

Oracle® Enterprise Manager Ops Center

Operations Reference

12c Release 3 (12.3.2.0.0)

E59971-04

July 2016

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

E59971-04

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

Primary Author: Uma Shankar

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

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

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

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

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

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

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

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

Contents

Preface	xi
Audience	xi
Related Documents.....	xi
Conventions.....	xi
1 Get Started with Operations	
Oracle Enterprise Manager Ops Center in Your Datacenter	1-1
About This Document	1-2
About the Document Library	1-2
User Preferences and Role Preferences.....	1-4
About the Current User Interface Preferences	1-4
Preferences By Role.....	1-6
Sign In and Start Page Preferences	1-6
Membership Graph Preferences.....	1-6
Time Interval Preferences.....	1-7
2 Understand User Roles	
Ops Center Administrator Role.....	2-1
Cloud Admin.....	2-1
Cloud User	2-1
3 Resolve Incidents	
Introduction to Incidents	3-1
Roles for Incidents	3-2
Actions for Incident Management.....	3-3
Actions for Incidents	3-3
Actions for Service Requests.....	3-4
Actions for Incidents Knowledge Base	3-4
Location of Incident and Service Request Information in the User Interface	3-4
About the Message Center	3-5
Categories in the Message Center	3-6
All Unassigned Incidents Dashboard.....	3-7

My Incidents Dashboard	3-8
About Incident Severity Badges	3-10
Displaying Incident Severity Badges.....	3-10
About Annotations	3-11
Viewing Annotations	3-11
About Creating Annotations	3-12
About the Incidents Knowledge Base.....	3-12
Managing Incidents.....	3-12
Methods of Incident Management.....	3-13
Viewing Unresolved Incidents.....	3-14
Viewing Incident Details.....	3-14
Assigning an Incident.....	3-14
Acknowledging Incidents	3-15
Adding an Annotation.....	3-16
Displaying Annotations.....	3-16
Viewing Comments.....	3-17
Taking Action on a Incident.....	3-17
Marking an Incident Repaired.....	3-18
About Closing an Incident	3-18
Closing an Incident	3-19
About Disabling and Enabling Incidents and Alerts.....	3-19
About Maintenance Mode.....	3-19
About Disabling Alert Monitoring	3-20
Using Oracle Services and Service Requests	3-21
Requirements for Oracle Services	3-21
About Contract and Warranty Information	3-22
Viewing Service Requests	3-23
About Filing a Service Request.....	3-24
About Auto Service Requests	3-24
Related Resources for Incidents.....	3-24

4 Create Reports

Introduction to Reports.....	4-1
Types of Reports.....	4-1
Scheduling Reports	4-3
Output of Reports.....	4-3
Roles for Reports.....	4-4
Actions for Reports.....	4-4
Location of Report Information in the User Interface	4-5
Creating Templates.....	4-5
Generating a Report from a Report Template	4-6
Deleting a Report	4-6
Updating a Report Template.....	4-6

Viewing a Report Result	4-7
Saving a Report Result	4-7
Creating an Operating System Report.....	4-8
Updating Compliance Reports	4-9
Oracle Linux and Oracle Solaris OS Update Reports	4-9
Creating a Change History Report	4-9
Creating a Baseline Analysis Report	4-11
Creating a Baseline Analysis Report	4-13
Profile Analysis Report.....	4-15
Recommended Software Configuration Report	4-17
Creating an Oracle Solaris Update Compliance Report	4-18
Creating an Incident Compliance Report	4-19
Creating a Host Compliance Report.....	4-22
System Catalog Report	4-24
System Information Reports	4-25
Creating System Information Reports.....	4-25
Oracle Engineered Systems Reports	4-26
Creating Oracle Engineered Systems Report	4-26
Incident Reports	4-28
Creating Incident Reports	4-29
Creating a Firmware Report.....	4-30
Creating Additional Operating System Reports.....	4-31
Creating a Distribution Update Report.....	4-32
Creating a Service Pack Compliance Report	4-32
Creating a Package Compliance Report.....	4-33
Related Resources for Reports	4-34

5 Manage the Hardware

Introduction to Managing Hardware Assets.....	5-1
Configuring Hardware Assets.....	5-1
Monitoring Hardware Assets	5-2
Maintaining Hardware Assets.....	5-2
Roles for Hardware Management	5-3
Actions for Hardware Management	5-3
Location of Hardware Information in the User Interface	5-4
Profiles for Hardware Management	5-5
Hardware Resource Profiles	5-5
Firmware Provisioning Profiles	5-5
Configuring the Service Processor	5-6
Creating a Service Processor Configuration Profile and Plan	5-6
Creating a BIOS Configuration Profile and Plan	5-7
Creating a Snapshot of a Service Processor Configuration.....	5-8
Applying a Snapshot of a Server Processor Configuration.....	5-9

Configuring a RAID Controller	5-10
Configuring a Dynamic System Domain	5-10
Configuring a Rack and Placing Components	5-10
Creating a Rack.....	5-10
Placing Assets in a Rack	5-11
Placing a Power Distribution Unit in a Rack.....	5-11
Hardware Monitoring.....	5-12
Hardware Status.....	5-12
Groups of Hardware Assets	5-12
Connectivity Status	5-12
Service Processor Details.....	5-12
RAID Controller Details	5-13
Oracle ZFS Storage Appliance Details	5-13
ALOM and ILOM Servers Details.....	5-14
M-Series Servers Details	5-15
Switch Details.....	5-21
Rack Details	5-22
PDU Details.....	5-23
Oracle Solaris Cluster Details	5-23
Monitoring Power Utilization.....	5-23
Energy Tab.....	5-24
Charts Tab	5-26
Maintaining Hardware Assets.....	5-27
Setting and Changing the Power Policy	5-27
Replacing a Failed Power Distribution Unit in a Rack	5-28
Installing and Upgrading Oracle Solaris Cluster.....	5-29
Firmware Provisioning	5-29
Firmware Profiles	5-29
Firmware Compliance Reports.....	5-30
Updating Firmware.....	5-30
Launching LOM and XSCF Browser User Interfaces.....	5-32
Related Resources for Hardware Management	5-32

6 Manage Operating Systems

Introduction to Operating System Management	6-1
Roles for Operating System Management	6-3
Actions for Operating System Management	6-4
Location of Operating System Management Information in the User Interface	6-5
Viewing Operating Systems.....	6-7
Displaying Operating System Details	6-7
Operating System Profiles	6-9
Using Agent Management for Operating Systems.....	6-9
Virtualization Agent Controllers	6-9

Functionality With and Without Agent Controllers	6-10
Switching Between Agent Controllers or Agent and Agentless	6-11
Monitoring Operating Systems.....	6-13
Disable Operating System Monitoring.....	6-14
Using Analytics	6-14
Displaying Analytics Information	6-15
Displaying the Analytics Summary	6-16
Displaying the Processes View.....	6-18
Displaying the Services View	6-18
Thresholds	6-19
Historical Data	6-21
Metrics.....	6-22
Displaying and Creating Charts.....	6-25
Displaying Virtualization Analytics	6-26
Customizing the Analytics View	6-27
Overview of Oracle Solaris Boot Environments.....	6-27
Understanding the Differences Between Oracle Solaris 11 and Oracle Solaris 10 Boot Environments	6-28
Monitoring Boot Environments	6-28
Boot Environments.....	6-29
Managing Boot Environments.....	6-30
Overview of Oracle Solaris 11 Boot Environments.....	6-32
Displaying Oracle Solaris 11 Boot Environment Details	6-32
About Boot Environment Profiles and Plans for Oracle Solaris 11.....	6-35
Creating an Oracle Solaris 11 Boot Environment	6-36
Overview of Oracle Solaris 10 Boot Environments.....	6-37
Requirements for Oracle Solaris 10 Live Upgrade and Oracle Solaris Zones	6-38
Displaying Boot Environment Details for Oracle Solaris 10	6-39
About Boot Environment Profiles and Plans for Oracle Solaris 10 and Earlier	6-40
Creating an Oracle Solaris 10 Boot Environment	6-42
Synchronizing Oracle Solaris 10 Boot Environments.....	6-47
Activating a Boot Environment.....	6-48
Related Resources for Operating System Management.....	6-48

7 Provision Operating Systems

Introduction to Operating System Provisioning	7-1
Default Profiles and Plans.....	7-4
Deployment Plans	7-4
Roles for Operating System Provisioning	7-5
Actions for Operating System Provisioning	7-5
Location of Operating System Provisioning Information in the UI.....	7-6
Planning for Operating System Provisioning.....	7-6
Enterprise and Proxy Controller Requirements for OS Provisioning	7-7

Networking for OS Provisioning	7-8
Using WAN Boot for Oracle Solaris Operating Systems.....	7-8
Using Dynamic Host Configuration Protocol (DHCP).....	7-12
Determining the Network Interface to Use	7-13
Provisioning an OS Using a User-Defined MAC Address.....	7-15
Defining IPMP in an OS Configuration Profile.....	7-16
Defining Link Aggregation in an OS Configuration Profile	7-16
Adding Images to Local Software Libraries.....	7-18
About NVRAC When Provisioning an OS on a SPARC Platform.....	7-19
Creating Custom Scripts.....	7-19
Determining Agent Management Mode.....	7-19
About OS Provisioning Profiles.....	7-20
About Oracle Solaris OS Provisioning Profiles.....	7-20
About Linux Provisioning Profiles	7-21
About OS Configuration Profiles	7-21
Defining Link Aggregation in an OS Configuration Profile	7-22
Defining IPMP in an OS Configuration Profile.....	7-23
Migrating OS Provisioning Profiles to the New Format.....	7-25
About Deployment Plans That Provision an Operating System	7-26
Provisioning Oracle Solaris 11	7-27
About Oracle Solaris 11 and Provisioning.....	7-27
Steps for Oracle Solaris 11 Provisioning Plan	7-28
Specifying Common Oracle Solaris 11 Parameters	7-29
Creating an Oracle Solaris 11 OS Provisioning Profile	7-30
Creating an Oracle Solaris 11 OS Configuration Profile.....	7-38
Provisioning Oracle Solaris 9 and 10	7-43
Specifying Common Oracle Solaris 9 and 10 Parameters	7-44
About JumpStart Enterprise Toolkit (JET) for Oracle Solaris	7-44
Creating an Oracle Solaris 9 or 10 OS Provisioning Profile	7-45
Creating an Oracle Solaris 9 or 10 OS Configuration Profile.....	7-46
Provisioning an Operating System on Logical Domains.....	7-47
Provisioning an Operating System on an Oracle Solaris Cluster	7-47
Using UAR for OS Provisioning.....	7-47
Provisioning Linux	7-48
Provisioning Linux.....	7-49
Specifying Common Linux Parameters	7-50
Specifying SuSE Parameters	7-50
Related Resources for Operating System Provisioning	7-51

8 Update Operating Systems

Introduction to Operating System Updates.....	8-1
Requirements for Updating Operating Systems.....	8-3
Methods of Running an Update Job	8-4

Options Available When Running an Update Job	8-4
Roles for Operating System Updates	8-4
Actions for Operating System Updates	8-5
Location of Operating System Updates in the User Interface	8-6
Using System Catalogs.....	8-6
Viewing and Modifying a Catalog.....	8-7
Comparing System Catalogs	8-7
About Operating System Update Reports	8-7
Creating Update Policies	8-8
Creating a User-defined Policy	8-9
Creating Update Profiles	8-9
Creating a New Profile	8-10
Updating Oracle Solaris 11 Operating Systems	8-12
Updating Oracle Solaris 11 Operating System.....	8-12
Updating Oracle Solaris 8, 9, and 10 and Linux Operating Systems	8-13
About Operating System Update Jobs	8-14
Updating an Operating System From a Deployment Plan	8-15
Updating an Operating System by Modifying a System Catalog	8-15
Updating an Operating System From an Operating System Report Result.....	8-16
Using a System Catalog.....	8-16
Updating an Oracle Solaris Boot Environment	8-17
Updating a Boot Environment	8-18
Updating Microsoft Windows Operating Systems.....	8-20
About Windows OS Update Jobs.....	8-20
Modify the Registry	8-21
Configure Oracle Enterprise Manager Ops Center for Updating the Windows Operating System.....	8-21
Creating an Update Job for the Windows Operating System.....	8-22
Related Resources for Operating System Updates	8-22

A Logs and Directories

Installation	A-1
Upgrades	A-2
Diagnosing Problems	A-2
High Availability	A-3
Software Update Component	A-3
Agents.....	A-3
Local Database.....	A-3
Controlling the Number of Common Agent Container Log Files.....	A-4

B JumpStart Enterprise Toolkit

JumpStart Enterprise Toolkit Configuration File Location	B-1
SUNWjet Parameters.....	B-1

Downloading Additional JET Packages	B-8
---	-----

C Library Incidents

UUID is not recognized	C-1
------------------------------	-----

Image information is missing.....	C-1
-----------------------------------	-----

File is not readable	C-2
----------------------------	-----

Glossary

Preface

The Oracle® *Enterprise Manager Ops Center Operations Reference* describes all features of the Oracle Enterprise Manager Ops Center software.

Audience

This document is intended for users who require a detailed description of features and functionality.

Related Documents

For more information, see the Oracle Enterprise Manager Ops Center Documentation Library at http://docs.oracle.com/cd/E59957_01/index.htm.

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 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.
monospace	Monospace type indicates commands within a paragraph, code in examples, text that appears on the screen, or text that you enter.

Get Started with Operations

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

The following sections are described in detail:

- [Oracle Enterprise Manager Ops Center in Your Datacenter](#)
- [About This Document](#)
- [About the Document Library](#)

Oracle Enterprise Manager Ops Center in Your Datacenter

As a monitoring tool, the software discovers and identifies all assets in its environment, and displays the status of assets and details of a specific asset. As a provisioning tool, the software deploys new assets in a manner consistent with existing assets because you use profiles to set the attributes and you use plans to deploy the profiles to one target or many targets. As a virtualization manager, the software creates and manages virtual operating systems, virtual servers such as Oracle VM Server for SPARC and Oracle Solaris Zone, and virtual data centers in the cloud.

Various sites and various users within each site value different aspects of the Oracle Enterprise Manager Ops Center software:

- As a monitoring tool, the software discovers and identifies all assets in its environment, and displays the status of assets and details of a specific asset. When an incident occurs, you can track the progress of the investigation or service request.
- As a provisioning tool, the software deploys new assets in a manner consistent with existing assets because you use profiles to set the attributes and you use plans to deploy the profiles to one target or many targets. In a similar way, when assets must be upgraded, you use the update profiles and plans to perform the operations.
- As a virtualization manager, the software creates and manages virtual operating systems, virtual servers such as Oracle VM Server for SPARC and Oracle Solaris Zone, and virtual data centers in the cloud. To support these virtual assets, Oracle Enterprise Manager Ops Center manages and provides resources for storage and networks.

Not every product feature is relevant to your site's activities or for your role. What you see in the user interface is affected by several factors:

- **The role attached to your user account:** The actions for your role are available in the Actions pane. The required roles for using a feature are listed in each chapter of this document. When you must accomplish a task and the necessary action is not available to you, your administrator can add the role to your user account. When you log in again, the action is available.
- **The current connection mode:** In Connected mode, actions that rely on OS and firmware images and packages use the latest images and packages downloaded from Oracle and vendor sites. 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. Also in Connection mode, you can create service request from incidents with full asset information and warranty status. In Disconnected mode, you must contact My Oracle Support and provide this information.

Changing the connection mode can be done easily and temporarily. See the for the procedure for changing the connection mode.

- **The scope of Oracle Enterprise Manager Ops Center:** The product software is designed to manage assets of a data center, from small to large. However, the product software is also installed in an Oracle Engineered System, which is a complete set of integrated hardware and software designed to reach a specific level of capability, capacity, and scale. In this case, the product software is managing the components of the engineered system and the virtual assets that the system supports. Some actions are not relevant to an engineered system and so are not visible in the user interface.

About This Document

This document describes the capabilities of the product software's features.

After the assets have been discovered and brought under the management of the software, as described in the *Manage Assets of the Configuration Reference document*, learn about the assets by selecting each one or each type and viewing the information in the center pane and its tabs.

When you are ready to perform a task such as discovering a type of hardware or upgrading a server's operating system, go to the How To tab of the documentation library to find the example procedure, which demonstrates one set of options. If you do not find an example of the procedure you want to perform, look in this document for the procedure. Use this document to learn about all the options for the product's operations so that you can determine how you will perform the procedure.

Where it is practical, all information about a feature is discussed in the same chapter but there are also links to other documents in the library.

About the Document Library

The document library describes the different tabs present in the library. You can use the site's Search feature to search throughout the library of product documents or to search a specific document. The site can also convert the documents to PDF, EPUB, and Mobipocket file formats.

All documentation for the Enterprise Manager Ops Center 12c Release 3 software is located at the site: http://docs.oracle.com/cd/E59957_01/index.htm.

The documentation library contains the documents in [Table 1-1](#). The Deploy How To tab at http://docs.oracle.com/cd/E59957_01/nav/deployhowto.htm and the Operate How To tab at http://docs.oracle.com/cd/E59957_01/nav/

[operatehowto.htm](#) have links to end-to-end examples and to workflows that combine the examples into deployment and operation scenarios.

Table 1-1 Documents for Enterprise Manager Ops Center

Document	Content
<i>Concepts Guide</i>	An overview of the product software's architecture and its features. This document also explains the product's user interface.
<i>Readme</i>	Links to the installation and upgrade information and a description of known issues in the current release.
<i>Release Notes</i>	Information about the current version, procedures for installation, and known issues.
<i>Installation Guide for Oracle Solaris Operating Systems</i>	Information about planning for a new installation of the product software and the procedure for installing the software on an Oracle Solaris server.
<i>Installation Guide for Linux Operating System</i>	Information about planning for a new installation of the product software and the procedure for installing the software on a Linux server.
<i>Ports and Protocols</i>	Lists the ports used by the product software, the protocol for each port, and its purpose. It also includes the websites that the product software uses.
<i>Upgrade Guide</i>	Information about updating an existing installation of the product software to the current version.
<i>Administration Guide</i>	Procedures for configuring each component of the product software, for configuring the software for high availability, for managing users and roles, and for maintaining the product database. This guide also has procedures for obtaining operating system updates, enabling Auto Service Requests (ASR), using the OCDoctor script, and upgrading the software.
<i>Operations Reference</i>	Descriptions of the product features in detail and with procedures.
<i>Operations for Oracle SuperCluster Reference</i>	Information about Oracle SuperCluster Management.
<i>Command Line Interface Guide</i>	Instructions for using the product's command-line interface and man pages for each command.
<i>Security Guide</i>	Descriptions and procedures for a secure Oracle Enterprise Manager Ops Center deployments.
<i>Certified System Matrix Guide</i>	Supported hardware, operating systems, virtualization technologies, databases, and browsers.
<i>Cloud Infrastructure API and CLI Reference Guide</i>	API and CLI commands to manage programmatically the allocated virtual resources for a virtual datacenter account and to create and manage vServers.
<i>System Monitoring Plug-in for Oracle Enterprise Manager Ops Center</i>	Procedure for installing and configuring the plug-in that enables Oracle Enterprise Manager Ops Center to connect to Enterprise Manager Cloud Control.

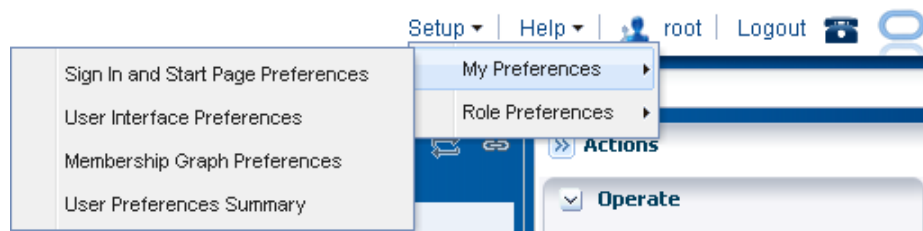
User Preferences and Role Preferences

Describes the features of the user interface.

The *Oracle Enterprise Manager Ops Center Concepts Guide* describes the features of the user interface. Some of the actions and the abilities can be changed, either by an individual user or by an administrator for all users with a specific role.

To see the current specifications or to change the specifications, click **Setup** in the title bar as shown in [Figure 1-1](#) and then click **My Preferences** to view information about how the your account has been specified.

Figure 1-1 Setting User Preferences



About the Current User Interface Preferences

Current User Interface Preferences displays summary window of user preferences.

[Figure 1-2](#) shows the User Preferences Summary window, which displays the current specifications for your start page, time intervals, and each asset type's default tab in the center pane. The current specification for the display of the Membership Graph and the Sign In and Start Page have separate windows.

- [Sign In and Start Page Preferences](#)
- [Membership Graph Preferences](#)

To change the specifications in the User Preferences Summary window, click **User Interface Preferences**. Make changes, then log out and log in again.

Figure 1-2 User Interface Summary

User Preferences Summary

Assigned Roles - User has chosen to customize preferences

Assigned User Roles: Role Management Admin, Asset Admin, User Management Admin, Security Admin, Storage Admin, Read, Fault Admin, Plan/Profile Admin, Ops Center Admin, Report Admin, Cloud Admin, Update Admin, Virtualization Admin, Exalogic Systems Admin, Apply Deployment Plans, Network Admin, SuperCluster Systems Admin

Start Page Preferences

At every sign in, start me on the following view: Assets - All Assets

Display Preferences

Message Center Plan Management Reports vDC Management

Assets Libraries Networks Administration

Incident Badges in Navigation Panel **Enhanced tooltips in Asset Panel** **Show OS for vServers's**

Visible Visible Visible

Timezone of the jobs to be displayed in the Jobs Panel and the Scheduler Panel

User cannot have multiple simultaneous login sessions

Disallow Multiple Sessions

Select one of these options to display nodes in the asset tree
Default option automatically collapses or expands the nodes based on the number of assets present in the group.

Default Expanded Collapsed

Time Intervals

Session Timeout: 30 minutes	Table Refresh Frequency: 30 seconds
Console Session Timeout: 120 minutes	Job Status Popup Duration: 5 seconds
Connectivity Check Interval: 15 minutes	

Asset Default Tab

Name	Start Tab
Rack	Dashboard
PDU	Dashboard
Server	Dashboard
Chassis	Dashboard
Storage	Dashboard

When you change any of the preferences, this window includes a note to indicate that the preferences are not the default specifications.

In the Assigned Roles section, the roles assigned to this user account are listed.

The Start Page Preferences specifies the default view after you log in.

The Display Preferences section provides the following preferences:

- Include or exclude each of the drawers in the Asset pane.
- Show or hide the items in the Asset pane: incident badges, tooltips, and the operating system of a vServer.
- Specify the time zones for the jobs in the Jobs pane.
- Disable simultaneous sessions. The default behavior is to allow a user to log in multiple times. This convenience can be a security risk.
- Change the way assets are expanded or collapsed in the Assets pane. The Default option relies on the number of assets to determine whether the node is expanded or collapsed. You can chose the Expanded option to always show all assets or the Collapsed option to always show only the Asset Type.

The Time Interval section shows the duration of the Session Timeout, the Table Refresh Frequency, the Console Session Timeout, the Job Status Popup Duration, and the Connectivity Check Interval.

The Asset Default Tab section lists each type of asset. For each asset type, you can specify the tab that is the default view displayed in the center pane when an asset of that type is selected.

Preferences By Role

As an administrator, you can set preferences for each role. All user accounts that are assigned the role share the same preferences.

Click **Setup** in the title bar and then click **Role Preferences**. The menu items are the same as for **My Preferences** with the addition of a drop-down list of roles. You select the role and then you select the specifications for all user accounts that have that role.

For example, the default behavior for logging in to the software is to allow the same user to log in multiple times. This is a convenience when monitoring the progress of an operation. However, it can be a security risk so an individual can disable this behavior by checking the **Disable Multiple Sessions** option in the User Interface Preferences window. As an administrator, you can disable this behavior for all users with a certain role by selecting the role and then disabling the option.

Sign In and Start Page Preferences

You can select a section of the Navigation pane as your default view.

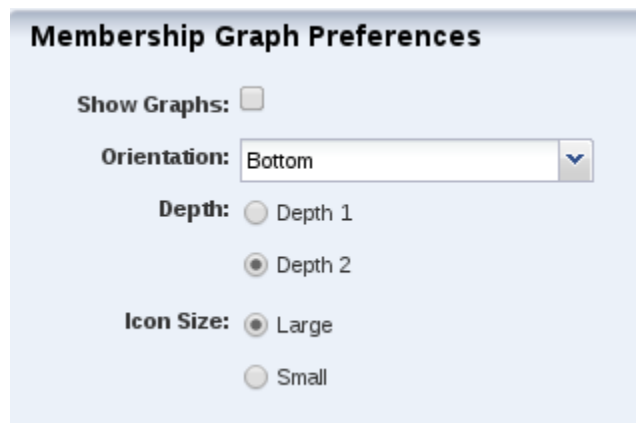
For example, you can specify that you see Plan Management when you log in. The Assets and Administration sections cannot be hidden. When you select Assets for display, you can choose a default tab to display. Your preferences override the default view for your role and any previous preferences that you.

Membership Graph Preferences

You can change the default orientation of the Membership Graph to left, right, top, or bottom. You can choose the icon size as small or large and the level of depth for the assets to be displayed.

Figure 1-3 shows Membership Graph Preferences window.

Figure 1-3 Membership Graph Preferences Window



Each time you perform an operation in the Assets pane, the membership graph in the center pane is refreshed. In a datacenter with many assets, you might experience a noticeable delay during the refresh operation. If you are not making changes to the assets or to their relationships, you can hide the membership graph, which eliminates

the refresh operation. Clear the **Show Graph** option, as shown in [Figure 1-3](#). You see the effect of the change after you select an asset.

Time Interval Preferences

You can set various time intervals to control when the software takes an action or performs an operation.

Select the **User Interface Preferences** action to set various time intervals to control when the software takes an action or performs an operation.

- **Session timeout:** Sets the interval to wait for activity before ending your user interface session. The default value is 30 minutes. You can set the time to wait from 5 to 120 minutes.
- **Console timeout:** Sets the interval to wait for activity from the serial console of managed assets before ending the session. The default value is 120 minutes. You can set the time to wait from 5 to 120 minutes.
- **Connectivity check interval:** Sets the time to wait before the software checks its 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:** Sets the time to wait before refreshing the tables in the user interface. The default value is 30 seconds and the minimum value is 10 seconds.
- **Job status popup duration:** Sets the time to wait after a job completes to display a status message window. The default value is 5 seconds.

Understand User Roles

In Oracle Enterprise Manager Ops Center, users are assigned several roles such as Asset Admin, Cloud Admin, SuperCluster Systems 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 other management roles.

You can add users to Oracle Enterprise Manager Ops Center from the local authentication subsystem of the Enterprise Controller's operating system. Each user is given a different role which grants or denies access to the different functions of Oracle Enterprise Manager Ops Center.

The following user roles are described in this chapter:

- [Ops Center Administrator Role](#)
- [Cloud Admin](#)
- [Cloud User](#)

Ops Center Administrator Role

The Ops Center Administrator user role is only used for initial discovery of the Oracle SuperCluster system.

As an Ops Center Admin user, though you have permissions, do not perform actions that are disabled for the SuperCluster Systems Admin Role. All discovery operations on Oracle SuperCluster systems must be started using Ops Center Administrator account only.

Cloud Admin

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 also its hardware management and OS management in general.

Resolve Incidents

This section describes how you can use the software to identify, assign, and resolve incidents.

The following information is included:

- [Introduction to Incidents](#)
- [Roles for Incidents](#)
- [Actions for Incident Management](#)
- [Location of Incident and Service Request Information in the User Interface](#)
- [About the Message Center](#)
- [About Annotations](#)
- [About the Incidents Knowledge Base](#)
- [About the Incidents Knowledge Base](#)
- [Managing Incidents](#)
- [About Disabling and Enabling Incidents and Alerts](#)
- [Using Oracle Services and Service Requests](#)
- [Related Resources for Incidents](#)

Introduction to Incidents

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:

- [About the Message Center](#): Central location for details on incidents, notifications, and service requests.
- [About Annotations](#): Comments, suggested actions, and operational plans that enable you to effectively manage an incident.
- [About the Incidents Knowledge Base](#): Database of your annotations and actions for specific types of incidents and severity levels.
- [Using Oracle Services and Service Requests](#): Service request details on all requests submitted to My Oracle Support through ASR or the Oracle Enterprise Manager Ops Center UI. See the for information about Auto 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 Incidents

Lists the tasks and the role required to complete the task. You can restrict privileges to specific targets or groups of targets.

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 for information about the different roles and the permissions they grant.

Table 3-1 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 3-1 (Cont.) Incident Management Tasks and Roles

Task	Role
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. Your role determines the actions that you can perform on incidents.

A incident consists of one or more alerts. The following incident details are recorded:

- 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

Actions for Incidents

Lists the various actions that you can perform on a specific incident.

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

Lists the 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 section.

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

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 warnings that are assigned to you.

Figure 3-1 Incidents Ticker



Click an icon to display the incidents dashboard for that category. You can also view incident details by expanding the asset and clicking the Incident tab.

Use the Message Center in the Navigation pane to view and manage notifications, service requests and an asset's warranty information.

Table 3-2 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.
Incidents assigned to you	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.

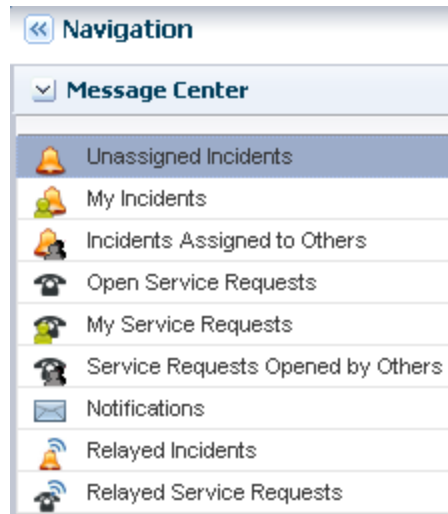
About the Message Center

Incidents, notifications, and service requests that are generated by assets appear in the Message Center.

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 but the incident is not cleared automatically. 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. While an incident is not closed, new alerts are aggregated into the existing incident. You must close an incident to clear it from the user interface.

Incidents, notifications, and service requests that are generated by assets appear in the Message Center, shown in [Figure 3-2](#), according to the categories described in [Categories in the Message Center](#).

Figure 3-2 Message Center

Categories in the Message Center

Lists the different categories in the message center. Incidents, notifications, and service requests appear in those categories 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 in to 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.

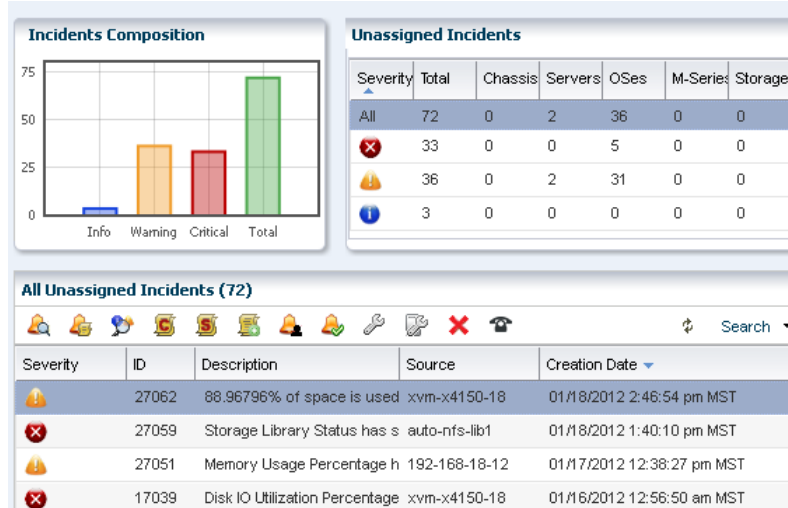
My Incidents, Unassigned Incidents, and Incidents Assigned to Others have a dashboard with the same format: a bar chart, a table of incident counts sorted by severity and asset, and a table of incidents sorted by ID.

All Unassigned Incidents Dashboard

The All Unassigned Incidents dashboard 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 3-3 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, to whom the incident was assigned, any suggested actions, the source of the incident, 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 Link Figure 9–3:

- View Alerts
- View Annotations
- View Possible Impacts and Causes

- View Comments
- View Suggested Actions
- Add Annotation to Incidents
- Assign Incidents
- Acknowledge Incidents
- Take Actions on Incident
- Mark Incidents as Repaired
- Close Incidents

Figure 3-4 Incident Actions

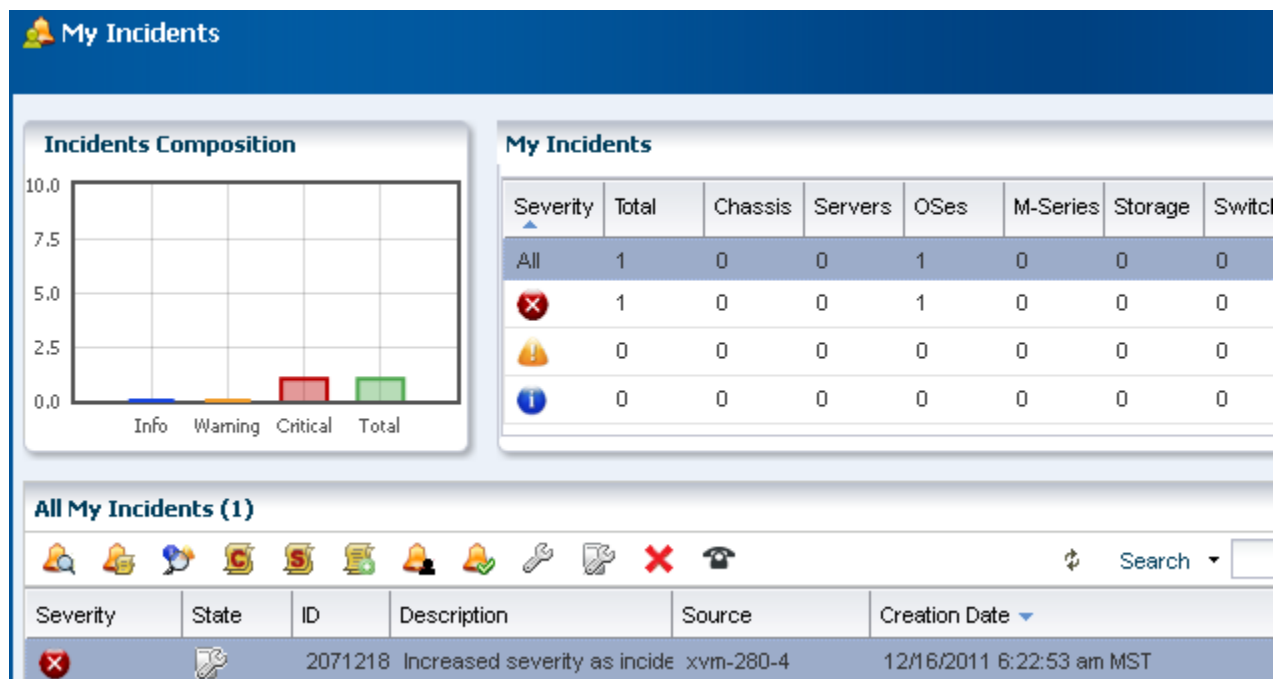


My Incidents Dashboard

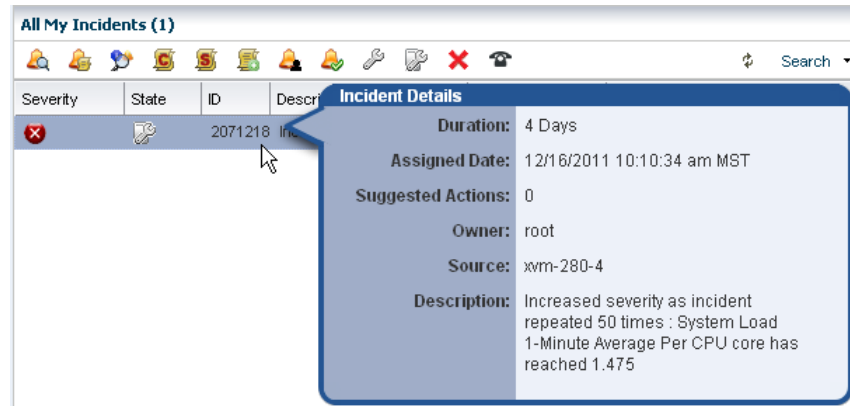
Incidents assigned to you appear in the My Incidents dashboard in the Message Center. Anybody with the appropriate permission level can see the incidents in your queue, can reassign incidents to another user, and can assign you new incidents.

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.

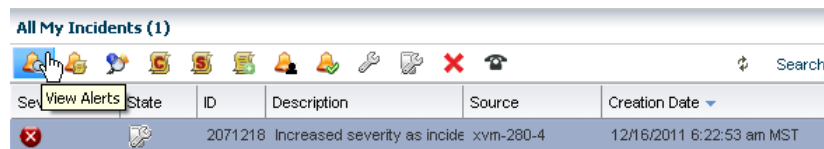
Figure 3-5 My Incidents



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 3-6 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 text to define the action.

Figure 3-7 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 Incidents
- Assign Incidents
- Acknowledge Incidents
- Take Actions on Incident
- Mark Incidents as Repaired
- Close Incidents
- Open a Service Request

The Notifications appear in the Message Center. You can also configure the software to send you e-mail or pager notification of incidents for critical assets or severity levels.

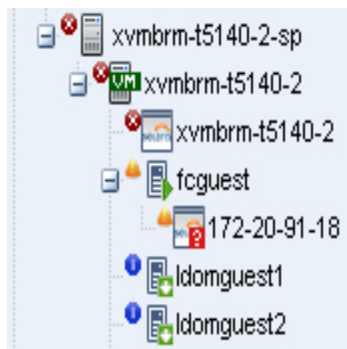
About Incident Severity Badges

You can display incident severity badges next to an asset in the Navigation pane and in the dashboard's membership graph. The highest severity badge in a group is also displayed next to the parent asset.

See Badges in the *Oracle Enterprise Manager Ops Center Concepts Guide* for a description of each badge.

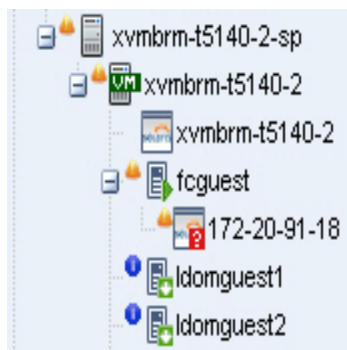
Figure 3-8 shows the example of the operating system for the asset `xvmbrrm-t5140-2` with a critical incident. The critical incident badge also appears on the system and service processor. Every group that this OS is a member of, such as All Assets and Operating Systems, also displays the badge.

Figure 3-8 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 3-9 Warning Incident Badge



After the incident is closed, its severity badge is not displayed in the asset hierarchy.

Displaying Incident Severity Badges

Procedure to display the badges in the Navigation pane.

1. Click **Setup** in the upper right corner of the UI.
2. Click **My Preferences**, then click **User Interface Preferences**.

3. Click the check box to make the badges visible in the user interface.

About Annotations

Annotations are comments, suggestions, or automated operations that run scripts. They are defined by an asset type, asset resource type, an attribute, or an incident type.

They are defined by an asset type, asset resource type, an attribute, or an incident type. At a minimum, use annotations in text to document an incident. You can also use annotations to build a Incidents Knowledge Base that contains a mixture of comments, suggested actions, and automated annotations that run scripts to perform operations. Annotations enable you to provide solutions or recommended actions for specific incidents.

You can **View Annotations**, **View Possible Impacts and Causes**, **View Comments**, **View Suggested Actions**, and **Add Annotations** associated with an incident in the Message Center or from the Incidents tab in the Asset view, as shown in [Figure 3-10](#).

Figure 3-10 Annotation Icons



Viewing Annotations

Annotations are available from several different locations in 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 section), when an annotation is associated with an asset type

When an annotation is associated with an incident, use the **View Annotations** icon to browse 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 3-1 Example Annotation

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.

About Creating Annotations

You can create annotations while you are working on a resolution, when you mark an incident as fixed, and when you close an incident. You can create annotations by asset type, asset resource type, attribute, or incident type.

Annotations contain automated operations with an operational profile, suggested fixes or actions, or text comments.

You have the option to add annotations for incident types to the Incidents Knowledge Base (KB). You can associate Automated Action and Suggested Action annotations with an operational profile, which can contain a script.

When you create an annotation, other users who have set up notification profiles to use e-mail or a pager are informed about the new annotation and see its content.

To see the procedure for creating annotations, see [Adding an Annotation](#).

About the Incidents Knowledge Base

The Incidents Knowledge Base contains your annotations, by asset type, and stores the information on the Enterprise Controller. Use annotations to collect information from prior incidents, add suggested fixes, or run automated fixes for a specific type of incident. You can add possible causes and impacts. You can create, update, and delete annotations in the Incidents Knowledge Base.

Annotations can be associated with 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. 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 a rule is triggered, and an alert or incident is identified, 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. Any Operational Profiles referenced in Automated Operation annotations are executed against the asset on which this incident was open. When a suggested action annotation is associated with the incident, the text and script (when available) appear in the incident details.

You can add annotations to the Incidents Knowledge Base in Plan Management or from a specific incident.

The following types of Annotations are available:

- **Automated Operation:** An annotation that references an Operational Profile and executes the profile when a specific incident occurs.
- **Suggested Action:** An annotation containing a suggested fix or course of action for a specific incident. The suggested course of action can be in text or you can refer to an Operational Profile.
- **Comment:** An annotation in text that updates the status or reports activity about an incident.

Managing Incidents

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 manage 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, 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.

Viewing 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.

Viewing Incident Details

Procedure 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.

Assigning 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 Incidents** 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 relocate 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**.

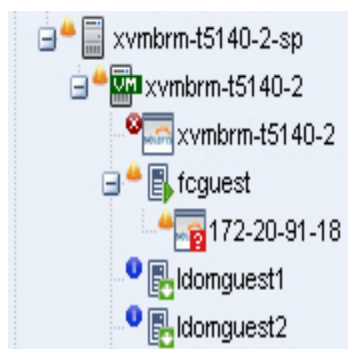
Acknowledging Incidents

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.

Acknowledging an incident might affect the asset's Incident severity badge. When the incident was 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 3-11 *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.

Adding 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. The UI does not have a character limit, 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**.

Displaying 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 appear in the center pane.

Viewing Comments

Procedure to view comments.

A comment is a type of annotation. To add a comment, see [Adding 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.
3. Click the **View Comments** icon.

Taking 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 an automated annotation, if one has been associated with the same issue. For other incidents, review the issue before deciding on the appropriate action.

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 Actions** 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, enter 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**.

Marking an Incident Repaired

The software cannot determine when an incident is repaired. However, you can open a known incident and 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.

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 Incidents as Repaired** icon in the center pane.
3. (Optional) Select the incident, then add a Note.
4. Click **Tag Incidents as Being Repaired**.

About Closing 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.

Closing 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 Incidents** 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. The action disables the monitoring rule for only the assets that were related to the incident to avoid raising a similar incident on the same assets.

5. Click **Close Incidents**.

About Disabling and Enabling Incidents and Alerts

Incidents and alerts are enabled by default. You can disable incidents from generating on individual assets or a group of assets. You can disable monitoring policies and prevents incidents and alerts from generating on all assets in your data center.

- [About Maintenance Mode](#): Disables incidents from generating on individual assets or a group of assets. This feature is designed to temporarily disable incidents while you perform maintenance tasks.
- [About Disabling Alert Monitoring](#): Disables monitoring policies and prevents incidents and alerts from generating on all assets in your data center.

Note:

Neither option disables the collection of data on managed assets.

About 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, reconfigure a system manually, or perform maintenance on a system and you do not want these incidents to be reported.

Note:

Monitoring still occurs and alerts are still generated on the asset while in maintenance mode. View alerts by selecting the **Alerts** subtab of the Incidents tab.

When you place an asset in maintenance mode, the severity badge of unassigned and assigned incidents affecting the asset and its children is not propagated in the asset hierarchy in the Navigation pane.

When you place a Proxy Controller in maintenance mode, you disable incidents from generating on the Proxy Controller and you disable all jobs that go through the Proxy Controller, including discovering, managing, and migrating assets.

When you place an Oracle VM Server that is a member of a server pool 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. 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. While in maintenance mode, you cannot create or place guests and guests cannot be recovered to the server from another control domain. When the Oracle VM Server is not a member of a server pool, or other servers are not available in the server pool, the virtual machines are stopped. To manually bring down the control domain and all of its guest domains, use the action **Disable Automatic Recovery** on the virtual machines to disable the auto-recovery, then put the control domain in maintenance mode.

Placing Assets in Maintenance Mode

Procedure to place assets in maintenance mode.

1. Select an asset in the Navigation pane.
2. Click **Place in Maintenance** in the Actions pane.
3. Click **Place** to confirm the action.

Removing Assets From Maintenance Mode

Procedure to remove assets from maintenance mode.

When the maintenance operations are completed, use the **Remove From Maintenance** action to restore the display of severity badges.

1. Select the asset in the Navigation pane.
2. Click **Remove From Maintenance** in the Actions pane.
3. Click **Remove** to confirm the action.

About Disabling Alert Monitoring

You can disable alerts and incidents for all assets in your data center by disabling all of the monitoring policies.

When you disable the policies, the monitors are no longer deployed on the assets. When you enable monitoring that you previously disabled, the monitoring rules defined by the default monitoring policies are reapplied to all of the assets.

Note:

Disabling monitoring disables the evaluation of monitoring rule conditions against collected data and prevents the deployment of monitors across your data center, it does not disable the collection of data on managed assets.

Disabling all monitoring for your data center is only available from the command line interface. See *Oracle Enterprise Manager Ops Center Command Line Interface Guide* for more information. See [About Maintenance Mode](#) for information about temporarily disable the software from generating incidents.

Using 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, Oracle 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 a service request filed outside of Oracle Enterprise Manager Ops Center, go to the Service Requests Home page on My Oracle Support.

Requirements for Oracle Services

Lists the requirements to use 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 3-12](#). 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 3-12 Connection Icons



About Contract and Warranty Information

When the serial number of the selected asset is associated with a My Oracle Support contract, a Support row is added to the Summary tab, displaying the contract ID and expiration date.

You can display contract information by asset or you can obtain entitlements associated with all contracts that are associated with a user. When the serial number of the selected asset is associated with a My Oracle Support contract, a Support row is added to the Summary tab, displaying the contract ID and expiration date.

The contract and warranty information is updated each week so contract changes or new contracts might take up to seven days to appear in the Summary tab.

When a contract or warranty is about to expire, an alert is displayed as an Incident in the Message Center and the display of information in the Summary tab changes:

- If the contract is within 90 days of expiration, the text color is orange.
- If the contract has expired, the text color is red.

Note:

Updating contract and warranty information requires using the product software in Connected mode. If you change to Disconnected Mode, the contract information becomes outdated.

Viewing Contract and Warranty Information for an Asset

Procedure 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.

The Support row of the Summary tab shows the contract ID and expiration date.

Viewing All Contracts Associated with a My Oracle Support Account

Procedure to view all contracts associated with a MOS 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.

Viewing Service Requests

The service request contains information about the request, including the request number, severity, a summary of the problem, the date and time last updated, contact information, and status.

You can see all current and completed service requests that are filed through Enterprise Manager Ops Center.

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 3-13 View Service Request

Oracle Enterprise Manager Ops Center - View Service Request

Information

Request Number	3-1863062401
Severity	1-Critical
Summary	Problem detected on: hs-x4100-2 - 172.20.28.190
Last Updated	Tue Oct 19 2010 15:13:34 GMT-0600 (MST)
Contact	MOSPatchOCMCollector Test
Status	Open
Sub Status	New
SR Email	mospatchtest14@sleepycat.com
SR Telephone	415-999-0000
Support ID	17251035
Address	Oracle UK Headquarters Oracle Parkway CA Reading RG6 1RA United Kingdom

Description

Problem detected by Ops Center instance: https:
 * Ops Center Problem ID: 432 Problem Severity: CRITICAL
 * Problem Description: hs-x4100-2 - 55.775578% of space is used on / filesystem.

Fri Oct 01 2010 22:37:10 GMT-0600 (MST)

Problems reported by Ops Center:
 Current Problem:
 Severity: CRITICAL
 ID: 432
 State: UNASSIGNED
 Description: hs-x4100-2 - 55.775578% of space is used on / filesystem.
 Creation Date: Fri Oct 01 16:36:02 MDT 2010

Associated Alerts:

Alert Type	Alert Source	Attribute	Current Status	Highest
Threshold	hs-x4100-2	FileSystemUsages.name=/.usedSpacePercentage	CRITICAL	CRITICAL

4. Click **Close**.

About Filing a Service Request

When your assets are associated with a contract and registered in the My Oracle Support database, you can create a service request directly from an incident or from an asset.

See [Requirements for Oracle Services](#) for requirements that must be met before filing a service request ticket. If the asset is not registered in My Oracle Support, the service request job fails. If the **Open Service Request** action is not available, the product software does not have a connection to My Oracle Support.

Filing a Service Request From an Incident

Procedure 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.

Filing a Service Request From an Asset

Procedure to file a service request from an asset.

1. Select the hardware in the Assets section of the Navigation pane.
2. Click **Open Service Request** in the Actions pane.

About Auto Service Requests

You can configure Oracle Enterprise Manager Ops Center to create service requests automatically for known issues. When Auto Service Requests (ASRs) are enabled, Oracle Enterprise Manager Ops Center generates service requests based on critical incidents.

Instead of manually filing a service request, you can configure Oracle Enterprise Manager Ops Center to create service requests automatically for known issues. When Auto Service Requests (ASRs) are enabled, Oracle Enterprise Manager Ops Center 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. 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 information about configuring and using auto service requests.

Related Resources for Incidents

This section lists the related resources for incidents.

For more information, see the Oracle Enterprise Manager Ops Center Documentation Library at http://docs.oracle.com/cd/E59957_01/index.htm.

For end-to-end examples, see the workflows and how to documentation in the library. For deployment tasks, go to http://docs.oracle.com/cd/E59957_01/nav/deploy.htm, for operate tasks go to <http://docs.oracle.com/cd/>

E59957_01/nav/operate.htm, and for administer tasks go to http://docs.oracle.com/cd/E59957_01/nav/administer.htm.

See the following How To documents:

- *Oracle Enterprise Manager Ops Center Managing Incidents*
- *Oracle Enterprise Manager Ops Center Tuning Monitoring Rules and Policies*
- *Oracle Enterprise Manager Ops Center Understanding OS Performance and Capacity*
- *Oracle Enterprise Manager Ops Center Using Service Requests*

See the *Oracle Enterprise Manager Ops Center Concepts Guide* for a description of the icons.

The *Oracle Enterprise Manager Ops Center Administration Guide* has information about user roles and permissions.

See *Monitoring Rules and Policies* for more information about creating and maintaining rules and profiles for creating incidents.

Create Reports

This chapter describes how to create reports in Oracle Enterprise Manager Ops Center. This chapter includes the following information:

- [Introduction to Reports](#)
- [Roles for Reports](#)
- [Actions for Reports](#)
- [Location of Report Information in the User Interface](#)
- [Creating Templates](#)
- [Generating a Report from a Report Template](#)
- [Deleting a Report](#)
- [Updating a Report Template](#)
- [Viewing a Report Result](#)
- [Saving a Report Result](#)
- [Creating an Operating System Report](#)
- [System Information Reports](#)
- [Oracle Engineered Systems Reports](#)
- [Incident Reports](#)
- [Creating a Firmware Report](#)
- [Creating Additional Operating System Reports](#)
- [Related Resources for Reports](#)

Introduction to Reports

Reports provide information about assets, such as job history, firmware, operating system updates, and incidents.

You can use the Reports feature to consolidate changes to hardware, software, and job conditions. You can use reports to export the information or to start jobs on targeted assets.

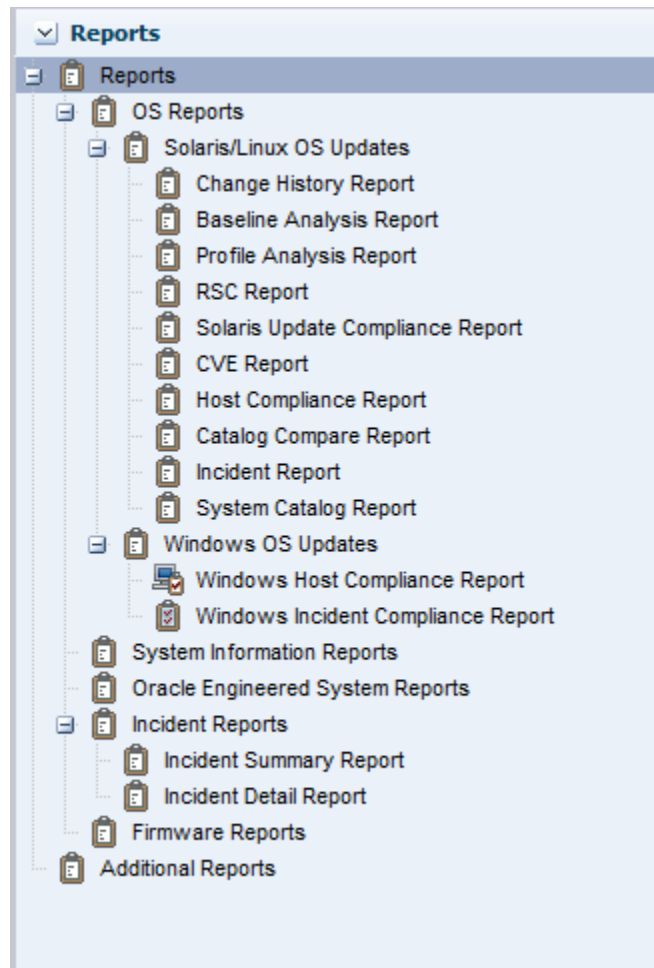
Types of Reports

Displays the types of reports.

Reports are grouped in Oracle Enterprise Manager Ops Center in the following way:

- **OS Reports:** OS reports includes Oracle Solaris Update reports, Oracle Linux Update Reports, and Windows Update reports. They enable you to check for new patches and security advisories. You can get a general report, or test a system or installed package for available fixes. See [Creating an Operating System Report](#) for more information.
- **System Information Reports:** System Information reports are used to obtain the information on assets such as OS, server, chassis, logical domains, global zone, non-global zone, and M-Series server. See [System Information Reports](#) for more information.
- **Oracle Engineered System Reports:** Oracle Engineered System reports enables you to view the rack setup for each of the rack within the system including the asset details related to the rack. These reports provide information about your assets, such as job history, firmware, OS updates, and incidents. See [Oracle Engineered Systems Reports](#) for more information.
- **Incident Reports:** Incident report 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. It also includes an audit trail consisting of state-change annotations, alert annotations, suggested-fix annotations, comment annotations, operation annotations. See [Incident Reports](#) for more information.
- **Firmware Reports:** Firmware Reports enables you to maintain consistent firmware versions across your data center. The Firmware Report feature compares the firmware images specified in a firmware profile to the firmware images installed on one or more hardware assets. The report indicates whether the firmware on the asset complies with the profile's specifications. See [Creating a Firmware Report](#) for more information.
- **Additional Reports:** Additional Reports enables you to obtain information from Service Pack Compliance Report, Distribution Update Report, and Package Compliance Report. See [Creating Additional Operating System Reports](#) for more information.

[Figure 4-1](#) displays the Reports of Oracle Enterprise Manager Ops Center.

Figure 4-1 Reports in Oracle Enterprise Manager Ops Center

Scheduling Reports

You can schedule to run the report using a set of specified 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.

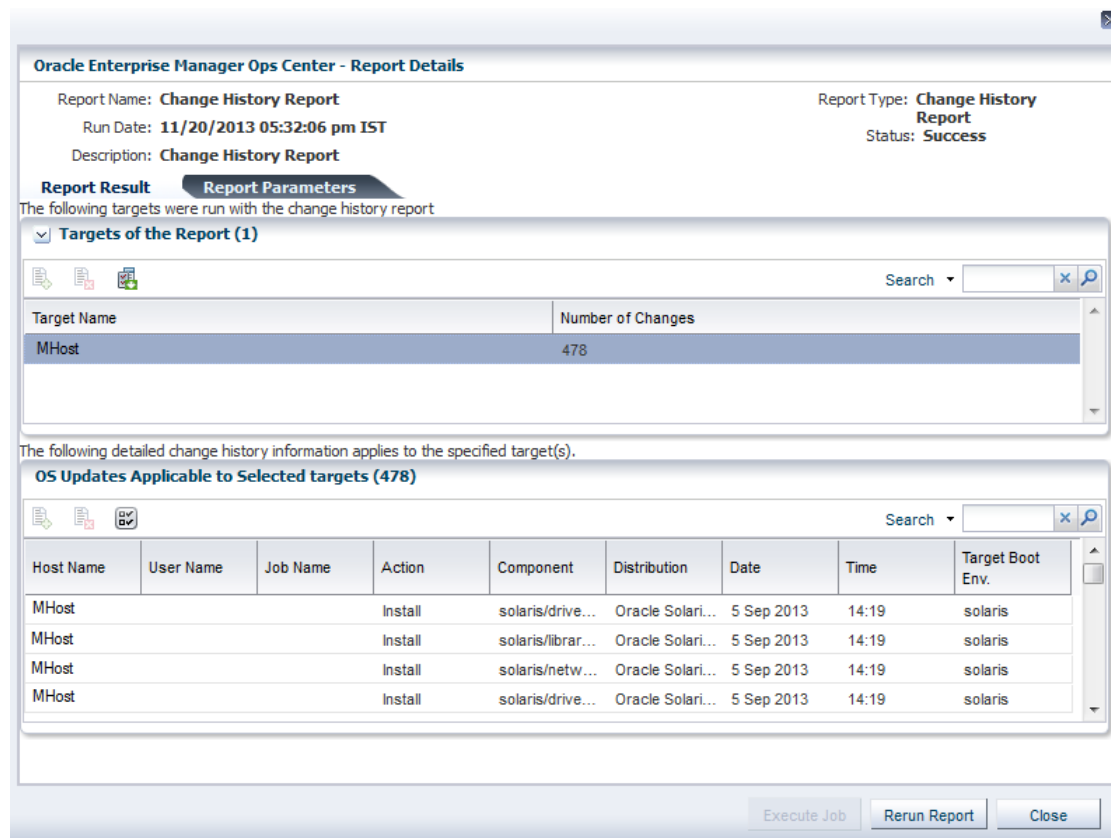
Output of Reports

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 4-2 displays an Interactive view of Report Result.

Figure 4-2 Interactive View of Report Result



Roles for Reports

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 for information about the different roles and the permissions they grant. [Table 4-1](#) illustrates the roles and permissions for reports.

Table 4-1 Reports Tasks and Roles

Tasks	Roles
View Reports	All
Create Reports	Asset Administrator

Actions for Reports

Lists the actions for reports.

You can perform the following actions in the reports section.

- Generate a Report from a Report Template
- Update a Report
- Delete a Report

- View a Report Result
- Save a Report Result

Location of Report Information in the User Interface

To see report information, expand Reports in the Navigation pane. This 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 4-2](#) illustrates the location of reports in the user interface.

Table 4-2 Location of Report Information in the UI

Object	Location
OS Reports	Expand the Reports 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 in the Navigation pane. Click System Information Reports. This displays the Create System Information Report wizard in the Actions pane.
Oracle Engineered System Reports	Expand the Reports in the Navigation pane. Click Oracle Engineered System Reports. This displays the Create Oracle Engineered System Report wizard in the Actions pane.
Incident Reports	Expand the Reports in the Navigation pane. Click Incident Reports. This displays the types of incident reports.
Firmware Reports	Expand the Reports in the Navigation pane. Click Firmware Reports. This displays the Create Firmware Report wizard in the Actions pane.
Additional Reports	Expand the Reports in the Navigation pane. Click Additional Reports. This displays the Distribution Update Report, Service Pack Compliance Report, and package Compliance Report wizards in the Actions pane.

Creating Templates

A report template is a pre-formatted file that serves as a starting point to create a new report. When you save a file created from a template, you are prompted to save a copy of the file so that you do not overwrite 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.

You can create a report template for any type of a report. In this example, you will create a report template for Change History Report. To create a report template, do the following:

1. Select **Reports** from the Navigation pane.

2. Select **Change History Report** and click **Create Change History Report** in the Actions pane. The **Create Change History Report** wizard is displayed.
3. 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**.
4. Click **Next** to schedule the report.
5. Select a desired schedule to run and generate the report.
6. Click **Next** to display the Summary.
7. Review the report parameters and click **Save Template and Close** to save the report template.

The created report template is displayed in **Report Templates** in the center pane.

Generating a Report from a Report Template

Procedure to generate a report from the report template.

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.

Deleting a Report

Procedure to delete a report from the report template.

1. Select **Reports** from the Navigation pane.
2. Select a saved report to delete from the center pane.
3. Click the **Delete Report** icon to delete the report.
4. Click **Ok** to confirm the delete action. The selected report is deleted.

Updating a Report Template

Procedure to update a report from the report template.

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.

Viewing a Report Result

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.

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 **View Interactive** icon to view the report result. The **Interactive Result viewer** opens the report result and displays the following information.
 - Report detail: This displays the name, type, run time, and the status of the report.
 - Report Result: This displays the targets on which the report is run and the corresponding operating system updates that are applicable.
 - Report Parameters: This displays the parameters that are used to generate the report.

Saving a Report Result

After you create and generate a report in Oracle Enterprise Manager Ops Center, you can save a report result in CSV or PDF format.

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 4-3](#) illustrates the report output in PDF format.

Figure 4-3 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
-------------	-------------------

Creating an Operating System Report

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 4-3](#) 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 4-3 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	No	No
RSC Report	Yes	Yes	No	No
System Catalog Report	Yes	Yes	Yes	No
Oracle Solaris Update Compliance Report	No	Yes	No	No
Baseline Analysis Report	No	Yes	No	No
Update Compliance Report	Yes	Yes	No	No
Incident Compliance Report	Yes	Yes	No	Yes
Host Compliance Report	Yes	Yes	No	Yes
Distribution Update Report	Yes	Yes	No	No
Service Pack Compliance Report	Yes	No	No	No
Package Compliance Report	No	Yes	No	No

Updating Compliance Reports

Host Compliance and Incidence Compliance reports are available for Linux, Oracle Solaris, and Windows operating systems.

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.

Oracle Linux and Oracle Solaris OS Update Reports

In addition to the reports created for all types of operating systems, reports are available for Oracle Linux and Oracle Solaris operating systems also.

- **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, CVEs, 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.
- **Recommended Software Configuration (RSC):** 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):** This helps to check the compliance of systems against newly released Oracle Solaris baselines.

Creating a Change History Report

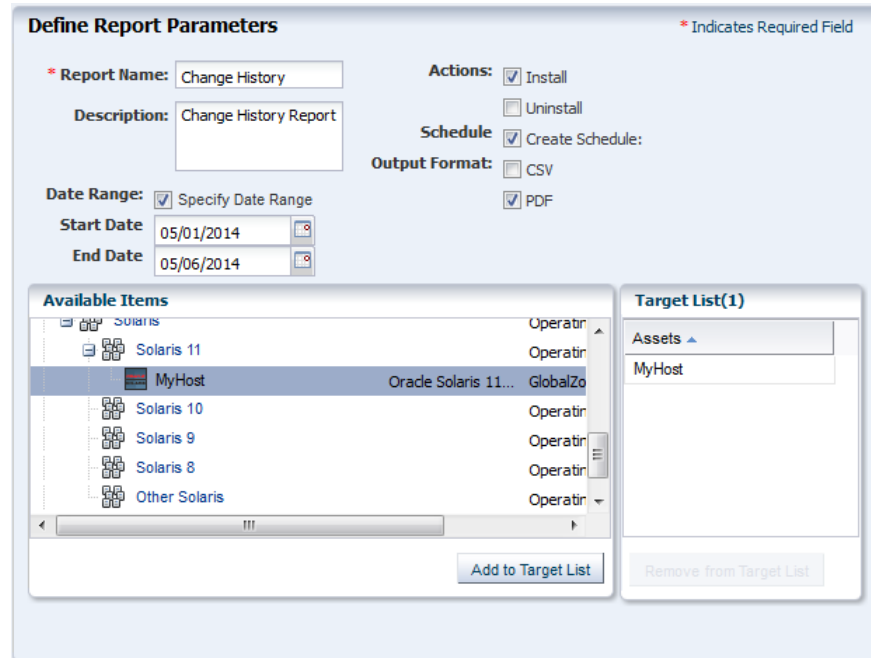
The Change History Report provides a history of operating system update install and uninstall jobs completed on managed Oracle Solaris or Linux systems. The report also displays the deployments made by the specific user, enabling you to track a team of operators.

Perform the following steps 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 4-4 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 [Viewing a Report Result](#) for more information about viewing a report result.

Creating a 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. This 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 deselecting this option.

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.

Creating 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 4-5 Selecting Baselines for Baseline Analysis Report

The screenshot displays the Oracle Enterprise Manager Ops Center interface for a report titled "Oracle Enterprise Manager Ops Center - Report Details".

Report Details:

- Report Name: **BAR1**
- Run Date: **01/10/2011 01:19:18 pm IST**
- Report Type: **Baseline Analysis Report**
- Status: **Successful But Not Compliant**

Report Result (Selected):

The following targets were run with the Baseline Analysis Report

Baseline	Target	OS	No of Changes	Status
Baseline 2010/12/08 [Full]	Host_1	SOLARIS_10_0_X86	161	NONCOMPLIANT

The following detailed Baseline Analysis information applies to the specified target(s).

OS Updates Applicable to Selected targets (161)

Target	Baseline	Action	Incident	Synopsis	Link
Host_1	Baseline 2010/12/08 [Full]	Install	125389-03	SunOS 5.10_x86: SNIA	www.example.com
Host_1	Baseline 2010/12/08 [Full]	Install	125216-03	SunOS 5.10_x86: wvget	www.example.com
Host_1	Baseline 2010/12/08 [Full]	Install	122260-03	SunOS 5.10_x86: SunFr	www.example.com
Host_1	Baseline 2010/12/08 [Full]	Install	142235-01	SunOS 5.10_x86: ntp.xr	www.example.com
Host_1	Baseline 2010/12/08 [Full]	Install	119118-52	Evolution 1.4.6_x86 patc	www.example.com

Buttons at the bottom: **Make Targets Compliant**, **Rerun Report**, **Close**

- 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 [Viewing a Report Result](#) 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.

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.

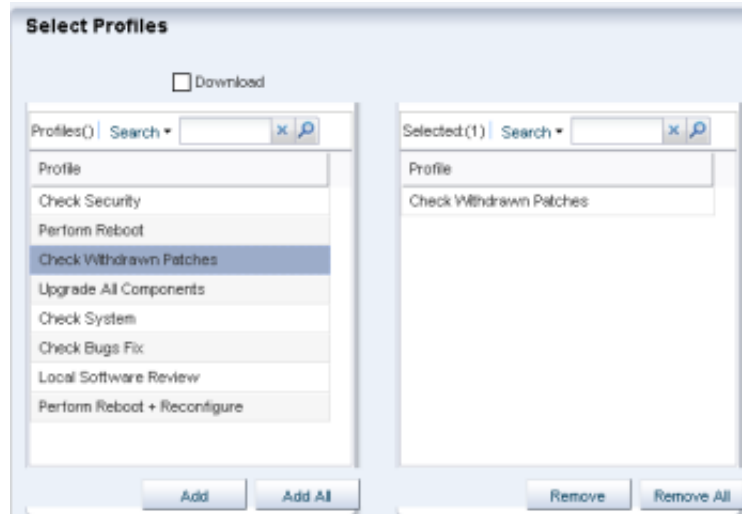
Creating Profile Analysis Report

Procedure 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 4-6 *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 [Viewing a Report Result](#) 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.

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.

Creating Recommended Software Configuration Report

Procedure 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 [Viewing a Report Result](#) for more information about viewing a report result and generating a compliance job from the result.

Creating an 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, perform the following steps:

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.

Creating an Incident Compliance Report

You can run an incident compliance report to determine whether the incidents on the managed hosts are compliant with the latest released version.

Incidents are the updates that are available for an application or feature. Incidents apply to one or more packages or RPMs.

Creating an Incident Compliance Report for Oracle Solaris or Linux

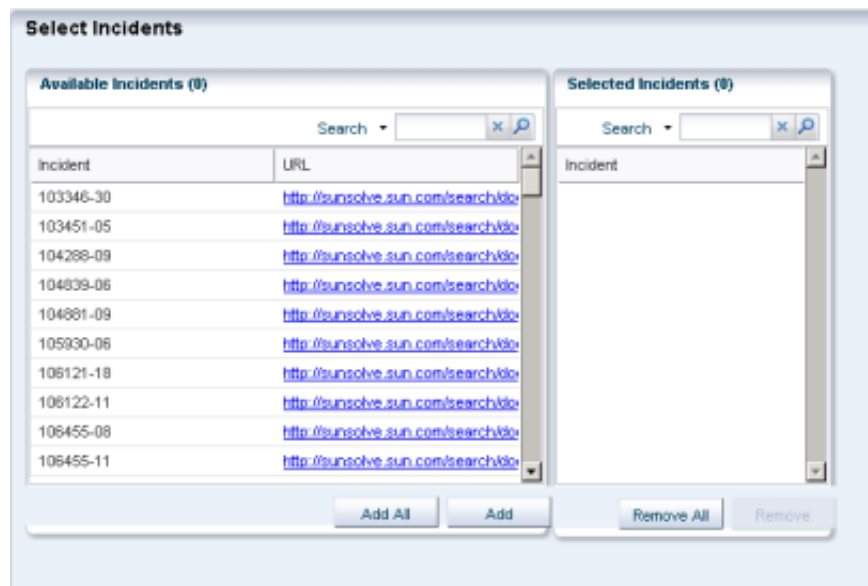
Procedure to create an Incident Compliance Report for Oracle Solaris or Linux.

You can run an incident compliance report to determine whether the incidents on the managed hosts are compliant with the latest released version.

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 4-7 *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 [Viewing a Report Result](#) for more information about viewing a report result and generating a compliance job from the result.

Creating an 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 Microsoft Windows, perform the following steps:

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.

Creating a 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.

Creating 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, perform the following steps:

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 [Viewing a Report Result](#) for more information about viewing a report result and generating a compliance job from the result.

Creating 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 Microsoft Windows, perform the following steps:

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.

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.

Creating a System Catalog Report

Procedure 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 [Viewing a Report Result](#) for more information about viewing a report result and generating a compliance job from the result.

System Information Reports

You can 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.

The information on assets include details like architecture, type, host id, host name, logical units, version, description and so on.

Creating System Information Reports

Procedure to create a Systems 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 [Viewing a Report Result](#) for more information about generating a compliance job from the result.

Oracle Engineered Systems Reports

The Oracle Engineered Systems report is all about viewing the rack setup for each of the rack within the system including the asset details related to the firmware.

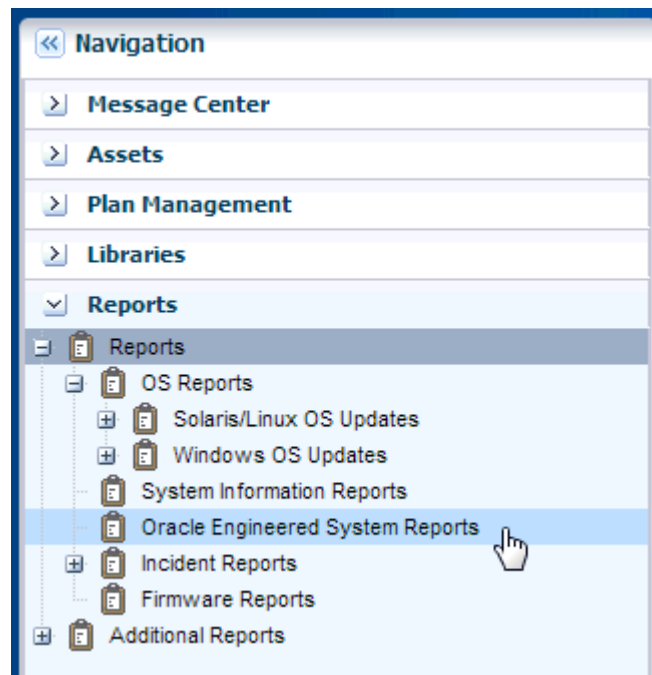
Using Oracle Enterprise Manager Ops Center, you can discover and manage Oracle Engineered Systems. You can view and access multiple Engineered Systems from a single datacenter through Oracle Enterprise Manager Ops Center. You can also view the Engineered System's assets, incidents reported from the Engineered Systems, and Service Requests. You can generate reports for all datacenter assets, including Engineered Systems. This also displays the number of assets in the rack by their types, such as compute nodes, switches, and storage nodes in the system.

Creating Oracle Engineered Systems Report

Procedure to create an Oracle Engineered Systems report.

You can generate and view the report for multiple engineered systems. Perform the following steps to create an Oracle Engineered Systems Report.

1. On the Navigation pane, click **Reports**.

Figure 4-8 Create Oracle Engineered System Reports

2. Click **Oracle Engineered Systems Reports**.
3. On the Actions pane, click **Create Oracle Engineered Systems Report**.
4. In the **Define Report Parameters** wizard, enter a name and description for the report.

The Schedule and Output Format are checked by default.

Figure 4-9 Oracle Engineered Systems Report Parameters

 A screenshot of the 'Define Report Parameters' wizard. The form contains the following fields and options:

- Report Name:** OES Report (marked as required with an asterisk).
- Description:** Oracle Engineered System report.
- Schedule:** Create Schedule:
- Output Format:** CSV, PDF.
- Targets:** A section with two panes:
 - Available Items:** A table with columns 'Assets', 'Product Name', and 'Description'.

Assets	Product Name	Description
Oracle Engineered Systems		OradeEngi
MyHost 1		Superclust
MyHost 2		Superclust
MyHost 3		Superclust
 - Target List(0):** A list box containing 'Assets'.

- Select **Create Schedule** if you want to run the report later or on a recurring schedule.
- Select the output formats of the result that will be generated for the report.

5. In the Targets section, select the asset for which you want to run the report and click **Add to Target List**.
6. Click **Next**. The Schedule wizard is displayed.
7. Select a schedule for the report. You can schedule the report to run on the following instances:
 - Now: Runs the report immediately.
 - 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, if 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.
8. Click **Next**. The Summary wizard is displayed.
9. Verify the report parameters and click 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.

Figure 4-10 Oracle Engineered Systems Report Results

Owner	Status	Report Name	Description	Report Type	Run Date
root	OK	OES RReport	Oracle Engineered System Report	Oracle Engineered...	08/13/2013 12:05:...
root	OK	jkl		Oracle Engineered...	08/12/2013 09:49:...

Incident Reports

You can create incident reports to obtain information about incidents.

The following types of incident reports are available:

- The Incident Summary Report: This 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: This 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.

Creating Incident Reports

Procedure 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, perform the following steps:

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**. This 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.

Creating a Firmware Report

Firmware Compliance Reports enables you 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, perform the following steps:

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, deselect the **Create Schedule** option.
 - **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 and Close** 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.
 - 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.
 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.

See for information about adding a product alias.
 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 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.
 3. Repeat the procedure to create a firmware report.

Creating Additional Operating System Reports

You can create 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.

Creating a 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 like SOLARIS10_SPARC has been updated with specific updates, or CVEs.

To create a Distribution Update Report, perform the following steps:

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. 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. 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.

Creating a 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, perform the following steps:

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.

Creating a 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, perform the following steps:

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.

Related Resources for Reports

This section lists the related resources for reports.

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

- For more information, see the Oracle Enterprise Manager Ops Center Documentation Library at http://docs.oracle.com/cd/E59957_01/index.htm.
- For end-to-end examples, see the workflows and how to documentation in the library. For deployment tasks, go to http://docs.oracle.com/cd/E59957_01/nav/deploy.htm, for operate tasks go to http://docs.oracle.com/cd/E59957_01/nav/operate.htm, and for administer tasks go to http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- For an example, see *Creating System Catalog Reports* in the Operate How To library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm.
- See [Introduction to Operating System Updates](#) for more information on System Catalogs.

Manage the Hardware

This section 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 you can configure and then monitor them to gather the information to maintain them.

Configuring Hardware Assets

Steps to configure 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.

Maintaining Hardware Assets

You can control and maintain your hardware assets and perform specified actions on it.

Based on your observations, you can control your hardware assets and do the following actions:

- Update management credentials.
- [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:

- [Updating Firmware](#)

- Update Storage Appliances
- Update BIOS Configuration

Roles for Hardware Management

Lists the tasks and the role required to complete the task.

[Table 5-1](#) 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 the for information about the different roles and the permissions they grant.

Table 5-1 Hardware Roles and Permissions

Task	Role
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

Lists all the actions for hardware after you manage your assets.

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

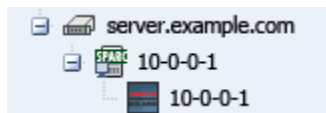
- Power systems on and off, including a forced power off
- Place in maintenance mode
- Get access to the serial console
- Use locator lights to identify a specific asset
- Check firmware compliance
- Update firmware
- Use a provisioning profile to update firmware

Location of Hardware Information in the User Interface

Hardware assets are visible in the All Assets section of the user interface.

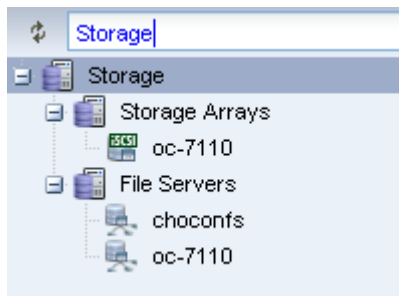
For assets with a service processor, both the service processor and the system are included, as shown in [Figure 5-1](#).

Figure 5-1 Managed System



Each type of hardware is also added to the appropriate group in the Resource Management view, as shown in [Figure 5-2](#).

Figure 5-2 Example of Resource Management View



[Table 5-2](#) shows where to find information.

Table 5-2 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.

Table 5-2 (Cont.) Location of Hardware Information in the BUI

To See	Location
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 and then takes the action you specify in the profile.

See [Firmware Compliance Reports](#) and [Firmware Provisioning](#).

Configuring the Service Processor

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.

The **Declare Unconfigured Asset** action includes the service processor in the Oracle Enterprise Manager Ops Center environment.

- 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.

Creating a Service Processor Configuration Profile and Plan

Procedure to create a 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, as shown in [Figure 5-3](#). Depending on the subtype and target you select, more steps are added.

Figure 5-3 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.

Creating a BIOS Configuration Profile and Plan

Procedure to create a BIOS configuration profile and plan.

1. Expand Plans in the Navigation pane and then select Plans.
2. Expand Update BIOS Configurations.
3. Click **Create Plan from Template**. [Figure 5-4](#) shows the first step of the wizard, which includes the Update BIOS profile.

Figure 5-4 Create Plan - BIOS

Oracle Enterprise Manager Ops Center - Create a Deployment Plan

Create a Deployment Plan ? ORACLE

* Indicates Required Field

* Plan Name:

Description:

Failure Policy: Stop at failure Complete as much as possible

Target Type: Hardware

Template Name: Update BIOS

Step	Profile/Plan Type	Associated Profile/Deployment Plan
Update BIOS	BIOS Profile	

4. Click the Update BIOS profile.
5. Click the **Create Profile** icon. [Figure 5-5](#) shows the window for creating the profile.

Figure 5-5 Create Profile-BIOS Configuration

Oracle Enterprise Manager Ops Center - Create Profile - BIOS Configuration

Create Profile - BIOS Configuration ORACLE

Steps Help

1. Identify Profile

2. Summary

Identify Profile * Indicates Required Field

* Name:

Description:

* Subtype: Subtype

- BIOS
- UEFI

Target Type: Target Type

- Servers

6. Enter a name and description and then select the type of BIOS and the type of target.
7. Click **Next** to review and then click **Finish** to submit the job.
8. When the job is completed, return to the Create a Deployment Plan window.
9. Specify a name for the plan and select the new profile.
10. Click **Save** to submit the job.

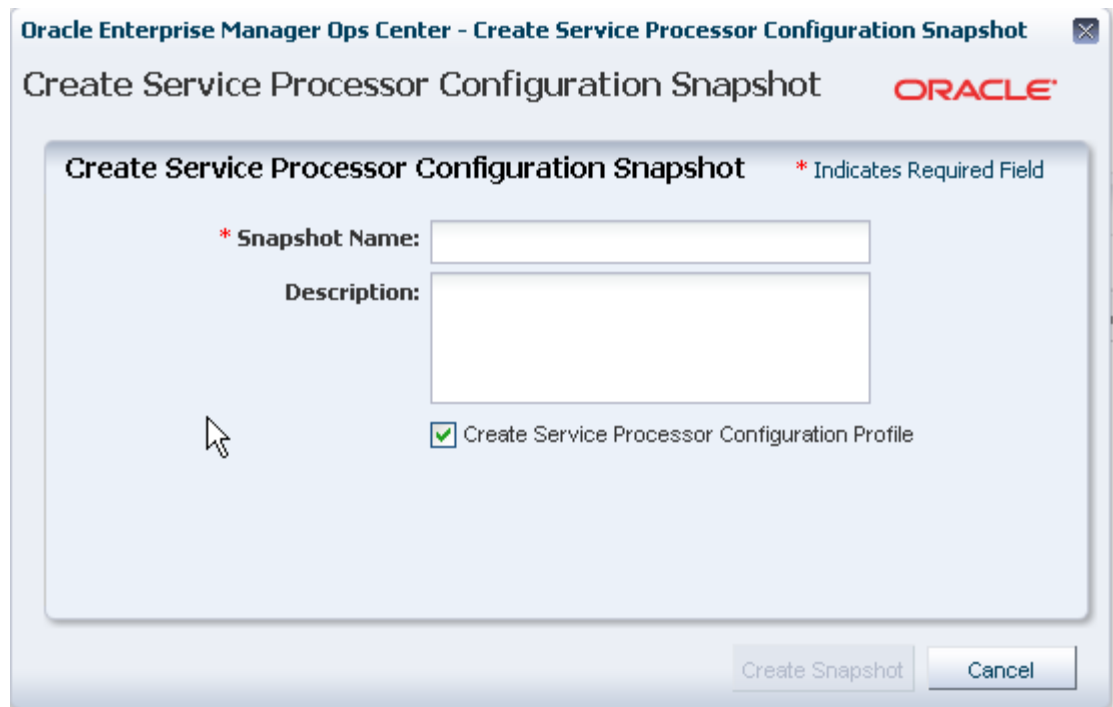
The new profile and plan are available from the Assets pane.

Creating a Snapshot of a Service Processor Configuration

Procedure to 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 window shown in [Figure 5-6](#).

Figure 5-6 Create Service Processor Configuration Snapshot



The screenshot shows a dialog box titled "Oracle Enterprise Manager Ops Center - Create Service Processor Configuration Snapshot". The main heading is "Create Service Processor Configuration Snapshot" with the Oracle logo to the right. Below the heading, there is a sub-heading "Create Service Processor Configuration Snapshot" followed by a legend "* Indicates Required Field". The form contains two input fields: "* Snapshot Name:" (a required field) and "Description:". Below these fields is a checkbox labeled "Create Service Processor Configuration Profile" which is checked. At the bottom right, there are two buttons: "Create Snapshot" and "Cancel".

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.

Applying a Snapshot of a Server Processor Configuration

Procedure to apply a snapshot to an unconfigured service processor.

This procedure applies a snapshot of a server's service processor to an unconfigured service processor. Use the **Update BIOS Configuration** action or use the snapshot profile as a step in the Install Server deployment plan.

Viewing 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.

Applying a Service Processor Snapshot

Procedure to apply a service processor snapshot.

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. A 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.

Applying a Service Process Snapshot Profile to a Server

Procedure to apply a service process 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.

Note:

When you reconfigure an existing RAID controller, all the data on the disk is lost.

Configuring a Dynamic System Domain

Procedure to configure 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 in to the XSCF processor.

To configure a Dynamic System Domain, you apply a deployment plan to an M-Series server, as described in [Link: Chapter 8](#). The plan includes the profile for the Dynamic System Domain.

Configuring a Rack and Placing Components

After you create the rack, you can 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.

The rack asset is a group that includes other managed assets installed in the physical rack, such as servers or compute nodes, storage arrays or appliances, switches, and power distribution units (PDU).

Creating a Rack

Procedure to create a rack and place assets into the 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

Procedure to place 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, which displays a list of all managed assets in the physical rack. 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**. 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.

Groups 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](#).

Connectivity Status

You can view information about a hardware asset's Network Interface Card (NIC). Connectivity is the network interface of the system.

Service Processor Details

Provides information about each component of the system.

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

Lists the RAID Controller details.

- RAID volume name
- RAID level
- Number of disks
- Stripe zone
- RAID Controller ID

Oracle ZFS Storage Appliance Details

The Oracle ZFS Storage Appliance supports 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

ALOM and ILOM Servers Details

Lists the general details displayed for the ALOM and ILOM servers.

This version of the product software discovers and manages servers that use the ALOM or ILOM service processors. The following are general details displayed for these servers.

For server hardware, the Summary tab displays:

- Server Name
- Description
- 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
- A table with the available Tags
- A table with the Firmware information

The Hardware Tab for ALOM servers display summary information and a table with all the firmware installed.

The Hardware Tab for ILOM servers include more information in the component navigation pane of the Hardware tab:

- System: Description, type, and version of all firmware installed except for disk firmware. See the Disk tab for firmware version.

- Processors or CPU: Architecture, number of Installed CPUs, Actual Power Consumption, Summary Description, number of Max CPUs, and Status. The Processors table displays for each CPU: Name, Model, Speed, Manufacturer, and Status.
- Memory: number of Installed DIMMs, Installed Size in bytes, number of Max DIMMs, Status, and Actual Power Consumption. The Memory table displays for each DIMM: Name, Size in bytes, Manufacturer, Part number, Serial number, and Status is displayed on the Memory table.
- Power or Power Supply: number of Installed Power Supplies, Actual Power Consumption in watts, Status, number of Max Power Supplies, and Max Permitted Power in watts. The Power Supplies table displays for each power supply: Name, Manufacturer, Part number, Serial number, and Status.
- Cooling or Fan Tray: number of Installed Chassis Fans, number of Installed PSU Fans, Inlet Temperature, Status, number of Max Chassis Fans, number of Max PSU Fans, and Exhaust Temperature. The Fans table displays for each item: Name, RPM (%), and Status. Servers with older versions of ILOM list a Fan Tray group instead including the identifier of each available fan and its speed (RPM).
- Storage or Disk: Installed Disk Size in bytes, number of Installed Disks, Status, Logical Volumes, and number of Max Disks. The Disks table displays for each item: Name, Presence Status, and Status.
- Networking or Network Adapter: number of Installed Ethernet Nics, and Status. The Network Adapters table displays for each item: Name, MAC Address, Description, and Status.
- PCI Devices: a table listing the PCI Devices. The table displays for each item: Name, Card Type, Description, Vendor ID, Device ID, and Part Number. This information is not available for servers with older versions of ILOM.
- Service Processor: Name, Auto DNS Via DHCP, Search Path, Use NTP Server, NTP Server 2, SNMP Community, DNS Servers, Time Zone, and NTP Server 1. The Service Processor Snapshots displays for each item: Name, Creation Date, Description, and Created By.

M-Series Servers 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 the following:

- Number of dynamic system domains it is supporting
- Model
- Serial Number
- Description
- Support contract
- XCP Firmware Version
- OBP Firmware Version

- XSCF Firmware Version
- Hypervisor 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.

You can find the following information on the Summary tab:

- Name
- Model
- Serial Number
- Management IP
- MAC Address
- Current Alert Status
- Power
- Locator Light
- Notification
- All firmware versions including Description, Type and Version.
- The table Domain displays for each item: Name, Model, Health, Power, Locator Light, Notification
- Model
- Serial Number
- State
- Power
- Locator Light
- Notification
- Operator Panel Switch State

The Hardware tab shows the state of the server or, if a Dynamic System Domain is selected, the state of that domain. At the System level, the Hardware tab includes the following information:

For the M-5000 server, the System level of the Hardware tab also 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

For Oracle SPARC M5-32 and M6-32 servers, the System level of the Hardware tab also includes:

- System Type
- Part Number
- System Identifier
- Management IP
- Management MAC Address
- Actual Power Consumption
- Status
- Data Source
- The Subsystem Status table displaying a summary including: name of Subsystem, Status, and Inventory.
- The Configured Dynamic System Domains table listing all the domains and their details: Domain ID, Domain Name, Priv MAC address, Auto Boot Policy, ILOM IP, Keyswitch State, and Operational Status
- The Unconfigured Dynamic System Domains table listing the same information as the table above except for Domain Name.
- Allocated Resources. No data is displayed on this table.
- Unallocated Resources. No data is displayed on this table.
- The Firmware table displaying for each item: Description, Type, and Version.

Oracle SPARC M5-32 and M6-32 servers include an ILOM 3.2 service processor. For more information about ILOM servers see [ALOM and ILOM Servers Details](#).

Note:

M5 and M6 servers are supported, but some features have additional limitations. For more information see the *Target Servers* section of the *Certified Matrix* document in the Oracle Enterprise Manager Ops Center document library.

Use the Component Navigation pane in the Hardware tab to view 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, and Value.

- Memory: Name, Type, Size in bytes, Serial number, Part number, Status For Sensors: Name, Description, Type, and Value.
- Board: Name, Serial number, Part number, Memory mirrored, Version, and Status.
- Power Supply: Name, Serial number, Part Number, Status For Sensors: Name, Description, Type, and Value.
- Board: Name, XSB Mode, Memory Mirrored, Serial Number, Part Number, Version, Status For Sensors: Name, Description, Type, and Value.
- IO Unit: Name, Serial Number, Part Number Version, Status For Sensors: Name, Description, Type, and Value.
- XSCF: Name, Host Name, Serial Number, Part Number, Version, and Status.
- Fan Tray: Name, Manufacturer, Part number, and Serial number.
- Fans: Name, Speed For Sensors: Name, Description, Type, and Value.

Oracle Enterprise Manager Ops Center monitors the voltage for the Board and IO Unit components and the speed for the Fan components. The Monitoring tab shows the actual value and the threshold values.

CPU Activation Keys for Fujitsu M10 Servers

Starting with Oracle Enterprise Manager Ops Center 12 c Release 3 (12.3.1.0.0), you can add CPU activation keys to Fujitsu M10 servers or you can move CPU activation keys from one Fujitsu M10 server to another Fujitsu M10 server. The CPU activation key is not limited to one machine, but the key is limited to the model of the M10 server, such as M10-1, M10-4, and M10-4S. For example, the CPU activation key from an M10-1 server can be moved to another M10-1 server, but not to M10-4 or M10-4S servers.

After CPU activation keys are added to Fujitsu M10 servers, some CPU resource based on the amount of the CPU Activation that is defined in the CPU activation keys, becomes assignable.

In the Summary tab of the M Series server, CPU Activation Keys section is displayed. The CPU Activation Keys section is displayed only for the Fujitsu M10 servers.

Perform the following steps to add CPU activation keys:

1. In the In the Navigation pane, under Assets, expand M-Series Servers, then click the server.

The screenshot displays the hardware monitoring interface for a Fujitsu M10-4S server. The interface includes a navigation pane on the left with tabs for Dashboard, Summary, Hardware, Connectivity, Incidents, and Service Request. The main content area shows server details such as Name, Model, Serial Number, Management IP, and MAC Address. It also displays the current alert status (OK), power status (On), locator light status (OFF), and notification status (Enabled). Below these details are sections for Firmware, Domains, CPU Activation Keys, and CPU Activation Assignments. The CPU Activation Keys section is highlighted with a red box and contains a table with the following data:

Index	Product	Sequence Number	CPU Cores
0	SPARC M10-4S	13422	2
1	SPARC M10-4S	13423	2
2	SPARC M10-4S	13427	2
3	SPARC M10-4S	13418	2
4	SPARC M10-4S	13508	2

Below the CPU Activation Keys section is the CPU Activation Assignments section, which contains a table with the following data:

Domain ID	Installed CPU Cores	Assigned CPU Cores
00	64	64

2. In the center pane, click the **Summary** tab.
3. Scroll down to the CPU Activation Keys section.
4. Click the **Add** icon to add a CPU activation key.
5. In the Operation Type field, select Upload File option.
6. Click **Browse** to locate the activation key.
7. Click **Add Key** to add the key to the XSCF.

The following are other actions that you can perform:

- Click the **Search** icon to view details of the selected CPU activation key.
- Click the **Delete** icon to delete the selected CPU activation key from the XSCF.
- Click the **Move** icon to move the selected CPU activation key to a different XSCF.
- Click the **History** icon to view the CPU activation history.

CPU Activation Assignments on Fujitsu M10 servers

After you have added CPU activation keys to Fujitsu M10 servers, you can assign additional CPU resources to dynamic system domains.

In the Summary tab of the M Series server, the CPU Activation Assignment section is displayed. CPU Activation Assignments section is displayed only for the Fujitsu M10 servers.

To add additional CPU Cores, perform the following steps:

1. On the Summary tab, in the CPU Activation Assignments section, click the **Set CPU Activation** icon.

The screenshot displays the Summary tab for a Fujitsu M10-4S server. The interface includes a navigation bar with tabs for Dashboard, Summary, Hardware, Connectivity, Incidents, and Service Requests. The Summary tab is active, showing server details such as Name, Model (Fujitsu M10-4S), Serial Number, Management IP, and MAC Address. It also displays status information like Current Alert Status (OK), Power (On), Locator Light (OFF), and Notification (Enabled). Key metrics include CPU Activation Keys (32), CPU Activation Cores (32 assigned, 64 total), and Installed CPU Cores (64). Below these details are sections for Firmware, Domains, CPU Activation Keys, and CPU Activation Assignments. The CPU Activation Keys section contains a table with columns for Index, Product, Sequence Number, and CPU Cores. The CPU Activation Assignments section is highlighted with a red border and contains a table with columns for Domain ID, Installed CPU Cores, and Assigned CPU Cores.

Index	Product	Sequence Number	CPU Cores
0	SPARC M10-4S	13422	2
1	SPARC M10-4S	13423	2
2	SPARC M10-4S	13427	2
3	SPARC M10-4S	13418	2
4	SPARC M10-4S	13508	2

Domain ID	Installed CPU Cores	Assigned CPU Cores
00	64	32

2. The Set CPU Activation window opens. In the Assigned CPU Cores column, enter a numeric value for the domain that you want to assign additional CPU Cores, then click **Set CPU Activation**.

Figure 5-7 Set CPU Activation

To set CPU Activation to domains, input a numeric value for each domain.

CPU Activation Cores: 64 assigned, 64 total

Domain ID	Installed CPU Cores	Assinged CPU Cores
00	64	64
01	0	0
02	0	0
03	0	0
04	0	0

Set CPU Activation Cancel

3. After the job is completed, click on the Summary tab to view the additional cores added to the server.
 - In the Summary Information, the assigned CPU Cores are displayed in the CPU Activation Cores field.
 - In the CPU Activation Cores table, the Installed CPU Cores and Assigned CPU Cores are displayed against the respective domains.

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.

Cisco Catalyst switches are also supported.

For more information about Oracle Datacenter and Ethernet switches, see: <http://www.oracle.com/technetwork/documentation/oracle-net-sec-hw-190016.html#legacysecapp>.

Summary Tab: 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

Hardware Tab: 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)

The Actions pane displays the set of available actions to manage a switch. It includes the **Launch Switch UI** for accessing and managing the switch directly from its Web UI. For the Cisco Catalyst switch, the Launch Switch UI action will be disabled if the HTTP server is not enabled in the switch.

Rack Details

Displays the details of the rack.

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

Displays the PDU details.

The Dashboard tab shows:

- Name and 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, Network, and Quorum tabs display details of the Oracle Solaris Cluster.

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.

Monitoring Power Utilization

You can monitor the input and output power.

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.

You can see current power usage and change the display of power graphs using the controls on the Energy tab and the Charts tab.

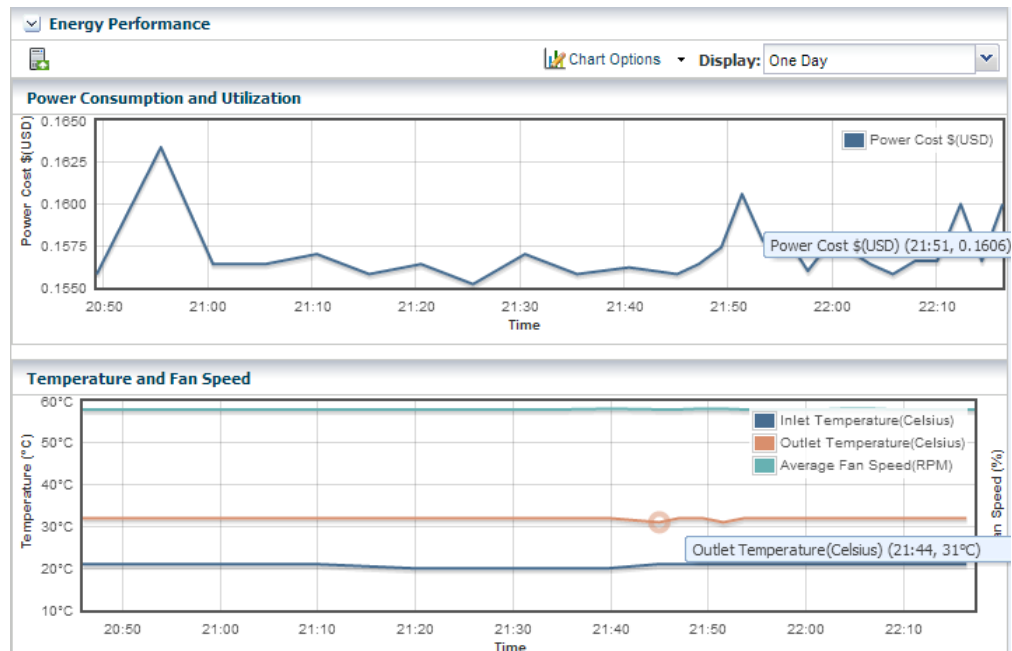
Energy Tab

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.

General Information: The following general information is displayed in the energy tab:

- Power consumption in watts.
- System load for an OS.
- Power policy.
- Utilization percentage for an Oracle VM Server for SPARC.
- Inlet and outlet temperature reporting the incoming and outgoing air temperature.
- Cost per kilowatt-hour in the selected currency.
- The 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 for information.
- The total power cost in the selected currency. The period of time used to compute the cost is determined by the value selected in the Display list.

Energy Performance Charts: The data over time is represented in the following charts:



- Power Consumption and Utilization. By default, the chart shows the power consumed in the last day in watts. If the server is shut down, the chart shows any existing historical data.
- Temperature and Fan Speed. By default, the chart shows the incoming air temperature and the outgoing air temperature in Celsius, and the average fan speed in RPM. Click any point in the chart to see the data for that point in time.

Note:

Servers that use the ALOM and ILOM data model report fan speed in RPMs. Servers with SDM enabled ILOM –such as the M5-32 and M6-32 servers– report fan speed as a percentage of the maximum speed of the fan.

You can set the units for the power consumption and utilization chart's power axis using the Chart Options list. You can select watts or cost.

You can use the Display list to set the period of time that the charts display to one of the following values:

Table 5-3 Values of the Display List of the Energy Performance Charts

Value	Charts' Points Sample Rate
Live	Five minutes
One hour	Five minutes
One day	Five minutes
Five days	Five minutes
Three weeks	One hour
Six weeks	12 hours

Table 5-3 (Cont.) Values of the Display List of the Energy Performance Charts

Value	Charts' Points Sample Rate
Six months	One 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 six weeks 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 one day 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 tool bar 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.

Power Supply and Fan Information Tables: The Power Supply table lists the power supply number, manufacturer, and part and serial numbers.

The Fan Information table lists: the fan number, and fan speed as a percentage or in RPM.

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

You can perform the listed actions on the hardware assets.

- Update management credentials
- 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.

Setting and Changing the Power Policy

The power policy allows you to set an asset in performance, elastic, or disabled mode.

The power policy allows you to set an asset in one of three different modes:

- **Performance:** Unused components are put into a slower speed or sleep state and power savings features with insignificant performance impact are enabled.
- **Elastic:** Components are brought in to or out of a slower speed or a sleep state to match the system's utilization of those components.
- **Disabled:** All components run at full speed or capacity. This option is available for some models and ILOM version.

Viewing an Asset's Power Policy

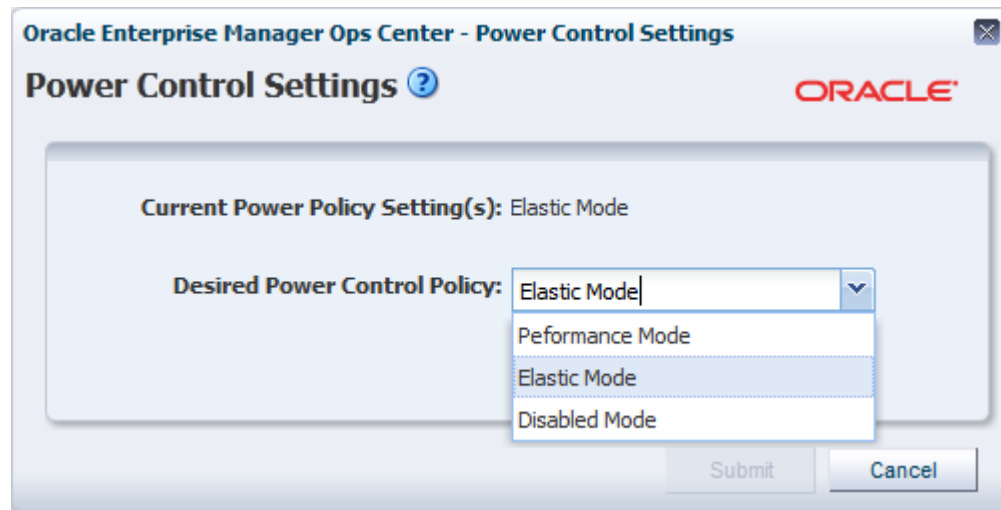
Perform the following steps to view the power policy of an asset.

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

Procedure to change the power policy of an asset.

1. Expand the Assets in the Navigation pane.
2. Select a hardware asset.
3. Click **Set Power Policy** in the center pane to display the window shown in [Figure 5-8](#).

Figure 5-8 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

Procedure to replace 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.
6. Install the new PDU and connect it to the network, according to the procedures in the Power Distribution Units User's Guide at http://docs.oracle.com/cd/E59957_01/nav/deploy.htm.
7. Verify that the new PDU has the same IP address as the failed PDU.
8. Use the PDU's web interface to configure the administrator user account, according to the procedure in the Power Distribution Units User's Guide.
9. Return to the Oracle Enterprise Manager Ops Center user interface and navigate to the same rack and the new PDU. Select the PDU.
10. Click **Remove From Maintenance Mode** in the Action pane.
11. To update the credentials for the administrator user, click **Update Management Credentials** in the Action pane. The wizard opens.
12. At the Management Type step, select HTTP credentials and then select the Create a new set of credentials option. Click **Next**.
13. Enter new credentials for the administrator user.

14. Click **Apply** to update credentials.
15. To create new SNMP credentials, click **Update Management Credentials** in the Actions pane again.
16. Select SNMP credentials and Create a new set of credentials.
Specify a community string that is different than the previous community string.
17. Press Apply to update credentials.

Installing and Upgrading Oracle Solaris Cluster

You can use cluster profiles in a deployment plan to install Oracle Solaris Cluster software and upgrade Oracle Solaris Cluster software.

You can use cluster profiles in a deployment plan to perform the following operations:

- Install Oracle Solaris Cluster software
- Upgrade Oracle Solaris Cluster software

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

Describes the steps to provision 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 Operate How To library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm.
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 Operate How To Library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm.
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.

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 [Creating a Firmware Report](#) for the procedure to create the report.

Updating Firmware

To update the firmware on one or many assets, you use a deployment plan to apply a firmware profile for the type of asset. For a server, the profile updates the firmware on a service processor, and restarts the service processor and operating system.

For storage components, profiles update firmware on a RAID controller, an expander, or disk.

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 and profiles is displayed.

To update 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 *Operate How To* library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm.

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 procedure performs a hard shutdown of the server.

Requirements for ALOM Service Processors and M-Series Servers

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.

Note:

Advanced Lights Out Management (ALOM) is a Sun Microsystems standard for servers such as: SunFire V125/V210/V215/V240/V245/V250/V440/T1000/T2000, Sun Netra 210/240/440, and SunBlade T6300.

If your site does not allow a temporary 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.

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.

Option for Deferring the Stop and Restart of the Operating System and Server

The procedure is available for Oracle Solaris 10 Update 10 operating systems running on servers with the ILOM x86 (3.0 and higher) service processor.

When you update the firmware of a service processor, the procedure stops the operating system and the server before the update and restarts them after the update so that the new BIOS takes effect. If you prefer to stop and restart at a convenient time, keeping the current BIOS in effect, use the following procedure to change the action of both Oracle Enterprise Manager Ops Center and the firmware's metadata:

1. On the Enterprise Controller, open the `/var/opt/sun/xvm/hal.properties` in an editor.
2. Add the following property to the file:


```
ilom.fwp.skipAutoReboot=true
```
3. On the Proxy Controller that provisions the firmware, enable the `ftp` service on Oracle Solaris or the `vsftpd` service for Oracle Linux systems.

4. At a later time, reboot the servers.

Launching LOM and XSCF Browser User Interfaces

When you select a server on the Assets pane, the **Launch LOM Controller** link is displayed on the Actions pane. This functionality launches the Browser User Interface (BUI) for servers with a Lights Out Management (LOM) port.

The **Launch SP Controller** link is only available to M-Series servers on the Actions pane for launching the specific BUI for the XSCF controller. The BUI is disabled by default on M-Series servers for security reasons and must be manually enabled before attempting to use this functionality.

The BUI for XSCF runs on the HTTPS protocol and can be enabled using the following command with a user with `platadm` privileges:

```
XSCF> sethttps -c enable
```

Related Resources for Hardware Management

This section lists the related resources for hardware management.

- For more information, see the Oracle Enterprise Manager Ops Center Documentation Library at http://docs.oracle.com/cd/E59957_01/index.htm.
- For current discussions, see the product blog at <https://blogs.oracle.com/opscenter>.
- For end-to-end examples, see the workflows and how to documentation in the library. For deployment tasks, go to http://docs.oracle.com/cd/E59957_01/nav/deploy.htm, for operate tasks go to http://docs.oracle.com/cd/E59957_01/nav/operate.htm, and for administer tasks go to http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- For more information about Oracle Datacenter and Ethernet switches, see: <http://www.oracle.com/technetwork/documentation/oracle-net-sec-hw-190016.html#legacysecapp>.
- See the Power Distribution Units User's Guide at <http://docs.oracle.com/cd/E19844-01/index.html>.
- For information about Oracle SPARC servers, including SPARC T5, SPARC M5-32, and SPARC M6-32 servers, see SPARC Systems at <http://www.oracle.com/technetwork/documentation/oracle-sparc-ent-servers-189996.html>.
- See Systems Management and Diagnostics at <http://www.oracle.com/technetwork/documentation/sys-mgmt-networking-190072.html> for information about ILOM configurations.

Manage Operating Systems

This section 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 System Management](#)
- [Roles for Operating System Management](#)
- [Actions for Operating System Management](#)
- [Location of Operating System Management Information in the User Interface](#)
- [Operating System Profiles](#)
- [Using Agent Management for Operating Systems](#)
- [Monitoring Operating Systems](#)
- [Using Analytics](#)
- [Overview of Oracle Solaris Boot Environments](#)
- [Overview of Oracle Solaris 11 Boot Environments](#)
- [Overview of Oracle Solaris 10 Boot Environments](#)
- [Related Resources for Operating System Management](#)

See [Provision Operating Systems](#) for how to install, or provision operating systems. See [Update Operating Systems](#) for information about patching and updating your operating systems.

Introduction to Operating System Management

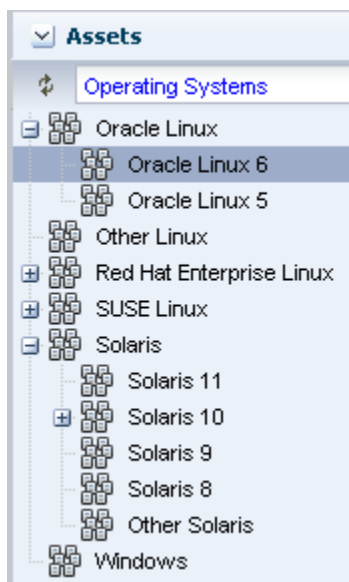
Oracle Enterprise Manager Ops Center provides comprehensive lifecycle management for Oracle Solaris and Linux operating systems in your datacenter. The software also enables you to patch, or update, Microsoft Windows operating systems.

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 6-1](#).

Figure 6-1 Managed System and Operating System

The operating system also appears in the appropriate platform-specific group in the Operating Systems view, as shown in [Figure 6-2](#).

Figure 6-2 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. Groups are 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.

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 the management type.

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.

Note:

The Enterprise Controller must be installed on an Oracle Solaris operating system in order to perform the following tasks:

- Provision Oracle Solaris 10 using JET customization.
- Provision Oracle Solaris 11 (requires that both the Enterprise Controller and Proxy Controller are running on an Oracle Solaris 11 operating system).
- Provision Oracle VM Server for SPARC (control domain).

-
- **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 [Update Operating Systems](#) for information.
 - **Reports and Snapshots:** A variety of reports are available for your operating systems. See [Create Reports](#) for OS reports. See [Update Operating Systems](#) for information on how to use the System Catalogs to maintain snapshots of your operating system.

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.

Roles for Operating System Management

Lists the management roles and permissions.

[Table 6-1](#) 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 for information about the different roles and the permissions they grant.

Table 6-1 OS Management Roles and Permissions

Task	Role
Reboot an OS	Asset Admin

Table 6-1 (Cont.) OS Management Roles and Permissions

Task	Role
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
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 System Management

Lists the actions that you can perform on the operating system.

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.

Agent managed is the more robust management mode because the Agent Controller 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.

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.
- Manage Oracle Solaris boot environments.
- Update or patch operating systems. See [Update Operating Systems](#).
- Provision or upgrade Oracle Solaris and Linux operating systems. See [Provision Operating Systems](#).

Note:

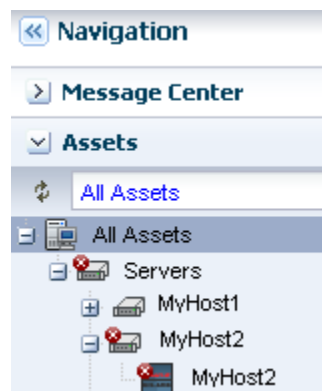
To perform actions, such as OS provisioning, updating, and managing boot environments, on an Oracle Solaris 11 operating system, the Enterprise Controller and Proxy Controller must be installed on an Oracle Solaris 11 operating system.

Location of Operating System Management Information in the User Interface

Operating Systems management information is displayed under the associated server in the All Assets view.

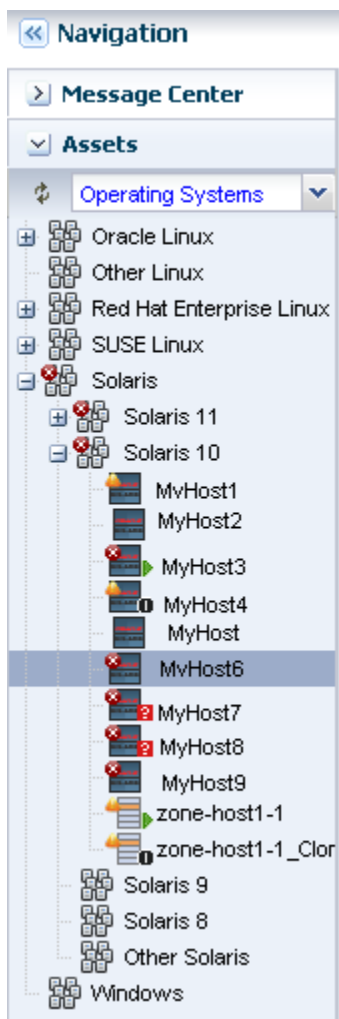
When you manage a physical or virtual operating system, it appears under the associated server in the All Assets view, as shown in [Figure 6-3](#) and it appears in a special pre-defined operating system group, as shown in [Figure 6-4](#).

Figure 6-3 All Assets View



Operating systems are automatically added to a homogenous group of operating systems. The group contains directories for each release. In [Figure 6-4](#), 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.

Figure 6-4 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 6-2 Location of Operating System Information in the UI

To Display	Select
Managed operating systems	Expand the Assets pane. Each operating system appears in the Assets Navigation 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.

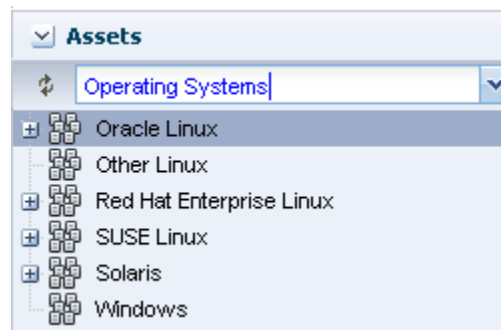
Table 6-2 (Cont.) Location of Operating System Information in the UI

To Display	Select
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.
Boot environments	Select an operating system in the Assets pane, then click the Boot Environments tab.

Viewing Operating Systems

You can view all managed assets in the Assets section of the Navigation pane, or you can filter to display a specific group of assets.

Figure 6-5 shows the asset filter menu where you can choose the Operating System group or user-defined groups.

Figure 6-5 Asset Filter Menu

Displaying Operating System Details

Details about a specific operating system appear in a number of tabs in the center pane of the UI. The tabs and contents might vary based on the type of operating system selected and whether the operating system is agent or agentlessly managed. When a tab is not applicable, it will not appear in the UI. For example, the Libraries tab does not appear when there are no libraries associated with the operating system.

To view the details in the UI, perform the following steps:

1. Expand **Assets** in the Navigation pane.
 - To display All Assets, expand **Servers**.

- To display the Operating System groups, select **Operating Systems** from the menu.
 - To display user-defined groups, select **All User Defined Groups** from the menu, then select the group.
2. Select an operating system in the Navigation pane.

The following tabs appear in the center pane:

- **Dashboard:** Displays the summary of the selected operating system, including the name, server name, whether the operating system is agent managed, the number of unassigned incidents, the current alert status, and the OS release. The dashboard also includes the operating system's membership graph, the status of incidents, and compliance reports, if any.
- **Summary:** Displays the name of the selected Oracle Solaris operating system, description, server name, operating system version, number of CPU threads, active boot environment, the state, the length of running time, and zone patching information. Tables display total CPU utilization and total ZPool Utilization for Oracle Solaris operating systems.
- **Libraries:** Displays library details when a library is associated with an operating system.
- **Storage:** Displays logical unit (LUN) details and iSCSI targets, when applicable. LUN details include the initiator, MPxIO details, the GUID, type, size, status, vendor, and product. The iSCSI details include the initiator, iSCSI target address, address type, port, and IP address. You can discover iSCSI addresses from this tab.
- **Analytics:** Displays utilization and metrics for the selected operating system and zones, when applicable.
- **Connectivity:** Displays Linux OS network interface of the system, including network connectivity and aggregated links.
- **Networks:** Displays Oracle Solaris network connectivity, IPMP groups, and aggregated links. For an Oracle Solaris 11 OS, the tab also provides bandwidth management.
- **Incidents:** Displays all incidents reported from the selected operating system.
- **Monitoring:** Displays the alert monitoring rules and service dependencies of the selected operating system.
- **Terminal:** Enables you to establish an SSH connection to the terminal window.
- **Boot Environments:** Displays Oracle Solaris boot environment details, including all available boot environments, the active and enabled boot environment, the size, and the creation or synchronization date. For a selected boot environment, you can view snapshot details, file system details, and any associated zone boot environments. This tab is only available for Oracle Solaris operating systems.
- **Jobs:** Displays current and historical job information for that operating system.
- **Service Request:** Displays the service request for the selected operating system.

- **Configuration:** Displays access points, or resources, that are associated with the operating system.

Operating System Profiles

OS Provisioning, Monitoring Profile, Oracle Solaris Zone, and Boot Environments are available in OS profiles.

The following categories of OS profiles are available:

- OS Provisioning
- Monitoring Profile
- Oracle Solaris Zone
- Boot Environments

Using Agent Management for Operating Systems

An agent managed operating system has an Agent Controller or a specialized virtualization, or VC, Agent Controller installed to gather information for the Enterprise Controller. The VC Agent Controller is for virtualization technology, such as zones and logical domains.

When you install the Agent Controller on the operating system, the following actions occur:

- The software registers the Agent Controller 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.

Virtualization Agent Controllers

In addition to the default Agent Controllers, Oracle Enterprise Manager Ops Center uses specialized virtualization Agent Controllers called VC Agent Controllers for Oracle VM Server and Oracle Solaris Zone assets.

You can install the agent during discovery, or at any time after discovery. You have the following agent management options:

- **Oracle VM Server for SPARC Virtualization Controller Agent:** Manages the logical domains that are running on the Control Domain. The Oracle VM Server, Control Domain and operating system are reflected in the UI. Using this agent enables full monitoring and management actions for the Oracle VM Server system.
- **Zones Virtualization Controller Agent:** Manages the zones that are running on the logical domains. The global zone is reflected in the UI. Using this agent enables full zone monitoring and management actions.
- **Agentlessly:** Limited management functionality is available with this method. Information is gathered by using SSH connection between the logical domains and the Proxy Controller.

For robust management, use the OVM Server for SPARC Virtualization Controller Agent to manage the domains. The agent runs on the Control Domain and monitors the configuration and reflects any changes on the configuration in its copy of the metadata.

Functionality With and Without Agent Controllers

The Agent Controller provides the most robust management features. However, you can manage your assets without using an Agent Controller. 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.

Some features are not available when the operating system is managed agentlessly. [Table 6-3](#) shows the information that are available for each management type.

Table 6-3 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
System Catalogs	Yes	Oracle Solaris 11: Yes Oracle Solaris 8-10, Linux, Windows: No
Terminal	Yes	No
Jobs	Yes	Yes
Configuration	Yes	Yes

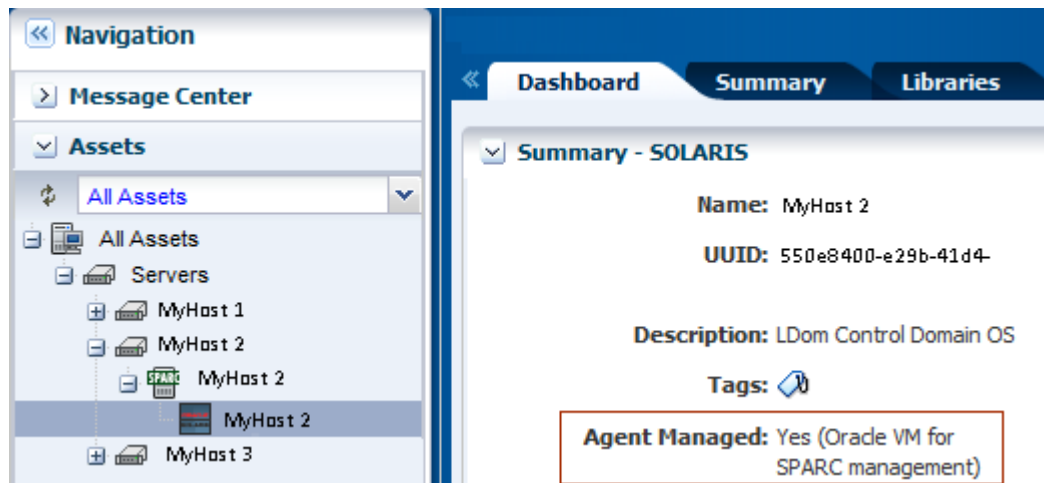
Table 6-3 (Cont.) Information Available for Agent Managed and Agentlessly Managed Assets

Tab or Feature	Agent Managed	Agentlessly Managed
OS update	Yes	Oracle Solaris 11, Windows: Yes Oracle Solaris 8-10, Linux: No
OS provisioning	Yes	Yes
Zone management: boot, shutdown, halt, delete, edit zone config, get zone console	Yes	Yes
Zone management: create, clone, migrate, add a filesystem to a zone, remove a filesystem from a zone, attach and detach networks, add storage to a zone	Yes	No

Switching Between Agent Controllers or Agent and Agentless

This section describes the procedure to change the management mode.

The current management mode of an operating system and the type of Agent Controller appears on the Dashboard for the operating system, as shown in [Figure 6-6](#).

Figure 6-6 Agent Managed

You can use the following methods to change the agent management mode:

- Unmanage the asset, 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 or to switch the type of agent.

When the operating system is agent managed and you use this action, the software removes the Agent Controller and changes the operating system to agentless. Select or create new credentials for the Proxy Controller to use to obtain information from the asset.

To switch between different types of Agent Controllers, such as changing from a default Agent Controller and a virtualization Agent Controller, you must use Management Access to unmanage and then manage again. When you manage the asset, you are prompted to choose the type of Agent Controller when it is not apparent to Oracle Enterprise Manager Ops Center which agent you want to install.

Using Switch Management Access

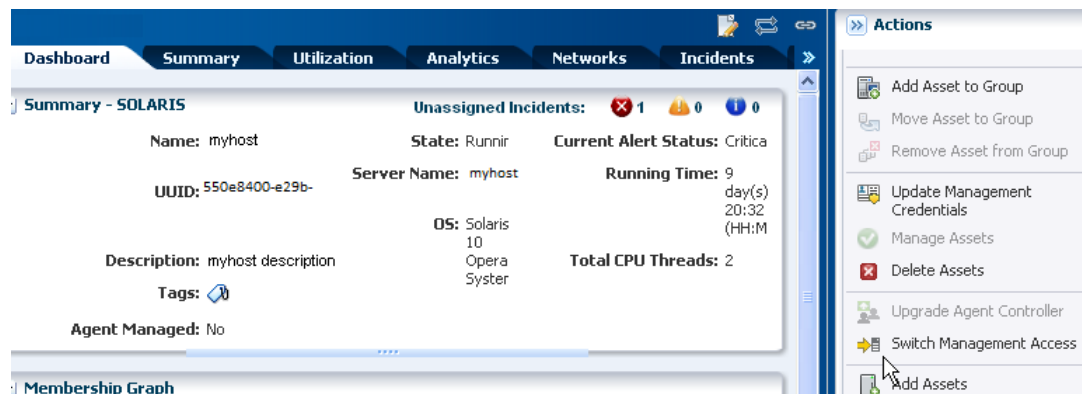
Procedure to use switch management process.

1. Expand **Assets** in the Navigation pane.
2. Expand the Assets tree, then select the operating system.

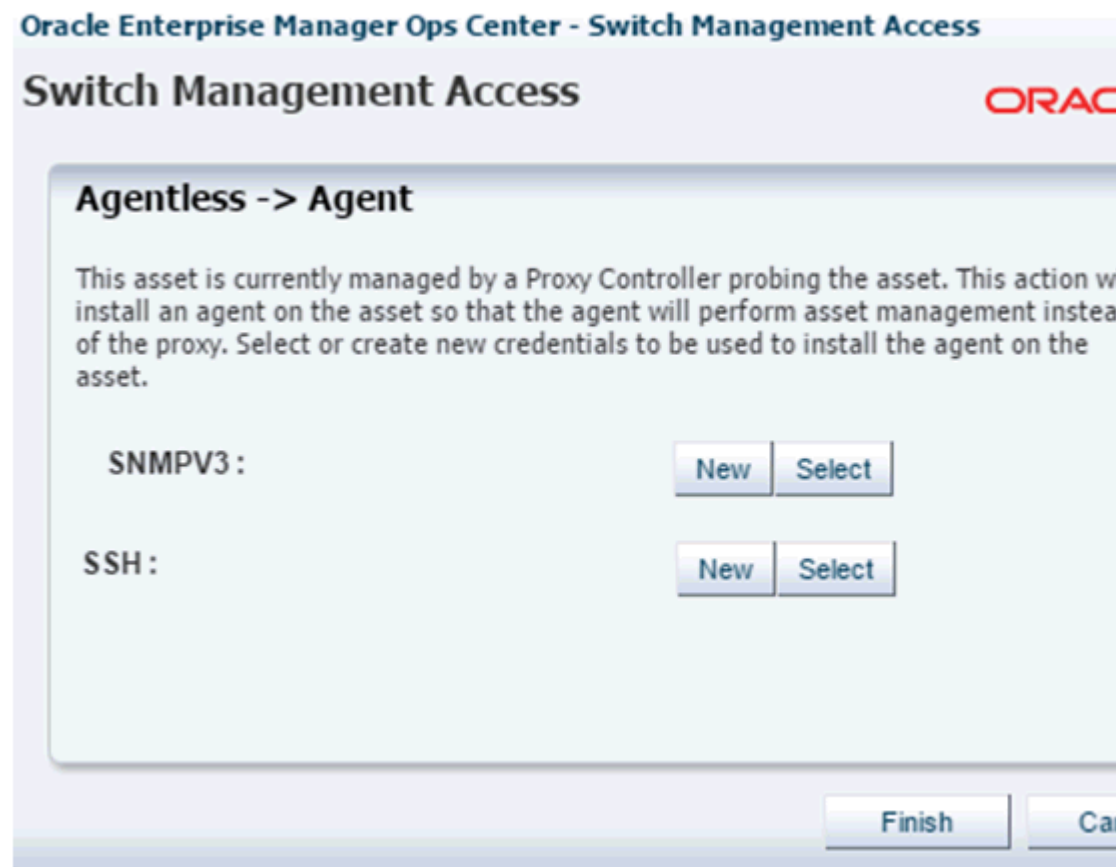
The current management status appears in the Dashboard tab.

3. Click **Switch Management Access** in the Actions pane.

Figure 6-7 Switch Management Access



4. Add or select SNMPv3 credentials and SSH credentials for the system, then click **Finish**.
 - (Optional) To create a new set of credentials, click **New** and complete the Create Credentials Wizard, then click **OK**.
 - (Optional) To select from a list of existing credentials, click **Select**, highlight the credentials from the list of available credentials, then click **OK**.

Figure 6-8 Switch Management Access Credentials

Monitoring Operating Systems

The software monitors the status of your operating systems right after asset discovery.

Oracle Enterprise Manager Ops Center uses 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 [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 [Resolve Incidents](#) for details about how incidents are generated, severity badges, how to assign and close an incident.

Disable Operating System Monitoring

You can disable OS monitoring by disabling the report service thereby suppressing all OS related metrics and analytics.

Perform the following steps to disable OS monitoring:

1. Edit the following resource controller file.

```
/opt/sun/nlgc/etc/xvmoc-resourcecontroller.xml
```

2. Comment the lines starting from `resource name="OperatingSystems" pattern="com.sun.hss.domain:type=OperatingSystem,*" > until /resource`
3. Restart the Enterprise Controller or stop and then restart the report service using the CLI command.

Using Analytics

The Analytics feature provides a view into operating system and zone performance and status. The charts, reports, and utilization data provide details of an individual eligible operating system or zone. You can use the information to analyze the behavior of an operating system to aid in peak performance and to diagnose and correct incidents.

Monitoring uses the Agent Controller to gather information. When an operating system is not an agent-managed system, or it is 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 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 6-4](#) shows a list of features and whether the feature is supported on an agent-managed or agentlessly-managed asset.

Table 6-4 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, for agent-managed guests	No

Table 6-4 (Cont.) Supported Analytics Information

Feature	Supported on Agent Managed OS	Supported on an Agentlessly Managed OS
Virtualization Analytics for Oracle Solaris 10 Zones	Yes, for an agent-managed global zone or non-global zone	No
Services	Yes	Yes
Processes	Yes, for an agent-managed guest, global zone, or non-global zone	No
Threshold	Yes	Yes
History	Yes, for an agent-managed guest, global zone, or non-global zone	No
Metrics	Yes	Yes

The current management mode appears in the Dashboard Summary page for the operating system.

Displaying Analytics Information

For each operating system, the information appears in the **Analytics** tab in the center pane.

The following diagnostic pages are available for an agent-managed operating system:

- OS Analytics view: Displays analytics details for an operating system.
 - System resource graphs
 - Top-consumers views
 - Processes information
 - View historical data and set thresholds
- Virtualization Analytics view: Displays analytics details for a zone.
 - Virtualized OS instance
 - Breakdown of resource usage of the physical server
 - Running OS instance
 - View historical data and set thresholds

Display the Analytics View

Procedure to display the analytics view.

1. Select an operating system, zone, or guest in the Navigation pane.
2. Click the **Analytics** tab.

Display the Both the OS Analytics and Zone Analytics Views

Procedure to display OS analytics and zone analytics views.

1. Select a global zone that has zones in the Navigation pane.
2. Click the **Analytics** tab to see the OS Analytics.
3. Click the **Zones Analytics** tab to view the Summary, Zones, History, and Resource Pool Utilization for all zones of the global zone.

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 6-4](#) 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.

Displaying the Analytics Summary

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.

Click the **View** icon for a row to display process details.

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 %.

- **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.

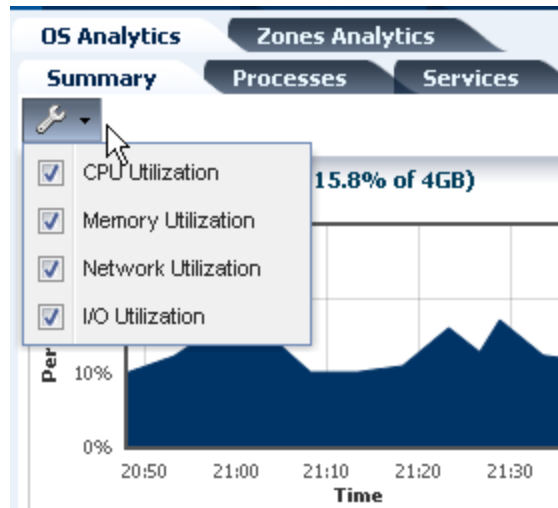
Oracle Enterprise Manager Ops Center collects information every five minutes on every managed asset and displays the last hour of data on the Summary tab. Each list has an icon before the PID column for each process. Click an icon to view details of the process. The type of resource determines the available 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.

Displaying and Configuring Graphs

When the icon that looks like a wrench appears on a page with graphs, click the icon to configure the graphs or change the graphs that appear on the page.

[Figure 6-9](#) shows an example where you can choose the system resource graphs that display on the Summary page.

Figure 6-9 Configure Graphs Menu

Displaying the 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 6-9](#) 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 , information about available targets appears in the Process view.

Displaying the 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.

The following actions are available from 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

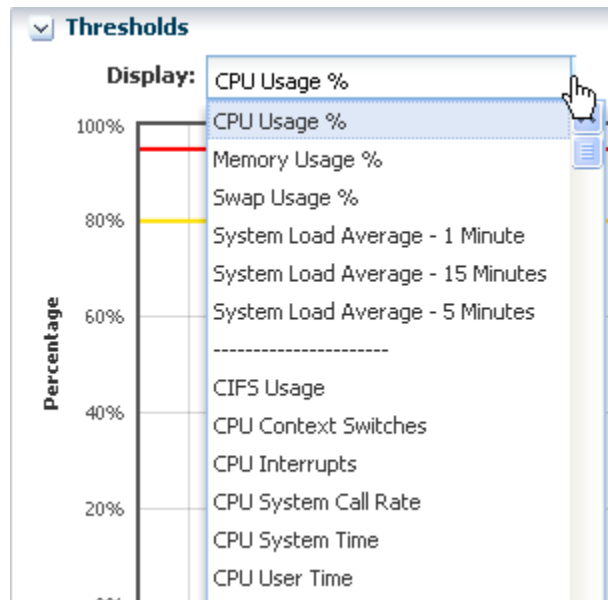
The Thresholds tab contains information about all monitored attributes for the selected operating system, including per-instance attributes such as File System Usage for each file-system on the asset.

Displaying Thresholds

Procedure to display thresholds.

1. Display the Analytics view.
2. Click the **Thresholds** tab.
3. Click the **Display** menu to show the available monitored attributes.

[Figure 6-10](#) shows a partial list of the monitored attributes available for display.

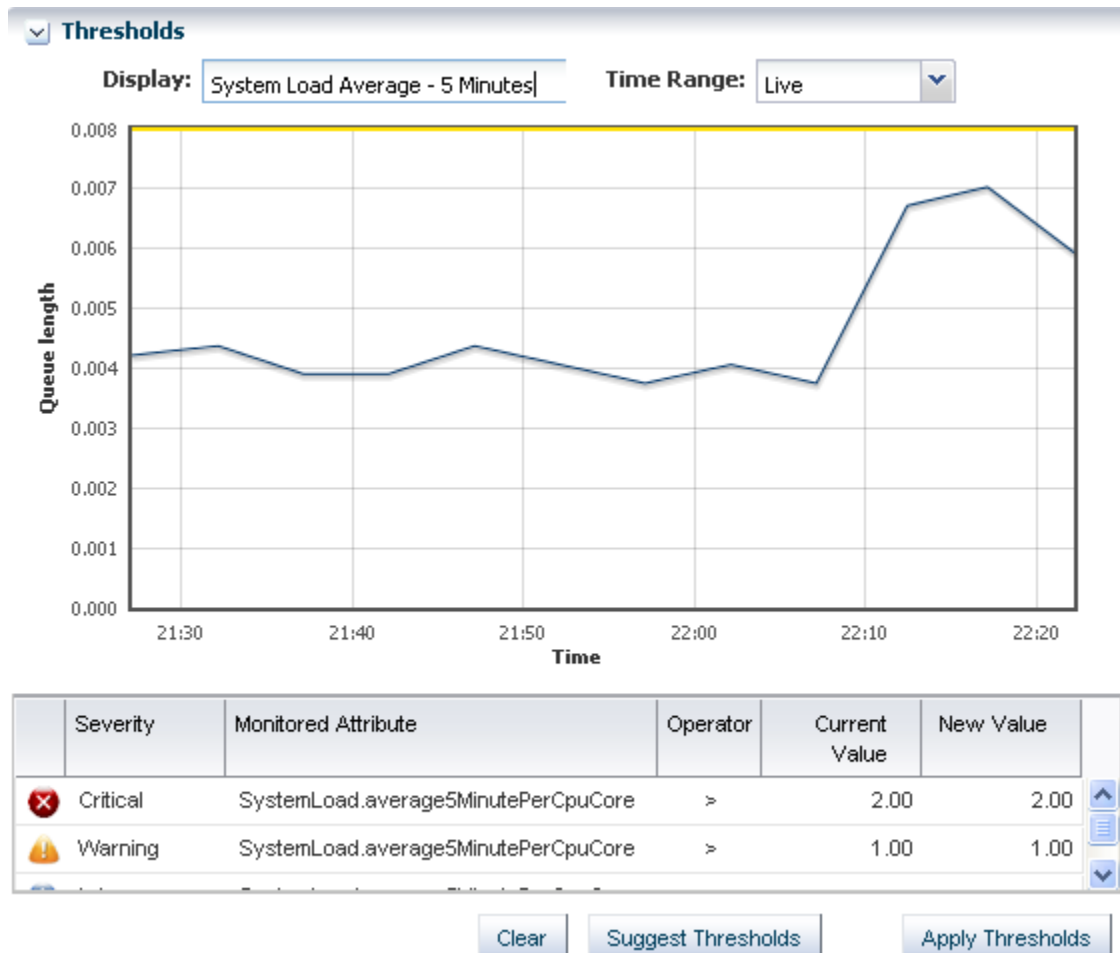
Figure 6-10 *Thresholds Display Options*

Charts for the historical data of those attributes show the alert monitor threshold levels, if configured, for that attribute. [Figure 6-11](#) 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 6-11 Thresholds Chart



Historical Data

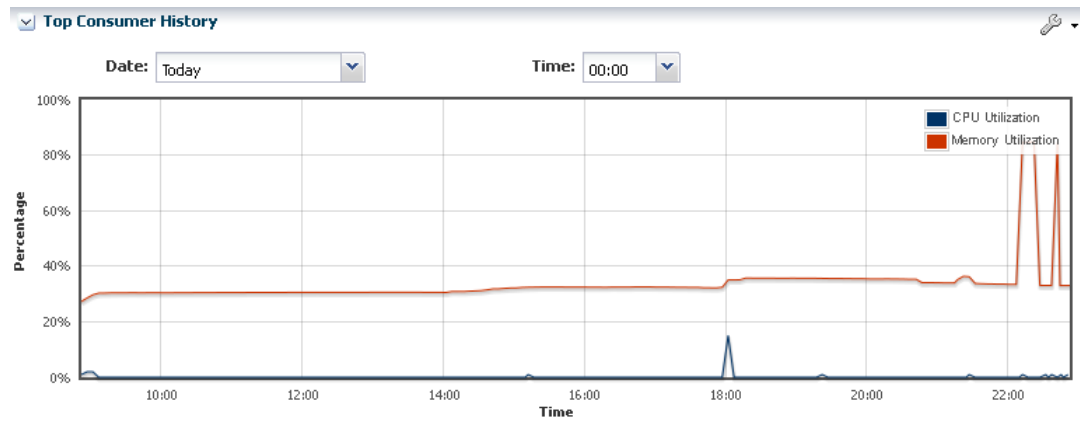
The history chart displays the most applicable chart interval for the selected date and time.

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. [Figure 6-12](#) is an example of a Top Consumer History chart.

Displaying Historical Data

Procedure to display historical data.

1. Display the Analytics view.
2. Click the **History** tab.
3. Click the wrench icon to select from a list of options to chart.

Figure 6-12 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.

Displaying Metrics

Procedure to display metrics.

1. Display the Analytics view.
2. Click the **Metrics** tab to see OS-specific components.

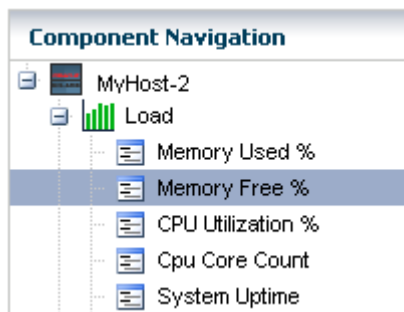
The following are the categories of component details available for an agent-managed Oracle Solaris OS:

- Load
- File Systems
- Networks
- Users
- Buffer Activity
- Disk Usage
- Paging Activity
- Message Activity
- Tables Status
- TTY Activity
- Kernel Memory
- DNLC

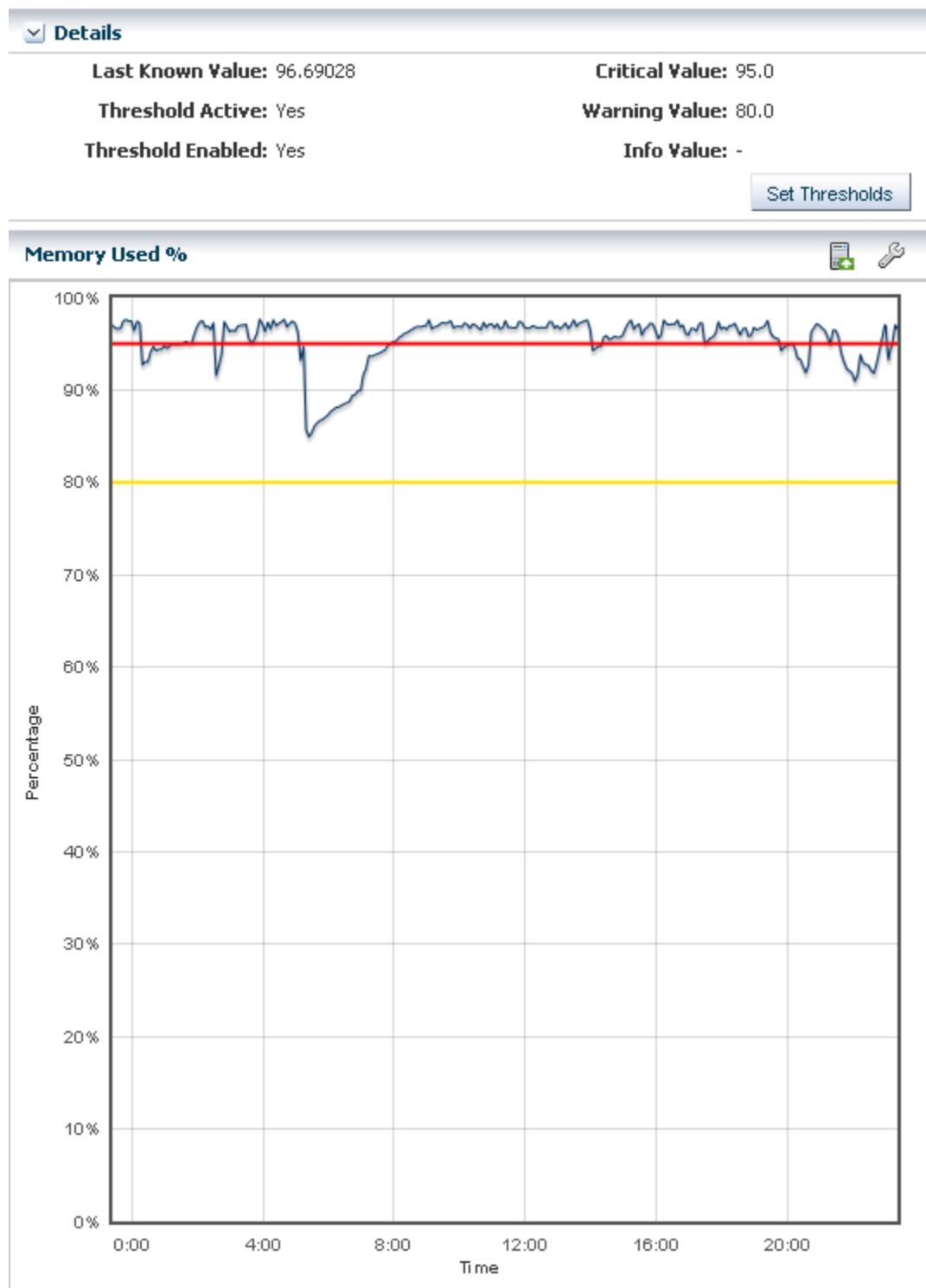
- IPC Message Queue
 - IPC Shared Memory
 - IPC Semaphore Usage
 - CPU Detail
 - File Access
 - Disk Errors
 - Memory Utilization
3. Expand a component to view the available elements.

Click an element to view the details. In [Figure 6-13](#), 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 6-13 Component Navigation



The type of resource determines the available details. [Figure 6-14](#) 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 6-14 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 appears. Editing a threshold value creates 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.

Displaying and Creating Charts

You can modify and change the type of charts.

The Charts tab enables you to modify the following charts to change the type of chart and 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, Oracle Enterprise Manager Ops Center 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

Oracle Enterprise Manager Ops Center deletes the data after six months.

Display Charts

Procedure to display charts.

1. Display the Analytics view.
2. Click the **Charts** tab.

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.

Create Charts

Procedure to create charts.

1. Display the Analytics view.

2. Click the **Charts** tab.
3. Select an option from the Chart type menu to display the output as a line, bar, or area chart.
4. Select **Live**, **1 Hour**, **1 Day**, **5 Days**, **3 Weeks**, **6 Weeks**, or **6 Months** from the X Axis (Time) menu to change the time frame for the data.
5. Select **Percentage** or **Unit of Measure** to configure the chart's Y Axis.
6. Select the component and options to plot from the Plot selection.

By default, the graphs show one day of data. Select **Live** in the X Axis menu 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. Click **Export Chart Data** 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.

Displaying Virtualization Analytics

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.

Customizing the Analytics 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 page affects the views of all analytics screens for the same OS or virtualized OS.

Customize the Analytics View

Procedure to customize the analytics view.

1. Select an operating system (global zone) or zone in the Navigation pane.
2. Click the **Analytics** tab.
3. Click the **Settings Menu** icon in the center pane.
4. If you select a global zone that has zone, click the **Zones Analytics** subtab, then click the **Settings Menu** icon in the center pane to change the view for the Zones Analytics page.

Overview of Oracle Solaris Boot Environments

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.

Understanding the 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 agentlessly-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 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.

Monitoring Boot Environments

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 navigation tree. A warning alert contains a suggested action.
- Critical: Generates a critical alert and displays the red critical badge in the Assets tree. By default, a critical alert contains an automated action.

Clear a Boot Environment Incident

Procedure to manually clear the disk space and close the incident.

Perform the following steps to manually clear the disk space and close the incident:

1. Click an OS in the Assets 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 Incidents** icon in the center pane.

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 does not appear 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 UI. Boot environments for non-global zones appear in the Boot Environment tab, not the Assets tree. Select a non-global zone in the Assets tree, then click the Boot Environments tab in the center pane.

Viewing Boot Environments

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 Assets 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 6-15](#).

Figure 6-15 Boot Environment Tab and Snapshots Subtab

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

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

- 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.

- 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.

- 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.

Managing Boot Environments

You can view all available boot environments for a system, and choose to activate an alternate boot environment or delete inactive environments.

Activating 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.

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 Assets tree.
2. Click the **Boot Environments** tab.

Existing boot environments for the OS appear in the center pane.

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.

Deleting 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 Assets 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 6-16](#) shows a snapshot selected for deletion.

Figure 6-16 Delete an Oracle Solaris 11 Snapshot

Overview of 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.

Displaying Oracle Solaris 11 Boot Environment Details

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:

- Displaying Total ZPools Utilization for Oracle Solaris 11 Boot Environments

- Displaying Oracle Solaris 11 Boot Environments
- Displaying Snapshots for Oracle Solaris 11 Boot Environments
- Displaying File Systems for Oracle Solaris 11 Boot Environments
- Displaying Associated Zone Boot Environments

Displaying 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 6-17](#).

Figure 6-17 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

Displaying Oracle Solaris 11 Boot Environments

All boot environments that are associated with the physical or virtual operating system that is selected in the Assets tree appear in the Boot Environments table.

As shown in [Figure 6-18](#), 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 two green check marks are visible in the Active column, the boot environment is active and is the active boot environment upon reboot.

Figure 6-18 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.

Displaying 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 6-19 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

Displaying 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 6-20](#), 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 6-20 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

Displaying Associated Zone Boot Environments

Associated Zone Boot Environments 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 when the boot environment selected is active. As shown in [Figure 6-21](#), you can see the boot environment name, the zone name, the size and when the boot environment was created. When you select an operating system that is not a zone, No Data appears in the table.

Figure 6-21 Oracle Solaris 11 Boot Environments Associated Zone BEs

Snapshots		File Systems		Associated Zone BEs	
Zone BE Associations of selected BE: solaris					
Active	BE name ▲	Zone Name		Size	Creation Date
No data					

About 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.

Note:

Oracle Solaris 11 boot environments cannot have spaces in the name. When you name a boot environment, do not use spaces.

Create Boot Environments Profile for Oracle Solaris 11

Procedure to create 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. Enter a unique profile name, without spaces, and provide a description to identify the profile. 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**.

Copy an Oracle Solaris 11 Boot Environments Profile

Procedure to copy an Oracle Solaris 11 boot environment 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. Enter a unique profile name, without spaces, and a description.
4. Change the boot environment parameters, as needed, then click **Finish**.

Creating an Oracle Solaris 11 Boot Environment

You can create a bootable or non-bootable copy an existing boot environment. A non-bootable copy is call a snapshot. You can create a boot environment from a snapshot.

A new alternate boot environment is automatically created when you install or update the operating system's kernel or system packages.

Create an Oracle Solaris 11 Boot Environment

Procedure 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 Assets tree, then click the **Boot Environments** tab.
2. Select the boot environment to copy, then click the **Create** icon.
3. Select either the **Create a Snapshot** or **Create a BE** option, then select the boot environment to use as the source. Enter a unique name for the boot environment, without spaces, and provide a description that includes the purpose of the boot environment and the name of the source boot environment. Click **Create**.

Figure 6-22 Create Boot Environment for Oracle Solaris 11

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.

Overview of Oracle Solaris 10 Boot Environments

Boot environments in Oracle Solaris 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).

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 10 OS. Use the packages and patches that are appropriate for your software instance.

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 *Oracle Solaris 10 Installation Guide: Solaris Live Upgrade and Upgrade Planning* at http://docs.oracle.com/cd/E18752_01/html/821-1910/preconfig-17.html. For information on other releases, see *Operating Systems Documentation* at <http://docs.oracle.com/en/operating-systems/>. 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 10 alternate boot environments, file systems are categorized into the following types:

- **Critical File Systems:** Non-sharable 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.
- **Sharable 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, sharable 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 sharable volume. Like a sharable 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 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. Sharable 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 sharable 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.

Requirements for Oracle Solaris 10 Live Upgrade and Oracle Solaris Zones

Lists the requirements 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.

Displaying Boot Environment Details for Oracle Solaris 10

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.

Boot Environments tab is not available for Oracle Solaris 10 non-global zones. The following information is available:

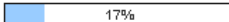
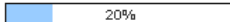
- Displaying Total ZPools Utilization for Oracle Solaris 10 and Earlier Boot Environments
- Displaying Oracle Solaris 11 Boot Environments
- Displaying File Systems for Oracle Solaris 10 and Earlier Boot Environments

Displaying 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 6-23](#).

Figure 6-23 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

Displaying 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 Assets tree appear in the Boot Environments table.

As shown in [Figure 6-24](#), 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 6-24 Boot Environments for Oracle Solaris 10 and Earlier

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.

Displaying 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 6-25](#), 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 6-25 Oracle Solaris 10 Boot Environments File Systems

Name	Type	Size	Mounted on	Shared
shripool/ROOT/EranSol10ABE	zfs	15.57 MB	/	false
/dev/zvol/dsk/shripool/swap	swap	4.00 GB	-	false

About Boot Environment 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. Determining Your Boot Environment Policy
2. Determining Your Live Upgrade Feature Requirements and Options

Determining Your Boot Environment Policy

Each Boot Environment profile can have a different boot environment policy.

The following options are available for Oracle Solaris 10:

- Activate Boot Environment and reboot on job completion.
- Synchronize existing Boot Environment before submitting a job.

Determining Your Live Upgrade Feature Requirements and Options

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.

For Oracle Solaris 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.

Overview of Boot Environments Profiles and Plans

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.

The following is a high-level overview of how to create an alternate boot environment for Oracle Solaris 10 and earlier releases.

1. Create a Boot Environments profile.

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*. When you use *BEName* as the variable name, the operational plan passes 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.

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](#).

Creating an Oracle Solaris 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 interface. With this method, you must login 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.

Defining Deployment Options for Oracle Solaris 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. For 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 resides.

The `-p` is not required when the source and target boot environments are within the same pool. The `-p` option does not support the splitting and merging of file systems in a target boot environment, instead use 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.

Creating an Oracle Solaris 10 Boot Environment 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.

You can use either of the following deployment plans to create an Oracle Solaris 10 boot environment:

- **Boot Environment:** A simple deployment plan that only creates an alternate boot environment. Use the default alternate boot environment profile and then override the applicable parameters to create a boot environment.
- **Software Deployment / Update:** A multi-step plan where one of the steps creates a boot environment. See the *Oracle Enterprise Manager Ops Center Updating Your Oracle Solaris 10 Operating System* for an example of how to use this plan.

Creating a Boot Environment Using Alternate Boot Environment Profile

Perform the following steps to create a boot environment using the Alternate Boot Environment profile and Boot Environment deployment plan:

1. Click an Oracle Solaris 10 OS global zone in the Assets 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.

4. Enter 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.

Creating an Oracle Solaris 10 Boot Environment from an Operational Plan

An operational profile contains a single script and can define variables. The associated plan launches the profile. 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 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 Controller, and the user credentials needed to execute the profile.

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. Enter 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 select EC Shell, browse to the location of the script in the Script File field, then click **Load Script**.
 - If you select Remote Shell, enter your script in the Script field.
7. Enter a numeric value in the Timeout field, then select Minutes or Seconds. The default timeout 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.

Creating an Update Profile for Oracle Solaris 10 Boot Environment

You can use an Update profile to create and update a boot environment.

Perform the following steps to create an update profile for Oracle Solaris 10 boot environment:

1. Expand **Plan Management**, then click **Update Profiles** in the Navigation pane.
2. Click **New Profile** in the Actions pane.
3. Enter 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, select the **Apply to all applicable distributions** check box.
9. Click **Profile Contents** and select an item, then click **Create OS Update Profile**.

Creating an Oracle Solaris 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 Assets 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 appears.

4. Enter 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.

Creating an Oracle Solaris 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. Enter 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** to upload the file to the selected distribution.

Creating a Boot Environment With an OS Update Job

Procedure 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 appears.
3. Complete the following Job Information parameters:
 - Enter 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
 - Select the **Boot Environment Type** check box.

- Select 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. Enter 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 mounting the alternate boot environment, select the **Sync ABE** check box.
 - To edit the description to describe the state of the Boot Environment, click **Modify Current BE**, and enter text in the Description field.
 - To edit the description to describe the state of the alternate boot environment, click **Modify Alternate BE**, and enter text in the Description field.
 - To switch boot environments after update, select 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: 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 new alternate boot environment is associated with the operating system. To verify that the alternate boot environment is created, click the operating system 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 only appears when at least one alternate boot environment associated with the operating system.

Synchronizing 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.

After you sync the boot environments, you can activate the inactive, or alternate, boot environment.

Activating a Boot Environment

Activating a boot environment switches a new boot environment to become the currently running boot environment when the system reboots.

1. Click an Oracle Solaris 10 OS global zone in the Assets tree to view the Boot Environment in the center pane.
2. Click the **Boot Environment** tab.
Existing boot environments for the operating system appear in the center pane.
3. Click **Activate Boot Environment and Reboot** in the Actions pane.
4. To schedule the activation for a later date or time, select the check box. Click **Next**.
5. If you selected the schedule option, complete the schedule, then click **Next**.
6. Review the Summary, then click **Finish**.

The new boot environment activates when you reboot the system.

Related Resources for Operating System Management

This section lists the related resources for OS management.

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

- For more information, see the Oracle Enterprise Manager Ops Center Documentation Library at http://docs.oracle.com/cd/E59957_01/index.htm.
- For end-to-end examples, see the workflows and how to documentation in the library. For deployment tasks, go to http://docs.oracle.com/cd/E59957_01/nav/deploy.htm, for operate tasks go to http://docs.oracle.com/cd/E59957_01/nav/operate.htm, and for administer tasks go to http://docs.oracle.com/cd/E59957_01/nav/administer.htm.
- See [Introduction to 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:

- For a list of the Oracle Linux documentation available in HTML and PDF formats, visit the Oracle Linux Documentation website at <http://www.oracle.com/us/technologies/linux/index.html>.
- For a list of the Oracle Solaris 11 documentation available in HTML and PDF formats, visit the Oracle Solaris 11 Documentation website at <http://>

www.oracle.com/technetwork/documentation/solaris-11-192991.html.

- For a list of the Oracle Solaris 10 documentation available in HTML and PDF formats, visit the Oracle Solaris 10 Documentation website at <http://www.oracle.com/technetwork/documentation/solaris-10-192992.html>.
- For a list of the Oracle Solaris 8 and 9 documentation, visit the Legacy Solaris Documentation website 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>.
- For JET documentation and to download additional modules, see <http://www.oracle.com/technetwork/systems/jet-toolkit/index.html>.

Provision Operating Systems

This section describes the operating system (OS) provisioning features that are available in Oracle Enterprise Manager Ops Center.

The following information is included:

- [Introduction to Operating System Provisioning](#)
- [Roles for Operating System Provisioning](#)
- [Actions for Operating System Provisioning](#)
- [Location of Operating System Provisioning Information in the UI](#)
- [Planning for Operating System Provisioning](#)
- [About OS Provisioning Profiles](#)
- [About OS Configuration Profiles](#)
- [Migrating OS Provisioning Profiles to the New Format](#)
- [About Deployment Plans That Provision an Operating System](#)
- [Provisioning Oracle Solaris 11](#)
- [Provisioning Oracle Solaris 9 and 10](#)
- [Provisioning an Operating System on Logical Domains](#)
- [Provisioning an Operating System on an Oracle Solaris Cluster](#)
- [Provisioning Linux](#)
- [Related Resources for Operating System Provisioning](#)

Introduction to Operating System Provisioning

The provisioning feature provides a method of automatically and consistently installing operating systems on managed systems from the Oracle Enterprise Manager Ops Center UI.

You can provision the following:

- Oracle Solaris operating systems
- Linux operating systems
- Oracle VM Server for SPARC
- Logical Domains

- Oracle Solaris Clusters

This chapter focuses on basic OS provisioning. Many of the concepts apply to other types of provisioning.

Provisioning an operating system installs a specific operating system release with your defined configuration. Earlier versions of the software used a single OS Provisioning profile to define both the operating system and the configuration. Beginning with Oracle Enterprise Manager Ops Center 12.2.0.0.0, the single profile is replaced with an OS Provisioning profile and an OS Configuration profile.

Note:

If you created OS Provisioning profiles in versions of the software earlier than 12c Release 2, see [Migrating OS Provisioning Profiles to the New Format](#) for how Oracle Enterprise Manager Ops Center updates your profiles and plans to the new format.

The following are needed to define your OS provisioning job:

1. **OS Provisioning profile:** Defines the image, provisioning, and installation requirements, including the basic OS configuration and boot network information.
2. **OS Configuration profile:** Defines the networking configuration. You can use a simple networking interface for any Oracle Solaris or Linux operating system, or advanced networking configurations for Oracle Solaris.

When you create a configuration profile for Oracle Solaris, you can configure the following advanced networking options:

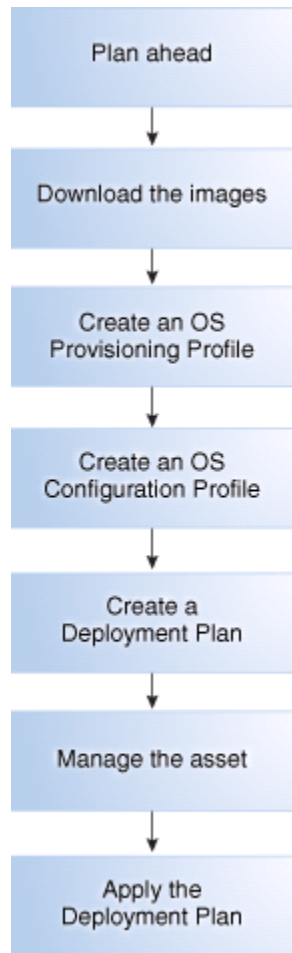
- **Link aggregation:** Provides high availability and higher throughput by aggregating multiple interfaces at the MAC layer. Link aggregation enables you to combine the capacity of multiple full-duplex Ethernet links into a single logical link.
- **IP multipathing (IPMP):** Provides features such as higher availability at the IP layer. IPMP enables you to configure multiple IP interfaces into a single IPMP group.

You can implement both Link Aggregation and IPMP methods on the same network because they work at different layers of the network stack.

After you create the profiles, you create a deployment plan to apply the profiles. As part of applying the plan, you can change some of the options that you defined earlier in the profiles.

3. **Provision OS deployment plan:** Defines the OS Provisioning and OS Configuration profiles to use and the targets to provision. The plan also provides you with an opportunity to provide a specific IP address and to make changes to the network and interface for the target.

[Figure 7-1](#) shows the basic steps that you need to plan for, and complete, a provisioning job:

Figure 7-1 Overview of OS Provisioning

As shown in [Figure 7-1](#), the following are the basic steps that you need to plan for, and complete, a provisioning job:

1. Plan ahead. See [Planning for Operating System Provisioning](#) for items to consider before provisioning.
2. Download a file with the OS image into the Software Library.
3. Create an OS Provisioning profile, edit an existing profile, or reuse an existing profile.
4. Create an OS Configuration profile, edit an existing profile, or reuse an existing OS Configuration profile.
5. For provisioning OS on logical domains, you cannot use the OS Provisioning and OS Configuration profiles created for bare-metal provisioning. You must select the Logical Domain subtype when you create OS provisioning profiles for logical domains.
6. Create or configure a deployment plan that includes the OS Provisioning profile and the OS Configuration profile.

Note:

To successfully provision an operating system, the plan must contain an OS Provisioning profile and an OS Configuration profile with the same platform, either SPARC or x86. For Oracle VM Server for SPARC, the control domain (CDom) version must be the same.

7. Manage the service processor for one or more systems that you want to provision.
 - To provision an existing system with a new operating system, verify that the service processor is discovered.
 - To provision a bare metal system, manage the service processor.
 8. Apply the deployment plan on one or more targets. When you choose a group as a target, it must be a homogeneous group where all members are the same.
-
-

Note:

The target must have a discovered and managed service processor for Oracle Enterprise Manager Ops Center to identify the system as a target.

Default Profiles and Plans

All default profiles and plans have a naming convention that begins with *default* and includes the type of profile or plan and ISO image information.

For example, the software creates the following for an Oracle Solaris 11.0 SPARC-10.1.0 Oracle Solaris Desktop package:

- OS Provisioning profile: `default-profile-Oracle Solaris 11.0 sparc-10.1.0-OracleSolarisDesktop v1`
- OS Configuration profile: `default-osc-profile-Oracle Solaris 11.0 sparc-10.1.0-OracleSolarisDesktop v1`
- Deployment Plan: `default-profile-Oracle Solaris 11.0 sparc-10.1.0-OracleSolarisDesktop-plan`

The default deployment plan references the associated default profiles for the package. You can edit the default profiles and plans, you can create copies of the default profiles and plans and edit them, or you can create your own profiles and plans.

Deployment Plans

A deployment plan defines the OS Provisioning and OS Configuration profiles to apply, the managed targets to provision, the network configuration and IP addresses for the targets, and the tasks to perform. Several different deployment plans let you provision an operating system.

The Provision OS plan is a simple plan with the sole task of provisioning the operating system. The Provision OS plan lets you install the OS on a single system, one or more groups of systems, or a combination of systems that are attached to your network. Other plans are multi-step or complex plans where OS provisioning is one of several tasks performed.

In some cases, the requirements are determined by the target type that you are provisioning. Each target type has different requirements and options.

Note:

To provision Oracle Solaris 11 or to manage Oracle Solaris 11 boot environments, 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.

To provision Oracle Solaris 10 using JET customization, the Enterprise Controller must be installed on a system that is running an Oracle Solaris operating system.

Roles for Operating System Provisioning

Lists the OS provisioning tasks and roles.

[Table 7-1](#) 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 for information about the different roles and the permissions they grant.

Table 7-1 OS Provisioning Tasks and Roles

Task	Role
Import or upload image	Storage Admin
Create OS Provisioning profile	Plan/Profile Admin Asset Admin Update Admin
Create OS Configuration profile	Plan/Profile Admin Asset Admin Update Admin
Create OS Provisioning Deployment Plan	Plan/Profile Admin Asset Admin Update Admin
Apply, or deploy a Deployment Plan	Apply Deployment Plans

Actions for Operating System Provisioning

List the actions for operating systems provisioning.

OS Provisioning enables you to deploy an Oracle Solaris or Linux operating system on a managed system or service processor.

The following actions are available for OS provisioning:

- Modify or create an OS Provisioning profile to define the OS platform, image, configuration, file system, naming service, and other installation parameters.
- Modify or create an OS Configuration profile to define the OS platform, OS management, and network interface configuration.

- Modify or create a Deployment Plan to define which OS Provisioning profile and OS Configuration profile to deploy, to identify the target systems, and to begin a provisioning job.

Location of Operating System Provisioning Information in the UI

Operating system information appears in the **Assets** section in the Navigation pane. The operating system appears beneath the system in the asset tree.

Click the OS in the **Asset** section to display information.

OS Provisioning profiles, OS Configuration profiles, and Deployment Plans appear in the **Plan Management** section in the Navigation pane. Click a profile or plan to view more details.

Planning for Operating System Provisioning

Lists the conditions to consider before provisioning.

The following are some of the items to consider before provisioning:

- Do you need the Enterprise Controller and Proxy Controller installed on Oracle Solaris 11?
- Do you want to use WAN boot or Dynamic Host Configuration Protocol (DHCP) services to support OS provisioning operations?
- Do you want to use advanced networking, either IPMP or Link Aggregation, for Oracle Solaris?
- Do you have OS images available in the library?
- Do you want to create custom scripts to add to the provisioning job?

You can create a script to perform a task that is not defined in the OS provisioning or OS Configuration profiles and include it in the OS provisioning job. For example, you might want to change permission levels or disable print capabilities.

- Do you want to install an Agent Controller on the new operating system for full management capabilities?
- Do you have networks and IP addresses available for provisioning?

Review the following information to plan for OS provisioning:

- Enterprise and Proxy Controller Requirements for OS Provisioning
- Networking for OS Provisioning
- Using WAN Boot for Oracle Solaris Operating Systems
- Using Dynamic Host Configuration Protocol (DHCP)
- Determining the Network Interface to Use
- Provisioning an OS Using a User-Defined MAC Address
- Defining IPMP in an OS Configuration Profile
- Defining Link Aggregation in an OS Configuration Profile
- Adding Images to Local Software Libraries

- About NVRAC When Provisioning an OS on a SPARC Platform
- Creating Custom Scripts
- Determining Agent Management Mode

Enterprise and Proxy Controller Requirements for OS Provisioning

The operating system that the Enterprise Controller and Proxy Controller are installed on might impact your ability to provision an operating system or Oracle VM Server for SPARC.

If you ever plan on provisioning, patching, or managing Oracle Solaris 11, install the Enterprise Controller and Proxy Controller on systems that are running the Oracle Solaris 11 operating system.

[Table 7-2](#) shows the actions that you can perform based upon which operating system that the Enterprise Controller and Proxy Controller are installed.

Table 7-2 Provisioning Actions Determined by the Operating System on which the Enterprise Controller and Proxy Controller are Installed

Action	Enterprise and Proxy Controllers on Oracle Solaris 11	Enterprise and Proxy Controllers on Oracle Solaris 10	Enterprise and Proxy Controllers on Linux
OS Provisioning Oracle Solaris 11	Supported	Not Supported	Not Supported
OS Provisioning Oracle Solaris 11 with JET and DHCP server	JET: Not Supported Oracle DHCP server: Not Supported ISC DHCP server: Supported	JET: Not Supported Oracle DHCP server: Not Supported	JET: Not Supported Oracle DHCP server: Not Supported
OS Provisioning Oracle Solaris 10	JET Supported Oracle DHCP server: Not Supported	JET Supported Oracle DHCP server: Supported	JET: Not Supported Oracle DHCP server: Not Supported
OS Provisioning Oracle Solaris 10 with JET and DHCP Server	JET: Supported Oracle DHCP server: Not Supported	JET: Supported Oracle DHCP server: Supported	JET: Not Supported Oracle DHCP server: Not Supported
OS Provisioning Linux	Supported	Supported	Supported
Provisioning Oracle VM Server for SPARC	Supported	Supported	Enterprise Controller: Supported Proxy Controller: Not Supported
Provisioning Oracle VM Server for x86	Supported	Supported	Supported

Note:

To provision Oracle Solaris 10 using JET customization, the Enterprise Controller must be installed on a system that is running an Oracle Solaris operating system.

Networking for OS Provisioning

The target system boots over the network and gets its network configuration and the location of the install server from a DHCP server or WAN boot.

When provisioning an operating system, the Proxy Controller must be attached to the same subnet as the assets that you want to provision. You can use DHCP or WAN boot (Oracle Solaris only). To improve security and bandwidth, consider establishing a provisioning network for OS deployment and a production network for guest management.

When you install a system from the network, you must provide a method of determining the network configuration (IP address and gateway), which server is going to perform the boot and install, and the installation instructions.

Oracle Enterprise Manager Ops Center uses DHCP services or WAN boot to support OS provisioning operations. DHCP servers enable you to obtain the IP configuration and the rest of the information needed on the NIC. You must configure DHCP services on the Proxy Controller on the same subnet as the target systems to support OS provisioning. Configure the DHCP services in the Oracle Enterprise Manager Ops Center user interface, not from the command line. Oracle Solaris 10 uses the Oracle DHCP server with a Proxy Controller that is running Oracle Solaris 10. Oracle Solaris 11 uses an ISC DHCP server.

WAN boot enables you to provision Oracle Solaris 10 or 11 on a SPARC platform across the network. With WAN boot, the software explicitly configures the information in the Open Boot PROM (OBP) and uses WAN boot for installation.

WANBoot has a number of benefits over broadcast-based installation:

- Not restricted to a single subnet
- Does not require special DHCP configuration or DHCP helpers
- Uses standard HTTP and HTTPS protocols, which cross firewalls much more easily than NFS-based package installations.

Using WAN Boot for Oracle Solaris Operating Systems

Provides information about using WAN Boot for Oracle Solaris OS.

The following information is in this section:

- Overview of WAN Boot
- Requirements for a WAN Boot Connection
- Checking OBP Support for WAN Boot on the Client
- Setting Up a WAN Boot Connection
- Disabling and Enabling WAN Boot

Overview of 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. For Oracle Solaris 10, you need a FLAR to use WAN boot. When you do not use the FLAR, you must enable DHCP before you can provision. 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 works 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). For Oracle Solaris 11, you can edit the SMF service to change the default port from 5555 to another port. See the *Oracle Enterprise Manager Ops Center Administration Guide* for how to reconfigure the default WAN boot port.

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. For more information about secure WAN boot installation configuration, see the *Security Configurations Supported by WAN Boot* section of the *Oracle Solaris 10 10/09 Installation Guide: Network-Based Installations* document at <http://docs.oracle.com/cd/E19253-01/821-0439/wanboottasks2-30/index.html>.

Note:

WANBoot is not available on older hardware.

Requirements for a WAN Boot Connection

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. For M-Series, the XSCF Control Package (XCP) file should be at least version 1082. The XCP file contains the hardware's control programs and includes the XSCF firmware and the OpenBoot PROM firmware.

- 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.

Note:

When the target does not have the required OBP firmware version, the Oracle Solaris 11 provisioning profiles do not appear in the target list for the server.

- Oracle Solaris 10
 - The target is a SPARC (ALOM-CMT, ILOM-SPARC or M-Series) and has the minimum OBP or XCP version
 - Use a FLAR image. WAN boot is only supported in Oracle Solaris 10 if you use flash archives. ISO images require DHCP.
 - 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.
 - The target has the required OBP firmware installed.

Note:

When the target does not have the required OBP firmware version, Oracle Solaris 10 provisioning reverts to a DHCP connection, or OBP/XCP versions + if an ISO is used.

- Verify that the `/opt/SUNWjet/etc/server*interface*` file on the Proxy Controller is updated to use the Proxy IP to target the network.

Checking OBP Support for WAN Boot on the Client

To determine if your client system has a WAN boot-enabled PROM, check the client Open Boot PROM (OBP) for WAN boot support.

1. Log in to a terminal window as root.
2. Enter 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` appears, 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. Use Firmware Provisioning to update the OBP to the required level.

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.

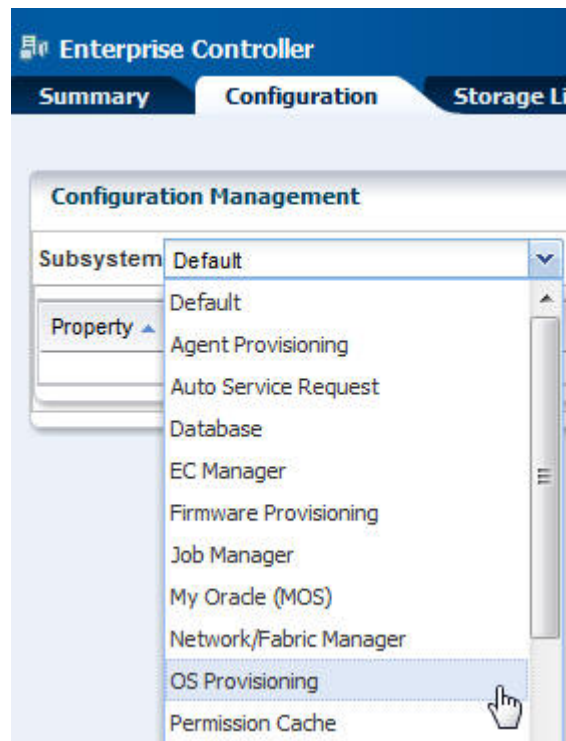
Disabling and Enabling WAN Boot

WAN boot is automatically installed and enabled when the Enterprise Controller is running on an Oracle Solaris operating system. You can disable or enable WAN boot in the Enterprise Controller configuration file.

Perform the following steps to disable and enable WAN boot:

1. Expand the **Administration** section in the Navigation pane, then click **Enterprise Controller**.
2. Click the **Configuration** tab.
3. Select **OS Provisioning** from the Subsystem menu.

Figure 7-2 Enterprise Controller's Configuration Tab



4. Scroll down to the WAN boot property:
 - For Oracle Solaris 11, see the following property: `usesS11WANBoot`.

- For Oracle Solaris 10, see the following property: `useS10WANBoot`.

When `true` appears in the value column, WAN boot is enabled, as shown in [Figure 7-3](#).

Figure 7-3 WAN Boot Configuration

The screenshot shows the 'Enterprise Controller' configuration page with the 'Configuration' tab selected. A table lists various properties and their values. The properties `useS10WANBoot` and `useS11WANBoot` are highlighted with a red box, both showing a value of `true`.

Property	Value
<code>ldom.pis_key.2.2</code>	LDOM_
<code>ldom.pis_key.3.0</code>	LDOM_
<code>ldom.pis_key.3.1</code>	LDOM_
<code>ldom.update_version.1.2</code>	7
<code>ldom.update_version.1.3</code>	7
<code>ldom.update_version.2.0</code>	7
<code>ldom.update_version.2.1</code>	9
<code>ldom.update_version.2.2</code>	10
<code>ldom.update_version.3.0</code>	10
<code>ldom.update_version.3.1</code>	10
<code>supported.ldom_versions</code>	3.1,3.0,
<code>useMSRCache</code>	true
<code>useS10WANBoot</code>	true
<code>useS11WANBoot</code>	true

5. (Optional) To disable WAN boot, change the value for the property to **false**.
6. (Optional) To enable WAN boot, change the value for the property to **true**.

Using Dynamic Host Configuration Protocol (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 *Oracle Enterprise Manager Ops Center Administration Guide* for information about how to configure DHCP and subnets for OS provisioning.

Note:

Oracle Solaris 10 supports an Oracle Solaris DHCP server. The external DHCP-related files are copied only if the Proxy Controller is running on an Oracle Solaris 10 operating system.

Oracle Solaris 11 only supports an ISC DHCP server.

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

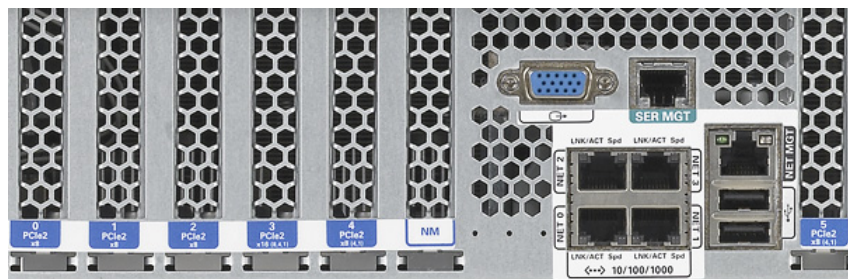
services are not enabled. The Install Server option to provision an OS on a server is not enabled if the DHCP is not enabled on any of the interfaces.

Determining the Network Interface to Use

The OS Configuration profile lets you define all network interfaces you want to use on the operating system. As part of the OS Configuration profile for Oracle Solaris, you have the option to establish Link Aggregation or IPMP network interfaces that the target system will use after the operating system is configured.

The OS Configuration profile lets you define all network interfaces you want to use on the operating system. When you use an on board interface for the provisioning network, you can pair the network with option card interfaces for Link Aggregation. Before you provision, you must know your network architecture. For example, the PCIe slot and NetN connection. [Figure 7-4](#) is an example of the PCIe slots on a T4-4 server.

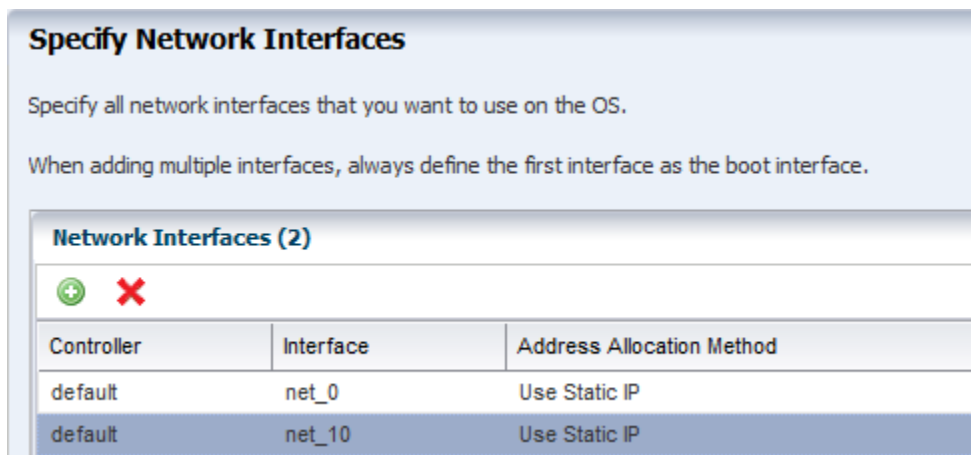
Figure 7-4 PCIe Slots on a T4-4 Server



You can use a built-in network interface or a network that is connected to a specific port on a network interface card (NIC). This information is not available from the Oracle Enterprise Manager Ops Center UI. You must contact your network administrator for the details.

The OS Configuration profile lets you define one or more interfaces. When you specify the network interfaces, you select an interface for the controller from a list of 32 interfaces. The 32 interfaces that appear in the wizard are all possible network interfaces, not available interfaces. Your network administrator can give you the list of available networks and interfaces. As shown in [Figure 7-5](#), the primary interface is `net_0` and is the boot interface in the OS Configuration profile. Always define the first interface that appears in the table as the boot interface. You can change the primary interface to a different network when you apply the plan.

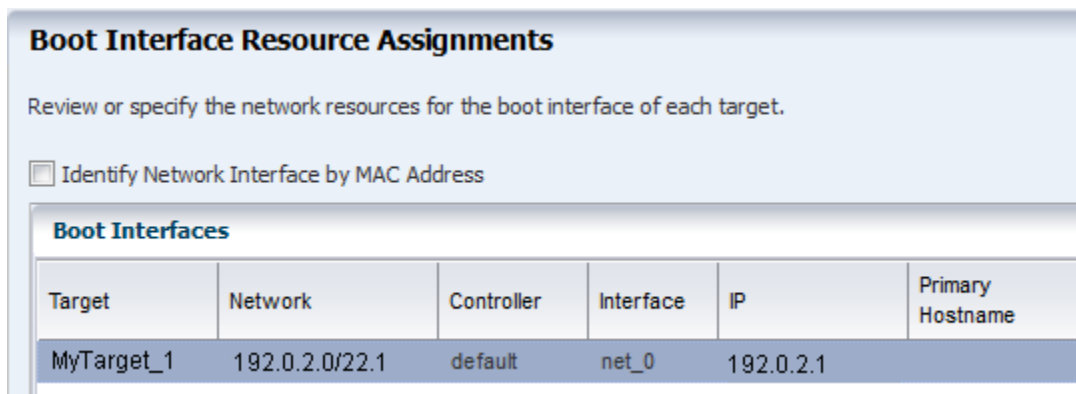
Figure 7-5 Specify Network Interfaces in the OS Configuration Profile



The Boot Interface Resources Assignments page in the OS Configuration profile lets you provide the network resources and host name for each target. By default, the first network listed is the IP address and host name for the primary boot interface. If you do not enter a host name, your DNS server provides the name.

As shown in [Figure 7-6](#), you specify the network resources for the boot interface of each target when you apply the plan, including assigning the network and the IP address for each target. Instead of using the network interface (NIC) to perform an OS provisioning job, you can provide a MAC address for the service processor. When you provide the MAC address, the DNS server provides the host name.

Figure 7-6 Assign Boot Interface Resources in the Deployment Plan



Note:

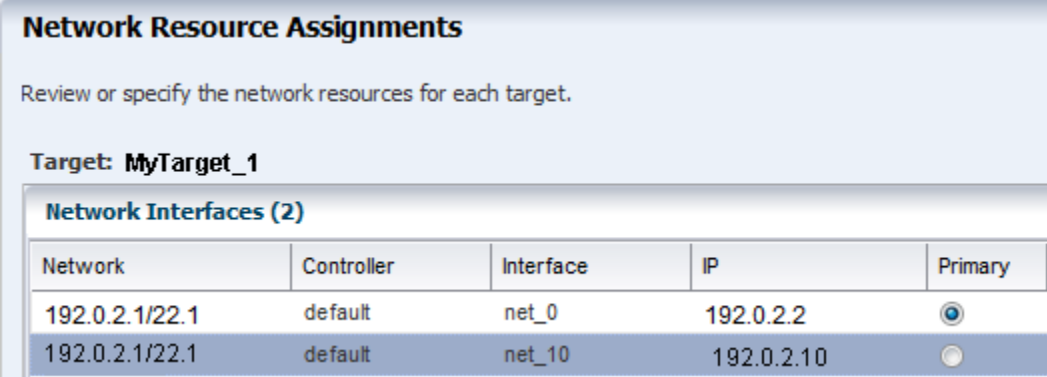
When you apply the plan, the OS Configuration provides a list of available tagged and untagged networks for the boot interface. However, OS provisioning cannot boot from a tagged network and the networks will only be configured in untagged mode.

You can change the networking when you apply a plan that includes OS provisioning, including changing the primary interface to a different interface for a specific target. The flexibility in defining networking is useful when you want to perform OS provisioning and boot on a backup or provisioning network, but you need the host name to match the primary interface. The first listed interface in the OS Configuration

profile is the primary interface and is the interface to use when setting the system host name. You can set a second network interface to be the boot interface.

As shown in [Figure 7-7](#), the deployment plan gives you the opportunity to define which network is the primary network when you have multiple network interfaces.

Figure 7-7 Network Resource Assignments in the Deployment Plan



Network	Controller	Interface	IP	Primary
192.0.2.1/22.1	default	net_0	192.0.2.2	<input checked="" type="radio"/>
192.0.2.1/22.1	default	net_10	192.0.2.10	<input type="radio"/>

Refreshing the Oracle Solaris 11 Service

Oracle Enterprise Manager Ops Center creates an Oracle Solaris 11 `installadm` Automated Installer service when you first configure the Proxy Controller.

If the service is not created during configuration, the software creates the service when you run the first Oracle Solaris 11 OS provisioning job. The service creates and updates the Oracle Solaris 11 Image Packaging System (IPS), which contains the packages that you need to install, provision, and update your Oracle Solaris 11 operating system.

The Oracle Solaris 11 `installadm` service creates and adds the existing network interfaces in the `/var/ai/ai-webserver/listen-addresses.conf`. When you add a new network interface, you must refresh the `installadm` service to enable Oracle Solaris 11 AI service access on that interface.

Note:

When you add a new network interface, run the `svcadm refresh system/install/server` command to refresh the service to enable Oracle Solaris 11 AI service access on that interface. Use the `installadm list` and the other options for `installadm` to check the status. See the *Oracle Enterprise Manager Ops Center Command Line Interface Guide* for more details.

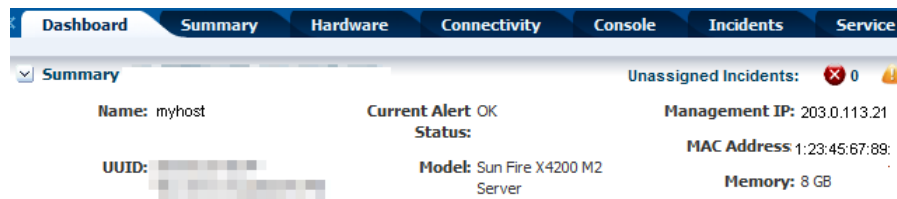
You cannot use new interfaces to provision or update Oracle Solaris 11 until you refresh the service.

Provisioning an OS Using a User-Defined MAC Address

Instead of using the IP address and NIC to perform an OS provisioning job, you can provide a MAC address for the service processor.

To view the MAC address, expand **Assets** in the Navigation pane, then select the service processor. The MAC address appears on the right side of the Summary section of the Dashboard tab, as shown in [Figure 7-8](#).

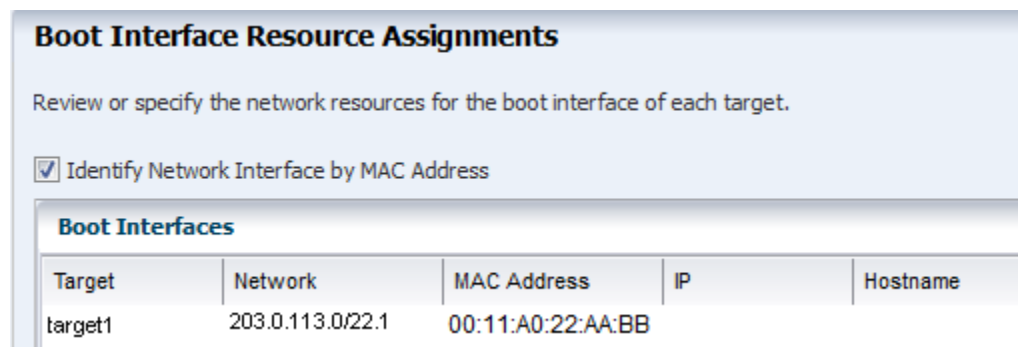
Figure 7-8 Dashboard Page Showing MAC Address



Special OS Provisioning and OS Configuration profiles are not required to use a MAC address for provisioning an operating system. When you apply a plan that includes the OS Provisioning and OS Configuration profiles, you step through the plan to verify the configuration and provide final information before starting the job.

The Boot Interface Resource Assignments page lets you provide the network resources and host name for each target. By default, the first network listed is the IP address and host name for the primary boot interface. Alternatively, you can choose to provide the MAC address. Click **Identify Network Interface by MAC Address** to display the MAC Address field, as shown in [Figure 7-9](#). Enter the MAC Address and the IP Address. When you provide the MAC address, the DNS server provides the host name.

Figure 7-9 Boot Interface Resource Assignments Using MAC Address



Defining IPMP in an OS Configuration Profile

IP multipathing (IPMP) groups provide network failover for your Oracle Solaris operating system, Oracle VM Server for SPARC system, and guests. Use IPMP to improve overall network performance by automatically spreading out outbound network traffic across the set of interfaces in the IPMP group.

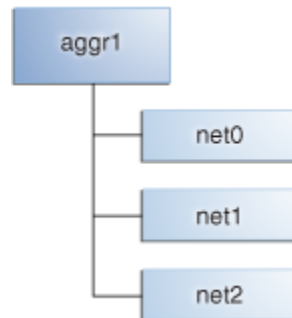
You can configure one or more physical interfaces into an IPMP group. After configuring the IPMP group, the system monitors the interfaces in the IPMP group for failure. If an interface in the group fails or is removed for maintenance, IPMP migrates, or fails over, the failed interface's IP addresses. The failover feature of IPMP preserves connectivity and prevents disruption of any existing connections. The network access changes from the failed interface to the standby interface in the IPMP group and the data address of the failed interface migrates to the standby interface. See [IP Multipathing Groups and Creating IPMP Groups](#) for more information about IPMP groups.

Defining Link Aggregation in an OS Configuration Profile

Link aggregation, as defined in the IEEE802.3ad standard, is an Oracle Solaris feature that enables you to pool several datalink resources into a single logical link to improve network performance and availability.

Figure 7-10 is an example of a link aggregation configured on a system. The aggregation, `aggr1`, has three underlying datalinks, `net0`, `net1`, and `net2`. The datalinks are dedicated to serving the traffic that traverses the system through the aggregation.

Figure 7-10 Link Aggregation



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 provide increased throughput when the network ports are also aggregated.

Link aggregation has the following features:

- **Increased bandwidth:** The capacity of multiple links is combined into one logical link.
- **Automatic failover and failback:** By supporting link-based failure detection, traffic from a failed link is failed over to other working links in the aggregation.
- **Improved administration:** All underlying links are administered as a single unit.
- **Less drain on the network address pool:** The entire aggregation can be assigned one IP address.
- **Link protection:** You can configure the datalink property that enables link protection for packets flowing through the aggregation. **Resource management:** Datalink properties for network resources as well as flow definitions enable you to regulate applications' use of network resources.

When you create an OS Configuration profile, link aggregation is a networking option that is available for Oracle Solaris and Oracle VM Server for SPARC. To define link aggregation networking, you must define a load balancing policy and a MAC address policy.

Aggregated interfaces are treated as a single network interface. Oracle Enterprise Manager Ops Center includes any link aggregations in the list of available NICs, as if the link aggregation were an individual interface. To assign a network with a link aggregation to an Oracle VM Server or 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.

Load Balancing Policy

Load balancing policy determines the outgoing link by hashing the header of each packet.

- **L2:** Determines the outgoing link by hashing the MAC (L2) header of each packet
- **L3:** Determines the outgoing link by hashing the IP (L3) header of each packet

- L4: Determines the outgoing link by hashing the TCP, UDP, or other ULP (L4) header of each packet

Link Aggregation Control Domain (LACP)

If the aggregation topology involves a connection through a switch, determine whether the switch supports LACP. When the switch supports LACP, you must configure LACP for the switch and the aggregation.

- LACP Mode: Select **No** when the switch does not support LACP. When the aggregation topology involves a connection through a switch that supports LACP, configure LACP for the switch and the aggregation and define whether LACP runs in Active or Passive mode.
- LACP Timer: Define the timer as either Short or Long.

MAC Address Policy

You can use Auto or Fixed MAC address of any network interface in the Link Aggregation

- Auto: Use MAC address of any network interface in the Link Aggregation
- Fixed: Use MAC address of a specific network interface. Select the network interface to use in the next step.

Link aggregations perform similar functions as IPMP to improve network performance and availability.

When interfaces are 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.

Adding Images to Local Software Libraries

You can add images and supporting metadata using Upload ISO Image, Import Image, and Download OS Image.

The images and supporting metadata that you use to provision and update operating systems are stored in software libraries, as shown in [Figure 7-11](#).

Figure 7-11 Software Libraries



The software libraries shown in [Figure 7-11](#) are created when you install Enterprise Manager Ops Center:

- **Oracle Solaris 11 Software Library:** Acts as a local copy of the Oracle Solaris 11 Image Packaging System (IPS) repository. This library contains the packages to install, provision, and update Oracle Solaris 11 operating systems.

- **Linux, Oracle Solaris 8-10 Software Library:** Contains Knowledge Base metadata, operating system package and patch content for Linux and Oracle Solaris and operating systems.
- **Initial EC Library:** Stores the operating system (and firmware) images that you download.

You can use the following methods to add images:

- **Upload ISO Image:** Copies the ISO image from a system's web browser to the library.
- **Import Image:** Copies the ISO or FLAR from a file system location on the Enterprise Controller system to the library.
- **Download OS Image:** Downloads the OS image from My Oracle Support to the library.

About NVRAC When Provisioning an OS on a SPARC Platform

When you run an OS provisioning job on a SPARC machine, Oracle Enterprise Manager Ops Center resets the configuration to the factory default configuration and removes the user-defined commands that are executed during start-up and that are stored in the NVRAMRC file in the non-volatile RAM (NVRAM).

The Control Domain OS Provisioning profile does give you the option to preserve the information in the NVRAMRC file.

Creating Custom Scripts

You can create a script and reference the script in the OS Provisioning profile. When the script is saved in a directory that the Enterprise Controller can access, Oracle Enterprise Manager Ops Center deploys the script as part of the provisioning job.

You can save scripts in a local directory of the Enterprise Controller, or in a directory that the Enterprise Controller mounts using NFS.

You cannot use custom scripts when provisioning Oracle Solaris 11.

Determining Agent Management Mode

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.

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.

Agent managed is the more robust management mode because the Agent Controller 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.

About OS Provisioning Profiles

OS Provisioning profiles define the provisioning and installation details.

To complete provisioning, you must have an OS Provisioning profile and an OS Configuration profile. OS Provisioning profiles define the provisioning and installation details.

The following information is covered in this section:

- About Oracle Solaris OS Provisioning Profiles
- About Linux Provisioning Profiles

You can create one or more new libraries to organize and save the images to a location other than the Initial EC Software Library. You can save the images in a local software library on the Enterprise Controller or in a Network Attached Storage (NAS) software library that you create on an NFS server that the Enterprise Controller can access.

After you download the OS images, you can copy or create new OS Provisioning profiles. You can reuse the profiles in a variety of plans that have OS provisioning as a step.

MPxIO is highly desirable on SPARC, whether for a standalone Global Zone or an Oracle VM Server for SPARC Control Domain. MPxIO is enabled on the default OS Provisioning profiles.

About Oracle Solaris OS Provisioning Profiles

When Oracle Solaris 11 OS Provisioning plan is applied, it creates an AI manifest based on the parameters provided to the plan.

For each OS Provisioning profile, you specify the OS image, OS setup parameters, user account details, iSCSI disk usage, file system parameters, and the naming service for the operating system.

When you specify the naming service in the OS Provisioning profile, you must ensure that you enter the correct information in each of the fields. IP addresses 0.0.0.0 or 255.255.255.255 are allowed. Enter each IP address in a new row in the Name Server field. In the Domain Name Search List field, enter each domain name, such as 1domain.com and 2domain.com, on a new line.

As an alternative, you can use a profile that specifies a custom manifest. You do this when you want to install a site-specific file system or OS version.

Automated Installer (AI) provides a customizable, hands-free installation mechanism for Oracle Solaris and uses an XML-based file format as the description of the installation parameters called an AI manifest. When Oracle Solaris 11 OS Provisioning plan is applied, it creates an AI manifest based on the parameters provided to the plan. Starting with Oracle Enterprise Manager Ops Center 12.3 release, you can provide your own AI manifest to use instead of using the AI manifest created by Oracle Enterprise Manager Ops Center. The custom manifest allows installation to be customized in various ways such as disk layout and the software to be installed on the system. You can choose custom manifest while creating the Solaris 11 OS Provisioning profile and upload the XML file containing the custom manifest.

JumpStart Enterprise Toolkit for Oracle Solaris 9 and 10

For Oracle Solaris 9 and 10 only, you can optionally use JumpStart Enterprise Toolkit (JET) modules to specify additional Installation Parameters. Oracle Solaris 11 uses the Automated Installer (AI) instead of JET.

Within the Oracle Enterprise Manager Ops Center UI, there are 2 methods of influencing the JET template variables:

- Import a JET Template
- Add JET variables to the OS provisioning profile

You cannot manipulate the JET template in the UI. When you want to make changes to a template, make the changes and then import the template.

About Linux Provisioning Profiles

Each profile is defined by the OS image that is in the Software Library.

When you specify the naming service in the OS Provisioning profile, ensure that you enter the correct information in each of the fields. IP addresses 0.0.0.0 or 255.255.255.255 are allowed. Enter each IP address in a new row in the Name Server field. In the Domain Name Search List field, enter each domain name, such as 1domain.com and 2domain.com, on a new line.

About OS Configuration Profiles

OS Configuration profiles define the operating system, network configuration details, host name, and server pool configuration.

The OS Configuration profile enables you to specify and assign the following network resources:

- Controller
- Interface
- Address Allocation Method
- Network
- IP address

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. Once created, you can edit the server pool settings.

You can create server pools for Oracle VM Server (for SPARC and x86) and for Oracle Solaris Zones. When you want the server to be added to a server pool, you can configure the OS Configuration profile to assign the newly provisioned server to a compatible server pool or you can create a new server pool based on the attributes of the newly provisioned server and assign default server pool settings.

Two advanced network interface options are available for Oracle Solaris and Oracle VM Server for SPARC systems:

- **Link Aggregation:** Provides high availability and higher throughput by aggregating multiple interfaces at the MAC layer.
- **IP Multipathing (IPMP):** Provides features such as higher availability at the IP layer.

You can implement both methods on the same network because they work at different layers of the network stack.

Defining Link Aggregation in an OS Configuration Profile

Link aggregation groups two or more NICs. All members of the link aggregation provide network access at the same time and are treated as a single network interface. The link aggregation appears in the list of available NICs in the UI as an individual interface.

Link aggregation is a networking option when you create an Oracle Solaris or Oracle VM Server for SPARC OS Configuration profile. You define the link aggregation load balancing policy and a MAC address policy.

1. Expand **Plan Management** in the Navigation pane.
2. Select **OS Configuration** in the **Profiles and Policies** tree. A list of existing OS Configuration profiles appears in the center pane.
3. Click **Create Profile** in the Actions or center pane.
4. Name the profile and enter a profile description. Select **Solaris** as the Subtype and **OSP SPARC** or **OSP x86** as the Target Type. Click **Next**.
5. The default setting is to automatically manage the OS with Oracle Enterprise Manager Ops Center and Deploy the Agent Controller. This option provides the most robust management capabilities. If you do not want to enable SAN storage connectivity, deselect Enable Multiplexed I/O (MPxIO). Click **Next**.
6. Select **Use Link Aggregation** for the Networking Services, then click **Next**.
7. Select a link aggregation name, define the Load Balancing Policy, LACP Mode, MAC Address Policy and the number of link aggregations you want. Click **Next**.
 - Load Balancing Policy determines the outgoing link:
 - L2: Hashes the MAC (L2) header of each packet
 - L3: Hashes the IP (L3) header of each packet
 - L4: Hashes the TCP, UDP, or other ULP (L4) header of each packet
 - LACP
Configure the LACP for the switch and aggregation when your link aggregation topology has a switch connection that supports LACP.
 - MAC Address Policy
 - Auto: Use MAC address of any network interfaces in the Link Aggregation.
 - Fixed: Use MAC address of a specific network interface. Select the network interface to use in the next step.

Figure 7-12 Specify Link Aggregations

Specify Link Aggregations

Specify the IEEE 802.3ad Link Aggregations and configuration parameters.

Link Aggregations (1)

+

✖

Link Aggregation Name	Load Balancing Policy	LACP Mode	LACP Timer	MAC Address Policy	Number of Interfaces
aggr1	L4	Off	Short	Auto	2

- Specify the interface for each link aggregation. The number of interfaces is determined by the number that you defined in step 7. A list of all possible interfaces appears in the wizard. Work with your network administrator to know the interfaces that are available and which interfaces to configure.

Figure 7-13 Specify Link Aggregation Interfaces

Specify Link Aggregation Interfaces

Specify the interfaces to be configured under each Link Aggregation.

NOTE: If the MAC Address Policy of a Link Aggregation is **Fixed**, selected interfaces will be used.

Network Interfaces in aggr1 (2)

Controller	Interface
default	net_0
default	net_10

- Review the summary of the parameters selected, then click **Finish** to create the OS Configuration profile for link aggregation.

Defining IPMP in an OS Configuration Profile

IP multipathing (IPMP) groups provide network failover for your Oracle Solaris operating system, Oracle VM Server for SPARC system, and guests.

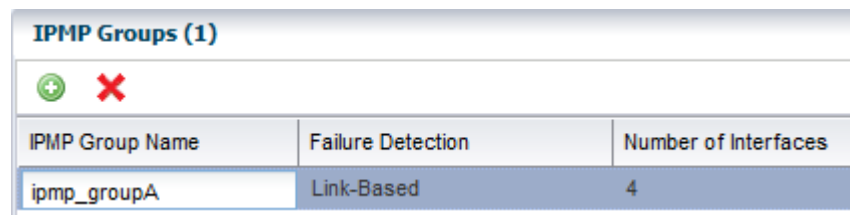
You can configure one or more physical interfaces into an IPMP group. After configuring the IPMP group, the system monitors the interfaces in the IPMP group for failure. If an interface in the group fails or is removed for maintenance, IPMP migrates, or fails over, the failed interface's IP addresses. The failover feature of IPMP preserves connectivity and prevents disruption of any existing connections. The network access changes from the failed interface to the standby interface in the IPMP group and the data address of the failed interface migrates to the standby interface. See IP Multipathing Groups and Creating IPMP Groups for more information about IPMP groups.

- Expand **Plan Management** in the Navigation pane.

2. Select **OS Configuration** in the **Profiles and Policies** tree. A list of existing OS Configuration profiles appears in the center pane.
3. Click **Create Profile** in the Actions or center pane.
4. Name the profile and enter a profile description. Select **Solaris** as the Subtype and **OSP SPARC** or **OSP x86** as the Target Type. Click **Next**.
5. The default setting is to automatically manage the OS with Oracle Enterprise Manager Ops Center and Deploy the Agent Controller. This option provides the most robust management capabilities. If you do not want to enable SAN storage connectivity, deselect Enable Multiplexed I/O (MPxIO). Click **Next**.
6. Select **Use IPMP** for the Networking Services, then click **Next**.
7. Use the default IPMP group name, or click the field and enter a name. Select the Failure Detection Policy, and enter the number of interfaces you want. Click **Next**.

Probe based failure detection probes the target systems to determine the condition of the interface. Each target system must be attached to the same IP link as the members of the IPMP group.

Figure 7-14 IPMP Groups



IPMP Groups (1)		
IPMP Group Name	Failure Detection	Number of Interfaces
ipmp_groupA	Link-Based	4

8. Specify the network interfaces. Select an interface from the list. For each interface, select either the Failover or Standby Interface check box. If you use Link and Probe based failure detection, you do not need to provide test IP addresses. The number of interfaces is determined by the number that you defined in step 7.

Note:

A list of all possible interfaces appears in the wizard. Work with your network administrator to know the interfaces that are available and which interfaces to configure.

Figure 7-15 Specify IPMP Interfaces

Specify IPMP Interfaces

Specify the physical network interfaces for each IPMP group. Select the appropriate check boxes for Failover Interface, Standby Interface, and to assign IP addresses when you configure the spec

Network Interfaces in ipmp_groupA (4)

Controller	Interface	Failover	Standby Interface	Assign IP Address
default	net_0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
default	net_2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
default	net_3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
default	net_4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	net_0			
	net_1			
	net_2			

- Review the summary of the parameters selected, then click **Finish** to create the OS Configuration profile for IPMP groups.

Migrating OS Provisioning Profiles to the New Format

If you have OS Provisioning profiles in a version of Oracle Enterprise Manager Ops Center earlier than 12c Release 2, use the Upgrade feature to upgrade to Oracle Enterprise Manager Ops Center 12.2 and automatically upgrade the profiles to the new format.

The software upgrade feature automatically migrates the OS Provisioning profiles to an OS Provisioning profile and an OS Configuration profile. The original names of the migrated profiles are appended with *osp* or *osc*.

In addition to updating the profiles, existing deployment plans that use an OS Provisioning profile are also updated to use the new OS Provisioning and OS Configuration profiles. Migrating to the new format does not change the version number of the profile or plan.

For every OS provisioning profile created in Oracle Enterprise Manager Ops Center 12.1, a new OS Provisioning profile and a new OS Configuration profile are created in the 12.2 release. The new profiles have the following naming convention: *<12.1_profile_name>-osp* and *<12.1_profile_name>-osc* respectively. Each profile is version one. For example, an OS Provisioning profile is named *S11_SPARC_LargeServer* in the 12.1 release. In the 12.2 release, the profile is converted into the following two profiles: *S11_SPARC_LargeServer_osp* and *S11_SPARC_LargeServer_osc*. The original profile *S11_SPARC_LargeServer* is deleted.

In the 12.1 release, both bare metal provisioning and logical domain guest provisioning were done using the same profiles. Beginning with 12.2, you can only provision a guest with the Logical Domain profile sub-type. When you upgrade from release 12.1 to release 12.2, a new Logical Domain profile is created for each Oracle Solaris 11 bare metal provisioning profile that was created in 12.1. The release 12.1 logical domain OS Provisioning profile is converted in the 12.2 release to a new logical domain OS Provisioning profile and a new OS Configuration profile and the original profile is deleted. The new profiles use the following naming convention:

<12.1_profile_name>-logicaldomain-osp and <12.1_profile_name>-logicaldomain-osc respectively. For example, an OS Provisioning profile is named *S11_SPARC_LargeServer* in the 12.1 release. In the 12.2 release, the profile is converted into the following two profiles: *S11_SPARC_LargeServer_osp* and *S11_SPARC_LargeServer_osc*.

The deployment plans conversion is similar to the profile conversion. New deployment plans are created from the old plans, the plan version is updated, and the plan name is prefixed with <12.1_plan_name>. For example, the name for the new logical domain plan is <12.1_plan_name>-logicaldomain-osp-plan. The new plans use the new OS Provisioning and OS Configuration profiles. For Provision OS plans, the just the version of the 12.1 plan is updated and the OS Provisioning and OS Configuration profiles are added to the plan.

About Deployment Plans That Provision an Operating System

Deployment plans execute the OS Provisioning profile and OS Configuration profile on the targets you select, enabling you to provision in a consistent and repeatable way. Deployment plans are all based on defined templates that provide a sequence of steps to perform a task.

Note:

When adding an OS Provisioning profile and an OS Configuration profile to a plan, use the profiles that reference the same platform subtype.

After you create the profiles to define your tasks, you select a deployment plan template and create a plan that uses specific profiles. You can reuse the profiles in different plans to create consistency.

The following simple, multi-step, and complex plans include steps for OS provisioning:

- Provision OS: Use this plan to provision an operating system.
- Install Server: Use this plan to provision an operating system on the server and update the OS. The Update Software step enables you to update the OS or install additional OS packages. This step is run as part of the OS provisioning job.
- 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 and Install Dynamic System Domain: Use this plan to create dynamic system domains, provision and update OS on 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 Logical Domains: Use this plan to create logical domains and provision OS on the logical domains.

When you select a plan to apply, a list of eligible targets appears in the target selector list. Targets are eligible when they meet the criteria of the profiles, such as type of platform, and for which you have the correct permissions to perform the provisioning tasks. Before deploying the plan on the selected targets, you have the ability to review,

add, and override the configuration settings for the plan. For example, you can change the IP address and the boot interface.

Provisioning Oracle Solaris 11

Lists the provisioning tasks.

The following information is in this section:

- About Oracle Solaris 11 and Provisioning
- Steps for Oracle Solaris 11 Provisioning Plan
- Specifying Common Oracle Solaris 11 Parameters
- Creating an Oracle Solaris 11 OS Provisioning Profile
- Creating an Oracle Solaris 11 OS Configuration Profile
- Provisioning an OS Using a User-Defined MAC Address

About Oracle Solaris 11 and Provisioning

Oracle Solaris 11 uses a new OS provisioning technology, called the Automated Installer. This feature replaces the older JumpStart Enterprise Toolkit (JET) 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 Enterprise Manager Ops Center can create and run multiple `installadm` services on the same Proxy Controller, one for each `solaris-auto-install` mini root. For example, Oracle Solaris 11, 11.1, 11.1.6.4.0, or whenever the `solaris-auto-install` version increases in an SRU (Support Repository Update). An SRU is a package of bug fixes and updates that releases on a regular basis. SRUs eliminate the ad hoc patching from Oracle Solaris 10 and earlier versions of the operating system. Each Oracle Solaris SRU builds upon, and only contains the changes from, the preceding Oracle Solaris 11 update. Oracle Solaris 11 uses a 5-digit taxonomy to define the SRU. The digits represent `Release.Update.SRU.Build.Respin`. For example, Oracle Solaris 11.1.6.4.0.

The Oracle Solaris 11 network architecture is significantly different from previous releases of Oracle Solaris. The implementation, the names of the network interfaces, the commands, and the methods for administering and configuring them is different from previous versions of Oracle Solaris. These changes were introduced to bring a more consistent and integrated experience to network administration, particularly as

administrators add more-complex configurations including link aggregation, bridging, load balancing, or virtual networks. In addition to the traditional fixed networking configuration, Oracle Solaris 11 introduced automatic network configuration through network profiles.

The OS Provisioning and OS Configuration profiles that you use for provisioning Oracle Solaris 11 contain all of the information needed, such as type of target, OS image, time zone and language setup disk partitions, naming services and network details. With Oracle Solaris 11, you can define link aggregations or IPMP groups for advanced networking.

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.

Steps for Oracle Solaris 11 Provisioning Plan

Steps to provision Oracle Solaris 11.

Note:

When you create the plan, both the OS Provisioning profile and the OS Configuration profile must have the same platform subtype, either Solaris SPARC or Solaris x86.

Prerequisites

Lists the prerequisites to follow before you provision the operating system.

Perform the following before you provision the operating system:

- Verify that the Oracle Solaris 11 Software Library is configured on the Enterprise Controller and the package you want is available in the library.

If the image is not in the Oracle Solaris 11 Software Library, import the OS image.

As an alternative, you can use a custom manifest. You do this when you want to install a site-specific file system or OS version.

Note:

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 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.

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.

Steps to Provision Oracle Solaris 11

Procedure to provision Oracle Solaris 11 operating system.

1. Create an Oracle Solaris 11 Provisioning profile.
2. Create an Oracle Solaris Configuration profile.
3. Create a deployment plan that uses Oracle Solaris 11 OS Provisioning and OS Configuration profiles, or verify that a plan and profiles are available and configured with the parameters you want to use.
4. Discover the service processor of the target system.
5. Place the asset in Maintenance Mode to prevent events related to a system going offline.
6. Select the deployment plan and define the targets for the plan. The target must be an x86 server or WAN boot-capable SPARC server. Review the configuration parameters and make any last minute changes in the plan before applying the plan to the target system.

Set SRU Version

When you provision the operating system, you can use the same SRU version that you selected when creating a profile to be used for provisioning.

Perform the following steps to set the SRU version.

1. In the Navigation pane, click **Administration**, then click **Enterprise Controller**.
2. In the center pane, click the **Configuration tab**.
3. In the Configuration Management section, select OS Provisioning from the Subsystem drop-down list.
4. Scroll down to useSRUVersion. The value is set to *false* by default.
 - To set the same SRU version that you selected in the profile to be used for provisioning your operating system, set the value to *true*.

Specifying Common Oracle Solaris 11 Parameters

Oracle Solaris 11 uses some components for OS provisioning.

The following components are used 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.

- **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.

As an alternative, you can prepare a custom manifest, as described in *About Using a Custom Manifest to Provision an OS in Oracle Enterprise Manager Ops Center Configure Reference*.

- **DCHP 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.

Creating an Oracle Solaris 11 OS Provisioning Profile

You can create multiple profiles to respond to subtle variations in hardware attributes, software profiles, or your organization's requirements.

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.

Oracle Solaris 11 System Software Groups

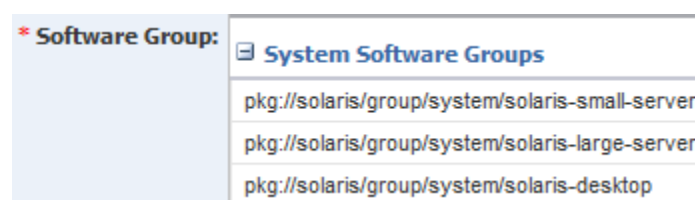
Oracle Solaris 11 provides three system software group packages that install different sets of packages appropriate for a larger server, a smaller server or non-global zone, or a graphical desktop environment.

The boot image is associated with the software group.

As shown in [Figure 7-16](#), you must select one of the following software groups:

- **large-server:** Provides common network services for an enterprise server. This group package also contains hardware drivers that are required for servers, such as InfiniBand drivers.
- **small-server:** Provides a smaller set of packages to be installed on a small server or non-global zone.
- **desktop:** Provides the GNOME desktop environment and other GUI tools such as web browsers and mail. It also includes drivers for graphics and audio devices.

Figure 7-16 System Software Groups



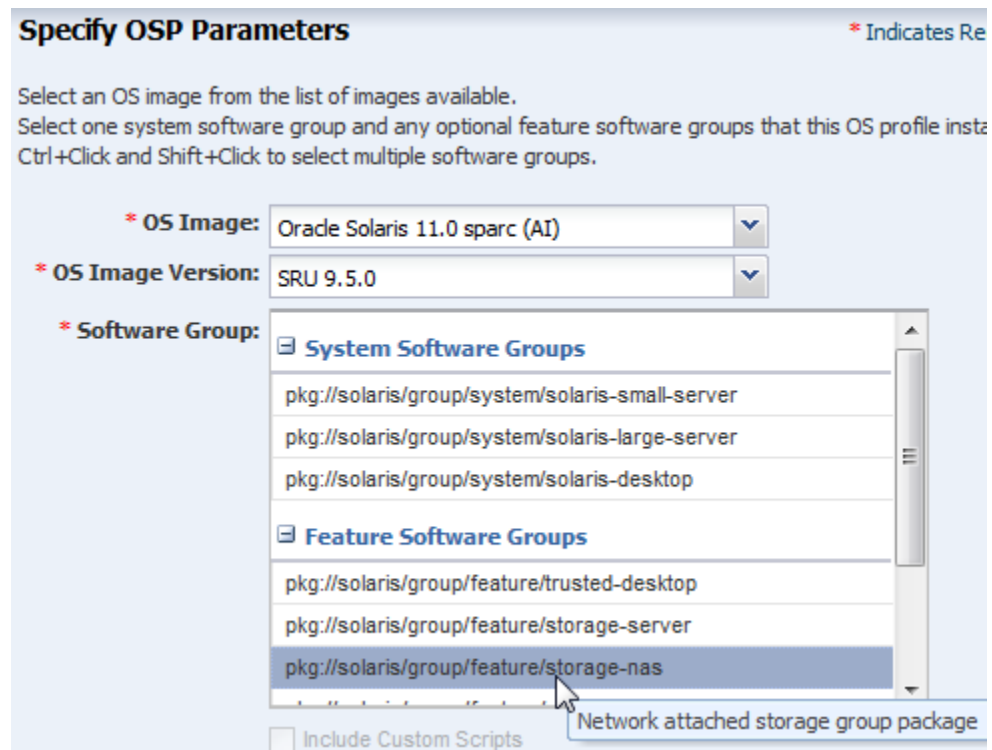
See the Oracle Solaris 11 Package Lists documentation for a detailed comparison of the three packages and list of contents.

Oracle Solaris 11 Feature Software Groups

The boot image might have additional software groups that you can select, such as trusted-desktop, storage-server and storage-nas.

Each group has a tool tip that describes the group, as shown in [Figure 7-17](#). You can select one or more of these groups.

Figure 7-17 Feature Software Groups



To install the operating system on 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

Note:

When you specify the naming service in the OS Provisioning profile, each IP address in the Name Server field must be entered in a new row. IP addresses 0.0.0.0 or 255.255.255.255 are allowed. In the Domain Name Search List field, enter each domain name, such as 1domain.com and 2domain.com, on a new line.

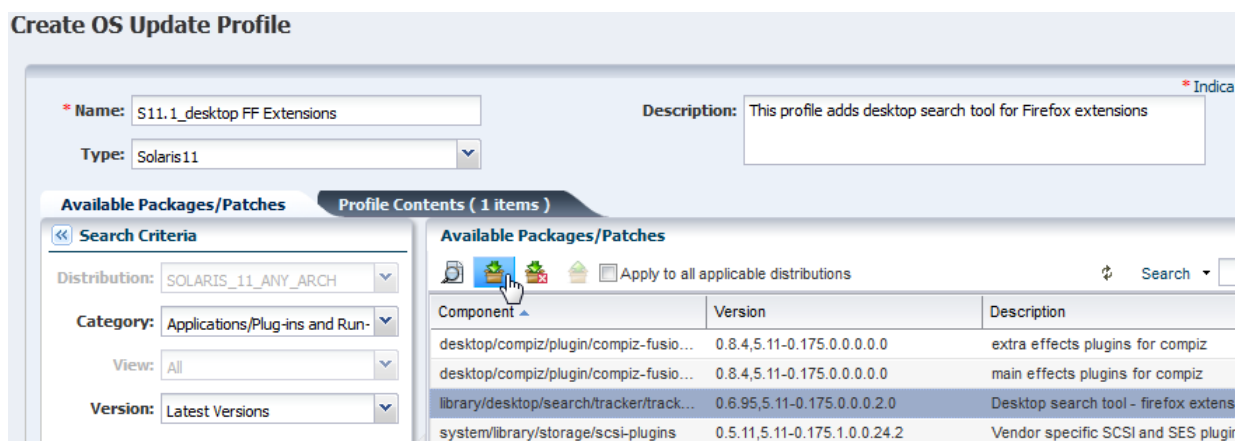
Creating an Oracle Solaris 11 OS Update Profile for Provisioning

You can create an update profile to install a specific Oracle Solaris 11 version or package, uninstall a package, or install a script. First, create a user-defined Oracle Solaris 11 Update Profile to define the action. When you create or edit an OS Provisioning profile, you can add your OS Update profile.

This example shows how to create an OS Update profile that installs the Firefox Extensions package.

1. Expand **Plan Management** in the Navigation pane, then select **Update Profiles** under **Profiles and Policies**.
2. Click **New Profile**.
3. Enter a name and description for the profile, then select **Solaris 11** as the Type.
4. Select Distribution, Category, View, and Version from the Search Criteria. Select Show Only **Support Repository Updates** to further filter the list. The available search criteria are determined by your selection. In this example, select **Applications/Plug-ins and Run-times** from the Category menu and **Latest Versions**. A list of available packages appears on the right side of the page.
5. Highlight the package. Click the **View Details** icon, which is the first icon, to get more information about your selection. To add the package components to the Profile Contents, select the components, then click the **Install** icon.

Figure 7-18 Create OS Update Profile



6. Click **Create OS Update Profile**. The profile appears in the list of Update profiles.

Creating an Oracle Solaris 11 Provisioning Profile

You can use the default profiles, copy a default profile to create a new profile, or create a new profile.

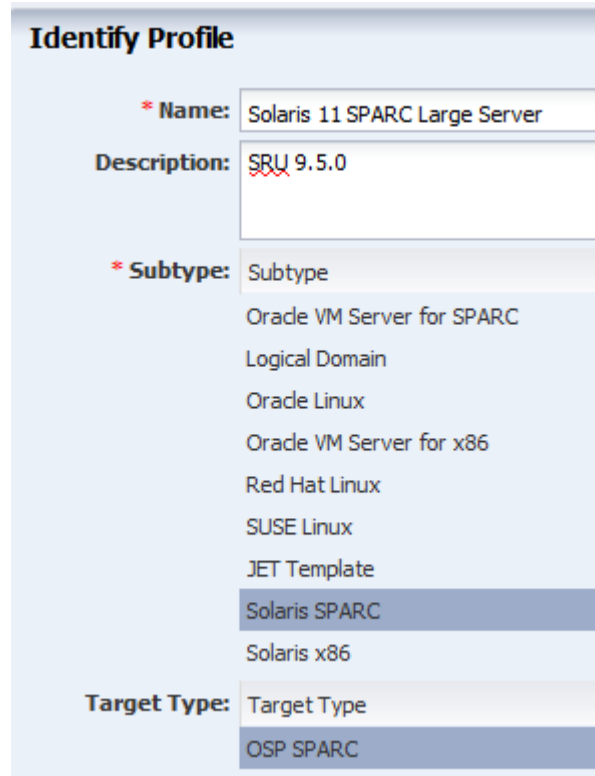
See the *Oracle Enterprise Manager Ops Center Provisioning Oracle Solaris 11 Operating System* document for how to create an OS provisioning profile, an OS Configuration profile, and a Provision OS deployment plan to complete a provisioning job.

This example shows how to create a new profile to provision a system with Oracle Solaris SPARC.

1. Expand **Plan Management** in the Navigation pane, then select **OS Provisioning** in the **Profiles and Policies** tree.

2. Click **Create Profile** in the Actions pane.
3. Name the profile and complete the profile description. A detailed description will help when determining which profile to use when several are available. Select Solaris x86 or Solaris SPARC from the Subtype and Target Type options, then click **Next**. Logical Domain is also supported for custom manifest.

Figure 7-19 Identify Oracle Solaris 11 OS Provisioning Profile



Identify Profile

* **Name:** Solaris 11 SPARC Large Server

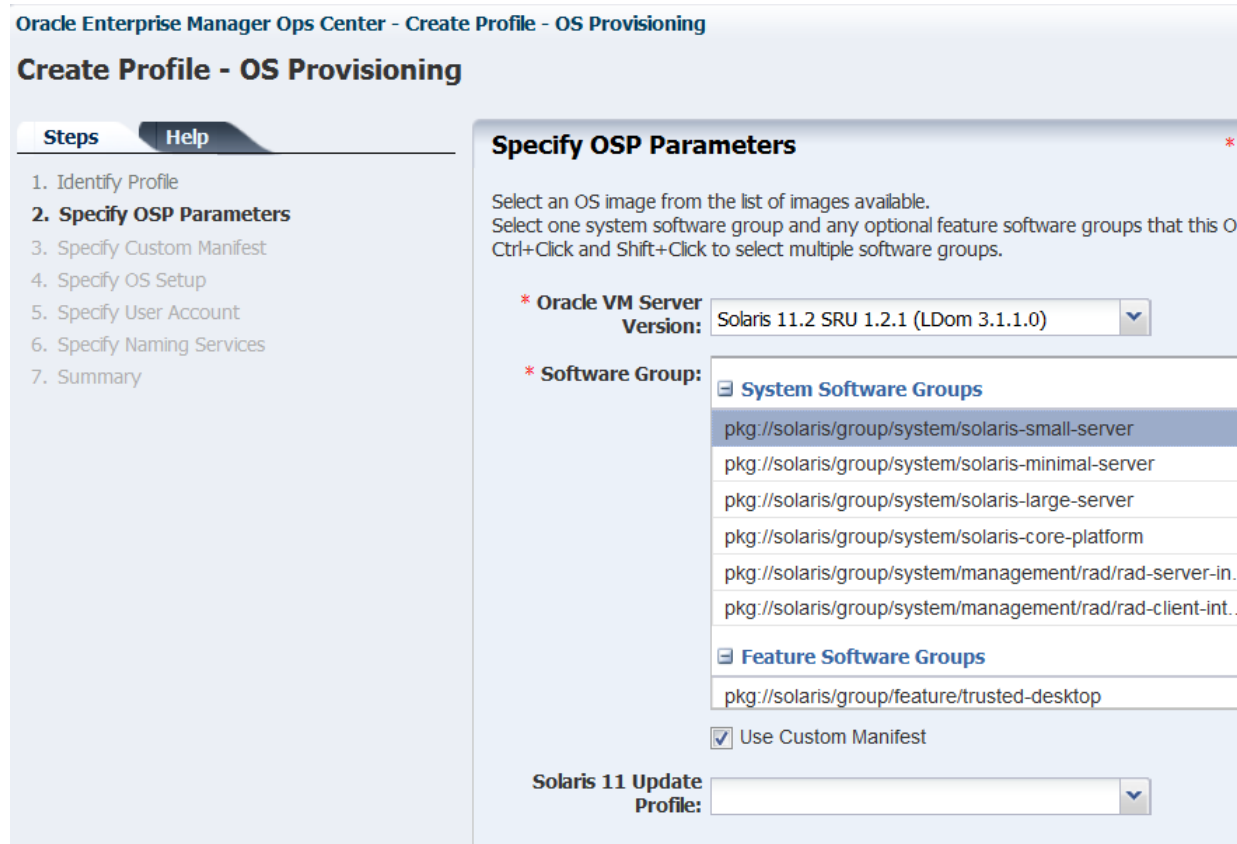
Description: SRU 9.5.0

* **Subtype:** Subtype
Oracle VM Server for SPARC
Logical Domain
Oracle Linux
Oracle VM Server for x86
Red Hat Linux
SUSE Linux
JET Template
Solaris SPARC
Solaris x86

Target Type: Target Type
OSP SPARC

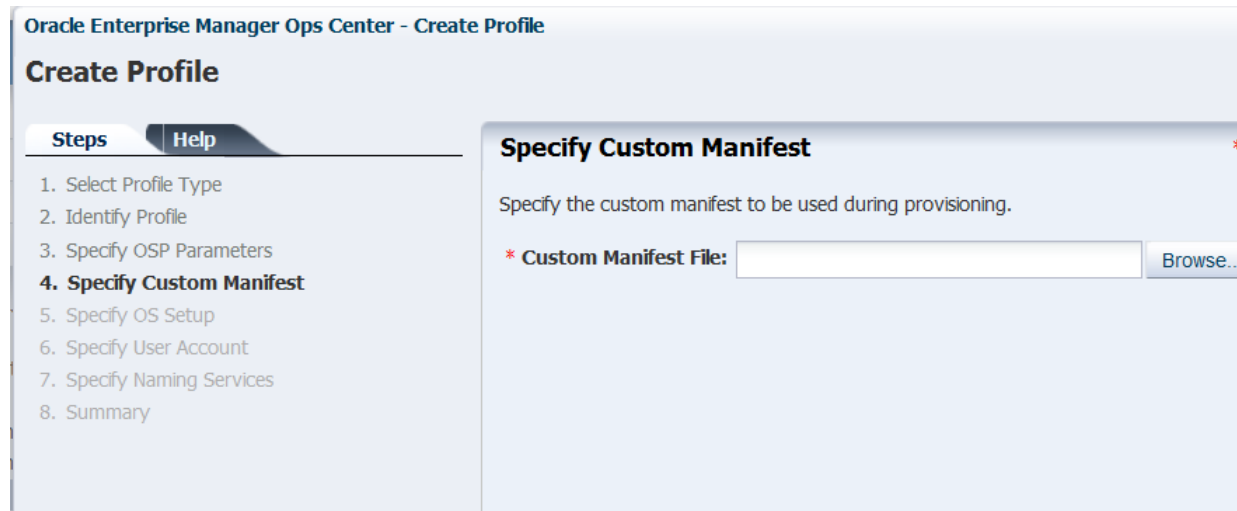
4. Select the OS image, OS Image Version, and Software group. Optionally, you can select a user-defined Solaris 11 Update profile. Click **Next**.

Figure 7-20 Specify OSP Parameters



If you are using a custom manifest, enable the **Use custom manifest** option. When you select this option, a step is added to the wizard so that you can specify the location of the custom manifest, as shown in [Figure 7-21](#).

Figure 7-21 Location of a Custom Manifest



Although not required, it is a good practice to identify profiles and plans that use custom manifests by using a naming convention.

5. Edit the OS Setup parameters for language, time zone, terminal type, console serial port and baud rate, and NFS4 Domain, as needed. Enter a password for root in the Root Password and Confirm Password fields. Click **Next**.
 - Language: Select a language from the list.
 - Time Zone: Specify the time zone for the OS.
 - Terminal Type: Select a terminal type from the list.
 - Console Serial Port: To monitor the installation using a serial connection, select the correct console serial port device.
 - Console Baud Rate: To monitor the installation using a serial connection, select the correct serial port device baud rate.
 - NFS4 Domain: Enter the NFS4 domain name that the target system will use. The dynamic value for NFSv4 domain name enables the NFSv4 domain to be derived dynamically, at run time, based on the naming service configuration. You can also provide valid domain name to hard code the value for NFSv4 domain.
 - Password: Enter the root password for the root user on systems provisioned using this profile. Re-enter the password for confirmation. The default password is *admin*.
 - Manual Net Boot: Select this option when you want to manually control booting from the network. When you select this option, you are prompted to manually boot the system before the provisioning job completes.
 - For DHCP servers: Use the `boot net - install` command to manually boot the system over the network.
 - For WAN boot servers: Set the WAN boot parameters in the Open Boot PROM (OBP) before running the `boot net - install` command.

Note:

The client-ID value of the WAN boot parameters must use the following format: `01<macaddress>`. For example, `client-id=0100123FF4E56E`.

Figure 7-22 Specify OS Setup

Specify OS Setup

Specify language, time zone, terminal type, console and root password for the OS.

Language: English (7-bit ASCII) ▼

Time Zone: GMT ▼

Terminal Type: vt100

Console Serial Port: ttya ▼

Console Baud Rate: 9600 ▼

NFS4 Domain: dynamic

Root Password: ●●●●

Confirm Password: ●●●●

Manual Net Boot

6. Specify the User Account details by entering a user name and password, then click **Next**.
7. On the Specify iSCSI Disk Image page, select the **Use iSCSI Disk** check box if you want to use an iSCSI disk for OS provisioning. When you select **Use iSCSI Disk**, another check box appears. Select **Manually Specify iSCSI Disk** to manually define the iSCSI disk resource assignments later. Click **Next**.

Figure 7-23 Specify iSCSI Disk Usage

Specify iSCSI Disk Usage

Specify if iSCSI disk is used for OS provisioning.

Use iSCSI Disk

Manually Specify iSCSI Disk

Note:

To assign a volume group and automatically create a new iSCSI disk, the DSL library must be attached to the server.

8. Review and edit the default file system layout, then click **Next**.

This example uses the default file system layout. To specify changes to the default File System space, click the size field for the file system, and redefine.

Figure 7-24 Specify File System Layout

Specify File System Layout

Specify the file systems that need to be created.

File Systems (2)

+ ×

File System Type	Mount Point	Device	Size (MB)
swap	swap	rpool	4096
zfs	/	rootdisk.s0	Remaining unused space

NOTE: To allocate the remaining unused disk space to a specific file system, do not enter any value for its size (leave the size field blank).

9. Select the Naming Service as **None**, **DNS**, **NIS**, or **LDAP**, then click **Next**.

Specify Naming Services * Indicates Required Field

Specify the name service, the domain name, and the corresponding name server.
 If the name service is specified, the hostname would be automatically derived from it.
 Otherwise, the hostname will be generated by substituting the '.' in the target's IP address with '-'.

Name Service: NONE DNS NIS NIS+ LDAP DNS+LDAP

When using a naming service, select the service and complete the required fields.

10. Review the parameters and click **Finish** to create the OS Provisioning profile for provisioning Oracle Solaris 11 operating system.

Figure 7-25 Oracle Solaris 11 OS Provisioning Profile Summary

Summary

Name: Solaris 11 SPARC Large Server

Description: SRU 9.5.0

Target Type: OSP SPARC

OS Image: Oracle Solaris 11.0 sparc (SRU 9.5.0) (AI)

Software Group: pkg://solaris/group/system/solaris-large-server

Language: U.S.A. (en_US.ISO8859-15)

Time Zone: GMT

Terminal Type:

Console Serial Port: ttya

Console Baud Rate: 9600

NFS4 Domain: dynamic

Manual Net Boot:

Solaris 11 Update Profile:

Username: Admin

Full Name: Admin

Use iSCSI Disk:

Manually Specify iSCSI Disk:

File Systems (2)

< Previous Finish Cancel

The profile appears in the center pane and in the Profiles and Policies section of **Plan Management**.

Creating an Oracle Solaris 11 OS Configuration Profile

The OS Configuration profile defines the networking configuration. You can use advanced networking configurations for Oracle Solaris.

When you create a configuration profile for Oracle Solaris, you can configure the following advanced networking options:

- **Link aggregation:** Provides high availability and higher throughput by aggregating multiple interfaces at the MAC layer. Link aggregation enables you to combine the capacity of multiple full-duplex Ethernet links into a single logical link.
- **IP Multipathing (IPMP):** Provides features such as higher availability at the IP layer. IPMP enables you to configure multiple IP interfaces into a single IPMP group.

You can implement both Link Aggregation and IPMP methods on the same network because they work at different layers of the network stack.

After you create the profiles, you create a deployment plan to apply the profiles. As part of applying the plan, you can change the options that you defined earlier in the profiles.

Note:

When you specify the network interfaces, select an interface for the controller from a list of 32 interfaces. The 32 interfaces that appear in the wizard are all possible network interfaces, not available interfaces. Your network administrator can give you the list of available networks. By default, the first interface listed is the boot interface.

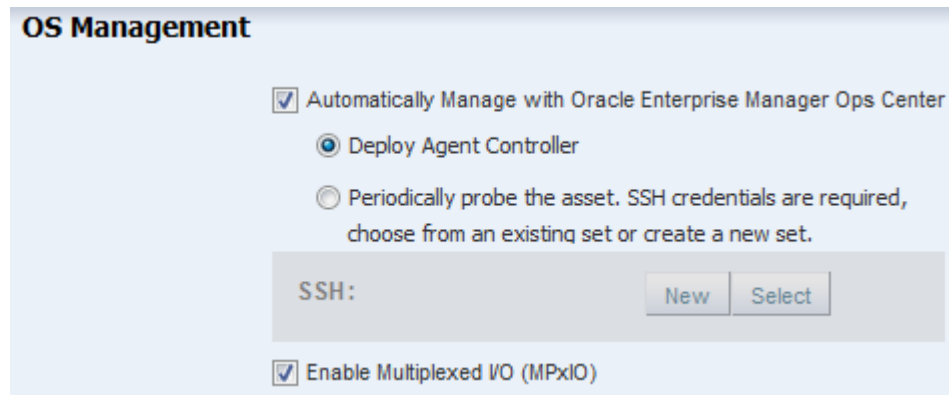
Creating an OS Configuration Profile

Procedure to create an OS Configuration Profile.

1. Expand **Plan Management** in the Navigation pane, then select **OS Configuration** in the **Profiles and Policies** tree.
2. Click **Create Profile** in the Actions pane.
3. Name the profile and complete the profile description. A detailed description will help when determining which profile to use when several are available. Select Solaris x86 or Solaris SPARC from the Subtype and Target Type options, then click **Next**.

Figure 7-26 Identify Oracle Solaris 11 OS Configuration Profile

4. Click **Next** to accept the default selection to **Automatically manage with Oracle Enterprise Manager Ops Center** and **Deploy the Agent Controller**. This option provides the most robust management capabilities.

Figure 7-27 OS Management

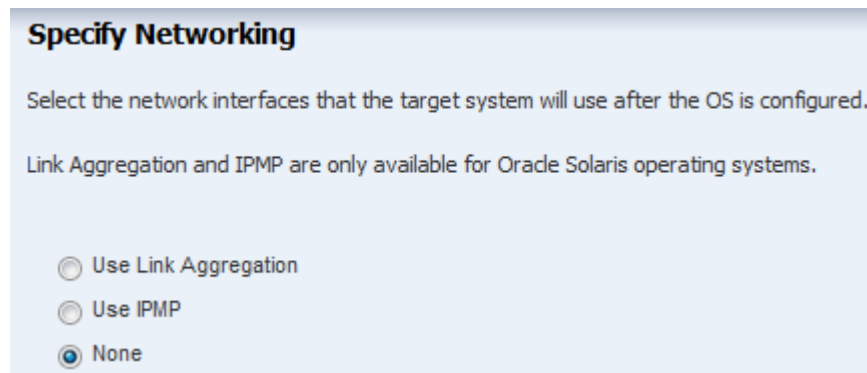
The screenshot shows the 'OS Management' configuration window. It features a title bar 'OS Management' and several options:

- Automatically Manage with Oracle Enterprise Manager Ops Center
- Deploy Agent Controller
- Periodically probe the asset. SSH credentials are required, choose from an existing set or create a new set.

Below these options is a section for SSH credentials, labeled 'SSH:', with a text input field and two buttons: 'New' and 'Select'.

- Enable Multiplexed IO (MPxIO)

5. Specify the networking you want to establish for the target system.
 - Use **Link Aggregation**, go to Step 6.
 - Use **IPMP**, go to Step 7.
 - **None**, go to Step 8.

Figure 7-28 Specify Networking

The screenshot shows the 'Specify Networking' configuration window. It features a title bar 'Specify Networking' and the following text:

Select the network interfaces that the target system will use after the OS is configured.

Link Aggregation and IPMP are only available for Oracle Solaris operating systems.

- Use Link Aggregation
- Use IPMP
- None

6. If you selected Link Aggregation in Step 5, complete the following steps for each link aggregation:
 - a. Specify the Link Aggregation parameters.

Figure 7-29 Specify Link Aggregations

Specify Link Aggregations

Specify the IEEE 802.3ad Link Aggregations and configuration parameters.

Link Aggregations (2)

+ ✖

Link Aggregation Name	Load Balancing Policy	LACP Mode	LACP Timer	MAC Address Policy	Number of Interfaces
aggr1	L4	Off	Short	Auto	2
aggr2	L4	Off	Short	Auto	2

- b. Specify the Link Aggregation interfaces for each Link Aggregation.

The 32 interfaces that appear in the list (net_0 - net_31) are possible network interfaces, not available interfaces. Contact your network administrator for a list of available interfaces.

Figure 7-30 Specify Link Aggregation Interfaces

Specify Link Aggregation Interfaces

Specify the interfaces to be configured under each Link Aggregation.

NOTE: If the MAC Address Policy of a Link Aggregation is **Fixed**, select the network interface whose MAC Address will be used.

Network Interfaces in aggr1 (2)

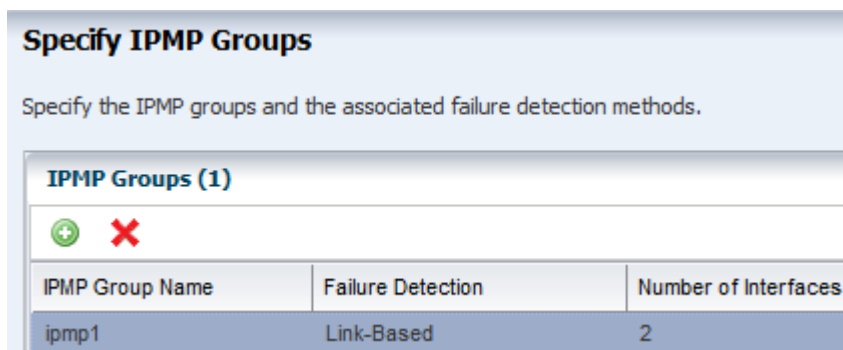
Controller	Interface
default	net_0
default	net_8

Network Interfaces in aggr2 (2)

Controller	Interface
default	net_10
default	net_11

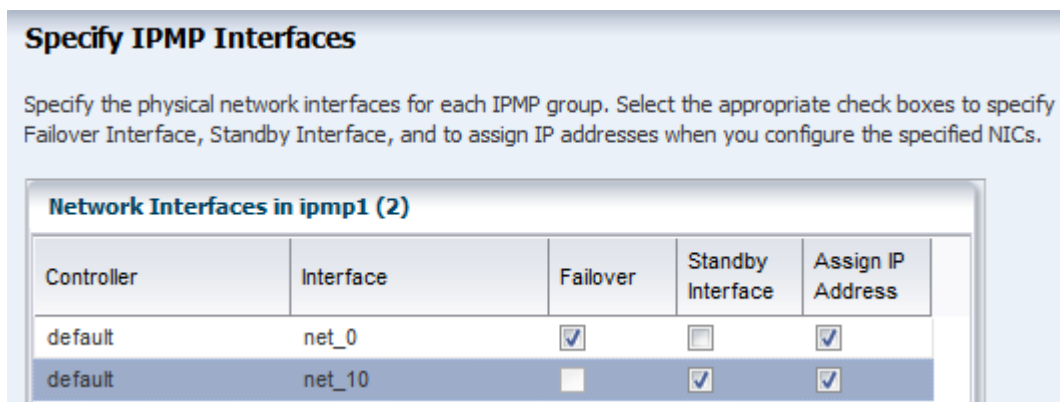
- c. Go to Step 9.
7. If you selected Use IPMP in Step 5, complete the IPMP parameters.
- a. Complete the Failure Detection method, either Link-Based or Link Based + Probe Based, and the number of interfaces.

Figure 7-31 Specify IPMP Groups



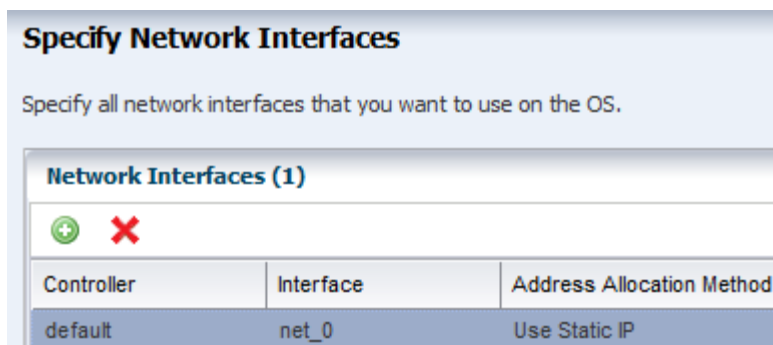
- b. Specify the interface. Select the check boxes to define the IPMP configuration for **Failover** and **Standby Interface**. Select **Assign IP Address** to assign the IP address.

Figure 7-32 Specify IPMP Interfaces



- c. Go to Step 9.
8. If you selected None for Networking in Step 5, define the network interfaces that you want to use on the operating system. The boot interface is typically net_0, as shown in Figure 7-33. You define the IP address when you apply the plan to a target system. Click the **Add** icon to add other interfaces.

Figure 7-33 Specify Network Interfaces



9. Review the Summary page, then click **Finish**. The new configuration appears in the table in the center pane. Click the profile to view the details.

Provisioning Oracle Solaris 9 and 10

You can create OS profiles for provisioning Oracle Solaris 9 or 10 on x86 or SPARC platforms. The OS Provisioning and OS Configuration profiles collect 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.

Perform the following before you provision the operating system:

- Import the OS image. 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.

Note:

Oracle Solaris 10 supports an Oracle Solaris DHCP Server. The external DHCP-related files are copied only if the Proxy Controller is running on an Oracle Solaris 10 operating system.

- 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.

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.

Complete the following steps to provision an operating system:

1. Verify that the OS Provisioning profile and OS Configuration profile are available and configured with the parameters you want to use.
2. Create a deployment plan that enables OS provisioning. The plan must contain an OS Provisioning profile and an OS Configuration profile that use the same subtype, either Oracle Solaris SPARC or x86.
3. Discover the service processors of the target systems.
4. Place the asset in Maintenance Mode to prevent events related to a system going offline.

5. Select the deployment plan and define the targets for the plan. Make any last minute changes in the plan, then submit the job.

See the *Oracle Enterprise Manager Ops Center Provisioning Oracle Solaris 10 Operating System Guide* for an end-to-end example.

Specifying Common Oracle Solaris 9 and 10 Parameters

Specify parameters to create a profile that installs the Oracle Solaris 9 or 10 OS.

To create a profile that installs the Oracle Solaris 9 or 10 OS, specify the following parameters:

- **Manual reboot:** 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.

- **Custom Scripts:** When you specify the OS Parameters, you have the option to include custom scripts. This feature is disabled for Oracle Solaris 11 profiles.

About JumpStart Enterprise Toolkit (JET) for Oracle Solaris

For Oracle Solaris 9 and 10 only, you can optionally use JumpStart Enterprise Toolkit (JET) modules to specify additional installation parameters. Oracle Solaris 11 uses the Automated Installer (AI) instead of JET.

JET provides a framework to simplify and extend the JumpStart functionality provided within the Oracle Solaris 9 and 10 operating system. The `SUNWjet` and `JetFLASH` packages are installed on the Proxy Controller during installation when the Proxy Controller is installed on an Oracle Solaris 10 operating system.

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 7-3](#) describes the JET modules that are installed on the Proxy Controller.

Table 7-3 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.

Within the Oracle Enterprise Manager Ops Center UI, there are 2 methods of influencing the JET template variables:

- Import a JET Template
- Add JET variables to the OS provisioning profile

You cannot manipulate the JET template in the UI. When you want to make changes to a template, make the changes and then import the template.

Creating 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 can save them on the Enterprise Controller and use them in your Oracle Solaris provisioning profiles.

Creating an Oracle Solaris 9 or 10 OS Provisioning Profile

The OS Provisioning profile defines the OS provisioning parameters, including the platform-specific OS image and software package, file system layout, user accounts, naming services, and other installation requirements.

Complete the following steps to create an OS Provisioning profile:

1. Expand **Plan Management** in the Navigation pane.
2. Select **OS Provisioning** under the **Profiles and Policies** section.
3. Click **Create Profile** in the Actions pane.
4. Define the following profile parameters in the **Create Profile-OS Provisioning** wizard, then click **Next**.
 - Name: The name of the profile.

- Description: A description of the profile.
 - Subtype: Select Solaris SPARC or Solaris x86.
 - Target Type: Select the target type, either SPARC or x86.
5. Select an **OS Image**, **OS Image Version**, and **Software Group**. This example does not include custom scripts. Click **Next**.
 6. Specify the following OS setup parameters:
 - Language: Select a language for the OS.
 - TimeZone: Specify the time zone for the OS.
 - Terminal Type: Enter a terminal type, if other than the default type listed.
 - Console Serial Port: A default port appears in the wizard. If incorrect, select the correct console serial port device for your environment. This port enables you to monitor the installation using a serial connection.
 - Console Baud Rate: A default serial port device baud rate is provided. If incorrect, select the correct baud rate for your device.
 - NFS4 Domain: Enter the NFS4 domain name that the target system will use. The dynamic value for NFSv4 domain name enables the NFSv4 domain to be derived dynamically, at run time, based on the naming service configuration. You can also provide valid domain name to hard code the value for NFSv4 domain.
 - Password: Enter the root password for the root user on systems provisioned using this profile. Re-enter the password for confirmation.
 7. Click **Next** to skip specifying the Installation Parameters.
 8. Review and edit the default file system layout, then click **Next**.

To specify changes, click the size field for the file system and redefine the size. To add another file system, click the **Add** icon and complete the fields.
 9. Select the naming service you want, or select **None**, then click **Next**.
 10. Review the parameters selected for Oracle Solaris 10 operating system provisioning, then click **Finish** to save the profile.

Creating an Oracle Solaris 9 or 10 OS Configuration Profile

The OS Configuration profile defines the networking configuration.

When you create a configuration profile for Oracle Solaris, you can configure the following advanced networking options:

- **Link aggregation:** Provides high availability and higher throughput by aggregating multiple interfaces at the MAC layer. Link aggregation enables you to combine the capacity of multiple full-duplex Ethernet links into a single logical link.
- **IP Multipathing (IPMP):** Provides features such as higher availability at the IP layer. IPMP enables you to configure multiple IP interfaces into a single IPMP group.

You can implement both Link Aggregation and IPMP methods on the same network because they work at different layers of the network stack.

After you create the profiles, you create a deployment plan to apply the profiles. As part of applying the plan, you can change some of the options that you defined earlier in the profiles.

Provisioning an Operating System on Logical Domains

When you create OS Provisioning and OS Configuration profiles, select the Logical Domain subtype.

To provision an operating system on logical domains, you must select the Logical Domain subtype when you create OS Provisioning and OS Configuration profiles and select UAR from the OS Image drop down list. You cannot use the OS profiles that are created for bare-metal provisioning.

Provisioning an Operating System on an Oracle Solaris Cluster

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 handles the pre-action and post-action operations.

See the Oracle Solaris Cluster documentation for how to install a new Oracle Solaris Cluster and to maintain existing Oracle Solaris Clusters.

Using UAR for OS Provisioning

You can use UAR when provisioning your operating system. UAR speeds up OS provisioning.

Unified Archive (UAR) is a feature introduced in Oracle Solaris 11.2. It enables you to clone existing systems or install new systems using a UAR image. Starting with Oracle Enterprise Manager Ops Center 12c Release 3 (12.3.1.0.0), you can use UAR images to create new Oracle Solaris 11 operating systems, control domains, logical domains, and global zones. Provisioning of kernel zones and non-global zones is not supported. You can import UAR images using the local library's Import Image action. To provision a system using a UAR image, the boot archive of the corresponding Oracle Solaris 11 version must be available on the MSR. Once a UAR image has been imported, you can select it as a source using the existing OS provisioning wizard.

If you import a UAR image to a NAS library, OSP jobs using the image might fail if the NFS settings are not correct. Create the file as root user in the mounted library on EC and verify that the file is owned by root user.

Renaming an ISO, FLAR, or UAR image causes plans using the image to fail. If necessary, delete the images and re-import them with a new name.

Perform the following steps to create an OSP profile using UAR to provision your operating system:

1. In the Navigation pane, select **Plan Management**, then expand **Plans and Profiles**.
2. Select OS Provisioning Profile and click **Create Profile** in the Actions pane. The Create Profile — OS Provisioning wizard opens.
3. Enter a name and description for the profile.
4. In the Subtype field, select the type of system you want to provision. For example, Solaris x86, Solaris SPARC, and so on.

5. Click **Next**.
6. In the OS Image field, select the UAR that corresponds to the system you want to provision.
7. In the OS Image Version field, select the OS image version.
8. Click **Next**.
9. Retain the default values for the OS setup parameters or edit the language, time zone, and NFS4 Domain values for your environment. Enter the root password and confirm the password. Click **Next** to specify the user account for Oracle Solaris 11 OS.
10. Root login is not enabled in Oracle Solaris 11 OS. Create a user account to SSH to the OS after provisioning. Provide a user name and password for the account.
11. Click **Next** to specify whether you want to use iSCSI disks for provisioning Oracle VM Server for SPARC.
12. Do not select the option to use iSCSI disk as this scenario does not involve the use of iSCSI disk for provisioning Oracle VM Server for SPARC. Click **Next** to specify the file system layout.
13. Retain the default values for the root (/) and swap file systems. You have the options to change the swap size and add more ZFS file systems.
14. Click **Next** to specify the name service.
15. If you have a naming service in place, select the appropriate one and provide the setup details.
16. Click **Next** to view the summary of the parameters selected for the profile.
17. Review the parameters selected for the profile and click **Finish** to create the OS provisioning profile.

Provisioning Linux

You can create OS Provisioning and OS Configuration profiles for provisioning Linux OS on x86 systems. The profiles collect all the information such as type of target, OS image, time zone and language setup disk partitions, naming services and network details.

Provisioning Oracle Linux and other supported versions of Linux is very similar to provisioning Oracle Solaris 10 x86. You add the Linux image, create the OS Provisioning and OS Configuration profiles, create a Provision OS deployment plan, then apply the plan to provision the operating system.

The OS Provisioning plan will use Kickstart as the install mechanism to perform the installation. You do not need to do anything to enable Kickstart.

Provisioning 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 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.

Note:

When you specify the naming service in the OS Provisioning profile, each IP address in the Name Server field must be entered in a new row. IP addresses 0.0.0.0 or 255.255.255.255 are allowed. In the Domain Name Search List field, enter each domain name, such as 1domain.com and 2domain.com, on a new line.

Perform the following before you provision the operating system:

- Import the OS image. 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 an OS Configuration 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.

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.

Provisioning Linux

Procedure to provision Linux operating system.

1. Verify that the Linux image you want to use is available in the library, or import the Linux image.
2. Create an OS Provisioning profile and an OS Configuration profile using Linux as the Target Type. Configure the profiles with the parameters you want to use.
3. Create a Provision OS deployment plan or other deployment plan that enables OS provisioning.
4. Discover the service processors of the target systems.
5. Place the asset in Maintenance Mode to prevent events related to a system going offline.
6. Select the deployment plan and click **Apply Plan** to define the targets for the plan. Make any last minute changes in the plan, then submit the job.
7. When the job completes and the new operating system is provisioned, take the asset out of Maintenance Mode.

Specifying Common Linux Parameters

You can specify 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 (-).

Specifying SuSE Parameters

Specify parameters to create a profile that installs the SuSE Linux OS.

- **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 (-).

Related Resources for Operating System Provisioning

This section lists the related resources for OS provisioning.

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

- For more information, see the Oracle Enterprise Manager Ops Center Documentation Library at http://docs.oracle.com/cd/E59957_01/index.htm.
- For current discussions, see the product blog at <https://blogs.oracle.com/opscenter>.
- For end-to-end examples, see the workflows and how to documentation in the library. For deployment tasks, go to http://docs.oracle.com/cd/E59957_01/nav/deploy.htm, for operate tasks go to http://docs.oracle.com/cd/E59957_01/nav/operate.htm, and for administer tasks go to http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- See *Monitoring Rules and Policies* for more information on how monitoring rules and policies work in the software.
- 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 *Oracle VM Server for SPARC* for the requirements and information needed to provision Oracle VM Server for SPARC and domains
- See *Oracle VM Server for X86* for the requirements and information needed to provision Oracle VM Server for SPARC and domains.
- See *Oracle Solaris Zones* for how to use Oracle Enterprise Manager Ops Center to install and upgrade Oracle Solaris Clusters.
- See [Introduction to Operating System Management](#) and [Introduction to Operating System Updates](#) for information about managing, patching, or updating, your operating systems.
- See [Introduction to Managing Hardware Assets](#) for information about provisioning firmware.

For more information about how to set up and manage the Enterprise Manager Ops Center infrastructure, including DHCP and WAN boot, see the *Oracle Enterprise Manager Ops Center Administration Guide*.

For in-depth information about Oracle Linux, Oracle Solaris, DHCP, WAN boot, and related features, see the following Oracle documentation:

- For a list of the Oracle Linux documentation available in HTML and PDF formats, visit the Oracle Linux Documentation at <http://www.oracle.com/us/technologies/linux/index.html>.
- For a list of the Oracle Solaris 11 and 11.1 documentation available in HTML and PDF formats, visit the Oracle Solaris 11 Documentation at <http://www.oracle.com/technetwork/documentation/solaris-11-192991.html>.
- For a list of the Oracle Solaris 10 documentation available in HTML and PDF formats, visit the Oracle Solaris 10 Documentation at <http://www.oracle.com/technetwork/documentation/solaris-10-192992.html>.
- For a list of the Oracle Solaris 8 and 9 documentation, visit the Legacy Solaris Documentation 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>.
- For JET documentation and to download additional modules, see <http://www.oracle.com/technetwork/systems/jet-toolkit/index.html>.

Update Operating Systems

This section 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](#)
- [Location of Operating System Updates in the User Interface](#)
- [Using System Catalogs](#)
- [About Operating System Update Reports](#)
- [Creating Update Policies](#)
- [Creating Update Profiles](#)
- [Updating Oracle Solaris 8, 9, and 10 and Linux Operating Systems](#)
- [Updating Oracle Solaris 11 Operating Systems](#)
- [Updating an Oracle Solaris Boot Environment](#)
- [Updating Microsoft Windows Operating Systems](#)
- [Related Resources for Operating System Updates](#)

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.

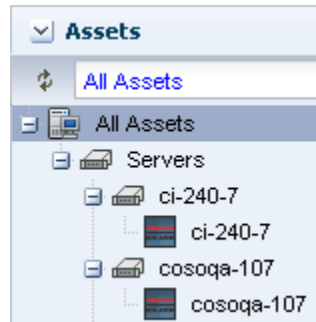
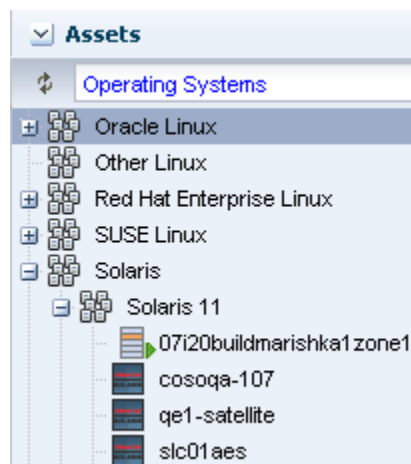
You create update jobs with operating system update profiles and policies to update an operating system. OS update profiles and policies define which updates to install, and how the update job proceeds after determining the update dependencies and user interaction. A set of system-defined update profiles is available in the UI. You can copy the profiles and edit them to create your own customized profiles.

When you run an OS Update job, Oracle Enterprise Manager Ops Center performs the following actions:

1. Locks the asset.
2. Creates a snapshot for Oracle Solaris 8-10 and Linux operating systems.
3. Queues the job on the Enterprise Controller for the associated Proxy Controller. The Agent Controller retrieves the job and performs the tasks on the asset.
4. Saves the job log on the Enterprise Controller.
5. Unlocks the asset.

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 8-1](#) and [Figure 8-2](#).

Figure 8-1 All Assets View**Figure 8-2 Operating Systems View**

Requirements for Updating Operating Systems

The Enterprise Controller obtains information about latest updates from the Knowledge Base, Oracle Solaris 11 parent repositories on Oracle.com, and vendor sites. You must have 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.
- **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.
- **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 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.

Methods of Running an Update Job

You can use different methods to run and update a job.

- Deployment plans that use the update profiles and policies. A deployment plan defines the profiles used, in some cases the plans used, and the sequence of operations (or steps). The following deployment plans include update: Install Server, Software Deployment/Update, and Update Solaris 11 OS.
- System catalogs for Oracle Solaris 8 - 10 and Linux.
- Reports.
- Update profiles.

Options Available When Running an Update Job

Lists the 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

Lists the OS management roles and permissions.

[Table 8-1](#) 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.

Contact your administrator if you do not have the necessary role or privilege to complete a task. See the for information about the different roles and the permissions they grant.

Table 8-1 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
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

Lists the actions for operating system updates.

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.

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.

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

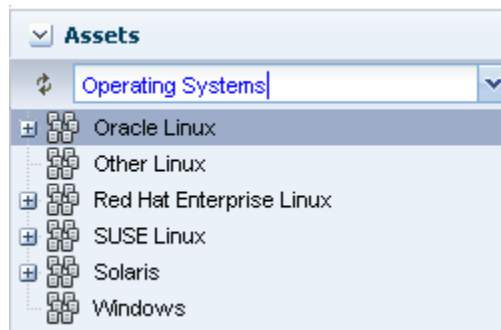
- Provision Oracle Solaris and Linux operating systems
- Manage Oracle Solaris boot environments
- Create a System Catalog
- Create an OS Report
- Update Oracle Solaris and Linux operating systems
- Update Microsoft Windows operating systems

Location of Operating System Updates 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 8-3](#).

Figure 8-3 Operating System Filter



Using System Catalogs

A system catalog is a software inventory of installed instances and versions of Oracle Solaris 8 - 10 OS updates, Linux RPMs, and local software.

Oracle Enterprise Manager Ops Center automatically takes a snapshot of the operating system after executing any job on the OS, including when you discover and manage the operating system, start the Agent Controller, and when you update the operating system. A snapshot is stored on the Enterprise Controller as a catalog with the time stamp and job details after every update job that you run on a system.

Note:

Oracle Solaris 11 operating systems do not have or use snapshots. or system catalogs. Instead, the Oracle Solaris 11 operating system manages the OS packages.

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.

Viewing and Modifying 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.

Comparing 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 are 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.

About Operating System Update Reports

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.

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.

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.

Creating 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:

By default, all operating system update plans use the **yes to all** policy.

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 8-4](#).

Figure 8-4 OS Update Policies and User Defined Policy Details

The screenshot displays the 'OS Update Policies' interface. At the top, there is a search bar and a list of policies. The '121288 Update Policy' is highlighted, showing its description and that it is user-defined. Below this, the 'User-defined Policy Detail' section is shown, including a 'Reboot Policy' and a table of exceptions.

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

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.

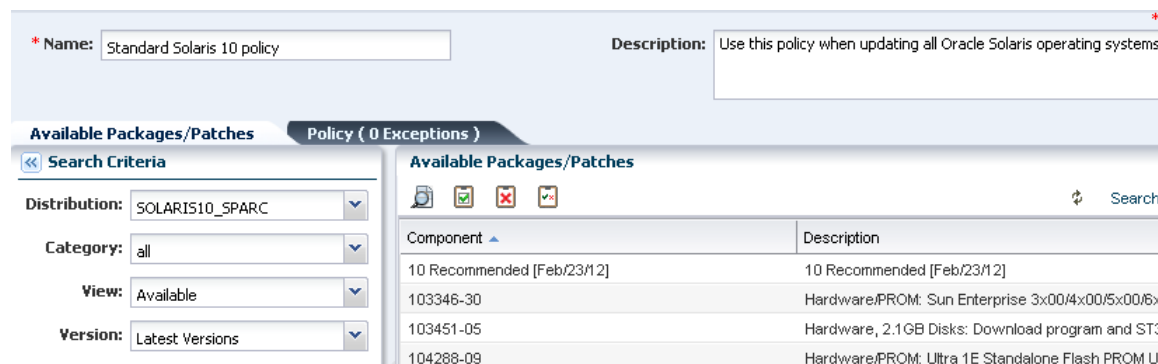
The update policy is not applicable when updating Microsoft Windows operating systems.

Creating a User-defined Policy

Procedure to 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:** View all, available, withdrawn, modified packages/updates, or reboot
 - **Version:** View All Versions or filter for the Latest Versions

Figure 8-5 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**.
6. (Optional) To view details of the component, click the **View** icon.
7. Click **Create OS Update Policy**.

Creating 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 identify the profile type when you create the profile. The profile type is a tag that filters the required profiles when you create a deployment plan.

The following are profile types:

- **Install:** Indicates that new components are added, or installed. Use the Install profile type for Oracle Solaris operating system updates, baselines, and patchclusters.
- **Upgrade:** Indicates that existing components are upgraded.
- **Script:** Indicates that action scripts are executed.

Note:

You can create profiles that perform all of the actions for the profile type. The profile tag filters the required profiles in deployment plans.

Creating a New Profile

Procedure 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. Enter a name and description for the profile.
 - b. Select a Profile Type tag, either **Upgrade**, **Install**, or **Script**, to categorize and filter the profiles later.
 - c. Select a distribution from the drop-down list. For example, SOLARIS10_SPARC.

- d. (Optional) You can further define the criteria by choosing a category, view, and version from the drop-down list.

Figure 8-6 OS Update Profile Search Criteria

Figure 8-7 Create an OS Update Profile

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. Click **Save as Named Profile**. When an existing profile has the same name, you are asked to confirm that you want to replace the profile.

Note:

You cannot replace system-defined profiles.

Updating Oracle Solaris 11 Operating Systems

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.

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.

Updating Oracle Solaris 11 Operating System

Procedure 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.

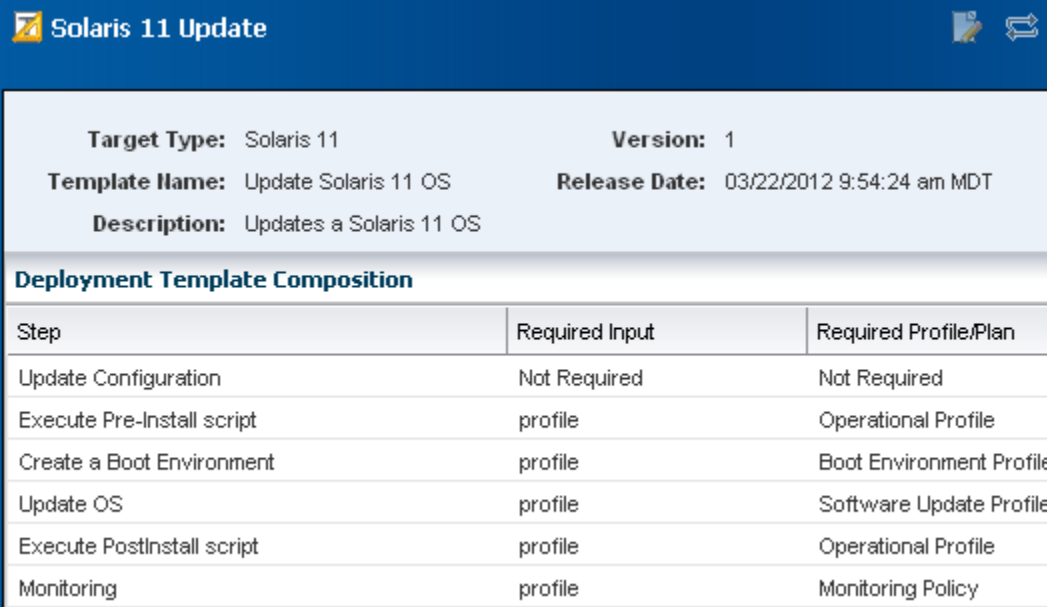
All update plans use the **yes to all** policy by default. If you do not want to automate the update by answering yes to all questions, you can create one or more customized update policies.

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.

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 8-8 Oracle Solaris 11 Deployment Template



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:** A profile is not 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.

Updating Oracle Solaris 8, 9, and 10 and Linux Operating Systems

Lists the update methods and options to update these operating systems.

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 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 8-2 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
Modify or compare a System Catalog	Yes	Yes
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.

About Operating System Update Jobs

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.

Updating 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.

Updating Oracle Solaris or Linux Operating System

Procedure 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 are constrained by the target systems to which the plan is applied. All update plans use "yes to all" policy.

Updating 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

Updating an Operating System 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. The report 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 [Create 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 New Update OS 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 does 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 to `/etc/release` to specify that the update bundle is applied.

Using 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 and 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.

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.

Updating an Oracle Solaris Boot Environment

You always need an update profile to update an Oracle Solaris Boot environment. You can use the update profile in an update deployment plan or the Update Job Wizard.

You can update an alternate boot environment as part of a Software Deployment / Update deployment plan by selecting the alternate boot environment as the target. See the *Oracle Enterprise Manager Ops Center Updating Your Oracle Solaris 10 Operating System* for an example of how to use this plan.

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: Whether to use an 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.

Updating a Boot Environment

Procedure 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, select the Download check box.
 - Actual Run. Updates the operating system.
 - 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
 - Select 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 create the script and upload it to the library before you can use this option.

5. Define the profile, policy and target for each task, or edit the profile and policy.
6. (Optional) 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. (Optional) To add a new task, click the **Add (+)** icon.
 - A second row appears. 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.
 - When 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 the option 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 synchronize 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.

Updating Microsoft Windows Operating Systems

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 website through the Internet and downloads the metadata that is used for compliance analysis. You can connect Oracle Enterprise Manager Ops Center to the Microsoft website to download updates that are then handled by SCCM for installation.

You do not need any authentication to access the Microsoft website. However, you must provide authentication information to access the SCCM server.

About Windows OS Update Jobs

Oracle Enterprise Manager Ops Center contains groups, roles, and reports 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 DCOM wire protocol (MSRPC) 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.

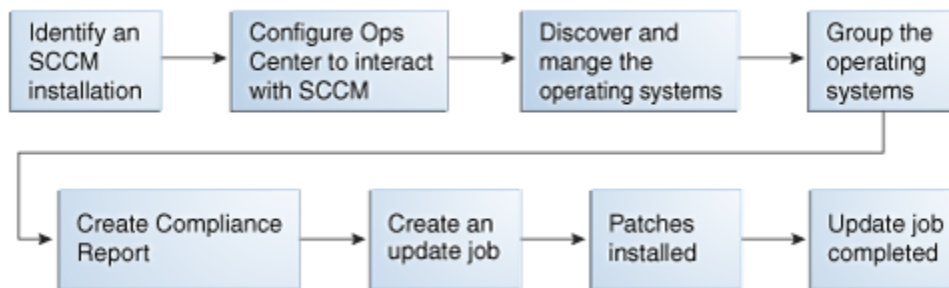
Note:

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.

Creating 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 8-9 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 Operating System Updates

This section lists the related resources for OS updates.

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

- For more information, see the Oracle Enterprise Manager Ops Center Documentation Library at http://docs.oracle.com/cd/E59957_01/index.htm.
- For end-to-end examples, see the workflows and how to documentation in the library. For deployment tasks, go to http://docs.oracle.com/cd/E59957_01/nav/deploy.htm, for operate tasks go to http://docs.oracle.com/cd/E59957_01/nav/operate.htm, and for administer tasks go to http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- See *Software Libraries* chapter for how to add and update operating system packages and images.
- See *Introduction to Operating System Management* for details on managing 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.

For in-depth information about these products, see the following Oracle documentation:

- For a list of the Oracle Linux documentation available in HTML and PDF formats, visit the Oracle Linux Documentation website 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
- Oracle Solaris 11 Information Library at http://docs.oracle.com/cd/E23824_01/index.html
- For a list of the Oracle Solaris 10 documentation available in HTML and PDF formats, visit the Oracle Solaris 10 Documentation website at <http://www.oracle.com/technetwork/documentation/solaris-10-192992.html>.
- For a list of the Oracle Solaris 8 and 9 documentation, visit the Legacy Solaris Documentation website at <http://www.oracle.com/technetwork/documentation/legacy-solaris-192993.html>.

Logs and Directories

Oracle Enterprise Manager Ops Center performs each action as a job. The details of a job show the order of tasks in the job and the managed assets that are 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. See **Viewing Jobs** for instructions.

In addition to the job, log files record events of different types and for different purposes. Some log files are protected by file permissions and require a user with root access to view them. Some log files can be displayed in the product's browser interface, using the following procedure:

1. Click the Enterprise Controller in the **Administration** section of the Navigation pane.
2. Click the **Logs** tab in the center pane.
3. Select a log from the drop-down list:
 - cacao log
 - UI log
 - Proxy log
 - Update error log
 - Update channel download log
 - Update channel error log
4. (Optional) Click **Refresh Log File** to update the display.

Installation

- Log of the most recent installation or uninstallation: `/var/tmp/opscenter/installer.log.latest/var/tmp/installer.log.latest`
- Log of previous installation or uninstallation operations: `/var/tmp/opscenter/installer.log./var/tmp/installer.log.xxxx`
- Log of a specific installation:
`/var/opt/sun/xvm/oracle/app/oraInventory/logs/silentInstall<yyyy-mm-dd-hh-mm-sspm>.log`
- Log of an agent installation: `/var/scn/install/log`

Upgrades

The log of upgrade actions are in these files:

- Enterprise Controller: `/var/opt/sun/xvm/update-saved-state/update_EC_minor_bundle_12.2.n.xxx/updateslog.txt`
- Co-located Proxy Controller: `/var/opt/sun/xvm/update-saved-state/update_PC_minor_bundle_12.2.n.xxx/updateslog.txt`
- Remote Proxy Controller: `/var/scn/update-saved-state/update_proxy_bundle_12.2.n.xxx/updateslog.txt`

If an upgrade fails, the database rolls back and a log of database actions is stored in the following directory: `/var/opt/sun/xvm/update-saved-state/update_EC_minor_bundle_12.2.n.xxx/dblogs` directory.

Diagnosing Problems

The following log files contain detailed information about the same events as the audit log files except for login information. They include the interactions between components of the product software.

- On Oracle Solaris: `/var/cacao/instances/oem-ec/audits/`
- On Linux: `/var/opt/sun/cacao/instances/oem-ec/audits/`

The following log files are specialized for specific events:

- Messages from operating system such as Info and Warning: `/var/adm/messages*`
- Login and connection information: `/var/opt/sun/xvm/logs/audit-logs*`
- Events in the user interface component: `/var/opt/sun/xvm/logs/emoc.log`
- Events between controllers and agents:
 - 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`
 - On each Oracle Solaris agent: `/var/cacao/instances/scn-agent/logs/cacao.n`
 - On each Oracle Linux agent: `/var/opt/sun/cacao/instances/scn-agent/logs/cacao.n`

High Availability

In a High Availability configuration, each Enterprise Controller is a Clusterware node. The Clusterware resource activity is logged 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 Update Component

The Software Update component has its own server. The following files record 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`
 - 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

- Agent log:
 - On Oracle Solaris: `/var/cacao/instances/scn-agent/logs/cacao.n`
 - On Oracle Linux: `/var/opt/sun/cacao/instances/scn-agent/logs/cacao.n`
- Agent update log files: `/var/scn/update-agent/logs` directory after an update
- Other agent log: `/var/opt/sun/xvm/logs`

Local Database

- On the Enterprise Controller:
 - For installation events:

```
/var/opt/sun/xvm/oracle/cfgtoollogs/dbca/OCDB/*  
/var/tmp/opscenter/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/opt/sun/xvm/logs/sat-backup-date-time.log  
/var/opt/sun/xvm/logs/sat-restore-date-time.log  
/var/opt/sun/xvm/logs/migrate.log
```

- For data files: `/var/opt/sun/xvm/oracle/oradata/OCDB`

- For redo log files: `/var/opt/sun/xvm/oracle/oradata/OCDB`

If you used OCDoctor to prepare a zpool directory with Oracle OS user permission, the log files are in: `/var/opt/sun/xvm/oracle/oradata/OCDB/REDO/`

- On the Proxy Controller: `/var/opt/sun/xvm/proxydb/*`
- On each agent: `/var/opt/sun/xvm/agentdb/*`

Controlling 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. Any event above the level of INFO is also logged in the `syslog`. You can view the contents of the current log file using the UI or by viewing the contents of the following files:

- 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`

- On each Oracle Solaris agent: `/var/cacao/instances/scn-agent/logs/cacao.n`
- On each Oracle Linux agent: `/var/opt/sun/cacao/instances/scn-agent/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 that are retained, 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 view the number of log files maintained for an agent use the following command on the system where the agent is running:

```
# cacaoadm get-param log-file-count -i scn-agent
log-file-count=3
```

To Change the Number of Log Files for an Enterprise Controller or Proxy Controller

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
```
3. 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
```
4. 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
```

5. Start the Enterprise Controller.

- On Oracle Solaris:

```
# /opt/SUNWxvmoc/bin/satadm start -w -v
```

- On Linux:

```
# /opt/sun/xvmoc/bin/satadm start -w -v
```

6. 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
```

7. Verify that all controllers have restarted completely before attempting other operations.

To Change the Number of Log Files for an Agent

To change the number of log files on an agent:

1. Verify that there are no active jobs.

2. Stop the Common Agent Container service on a the agent:

- On Oracle Solaris:

```
# /opt/SUNWxvmoc/bin/agentadm stop -v
```

- On Linux:

```
# /opt/sun/xvmoc/bin/agentadm stop -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.

```
# cacaoadm set-param log-file-count=10 -i scn-agent
```

4. Start the agent:

- On Oracle Solaris:

```
# /opt/SUNWxvmoc/bin/agentadm start -v
```

- On Linux:

```
# /opt/sun/xvmoc/bin/agentadm start -v
```

5. Verify that all controllers have restarted completely before attempting other operations.

JumpStart Enterprise Toolkit

Use JumpStart Enterprise Toolkit (JET) to extend the JumpStart installation functionality provided within the Oracle Solaris 9 and 10 operating systems.

JET is a framework designed to simplify and extend the JumpStart installation capabilities for provisioning the Oracle Solaris 9 or 10 operating system. JET provides a set of helper scripts to simplify the use of Jumpstart for the installation of Solaris 10 and earlier on both SPARC and x86 servers. Oracle Solaris 11 does not use JET, instead, it uses the automated installer (AI).

The SUNWjet and JetFLASH packages are installed on the Proxy Controller during installation. See the JET page on the Oracle Technology Network at <http://www.oracle.com/technetwork/systems/jet-toolkit/jet-toolkit-1614844.html> for more information on JET, including additional packages available for download and a link to the user documentation.

Note:

JET must run on a Proxy Controller that is running on an Oracle Solaris 9 or 10 operating system.

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

The main JET framework is supplied in a single SVR4 package called SUNWjet. This package contains everything necessary to do a standard Oracle Solaris installation using either bootp or dhcp.

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 Oracle 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 targetable component.
Default Value: `[targetableComponent:kernel_arch]`
- `base_config_ClientEther`: Ethernet MAC address. By default, this is set to the Ethernet MAC address of the targetable component.
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 Oracle 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, host name2, 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 `cntndn`. 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 has 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 after 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 a 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 Oracle 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`: Oracle Solaris software group package.
 - Default Value: `SUNWCreq`
 - Example:
`SUNWCreqSUNWCuserSUNWCprogSUNWCallSUNWCXallSUNWCrnet`
- `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.

Default Value: /opt

Note:

If you are using Oracle 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.

- `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 `ctndn` or the keyword `rootdisk`. If the value is `rootdisk`, then the current boot disk is 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, JumpStart uses value from the `defaultrouter_base_config` variable. If that is also blank, or for another net interface, JumpStart `sysidcfg` gets 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: `n_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 Oracle 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`. Oracle 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`.
Default Value: `all`

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.

- `base_config_update_terminal`: If set, put the `sysidcfg` terminal type into `inittab`.
Default Value: `yes`
- `base_config_x86_confflags`: For Oracle 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 Oracle Solaris x86 systems, disables the `kdmconfig` interactive utility for configuring the keyboard, display,

and mouse of the target host. If you are installing an Oracle Solaris OS with the GRUB bootloader, set this variable value to `yes`.

- `base_config_x86_nowin`: For x86 systems, prevents Oracle 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 attempts to boot from disk, you must set this option to `yes`.

Downloading Additional JET Packages

Additional JET packages are available. To download JET packages and the JET user guide, go to <http://www.oracle.com/technetwork/systems/jet-toolkit/index.html>.

Library Incidents

Oracle Enterprise Manager Ops Center relies on the `library.xml` file to manage and maintain the libraries that are backed by NFS shares. This file can be affected by operations that result in an incident being reported.

UUID is not recognized

Incident: `library.xml` file was deleted. Please try to recover with uuid *<identifier>*

Cause: The `library.xml` file contains the original UUID for the library. Because the library was deleted and created again, the library has a new UUID.

Action: Update the `library.xml` file with the new UUID.

1. Edit the `library.xml` file.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<LibraryData>
  <IsReadOnly>>false</IsReadOnly>
  <UserFriendlyName>Local Storage Library (xvmsrv-005)</UserFriendlyName>
  <Description>Default virtual image local library</Description>
  <CreationTime>1382430667160</CreationTime>
  <ModificationTime>1382430667160</ModificationTime>
  <SemanticTags/>
  <UUID>d46372fa-1f39-4152-b082-7e501fda459d</UUID>
</LibraryData>
```

2. Change the UUID to the UUID displayed in the incident.
3. Save and close the file.
4. Run the OCDoctor utility to verify the `library.xml` file is in the correct state:

```
/var/opt/sun/xvm/OCDoctor/toolbox/library-check.sh
```

5. If the OCDoctor output indicates a problem with the library, use the following command to associate the new UUID with the library's location:

```
/var/opt/sun/xvm/OCDoctor/toolbox/library-check.sh -f <path/to/library>
```

Image information is missing

Incident: `library.xml` is missing some images. Number of images in the xml is *n*. Number of images in the directory is *x*.

Cause: Image files have been moved into the NFS share location but Oracle Enterprise Manager Ops Center does not manage them.

Action: Do the following

1. Run the OCDoctor utility to verify that images are missing:
`/var/opt/sun/xvm/OCDoctor/toolbox/library-check.sh`
2. Verify there is no current jobs that modify the library, such as actions that create a guest or add storage.
3. Use the OCDoctor utility to restore the library's images:
`/var/opt/sun/xvm/OCDoctor/toolbox/library-check.sh -f <path/to/library>`
4. Save and close the file.
5. Run the OCDoctor utility to verify the `library.xml` file is in the correct state:
`/var/opt/sun/xvm/OCDoctor/toolbox/library-check.sh`

File is not readable

Incident: library.xml is corrupted.

Cause: Oracle Enterprise Manager Ops Center cannot open the file.

Action: Create a new `library.xml` file:

1. Open a file with the name `library.xml`.
2. Enter the following contents, using the format in the example:
 - `isReadOnly = false`
 - Description is empty. You can add or change using the Edit Attributes action.
 - `CreationTime` is the current time in EPOC time
 - `ModificationTime` is the current time in EPOC time
 - `SemanticTags` is empty.
 - `UUID` is the `UUID` displayed in the Incident Details message.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<LibraryData>
  <IsReadOnly>>false</IsReadOnly>
  <UserFriendlyName>Local Storage Library (xvmsrv-005)</UserFriendlyName>
  <Description>Default virtual image local library</Description>
  <CreationTime>1382430667160</CreationTime>
  <ModificationTime>1382430667160</ModificationTime>
  <SemanticTags/>
  <UUID>d46372fa-1f39-4152-b082-7e501fda459d</UUID>
</LibraryData>
```

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. Account defines the amount of vCPU, memory and storage resources that can be used from the available vDC resources.

actions 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.

audit log

An audit log file stores details about user log ins, changes to user accounts, and job details. It shows the activity on the Enterprise Controller and the Proxy Controller.

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.

See also [white list](#).

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. Zones 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. Deployment plans also include 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.

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. Enterprise Controller stores management information, such as firmware and operating system images, plans, profiles, and policies and 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.

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.

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.

Guest Domain

A guest domain is a non-I/O domain that consumes virtual device services that are provided by one or more service domains. A guest domain does not have any physical I/O devices, but only has virtual I/O devices, such as virtual disks and virtual network interfaces.

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 has additional paravirtualized drivers for improved performance of the virtual machine. PVHVM improves the performance level of Microsoft Windows running in guests.

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.

I/O Domain

An I/O domain has direct access to a physical I/O device, such as a network card in a PCI EXPRESS (PCIe) controller. An I/O domain can own a PCIe root complex, or it can own a PCIe slot or on-board PCIe device by using the direct I/O (DIO) feature. An I/O domain can share physical I/O devices with other domains in the form of virtual devices when the I/O domain is also used as a service domain.

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. Knowledge base stores information about patch dependencies, patch compatibilities, withdrawn patches, downloads, and deployment rules and also 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.

maintenance mode

Disables incidents from displaying in the UI, but does not disable monitoring. This mode is useful when you do not want incidents generated during system maintenance.

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. Message Center 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. navigation pane 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. Oracle Engineered System 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. Oracle Solaris Clusters are used to improve the availability of software services such as databases, file sharing on a network, electronic commerce websites, 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. This 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. This 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.

OS Provisioning Profile

Defines the image, provisioning, and installation requirements.

OS Configuration Profile

Defines the OS and network configuration.

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 Domain

A root domain has a PCIe root complex assigned to it. This domain owns the PCIe fabric and provides all fabric-related services, such as fabric error handling. A root domain is also an I/O domain, as it owns and has direct access to physical I/O devices.

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 so that your trusted computers can get access to 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.

Service Domain

A service domain provides virtual device services to other domains, such as a virtual switch, a virtual console concentrator, and a virtual disk server. You can have more than one service domain, and any domain can be configured as a service domain.

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.

shared storage

A shared storage library in Oracle Enterprise Manager Ops Center is one that is accessible by the server and operating system. It is not related to Zones on Shared Storage in Oracle Solaris 11.1.

snapshot

Snapshot, a point in time image of a volume 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.

Support Repository Update (SRU)

Support Repository Update (SRU) is a package of Oracle Solaris 11 operating system updates that releases on a regular basis.

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. This offers an access point through which you can allocate and control the resources inside. This is created during the set up phase.

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. This consumes CPU and memory resources. This 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.

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.

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.

See also [black list](#).

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. WS - Man 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, [6-27](#)
Acknowledge Incident, [3-7](#), [3-8](#), [3-15](#)
Acting on an incident, [3-17](#)
activate, [6-48](#)
Add Annotation to Incident, [3-7](#), [3-8](#)
Agent Controllers
 log file, [A-3](#)
 operating systems, [6-9](#)
Agent-managed operating systems
 changing mode, [6-11](#)
 updating, [8-3](#)
Agentless-managed operating systems
 changing mode, [6-11](#)
Alerts
 clearing, [3-5](#)
 disabling and enabling, [3-20](#)
All Unassigned Incidents, [3-7](#)
Analytics
 operating systems, [6-14–6-19](#), [6-21](#), [6-22](#), [6-26](#),
 [6-27](#)
Annotations
 Automated Operation, [3-12](#)
 Comment, [3-12](#)
 deleting, [3-12](#)
 incident, [3-11](#), [3-16](#)
 Suggested Action, [3-12](#)
 viewing, [3-11](#), [3-16](#)
Asset management
 incidents, [3-11](#)
 Oracle Services, [3-22](#)
Assign Incident, [3-7](#), [3-8](#), [3-14](#)
Automated Operation, [3-12](#)

B

Badges
 incident severity, [3-10](#)
Baseline Analysis Report
 black list, [4-12](#)
 white list, [4-12](#)
beadm, [6-28](#)

Black list, [4-12](#), [4-15](#)
Boot environments
 activating, [6-30](#), [6-31](#)
 active, [6-27](#)
 alternate, [6-27](#), [6-42](#)
 deleting, [6-31](#)
 dual, [6-27](#)
 incidents, [6-29](#)
 Live Upgrade, [6-41](#)
 monitoring, [6-28](#)
 Oracle Solaris 10, [6-28](#), [6-38](#), [6-47](#), [6-48](#)
 Oracle Solaris 10-8, [6-37](#), [6-39](#), [6-40](#), [6-42–6-46](#)
 Oracle Solaris 11, [6-28](#), [6-32–6-36](#)
 policy, [6-41](#)
 profiles, [6-41](#)
 requirements, [6-41](#)
 update profile, [8-17](#)
 updating operating systems, [8-17](#)
 viewing, [6-29](#)
Boot interface, [7-48](#)

C

Change History Report, [4-9](#)
Charts
 creating, [6-25](#)
 operating systems, [6-19](#), [6-25](#)
Close Incident, [3-7](#), [3-8](#)
Closing an incident, [3-18](#), [3-19](#)
Cloud Admin
 prerequisites, [2-1](#)
Cloud User
 prerequisites, [2-1](#)
Comment, [3-12](#), [3-17](#)
Compare Catalogs, [8-7](#)
Connectivity check interval, [1-7](#)
Console timeout, [1-7](#)
Contracts, [3-21–3-23](#)
Critical, [3-12](#)
CSV reports, [4-3](#)

D

Database
 log file, [A-3](#)
Deleting annotations, [3-12](#)
Deployment plans
 boot environments, [6-43](#)
 Linux, [7-27](#), [7-43](#), [7-48](#)
 operating systems, [7-27](#), [7-43](#), [7-48](#)
 Oracle Solaris 11, [7-27](#)
 updating operating systems, [8-15](#)
 updating Oracle Solaris 11, [8-12](#)
DHCP, [7-12](#)
Disable Multiple Sessions, [1-6](#)
Distribution Update Report, [4-32](#)
Dynamic Host Configuration Protocol (DHCP), [7-43](#),
 [7-48](#)

E

Engineered System Report, [4-26](#)

F

File systems
 boot environments, [6-34](#), [6-40](#)
Firmware Compliance Report, [4-30](#), [5-30](#)
Formatting reports, [4-3](#)

G

Generate Report, [4-6](#)

H

Host Compliance Report, [4-22](#), [4-23](#)

I

Icons
 Acknowledge Incident, [3-7](#), [3-8](#)
 Add Annotation to Incident, [3-7](#), [3-8](#)
 annotation, [3-11](#)
 Assign Incident, [3-7](#), [3-8](#)
 Close Incident, [3-7](#), [3-8](#)
 Edit View, [4-6](#)
 Generate Report, [4-6](#)
 Mark Incident as Repaired, [3-7](#), [3-8](#)
 Open Service Request, [3-8](#)
 Take Action on Incident, [3-7](#), [3-8](#)
 URL, [3-7](#)
 View Alerts, [3-7](#), [3-8](#)
 View Annotations, [3-7](#), [3-8](#)
 View Comments, [3-7](#), [3-8](#)
 View Possible Impacts and Causes, [3-7](#), [3-8](#)
 View Suggested Actions, [3-7](#), [3-8](#)

Icons (*continued*)
 wrench, [6-24](#)
Image Packaging System, [7-15](#)
Images, [C-1](#)
Incident Compliance Report, [4-19](#), [4-21](#)
Incident Detail Report, [4-28](#)
Incident Severity Badges
 Asset icon, [3-10](#)
Incident Summary Report, [4-28](#)
Incidents
 Acknowledge Incident, [3-7](#)
 acknowledging, [3-15](#)
 acting, [3-17](#)
 Add Annotation to Incident, [3-7](#)
 alerts, [3-5](#)
 annotating, [3-16](#)
 annotations, [3-11](#)
 Assign Incident, [3-7](#)
 Assigned to Others, [3-6](#)
 assigning, [3-14](#)
 boot environments, [6-29](#)
 Close Incident, [3-7](#)
 closing, [3-18](#), [3-19](#)
 comments, [3-17](#)
 Critical, [3-12](#)
 details, [3-3](#), [3-14](#)
 disabling, [3-19](#)
 icons, [3-4](#)
 ID, [3-7](#)
 Informational, [3-12](#)
 Mark Incident as Repaired, [3-7](#)
 Message Center, [3-5](#)
 monitoring rules, [3-12](#)
 My Incidents, [3-6](#)
 My Service Requests, [3-6](#)
 Notifications, [3-6](#)
 Open Service Requests, [3-6](#)
 Relayed, [3-6](#)
 Relayed Service Requests, [3-6](#)
 repaired, [3-18](#)
 roles, [3-2](#)
 Service Requests Opened by Others, [3-6](#)
 Take Action on Incident, [3-7](#)
 unassigned, [3-6](#)
 unresolved, [3-14](#)
 View Alerts, [3-7](#)
 View Annotations, [3-7](#)
 View Comments, [3-7](#)
 View Possible Impacts and Causes, [3-7](#)
 View Suggested Actions, [3-7](#)
 viewing annotations, [3-16](#)
 Warning, [3-12](#)
Incidents Assigned to Others, [3-6](#)
Incidents Knowledge Base, [3-12](#), [3-13](#)
Incidents tab, [3-13](#)
Informational, [3-12](#)

Installing operating system

See Provisioning, [7-1](#)

Interactive reports, [4-3](#)

IPMP

Oracle VM Server for SPARC, [7-23](#)

IPMP groups

Oracle VM Server for SPARC, [7-16](#)

IPS, [7-15](#)

J

JET

See JumpStart Enterprise Toolkit, [7-44](#)

JetFLASH, [7-44](#)

Job status popup duration, [1-7](#)

Jobs

Update Microsoft Windows, [8-20](#)

updating operating systems, [8-14](#)

JumpStart Enterprise Toolkit

location, [B-1](#)

parameters, [B-1](#)

templates, [7-45](#)

L

Library incidents, [C-1](#)

library.xml, [C-1](#)

Linux

Boot environments

updating operating systems, [8-13](#)

Live Upgrade

updating operating systems, [8-13](#)

Operating systems

updates, [8-13](#)

provisioning parameters, [7-50](#)

update policies, [8-8](#)

update profiles, [8-9](#)

updates

requirements, [8-3](#)

Linux See operating systems, [8-1](#)

Linux SuSE

provisioning parameters, [7-50](#)

Live Upgrade

synchronize, [6-47](#)

updated operating systems, [6-46](#)

updating operating systems, [6-45](#)

Log files, [A-1](#)

Logs

cacao, [A-4](#)

installation, [A-1](#)

upgrades, [A-2](#)

lucreate, [6-28](#), [6-40](#)

M

Maintenance mode

disabling incidents, [3-19](#)

Manual Net Boot, [7-44](#)

Mark Incident as Repaired

Repaired incidents, [3-18](#)

Membership graph

preferences, [1-6](#)

Membership Graph, [1-6](#)

Message Center

annotations, [3-11](#)

incidents, [3-5](#)

My Incidents, [3-8](#)

Notifications, [3-8](#)

Microsoft System Center Configuration Manager, [8-20](#)

Microsoft Windows

registry, [8-21](#)

update job, [8-22](#)

updates, [8-20](#), [8-21](#)

updating, [8-20](#)

Monitoring

boot environments, [6-28](#)

operating systems, [6-13](#), [6-19](#), [6-24](#)

Monitoring policies, [6-13](#)

Monitoring rules

incidents, [3-12](#)

My Incidents

Acknowledge Incident, [3-8](#)

Add Annotation to Incident, [3-8](#)

Assign Incident, [3-8](#)

Close Incident, [3-8](#)

Mark Incident as Repaired, [3-8](#)

new, [3-8](#)

Open Service Request, [3-8](#)

Take Action on Incident, [3-8](#)

unassigned, [3-8](#)

View Alerts, [3-8](#)

View Annotations, [3-8](#)

View Comments, [3-8](#)

View Possible Impacts and Causes, [3-8](#)

View Suggested Actions, [3-8](#)

My Oracle Support, [3-1](#)

My Service Requests, [3-6](#)

N

New Update OS Job, [8-14](#)

NFS shares, [C-1](#)

Notifications, [3-6](#), [3-8](#)

NVRAC, [7-19](#)

O

OCDoctor, [C-2](#)

Open Service Requests, [3-6](#), [3-8](#)

Operating system updates

roles, [8-4](#)

Operating systems

agent-managed

- Operating systems (*continued*)
 - agent-managed (*continued*)
 - changing mode, [6-11](#)
 - agentless-managed
 - changing mode, [6-11](#)
 - Analytics
 - charts, [6-19](#)
 - custom, [6-17](#), [6-27](#)
 - Summary, [6-16](#)
 - boot environments, [6-27–6-37](#), [6-39–6-46](#)
 - charts, [6-25](#)
 - CPU Utilization, [6-16](#)
 - deployment plans, [7-27](#), [7-43](#), [7-48](#)
 - History, [6-21](#)
 - Metrics, [6-22](#)
 - Microsoft Windows, [8-21](#), [8-22](#)
 - monitor thresholds, [6-19](#)
 - monitoring, [6-13](#)
 - parameters, [7-29](#), [7-44](#), [7-50](#)
 - Processes, [6-18](#)
 - profiles, [6-9](#), [7-20](#), [7-30](#), [7-43](#), [7-44](#), [7-48](#)
 - provisioning, [7-1](#)
 - Report Result, [8-16](#)
 - roles, [6-3](#), [7-5](#)
 - Services, [6-18](#)
 - status, [6-7](#)
 - system catalog, [8-6](#), [8-7](#)
 - threshold, [6-24](#)
 - update job, [8-14](#)
 - update policies, [8-8](#), [8-9](#)
 - update profiles, [8-9](#), [8-10](#)
 - updates
 - requirements, [8-3](#)
 - Virtualization Analytics, [6-26](#)
- Operational plans
 - boot environments, [6-44](#)
- Oracle 8,9,10, [7-43](#), [7-48](#)
- Oracle Services
 - contracts, [3-21–3-23](#)
 - requirements, [3-21](#)
 - service requests, [3-21](#), [3-23](#), [3-24](#)
 - warranty, [3-21](#), [3-22](#)
- Oracle Solaris
 - update policies, [8-8](#)
 - update profiles, [8-9](#)
 - updates, [8-3](#)
- Oracle Solaris 10
 - boot environments, [6-28](#), [6-38](#), [6-47](#), [6-48](#)
- Oracle Solaris 10-8
 - boot environments
 - profiles, [6-40](#)
- Oracle Solaris 11
 - boot environment, [8-17](#)
 - boot environments
 - file systems, [6-34](#)
 - profiles, [6-35](#), [6-36](#)
 - snapshots, [6-34](#), [6-36](#)

- Oracle Solaris 11 (*continued*)
 - boot environments (*continued*)
 - zones, [6-34](#)
 - parameters, [7-29](#)
 - provisioning parameters, [7-29](#)
 - provisioning profiles, [7-30](#)
 - updates, [8-12](#)
- Oracle Solaris 11 Software Update Library, [7-15](#), [8-12](#)
- Oracle Solaris 9 and 10
 - parameters, [7-44](#)
 - provisioning parameters, [7-44](#)
- Oracle Solaris See operating systems, [8-1](#)
- Oracle Solaris Update Compliance Report, [4-18](#), [8-16](#)
- Oracle Solaris Zones
 - boot environments, [6-34](#)
 - Live Upgrade, [6-38](#), [6-47](#), [6-48](#)
- Oracle VM Server for SPARC
 - IPMP, [7-16](#), [7-23](#)
- OS Update, [8-7](#)

P

- Package Compliance Report, [4-33](#)
- PDF reports, [4-3](#)
- Plan Management
 - Incident Knowledge Base, [3-11](#)
- Policies
 - boot environments, [6-41](#)
 - update, [8-8](#), [8-9](#)
- Profile Analysis Report
 - black list, [4-15](#)
 - white list, [4-15](#)
- Profiles
 - boot environments, [6-35](#), [6-36](#), [6-40](#), [6-41](#), [6-44](#), [6-45](#), [8-17](#)
 - operating systems, [6-9](#)
 - provisioning operating systems
 - boot interface, [7-48](#)
 - JumpStart Enterprise Toolkit, [7-44](#)
 - Linux, [7-50](#)
 - Linux SuSE parameters, [7-50](#)
 - Manual Net Boot, [7-44](#)
 - Oracle Solaris 11, [7-29](#)
 - Oracle Solaris 9 and 10, [7-44](#)
 - Oracle Solaris profiles, [7-20](#)
 - system catalog, [8-17](#)
 - update, [8-9](#), [8-10](#)
 - updating operating systems, [8-14](#)
- Provisioning operating systems, [7-1](#)

R

- Recommended Software Configuration Report, [4-17](#)
- Relayed incidents, [3-6](#)
- Relayed service requests, [3-6](#)
- Report Result
 - updating operating systems, [8-16](#)

Reports

- Baseline Analysis Report, [4-11](#)
- Change History Report, [4-9](#)
- Distribution Update Report, [4-32](#)
- Engineered System Report, [4-26](#)
- Firmware Compliance Report, [4-30](#), [5-30](#)
- formatting, [4-3](#)
- Generate Report, [4-6](#)
- Host Compliance Report for Microsoft Windows, [4-23](#)
- Host Compliance Report for Oracle Solaris or Linux, [4-22](#)
- Incident Compliance Report, [4-19](#)
- Incident Compliance Report for Microsoft Windows, [4-21](#)
- Incident Compliance Report for Oracle Solaris or Linux, [4-19](#)
- Incident Detail Report, [4-28](#)
- Incident Summary Report, [4-28](#)
- Oracle Solaris Update Compliance Report, [4-18](#), [8-16](#)
- OS Update, [8-7](#)
- Package Compliance Report, [4-33](#)
- Profile Analysis Report, [4-15](#)
- Recommended Software Configuration Report, [4-17](#)
- Results, [4-7](#)
- roles, [4-4](#)
- scheduling, [4-3](#)
- Service Pack Compliance Report, [4-32](#)
- System Catalog, [8-7](#)
- System Catalog Report, [4-24](#)
- System Information Report, [4-25](#)
- templates, [4-5](#), [4-6](#)

requirements, [8-3](#)

Role

- root, [2-1](#)

Roles

- Cloud Admin, [2-1](#)
- Cloud User, [2-1](#)
- incidents, [3-2](#)
- operating system updates, [8-4](#)
- operating systems, [6-3](#), [7-5](#), [8-4](#)
- Reports, [4-4](#)
- user interface, [1-6](#)

Root user role, [2-1](#)

S

SCCM See Microsoft System Center Configuration Manager, [8-20](#)

Scheduling reports, [4-3](#)

Service Pack Compliance Report, [4-32](#)

Service requests

- automated, [3-24](#)
- creating, [3-24](#)

Service Requests Opened by Others, [3-6](#)

Session timeout, [1-7](#)

Sessions, [1-6](#)

Show Graph, [1-6](#)

Snapshots

- boot environments, [6-34](#), [6-36](#)

Solaris See Oracle Solaris, [8-1](#)

Start page preferences, [1-6](#)

Suggested Action, [3-12](#)

SUNWjet, [7-44](#)

Switch Management Access, [6-11](#)

System Catalog

- creating profiles, [8-17](#)
- updating operating systems, [8-15](#), [8-16](#)
- viewing, [8-7](#)

System Catalog Report, [4-24](#)

System Information Report, [4-25](#)

T

Table refresh frequency, [1-7](#)

Take Action on Incident, [3-7](#), [3-8](#)

Templates

- deleting report template, [4-6](#)
- edit report template, [4-6](#)
- JumpStart Enterprise Toolkit, [7-45](#)
- Reports, [4-5](#)

Time interval, [1-7](#)

U

Unassigned incidents, [3-6](#)

Update, [8-1](#)

Update job

- Microsoft Windows, [8-22](#)

Update policies

- custom, [8-8](#), [8-9](#)

Update Profile, [6-44](#), [6-45](#)

Update profiles, [8-9](#), [8-10](#), [8-17](#)

Updates See operating system updates, [8-1](#)

User interface preferences

- connectivity check interval, [1-7](#)
- console timeout, [1-7](#)
- job status popup duration, [1-7](#)
- membership graph, [1-6](#)
- session timeout, [1-7](#)
- start page, [1-6](#)
- table refresh frequency, [1-7](#)
- time interval, [1-7](#)

User preferences

- by role, [1-6](#)
- membership graph preferences, [1-6](#)
- summary, [1-4](#)

V

View Alerts, [3-7](#), [3-8](#)
View Annotations, [3-7](#), [3-8](#)
View Comments, [3-7](#), [3-8](#)
View Interactive, [4-3](#)
View Possible Impacts and Causes, [3-7](#), [3-8](#)
View Suggested Actions, [3-7](#), [3-8](#)
Viewing annotations, [3-11](#), [3-16](#)
Viewing comments, [3-17](#)
Viewing incident details, [3-3](#), [3-14](#)
Viewing unresolved incidents, [3-14](#)

W

WAN boot

WAN boot (*continued*)
 disable and enable, [7-11](#)
 requirements, [7-9](#)
 setup, [7-11](#)
Warning, [3-12](#)
Warranty, [3-21](#), [3-22](#)
White list, [4-12](#), [4-15](#)
Windows
 updating, [8-20](#)
Windows Update, [8-20](#)
WMI, [8-20](#)

Z

Zpools, [6-28](#), [6-29](#), [6-33](#)