8, 13-11
  - boot environments, 12-40, 12-42, 12-43
  - profiles, 12-44
- Oracle Solaris 11, 13-14
  - boot environment, 13-16
  - boot environments, 12-32, 12-36, 12-37, 12-42, 13-16
  - file systems, 12-38
  - profiles, 12-39

- snapshots, 12-38, 12-40
  - zones, 12-38
- branded root zones, 14-15
- non-global zones, 14-15
- updates, 5-6, 13-15
- Oracle Solaris 11 deployment plan, 12-31
- Oracle Solaris 11 Package Repository, 5-3, 5-4
- Oracle Solaris 11 provisioning profiles, 12-31
- Oracle Solaris 11 Software Update Library, 5-6, 13-14
  - adding content, 5-9
  - deleting, 5-9
  - initializing, 5-7
  - non-global zones, 14-15
  - parent repositories, 5-7
  - status, 5-7
  - synchronizing, 5-8
  - viewing, 5-8
- Oracle Solaris 8-10 Software Update Library, 5-4
- Oracle Solaris Cluster
  - monitoring policy, 4-11
  - upgrading, B-1
- Oracle Solaris Cluster node
  - monitoring policy, 4-11
- Oracle Solaris Cluster Zone Cluster Groups
  - monitoring policy, 4-11
- Oracle Solaris Cluster Zone Cluster Node
  - monitoring policy, 4-11
- Oracle Solaris Clusters
  - discovery, 2-24
  - importing, B-4
  - uploading, B-3
- Oracle Solaris Container
  - See Oracle Solaris Zones, 14-1
- Oracle Solaris Update Compliance Report, 10-16, 13-7, 13-13
- Oracle Solaris Zones, 14-1
  - boot environments, 12-38
  - Live Upgrade, 12-42
  - networks, 7-7
  - roles, 14-2
  - server pools
    - adding virtualization hosts, 17-20
    - creating, 17-12
    - modifying, 17-20
    - networks, 17-11
    - policies, 17-12
    - requirements, 17-11
  - storage libraries, 17-24
- Oracle VM Manager, 16-2
  - details, 16-10
  - discovering, 16-3
  - discovery profile, 16-3, 16-4, 16-5
  - file system, 16-11, 16-12
  - iSCSI storage, 16-11, 16-12
  - Oracle Engineered Systems, 20-7
  - Oracle VM Server, 16-5
  - ownership, 16-10
  - password, 16-7
  - SAN storage, 16-11, 16-12
  - server pools, 16-17
  - storage, 16-11, 16-12
  - YUM repository
    - GPG key, 16-16
- Oracle VM Server, 16-6
  - block storage, 16-12, 16-13
  - file system, 16-12
  - networks, 7-8
  - storage libraries, 16-12, 16-13
- Oracle VM Server for SPARC, 15-1, 15-12
  - Analytics, 15-15
  - Attach Networks, 15-14
  - control domains, 15-2, 15-10, 15-11, 15-12, 15-13
  - deployment plans, 15-9, 15-10
  - details, 15-15
  - installing, 15-10, 15-11
  - IPMP groups, 15-14
  - Link aggregation, 15-9, 15-14
  - logical domains, 15-2, 15-17, 15-18, 15-20, 15-21, 15-22, 15-23, 15-24, 15-26, 15-27
  - Modify Physical Connectivity, 15-15
  - modifying, 15-13
  - monitoring, 15-16
  - monitoring policies, 4-11
  - networks, 15-13, 15-14
  - operating systems, 12-27, 15-21
  - profile, 15-4, 15-5, 15-12
  - reboot, 15-15
  - requirements, 15-3, 15-4, 15-12
  - roles, 15-2
  - server pools, 15-10, 15-17
    - adding virtualization hosts, 17-20
    - creating, 17-8
    - networks, 17-6
    - policies, 17-6
    - requirements, 17-5
    - storage, 17-6
  - service processor, 15-12
  - storage libraries, 15-13, 17-24
  - Unbind Network, 15-15
- Oracle VM Server for x86, 16-1, 17-1
  - Agent Controller, 16-7
  - deployment plans, 16-9
  - discovery profile, 16-6, 16-7
  - editing, 16-15
  - image, 16-7
  - IPMI, 16-15
  - monitoring policies, 4-11
  - networks, 16-13, 16-14
    - management network, 16-13
  - ownership, 16-10
  - Place in Maintenance Mode, 16-15
  - profile, 16-7
  - roles, 16-2
  - server pools, 16-11, 16-17, 17-15
    - adding virtualization hosts, 17-20
    - cluster file system, 16-17, 17-15
    - Create Server Pool, 16-18
    - creating, 17-17
    - policies, 16-17, 17-16

- requirements, 16-17
- Server Pool Master, 16-17, 17-16
- storage libraries, 17-24
- updating, 16-16
- virtual machines, 16-20
  - creating, 16-21
  - creating from a virtual machine, 16-22
  - creating from image, 16-22
  - creating from network, 16-22
  - creating from templates, 16-22
  - profiles, 16-21
- Oracle VM Server Host, 15-10
- Oracle VM Storage Repositories, 6-7, 16-12, 16-23, 17-24
- OS image, 5-10
- OS Update, 13-7

## P

---

- Package Compliance Report, 10-25, 13-7
- Parent repositories, 5-4, 5-7
  - Oracle Solaris 11 Software Update Library, 5-7
  - synchronizing, 5-8
- Partition
  - partition keys, 7-2
- PDF reports, 10-1
- PDU
  - firmware, 5-12
  - profile, 5-13
- Physical fabric, 7-1
- Physical network interface card, 7-5
- Place in Maintenance Mode
  - Maintenance mode, 16-15
- Placement Policy
  - Lowest allocated CPU and memory resources, 17-14
  - Lowest relative load, 17-14
  - Minimize power consumption, 17-15
- Plan Management
  - Incident Knowledge Base, 9-11
  - Monitoring policies, 4-8
- Plans
  - provisioning, 12-28
- PNIC, 7-5
- Policies
  - Automatic Load Balancing Policy, 17-3
    - thresholds, 17-4
  - Minimize Power Consumption, 17-3
    - monitoring, 4-2, 4-3, 4-7, 4-8, 4-12
  - Oracle Solaris Zones, 17-12
  - Oracle VM Server for x86, 17-16
  - Placement Policy, 17-3
  - server pools, 16-17, 17-2, 17-3, 17-4, 17-6, 17-12, 17-16
  - update, 13-7, 13-8
- Policy
  - boot environments, 12-44
- Ports, 7-21
  - Ethernet switch
  - InfiniBand switch, 18-6
- Power Distribution Units, 20-31
- Power distribution units
  - monitoring policies, 4-11
- Private networks, 18-12, 18-25
  - accounts, 18-6
  - dynamic, 7-4, 18-6, 18-7
  - Physical fabric, 18-6
  - requirements, 18-7
  - static, 7-4, 18-7
- Private vNets, 18-7, 18-25
  - allocating vIP, 18-25
  - creating, 18-25
  - managing, 18-25
- Processes
  - icons, E-15
- Profile Analysis Report, 10-13, 13-7
  - black list, 10-13
  - white list, 10-13
- Profiles, 15-12
  - boot environments, 12-39, 12-44, 12-45, 12-48, 13-16
  - clusters, B-1, B-2, B-3, B-4
  - discovery, 2-6, 2-7, 2-8, 2-9, 16-12
  - logical domains, 15-17, 15-18
  - network, 7-13
  - non-global zones, 14-15, 14-16
  - operating systems, 12-6
  - Oracle VM Manager, 16-3, 16-4
  - Oracle VM Server for SPARC, 15-4, 15-5
  - Oracle VM Server for x86, 16-6, 16-7
  - provisioning operating systems, 12-25, 12-31
    - boot interface, 12-26
    - JumpStart Enterprise Toolkit, 12-27
    - Linux parameters, 12-25
    - Linux SuSE parameters, 12-26
    - Manual Net Boot, 12-27
    - Oracle Solaris profiles, 12-26
    - Oracle VM Server for SPARC, 12-27
  - storage, 6-16
  - system catalog, 13-14
  - update, 13-9, 13-10
  - updating operating systems, 13-12
  - virtual machines, 16-21
  - zones, 14-15, 14-16
- Protocols, 7-21
- Provisioning
  - operating systems, 12-22
- Provisioning operating systems
  - hardware virtualization, 16-21
  - hardware virtualization with paravirtual drivers, 16-21
  - HVM, 16-21
  - HVM with PV, 16-21
  - Oracle VM Server for x86, 16-7, 16-9
  - paravirtualization, 16-21
  - PVHVM, 16-21
  - PVM, 16-21
  - virtual machines, 16-25
- Provisioning plans, 12-28
- proxyadm, 19-10

- Public API
  - API, F-4
  - JMX, F-7
  - WS-Management, F-7, F-8
- Public external networks, 18-7
- Public networks, 18-24
- Publisher, 5-4

## R

---

- Racks
  - Oracle Engineered Systems, 20-5
  - Oracle Exalogic Elastic Cloud, 20-14, 20-15, 20-16
  - SPARC SuperCluster, 20-19, 20-26, 20-27
- RAID Controller, 6-12
- Reboot Guests, 16-26
- Reboot Zone, 14-23
- Recommended Software Configuration
  - Report, 10-15, 13-7
- Recovering zones, 14-37
- Relayed incidents, 9-7, 20-6
  - closing, 20-6
  - viewing, 20-6
- Relayed Service Requests
  - viewing, 20-6
- Relayed service requests, 9-7, 20-6
- Release Ownership, 16-11
- Remove Asset from Group, 2-28
- Replicate Zone, 14-24
- Report Result
  - updating operating systems, 13-13
- Reports
  - Baseline Analysis Report, 10-9, 13-7
  - Change History Report, 10-8
  - CVE Report, 10-22, 13-7
  - Distribution Update Report, 10-24
  - Exalogic Report, 10-28
  - Exalogic System Report, 20-2, 20-17, 20-18
  - Firmware Compliance Report, 10-5, 11-22
  - formatting, 10-1
  - Generate Report, 10-3
  - Host Compliance Report, 13-7
  - Host Compliance Report for Microsoft Windows, 10-21
  - Host Compliance Report for Oracle Solaris or Linux, 10-20
  - icons, E-15
  - Incident Compliance Report, 10-17, 13-7
  - Incident Compliance Report for Microsoft Windows, 10-19
  - Incident Compliance Report for Oracle Solaris or Linux, 10-17
  - Incident Detail Report, 10-26
  - Incident Summary Report, 10-26
  - Oracle Solaris Update Compliance Report, 10-16, 13-7, 13-13
  - OS Update, 13-7
  - Package Compliance Report, 10-25, 13-7
  - Profile Analysis Report, 10-13, 13-7
  - Recommended Software Configuration

- Report, 10-15, 13-7
- Results, 10-3
- roles, 10-2
- scheduling, 10-1
- Service Pack Compliance Report, 10-24
- SPARC SuperCluster System Report, 20-30, 20-31
- System Catalog, 13-6
- System Catalog Report, 10-23
- System Information Report, 10-27
- templates, 10-2, 10-3

## Repositories

- Oracle Solaris 11 Package Repository, 5-3
- Oracle VM Server, 6-7
  - parent, 5-4, 5-7
  - publisher, 5-4
  - YUM, 16-16

## Roles

- asset management, 2-1
- Cloud Admin, 20-8
- Cloud User, 20-8
- Exalogic System Admin, 20-8
- incidents, 9-2
- jobs, 3-3
- monitoring, 4-1
- networks, 7-2
- operating system updates, 13-4
- operating systems, 12-3
- Oracle Solaris Zones, 14-2
- Oracle VM Server for SPARC, 15-2
- Oracle VM Server for x86, 16-2
- Reports, 10-2
- server pools, 17-2
- Software libraries, 5-2
- storage libraries, 6-1
- SuperCluster System Admin, 20-20
- vDC Cloud, 18-17
- virtual datacenters, 18-3

- Routing mode, 7-11
- Rule set, 4-8
- Rules for monitoring, 4-2
- Run ID, 3-2

## S

---

- SAN libraries, 17-24
- SAN storage, 6-4
  - monitoring policies, 4-11
- SAN storage arrays
  - monitoring policies, 4-11
- SCCM See Microsoft System Center Configuration Manager, 13-19
- Scheduling reports, 10-1
- Scripts, 5-13
- See NFS, 6-5
- Server Management, 16-13
- Server Pool Master, 16-17, 17-16
- Server pools, 17-1
  - adding virtualization hosts, 17-21
  - Automatic Load Balancing Policy, 17-3, 17-4
  - Automatic Recovery, 17-4



- balance resources, 17-26
- deleting, 17-27
- logical domains, 17-24, 17-26
- modifying, 17-19
- monitoring policies, 4-11
- network domains, 17-21, 17-22
- networks, 7-7, 17-5, 17-22, 17-23
- non-global zones, 17-24, 17-25
- Oracle Solaris Zones, 17-11, 17-12, 17-20
- Oracle VM Manager, 16-17
- Oracle VM Server for SPARC, 15-10, 15-17, 17-5, 17-6, 17-8, 17-20
- Oracle VM Server for x86, 16-11, 16-17, 16-18, 17-15, 17-16, 17-17, 17-20
- Placement Policy, 17-3
- policies, 17-2, 17-3, 17-4, 17-6
- roles, 17-2
- software libraries, 17-5
- storage libraries, 6-3, 17-5, 17-24
- vDC, 18-9, 18-11
- virtual datacenter, 18-4
- virtual hosts, 17-2
- virtual machines, 17-24, 17-26
- virtualization hosts, 17-2
- zones, 14-38
- Servers
  - monitoring policies, 4-11
- Service Pack Compliance Report, 10-24
- Service Requests
  - Oracle Engineered Systems, 20-6
  - Relayed, 20-6
- Service requests, 9-13, 9-14, 9-15, 20-6
  - automated, 9-15
  - creating, 9-15
- Service Requests Opened by Others, 9-6
- Service tags, 2-7
- session timeout
  - user interface preferences, 1-2
- Shared IP mode, 7-7, 14-4, 17-11
- Shut Down Guest, 16-26
- Shutdown a logical domain, 15-22
- Shutdown Zone, 14-23
- Snapshot
  - volume, 18-29
- Snapshots
  - assembly templates, 18-30
  - boot environments, 12-38, 12-40
  - volumes, 18-30, 18-31
- Software libraries, 5-1
  - creating, 5-5
  - EC Library, 5-3
  - file system, 5-4
  - Firmware images, 5-1
  - icons, E-10
  - Linux and Oracle Solaris 8-10 Software Update Library, 5-9
  - local, 5-4
  - NAS, 5-4
  - OS images, 5-1
  - roles, 5-2
  - server pools, 17-5
  - specifying EC Library, 5-3
  - uploading, 5-18
  - viewing, 5-4, 5-19
- SPARC SuperCluster
  - Dashboard, 20-22
  - Incidents tab, 20-25
  - Networks tab, 20-25
  - Rack View, 20-26
  - System View, 20-25
- SPARC SuperCluster Rack View, 20-27
- SPARC SuperCluster System Report
  - Baseline Check, 20-31
  - Compute Nodes, 20-30
  - Exadata Storage Server, 20-31
  - power distribution units, 20-31
  - Storage Appliances, 20-31
  - Switches, 20-31
  - validation, 20-31
- SPARC SuperCluster System View
  - actions, 20-26
- SPARC SuperCluster T4-4, 20-2
  - See Oracle Engineered Systems, 20-19
- SPARC SuperCluster View, 20-21, 20-22, 20-24, 20-25
  - Membership Graph, 20-23
  - Status, 20-23
  - Summary, 20-23
- Sparse root zones, 14-2
  - requirements, 14-14
- ssh, 16-6
- Start Logical Domain, 15-22
- start page preferences
  - user preferences, 1-2
- Start Selected Guest, 16-26
- Static block storage, 6-6
- Static IP, 7-11
- Static private networks, 7-4, 18-7
- Static route, 7-11
- Status
  - jobs, 3-1
- Storage
  - Exadata Storage Server, 20-28
  - monitoring policies, 4-11
  - non-global zones, 14-28
  - SPARC SuperCluster, 20-28
  - storage libraries, 6-1
  - vDC, 18-9, 18-20, 18-28, 18-29, 18-30
  - virtual datacenter, 18-4, 18-5
- Storage array
  - iSCSI SAN, 6-15
- Storage Connect plug-ins
  - Oracle VM Manager, 6-11
- Storage libraries
  - block storage, 6-5, 6-9
    - dynamic, 6-6
    - static, 6-6
  - file system, 6-3, 6-7, 6-8, 6-9
  - global zones, 14-4
  - high availability, 6-16
  - icons, E-10

- local, 6-3, 6-7
  - creating, 6-8
  - deleting, 6-9
  - editing, 6-8
  - viewing, 6-7
- logical domains, 15-23
- metadata, 6-3
- NAS, 6-5, 6-14, 17-24
- non-global zones, 14-25
- Oracle Solaris Zones, 17-24
- Oracle VM Server, 16-12, 16-13
- Oracle VM Server for SPARC, 15-13, 17-24
- Oracle VM Server for x86, 17-24
- repositories, 6-7
- roles, 6-1
- SAN, 6-4, 17-24
- server pools, 6-3, 17-5, 17-24
- virtual machines, 16-23
- Storage role, 16-13
- Storage servers, 16-12
  - Exadata, 6-16
- Suggested Action, 9-12
- Sun ZFS Storage Appliances, 2-22
  - discovery, 2-23
  - SPARC SuperCluster, 20-19
- SUNWjet, 12-27
- SuperCluster, 20-2
  - icons, E-17
  - See Oracle Engineered Systems, 20-19
- SuperCluster System Admin, 20-20
  - prerequisites, 20-20
- SuperCluster System System Report, 20-30
  - Report Parameters, 20-30
  - Summary Table, 20-30
- Suspend Selected Guest, 16-26
- Switch Management Access, 12-8
- Switches, 7-13, 20-31
  - icons, E-18
  - monitoring policies, 4-11
  - Oracle Engineered Systems, 20-29
  - SPARC SuperCluster, 20-19
- System Catalog, 13-6
  - creating profiles, 13-14
  - updating operating systems, 13-13, 13-14
  - viewing, 13-6
- System Catalog Report, 10-23
- System Information Report, 10-27
- System-defined monitoring policies, 4-9, 4-10
- System-defined rules, 4-3

## T

---

- table refresh frequency
  - user interface preferences, 1-2
- Tags
  - asset attributes, 2-18, 2-24, 2-25
  - service, 2-7
- Take Action on Incident, 9-8, 9-10
- Take Ownership, 16-11
- Task Execution Order, 3-2

- Templates
  - assembly, 18-30
  - deleting report template, 10-3
  - edit report template, 10-3
  - JumpStart Enterprise Toolkit, 12-28
  - Reports, 10-2
  - virtual machines, 16-22
  - vServer, 18-20, 18-26, 18-28
- Thresholds, 4-2, 4-3, 4-6
- time interval
  - user interface preferences, 1-2
- Time zone attributes, A-10

## U

---

- Unassigned incidents, 9-6
- Unbind Network, 14-11, 15-15
- Unbreakable Linux Network, 16-16
- Unconfigured assets, 2-5
- Universal icons, E-19
- Unmanaged fabrics, 7-4, 18-6
- Update job
  - Microsoft Windows, 13-21
- Update Oracle VM Server Host, 16-16
- Update policies, 13-7
  - custom, 13-8
- Update Policy
  - icons, E-20
- Update Profile, 12-48
- Update Profiles, 13-16
  - icons, E-20
- Update profiles, 13-9, 13-10
- Update Virtual Datacenter, 18-9
- updating, 2-16
- Upload, 5-18
  - results, 5-19
- Upload images, 5-12
- User Accounts
  - See *Oracle Enterprise Manager Ops Center Administration Guide*, 20-8
- User Interface Preferences, 9-5
- user interface preferences
  - connectivity check interval, 1-2
  - console timeout, 1-2
  - job status popup duration, 1-2
  - session timeout, 1-2
  - table refresh frequency, 1-2
  - time interval, 1-2
- user preferences
  - membership graph preferences, 1-2
  - user preferences summary, 1-2
- user preferences summary
  - user preferences, 1-2
- User-defined monitoring policies, 4-8, 4-14
- User-defined rules, 4-3
  - Boolean Control, 4-3
  - Enumerated Control, 4-3
  - Expression, 4-3
  - parameters, 4-3
  - rule types, 4-3

thresholds, 4-3

## V

### vDC

- accounts, 18-3, 18-12
  - adding, 18-13
  - deleting, 18-14
  - quotas, 18-19
  - removing, 18-13
  - updating, 18-13
- API, 18-16
- CLI, 18-17
- cloud user, 18-16
- creating, 18-7
- deleting, 18-11
- managing, 18-9
- network, 18-6
- network domain, 18-7
- Networks, 18-10
- networks, 7-8, 18-4, 18-20, 18-21
- operating systems, 18-21
- Oracle Engineered System, 18-2
- requirements, 18-7
- roles, 18-3
- server pools, 18-4, 18-9, 18-11
- storage, 18-4, 18-5, 18-9, 18-20
- storage volumes, 18-28
- updating, 18-9
- user resources, 18-20
- volumes, 18-5
  - creating, 18-28
  - deleting, 18-30
  - importing, 18-29
  - snapshot, 18-29
  - updating, 18-30
- vServer type, 18-14
  - creating, 18-15
  - deleting, 18-16
  - editing, 18-16
  - system-defined, 18-15
- vServers, 18-20
  - cloud user, 18-16
  - creating, 18-20, 18-22
  - managing, 18-23
  - network, 18-21
  - server templates, 18-20, 18-26, 18-28
- vDC Cloud
  - roles, 18-17
- View Alerts, 9-8, 9-9
- View Annotations, 9-8, 9-9
- View Associated Assets, 4-13
- View Comments, 9-8, 9-10
- View Interactive, 10-1
- View Possible Impacts and Causes, 9-8, 9-9
- View Suggested Actions, 9-8, 9-10
- Viewing annotations, 9-20, 9-23
- Viewing comments, 9-20
- Viewing incident details, 9-17
- Viewing unresolved incidents, 9-17

Virtual datacenter See vDC, 18-2

Virtual disk, 6-4

Virtual hosts

- logical domain, 17-1
- non-global zones, 17-1
- virtual machines, 17-1

Virtual image, 5-10

Virtual machines, 15-2, 18-7, 18-20

- creating, 16-21, 16-22
- deleting, 16-26
- deployment plans, 16-24
- monitoring policies, 4-11
- network, 16-13
- network domain, 16-24
- operating systems, 16-25
- Oracle VM Server for x86, 16-20
- profiles, 16-21
- reboot, 16-26
- server pools, 17-24, 17-26
- shutdown, 16-26
- starting, 16-26
- storage libraries, 16-23
- suspending, 16-26
- type, 18-14

Virtual resources, 18-20

Virtual servers, 18-3

Virtual switches, 7-8, 15-13, 15-14, 17-6

Virtualization

- icons, E-14

Virtualization hosts

- adding to server pool, 17-20, 17-21
- control domain, 17-1
- global zone, 17-1
- Oracle Solaris Zones, 17-1
- Oracle VM Server for SPARC, 17-1
- Oracle VM Server for x86, 17-1

Virtualization stack, F-8

Virtualization types, 16-21, 16-22

- HVM, 16-21
- HVM with PV, 16-21
- PVHVM, 16-21
- PVM, 16-21

VLAN, 7-12

VM Type

- See Virtualization types, 16-22

Volumes

- snapshots, 18-30
- vDC, 18-5, 18-28, 18-29, 18-30

vServer type, 18-14, 18-15, 18-16, 18-20, 18-22

vServers, 18-3, 18-11, 18-16

- create server templates, 18-26
- delete server templates, 18-28
- register server templates, 18-28
- update server templates, 18-28
- upload server templates, 18-26
- vDC, 18-20, 18-22, 18-23, 18-26

## W

Wake on LAN, 16-18

- Wake-on-LAN, 16-15
- WAN boot, 12-23
  - disable and enable, 12-25
  - requirements, 12-23
  - setup, 12-24
- Warning, 4-3, 9-16
- Warranty, 9-13, 9-14
- Web Interface, 20-6
- White list, 10-10, 10-13
- Whole root zones, 14-2
  - requirements, 14-14
- Windows
  - discovering, 2-20
  - updating, 13-19
  - Windows Firewall, 2-21
  - WMI, 2-20
- Windows Firewall, 2-20, 2-21
- Windows Management Instrumentation
  - See WMI, 2-20
- Windows Update, 13-19
- WMI, 2-20, 13-19

## **Y**

---

- YUM Repository, 16-16

## **Z**

---

- zone path, 14-18
- Zpools, 12-33, 12-37, 14-21, 14-25