Oracle® Enterprise Manager Ops Center

Provision and Update Guide,

11*g* Release 1 Update 3 (11.1.3.0.0)

E18417-04

November 2011

Oracle Enterprise Manager Ops Center Provision and Update Guide 11*g* Release 1 Update 3 (11.1.3.0.0)

E18417-04

Primary Author: Shanthi Srinivasan

Contributing Author: Laura Hartman, Barbara Higgins

Contributor:

Contents

5 Updating a Windows OS

6 Oracle Solaris Live Upgrade

7 Upgrading an Oracle Solaris Cluster

8 Firmware and OS Update Reports

B Sample JET Template

Preface

The Oracle® Enterprise Manager Ops Center Provision and Update Guide describes how to provision and update firmware and operating systems in your data center using Enterprise Manager software.

Audience

This document is intended for 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 System*
- *Oracle Enterprise Manager Ops Center User's Guide*
- *Oracle Enterprise Manager Ops Center Advanced User's 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*
- *Oracle Enterprise Manager Ops Center Security 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, file names, and directories within a paragraph, and code in examples.

1 Overview

Enterprise Manager Ops Center provides a comprehensive data center management solution for managing your physical and virtual systems in the data center. This software enables you to discover, provision, patch, virtualize, manage, and monitor the assets in your data center from a single browser user interface (UI).

Once you discover and manage your assets in Enterprise Manager Ops Center, provisioning and patching options are enabled for the assets. This guide takes you through the various options and procedures for provisioning and updating your systems using Enterprise Manager Ops Center.

The following sections provide a brief description of the chapters discussed in this guide.

Provisioning

OS Provisioning enables you to install operating systems onto systems that are attached to your network, making it easy to install one or many systems simultaneously. It does not require any manual interaction with the system to install the OS. All the actions can be performed on the system right from the Enterprise Manager Ops Center UI. You can automate the installation of the OS on your servers across the data center to maintain consistent configuration. You can even provision bare-metal systems from Enterprise Manager Ops Center.

There are three main tasks before provisioning an OS or firmware:

- Import the required OS and firmware image and maintain them in the image library.
- Create OS provisioning profiles that are applicable for different targets.
- Apply the profile to provision the firmware or OS.

The provisioning profiles collects all the information such as type of target, OS image, timezone and language setup, required JET modules, disk partitions, naming services and network details. Apply the profile on the selected server and install the OS.

You can provision and update the following operating systems in Enterprise Manager Ops Center:

- Oracle Solaris 8, 9, and 10
- Oracle Linux
- Red Hat Enterprise Linux
- SUSE Enterprise Linux

For detailed concepts and procedures, refer to Provisioning Firmware and Provisioning an OS.

Updating

After provisioning OS on your systems, it is essential to maintain your assets to the recommended and latest updates. To maintain your assets to latest updates, you must apply patches to your systems. Updating or patching is a complex task in a data center for an administrator. It involves downloading the patches from the appropriate vendor sites, look out for patch dependencies, testing your patches for the production environment, rollback your systems to previous state if the patch is not stable in your environment, and maintain consistent component configuration of your systems to the latest security updates.

Enterprise Manager Ops Center provides one stop solution for all the requirements for patching your assets. It provides you Update Profiles and Policies that help define which components must be installed and the level of automation of patch installation. Enterprise Manager Ops Center provides system catalogs that records the state of the system at any point of time. You can use these catalogs to rollback your systems to any previous configurations, or create a update profile out of it for consistent configuration in a data center.

Enterprise Manager Ops Center also provides solutions to update assets when the Enterprise Controller is in the disconnected mode.

For detailed information and procedures, refer to Updating an OS and Updating a Windows OS.

Solaris Live Upgrade

Solaris Live Upgrade technology enables you to run the Oracle Solaris OS normally while an administrator upgrades or performs normal maintenance on an inactive boot environment. This reduces the downtime required to update your OS and enables you to test the update before using it in the production environment.

You require a boot environment and alternate boot environment (ABE) to test the patches and apply the patches. You can create an ABE or use ABE that was created outside the Enterprise Manager Ops Center. It automatically discovers and manages the alternate boot environment, if any.

You can view the different environments, manage the environments, run update jobs on the ABE, synchronize the boot environments, and activate the alternate boot environment as the active boot environment.

See Oracle Solaris Live Upgrade for more information about Live Upgrade.

Reporting

Reports help to check the compliance of the assets for the latest and recommended updates, and other audit purposes. There are variety of reports that can be generated for all types of OS. You can save the report templates and use them later. Enterprise Manager Ops Center provided interactive result viewer to view the report results. From result viewer, you can even initiate update jobs to make the systems compliant. You can download and save the report results in different formats such as CSV and PDF.

You can schedule the reports to be generated at required time period and intervals.

See Firmware and OS Update Reports for detailed procedure about creating reports for various operating systems.

2 Provisioning Firmware

The Enterprise Manager Ops Center provisioning feature installs firmware on the managed hardware assets. You initiate the installations from the UI, rather than from the asset itself.

About Firmware Provisioning

The general procedure for provisioning firmware has the following steps:

1. Import a file with the firmware and the associated metadata into a storage library. See *Oracle Enterprise Manager Ops Center Advanced User's Guide* for uploading firmware images.
2. Create a firmware profile, based on one or more firmware images.

   See *Oracle Enterprise Manager Ops Center Advanced User's Guide* to create a firmware profile and add images to the profile.
3. Shut down the server gracefully. Most firmware requires that the server is not running when the firmware is updated. Most firmware images include a power-off command for a running server, which causes a hard shutdown of the server.
4. Apply the firmware profile, as described in Updating Firmware, or create a deployment plan that includes the profile.

An alternate procedure is to import the firmware file and then create a Firmware Report. You then use the report results to update the firmware. See Using the Firmware Compliance Report.

The benefit of using a profile to install firmware is that the firmware is installed consistently, no matter how many assets you provision. The benefit of using the Firmware Report is to determine the condition of the firmware on a specific asset or set of assets.

Updating Firmware

To update the firmware on an asset, you execute an deployment plan, which includes a firmware profile for the type of asset. For a server, the plan includes a profile that updates the firmware on a service processor. For storage components, the plan includes profiles that update firmware on a RAID controller, an expander, or disk. To see the deployment plans that update firmware, expand the Deployment Plans section of the Navigation pane and then click Firmware. A list of existing plans is displayed. A default plan and a default profile is created for a firmware image when it is imported into Enterprise Manager Ops Center. As an alternative, if you are updating the firmware of one asset, you can use the Update Firmware action to apply a firmware profile. Select the service processor from the Asset section of the Navigation pane and click the Update Firmware menu item in the Actions pane

Before You Begin

If you are updating the firmware on a server, shut down the server before you update the firmware. A firmware update to a server's service processor usually requires that the server is not running. If you start to update the firmware on a running server's service processor, the firmware image performs a hard shutdown of the server.

If a network failure occurs while updating the firmware, repeat the firmware update procedure. If you do not repeat the procedure, the firmware inventory list might be incomplete.

To Update the Firmware

1. Expand Plan Management in the Navigation pane.
2. Expand Deployment Plans and click Firmware. A list of existing plans is displayed. If no plans exist, create a deployment plan.

   See *Oracle Enterprise Manager Ops Center Advanced User's Guide* for information about creating a deployment plan.
3. Select a plan. The details of the plan, including the profiles it uses, are displayed. By default, the firmware is updated according to values in the profile without any interaction.
4. 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.
5. Click Apply the Deployment Plan in the Actions pane. The Update Firmware wizard starts and displays a list of assets.
6. Select one or more assets 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.
7. Review the attributes of the firmware. Click Next. The Summary page shows the values in the profile and the list of targets.
8. Review the Summary page and when you are ready to update the firmware on the target assets, click Apply. The update job is submitted. The plan updates the firmware, according to the profile.

Viewing the Firmware Version

The Summary and Hardware tabs in the center pane show the current firmware version. Enterprise Manager Ops Center refreshes the information every 30 minutes. To see the current firmware version before the next interval:

- If you updated the firmware through the UI, refresh the browser.
- If you have updated the firmware manually, click Refresh in the Actions pane. When the Refresh job completes, the current firmware version is displayed.

3

Provisioning an OS

You can provision different types of targets using this software. You must create profiles to capture the provisioning requirements. You can create the following OS provisioning profiles:

- Oracle VM Server for SPARC
- Oracle Linux
- Red Hat Linux
- SUSE Linux
- JET Template
- Solaris SPARC
- Solaris x86

About OS Provisioning

Enterprise Manager Ops Center's provisioning feature installs operating systems on the managed systems, automatically and consistently. When you want to initiate OS provisioning through the service processor, it does not require manual intervention except for manual netboot option. You initiate the installations from the UI.

OS provisioning is handled by a deployment plan, which can be single step or multi-step plan. For a profile that requires the OS image, Enterprise Manager Ops Center retrieves the OS image from the Software Library and uses it to provision the target servers. The Software Library is located either in a directory on the Enterprise Controller or on a Network Attached storage appliance that the Enterprise Controller can access.

The general procedure for provisioning an OS has the following steps:

1. Import a file with the OS image into a Software Library. The process creates a provisioning profile.
2. Use a deployment plan that includes the profile. Create a plan if it does not exist.
3. Apply the deployment plan on the targets.

Importing OS images and creating OS profiles are one-time tasks for each OS configuration to provision. After an OS image and an associated OS profile are created, you can use deployment plans to provision the OS onto many managed systems.

Enterprise Manager Ops Center enables OS provisioning on single systems, groups of systems, a combination of the single systems and groups, and Oracle Solaris Clusters.

OS provisioning for groups of systems requires using homogeneous groups, as described in *Oracle Enterprise Manager Ops Center User's Guide*.

For provisioning an Oracle Solaris Cluster, you provision the same OS on all nodes of a cluster. The Cluster OS Profile profile handles the pre-action and post-action operations.

About OS Provisioning Subtypes

Using Ops Center, you can provision different types of targets. You can create OS provisioning profiles for the following:

- Oracle VM Server for SPARC
- Oracle Linux
- Red Hat Linux
- SUSE Linux
- JET Template
- Solaris SPARC
- Solaris x86

This section describes some additional parameters that must be defined while provisioning Oracle VM Server for SPARC, Oracle Linux, Red Hat Linux, SUSE Linux, and JET Template.

Oracle VM Server for SPARC

You can create profiles for installing Oracle VM Server Control Domain. You must define the following parameters while creating this profile:

- CPU Threads
- Memory
- Crypto Units
- Virtual Console Port Range
- Enable JASS
- Enable Multiplexed I/O

Enabling JASS results in installation of SUNWJass package to harden the system. This option is supported only for installing Oracle VM Server 1.2 or lower versions. 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.

Enabling multiplexed I/O results in enabling the Fibre Channel ports on the system that is configured for storage.

Oracle Linux and Red Hat Linux

You must define the following parameters for creating profiles for provisioning Oracle Linux and Red Hat Linux:

- Installation number – You can enter the installation number that is used to allow installation of all of the Red Hat 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 to include or exclude during provisioning. To include a package, enter the package name in a line. To exclude any package, enter the package name preceded by a dash (-).

SUSE Linux

You must define the following parameters for provisioning SUSE Linux OS:

- FTP proxy server – Enter the name of the FTP proxy server to support FTP services.
- HTTP proxy server – Enter the name of the HTTP proxy server to support HTTP services.
- Install protocol – Specify HTTP or NFS as the install protocol.
- Enable proxy servers – Select this option to enable the FTP and HTTP proxy servers that you specified in the FTP Proxy Server and HTTP Proxy Server fields.
- Kernel parameters – Enter kernel parameters for the GRUB menu of the target system, if necessary.
- Reboot action – Select whether you want to reboot the target system after OS installation.
- Linux packages – You can specify the Linux packages to include or exclude during provisioning. To include a package, enter the package name in a line. To exclude any package, enter the package name preceded by a dash (-).

JET Templates

You must select the JET template which defines all the parameters for OS provisioning. See Using JET for OS Provisioning for more information about creating an OS profile with JET template.

Preparing to Provision an OS

Before You Begin

- Import the image to Enterprise Manager Ops Center.

  See *Oracle Enterprise Manager Ops Center Advanced User's Guide* for information about importing images into Enterprise Manager Ops Center.

- Create an OS profile for the target systems. Creating an OS Profile for Provisioning Solaris OS, Creating an OS Profile for Provisioning Linux OS, and Using JET for OS Provisioning describe ways to create OS profiles.

- Discover the service processors of the target systems. You can use Custom Discovery option to discover the service processor.

  See *Oracle Enterprise Manager Ops Center Advanced User's Guide* for information about using custom discovery method to discover the service processor.

- Disable monitoring for the target systems to prevent events related to a system going offline. See Disabling System Monitoring for more information.

- Verify that the Dynamic Host Configuration Protocol (DHCP) services are enabled on Proxy Controllers. You cannot create a profile or assign any network if the DHCP services are not enabled. The Install Server option to provision OS on a server is not enabled if the DHCP is not enabled on any of the interfaces.

- If you are provisioning a dynamic system domain of an M-Series server, the domain must have an IP address.

Disabling System Monitoring

To disable the monitoring of a system, you uninstall its agent software.

1. Select Assets from the Navigation pane. The All Managed Assets list is displayed.
2. On the system that you want to provision, select the OS instance.
3. Click the Unmanage/Delete Asset icon. The Unmanage and Delete Asset wizard is displayed.
4. Read the Introduction and click Next. The Enter Server Credential pane is displayed.
5. Enter the ssh user name and password for the root or privileged user on the target system.
6. Select an option that controls how the credentials apply to the listed assets. Click Next:
   - Use the Same ssh Username and Password for All Assets Listed Below
   - Use Different ssh Username and Password for All Assets Listed Below
7. In the Unmanage/Delete panel, verify that the correct system to unmanage is listed. Click Next. The Summary pane is displayed.
8. Click Unmanage/Delete Asset to submit the job to unmanage and delete the selected asset.

Creating an OS Profile for Provisioning Solaris OS

You can create OS profiles for provisioning 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 profile.

Before You Begin

- Import the required OS image.
- 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. See Installing JET Modules for more information about installing JET modules.
- 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 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 according to 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 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 require additional package dependencies to be added.

8. Select Include Custom Scripts to add any scripts. Specify the scripts 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 fails.

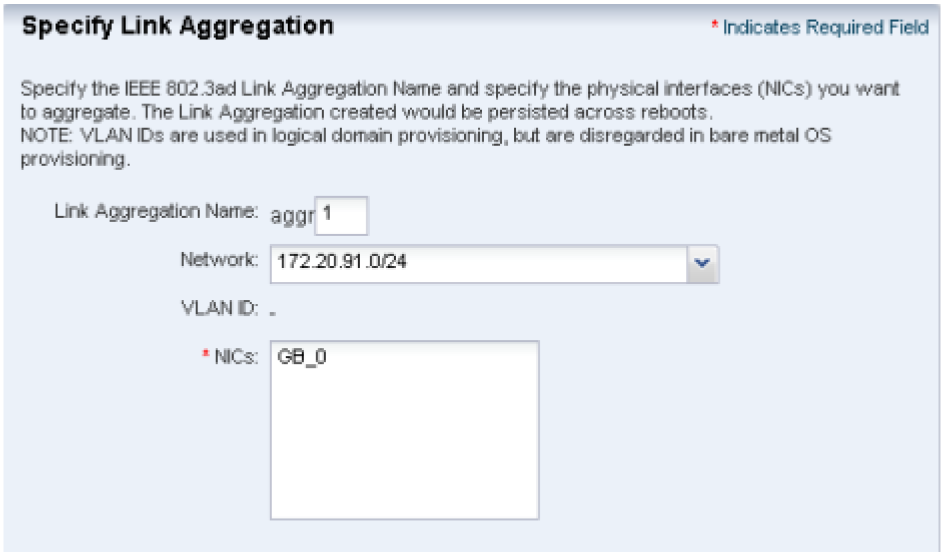
13. Click Next to specify the JET modules and parameters.
14. Enter a comma-separated list of JET module names. Enter the names of any additional JET modules that you have installed on the Proxy Controller to perform the provisioning operations described by this profile. The base_config, custom, and 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 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, define the following information in Specify Link Aggregation:

Figure 3–1 Specifying Link Aggregation



Specify Link Aggregation

* Indicates Required Field

Specify the IEEE 802.3ad Link Aggregation Name and specify the physical interfaces (NICs) you want to aggregate. The Link Aggregation created would be persisted across reboots.
NOTE: VLAN IDs are used in logical domain provisioning, but are disregarded in bare metal OS provisioning.

Link Aggregation Name: aggr 1

Network: 172.20.91.0/24

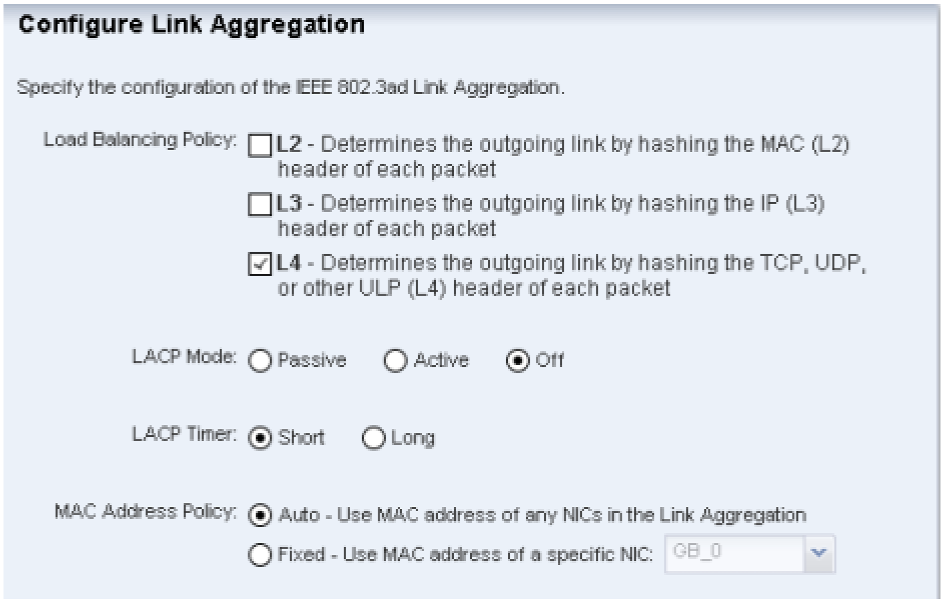
VLAN ID: -

* NICs: GB_0

- Link Aggregation Name – The name of the Link Aggregation is set as aggr. Add a number to it to differentiate from other aggregation.
- Network – Select a network from the list.
- NICs – List out the physical interfaces of the selected network the must be configured as a single logical unit. Click Next to configure the link aggregation.

26. Configure the IEEE 802.3ad Link Aggregation with the following parameters in Configure Link Aggregation:

Figure 3–2 Configuring Link Aggregation



Configure Link Aggregation

Specify the configuration of the IEEE 802.3ad Link Aggregation.

Load Balancing Policy:
□ **L2** - Determines the outgoing link by hashing the MAC (L2) header of each packet
□ **L3** - Determines the outgoing link by hashing the IP (L3) header of each packet
☑ **L4** - Determines the outgoing link by hashing the TCP, UDP, or other ULP (L4) header of each packet

LACP Mode: ○ Passive ○ Active ● Off

LACP Timer: ● Short ○ Long

MAC Address Policy:
● Auto - Use MAC address of any NICs in the Link Aggregation
○ Fixed - Use MAC address of a specific NIC: GB_0

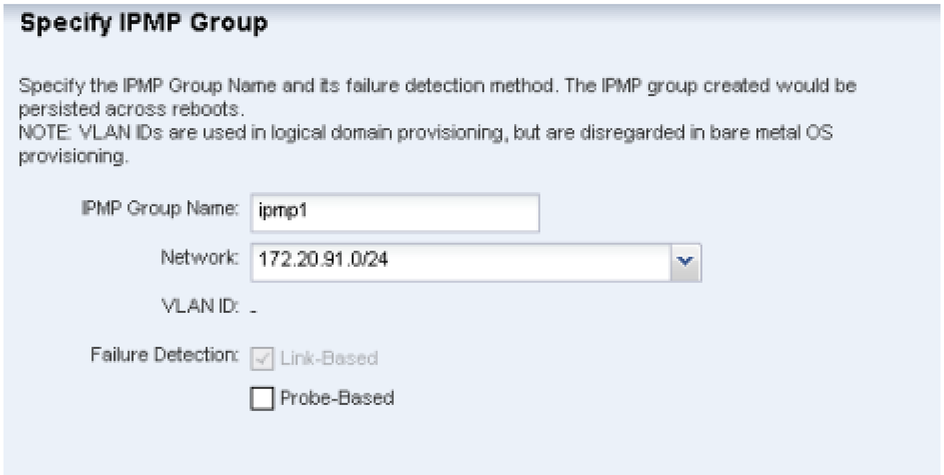
- Load Balancing Policy – Define the policy for outgoing traffic.
- Aggregation Mode and Switches – If the aggregation topology involves connection through a switch, you must note whether the switch supports the

link aggregation control protocol (LACP). If the switch supports LACP, you must configure LACP for the switch and the aggregation. Define a mode in which LACP should operate.

- MAC Address Policy – Define whether the MAC address of the NICs are fixed or not.

27. To use IPMP, define the following information in Specify IPMP Group:

Figure 3–3 Specifying IPMP Group



Specify IPMP Group

Specify the IPMP Group Name and its failure detection method. The IPMP group created would be persisted across reboots.
NOTE: VLAN IDs are used in logical domain provisioning, but are disregarded in bare metal OS provisioning.

IPMP Group Name: ipmp1

Network: 172.20.91.0/24

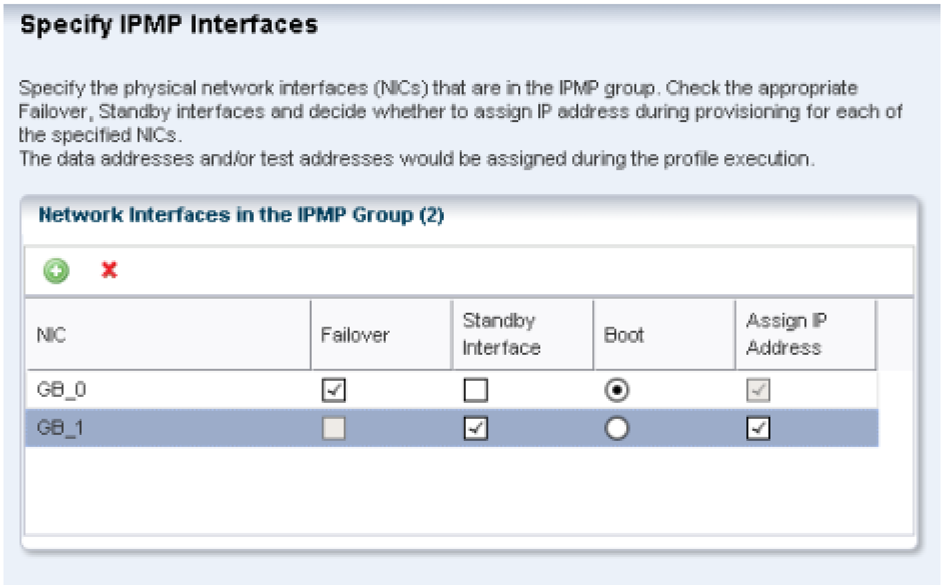
VLAN ID: -

Failure Detection: ☑ Link-Based
□ Probe-Based

- 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. To include Probe based detection, select Probe based option. Click Next to specify the IPMP interfaces.

28. Define the following information in Specify IPMP Interfaces:

Figure 3–4 Specifying IPMP Interfaces



Specify IPMP Interfaces

Specify the physical network interfaces (NICs) that are in the IPMP group. Check the appropriate Failover, Standby interfaces and decide whether to assign IP address during provisioning for each of the specified NICs.
The data addresses and/or test addresses would be assigned during the profile execution.

Network Interfaces in the IPMP Group (2)

NIC	Failover	Standby Interface	Boot	Assign IP Address
GB_0	☑	□	●	☑
GB_1	□	☑	○	☑

- 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.

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

29. If you have selected none for networking option, select a DHCP enabled network interface for the boot interface in Select Networks.
30. Click the Add icon to add multiple networks. 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.
31. Click Next to view the Summary of the parameters selected for Solaris OS provisioning.
32. Review the parameters and click Finish to save the profile. The profile is created for provisioning Solaris OS.

Creating an OS Profile for Provisioning Linux OS

You can create OS profiles for provisioning 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 profile.

You can provision the following Linux operating systems:

- Oracle Linux
- Red Hat Linux
- SUSE Linux

Before You Begin

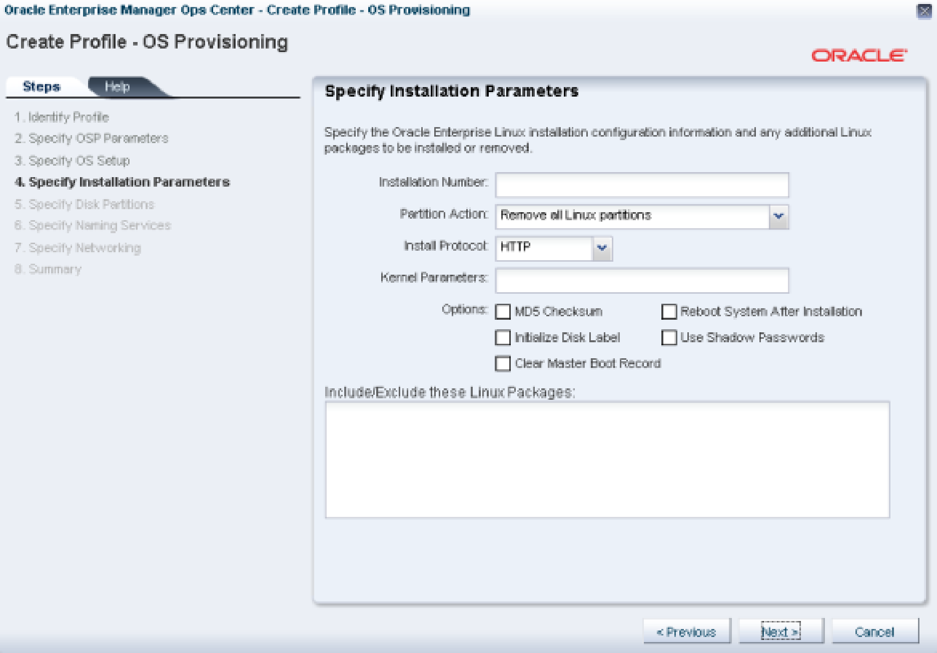
- Import the required OS image.
- Verify that any scripts the profile uses are in a directory that the Ops Center Enterprise Controller can access. Scripts can be located in a local directory of the Enterprise Controller, or in a directory that the Enterprise Controller mounts using NFS.

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 Oracle Linux, Red Hat Linux or SUSE Linux according to 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 to add any scripts. Specify the scripts 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 and Red Hat Linux, specify the following parameters:

Figure 3–5 Specifying Installation Parameters for Linux OS


Oracle Enterprise Manager Ops Center - Create Profile - OS Provisioning
ORACLE
Steps
Help
< Previous
Next >
Cancel

Create Profile - OS Provisioning

1. Identify Profile
2. Specify OSP Parameters
3. Specify OS Setup
4. **Specify Installation Parameters**
5. Specify Disk Partitions
6. Specify Naming Services
7. Specify Networking
8. Summary

Specify Installation Parameters

Specify the Oracle Enterprise Linux installation configuration information and any additional Linux packages to be installed or removed.

Installation Number:

Partition Action: Remove all Linux partitions

Install Protocol: HTTP

Kernel Parameters:

Options: □ MD5 Checksum □ Reboot System After Installation □ Initialize Disk Label □ Use Shadow Passwords □ Clear Master Boot Record

Include/Exclude these Linux Packages:

- Installation number – You can enter the installation number that is used to allow installation of all of the Red Hat 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 multiple networks. 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.

   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.

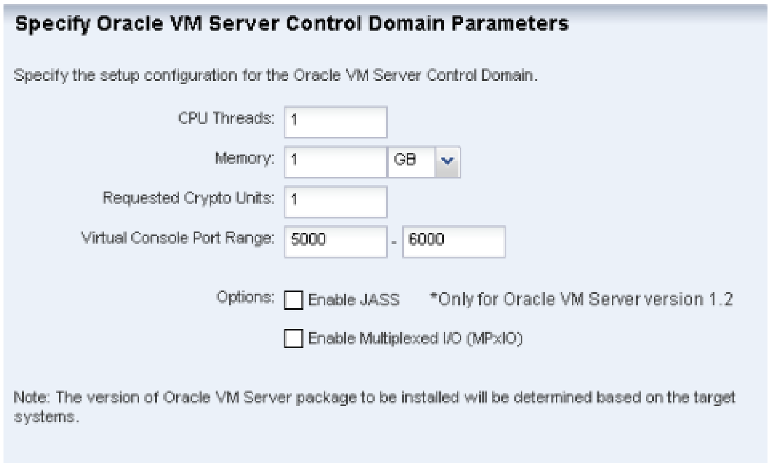
> **Note:** Ensure that for systems to be managed, you have selected the appropriate Distribution Type. Otherwise, the OS provisioning job can fail.

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:

Figure 3–6 Setting Up Control Domain Parameters



Specify Oracle VM Server Control Domain Parameters

Specify the setup configuration for the Oracle VM Server Control Domain.

CPU Threads: 1

Memory: 1 GB

Requested Crypto Units: 1

Virtual Console Port Range: 5000 - 6000

Options: □ Enable JASS *Only for Oracle VM Server version 1.2

□ Enable Multiplexed I/O (MPxIO)

Note: The version of Oracle VM Server package to be installed will be determined based on the target systems.

- 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 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.

Using JET for OS Provisioning

JumpStart Enterprise Toolkit (JET) provides a framework to simplify and extend the JumpStart functionality provided within the Oracle Solaris operating system. The JET framework is supplied in a single package called SUNWjet, which is automatically installed during OS provisioning. You can extend the functionality by adding modules, which are also supplied in package format.

> **Note:** Install JET modules only on Proxy Controllers that run Oracle Solaris OS. Do not attempt to install JET modules on Proxy Controllers that run the Red Hat Enterprise Linux OS.

The Oracle Solaris operating system includes the SUNWjet package, which installs the base_config, custom, and flash JET modules, but you must install any additional JET modules onto the Proxy Controllers manually. The following sections describe how to install additional JET modules. In general, you download the JET datastream package, which includes all JET modules and then and use it to install only the packages with the modules that you want to use.

About JET Modules

When you install JET on the jumpstart server, you have the following advantages:

- Install any of multiple versions of Solaris
- Deploy flash archives
- Utilize multiple boot methods
- Install recommended patches
- Configure all your network interfaces

For more information about JET resources and documentation, see *Solaris 10 10/09 Installation Guide: Custom JumpStart and Advanced Installations* available at:

http://www.oracle.com/technetwork/indexes/documentation/index.html

Enterprise Manager Ops Center installs some JET packages on the Proxy Controller during installation. Hence, always check for the package before installation. Do not uninstall or upgrade these packages as they are considered a core part of the Enterprise Manager Ops Center product.

Packages of JET Module

The following are the list of associated packages with the JET modules:

Table 3–1 JET Modules and Associated Packages

JET Module Name	JET Package	Installed by Default	Description
base_config	SUNWjet	Yes	Provides the standard installation configuration for the client, including the information required to set up the JumpStart server to allow the client to boot and build.
custom	SUNWjet	Yes	Adds functionality to the JumpStart framework to handle packages, patches, scripts, and files.
explo	JetEXPLO	No	Adds explorer support to the JET JumpStart framework.
flash	JetFLASH	Yes	Adds the ability for the JumpStart server to deliver Solaris images in Solaris Flash format.
jass	JetJASS	Yes	Adds the ability for the JumpStart server to install, configure, and execute JASS.
ldom	JetLDOM	Yes	Adds capability to install and configure Logical Domains.
san	JetSAN	No	Installs and patches the SAN Foundation kit and SNIA packages, and configures STMS.
sbd	JetSBD	No	Adds capability to configure the Secure by Default feature in Solaris 10.
sds	JetSDS	No	Adds Solstice DiskSuite (Solaris Volume Manager) support to the JumpStart framework.
vts	JetVTS	No	Adds support for installation of the Sun VTS software under the JumpStart framework.
zfs	JetZFS	No	Adds capability to configure ZFS file systems on JumpStart clients.
zones	JetZONES	No	Allows creation of simple zones on Solaris 10 systems.

JET Module Parameters

The SUNWjet and JetFLASH packages are installed by default on Enterprise Manager Ops Center Proxy Controllers. The SUNWjet package installs the base_config and custom JET modules. The JetFLASH package installs the flash JET module. The parameters of these JET modules are available for use in OS profiles by default. You can review the parameters for these modules by looking at the `sample.template` file in the `/opt/SUNWjet/Templates` directory on a Proxy Controller.

Refer to the module.conf configuration files that are associated with JET modules for information about parameters for specific JET modules. Configuration files for installed JET modules reside in the `/opt/SUNWjet/Products/module` directories on the Proxy Controller, where module is the name of the JET module. For example, the configuration files for the custom and flash JET modules are `/opt/SUNWjet/Products/custom/custom.conf` and `/opt/SUNWjet/Products/flash/flash.conf` respectively.

JET base_config Module Parameters

If you specify JET parameters with an OS profile, the following parameters from the base_config JET module are automatically updated within the OS profile and must not be modified:

- base_config_ClientArch
- base_config_ClientEther
- base_config_client_allocation
- base_config_sysidcfg_network_interface
- base_config_sysidcfg_ip_address
- base_config_sysidcfg_netmask
- base_config_sysidcfg_nameservice
- base_config_sysidcfg_system_locale
- base_config_sysidcfg_terminal
- base_config_sysidcfg_timeserve
- base_config_sysidcfg_timezone
- base_config_sysidcfg_root_password
- base_config_sysidcfg_security_policy
- base_config_sysidcfg_protocol_ipv6

The following list describes the parameters that are associated with the base_config JET module. These parameters provide basic operating system configuration information. Values for many of these parameters use the term `targetableComponent` to represent the target system.

- base_config_client_allocation – The mechanism used to build this client. By default, the options listed in `/opt/SUNWjet/etc/jumpstart.conf` are used. Leave the value blank unless you need to do something different from the default for this specific client. If you are provisioning the Solaris 10 1/06 x86 release, set the value of this variable to GRUB to enable GRUB-based booting and installation.
- base_config_ClientArch – Kernel architecture, such as sun4u or x86. By default, this is set to the kernel architecture of the targetable component.

  - Default Value – [targetableComponent:kernel_arch]
- base_config_ClientEther – Ethernet MAC address. By default, this is set to the Ethernet MAC address of the targetable component.
  - Default Value – [targetableComponent:ethernet_mac_address]
- base_config_ClientOS – Version of the OS to be provisioned.
  - Example – Solaris9_u7_sparc
- base_config_dedicated_dump_device – If set, the dumpadm utility configures the partition as a Dedicated Dump Device. See `dumpadm(1M)` for supported Operating Environments.
- base_config_defaultrouter – Value to use for `/etc/defaultrouter`.
- base_config_disable_sysid_probe – If set, skip the sysid step on the first reboot. This can significantly increase provisioning efficiency on systems that have many unused network adapters.
  - Default Value – yes
- base_config_dns_disableforbuild – Delay DNS configuration until later. If DNS is not available in the build environment, set this variable to yes.
- base_config_dns_domain – DNS domain entry for the `/etc/resolv.conf` file.
- base_config_dns_nameservers – Space-separated list of IP addresses to use for DNS name server entries in the `/etc/resolv.conf` file.
- base_config_dns_searchpath – List of entries to go in the DNS search line in `/etc/resolv.conf` file.
- base_config_dumpadm_minfree – Set a limit so that crash dumps do not fill up the dump file system. See the `dumpadm(1M) -m` option for possible values.
  - Example – 20000k
- base_config_enable_altbreak – If set, enable alternate break sequence.
- base_config_enable_rootftp – If set to any value, enable root FTP access.
- base_config_enable_rootlogin – If set to any value, enable network root login from telnet, rsh, and ssh.
- base_config_enable_savecore – If set to any value, enable save core for Solaris 2.6 systems.
  - Default Value – yes
- base_config_grub_append – For Solaris 10 1/06 x86 systems, specifies additional options or arguments to pass to the GRUB bootloader.
- base_config_ipmp_networkifs – Space-separated list of interfaces to be defined under IPMP control. For each interface listed, define sets of variables to provide the netgroup, mode, test1, test2, netmask, host name, log-ip, hostname2, and log-ip2 for the interface.
  - Example – qfe0_qfe4!database-net l 10.0.0.1 10.0.0.2 24 oracle-db 10.0.0.3 apache 10.0.0.4
- base_config_networkifs – Space-separated list of additional network interfaces to be defined. For logical interfaces, use underscores (_) rather than colons (:). Use the format c_ntndn. For each interface listed, define sets of variables to provide the netname, netmask, host name, and IP address for the interface.

  - Example – le1!netB 255.255.255.0 myhost-netB 192.168.1.0
- base_config_nfs_mounts – Space-separated list of remote NFS mount points. Use ? to separate the mount source from the mount target, as shown in the example.
  - Example – fs?1.1.1.1:/fs
- base_config_nfsv4_domain – Set up the NFSv4 domain to prevent being prompted at first reboot. If not set, look first for the entry in base_config_dns_domain, and second for the domain value in `/etc/default/nfs`.
- base_config_noautoshutdown – If set to any value, disable power management.
  - Default Value – pm_disabled
- base_config_nodename – Value to use for `/etc/nodename` if not the default host name.
- base_config_notrouter – If set to y, then disable IPv4 forwarding and create the `/etc/notrouter` file.
- base_config_ntp_servers – Space-separated list of names or IP addresses for the NTP servers. The first server will be given a prefer tag. This section places lines of the form: server [prefer] into the `/etc/inet/ntp.conf` file. For additional NTP control, use the custom module to deploy your own custom ntp.conf file.
- base_config_patchdir – Path to the patches. If blank, use information from the jumpstart.conf file and the IP address of the JET server. If your patch files are not stored on the JET server, then provide an NFS-style path to the location of the patches.
- base_config_poweroff_afterbuild – If set, shut down the system once the build completes.
- base_config_productdir – Path to the products. If blank, use information from the jumpstart.conf file and the IP address of the JET server. If your package files are not stored on the JET server, then provide an NFS-style path to the location of the packages.
- base_config_products – JET modules to provision.
- base_config_profile – Create your own custom JumpStart profile. By default, if you leave this variable blank, the OS provisioning plug-in creates the `/opt/SUNWjet/Clients/hostname/profile` based on the other base_config_profile variables. Alternatively, you can create your own custom JumpStart profile. To use the profile that you created manually, set the base_config_profile variable to the name of the created profile. By default, the OS provisioning plug-in looks for the profile in the `/opt/SUNWjet/Clients/hostname` directory. To direct the plug-in to a profile in another directory, provide an absolute path name in the base_config_profile variable.

  Note: If you are provisioning the Solaris OS on x86 target hosts, you must create a custom JumpStart profile that deletes any existing partitions, and point to that profile in the base_config_profile variable.

- base_config_profile_add_clusters – Space-separated list of cluster packages to add.
- base_config_profile_add_geos – Comma-separated list of geographical regions to add.
  - Example – N_Europe, C_Europe

- base_config_profile_add_locales – Comma-separated list of locales to add.
  - Example – fr_FR, ja_JP.UTF-8
- base_config_profile_add_packages – Space-separated list of packages to add.
- base_config_profile_additional_disks – A list of disks to use and configure in addition to the boot disk. Use the format c*n*t*n*d*n*. For each disk listed, define sets of variables for each slice to identify the mount point and the size.
- base_config_profile_cluster – Solaris software group package.
  - Default Value – SUNWCreq
  - Example – SUNWCreqSUNWCuserSUNWCprogSUNWCallSUNWCXallSUNWCrnet
- base_config_profile_del_clusters – Space-separated list of cluster packages to remove.
  - Example – SUNWCpm SUNWCpmx SUNWCdial SUNWCdialx
- base_config_profile_del_geos – Comma-separated list of geographical regions to delete.
- base_config_profile_del_locales – Comma-separated list of locales to delete.
- base_config_profile_del_packages – Space-separated list of packages to remove. To prevent interactive installations on Solaris x86 headless target hosts, set this value to SUNWxwssu SUNWxwscf.
- base_config_profile_dontuse – A comma-separated list of disks that should not be used. Use the format c*n*t*n*d*n*. This variable applies only if base_config_profile_usedisk is not set.
- base_config_profile_root – Root space (free, or size in Megabytes)
  - Default Value – free.
- base_config_profile_s3_mtpt – Mount path to slice 3.

> **Note:** If you are using VxVM and you want your boot disk to look like the mirror, then leave slices 3 and 4 empty.

- base_config_profile_s3_size – Size of slice 3 (in Megabytes).
- base_config_profile_s4_mtpt – Mount path of slice 4.
- base_config_profile_s4_size – Size of slice 4 (in Megabytes).
- base_config_profile_s5_mtpt – Mount path of slice 5.
  - Default Value – `/var`
- base_config_profile_s5_size – Size of slice 5 (in Megabytes).
- base_config_profile_s6_mtpt – Mount path of slice 6.
  - Default Value – `/usr`
- base_config_profile_s6_size – Size of slice 6 (in Megabytes).
- base_config_profile_s7_mtpt – Mount path of slice 7.

> **Note:** If you are using Solaris Volume Manager (SVM), the default behavior is to use slice 7 as a location for metastate databases. If you are using the SVM default configuration, do not use slice 7 for data.

  - Default Value – /opt
- base_config_profile_s7_size – Size of slice 7 (in Megabytes).
- base_config_profile_swap – Swap space (in Megabytes).
  - Default Value – 256
- base_config_profile_usedisk – Defines the boot disk onto which the OS will be loaded. Use the format c*n*t*n*d*n* or the keyword rootdisk. If the value is rootdisk, then the current boot disk will be used.
  - Default Value – rootdisk
- base_config_shutup_sendmail – If set, create an alias host name to disable sendmail.
  - Default Value – yes
- base_config_sysidcfg_default_route – Router IP address to use during JumpStart for Solaris 9 or later environments. If blank, will try to use value from the `defaultrouter_base_config` variable. If that is also blank, or for another net interface, JumpStart sysidcfg will get a router IP from the JET server.
- base_config_sysidcfg_ip_address – IP address to use at initial boot. By default, this is set to the IP address of the targetable component.
  - Default Value – [targetableComponent:ethernet_ip_address]
- base_config_sysidcfg_nameservice – Name service to configure at initial boot.
  - Default Value – NIS
- base_config_sysidcfg_netmask – Netmask to use at initial boot. By default, this is set to the netmask of the targetable component.
  - Default Value – [targetableComponent:ethernet_netmask]
- base_config_sysidcfg_network_interface – Network interface to use at initial boot.
  - Default Value – NONE
- base_config_sysidcfg_protocol_ipv6 – Whether to use IPv6 protocol at initial boot.
  - Default Value – no
- base_config_sysidcfg_root_password – Encrypted root password.
- base_config_sysidcfg_security_policy – Kerberos security policy to use at initial boot.
  - Default Value – NONE
- base_config_sysidcfg_system_locale – System locale to use at initial boot.
  - Example – en_US.ISO8859-1
- base_config_sysidcfg_terminal – Terminal emulator to set at initial boot.
  - Default Value – vt100

- base_config_sysidcfg_timeserver – Where to get system time for initial boot. If blank, system time comes from the JET server. Alternatively, you can set this variable to localhost to get the system time from the hardware clock on the client.
- base_config_sysidcfg_timezone – System time zone to use for initial boot.
  - Example – US/Pacific
- base_config_sysidcfg_x86_kdmfile – For Solaris x86 systems, specifies the name of a keyboard, display, and mouse configuration file to append to the sysidcfg file.
  - Default Value – /sysidcfg-addon-file
- base_config_ufs_logging_filesys – For Solaris 7 and later systems, a space-separated list of mount points to use for logging. To enable logging on all UFS file systems, use the keyword all. Solaris 9 09/04 enables logging by default. To disable logging on a specific file system, add a hyphen in front of the mount point. To disable logging on all file systems, use the keyword none.

  > **Note:** You cannot mix keywords and mount points. You can specify the root file system (/), although the root file system is included as part of the all and none keywords.

  - Default Value – all
- base_config_update_terminal – If set, put the sysidcfg terminal type into inittab.
  - Default Value – yes
- base_config_x86_confflags – For Solaris 9 x86 systems, specifies arguments to be used with the confflags attribute of the `add_install_client` command.
  - Example – -f -P /boot/solaris/dca
- base_config_x86_console – For x86 systems, set the console to the correct tty port if you are not going to connect a keyboard and monitor to the client. Setting this variable enables you to perform installs through the serial port. For b1600, v20z, and v40z systems, use ttya. For lx50, v60x, and v65x systems, use ttyb.
- base_config_x86_disable_acpi – For x86 systems, any value disables ACPI. Disabling ACPI might make the installation process proceed better due to how the interrupts are handled.
- base_config_x86_disable_kdmconfig – For Solaris x86 systems, disables the kdmconfig interactive utility for configuring the keyboard, display, and mouse of the target host. If you are installing a Solaris OS with the GRUB bootloader, set this variable value to yes.
- base_config_x86_nowin – For x86 systems, prevents Solaris from trying to run Windows during the install.
  - Default Value – yes
- base_config_x86_safetoreboot – For x86 systems, controls whether the system automatically reboots. If your PXE boot is a one-time option, and the next reboot will attempt to boot from disk, you should set this option to yes.

Installing JET Modules

To use any JumpStart Enterprise Toolkit (JET) module other than the base_config, custom, and flash JET modules, you must install the modules. The default installation of the Proxy Controller software includes the SUNWjet and JetFLASH packages, which provide the base_config, custom, flash, jass, and ldom JET modules. Additional modules that you might install require that the SUNWjet package be installed.

JET modules are only used on Solaris OS-based Proxy Controllers. Do not install JET modules on Linux-based Proxy Controllers.

To Check for Installed JET Modules

To see the JET modules installed on a Proxy Controller, list the contents of the `/opt/SUNWjet/Products` directory, which contains a separate subdirectory for each installed JET module. In the following example, the Proxy Controller has the default set of JET modules for Enterprise Manager Ops Center:

```
# cd /opt/SUNWjet/Products
# ls
base_config  custom   flash   jass   ldom
#
```

To Install a JET Module

Use this procedure on the Proxy Controller to install a JET module.

1. Download the JET datastream package, `jet.pkg`. The JET datastream package contains the complete set of JET packages.
2. Use the `pkginfo` command to list the included packages:

   ```
   # pkginfo -d jet.pkg
   application JetEXPLO   jet explo product
   application JetISO     JET ISO product
   application JetRBAC    JET RBAC product
   application JetSAN     JET san product
   application JetSBD     Secure By Default product
   application JetSDS     JET sds product
   application JetVTS     JET VTS product
   application JetZFS     JET zfs product
   application JetZONES   JET Zones module
   application SUNWjet    Sun JumpStart Enterprise Toolkit
   application SUNWjetd   JET Documentation
   #
   ```
3. Identify the name of the package that contains the module you want to install.
4. Use the `pkgadd` command to install the package. For example:

   ```
   # pkgadd -d jet.pkg JetZONES

   (output omitted)

   Do you want to continue with the installation of <JetZONES> [y,n,?] y

   (output omitted)

   Installation of <JetZONES> was successful.
   ```

   Note: Support is provided only for the core JET modules that are bundled with Enterprise Manager Ops Center.

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 Solaris OS provisioning. You can use JET templates to standardize the configurations as it provides more options for defining the jumpstart parameters.

JET Templates

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. A sample template is provided for your reference.

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 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 multiple networks. 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 must 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 is created. Create a plan from this profile and apply it on the server to provision the OS.

For more information about creating and applying a deployment plan associated with this profile, see *Oracle Enterprise Manager Ops Center Advanced User's Guide*.

For more information about JET Templates, see *Solaris 10 Installation Guide: Custom JumpStart and Advanced Installations* available at:

`http://www.oracle.com/technetwork/indexes/documentation/index.html`

Provisioning the OS

Using the provisioning profiles created for different targets, create a deployment plan with the associated profile.

Before You Begin

Ensure that you have the ISO images imported and verified the procedures in Preparing to Provision an OS.

To Create a Deployment Plan for Provisioning

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 must 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 to create a profile for the plan. This option takes you to the OS provisioning profile creation wizard.
8. Provide any additional parameter required, if any.
9. Click Save to save the plan.

To Apply a Deployment Plan for Provisioning

1. Expand Plan Management in the Navigation pane.

2. In the Provision OS section, select the deployment plan. The profiles included in the plan are listed in the center pane.
3. Select Apply Deployment Plan from the Actions pane. The Select Target Assets window is displayed.
4. Choose one or more targets from the list of available targets and click Add to Target List.
5. Select whether you want to apply the plan with minimal user interaction or override any profile values.
6. Click Next to view the summary of the parameters
7. Click Apply the deployment plan on the selected targets. The provisioning job starts. View the progress of the job by selecting the View Job Details icon in the Jobs pane.

For more information about creating and applying deployment plans that use nested plan for OS provisioning, see *Oracle Enterprise Manager Ops Center Advanced User's Guide*.

See *Oracle Enterprise Manager Ops Center User's Guide* for more detailed information about provisioning Oracle VM Server for SPARC.

OS Provisioning for an Oracle Solaris Cluster

You can provision clusters with an OS and the Oracle Solaris Cluster software. You must create the provisioning profile by importing the cluster profile and editing it to include the post-action script.

See *Oracle Enterprise Manager Ops Center Advanced User's Guide* for information about importing a cluster profile.

To provision an OS on an Oracle Solaris Cluster, use the procedure described in Creating an OS Update Job with the cluster provisioning profile and select the cluster as the target of the update job.

To provision both an OS and the Oracle Solaris Cluster software onto a server, use a deployment plan.

For detailed instructions in creating a complex plan, see *Oracle Enterprise Manager Ops Center Advanced User's Guide*.

In general, the procedure is as follows:

1. Create the OS provisioning profile.
2. Import and edit the cluster provisioning profile.
3. Create a deployment plan using the Install Server template.
4. Select the OS provisioning profile as Step 1.
5. Select the cluster provisioning profile as Step 2.
6. Complete the plan.

4

Updating an OS

Enterprise Manager Ops Center enables you to update, or patch, the following operating systems:

- Oracle Solaris 8, 9, and 10 (SPARC)
- Oracle Solaris 10 (x86)
- Oracle Linux
- Red Hat Linux Advanced Server 3, 4, and 5
- SUSE Linux Enterprise 8, 9, and 10
- Microsoft Windows

About Updating an OS

You can use Enterprise Manager Ops Center to update operating systems, such as Solaris, Linux and Windows, to the latest released patches. It reduces the complexity of patching a large number of systems, standardizes the patch installation process, minimizes downtime, and automates patching without user interaction. You can manage different patching conditions that exist for installing a patch. The software helps you to keep track of the patching conditions and helps you do your work efficiently and effectively.

How to Start Patching in Enterprise Manager Ops Center?

You must first discover and manage the OS. Managing an OS enables the patching operations through Enterprise Manager Ops Center. Discovering and managing an OS gathers information about the OS and installs the agent controller software on the OS. When you install the agent controller on the OS, the following actions occur:

- It takes at least 5 minutes for the agent to be registered. You cannot update the OS until the agent is registered.
- A notification is sent when the update function is enabled for the OS.
- The agent controller runs an inventory check on the OS and creates a catalog for the OS. The catalog lists the patches and packages, and the versions that are currently installed on the OS.

The update function enabled for a user depends on the roles that are granted for that user. See Update Roles and Authorizations for the roles granted to a user. Contact your administrator to get the appropriate role.

What Does Enterprise Manager Ops Center Provide to Help Patching?

Enterprise Manager Ops Center provides the following:

- Update Profiles
- Update Policies
- Catalogs
- Reports

You create update jobs with OS update profiles and policies to patch an OS. OS Update profiles and policies define which patches must be installed, and how the update job proceeds after determining the patch dependencies and user interaction. There are system-defined update profiles and you can also create your own customized profiles and policies.

The snapshots of the OS are taken after executing any job on the OS. The snapshots are stored as catalogs with a time and date stamp. You can also create a catalog and store the catalogs. You can compare the catalogs between operating systems and create profiles from the saved catalogs that can be later used for creating systems. At any point of time, you can roll back to a saved state of the system.

Enterprise Manager Ops Center provides reports for different operating systems. Reports give an insight into the OS compliance status to the recommended patches and packages. Generate reports to know the state of your OS patch levels.

How Does the Enterprise Controller Provide the Latest Updates?

The Enterprise Controller obtains information about latest updates from the Knowledge Base. It requires an Internet connection to connect to the Knowledge Base to download the patches from OS vendor sites. In the absence of an Internet connection to the Enterprise Controller, you can get the latest updates using different ways. See Using Knowledge Base and Connection Modes for more information about knowledge base and connected mode.

How to Run an Update Job in Enterprise Manager Ops Center

When you manage an OS, the update functions are enabled for the OS. The New Update OS Job option is enabled in the Actions pane for the OS. This option invokes a wizard where you define the job parameters. You can also run an update job in Enterprise Manager Ops Center from:

- Update profiles and policies
- System catalogs
- Reports

You can use the appropriate options to run an update job from these sections. These sections launch an update job with patches that must be installed or removed accordingly.

What are the Options Available When Running an Update Job?

You have the following options available when running an update job:

- Select update profiles and policies.
- Select different targets for each task in the job.

- Select job simulation mode. Simulating a patching job helps to estimate the time required to run the job, to know the patch dependencies and the expected job result. In the simulation mode, you can select to download the required patches.
- Roles specification for an user to carry out only specific tasks on an asset.
- Failure policy to determine the action when a task fails.

Using Knowledge Base and Connection Modes

This section provides information about Knowledge Base and the connection modes of the Enterprise Controller. It describes the procedure to switch the Enterprise Controller mode, and how to get the latest updates of an OS in the disconnected mode.

Knowledge Base

The Knowledge Base (KB) is the repository for metadata about Solaris and Linux OS components. The metadata includes patch dependencies, standard patch compatibilities, withdrawn patches, downloads, and deployment rules. The KB stores a mapping of the OS download URLs and uses those URLs to download the components from the appropriate vendor download site.

The following operating systems are supported:

- Solaris 10, 9, and 8 OS
- Oracle Linux
- Red Hat Enterprise Linux (RHEL)
- SUSE Linux Enterprise Server (SLES)

KB Update Intervals

The following are the maximum intervals between updates:

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

Connection Modes

The Enterprise Controller requires an Internet connection to connect to the KB and to download the patches from the OS vendor sites. In the connected mode, the Enterprise Controller has an Internet connection to connect to the KB. The KB contains the metadata information about the latest patches and packages released. By default, Enterprise Manager Ops Center is configured in connected mode, where the Enterprise Controller has an Internet connection to the KB. When an update job is started, the agent sends a request to the KB through the Enterprise Controller. When running in connected mode, the KB is updated on a regular basis.

You can configure your environment and Enterprise Manager Ops Center to run in disconnected mode by changing the connection mode of the Enterprise Controller. In disconnected mode, the Enterprise Controller does not have Internet access to connect to the KB.

In disconnected mode, you must manually upload all the required content to the Enterprise Controller. If the software and other files are not uploaded, an error message similar to `Not installable by current KB` is displayed when you run jobs. You can create a local KB on your Enterprise Controller when you are operating your Enterprise Controller in disconnected mode.

Uploading patches and packages to the Enterprise Controller in disconnected mode is similar to uploading local content, and is identified as local content. To upload all of the current and appropriate software and patches, use Bulk Upload Packages and Patches option. Several other upload options are available to upload all the patches, packages, and RPM content, including uploading from an EIS DVD or Solaris CD/CD.

For more information about uploading local contents, see *Oracle Enterprise Manager Ops Center Advanced User's Guide*.

To create a local KB, you can run a harvester script provided by Enterprise Manager Ops Center on a system outside the data center that has Internet access. The harvester script downloads the patches and packages. You can then save the downloaded information to a portable media device, such as a CD or DVD, bring it into to your data center, and manually upload to the Enterprise Controller.

You can operate the Linux-based Enterprise Controller in disconnected mode. However, you cannot use the harvester script to obtain the KB bundle. The harvester script is mainly for the Solaris OS.

Semi-disconnected Mode

If your data center allows Internet access or infrequent access, you can run your Enterprise Controller in disconnected mode until you need patches or packages. You can then change the Enterprise Controller's connection mode to Connected, download the required patches and packages, and then change the Enterprise Controller back to Disconnected mode.

> **Note:** You can import only signed patches from My Oracle Support or EIS DVD and the patches must be of the format jar, jar.gz or in the patch directory.

Switching the Enterprise Controller Mode

During the initial Enterprise Controller configuration, you have an option to set up Enterprise Manager Ops Center in disconnected mode. If you select this mode, you have the option to change the mode to connected after the Enterprise Controller is operational (the assets are discovered, agents are provisioned, systems are updated, and so forth.)

When in connected mode, authentications, such as Online Account or My Oracle Support (MOS) credentials, are necessary to download updates and other content from Oracle and third-party sites.

Note: The first time you change to connected mode, you must add your Online Account in the UI to access the Knowledge Base Service and any HTTP proxy to access the Internet.

To Switch to Connected Mode

1. Select Administration from the Navigation pane.
2. Select Setup Disconnected Mode from the Actions pane.
3. Select Switch to Connected Mode. A confirmation window is displayed. Click Confirm to switch to connected mode.

To Switch to Disconnected Mode

You must first load a KB bundle or you will be unable to switch modes.

1. Select Administration from the Navigation pane.
2. Select Setup Disconnected Mode from the Actions pane.
3. Specify a KB bundle and click Load KB Bundle.
4. Select Switch to Disconnected Mode. A confirmation window is displayed. Click Confirm to switch to disconnected mode.

Obtaining a KB Bundle With the Harvester Script

When the Enterprise Controller runs in disconnected mode, the harvester script that downloads the metadata and patches does not operate. You must use another system that connects to the Internet to get the Knowledge Base (KB) bundle and provide it to the Enterprise Controller.

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

1. Identify a system that can connect to the Internet.
2. Load the prerequisite software onto the system.
3. Transfer the harvester bundle to the system.
4. Use the harvester script to download the KB bundle.
5. Copy the bundle onto removable media such as a CD, DVD or memory stick.
6. Bring the media to the system that runs the Enterprise Controller and copy the KB bundle to a directory on the local file system of the Enterprise Controller.

Note: Disconnected mode is supported on a Linux Enterprise Controller. However, the harvester script to get a KB bundle is not supported on Linux.

Harvester Script Utility

The harvester script is available at `https://updates.oracle.com/OCDoctor/harvester_bundle-latest.zip`. This script must be run on a system that is connected to the Internet. This script helps to download the latest KB bundle.

Loading Prerequisite Software

The harvester script requires that the system has wget version 1.10.0 or later installed. Perform the following steps to install the appropriate version of wget software:

1. To check the version of wget, run the wget command with the `-V` option, for example:

   ```
   # /usr/sfw/bin/wget -V
   GNU Wget 1.10.2

   Copyright (C) 2005 Free Software Foundation, Inc.
   This program is distributed in the hope that it will be useful,
   but WITHOUT ANY WARRANTY; without even the implied warranty of
   MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
   GNU General Public License for more details.
   #
   ```

2. If an older version of the wget is installed, download the version 1.10.0 or later and install it on the system connected to the Internet.

   The latest version of wget is available at:

   http://sunfreeware.com

   ```
   # pkgadd -d wget-1.11.4-sol10-sparc-local

   The following packages are available:
   1 SMCwget wget
   (sparc) 1.11.4

   Select package(s) you wish to process (or 'all' to process
   all packages). (default: all) [?,??,q]:

   Processing package instance <SMCwget> from </jf/wget-1.11.4-sol10-sparc-local>

   wget(sparc) 1.11.4
   Free Software Foundation
   Using </usr/local> as the package base directory.
   (output omitted)

   Installation of <SMCwget> was successful.
   #
   ```

   wget version 1.11.4 depends on additional software:

   - openssl-0.9.8j
   - libiconv
   - libintl
   - `/usr/local/lib/libgcc_s.so.1` and `/usr/local/lib/libstdc++.so.6` - Installing `libgcc-3.4.6` or `gcc-3.4.6` installs these files. Download each of these objects from sunfreeware.com and install them on the Internet-facing system.

3. With the additional software installed, verify that the wget command runs. The wget command installs into the `/usr/local/bin` directory, for example:

   ```
   # /usr/local/bin/wget -V
   GNU Wget 1.11.4

   Copyright (C) 2008 Free Software Foundation, Inc.
   License GPLv3+: GNU GPL version 3 or later
   <http://www.gnu.org/licenses/gpl.html>.
   ```

```
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

Transferring the harvester Bundle to the System

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

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

Using the harvester Script to Obtain the KB Bundle

1. On the system, create a temporary directory, for example, `/var/tmp/OpsCtr`, to hold the password file that you create in this procedure.

   ```
   # mkdir -p /var/tmp/OpsCtr
   ```

2. Create an empty file named `/var/tmp/OpsCtr/`mypasswd, and set its permission mode to 400.

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

3. Edit the `/var/tmp/OpsCtr/mypasswd` file so that it contains the password of your Online Account. The following `echo` command appends the password to the `/var/tmp/OpsCtr/mypasswd` file. (Replace *password* with the correct password.) For example:

   ```
   # echo password > /var/tmp/OpsCtr/mypasswd
   ```

4. Change the permission of the harvester script to 744. For example:

   ```
   # chmod 744 harvester
   # ls -l
   total 36
   -rwxr--r-- 1 root root 17546 Jan 27 04:56 harvester
   #
   ```

5. Run the harvester script, with at least the `-u` and `-p` options:
   - `-u` *Online Account user name* – Specify the Online Account user name that you have registered with the Oracle Inventory online environment.
   - `-p` *password-file* – Specify the full path name of the file that contains the Online Account password.
   - `-x` *proxy url* – Specify the https URL to the proxy server.
   - `-U` *proxy user* – Specify the proxy user name.
   - `-P` *proxypassfile* – Specify the full path name of the file that contains only the proxy password.
   - `-t` *dir* – Specify the temporary directory for storing the downloaded contents. Ensure that this directory is empty before running the script.
   - `-c` – Use this option to clean up the temporary directory if the downloaded contents exist. By default, all the downloaded contents are stored and not cleared.

- -d *list* – Specify the distributions for which you want to download all the Solaris patches. Specify a quoted, space separated list of the names of Solaris OS distributions for which you want to download patches. If the distribution is not specified, the patches for all Solaris distributions are downloaded. Without the -d option, the harvester script downloads only the metadata. Available distributions are:
  - SOLARIS_10_0_SPARC
  - SOLARIS_10_0_X86
  - SOLARIS_9_0_SPARC
  - SOLARIS_8_0_SPARC

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

  Note: Do not use the -d option while running the harvester script. It might take couple of days for the harvester script to finish running with the -d option. You can upload the patches in bulk from the EIS DVD.

- -R *revisions* – Specify the number of revisions of a patch to download. By default, the revision number is 100.
- -s *distro* – This option displays the baselines for a given distribution. You can enter only one distribution at a time. Valid distributions are:
  - SOLARIS_10_0_SPARC
  - SOLARIS_10_0_X86
  - SOLARIS_9_0_SPARC
  - SOLARIS_8_0_SPARC
- -b *ID* – Specify the Solaris baseline ID to download.

  Note: When you use the -b option, you must use the -d option. You can use the option only for one distribution.

- -k *host* – Specify the hostname of a different Knowledge Base which hosts the metadata information.

Examples of Running the harvester Script

Example 4–1 Running Harvester Script with Online Account

Running the harvester script only with the Online Account user name and password.

```
# ./harvester -u username@oracle.com -p /var/tmp/OpsCtr/mypasswd
Directory /export/home/public not found. This directory will be created.
Setting up local directory structure at: /export/home/public
Initialization: Downloading channels.xml
Tue Jan 27 05:08:01 MST 2009 Clearing cookies to initialize new session.
Distributions:
Identifying and Downloading the Notifications and Seeker scripts
```

```
Creating tarball...

Tarball successfully created at /discon/standalone-0127.tar.gz

Start time: Tue Jan 27 05:08:00 MST 2009
Completion time: Tue Jan 27 05:08:01 MST 2009

Tarball includes 0 distribution(s):


Tarball includes only distribution metadata (no patches.)

Please copy this file to a Ops Center server and
use the BUI to configure Update Disconnected Mode.

When you are finished you can delete the content in /export/home/public
#
```

The harvester script without the `-d` option generates a `.tar.gz` file that contains the KB metadata only (no patch content). In this example, the harvester script created the `/discon/standalone-0127.tar.gz` KB bundle.

Example 4–2 Running Harvester Script to Download Solaris 10 SPARC patches

Running the harvester script to download Solaris 10 patches up to four revisions for a SPARC distribution

```
./harvester.sh -u username@oracle.com -p /var/tmp/OpsCtr/mypasswd -d "SOLARIS_10_
0_SPARC SOLARIS_10_0_X86" -R 4
```

Example 4–3 Running Harvester Script to Display Baselines for Solaris 10 SPARC

Running the harvester script to display the available Solaris baselines for a Solaris 10 SPARC distribution.

```
./harvester.sh -u username@oracle.com -p /var/tmp/OpsCtr/mypasswd -s SOLARIS_10_0_
SPARC
```

Example 4–4 Running Harvester Script to Download Security Baselines for Solaris 10 SPARC

Running the harvester script to download the security baseline DEC-2009 for a Solaris 10 SPARC distribution.

```
./harvester.sh -u username@oracle.com -p /var/tmp/OpsCtr/mypasswd -d "SOLARIS_10_
0_SPARC" -b 40011729
```

Example 4–5 Running Harvester Script Using a Proxy Server

Running the harvester script using a proxy server instead of directly connecting to the Oracle Knowledge Base Service.

```
./harvester.sh -u username@oracle.com -p /var/tmp/OpsCtr/mypasswd -x
http://www.oracle.com -U proxyuser -P /var/tmp/proxypassword
```

Example 4–6 Running Harvester Script Using Different Knowledge Base Server

Running the harvester script using a different Knowledge Base server. You can point it to another server instead of the default server getupdates.oracle.com.

```
./harvester.sh -u username@oracle.com -p /var/tmp/OpsCtr/mypasswd -k
servername.com
```

Enhancements in the Harvester Script

The following enhancements were made to the harvester script:

- The new harvester script performs incremental downloads. The user can choose not to delete the previously downloaded data. This action makes subsequent runs of the harvester script faster.
- The new option `-R` is provided to define the number of revisions of a patch to be downloaded. This reduces the number of patches to be downloaded.
- The new option `-b` is provided to download the full baselines. The download includes the dependencies for the patches in the baselines also.
- The patch download progress counter was added; it displays the number of patches to be downloaded. This counter is updated after every 10 patches are downloaded.

Transferring the KB Bundle to the Enterprise Controller

1. Copy the KB bundle onto removable media that you can use to install the KB bundle on the Enterprise Controller.
2. Copy the KB bundle into a directory on a local file system of the Enterprise Controller.
3. Load the KB bundle into Ops Center on the Enterprise Controller. See Loading and Refreshing a KB Bundle for more information about loading and refreshing a KB bundle.

Loading and Refreshing a KB Bundle

To load or refresh a KB bundle, a new KB bundle must be generated by the harvester script and then loaded. To refresh with a newer KB bundle, run the harvester script again and load the KB bundle. For more information about obtaining a KB bundle, see Obtaining a KB Bundle With the Harvester Script.

To Load and Refresh a KB Bundle

Perform the following steps to load and refresh a KB bundle:

1. Select Administration from the Navigation pane.
2. Select Setup Connection Mode from the Actions pane. The Configuring Disconnected Mode window is displayed.
3. Browse for and select a KB bundle, then click Load KB Bundle.
4. Switch to disconnected mode.

> **Note:** Unpacking and untarring can take some time depending on the size of the bundle. The absolute path to the generated KB bundle must be specified when you load the bundle. For example, a bundle could be located at `/tmp/standalone-0127.tar.gz`.

Update Profiles

Update profiles specify which update components are to be installed and which are not allowed, and actions to perform on a system. You use profiles to maintain the configuration of the system that you want to manage.

Enterprise Manager Ops Center provides system-defined policies that are not editable and cannot be deleted. You can also create customized profiles by selecting the required OS update components and the required action that must be applied.

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 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.

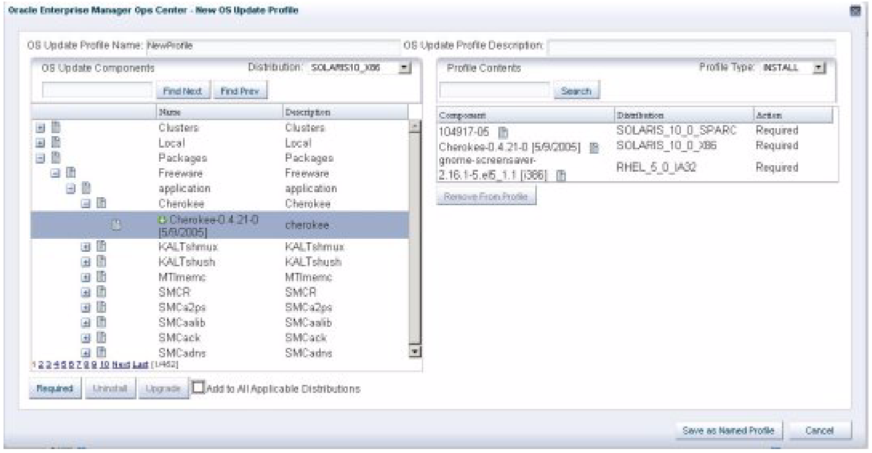
> **Note:** The process of managing an asset and activating its distribution takes few minutes to complete.

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 4–1 Create an OS Update Profile



Oracle Enterprise Manager Ops Center - New OS Update Profile

OS Update Profile Name: NewProfile

OS Update Profile Description:

OS Update Components

Distribution: SOLARIS10_X86

Name	Description
Clusters	Clusters
Local	Local
Packages	Packages
Freeware	Freeware
application	application
Cherokee	Cherokee
Cherokee-0.4.21-0 [5/9/2005]	cherokee
KALTshmux	KALTshmux
KALTshush	KALTshush
MTImemc	MTImemc
SMCR	SMCR
SMCa2ps	SMCa2ps
SMCaalib	SMCaalib
SMCack	SMCack
SMCadns	SMCadns

1 2 3 4 5 6 7 8 9 10 Next Last (14452)

□ Add to All Applicable Distributions

Profile Contents

Profile Type: INSTALL

Component	Distribution	Action
104917-05	SOLARIS_10_0_SPARC	Required
Cherokee-0.4.21-0 [5/9/2005]	SOLARIS_10_0_X86	Required
gnome-screensaver-2.16.1-5.el5_1.1 [i386]	RHEL_5_0_IA32	Required

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 *Oracle Enterprise Manager Ops Center Advanced User's Guide* for more information about complex plans.

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.

Profile Creation

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 o 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

Update policies define how an OS update job must be performed. Policies helps to automate the update jobs without user interaction. You can use the policy to specify the update tasks about which you want to be notified.

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.

Enterprise Manager Ops Center provides 3 system-defined policies. You can also create policies by setting the action for a selected OS update component.

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.

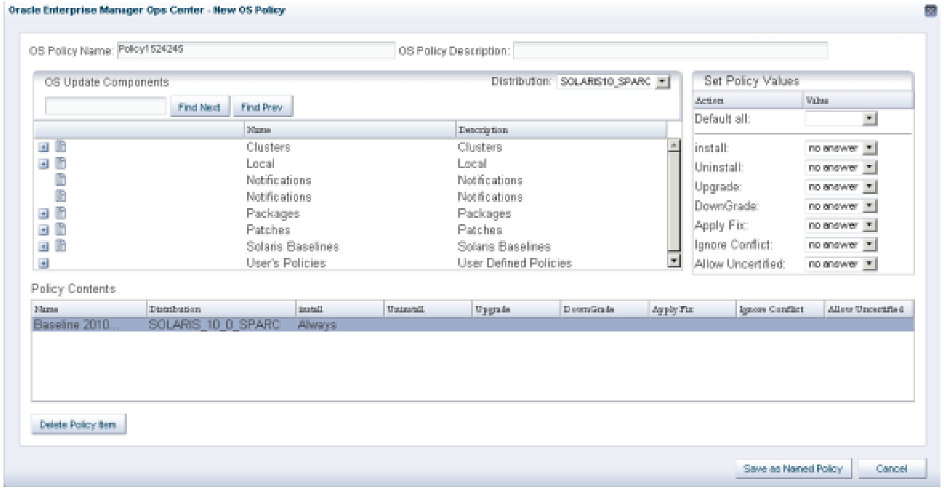
To Create an OS Update Policy

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 4–2 Create an OS Update Policy



Oracle Enterprise Manager Ops Center - New OS Policy

OS Policy Name: Policy1524245 OS Policy Description:

OS Update Components Distribution: SOLARIS10_SPARC

	Name	Description
	Clusters	Clusters
	Local	Local
	Notifications	Notifications
	Notifications	Notifications
	Packages	Packages
	Patches	Patches
	Solaris Baselines	Solaris Baselines
	User's Policies	User Defined Policies

Set Policy Values

Action	Value
Default all:	
install:	no answer
Uninstall:	no answer
Upgrade:	no answer
DownGrade:	no answer
Apply Fix:	no answer
Ignore Conflict:	no answer
Allow Uncertified:	no answer

Policy Contents

Name	Distribution	install	Uninstall	Upgrade	DownGrade	Apply Fix	Ignore Conflict	Allow Uncertified
Baseline 2010...	SOLARIS_10_0_SPARC	Always						

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.

System Catalogs

A system catalog is a list of OS software components that are installed on a particular managed system. An initial catalog is created after the system is discovered and managed.

After an operating system is available and selected, catalogs can be viewed and modified, and historical catalogs (snapshots of the system) can be created.

Modifying a catalog is an alternate way to run an OS update job to install, uninstall, or upgrade a component. Modifying a catalog does not require an update profile to run the update job. It is a quick way of changing the component configuration of a system.

System catalogs of two managed systems can be compared. You can view the summary of the comparison and also have the option to make the target system the same as the source system.

Catalogs provide the capability to directly manipulate the installed software components on a single operating system or a group of operating systems. Alternatively, a catalog can be saved as a profile, and then an OS update job can be run using this profile.

Creating a Historical Catalog

You can create a historical catalog (snapshots) for an OS. A snapshot of a system is created, then stored with the time stamp and job details after every job is executed on a system. All the snapshots are listed in the catalog list.

When you create a historical catalog, the current state of the selected system is identified and stored as the previous catalog of the system. The saved previous catalog is the most recent system catalog.

Note: You can create a historical catalog only for the current state of the system.

The catalog list always provides the listing of the most recent catalog. The catalog list is populated when the system is updated or a historical catalog is created. The current catalog is identified with a time stamp when you create a historical catalog.

To Create a Historical Catalog

1. Select Assets from the Navigation pane.
2. Select an OS group or a specific OS from the Assets section.
3. Select View/Modify Catalog.
   - If you selected an OS Group, the available systems appear in the center pane. After you select a system, the View/Modify Catalog icon is available above the list of systems.
   - If you select a specific system from the Assets section, the View/Modify Catalog option appears in the Actions pane. The View/Modify Catalog window is displayed.
4. In the View/Modify Catalog window, click Create Historical Catalog. The Save Inventory as Snapshot window is displayed.
5. (Optional) You can edit the name of the snapshot to be saved.
6. Click Save Snapshot to save the current state of the system. The saved snapshot will be listed in the Catalog list of View/Modify Catalog window.

You can use the created historical catalog to create a profile and apply to configure the systems.

Viewing and Modifying a Catalog

A catalog is available for each system that you discover and manage in Enterprise Manager Ops Center. A catalog is automatically created when you manage a system.

If you are using dual boot environments for Solaris Live Upgrade, the catalog displays the inventory of the active boot environment of the operating system. To view the catalog of an alternate boot environment (ABE), you must first activate the ABE from the UI, and then wait for the job to finish. The current catalog is updated and contains the ABE catalog information and OS software components. This will also automatically update the catalog of any zones.

To View a Catalog

1. Select Assets from the Navigation pane.
2. Select an OS from Assets section.
3. Select View/Modify Catalog from the Actions pane. The View/Modify Catalog window is displayed. The current catalog is displayed by default.
4. If a previous catalog is available, select a catalog from the Catalog list. The installed components are displayed.

To Modify a Catalog

1. Select Assets from the Navigation pane.
2. Select an OS from the Assets section.
3. Select View/Modify Catalog from the Actions pane. The View/Modify Catalog window is displayed.
4. Select a catalog from the Catalog list. The components that are installed on the system are displayed.

5. Select the component for which you want to modify the action. The available actions are No Action, Required, Uninstall and Upgrade. The actions that are available for the selected component are enabled accordingly.
6. Select the action for the component that you want to modify.
7. Click Launch Modification Job. A New Job wizard is displayed.
8. Complete the job Information as required.
9. Either click Run Now to run the job immediately or click Next to schedule the job later.

Comparing System Catalogs

You can compare two managed systems or two system catalogs for differences in the installed update components. You can also compare the current system catalog and saved snapshots of the same managed system to examine the differences in the components that were installed and uninstalled after executing a job.

Use the Compare Catalogs option to change the software components of a particular operating system to that of the source system.

Before You Begin

If you have an alternate boot environment (ABE), you cannot create and compare catalogs until you activate the ABE. By default, only the catalogs of the active boot environment are compared.

To view differences between the target and one of its ABEs, perform the following steps:

1. Create a snapshot of the current BE.
2. Activate the ABE.
3. Wait for the Activate job to finish and for the catalog of the ABE to be reported. Check the notification alerts. When the activation is complete, an OS Update Inventory is Available message appears.
4. Select the snapshot created in Step 1 as the source.
5. Select the new BE (previous ABE) to compare as the target.

To Compare System Catalogs and Copy a Catalog

1. Select an OS from the Assets section in the Navigation pane.
2. Click Compare System Catalogs from the Actions pane. The Compare Catalogs window is displayed. The source system is displayed first.
3. Select a catalog for the source system.
4. Click Select target(s) from inventory. The Select Target window is displayed.
5. Select the target systems.
6. Select one of the following options:
   - Differences Between Systems – Displays the difference between the source and the target systems update components. The difference is displayed in the Compare Catalog window.}
   - Tasks to Make Target Like Source – Creates the list of components that must be installed on the target system. Select Include for the components that you want to install on the target system.

7. Click Create job to copy the source to the target(s). The New Update OS Job wizard is displayed.
8. Complete the job information in the wizard.
9. Either click Run Now to run the job immediately or click Next to schedule the job to run later.

Creating an Update Profile From a System Catalog

You can save the catalog of a system as a profile. Using this profile, you can create the systems with the required configuration in your data center.

To Create an Update Profile from a System Catalog

1. Select Assets in the Navigation pane.
2. Select an OS from the Assets section.
3. Choose View/Modify Catalog from the Actions pane. The View/Modify Catalog window is displayed.
4. Select a system catalog to save as a profile. The installed components for the selected catalog are displayed.
5. (Optional) Select the option Profile should include the removal actions to save the exact state of the system. This option ensures that the components that are not installed are selected with Uninstall as the Action in the profile. The removal actions option is selected. The default is no removal actions included in the profile.
6. To save the catalog as a profile, click Convert Catalog to Profile. The Profile window is displayed. You can edit the profile name and description. If necessary, you can add or delete any component, or modify a component action in the profile settings.
7. Click Save as Named Profile to save the profile.

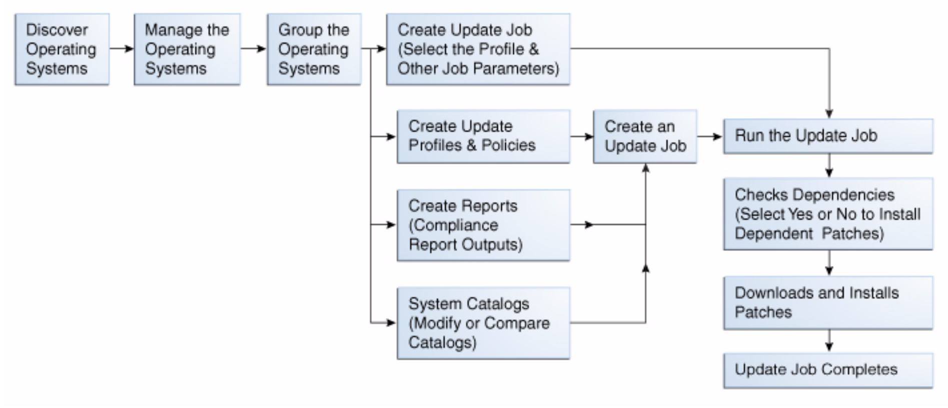
Methods of Updating an OS

When an OS is first discovered and managed, a system catalog of the OS is created. The catalog shows the system update components that are installed on the system. You can create reports to identify the system compliance with the recommended updates. You must update the system with the required and recommended updates for security and other application requirements.

This section describes how to update an OS using different options that are available in Enterprise Manager Ops Center. The following figure describes the different methods available for updating your OSs:

- Use predefined or custom profiles to update a system or group of systems. This method is mainly used for a Linux OS.
- Use a system catalog to create a simple update job without creating a profile. This method is used to apply a single patch quickly.
- Use the compliance reports output to update your OS. This method is used to make your systems compliant with newly released updates.
- Use compare catalogs to roll a system back to its previous state.

Figure 4–3 Different Methods of Updating an OS


Discover Operating Systems
Manage the Operating Systems
Group the Operating Systems
Create Update Job (Select the Profile & Other Job Parameters)
Create Update Profiles & Policies
Create an Update Job
Run the Update Job
Create Reports (Compliance Report Outputs)
Checks Dependencies (Select Yes or No to Install Dependent Patches)
System Catalogs (Modify or Compare Catalogs)
Downloads and Installs Patches
Update Job Completes

In addition to the methods described previously, you can use Live Upgrade and alternate boot environments to update your Solaris OS with a minimum of downtime.

See Updating a Windows OS for updating your Windows OS using Enterprise Manager Ops Center.

Creating an OS Update Job

Creating a new update job enables you to use custom or predefined profiles. This method is typically used for complex update scenarios.

Before You Begin

The New Update OS Job option enables you to create customized update jobs. When creating a job, you must define the following job parameters:

- Name of the update job.
- Profile – Defines what updates are to be installed, uninstalled, or upgraded on an OS. Select a profile from the list of profiles. Predefined profiles are available, or you can create customized profiles. See UPDATE PROFILES for more information.
- Policy – Defines how a job is performed and sets the automation level of the job. Select a policy from the list of available policies. You can also create your own policies. See UPDATE POLICIES for more information.
- Target Settings – Defines whether the target must be different or similar for each task in the job.
- Run Type – Defines the type of update job:
  - Simulation – Determines the actions and results of a job, and estimates how much time is required to complete the job. A job simulation also indicates whether your policy and profile responses will enable the job to succeed. You can run a simulation with or without downloading patches.
  - Actual Run – Deploys the update job.
- Task Execution Order – Specifies whether the tasks must be run in parallel or sequentially.
- Task Failure Policy – Specifies what action to take if a task fails.
- Targets – Select the target operating systems for this job.

> **Note:** To use an alternate boot environment (ABE) and run ABE pre-action scripts for Solaris OS, see the procedures in Oracle Solaris Live Upgrade.

To Create an Update OS Job

1. Select an OS from the Assets section in the Navigation pane.
2. Click New Update OS Job in the Actions pane. The New Update OS Job wizard is displayed.
3. In the Job Information, specify the job parameters.
4. Enter a name for the update job.
5. Select the Target Setting:
   - Use the same Targets for all tasks in the job
   - Use different Targets for each task in the job
6. Select a Run type:
   - Simulation – Enables you to run a job simulation without downloading patches.
     - Download – Click the Download check box to download the patches as part of the job simulation.
   - Actual Run – Enables you to download the patches and run the update job.
7. Select the Task Execution Order:
   - Sequential
   - Parallel
8. Select the Task Failure Policy:
   - Complete as much of job as possible
   - Stop at failure and notify
9. To use an alternate boot environment (ABE) and run ABE pre-action scripts, see the procedures in Oracle Solaris Live Upgrade.
10. Click the Add icon to add more tasks to the update job. You can define the profile, policy, and target for each task. If the target setting is a different target for each task in the job, then the new task includes the Select Targets button. Click Select Targets to select the target for the task.
11. To change the profile or policy, click the appropriate table cell for the target to display a drop-down list. Select the profiles and policies from the lists.

    > **Note:** If there is a conflict between a profile and policy, the profile overrides the policy.

12. To change the selected target system, select the row and click Edit Targets. The Select Targets window is displayed. Select the targets on which you want to run the update job. You can select multiple targets.
13. Determine how you want to run the job:
    - To schedule the job to run later, click Next.

- To run the job immediately, click Run Now.

14. Select a schedule option.
    - Now – Starts the update job immediately.
    - Start Date – Enables you to define a start date.
    - On a Recurring Schedule – Enables you to create a recurring schedule.
15. Click Next to display the Job Summary.
16. Click Finish to run the update job according to the defined configuration and schedule.

Updating an OS by Modifying a System Catalog

A system catalog is a list of OS software components that are installed on a managed system. Catalogs provide the capability to directly manipulate the installed software components on a single operating system or a group of operating systems.

See System Catalogs for more information about managing catalogs.

Updating an OS by modifying a system catalog provides the following advantages:

- Enables you to create a quick ad hoc job
- Provides an easy method of applying a single patch, baseline, or package
- Enables you to update an OS without creating a profile for a one-time job

To Update an OS by Modifying a System Catalog

1. Select Asset from the Navigation pane.
2. Select an OS from the Asset tree.
3. Select View/Modify Catalog from the Actions pane. The View/Modify Catalog window is displayed.
4. Select a catalog from the Catalog list. The components that are installed on the system are displayed.
5. Select the component for which you want to modify the action. The available actions are No Action, Required, Uninstall, and Upgrade. The actions that are available for the selected component are enabled accordingly.
6. Select the action for the component that you want to modify.
7. Click Launch Modification Job. A New Update OS Job wizard is displayed.
8. Complete the job Information as required.
9. Either click Run Now to run the job immediately or click Next to schedule the job to run later.

Updating From an OS Profile

In Enterprise Manager Ops Center, you can create an update job from Update Profiles in the Plan Management section. In the Update Profile section, the New OS Update Job option is available to run an update job.

To Create a Job From a Profile

1. Select Plan Management section in the Navigation pane.
2. Select Update Profiles in the Profiles tree.

3. Select a profile from the predefined profile or user-defined profile list.
4. Click New Update OS Job in the Actions pane. The New Update OS Job wizard is displayed.
5. Enter a name and description for the update job in the Job Information step.
6. Select the run type for the job. It can be either Simulation or Actual Run.
7. Make your selections from the following:
   - Task Execution Order
   - Target Setting
   - Task Failure Policy
   - Boot Environment Type
   - Run ABE Pre-action Script
8. Select the profile and policy from the drop-down list under the Profile and Policy columns in the Tasks table.
9. Click the link below the Targets column in the Task table to select the target for the task. The Select Targets window is displayed. Select the target on which you want to run the update job and click Add to Target List. You can select multiple targets.
10. Click Select in the Select Targets window.
11. Click Run Now to run the job immediately or click Next to schedule the job to run later.

Updating From an OS Report Result

In Enterprise Manager Ops Center, you can generate the following compliance reports for an OS from which you can create an OS update job:

- Baseline Analysis Report
- Host Compliance Report
- Incident Compliance Report
- CVE Compliance Report
- Profile Report
- Package Compliance Report
- Recommended Software Configuration Report

See Firmware and OS Update Reports for information about generating these reports. You can generate these reports for non-compliant components. The report result is displayed with the option to install the patches, packages, updates, and incidents.

The report results are stored in the database associated with the Enterprise Controller. The history of the reports is maintained for analysis purposes.

From the report result, you can initiate a job to install the non-compliant component updates. The New Update OS Job wizard starts, enabling you to enter job information and to schedule the job. The required data for profiles, policies, and targets are automatically pre-populated in the job wizard.

After you submit the job to run the report, the result is displayed under the Report Results.

To Use Report Result to Update an OS

1. Click Reports from the Navigation pane. The saved report templates and the report results are displayed in the content pane under All Reports.
2. In the Report Results section, select the required report and click the View Interactive icon. The interactive result viewer opens the Report Details window. The Report Details lists the targets for which the report was generated.
3. Select a target from the list. The applicable OS updates are listed. The report lists the patch number, required action for the patch and the link to the patch information in the applicable vendor Web site.
4. Select the updates that you want to install and click Make Targets Compliant. The New Update OS job wizard is displayed with defined profiles and targets.
5. Complete the wizard and run the update job.

Updating Zones

Enterprise Manager Ops Center enables you to update the global and non-global zones of your Solaris OS. You can update both the greenfield and brownfield zones. You can also patch zones that are running on a supported configuration. The installation of the patches on the zones depend on the package parameters and the attribute set for the patch commands. This section describes the parameters for installation of the packages and patches. The concepts involved in updating global and non-global zones, and the procedures to update the zones are described in this section.

Installing Packages and Patches on Zones

A patch is a collection of files and directories that replace existing files and directories that are preventing proper execution of the software.

You can install packages and patches on a zone. The patchadd and pkgadd commands operate in the background to install a patch and package respectively. However, the installation of packages on zones also depends on the parameters SUNW_PKG_ALLZONES, SUNW_PKG_HOLLOW, and SUNW_PKG_THISZONE. These parameters control whether a package can be installed on global zones or non-global zones. The actions for the parameters are as follows:

- **SUNW_PKG_ALLZONES** – If the value is true, the package is installed on all zones, both global and non-global.
- **SUNW_PKG_HOLLOW** – If the value is true, the package information is propagated to the non-global zones, but the package is not installed.
- **SUNW_PKG_THISZONE** – If the value is true, the package is installed only in that zone.

Configuring patchadd and pkgadd Commands

In Enterprise Manager Ops Center, the patchadd, pkgadd, patchrm, and pkgrm commands are implemented without the `-G` switch by default. To install updates or packages only on the current zone, enable the `-G` switch by editing the .uce.rc file.

> **Note:** There is a `uce.rc` file and a `.uce.rc` file. The `uce.rc` file is the default file and should not be edited. Please ensure that you are editing the `.uce.rc` file.

Editing the .uce.rc File

1. Open the `.uce.rc` file in the `/SUNWuce/agent/bin` directory in the managed system.
2. Add the following lines to the `.uce.rc` file:

   ```
   ( all ) (invisible.__is_patchadd_g_specified, false)
   ( all ) (invisible.__is_patchremove_g_specified, false)
   ( all ) ( invisible.__is_pkgadd_g_specified, false)
   ```
3. Set the `-G` parameter to true for the action that you want to perform.
4. Save and close the file.
5. For this change to take effect, restart the services using the following commands:

   ```
   svcadm disable -s update-agent
   svcadm enable -s update-agent
   ```

Updating a Global Zone

In Enterprise Manager Ops Center, when a package or patch is installed, the patchadd and pkgadd commands are implemented in the background as shown in the following example:

```
patchadd <patchid>
pkgadd <pkgname>
```

You can change the way that these commands are implemented by enabling the `-G` switch. You can enable the `-G` switch to cause the patch or package to be installed to the target zone only if the package parameter SUNW_PKG_THISZONE is set to true. See Installing Packages and Patches on Zones for information about configuring the patchadd and pkgadd commands on the managed systems.

See the following scenarios when you are updating a global zone. The result for each scenario determines whether the update job will be successful, depending on the package information.

Table 4–1 Updating a Global Zone Scenarios

SUNW_ PKG_ ALLZONES	SUNW_ PKG_ THISZONE	SUNW_PKG_ HOLLOW	Impact	Impact with -G Configuration
False	False	False	The package will be installed on the global zone, and all the non-global zones	The package is installed only on the global zone.
True	False	False	The package is installed on the global zone and all the non-global zones.	The `-G` switch cannot override the SUNW_PKG_ ALLZONES parameter, and the package is installed on all the zones.
True	False	True	The package is installed on the global zone and the package information is made available on all the non-global zones.	The `-G` switch cannot override the SUNW_PKG_ ALLZONES parameter, and the package is installed on all the zones.

Table 4–1 (Cont.) Updating a Global Zone Scenarios

SUNW_ PKG_ ALLZONES	SUNW_ PKG_ THISZONE	SUNW_PKG_ HOLLOW	Impact	Impact with -G Configuration
False	True	False	The package is installed only on the global zone.	The package is installed only on the global zone.

Patches are sets of updates to packages. When you install a patch, the patch is installed on the global zone and the non-global zones, depending on the package parameters as shown in the previous table.

Note: Use caution while enabling the `-G` option on a host with sparse zones. Packages that are inherited from the global zone that are not SUNW_ALL_ZONES cannot be patched within a sparse zone.

Updating Non-Global Zones

As a zone administrator, you can install packages and patches on non-global zones. The patchadd and pkgadd command must be used without any options. Do not configure the `-G` switch to the commands while updating the non-global zones.

See the following scenarios when you are updating a non-global zone. The results of each scenario determine whether the update job will be successful, depending on the package information.

Note: The `-G` switch does not have any effect on installing packages or patches in a non-global zone.

Table 4–2 Updating Non-Global Zones Scenarios

SUNW_ PKG_ ALLZONES	SUNW_PKG_ THISZONE	SUNW_PKG_ HOLLOW	Impact
False	False	False	The package is installed only on the target non-global zone.
True	False	False	The package installation fails.
True	False	True	The package installation fails.
False	True	False	The package is installed only on the target non-global zone.

Note: When the patch is installed only on the non-global zone, ensure that autoboot property is set to true for the zone. Otherwise, single user mode patches will fail to apply as the zone does not come up after the reboot.

Patches are sets of packages that must be installed. If any one of the packages has the SUNW_PKG_ALLZONES parameter set to true, then the patch installation fails. For a successful patch installation, ensure that none of the packages have SUNW_PKG_ ALLZONES parameter set to true.

Note: Packages that deliver to read-only inherit directories will not install to sparse root zones. These packages must be installed from the global zone with the `-G` switch disabled. If a package has the parameter SUNW_PKG_THISZONE=true, it will not appear as installed from the sparse zone and the software might not function correctly. In this case, a whole root zone must be used. Packages with SUNW_PKG_THISZONE=true must not deliver to read-only inherit directories.

OS Update Capability

The list of services that are provided by Enterprise Manager Ops Center for the operating systems such as Solaris, Linux, and Windows.

Table 4–3 List of Services

Service	Solaris	Linux	Windows	Zones	Branded Zones
Patch analysis	Yes	Yes	Yes	Yes	Yes
Job simulation	Yes	Yes	No	Yes	Yes
Job scheduling	Yes	Yes	Yes	Yes	Yes
Rollback and recovery	Yes	Yes	No	*NA*	*NA*
Custom packages	Yes	Yes	No	Yes	Yes
Active dependency rules	Yes	Yes	No	Yes	Yes

OS Update Reports

Several predefined OS Update reports are available. The reports enable you to check for new patches and security advisories. You can get a general report, or test a system or installed package for available fixes.

When you create a report, you select the criteria that are relevant to you, such as a list of hosts that have a specific patch or a list of hosts that do not have a specific patch.

The following reports are available for the hosts such as Oracle Solaris and Linux:

- CVE report
- Host compliance report
- Incidence compliance report
- Package compliance report
- Service pack compliance report
- Distribution update report
- Recommended software configuration report
- Profile report
- Change history report

The following reports are exclusive to Oracle Solaris OS:

- Baseline analysis report

- Solaris update compliance report

The following reports can be generated for Windows OS:

- Host compliance report
- Incidence compliance report

Update Roles and Authorizations

To use the Update feature, you must have the proper permissions, or user role, for the asset.

An Enterprise Manager Ops Center administrator can grant a user the following roles for a group or asset:

- Admin – To perform administration actions such as grouping
- Update – To update a system or group of systems
- Update Sim – To run simulated update jobs
- Provision – To provision new operating systems
- Manage – To use management actions, such as rebooting

An Admin can assign a user role for a specific asset, such as the Enterprise Controller, or an asset group. When a user is assigned a group role, the user also has the same permissions to all subgroups.

To update multiple operating systems with a single job, you must use a homogeneous OS group as the target. See *Oracle Enterprise Manager Ops Center User's Guide* for information about how to create a group and add operating systems to the group. Homogeneous groups contain the same release of an OS.

To update a Linux OS, you must provide your Red Hat or SUSE login credentials. Enterprise Manager Ops Center uses the credentials to log in to the third-party site and download the patches or packages.

To provide or update your My Oracle Support or third-party vendor credentials, see *Oracle Enterprise Manager Ops Center Reference Guide* for information about editing authentications.

The following tasks are available for an admin:

- Reports
  - Save, run, and view BAR from Database Report
  - Save and view BAR from Agent Report
  - Run BAR from Agent Report
  - Save, Run and View Compliance Report
- Job Submission
  - Launch Job Wizard from Asset, Group and Profile
  - View Catalog and Catalog Compare
  - Launch Job Wizard from Catalog and Catalog Compare
  - Submit Simulation Job
  - Submit Deploy Job
  - Answer questions

    - Rerun job
    - Launch Copy Job wizard
- Profile and Policy Management
    - Create Profile and Policy
    - Save Profile and Policy from job
    - Edit Profile and Policy
    - Delete Profile and Policy
    - View Profile and Policy
    - View Profile and Policy from job
- Administration
    - Edit Authentications
    - Setup Connection Mode
    - OS Update Library Actions

For a non-admin, the following tasks are available:

- Reports
    - Save, run, and view BAR from Database Report
    - Save and view BAR from Agent Report
    - Run BAR from Agent Report – If you have the Update or Update Sim role for the OS targets
    - Save, Run and View Compliance Report
- Job Submission
    - Launch Job Wizard from Asset, Group and Profile
    - View Catalog and Catalog Compare
    - Launch Job Wizard from Catalog and Catalog Compare
    - Submit Simulation Job – if you have the Update or Update Sim role for the OS targets
    - Submit Deploy Job – if you have the Update role for the OS targets
    - Answer questions – if you have the Update or Update Sim role for the job targets
    - Rerun job – if you have the Update or Update Sim role for the job targets
    - Launch Copy Job wizard
- Profile and Policy Management
    - Edit Profile and Policy – if you have the admin role for profile and policy
    - Delete Profile and Policy – if you have the admin role for profile and policy
    - View Profile and Policy
    - View Profile and Policy from job

Note: You must have root permissions to view system profiles and policies. You cannot view a system defined profile or policy from a job.

Updating Clusters

You can provision clusters with an OS and the Oracle Solaris Cluster software. You must create the provisioning profile by importing the cluster profile and editing it to include the post-action script.

See *Oracle Enterprise Manager Ops Center Advanced User's Guide* for more information about importing a cluster profile.

To provision an OS on an Oracle Solaris Cluster, use the procedure described in Creating an OS Update Job with the cluster provisioning profile and select the cluster as the target of the update job.

5

Updating a Windows OS

Enterprise Manager Ops Center enables you to update your managed Windows operating systems by using the Microsoft System Center Configuration Manager (SCCM) and Windows Management Instrumentation (WMI) software.

About Updating a Windows OS

Enterprise Manager Ops Center enables you to update your managed Windows operating systems by using the Microsoft SCCM and WMI software. The Windows Update functionality depends on the SCCM's agent installed on the managed systems. You can configure SCCM to install agents on your managed Windows systems either automatically or through a manual process.

Enterprise Manager Ops Center uses Microsoft SCCM 2007 to implement the software updates for the Windows OS. More specifically, it uses the Windows software update capability of SCCM to update any Windows operating systems that are discovered and managed. You must be able to identify a functional SCCM that is configured for software update and management of the Windows systems that are managed by Enterprise Manager Ops Center. The Windows Update functionality depends on the SCCM's agent installed on the managed systems.

Patching in Connected and Disconnected Mode

The Enterprise Controller connects to the SCCM to get the latest information about patches and packages. The SCCM is connected to the Internet for downloading the metadata that is used for compliance analysis. Enterprise Manager Ops Center can also be connected to the Internet to download patches that are then handled by SCCM for installation.

When you want to download and install a patch, the patch is downloaded from the Microsoft Web site. You do not need any authentication to access the Microsoft Web site. However, you must provide authentication information to access the SCCM server.

You can also update the managed systems when the Enterprise Controller is in disconnected mode, that is, when the Enterprise Controller is not connected to the Internet.

Reports

To ensure that your managed systems are up to date, you must determine which patches, updates, and actions to apply to your system. The Windows OS update reports help you to determine the patches that are applicable to your systems and how many of the applicable patches are compliant or not compliant for the selected systems.

Several predefined OS Update reports are available. The reports enable you to check for new patches and update your systems. You can get a general report, or test a system for available fixes.

When you create a report, you select the criteria that are relevant to you, such as category, severity, superseded, and release date of the update patches. You can also select specific updates on which to run the compliance reports.

Update Job

Enterprise Manager Ops Center contains the following options in an update job to maintain control and consistency across your data center:

- Groups – Help you to organize your assets in the user interface and act as targets for many types of jobs.
- Roles – Enable you to determine the tasks that a user can perform on a specific piece of an asset or a group of assets.
- Reports – Enable you to run compliance reports and create update jobs from the compliance reports.

You can define the following job parameters while creating a windows update job:

- Name and Description – Identify the name of the report against which you want to create a Windows OS update job. A detailed description is helpful to clearly identify the job in the historical record.
- Reboot behavior – Lets you select the reboot behavior if a reboot is required after the new update job is executed. You can select whether you want the system to reboot immediately following the update operation or whether you want to reboot the system at the default setting of the SCCM server.
- License Terms – Lets you review the license terms and either accept or decline them. The License Terms window appears only when the updates in the report require License Terms that must be reviewed.
- Schedule – Lets you decide how you want to schedule the execution of the new update job.

Configuring Enterprise Manager Ops Center for Updating the Windows OS

Enterprise Manager Ops Center uses the `j-Interop` command to access the Windows Management Instrumentation (WMI) and get Windows update information. It uses the software update capability of the Microsoft System Center Configuration Manager (SCCM) to update any managed Windows operating systems.

Before You Begin

Before you can use Enterprise Manager Ops Center to update your Windows systems, you must configure it to interact with the identified Microsoft System Center Configuration Manager (SCCM). In addition, you might need to modify the WMI registry.

To configure Enterprise Manager Ops Center to interact with the identified SCCM, you must have the following credentials:

- SCCM Server
  - Server Name
  - Domain Name
  - Site Name
  - User Name
  - Password
- SCCM Share
  - URL
  - Domain Name
  - User Name
  - Password

The configuration information is displayed in the Configuration tab of the Windows Update window.

> **Note:** Enterprise Manager Ops Center uses the same SCCM credentials to access the SCCM server and enable the SCCM share. Use the <*domain*> format for the Domain Name field. Do not use the <*domain*>\<*username*> format. If you entered an incorrect format for the Domain Name field and if the configuration task returns an error, then unconfigure the SCCM and configure the SCCM again with the correct format for the credentials.

To Configure Enterprise Manager Ops Center to Interact With the Identified SCCM

1. In the Navigation pane, click Administration, then click Windows Update.
2. In the Actions pane, click SCCM Configuration. An SCCM Configuration window is displayed.
3. Enter the credentials for the following fields:
   - SCCM Server
     - Server Name
     - Domain Name
     - Site Name
     - User Name
     - Password
     - Confirm Password
   - SCCM Share
     - URL
     - Domain Name
     - User Name
     - Password
     - Confirm Password

4. Click Submit.

Enterprise Manager Ops Center is now configured to interact with the SCCM.

To Unconfigure Enterprise Manager Ops Center's Interaction With the SCCM

1. In the Navigation pane, click Windows Update from the Administration section.
2. In the Actions pane, click Unconfigure. A confirmation window appears.
3. Click Yes to unconfigure Enterprise Manager Ops Center's interaction with the SCCM.

Modifying the Registry

Due to some changes that Microsoft introduced for registry key ownership, you must manually modify the registry and change of ownership permissions for the Administrators group.

Note: This procedure is required only on a Windows Server 2008 R2. Other Windows servers, such as 2008 Server SP2, do not require you to modify the registry.

To Modify the Registry

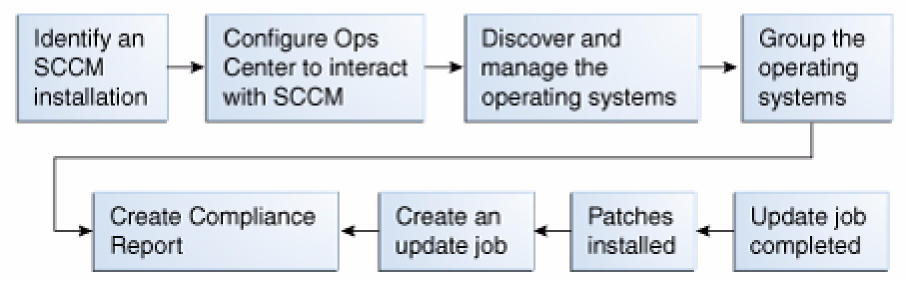
1. Log in to the target remote host as an Administrator.
2. Run the Regedit program.
3. Click Yes when you are asked to allow the Regedit program to make changes to the computer.
4. Go to the Registry item `HKEY_CLASSES_ROOT\CLSID\76a64158-cb41-11d1-8b02-00600806d9b6`
5. Right click the registry item and select Permissions.
6. Click Advanced, then click the Owner tab.
7. In the Change Owner to... box, select the account that you are currently logged in as, then click Ok.
8. Click Ok.
9. Right click the registry item again and select Permissions.
10. Select the Administrators group, then select the Allow check box to give Full Control permissions to the Administrators group.
11. Click Ok.

Creating an Update Job for Windows OS

Enterprise Manager Ops Center enables you to use the output from compliance reports to update your Windows OS to be compliant with the newly released updates.

From the results of the Windows Host Compliance Report and the Windows Incident Compliance Report you can make your systems compliant by initiating an update job for the Windows OS.

Figure 5–1 Process for Updating Windows OS


Identify an SCCM installation
Configure Ops Center to interact with SCCM
Discover and manage the operating systems
Group the operating systems
Create Compliance Report
Create an update job
Patches installed
Update job completed

Before You Begin

The Create New Windows Update Job wizard enables you to create an update job. When creating a new update job, you must define the following job parameters:

- Name and Description for the new Windows software update job.
- Reboot behavior – Lets you select whether you want the system to reboot immediately following the update operation or at the default setting of the SCCM server.
- License Terms – Lets you review the license terms and either accept or decline them. The License Terms window appears only when the updates in the report require license terms that must be reviewed.
- Schedule – Lets you decide how you want to schedule the execution of the new update job.

To Create an Update Job for Windows OS

1. Click Reports in the Navigation pane.
2. Click Windows OS Updates.

   The executed reports are listed under the Report Results List tab in the center pane.
3. Select a report from the list of the executed reports in the Windows OS Update Report Results table.
4. Click the View Report icon.

   A compliance report details window is displayed.
5. Click Make Targets Compliant.

   The Create New Windows Update Job wizard is displayed.
6. Enter a name and description for the update job in the Job Information window.
7. Select whether you want the system to reboot immediately following the update operation or whether you want to reboot the system at the default setting of the SCCM Server. Click Next.

   When you click Next, either the License Terms window or the Schedule window is displayed. The License Terms window is displayed only when the updates in the report require license terms to be reviewed.
8. Review and accept the Software License Terms for the updates that require license terms.

The table shows only the updates for the license terms that were not accepted or were declined before. Under Search, you can select Select All to include a bulletin ID, article ID, title, and license terms in your search, or you can select specific fields to narrow your search. Click Next.

9. Select the schedule for the new Windows software update job from the following options:

   - Now (immediately)
   - Start Date and Start Time
   - On a Recurring Schedule by specifying Month, Days, Earliest Job Start Time, and Latest Job Start Time

   Click Next.

10. Verify the information in the Summary window. Click Finish to execute the Windows OS update job.

6

Oracle Solaris Live Upgrade

You can use the Oracle Solaris Live Upgrade technology in Enterprise Manager Ops Center to apply patches to a duplicate, inactive boot environment. This reduces the amount of downtime required to update your Oracle Solaris software and enables you to fully test the update before introducing it in your production environment. When you are satisfied with the update, you can switch boot environments and deploy the updated boot environment. The downtime is the time it takes to reboot into the new environment.

You must have a boot environment (BE) and an alternate boot environment (ABE) in order to use this method of patching. You can use an ABE that was created outside of Enterprise Manager Ops Center; however, the preferred method is to save Oracle Solaris Live Upgrade scripts in the Local Contents section of the Update Library in Enterprise Manager Ops Center and use these scripts to create an ABE in Enterprise Manager Ops Center. Using this method provides you with an exact replica of your boot environment.

See Managing Boot Environments in the User documentation for the following topics:

- Displaying BE and ABE Information – Display the active boot environment and any associated alternate boot environments.
- Synchronize Boot Environments – Create an ABE identical to the currently running BE.
- Activate a Boot Environment – Make the ABE the active boot environment.

About Oracle Solaris Live Upgrade

A boot environment is the set of all file systems and devices that are unique to an Oracle Solaris OS instance on a system. A dual boot environment consists of a live boot environment (BE) and an inactive alternate boot environment (ABE). You can use the Oracle Solaris Live Upgrade technology and a dual boot environment within Enterprise Manager Ops Center to manage your Oracle Solaris software updates and significantly reduce the service outage time that is usually associated with patching.

The Live Upgrade technology enables you to duplicate a boot environment and perform the following tasks without affecting the currently running system:

- Run an Oracle Solaris software update simulation on the inactive boot environment. You can run the simulation with or without downloading the patches.
- Update your Oracle Solaris OS on the inactive boot environment and test the update before deploying it as your active environment.

- Maintain multiple boot environments with different images. For example, you can create one boot environment that contains all current patches and another that contains only security patches.

This section provides a brief overview of how Oracle Solaris Live Upgrade uses files systems and guidelines for selecting slices for shareable file systems.

For more information about system administration tasks such as managing file systems, mounting, booting, and managing swap space, see *Solaris 10 System Administration Guide: Devices and File systems* available at:

`http://www.oracle.com/technetwork/indexes/documentation/index.html`

File Systems

When using alternate boot environments with Oracle Solaris Live Upgrade, file systems are categorized into the following types:

- Critical File Systems – Non-shareable file systems that are required by the Oracle Solaris OS, such as root (/), /usr, /var, and /opt. These file systems are separate mount points in the vfstab of the active and inactive boot environments and are always copied from the source to the inactive boot environment.
- Shareable File Systems – User-defined files, such as /export, that contain the same mount point in the vfstab in both the active and inactive boot environments. Updating shared files in the active boot environment also updates data in the inactive boot environment. When you create a boot environment, shareable file systems are shared by default. If you specify a destination slice, also known as a partition, the file systems are copied.
- Swap – Swap depends on the type of file system:
  - For UFS file systems, swap is a special shareable volume. Like a shareable file system, all swap slices are shared by default. If you specify a destination directory for swap, the swap slice is copied.
  - For ZFS file systems, swap and dump volumes are shared within the pool.

Guidelines for Selecting Slices for Shareable File Systems

Live Upgrade copies the entire contents of a slice to the designated new boot environment slice. You might want some large file systems on that slice to be shared between boot environments rather than copied to conserve space and copying time. File systems that are critical to the OS such as root (/) and /var must be copied. File systems such as /home are not critical file systems and could be shared between boot environments. Shareable file systems must be user-defined file systems and on separate swap slices on both the active and new boot environments. You can reconfigure the disk several ways, depending your needs.

You can reslice, or partition, the disk before creating the new boot environment and put the shareable file system on its own slice. For example, if the root (/) file system, /var, and /home are on the same slice, reconfigure the disk and put /home on its own slice. When you create any new boot environments, /home is shared with the new boot environment by default.

To share a directory, the directory must be split off to its own slice. The directory is then a file system that can be shared with another boot environment. You can use the `lucreate` command with the `-m` option to create a boot environment and split a directory off to its own slice. But, the new file system cannot yet be shared with the original boot environment. You must run the `lucreate` command with the `-m` option again to create another boot environment. The two new boot environments can then share the directory.

Configuring Swap for the New Boot Environment

These guidelines contain configuration recommendations and examples for selecting a slice for a swap file system.

You can configure a swap slice in three ways by using the `lucreate` command with the `-m` option:

- If you do not specify a swap slice, the swap slices belonging to the current boot environment are configured for the new boot environment.
- If you specify one or more swap slices, these slices are the only swap slices that are used by the new boot environment. The two boot environments do not share any swap slices.
- You can specify to both share a swap slice and add a new slice for swap.

The following examples show the three ways of configuring swap. The current boot environment is configured with the root (/) file system on `c0t0d0s0`. The swap file system is on `c0t0d0s1`.

Example – No Swap Slice is Specified

- In the following example, no swap slice is specified. The new boot environment contains the root file system on `c0t1d0s0`. Swap is shared between the current and new boot environment on `c0t0d0s1`.

```
# lucreate -n be2 -m /:c0t1d0s0:ufs
```

Example – Swap Slice is Specified

- In the following example, a swap slice is specified. The new boot environment contains the root file system on `c0t1d0s0`. A new swap file system is created on c0t1d0s1. No swap slice is shared between the current and new boot environment.

```
# lucreate -n be2 -m /:c0t1d0s0:ufs -m -:c0t1d0s1:swap
```

Example – Add a Swap Slice and Share a Swap Slice

- In the following example, a swap slice is added and another swap slice is shared between the two boot environments. The new boot environment contains the root file system on `c0t1d0s0`. A new swap slice is created on `c0t1d0s1`. The swap slice on `c0t0d0s1` is shared between the current and new boot environment.

```
# lucreate -n be2 -m /:c0t1d0s0:ufs -m -:shared:swap -m -:c0t1d0s1:swap
```

Failed Boot Environment Creation if Swap is in Use

A boot environment creation fails if the swap slice is being used by any boot environment except for the current boot environment. If the boot environment was created using the `-s` option, the alternate-source boot environment can use the swap slice, but not any other boot environment.

Supported Live Upgrade Configurations

The Oracle Solaris Live Upgrade functionality enables you to run an OS Update job to create an alternate boot environment, manage boot environments, or to patch a managed Oracle Solaris OS. You cannot use Oracle Solaris Live Upgrade in Enterprise

Manager Ops Center to upgrade from one Oracle Solaris OS version to another, such as upgrading from the Oracle Solaris 8 OS to the Oracle Solaris 10 OS.

See LIVE UPGRADE REQUIREMENTS to verify that you have the required packages and patches needed to successfully perform a live update.

Supported Operating Systems

The following operating systems are supported with Oracle Solaris Live Upgrade in Enterprise Manager Ops Center:

- Oracle Solaris 10 OS for x86 Platforms up to and including Oracle Solaris 10 5/09 – Update alternate boot environments for physical systems.
- Oracle Solaris 10 OS for SPARC up to and including Oracle Solaris 10 5/09 – Update alternate boot environments for physical and virtual machines, including Oracle Solaris Zones and Oracle VM Server for SPARC (formerly known as Logical Domains).
- Oracle Solaris 9 OS SPARC – Update alternate boot environments for physical machines.
- Oracle Solaris 8 OS SPARC – Update alternate boot environments for physical machines.

Note: Additional packages and patches might be required to support Live Upgrade. See LIVE UPGRADE REQUIREMENTS for a list of required patches and packages and for special patch instructions when using Oracle Solaris Live Upgrade on Oracle Solaris 8 software.

Note: Using Oracle Solaris Live Upgrade and alternate boot environments is not supported for your Enterprise Controller and Proxy Controller systems. Live Upgrade does not synchronize all of the files that are required for the Enterprise Controller and Proxy Controller.

Oracle Solaris Live Upgrade and Oracle Solaris Zone Support

If you use Oracle Solaris Live Upgrade to update the OS in a greenfield zone (an zone created in Enterprise Manager Ops Center) the following conditions must be met:

- Agent must be running at least Oracle Solaris 10 5/09 (update 7) OS
- Must have a ZFS root file system
- Storage library used to house the zones cannot be part of the root pool; you must create a separate pool
- You cannot use the `lucreate -p` option to create ABEs

The `-p` option, which copies between two root pools on ZFS configuration, is not supported with the `lucreate` command.

Note: If your root file system is UFS and you create a brownfield zone, one that is created outside of Enterprise Manager Ops Center, you cannot create ZFS based non-global zones.

The following zone configurations with an alternate boot environment are supported in this release:

- UFS zones
- ZFS zones on the same root pool as the global zone

> **Note:** If you plan to use ABEs with zones, you must designate sufficient zone storage space. When you create the zones and configure the zone storage, specify twice the size of the zone file system for the / file system of the zone. For example if your zone / file system was configured as 8 GB, the storage used to back up the zone should be at least 16 GB.

See Updating Zones to patch Oracle Solaris Zones without using a dual boot environment.

Adding a Live Upgrade Script to Local Content

Oracle Solaris Live Upgrade contains a suite of script commands. To create an alternate boot environment with Enterprise Manager Ops Center, use the `lucreate` command to write one or more Oracle Solaris Live Upgrade scripts and then add the scripts to the Local Content library in Enterprise Manager Ops Center.

When you use Enterprise Manager Ops Center to create the ABE, the scripts must meet the following requirements:

- The script cannot contain parameters.
- The ABE name must be hard-coded into the script itself or otherwise be provided outside of Enterprise Manager Ops Center.
- The ABE name defined in the script must match the ABE name that you use when you run the update job to create the ABE.
- The script must return 0 on success and non-zero on failure.

For detailed instructions and examples for using the `lucreate` command to create a boot environment, see *Oracle Solaris 10 9/10 Installation Guide: Solaris Live Upgrade and Upgrade Planning* available at:

`http://www.oracle.com/technetwork/indexes/documentation/index.html`

To Add a Live Upgrade Script to Local Content

1. Expand Libraries in the Navigation pane.
2. Click Local Content in the Solaris/Linux OS Updates library.
3. Click Upload Local Action in the Actions pane.
4. Type a name for the file.
5. Enter a brief description of the purpose of the action.
6. In the Action list, click the Pre-action type of action. This will run the script on the managed host before job tasks are carried out.
7. Click the name of the distribution that uses the action in the Distribution list. The Parent field shows the category, based on the type of Action.
8. Click Browse to locate and select the file.

9. Click Upload. The file is uploaded to the selected distribution.

Creating an ABE Profile

Profiles specify which components are to be installed and which are prohibited, and the actions to be performed on a system. By defining the ABE create script as a pre-action, the profile helps you to automate creating alternate boot environments, manage dependencies, and ensure consistency.

To Create an ABE Profile

1. Expand Plan Management, then click Update Profiles.
2. Click New Profile from the Actions pane. The New OS Update Profile window is displayed.
3. Type a name and brief description of the new profile.
4. Select the OS Distribution from the drop-down list.
5. Search for your Live Upgrade ABE create script, or expand Local in the OS Update Components tree and select the script from the Pre-actions category.
6. Click Required.
7. Click Save as Named Profile.

Creating an ABE

Oracle Solaris Live Upgrade scripts are used to create an alternate boot environment (ABE). To create an exact replica of your boot environment, run the script in Enterprise Manager Ops Center to create the ABE.

The following methods are available to create the ABE:

- Upload an Oracle Solaris Live Upgrade script as Local Content in Enterprise Manager Ops Center.
  - Run an OS update job and specify a pre-action which runs the script. You can select multiple compatible targets and create an ABE for each target using the same script at the same time.
  - Create an OS Profile, and then run an OS Update job. The profile enables you to define the components and the actions to be performed every time you use the profile to create an ABE.
- Run an Oracle Solaris Live Upgrade script from the command line. With this method, you must log in to each agent and then run the script to create the ABE.

When you create the ABE with an OS Update job, you can choose to run the job immediately, or you can schedule the job to run during your maintenance window. In all methods, the new boot environment is automatically discovered and a new Boot Environment tab will appear in the center pane for OS management.

This task describes how to run a New OS Update job to create the ABE. Although it is a New OS Update job, the sole purpose of the job is to create an ABE. The job will use the Live Upgrade script that you uploaded to Local Content to create a duplicate of your boot environment.

Note: Do not use Oracle Solaris Live Upgrade on your Enterprise Controller or Proxy Controllers. It does not synchronize all of the files that are required for these Enterprise Manager Ops Center components.

Before You Begin

Review the following information before you create an ABE:

- Check for boot environment file system considerations, including slicing swap. See About Oracle Solaris Live Upgrade for more information.
- Check for supported operating systems and zone configurations. See Supported Live Upgrade Configurations for more information.
- Check for disk space, patch, and package requirements.

  See *Oracle Enterprise Manager Ops Center Reference Guide* for more information.
- (optional) Check for the steps to create a profile that includes the Live Upgrade script. See Creating an ABE Profile for detailed procedure.
- Check for script requirements and the steps to add a script to Local Content. See Adding a Live Upgrade Script to Local Content for more information.

To Create an ABE With an OS Update Job

1. Highlight the OS in the Assets section of the Navigation pane.
2. Click New Update OS Job in the Update section of the Actions pane. The New Update OS Job wizard is displayed. The Job Information window is displayed first.
3. Complete the following Job Information parameters:
   - Type a job name.
   - Select Actual Run, which will create the ABE at the time that you specify in Step 5.
   - Select the Sequential task execution order.
   - Select the Target Setting: Use the same Targets for all tasks in the job.
   - Select a Task Failure Policy:
     - Complete as much of the job as possible
     - Stop at failure and notify
   - Click the Boot Environment Type check box.
   - Click the Run ABE Pre-action Script check box.
4. (Optional) To add tasks to the job, click the Add Task icon. To edit, click the Profile and Policy fields.
5. Click Next.
6. Type the name of the ABE, as defined in the script. Select a script, then click Next.
7. (Optional) Complete the Boot Environment Workflow, then click Next.
   - To synchronize the alternate boot environment with the current boot environment before the ABE is mounted, click the Sync ABE check box.

- To edit the description to describe the state of the BE, click Modify Current BE, and add text to the Description field.
- To edit the description to describe the state of the ABE, click Modify Alternate BE, and add text to the Description field.
- To switch boot environments after update, click the Activate and Reboot ABE check box.

8. Schedule the job, then click Next.
   - Run Now starts the job immediately after you click Finish in the Job Summary.
   - Start Date enables you to select a date and time to start the job.
   - On a recurring schedule enables you to run the same job on a monthly or daily scheduled time.
9. Review the Job Summary, then click Finish to run the job as scheduled in the previous step.

When the job completes, the ABE is created and associated with the OS. To verify that the ABE was created, click the OS in the Assets pane. The Boot Environment tab appears in the center pane. Click the Boot Environment tab to display the new ABE, as specified in the Live Upgrade script. An OS can have multiple associated ABEs.

> **Note:** The Boot Environment tab is only displayed if there is at least one ABE associated with the OS.

To Create an ABE With a Profile

1. Create a profile and define the ABE create script as the pre-action.
   1. Expand Plan Management, then click Update Profiles in the Navigation pane.
   2. Click New Profile from the Actions pane. The New OS Update Profile window is displayed.
   3. Type a name and brief description of the new profile.
   4. Select the OS Distribution from the drop-down list.
   5. Search for your ABE create script, or expand Local in the OS Update Components tree and select the script from the Pre-actions category.
   6. Click Required.
   7. Click Save as Named Profile.
2. Create an OS Update job that uses your pre-action script and the ABE profile that you created in the previous step.
3. Click New Update OS Job in the Actions pane. The New Update OS Job wizard is displayed. The Job Information window is displayed first.
4. Complete the following Job parameters:
   - Type a job name.
   - Select Actual Run.
   - Select the Sequential task execution order.
   - Select the Target Setting: Use the same Targets for all tasks in the job.
   - Select a Task Failure Policy:

  - Complete as much of the job as possible
  - Stop at failure and notify
- To edit the profile or policy of the default task, click the Profile or Policy cell for the task to display a drop-down menu. Select the profile that you created in step 2 from the menu.
- Click the Target link, expand the Assets tree, highlight an OS, click Add to Target List, then click Select.

Click Next.

5. Schedule the job, then click Next.
   - Run Now starts the job immediately after you click Finish in the Job Summary.
   - Start Date enables you to select a date and time to start the job.
   - On a recurring schedule enables you to run the same job on a monthly or daily scheduled time.
6. Review the Job Summary, then click Finish to run the job as scheduled in the previous step.
7. When the job completes, the ABE is created and associated with the OS. To verify that the ABE was created, click the OS in the Assets pane. The Boot Environment tab appears in the center pane. Click the Boot Environment tab to display the new ABE, as specified in the lucreate script. An OS can have multiple associated ABEs.

Note: The Boot Environment tab is only displayed if there is at least one ABE associated with the OS.

Updating an ABE

You can create a customized update job, including the option to use an alternate boot environment (ABE) to perform a live upgrade of your Oracle Solaris 10 OS. With Live Upgrade, you create an inactive ABE, update and patch the ABE, synchronize the ABE and BE, and then switch boot environments. When you switch boot environments, the patched and tested ABE becomes the active boot environment.

Note: Do not use Live Upgrade on your Enterprise Controller or Proxy Controllers. Live Upgrade does not synchronize all of the files that are required for these components.

You must run a separate update job for systems that use an ABE from those that do not use an ABE. When creating a job, you must define the following job parameters:

- Name and description of the update job.
- Alternate Boot Environment.
- Profile – Defines what updates are to be installed, uninstalled, or updated on an OS. Select a profile from the list of predefined and customized profiles.
- Policy – Defines how a job is performed and sets the automation level of the job. Select a policy from the list of available policies. You can also create your own policies.

- Target Settings – Defines whether the target should be different or similar for each task in the job.
- Actual Run – Defines whether this job is in simulation mode. You can choose to deploy the job, or to run a job simulation. A job simulation determines the actions and results of a job, and estimates how much time is required to complete the job. A job simulation also indicates whether your policy and profile responses will enable the job to succeed.
- Task Execution Order – Specifies whether the tasks should be run in parallel or sequentially.
- Task Failure Policy – Specifies what action should be taken if a task fails.
- Targets – Select one or more target hosts for this job.

Before You Begin

To create an ABE as part of this job, you must write at least one script that uses the `lucreate` command and then upload the script to the Local Content.

See *Oracle Enterprise Manager Ops Center Advanced User's Guide* for a detailed procedure to upload a local action.

> **Note:** The ABE name defined in the script must match the ABE name that you use when you run the update job to create the ABE.

To Update an ABE

1. Click Assets in the Navigation pane.
2. Expand All Assets, or use the All Assets filter to locate the Oracle Solaris 10 OS instance.
3. Click New Update OS Job from the Actions pane. The New Update OS Job wizard is displayed. The Job Information window is displayed first.
4. Complete the following Job parameters:
   - Type a job name.
   - Select the Run Type:
     - Simulation. To download the required patches as part of the simulation, click the Download check box.
     - Actual Run.
   - Select the task execution order:
     - Sequential
     - Parallel
   - Choose the Target Setting:
     - Use the same Targets for all tasks in the job
     - Use different Targets for each task in the job
   - Choose the Task Failure Policy:
     - Complete as much of the job as possible
     - Stop at failure and notify

- Click the ABE check box.
- (optional) To create an alternate boot environment during this job by running an ABE Pre-Action Script, click the Enable check box.

> **Note:** You must have created the script and uploaded it to the Library for this option.

5. You can define the profile, policy and target for each task, or edit the profile and policy.
6. To edit the profile or policy of the default task, click the Profile or Policy cell for the task to display a drop-down menu. Select the profile or policy from the menu.
7. To add a new task, click the plus (+) icon.
   - A second row will appear. Click the Profile cell for that row to display a drop-down menu. Select the new profile that you want to add.
   - To change the policy for the new profile, click the Policy cell and select a new policy from the drop-down menu.
   - If you chose the parameter to use a different target for each task, click the Targets cell to display the Select Targets page. Select one or more target from the list of Available Items, then click Select to include the asset in the Target List. Click Add to Target List to close the page.
   - Click Next.
8. If you selected chose to create an ABE as part of the job, the Create ABE page appears.
9. If you have only one ABE, the Boot Environment Workflow page appears, go to step 10. If you have multiple alternate boot environments, the ABE Selection page appears.
   - One or more of the targets has more then one possible associated ABE. Select the ABE from the drop-down menu for each of the Targets. You can use the Select ABE field to filter for the ABE name.
   - Click Next. The Boot Environment Workflow page is displayed.
10. If you selected Simulation in the job parameters, the boot environment workflow cannot be edited, Click Next. Skip to step 12.
11. If you selected Actual Run in the job parameters, you can edit the pre-actions and post-actions in the workflow.
    - Pre-actions by default will unmount and then mount the ABE. To synch the ABE with the BE before mounting, click the Sync ABE check box.
    - Post-Actions by default will unmount the ABE.
      - Click Modify Current BE to edit the description of the current boot environment. You might use this to describe the state of the current BE. For example, Boot environment running Oracle Solaris 10 5/08 OS before applying the Oracle Solaris 10 OS September baseline.
      - Click Modify Alternate BE to edit the description of the ABE. You might use this to describe the state of the ABE. For example, Boot environment running Oracle Solaris 10 5/08 OS after applying the Oracle Solaris 10 OS September baseline.

- Click Activate and Reboot ABE to switch boot environments after update.

12. Schedule the job, then click Next.
    - Run Now starts the job immediately after you click Finish in the Job Summary.
    - Start Date enables you to select a date and time to start the job.
    - On a recurring schedule enables you to run the same job on a monthly or daily scheduled time.
13. Review the Job Summary, then click Finish to run the job as scheduled in the previous step.

BE Reports and System Catalogs

The OS Update Reports and Catalogs are those of the active boot environment (BE). To see the differences between the active BE and the alternate boot environment (ABE), you must reboot into the ABE and then compare the snapshots. To create an OS report or catalog, make the ABE the active BE, then see Using the Solaris OS Update Reports.

Reports

You can run all available reports for the active BE, including compliance reports. Reports are generally not available for the ABE, and any reports are typically outdated.

To create a report for an ABE, you must reboot into it to make it the active BE, then run the compliance report.

Catalogs

An update catalog is an OS inventory of your OS and is automatically created when you manage a system. When you have a dual boot environment, the OS Update catalog displays the name and description of the active boot environment.

The catalog is the inventory of the active boot environment. To view the current inventory of an ABE, you must make it the active boot environment and create a historical catalog (snapshot).

When you create the snapshot, manually specify the system. The snapshot is of the current active boot environment and does not indicate that the system might be an ABE.

Viewing and updating an OS Update catalog for a boot environment is the same as other OS catalog.

7

Upgrading an Oracle Solaris Cluster

The cluster update procedures operate on complete clusters. It is not possible to upgrade only a cluster node.

To upgrade a cluster to a newer version of the Oracle Solaris Cluster software, use a profile that defines the new version. You can begin the procedure by either selecting the target cluster and then the deployment plan or selecting the deployment plan and then the target. In either case, you use the Solaris Cluster Upgrade Job wizard to specify how the deployment operates.

Before You Begin

Import the cluster profile.

See *Oracle Enterprise Manager Ops Center Advanced User's Guide* for detailed procedure about importing a cluster profile.

To Upgrade the Cluster

1. Expand Plan Management in the Navigation pane.
2. In the Profiles and Policies section, click Update Profiles.
3. Select Oracle Solaris Upgrade Job in the Actions pane. The Oracle Solaris Upgrade Job wizard starts.
4. Enter a name for the upgrade job.
5. Click display the cluster targets.
6. Choose one or more clusters and click Select/Add to Target List.
7. Select Dual Partition Mode.
8. Select the policy to use if a task in the upgrade cannot be completed.
9. Select the profile that you imported.
10. Review the summary of the job and click Finish. The upgrade job is submitted. You can follow the progress of the job by clicking the View Job Details icon in the jobs pane.

8 Firmware and OS Update Reports

A number of firmware compliance, and OS update reports are available. Enterprise Manager Ops Center provides reports that are very specific to Oracle Solaris such as Baseline Analysis Report. There are reports that are more commonly used for the compliance status of the OS.

Reports are grouped in the UI in the following way:

- OS Reports – Includes Oracle Solaris and Linux OS Updates and Windows Updates Reports.
- System Information Report – Provides report for different assets such as OS, server, and chassis.
- Problem Reports – See *Oracle Enterprise Manager Ops Center User's Guide* for more information.
- Additional Reports – Includes reports such as Distribution Update, Service Pack Compliance, Oracle Solaris Update Compliance, and Package Compliance.

Enterprise Manager Ops Center provides option to save the report parameters which can be used for later use. It provides interactive result viewer to view the report results in interactive mode which provides option to make the targets compliant.

You also have option to view and save the results in CSV or PDF formats.

> **Note:** Large reports can consume significant disk space. Report PDF and CSV files are stored in the `/var/opt/sun/xvm/reports` directory. You can relocate this directory to a dedicated disk. To free up disk space, remove old report results.

Using the Firmware Compliance Report

The Firmware Report feature compares the firmware images specified in a firmware profile to the firmware images installed on one or more hardware assets. The report indicates whether the firmware on the asset complies with the profile's specifications. You have the option of updating the firmware on any non-compliant assets by clicking the Make Targets Compliant button in the Interactive report.

To Create a Firmware Report

1. Expand Reports in the Navigation pane.
2. Select Firmware Reports.
3. Select Create Firmware Report from the Actions pane. The Create Firmware Report wizard is displayed.

4. Specify the name and a description for the report.
5. If you do not plan to create this report routinely, clear the Create Schedule checkbox.
6. By default, the report is created in PDF format and CSV format. Clear the checkbox for the type of file format you do not want to create.
7. Select the firmware profile and click Next. You can select a profile for a service processor or for a storage component, such as a RAID controller, expander, or disk.
8. Select the targets you want to test against the profile. Select the asset from the Available Items hierarchy and click Add to Target List. When you have selected all the targets, click Next.
9. If you plan to create the report routinely, define the schedule. You can choose to run the report immediately, at a set date, or routinely at a set time.
10. Review the summary and click Run Report to create the report job. You also have the option of saving the report as a template for subsequent reports. The report job starts at the time you specified and compares the values in the profile to the existing values on the targets you selected.

The report shows whether a target asset is compliant, not compliant, or not applicable:

- A compliant asset has the firmware images specified in the profile.
- A non-compliant asset does not have the same firmware images as specified in the profile. You can update the firmware on the asset, by either clicking the Make Targets Compliant button in the Interactive report or using the procedure in Updating Firmware.
- A non-applicable asset indicates that a firmware image in the profile does not match the model of service processor in the asset. This condition can occur when either the profile does not recognize the model that the service processor is reporting or the profile includes firmware images that are not designed for the service processor.

  1. Compare the model of the service processor displayed in the asset's Summary tab with the model of the service processor included in the profile. If they are different, add the name in the profile to the asset's data.

     See *Oracle Enterprise Manager Ops Center Administration Guide* for information about adding a product alias.

  2. When the firmware profile was created, only images that matched the service processor could be included. However, if the service processor did not report all the firmware types it supported, an image that did not match the service processor could have been included in the profile. To update the Enterprise Manager Ops Center software with all the service processor's supported firmware types, use the Refresh action to update the information about the service processor. When the job is completed, view the service processor's Summary tab to see all firmware types.
  3. Repeat the procedure to create a firmware report.

Using the Solaris OS Update Reports

Solaris OS Update reports enable you to check for new patches and security advisories. You can get a general report, or test a system or installed package for available fixes. For auditing purposes, you can create a change history report.

When you create a report, you select the criteria that are relevant to your data center, such as a list of targets that have a specific patch or a list of targets that do not have a specific patch. The CVE Compliance report enables you to search for specific Solaris patches by their CVE IDs.

Reports like Baseline Analysis are exclusive for Solaris OS which generates compliance reports for released Solaris baselines.

The following topics are covered in this section:

- Creating a Baseline Analysis Report
- Creating a Baseline Analysis Report in Disconnected Mode
- Creating a Host Compliance Report (Solaris)
- Creating an Incident Compliance Report (Solaris)
- Creating a CVE Report (Solaris)
- Creating a Profile Report (Solaris)
- Creating a Recommended Software Configuration Report (Solaris)
- Creating a Change History Report (Solaris)
- Creating a Distribution Update Report (Solaris)
- Creating a Package Compliance Report (Solaris)
- Creating a Solaris Update Compliance Report
- Creating a Service Pack Compliance Report (Solaris)

Creating a Baseline Analysis Report

The Baseline Analysis Report (BAR) enables you to determine whether your managed system is compliant with recently released Solaris baselines. Baselines pertain only to Solaris systems. This section describes Solaris baselines, white list, black list, and how to run a Baseline Analysis report in connected and disconnected mode of the Enterprise Controller.

Solaris Baselines

A Solaris baseline is a dated collection of Solaris patches, patch metadata, and tools. Oracle releases Solaris baselines on a monthly basis. When you install the patches of a baseline on a host, that system is considered to be compliant with that baseline.

Each dated baseline contains these patch sets:

- Full – Includes all Solaris patches
- Recommended – Includes Solaris recommended patches and security patches
- Security – Includes only Solaris security patches

All baselines include patches for a specific time frame. However, the Full baseline often contains Solaris OS patches that are not included in the Recommended baseline. The Full baseline includes additional patches based on feedback from various customer support groups within Oracle. These patches are not always included in the Recommended baseline.

To install the Recommended and Security baselines, you must either deploy two jobs or have a job that includes multiple tasks. This might result in multiple reboots, for example, if both tasks (baselines) include patches that have Single User mode requirements.

Enterprise Manager Ops Center's Knowledge Base (KB) is updated with the information about the baselines. This is done a few days after the official release of baselines by Oracle.

Note: The Solaris 8 OS was placed into End of Service Live (EOSL) on March 31, 2009. Solaris 8 OS baselines are available through March 2009. The KB might contain artificial baselines after that date. Do not use baselines dated after March 2009.

Using Solaris baselines enables you to easily identify the patch level of your hosts. For example, you install some test hosts with a particular baseline. Then, you test these hosts for a period to see whether the patches in this baseline are stable enough to be used on your production hosts. When the testing reveals that this baseline is stable, you can install the same baseline on your production hosts.

Solaris baselines are available as a component in the recommended component list. It contains a list of dated baselines.

The Baseline Analysis report helps to verify the compliance of your system against the newly released baselines (as and when they are available in Knowledge Base).

White List

A white list is the list of patches that you want to install in addition to the patches in the baseline. To establish a white list, create a profile using the Required setting. You can also specify a white list when generating a Baseline Analysis report. Select the white list either from the created profile or enter the patch IDs separated by new lines.

For example, baseline B includes patches X, Y, and Z, and the white list has patches U, V, and W. When your Baseline Analysis report is created, the host is marked compliant only when all six patches X, Y, Z, U, V, and W are present.

Black List

A black list is a list of patches that you do not want installed. You create a black list by creating a policy with the specified action for the patches. You can select a black list option when you create a Baseline Analysis report. Select the black list either from the created policy or enter the patch IDs separated by new lines.

If a particular patch in the profile is set with the policy component setting as Never for an install action, then the patch is not installed. If the patch is already installed, it will not be uninstalled or removed.

For example, if baseline A has patches X, Y, and Z, and the black list specifies only Y and Z, the system is compliant if X is installed. If the patches Y and Z are already installed, they will not get uninstalled if you run a compliance job from the report results. If Y and Z are not installed, they will not be listed in the non compliant result and will not be added in the compliance job.

This section describes how to generate a BAR. The report gives the compliance status of the managed system with the selected Solaris baseline that was released.

You can generate two types of BARs:

- Agent-based BAR
- Database-based BAR

In an agent-based BAR, a simulated job is executed against the managed hosts. This type of report takes time to complete because it checks for dependent components and missing dependencies, and then downloads the patches that must be installed. When you run a compliance job from this report result, the job is completed quickly because the patches are already downloaded. However, to improve the report performance of a BAR, you can skip the downloads in a simulated job by clearing the check box that is provided for this purpose.

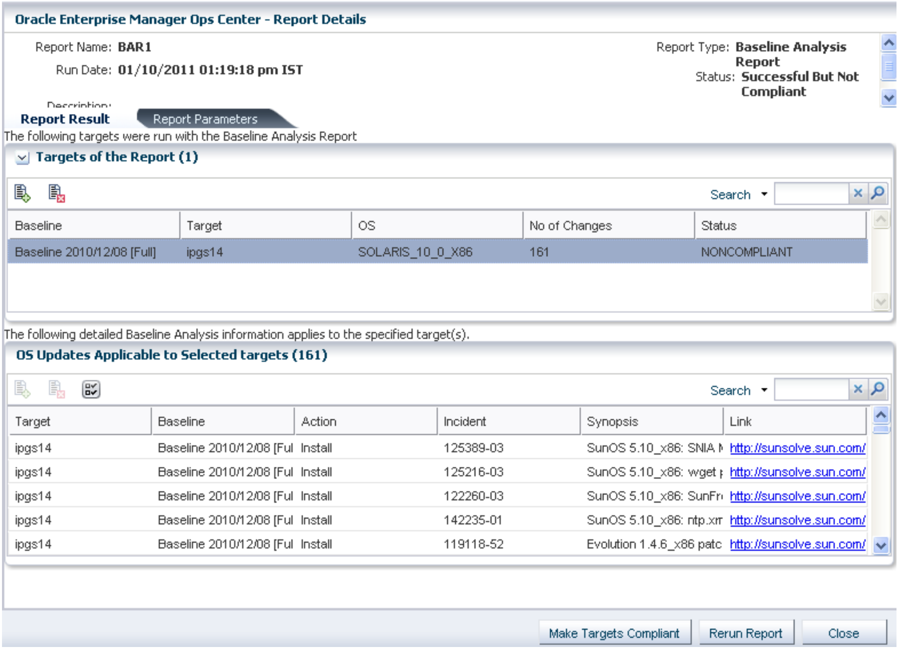
In a database-based BAR, the report is run against the database of the management server, the selected baselines are broken down into individual patch IDs, and then formed into an incidents list. The report is generated based on the information that are available on the database. Based on the report result, you can run a compliance job.

To Generate a Baseline Analysis Report

This report provides information about the hosts that are compliant with a baseline OS.

1. Select Reports from the Navigation pane.
2. Select Solaris/Linux OS Updates from the Reports section.
3. Select Create Baseline Report from the Actions pane. The Create Baseline Analysis Report wizard is displayed.
4. Define the report parameters:
   - Report Name – Name of the report.
   - Description – The description of the report.
   - Schedule – Select Create Schedule to schedule the report.
   - Output Format – Select the output format of the report result. CSV and PDF formats are available.
   - Select Targets – Add the targets by selecting them from the list of Available Items and clicking Add to Target List
5. Click Next to select the Solaris baselines.
6. In Select Baseline(s), select the following options:

Figure 8–1 Selecting Baselines for Baseline Analysis Report



Oracle Enterprise Manager Ops Center - Report Details

Report Name: **BAR1**

Run Date: **01/10/2011 01:19:18 pm IST**

Description:

Report Type: **Baseline Analysis Report**

Status: **Successful But Not Compliant**

The following targets were run with the Baseline Analysis Report

Targets of the Report (1)

Baseline	Target	OS	No of Changes	Status
Baseline 2010/12/08 [Full]	ipgs14	SOLARIS_10_0_X86	161	NONCOMPLIANT

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

OS Updates Applicable to Selected targets (161)

Target	Baseline	Action	Incident	Synopsis	Link
ipgs14	Baseline 2010/12/08 [Ful	Install	125389-03	SunOS 5.10_x86: SNIA M	http://sunsolve.sun.com/
ipgs14	Baseline 2010/12/08 [Ful	Install	125216-03	SunOS 5.10_x86: wget p	http://sunsolve.sun.com/
ipgs14	Baseline 2010/12/08 [Ful	Install	122260-03	SunOS 5.10_x86: SunFr	http://sunsolve.sun.com/
ipgs14	Baseline 2010/12/08 [Ful	Install	142235-01	SunOS 5.10_x86: ntp.xm	http://sunsolve.sun.com/
ipgs14	Baseline 2010/12/08 [Ful	Install	119118-52	Evolution 1.4.6_x86 patc	http://sunsolve.sun.com/

- Select either Run Against Database or Run Against Agent.
- Select Download for Run Against Agent to download the patches that must be installed on the target.
- Select the distribution type and select the baselines from the list. You can select targets of multiple distribution. For each distribution, select the corresponding baselines. A warning message is displayed if you have not selected baselines for a distribution.

> **Note:** If you have multiple distributions, then you must select baselines for at least one distribution to continue further in the wizard. If you have not selected baselines for a distribution, then the targets of that distribution will not be in the report result.

- Click Add or click Add All to select all the baselines.

7. Click Next to modify the patch lists that are applied to the report.
8. Select a White List option:
   - None – No white list.
   - Manual Input – Enter a list of patches.
   - Specify with Profile – Select a profile to import as a white list.
9. Select a black list option:
   - None – No black list.
   - Manual Input – Enter a list of patches.
   - Specify with Policy – Select a policy to import as a black list.
10. Click Next to schedule the report.
11. Select a schedule for the report. You can schedule the report to run:

- Immediately.
- On a start date and time – Select a date and time to generate the report.
- On a recurring schedule – Select the month and day when you want to generate the report. Select the Start Time, End Time and Number of Hours between runs. This is to set the number of times the report generated between the specified start and end time. For example, if you set the start time at 6.00 a.m, end time at 12.00 a.m and the number of hours between runs as 2, then the report is run at 6.00 a.m, 8.00 a.m, 10.00 a.m and 12.00 a.m.

12. Click Next to view the summary of the report.
13. Review the report parameters and select one of the options as required:
    - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate reports later.
    - Run and Close – Runs the report and closes the wizard window.

The report result is displayed under the Report Results in the center pane. See Viewing and Exporting Report Results for more information about viewing a report result and generating a compliance job from the result.

Creating a Baseline Analysis Report in Disconnected Mode

During the initial Enterprise Controller configuration, you have the option to set up Enterprise Manager Ops Center in disconnected mode. If your system is not in disconnected mode, you must specifically switch to disconnected mode. To run a BAR in disconnected mode, you must upload the appropriate month's EIS-DVD to Enterprise Manager Ops Center. Another option is to include the baselines in the KB bundle that is generated by the harvester script. With this option, you do not have to upload the EIS-DVD to Enterprise Manager Ops Center.

To Create a Baseline Analysis Report in Disconnected Mode

1. Generate a KB bundle. See Obtaining a KB Bundle With the Harvester Script for more information.
2. Select Administration from the Navigation pane.
3. Select Setup Disconnected Mode from the Actions pane.
4. Specify a KB bundle and click Load KB Bundle.
5. Select Switch to Disconnected Mode. You must first load a bundle or you will be unable to switch.
6. Upload the EIS-DVD contents.
7. Run the Baseline Analysis Report. See Creating a Baseline Analysis Report for the detailed procedure.
8. View the report result and initiate a compliance job to install the latest patches.

Creating a Change History Report (Solaris)

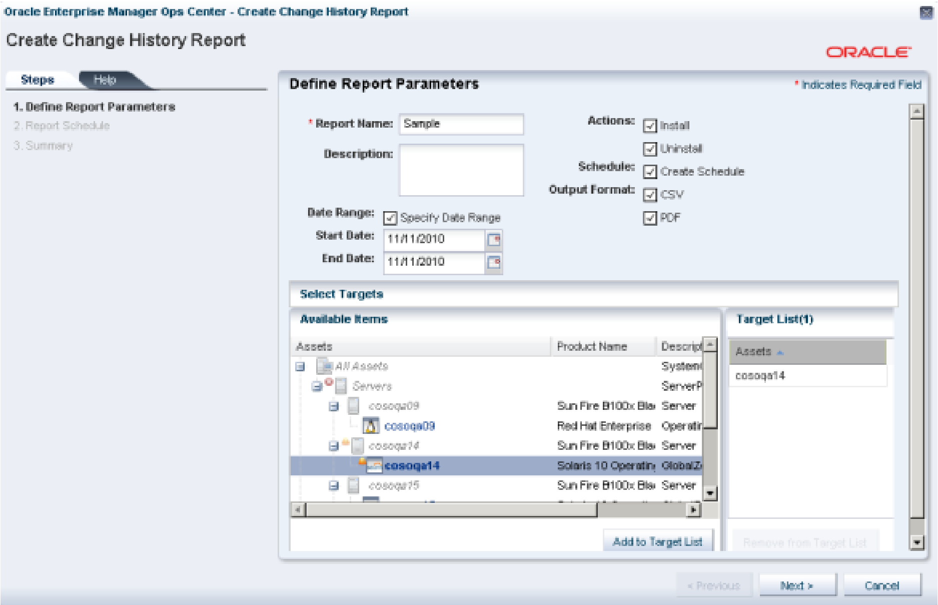
The Change History report provide a detailed history of the install and uninstall actions taken on an asset managed by Enterprise Manager Ops Center. This report also shows which user made the deployments, enabling you to track a team of operators. After your report criteria is selected, you can generate a report and save it as a template. The saved report template enables you to run the report again with the same specified parameters for the targeted systems, install actions, and time period.

To Generate a Change History Report for Solaris OS

1. Select Reports from the Navigation pane.
2. Select Solaris/Linux OS Updates from the Reports section.
3. Select Create Change History Report from the Actions pane.

   The Create Change History Report wizard is displayed.

Figure 8–2 Defining Report Parameters for Change History Report



Oracle Enterprise Manager Ops Center - Create Change History Report

Create Change History Report

1. Define Report Parameters
2. Report Schedule
3. Summary

Define Report Parameters

* Indicates Required Field

* Report Name: Sample

Description:

Date Range: ☑ Specify Date Range

Start Date: 11/11/2010

End Date: 11/11/2010

Actions: ☑ Install ☑ Uninstall

Schedule: ☑ Create Schedule

Output Format: ☑ CSV ☑ PDF

Select Targets

Available Items

Assets	Product Name	Descript
All Assets		System
Servers		ServerP
cosoqa09	Sun Fire B100x Bla	Server
cosoqa09	Red Hat Enterprise	Operati
cosoqa14	Sun Fire B100x Bla	Server
cosoqa14	Solaris 10 Operatin	GlobalZ
cosoqa15	Sun Fire B100x Bla	Server

Target List(1)

Assets
cosoqa14

4. Define the report parameters:
   - Report Name – The name of the report.
   - Description – A description of the report.
   - Date Range – Specify the start date and end date between which the report will cover.
   - Actions – Select the actions that you want to be reported. You can select Install, Uninstall or both.
   - Schedule – Select Create Schedule to schedule the report.
   - Output Format – Select the output format of the report result. CSV and PDF formats are available.
   - Select Targets – Add the targets by selecting them from the list of Available Items and clicking Add to Target List.
5. Click Next to schedule the report.
6. Select a schedule for the report. You can schedule the report to run:
   - Immediately.
   - On a start date and time – Select a date and time to generate the report.
   - On a recurring schedule – Select the month and day when you want to generate the report. Select the Start Time, End Time and Number of Hours between runs. This is to set the number of times the report generated between the specified start and end time. For example, if you set the start time at 6.00

a.m, end time at 12.00 a.m and the number of hours between runs as 2, then the report is run at 6.00 a.m, 8.00 a.m, 10.00 a.m and 12.00 a.m.

7. Click Next to view the summary of the report.
8. Review the report parameters and select one of the options as required:
   - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
   - Run and Close – Runs the report and closes the wizard window.

The report result is displayed under the Report Results in the center pane. See Viewing and Exporting Report Results for more information about viewing a report result.

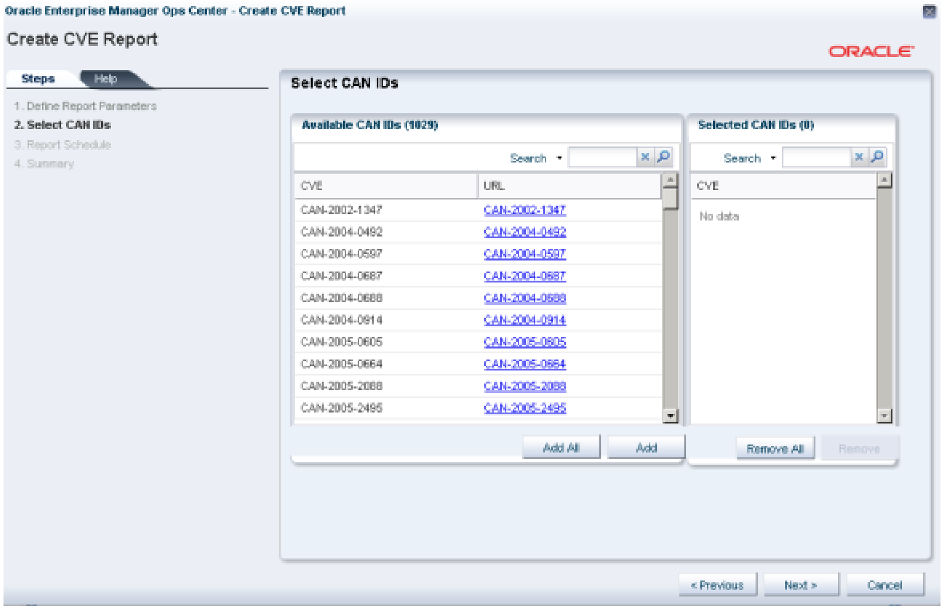
Creating a CVE Report (Solaris)

The CVE report provides information about incidents that are related to specific CVE IDs and the systems that must have these incidents installed. Common Vulnerability and Exposure Identifiers (CVE IDs) are unique, common identifiers for publicly known security vulnerabilities. The patches and packages from a list of vendors are published as common vulnerabilities and security exposure incidents. CVEs are identified by a candidate ID (CAN ID).

To Generate a CVE Report for Solaris OS

1. Select Reports from the Navigation pane.
2. Select Solaris/Linux OS Updates from the Reports section.
3. Select Create CVE Report from the Actions pane. The Create CVE Report wizard is displayed.
4. Define the report parameters. They include:
   - Report Name – The name of the report.
   - Description – A description of the report.
   - Compliance – Select either compliant or non-compliant report.
   - Schedule – Select Create Schedule to schedule the report.
   - Output Format – Select the output format of the report result. CSV and PDF formats are available.
   - Select Targets – Add the targets by selecting them from the list of Available Items and clicking Add to Target List.
5. Click Next to select the CAN IDs.
6. Select one or more CAN IDs and click Add or click Add All to select all the available CAN IDs.

Figure 8–3 Selecting CAN IDs in CVE Report



Select CAN IDs

Available CAN IDs (1029)

CVE	URL
CAN-2002-1347	CAN-2002-1347
CAN-2004-0492	CAN-2004-0492
CAN-2004-0597	CAN-2004-0597
CAN-2004-0687	CAN-2004-0687
CAN-2004-0688	CAN-2004-0688
CAN-2004-0914	CAN-2004-0914
CAN-2005-0605	CAN-2005-0605
CAN-2005-0664	CAN-2005-0664
CAN-2005-2088	CAN-2005-2088
CAN-2005-2495	CAN-2005-2495

Selected CAN IDs (0)

CVE
No data

7. Click Next to schedule the report.
8. Select a schedule for the report. You can schedule the report to run:
   - Immediately.
   - On a start date and time – Select a date and time to generate the report.
   - On a recurring schedule – Select the month and day when you want to generate the report. Select the Start Time, End Time and Number of Hours between runs. This is to set the number of times the report generated between the specified start and end time. For example, if you set the start time at 6.00 a.m, end time at 12.00 a.m and the number of hours between runs as 2, then the report is run at 6.00 a.m, 8.00 a.m, 10.00 a.m and 12.00 a.m.
9. Click Next to view the summary of the report.
10. Review the report parameters and select one of the options as required:
    - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
    - Run and Close – Runs the report and closes the wizard window.

The report result is displayed under the Report Results in the center pane. See Viewing and Exporting Report Results for more information about viewing a report result and generating a compliance job from the result.

Creating a Distribution Update Report (Solaris)

The Distribution Update report provides a mapping between selected updates, packages, and CVEs and selected distributions so that you can find out whether the updates are installed. This report shows whether a specific distribution has been updated with specific updates, packages, or CVEs.

To Generate a Distribution Update Report for Solaris OS

1. Select Reports from the Navigation pane.

2. Select Additional Reports from the Reports section.
3. Select Distribution Update Report from the Actions pane. The Distribution Update Report Creation Wizard is displayed.
4. Specify the report parameters:
   - Name – The name of the report.
   - (Optional) Description – A description of the report.
   - Category – Select one or more of the following:
     - Security
     - Bug fix
     - Enhancement
     - Service pack
     - Solaris update
     - CD
   - Type – Select package, update or both.
   - Release Date – Select a start date and end date between which the update was released.
5. Click Next to specify the distribution. The Specify Distributions page is displayed.
6. Select the distributions by clicking them and clicking Add or by clicking Add All, then click Next. The Select Updates page is displayed.
7. Select the updates by clicking them or clicking Select All, then click Next. The Select Packages page is displayed.
8. Select the packages by clicking them or clicking Select All, then click Next. The Select CVE page is displayed.
9. Select one or more CVEs by clicking them or clicking Select All, then click Next. The Summary page is displayed.
10. (Optional) Click Save Report to save the report for future use. This returns you to the Reports tab, where you can run the report by selecting it from the Saved Reports section and clicking Re-run Report.
11. Click Run Report. The report result is displayed.
12. (Optional) Click Export to CSV to export the report result.
13. Click Done to close the report.

Creating a Host Compliance Report (Solaris)

You can run a host compliance report to determine whether the hosts are complaint with security and bug fix incidents.

To Generate a Host Compliance Report for Solaris OS

1. Select Reports from the Navigation pane.
2. Select Solaris/Linux OS Updates from the Reports section.
3. Select Create Host Compliance Report from the Actions pane. The Create Host Compliance Report wizard is displayed.

4. Define the report parameters:
   - Report Name – The name of the report.
   - Description – A description of the report.
   - Update Level – Select whether you want the compliant status for Security and Bug Fixes or for only Security Updates.
   - Compliance – Select either Compliant or Non-Compliant.
   - Schedule – Select Create Schedule to schedule the report.
   - Output Format – Select the output format of the report result. CSV and PDF formats are available.
   - Select Targets – Add the targets by selecting them in the list of Available Items and clicking Add to Target List.
5. Click Next to schedule the report.
6. Select a schedule for the report. You can schedule the report to run:
   - Immediately.
   - On a start date and time – Select a date and time to generate the report.
   - On a recurring schedule – Select the month and day when you want to generate the report. Select the Start Time, End Time and Number of Hours between runs. This is to set the number of times the report generated between the specified start and end time. For example, if you set the start time at 6.00 a.m, end time at 12.00 a.m and the number of hours between runs as 2, then the report is run at 6.00 a.m, 8.00 a.m, 10.00 a.m and 12.00 a.m.
7. Click Next to view the summary of the report.
8. Review the report parameters and select one of the options as required:
   - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
   - Run and Close – Runs the report and closes the wizard window.

The report result will be displayed under the Report Results in the center pane. See Viewing and Exporting Report Results for more information about viewing a report result and generating a compliance job from the result.

Creating an Incident Compliance Report (Solaris)

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

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

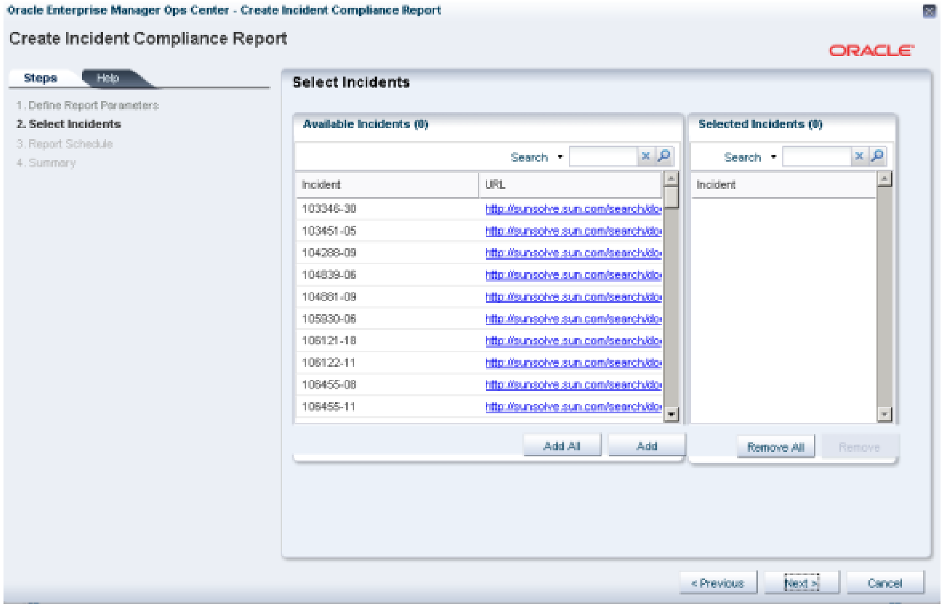
To Generate an Incident Compliance Report for Solaris OS

1. Select Reports from the Navigation pane.
2. Select Solaris/Linux OS Updates from the Reports section.
3. Select Create Incident Report from the Actions pane. The Create Incident Compliance Report wizard is displayed.
4. Define the report parameters:
   - Report Name – The name of the report.

- Description – A description of the report.
- Criteria – Select the criteria for selecting the patches that are used as a comparison. Depending on the selection of criteria the wizard steps vary. You can select Select Updates or Filter Updates.
- Compliant – Select either Compliant or Non-compliant for compliance status.
- Schedule – Select Create Schedule to schedule the report.
- Output Format – Select the output format of the report result. CSV and PDF formats are available.
- Select Targets – Add the targets by selecting them from the list of Available Items and clicking Add to Target List.

5. Click Next to select the updates.
6. If you have selected Select Updates in the previous step, the list of available incidents is displayed.

Figure 8–4 Selecting Incidents for Incident Compliance Report



Oracle Enterprise Manager Ops Center - Create Incident Compliance Report

Create Incident Compliance Report

1. Define Report Parameters
2. Select Incidents
3. Report Schedule
4. Summary

Select Incidents

Available Incidents (0)

Incident	URL
103346-30	http://sunsolve.sun.com/search/do
103451-05	http://sunsolve.sun.com/search/do
104288-09	http://sunsolve.sun.com/search/do
104839-06	http://sunsolve.sun.com/search/do
104881-09	http://sunsolve.sun.com/search/do
105930-06	http://sunsolve.sun.com/search/do
106121-18	http://sunsolve.sun.com/search/do
106122-11	http://sunsolve.sun.com/search/do
106455-08	http://sunsolve.sun.com/search/do
106455-11	http://sunsolve.sun.com/search/do

Selected Incidents (0)

Incident

7. Select the incidents and click Add or click Add All to select all the listed incidents.
8. If you have selected Filter Updates in the first step, then select the following:
   - Select Packages – You can select the packages based on the category, update type and releases date. Select the packages and click Add or click Add All to select all the packages in the Available Packages list. Click Next to select the CAN IDs.
   - Select CAN IDs – Select from the list of Available CAN IDs. Click Add or Add All as required.
9. Click Next to schedule the report.
10. Select a schedule for the report. You can schedule the report to run:
    - Immediately.
    - On a start date and time – Select a date and time to generate the report.

- On a recurring schedule – Select the month and day when you want to generate the report. Select the Start Time, End Time and Number of Hours between runs. This is to set the number of times the report generated between the specified start and end time. For example, if you set the start time at 6.00 a.m, end time at 12.00 a.m and the number of hours between runs as 2, then the report is run at 6.00 a.m, 8.00 a.m, 10.00 a.m and 12.00 a.m.

11. Click Next to view the summary of the report.
12. Review the report parameters and select one of the options as required:
    - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
    - Run and Close – Runs the report and closes the wizard window.

The report result will be displayed under the Report Results in the center pane. See Viewing and Exporting Report Results for more information about viewing a report result and generating a compliance job from the result.

Creating a Package Compliance Report (Solaris)

The Package Compliance report provides details pertaining to the selected packages on the managed system and shows whether the system is compliant with the latest recommended available version.

To Generate a Package Compliance Report for Solaris OS

1. Select Reports from the Navigation pane.
2. Select Additional Reports from the Reports section.
3. Select Package Compliance Report from the Actions pane. The Package Compliance Report Creation Wizard is displayed.
4. Specify the report parameters:
    - Name – The name of the report.
    - Description – A description of the report.
    - Status – Select either Compliant or Not Compliant.
    - Level – Select Security Updates or Security and Bug Updates.
5. Click Next to select the targets for which you want to run the report. The Select Targets page is displayed.
6. Add the targets by selecting them from the list on the left and clicking Add to Target List, then click Next. The Select Packages page is displayed.
7. Select the packages by clicking them or click Select All, then click Next. The Summary page is displayed.
8. (Optional) Click Save Report to save the report for future use. This returns you to the Reports tab, where you can run the report by selecting it from the Saved Reports section and clicking Re-run Report.
9. Click Run Report. The report is displayed.
10. (Optional) Select the packages by clicking them or by clicking Select All, then click Install Package(s) to start a job to install them on the target.
11. (Optional) Click Export to CSV to export the report result.
12. Click Done to close the report.

Creating a Profile Report (Solaris)

The Profile report provides information about the system compliance with the OS Update Profiles that are defined in Enterprise Manager Ops center. The update profiles include both the system-defined and user-defined profiles in Enterprise Manager Ops Center.

> **Note:** You can avoid running reports for system-defined profiles like Perform Reboot+Reconfigure and Perform Reboot as these profiles do not contain any patches.

Before You Begin

You can modify the patch list that is applied to generate the report by selecting a white list and a black list.

A white list is the list of patches that you want to install. To establish a white list, create a profile using the Required setting. Select the white list either from the created profile or enter the patch IDs separated by new lines.

For example, baseline B includes patches X, Y, and Z, and the white list has patches U, V, and W. When your Baseline Analysis Report is created, the host is marked compliant only when all six patches (X, Y, Z, U, V, and W) are present.

A black list is a list of patches that you do not want them to be installed. You create a black list by creating a policy with the specified action for the patches. Select the black list either from the created policy or enter the patch IDs separated by new lines.

If a particular patch in the profile is set with the policy component setting as Never for the install action, then the patch is not installed. If the patch is already installed, it is not uninstalled or removed.

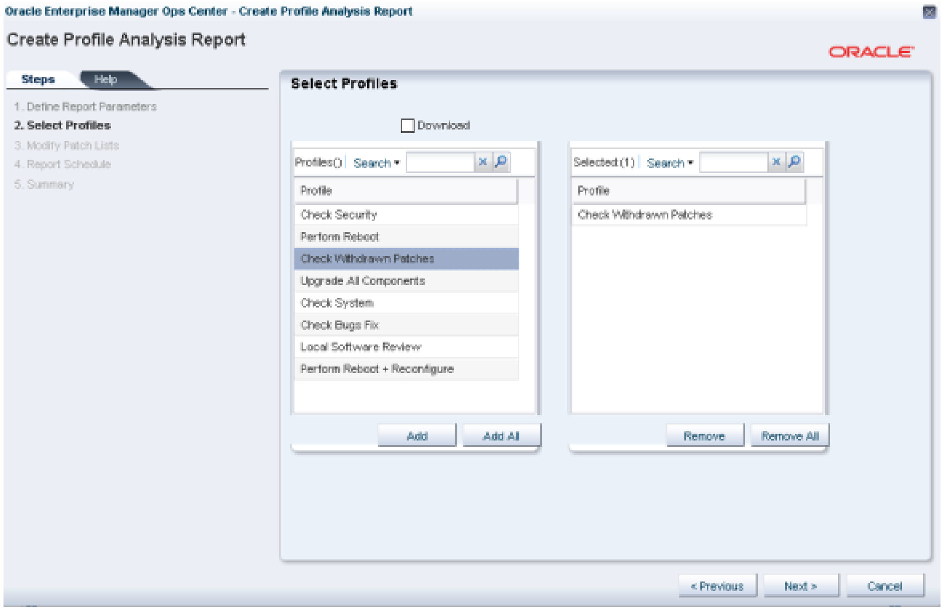
For example, if baseline A has patches X, Y, and Z, and the black list specifies only Y and Z, the system is compliant if X is installed. Even if the patches Y and Z are installed, they will not be uninstalled if you run a compliance job from the report results.

To Generate a Profile Report for Solaris OS

1. Select Reports from the Navigation pane.
2. Select Solaris/Linux OS Updates from the Reports section.
3. Select Create Profile Report from the Actions pane. The Create Profile Report wizard is displayed.
4. Define the report parameters:
   - Report Name – The name of the report.
   - Description – A description of the report.
   - Schedule – Select Create Schedule to schedule the report.
   - Output Format – Select the output format of the report result. CSV and PDF formats are available.
   - Select Targets – Add the targets by selecting them from the list of Available Items and clicking Add to Target List.
5. Click Next to select the profiles.

6. Select the profiles from the list and click Add or click Add All to select all the available profiles.

Figure 8–5 Selecting Profiles for Profile Analysis Report



7. Select the Download option to download the patches that must be installed for the system compliance.

8. Click Next to modify the patch lists that are applied to the report.

9. Select a White List option:
   - None – No white list.
   - Manual Input – Enter a list of patches.
   - Specify with Profile – Select a profile to import as a white list.

10. Select a black list option:
    - None – No black list.
    - Manual Input – Enter a list of patches.
    - Specify with Policy – Select a policy to import as a black list.

11. Click Next to schedule the report.

12. Select a schedule for the report. You can schedule the report to run:
    - Immediately.
    - On a start date and time – Select a date and time to generate the report.
    - On a recurring schedule – Select the month and day when you want to generate the report. Select the Start Time, End Time and Number of Hours between runs. This is to set the number of times the report generated between the specified start and end time. For example, if you set the start time at 6.00 a.m, end time at 12.00 a.m and the number of hours between runs as 2, then the report is run at 6.00 a.m, 8.00 a.m, 10.00 a.m and 12.00 a.m.

13. Click Next to view the summary of the report.

14. Review the report parameters and select one of the options as required:
    - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
    - Run and Close – Runs the report and closes the wizard window.

The report result will be displayed under the Report Results in the center pane. See Viewing and Exporting Report Results for more information about viewing a report result and generating a compliance job from the result.

Creating a Recommended Software Configuration Report (Solaris)

The Recommended Software Configuration (RSC) report provides information about the system compliance for installing a specific application. The Knowledge Base provides a list of application configuration requirements with which you can check your system compliance status.

For example, you can check the system compliance status of Solaris OS for installing Oracle 11g Database. The report provides information about the packages and patches that must be installed, uninstalled, or upgraded for installing the Oracle database.

For a Solaris OS, you cannot upgrade a package component from the existing lower version to the recommended higher version. Such instances will be marked as Error in the RSC report result. In such scenarios, you cannot make the target system fully compliant with the recommended software components by the report.

Before You Begin

You can generate different types of RSCs:

- Agent-based
- Database-based

In an agent-based RSC, the report is generated based on the information from the target system. The dependencies for the updates are checked and can be downloaded if required. This report takes time to generate because it checks dependencies and downloads patches that must be installed. In a database-based RSC, the report is generated based on the target system information that is available on the database of the Enterprise Controller. The dependencies are not checked and required patches are not downloaded. This type of report is generated quickly.

To Generate a Recommended Software Configuration Report

This report provides information about the system compliance for installing a specific application.

1. Select Reports from the Navigation pane.
2. Select Solaris/Linux OS Updates from the Reports section.
3. Select Create Recommended Software Configuration Report from the Actions pane. The Create Recommended Software Configuration Report wizard is displayed.
4. Define the report parameters:
    - Report Name – The name of the report.
    - Description – A description of the report.
    - Schedule – Select Create Schedule to schedule the report.

- Output Format – Select the output format of the report result. CSV and PDF formats are available.
- Select Targets – Add the targets by selecting them from the list of Available Items and clicking Add to Target List

5. Click Next to select the recommended software configurations.
6. In Select Recommended Software Configurations, select the following options:
   - Select either Run Against Database or Run Report Against Agent.
   - Select Download for Run Report Against Agent to download the patches that must be installed on the target.
   - Select the Distribution type.
   - Select the recommended software component from the list and select the required configuration. The recommended configuration describes the prerequisite list of patches and packages for the selected application. You can select targets of multiple distribution. For each distribution, select the corresponding RSCs. A warning message is displayed if you have not selected RSCs for a distribution.

   Note: If you have multiple distributions, then you must select RSCs for at least one distribution to continue further in the wizard. If you have not selected RSCs for a distribution, then the targets of that distribution will not be in the report result.

7. Click Next to schedule the report.
8. Select a schedule for the report. You can schedule the report to run:
   - Immediately.
   - On a start date and time – Select a date and time to generate the report.
   - On a recurring schedule – Select the month and day when you want to generate the report. Select the Start Time, End Time and Number of Hours between runs. This is to set the number of times the report generated between the specified start and end time. For example, if you set the start time at 6.00 a.m, end time at 12.00 a.m and the number of hours between runs as 2, then the report is run at 6.00 a.m, 8.00 a.m, 10.00 a.m and 12.00 a.m.
9. Click Next to view the summary of the report.
10. Review the report parameters and select one of the option as required:
    - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
    - Run and Close – Runs the report and closes the wizard window.

The report result will be displayed under the Report Results in the center pane. See Viewing and Exporting Report Results for more information about viewing a report result and generating a compliance job from the result.

Creating a Solaris Update Compliance Report

The Solaris Update Compliance report enables you to determine whether a specific Solaris system is compliant with a particular released Update.

To Generate a Solaris Update Compliance Report

1. Select Reports from the Navigation pane.
2. Select Additional Reports from the Reports section.
3. Select Solaris Update Compliance from the Actions pane. The Solaris Update Compliance Report wizard is displayed.
4. Specify the report parameters:
   - Name – The name of the report.
   - (Optional) Description – A description of the report.
   - Status – Select either Compliant or Not Compliant.
   - Updates – Select an update release against which the target asset is to be compared.
5. Click Next to select the target asset. The Select Targets page is displayed.
6. Add the targets by selecting them from the list on the left and clicking Add to Target List, then click Next. The Summary page is displayed.
7. (Optional) Click Save Report to save the report for future use. This returns you to the Reports tab, where you can run the report by selecting it from the Saved Reports section and clicking Re-run Report.
8. Click Run Report. The report is displayed.
9. (Optional) Click Export to CSV to export the report result.
10. Click Done to close the report.

Creating a Service Pack Compliance Report (Solaris)

The Service Pack Compliance report provides information about incidents created by the publication and release of a service pack by a vendor. This helps to determine whether the systems have the latest service packs that were released by the vendor.

To Generate a Service Pack Compliance Report for Solaris OS

1. Select Reports from the Navigation pane.
2. Select Additional Reports from the Reports section.
3. Select Service Pack Compliance from the Actions pane.

   The Service Pack Compliance Report Creation Wizard is displayed.
4. Specify the report parameters:
   - Name – The name of the report.
   - (Optional) Description – A description of the report.
   - Status – Select either Compliant or Not Compliant.
   - Services – The services to be covered in the report.
5. Click Next.

   The Select Targets page is displayed.
6. Add the targets by selecting them from the list and clicking Add to Target List, then click Next.

   The Summary page is displayed.

7. (Optional) Click Save Report to save the report for future use. This returns you to the Reports tab, where you can run the report by selecting it from the Saved Reports section and clicking Re-run Report.
8. Click Run Report.

   The report result is displayed.
9. (Optional) Click Export to CSV to export the report results.
10. Click Done to close the report.

Using the Linux OS Update Reports

Linux OS update reports enable you to check for new patches and security advisories. You can get a general report, or test a system or installed package for available fixes. For auditing, you can create a Change History report.

When you create a report, you select the criteria that are relevant to you, such as a list of hosts that have a specific patch or a list of hosts that do not have a specific patch.

You can generate the following reports for a Linux OS in Enterprise Manager Ops Center:

- Creating a Change History Report (Linux)
- Creating a Host Compliance Report (Linux)
- Creating an Incident Compliance Report (Linux)
- Creating a CVE Report (Linux)
- Creating a Package Compliance Report (Linux)
- Creating a Profile Report (Linux)
- Creating a Recommended Software Configuration Report (Linux)
- Creating a Distribution Update Report (Linux)
- Creating a Service Pack Compliance Report (Linux)

Creating a Change History Report (Linux)

The Linux OS Change History report provides a history of the install and uninstall actions taken on systems throughout Enterprise Manager Ops Center. This report also shows which user made the deployments, enabling you to track a team of operators. After your report criteria is selected, you can generate a report and save it as a template. The saved report template enables you to run the report again with the same specified parameters for the targeted systems, installation actions, and time period.

To Generate a Change History Report for Linux OS

1. Select Reports from the Navigation pane.
2. Select Solaris/Linux OS Updates from the Reports section.
3. Select Create Change History Report from the Actions pane. The Create Change History Report wizard is displayed.
4. Define the report parameters:
   - Report Name – The name of the report.
   - Description – A description of the report.

- Date Range – Enter the start date and end date for the report.
- Actions – Select the actions that you want to be reported. You can select install, uninstall, or both.
- Schedule – Select Create Schedule to schedule the report.
- Output Format – Select the output format of the report result. CSV and PDF formats are available.
- Select Targets – Add the targets by selecting them from the list of Available Items and clicking Add to Target List.

5. Click Next to schedule the report.
6. Select a schedule for the report. You can schedule the report to run:
   - Immediately.
   - On a start date and time – Select a date and time to generate the report.
   - On a recurring schedule – Select the month and day when you want to generate the report. Select the Start Time, End Time and Number of Hours between runs. This is to set the number of times the report generated between the specified start and end time. For example, if you set the start time at 6.00 a.m, end time at 12.00 a.m and the number of hours between runs as 2, then the report is run at 6.00 a.m, 8.00 a.m, 10.00 a.m, and 12.00 a.m.
7. Click Next to view the summary of the report.
8. Review the report parameters and select one of the options as required:
   - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
   - Run and Close – Runs the report and closes the wizard window.

The report result is displayed under the Report Results in the center pane. See Viewing and Exporting Report Results for more information about viewing a report result.

Creating a CVE Report (Linux)

The CVE report provides information about incidents that are related to specific CVE IDs and the systems that must have these incidents installed. Common Vulnerability and Exposure Identifiers (CVE IDs) are unique, common identifiers for publicly known security vulnerabilities. The patches and packages from a list of vendors are published as common vulnerabilities and security exposure incidents. CVEs are identified by a candidate ID (CAN ID).

To Generate a CVE Report for Linux OS

1. Select Reports from the Navigation pane.
2. Select Solaris/Linux OS Updates from the Reports section.
3. Select Create CVE Report from the Actions pane. The Create CVE Report wizard is displayed.
4. Define the report parameters:
   - Report Name – The name of the report.
   - Description – A description of the report.
   - Compliance – Select either compliant or non-compliant report.

- Schedule – Select Create Schedule to schedule the report.
- Output Format – Select the output format of the report result. CSV and PDF formats are available.
- Select Targets – Add targets by selecting them from the list of Available Items and clicking Add to Target List.

5. Click Next to select the CAN IDs.
6. Select the CAN IDs and click Add or click Add All to select all the available CAN IDs.
7. Click Next to schedule the report.
8. Select a schedule for the report. You can schedule the report to run:
   - Immediately.
   - On a start date and time – Select a date and time to generate the report.
   - On a recurring schedule – Select the month and day when you want to generate the report. Select the Start Time, End Time and Number of Hours between runs. This is to set the number of times the report generated between the specified start and end time. For example, if you set the start time at 6.00 a.m, end time at 12.00 a.m and the number of hours between runs as 2, then the report is run at 6.00 a.m, 8.00 a.m, 10.00 a.m, and 12.00 a.m.
9. Click Next to view the summary of the report.
10. Review the report parameters and select one of the options as required:
    - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
    - Run and Close – Runs the report and closes the wizard window.

The report result is displayed under the Report Results in the center pane. See Viewing and Exporting Report Results for more information about viewing a report result and generating a compliance job from the result.

Creating a Distribution Update Report (Linux)

The Distribution Update report provides a mapping between selected updates, packages, and CVEs and selected distributions so that you can find out whether the updates are installed. This report shows whether a specific distribution has been updated with specific updates, packages, or CVEs.

To Generate a Distribution Update Report for Linux OS

1. Select Reports from the Navigation pane.
2. Select Additional Reports from the Reports section.
3. Select Distribution Update Report from the Actions pane. The Distribution Update Report Creation Wizard is displayed.
4. Specify the report parameters:
   - Name – The name of the report.
   - (Optional) Description – A description of the report.
   - Category – Select one or more of the following:
     - Security

  - Bug fix
  - Enhancement
  - Service pack
  - Solaris update
  - CD
- Type – Select package, update or both.
- Release Date – Select a start date and end date between which the update was released.

5. Click Next to specify the distribution. The Specify Distributions page is displayed.
6. Select the distributions by clicking them and clicking Add or by clicking Add All, then click Next. The Select Updates page is displayed.
7. Select the updates by clicking them or clicking Select All, then click Next. The Select Packages page is displayed.
8. Select the packages by clicking them or clicking Select All, then click Next. The Select CVE page is displayed.
9. Select the CVEs by clicking them or clicking Select All, then click Next. The Summary page is displayed.
10. (Optional) Click Save Report to save the report for future use. This returns you to the Reports tab, where you can run the report by selecting it from the Saved Reports section and clicking Re-run Report.
11. Click Run Report. The report result is displayed.
12. (Optional) Click Export to CSV to export the report result.
13. Click Done to close the report.

Creating a Host Compliance Report (Linux)

You can run a host compliance report to check whether the systems are complaint with security and bug fix incidents.

To Generate a Host Compliance Report for Linux OS

1. Select Reports from the Navigation pane.
2. Select Solaris/Linux OS Updates from the Reports section.
3. Select Create Host Compliance Report from the Actions pane. The Create Host Compliance Report wizard is displayed.
4. Define the report parameters:
   - Report Name – The name of the report.
   - Description – A description of the report.
   - Update Level – Select whether you want the compliant status for Security and Bug Fixes or for only Security Updates.
   - Compliance – Select either Compliant or Non-Compliant.
   - Schedule – Select Create Schedule to schedule the report.
   - Output Format – Select the output format of the report result. CSV and PDF formats are available.

- Select Targets – Add the targets by selecting them from the list of Available Items and clicking Add to Target List.

5. Click Next to schedule the report.
6. Select a schedule for the report. You can schedule the report to run:
   - Immediately.
   - On a start date and time – Select a date and time to generate the report.
   - On a recurring schedule – Select the month and day when you want to generate the report. Select the Start Time, End Time and Number of Hours between runs. This is to set the number of times the report generated between the specified start and end time. For example, if you set the start time at 6.00 a.m, end time at 12.00 a.m and the number of hours between runs as 2, then the report is run at 6.00 a.m, 8.00 a.m, 10.00 a.m, and 12.00 a.m.
7. Click Next to view the summary of the report.
8. Review the report parameters and select one of the options as required:
   - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
   - Run and Close – Runs the report and closes the wizard window.

The report result is displayed under the Report Results in the center pane. See Viewing and Exporting Report Results for more information about viewing a report result and generating a compliance job from the result.

Creating an Incident Compliance Report (Linux)

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

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

To Create an Incident Compliance Report for Linux OS

1. Select Reports from the Navigation pane.
2. Select Solaris/Linux OS Updates from the Reports section.
3. Select Create Incident Report from the Actions pane. The Create Incident Compliance Report wizard is displayed.
4. Define the report parameters:
   - Report Name – The name of the report.
   - Description – A description of the report.
   - Criteria – Select the criteria for selecting the patches that will be used as a comparison. Depending on the selection of criteria the wizard steps vary. You can select Select Updates or Filter Updates.
   - Compliant – Select either Compliant or Non-compliant for compliance status.
   - Schedule – Select Create Schedule to schedule the report.
   - Output Format – Select the output format of the report result. CSV and PDF formats are available.

- Select Targets – Add the targets by selecting them from the list of Available Items and clicking Add to Target List.

5. Click Next to select the updates.
6. If you have selected Select Updates in the previous step, the list of available incidents is displayed. Select the incidents and click Add or click Add All to select all the listed incidents.
7. If you have selected Filter Updates in the first step, then select the following:
   - Select Packages – You can select the packages based on the Category, Update Type and Releases date. Select the packages and click Add or click Add All to select all the packages in the Available Packages. Click Next to select the CAN IDs.
   - Select CAN IDs – Select from the list of Available CAN IDs. Click Add or Add All as required.
8. Click Next to schedule the report.
9. Select a schedule for the report. You can schedule the report to run:
   - Immediately.
   - On a start date and time – Select a date and time to generate the report.
   - On a recurring schedule – Select the month and day when you want to generate the report. Select the Start Time, End Time and Number of Hours between runs. This is to set the number of times the report generated between the specified start and end time. For example, if you set the start time at 6.00 a.m, end time at 12.00 a.m and the number of hours between runs as 2, then the report is run at 6.00 a.m, 8.00 a.m, 10.00 a.m, and 12.00 a.m.
10. Click Next to view the summary of the report.
11. Review the report parameters and select one of the options as required:
    - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
    - Run and Close – Runs the report and closes the wizard window.

The report result is displayed under the Report Results in the center pane. See Viewing and Exporting Report Results for more information about viewing a report result and generating a compliance job from the result.

Creating a Package Compliance Report (Linux)

The Package Compliance report provides information about the selected packages on the managed system and shows whether the system is compliant with the latest recommended version available.

To Generate a Package Compliance Report for Linux OS

1. Select Reports from the Navigation pane.
2. Select Additional Reports from the Reports section.
3. Select Package Compliance Report from the Actions pane. The Package Compliance Report Creation Wizard is displayed.
4. Specify the report parameters:
   - Name – The name of the report.

- Description – A description of the report.
- Status – The compliance status that the report will cover. Select either Compliant or Not Compliant.
- Level – Select Security Updates or Security and Bug Updates.

5. Click Next to select the targets for which you want to run the report. The Select Targets page is displayed.
6. Add the targets by selecting them from the list on the left and clicking Add to Target List, then click Next. The Select Packages page is displayed.
7. Select the packages by clicking them or click Select All, then click Next. The Summary page is displayed.
8. (Optional) Click Save Report to save the report for future use. This returns you to the Reports tab, where you can run the report by selecting it from the Saved Reports section and clicking Re-run Report.
9. Click Run Report. The report is displayed.
10. (Optional) Select the packages by clicking them or by clicking Select All, then click Install Package(s) to start a job to install them on the target.
11. (Optional) Click Export to CSV to export the report result.
12. Click Done to close the report.

Creating a Profile Report (Linux)

The Profile report provides information about the system compliance with the OS Update Profiles that are defined in Enterprise Manager Ops center. The Update Profiles include both the system-defined and user-defined profiles in Enterprise Manager Ops Center.

Note: You can avoid running reports for system-defined profiles like Perform Reboot+Reconfigure and Perform Reboot as these profiles do not contain any RPMs.

Before You Begin

You can modify the RPM list that are applied to generate the report by selecting a white list and a black list.

A white list is the list of RPMs that you want to install. To create a white list, create a profile using the Required setting. Select the white list either from the created profile or enter the RPMs separated by new lines.

A black list is a list of RPMs that you do not want them to be installed. You create a black list by creating a policy with the specified action for the RPMs. Select the black list either from the created policy or enter the RPMs separated by new lines.

If a particular RPM in the profile is set with the policy component setting as Never for the install action, then the RPM will not be installed. If the RPM is already installed, it will not be uninstalled or removed.

To Generate a Profile Report for Linux OS

1. Select Reports from the Navigation pane.
2. Select Solaris/Linux OS Updates from the Reports section.

3. Select Create Profile Report from the Actions pane. The Create Profile Report wizard is displayed.
4. Define the report parameters:
   - Report Name – The name of the report.
   - Description – A description of the report.
   - Schedule – Select Create Schedule to schedule the report.
   - Output Format – Select the output format of the report result. CSV and PDF formats are available.
   - Select Targets – Add the targets by selecting them from the list of Available Items and clicking Add to Target List.
5. Click Next to select the profiles.
6. Select the profiles from the list and click Add or click Add All to select all the available profiles.
7. Select the Download option to download the RPMs that must be installed for the system compliance.
8. Click Next to modify the RPM lists that are applied to the report.
9. Select a White List option:
   - None – No white list.
   - Manual Input – Enter the list of RPMs.
   - Specify with Profile – Select a profile to import as a white list.
10. Select a black list option:
    - None – No black list.
    - Manual Input – Enter the list of RPMs.
    - Specify with Policy – Select a policy to import as a black list.
11. Click Next to schedule the report.
12. Select a schedule for the report. You can schedule the report to run:
    - Immediately.
    - On a start date and time – Select a date and time to generate the report.
    - On a recurring schedule – Select the month and day when you want to generate the report. Select the Start Time, End Time and Number of Hours between runs. This is to set the number of times the report generated between the specified start and end time. For example, if you set the start time at 6.00 a.m, end time at 12.00 a.m and the number of hours between runs as 2, then the report is run at 6.00 a.m, 8.00 a.m, 10.00 a.m, and 12.00 a.m.
13. Click Next to view the summary of the report.
14. Review the report parameters and select one of the options as required:
    - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
    - Run and Close – Runs the report and closes the wizard window.

The report result is displayed under the Report Results in the center pane. See Viewing and Exporting Report Results for more information about viewing a report result and generating a compliance job from the result.

Creating a Recommended Software Configuration Report (Linux)

The Recommended Software Configuration (RSC) report provides information about the system compliance for installing a specific application. The Knowledge Base provides a list of application configuration requirements for which you can check your system compliance status.

For example, you can check the system compliance status of Oracle Linux OS for installing Oracle 11g Database. The report provides information about the RPMs that must be installed, uninstalled or upgraded for installing Oracle Database.

Before You Begin

You can generate different types of RSCs:

- Agent-based
- Database-based

In an agent-based RSC, the report is generated based on the information from the actual target system. The dependencies for the updates are verified and can be downloaded if required. This report takes time to generate because it checks for dependencies and downloads RPMs that must be installed. In a database-based RSC, the report is generated based on the target system information that is available on the database of the Enterprise Controller. The dependencies are not verified and required RPMs are not downloaded. This type of report is generated quickly.

To Generate a Recommended Software Configuration Report

This report provides information about the system compliance for installing a specific application.

1. Select Reports from the Navigation pane.
2. Select Solaris/Linux OS Updates from the Reports section.
3. Select Create Recommended Software Configuration Report from the Actions pane. The Create Recommended Software Configuration Report wizard is displayed.
4. Define the report parameters:
   - Report Name – The name of the report
   - Description – A description of the report
   - Schedule – Select Create Schedule to schedule the report
   - Output Format – Select the output format of the report result. CSV and PDF formats are available.
   - Select Targets – Add the targets by selecting them from the list of Available Items and clicking Add to Target List
5. Click Next to select the recommended software configurations.
6. In the Select Recommended Software Configuration(s) step, select the following options:
   - Either Run Against Database or Run Report Against Agent.

- Download for Run Report Against Agent to download the RPMs that must be installed on the target.
- The Distribution type.
- The recommended software component from the list and select the required configuration. The recommended configuration describes the prerequisite list of RPMs for the selected application. You can select targets of multiple distribution. For each distribution, select the corresponding RSCs. A warning message is displayed if you have not selected RSCs for a distribution.

  Note: If you have multiple distributions, then you must select RSCs for at least one distribution to continue further in the wizard. If you have not selected RSCs for a distribution, then the targets of that distribution will not be in the report result.

7. Click Next to schedule the report.
8. Select a schedule for the report. You can schedule the report to run:
   - Immediately.
   - On a start date and time – Select a date and time to generate the report.
   - On a recurring schedule – Select the month and day when you want to generate the report. Select the Start Time, End Time and Number of Hours between runs. This is to set the number of times the report generated between the specified start and end time. For example, if you set the start time at 6.00 a.m, end time at 12.00 a.m and the number of hours between runs as 2, then the report is run at 6.00 a.m, 8.00 a.m, 10.00 a.m, and 12.00 a.m.
9. Click Next to view the summary of the report.
10. Review the report parameters and select one of the options as required:
    - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
    - Run and Close – Runs the report and closes the wizard window.

The report result is displayed under the Report Results in the center pane. See Viewing and Exporting Report Results for more information about viewing a report result and generating a compliance job from the result.

Creating a Service Pack Compliance Report (Linux)

This report provides information on incidents created by the publication and release of a service pack by a vendor. This helps to determine whether the systems have the latest service packs that were released by the vendor.

To Generate a Service Pack Compliance Report for Linux OS

1. Select Reports from the Navigation pane.
2. Select Additional Reports from the Reports section.
3. Select Service Pack Compliance from the Actions pane.

   The Service Pack Compliance Report Creation Wizard is displayed.
4. Specify the report parameters. They include:
   - Name – A name for the report.

- (Optional) Description – A description of the report.
- Status – The compliance status that the report will cover. Select either Compliant or Not Compliant.
- Services – The services to be covered in the report.

5. Click Next.

   The Select Targets page is displayed.
6. Add one or more targets by selecting them in the list and clicking Add to Target List, then click Next.

   The Summary page is displayed.
7. (Optional) Click Save Report to save the report for future use. This returns you to the Reports tab, where you can run the report by selecting it from the Saved Reports section and clicking Re-run Report.
8. Click Run Report.

   The report result is displayed.
9. (Optional) Click Export to CSV to export the report results.
10. Click Done to close the report.

Windows OS Update Reports

Compliance reports provide information about Windows systems that are compliant with the Windows updates incidents. You can get a report on the number of applicable Windows updates for each system. You can also get a report that shows the number of systems to which the selected Windows updates apply.

When you create a report, you select the criteria that are relevant to you, such as Category, Severity, Superseded, and Release Date of the update patches. You can also select specific updates on which to run the compliance reports.

You can create a Windows update job from the results of the compliance reports. See Creating an Update Job for Windows OS for information about how to create an update job from the report results.

The following reports are available:

- Creating a Windows Host Compliance Report – Provides information about the applicable Windows updates.
- Creating a Windows Incident Compliance Report – Provides information about the number of systems to which the selected Windows updates apply.

Creating a Windows Host Compliance Report

The Host Compliance Report provides information about whether your systems are compliant with the Windows updates incidents. This report shows the number of Windows updates that are applicable to each system, and whether the updates are already installed or must be installed to make the system compliant. You can also create a Windows update job based on the results of a Host Compliance Report.

To Create a Host Compliance Report for Windows Updates

1. Select Reports from the Navigation pane.

2. Select Windows Host Compliance Report from the Actions pane. The Windows Host Compliance Report wizard is displayed.
3. Specify the report parameters. They include:
   - Report Name – A name for the report.
   - (Optional) Description – A description of the report.
   - Specify the Windows OS updates on which to run the report. You can specify filter criteria such as Category, Severity, Superseded, and Release Date for Windows OS updates, or you can select specific Windows OS updates to run the report.
4. Click Next. Based on your selection in Step 4, either the Define Updates Filter window is displayed or the Select Updates window is displayed. If the Define Updates Filter window is displayed, go to Step 6. If the Select Updates window is displayed, proceed to Step 7.
5. Make your selections in the Define Updates Filter screen. They include:
   - Category – Includes Application, Critical Updates, Definition Updates, Drivers, Service Packs, Security Updates, Tools, Update Rollups, and WSUS Infrastructure Updates. You can select either All available updates under all category or Selected categories only. Use the Control key on the keyboard to select multiple items in the list under Selected category only.
   - Severity – Includes Critical, Important, Moderate, Low, and Default. You can select either All updates with any severity or Selected severities only. Use the Ctrl key on the keyboard to select multiple items in the list under Severity.
   - Superseded – Enables you to select all or just the most recent updates.
   - Release Date – Refers to the date that the update patches were released. You can select the range of release dates that you want to include in your report by filling in the From and To fields. Click Next. Go to Step 8.
6. Make your selections in the Select Updates window. Under Search, Select All enables you to include a bulletin ID, article ID, and title in your search, or you can select specific fields to narrow your search. Use the Control key on the keyboard to make multiple selections in the list under Available Windows Software Updates. Click Add to Updates List, then. Click Next.
7. Add the targets by selecting them from the list of Available Items. Click Add to Target List, then click Next. The Summary page is displayed.
8. (Optional) Click Save as Template to save the parameters of the report as a template for future use. After you click Save as Template, you will not have the option of returning to the previous steps. The Save as Template button and the Previous button will be grayed, and the only two options that you will have is to either click Finish or Cancel. After a template is saved, you can view, delete, edit, or run the report from Report Templates.
9. Click Finish to run the report. The results of the report are displayed under Report Results list.

Creating a Windows Incident Compliance Report

The Incident Compliance Report provides information about whether your systems are compliant with the Windows updates incidents. This report shows the number of systems to which the selected Windows updates apply, how many systems have the updates installed, and how many systems require the updates to be installed to make the systems compliant. You can create a Windows update job based on the results of an Incident Compliance Report.

To Create an Incident Compliance Report for Windows Updates

1. Select Reports from the Navigation pane.
2. Select Windows Incident Compliance Report from the Actions pane. The Windows Incident Compliance Report wizard is displayed.
3. Specify the report parameters. They include:
   - Report Name – The name of the report.
   - (Optional) Description – A description of the report.
   - Specify the Windows OS updates on which to run the report – You can specify filter criteria such as Category, Severity, Superseded, and Release Date for Windows OS updates, or you can select specific Windows OS updates to run the report.
4. Click Next. Based on your selection in Step 4, either the Define Updates Filter window is displayed or the Select Updates window is displayed. If the Define Updates Filter window is displayed, go to Step 6. If the Select Updates window is displayed, go to Step 7.
5. Make your selections in the Define Updates Filter screen. They include:
   - Category – Includes Application, Critical Updates, Definition Updates, Drivers, Service Packs, Security Updates, Tools, Update Rollups, and WSUS Infrastructure Updates. You can select either All available updates under all category or Selected categories only. Use the Control key on the keyboard to select multiple items in the list under Selected category only.
   - Severity – Includes Critical, Important, Moderate, Low, and Default. You can select either All updates with any severity or Selected severities only. Use the Ctrl key on the keyboard to select multiple items in the list under Severity.
   - Superseded – Enables you to select all or just the most recent updates.
   - Release Date – Refers to the date that the update patches were released. You can select the range of release dates that you want to include in your report by filling in the From and To fields. Click Next. Go to Step 8.
6. Make your selections in the Select Updates window. Under Search, Select All enables you to include a bulletin ID, article ID, and title in your search, or you can select specific fields to narrow your search. Use the Control key on the keyboard to make multiple selections in the list under Available Windows Software Updates. Click Add to Updates List, then. Click Next.
7. Add the targets by selecting them in the list of Available Items. Click Add to Target List, then click Next. The Summary page is displayed.
8. (Optional) Click Save as Template to save the parameters of the report as a template for future use. After you click Save as Template, you will not have the option of returning to the previous steps. The Save as Template button and the Previous button will be grayed, and the only two options that you will have is to either click Finish or Cancel. After a template is saved, you can view, delete, edit, or run the report from Report Templates.
9. Click Finish to run the report. The results of the report are displayed under the Report Results list.

Creating a System Information Report

You can run a system information report to obtain the information about different resource types such as OS, server, chassis, logical domains, global zone, non-global zone, and M-Series server.

To Generate a System Information Report

1. Select Reports from the Navigation pane.
2. Select System Information Reports from the Reports section.
3. Select Create System Information Report from the Actions pane. The Create System Information Report wizard is displayed.
4. Define the report parameters. They include:
   - Report Name – A name for the report.
   - Description – A description of the report.
   - Resource Type – Select a resource type from the list. You can select the following types:
     - Operating system
     - Non-global zone
     - Server
     - Chassis
     - M-Series server
     - Global zone
     - Logical domain
   - Schedule – Select Create Schedule to schedule the report.
   - Output Format – Select the output format of the report result. The CSV and PDF formats are available.
   - Select Targets – Add one or more targets by selecting them in the list of Available Items and clicking Add to Target List.
5. Click Next to select the attributes. Depending on the type of resource selected in the previous step, the resource attributes are listed.
6. Select one or more attributes from the list and click Add or click Add All to choose all the attributes listed.
7. Click Next to set filters for the attributes.
8. Select the attribute for which you want to set the filter and specify the condition for the attribute. The attribute filter is taken care when generating the report.
9. Click the Add icon to set filters for other attributes.
10. Click Next to schedule the report.
11. Select a schedule for the report. You can schedule the report to run:
    - Immediately.
    - On a start date and time – Select a date and time to generate the report.
    - On a recurring schedule – Select the month and day when you want to generate the report. Select the Start Time, End Time and Number of Hours

between runs. This is to set the number of times the report generated between the specified start and end time. For example, if you set the Start Time at 6.00 AM, End Time at 12.00 AM and the Number of hours between runs as 2, then the report is run at 6.00 AM, 8.00 AM, 10.00 AM and 12.00 AM.

12. Click Next to view the summary of the report.
13. Review the report parameters and select one of the option as required:
    - Save Template and Close – Saves the report as a template and closes the wizard. You can use the report template to generate the report later.
    - Run and Close – Runs the report and closes the wizard window.

The report result will be displayed under the Report Results in the center pane. Refer to Viewing and Exporting Report Results for more information about viewing a report result and generating a compliance job from the result.

Viewing and Exporting Report Results

Enterprise Manager Ops Center provides an interactive result viewer to view the results. The generated report results are displayed under the Report Results in the All Reports page. All the reports results are displayed. Select the report for which you want to view the result.

You can view and save the report results in CSV or PDF formats.

Viewing the Report Result

1. Select Reports in the Navigation pane. The All Reports page in the center pane displays all the report templates and report results.
2. Select a report result under the Report Result section in the center pane.
3. Click the Interactive icon to view the report result. The Interactive Result viewer opens the report result and displays the following information:
    - Report details – The name, type, run time and the status of the report are displayed.
    - Report Result – The targets on which the report was run and the corresponding OS updates applicable are displayed.
    - Report Parameters – The parameters that were used to generate the report are displayed.

Saving the Report Result

1. Select Reports in the Navigation pane. The All Reports page in the center pane displays all the report templates and report results.
2. Select a report result under the Report Result section in the center pane.
3. Click the View CSV or View PDF icon. You can save or open the report in CSV or PDF formats.

Adding a Summary Row to a Black List

1. Select Reports in the Navigation pane. The All Reports page in the center pane displays all the report templates and report results.
2. Select a report result under the Report Result section in the center pane.

3. Click the Interactive icon to view the report result.
4. Select a target from the list of targets on which the report was run.
5. Click the Add Summary Row to Black List icon. The target and the applicable updates for the corresponding target are strike out from the list. Also, this list will be excluded from the OS update job that is initiated from the result using the Make Targets Compliant option.

Adding a Detail Row to a Black List

1. Select Reports in the Navigation pane. The All Reports page in the center pane displays all the report templates and report results.
2. Select a report result under the Report Result section in the center pane.
3. Click the Interactive icon to view the report result.
4. Select a target from the list of targets on which the report was run. The corresponding applicable OS updates are listed.
5. Select the updates that you want to exclude from the list. Use the Shift and Ctrl keys to select multiple updates.
6. Click the Add Detail Row to Black List icon. The selected targets are strike out from the list and will be excluded from the OS update job that is initiated from the result using the Make Targets Compliant option.

Removing a Summary or Details Row From a Black List

1. Select Reports in the Navigation pane. The All Reports page in the center pane displays all the report templates and report results.
2. Select a report result under the Report Result section in the center pane.
3. Click the Interactive icon to view the report result.
4. Select the black listed target or the updates.
5. Click the Remove Summary Row From Black List or Remove Detail Row From Black List icon. The strike outs on the target or updates are removed.

Managing Report Templates

Enterprise Manager Ops Center enables you to manage the saved templates of the reports:

- You can edit a report template.
- You can run a report from a template.
- You can delete a report template

This sections describes how to edit, run and delete a report from a report template.

Editing a Report Template

1. Select Reports from the Navigation pane.
2. Select a saved report template from the center pane.
3. Click the Edit View icon to edit the selected report template. The corresponding report wizard is displayed.

4. Edit the report parameters as required in the wizard.
5. Either click Run and Close to run the report or click Save Template and Close to save the report template. When you click Run and Close, the report is generated but the edits for the report are not saved.

Generating a Report from Report Template

1. Select Reports from the Navigation pane.
2. Select a saved report template from the center pane.
3. Click the Generate Report icon to run the report. The corresponding report is generated and the results will be displayed under Report Results.

Deleting a Report Template

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

A

Learn More

This section provides sample reports that can be created using Enterprise Manager Ops Center.

Example - Baseline Analysis Report

A Solaris baseline is a dated collection of Solaris patches, patch metadata, and tools. Oracle releases Solaris baselines on a monthly basis. When you install the patches of a baseline on a managed system, it is considered to be compliant with that baseline.

Each dated baseline contains these patch sets:

- Full – Includes all Solaris patches
- Recommended – Includes Solaris recommended patches and security patches
- Security – Includes only Solaris security patches

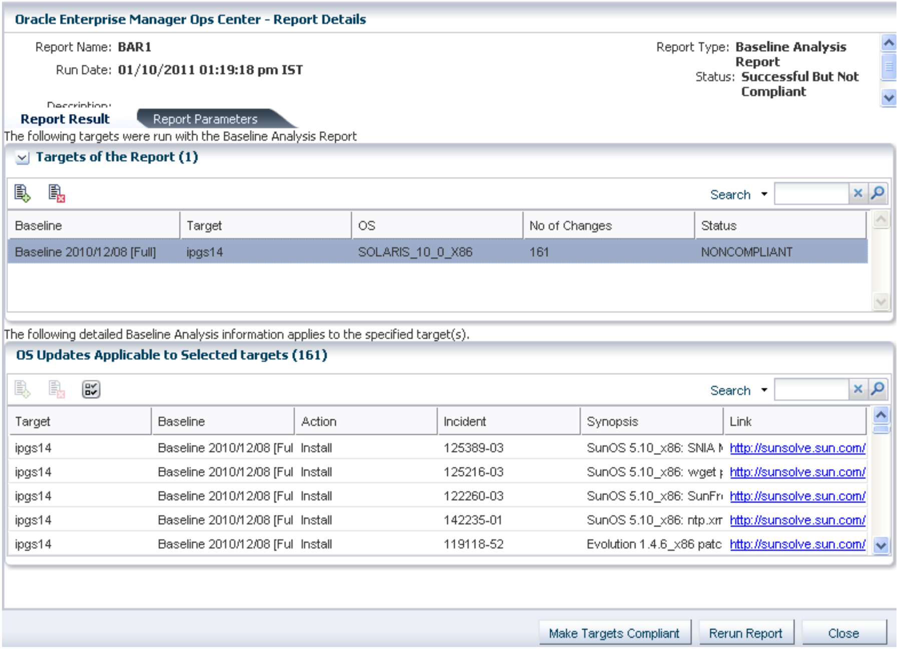
The Baseline Analysis Report (BAR) enables you to determine whether your managed system is compliant with recently released Oracle Solaris baselines.

In this example, a BAR is generated for a Solaris 10 x86 OS and the compliance is checked with the latest released recommended baselines. Ensure that the Oracle Solaris 10 OS is managed using Enterprise Manager Ops Center and the Enterprise Controller is in connected mode. If the Enterprise Controller is in disconnected mode, you must download the baselines using the harvester script.

See Creating a Baseline Analysis Report for information about how to generate a baseline analysis report. In the report wizard, select to run the agent based report to view the actual status of the OS compliance for the selected baseline.

A sample report result is displayed as shown in the figure.

Figure A–1 Sample Baseline Analysis Report



Oracle Enterprise Manager Ops Center - Report Details

Report Name: **BAR1**
Run Date: **01/10/2011 01:19:18 pm IST**
Description:

Report Type: **Baseline Analysis Report**
Status: **Successful But Not Compliant**

The following targets were run with the Baseline Analysis Report

Targets of the Report (1)

Baseline	Target	OS	No of Changes	Status
Baseline 2010/12/08 [Full]	ipgs14	SOLARIS_10_0_X86	161	NONCOMPLIANT

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

OS Updates Applicable to Selected targets (161)

Target	Baseline	Action	Incident	Synopsis	Link
ipgs14	Baseline 2010/12/08 [Ful	Install	125389-03	SunOS 5.10_x86: SNIA	http://sunsolve.sun.com/
ipgs14	Baseline 2010/12/08 [Ful	Install	125216-03	SunOS 5.10_x86: wget	http://sunsolve.sun.com/
ipgs14	Baseline 2010/12/08 [Ful	Install	122260-03	SunOS 5.10_x86: SunFr	http://sunsolve.sun.com/
ipgs14	Baseline 2010/12/08 [Ful	Install	142235-01	SunOS 5.10_x86: ntp.xm	http://sunsolve.sun.com/
ipgs14	Baseline 2010/12/08 [Ful	Install	119118-52	Evolution 1.4.6_x86 patc	http://sunsolve.sun.com/

Report Result

In the report result, the status of the report is displayed as Success But Not Compliant. This means that the report generation was success but the Solaris OS is not updated with the patches for the selected baselines. The report lists the patches that must be applied or removed from the OS to make it compliant with the selected baseline.

The report provides the number of changes that must be made on the OS for making it compliant with the selected baseline. The report lists out the patch number, patch information, and the download point from My Oracle Support.

To make the OS compliant, click the Make Targets Compliant button to launch the job wizard to download and install the patches.

If you do not want to install some patches from the list, you can always select those and black list using the Add detail row to black list option.

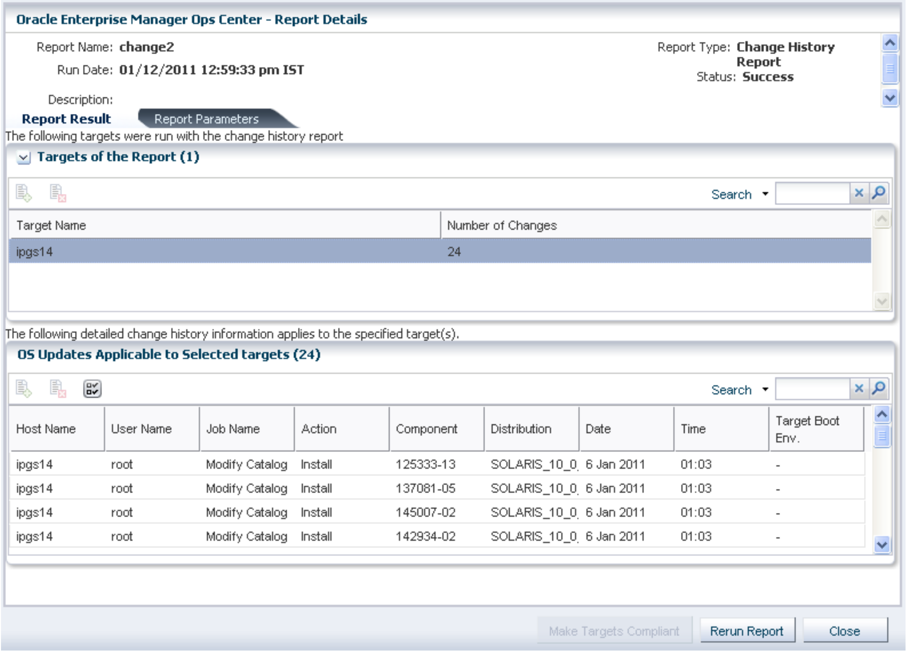
Example - Change History Report

The change history report provides the installs and uninstalls done using Enterprise Manager Ops Center on the managed systems. This report shows which user made the deployments, enabling you to track a team of operators.

Refer to Creating a Change History Report (Solaris) for a detailed procedure to generate a report.

When you generate the report, you can also specify the time frame in which you want to know the changes that have been made to a system. A sample report result of change history report is displayed as follows.

Figure A–2 Change History Report Result



Oracle Enterprise Manager Ops Center - Report Details

Report Name: **change2**

Run Date: **01/12/2011 12:59:33 pm IST**

Report Type: **Change History Report**

Status: **Success**

Description:

The following targets were run with the change history report

Targets of the Report (1)

Target Name	Number of Changes
ipgs14	24

The following detailed change history information applies to the specified target(s).

OS Updates Applicable to Selected targets (24)

Host Name	User Name	Job Name	Action	Component	Distribution	Date	Time	Target Boot Env.
ipgs14	root	Modify Catalog	Install	125333-13	SOLARIS_10_0	6 Jan 2011	01:03	-
ipgs14	root	Modify Catalog	Install	137081-05	SOLARIS_10_0	6 Jan 2011	01:03	-
ipgs14	root	Modify Catalog	Install	145007-02	SOLARIS_10_0	6 Jan 2011	01:03	-
ipgs14	root	Modify Catalog	Install	142934-02	SOLARIS_10_0	6 Jan 2011	01:03	-

In the sample report, a modify catalog job was executed on the OS which resulted in installing some patches on the target OS. This could be derived from the report result which lists what action was taken on the target, the job that called for the action, and the component on which the action was performed. It also provides the user who initiated the job, and the date and time of the action.

The change history report can be used for auditing purposes as it provides the detailed information about the job executed on the systems by different operators, if any.

Example - CVE Report

Generate CVE reports to find the incidents related to specific CVE IDs and the managed systems that should have these incidents installed. You can choose to get a report that lists hosts that are compliant; or a report of those that must be fixed for the selected CVE IDs.

Select a target OS to create a CVE report. Refer to Creating a CVE Report (Solaris) for a detailed procedure to generate a CVE report.

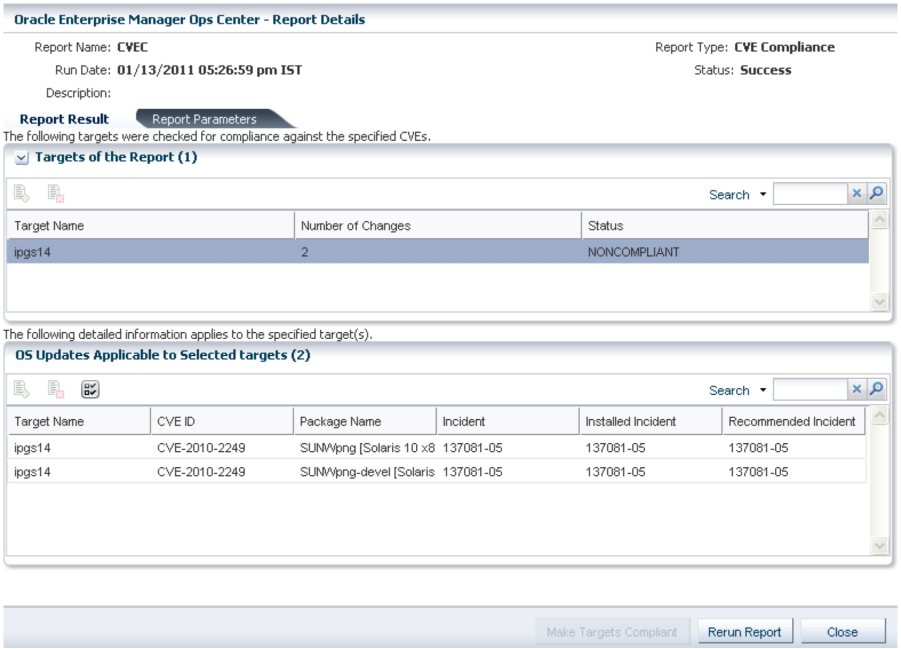
In this example a CVE report is generated for a Solaris 10 5/09 OS for the following CVE IDs:

- CVE-2010-1624
- CVE-2010-1797
- CVE-2010-2065
- CVE-2010-2227
- CVE-2010-2249
- CVE-2010-2443
- CVE-2010-2528
- CVE-2010-3069

- CVE-2010-3170
- CVE-2010-3654

For a compliant CVE report, the report result shows the incident-packages that are installed on the OS to be compliant with the selected CVE IDs. The report result of compliant CVE report is displayed as follows:

Figure A–3 Compliant CVE Report Result



Oracle Enterprise Manager Ops Center - Report Details

Report Name: **CVEC**
Run Date: **01/13/2011 05:26:59 pm IST**
Description:

Report Type: **CVE Compliance**
Status: **Success**

The following targets were checked for compliance against the specified CVEs.

Targets of the Report (1)

Target Name	Number of Changes	Status
ipgs14	2	NONCOMPLIANT

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

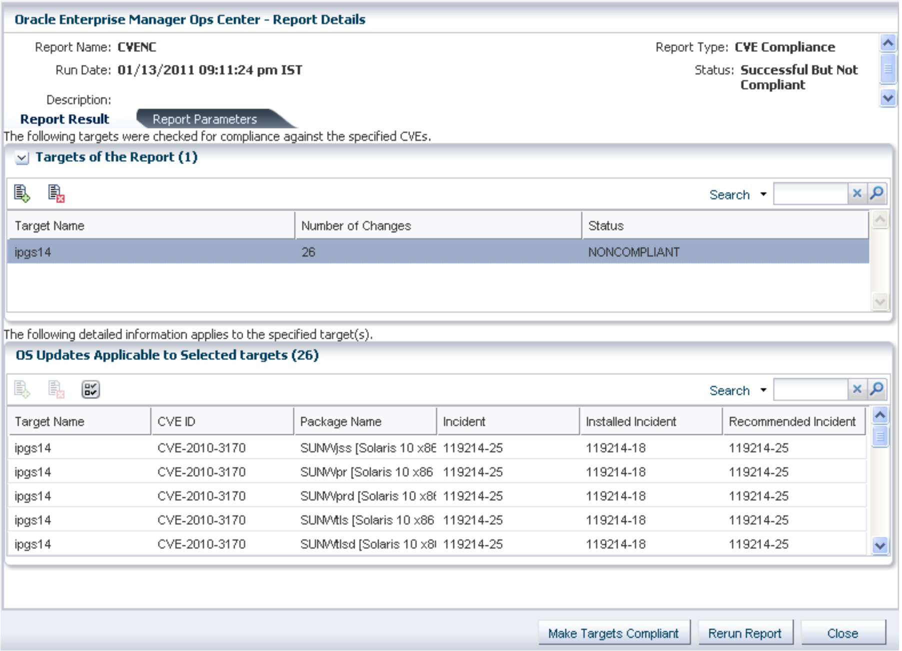
OS Updates Applicable to Selected targets (2)

Target Name	CVE ID	Package Name	Incident	Installed Incident	Recommended Incident
ipgs14	CVE-2010-2249	SUNWpng [Solaris 10 x8	137081-05	137081-05	137081-05
ipgs14	CVE-2010-2249	SUNWpng-devel [Solaris	137081-05	137081-05	137081-05

The report result shows the CVE IDs you selected and the number of incident-packages with the compliance status. The report shows how many incidents have been installed on the hosts to be compliant with the selected CVE IDs. In this example, the incident 137081-05 is installed to be compliant with the CVE ID CVE-2010-2249.

For a not compliant report, the report result shows the incident-packages that must be installed on the target for the selected CVE IDs. The report result of not compliant CVE report is displayed as follows:

Figure A–4 Not Compliant CVE Report Result



Oracle Enterprise Manager Ops Center - Report Details

Report Name: CVENC

Run Date: 01/13/2011 09:11:24 pm IST

Description:

Report Type: CVE Compliance

Status: Successful But Not Compliant

The following targets were checked for compliance against the specified CVEs.

Targets of the Report (1)

Target Name	Number of Changes	Status
ipgs14	26	NONCOMPLIANT

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

OS Updates Applicable to Selected targets (26)

Target Name	CVE ID	Package Name	Incident	Installed Incident	Recommended Incident
ipgs14	CVE-2010-3170	SUNWjss [Solaris 10 x86	119214-25	119214-18	119214-25
ipgs14	CVE-2010-3170	SUNWpr [Solaris 10 x86	119214-25	119214-18	119214-25
ipgs14	CVE-2010-3170	SUNWprd [Solaris 10 x86	119214-25	119214-18	119214-25
ipgs14	CVE-2010-3170	SUNWtls [Solaris 10 x86	119214-25	119214-18	119214-25
ipgs14	CVE-2010-3170	SUNWtlsd [Solaris 10 x8	119214-25	119214-18	119214-25

The report result shows the incident-packages that must be installed on the target OS to make it compliant for the selected CVE IDs. The sample report lists the CVE IDs and its recommended incidents that must be installed for making the OS compliant.

Use the option Make Targets Compliant to initiate the compliance job to install the recommended incidents.

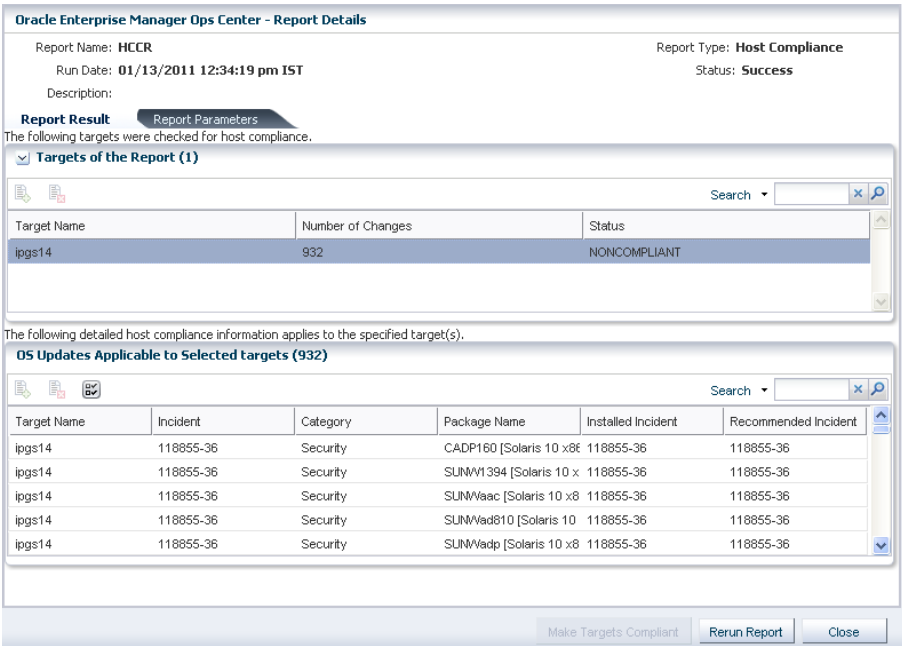
Example - Host Compliance Report

Host Compliance reports helps to discover systems that should be updated for security fixes. You can choose to get a report that lists hosts that are compliant; or a report of those that must be fixed. The security issues could be of those incidents that are security; or it could include both security and bug fixes.

Select an target OS to generate a host compliance report. Refer to Creating a Host Compliance Report (Solaris) for a detailed procedure for generating a host compliance report.

In this example, a host compliance report is generated to list both security and bug fixes. For a compliant report, the report results shows how many incidents have been installed on the target OS. A sample compliant report result is displayed as follows:

Figure A–5 Compliant Host Compliance Report Result



Oracle Enterprise Manager Ops Center - Report Details

Report Name: **HCCR**
Run Date: **01/13/2011 12:34:19 pm IST**
Description:

Report Type: **Host Compliance**
Status: **Success**

The following targets were checked for host compliance.

Targets of the Report (1)

Target Name	Number of Changes	Status
ipgs14	932	NONCOMPLIANT

The following detailed host compliance information applies to the specified target(s).

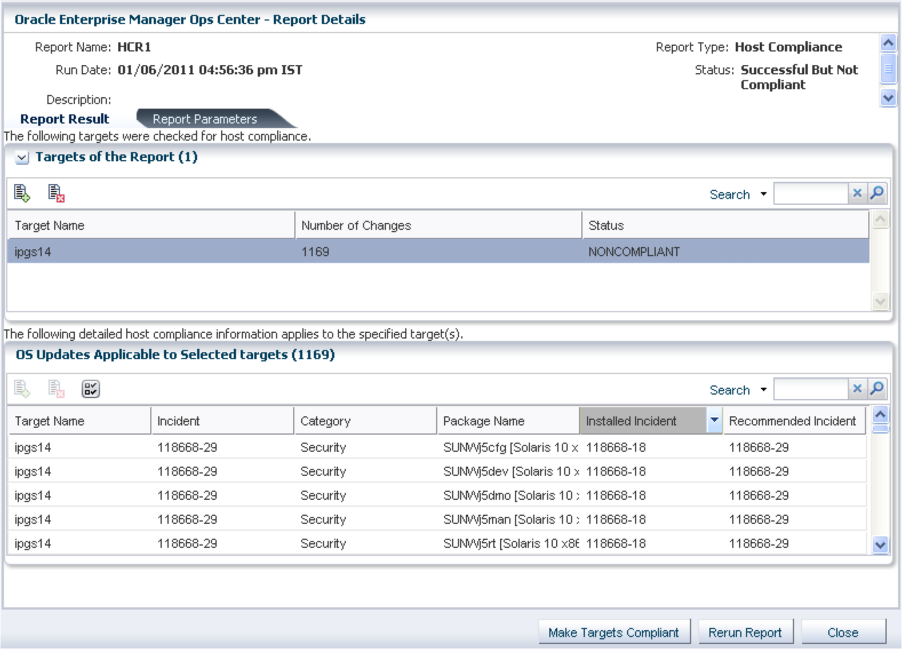
OS Updates Applicable to Selected targets (932)

Target Name	Incident	Category	Package Name	Installed Incident	Recommended Incident
ipgs14	118855-36	Security	CADP160 [Solaris 10 x8	118855-36	118855-36
ipgs14	118855-36	Security	SUNWi1394 [Solaris 10 x	118855-36	118855-36
ipgs14	118855-36	Security	SUNWaac [Solaris 10 x8	118855-36	118855-36
ipgs14	118855-36	Security	SUNWad810 [Solaris 10	118855-36	118855-36
ipgs14	118855-36	Security	SUNWadp [Solaris 10 x8	118855-36	118855-36

The report result shows the recommended incidents that have been installed on the system for the required security and bug fixes. The status of the target is displayed as NONCOMPLIANT which means that the target OS still require management to be compliant.

If you have selected to create a noncompliant report, the report result shows how many incidents have to be installed on the target OS. A sample compliant report result is displayed as follows:

Figure A–6 Not Compliant Host Compliance Report Result



Oracle Enterprise Manager Ops Center - Report Details

Report Name: **HCR1**
Run Date: **01/06/2011 04:56:36 pm IST**
Description:

Report Type: **Host Compliance**
Status: **Successful But Not Compliant**

The following targets were checked for host compliance.

Targets of the Report (1)

Target Name	Number of Changes	Status
ipgs14	1169	NONCOMPLIANT

The following detailed host compliance information applies to the specified target(s).

OS Updates Applicable to Selected targets (1169)

Target Name	Incident	Category	Package Name	Installed Incident	Recommended Incident
ipgs14	118668-29	Security	SUNWj5cfg [Solaris 10 x	118668-18	118668-29
ipgs14	118668-29	Security	SUNWj5dev [Solaris 10 x	118668-18	118668-29
ipgs14	118668-29	Security	SUNWj5dmo [Solaris 10	118668-18	118668-29
ipgs14	118668-29	Security	SUNWj5man [Solaris 10	118668-18	118668-29
ipgs14	118668-29	Security	SUNWj5rt [Solaris 10 x8	118668-18	118668-29

The report results shows the list of installed incidents that are not compliant with the recommended incidents. The report result provides option to run a compliant job to install the recommended incidents. Click Make Targets Compliant to initiate the compliance job.

You can use the search functionality to find out the packages from the list. You can use the search function based on the columns that are displayed for the report result.

Scenario - Setting the Number of Zones for Parallel Patching

The Solaris 10 utilities patch 119254-66 (SPARC) and 119255-66 (x86) are now installed during agent installation in Enterprise Manager Ops Center. You can now set the maximum number of non-global zones to be patched in parallel in the configuration file `/etc/patch/pdo.conf`.

When you patch non-global zones in Enterprise Manager Ops Center, the zones are patched in parallel. At present, the number of zones that can be patched in parallel is set to 1 by default. You can modify the number of zones that must be patched in parallel.

You must set the maximum number of zones that must be patched in parallel in the pdo.conf configuration file. This file is present in the `/etc/patch` directory of the Enterprise Controller. Edit this file and change the value for num_proc. For example, you can edit the value of num_proc=8, which means that at a time 8 non-global zones can be patched in parallel.

Refer to the patch 119254 README for more information about the factors that affect the parallel patching in zones.

You can use the Local Content and View Catalog option to initiate this change before applying a patch on the zones. The typical steps that are required in Enterprise Manager Ops Center are as follows:

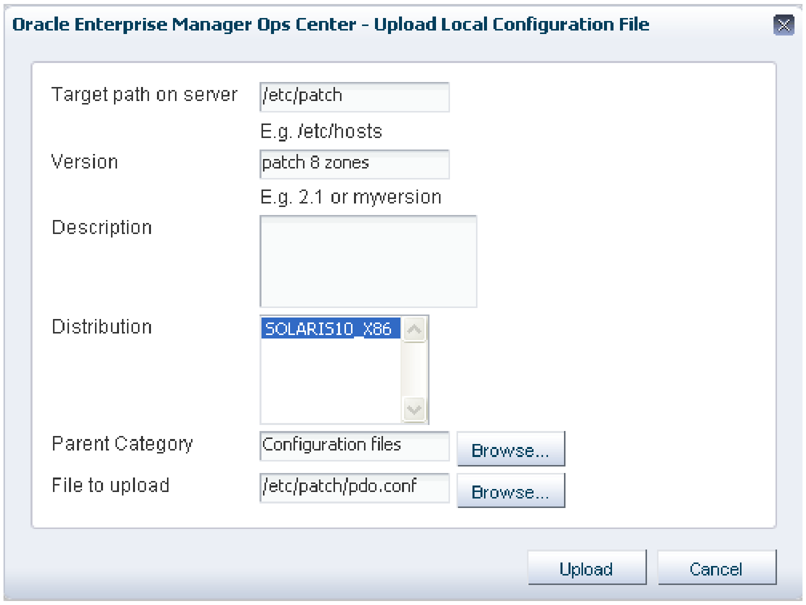
- Upload the local configuration file `pdo.conf`
- View the catalog and mark the uploaded configuration file as Required
- Launch a modification job to install the component

Uploading the Configuration File pdo.conf

1. From the Navigation pane, select Libraries section.
2. Expand Solaris/Linux OS Updates and select Local Contents. The OS Update Components are displayed in the center pane.
3. From the Actions pane, select Upload Local Configuration File. The Upload Local Configuration File window is displayed.
4. Enter the target path on the server. The target path is `/etc/patch`.
5. In Version, type a character string to identify this version of the file.

   The version is appended to the file name when it is displayed in the Components list. For example, the version can be named as "patch 8 zones".

Figure A–7 Uploading Local Configuration File



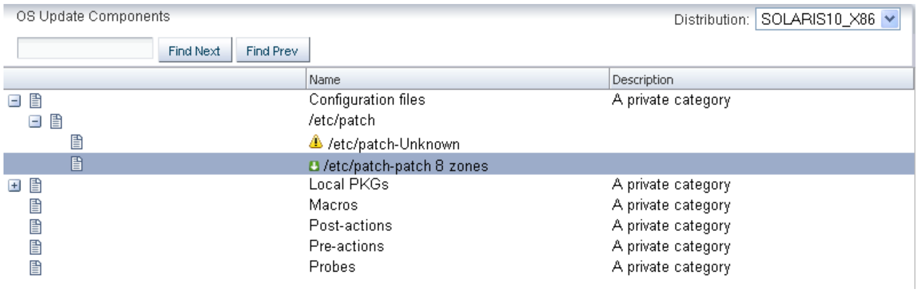
Oracle Enterprise Manager Ops Center - Upload Local Configuration File

Target path on server	/etc/patch E.g. /etc/hosts
Version	patch 8 zones E.g. 2.1 or myversion
Description	
Distribution	SOLARIS10_X86
Parent Category	Configuration files
File to upload	/etc/patch/pdo.conf

6. Enter a brief description of the configuration file.
7. Select the distribution for which the configuration file is applicable. You can select multiple distributions.
8. In Parent, accept the Configuration Files category.
9. Enter the directory in which the configuration file is saved. For example, in this case the file is saved in the `/etc/patch` directory.
10. Click Upload to upload the configuration file. A job is submitted to upload the configuration file to the selected distributions.

The uploaded configuration file will be displayed in the OS update components list as shown in the figure.

Figure A–8 OS Update Components List



OS Update Components

Distribution: SOLARIS10_X86

Name	Description
Configuration files	A private category
/etc/patch	
⚠ /etc/patch-Unknown	
/etc/patch-patch 8 zones	
Local PKGs	A private category
Macros	A private category
Post-actions	A private category
Pre-actions	A private category
Probes	A private category

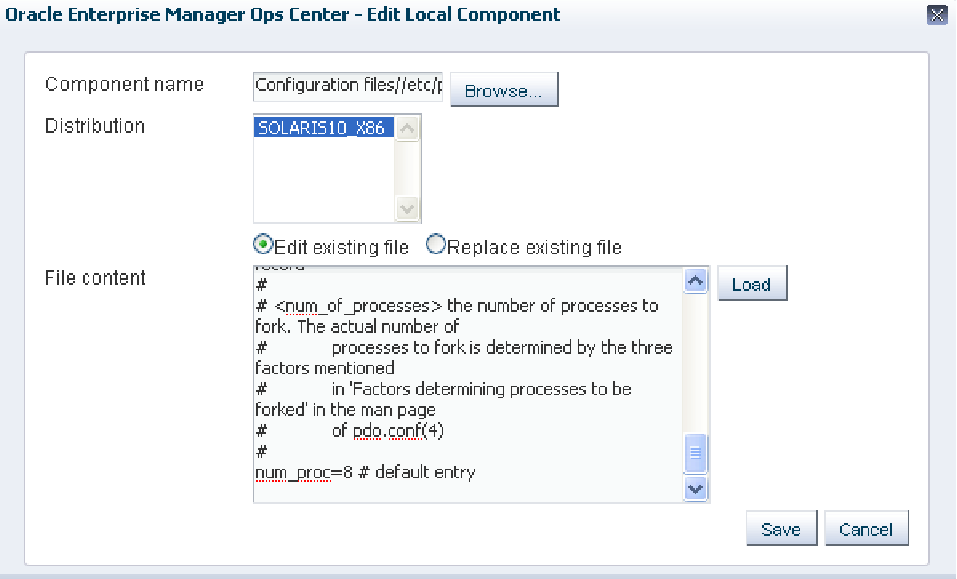
You can edit the configuration file pdo.conf to change the number of zones. Use the Edit Local Component File to modify the pdo.conf file.

Editing the Configuration File

1. From the Navigation pane, select Libraries section.
2. Expand Solaris/Linux OS Updates and select Local Contents. The OS Update Components are displayed in the center pane.

3. From the Actions pane, select Edit Local Component File option. The Edit Local Component window is displayed.
4. Either specify the name of the file as `pdo.conf` or click Browse to select the file under the parent category.
5. Select Edit Existing File option.
6. Click Load to load the file. The pdo.conf file will be displayed in the box.
7. Edit the configuration to change the value of num_proc.

Figure A–9 Editing the Local Configuration File



Oracle Enterprise Manager Ops Center - Edit Local Component

Component name: Configuration files//etc/p

Distribution: SOLARIS10_X86

● Edit existing file ○ Replace existing file

File content:

```
#
# <num_of_processes> the number of processes to
fork. The actual number of
#           processes to fork is determined by the three
factors mentioned
#           in 'Factors determining processes to be
forked' in the man page
#           of pdo.conf(4)
#
num_proc=8 # default entry
```

8. Click Save to save the changes made to the pdo.conf file.

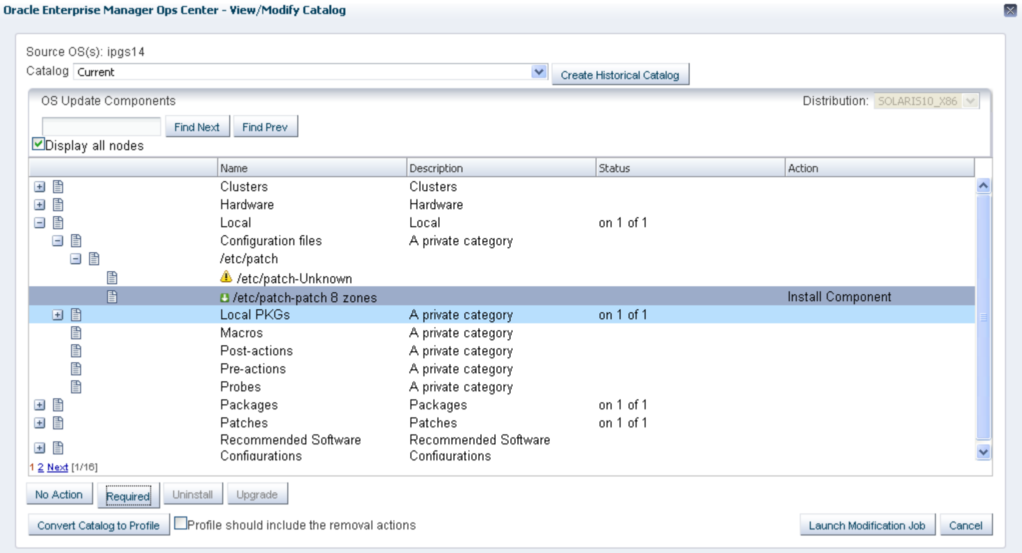
You must apply this configuration file to the selected global zone managed in Enterprise Manager Ops Center. You must install this component using the catalog option of an OS.

Viewing or Modifying Catalog of an OS

1. From the Navigation pane, select Assets section.
2. Select the global zone OS in the Assets tree. The global zone OS details are displayed in the center pane.
3. From the Actions pane, select View/Modify Catalog. The OS Update Components that are installed on the global zone are listed.
4. Expand the Configuration files component. The uploaded configuration file pdo.conf with the version "patch 8 zones" attached to it is displayed. You can see that this component is not installed on the OS.
5. Select the configuration file with "patch 8 zones" and click the Required button.

   The action for the component is set to Install Component.

Figure A–10 Modifying the System Catalog


Oracle Enterprise Manager Ops Center - View/Modify Catalog
Create Historical Catalog
OS Update Components
Find Next
Find Prev
No Action
Required
Uninstall
Upgrade
Convert Catalog to Profile
Launch Modification Job
Cancel

Source OS(s): ipgs14

Catalog: Current

Distribution: SOLARIS10_X86

☑ Display all nodes

Name	Description	Status	Action
Clusters	Clusters		
Hardware	Hardware		
Local	Local	on 1 of 1	
Configuration files	A private category		
/etc/patch			
/etc/patch-Unknown			
/etc/patch-patch 8 zones			Install Component
Local PKGs	A private category	on 1 of 1	
Macros	A private category		
Post-actions	A private category		
Pre-actions	A private category		
Probes	A private category		
Packages	Packages	on 1 of 1	
Patches	Patches	on 1 of 1	
Recommended Software Configurations	Recommended Software Configurations		

1 2 Next [1/16]

□ Profile should include the removal actions

6. Click Launch Modification Job to install the component. A job is submitted to install the component on the OS.

B

Sample JET Template

The following sample JET Template provides an example of provisioning an OS with zones.

```
# Client template file
#
# Client: sample.template
# Created: Mon Jun 23 04:08:51 MDT 2008
#
# This file was automatically generated using 'make_template'
###############################################################################
###############################################################################
#
# Product: base_config
#
# Synopsys: Basic host information
#
###############################################################################
############
#
# Architecture type:
# sun4c : e.g. SS1, SS2, SS IPX
# sun4d : e.g. SS1000, SS2000
# sun4e : ?
# sun4m : e.g. SS LX, SS4, SS5, SS10, SS20
# sun4u : UltraSparc - U1, U2, E3x00, E4x00 etc
# sun4u1 : E10K
# sun4v : T2000
#
# i86pc : Intel X86
#
# Ethernet can be obtained from the 'banner' command at OBP
#
# OS is one of the values you used to register the solaris media using
# the add_solaris_location command
#
base_config_ClientArch=
base_config_ClientEther=
base_config_ClientOS=
############
#
# Client allocation
#
# The mechanism used to build this client; by default, the options listed
# in /opt/jet/etc/jumpstart.conf will be tried; you should only set this
# if this particular client needs to do something different.
# JET supports bootp, dhcp, and grub as allocation options.
# Currently grub is only supported on i86pc architectures.
#
base_config_client_allocation=""
# If you are using grub, you can set this variable to apply additional
# grub directives to the menu.lst.<MACADDRESS> file.
#
base_config_grub_append=""
############
#
# products is the set of products to install after base_config; this
# should be updated automatically by make_template, so you
# will only need to change it, if you wish to omit certain
# modules when testing/debugging.
#
base_config_products=""
############
#
# JumpStart sysidcfg information
#
# The sysidcfg file provides information at initial boot time so that the
# system can properly identify itself. The interface and ip address defined
# here MUST be on the same subnet as the JumpStart server. The root password
# is set here also and must be written in encrypted format. The default value
# shown here is "newroot". The timeserver is normally the IP address of the
# JumpStart server.
#
# nameservice examples:
# NONE
# NIS { domain_name=uk.sun.com name_server=nis.uk.sun.com(129.159.91.1) }
# or for DNS
# DNS { domain_name=uk.sun.com name_server=192.168.1.1 search=uk.sun.com }
#
# network_interface:
# le0, hme0
# or PRIMARY (the default interface - net in OBP)
# N.B. PRIMARY is only valid from Solaris 7 upwards
#
# locale:
# en_GB for Solaris 7 and above
#
# timeserver: Where the client gets the current time from.
# Leave blank to default the the JumpStart server
#
# Alternatively, set to 'localhost' to trust the current
# hardware clock on the client
#
# terminal: terminal type (vt100/vt220/sun etc)
#
# security_policy: Kerberos policy (Solaris 8 +)
#
# protocol_ipv6: Use ipv6 or not (Solaris 8 +)
#
# default_route: Solaris 9 allows a default route to be set
# (ignored on all other versions of Solaris, less than 9)
#
base_config_sysidcfg_nameservice=NONE
base_config_sysidcfg_network_interface=PRIMARY
base_config_sysidcfg_ip_address=
base_config_sysidcfg_netmask=
base_config_sysidcfg_root_password=
base_config_sysidcfg_system_locale=
base_config_sysidcfg_timeserver=
base_config_sysidcfg_timezone=
base_config_sysidcfg_terminal=vt100
base_config_sysidcfg_security_policy=NONE
base_config_sysidcfg_protocol_ipv6=no
base_config_sysidcfg_default_route=
########################################
# X86, X64 specific settings. If this is an x86 client, then you may need
# to configure these settings. They are ignored for SPARC builds.
#
# base_config_x86_nowin:
# This stops Solaris from trying to run windows during the install.
# the default value is yes.
#
# base_config_x86_console:
# Set the console to the correct tty port. This is used for doing installs
# via the serial port or the SP. b1600,v20z and v40z use ttya. lx50, v60x,
# and v65x use ttyb. NOTE: you only need to set this if you are NOT going
# to connect a keyboard and monitor to the client.
#
# base_config_x86_disable_acpi:
# Disable ACPI - sometimes disabling ACPI makes the install go
# better due to how the interrupts are handled. Non-Null disables ACPI.
#
# base_config_x86_safetoreboot:
# The Solaris installer can't control the BIOS, therefore does not
# know if its safe to reboot the client as it may simply jumpstart
# again. If your PXE boot is a one time option, and the next reboot
# will attempt to boot from disk, then you probably want to set this
# option to "yes". Otherwise, leave it as it is so that it won't reboot
# and therefore allow you to manually change your BIOS to boot from disk.
#
# base_config_x86_disable_kdmconfig:
# X86 systems sometimes go interactive on the first reboot (Bug 6321043)
# on Solaris 10 Update 1. Setting this parameter will stop this from
# happenning.
#
# base_config_x86_confflags
# The parameters specified for this variable are passed directly to
# add_install_client -b confflags= option.
# For e.g., by specifying,
# base_config_x86_confflags="-f -P/boot/solaris/dca"
#
# add_install_client is called with -b confflag="-f -P /boot/solaris/dca"
# option.
#
# base_config_sysidcfg_x86_kdmfile
# Append the file specified here to sysidcfg file.
# This variable can reference a file relative to the
# Clients/<clientname> directory or a absolute path.
#
#
base_config_x86_nowin="yes"
base_config_x86_console=""
base_config_x86_disable_acpi=""
base_config_x86_safetoreboot=""
base_config_x86_disable_kdmconfig=""
base_config_x86_confflags=""
base_config_sysidcfg_x86_kdmfile=""
```

```
#
#
#
#
#######
# Disk labelling
# In some cases the disks in the server may not be labelled, the
# following variable allows you to label all the unlabelled disks.
#
# Allowed values:
#
# base_config_label_disks="" Do not label any disks.
# base_config_label_disks="all" Label ALL unlabelled disks.
# base_config_label_disks="cxtydz cmtndo" Label listed disks.
#
base_config_label_disks=""
#######
# Disk partitioning
# In some cases, the disks may already be used, or may have other O/Ss
# installed in other partitions. The following variable allows you to
# modify the partitioning configuration of the disks. It is primarily
# useful for x64/x86 based machines.
#
# Allowed values:
#
# base_config_profile_fdisk="" Do not alter current partitioning.
# Solaris will either use an existing
# Solaris partition, or use any
# unused free space on the disk.
# base_config_profile_fdisk="freedisk" Remove any existing Solaris
# partitions. Create one of maxsixe
# in remaining space.
# base_config_profile_fdisk="alldisk" Remove ALL existing partitions.
# Create a single Solaris partition
# using the whole disk.
base_config_profile_fdisk=""
#
# Want to create your own custom profile ? if so, use this variable to
# reference a file relative to the Clients/<clientname> directory or
# absolute path, otherwise fill in the other details below to get toolkit
# to create one for you.
#
# If absolute path is specified, then the profile file is copied
# to Clients/<clientname> directory.
#
# It is also possible to append additional profile information to the JET
# derived one. Do this using the base_config_profile_append variable, but
# don't forget to fill out the remaining base_config_profile variables.
#
base_config_profile=""
base_config_profile_append=""
#
#######
# OR fill out the base_config_profile variables below.
############
#
# JumpStart profile information
#
#
# A limited profile can be automatically generated here. If further
# customisation is required, then you can manually create a profile in the
# client directory and reference it in the base_config_profile variable.
#
# Cluster:
# SUNWCrnet : Minimal. Solaris 10 only
# SUNWCreq : Required - really basic, good for testing
# SUNWCuser : User collection
# SUNWCprog : User + Developers collection
# SUNWCall : All packages
# SUNWCXall : All + OEM packages (mandatory for E10K)
#
# usedisk: defines the disk that the OS will be loaded on to - bootdisk
# (if this is set to rootdisk. , then the current boot disk will
# be used)
#
# dontuse: defines disks that should not be used..
# ** N.B. This will only be used if 'usedisk' is NOT set
# Space separated list of disks of the form c?t?d?
#
# partition sizes:
#
# if partitions are not required simply leave blank. In order to maintain
# consistency the partitions will always use the same slice number:
#
# / s0
# swap s1
#
# We've prepopulated the remaining slices based on Sun defaults,
# but you can change this.
# /var s5
# /usr s6
# /opt s7
#
# at most one partition can have the size 'free' which denotes all the
# unallocated/spare space on a disk.
#
base_config_profile_cluster=SUNWCuser
base_config_profile_usedisk=rootdisk.
base_config_profile_dontuse=""
base_config_profile_root=free
base_config_profile_swap=256
#
# If you are using VxVM and want your boot disk to look like the mirror, then
# leave slices 3 and 4 empty. If you do not care about keeping the two disks
# looking cosmetically the same, please just make sure you have two free slices
# somewhere on the disk for VxVM!
#
# If you are not using VxVM, then you can use s3 and s4 for whatever you wish!
#
base_config_profile_s3_mtpt=""
base_config_profile_s3_size=""
base_config_profile_s4_mtpt=""
base_config_profile_s4_size=""
base_config_profile_s5_mtpt="/var"
base_config_profile_s5_size=""
base_config_profile_s6_mtpt="/usr"
base_config_profile_s6_size=""
#
# If you are using DiskSuite, the default behaviour is to use slice 7 as a
# location for metastate databases. If you are using DiskSuites default config,
# please avoid using s7 for data!
#
base_config_profile_s7_mtpt="/opt"
base_config_profile_s7_size=""
#
############
############
#
# You can specify additional disks to use/configure here
#
# additional_disks is a space separated list of c?t?d? type disk names
#
# For each disk listed in additional_disks, a pair of variables of the form
#
# base_config_profile_disk_c?t?d?s?_mtpt="...."
# base_config_profile_disk_c?t?d?s?_size="...."
#
# should be defined for each slice required on the disk.
#
# N.B. DO NOT SET THE BOOT DISK UP HERE !
#
base_config_profile_additional_disks=""
############
#
# Additional locales/geos e.g. N_Europe, C_Europe
#
#
base_config_profile_add_locales=""
base_config_profile_del_locales=""
base_config_profile_add_geos=""
base_config_profile_del_geos=""
############
#
# UFS Logging
#
# Solaris 7 and above support UFS+, which allows for a logging filesystem
# under UFS. If you want to use this feature on any of the UFS mount points,
# please specify the mount points here, as a space separated list, or enter
# the keyword "all" to enable logging on all UFS filesystems.
#
# Solaris 9 09/04 enables logging by default. You can also specify mountpoints
# preceded by a - sign to say that you DON'T want logging enabled on that
# filesystem, or you can use the keyword "none" to say you don't want any
# ufs logging turned on at all.
#
# N.B. root (/) can be included in the list, and is included by default if
# using either the "all" or "none" keyword.
#
# Finally, you can't mix keywords and mountpoints. i.e. "all -/" is NOT
# valid.
# e.g. base_config_ufs_logging_filesys="all" : log all filesystems
# base_config_ufs_logging_filesys="none" : log no filesystems
# base_config_ufs_logging_filesys="-/ /var -/usr" : log /var, but not / and /usr.
#
base_config_ufs_logging_filesys="all"
############
#
# Packages to add to/remove from the selected cluster
#
# Use this to populate the profile with package <pkg> <add|delete> entries
```

```
#
base_config_profile_add_packages=""
base_config_profile_del_packages=""
############
#
# Clusters to add to/remove
#
# Use this to populate the profile with cluster <cluster> <add|delete> entries
#
base_config_profile_add_clusters=""
base_config_profile_del_clusters="SUNWCpm SUNWCpmx SUNWCdial SUNWCdialx"
############
#
# Remote file systems (NFS)
#
# Specify these as space separated list of pairs as follows, using ? as
# the separator (as : has special meanings with nfs!)
#
# e.g. to mount 1.1.1.1:/fs on /fs you would create the entry
# base_config_nfs_mounts="fs?1.1.1.1:/fs"
#
base_config_nfs_mounts=""
############
#
# Host information
#
# This section defines most things network related etc.
#
# In addtion, if the machine will be JumpStarted as one name/address and
# needs to have a different name/address once installed, this is where you
# can set that information.
#
# nodename: the value for /etc/nodename if it's not the default
# hostname
#
# defaultrouter: the value for /etc/defaultrouter.
#
# notrouter: if this is set, the file /etc/notrouter will be created
#
# dns_domain: domain entry for /etc/resolv.conf
#
# dns_nameservers: nameserver entries for /etc/resolv.conf
# (list of ip addresses, space separated)
#
# dns_searchpath: list of entries to go in the search line
#
# dns_disableforbuild: If there is no DNS available in the build
# environment, set this to delay the configuration
# of DNS until later on.
#
base_config_nodename=""
base_config_defaultrouter=""
base_config_notrouter=""
base_config_dns_domain=""
base_config_dns_nameservers=""
base_config_dns_searchpath=""
base_config_dns_disableforbuild="yes"
###########
#
# NTP configuration
```

```
#
# Specify a list of names or ip addresses for the NTP servers. The first
# one will be given a 'prefer' tag. This section will only place lines
# of the form: server <ipaddress/name> [prefer]
# into the /etc/inet/ntp.conf file. If you require more control of ntp,
# please use the custom module to deploy your own custom ntp.conf file.
#
# N.B. If you do use names, they must be resolvable in your name service.
#
base_config_ntp_servers=""
############
#
# Network Interface information
#
#
# networkifs: a list of interfaces to be defined,
# space separated "le0 hme0".
# N.B. the sysidcfg interface will already be configured
#
# Logical interfaces should be defined using _'s rather
# than :'s.
#
# networkif_<ifname>: the details of the interface <if>
# "netname netmask hostname address"
#
# netname: arbritrary name for /etc/networks
# netmask: netmask of this if (e.g. 255.255.255.0)
# hostname: unique hostname (N.B. not multihomed)
# address: IP address of this interface
#
# For example:
#
# base_config_networkifs="ge0 ge0_1"
# base_config_networkif_ge0="bkp 255.255.255.0 me-bkp 192.168.1.0"
# base_config_networkif_ge0_1="bkp2 255.255.255.0 me-bkp2 192.168.2.0"
#
base_config_networkifs=""
base_config_networkif_le0=""
# N.B. Logical interfaces MUST use _ rather than : as illustrated below
base_config_networkif_le0_1=""
############
#
# IP Multipathing (Solaris 8+)
#
# IPMP default mode is automatic failback.
# To change this mode edit /etc/default/mpathd
#
# ipmp_networkifs: a list of interfaces to be defined under ipmp control
# a space separated list of pairs only
# e.g. "qfe0_qfe4 qfe1_qfe5"
#
# N.B. If the primary interface is used in an ipmp group, the
# system must be rebooted manually after installation to
# activate ipmp.
#
# N.B. Can only setup ipmp group with pairs of interfaces in one
# of the following configurations:
# active-standby failover:
# Set ipmp mode = s, and specify one logical
# hostname/ip address pair.
# failover with outbound load spreading:
# Set ipmp mode = l, and specify one logical
# hostname/ip address pair.
# active-active with outbound load spreading:
# Set ipmp mode = l, specify a second logical
# hostname/ip address pair for the second interface.
#
# ipmp_networkif_<if>_<if>: "netgroup mode test1 test2 mask hostname log-ip
hostname2 log-ip2"
#
# details of the interfaces in the ipmp group
# e.g. networkif_ipmp_qfe0_qfe4
#
#
# netgroup: ipmp interface group name
# e.g. database-net
#
# ipmp mode: s = standby (failover only)
#
# ** test addresses are allocated last,
# ** first test address will be on the
# ** first virtual interface of the
# ** first physical adapter. Second
# ** test address will be on the second
# ** physical adapter.
#
# l = load spreading / active-active
#
# ** test addresses are allocated on
# ** first virtual interfaces on both
# ** the first and second physical
# ** adapters.
#
# To force the test addresses onto the physical
# adapters, use the suffix 'p' to the above
# modes, i.e. 'sp' or 'lp'. This is not
# recommended and may break certain applications.
#
# test1: ipmp test address1
# test2: ipmp test address2
#
# N.B. these addresses must not be used or
# placed in the hosts file
#
# mask: netmask for ipmp pair
#
# hostname: unique hostname for logical ip
#
# log-ip: logical ip address for first i/f of pair
#
# N.B. The following two parameters are for active-active
# configurations only. Do not specify them for an
# active-standby configuration.
#
# hostname2: unique hostname for logical ip
#
# log-ip2: logical ip address for second i/f
# of pair
# IPMP on Solaris 10.
# If you are running Solaris 10, you can optionally configure the
# system to have NO test addresses. In this case, the ipmp mode should be set
# to "ln" or "sn" depending on whether you want outbound load spreading or
# not and the 2 test addresses do not need to be privided.
#
# Examples:
# --------
#
#
# base_config_ipmp_networkifs="qfe0_qfe1"
# Outbound load spreading 2 hostnames, test on virtual interfaces.
# base_config_ipmp_networkif_qfe0_qfe1="db l 10.0.0.1 10.0.0.2 24 oracle-db
10.0.0.3 apache 10.0.0.4"
# Outbound load spreading 1 hostname, test on physical interfaces.
# base_config_ipmp_networkif_qfe0_qfe1="db lp 10.0.0.1 10.0.0.2 24 oracle-db
10.0.0.3"
# Failover, 1 hostname, test on physical interfaces.
# base_config_ipmp_networkif_qfe0_qfe1="db sp 10.0.0.1 10.0.0.2 24 oracle-db
10.0.0.3"
# Failover, 1 hostname, no test addresses (Sol 10 only).
# base_config_ipmp_networkif_qfe0_qfe1="db sn 24 oracle-db 10.0.0.3"
#
#
base_config_ipmp_networkifs=""
base_config_ipmp_networkif_qfe0_qfe1=""
############
#
# Misc options
#
# this section is a catchall for other options not included above
#
# update_terminal: if set, put the sysidcfg terminal type into inittab
#
# enable_savecore: if set to any value, enable save core (Solaris 2.6 only)
#
# dumpadm_minfree: set a limit so that crash dumps don't fill up the
# dump filesystem. See dumpadm(1M) -m option for
# possible values.
#
# noautoshutdown: if set to any value, disable power management
#
# enable_rootlogin: if set to any value, enable network root login
# from both telnet/rsh and ssh
#
# enable_rootftp: if set to any value, enable root ftp access
#
# shutup_sendmail: if set, create an alias hostname. to shut up sendmail
#
# poweroff_afterbuild: if set, shut the machine down once it has been built
#
# base_config_dedicated_dump_device:
# if set, dumpadm will configure the partition as a
# Dedicated Dump Device. See dumpadm(1M) for supported
# Operating Environments.
# (Device path e.g. /dev/dsk/c?t?d?s? or rootdisk.sn)
#
# N.B. This partition is for the SOLE use of the crashdump utility !
#
# enable_altbreak: if set, enable alternate break sequence
#
# disable_sysid_probe: if set, skip the sysid stuff on the first reboot; this
# usually just tries to rarp ip addresses for additional
# interfaces and takes *ages* on machines with lots
# of unused network adapters.
#
#
base_config_update_terminal="yes"
base_config_enable_savecore="yes"
base_config_dumpadm_minfree="20000k"
base_config_noautoshutdown="pm_disabled"
base_config_enable_rootlogin=""
base_config_enable_rootftp=""
base_config_shutup_sendmail=""
base_config_poweroff_afterbuild=""
base_config_dedicated_dump_device=""
base_config_enable_altbreak=""
base_config_disable_sysid_probe=""
############
#
# NFSv4
#
# Set up the NFSv4 domain to prevent being prompted at first reboot.
# If not set, this will default to the entry in base_config_dns_domain,
# and if that is not set, to the value 'domain', which is the default
# in /etc/default/nfs
#
base_config_nfsv4_domain=""
############
#
# N.B. Unless you need to point this client at alternate media for patches
# and packages that is not held on this server, please skip this section!
#
# productdir is where to find the products. This should be a URI style
# path, i.e. nfs://192.168.1.1/export/install/pkgs. If the server
# is the JumpStart server, then it should just be specified
# as a normal path.
#
# patchdir is where to find the patches. Same format as productdir.
#
# --------------------------------------------------------------------------
# Leaving the following blank means they will be populated using jumpstart.conf
# and the JumpStart servers ip address. This is the default behaviour
# and should only be changed if your patch/package repository is not held
# on this server.
# --------------------------------------------------------------------------
base_config_productdir=""
base_config_patchdir=""
#
# Last one - mainly for developing JumpStart scripts!
#
# If you set this, the rc3.d/S99jumpstart script will be disabled
# (set to rc3.d/s99jumpstart) every time it is processed - this allows you
# to run it by hand and invoke each reboot step
# This does not work on Solaris 10.
#
base_config_debug_jumpstart_postinstall=""
#
###############################################################################
###############################################################################
#
# Product: Custom
```

```
#
# Synopsis: The custom product can install packages and patches that
# would not otherwise be included by the standard
# installation products.
#
################################################################################
############
#
# Which additional packages are to be installed
# (by default, these get added during the main Solaris installation phase)
#
# O.S. Specific versions:
# as a side effect, if a directory exists under the package dir named
# after the OS, (uname -r), the subdirectory will be used instead of the
# main package directory
#
# i.e /export/install/pkgs/custom/sparc/5.8 takes preference over
# /export/install/pkgs/custom/sparc for a Solaris 8 box
#
# Package Response files:
# If a custom package needs a response file, create a directory called
# /opt/jet/Clients/<clientname>/responses
# and put the response file in to it, named the same as the package.
#
# i.e. for a package called Fred, on client1, use pkgask to create
# pkgask -r /opt/jet/Clients/client1/responses/Fred Fred
#
# (Space seperated list of packages)
#
custom_packages=""
#
# Custom packages at subsequent boots
#
# <number> denotes the boot number you want the action to be performed.
# You can create new variables for boot levels 2,3,4 etc.
# n means after the last reboot. i.e. last.
# m means n-1. i.e. before the last reboot. Use m if you need to
# guarantee a reboot after the action is performed.
#
custom_packages_1=""
custom_packages_m=""
custom_packages_n=""
############
#
# Which additional patches are to be installed
# (by default, these get added during the main Solaris installation phase)
# (Space seperated list of patches)
#
custom_patches=""
#
# Custom patches at subsequent boots
#
# <number> denotes the boot number you want the action to be performed.
# You can create new variables for boot levels 2,3,4 etc.
# n means after the last reboot. i.e. last.
# m means n-1. i.e. before the last reboot. Use m if you need to
# guarantee a reboot after the action is performed.
#
custom_patches_1=""
custom_patches_m=""
```

```
custom_patches_n=""
#
# Custom patch sets... create a directory in the patch directory named after
# the set, and put a patch_order file in it, along with the patches...
# (Space seperated list of patch set names)
#
# N.B. as a side effect, if a directory exists under the patch set dir named
# after the OS, (uname -r), the subdirectory will be used instead of the
# main patchset directory
# i.e /export/install/patches/patchset/5.8 takes preference over
# /export/install/patches/patchset
#
custom_patchsets=""
#
# Custom patchsets at subsequent boots
#
# <number> denotes the boot number you want the action to be performed.
# You can create new variables for boot levels 2,3,4 etc.
# n means after the last reboot. i.e. last.
# m means n-1. i.e. before the last reboot. Use m if you need to
# guarantee a reboot after the action is performed.
#
custom_patchsets_1=""
custom_patchsets_m=""
custom_patchsets_n=""
############
#
# Search paths
#
# The files and scripts sections below will look for source files relative
# to the Clients/<clientname> directory. If you wish to look in other places
# for files, please fill out the search path option below. Items in the
# search path are relative to the Clients/<clientname> directory, since the
# client has no knowledge of the filesystem layout of the server
#
# e.g. for a client 'fred', the default location for all custom files/scripts
# is /opt/jet/Clients/fred
#
# if the search path was set to "../common" then the installation routines
# would look first in Clients/fred then
# Clients/fred/../common (or Clients/common in this case)
#
# Search path is a space separated list of places to search
#
# THE SEARCHPATH IS ONLY VALID FOR files & scripts. NOT PACKAGES/PATCHES!
#
custom_search_path="../common.files"
############
#
# Files to be copied to the client. The filenames must be of the form
#
# filename1:[a|o]:filename2
#
# Where filename1 is the name of the source file in the
# /opt/jet/Clients/<clientname> directory
# filename2 is the full path of the file on the installed client
# and the middle option is whether to a - append, or o - overwrite the file
#
# (by default, these get added during the main Solaris installation phase)
#
```

```
# (Space seperated list of tuples)
#
# N.B. Please see section above regarding where to place the source files
#
# N.B. (2):
# appending to /etc/hosts is a special case; instead of just appending
# the file, the module will do an 'intelligent merge' of the new hosts
# file with the existing one.
#
# custom_files="hosts:a:/etc/hosts"
#
custom_files=""
#
# Custom files at subsequent boots
#
# <number> denotes the boot number you want the action to be performed.
# You can create new variables for boot levels 2,3,4 etc.
# n means after the last reboot. i.e. last.
# m means n-1. i.e. before the last reboot. Use m if you need to
# guarantee a reboot after the action is performed.
#
custom_files_1=""
custom_files_m=""
custom_files_n=""
############
#
# Scripts to be run on the client at the end of the build
#
# The scripts must be placed in the directory
# /opt/jet/Clients/<clientname>
# and will be copied to the client.
#
# If you want to run custom scripts during the Jumpstart
# phase, use the custom_scripts_f variable below.
#
# Custom scripts at subsequent boots
#
# <number> denotes the boot number you want the action to be performed.
# You can create new variables for boot levels 2,3,4 etc.
# n means after the last reboot. i.e. last.
# m means n-1. i.e. before the last reboot. Use m if you need to
# guarantee a reboot after the action is performed.
#
custom_scripts_1=""
custom_scripts_m=""
custom_scripts_n=""
#
# Special JumpStart 'Begin' and 'Finish' phase scripts
#
# If you need to run scripts in the 'begin' or 'finish' phase of the
# JumpStart, you can supply them here. Please note, that in the 'begin'
# phase, the new OS has not been installed and the majority of the OS
# running will be read-only from the JumpStart server. In the 'finish'
# phase, the newly installed O/S is not yet running, and is mounted
# on ${ROOTDIR} (normally /a)
#
custom_scripts_b=""
custom_scripts_f=""
################################################################################
################################################################################
```

```
#
# Product: Flash configuration
#
# Synopsis: This section contains details of how to use a flash image
# while building the client
#
################################################################################
############
#
# Flash image creation
# --------------------
#
# You need to pre-build a host and create a flash image *before* you can
# use this module.
#
# To create an image, use the following command on the target host to create
# the image.
#
# flarcreate -n "WebServer" -c -S -R / /export/install/flash
#
# -n -> Name of the image
# -c -> compress the image
# -R -> Start at / for this image
#
# save archive in /export/install/flash
#
# for more options, please see flarcreate(1M)
#
############
############
#
# Specify archive locations - you can install more than one, especially
# if you create archives for layered products etc.
#
# Space seperated list of items; each item is of the form...
#
# nfs://10.1.1.11/archives/sample
# http://www.quakeworld.com/games.flar
#
# locations that specifiy a directory only will default to look for
# an archive called installsvr
#
flash_archive_locations=""
############
#
# As described in SRDB 44793, some devices are not compatible with flash
# installs and cause an arithmetic exception during the JumpStart.
#
# The srdb recommends that the offending devices are removed from the
# memory based mini root prior to the flash install being performed.
#
# Add such devices to the following variable to make the begin script
# clean out the devices as prescribed in the SRDB.
#
# The variable should be a space seperated list of the form
# c?[t?][d?][s?]
#
# For example
#
# flash_incompatible_devices="c1 c2t3 c3t4 c5t0d0s0"
```

```
#
flash_incompatible_devices=""
############
#
# Cleanup scripts
#
# The flash_cleanup_scripts variable allows you to run scripts after
# the flash restore and prior to any other module scripts being executed.
#
# This facility allows you to correct or alter any information that was
# restored from the flash image.
#
# To execute scripts after the first reboot, use the custom module.
#
# ---------------------------------------------------------------------
#
# The scripts variable below will look for source files relative
# to the Clients/<clientname> directory. If you wish to look in other places
# for files, please fill out the search path option below. Items in the
# search path are relative to the Clients/<clientname> directory, since the
# client has no knowledge of the filesystem layout of the server
#
flash_search_path=""
flash_cleanup_scripts=""
############
#
# Set this to make the install skip the recommended patches - if your
# flash image already contains recommended patches, then this can speed up
# your builds.
#
# WARNING: by setting this you could well be missing important patches
#
# Use at your own risk - this is not default behaviour!
#
flash_skip_recommended_patches=""
############
#
# Set this to leave the md.tab files (SVM) as delivered in the flar;
# useful if you intend to re-create metadevices yourself and not use
# the JET sds module.
#
# N.B. setting this flag AND using the JET sds module may give you
# some strange metadevice numbers, or might end up running out of
# md numbers before the root disk has been mirroed - you have been
# warned!
#
flash_skip_md_cleanup=""
#
###############################################################################
###############################################################################
#
# Product: zones configuration
#
# Synopsis: This section contains details of how to set up
# zones on this client.
#
###############################################################################
############
#
# Zones are part of Solaris 10 (or higher), and can be defined here for
# creation when the target system is built.
############
#
# Where the zones will pick up their config information; leave these
# blank to make the zones pick up their config from the current JET
# server.
#
# zones_jet_serverip="" # IP address of JET server; leave blank to
# # use the same server as this host
#
# zones_jet_cfgdir="" # Location of the JET config area on the
# # JumpStart server above; leave blank to use
# # the same location as the current JET server
#
zones_jet_serverip=""
zones_jet_cfgdir=""
############
#
# Default location of where to create new zone directories that are to
# be hosted on this system
#
zones_default_path="/export/zones"
############
#
# Give a list of zone names to create; this will be the 'nodename' for
# the zone; it is expected that you will create these zones using the
# 'make_zone_template' and 'make_client' commands.
#
# i.e. zone1 zone2 zone3 my-zone
#
zones_names=""
```

See Provisioning an OS for more information about provisioning an OS using JET templates.