Oracle® Enterprise Manager Ops Center

Advanced User's Guide

11*g* Release 1 Update 3 (11.1.3.0.0)

E18416-04

November 2011

ORACLE®

Oracle Enterprise Manager Ops Center Advanced User's Guide, 11*g* Release 1 Update 3 (11.1.3.0.0)

E18416-04

Primary Author: Laura Hartman

Contributing Author: Barbara Higgins, Owen Allen, Shanthi Srinivasan

Contents

6 Managed Networks

7 Update Profiles and Policies

8 Hardware and Provisioning Profiles

9 Monitoring Rules and Profiles

13 Complex Plan Management

A Scenario – Deploying a Bare-Metal System

Preface

The *Oracle Enterprise Manager Ops Center Advanced User's Guide* is a user reference that teaches you how to perform more advanced tasks and tasks that are used to help configure the Enterprise Manager Ops Center software. The goal of this book is to help you understand the concepts behind the product. It teaches you how to perform all common tasks needed to effectively monitor and manage assets within your environment.

Audience

This document is intended for advanced users and senior system administrators.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents in the Oracle Enterprise Manager Ops Center 11*g* documentation set:

- *Oracle Enterprise Manager Ops Center Release Notes*
- *Oracle Enterprise Manager Ops Center Concepts Guide*
- *Oracle Enterprise Manager Ops Center Site Preparation Guide*
- *Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System*
- *Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems*
- *Oracle Enterprise Manager Ops Center User's Guide*
- *Oracle Enterprise Manager Ops Center Provision and Update Guide*

- *Oracle Enterprise Manager Ops Center Administration Guide*
- *Oracle Enterprise Manager System Monitoring Plug-in for Oracle Enterprise Manager Ops Center Guide*
- *Oracle Enterprise Manager Ops Center Reference Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Overview

Advanced User concepts and tasks are typically performed by a senior system administrator that has Enterprise Controller Admin or All Assets role permissions. See "Roles and Authorizations" in the *Oracle Enterprise Manager Ops Center Administration Guide* for the set of authorizations granted for each role.

Many of the tasks described in this document are used to configure Oracle Enterprise Manager Ops Center to comply with your organization's system administration policies and procedures. Once established, these tasks are not performed on a daily basis.

The following topics are covered:

- Asset Management
- Software Libraries
- Images and Local Content
- Managed Networks
- Update Profiles and Policies
- Hardware and Provisioning Profiles
- Monitoring Rules and Profiles
- Problems Knowledge Base
- Operational Profiles and Plans
- Deployment Plans
- Complex Plan Management

Overview

The first step is to discover the assets that you want to manage. A number of discovery methods are available for you to locate the physical and virtual hardware and operating systems that are present in your data center. Each discovery method launches a discovery job. When the job is successfully completed, the asset is displayed in the Available to be Managed tab in the UI.

After you install the software, determine the data center assets that you want to manage with the software. Asset management enables you to use a variety of methods to identify the assets in your data center and display them in the user interface. This is a prerequisite for almost every action inEnterprise Manager Ops Center.

The second step is to manage the assets. Managing assets allows you to use the management console to monitor and control them. Agent software is installed on

operating systems during the management process. An Agent is lightweight Java software that identifies the asset and can respond to inquiries from the Proxy Controller. It is required to perform some OS update, management, and monitoring operations. All managed assets appear in the Asset section of the Navigation pane.

You can register your managed assets with My Oracle Support and gain access to eligible Oracle services, such as displaying warranty information and filing service requests, from the Oracle Enterprise Manager Ops Center UI.

Managed Networks

Managed networks are used by the virtualization technology. If your organization is using Oracle VM Server for SPARC or Oracle Solaris Zones, you can establish and configure storage libraries and networks for virtualization.

Libraries

Libraries are used to store cached data, images, packages, and metadata. The following types of libraries are available:

- Software – Contains images, supporting metadata, and profiles that are used in provisioning
- Solaris and Linux OS Update – Contains OS update packages and your custom programs and scripts, known as local content
- Storage – Contains virtual images, the profiles that create the virtual images, and the data used by them
  - NAS storage libraries contains metadata and data for any virtual image associated with the storage library
  - Fibre Channel storage libraries contain virtual images' data

You can create virtual pools for your Oracle VM Server for SPARC instances and share resources between members of the virtual pool. This enables you to associate multiple virtual hosts with a storage library and share the content with other hosts in the virtual pool. This type of library can be accessed through an NFS server or SAN network, or can reside locally on the virtual host's server.

Policies, Profiles, and Plans

You can configure a variety of policies, profiles, and plans to monitor, manage, and update your data center environment.

The following are the major profile categories:

- Monitoring rules and profiles
  - Monitoring rules - Define the rule parameters and alerting conditions
  - Monitoring profiles - Contain user-defined alert configurations that are used to monitor a managed asset, including thresholds and alert monitors
- OS Update policies and profiles
  - Update policies - Define the component configuration of the systems to update
  - Update profiles - Define what update actions to take and in what order
- Provisioning profiles - Define firmware and OS provisioning tasks

- Operational profiles - Contain a shell script, utility, or suggested action that are required to operate your environment or to perform problem resolution

Plans

You can use profiles to create operational and deployment plans to create consistency and efficiency when performing simple or complex tasks.

The following types of plans are available:

- Operational plan
- Deployment plan

An operational plan associates one or more targets with an operational profile. You can use an operational plan to perform a specific task, such as providing an automated response to a monitoring alert or problem.

A deployment plan defines the sequence of operations or steps that must be performed to deploy or manage an asset. It can contain multiple profiles and operational plans. A comprehensive set of deployment plan templates is available, including virtualization templates. A deployment template is an unbound deployment plan which defines the steps of execution but not the profiles and assets. You can copy the templates to create custom deployment plans.

Only the user that creates a plan can edit the plan, including updating the profile version. Other users can edit the plan for a specific deployment, but they cannot change the plan itself. This section describes how to create and manage deployment plans. Information about how to deploy a plan is available in the *Oracle Enterprise Manager Ops Center User's Guide*.

2

Asset Management

Asset management is the process through which Oracle Enterprise Manager Ops Center begins to manage and monitor your assets, which include hardware, operating systems, and virtualization software. Managing your assets is a prerequisite for almost every action in the software.

The following topics are covered in this section:

- Discover Assets When Enterprise Manager Ops Center discovers an asset, the asset is displayed in the center pane, showing you the assets available to be managed. You can discover assets by using specific discovery criteria, by running a search for service tags, or by specifying server information.
- Manage Assets Managing assets gives Enterprise Manager Ops Center full access to the assets and enables you to monitor, update, and provision them. After you have discovered assets, you install agents to manage them.
- Register Assets Registering your assets sends basic asset data, such as the asset type, to Oracle. You can view the hosted list of your registered assets. Registration is not required.

Overview

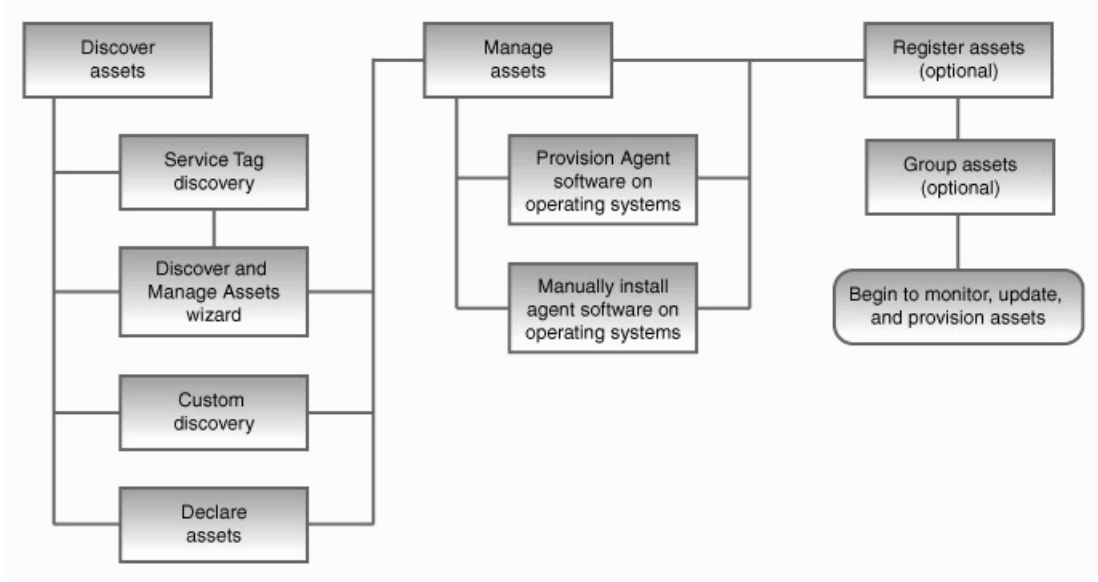
Asset Management is a process that enables Enterprise Manager Ops Center to discover assets, monitor them, and launch jobs that target them.

Asset management includes the following steps:

1. Discovering assets
2. Managing assets
3. Registering assets

Figure 2–1 shows the basic flow and options available with each task.

Figure 2–1 Asset Management Task Map



Discovering Assets

Asset Discovery enables Enterprise Manager Ops Center to determine what hardware, operating systems, and virtualization tools are present in the data center. All assets must be discovered before they can be managed.

For hardware with existing operating systems, you should discover the operating system first, followed by the hardware assets.

Four discovery methods are available:

- Custom Discovery – This method uses standard protocols such as SSH, IPMI, Telnet, and SNMP to discover assets. Use this method to discover specific assets, or assets not equipped with Service Tags.
- Declare Assets – This method uses a manual discovery file or user-supplied data to discover assets. Use this method to discover bare-metal hardware before OS provisioning.
- Discover and Manage Assets – A wizard that uses both service tags and custom discovery to quickly discover and manage assets. Use this method to discover large numbers of Service Tag-equipped assets quickly.
- Automatic Discovery – This method searches for service tags attached to assets. Use this method to identify large numbers of Service Tag-equipped assets quickly as a precursor to other discovery methods.

Custom Discovery

Custom discovery lets you discover assets by IP address, IP range, subnet, or host name. The discovery uses the protocols and credentials that you provide, and default credentials if you choose, to discover the addresses and hosts that you specify. A service tag discovery is also performed on those addresses and hosts.

If valid service tags are found for the assets, specific resource discovery drivers are launched based on the service tags. If no valid service tags can be found, all resource

discovery drivers are used. In some cases, these drivers do not match the credential types entered in the wizard, but do represent the best matches for the asset.

Assets discovered by a Custom Discovery are placed in the Available to be Managed Assets tab. Discovered assets that cannot be managed by Enterprise Manager Ops Center are placed in the Unclassified Assets tab.

When you discover a system with Oracle Solaris 10 8/07 OS or later, the zone features are identified in the system. When you discover a global zone, all of its local zones are discovered as well.

To discover an instance of the Oracle Solaris 8 operating system using this method and the SSH protocol, you must first install OpenSSH on the OS.

To discover an ILOM system, the specified user name must have administrator privileges on the system, and both IPMI and ssh credentials must be provided.

To Run a Custom Discovery

1. Click All Assets in the Assets section of the Navigation pane.
2. Click Custom Discovery in the Actions pane. The Custom Discovery wizard is displayed.
3. (Optional) Create new criteria by clicking the Add Criteria icon.
    a. (Optional) Check Save Criteria for Future Use to save the criteria for future use.
    b. (Optional) Check Save Password in Criteria to save the passwords as part of the discovery criteria. This enables you to reuse the criteria for future jobs. If you do not check this option, the password is still saved as an MBean on the Proxy Controller. You can edit the system configuration to remove the access point between the system and the Proxy Controller.
    c. Enter the Criteria name. If you check Save criteria for future use, the criteria is saved under this name.
    d. Enter the Target Proxy Controller. This specifies the Proxy Controller to use for the discovery. The Automatic option selects the most appropriate Proxy Controller.
    e. Enter the One or more IP addresses to scan. These can be entered as a comma-separated list, an IP range specified by (starting address)-(end address), or a subnet specified by (network address)/(bit mask).
    f. Enter the One or more Host names to scan. All host names must be resolvable by the Enterprise Controller.
    g. (Optional) Enter a service tag passphrase. Necessary if a service tag has been configured to be encrypted.
    h. (Optional) Enter a service tag port. Necessary if a service tag has been configured to use a port other than the default of 6481.
    i. (Optional) Enter a service tag timeout. The default value is 20 seconds.
    j. Enter the type of asset to target. Specifying a type of asset restricts the list of available discovery credential types.
    k. To view all discovery credentials or discover multiple types of asset, select All.
    l. Enter the discovery protocol or protocols to use and their credentials.

If you check Also Use Default Credentials, then the discovery may use default credentials, including root credentials, in addition to those specified.

If you select SSH, two sets of credentials can be entered. To use root credentials, enter the root credentials as the first set. To log in as a non-root user and then switch to root, enter the non-root credentials as the first set and the root credentials as the second set.

Note: To discover an ILOM system, the specified user name must have administrator privileges on the system, and both IPMI and ssh credentials must be provided

---

m. Click Save.

4. Select one or more discovery criteria.
5. Click Discover Assets. A Custom Discovery job is launched for each set of criteria submitted. Discovered assets are displayed in the Available to be Managed Assets tab.

Automatic Discovery

When an Automatic Discovery is launched, Enterprise Manager Ops Center searches the subnets associated with the configured network interfaces of every Proxy Controller for embedded Service Tags. No credentials or specific targets are required. This discovery method is useful for initial discovery and regular discoveries of service tag-equipped assets.

Once discovered, service tag-equipped assets are placed in the Unclassified Assets tab, where they can be grouped and registered. To begin managing these assets, you must use the Discover and Manage Assets wizard or discover them using a Custom Discovery .

To Run an Automatic Discovery

1. Click All Assets in the Assets section of the Navigation pane.
2. Click Automatic Discovery in the Actions pane. The Automatic Discovery window is displayed.
3. Click Discover Assets. An Automatic Discovery job is launched. Discovered assets are displayed in the Unclassified Assets tab.

Discover and Manage Assets

The Discover and Manage Assets wizard enables you to discover assets and install Agent software to begin managing them.

The wizard launches a service tag discovery to discover assets equipped with service tags. It then lets you select what hardware and operating systems you want to manage with Enterprise Manager Ops Center.

Products without service tags cannot be discovered using this method.

To discover an instance of the Oracle Solaris 8 operating system using this method and the SSH protocol, you must first install OpenSSH on the OS.

To Discover and Manage Assets

1. Click All Assets in the Assets section of the Navigation pane.

2. Click Discover/Manage Assets in the Actions pane. The Discover/Manage page of the Discover/Manage Assets wizard is displayed.
3. Select a discovery option, then click Next.
   - Click Run Discovery Now to launch an Automatic Discovery. When the discovery has completed, click Close.
   - Click I Have Already Run Discovery to skip discovery and proceed to asset management.

   Note: You cannot manage assets without first discovering them. The Discovered Hardware page is displayed.

4. Select the hardware to manage and click Next. The Manage Hardware page is displayed.
5. Enter management information for the selected hardware, including:
   - Target Proxy - Select which Proxy Controller will manage the assets.
   - Credentials for accessing the selected hardware. Three options are available:
     - Use factory-set credentials – Uses factory standard credentials to access the hardware.
     - Use the same credentials for all systems – Uses the credentials that you provide for all hardware that you want to manage.
     - Use individual credentials for all systems – Lets you enter separate criteria for each piece of hardware.

   Note: To discover an ILOM system, the specified user name must have administrator privileges on the system, and both IPMI and ssh credentials must be provided.

6. Click Next. The Discovered Operating Systems page is displayed.
7. Select the operating systems that you want to manage and click Next. The Manage Operating Systems page is displayed.
8. Enter management information for the selected assets, including:
   - Target Proxy - Select which Proxy Controller will manage the assets.
   - Credentials for accessing the selected operating systems. Two options are available:
     - Use the same SSH credentials for all systems – Uses the credentials that you provide for all operating systems that you want to manage.
     - Use individual SSH credentials for all systems – Lets you enter separate criteria for each operating system.
9. Click Next. The Summary page is displayed, and jobs are launched to manage assets.
10. Click Finish.

Declare Configured Assets

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

Configured Assets are hardware assets with their network parameters already set.

This option gathers all of the information needed for OS provisioning, including:

- MAC address of the system, host, or domain
- Potential IP address to determine the Proxy Controller which should act as install server You do not need to use a server's actual IP address. You can use an IP address that is on the same subnet as the server to be discovered. The IP address is used to match the declared asset with the correct Proxy Controller.
- Hardware type to allow filtering of applicable OS Profiles (SPARC or x86 platforms)

To discover multiple servers with Declare Assets, you use a discovery file that you create and upload to Enterprise Manager Ops Center. The file contains the name, model, GUID, IP address, logical port name, and MAC ID for the servers that you want to discover. You can also declare a single server by entering the information directly into the Declare Asset wizard.

Declared assets are placed in the Available to be Managed Assets tab.

To Declare Assets

1. (Optional) If you want to declare multiple servers, create a discovery file.
2. Click All Assets in the Assets section of the Navigation pane.
3. Click Declare Configured Assets in the Actions pane. The Declare Assets wizard is displayed.
4. Select a method for declaring assets.
    - To declare multiple servers at once, select Declare All Servers and enter the path of the discovery file. Click Browse to locate the discovery file.
    - To declare a single server, select Declare a Single Server and enter the required information.
        * Server Name – The name that the server should appear under in the UI.
        * IP Address – Specify an IP address
        * Model Category – Select the category in which the asset model appears.
        * Model – The model of the asset.
        * MAC Address and Port combination – Used to connect to the server once it is available on the network. Click the Add or Edit icons to add or edit a MAC Address/Port combination, then select the combination.
        * Enter a logical port name for each network interface. One of these logical port names must be GB_0. Available logical port names are GB_0 through GB_11. You can also use "mgmt" as a management port. These logical port names are mapped to network interfaces after the asset has been provisioned, according to the MAC addresses that you specify. If the server has only one network interface, use GB_0.
        * Enter the MAC addresses of the network interfaces in the server that you want to declare.

5. Click Declare Assets. A Discovery Job is launched for each declared asset. Declared assets are placed in the Available to be Managed Assets tab.

Example Discovery File

Here is an example of a discovery file.

```
<?xml version='1.0' encoding='utf-8'?>
<servers>
<server name="server1" model="V20z" guid="123"
ipAddress="129.147.247.1" >
<ethernetPort name="GB_0" mac="00:09:3D:11:CC:0E"/>
</server>
<server name="server2" model="V20z" guid="123"
ipAddress="129.147.247.2" >
<ethernetPort name="GB_0" mac="00:0A:2D:11:AC:31"/>
</server>
</servers>
```

Variables used:

- **server name** – The name that the server should appear under in the UI
- **model** – Must be a model supported by Enterprise Manager Ops Center
- **guid** – A unique identifier for the server
- **Ethernet port name** - Used to connect to the server once it is available on the network
- **Ethernet Port mac** – Used to connect to the server once it is available on the network

Declare Unconfigured Assets

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

Unconfigured assets are assets with none or some of their network parameters set.

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

Declared assets are placed in the Available to be Managed Assets tab.

To Declare Unconfigured Assets

1. Click All Assets in the Assets section of the Navigation pane.
2. Click Declare Unconfigured Assets in the Actions pane. The Declare Assets wizard is displayed.
3. Enter data for the server or servers to be discovered:
   - Number of Servers – The total number of servers to be discovered.
   - Model Categories – The model category of the servers.
   - Model – The specific model of the servers.

- Server Names – The names of the servers, including:
  - Prefix – A prefix that appears before each server name. This field is required.
  - Starting Number – The number of the first server. The number is increased by one for each additional server. This field is required.
  - Suffix – A suffix that appears after each server name.
- Network – The network on which the server or servers is added.
- IP address – The IP addresses to be used for the servers.
- MAC Address – The MAC Addresses of the servers.

4. Click Declare Asset. A Discovery Job is launched for each declared asset. Declared assets are placed in the Managed Assets tab.

Managing and Registering Assets

Managing assets allows Enterprise Manager Ops Center to monitor and control them. The Agent software is installed on operating systems during the management process.

Assets can also be registered, making a hosted version of your inventory available.

After you have discovered assets, you manage them. Managing assets changes their status so that Enterprise Manager Ops Center can monitor the assets and launch jobs that target them. Managing operating systems installs Agent software on them, while hardware can be managed without Agent software.

Agent software can be installed on Oracle Solaris, Oracle Linux, and SUSE Linux Enterprise Server operating systems. Agent software can also be installed in zones, by installing packages in directories such as the /usr directory.

When you click the Manage Assets button, assets in the Available to be Managed Assets tab move to the Managed Assets tab. To manage assets in the Unclassified Assets tab, discover them using a Custom Discovery or use the Discover and Manage Assets wizard.

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

To manage a global zone with sparse root zones, you must first manage the global zone and then manage each sparse root zone. This order ensures that the sparse root zone inherit the global zone's attributes. This does not apply to the whole root zone because it does not inherit the directories from the global zone.

To Manage Assets

1. Click All Assets in the Assets section of the Navigation pane.
2. Click the Available to be Managed Assets tab in the center pane.
3. Select one or more assets, and click the Manage Assets button.
   - If an asset is hardware, a job is launched to manage the asset.
   - If an asset is an operating system, the Manage Assets wizard is displayed.
4. Select an option to provide SSH credentials for the systems that you want to manage:

- Reuse the SSH credentials used to discover the asset. Discovery Credentials expire one hour after discovery.
- Enter one set of SSH credentials to use for all asset.
- Enter separate SSH credentials for each asset.

5. Click Next. The Start Managing page is displayed.
6. Confirm your selection and click Next. The Summary page is displayed. A job is launched to install Agent software.
7. Click Close.

Installing Agents Manually

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

Before You Begin

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

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

Some example agentadm commands in this procedure use the alternative administrative user name droot. In these examples, the droot user exists on the Enterprise Controller associated with this example Enterprise Manager Ops Center installation.

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

To Manually Install an Agent

- Transfer an Agent software bundle to the system where you want the Agent to run
- Install the Agent software
- Configure the Agent software

See To Transfer and Install Agent Software for information about transferring an Agent bundle from the Enterprise Controller to the target system, and install the Agent software.

See either To Configure Agent Software Using User Credentials or To Configure Agent Software Using a Token to configure the Agent software, depending on your site security requirements.

To Transfer and Install Agent Software

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

```
# cd /var/opt/sun/xvm/images/agent/
# ls
SunConnectionAgent.Linux.i686.2.6.0.1483.zip
SunConnectionAgent.Linux.i686.2.6.0.1483.zip.sig
SunConnectionAgent.SunOS.i386.2.6.0.1483.zip
SunConnectionAgent.SunOS.i386.2.6.0.1483.zip.sig
SunConnectionAgent.SunOS.sparc.2.6.0.1483.zip
SunConnectionAgent.SunOS.sparc.2.6.0.1483.zip.sig
#
```

2. Identify the Agent archive that is appropriate for the system where you intend to install the Agent.

3. On the system where you want to install the Agent (the target system), create a directory named `/var/tmp/OC`.

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

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

```
# scp SunConnectionAgent.SunOS.sparc.2.6.0.1483.zip
root@10.5.241.74:/var/tmp/OC
Password:
SunConnectionAgent.S 100%
|*****************************************************************| 34695
KB 00:32
#
```

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

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

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

```
# unzip SunConnectionAgent.SunOS.sparc.2.6.0.1483.zip
(output omitted)
```

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

```
# SunConnectionAgent/install -a
Installing Ops Center Agent.
No need to install 120900-04.
No need to install 121133-02.
No need to install 119254-63.
No need to install 119042-09.
No need to install 121901-02.
```

```
No need to install 137321-01.
Installed SUNWjdmk-runtime.
Installed SUNWjdmk-runtime-jmx.
(output omitted)
6 patches skipped.
19 packages installed.
Installation complete.
Detailed installation log is at /var/scn/install/log.
Uninstall using /var/scn/install/uninstall.
#
```

To Configure Agent Software Using User Credentials

This procedure creates a file that holds the password of the administrative user for your Enterprise Manager Ops Center installation. If you prefer to avoid creating this file, use To Configure Agent Software Using a Token instead of this procedure to configure your Agent software.

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

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

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

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

3. Use the agentadm command to associate the Enterprise Manager Ops Center Agent with the Proxy Controller.

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

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

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

     ```
     # /opt/SUNWxvmoc/bin/agentadm configure -u droot -p /var/tmp/OC/mypasswd -x
     ```

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

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

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

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

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

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

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

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

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

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

To Configure Agent Software Using a Token

This procedure uses a token to configure your Agent software. If you prefer to use user credentials for this purpose, see To Configure Agent Software Using User Credentials.

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

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

(output omitted)

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

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

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

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

   - Replace auto-reg-token with autoregToken.
   - Remove any backslash characters from the token string. For example:

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

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

   - Oracle Solaris OS – Use the `/opt/SUNWxvmoc/bin/agentadm` command.
   - Linux OS – Use the `/opt/sun/xvmoc/bin/agentadm` command. The example commands below use the following options:
   - configure – Causes an Agent configuration operation to take place.

- -t – Specifies the absolute path name of the file that contains the registration token.
- -x – Specifies the IP address or host name of the Proxy Controller to which this Agent will connect.
- -a – Specifies the IP address to use during Agent registration. This selects the network interface that the Agent will use for registration. Accept the server's certificate when prompted. For example:

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

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

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

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

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

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

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

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

```
End of validation

{output omitted}
End of configuration.
```

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

6. Use the sc-console command to list the Agent connection. For example:

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

Registering the Target System

When you manually install an Agent, the target system is listed in the Managed Assets tab as a managed system. However, the target system is not automatically registered.

To Register the Target System

1. Select Assets from the Navigation pane in the Enterprise Manager Ops Center UI.
2. Select the All Assets item. The Register Assets action item is displayed in the Actions list.
3. Select the Register Assets action. The Introduction pane of the Register Assets Wizard is displayed. Click Next. The Select Assets pane is displayed.
4. Select the system that you want to register. Click Next. The Register Assets pane is displayed.
5. Click Register to submit the job.
6. Click Close to exit the Register Assets wizard.

Unmanaging and Deleting Assets

The Unmanage/Delete Asset option will uninstall Agent software and remove an asset from Enterprise Manager Ops Center.

The operating systems that support the Enterprise Controller and Proxy Controllers cannot be unmanaged.

> **Note:** To unmanage a global zone, you must first unmanage any subordinate zones and then unmanage the global zone.

To Unmanage and Delete an Asset

1. Click All Assets in the Assets section of the Navigation pane.
2. Select the asset or assets that you want to remove from the Managed Assets or Available to be Managed Assets tabs.
3. Click Unmanage/Delete Asset if the asset is managed, or click Delete Asset if the asset is not managed. For assets that do not have an Agent Controller installed, a job is launched to delete the asset. For assets that have an Agent Controller installed, the Unmanage and Delete Asset wizard is displayed. The Enter Credentials page is displayed.

4. Select an option for providing SSH credentials for the systems that you want to unmanage:
   - Reuse the SSH credentials used to discover the asset
   - Enter one set of SSH credentials to use for all asset
   - Enter separate SSH credentials for each asset
5. Click Next. The Unmanage/Delete page is displayed.
6. Confirm your selection and click Next. A job is launched to unconfigure and uninstall the Agent Controllers. A second job is launched to delete the assets from Enterprise Manager Ops Center. The Summary page is displayed.
7. Click Close.

Removing Assets

The Remove Assets option removes assets from Enterprise Manager Ops Center, but does not uninstall Agent software.

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

To Remove Assets

1. Click All Assets in the Assets section of the Navigation pane.
2. Select the asset or assets that you want to remove from the Managed Assets or Available to be Managed Assets tabs.
3. Click Remove Assets. A confirmation window is displayed.
4. Click Remove. A job is launched to remove the assets.

Updating Discovery Credentials

Enterprise Manager Ops Center stores the credentials that were used to discover each asset. These credentials may be reused for other jobs that require access to an asset.

The Update Discovery Credentials procedure lets you add, edit, or delete these credentials.

To Update Discovery Credentials

1. Select one or more assets.
   - Click All Assets in the Assets section of the Navigation pane, then select an asset.
   - Select a user-defined group.
2. Click Update Discovery Credentials in the Actions pane. The Update Discovery Credentials wizard is displayed.
3. Enter new credentials or edit existing credentials:
   - Username – The user name to be used for the initial login. If root SSH access is permitted, use the root user name. If not, use an alternate user name.
   - Password – The password to be used for the initial login.
   - Role – The secondary user name. If root SSH access is permitted, leave this field blank. If not, use the root user name here.

- Role Password – The secondary password.

4. (Optional) Remove existing credentials by deleting their user name.
5. Click Next. A job is launched to update the discovery credentials. The Summary page is displayed.
6. Click Close.

Editing Attributes of an Asset

All assets have three attributes that can be edited: the name field, the description field and the tag field.

The name field is the name used for the asset in the UI. This name is created by the Proxy Controller during discovery. If the Enterprise Controller and Proxy Controller used in a discovery resolve different names for the asset's IP address, the user-friendly name might not match the name used in the discovery.

Use the description field for descriptive information about a system.

The tag field enable you to categorize assets and simplify later searches. It is automatically populated with one or more tags based on its asset type. For example, managed systems have the 'agent' tag. These default tags can be removed, and additional tags can be added.

To Edit All Attributes

Perform the following steps to edit an asset's attributes:

1. Click All Assets in the Assets section of the Navigation pane.
2. Click the Managed Assets tab. The managed assets list is displayed.
3. Select an asset from the managed asset list.
4. Click the Edit Asset icon. The Edit Asset window is displayed.
5. Edit one or more of the attribute fields.
6. Click Save.

A job is launched to update the asset attributes.

To Edit the Description and Tags Attributes

Perform the following stgeps to edit the description or tags for an asset:

1. Select an asset in the Assets section of the Navigation pane.
2. Click Edit Attributes in the Actions pane or click the Edit Attributes icon in the center pane. The Description and Tags fields are editable.
3. Edit the description and tags fields.
4. Click the Save icon in the center pane. The asset attributes are updated.

Viewing Access Points

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

The following are possible access points:

- The discovery credentials used to discover the asset.

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

To View Access Points

1. Expand All Assets in the Assets section of the Navigation pane.
2. Select an asset.
3. Click the Configuration tab. The access points for the asset are displayed.

Deleting Access Points

An asset's access points show how Oracle Enterprise Manager Ops Center connects to the asset. You can remove access points from Oracle Enterprise Manager Ops Center if they are incorrect or no longer necessary.

To Delete Access Points

1. Expand All Assets in the Assets section of the Navigation pane.
2. Select an asset.
3. Click the Configuration tab. The access points for the asset are displayed.
4. Select one or more access points.
5. Click the Delete Access Point icon. A confirmation window is displayed.
6. Click Delete. The Access Points are deleted.

Register Assets

Registering your assets uploads your asset data to My Oracle Support, matching it with your Online Account.

Assets cannot be registered until the Enterprise Controller is registered. If you click Register Assets and have not registered the Enterprise Controller, you are prompted to do so.

To Register Assets

1. Click All Assets in the Assets section of the Navigation pane.
2. Click Register Assets in the Actions pane. The Register Assets wizard is displayed.
3. The introduction page is displayed. Click Next.
   - If you have registered your Enterprise Controller, the Discovery page is displayed.
   - If you have not yet registered the Enterprise Controller, the HTTP Proxy page is displayed.
4. Register the Enterprise Controller with Oracle.
   - If an HTTP Proxy is needed for the Enterprise Controller to access the Internet, enter the HTTP Proxy information, then click Next. The Online Account Page is displayed.

- Enter a valid Online Account and password, then click Next. If the specified Online Account is associated with more than one team, the Team page is displayed. Otherwise, the Discovery page is displayed.
- Select a Team and click Next. The Discovery page is displayed.

5. Select a discovery option.
   - Select Discover Systems Now to run a Service Tag discovery.
   - Select Do Not Run Discovery Now to skip discovery. You can still register assets that were discovered before this wizard. Click Next. A job is launched to reconcile discovered assets with registered assets. A popup is displayed showing the status of this job.
6. When the job is finished, click Close. The Select Assets page is displayed.
7. Select the assets to register, then click Next. The Register Assets page is displayed.
8. Confirm your selection, then click Register.

   An Asset Registration job is launched. The Summary page is displayed.
9. Click Close.

Special Discovery and Management Procedures

Most assets can be discovered and managed using the procedures in the Discovering Assets and Managing Assets sections. However, some types of assets must be discovered or managed using special procedures. These procedures should be used when any of the asset types listed below is discovered or managed.

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

SPARC Enterprise M-Series Server Support

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

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

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

Ops Center supports the SPARC Enterprise M-series servers in the following ways:

- Discover XSCF service processors and existing dynamic system domains.
- Power On/power off the XSCF service processors and their dynamic system domains.
- Provision an Oracle Solaris OS in dynamic system domains.
- Update the Oracle Solaris OS in dynamic system domains.
- Provision firmware on the service processor.
- Add the system board to domain and remove it.
- Monitor the service processor hardware.
- Monitor a dynamic system domain's sensor information and hardware.
- Create and delete dynamic system domains.

Requirements for Managing M-Series Servers

The following is required to manage this type of asset:

- The XSCF service processor has a user account with the platadm privilege.
- The server is assigned to homogeneous asset groups.
- The server is discovered and managed.

To Discover a SPARC Enterprise M-Series Server

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

Perform the following tasks before discovering this type of asset:

- In the XSCF service processor, create a user account with platadm privilege.
- Ensure that user privileges and the status of each dynamic system domain are correct.
- Check the status of each dynamic system domain, using the showdomainstatus -a command. Ops Center can only discover domains that do not have a "-" status.

1. Log in to the XSCF shell from an XSCF-LAN port or from the serial port.
2. Log in to Oracle Enterprise Manager Ops Center.
3. Expand All Assets in the Navigation pane.
4. Click Custom Discovery in the Actions pane. The Custom Discovery wizard is displayed.
5. (Optional) Create new criteria by clicking the Add Criteria icon. If you have already created criteria for discovering this SPARC Enterprise M-Series Server, skip this step.
    a. (Optional) Check Save Criteria for Future Use if you intend to discover other SPARC Enterprise M-Series servers.
    b. (Optional) Check Save Password in Criteria.

c. Criteria name. When you check Save criteria for future use, the criteria is saved with this name.

d. Targeted Proxy Controller. Specify the Proxy Controller to use for the discovery. The Automatic option selects the most appropriate Proxy Controller.

e. The IP address of the XSCF Service Processor

f. The type of asset to target Specify XSCF Service Processor.

g. The discovery protocol to use and its credentials. Select either telnet or ssh and enter the credentials for the account with platadm privileges.

h. Click Save.

6. Select your discovery criteria.

7. Click Discover Assets. A Custom Discovery job is launched. Dynamic system domains and the XSCF service processor are discovered at the same time. When the job is complete, the domains and the XSCF service processor are displayed in the Available to be Managed Assets tab. The XSCF service processor is listed as a chassis and the dynamic system domains are listed as blade servers under the chassis. See Adding SPARC Enterprise Manager M-Series Servers to a Group in the *Oracle Enterprise Manager Ops Center User's Guide* to create a group for each server.

Sun ZFS Storage Appliance Support

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

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

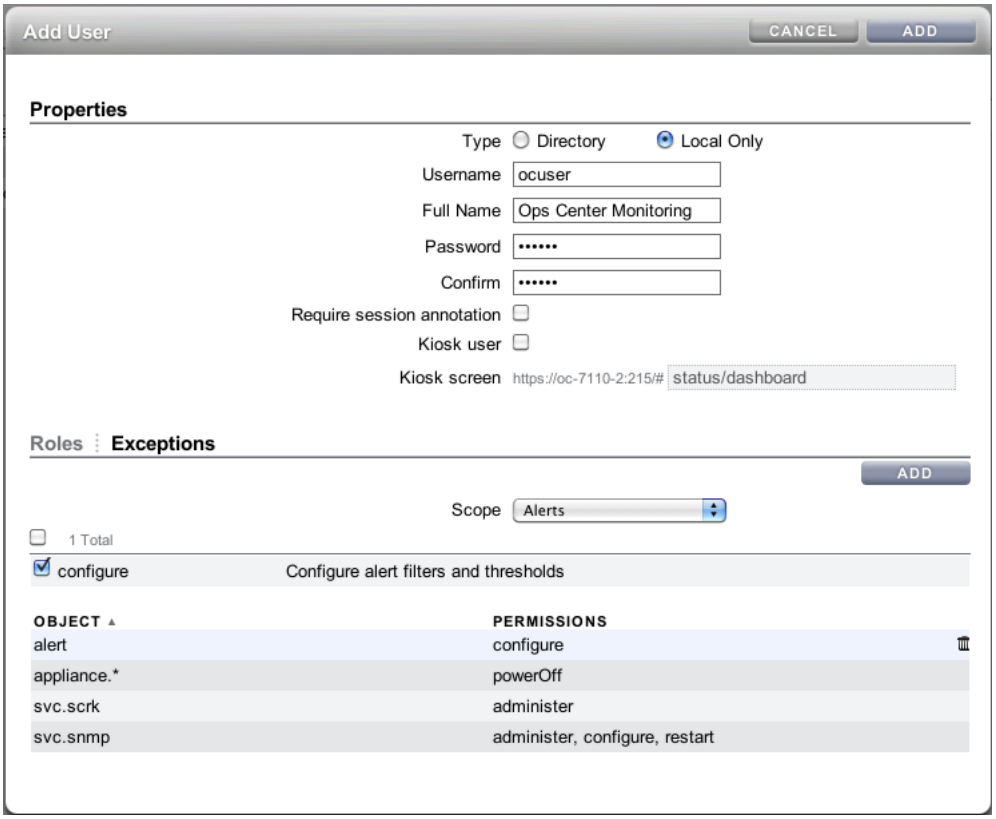
To manage a Sun ZFS storage appliance, you must discover both the storage appliance and its service processor, and follow special procedures to manage them.

1. Create a user account on the appliance with the username *ocuser* with the basic administration role and the following permissions and characteristics:

   - Permission to configure alert filters and thresholds
   - Permission to administer the Phone Home Service. If the user account does not have this permission, it is not possible to use the Enable Appliance Phone Home or Disable Appliance Phone Home actions.
   - Permission to power off the appliance. If the user account does not have this permission, it is not possible to power off the storage appliance remotely.
   - Permission to administer, configure and restart the SNMP service (required).

   A sample user account is shown in the following figure:

Figure 2–2 Sun ZFS Storage Appliance Support



- User account must not be a kiosk type.
- User account must not require session annotation.

2. Power on and configure the Sun ZFS Storage Appliance.
3. Configure the storage pool on the appliance.

See the *Oracle Enterprise Manager Ops Center Reference Guide* for instructions on getting access to Sun ZFS Storage Appliance documentation for creating user accounts. See Discovering a Sun ZFS Storage Appliance for instructions on discovering this storage appliance.

Provisioning and Updating a Sun ZFS Storage Appliance

Unlike other hardware that you provision through a deployment plan, the Sun ZFS Storage appliance's software and firmware is handled by its own feature, Manage Appliance Updates. The software and firmware are packaged in a proprietary format and it is not possible to provision other images or packages on a Sun ZFS Storage Appliance. Therefore, Enterprise Manager Ops Center provisioning wizards do not include these storage appliances in the list of available targets.

Reports for a Sun ZFS Storage Appliance

The Enterprise Manager Ops Center software creates reports from the information it retrieves from an asset and creates charts from the history recorded for the asset. The Sun ZFS Storage Appliance has the Analytics feature that can provide information about the appliance dynamically. Click Launch Analytics in the Actions pane to start the appliance's management UI.

See Managing a Sun ZFS Storage Appliance for more information about this storage appliance.

Discovering a Sun ZFS Storage Appliance

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

- Use Automatic Discovery. Each storage appliance is discovered as two assets: a service processor asset in the Servers section and a storage appliance asset in the Storage section. These assets are listed in the Unclassified Assets tab in the center pane. To manage the storage appliance, use the Discover and Manage Assets action. Select both the appliance and its service processor and enter the user credentials. Enterprise Manager Ops Center removes the generic server from the Servers section and displays only the asset in the Storage section. Use Discover and Manage Assets.
- Use Custom Discovery to discover the storage appliance first and then discover its service processor. When you discover the storage appliance, Enterprise Manager Ops Center displays the device in the Storage section of the Assets tree. When you discover the service processor, its information is mapped to the already-discovered appliance.

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

See the *Oracle Enterprise Manager Ops Center Reference Guide* for instructions on getting access to Sun ZFS Storage Appliance documentation for creating user accounts.

Managing a Sun ZFS Storage Appliance

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

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

- Manage Appliance Updates opens a new browser window or tab for the provisioning software and firmware page.

Problem Management for a Sun ZFS Storage Appliance

The Sun ZFS Storage Appliance can create service requests when it detects a problem condition. When the Enterprise Manager Ops Center software manages the appliance, this software also reports the problem. To avoid creating duplicate reports, disable the appliance's Phone Home Service and allow the Enterprise Manager Ops Center software to report all problems. In the Action pane, two actions toggle this function. Choose Disable Appliance Phone Home Service to turn off the appliance's Phone Home service. If you unmanage a Sun ZFS Storage Appliance and want to restore the appliance's Phone Home service, use the appliance's UI or CLI and navigate to the Configuration > Services section.

Discovering an Oracle Solaris Cluster

Discovering and managing an Oracle Solaris Cluster has some specific requirements.

To Discover an Oracle Solaris Cluster

1. Verify that all global nodes in the cluster are in cluster mode.
2. Discover each of the cluster's global nodes. You must provide both ssh credentials and JMX credentials for each global node.
3. Discover the cluster by selecting Solaris Cluster or All.

Managing an Oracle Solaris Cluster

To manage a cluster, you must manage all the cluster nodes and zone cluster nodes.

The following error can be reported when a cluster is managed:

```
The following Oracle Solaris Cluster nodes are either missing an Operating System
association or an Operating System for them was not discovered:
<name(s)_of_the_nodes>
Before trying to manage the Oracle Solaris Cluster, discover these missing
Operating Systems or delete the Oracle Solaris Cluster asset and re-discover.
```

This message indicates one of the following conditions:

- Not all of the nodes in the cluster were discovered so the association with the OS asset cannot be made. OR
- After the cluster was discovered, a zone cluster was configured. Although the zone cluster and its zone cluster nodes are displayed in the Navigation pane, the associations with the OS asset cannot be made. The cluster either cannot be managed or, if the cluster was managed previously, it becomes unmanaged.

Use one of the following solutions:

- Restart the cacao agent on all the global cluster nodes using the following command to create the missing associations and manage the cluster:

  ```
  cacaoadm restart -i scn-agent
  ```
  OR
- Delete the cluster and use the Unmanage/Delete action on the OS asset on all the cluster nodes. Then discover the cluster and manage the cluster.

Another possible cause of the error condition is that a new global node has been added to the cluster. This causes a managed cluster to become unmanaged. The new global

node and its system are not displayed in the Navigation pane. In this case, discover the global node as a Solaris Cluster type. Then use the Manage to re-manage the cluster.

Configuring a Windows OS for Discovery

Windows Management Instrumentation (WMI) is the infrastructure used by Windows systems for remote management and monitoring operations. It is installed on Microsoft Windows XP and Windows Server 2008, but it is often disabled. To manage and monitor a Windows system, you must configure the target system to enable (WMI) and then allow WMI through the Windows Firewall or Internet Connection Firewall.

To Enable WMI

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

1. Log in to the WMI on the target host.
2. Click Administrative Tools, then click Computer Management.
3. Expand Services and Applications.
4. On WMI Control, right click Properties.
5. Click the Security tab.
6. Click the Security button.
7. Add the monitoring user (if needed).
8. Click the checkbox to allow Remote Enable.

To Allow WMI Through the Windows Firewall

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

1. Go to the command prompt on the target system.
2. Type the following command:

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

3

Software Libraries

The Enterprise Controller must have at least one Software Library to store the new versions of images that are downloaded automatically from the Knowledge Base. You can create additional Software Libraries to organize the images for your site's purposes and you can change which library accepts the automatic download operations.

The following topics are covered in this section:

About Software Libraries

Enterprise Manager Ops Center uses libraries to store and manage cached data, images, packages, and metadata. A library designated to store images for provisioning operations is called a Software Library. The Enterprise Controller requires at least one Software Library to accept the following types of images downloaded from the Knowledge Base:

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

When Enterprise Manager Ops Center provisions target systems with an operating system or firmware, it copies the images files from the designated Software Library to each Proxy Controller. The Proxy Controllers handle the provisioning operations. When Enterprise Manager Ops Center provisions target systems with an update to an operating system, it uses the Solaris/Linux Updates Library, a software library with the following sub-libraries:

- Clusters: Profiles for provisioning Oracle Solaris Cluster software
- Local: scripts to use in provisioning
- Packages: Operating systems, according to the selected Distribution
- Patches: Updates, according to the selected Distribution
- Solaris Baselines: Packages for the Solaris Baseline, according to the selected Distribution
- User's Profiles: Stores profiles and deployment plans that are created at a site.

You can create additional Software Libraries and organize their content, according to your site's purposes. You can use a file system on the Enterprise Controller's system or a shared file system on an NFS server that the Enterprise Controller mounts.

Creating a Software Library

You can create a software library that uses space on a file system on the Enterprise Controller's system. This is called a EC Local Library.

You can also create a software library that uses space on a shared file system on an NFS server. This is called a EC NAS Library.

If you use both local and NAS software libraries, do not use the same name for the library.

To Create an EC Local Software Library

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

To Create an EC NAS Software Library

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

Setting the Software Library for Download Operations

In Connected mode, one Software Library must be designated to accept the images from the automatic download operations from the Knowledge Base. In most cases, the library is created during the configuration of the Enterprise Controller. At any time, you can designate a different library to accept the downloaded images.

If another software library does not exist, create one using the procedure in Creating a Software Library.

To Change Software Libraries

1. Expand Libraries in the Navigation pane. The current active library is identified by its badge.
2. Click Set Enterprise Controller Software Library in the Action pane. The display lists all of the libraries and the current library is highlighted.

3. Click the library you want to store the images from the automatic download operations.
4. Click Apply.

Viewing the Contents of a Software Library

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

To View the Contents of a NAS Software Library

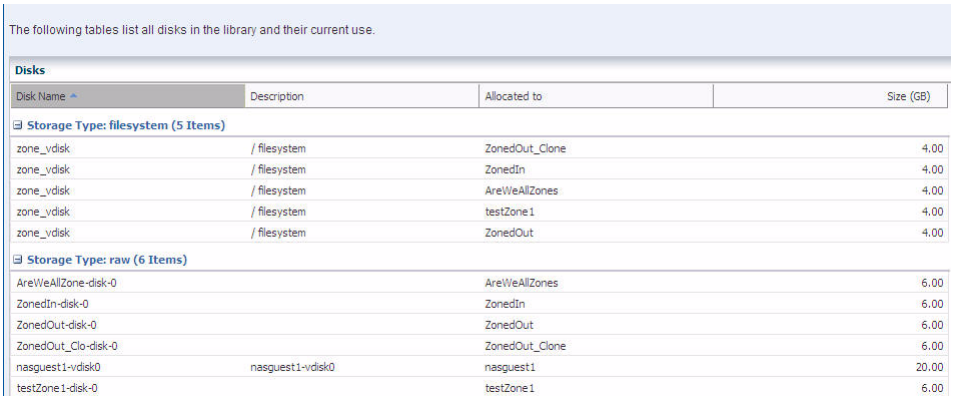
1. Expand Libraries pane in the Navigation pane.
2. Click NAS Storage in SoftwareLibraries.
3. Click a software library.

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

   - URL – NFS.
   - Size – Total storage capacity of the library.
   - Used Space – Space assigned to guests and zones.
   - State – State of the library.
   - Access – Read-Write The Library Contents table lists all the images in the library, organized by type, and includes the size and date the image was modified.
4. To see all the disks in the library, click the Disks tab.

   The Disks tab lists all disks in the library by name and description and shows the current use of each one by allocation and size.

Figure 3–1 Disks Tab



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

Disks

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

5. To see any problems discovered by monitoring the software library, click the Problems tab.
6. To see the attributes and values that are being monitored, click the Monitoring tab.

To View Local Libraries

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

4

Storage Libraries

Enterprise Manager Ops Center stores a guest's configuration for its operating system, data, CPU, memory, and network as metadata in the storage library associated with the virtual host. The guest's data, which results from its use, can reside in the same storage library or in a different storage library.

The following topics are covered in this section:

About Storage Libraries

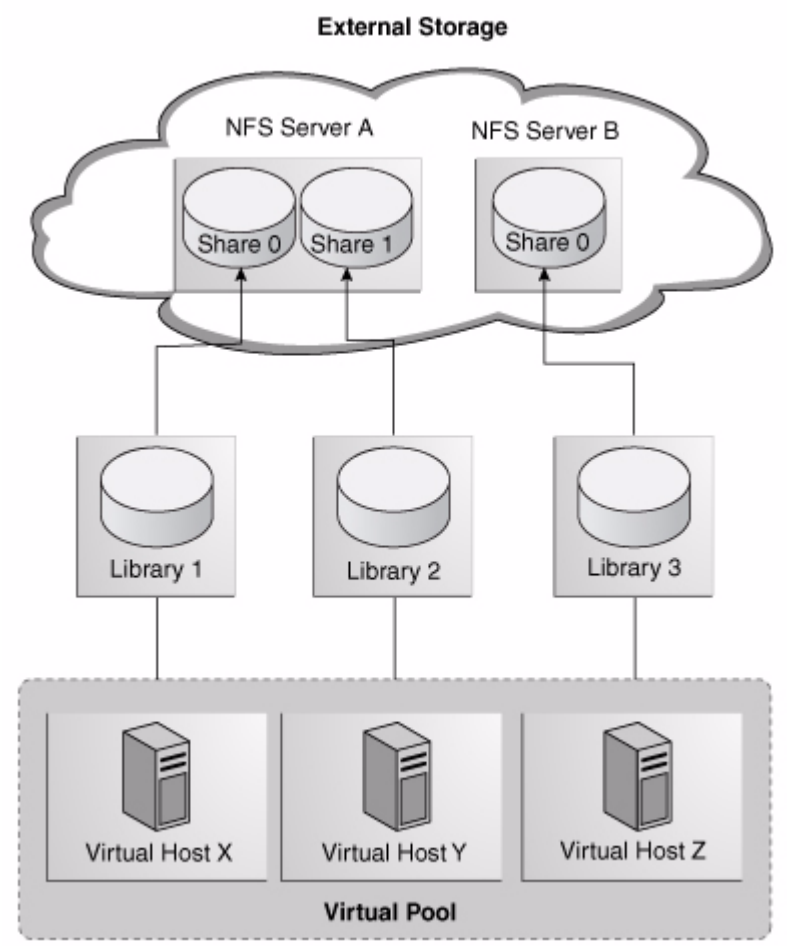
A storage library can be a local, that is, a file system on the virtual host's server or it can be accessed through an NFS server or SAN network. When you create a guest, you assign it to one of the storage libraries associated with its virtual host. The guest's metadata, that is, the configuration of its operating system, CPU, memory, and network is saved in this storage library. The guest's data, which results from its operations, can reside in the same storage library or in a different storage library.

- For the metadata of its local guest, both types of virtual hosts (Oracle VM Server for SPARC and global zones) can use a local storage library.

- For metadata of all guests, both types of virtual hosts must use Network Attached Storage (NAS) storage library.
- For data, Oracle VM Server for SPARC can use either NAS shares or Fibre Channel LUNs for itself and for its logical domains. A global zones can use either Fibre Channel LUNs or NAS shares for itself and for its non-global zones. The storage library must be associated with the virtual host.
- A virtual pool must use a NAS storage library.

You can group hosts with the same processor architecture to create a virtual pool. The hosts in the virtual pool share any storage and networks associated with the virtual pool. If you add a host to a virtual pool, the libraries associated with that host become available to all the other hosts in the virtual pool. The following illustration shows hosts in a virtual pool get access to storage libraries.

Figure 4–1 External Storage

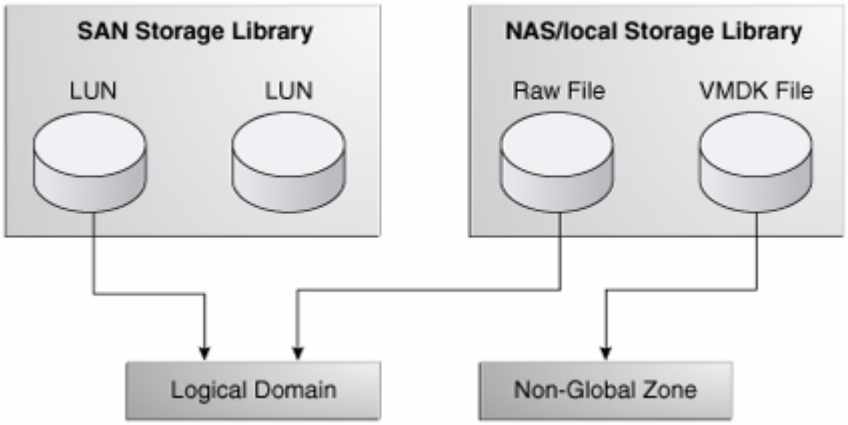


Enterprise Manager Ops Center does not manage storage resources; it does not create, modify or update LUNs on disk arrays and it does not manage NAS shares on NAS systems. Enterprise Manager Ops Center manages the storage libraries, which stores guests' metadata. Virtual hosts use appropriate storage management utilities and services to attach to the storage libraries.

The diagram shows how the storage libraries and types of virtualization interact with virtual disks.

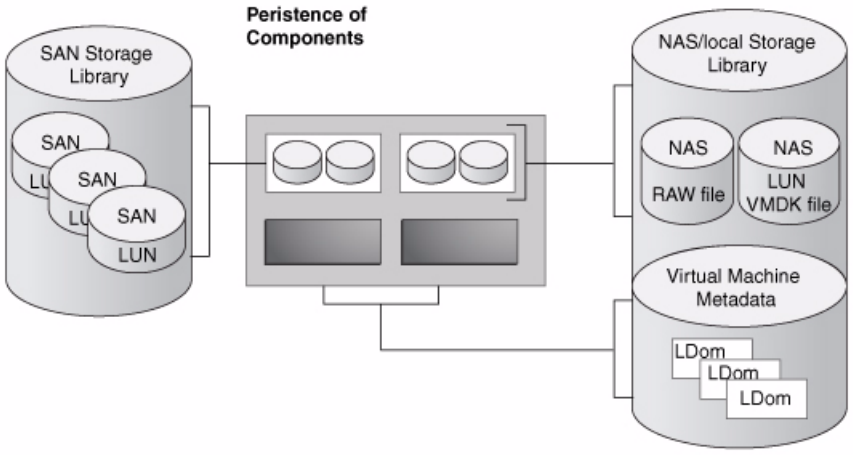
- SAN storage libraries expose data as logical units (LUNs), identified by their LUN GUIDs. A control domain makes raw partitions available to its logical domains using Fibre Channel: Fibre Channel Storage Libraries
- NAS storage libraries expose data as raw files and files in VMDK format. All types of virtual hosts store metadata using either NFS services: Network Attached Storage (NAS) Storage Libraries

Figure 4–2 SAN and NAS Storage Libraries



The LUNs, raw files, and raw volumes store data and metadata for the guests. The metadata for NAS virtual disks are stored in the NAS storage library. Metadata for SAN virtual disks is persisted in the SAN Storage Library.

Figure 4–3 Storage Library Metadata



Network Attached Storage (NAS) Storage Libraries

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

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

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

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

Fibre Channel Storage Libraries

A Fibre Channel storage library is SAN (storage attached network) storage, which you use to store the data for virtual hosts and their guests. A Fibre Channel storage library consists of groups of LUNs. A LUN (Logical Unit Number) is a slice of a storage volume, which is a collection of disks. Each LUN is for the exclusive use of its assigned guest or zone.

- Disk – Physical storage media. A set of disks is a disk array.
- Volume – An aggregation of storage space provided by several disks.
- Slice – A partition of a volume that is exposed to the servers connected to the disk array.
- LUN (Logical Unit Number) – The representation of a slice as seen from the outside world.
- GUID – The Global Unique Identifier for a LUN.

Because a LUN has a fixed size and cannot be shared among zones, you must plan how to optimize the available storage in the storage library. You want to assign a LUN of the appropriate size to the zone. If you need more storage, you can add a LUN to the Fibre Channel storage library

Local Storage Libraries

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

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

Editing Attributes of a Storage Library

You can change the name and description of the storage library and you can add LUNs to a Fibre Channel storage library.

To Edit Attribures of a Storage Library

1. Expand Libraries in the Navigation pane.
2. In Storage Libraries, click either Fibre Channel Storage or NAS Storage.
3. Click the storage library you want to change.
4. Click Edit Library Attributes in the Actions pane.
5. Edit the library name and description.
6. Click Save.

See Adding LUNs to a Fibre Channel Library to change the storage capacity of the storage library.

Removing a Storage Library

Removing a storage library removes its association with a virtual pool, control domain, or global zone. The guests of those virtual hosts or pool whose data is stored in the storage library are no longer accessible.

Note: If you are removing a Fibre Channel storage library, verify that no LUN in the Fibre Channel storage library is associated with any guest.

To Remove a Storage Library

1. Expand Libraries in the Navigation pane.
2. In Storage Libraries, click either Fibre Channel Storage or NAS Storage, depending on the type of storage library.
3. Click the storage library you want to remove.
4. In the Actions pane, click either Remove Fibre Channel Library or Remove NAS Library. The Remove Library popup is displayed. Guests associated the storage library are listed in the Virtual Guests table.
5. Click Remove Library.

   A job is submitted to remove the association.

Disassociating a Storage Library

Control domains, global zones, and virtual pools are associated with storage libraries so that their guests' images and data can be stored.

To Disassociate a Storage Library

1. Select Assets in the Navigation pane.
2. Click the All Assets drop-down list.
3. Select the virtual host or virtual pool you want to disassociate from its storage library.

4. Click the Libraries tab in the center pane. The associated libraries and the guests that are stored in the libraries are listed.
5. Select the library you want to disassociate.
6. Click the Disassociate Library icon. The selected library is detached from the virtual asset.

   See About Storage Libraries for information about how storage libraries are used.

Preparing Storage

The following procedures are the general procedures for setting up NAS storage and Fibre Channel storage.

To Configure Storage for NAS Storage Libraries

The following is the general procedure for setting up a NAS storage library:

1. Set up the mountpoint. See Setting Up the NFS Server.
2. Define the storage library. See Creating a NAS Storage Library
3. Add images to the storage library. See the topics in Images
4. Associate the storage library with a virtual host or zone. See Managing Storage Libraries of a Virtual Pool in the *Oracle Enterprise Manager Ops Center User's Guide*.

To Configure Storage for Fibre Channel Libraries

You configure storage hardware for Fibre Channel libraries external to Enterprise Manager Ops Center. Use a vendor-qualified Fibre Channel disk array and a Fibre Channel switch with sufficient ports. The following is the general procedure for configuring storage. See your vendor's storage documentation for the procedure.

1. Log in to the disk array using the service processor credentials.
2. Define volumes on the disk array with the required number of disks.
3. Initialize the volumes.
4. Create slices from a volume. These are the LUNs.
5. Map the LUNs.
6. Enable the Multipath support (MPxIO) on the disk array so that the LUNs are visible through Oracle Solaris multipathing.

See vendor-specific storage documentation.

Using a Sun ZFS Storage Appliance For a Storage or Software Library

When a Sun ZFS Storage Appliance provides the storage library for a virtual pool, all of the virtual hosts in the virtual pool can use the storage appliance. When you create a new zone or logical domain, you can choose the storage appliance as the location for storing the virtual machine's data and metadata. When used as a software library, the Sun ZFS Storage Appliance stores images for both physical and virtual provisioning.

The Sun ZFS Storage Appliance family of products serves shares through various protocols including NFS and CIFS. The Enterprise Manager Ops Center software supports only NFS shares as storage for its software and storage libraries, but can report on the appliance's CIFS usage. Use the appliance's Charts tab to monitor the performance of CIFS shares exported by the Sun ZFS Storage Appliance.

The Sun ZFS Storage Appliance family of product is unified storage: it provides both file format storage (NAS) and block format storage (SAN) simultaneously. Enterprise Manager Ops Center displays information about NAS shares on the appliance's Storage Shares tab and displays information about LUNs on the appliance's Logical Units tab. When you create a new NAS library and you specify the NFS service, you can select a Sun ZFS Storage Appliance. All of the appliance's exported shares are then listed for selection. In a similar way, when you create a Fibre Channel library and you specify a LUN, you can select an appliance and then select one of the appliance's exported logical units

Viewing the Contents of a NAS Storage Library

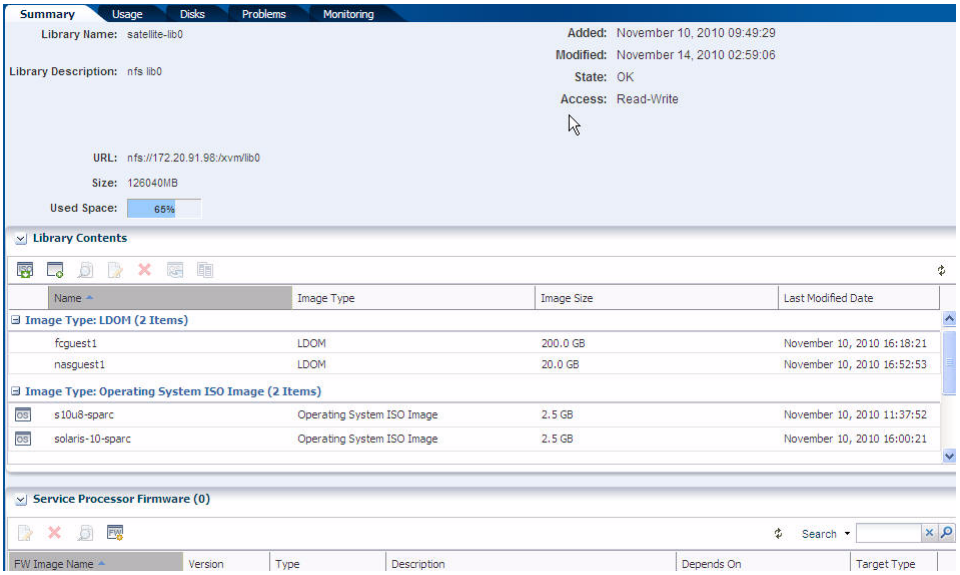
You can display the contents of the storage library, its associations, and details about the disks in the storage library. You can also see how the library is being monitored and any problems.

To View the Contents of a NAS Storage Library

1. Expand Libraries pane in the Navigation pane.
2. Click NAS Storage in Storage Libraries.
3. Click one of the storage libraries.

   The details of the selected NAS library are displayed in the central pane in a set of tabs.

Figure 4–4 NAS Storage Library Summary



The Summary tab shows information about the entire storage library:

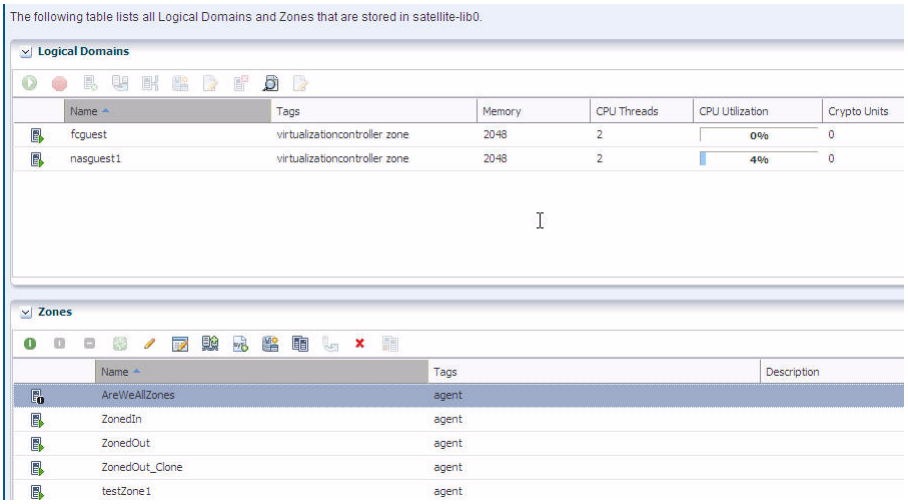
- URL – NFS.
- Size – Total storage capacity of the library.
- Used Space – Space assigned to guests and zones.

- State – State of the library.
- Access – Read-Write The Library Contents table lists all the images in the library, organized by type, and includes the size and date the image was modified.

4. To see the guests that use this storage library, click the Usage tab.

   The Usage tab contains a table for logical domains and zones.

Figure 4–5 Usage Tab

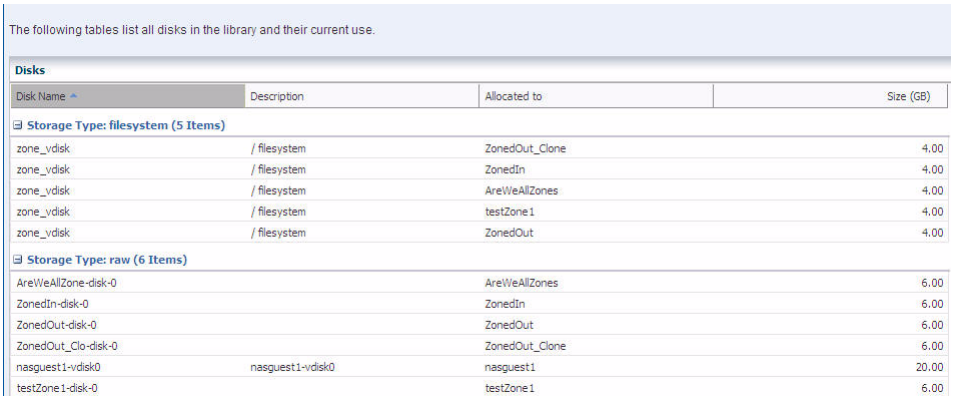


   For each guest, the table shows the following information: Name, Tag, Memory, vCPU, vCPU Utilization, and Image Size or Crypto Unit.

5. To see all the disks in the library, click the Disks tab.

   The Disks tab lists all disks in the library by name and description and shows the current use of each one by allocation and size.

Figure 4–6 Disks Tab



6. To see any problems discovered by monitoring the storage library, click the Problems tab.

7. To see the attributes and values being monitored, click the Monitoring tab.

Creating a NAS Storage Library

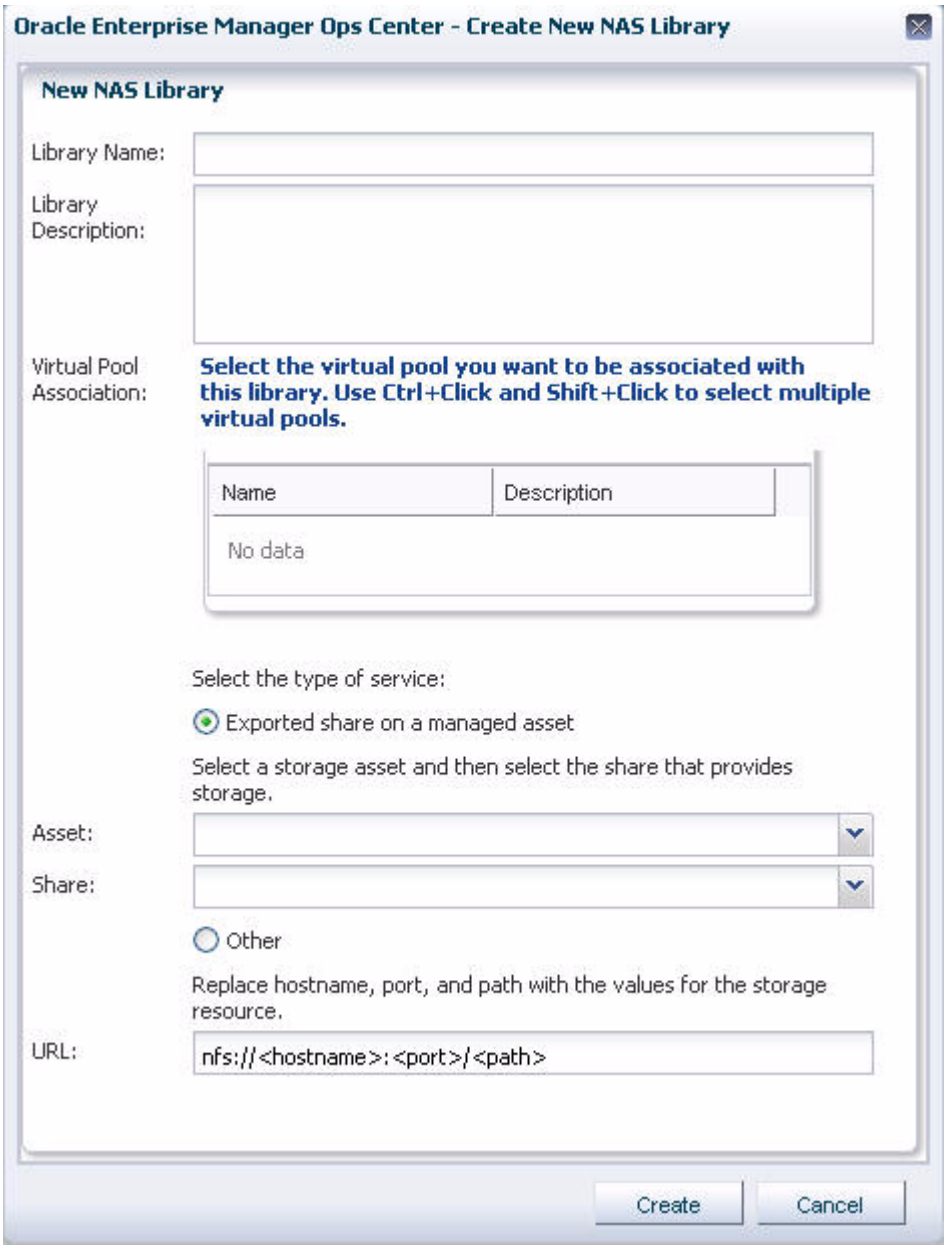
When you first create a new storage library, it has a size of -2 MB and a state of UNKNOWN because the storage library is not yet mounted. For storage libraries that use NFS mount points and an Enterprise Controller on Linux OS systems, the storage library is mounted when a virtual pool is associated with the storage library. The mount process occurs on a host in the virtual pool. After the virtual pool is associated with a storage library and mounted, all the actions on the library are enabled and the size of the storage library is accurate.

To Create a NAS Storage Library

1. Expand Libraries in the Navigation pane.
2. In Storage Libraries, click NAS Storage.
3. In the Actions pane, click New NAS Storage.

   The Create New NAS library window is displayed.

Figure 4–7 Create New NAS Library



4. Enter a name for the library and a description.
5. Select one or more virtual hosts to be associated with this library.
6. For the Type, select NFS to indicate the mount point of the library.
7. You have a choice of either entering the path of a shared directory or, if Enterprise Manager Ops Center is managing a unified storage appliance, selecting the appliance and specifying the exported share you want to use.
8. Click the New NAS Library button to create the library.
9. Associate the library with one or more virtual hosts:
   - Associating Libraries with Oracle VM Server

- Adding Libraries to the Global Zone
- Managing Storage Libraries of a Virtual Pool

Viewing the Contents of a Fibre Channel Storage Library

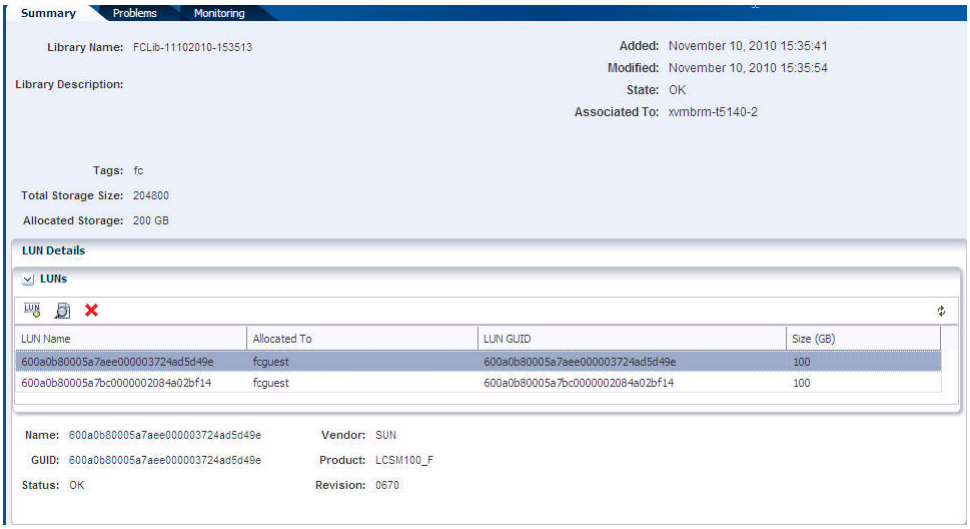
You can display the contents of a Fibre Channel storage library, its association, and details about the LUNs in the library. You can also see how the storage library is being monitored and any problems. You can adjust the capacity of the storage library by adding and removing LUNs.

To View the Contents of a Fibre Channel Storage Library

1. Expand Libraries pane in the Navigation pane.
2. Click Fibre Channel Storage in Storage Libraries.
3. Click one of the storage libraries.

   The details of the selected Fibre Channel library appear in the center pane.

Figure 4–8 Contents of a Fibre Channel Storage Library



The Summary tab shows information about the entire storage library:

- Total Storage Size – Size of all LUNs in the library
- Allocated Storage – Size of all LUNs in the library that are assigned to guests and zones
- State – State of the Fibre Channel library. The state of the library depends on each LUN
- Associated To – Names of the virtual pools, Oracle VM Server for SPARC, or global zones that use this library The LUN Details table lists each LUN in the Fibre Channel library. The first LUN is selected by default and shows the following information:
- LUN Name – Name of the LUN
- Allocated To – Name of the guest or zone that this LUN is allocated
- LUN GUID – Global Unique Identifier that is associated with each LUN

- Size (GB) – Size of the LUN in Gigabytes

4. From the LUNs table, you can add, edit, and delete LUNs.

To see any problems discovered by monitoring the storage library, click the Problems tab. To see how the storage library is being monitored, click the Monitoring tab.

Creating a Fibre Channel Library

When you create a Fibre Channel library, you specify the LUNs that are in the library in either of these ways:

- To Add LUNs To the Library Manually
- To Select LUNs For the Library

Before You Begin

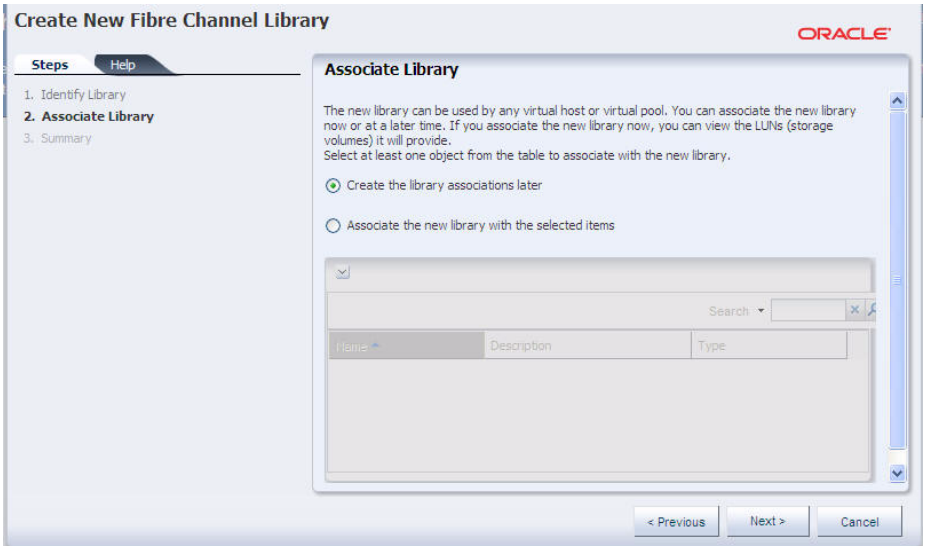
Use the vendor documentation to configure storage for Fibre Channel libraries so that LUNs are mapped to and accessible to the host. See Preparing Storage for the general procedure. If you want to identify the LUNs to add to the library, you must have the GUID or WWN for each LUN.

To Create a Fibre Channel Library

1. Expand Libraries in the Navigation pane.
2. Click Fibre Channel Storage in Storage Libraries.
3. Click New Fibre Channel Library in the Actions pane.
4. In the Identify Library pane, enter the name and description of the library. Click Next.

   The wizard presents two options for identifying the LUNs for the new library.
5. Specify LUNs.
   - To add specific LUNs to the library by name, select the Create the library associations later option.

Figure 4–9 Create New Fibre Channel Library

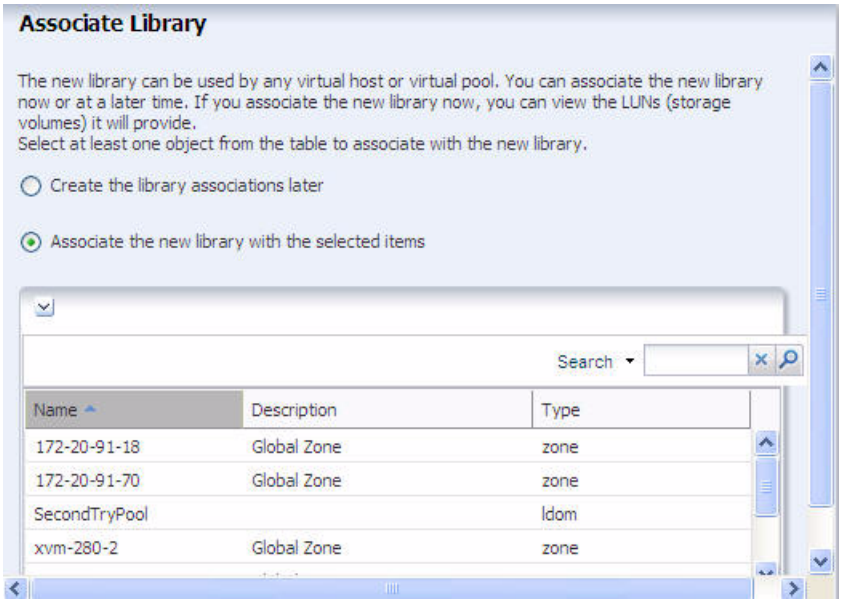


a. Click Next.

b. See the To Add LUNs To the Library Manually procedure.

- To select LUNs from a set of available LUNs, select the Associate the new library with the selected items option.

Figure 4–10 Associate Library



a. Select at least one of the virtual pools, control domains, or global zones from the table.

b. Click Next.

c. See the To Select LUNs For the Library procedure.

Adding LUNs to a Fibre Channel Library

If the Fibre Channel storage library is not associated with a virtual pool, control domain, or global zone, add storage capacity by specifying the LUNs to add by name. If the storage library is associated, you can also add LUNs by selecting them from a list of the LUNs mapped to those objects.

To Add LUNs to a Fibre Channel Library

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

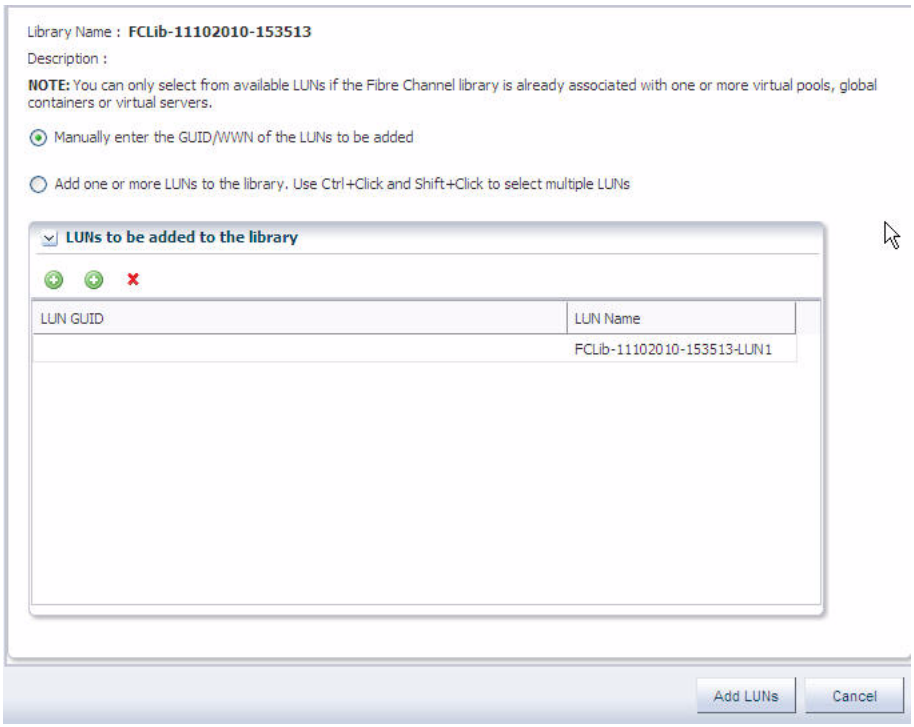
To Add LUNs To the Library Manually

You use this procedure in the following situations:

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

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

Figure 4–11 Manually Adding LUNs



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

If you are creating a new Fibre Channel storage library, you can now associate the storage library with a virtual pool, control domain, or zone.

To Select LUNs For the Library

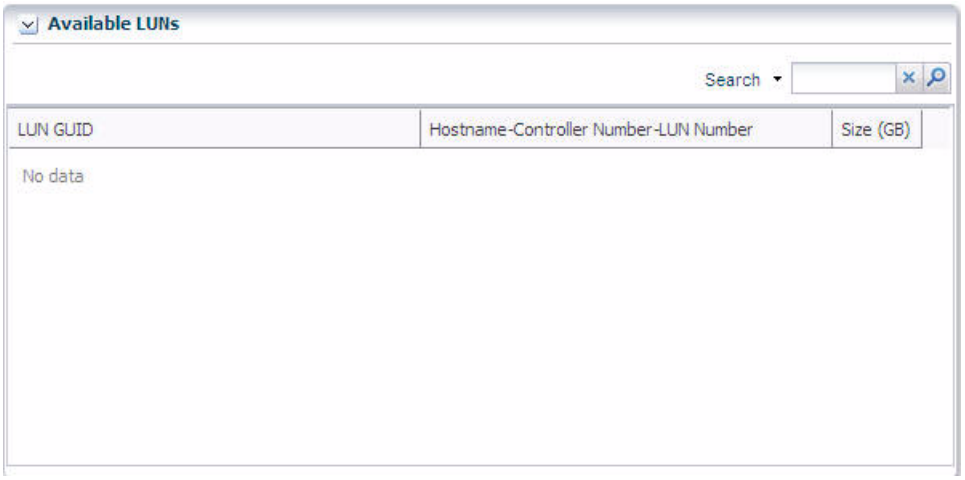
You use this procedure in the following situations:

- You are creating a new Fibre Channel storage library and have associated the new library with a virtual host or virtual pool immediately.
- You are increasing the storage capacity of an existing Fibre Channel storage library and chose to select LUNs, using the following procedure:

  1. Select the library.
  2. Click the Add LUN action.
  3. Click the Select from available LUNs option.

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

Figure 4–12 Available LUNs



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

- LUN GUID - The unique 32-digit identifier for the LUN.
- Host information for the LUN:
  - Hostname - Name or IP address of the host that can access the LUN.
  - Controller Number - The host's identifier for the HBA port, which is the physical interface to the Fibre Channel disk array.
  - LUN Number - The host's identifier for the LUN.
- Size (GB) - Size of each LUN in Gigabytes. Use the Search box to locate a specific LUN.

1. Click one or more LUNs. When you finished, click Next or Add LUN.
2. If you are adding a LUN to an existing storage library, a new job starts. If you are creating a Fibre Channel storage library, review the details of the LUNs you have configured in the Summary pane.
3. Click Finish to close the Fibre Channel library.

Viewing Local Libraries

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

To View a Virtual Host's Local Libraries

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

Editing the Attributes of a Local Library

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

To Edit a Local Library

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

Creating a Local Library

Each virtual host has a local library, located at `file: ///guests`, where all images for the guests are stored by default. In addition to the default local library, you can create other local libraries to use your storage resources efficiently or organize your images. When you create a new guest, you have the option of using the default local library or one that has been created for the virtual host.

Note: To create a local library, you specify a filesystem. This filesystem must already exist and must have read/write permissions for only the root user.

To Add a Local Library To an Virtual Asset

1. Expand Assets in the Navigation pane.

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

See About Storage Libraries for information about using libraries.

Deleting a Local Library

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

To Delete a Local Library

1. Expand Assets in the Navigation pane.
2. Select a virtual host.
3. Click the Libraries tab in the center pane. The asset's associated libraries and the guests that are stored in the libraries are listed.
4. Select the local library you want to delete. You can select more than one library.
5. Click the Delete Local Library icon.
6. In the Delete Local Library pane, verify that the library is the one you want to delete.
7. Click the Delete the libraries and their content button **Or** Click the Delete the libraries but keep the content button.

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

5

Images and Local Content

When Enterprise Manager Ops Center provisions or updates its assets, it uses images and other software that has been created or provided for those specific assets. The images and software are uploaded from a CD/DVD or from a local directory or downloaded from an Oracle or vendor site and stored in a software library.

Images

You create images within Enterprise Manager Ops Center or obtain them from a location external to Enterprise Manager Ops Center and then import or upload them into Enterprise Manager Ops Center. Enterprise Manager Ops Center manages the following categories of images:

- Firmware image - In Enterprise Manager Ops Center, a firmware image consists of the hardware's firmware and the instructions for its use such as its platform and its software dependencies. These images are stored in the Software Libraries. The following firmware types are supported:
  - Server Service Processor firmware
  - Chassis firmware
  - Storage Component firmware to update firmware on RAID Controllers, Expanders and Disks The maximum size of a firmware image is 20 MB.
- OS image – An OS image contains an entire operating system. A subset of OS images are branded images, which install an operating system that is optimized for a specific purpose and can also install applications. For example, a branded image for Oracle Solaris 9 can be installed in a nonglobal zone of a system running Oracle Solaris 10. The maximum size of an OS image is 2 GB. These images are stored in the Software Libraries.
- ISO image – The image, also called a disk image, contains uncompressed directories and files of any type. This is the image that resides on removable media. It can be an application or data or both. These images are stored in the Software Libraries. The maximum size of an ISO image that you can transfer using browser operations is 2 GB. If the image is larger than 2 GB, move the file manually to the Enterprise Controller's system and then import it.
- guest metadata – The image contains the all configuration information for a virtual host's guest, its operating system, and the applications used by a virtual host's guest. In Enterprise Manager Ops Center, the guests are either guest domains or nonglobal zones, depending on the type of virtual host. These images are stored in the Storage Libraries. ISO images and guest metadata maintain virtual hosts and guests.

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

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

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

Uploading ISO Images

To use an image for provisioning, the image must be included in one of the Enterprise Manager Ops Center's software libraries. You can upload an image or import an image, depending on where the image resides.

- If the image resides on the Enterprise Controller's system, import the image. See Importing Images.
- If the image does not reside on the Enterprise Controller's system, use the following procedure to upload the image.

  In both cases, you are moving the image from a location external to Enterprise Manager Ops Center's management into one of its libraries.
- The OS image must be in a file in the ISO format. In previous versions of Enterprise Manager Ops Center, an image could be converted to an ISO file during the upload procedure. In the current version, you must verify that the image you want to upload is an ISO file. If image is not in an ISO file, create the file. For example, on an Oracle Solaris system, use the following command collects all OS component files on the auto-mounted file system into an ISO file.

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

- The Enterprise Manager Ops Center software loads one ISO file per operation. If an ISO file spans more than one CD, combine the content on one DVD.
- The size of the ISO file containing the image must not exceed 2 GB to upload an image from the system running the browser to the system running the Enterprise Controller. If the file is larger than 2 GB, copy the file manually to a file system on the Enterprise Controller's system and then use the procedure in Importing Images.

Before You Begin

- Verify that the image and directory has the correct permissions for uploading.
- Verify that the size of the image does not exceed 2 GB.

To Upload Images

1. Expand Libraries from the Navigation pane.
2. In Software Libraries or Storage Libraries, select the library in which you want to store the image.
3. Click Upload ISO Image in the Actions pane.
4. Enter the name of the file in the Source of ISO File field or click Browse to select the image.
5. Enter the name and description of the image.
6. Click Upload Image. The progress of the upload to the Enterprise Controller is displayed. After uploading, the image is copied to the software library.

Importing Images

To use an image for provisioning, the image must be included in one of the Enterprise Manager Ops Center's software libraries. You can upload an image or import an image, depending on where the image resides.

- If the image does not reside on the Enterprise Controller's system, upload the image. See either Uploading ISO Images or Uploading Firmware Images.
- If the image resides on the Enterprise Controller's system, use the following procedure to import the image.

  In both cases, you are moving the image from a location external to Enterprise Manager Ops Center's management into one of its libraries.
- OS images cannot be imported from ISO files made from Oracle Solaris installation CDs.
- When importing a SUSE Linux Enterprise Server (SLES) 9 SP3 OS distribution from ISO files, you must perform the import procedure twice, and specify the same OS image name each time. Import the SLES 9 distribution first, and then import the SLES 9 Update 3 distribution.

Before You Begin

- Verify the location of the image you want to import. To import the image, it must reside in one of these locations:
  - A `blobs` directory, for example, if the NFS mountpoint is `server1/nfs_share/lib1`, the image must be in `server1/nfs_share/lib1/blobs` and if the EC Local Library is in `/var/opt/ec-01-OSlib`, the image must be in `/var/opt/ec-01-OSlib/blobs`.
  - A directory that the Enterprise Controller can access on either the NFS server or the Enterprise Controller.
- Verify that the size of the image does not exceed 2 GB. If the file is greater than 2 GB, move the file manually to the system that is running the Enterprise Controller and then use the procedure in Uploading ISO Images.

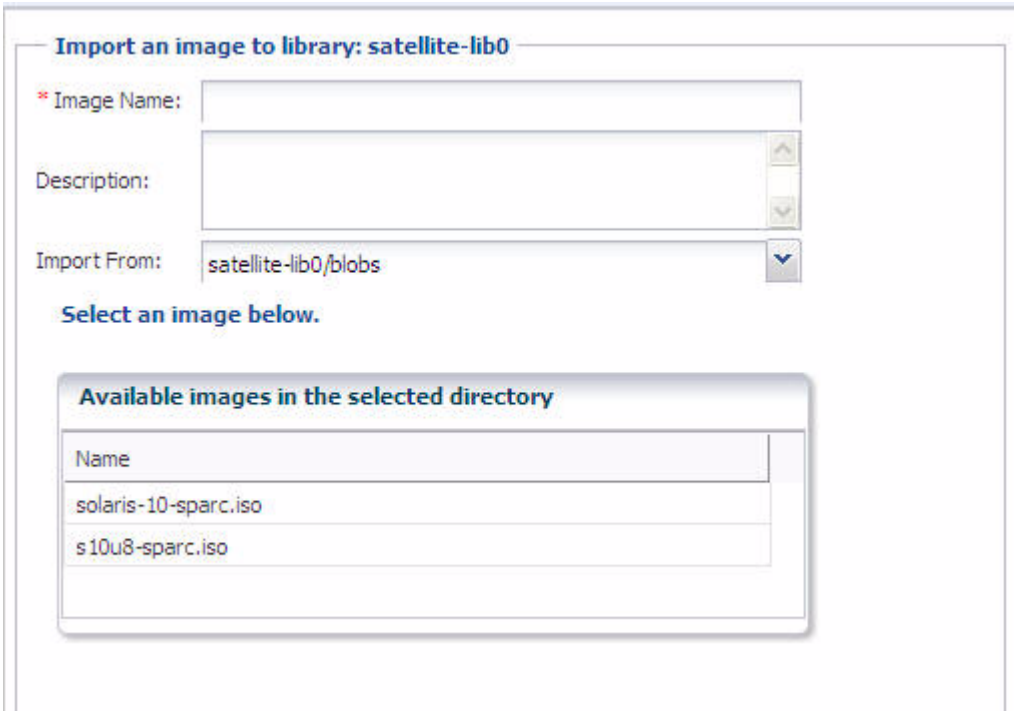
To Import Images

1. Expand Libraries in the Navigation pane.
2. Click Software Libraries or Storage Libraries to expand.
3. Click the library.

4. Click Import Image in the Actions pane.

   The Import an Image window is displayed.

Figure 5–1 Import an Image to a Library



5. Enter a name for the image and a description. Image names must be unique, can consist of up to 100 characters, and can include numbers, letters, and some special symbols. The following special symbols are prohibited: comma, asterisk, single quote, double quote, parenthesis, question mark, equal sign, and newline.
6. Specify the location of the image. All of the images in the location are displayed.
7. Select the image you want to import.
8. Click Import Image to copy the image to the library.

Moving an Image

You can move an image from one library to another library.

Before You Begin

- To move the image of a virtual host, shut down all of its guests.
- Verify that the destination library has enough free space for the image.

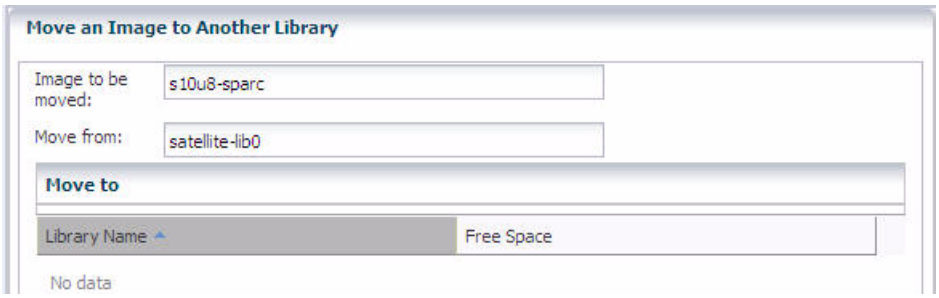
To Move an Image

1. Expand Libraries in the Navigation pane.
2. Click Software Libraries or Storage Libraries to expand.
3. Click the library. The Summary tab shows the images in the library, in a separate table for each type. The table also shows the image's size and the date it was last modified.
4. Select the image.

5. Click the Move Image icon.

   The Move an Image to Another Library window is displayed with the library and image you selected. The Move To table lists all the NAS storage libraries.

Figure 5–2 Move an Image to Another Library Window



6. Click the library to which you want to move the image, that is, the destination library.
7. Click Move Image. The image is moved from the original library to the destination library.

Viewing Image Details

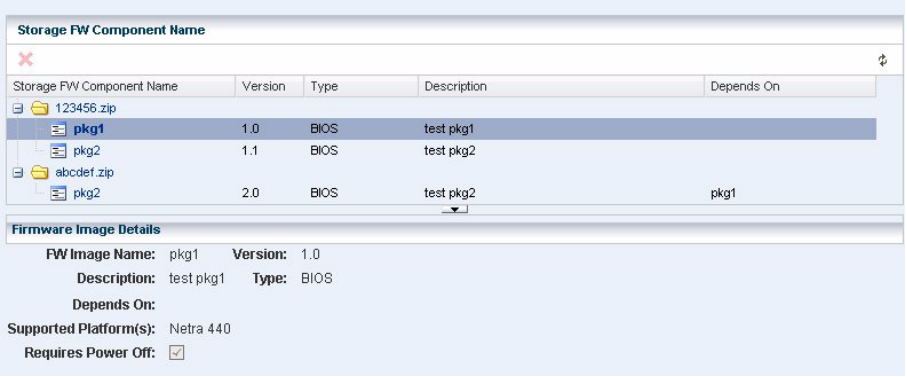
The library's Summary page lists all the images in that library by type:

- Operating system ISO image
- Logical domain
- Non-global zone
- Service Processor firmware
- Component firmware for storage devices

To View Image Details

1. Expand Libraries in the Navigation pane.
2. Click Software Libraries or Storage Libraries to expand.
3. Click the library. The Summary tab shows the images in the library, in a separate table for each type. The table also shows the image's size and the date it was last modified.
4. Select the image.
5. Click the View Image Details icon. For an ISO image, the Image Name and Description are displayed. Click the Edit icon to change them. For an LDom guest or zone guest (non-global zone), the Summary page for the virtual asset is displayed. This is the same display you see when you choose the logical domain or zone from Assets in the Navigation pane. For disk firmware, the compressed files containing the images are displayed:
   1. Click one of the compressed files to see the packages.
   2. Click a package to see the image's metadata.

Figure 5–3 Firmware Image Details



Editing Image Details

You can change the image name and description of an ISO image. For guests and non-global zones, you can change the name, description, tags, allocated memory, and its physical media.

To Edit Image Details

1. Expand Libraries in the Navigation pane.
2. Click Software Libraries or Storage Libraries to expand.
3. Click the library. The Summary tab shows the images in the library, according to type of image.
4. Select the image.
5. Click the Edit Image Details icon. For an ISO image, you can change the Image Name and Description. For guests and non-global zones, the Summary page is displayed. You can change the following fields:
   - Name
   - Description
   - Tags
   - Allocated Memory
   - CD/DVD
6. Click Submit to create the job.

Deleting Images

When you delete the image for a virtual host, its corresponding guests are also deleted.

You cannot delete an OS image that is used by an OS profile.

To Delete Images

1. Expand Libraries in the Navigation pane.
2. Click Software Libraries or Storage Libraries to expand.

3. Click the library. The Summary tab shows the images in the library, in a separate table for each type. The table also shows the image's size and the date it was last modified.
4. Select the image.
5. Click the Delete Image Details icon to delete the image.
6. Click OK to confirm the delete action.

Determining Metadata for a Firmware Image

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

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

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

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

- To determine the models supported:

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

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

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

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

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

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

Uploading Firmware Images

Firmware images are platform-specific and rely on metadata to provision and update managed assets. They reside in one of the Software or Storage Libraries.

Before You Begin

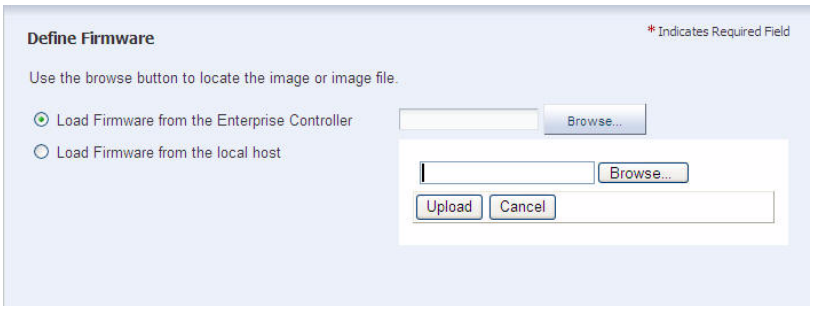
- Put the firmware images or packages on the local file system or an NFS-mounted file system that is accessible to the Enterprise Controller.
- Uncompress any compressed files to see the firmware image and its associated README file.
- Verify that the size of the image does not exceed 20 MB.
- Open the README file to identify information that you use to create the image's metadata. See Determining Metadata for a Firmware Image for instructions and an example.

To Upload a Firmware Image

1. Expand Libraries in the Navigation pane.
2. Click Software Libraries or Storage Libraries to expand.
3. Click the library.
4. Click Upload Firmware in the Actions pane.

   The Upload Firmware window is displayed.

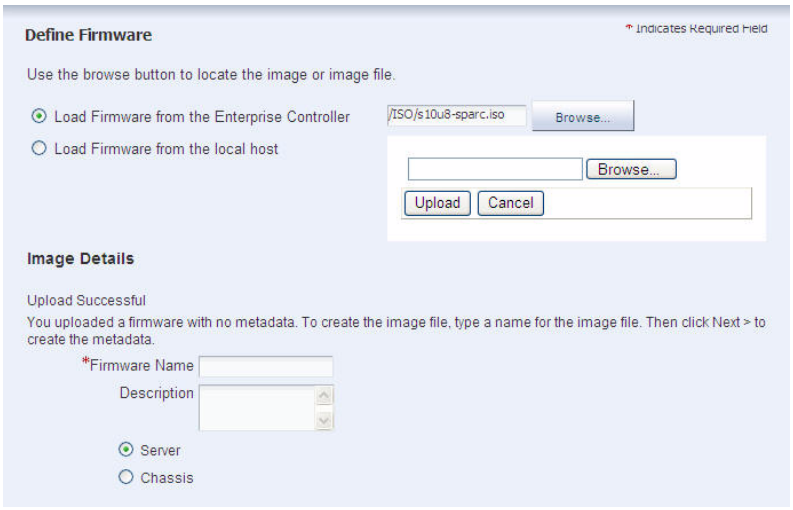
Figure 5–4 Upload Firmware Window



5. Choose the location of the firmware image and then click the Browse button to navigate to its location.
6. Select the firmware image and click the Select File button. If you are loading the firmware image from a location on the Enterprise Controller, the image is uploaded now.
7. If you are loading the firmware image from the local host, click the Upload button.
   - If you chose to upload an image file, that is, a file that contains an image and its metadata, Ops Center displays the message "Upload successful. You uploaded a firmware image with metadata." Click Next to see the Summary page.
   - If you chose to upload an image, you now provide the metadata to create the image file.

     The Upload Firmware window displays additional fields.

Figure 5–5 Upload Firmware Window



- Type a name and description for the image file and specify the type of firmware image. Then click Next.

8. Select the platforms for the firmware image. From the list of available platforms, choose at least one platform and then click the Add button. When the list of Supported Platforms is complete, click Next.
9. Specify the type and version of the firmware image. The version must match the version number of the firmware image file. For example, if you create a firmware image for the image file FFXCP1080.tar.gz, enter 1080 as the version.
10. If this image depends on other firmware images, select those firmware images from the list.
11. If this firmware's README file states that the server must be shut down before updating the Service Processor, select Power Off. If you are not certain about this requirement, select Power Off. When a firmware image has the Power Off attribute, you must stop the OS and shut down the server before you attempt to provision firmware.
12. Review the details in the Summary page and click Finish.

Downloading OS Images

Profiles that provision an OS use OS images. You must ensure that the required images are in the software library used by the profile, If not, download them from the Knowledge Base.

When Enterprise Manager Ops Center is in Disconnected mode, you cannot download OS images from the Knowledge Base. Because your local copy of the Knowledge Base does not include these images, you must obtain the images using an alternate method:

- Change to Connected mode temporarily, if this is allowed at your site, to download the images.
- Obtain the images from a system that is allowed to have Internet access and can download the images.
- Upload the images from CD/DVD.

To Download an OS Image

1. Expand Libraries in the Navigation pane.
2. Click Software Libraries or Storage Libraries to expand.
3. Click the library.
4. Click Download OS Image in the Actions pane.

   The Download OS Image wizard is displayed.
5. Select the OS image that you want to download.
6. If a license is associated with the OS image , complete the following actions:
   - Click View License to display the associated license.
   - Click Accept License and Download to start the download process. The job for the download operation is submitted.

Loading OS Images From CD or DVD

To obtain OS images from physical media, use the Bulk Upload Packages and Patches action with the following conditions:

- The OS image must be in a file in the ISO format. In previous versions of Enterprise Manager Ops Center, an OS image could be converted to an ISO file during the upload procedure. In the current version, you must verify that the CD or DVD contains an ISO file of the OS image. If image is not in an ISO file, create the file. For example, on an Oracle Solaris system, the following command collects all the OS component files on the auto-mounted file system into an ISO file.

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

  If you have access to the CD/DVD drive of the Enterprise Controller's system, you can use the same command to create the ISO file on the system. The following example creates the ISO file in the directory myimages. In this case, you do not need to use the Bulk Upload Packages and Patches action. Instead, use the procedure in Importing Images.

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

- The Enterprise Manager Ops Center software loads one ISO file per operation. If an ISO file spans more than one CD, combine the content on one DVD.
- The size of the ISO file containing the OS image must not exceed 2 GB to upload an image from the system running the browser to the system running the Enterprise Controller. If the file is larger than 2 GB, copy the file manually to a file system on the Enterprise Controller's system and then use the procedure in Importing Images.

Before You Begin

- Load the CD or DVD into the system drive and verify that the OS image on the physical medium is in ISO format, usually indicated by the file extension iso.
- Verify that the file size does not exceed 2 GB and can fit onto one CD or DVD.

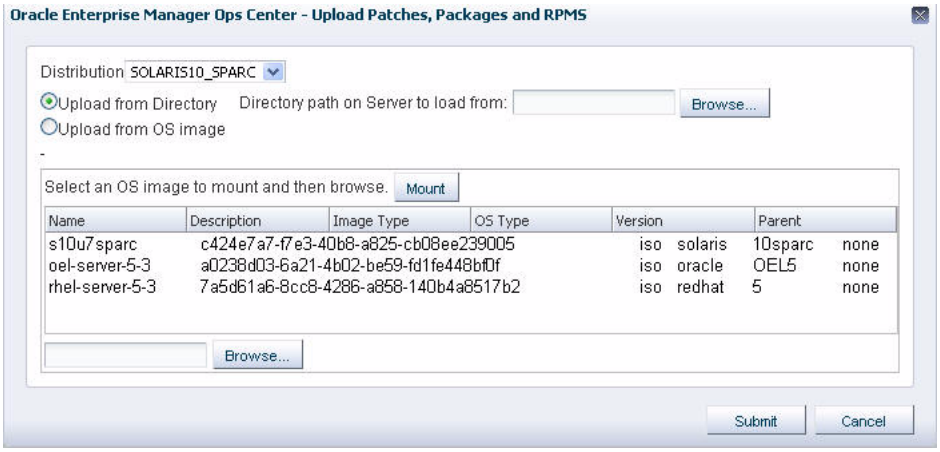
To Load an OS Image From CD or DVD

1. Load the CD or DVD into the drive of the Enterprise Controller's system.
2. Expand Libraries in the Navigation pane.

3. Click Local Content in the Solaris/Linux OS Updates library.
4. Click Bulk Upload Packages and Patches in the Actions pane.

   The Upload Patches, Packages, and RPMS window is displayed.

Figure 5–6 Upload Patches, Packages, and RPMs



5. Click Distribution to select the distribution that applies to these files.
6. Select Upload from Directory.
7. Specify the path to the OS image or directory on the CD/DVD or click Browse to locate and select it. If you specify a directory, all files in the directory and its subdirectories are uploaded. If you specify an OS image, you must mount the OS image and select the files.
   a. Click one of the OS images and click Mount.
   b. Click Browse to locate and select the files.
8. Click Submit to upload the files. The Upload Job is submitted. To use the OS images, you must import them. See Importing Images.

Local Content

In addition to packages and updates, the Updates library also stores and gives access to site-specific configuration files, and scripts. Other local content your site requires can be data files, executable files, or binary files. For example, you might develop a script to test servers before running a provisioning job.

Files in Local Content section of the Updates Library have no connection to the Knowledge Base. You upload files to the Updates library into one of the categories and then manage their life cycle. You can create subcategories under any parent category to organize the uploaded files.

In addition to the operating system and firmware images, Enterprise Manager Ops Center can be directed to use other software to manage assets. This software is site-specific and consists of configuration files and scripts that are used in deployment plans and profiles to complete an action. The content can also be files that must be included in the deployment.

See Update Profiles and Policies for more information about the Updates Library.

Viewing Component Details

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

To View Component Details

1. Expand Libraries in the Navigation pane.
2. Click Local Content in the Solaris/Linux OS Updates library. The center pane displays the standard categories of local content: Configuration files, Local packages, Macros, Pre-actions, Post-actions, and Probes.
3. Expand a category to see view its components. For the local packages category, the content is organized further by the name of the server that discovered the package, for example Agent<*hostname*>auto register, so you must also expand this subcategory.
4. Double-click the component to view information about it. Details about the component are displayed, with tabs to organize the information such as General, Incident, Dependencies, Installed, and Rules.
5. To dismiss the component details, click Close.

Uploading a Local Configuration File

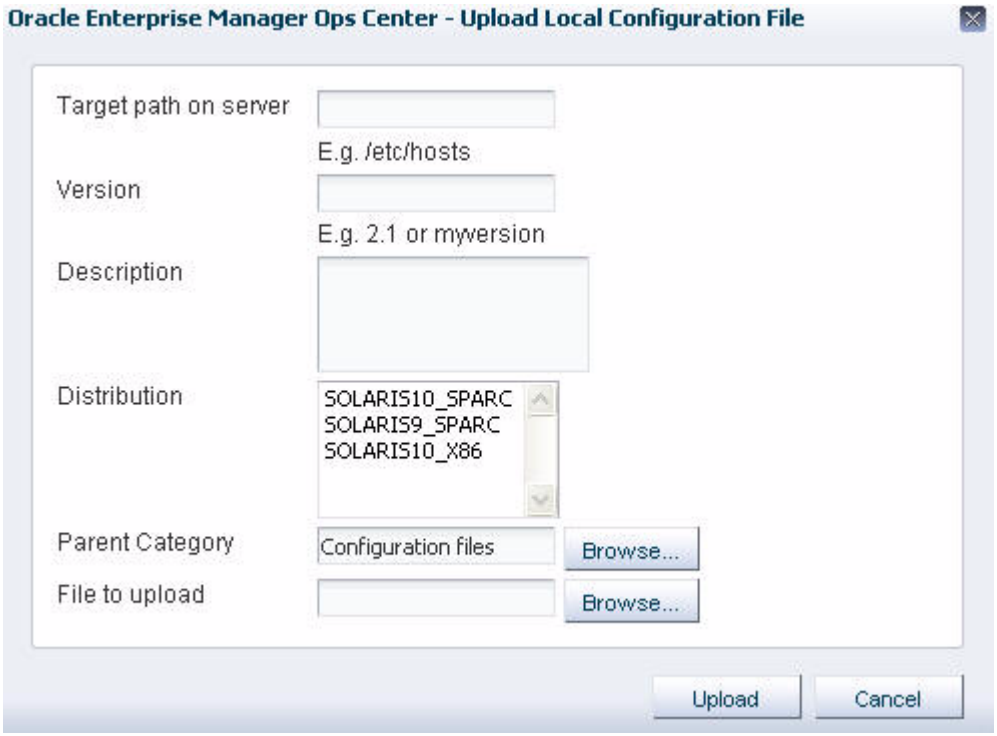
A configuration file is a text file, binary file, or non-RPM application that contains the settings and values for an asset type. A profile or deployment plan then uses the configuration file on all of the assets defined for it.

To Upload a Local Configuration File

1. Expand Libraries in the Navigation pane.
2. Click Local Content in the Solaris/Linux OS Updates library.
3. Click Upload Local Configuration File in the Actions pane.

   The Upload Local Configuration File window is displayed.

Figure 5–7 Upload Local Configuration File



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

Uploading a Local Software Package

You can upload software in the following formats:

- pkg
- rpm (for Linux RPMs)
- Package data stream and package directories
- tar
- zip
- gzip
- compress

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

Before You Begin

Verify that all extracted files are of one of the supported types.

To Upload a Local Software Package

1. Expand Libraries in the Navigation pane.
2. Click Local Content in the Solaris/Linux OS Updates library.
3. Click Upload Local Software Packages in the Actions pane.
4. Select Yes if the package is a security fix for a previous version of the software. Otherwise, select No.
5. Click the name of the distribution to which you want to add this package.
6. In Parent, click Local PKGs or click Browse to locate a subcategory.
7. In Files, click Add to see the list of files. Select at least one software package.
8. Click Upload. The software package is uploaded and listed under the Local Content.

Uploading a Local Action

An action is a script, binary file, or executable file that makes changes to a host. The following actions are available:

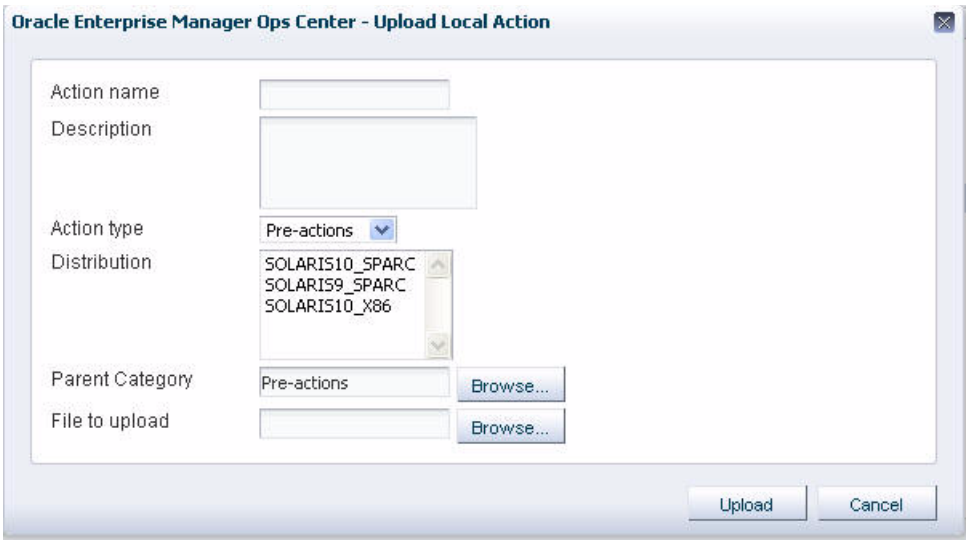
- Pre-Actions – Script that runs on a managed host before job tasks are carried out.
- Post-Actions – Script that runs on a managed host after job tasks are completed.
- Probes – Script that runs on a managed host to verify that a job task can be performed.
- Macros – Script that outputs a single line. This output replaces a macro sign in a local configuration file. The macro value is used to customize a configuration file for its host machine. The macro actions can be leveraged to deploy a single configuration file across multiple hosts by customizing the configuration file for different environments.

To Upload a Local Action

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.

   The Upload Local Action window is displayed.

Figure 5–8 Local Upload Action



4. Type a name for the action.
5. Enter text to describe the purpose of the action.
6. Select the type of action.
7. Click the name of the distribution that uses the action. The Parent field shows the category, based on the type of Action.
8. Click Browse to locate and select the file.
9. Click Upload. The file is uploaded.

Editing a Local Component File

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

To Edit Local Component Files

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

Deleting a Local Component

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

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

To Delete a Local Component File

1. Expand Libraries in the Navigation pane.
2. Click Local Content in the Solaris/Linux OS Updates library.
3. Click Delete Local Component in the Actions pane.
4. Expand the category to display the component you want to delete. To change the distribution that is displayed, click Distribution.
5. Select the component or a subcategory to delete.
6. Click Delete.

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

Adding a Local Category

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

To Add a Local Category

1. Expand Libraries in the Navigation pane.
2. Click Local Content in the Solaris/Linux OS Updates library.
3. Click Add Local Category in the Actions pane.
4. Enter a name for the new subcategory.
5. Enter a brief description for the new subcategory such as its purpose.
6. Click Distribution to assign to the subcategory.
7. Click Parent to select one of the default categories for the subcategory.
8. Click Apply. The new subcategory is created under the selected default category. You can now upload software packages and files into the new subcategory.

You cannot edit or delete one of the default categories. However, you can edit and delete a subcategory and you can delete the content in the subcategory. See Deleting a Local Component.

Uploading Local Software in Bulk

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

The files must be in the following formats:

- pkg
- rpm (for Linux RPMs)
- Package data stream and package directories
- tar
- zip
- gzip
- compress

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

Before You Begin

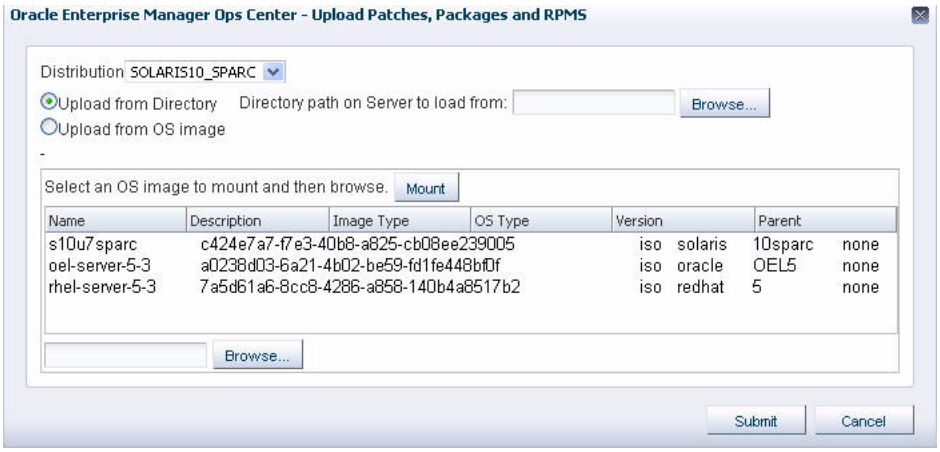
- Verify that the files have the supported file types.
- Verify that the file size does not exceed 2 GB. If the file is larger than 2 GB, copy the file manually to a file system on the Enterprise Controller's system.
- If you are uploading from removable media, insert the media.

To Upload Local Software in Bulk

1. Expand Libraries in the Navigation pane.
2. Click Local Content in the Solaris/Linux OS Updates library.
3. Click Bulk Upload Packages and Patches in the Actions pane.

   The Upload Packages, Patches, and RPMS window is displayed

Figure 5–9 Local Software Upload



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

   1. Click one of the OS images and click Mount.

2. Click Browse to locate and select the files.

7. Click Submit. The upload job is created.

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

To view the certified packages that have been uploaded, click Update Components in the Navigation pane. To view non-certified packages that have been uploaded, click Local Content in the Navigation pane.

Viewing Bulk Upload Results

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

To View Bulk Upload Results

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

Backing Up Images and Local Content

The satadm command that backs up the Enterprise Controller does not include the Storage or Software Libraries. You must back up the images manually.

To Back Up Images and Local Content

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

Uploading Software in Disconnected Mode

In Disconnected mode, all content required for provisioning and updating an OS or firmware must be uploaded manually in addition to any local content. If any required content is missing, Enterprise Manager Ops Center reports an error similar to "Not installable by current KB"

- Use the Bulk Upload Packages and Patches action, as described in Loading OS Images From CD or DVD, to move images files and other content from physical media to Enterprise Manager Ops Center's libraries.

To view the Oracle Solaris-certified packages that have been uploaded, click Update Components in the Navigation pane. To view non-certified packages that have been uploaded, click Local Content in the Navigation pane.

6

Managed Networks

The following topics are described in this chapter.

About Managed Networks

Enterprise Manager Ops Center manages networks for its virtual hosts. Guests in the network communicate with each other or with the Internet through these virtual hosts. The networks are defined only within Enterprise Manager Ops Center so you cannot manage the network connections for servers and chassis.

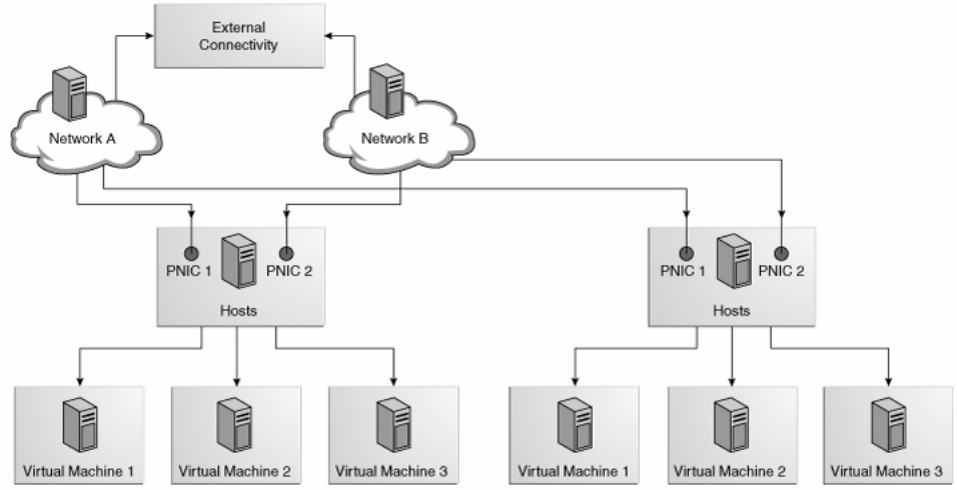
You can use networks to do the following:

- Manage individual hosts
- Connect hosts to the Proxy Controller
- Allow guests to communicate with each other or with the Internet
- Connect remote JMX with the public API

A managed network depends on the physical network interface card (PNIC) that is available the host. You can create one managed network for each physical network interface card. If one host has two PNICs, it is a good practice to create two managed networks: a management network and a data network. This configuration lets you place all the guests on the data network, keeping them separated from the management network, which gives access to internal resources of the data center.

The following configuration shows how two hosts participate in two managed networks. The actual network connection is made to the PNICs in the virtual host. Network A is connected to PNIC 1 of both hosts and Network B is connected to PNIC 2 of the hosts.

Figure 6–1 Network with Virtual Machines



See Virtual Pools and Networks for information about virtual pools and networks.

About IPMP Groups and Aggregated Links

You can create managed networks that use IPMP groups. In IPMP, two or more physical network interface cards (NIC) form an IPMP group and use the same IP Address. If one NIC fails, another NIC in the group can maintain network access. You can also create managed networks that use 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. While both methods provide high availability and load balancing, an aggregated link can also provide increased throughput if the network ports are also aggregated. You can implement both methods on the same network because they work at different layers of the network stack. See Additional Resources for links to the Oracle Solaris documentation for these services, which explains how to implement IPMP and link aggregation.

About IPMP Groups

IPMP (IP network multipathing) provides increased reliability, availability, and network performance for systems with multiple physical interfaces. It provides physical interface failure detection and transparent network access failover.

Occasionally, a physical interface or the networking hardware attached to that interface might fail or require maintenance. By using IPMP, you can configure one or more physical interfaces into an IP multipathing group, or IPMP group. After configuring IPMP, the system automatically monitors the interfaces in the IPMP group for failure. If an interface in the group fails or is removed for maintenance, IPMP automatically migrates, or fails over, the failed interface's IP addresses. The failover feature of IPMP preserves connectivity and prevents disruption of any existing connections.

You can create networks that includes IPMP groups. The association between an IPMP group and a network must be unique; an IPMP group can be associated with only one network and a network can be associated with only one IPMP group or individual NICs.

In an IPMP group, you define whether each interface is a failover or a standby one. The actions of each type differ if the current network interface fails:

- Network access changes from the failed interface to the failover interface in the IPMP group and uses the failover interface data address. You must provide the data address for an interface that is defined as failover.
- Network access changes from the failed interface to the standby interface in the IPMP group but does not change its data address. The data address of the failed interface migrates to the standby interface.

Link-based failure detection in an IPMP group is always enabled if your interface supports this type of failure detection. You can also set for probe-based failure detection by providing a test address for each interface in the group.

You can create IPMP groups while provisioning OS. You can create only one IPMP group while provisioning an OS. If you create IPMP groups manually, Enterprise Manager Ops Center identifies and displays the groups on the UI.

IPMP Groups and Global Zones

A network that has an IPMP group can be assigned to a global zone. You can assign the network to the global zone and select the IPMP group from the list of interfaces. After you finish the configuration, the network details for the global zone displays the members of IPMP group that are now associated with the network.

If you need to remove a NIC from the IPMP group, you must first verify that the global zone is not using the NIC. If the zone is using the NIC, you must stop the zone, detach the network from the zone, and then re-attach the network using a different NIC in the IPMP group. If you remove a NIC from the IPMP group while the zone is using it, the zone continues to function but the NIC is not able to communicate with the network.

Note: When Enterprise Manager Ops Center discovers and manages a brownfield zone that has a network with an IPMP group, it does not detect the IPMP group and represents the NICs individually.

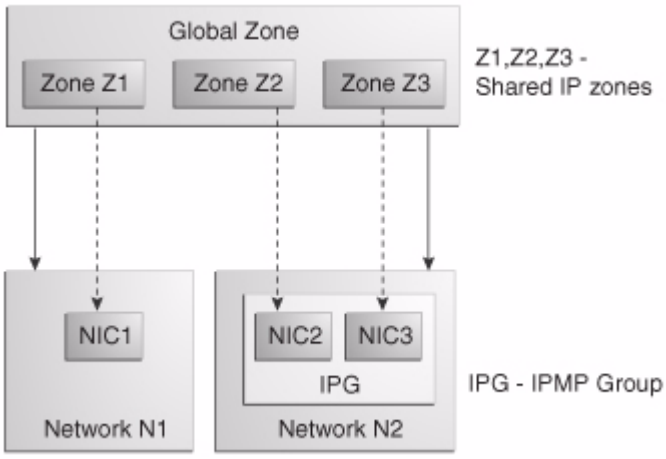
Shared IP Zones With IPMP Groups

When you create a shared IP zone on a network associated with an IPMP group, all the available interfaces of the group will be displayed on the UI except the failed and standby interfaces. The IPMP groups are not detected for shared IP zones and the available interfaces of the groups are presented directly for association. The shared IP zones use the interfaces individually and not as a group.

For example, the global zone is GZ associated with network N1 and N2 which is in shared IP mode. N2 has the IPMP group IPG. IPG consists of NIC2 and NIC3. GZ has three shared IP zones z1, z2, and z3. Zones z1, z2, and z3 are connected to the shared IP network N1 and N2. z2 and z3 can be connected through NIC2 and NIC3 of the IPMP group and zone z1 through the NIC1 of network N1.

The connection of shared IP zones to a network with IPMP groups is described in the following illustration.

Figure 6–2 Shared IP Zones



Exclusive IP Zones With IPMP Groups

For an exclusive IP zone, you can connect to a network multiple times. You can then manually define the IPMP group in the exclusive IP zone.

IPMP Groups and Oracle VM Server for SPARC

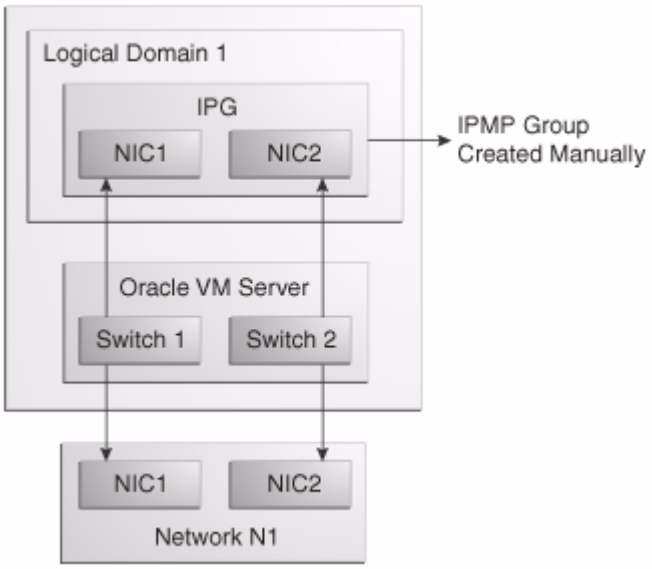
For a logical domain, you can associate a network multiple times on the same Oracle VM Server. The multiple connections are made through different switches on the Oracle VM Server. Each switch can connect to only NIC at a time.

Connecting a logical domains multiple times to a network on the same Oracle VM Server will allow to create IPMP groups in the logical domains. You can create and define the IPMP groups in the logical domains.

There is a naming pattern for the switches that are created in Oracle VM Server. If an Oracle VM Server is connected to a network, for an example network 1.1.1.0/24, the name of the virtual switches will be 1.1.1.0_24, 1.1.1.0_24_1, 1.1.1.0_24_2 and 1.1.1.0_24_3. When a network connection is made to the Oracle VM Server, the virtual switch created is incremented.

Each virtual switch created has to be connected to an interface. You can then define the IPMP groups in the logical domains with the connected interfaces to it. The network connections with IPMP group is described in the following illustration.

Figure 6–3 Network Connections with an IPMP Group



About Link Aggregation

Link aggregation is a standard defined in IEEE802.3ad. An aggregated link consists of several interfaces on a system configured as a single, logical unit. Link aggregation increases the speed and high availability of a connection between a server and a switch. The most common protocol used to manage link aggregation is LACP (Linked Aggregation Control Protocol). See Additional Resources for more information about link aggregation.

You can create a link aggregation while provisioning an OS. You can configure the interfaces together as a logical unit and define the link aggregation information if the following conditions are met:

- All the members of the aggregated link are connected to the same switch.
- The members of the aggregated link are of the same type. For example, NICs with the e1000g interface cannot be mixed with NICs that use the bge interface.
- For Oracle Solaris OS, the required driver is GLDv3.

> **Note:** You can create only one link aggregation while OS provisioning. Enterprise Manager Ops Center displays the link aggregation that are created manually

When interfaces have been aggregated, they are treated as a single network interface. Enterprise Manager Ops Center displays the link aggregation in the list of available NICs as if it were an individual interface. When you assign a network with a link aggregation to an Oracle VM Server, logical domain, global zone, or a non-global zone, select the link aggregation from the NIC list. You can view the link aggregation details on the Oracle VM Server's or global zone's Network tab.

Viewing a Managed Network's Configuration

Use the tabbed pages in the center pane to learn about a managed network.

1. Expand Managed Networks in the Navigation pane.
2. Select the network you want to view. The Dashboard page is displayed. The Summary section shows the attributes that were specified when the network was created or last modified and also includes a set of Problem icons for the network.
   - For detailed information about problems, scroll down to view the Status table.
   - For detailed information about all problems, click the Problems tab.
   - For information about what values are being monitored, click the Monitoring tab. The Membership Graph section shows the relationship of the selected network to other Ops Center assets. For detailed information about these network objects, click the Network Connections tab.
3. Click the Network Details tab. This page repeats the information in the Summary tab and also lists the static routes that have been defined for the network.
4. Click the Network Services tab to show the services that have been specified for this network. To change any services, use the procedure in Editing Network Services.
5. Click the Network Connections tab to see a table of all the virtual pools that this network is assigned to and all the guests assigned to this network.

To change some of the network information, see the procedure in Editing Network Attributes.

Viewing the Virtual Hosts and Guests Using a Network

Use the following procedure to display the guests that use a specific network.

1. Expand Managed Networks in the Navigation pane. A list of physical networks is displayed.
2. Select a network.
3. Click the Network Connections tab. A table of virtual pools is displayed with the virtual hosts in the virtual pools.
4. Expand each virtual pool and virtual host to see all the guests.

The management IP address and MAC address of each virtual host that is using the network is displayed. The IP address and MAC address of each guest that is using the network is displayed.

Virtual Pools and Networks

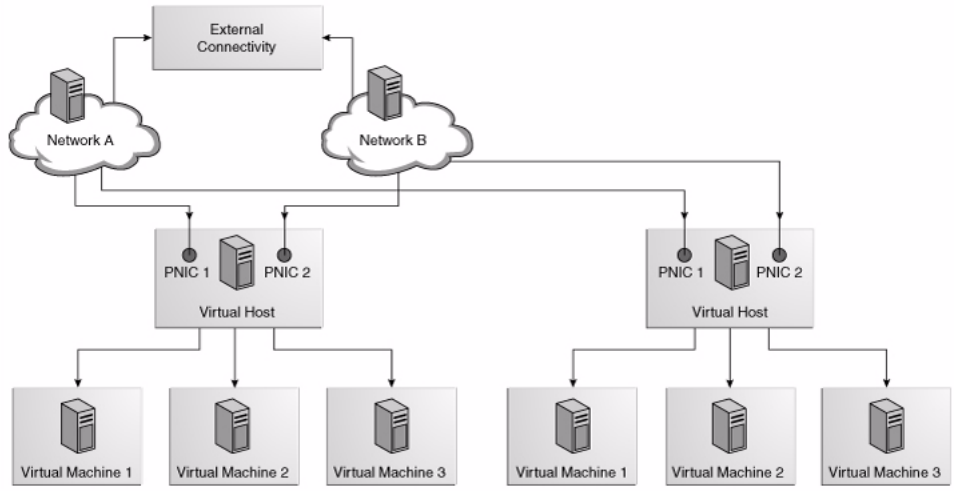
In Enterprise Manager Ops Center, networks are associated with virtual pools so even a standalone virtual host is considered a virtual pool with one member. However, most virtual pools have more than one virtual host. When you assign a network to a virtual pool, the network is accessible to all virtual hosts in the pool and every guest of each virtual host can use the network.

A virtual pool must have at least one associated network. When associate more than one network with a virtual pool, all virtual hosts in the virtual pool are associated with the same set of networks. When you add a virtual host to a virtual pool, the virtual host is configured for all the virtual pool's associated networks. The virtual host has

access to all the networks defined for the pool and can be an active member of the pool. This ensures that all guests have access to the network if you migrate a guest from one virtual host to another one within the pool.

The following figure illustrates the view for network connections to two virtual hosts in a virtual pool. This virtual pool has two virtual hosts and two network associations.

Figure 6–4 Virtual Pool



See Viewing the Virtual Hosts and Guests Using a Network.

Viewing a Virtual Pool's Networks

Use the following procedure to display the networks of the virtual hosts in a virtual pool.

To View a Virtual Pool's Networks

1. Expand Assets in the Navigation pane.
2. Expand Virtual Pools.
3. Select the virtual pool.
4. Click the Network tab. A table of the virtual hosts in the virtual pool in displayed.
5. Expand each virtual host to see all the guests.

The management IP address and MAC address of each virtual host that is using the network is displayed. The IP address and MAC address of each guest that is using the network is displayed.

Assigning a Network to a Virtual Pool

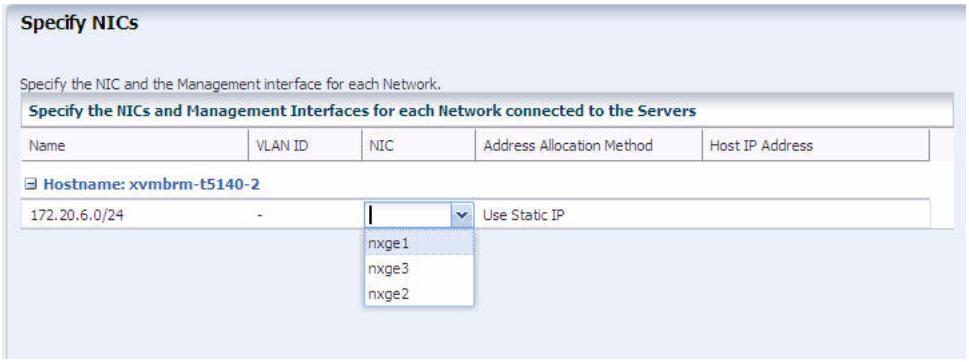
When you create a network, you use the Manage Network wizard to assign the network to virtual pools. Use this procedure to assign the network to a different virtual pool.

To assign a network to a global zone, see Assigning Networks to a Global Zone in the *Oracle Enterprise Manager Ops Center User's Guide*.

To Assign a Network to Virtual Pools

1. From the Navigation pane, click Managed Networks. A list of physical networks appear under the Managed Networks section.
2. Select a network from the list of networks.
3. Click Assign Network. The Assign Network to Virtual Pool wizard is displayed.
4. In the Select Virtual Pools step, select the virtual host or virtual pool to which you want to assign this network. Click Next.
5. In the Specify NICs screen, identify the network connection and its management interface.

Figure 6–5 Specify NICs



The NIC drop-down list displays all the available NICs and link aggregations. For each host, specify the network connection. For the Address Allocation Method, choose to use either a static IP address or an IP address assigned by DHCP.

- For a static IP address, type the IP address in the Host IP Address field.
- For a dynamic IP address, type the IP address of the DHCP server in the Host IP Address field. Click Next.

6. Review the selections that you made.
7. Click Save.

Changing the Routing Mode

A virtual host uses the network assigned to it according to the host's routing mode. You specify a virtual host's routing mode during its initial configuration if you do not accept the default mode, Automatic Routing. Enterprise Manager Ops Center supports the following routing modes:

- Automatic Routing This is the default routing mode. Applying the static routes depends on the following conditions:
  - If a default gateway or static route is defined by the user or retrieved from the DHCP server, this route is used and dynamic routing is disabled.
  - If no default gateway or static route is available, dynamic routing is enabled.
- Dynamic Routing Off The virtual host uses the default gateway and any static routes configured for the network. The default gateway is retrieved from the DHCP server.

- Dynamic Routing On The virtual host uses routes provided by the dynamic routing service. The default gateway and any static routes configured for the network are ignored.

To Change the Routing Mode of a Virtual Host

1. From the Assets pane, select Virtual Pools.
2. Select the virtual pool that contains the virtual host for which you want to change the routing mode.
3. Select the Summary tab.
4. Select a virtual host from the table.
5. Click the More Actions drop-down list in the table.
6. Click Change Routing Configuration.
7. Specify the routing mode that you want to set.

Specifying the Maximum Transmission Unit (MTU)

The default size for the network's Maximum Transmission Unit (MTU) is 1500 bytes. If your network interface card is one of the following types, you can change the size of the MTU to a size between 576 and 9216 bytes:. However, to assign the network to a logical domain, the minimum MTU size is 1500 bytes.

nxge
ixgbe
hxge
e1000g
ce
bge
ipge

When you specify a size greater than 1500 bytes, Enterprise Manager Ops Center modifies the network interface card's MTU size. For other types of network interface cards, the MTU is changed when the card's driver firmware is updated to support the new MTU size. However, to change the MTU value for an IPMP group, you must edit the MTU value manually.

When you assign the network to a virtual host, complete the following tasks so that the network's MTU size takes effect.

Note: This procedure succeeds when the Oracle VM Server's switch was created using Enterprise Manager Ops Center 11 g. It is not possible to change the MTU size for a switch created with previous versions of the software.

---

1. For a network with an MTU greater than 1500 bytes that is assigned to an Oracle VM Server, change the Oracle VM Server's switch's MTU manually to accommodate the network's MTU size, using the following command:

   ```
   ldm set-vswitch mtu=<value> <vswitchname>
   ```

   For example, to change the MTU of 192.192.192.0_24 to 4000, use the following command:

   ```
   ldm set-vswitch mtu=4000 192.192.192.0_24
   ```

2. Reboot the global zone or Oracle VM Server assigned to the network. If you change the MTU of a network assigned to a logical domain, stop and restart the logical domain.

   Note: When you provision an OS, the MTU size resets to the default value. You must change the MTU again after you provision the system.

Dissociating a Network from a Virtual Pool

Use the following procedure to disconnect a network from a virtual pool.

To Dissociate a Network from a Virtual Pool

1. Select the appropriate virtual pool.
2. From the Assets pane, select Virtual Pools.
3. Select the virtual pool.
4. Click the Networks tab.
5. Select the network that you want to dissociate from the virtual pool.
6. Click the Unbind Network in the Action pane. The network is no longer assigned to the virtual pool.

Creating a Network

Use the following procedure to create a new network.

Before You Begin

You must have a physical network interface card that is not used. You can also specify a link aggregation.

The mandatory network parameters are:

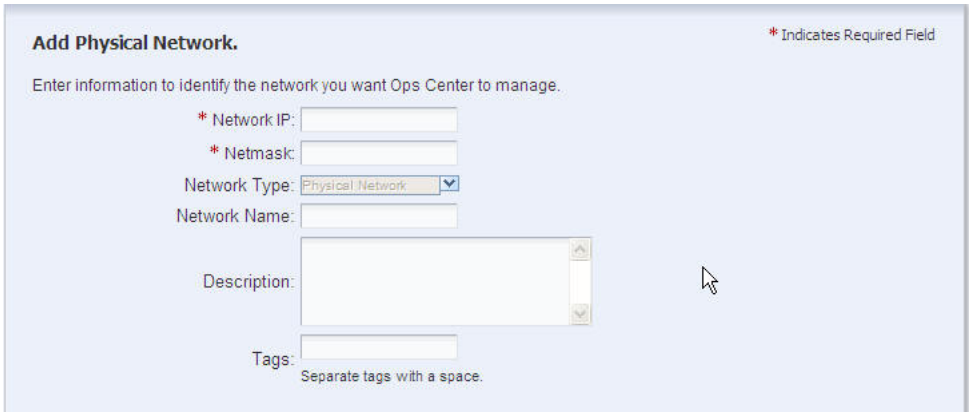
- IP address of the network
- Netmask
- If you use static IP addressing, the IP address of the management interface
- If you use dynamic IP addressing, the range of allowed IP addresses and the gateway address

To Create a Network

1. Expand Managed Networks in the Navigation pane.
2. Click Manage Network in the Actions pane. The Manage Network wizard opens.
3. In the Identify Network screen, type the IP address of the network and netmask.

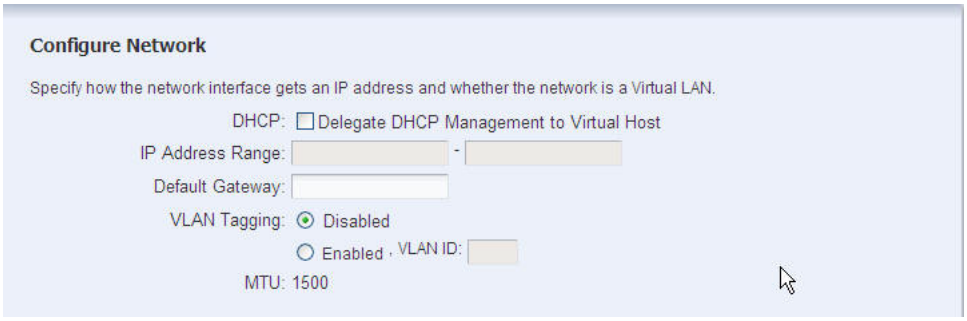
   Type the network name, description, and tags for the network. Click Next.

Figure 6–6 Adding a Network



4. In the Configure Network screen, choose whether to use a DHCP server to assign IP addresses.

Figure 6–7 Configure Network



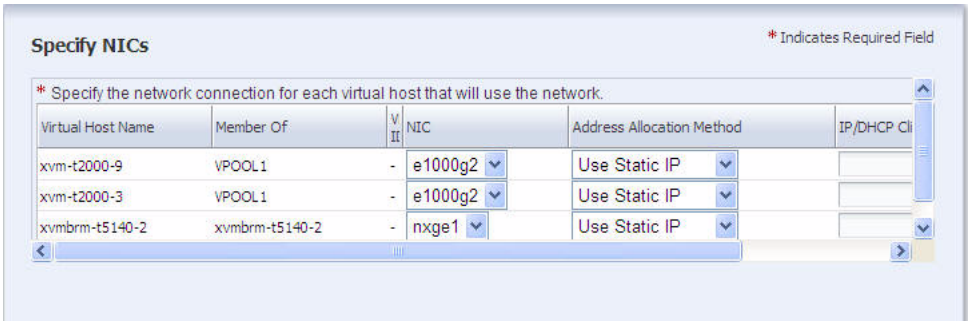
Type the range of IP addresses for the network in the Assignable IP range field. Type the default gateway address in the Default Gateway field. MTU specifies the size of the packet in bytes. The default size is 1500 bytes. Click Next.

5. In the Specify Static Routes screen, add the static routes for the network. However, the static routes and the default gateway are not used if the host uses Dynamic Routing mode. Type the destination IP, netmask, and the default gateway. If you want to add additional static routes, click Add and type the required information. Click Next.
6. In the Specify Network Service screen, specify the time server, WINS, DNS, and NIS services for the guests. This information configures the DHCP server, if DHCP support has been enabled. Type the NIS domain name before typing NIS servers. However, you can type the DNS servers without typing a DNS domain name. Click Next.
7. In the Assign Network screen, select the virtual pools or virtual hosts.

Note: Although this screen includes global zones, you cannot select them. To assign a global zone to this network, use the procedure in Assigning Networks to a Global Zone after you complete this procedure. Click Next.

8. In the Specify NICs screen, attach one or more hosts to the network.

Figure 6–8 Specify NICs



For selected virtual host, identify its network connection and its management interface.

- The NIC drop-down list displays all the available NICs and link aggregations. For each host, specify the network connection.
- For the Address Allocation Method, choose to use either a static IP address or an IP address assigned by DHCP.
- For a static IP address, type the IP address in the IP/DHCP Client ID field.
- For a dynamic IP address, type the IP address of the DHCP server in the IP/DHCP Client ID field.
- Click Next.

9. In the Summary screen, review the network specifications. Click Finish to create the new network. The new network is listed in the Managed Networks section.

When you have finished creating a network, you can assign this network to serve a virtual pool, as described in Assigning a Network to a Virtual Pool , or connect guests in the host to this network, as described in Connecting Guests to a Network.

Adding and Modifying VLAN Tags

The ability to use VLAN tags is an attribute of each managed network. Use the Edit Network Attributes action to add or change the VLAN capability.

To Edit the Network Attributes for VLAN

1. Expand Managed Networks in the Navigation pane.
2. Select a network from the list of networks.
3. Click Edit Network Attributes in the Actions pane or click the Edit icon in the center pane.
4. Click Enabled to activate VLAN tagging.

5. To add a VLAN tag, type the tag in the VLAN Tags field. Separate a series of tags with commas.

Adding a Static Route for the Network

Static routes specify the route that must be taken by the network to have external access. Although you define a default gateway for a managed network, it might not reach a particular subnet. In this case, you must also provide a static route for the subnet.

When you create a network, you can specify the static route. To add static routes after the network has been created, use the following procedure.

To Add a Static Route for the Network

1. Click Managed Networks in the Navigation pane.
2. Select a network from the list of networks.
3. Click Edit Network Attributes in the Actions pane.
4. Click the Add icon in the Static Routes table. A row is added to the table.
5. Type the values for destination IP, netmask, and gateway.
6. To modify an existing static route, click the route and change the value in the field.
7. Click Finish.

You can delete a static route and change the order of the routes using the icons in the Static Routes table.

Editing Network Attributes

The characteristics of a managed network are displayed in its Network Details tab. You can edit the network name and description, MTU size, assignable IP range, and default gateway. The network IP address, netmask, and its network type cannot be changed. You can also enable and disable DHCP service, VLAN tagging, and manage the static routes of the network. To change the MTU size, see the instructions in Specifying the Maximum Transmission Unit (MTU).

To Edit the Network Attributes

1. Expand Managed Networks in the Navigation pane.
2. Select a network from the list of networks.
3. Click Edit Network Attributes in the Actions pane.
4. Modify the values of the network attributes. Network name cannot be empty.
5. Click Finish.

If you changed the MTU value, also change the virtual host's MTU value and reboot.

Editing Network Services

The network services that a managed network provides are shown on its Network Services tab: time server, WINS, DNS, and NIS. To modify these services, edit the network services. You cannot change the network's IP address or name.

To Edit the Network Services

1. Expand Managed Networks in the Navigation pane.

2. Select a network from the list of networks.
3. Click Edit Network Services in the Actions pane. The Edit Network Services window shows the current definition of the network's services.
4. For either Time Server or WINS, enter the IP address of the server for that service. For DNS or NIS, you can edit the IP address of the current server, add an alternate server, delete a server, or change the order of the servers. Use the icons in each table to configure the network service.
5. Click Submit.

Deleting a Network

When you delete a managed network, any assigned resources such as a DHCP server are released from the network.

Note: You cannot delete the last network.

Before You Begin

Verify that the network you want to delete is not associated with any virtual pool and not connected to any guest.

To Delete a Network

1. Expand Managed Networks in the Navigation pane.
2. Select the network you want to delete.
3. Click Delete Network in the Actions pane. The Delete a Network window is displayed, showing the IP address and name of the network you selected.
4. Click Delete Network.

Connecting Guests to a Network

The guests of a virtual host can use the network that is assigned to the virtual host or to the virtual pool to which the virtual host belongs. Each guest must be connected to a network. Use this procedure to connect a disconnected logical domain.

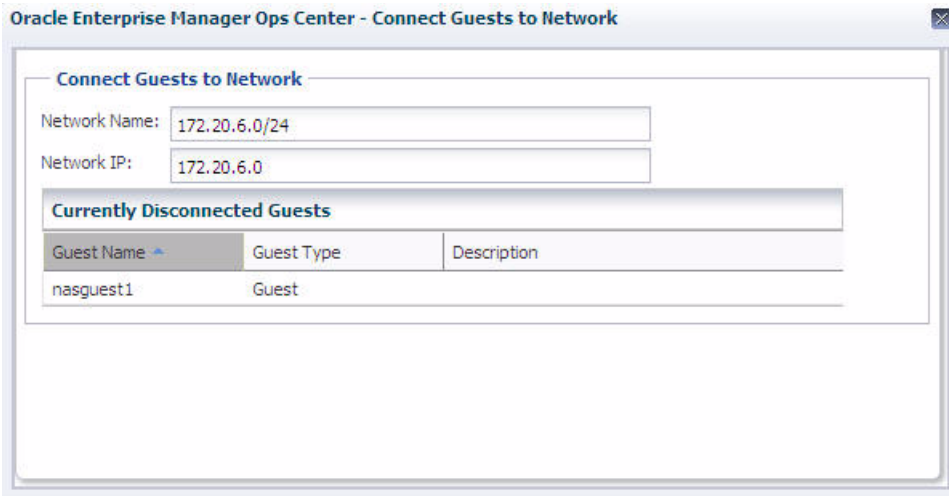
Before You Begin

Stop the guests and verify they are in **stopped** state.

To Connect Guests to a Network

1. Expand Managed Networks in the Navigation pane.
2. Select the network to which you want to connect guests.
3. Click Connect Guests in the Actions pane.
4. The Connect Guests to Network window is displayed, including a table of guests that are not connected to a network.

Figure 6–9 Connecting Guests to a Network



Note: Zone guests are not displayed in this table.

5. Select one or more guests from the table.
6. Click Connect Guests. A new connection between the guest and the network is created.
7. When the job is completed, re-start the guest.

Disconnecting a Guest From a Network

The guest you want to disconnect must be in the **stopped** state. You can disconnect a guest from a network in two ways.

To Disconnect a Guest From a Network

Use the following procedure to disconnect a guest from its network.

1. Expand Managed Networks in the Navigation pane.
2. Select a network from the list of networks.
3. Select the Network Connections tab.
4. Select the logical domain or non-global zone that you want to disconnect.
5. Click the Disconnect Guest icon. The Disconnect Guests From Network pop-up window appears.
6. Click Disconnect Guests.

   The guests that are disconnected from the network are removed from the Network Connections table of the network.

1. Expand Assets in the Navigation pane.
2. Select a logical domain or a non-global zone.
3. Select the Network tab.
4. Select a network from which you want to disconnect the guest.

5. Click the Disconnect Guest From Network icon. The Unbind a Network pop-up window appears.
6. Select the network from the pop-up window.
7. Click Disconnect From Network. The guests that are disconnected from the network are removed from the Network Connections table of the network.

7

Update Profiles and Policies

Update profiles and policies assist you in managing OS updates to your Oracle Solaris and Linux systems consistently. Update policies and procedures are not available for Windows updates.

This section discusses update profiles and policies and how the software uses them.

About Update Profiles and Policies

Profiles specify which components to install and which are not allowed, and actions to perform on a system. You use profiles to configure and maintain the systems that you want to manage.

Policies define how an update job should be performed. Policies help in automating the update jobs without user interaction, allowing you to specify which update tasks you want to be notified about and which tasks can be performed without additional confirmation.

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 should thoroughly understand your system settings and requirements.

Predefined profiles are provided to perform common system-wide checks and to automate the operating system updates. These profiles cannot be edited or deleted.

The following predefined profiles are available:

- Check Bugs Fix – Checks every bug fix patch known to the Enterprise Controller of the selected distribution to see whether the patch applies to the installed components.
- Check Security – Checks every security update known to the Enterprise Controller of the selected distribution to see whether the update applies to the installed components.
- Check System – Installs or upgrades missing dependent components according to the rules that are set in the satellite local services of the selected distribution.
- Check Withdrawn Patches – Checks all installed patches to find out whether any patches have been withdrawn. If any patches are withdrawn, the profile either upgrades to a newer patch or downgrades to a supported version.
- Local Software Review – Checks local components against the Enterprise Controller of the selected distribution. This profile helps to locate uncertified versions of software packages. If you confirm the actions of this profile, the currently installed version is replaced with a certified version.
- Perform Reboot – Restarts the selected system.
- Perform Reboot + Reconfigure – Restarts the selected system and performs specific post-installation configurations.
- Upgrade All Components – Checks all the installed components of the selected distribution to see if any of those components can be upgraded.

Creating an OS Update Profile

You must have the Admin role to create update profiles in Ops Center. An OS update job requires one profile and one policy. Profiles cannot be nested or combined, except as noted below. When the job is submitted a component called the Dependency Resolver (DR) attempts to find a series of actions that can be performed on the target which satisfy the the requirements of the Profile and any conditions imposed by the Policy.

It is important to note that a Profile is not limited to a set of actions for a single operating system; it can contain actions for one or more different operating systems, but each action is OS-specific. When the profile is applied on the target system, actions which do not apply to the target OS are disregarded without informing the user. Thus a job containing a profile which has no actions applicable to the target OS will take no action and will report a successful run.

The options associated with Update Profiles will be disabled if no distributions are activated. This can happen if you have selected not to configure the Software Update Service from the initial configuration wizard of the Enterprise Controller. Similarly, profiles can only be created for active distributions. To resolve these issues select an existing asset of the required OS type and manage it.

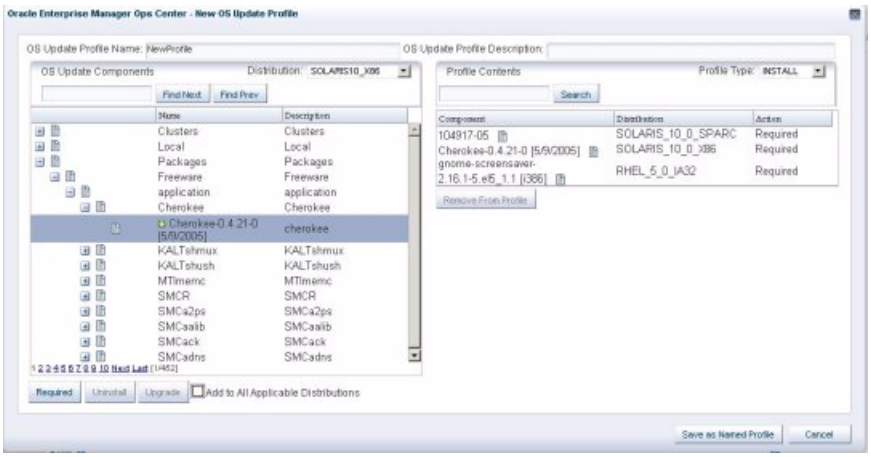
Note: The process of managing an asset and activating its distribution takes few minutes to complete.

To Create a New Profile

1. Select Plan Management from the Navigation pane.
2. Select Update Profiles from the Profiles and Policies tree.
3. Select New Profile from the Actions pane.

The New OS Update Profile window is displayed.

Figure 7–1 Create an OS Update Profile



4. Enter a profile name and brief description of the profile.
5. (Optional) Select a Profile Type. Valid types include Upgrade, Install and Script. The default type is Unknown. The profile type is simply a tag to assist when creating deployment plans.
   - Install indicates that new components to be installed
   - Upgrade indicates that existing components are upgraded
   - Script indicates that action scripts are executed.

   Note: It is possible to create profiles that do all the actions of the profile type, or to tag a profile with a type inconsistent with its actions. The tag is used for filtering the required profiles in deployment plans. See Complex Plan Management for more information.

6. For each OS that the profile applies to, select the Distribution from the drop-down list. (For example, SOLARIS10_X86)
7. Locate and select a Component from the Component tree. You can locate the component by clicking the Expand (+) icon, or by entering any part of the component name in the search. If a component cannot be found, check whether the selected Distribution is correct.
8. If required, select the check box to specify that the component should be 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.

9. 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.

10. (Optional) You can repeat the preceding actions to select multiple components for the same or different operating systems.
11. When you are finished, click Save as Named Profile. If a profile of that name exists you will be asked to confirm that it is to be replaced.

Note: You cannot replace system-defined profiles.

To Create a New Profile

As components are added to the profile, Profile Contents shows the Component Name, Distribution, and type of action. To remove a component from the list, select the component from Profile Contents list and click Remove from Profile.

The UI will not allow you to select contradicting combination of actions. For example, you cannot mark the same package as both Required and Uninstalled, or request multiple versions of the same component. However, this does not guarantee that the set of actions in the Profile has a valid solution. The UI does not check for dependencies or conflicts, this is handled by the Dependency Resolver on the target when the job is processed.

As stated earlier, profiles cannot be nested or combined. You can import the actions from another profile by selecting the profile and clicking Required. This causes the actions from the profile to be copied into the current profile. Any future edits to the profile will not affect the current profile.

For example, you can import the actions of Profile A and create another profile B. If you edit Profile A, it will not be modified in Profile B.

Editing an OS Update Profile

Check for roles and permission to edit an update profile. You must have edit permission to modify the profiles. You cannot alter the system-defined profiles.

When you change the name of the profile, a new profile is created. The existing profile is not modified for other changes and retained.

To Edit a Profile

1. Select Plan Management from the Navigation pane.
2. Select Update Profiles from the Profiles and Policies tree. The system-defined and use-defined profiles are listed in the center pane.
3. Select a profile from the user-defined profiles list.
4. Click the Edit Profile icon.
5. The Edit OS Update Profile window is displayed.
6. Edit the profile details as required. You can add or remove Components and change profile settings, such as the name, description, or type.
7. Click Save as Named Profile to save the changes made to the profile. If you changed the profile name the system will save the profile under the new name and

the old version will be unaffected. If you did not change the profile name, or changed it to match an existing profile, the system will warn you before you overwrite the existing version.

Exporting an OS Update Profile

If you have the Admin role, you can export user-defined profiles one profile at a time. System-defined profiles cannot be exported. The exported profile is in an XML-style format which can be read and copied easily. You can edit the profile with any standard text editor.

To Export an OS Update Profile

1. Select Plan Management section from the Navigation pane.
2. Select Update Profiles from the Profiles and Policies tree. The system-defined and user-defined profiles are listed in the center pane.
3. Select a user-defined profile.
4. Click the Export Profile icon in the center pane. Depending on your browser, you will get a pop-up window from which you can either open the file or save the file to a disk.
5. Click either Open or Save to disk, then click OK.

Importing an OS Update Profile

Once a profile has been exported, you can import it into a different environment. In this release, the profile might not contain any components for distributions which are not activated; attempting to do so will result in an error. (A solution is to manually edit the profile to remove any such entries). Additionally, any profile entries referring to 'NCOs', such as local content, are silently removed during the import process.

To Import an OS Update Profile

1. Select Plan Management section from the Navigation pane.
2. Select Update Profiles from the Profiles and Policies tree.
3. Click on the Import Profile icon in the center pane. An Import OS Update Profile window is displayed.
4. Enter the file name or click Browse to locate the file to be imported.
5. Click Import Profile. If the import is successful, the Edit Profile window is displayed. See Editing an OS Update Profile for more information.
6. Review the profile and make changes, as appropriate.
7. Save the profile to the database.

Note: If you do not save the profile, it is discarded.

Deleting an OS Update Profile

You can delete profiles that you have created. You cannot delete a system-defined profile or profiles created by other users.

To Delete an OS Profile

1. Select Plan Management from the Navigation pane.
2. Select Update Profiles from the Profiles and Policies tree. The system-defined and user-defined profiles are listed in the center pane.
3. Select the user-defined profile that you want to delete from the list.
4. Click the Delete Profile icon.
5. Click Yes to confirm the delete action.

Note: This marks the profile as deleted in the database; it can no longer be accessed through the UI and will not appear in the lists. Completely removing the profile, or recovering a deleted profile, is a task for a database administrator and is beyond the scope of these instructions.

Update Policies

When an OS Update job is executed, the dependency resolver examines the profile to determine what actions to take and in what order. Often there will be dependencies on other components, actions that must be performed in single user mode, a requirement to reboot the target operating system, etc. By default the user will be prompted to confirm or reject each of these steps during a question and answer exchange. The user can provide answers to the questions in advance by supplying a policy.

A policy is a list of actions that are explicitly approved or denied. They can be created by the user in advance of submitting a job; alternatively the question and answer exchange when a job is executed can be saved as a policy for future re-use.

As with profiles, policies can contain actions relating to more than one operating system. There are a number of system policies which can be used to automate the update jobs.

Policy settings are hierarchical; if there is not a policy setting for a component then 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 to Windows OS.

Creating an OS Update Policy

Policies focus on the component level. Depending on the selected distribution, OS Update Components categories may include:

- Oracle Solaris Baselines
- Packages or Software
- Patches
- Clusters
- Notifications

There is also a category of User's Policies, which allows existing policy definitions to be merged into the current policy.

You can select a single component within a category, such as the latest Oracle Solaris baseline, or an entire category. You can set the following policy actions for the selected component:

- Install
- Uninstall
- Upgrade
- Downgrade
- Apply Fix
- Ignore Conflict
- Allow Uncertified

If the selected component is a category or a package group, the setting applies to all the packages in the category or package group. Once you select the component and OS distribution, you can define the policy actions. The Policy Component and Action Settings are described below.

- Install or Uninstall
  - Ask Me – Pause the job for confirmation before installing or uninstalling the selected component.
  - Yes – Install or uninstall the selected component automatically, as required by solution.
  - No – Find a solution that does not install or uninstall the selected component.
- Upgrade from or Downgrade from
  - Ask Me – Pause the job for confirmation before changing the version of the selected component.
  - Yes – Upgrade or downgrade the selected component automatically, as required by solution.
  - No – Find a solution that does not upgrade or downgrade the selected component.
- Apply Fix
  - Ask Me – Pause the job for confirmation before fixing dependency, security, or bug issues on selected component.
  - Yes – Automatically apply the fix.
  - No – Find a solution that does not apply a fix on the selected component.
- Ignore File Conflict A file conflict will occur if the selected component provides a file that cannot be installed on a system with a file provided by another component that is already installed. If both components are certified, the rules of the knowledge base handle deployment without conflicts. If one or both are local components that are not in the knowledge base, the conflict will cause the job to fail.

> **Note:** Do not set the Ignore File Conflict setting to Yes unless you know the conflict.

- Ask Me – Pause the job for confirmation, so you see the conflict and decide at run-time whether to ignore it and continue the job, or to fail the job.
- Yes – The conflict is understood and known to be unimportant. Continue the job without pause.
- No – Find a solution that does not allow for any file conflicts.

- Allow Uncertified Allow the agent to install an uncertified Object, one that is not officially recognized by the software update service.
  - Ask Me – Pause the job for confirmation before installing the object.
  - Yes – Install the object automatically, as required by the solution.
  - No – Look for a solution that does not depend on the uncertified object.

If a policy has the Ask Me action, the job pauses for confirmation before continuing. The user will receive a notification that there is a job waiting for an answer. Click Jobs to view the job status. If a job is paused, the Waiting User Input icon appears in the status column. Click the icon to answer the questions.

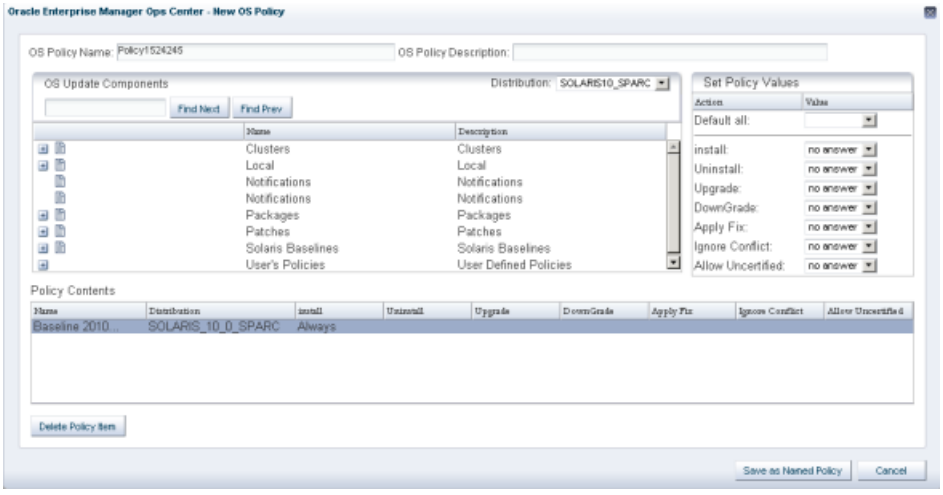
To Create an OS Update Policy

This procedure enables you to create an OS policy that you can use in update jobs. All user roles can create an OS Policy. Other users see the policies as read-only and can use or copy your policies, but they cannot edit or delete them.

1. Select Plan Management section from the Navigation pane.
2. Select Update Policies from the Profiles and Policies tree. A list of existing policies is displayed in the Summary tab.
3. Click New Policy in the Actions pane or click New Policy icon in the Summary tab.

   The New OS Policy window is displayed.

Figure 7–2 Create an OS Update Policy



4. A default policy name is provided. Edit the policy name and add a brief OS Policy Description.
5. Select the distribution from which you want to select a component.

6. Select a category or component. Expand a category to display the available components.
7. Click on the component for which you want to specify policy values
8. Set the policy values for each action. Once an action has been set for a component that component will appear in the Policy Contents area.
9. Repeat for additional components.
10. Click Save as Named Policy. The policy appears in the OS Update Policies Summary page.

> **Note:** It is important to know that policy value changes apply to the component currently selected in the component tree. To make additional changes to a component, it is necessary to find that component in the tree again. Selecting the entry under Policy Contents has no effect.

Editing an OS Update Policy

You can edit the user-defined policies that you have created. You have read-only option for policies created by other users.

To Edit an OS Update Policy

1. Select Plan Management section from the Navigation pane.
2. Select Update Policies from the Profiles and Policies tree. A list of policies is displayed in the center pane.
3. Select a policy from the user-defined policies list.
4. Click the Edit Policy icon in the center pane. The Edit OS Policy window is displayed. You can change the name, description, and policy settings.
5. Click Save as Named Policy to save the changes. If you changed the policy name the system will save the policy under the new name and the old version will be unaffected. If you did not change the policy name, or changed it to match an existing policy, the system will warn you before you overwrite the existing version.

Exporting an OS Update Policy

You can export only the user-defined policies, not the system-defined policies. You can export policies one at a time. The exported policy is in an XML-style format which can be read and copied easily. It can also be edited with any standard text editor.

To Export an OS Update Policy

1. Select Plan Management section from the Navigation pane.
2. Select Update Policies from the Profiles and Policies tree.
3. Select a policy from the user-defined policies table in the center pane.
4. Click the Export Policy icon in the center pane. Depending on your browser, you will get a pop-up window from which you can either open the file or save the file to a disk.
5. Click either Open or Save to disk, then click OK.

Importing an OS Update Policy

A policy that has been exported can be imported into a different environment. Unlike Profiles, the policy might contain components for distributions which are not activated; however the UI will be unable to display these correctly. They will appear as "System Policy Item" and the Distribution will appear as "Unknown". You can delete them, but you cannot edit them. Additionally, any policy entries referring to NCO, such as local content, are silently removed during the import process.

To Import an OS Update Policy

1. Select Plan Management section from the Navigation pane.
2. Select Update Policies from Profiles and Policies tree.
3. Click on the Import Policy icon in the center pane. An Import OS Update Policy window is displayed.
4. Enter the file name or click Browse to locate the file to be imported.
5. Click Import Policy.

If the import is successful, the Edit Policy window is displayed. You can review the policy, making changes as appropriate, before saving it to the database.

Note: If you do not save the policy, it will be discarded.

Deleting an OS Update Policy

You can delete the policies that you have created. You cannot delete the policies created by other users.

Note: This marks the policy as deleted in the database. It can no longer be accessed through the UI and will not appear in the lists. Completely removing the policy, or recovering a deleted policy, is a task for a database administrator and is beyond the scope of these instructions.

To Delete an OS Update Policy

1. Select Plan Management section from the Navigation pane.
2. Select Update Policies from the Profiles and Policies tree. A list of policies is displayed in the center pane.
3. Select a policy from the user-defined policies list.
4. Click the Delete Policy icon.
5. Click Yes to confirm the delete action.

Example – Solaris Update Profile and Policy

This example describes to create an update profile for a Solaris Baselines and update policy for applying the Solaris baselines.

If the Enterprise Controller is in disconnected mode, see the Knowledge Base and Connection Modes to obtain the latest Knowledge Base bundle.

To Create an Update Profile for Solaris Baselines

1. Select Plan Management section from the Navigation pane.
2. Select Update Profiles from the Profiles and Policies tree.
3. Choose New Profile from the Actions pane. The New OS Update Profile window displays.
4. Enter the name for the profile as Baseline09.
5. Select Solaris Baselines from the OS Update Component list.
6. Expand the list of Solaris baselines. The baselines that are released are listed according to the date of release.
7. Select the latest baseline from the list.
8. Select the Recommended set from the baseline list.
9. Click Required to add to the Profile Contents.
10. Select the Profile Type as Install to install the selected baselines.
11. Click Save as Named Profile to save the profile. The new profile will be listed in the User-defined profiles list.

To Create an Update Policy for Solaris Baselines

1. Select Plan Management section from the Navigation pane.
2. Select Update Policies from the Profiles and Policies tree.
3. Choose New Policy from the Actions pane. The New OS Policy window displays.
4. Enter the name for the policy as Baseline09Policy.
5. Select Solaris Baselines from the OS Update Component list.
6. Expand the list of Solaris baselines. The released baselines are listed according to the date of release.
7. Select the latest baseline from the list.
8. Select the Recommended set from the baseline list.
9. Select the following policy values for the actions:
   - Install – Always
   - Uninstall – Never
   - Upgrade – Always
   - Downgrade – Never
   - Apply Fix – no answer
   - Ignore Conflict – Ask
   - Allow Uncertified – Never
10. Click Save as Named Policy to save the policy. The new policy will be listed in the User-defined policies list.

8

Hardware and Provisioning Profiles

Deployment starts from configuring the hardware, installing the correct firmware, provisioning the OS, and applying the required patches. Enterprise Manager Ops Center deploys assets using deployment plans and the profiles that are included in the plans.

The following topics are covered in this section:

About Hardware and Provisioning Profiles

See Update Profiles and Creating a Software Deployment Plan for information about profiles that update software.

The work flow of an asset deployment can be captured and enacted in a highly repeatable fashion using deployment plans and the profiles included in the plans. 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.

The deployment is not only for servers with an OS installed but also for chassis, M-Series servers, and Oracle VM Server. The server deployment provides provisioning and updating operating systems, creating and provisioning logical domains.

Use hardware resource profiles to configure, install, or update systems. Use provisioning profiles to install an OS on physical or virtual servers. By applying the profile to multiple targets, you install the OS on multiple systems simultaneously. The profile contains all the attributes required for OS provisioning.

You can create profiles for different types of targets:

- Oracle Solaris SPARC
- Oracle Solaris x86
- Oracle Linux

- SUSE Linux
- Oracle VM Server and its logical domains Although the profile defines the configuration parameters, the binding of the resources such as network and storage occur when you apply the profile.

See Managing Profiles for information about viewing and creating profiles.

Hardware Resource Profiles

The Enterprise Manager Ops Center software provides the following hardware profiles:

- Service Processor – You can configure Service Processors, Chassis, and Dynamic System Domains.
- RAID Controller – You can configure and update the hardware devices that can done only through the host OS. This profile provisions a reduced OS image along with the management pack on the target to configure RAID.
- Dynamic System Domain – You can create domains on a M-series server.

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.

- Configuring a Service Processor
- Configuring a RAID Controller
- Creating a Dynamic System Domain
- Creating a Service Processor Profile
- Creating a RAID Controller Profile
- Creating a Dynamic System Domain Profile

Configuring a Service Processor

Use a deployment plan to configure the service processor on one or more servers. You can configure only unconfigured service processors, that is, a processor in its factory default state.

Before You Begin

- Connect the server hardware in its unconfigured state.
- Use the Declare Unconfigured Asset action to include the service processor in the Enterprise Manager Ops Center environment.
- For an M-Series server, verify that a user account with platadm privilege exists on the XSCF processor and is included in the profile.
- For an M-Series server, verify that you can use ssh to log into the XSCF processor.

To Configure a Service Processor

1. Display the list of existing plans by performing one of the following:
   - Expand Plan Management, click Deployment Plans, then click Configure Service Processor. or
   - Expand the All Assets tree, select the service processor, then click Configure and Deploy Server in the Action pane. A list of existing plans is displayed. If no plans exist, create one using the procedure in Creating a Deployment Plan.

2. Select the plan you want to use. The details of the plan, including the profile it uses, are displayed. By default, the service processor are configured according to values in the profile without any interaction. The service processors of all target servers have the same password.
3. If you want to apply the plan but make some changes during the configuration, click the "Allow me to override any profile values" option. During the configuration, you can enter different values.
4. Click Apply Deployment Plan in the Actions pane. The Configure Service Processor wizard starts and displays a list of assets.
5. Select one or more servers and click Add To Target List. When you are finished, click Next. The Resource Assignment panel is displayed. At any time, you can click the Targets tab to review the selected servers.
6. Type the System Identifier, Contact, and Location. Click Next. If you selected more than one target, a list of all the targets is displayed, showing the same resource assignments for each target. Edit the resource assignments for any target that you want to identify uniquely. Click Next. The Summary page shows the values in the profile and the list of each target.
7. Review the Summary page and when you are ready to configure the service processors, click Apply. The configuration job is submitted. View the progress of the job by clicking the View Job Details icon in the Jobs pane.

Configuring a RAID Controller

Enterprise Manager Ops Center provides a default profile for configuring RAID controllers. Use this procedure to configure the RAID controller.

Note: When you re-configure an existing RAID controller, all the data on the disk is lost.

To Configure a RAID Controller

1. Expand Plan Management and click Deployment Plans.
2. Click Configure RAID. A list of existing plans is displayed. If no plans exist, create one using the procedure in Creating a Deployment Plan.
3. Select a plan.
4. Click Apply Deployment Plan in the Actions pane. The details of the plan, including the profile it uses, are displayed. By default, the RAID controller is configured according to values in the profile without any interaction.
5. If you want to apply the plan but make some changes during the configuration, click the "Allow me to override any profile values" option. During the configuration, you can enter different values.
6. Click Apply Deployment Plan in the Actions pane. The Configure RAID Controller wizard starts and displays a list of assets.
7. Select one or more servers and click Add To Target List. When you are finished, click Next. The Resource Assignment panel is displayed. At any time, you can click the Targets tab to review the selected servers.
8. Review the attributes of the RAID controller. Click Next. The Summary page shows the values in the profile and the list of targets.

9. Review the Summary page and when you are ready to configure the RAID controllers, click Apply. The configuration job is submitted. The plan configures the server's RAID controller, according to the profile. To view the progress of the job, click the View Job Details icon in the Jobs pane.

Creating a Dynamic System Domain

To create a Dynamic System Domain, you apply a deployment to an M-Series server. The plan includes the profile of the Dynamic System Domain.

To Create a Dynamic System Domain

1. Discover and manage an M-Series server.
2. Expand Plan Management and click Deployment Plans.
3. Click Create Dynamic System Domain. A list of existing plans is displayed. If no plans exist, create one using the procedure in Creating a Deployment Plan.
4. Select one of the deployment plans. The details of profiles in the plan are displayed in the center pane.
5. Click Apply Deployment Plan in the Actions pane.
6. Select the M-Series server. The plan creates the new domain, according to the profile you select. You can view the progress of the plan by clicking the View Job Details icon in the Jobs pane.

Creating a Service Processor Profile

Enterprise Manager Ops Center provides a default profile for configuring service processors. Use this procedure to create a new profile and, optionally, a deployment plan.

To Create a Service Processor Profile

1. Expand Plan Management and click Profiles and Policies.
2. Click Service Processor. A list of existing profiles is displayed.
3. Click Create Profile in the Actions pane. The Create Profile wizard starts.
4. Type a name to identify the profile. Although the maximum is 255 characters, a practical limit for display purposes is 20 characters. Type a description to explain the purpose of the profile. By default, creating a profile also creates a deployment plan with the new profile as its only step. If you prefer not to create a deployment plan from this profile at this time, click the checkbox to clear it.
5. In the Subtype field, select one of the types of service processors. If you choose the service processor for an M-Series server, you also choose the type of M-Series server. Click Next. The Specify Credentials pane is displayed.
6. Type a password for root access to the service processor and then re-enter the password to confirm. If you are configuring the service processors of M-series servers, enter the account name and password for the user account you created with platadm permissions.

Note: When you use this profile, the service processors of all target servers have this password.

7. The Specify DNS Setting pane provides the option of enabling Dynamic Name Service. To enable the service, click the Use DNS checkbox. The wizard displays fields for this service:
   - DNS Servers – Enter a comma-separated list of IP addresses for up three DNS server.
   - Search Path – Enter a comma-separated list of up to six DNS domain names.
   - Retries – Enter a value between 0 and 5 for the number of retries.
   - Timeout – Enter a value between 1-10 for the number of seconds to expire. Check the Auto DNS field, to enable auto DNS. Click Next.
8. In the Clocks and SNMP Settings pane, specify the time zone for the service processor. You have the option of also using NTP service. The default action is to use the proxy controller's date and time. To enable NTP service, click the checkbox and enter the IP address of at least one NTP server. Click Next.
9. If you are creating a configuration profile for an CMM SP or Server SP, review the Summary page. If you are creating a configuration profile for an M-series server's SP, define its network connections. Enter the IP address and netmask of the Domain to DSCP (Service Processor Communication Protocol) server. You can accept or change the displayed addresses for the active XSCFU ISN IP address, the standby XSCFU ISN IP address, and the ISN Netmask. You can choose to include the address of the duplicate LAN of the Service Processor XSCF, the LAN#1-XSCF. The primary LAN, LAN#0-XSCF, is named when the Service Processor is started. Click Next.
10. Review the Summary page and click Finish to submit the job to create the new profile. When the job is complete, the new profile and, if you chose that option, the new deployment plan are listed in the Plan Management tree. You can use the default profile or the profile that you customized to configure service processors.

Creating a RAID Controller Profile

In this procedure, you must provide identifiers for the disks in the RAID configuration or the identifier of the RAID Controller.

To Create a RAID Controller Profile

1. Expand Plan Management and click Profiles and Policies.
2. Click RAID Controller. A list of existing profiles is displayed.
3. Click Create Profile in the Actions pane. The Create Profile wizard starts.
4. Type a name to identify the profile. Although the maximum is 255 characters, a practical limit for display purposes is 20 characters. Type a description to explain the purpose of the profile. By default, creating a profile also creates a deployment plan with the new profile as its only step. If you prefer not to create a deployment plan in this way, click the checkbox to clear it. Click Next. The Specify RAID Configuration pane is displayed.
5. Type a name for the RAID volume. The minimum values for the RAID level, number of disks, and stripe size are displayed. You can accept or change these values, according to your RAID array. If you want divide the disks into subpools, enter the number of subpools, or legs, in the Legs field. Click Next.
6. In the Specify Disks pane, you identify which disks are in the RAID volume. You can either identify each disk by name or you can allow the RAID controller to use

available disks. Type either the disk names for each disk or type the identifier for the RAID controller.

7. Review the Summary page and click Finish to submit the job to create the new profile. When the job is complete, the new profile and, if you chose to create it, the new deployment plan are listed in the Plan Management tree. You can use the default profile or the profile that you customized to configure RAID controllers.

Creating a Dynamic System Domain Profile

Enterprise Manager Ops Center provides a default profile for configuring the Dynamic System Domains of a M-Series servers. Use this procedure to create a new profile and then use the new profile in a deployment plan to create a new domain.

To Create a Dynamic System Domain Profile

1. Expand Plan Management and click Profiles and Policies.
2. Click Dynamic System Domain. A list of existing profiles is displayed.
3. Click Create Profile in the Actions pane. The Create Profile wizard starts. Although the profile appears to have one step, more steps are added after you identify the new domain.
4. Type a name to identify the profile. Although the maximum is 255 characters, a practical limit for display purposes is 20 characters. Type a description to explain the purpose of the profile. By default, creating a profile also creates a deployment plan with the new profile as its only step. Click the check box to clear it and to prevent creating a new deployment plan.
5. In the Subtype field, select one of the types of M-Series server. Click Next. The Specify Dynamic System Domain Identity pane is displayed.
6. Type a name for the new domain and a description of its purpose or role. The default description is the name of this profile. You can also add one or more tags, separated by commas, to label the domain, for example "finance" or "R&D."
7. Specify how the new domain gets an identifying number, either by assigning it a number or letting the domain take the next available number. Click Next.
8. In the Select and Partition PSBs pane, specify each physical system board and each Extended System Board:
    1. For each physical system board (PSB), specify its Extended System Board (XSB) mode, either Uni to optimize performance or Quad to optimize availability.
    2. For each physical system board (PSB) that uses Uni mode, enable or disable Memory Mirroring. Click Next.
9. On the Configure Dynamic System Domain pane, accept the default role of each XSB or specify whether each XSB participates in the new domain. By default, all XSBs are in the new domain so all CPUs, memory, and PCI/O slots can be used by the domain. To exclude an XSB from the domain, click the check box to clear it.
10. By default, the new domain has power. Click to clear the check box and create the domain without power.
11. By default, the new domain can boot automatically. Click to clear the check box and create the domain with a manual boot.

12. By default, Ops Center isolates any failed component of an XSB and continues. You can choose an alternate action, either to isolate the XSB and continue, or to stop the system.
13. When you are finished specifying the new domain, click Next. The Summary page is displayed.
14. Click Finish to submit the job to create the new profile. When it is complete, the new profile and, if you chose that option, the new deployment plan are listed in the Plan Management tree. You can use the default profile or the profile that you customized to create a Dynamic System Domain.

Firmware Profiles

A firmware profile is a set of actions and values that define how to update one or more assets with one or more firmware images. A firmware profile updates assets completely and consistently. When you apply a firmware profile, Enterprise Manager Ops Center compares the versions of each firmware image specified in the profile with the versions of the existing firmware on the asset. It then takes the action you specify in the profile. At any time, use the Firmware Compliance Report to apply a firmware profile to a set of assets to see if they conform to the profile.

This section describes how to create, edit, view, and delete firmware profiles.

Configuring Firmware Updates

Enterprise Ops Center provides default profiles for configuring firmware for servers and for disk storage. Use this procedure to create a new profile and, optionally, a deployment plan and then use the new profile or plan to provision firmware.

Before You Begin

The software library must contain the images you want to select. Perform the procedure in Uploading Firmware Images to upload a file with the firmware and the associated metadata.

To Create a Firmware Profile

1. Expand Plan Management in the Navigation pane.
2. Click Profiles and Policies.
3. Click Firmware.
4. Click Create Profile in the Actions panel. The Create Profile-Firmware wizard is displayed.
5. In the Identify Profile pane, specify a profile name.
6. By default, creating a profile also creates a deployment plan with the new profile as its only step. If you prefer not to create a plan from this profile at this time, click the checkbox to clear it.
7. Choose one of the target types for the profile: Blade Chassis, Server, or Storage Components. Click Next.
8. Choose one or more policies for provisioning the firmware. During provisioning, Enterprise Manager Ops Center compares the firmware image in the profile with the firmware image on the target. If the profile has a higher version of firmware, the firmware image is installed. If the profile has the same or a lower version, Enterprise Manager Ops Center follows the policies you set:

- Force Reinstall to install the firmware if the target has firmware at the same version.
- Force Downgrade to install the firmware if the target system has firmware at a higher version.

9. Select the Reset Service Processor check box to reset the service processor before the firmware update. This option is helpful for older service processors. This action is supported only for only for servers. Click Next. The Select Firmware Images pane displays a list of firmware images that are appropriate for the type of target you selected.
10. Select one or more firmware images and click the arrow button to move them to Selected Firmware Images list. You can choose to include all of the images and then adjust the list by excluding some images. A firmware profile cannot contain two different versions of the same firmware image. When you are finished, click Next.
11. Review the details in the Summary screen, then click Finish to create a firmware profile. When the new job is complete, the new profile and, if you chose that option, the new deployment plan are listed in the Plan Management tree.

Configuring Firmware for a SPARC Enterprise M-Series Server

The procedure to update firmware on a Sun or Fujitsu SPARC Enterprise® M3000/M4000/M5000/M8000/M9000 server, referred to as SPARC Enterprise M-series servers, differs slightly from firmware provisioning on other types of systems. Create firmaware image files and profiles that are specific to one type of M-Series server, using the following procedures:

1. About the M-Series Firmware Image File
2. Uploading Firmware Images
3. About Firmware Profiles for M-Series Servers
4. Updating Firmware

Before You Begin

- Use the user account with platadm privileges. This account was created to discover the SPARC Enterprise M-series server.
- Verify that the server is in a homogeneous asset group.
- Verify that the asset group has the Admin role assigned to it.

About the M-Series Firmware Image File

The firmware image file includes the images for XSCF, XCP, and OBP. The M-Series servers do not support OpenBoot PROM (OBP) images. The naming convention for an M4000 or M5000 firmware image is:

```
{FF}XCP{VVVV}.tar.gz
```

The naming convention for an M8000 or M9000 firmware image is:

```
{DC}XCP{VVVV}.tar.gz
```

The naming convention for an M3000 firmware image is:

```
{IK}XCP{VVVV}.tar.gz
```

Use the procedure for creating a firmware image file in Uploading Firmware Images.

About Firmware Profiles for M-Series Servers

The profile must contain only the SPARC Enterprise server firmware images.

Use the procedure for provisioning firmware from a profile or plan. After updating the firmware, reboot the domains.

OS Provisioning Profiles

OS Provisioning feature installs the operating system on one or more managed systems. You can provision the following operating systems in Enterprise Manager Ops Center:

- Oracle Solaris SPARC and x86
- Oracle Linux
- SUSE Linux

The OS provisioning requirements are captured and saved as a profile. You can create customized profiles for specific target systems. Using the profile, you can install the OS on the selected target systems. You can select the following type of targets to install the OS:

- Oracle VM Server
- Oracle Linux
- SUSE Linux
- Solaris SPARC
- Solaris x86

Depending on the target system selected, the OS provisioning wizard includes the step in the wizard for defining the parameters.

Creating an OS Profile for Provisioning Oracle Solaris OS

You can create OS profiles for provisioning Oracle Solaris OS on SPARC and x86 systems. Whenever you import an OS image, a default profile is always created. You can either edit the profile or create a new profile.

Before You Begin

- Import the required OS image.
- If you want to use JET modules other than the base_config, custom, and flash modules that are installed by default, then install those additional modules on the Proxy Controllers that will use them.
- Verify that any scripts the profile uses are in a directory that the Enterprise Controller can access. Scripts can be located in a local directory of the Enterprise Controller, or in a directory that the Enterprise Controller mounts using NFS.

To Create an OS Provisioning Profile for Oracle Solaris Systems

1. Click Plan Management in the Navigation pane.
2. Select OS Provisioning in the Profiles and Policies tree. A list of existing OS profiles is displayed in the center pane.

3. Click Create Profile in the Actions pane. The Create Profile-OS Provisioning wizard is displayed.
4. Define the profile parameters:
   - Name – The name of the profile.
   - Description – A description of the profile.
   - Create a deployment plan for this profile – This option is selected by default to automatically create a plan using this profile. However, you can deselect this option if you do not want to create a plan automatically.
   - Subtype – Select Solaris SPARC or Solaris x86 as per your target system.
   - Target Type – The target types are automatically defined to SPARC or x86.
5. Click Next to define the OSP Parameters.
6. Select an OS image in the OS Image List. The images that are applicable only for SPARC or x86 are listed.
7. Select a Distribution Type from the list of types. You can select any distribution if you do not want the system to be managed by Enterprise Manager Ops Center.

   Note: Select the appropriate distribution if you want to manage the system by Enterprise Manager Ops Center because the agent can be installed only in certain distribution. Minimum requirement of end user distribution is required. Distributions that are lower than end user will require additional package dependencies to be added.

8. Select Include Custom Scripts if you want to add any scripts. Specify the scripts if you want to include custom scripts.
   - Click the Add icon to add custom scripts.
   - Enter the script location, and specify whether you want to execute it before or after the provisioning operation. The scripts should be accessible from the Enterprise Controller.
9. Click Next to specify the OS setup.
10. Specify the following OS setup parameters:
    - Language – Select a language from the list.
    - TimeZone – 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.

11. Select the Manual Net Boot option to enable manual control of network boot operations for the target system. You must select this option for a target system that does not have a service processor because Ops Center cannot remotely control the network boot process on these systems.
12. Select Automatically Manage with Oracle Enterprise Manager Ops Center to install the agent on the system and manage the system with Ops Center.

    Note: Ensure that for systems that must be managed by Ops Center, you have selected the appropriate distribution type. Otherwise, the OS provisioning job will fail.

13. Click Next to specify the JET modules and parameters.
14. Enter a comma-separated list of JET module names. Enter the names of any additional JET modules that you have installed on the Proxy Controller to perform the provisioning operations described by this profile. The base_config, custom, and flash JET modules are always installed, and do not specify them here.
15. Click the Add icon to add JET name-value pairs. The JET parameters helps to customize how this profile provisions the target systems.
16. Enter the name of the JET parameter that you want to add in the Name field.
17. Enter the value that you want to assign to the JET parameter in the Value field.
18. Click Next to define the disk partitions.
19. Specify the disk partitions and file systems that you want to create on the target system.
20. Click the Add icon to define a new partition. The root (/) and a swap file system are defined by default. For each partition that you define, provide the following information:
    - File System Type – Select a file system type, either ufs, unnamed, or swap.
    - Mount Point – Enter a directory to use as a mount point for partitions.
    - Device – Enter the rootdisk keyword and a slice value to describe a partition on the target system's boot disk, for example, rootdisk.s0, or enter the logical device name, for example, c1t0d0s0, of the partition that you want to create.
    - Size (MB) – Enter the size that you want to assign to the partition, expressed in MB. When you want to allocate the remaining unused disk space to a file system, do not enter any value for the size.

      Note: Ensure that you do not use rootdisk.s2 or slice 2 for Oracle Solaris OS. Slice 2 represents the whole disk. You can use other slices 3, 4, 5, 6, and 7

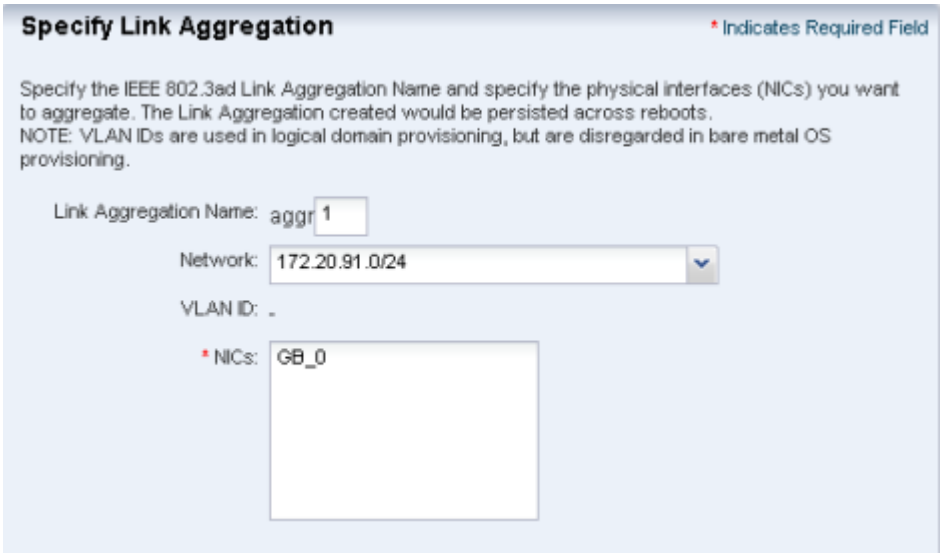
21. Click Next to specify the naming services.
22. Specify the name service, domain name and the corresponding name server. You can select the following name service:
    - DNS – Enter the domain name of the DNS server. Provide the IP address of the DNS server in the Name Server field. You can enter up to three IP addresses as the value for the Name Server. Provide the additional domains to search for name service information in the Domain Name Search List. You can specify up

to six domain names to search. The total length of each search entry cannot exceed 250 characters.

- NIS or NIS+ – Enter the domain name of the NIS or NIS+ server. If you know the NIS server details, choose the option Specify an NIS Server and provide the NIS server host name and the IP address.
- LDAP – Enter the domain name of the LDAP server. Specify the name of the LDAP Profile you want to use to configure the system. Enter the IP address of the LDAP Profile Server. You can also optionally provide the Proxy Bind Distinguished Name and Password.
- None – Select None when there is no naming service configured.

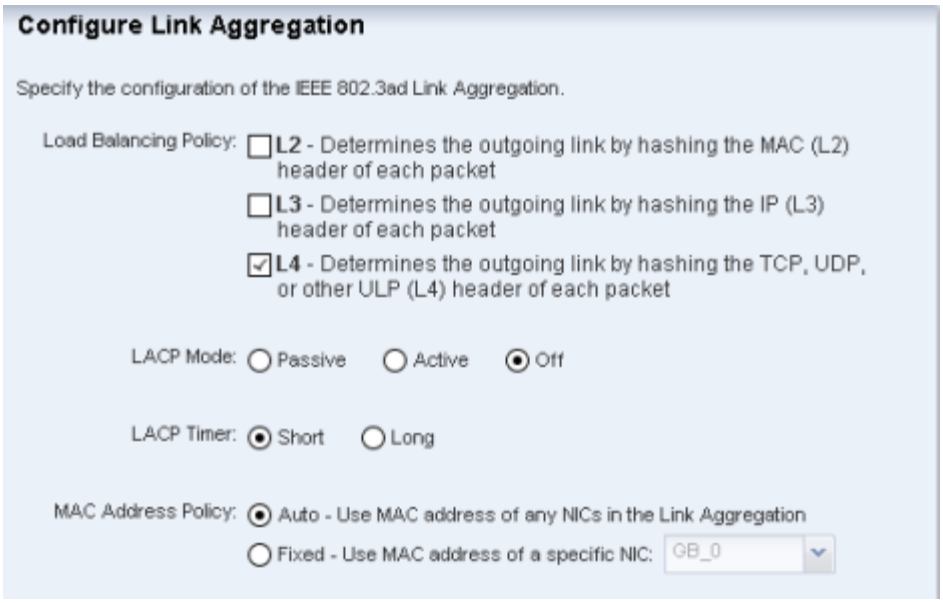
23. Click Next to specify the networking.
24. Select the network interface that the target system will use after the OS has been installed. You can define the following options for networking:
    - Use Link Aggregation
    - Use an IPMP group
    - None
25. To use link aggregation, enter the following information
    - Define the following parameters in Specify Link Aggregation:

Figure 8–1 Specify Link Aggregation



  - Link Aggregation Name – The name of the Link Aggregation is begins with aggr. Add a number to differentiate it from other aggregations.
  - Network – Select a network from the list.
  - NICs – List the physical interfaces of the selected network that must be configured as a single logical unit. Click Next to configure the link aggregation.
- Configure the IEEE 802.3ad Link Aggregation with the following parameters in Configure Link Aggregation:

Figure 8–2 Configure Link Aggregation

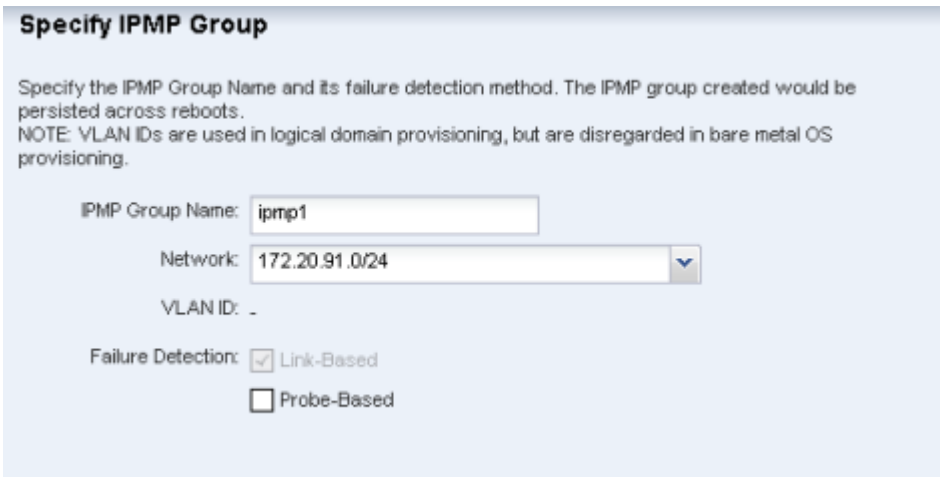


- Load Balancing Policy – Define the polidy for outgoing traffic.
- Aggregation Mode and Switches – If the aggregation topology involves connection through a switch, you must note if the switch supports the link aggregation control protocol (LACP). If the switch supports LACP, you must configure LACP for the switch and the aggregation. Define one of the modes in which LACP should operate.
- MAC Address Policy – Define whether the MAC address of the NICs are fixed or not.

26. To use IPMP, enter the following information:

- Define the following information in Specify IPMP Group:

Figure 8–3 Specify IPMP Group

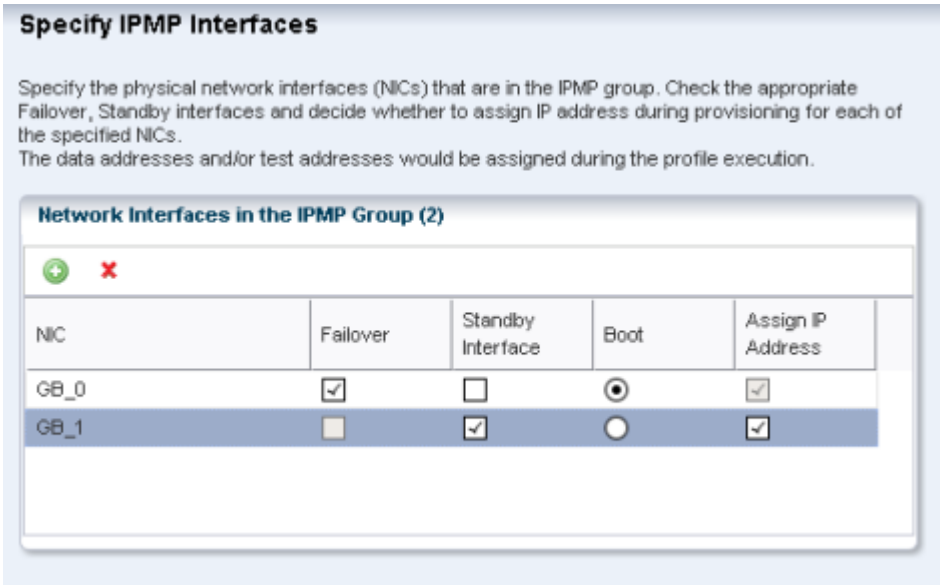


- IPMP Group Name – Provide a name for the IPMP group.

- Network – Select a network from the list.
- Failure Detection – The Link based detection is always embedded. If you want to include Probe based detection, select Probe based option. Click Next to specify the IPMP interfaces.

- Define the following information in Specify IPMP Interfaces:

Figure 8–4 Specify IPMP Interfaces



- Specify the interfaces that will be part of the IPMP group.
- Define the interfaces as Failover or Standby.
- Configure additional IP addresses for the interfaces.

Note: The data and test addresses are assigned during profile execution.

Test address is not required for probe-based failure detection.

---

27. If you have selected none for networking option, select a DHCP enabled network interface for the boot interface in Select Networks.
28. Click the Add icon to add more than one network. Select a NIC from the list of available logical interfaces for each network. Select the Address Allocation Method for the selected networks except the boot interface. All the networks that are defined in Ops Center are displayed in the Network list. If you have selected Use Static IP for Address Allocation Method then you must provide the IP address when you apply the profile. The specific IP address is assigned to the target system after provisioning.
29. Click Next to view the Summary of the parameters selected for Oracle Solaris OS provisioning.
30. Review the parameters and click Finish to save the profile. The profile is created for provisioning Oracle Solaris OS.

Creating an OS Profile for Provisioning Linux OS

You can create OS profiles for provisioning on supported Linux OS on x86 systems. Whenever you import an OS image, a default profile is always created. You can either edit the profile or create a new profile.

Before You Begin

- Import the required OS image.
- Verify that any scripts the profile uses are in a directory that the Ops Center Enterprise Controller can access. Scripts can be located in a local directory of the Enterprise Controller, or in a directory that the Enterprise Controller mounts using NFS.

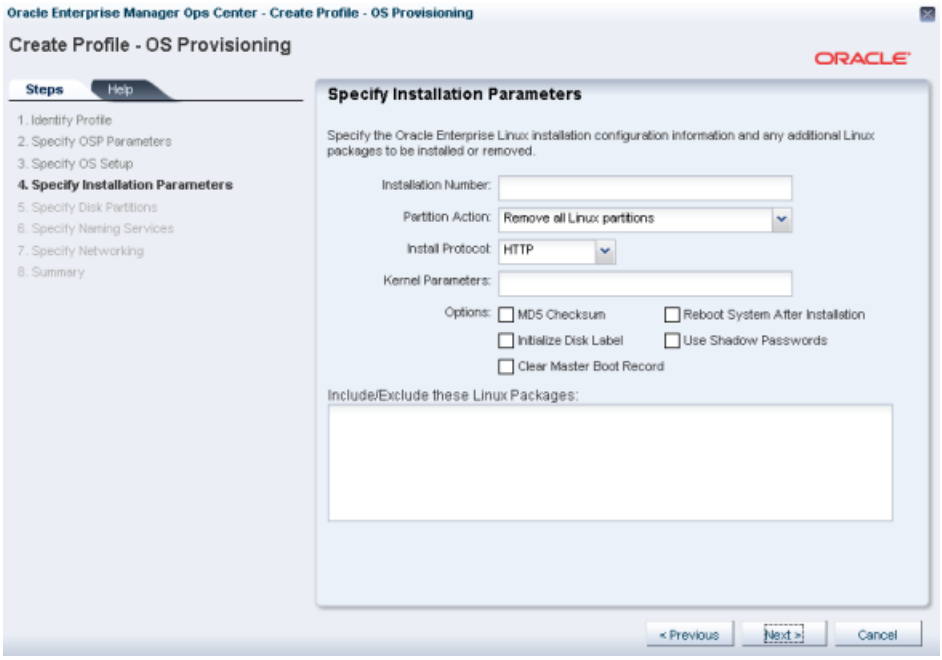
To Create an OS Provisioning Profile for Linux OS

1. Click Plan Management in the Navigation pane.
2. Select OS Provisioning in the Profiles and Policies tree. A list of existing OS profiles is displayed in the center pane.
3. Click Create Profile in the Actions pane. The Create Profile-OS Provisioning wizard is displayed.
4. Define the profile parameters:
   - **Name** - Name of the profile.
   - **Description** - The description of the profile.
   - **Create a deployment plan for this profile** - This option is selected by default to automatically create a plan using this profile. However, you can deselect this option if you do not want to create a plan automatically.
   - **Subtype** - Select the Linux release, as per your requirement.
   - **Target Type** - The target types are automatically defined to x86.
5. Click Next to define the OSP Parameters.
6. Select an OS image in the OS Image List. The images that are applicable only for the selected subtype are listed.
7. Select a Distribution Type from the list of types. You can select more than one distribution.
8. Select Include Custom Scripts if you want to add any scripts. Specify the scripts if you want to include custom scripts.
   - Click the Add icon to add custom scripts.
   - Enter the script location, and specify whether you want to execute it before or after the provisioning operation. The scripts should be accessible from the Enterprise Controller.
9. Click Next to specify the OS setup.
10. Specify the following OS setup parameters:
    - Language - Select a language from the list.
    - TimeZone - 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.
- Password - Enter the root password for the root user on systems provisioned using this profile. Re-enter the password for confirmation.

11. Select the Manual Net Boot option to enable manual control of network boot operations for the target system. You must select this option for a target system that does not have a service processor because Ops Center cannot remotely control the network boot process on these systems.
12. Select Automatically Manage with Oracle Enterprise Manager Ops Center to install the agent on the system and manage the system with Ops Center.
13. Click Next to specify the installation parameters.
14. For Oracle Linux, specify the following parameters:

Figure 8–5 Create OS Provisioning Profile



- Installation number – You can enter the installation number that is used to allow installation of all of the Linux software that is included in your subscription.
- Partition action – Select whether 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 – If necessary, enter kernel parameters for the GRUB menu of the target system.
- 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 that you want 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 (-).

15. For SUSE Linux, specify the following parameters:
    - FTP proxy server – Enter the name of the FTP proxy server to support FTP services.
    - HTTP proxy server – Enter the name of the HTTP proxy server to support HTTP services.
    - Install protocol – Specify HTTP or NFS as the install protocol.
    - Enable proxy servers – Select this option to enable the FTP and HTTP proxy servers that you specified in the FTP Proxy Server and HTTP Proxy Server fields.
    - Kernel parameters – Enter kernel parameters for the GRUB menu of the target system, if necessary.
    - Reboot action – Select whether you want to reboot the target system after OS installation.
    - Linux packages – You can specify the Linux packages that you want 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 (-).
16. Click Next to define the disk partitions.
17. Specify the disk partitions and file systems that you want to create on the target system.
18. Click the Add icon to define a new partition. The root (/) and a swap file system are defined by default. For each partition that you define, provide the following information:
    - File System Type – Select a file system type, either ufs, unnamed, or swap.
    - Mount Point – Enter a directory to use as a mount point for partitions.

- Device – Enter the rootdisk keyword and a slice value to describe a partition on the target system's boot disk, for example, rootdisk.s0, or enter the logical device name, for example, c1t0d0s0, of the partition that you want to create.
- Size (MB) – Enter the size that you want to assign to the partition, expressed in MB. When you want to allocate the remaining unused disk space to a file system, do not enter any value for the size.

19. Click Next to specify the naming services.
20. Specify the name service, domain name and the corresponding name server. You can select the following name service:
    - DNS – Enter the domain name of the DNS server. Provide the IP address of the DNS server in the Name Server field. You can enter up to three IP addresses as the value for the Name Server. Provide the additional domains to search for name service information in the Domain Name Search List. You can specify up to six domain names to search. The total length of each search entry cannot exceed 250 characters.
    - NIS or NIS+ – Enter the domain name of the NIS or NIS+ server. If you know the NIS server details, choose the option Specify an NIS Server and provide the NIS server host name and the IP address.
    - LDAP – Enter the domain name of the LDAP server. Specify the name of the LDAP Profile you want to use to configure the system. Enter the IP address of the LDAP Profile Server. You can also optionally provide the Proxy Bind Distinguished Name and Password.
    - None – Select None when there is no naming service configured.
21. Click Next to specify the networking.
22. Select the network interface that the target system will use after the OS has been installed. None is selected by default.
23. Click Next to select a DHCP enabled network interface for the boot interface.
24. Click the Add icon to add more than one network. Select a NIC from the list of available logical interfaces for each network. Select the Address Allocation Method for the selected networks except the boot interface. All the networks that are defined in Enterprise Manager Ops Center are displayed in the Network list. If you have selected Use Static IP for Address Allocation Method then you must provide the IP address when you apply the profile. The specific IP address is assigned to the target system after provisioning.
25. Click Next to view the summary of the parameters selected for Linux OS provisioning.
26. Review the parameters and click Finish to save the profile. The profile is created for provisioning Linux OS.

Creating an OS Profile for Provisioning Oracle VM Server

This section describes how to create an OS profile for Oracle VM Server. This profile is the first step towards installing the Oracle VM Server for SPARC software. In the profile, all the requirements for provisioning an Oracle VM Server such as parameters for installing an OS with the Oracle VM Server for SPARC software and resource definition for the Control Domain are all defined.

Use this profile to create a deployment plan and apply to provision the service processor with Oracle VM Server for SPARC.

Refer to Hardware and Provisioning Profiles and Deployment Plans for more information about creating profiles and plans, and applying the plans.

To Create an OS Profile for Oracle VM Server

1. Select Plan Management from the Navigation pane.
2. Select OS Provisioning option in the Profiles and Policies tree. The OS Provisioning page is displayed in the center pane.
3. Select Create Profile in the Actions pane. The Create Profile-OS Provisioning wizard is displayed.
4. In the Identify Profile step, provide the following information:
   - Enter a name for the profile.
   - Enter a description for the profile.
   - To create a deployment plan using this profile, select the option Create a deployment plan for this profile.
   - Select Oracle VM Server in the subtype to create a profile for installing Oracle VM Server for SPARC on the service processor.
5. Click Next to specify the OSP parameters.
6. Select an OS image in the OS Image List. Oracle Solaris 10 10/09 SPARC or higher versions will be populated in the image list for Oracle VM Server.
7. Select a Distribution Type from the list of types.

   Note: Minimum requirement of End User distribution is required. Distributions that are lower than End user will require additional package dependencies to be added.

8. Select Include Custom Scripts if you want to add any scripts. You will directed to Specify Scripts if you have selected Include Custom Scripts.
   - Click the Add icon to add custom scripts.
   - Enter the script location, and specify if you want to execute it before or after the provisioning operation. The scripts must be accessible from Enterprise Controller.
9. Click Next to specify the OS setup.
10. Specify the following OS setup parameters:
    - Language – Select a Language from the list.
    - TimeZone – 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.

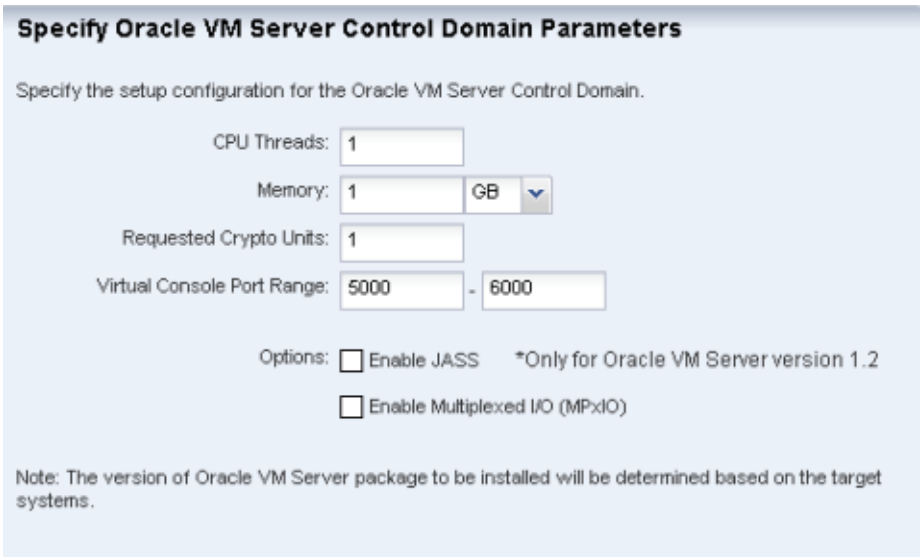
- Password – Enter the root password for the root user on systems provisioned using this profile. Re-enter the password for confirmation.

11. Select the Manual Net Boot option to enable manual control of network boot operations for the target system. You must select this option for a target system that does not have a service processor because Enterprise Manager Ops Center cannot remotely control the network boot process on these systems.
12. Select Automatically Manage with Oracle Enterprise Manager Ops Center to install an agent on the system and manage the system with Enterprise Manager Ops Center.

Note: Ensure that for systems to be managed, you have selected the appropriate Distribution Type. Otherwise, the OS provisioning job can fail.

---

13. Click Next to specify the JET modules and parameters.
14. Enter a comma-separated list of JET module names. Enter the names of any additional JET modules that you have installed on the Proxy Controller to perform the provisioning operations described by this profile. The base_config, custom, and flash JET modules are always installed, and you need not specify them here.
15. Click the Add icon to add JET name-value pairs. The JET parameters helps to customize how this profile provisions the target systems.
16. Enter the name of the JET parameter that you want to add in the Name field.
17. Enter the value that you want to assign to the JET parameter in the Value field.
18. Click Next to specify the Oracle VM Server Control Domain parameters,
19. Specify the following resources that you want to assign to the control domain:



- CPU Threads – Specify the number of CPU threads that you want to assign to the control domain. The remaining CPU threads are available for the logical domains.

- Memory – Specify the amount of memory that you want to assign to the control domain. The remaining memory is available for the logical domains.
- Requested Crypto Units – Specify the number of crypto units that you want to assign to the control domain. The remaining crypto units are available for the logical domains.
- Virtual Console Port Range – Specify the minimum port and maximum port of the virtual console of the control domain. The default port range for virtual console is 5000 to 6000.
- Enable JASS – Select this check box to harden the system by installing the SUNWjass package.

Note: JASS is not supported for Oracle VM Server for SPARC 1.3 or higher versions. This option is disregarded even if you select Enable JASS in the profile when Oracle VM Server for SPARC version 1.3 or 2.0 is being installed.

- Enable Multiplexed I/O (MPxIO) - Select this check box to enable Fibre Channel connectivity for the control domain. This action enables the Fibre Channel ports on the system that is configured for storage.

Note: The version of Oracle VM Server for SPARC to be installed depends on the target systems

Note: After the provisioning job starts, an information problem mentions the Oracle VM Server for SPARC version that is installed on the target server.

20. Click Next to define the disk partitions.
21. Specify the disk partitions and file systems that you want to create on the target system.
22. Click the Add icon to define a new partition. The root (/) and a swap file system are defined by default. For each partition that you define, provide the following information:
    - File System Type – Select a file system type, either ufs, unnamed, or swap.
    - Mount Point – Enter a directory to use as a mount point for partitions.
    - Device – Enter the rootdisk keyword and a slice value to describe a partition on the target system's boot disk, for example, rootdisk.s0, or enter the logical device name, for example, c1t0d0s0, of the partition that you want to create.
    - Size (MB) – Enter the size that you want to assign to the partition, expressed in MB. Do not enter any value for the size when you want to allocate the remaining unused disk space to a file system.
23. Click Next to specify the naming services.
24. Specify the name service, domain name and the corresponding name server. You can select the following name service:

- DNS – Enter the domain name of the DNS server. Provide the IP address of the DNS server in the Name Server field. You can enter up to three IP addresses as the value for the Name Server. Provide the additional domains to search for name service information in the Domain Name Search List. You can specify up to six domain names to search. The total length of each search entry cannot exceed 250 characters.
- NIS or NIS+ – Enter the domain name of the NIS or NIS+ server. If you know the NIS server details, choose the option Specify an NIS Server and provide the NIS server host name and the IP address.
- LDAP – Enter the domain name of the LDAP server. Specify the name of the LDAP Profile you want to use to configure the system. Enter the IP address of the LDAP Profile Server. You can also optionally provide the Proxy Bind Distinguished Name and Password.
- None – Select None when there is no naming service configured.

25. Click Next to specify the networking.
26. Select the network interface that the target system will use after the OS has been installed. You can define the following options for networking:
    - Use Link Aggregation – Go to step 28
    - Use an IPMP group – Go to step 29
    - None – Go to step 27
27. Select a DHCP enabled network interface for the boot interface. Click the Add icon to add more than one network. Select a NIC from the list of available logical interfaces for each network. Select the Address Allocation Method for the selected networks except the boot interface. All the networks that are defined in Enterprise Manager Ops Center are displayed in the Network list. If you have selected Use Static IP for Address Allocation Method then you must provide the IP address when you apply the profile. The specific IP address is assigned to the target system after provisioning.
28. You must specify and configure the Link Aggregation.
    - In the Specify Link Aggregation step, enter the following details:
      - Link Aggregation Name – The name of the Link Aggregation is already set as aggr. Add a number to it to differentiate it from other aggregation.
      - Network – Select a network from the list.
      - NICs – List out the physical interfaces of the selected network that must be configured as a single logical unit. Click Next to configure the link aggregation.
    - In the Configure Link Aggregation step, configure the IEEE 802.3ad Link Aggregation with the following parameters:
      - Load Balancing Policy - Define the policy for outgoing traffic.
      - Aggregation Mode and Switches -- If the aggregation topology involves connection through a switch, you must note whether the switch supports the link aggregation control protocol (LACP). If the switch supports LACP, you must configure LACP for the switch and the aggregation. Define one of the modes in which LACP must operate.
      - MAC Address Policy - Define whether the MAC address of the NICs are fixed or not.

29. For IPMP group, you must specify the IPMP group and interfaces.
    - In the Specify IPMP Group step, define the following information:
      - IPMP Group Name - Provide a name for the IPMP group.
      - Network - Select a network from the list.
      - Failure Detection - The Link based detection is always embedded. If you want to include Probe based detection, select Probe based option. Click Next to specify the IPMP interfaces.
    - In the Specify IPMP Interfaces step, define the following information:
      - Specify the interfaces that will be part of the IPMP group.
      - Define the interfaces as Failover or Standby.
      - Configure additional IP addresses for the interfaces.

    Note: The data and test addresses will be assigned during profile execution.

    Note: Test address is not required for probe-based failure detection.

30. Click Next to view the Summary of the parameters selected for Oracle VM Server provisioning.
31. Review the parameters and click Finish to save the profile. The profile will be created for provisioning Oracle VM Server.

See Deployment Plans and Complex Plan Management for creating a plan with this profile and apply the plan to provision the Oracle VM Server.

Creating an OS Provisioning Profile with JET Templates

You can create OS provisioning profiles with JET templates. You can create your own JET templates and use it for Oracle Solaris OS provisioning. You can use the JET templates to standardize the configurations as it provides more options for defining the jumpstart parameters.

Ensure that you place the JET template on a directory that the Enterprise Controller can access. JET templates can be located in a local directory of the Enterprise Controller, or in a directory that the Enterprise Controller mounts using NFS.

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**

You can edit the template and fill in the OS information. Save the template.

You can change the values in the JET template as required. During provisioning the OS provisioning parameters are read from the template. Ensure that you have the template on the Enterprise Manager Ops Center before provisioning.

To Create an OS Provisioning Profile with JET Templates

1. In the Navigation pane, select Plan Management section.
2. Expand Profiles and Policies and select OS Provisioning profile. The existing OS provisioning profiles are listed in the center pane.

3. In the Actions pane, select Create Profile option. The Create Profile-OS Provisioning wizard is displayed.
4. Provide a name and description for the profile.
5. The Create a deployment plan for this profile option is selected by default. If you do not want to automatically create a plan, deselect the option.
6. In the Subtype list, select JET Template.
7. Select the Target Type as OSP x86 or OSP SPARC.
8. Click Next to define the OSP parameters.
9. Select an Oracle Solaris OS image from the available ISO images list.
10. Click Browse to select the JET template location on the Enterprise Controller.
11. Select the Manual Net Boot option to enable manual control of network boot operations for the target system. You must select this option for a target system that does not have a service processor because Enterprise Manager Ops Center cannot remotely control the network boot process on these systems.
12. Select Automatically Manage with Oracle Enterprise Manager Ops Center to install an Agent on the system and manage the system with Enterprise Manager Ops Center.
13. Click Next to specify the networks for the OS.
14. Click Next to select the network interface that the target system will use after the OS has been installed. You cannot define IPMP groups or link aggregation for a JET template profile.
15. Select a DHCP enabled network interface for the boot interface.
16. Click the Add icon to add more than one network. All the networks that are defined in Enterprise Manager Ops Center are displayed in the Network list.
17. Select a NIC from the list of available logical interfaces for each network. If you have selected Use Static IP for Address Allocation Method then you need to provide the IP address when you apply a deployment plan with this profile. The specific IP address is assigned to the target system after provisioning. You can select the Address Allocation Method for the selected networks except the boot interface.
18. Click Next to view the summary of the selected profile properties.
19. Click Finish to create the profile. On a successful job completion, an OS provisioning profile will be created. Create a plan from this profile and apply it on the server to provision the OS.

See Deployment Plans and Plans for information creating and applying a deployment plan associated with this profile.

For more information about JET Templates, see Additional Resources.

Logical Domain Profiles

Logical Domain profiles captures the requirements for creating a logical domain in an Oracle VM Server. Using the profile, you can create one or more logical domains. The logical domain provisioning is not covered in this profile. The logical domain profile specification require the domain identification, CPU Threads, memory, storage and networks information.

The OS provisioning profile provides option to provision the logical domains. These profiles have to be combined together in a plan and deployed for creating and provisioning logical domains.

You can create logical domains on an Oracle VM Server using the logical domain profiles. This plan involves only creating logical domains on the Oracle VM Server. You need to apply another plan of installing the OS on the created logical domains. Otherwise, see Configure and Install Logical Domains for complete steps of creating logical domains and installing OS on the domains.

Use this plan exclusively for creating only logical domains.

This section describes how to create a logical domain profile. Using this profile, you can create one or more logical domains on an Oracle VM Server. Use this profile in a plan combined with an OS provisioning profile for a complete logical domains installation.

Before You Begin

Ensure that you have the following information before you create a profile:

- CPU and memory requirements for the logical domains.
- Storage resources.
- Network resources and number of connections for a network.

To Create a Logical Domain Profile

1. Select the Plan section from the Navigation pane.
2. Select Logical Domain from the Profile tree.
3. Click Create Profile from the Actions pane. The Create Logical Domain Profile wizard is displayed.
4. Provide a name and description to identify the profile.
5. Select Create a deployment plan for this profile to automatically create a plan using this profile.
6. Click Next and provide a name and the starting number for the logical domain. Using this profile, you can create more than one logical domain. For unique identification of the domains to be created, provide a prefix start name and starting number. For example, assume that the Start Name is TestDomain and the starting number is 10. If the number of domain creation is 3, then the logical domains will be created with the name TestDomain10, TestDomain11 and TestDomain12.
7. Click Next to configure the CPU Threads and memory. The physical CPUs of the Oracle VM Server are shared among the CPU threads of all the logical domains. Each logical domain requires:
   - At least one Gigabyte of memory.
   - At least one CPU thread. Crypto units are assigned based on CPU thread assignments. You can request the number of crypto units to be assigned to the logical domain. However, the number of crypto units assigned might be different than the amount requested because we can only allocate a crypto unit for every given number of CPU thread allocation, depending on the server hardware.When the logical domain is created, view the job notification to see the actual number of Crypto Units assigned to the logical domain. You can edit the logical domain configuration, storage, and networks.

8. Click Next to specify the library for storing the domain metadata and storage disks for the logical domain.
9. Select a library to store the logical domain metadata. You can select only the local or NAS library to store the domain metadata.
10. Select one or more libraries that form the domain storage disks. The libraries for virtual disk can be local, local device, NAS, or Fibre Channel.

> **Note:** You can define the disk size for local and NAS libraries. Whereas, you cannot define the size for local device and Fibre Channel libraries. Select a disk from the list and the size of the disk is automatically displayed.

11. Click Next to specify the networks for the domains.
12. Select at least one network from the list of networks identified by the Ops Center. You can associate a logical domain with more than one network.
13. Enter the number of connections for each network. You can connect to a network multiple times to the logical domain. When you create a logical domain, the number of connections for a network translate to the number of virtual network devices created for the logical domain. The number of virtual network devices created depends on the number of virtual switches present in the Control Domain. When you start a logical domain, you have to define the virtual switches through which you connect the logical domain to the external network.
14. Click Next to view the summary of the details selected for creating a logical domain.
15. Review the information and click Finish to save the profile. If you have opted to create a deployment plan with this profile in the first step, then a corresponding logical domain plan is also created.

> **Note:** If you make any changes to the profile, a new version of the profile is created. If required, you can change the profile reference in the plans that have used the older version of the profile.

Cluster Profiles

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

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

The profiles and deployment plans rely on pre-action and post-action scripts to suspend cluster operations and save configuration information during the update process.

The following cluster-specific profiles and scripts are located in Enterprise Manager Ops Center's Local Content software library. As the Oracle Solaris Cluster software is revised, new profiles are made available to you through the Java.net site's Ops Center Cluster Profiles project. You download these new profiles and scripts, then import them into the Local Content library. See Obtaining the Cluster Profiles and Scripts for instructions to get these files.

- Profiles for Provisioning Oracle Solaris Cluster Software version 3.2u3

  - SPARC
    - sc-3.2u3-core-sparc
    - sc-3.2u3-manager-sparc
    - sc-3.2u3-agents-sparc
  - x86
    - sc-3.2u3-core-x86
    - sc-3.2u3-manager-x86
    - sc-3.2u3-agents-x86
- Profiles for Upgrading Version 3.2u3 to Version 3.3 or for Provisioning an Oracle Solaris Cluster Software Version 3.3
  - SPARC
    - sc-3.3-core-sparc
    - sc-3.3-manager-sparc
    - sc-3.3-agents-sparc
  - x86
    - sc-3.3-core-x86
    - sc-3.3-manager-x86
    - sc-3.3-agents-x86
- Scripts for pre-action and post-action
  - Post-action script for provisioning either version 3.2 or 3.3: SolarisCluster-Post.ksh
  - Post-action script for upgrading version 3.2 to 3.3: SolarisCluster3.21109-Post
  - Pre-action script for upgrading version 3.2 to 3.3: SolarisCluster3.21109-Pre

Obtaining the Cluster Profiles and Scripts

To obtain profiles and scripts for a new release of Oracle Solaris s Cluster software, download them to the system that is running the Enterprise Controller.

> **Note:** When you download, transfer, upload, or import these files, do not change the file name. Keep the same name throughout the procedure.

To Obtain the Cluster Profiles and Scripts

1. Go to http://java.net/projects/oc-cluster-profiles
2. Click the Downloads button.
3. Select the folder for the profiles you want:
   - To provision Oracle Solaris Cluster Software version 3.2u3, select the Version-3.2u3 folder.
   - To upgrade version 3.2u3 to version 3.3, select the Version-3.3 folder.

- To provision Oracle Solaris Cluster Software version 3.3, select the Version-3.3 folder.

4. In the version folder, select the platform you want, either SPARC or x86.

   The platform folder contains three files: Agents, Core, and Manager. You need all three files to complete upgrade or provision operations.

5. Use the browser window's Save feature to save each file, keeping its file name.
6. Return to the home page for the project and select the Action-Scripts folder.
7. Select the scripts that complete the core profiles:
   - To upgrade version 3.2u3 to version 3.3, select the Pre-Upgrade and Post-Upgrade scripts.
   - To provision version 3.2u3 or version 3.3, select the Post-Provision script.
8. Upload the profiles and scripts, according to Uploading the Cluster Profiles and Scripts.

Uploading the Cluster Profiles and Scripts

The files containing the profiles and scripts must reside on the same system that is running the browser and they must reside in the same directory. This operation uploads all files in the selected directory.

1. Move the profiles and scripts to the appropriate system and directory.
2. Expand Libraries in the Navigation pane.
3. Click Local Content in the Solaris/Linux OS Updates library.
4. Click Bulk Upload Packages and Patches in the Actions pane.
5. Click Distribution to select the distribution that applies to these files.
6. Select Upload from Directory.
7. Specify the path to the directory or click Browse to locate and select it.

   All files in the directory and its subdirectories are uploaded.

8. Click Submit.
9. Import the profiles into Enterprise Manager Ops Center, according to Importing Cluster Profiles and Scripts.

Importing Cluster Profiles and Scripts

Before You Begin

- To import profiles, use the browser on the same system or transfer the profiles to the system on which you are running the browser.
- To import scripts, transfer the files to the Enterprise Controller's system.

Note: When you download, transfer, upload, or import these files, do not change the file name. Keep the same name throughout the procedure.

To Import a Cluster Profile

1. Expand Plan Management in the Navigation pane.
2. Click Update Profiles.
3. Click the Import Profile icon.
4. For each profile and script:
   a. Enter the name of the file you downloaded. Do not change the name.
   b. Click Import.
5. Expand Libraries in the Navigation pane.
6. Select Solaris/Linux OS Updates.
7. Select Local Content.
8. Click Upload Local Action.
9. For each profile:
   a. Enter the name of the profile as you want it to be displayed in the Plan Management section.
   b. Select the distribution of the OS that uses the profile.
   c. Enter the name of the file that contains the profile. Do not change the name.
   d. Click Upload.
10. For each script:
    a. Select action type, the matching parent category, and the OS distribution.
    b. Enter the name of the file that contains the script. Do not change the name.
    c. Click Upload.
11. For provisioning profiles, edit the core profiles to include the Post-Provision scripts, according to Editing the Core Profile for Provisioning

    To upgrade a cluster, no modification is needed because the scripts are available to the upgrade profile after the import operation.

Editing the Core Profile for Provisioning

1. Expand Plan Management in the Navigation pane.
2. Click Update Profiles.
3. In the OS Update Profiles table, select the core profile.
4. Click the Edit Profile icon.
5. In the Edit OS Update Profile window, navigate from Local to either Post-actions or Pre-action.
6. Select the script and click Required. For example, to edit the core profile for provisioning, navigate to Post-actions, select SolarisCluster-Post.ksh, and click Required. The file is now listed in the Profile Contents section.
7. Click the Saved as Named Profile button.

Managing Profiles

All functions such as configuring service processors, provisioning servers, and updating in Ops Center can be captured in the form of profiles and used again and again to create consistent configurations.

Profiles form the building blocks upon which the deployment plans are created. You need to manage the profiles, and its versions. Name your profiles for clear understanding. Depending on the user role prescribed, you have options to view, edit, copy, delete profiles.

Viewing Profiles

You can select a profile and view its details, plans that use the profile, and the version history of the profile.

To View Details of a Profile

1. Select Plan Management section from the Navigation pane.
2. Select a profile type from the Profiles and Policies tree.
3. Choose a profile from the list of profiles. The profile details of the latest version are displayed in the center pane:
   - Name and description of the profile
   - Subtype - The different types of product for which you want to create a profile
   - Target type - Defines the type of hardware on which the profile can be applied
   - Version and last modified date
   - The parameters that are collected for creating a profile are displayed.
4. Select Referrers tab in the center pane. The plans that reference the selected profile are listed.
5. Select Version History tab in the center pane. The versions that are available for the profile are listed.
6. Select a version and click the View Version Details icon. The profile details are displayed.

The profile with different versions will be displayed with the version number while selecting them in a plan. For example, if the profile name is logdom, the versions of it will be displayed as logdom v1 and logdom v2.

Copying Profiles

You can create an exact instance of an existing profile using the Copy Profile option. You create another profile with a new name for the profile. You can edit the other parameters of the profile except for the target type and sub type of the profile.

To Copy a Profile

1. Select Plan Management section from the Navigation pane.
2. Select the profile type from the Profiles and Policies tree.
3. Select a profile from the list. The profile details are displayed in the center pane.

4. Select Copy Profile from the Actions pane. Alternatively, you can select the profile type, select the profile from the list in the center pane and click the Copy Profile icon. The corresponding Create Profile wizard is displayed.
5. Edit the parameters in the wizard as required. The name of the profile is displayed as Copy of <profile name>. You can modify the name and other parameters of the profile as required. You cannot modify the profile parameters Subtype and Target type of the profile.
6. Click Finish to copy the profile. The profile will be copied and the new profile will be listed.

Editing Profiles

You can edit the profile parameters in Ops Center. When you edit the profile parameters, a new version of the profile will be created. If you change the name of the profile, then it will be created as a new profile and the existing profile will not be modified.

Note: When you edit a profile, the plans that refer to the profile are not updated to the new profile version. You need to update the plan to the updated profile version, as required.

You must have appropriate roles and permissions to edit the profiles.

To Edit a Profile

1. Select Plan Management from the Navigation pane.
2. Select the profile type from the Profiles and Policies tree.
3. Select a profile from the list that you want to modify. The selected profile details are displayed in the center pane.
4. Select Edit Profile in the Actions pane. Alternatively, you can select the profile type, select the profile from the list in the center pane and click the Edit Profile icon. The Edit Profile wizard displays.
5. Modify the profile parameters as required in the wizard.

Note: If you change the name, the profile is stored as a new profile.

6. Click Finish to update the profile. The profile is saved with the new changes and the version is incremented by 1.

Deleting Profiles

You can delete the profile versions that you have created.

To Delete a Version of a Profile

1. Select Plan Management from the Navigation pane.
2. Select the profile type from the Profiles and Policies tree.
3. Select the profile that you want to delete. The profile details are displayed in the center pane.
4. Select Delete Version in the Actions pane to delete the latest version.

5. To delete previous versions, select Version History in the center pane. All the versions of the profile are listed.
6. Select a profile version.
7. Click the Delete Version icon.
8. Confirm the delete action.

The selected version of the profile will be deleted and any plans that references the profile will be updated accordingly. You need to update the plans manually that references the deleted profile.

9

Monitoring Rules and Profiles

Monitoring rules and profiles are used to define the monitoring parameters. This section discusses the types of monitoring rules and how the software uses the monitoring rules and profiles that you define to generate alerts and problems in the UI.

About Monitoring Rules and Profiles

Monitoring rules, profiles, and plans detect components or attributes of a managed asset or resource that are not operating within specified parameters. A resource is a generic term for any resource managed through Enterprise Manager Ops Center, it can be an asset (hardware or OS), a group, a network, or a library. An Enterprise Manager Ops Center administrator has permissions to edit and add monitoring rules and profiles.

- Monitoring Rules – Express alerting conditions. You can apply one or more rules to an asset in order to monitor the asset and raise an alert when the monitoring rule condition is met.
- Monitoring Profiles – A set of monitoring rules targeted to a specific asset type. Default monitoring profiles contain a set of rules that are automatically applied. You can copy a profile and manually configure the rules in the profile.

The following are the main components of a complete monitoring configuration:

Other features, such as annotations and operational profiles, will greatly enhance monitoring and problem management capabilities. Annotations enable you to add comments, suggested actions, or automated scripts for a specific problem, or you can add associate an annotation with a specific problem and asset type and add it to the Problems Knowledge Base. Operational profiles and plans are another method of adding consistency to problem management. You can create an operational profile that contains a script that can be run against a known problem. Annotations and operational profiles are discussed in more detail in their respective sections.

Monitoring Rules

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

Two main types of rules exist:

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

The following types of editable user-defined rule parameters are available:

- Threshold – a numeric value above or below a defined level
- Boolean Control – a true-false check
- Enumerated Control – a series of values
- Expression – an instruction to execute something that will return a value

Not all rule parameters can be modified, but most rules include some parameters that an administrator can tune, or edit to meet your organization's requirements. The following are some examples of editable parameters:

- Severity
- Raising and clearing values
- Time constraints after an alert is raised, after what time period is a rule disabled (timer-driven alert condition check)
- Data collection script to trigger upon alert
- Other monitoring parameters that are specific to the rule type, such as threshold settings trigger level, clear level, time-across-threshold-before-alert

Generally, you can add, edit, enable, disable, and remove resource monitoring rules. For each managed resource, there is a Monitoring tab. You can tune the rules for a specific managed resource from this tab.

Each rule is associated with a severity level of Info, Warning, or Critical. Default values and severity levels are provided at installation, but are editable. For user-defined rules, you can define the time between when the alerting condition is identified and when an alert or problem is generated.

You can configure the software to send an e-mail or pager message when a Warning or Critical problem is identified.

Monitoring Profiles

A monitoring profile contains information to monitor a managed asset with user-defined alert configurations, including defining thresholds and setting up alert monitors.

Monitoring profiles are automatically applied when an asset becomes a managed asset, when an agent is deployed. Some assets, such as networks, are managed and monitored at inception. You can apply any monitoring profile to an arbitrary managed asset or group of assets to change the monitoring configuration on the subset of those resources of a compatible type.

The following pre-defined monitoring profiles are included in the software:

- System-defined - For Sun Oracle hardware and operating systems
- User-defined - Customized profiles for your managed assets
- Generic - Default set of profiles for systems that do not have a specific profile

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

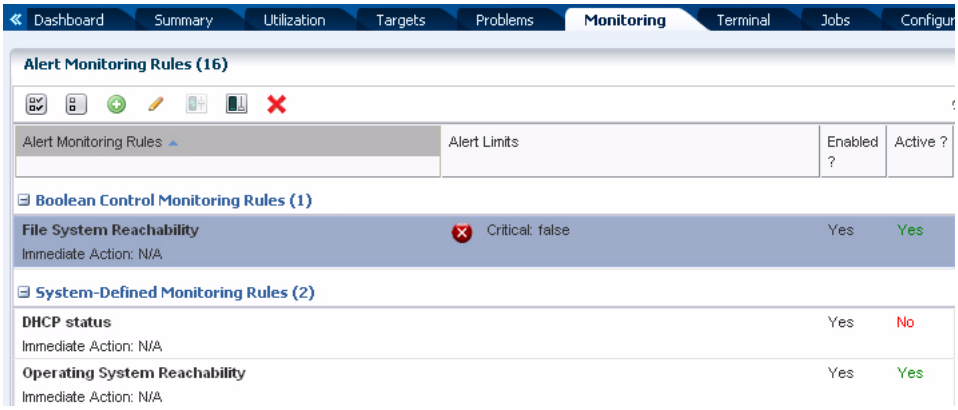
Enabled and Active Rules

Monitoring rules have two types of states:

- Enabled or Disabled – Determined by the user configuration. Disabling a rule removes that attribute from monitoring. You can disable and enable rules on a per asset or group basis.
- Active or Inactive – Reflects the system's state and indicates whether or not monitoring is actually being performed. 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 Enabled? and Active? fields indicates if the rule is enabled and active. A rule is disabled or inactive if "No" appears in the corresponding field. The following graphic shows the DHCP status as enabled, but not active.

Figure 9–1 IActive and Inactive Monitoring Rules



When a rule is enabled, the active state reflects the system's actual state and indicates if monitoring is being performed. The following are some of the reasons that an enabled rule might display as not active:

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

Annotations

For more robust problem management, you can associate an annotation with a rule and store the annotation in the Problems Knowledge Base. Annotations in the Problems Knowledge Base enable you to provide an automated solution or a suggested action when a specific problem is detected. To provide an automated

solution, create an operational plan that contains a shell script. When a specific problem occurs, the script is executed automatically. To provide a suggested fix or course of action for a specific problem, you can create a text only annotation that provides a suggested course of action, or you can include a shell script.

When a rule is triggered, and an alert or problem is identified, the software checks the Problems Knowledge Base and Problem Profiles for the Problem Type and any associated Annotations. It generates a problem of the defined type and severity level and attaches any annotations. If an automated operation annotation is associated with the problem, the script is executed. If a suggested action annotation is associated with the problem, the text and script (if available) appear in the problem details.

Monitoring Rules

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

Editing a Monitoring Rule

Monitoring rules have pre-defined parameters. You can change the parameters, including the threshold values and the monitoring level, to meet your data center guidelines. You can define the parameters by system or by group. By creating a group for each type of asset, such as operating systems, you can set specific threshold values for all members of that group and apply a monitoring profile to the group instead of editing each individual OS. By defining a group of asset and applying a monitoring profile to that group, you can easily apply a given set of monitoring rules to a large number of assets.

You might want to edit the monitoring rule parameters for an individual system if that system is on a critical path. For example, if the Enterprise Controller is considered a critical path system, you can monitor the system continuously and create more stringent monitoring thresholds for that system.

You might want to create separate monitoring groups for a set of high priority systems and a set of low priority systems. By establishing the groups, you can consistently and efficiently define the parameters for all systems in each group.

As an administrative user, you can edit monitoring rules to change the values of the monitoring variables to meet your data center guidelines.

You can perform the following tasks:

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

For example, you can create a threshold on the Enterprise Controller system that sends a warning if the file system use rises above 90%. This will alert you if the Enterprise Controller file system is almost full.

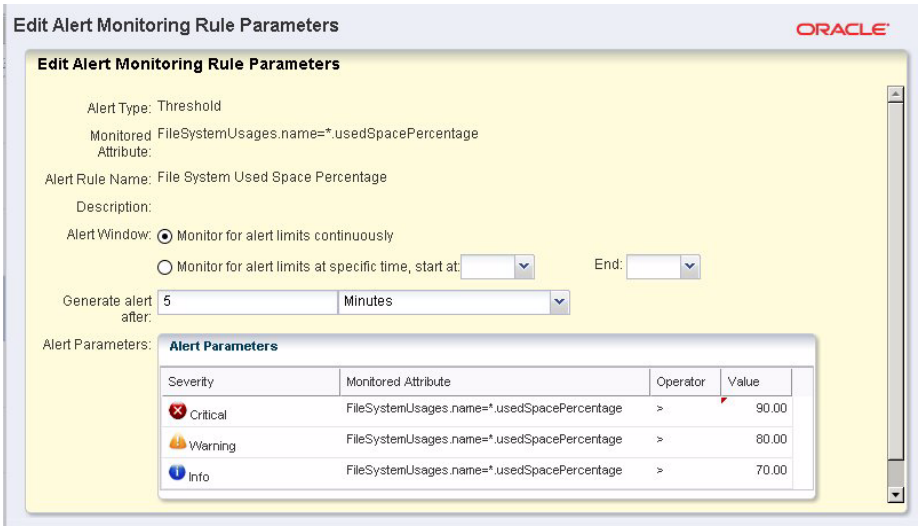
You can edit a monitoring rule in the context of the asset or the monitoring rule.

To Edit a Monitoring Rule From the Asset View

1. Select Assets in the Navigation pane.
2. Select an asset The Summary page is displayed with the status of the asset.
3. Select the Monitoring Configuration tab.
4. Click the Monitoring tab to see a list of all the monitoring variables, both hardware and OS, the latest value of each one, and the values of their thresholds.
5. Select the monitoring variable you want to change.
6. Click the Edit Alert Monitoring Rule Parameters icon. The Edit Alert Monitoring Rule Parameters window is displayed. The following is an example of the Edit Alert Rule parameter.

   The details of the selected rule are displayed.

Figure 9–2 Edit Alert Monitoring Rule Parameters



7. For a threshold alert, you can change how often and for how long the value is monitored, and you can change the threshold values.
   - Alert window – Enables you to specify a period of the day when the monitoring rule is enabled. For example, if a daily maintenance operation that will cause a monitored attribute to exceed a threshold, you can exclude monitoring for that time. Effectively disabling monitoring for that maintenance window.
   - Generate alert after – Enables you to configure monitoring to ignore a monitored attribute that is outside the defined monitoring parameters for a short period of time. You might want to do this if you do not want an alert to generate when a short peak occurs. Specifying a delay here means an alert is generated only if the value remains above the specified limit for a given duration. An alert is not generated if the value goes above the limit at one time and then immediately goes back to normal.
8. To change a value, click the entry in the Value column and type the new value.
9. Click Apply to submit the changes.

To Edit a Monitoring Rule in the Profile

1. Click Plan Management in the Navigation pane.
2. Expand Monitoring Profiles and click a profile. The Profile Details page is displayed.
3. Click the Edit Alert Monitoring Rule Parameters icon. The Edit Alert Monitoring Rule Parameters window is displayed.
4. For a threshold alert, you can change how often and for how long the value is monitored, and you can change the threshold values.
   - Alert window – Enables you to specify a period of the day when the monitoring rule is enabled. For example, if a daily maintenance operation that will cause a monitored attribute to exceed a threshold, you can exclude monitoring for that time. Effectively disabling monitoring for that maintenance window.
   - Generate alert after – Enables you to configure monitoring to ignore a monitored attribute that is outside the defined monitoring parameters for a short period of time. You might want to do this if you do not want an alert to generate when a short peak occurs. Specifying a delay here means an alert is generated only if the value remains above the specified limit for a given duration. An alert is not generated if the value goes above the limit at one time and then immediately goes back to normal.
5. To change a value, click the entry in the Value column and type the new value.
6. Click Apply to submit the changes.

See Appendix A, "Scenario – Deploying a Bare-Metal System" for a list of the attributes that are available for use in monitoring rules.

Adding a Monitoring Rule

Each monitoring profile contains a default set of rules. The ruleset and default parameters depend on the managed asset subtype.

The following rule parameters, also known as rule types, are available:

- Threshold – Sets an upper or lower monitoring threshold for the monitored attribute.
- Boolean Control – Sets a logical operator of true or false for the monitored attribute.
- Enumerated Control – Defines a subset of specific values among the possible values of the monitored attribute. An alert is raised if the attribute matches one of those specific values.
- Expression – Defines the variables, literals, and operators for an attribute.

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

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

- `CpuUsage.usagePercentage`
- `ProcessUsage.topMemoryProcesses.pid=*.physicalMemoryUsage`

- `DiskUsageSet.name=*.busyPercentage.`

Monitored attributes are available in the javadoc that is published in the Enterprise Manager Ops Center Software Developer's Kit (SDK). Install the SUNWxvmoc-sdk.pkg package, which is located in the `dvd/`*`platform`*`/Product/components/packages` directory.

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

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

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

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

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

You can perform a query which scans across all members of a collection by specifying the '*' wildcard value for the key or name. If you do, you must use one of the 'max', 'min' or 'like' operators. These are the only ones that understand the manipulation of collections. The DomainQuery java class's javadoc defines the query syntax to use. See Appendix A, "Scenario – Deploying a Bare-Metal System" for a list of the attributes you can use in monitoring rules.

You can edit a monitoring rule in the context of the asset or the monitoring profile.

To Add a Monitoring Rule in the Profile

1. Expand Plan Management in the Navigation pane.
2. Click Monitoring Profiles, then double-click the profile in the center content pane or click the profile from the Navigation pane.

   The Profile Details page is displayed.
3. Click the Add Alert Monitoring Rule icon in the center pane.
4. Provide a name and description for the rule that will appear in the Profile Details page.
5. Select the Asset type. The asset type is based on the profile. If another asset type is available, the option will appear in the drop-down menu.
6. Complete the Monitored Attribute. If you selected Expression, the Monitored Attribute option is not available.

7. Define the monitoring schedule, either continuously or for a specific time period. The start and end times are based on the monitored asset's time zone.
8. Define how long the alerting condition must last to be considered an alert. The default setting is 5 minutes. You can change the amount of time and the unit of measurement to be either minutes, hours, or days.
9. Complete the Alert parameters for the different severity levels.
10. Use the Immediate Action field to define what action should take place when a problem is detected.
11. Click Apply to save the rule. The new rule will appear in the profile.

To Add a Monitoring Rule From the Asset View

1. Click Assets in the Navigation pane, expand the tree and click the asset to which you want to add the rule.
2. Click the Monitoring tab to see a list of all the monitoring rules.
3. Click the Add Alert Monitoring Rule icon in the center pane. The Add Alert Monitoring Rule Parameters window is displayed.
4. Select a Rule Type from the drop-down menu: Threshold, Boolean Control, Enumerated Control or Expression
5. Select an Asset Type from the drop-down menu.
6. Complete the Monitored Attribute. If you selected Expression, the Monitored Attribute option is not available.
7. Provide a name and description for the rule that will appear in the Profile Details page.
8. Define the monitoring schedule, either continuously or for a specific time period. The start and end times are based on the monitored asset's time zone.
9. Define how long the alerting condition must last to be considered an alert. The default setting is 5 minutes. You can change the amount of time and the unit of measurement to be either minutes, hours, or days.
10. Complete the Alert parameters for the different severity levels.
11. Use the Immediate Action field to define what action should take place when a problem is detected.
12. Click Apply to save the rule. The new rule will appear in the profile.

See Appendix A, "Scenario – Deploying a Bare-Metal System" for a list of the attributes that are available for use in monitoring rules.

Disabling and Enabling Monitoring Rules

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

To Disable and Enable Monitoring Rules

1. Click Assets in the Navigation pane.
2. Select the All Assets view, then select an asset.
3. Click the Monitoring tab.

4. Click the monitoring rule, then click the Disable Alert Monitoring Rule(s) or Enable Alert Monitoring Rule(s) icon in the center pane.
   - To select more than one rule, use Ctrl-click.
   - To select all rules, click the Select All Rules icon.

Monitoring Profiles

A monitoring profile defines alert configurations to be performed on one or more managed resources. A profile is for a specific type of resource, such as operating systems. A more specific profile might apply to all Oracle Solaris operating systems. Each monitoring profile contains a number of alert monitors for a specific type of resource. Alert monitors watch the state of managed resources and their attributes and raise an alert when the state is outside the pre-defined thresholds.

Displaying a List of Monitoring Profiles

A monitoring profile is a collection of rules that are associated with each type of monitored asset. The profile defines the resources monitored and the rules for that asset type. An Ops Center administrator can add and edit profiles and determine which profile is the default profile for a specific asset type. Each profile contains a version history.

The Monitoring Profiles page displays a list of all profiles, the default status of the profile, and the intended asset or target type. The following types of monitoring profiles are available:

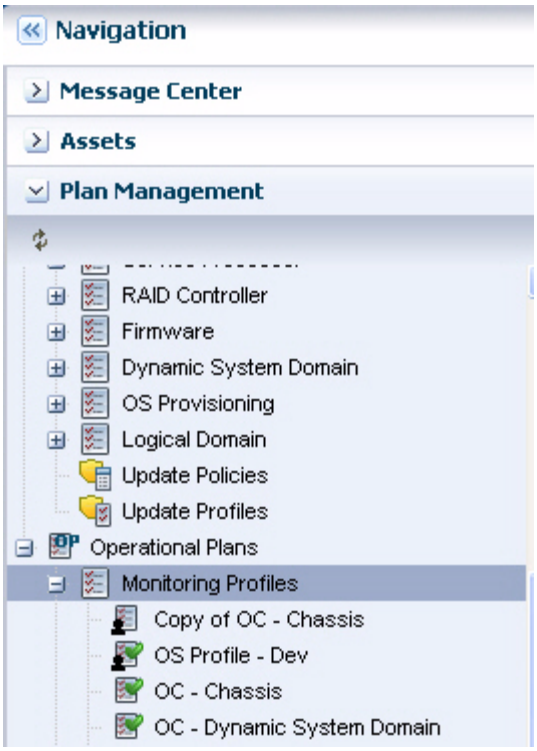
- User-Defined Profiles – Typically use generic rules and contain monitoring thresholds. A Operating System profile is an example of a user-defined profile that monitors the following generic OS parameters: CPU usage, disk IO queue length and utilization percentage, file system usage, memory usage, network bandwidth utilization, and swap usage, and system load.
- System Defined Profiles – Typically use asset specific rules. The monitored details depend on what is implemented on the asset and the ability to configure these rules is limited to turning the rule on or off. An example of a system-defined profile is the MSeriesChassis profile that monitors the Xsb Mode of a SPARC M-series chassis.

The naming convention for system-defined profiles is that the name always begins with "OC".

To Display a List of Monitoring Profiles

1. Click Plan Management in the Navigation pane.
2. Expand Operational Plans, then click Monitoring Profiles in the Navigation pane. In the following graphic, the list of profiles appears in the left Navigation pane and in the center pane. The Navigation pane and center pane both display user-defined profiles followed by system-defined profiles. The icons and naming convention help to identify the type of profile in the Navigation pane. The profiles appear in different sections in the center pane.

Figure 9–3 List of Monitoring Profiles



Displaying Monitoring Profile Details

Monitoring profile details vary, depending on the asset and associated resources being monitored. The details page contains information about the profile, including the name, description, and if the profile is system defined or user defined. The summary information also describes the applicable types of assets or targets, if the profile is a sub-type of another profile, when the profile was last modified, and if the profile is the default profile for the target types.

The following profile details:

- Monitoring rule
- Alert condition (Critical, Warning, or Informational)
- URL
- Enabled status

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

- Chassis – Monitors the chassis fan and power supply
- GlobalZone – Monitors the DHCP status, appliance health, CPU usage, disk IO, file system usage, memory usage, network bandwidth, Swap usage, and system load of a global zone.
- LDomGuest – Monitors Oracle VM Server for SPARC guest status, including the migration status, if the guest is running, and if the guest is powered on.
- LDomHost – Monitors Oracle VM Server for SPARC status, including the DHCP client, appliance health, and free virtual CPU (VCPU) usage.
- MSeriesChassis – Monitors the Xsb Mode of a SPARC M-series chassis

- NonGlobalZone – Monitors CPU usage, disk IO queue length and utilization percentage, memory usage, network bandwidth utilization, and swap usage for non-global zones.
- OperatingSystem – Monitors the following generic OS parameters: CPU usage, disk IO queue length and utilization percentage, file system usage, memory usage, network bandwidth utilization, and swap usage, and system load.
- Server – Monitors the following parameters on a generic server: Power status, server port status, CPU, NIC, fan, fan tray, memory, and power supply.
- Storage – Monitors the following parameters for a generic storage device: OS status, power status, server port status, and storage alert.
- Switch – Monitors an ethernet switch's power status, switch port status, and switch status.

To Display Monitoring Profile Details

1. Click Plan Management in the Navigation pane.
2. Expand Profiles, then expand Monitoring Profiles in the Navigation pane.
3. Click the profile that you want to display. The profile type, name, description, target type, and whether or not the profile is the default for the target type are displayed in the center pane. The page also displays the last edit date.

Creating a Monitoring Profile

Each Monitoring profile contains a default set of rules. The ruleset and default parameters depend on the managed asset subtype.

The following methods are available for creating a new profile:

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

To Create a Monitoring Profile

1. Expand Plan Management in the Navigation pane.
2. Click Monitoring Profiles.
3. Click Create Profile in the Action pane.
4. Provide a name and description for the monitoring profile, then select the resource type for the profile from the Subtype list.
5. Click Finish to save the profile. The new profile will appear in the center content pane.
6. (Optional) To add or remove rules or change monitoring parameters, double-click the profile in the center content pane.
7. (Optional) To make this profile the default monitoring profile, click the Set as Default Profile icon.

Extracting a Monitoring Profile

Extracting a Monitoring Profile is similar to copying a profile. Copying a profile is performed from the profile view, while extracting a profile is performed from the asset view. By extracting a profile from the asset view, you filter the possible subtypes to

only those that are valid. You can change the target subtype to a more specific or a more generic eligible target type. To be eligible, the profile must be a member of a more general profile for the specified target. If a list of valid target types does not display, then the target type cannot be changed.

Each Monitoring profile contains a default set of rules. The default ruleset and parameters depend on the managed asset subtype that you select. For example, you can highlight a Solaris OS and extract a monitoring profile for an operating system. You can specify one of the following as the OS subtype for the new profile:

- Solaris 10 – Any Solaris 10 OS that is supported by Ops Center
- Solaris 10 Operating System – Any Solaris 10 8/07 (update 4) or higher OS that is supported by Ops Center. You might use this subtype if you was to use the profile for Solaris Zones.
- Solaris – Any Solaris OS release that is supported by Ops Center
- Operating System – Any Solaris, Linux, or Windows OS that is supported by Ops Center

To Extract a Monitoring Profile

1. Expand Assets in the Navigation pane.
2. Click an asset type, such as operating system, in the Navigation pane.
3. Click Extract Monitoring Profile in the Action pane.
4. Provide a name and description for the monitoring profile.
5. Select the resource type, such as Solaris 10 Operating System or Operating Systems, for the profile from the Subtype list.
6. Click Finish to save the profile. The new profile will appear in the center content pane.
7. (Optional) To add or remove rules or change monitoring parameters, double-click the profile in the center content pane.
8. (Optional) To make this profile the default monitoring profile, click the Set as Default Profile icon.

10

Problems Knowledge Base

The Problems Knowledge Base contains annotations based on asset type. Annotations are text files or shell scripts that can automate an operation, provide a suggested action, or record a comment. An administrator can associate an annotation with a problem and an asset type that can help a user to investigate or fix a Problem when it occurs for a specific asset type.

This section provides an overview of the Problems Knowledge Base and how to add annotations to the Problems Knowledge Base and how to remove them.

About the Problems Knowledge Base

Annotations in the Problems Knowledge Base are created, updated, and deleted by a user with Enterprise Controller Admin or Admin permissions. Annotations are defined by an asset type, asset resource type, an attribute, or a problem type.

The following types of Annotations are available:

- Automated Operation – Enables you to create an annotation that references an Operational Profile and automatically executes the profile when a specific problem occurs.
- Suggested Action – Enables you to provide a suggested fix or course of action for a specific problem. The suggested course of action can be text only, or you can reference an Operational Profile.
- Comment – A text only field that you can use to write notes about the situation, such as the current status of a problem.

As an administrator, you can add annotations to the Problems Knowledge Base that provide solutions or recommended actions for specific problems. You can also add an annotation to the Problems KB when you add an annotation to a specific problem.

When a problem is detected, Ops Center checks the Problems Knowledge Base and Problem Profiles for the asset type and corresponding problem type. Any associated Annotations are added to the Problem and Operational Profiles referenced in Automated Operation annotations are executed against the asset on which this problem was open.

Adding an Annotation to the Problems KB

Annotations are created by a user with Ops Center administrator permissions and are defined by an asset type, asset resource type, an attribute, or a problem type. The annotations are stored in the Problems Knowledge Base (KB) and can be automated operations with associated operational profile, suggested fixes or actions, or text only

comments. An administrator can associate Automated Action and Suggested Action annotations with an operational profile, which can contain a script.

You can also add an annotation to the Problems KB when you add an annotation to a specific problem, as described in "Adding an Annotation".

To Add an Annotation to the Problems KB

1. Click Plan Management in the Navigation pane, expand Operational Plans, then expand Problems Knowledge Base.
2. Select the asset type. The Annotations associated with the asset type are displayed in the center pane.
   a. Click the Add icon in the center pane. The Add Problem Type Annotation page appears.
3. Define the Problem Type. The attributes displayed depend upon the target and Asset Type.
   a. Select an Asset Type from the drop-down menu.
   b. Select a Monitored Attribute from the drop-down menu or enter an attribute to be monitored. For a list of valid attributes for each asset type, see the javadoc public API.

      Note: The drop-down menu for asset type and monitored attribute are retrieved from the Monitoring Rules deployed on the setup. If an attribute is not listed, it is not monitored. To add an attribute to the menu, define a Monitoring Rule for this attribute as described in Adding a Monitoring Rule. To enter an attribute that is not in the drop-down menu, you can use a wildcard such as CpuUsage.*.

   c. Define the list of severities to which this annotation applies. The annotation is added to a Problem only once, at creation or the first time this Problem reaches one of the severity levels defined here. When the annotation is an Automated Action, the associated operational profile is executed as soon as it is added to the Problem.
4. Determine the Annotation to associate with the problem.
   a. Select the Annotation Type from the drop-down menu. The following options are available:
      * Comment – Text only option that is designed to be used to add a note or editorial comment.
      * Suggested Action – Text is required. An Operational Profile is optional.
      * Automated Action – Text and an Operational Profile are required.
5. Select an operational plan from the drop-down menu. The operational plans presented in the drop-down menu are your organization's custom scripts and operational profiles. Automated actions must have an associated operational plan.
6. The Synopsis field is automatically completed based on the asset type. Edit the synopsis, as needed.
7. Type a description or instructions in the Note field.
8. Click Save.

Removing an Annotation From the Problems KB

Annotations in the Problems Knowledge Base (KB) are associated with types of problems. A user with an Ops Center administrator role can delete an annotation in the the Plan Management section of the user interface.

To Remove an Annotation From the Problems KB

1. Click Plan Management in the Navigation pane, then expand Operational Profiles.
2. Expand Problems Knowledge Base in the Navigation pane, then select the target type. The annotations associated with the target type are displayed in the center pane.
3. Highlight the annotation you want to delete, then click the Delete icon. The Delete Problem Type Annotation page appears.
4. Click Delete.

11

Operational Profiles and Plans

An operational plan contains an operational profile that is required to operate your environment. These include problem rule configurations and thresholds, scripts and utilities to fix common problems, and a knowledge base that can be built up around problems in your environment.

About Operational Profiles and Plans

An operational profile and associated plan is a powerful tool in automating process actions in Enterprise Manager Ops Center. An operational profile defines the type of asset to be targeted, contains a shell script, and enables you to provide additional required or optional variables. A plan provides the framework for the profile, including the targets and the level of interaction.

When you create an operational profile, the default option is to create an associated operational plan with the same name. You can also create an operational profile as part of creating an operational plan.

You can use operational profiles and plans to operate your environment, including:

- Add automation and consistency
- Install probes for monitoring purposes
- Define problem rule configurations and thresholds
- Create annotations to fix common problems
- Build a problems knowledge base of issues and solutions for your environment

You can apply, or execute, an operational plan as a stand-alone action, or you can combine one or more operational plans and deployment profiles as part of a larger deployment plan, such as a server provisioning plan.

The following are some of the applications:

- Automatic or manual configuration of thresholds and other instrumentation of a managed resource or group of resources.
- Automated or semi-automated step of a server provisioning plan.
- Manual actions taken against a managed resource or group of resources.
- Automated or semi-automated step in the processing of an problem, such as automatically closing a problem.
- Use plans as annotations that can automate or provide recommended actions when a problem occurs. For example, you can create an annotation for a specific

critical problem. When the problem occurs, the script in the operation profile is automatically triggered.

Plans are stored in the Problems Knowledge Base on the Enterprise Controller and are executed against the root cause of a problem in the context of a managed resource.

Plans and profiles are editable. However, only the user that created the profile and plan can edit the entire profile. Users that have permissions to apply a plan, but who did not create the plan, can override some profile values for a specific job. They cannot permanently change the profile.

Version Control

When a profile is edited, a new version is created. Older versions are still available for use.

When an operational profile is associated with an operational plan, the plan uses the associated profile and version. The plan is not updated when you create a new version of the profile. If you want to use the new version, you must update the plan to revise the profile version.

When an operational profile is used as an action for problem management, the latest version of the profile is executed.

Operational Profiles

An operational profile contains a shell script and, optionally, environmental variables that you can use in operational and deployment plans. By default, creating a profile also creates an operational plan.

You can perform the following tasks:

- Creating an Operational Profile
- Editing an Operational Profile
- Copying an Operational Profile
- Deleting an Operational Profile

Creating an Operational Profile

An operational profile uses a shell script to define one or more operations that are to be performed on a managed resource or group of resources. For example, deploying thresholds onto a managed resource, or performing state changing actions such as shutting down all logical domains and then shutting down an Oracle VM Server for SPARC.

For each profile, you can choose one of the following types of shell scripts:

- EC Shell – The script will only run on the Enterprise Controller. It is executed with the logged-in user's credentials
- Remote Shell – The script can run on any managed system that contains a remote agent. It is executed with root permissions.

You can save a shell script on the Enterprise Controller and download it into the plan, or you can enter the script in a text field when you create the plan. Both types of shell scripts are executed by the user. They differ in the location (on the Enterprise Controller or on the remote Agent) and the manner (user credentials) of the execution.

To Create an Operational 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. Type a name for the new plan and a description of its purpose or role.
4. Select an asset type from the Subtype list.
5. Click Next.
6. Select the Operation Type from the drop-down menu, either EC Shell or Remote Shell.
   - If you selected EC Shell, browse to the location of the script in the Script File field, then click Load Script.
   - If you selected Remote Shell, type your script in the Script field.
7. Enter a numeric value in the Timeout field, then select Minutes or Seconds. The default is 60 minutes.
8. (Optional) Click View System Variables to view the default variables, such as Alarm_ID$. This variable adds the problem identifier number for easier problem management.
9. Click Next.
10. Specify Additional Variables.

Editing an Operational Profile

If you created the profile, you can edit it and create a new version. When you create a new version, the operational and deployment plans that are already using the profile are not updated with the new version.

If you did not create the profile, you do not have edit permissions to create a new version. You can copy an existing operational profile, rename it, and create a new profile and plan.

To Edit an Operational Profile

1. Click Plan Management in the Navigation pane, then click Operational Profiles. The Operation Profiles are displayed in the center pane.
2. In the center pane, highlight the plan you want to copy.
3. Click the Copy icon in the center pane. The Create Profile - Operation page appears.
4. Type a name for the new plan and a description of its purpose or role. By default, a plan is created with the same name as the profile. If you do not want to create an operational plan with this profile, click the check box to deselect the option.

   Note: A profile must be applied as part of a plan.

5. Select an asset type from the Subtype list.
6. Click Next.
7. Define the script.

a. Select the Operation Type from the drop-down menu, either EC Shell or Remote Shell.

b. In the Script File field, browse to the location of the script.

c. Click Load Script.

d. Enter a numeric value in the Timeout field, then select Minutes or Seconds. The default is 60 minutes.

e. Type your script in the Script field.

f. (Optional) to view the system-defined variables, click View System Variables.

g. Click Next.

8. (Optional) Specify Additional Variables.

Copying an Operational Profile

You can copy an existing operational profile, rename it, and create a new profile and plan.

To Copy an Operational Profile

1. Click Plan Management in the Navigation pane, then click Operational Profiles. The Operation Profiles are displayed in the center pane.
2. In the center pane, highlight the plan you want to copy.
3. Click the Copy icon in the center pane. The Create Profile - Operation page appears.
4. Type a name for the new plan and a description of its purpose or role. By default, a plan is created with the same name as the profile. If you do not want to create an operational plan with this profile, click the check box to deselect the option.

Note: A profile can only be applied as part of a plan.

---

5. Select an asset type from the Subtype list.
6. Click Next.
7. Define the script.
   a. Select the Operation Type from the drop-down menu, either EC Shell or Remote Shell.
   b. In the Script File field, browse to the location of the script.
   c. Click Load Script.
   d. Enter a numeric value in the Timeout field, then select Minutes or Seconds. The default is 60 minutes.
   e. Type your script in the Script field.
   f. (Optional) to view the system-defined variables, click View System Variables.
   g. Click Next.
8. (Optional) Specify Additional Variables.

Deleting an Operational Profile

When a profile is edited, a new version is created. You can view version details by highlighting the plan, then clicking the View Version Details icon. Use the arrows to view the different versions. You can delete a version of a profile, or you can delete all versions of the profile and the associated plan.

Note: If you delete a version and more than one version exists, the previous version becomes the default. If only one version of the plan exists, the operational profile and plan are deleted.

To Delete an Operational Profile

1. Click Plan Management in the Navigation pane, then expand Profiles.
2. Click Operation in the Navigation pane. The Operation Profiles are displayed in the center pane.
3. To delete a version of the profile, Delete Version icon in the center pane
4. To delete the entire profile and the associated operational plan, click Delete Profile.
5. Click Delete to confirm your action.

Operational Plans

Operational Plans define how the Operation Profile scripts are deployed, and against which targets.

Creating an Operational Plan

An operational plan defines the targets and failure policy for an operational profile. The profile defines one or more operations that are to be performed on a managed resource or group of resources. For example, deploying thresholds onto a managed resource, or performing state changing actions such as shutting down all logical domains and then shutting down an Oracle VM Server for SPARC.

The profile uses a shell script to define the operations. If you do not already have an operational profile, you can create a profile when you create the plan. When you create the profile, you can download a shell script that is already saved on the Enterprise Controller (EC Shell script), or you can type a shell script (Remote Shell script) in the profile.

The EC Shell and Remote Shell are both shell scripts that are executed by the user. They differ in the location (on the Enterprise Controller or on the remote Agent) and manner (user credentials) of the execution. The EC Shell is executed with the credentials of the user that is logged in. The Remote Shell can run on any managed system that contains a remote agent and is executed with root permissions.

A plan contains one or more steps that are bound to a profile or plan. Specify the profile or plan that the step will use when it is applied to a target asset.

Actions available to a step are:

- A new profile can be created and used by the step. Not every step can create a new profile
- View the details of the profile or plan
- Some steps can be duplicated and assigned a unique profile or plan.

- Duplicated steps can be removed
- Some steps can specify which result targets will be used when the plan is applied to a target asset

To Create an Operational Plan

1. Click Plan Management in the Navigation pane, then click Operational Plans. The Operational Plans are displayed in the center pane.
2. Click Create Operational Plan in the Actions pane.
3. Type a name for the new plan and a description of its purpose or role.
4. Specify how to handle a failure when the plan is applied to a target asset, either stop at the first failure, or attempt to complete as much as possible.
5. Click the step field, then click Create Profile. The Create Profile - Operation page appears.
6. Type a name for the new profile and a description of its purpose or role.
7. Select an asset type from the Subtype list, then click Next.
8. Define the script by selecting either EC Shell or Remote Shell from the Operation Type drop-down menu.
9. Select the Operation Type from the drop-down menu, either EC Shell or Remote Shell.
   - If you selected EC Shell, browse to the location of the script in the Script File field, then click Load Script.
   - If you selected Remote Shell, type your script in the Script field.
10. Enter a numeric value in the Timeout field, then select Minutes or Seconds. The default is 60 minutes.
11. (Optional) Click View System Variables to see default system variables, such as Alarm_ID$. This variable adds the problem identifier number for easier problem management.
12. Click Next.
13. Specify Additional System Variables.

Copying an Operational Plan

An Operational Plan is a plan that defines one or more operations that are to be performed on a managed resource or group of resources. For example, deploying thresholds onto a managed resource, or performing state changing actions such as shutting down all logical domains and then shutting down an Oracle VM Server for SPARC.

To Copy an Operational Plan

1. Click Plan Management in the Navigation pane, then click Operational Plans.
2. In the center pane, highlight the plan you want to copy. The Operation Profiles are displayed in the center pane.
3. Click the Copy Operational Plan icon in the center pane.
4. Type a name and description for the plan.

5. Complete the Failure Policy, either Stop at failure or Complete as much as possible. (Optional) To view details about a profile or step, highlight the step, then click the Associated Profile/Operational Plan Details icon. Close the window.
6. Click Save.

Editing an Operational Plan

An Operational Plan is a plan that defines one or more operations that are to be performed on a managed resource or group of resources. You cannot edit the plan name, but you can edit the description, Failure Policy, and associated profiles, or create a new operational profile.

To Edit an Operational Plan

1. Click Plan Management in the Navigation pane, then click Operational Plans.
2. In the center pane, highlight the plan you want to edit. The Operation Profiles are displayed in the center pane.
3. Click the Edit Operational Plan icon in the center pane.
4. (Optional) Edit the plan description.
5. (Optional) Change the Failure Policy, either Stop at failure or Complete as much as possible.
6. (Optional) To view details of the associated profile or plan, highlight the step and then click the Associated Profile/Operational Plan Details icon in the table in the center pane.
7. (Optional) To create a new profile, click the Create New Profile icon in the table in the center pane. The Create Profile - Operation page appears.
   a. Type a name and description for the new profile.
   b. Select a Subtype from the list of available asset types.
   c. Click Next.
   d. Select the Operation Type from the drop-down menu.
   e. (Optional) Browse for the script file, then click Load Script.
   f. Define the time out number and unit of measurement, either Minutes or Seconds.
   g. If you did not load a script, add the script in the text box, then click Next.
   h. Use the Add icon to specify any additional variables, then click Next.
   i. Click Finish.
8. Click Save.

Viewing a Version of an Operational Plan

An Operational Plan is a plan that defines one or more operations that are to be performed on a managed resource or group of resources. When a plan is modified, a new version is created. Use this option to quickly view the differences between plan versions.

To View a Version of an Operational Plan

1. Click Plan Management in the Navigation pane, then click Operational Plans. The plans are displayed in the center pane.
2. Click the View Version Details icon in the center pane.
3. Use the arrows to view the different versions.
4. Close the window by using the close icon in the upper right corner of the window.

Deleting an Operational Plan

You cannot delete a version of an operational plan version unless you created the version. Deleting a version of a plan might impact the Problem Knowledge Base or deployment plans that reference the version. Before deleting a version, verify that the version is not being used.

To Delete a Version of an Operational Plan

1. Click Plan Management in the Navigation pane, then click Operational Plans.
2. In the center pane, highlight the plan you want to copy. The Operation Profiles are displayed in the center pane.
3. Click the Delete Version icon in the center pane.
4. Click Save.

An Operation Plan is a plan that defines one or more operations that are to be performed on a managed resource or group of resources. For example, deploying thresholds onto a managed resource, or performing state changing actions such as shutting down all logical domains and then shutting down an Oracle VM Server for SPARC.

To Delete an Operational Plan

1. Click Plan Management in the Navigation pane, then click Operational Plans.
2. In the center pane, highlight the plan you want to delete.
3. Click the Delete Operational Plan icon in the center pane.
4. Click Delete to confirm that you want to delete the plan.

12

Deployment Plans

Enterprise Manager Ops Center provides life cycle management services for all the deployment plans. After creating a plan, you can maintain its version, view, edit, copy and delete a plan.

About Deployment Plans

A deployment plan defines the sequence of operations or steps that must be carried out on an asset to deploy it together with the specification or profile that each step should apply and the resources that will be required to apply it such as network addresses, host names and so on.

A deployment template is an unbound deployment plan which defines the steps of execution but not the profiles and assets. Deployment templates are patterns from which deployment plans can be created. The software provides a comprehensive set of templates for all assets, including the virtualization platforms and virtual machines.

The deployment framework provides the user with necessary mechanism to create, configure, manage and execute customized deployment plans which enables the hardware, firmware and software provisioning activities in a repeatable fashion. You can create deployment plans from templates. For each plan loaded from the template, identify the profiles to satisfy each step. Each step can be associated with a profile or a plan but not both. Bind the profile or plan with each step. If you do not want to include a particular step, skip that step in the plan. You cannot arbitrarily add any steps to a plan. You can use only those steps that are defined in the template from which the plan is derived.

The settings and values in the profiles bound to each step are defaults and can be modified when the plan is actually applied. The profile settings and values can actually be further constrained by the target systems to which the plan is applied.

You have the following deployment templates:

- Configure M-Series Hardware, Create and Install Domain – Use this plan to configure a M-Series server, create dynamic system domains, provision OS on the domains and update the domains.
- Configure RAID – Use this plan to configure the RAID controller on your server.
- Configure Server Hardware and Install OS – Use this plan to configure a service processor or a chassis, provision OS and update the OS.
- Configure Service Processor – Use this plan to configure the service processor or your chassis.
- Configure and Install Dynamic System Domain – Use this plan to create dynamic system domains, provision and update OS on the domains.

- Configure and Install Logical Domains – Use this plan to create logical domains and provision OS on the logical domains.
- Create Dynamic System Domain – Use this plan to create only dynamic system domains.
- Create Logical Domains – Use this plan to create only logical domains.
- Install Server – Use this plan to provision and update the OS.
- Provision OS – Use this plan to provision OS.
- Software Deployment/Update – Use this plan to apply script based update profiles.
- Update Firmware – Use this plan to update the firmwares.

Apart from the deployment plans, you have Operational Plans that encapsulates monitoring profiles, operational profiles and problems knowledge base.

An operational plan uses a single operational profile, that contains and defines a shell script. An operational plan can run as a stand-alone plan, or as a step within a deployment plan. You can use operational plans to operate specific tasks in your environment, such as creating an alternate boot environment, or to run scripts to assist in problem management. See About Operational Profiles and Plans for more information about using operational plans.

The thresholds and monitoring configuration are derived as monitoring rules and monitoring profiles are created out of it. You can use the operational plans and monitoring profiles in the multi-step deployment plans for configuring your systems.

See Roles and Authorizations for information about permissions required to create and manage deployment plans.

Creating a Deployment Plan

You can create deployment plans from deployment templates and configure the plans using profiles. You can also use other plans leading to nested plans and complex plan management. See Complex Plan Management for detailed procedures about creating nested plans.

To Create a Deployment Plan

1. Select Plan Management section in the Navigation pane.
2. Select the appropriate plan in the Deployment Plan tree.
3. Select Create Plan from Template in the Actions pane. Create a Deployment Plan window is displayed.
4. Enter a name and description for the plan.
5. Select the type of failure policy. Failure Policy defines the course of action to be taken when there is a failure in the steps of plan execution.
6. In the Deployment Steps, select the profile or plan that needs to be applied for the step. The Associated Profile/Plan drop-down lists only the applicable profiles or plans for each step in the plan.
7. (Optional) Click the Create Profile icon if you want to create a profile for the plan. This option will take you to the corresponding profile creation wizard.

8. Provide any additional parameter required, if any. For Create Logical Domains plan, you can enter the number of logical domains to be created on applying the profile.
9. Click Save to save the plan.

Apply the plan to execute the steps on the system for the desired configuration.

Editing a Deployment Plan

You can edit the deployment plan details, alter the plan configuration by skipping steps in the plan, change the profile or plan bound to each step, or save the plan under a different name to create a new plan.

> **Note:** When you edit a deployment plan that is referred to by another plan, for example, in a nested plan, the referring plan is not automatically updated to refer to the edited plan's version. You must manually modify the referring plan if you want it to use the modified version.

To Edit a Deployment Plan

1. Select Plan Management from the Navigation pane.
2. You can use either of the way to select Edit Deployment Plan option:
   - Method 1 – Select the deployment type from the tree and select a plan from the list. The Edit Deployment Plan icon is enabled. Click the Edit Deployment Plan icon.
   - Method 2 – Expand the selected deployment type and select a plan from the list. The plan details are displayed. Select Edit Deployment Plan from the Actions pane. The Edit Deployment Plan window is displayed.
3. Edit the following details of the plan:
   - Plan Name – When you can modify the name of the plan, a new plan is created. Edit the name to create a new plan.
   - Description – Provide a description of the plan.
   - Failure Policy – Select whether you want the plan execution to stop at failure or complete as much as possible.
4. You can configure a step of the plan by setting or changing the associated profile, or by creating a new profile.
5. You can edit the plan by replicating the steps and associate targets depending on the type of plan selected, if any.
6. Click Save to save any changes made to the plan. If you have changed the name, a new plan will be saved with the version v1.

Copying a Deployment Plan

You can copy an existing deployment plan, rename it, and create a new plan.

To Copy a Deployment Plan

1. Select Plan Management from the Navigation pane.

2. You can use either of the way to select Copy Deployment Plan:
   - Method 1 – Select the deployment type from the tree and select a plan from the list. The Copy Deployment Plan icon is enabled. Click the Copy Deployment Plan icon.
   - Method 2 – Expand the selected deployment type and select a plan from the list. The plan details are displayed. Select Copy Deployment Plan from the Actions pane. The Create a Deployment Plan window is displayed.
3. Edit the following details of the plan:
   - Description – Provide a description of the plan.
   - Plan Name – By default, the plan name is Copy of <<plan name>>. If required, you can modify the name.
   - Failure Policy – Select whether you want the plan execution to stop at failure or complete as much as possible.
4. You can configure a step of the plan by setting or changing the associated profile, or by creating a new profile.
5. You can edit the plan by replicating the steps and associate targets depending on the type of plan selected, if any.
6. Click Save the new plan. A new plan will be saved with the version v1.

Deleting a Deployment Plan

You can delete a deployment plan or only a version of the plan. If the selected deployment plan is not referenced by any other plans, then you can confirm deleting the plan or its version. If the plan is used in other plans, then the Delete Deployment Plan option will not be enabled.

To Delete a Deployment Plan

1. Select Plan Management from the Navigation pane.
2. You can use either of the way to select Delete Deployment Plan option:
   - Method 1 – Select the deployment type from the tree. The plans of that type are listed in the center pane. Select a plan from the list. The Delete Deployment Plan and Delete Version icon is enabled. Click Delete Deployment Plan or Delete Version icon accordingly.
   - Method 2 – Expand the selected deployment type and select a plan from the list. The plan details are displayed. Select Delete Deployment Plan or Delete Version from the Actions pane. The Delete Plan window is displayed.
3. Click Delete to confirm the delete action.

13

Complex Plan Management

You can use a combination of profiles, deployment plans, and operational plans to create a complex deployment plan that enables you to automate a variety of detailed workflows into a single plan. This increases consistency and allows for a greater level of automation.

About Complex Plan Management

Enterprise Manager Ops Center provides you with the ability to create, configure, manage and execute deployment plans which drive the hardware, firmware and software provisioning activities in a repeatable fashion. You create plans from defined templates. Each plan defines the sequence of steps that need to be carried out for configuration or provisioning of a system. Plans may contain a single step or a sequence of multi-steps. Each step in the plan is configured by associating a profile or another plan.

Several deployment templates with multi-step sequences are available. These complex plans are aimed at providing the user with a configurable and repeatable way to do many common operations at a single click.

The following are the complex plans and templates provided by Enterprise Manager Ops Center:

- Configure M-series Hardware, Create and Install Domain
- Configure Server Hardware and Install OS
- Configure and Install Dynamic System Domain
- Configure and Install Logical Domains
- Install Server

When you create complex deployment plans, you can opt to skip a step in the plan. Skipped steps will not be processed when the plan is applied. You may also replicate certain steps in order to perform the same operation but using a different profile or nested plan. Both mechanisms provide flexibility to structure complex plans that meet your local requirements.

Configure M-Series Hardware, Create and Install Domain

This plan consists of the following steps:

1. Configure Service Processor – Service Processor profile
2. Update Firmware – Firmware profile

3. Create Dynamic System Domain – Dynamic System Domain profile (this step can be replicated)
4. Install and Update OS – Install Server plan (this step can be replicated)

Configure Server Hardware and Install OS

This plan consists of the following steps:

1. Configure Service Processor – Service Processor profile
2. Configure RAID Controller – RAID Controller profile
3. Update Firmware – Firmware profile
4. Install and Update OS – Install server plan

Configure and Install Dynamic System Domain

This plan consists of the following steps:

1. Create Dynamic System Domain – Dynamic System Domain profile (this step can be replicated)
2. Install and Update OS – Install Server plan (this step can be replicated)

Configure and Install Logical Domains

This plan consists of the following steps:

1. Create Logical Domains – Logical Domain profile (this step cannot be replicated, but can be configured to create multiple Logical Domains)
2. Install and Update OS – Install Server plan (this step can be replicated)

Install Server

This plan consists of the following steps:

1. OS Provision – OS Provisioning profile
2. Execute Pre-install – Script-type Profile (this step can be replicated)
3. Update OS – Update profile (this step can be replicated)
4. Install Applications – Install-type profile (this step can be replicated)
5. Update Applications – Update profile (this step can be replicated)
6. Execute Post-install – Script-type Profile (this step can be replicated)
7. Operation – Operational profile (this step can be replicated)
8. Monitoring – Monitoring profile

For more information about Update Profile types, see Update Profiles and Local Content for uploading any scripts and software packages.

Complex Plans

Enterprise Manager Ops Center provides several plans comprised of more than one step. Certain steps in these plans can be associated with another plan, the associated plan is referred to as a nested plan. These nested plans can be used as shared building blocks much in the same way as profiles are. Configuring a single nested plan once

and reusing it in many other plans will reduce the number of operations that need to be carried out by the user on the UI.

The plans that can be nested are:

- Install Server
- Provision OS (single step plan)

The following plans use the nested plans Install Server or Provision OS plans for provisioning OS:

- Configure and Install Dynamic System Domain
- Configure and Install Logical Domains
- Configure Server Hardware and Install OS

The Software Deployment plan is a multi-step plan that use associated profiles for each step.

The following complex plans are available:

- Configuring and Installing Dynamic System Domain
- Configuring and Installing Logical Domains
- Configuring Server Hardware and Installing OS
- Creating a Software Deployment Plan
- Installing Server

Configuring and Installing Dynamic System Domain

Configure and install dynamic system domain comprises procedure for configuring the dynamic system domains of M-series servers, provisioning OS on the dynamic system domains, updating the OS with the required patches, installing or updating any required applications, applying operational profiles and monitoring rules.

This plan consists of two steps:

1. Create Dynamic System Domain – You must associate a Create Dynamic System Domain profile to this step.
2. Install and Update OS – You can associate a simple Provision OS plan or a multi-step Install Server plan to this step.

Before You Begin

You need to have the following profiles and plan for creating and applying this plan:

- Create a dynamic system domain profile, as described in Creating a Dynamic System Domain
- Create an OS provisioning profile, as described in OS Provisioning Profiles and plan to provision the dynamic domains. Or, you can create an Install Server plan.

> **Note:** Ensure that you select the profile created for OS provisioning is for regular Oracle Solaris OS and the target type is Solaris SPARC.

To Create a Configure and Install Dynamic System Domain Plan

1. Select Plan Management from the Navigation pane.

2. Select Configure and Install Dynamic System Domain from Deployment Plans. The deployment template composition and any existing plans are displayed in the center pane.
3. Select Create Plan from Template option from the Actions pane. The Create a Deployment Plan window is displayed.
4. Provide a name and description for the new plan.
5. Select the failure policy for the plan to either stop at failure or complete as much as possible.
6. Select the profiles or plans for the Deployment Steps:
   - Create Dynamic System Domain - Select a profile from the list of applicable profiles for creating a dynamic system domain. You can replicate this step to create another domain. You must have unique profiles for each Create Dynamic System Domain step.
   - Install and Update OS - Select the plan from the list of applicable plans for installing OS on the domains. You can select a simple Provision OS plan or a multi-step Install Server plan. You can also replicate this step to select different install and update OS plan for each domain. Depending on the number of domains created, you can opt to select on which domains you want to apply different plans. Click on the Associate Targets icon to select the domains on which you want to apply this plan.
7. Click Save to save the deployment plan created.

   A new plan will be created with version 1.

See the *Oracle Enteprise Manager Ops Center User's Guide* for information about applying and viewing deployment plans.

Configuring and Installing Logical Domains

This plan provides steps to create logical domains and provision OS on each logical domains created. You can use this plan to target a one or more stand alone Oracle VM Servers, one or more Oracle VM Servers in a virtual pool, or multiple virtual pools to create one or more logical domains.

Before You Begin

You have to use the option Configure and Install Logical Domain option from Deployment Plan tree to create a logical domain and provision OS on it. This plan consists of Create Logical Domain profile and a nested plan to install and update the OS. You require the following profiles before creating a plan:

- Create a logical domain profile before creating a plan. See Logical Domain Profiles for a detailed procedure about creating a logical domain profile.
- Create an OS provisioning profile that is required to provision the logical domains. Either create an install and update OS plan, as described in Installing Server, or Provision OS plan. See OS Provisioning Profiles for detailed procedure for creating an OS provisioning profile. Ensure that you select the profile created for OS provisioning is for regular Oracle Solaris OS and the target type is Solaris SPARC.

To Configure, and Install a Logical Domain Plan

The following procedure describes how to create a configure and install logical domain plan:

1. Select Plan Management section from the Navigation pane.
2. Select Configure and Install Logical Domains from the Deployment Plan tree.
3. Select Create Plan from Template option from the Actions pane. The Create a Deployment Plan window is displayed.
4. Enter a name and description for the plan.
5. Select the type of failure policy. Failure Policy defines the course of action to be taken when there is a failure in the steps of plan execution.
6. Select profiles for the deployment steps as defined in the template. You can choose to select a profile or skip the step as required.
7. In the Create Logical Domain step, enter the number of logical domains to be created on the Oracle VM Server. The results of the step is displayed with the number of logical domains that can be created.
8. In the Install and Update OS step, select a plan from the list to provision and update the logical domains.
9. Click Associate Targets icon to associate the result of the source step to the destination step. The Associate Targets window is displayed. The result of the Create Logical Domain step is the number of logical domains to be created. You need to associate each of these resultant target to the Install and Update step to provision the OS on the logical domains.

   Note: You need to associate the resultant target to the next step only when the resultant target is more than one.

10. Click Save in the Associate Targets window.
11. Click Save in the Create Deployment Plan window. Deployment plan creation job is submitted and a plan is created at the end of a successful job.

See the *Oracle Enteprise Manager Ops Center User's Guide* for information about applying and viewing deployment plans.

Configuring Server Hardware and Installing OS

This plan covers all the essentials of bringing a server into a production state in your data center. If the requirements of the server and OS configuration are captured with corresponding profiles, this plan can be created and applied onto a system. The configure server hardware and install OS plan template consists of the following steps:

1. Configure Service Processor
2. Configure RAID Controller
3. Update Firmware
4. Install and Update OS

Before You Begin

You have to discover and manage the server on which you want to apply this plan. If your server is a bare-metal, refer to Declare Configured Assets or Declare Unconfigured Assets to discover the servers. After discovery, manage the hardware to enable the functions available for it. Import the required OS image that you want to use for provisioning.

You need to create the following profiles and plans:

- Configure service processor Configure service processor profile, as described in Configuring a Service Processor
- Configure RAID controller profile, as described in Configuring a RAID Controller
- Update firmware profile, as described in Configuring Firmware Updates
- Install and update OS plan, as described in Installing Server

To Create a Configure Server Hardware and Install OS Plan

1. Select Plan Management section from the Navigation pane.
2. Expand Deployments Plan and select Configure Server Hardware and Install OS plan type. The plan template composition and existing plans are listed in the center pane.
3. Select Create Plan from Template from the Actions pane. The Create Deployment Plan window is displayed.
4. Provide a name and description for the plan.
5. Select the failure policy for the plan to either stop at failure or complete as much as possible during execution.
6. Select the profiles or plans for the Deployment Steps:
   - Configure Service Processor - Select a profile from the list of applicable profiles for service processor configuration.
   - Configure RAID Controller - Select a profile from the list. When you re-configure an existing RAID controller, all the data on the disk will be lost.
   - Update Firmware - Select an update firmware profile.
   - Install and Update OS - Select an install server plan to install and update the OS.
7. Click Save to create the deployment plan. A new plan will be created with version 1.

See the *Oracle Enteprise Manager Ops Center User's Guide* for information about applying and viewing deployment plans.

Creating a Software Deployment Plan

This plan is for applying your update profiles that have been created using system-defined profiles, custom-defined profiles, and local contents such as pre-action scripts, post-action scripts, and software packages.

The software deployment/update plan comprises the following steps:

- Execute pre-install – The update profiles that are of script type are listed. You can upload scripts using the local content. Create an update profile of type Script. You can select those profiles from this list.
- Update OS – The update profiles that contains system-defined or custom-defined profiles for updating the OS.
- Install software – The update profiles that contains the software packages for installation.
- Update software – The update profiles that contains packages or updates for updating a software packages.

- Execute post-install – The update profiles that are of script type are listed. It is similar to Execute pre-install step.

Before You Begin

You can create this plan for applying the update profiles that have created for applying scripts and packages. Ensure that you have the appropriate profiles for creating this plan.

Ensure that when you create update profiles you specify the appropriate profile type as Install, Upgrade or Script. Script profiles may be used on Execute Pre-install and Post-install steps. Update profiles may be used on Update steps and Install profiles may be used on Install steps. Only profiles of the appropriate type will be available in the list of available profiles for these steps.

Note: The default policy is set to yes to install any update dependencies while applying a profile.

To Create a Software Deployment Plan

1. Select Plan Management section in the Navigation pane.
2. Select Software Deployment/Update plan type in the Deployments Plan tree. The steps details of the plan are displayed in the center pane.
3. Select Create Plan from Template in the Actions pane. The Create Deployment Plan window is displayed.
4. Provide a name and description for the plan.
5. Select whether the plan should complete as much as possible or stop at failure for failure policy.
6. Select the required steps of the plan. Leave others as skipped. The plan comprises the following steps:
   a. Execute Pre-Install – The update profile to execute a pre-action script before installing any software packages or updates. This step may be replicated if more than one script needs to be executed.
   b. Update OS – The update profile to install, remove or upgrade any patches of the OS. This step may be replicated if more than one update is required.
   c. Install Software – The update profile to install any software applications. This step may be replicated if more than one application installation is required.
   d. Update Software – The update profile to update any software applications. This step may be replicated if more than one application update is required.
   e. Execute Post-Install – The update profile to install any scripts after installing any software packages or updates. This step may be replicated if more than one script needs to be executed.
7. Click Save to create the new deployment plan.

See the *Oracle Enteprise Manager Ops Center User's Guide* for information about applying the deployment plans. See Update Profiles to create any update profile. See Local Content for uploading any scripts and software packages.

Installing Server

This plan comprises the steps to provision an OS, update the OS, install and update any applications, apply operational profiles and set monitoring rules and parameters for the OS.

The plan template composition is:

- OS provisioning profile
- Execute pre-install – The update profiles that are of script type are listed. You can upload scripts using the local content. Create an update profile of type Script. You can select those profiles from this list.
- Update OS – The update profiles that contains system-defined or custom-defined profiles for updating the OS.
- Install software – The update profiles that contains the software packages for installation.
- Update software – The update profiles that contains packages or updates for updating a software packages.
- Execute post-install – The update profiles that are of script type are listed. It is similar to Execute pre-install step.
- Operation profile
- Monitoring profile

Before You Begin

See the following sections for creating the required profiles:

- OS Provisioning Profiles
- Update Profiles for updating and OS and application profiles
- Local Content for install applications profile
- Operational Profiles
- Monitoring Profiles

To Create an Install Server Plan

1. Select Plan Management section from the Navigation pane.
2. Expand Deployments Plan and select Install Server plan. The plan template composition and existing plans are displayed.
3. Select Create Plan from Template from the Actions pane. The Create a Deployment Plan window is displayed.
4. Provide a name and description for the plan.
5. Select the failure policy for the plan to either stop at failure or complete as much as possible.
6. Select the profiles for the Deployment Steps:
   - Os Provision – Select an OS provisioning profile to provision the OS.
   - Execute Pre-install – Select a software update script profile for a custom local pre-action script. This step might be replicated if more than one script needs to be executed.

- Update OS – Select an update profile to apply the required patches to the OS. The update policy is set to default Yes for the dependencies that must be installed for a patch. This step might be replicated if more than one update is required.
- Install Software – Select a software installation profile that comprises installation of a software package. This step might be replicated if more than one application installation is required.
- Update Software – Select a software update profile that comprises update to an installed software package. This step might be replicated if more than one application update is required.
- Execute Post-install – Select an update script that consists of custom local post-action script. This step might be replicated if more than one script needs to be executed.
- Operation – Select an operational profile for automating some of the process actions.
- Monitoring – Select a monitoring profile that defines the system thresholds and setting up alert monitors.

7. Click Save to save the plan. A new plan will be created with version 1.

See the *Oracle Enteprise Manager Ops Center User's Guide* for information about applying and viewing deployment plans.

A

Scenario – Deploying a Bare-Metal System

This scenario describes the steps required in Ops Center to deploy a bare-metal system in your data center. Deploying a bare-metal system in the data center involves the following steps in Ops Center:

- Discovering the service processor
- Configuring the service processor
- Provisioning the OS
- Updating the OS

Scenario Assumptions

Discovering the bare-metal server depends on the network information that is available for the service processor. You must use Custom Discovery, Declare Configured Assets or Declare Unconfigured Assets procedure accordingly to discover your bare-metal server.

The following are the assumptions in carrying out the bare-metal deployment:

- The bare-metal is an unconfigured SPARC T3-1 server.
- Use Declare Unconfigured Assets procedure to discover the bare-metal server.
- The required Solaris 10 OS image is imported into Enterprise Manager Ops Center library for provisioning.
- Configure Server Hardware and Install OS plan is used to configure the discovered service processor and provision the OS.

Plans and Profiles

The Configure Server Hardware and Install OS plan consists of the following steps:

- Configure service processor
- Configure RAID controller
- Update firmware
- Install and Update OS

For each step in the profile, you must select the appropriate profile or plan. If you do not want to apply any step, you can simply skip the step in the plan. This scenario requires the following steps of the plan:

- Configure Service Processor

- Install and Update OS

The list of profiles that are required to create the plan:

- Configure Service Processor
- Provision OS

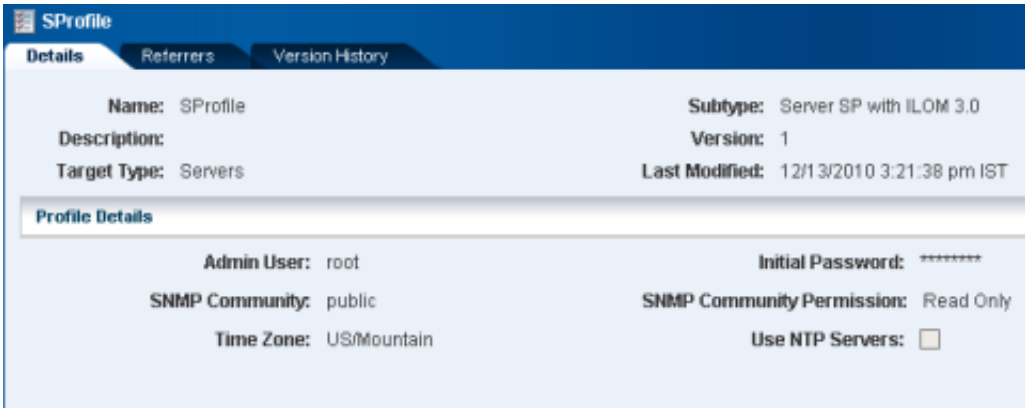
Service Processor Profile Parameters

Use the following information for creating a service processor profile:

- Processor Subtype – Server SP with ILOM 3.0. The server is a SPARC T3-1 which has ILOM configuration.
- Provide a new password.
- If you want to use DNS, provide the IP addresses of three DNS servers, 6 domains names, number of retries, and timeout in seconds.

See Configuring a Service Processor to create a profile.

A sample format of the service processor profile is provided in this illustration.



OS Provisioning Profile Parameters

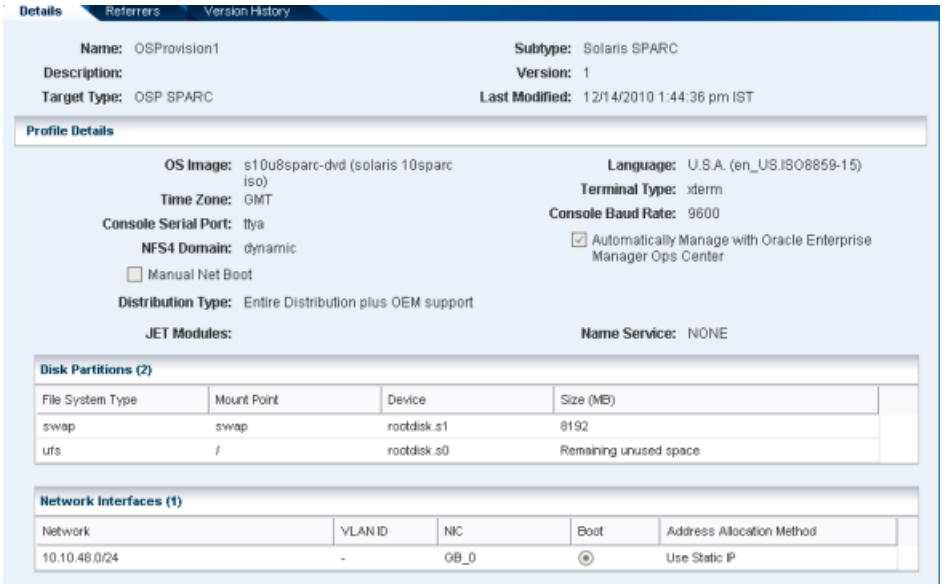
Use the following information for creating an OS provisioning profile:

- OS image – Oracle Solaris 10 image
- OS distribution type – Entire Distribution plus OEM Support
- Language – U.S.A(en_US.ISO8859-15)
- Time Zone – US/Pacific
- Terminal Type – xterm
- Console Serial Port – ttya
- Console Baud Rate – 9600
- JET Modules – None
- Name Service – None
- Automatically Manage with Oracle Enterprise manager Ops Center – Select this option to install the agent. Ensure that the distribution selected is not lower than End user distribution.

- Disk partitions – Provide the disk space for swap and root file system.
- Network – Select the network and the NIC.

See OS Provisioning Profiles to create an OS provisioning profile.

A sample format of the OS provisioning profile is provided in this illustration.



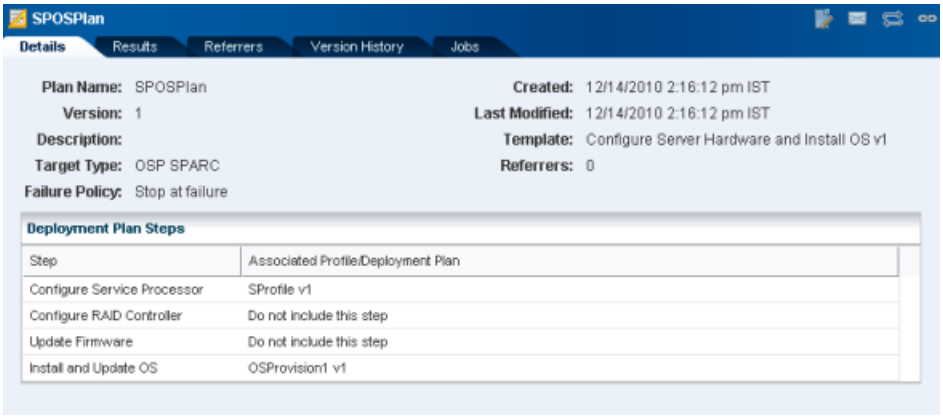
To Create a Configure Server Hardware and Install OS Plan

To Create a Configure Server Hardware and Install OS Plan

1. Select Plan Management section from the Navigation pane.
2. Select Configure Server Hardware and Install OS plan from the Deployments Plan tree.
3. Select Create Plan from Template from the Actions pane. The Create a Deployment Plan window displays.
4. Provide a name and description for the plan. For example, the name of the plan can be "sposplan".
5. Select a failure policy for the job that runs the plan.
6. In the Deployment Plan Steps, select the associated profiles or plans for the following steps:
   - Select the profile from the list for Configure Service Processor.
   - Select the plan for Install and Update OS. Select Do not include this step for all other steps.
7. Click Save to create the deployment plan.

The configure server hardware and install OS plan will be created and listed under the deployment tree.

A sample plan is illustrated in this figure.



To Apply the Configure Server Hardware and Install OS Plan

1. Select Plan Management section from the Navigation pane.
2. Select Configure Server Hardware and Install OS plan from the Deployment Plan tree.
3. Select the plan "sposplan" from the list. The plan details are displayed in the center pane.
4. Select Apply Deployment Plan from the Actions pane. The Select Target Assets window displays.
5. Select the server from the available list of items.
6. Click Add to Target list to add the selected server to the target list.
7. Select how you want to apply the plan:
   - Apply with minimal interaction - This is to accept the already set profile values and enter only the required resources at the time of application.
   - Allow me to override any profile values - This is to modify any set profile values.
8. Click Next to display the Configure Server Hardware and Install OS wizard.

You must provide the IP address during network resource assignment, complete the wizard and apply the plan.