Oracle® Enterprise Manager Ops Center

Site Preparation Guide

11*g* Release 1 Update 3 (11.1.3.0.0)

E18418-04

November 2011

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

E18418-04

Primary Author: Barbara Higgins

Contributing Author: Laura Hartman, Owen Allen, Shanthi Srinivasan

Contents

Preface v

Audience v
Documentation Accessibility v
Related Documents v
Conventions vi

1 Planning For Enterprise Manager Ops Center

Will You Use Connected Mode or Disconnected Mode? 1-1
Connected Mode 1-1
Disconnected Mode 1-2
Will You Manage Virtual Assets? 1-3
Using Zones 1-3
Using Logical Domains 1-4
What Type of Network Configuration? 1-4
Network Requirements 1-4
Examples of Network Configurations 1-6
Does Your Site Require High Availability? 1-13
High Availability for the Enterprise Controller 1-13
High Availability for Storage Resources 1-14
How Will You Use Enterprise Manager Ops Center? 1-15
Hardware Management 1-15
Hardware Management + OS Provisioning 1-15
Hardware Management + OS Provisioning + Update Management 1-15
Hardware Management + OS Provisioning + Update Management + Virtualization Management 1-15
What Are the System Requirements? 1-16
Cache Requirements 1-16
Oracle VM Server for SPARC Requirements 1-17
Oracle Solaris Zones Requirements 1-19

2 Getting Ready

Preparing an Oracle Solaris System for Installation 2-2
Requirements for Installation on Oracle Solaris OS 2-2
Verifying System Resources on Oracle Solaris 2-4
Preparing a System for Installation on Linux 2-9

Requirements for Linux OS Installation 2-9
Verifying System Resources on Linux 2-10
Prepare the Agents 2-15
Oracle Solaris OS: To Verify Required Packages and Devices 2-15
Linux OS: To Verify Required Packages 2-16
To Verify ssh Installation 2-17
To Verify Patches on Oracle Solaris 10 Systems With Non-Global Zones Installed 2-17
To Identify and Remove Duplicate Service Tags 2-17
To Check for Agent Patch Dependencies 2-19
To Verify the umask Value 2-19
Oracle Solaris OS: To Verify cryptosvc and gss Services 2-19
Verifying Account Access 2-19
Configuring for High Availability 2-20
Configuring Storage 2-20
Obtaining the Product Software 2-20

A Planning Checklist

Oracle Solaris A-1
Linux A-2
Assets To Be Managed A-4

Preface

The *Oracle Enterprise Manager Ops Center Site Preparation Guide* describes the choices you have in using the software at your site and helps you to prepare for the software installation.

Audience

This document is intended for site administrators who are responsible for planning the configuration of a data center.

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 Concepts Guide*
- *Oracle Enterprise Manager Ops Center User's Guide*
- *Oracle Enterprise Manager Ops Center Advanced User's Guide*
- *Oracle Enterprise Manager Ops Center Provision and Update Guide*
- *Oracle Enterprise Manager Ops Center Administration Guide*
- *Oracle Enterprise Manager Ops Center Reference Guide*
- *Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System*
- *Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems*

- *Oracle Enterprise Manager System Monitoring Plug-In for Oracle Enterprise Manager Ops Center Guide*
- *Oracle Enterprise Manager Ops Center Release Notes*
- *Oracle Enterprise Manager Ops Center Readme*

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

Planning For Enterprise Manager Ops Center

The *Oracle Enterprise Manager Ops Center Concepts Guide* (Part Number E17968) introduces you to the role the Enterprise Manager Ops Center software plays in monitoring and managing your hardware and software assets at local and remote sites throughout the life cycle of the assets. All asset types are not managed in the same way and some types of assets are limited in their ability to be managed. Also, some features of Enterprise Manager Ops Center might not be of use to your business. Use this document to plan how the Enterprise Manager Ops Center software operates at your site and to prepare for its installation.

When you are ready to install the software, get the product software and the product documentation from the Oracle Technology Network, as described in Obtaining the Product Software.

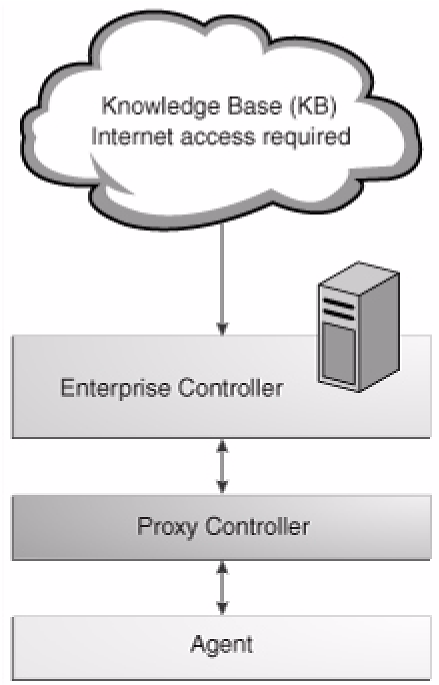
Will You Use Connected Mode or Disconnected Mode?

The Enterprise Manager Ops Center software operates in either Connected mode or Disconnected mode. Because you can change modes easily, you can also consider using a combination of Connected and Disconnected modes to maintain your data center. You can run the software in Disconnected mode until you need to access the Knowledge Base or third-party sites and then change to Connected mode. For example, to check for OS updates, change the Enterprise Controller to Connected Mode, connect to the Internet to check the Knowledge Base, and then return the Enterprise Controller to Disconnected Mode.

Connected Mode

The Enterprise Controller connects to the Internet to download OS updates, Oracle Solaris images, and updates for the Enterprise Manager Ops Center software itself. This mode of operation is called Connected mode and is the default setting. If your site policy does not allow an Internet connection, use operate Ops Center in Disconnected mode.

Figure 1–1 Enterprise Controller in Connected Mode

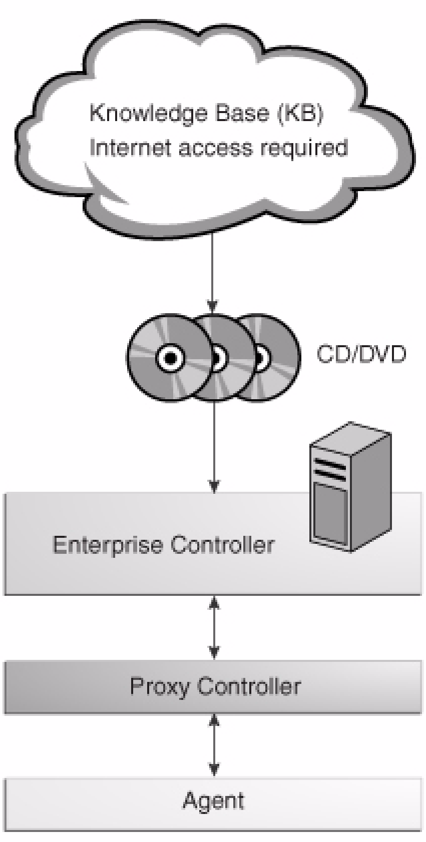


Disconnected Mode

Disconnected mode enables you to use the Enterprise Manager Ops Center software in a secured environment without Internet access. To support provisioning and updating functions, you must load images and updates to the Enterprise Controller manually. Because the Enterprise Controller does not download new software automatically, you must plan how and when your site obtains updated software.

To obtain updates, images, and metadata, you run a product script on an Oracle Solaris system that is allowed to be connected to the Internet, download a static version of the Knowledge Base (KB), and copy it to the Enterprise Controller. For other supported operating systems, you can obtain software in a media format such as a DVD, and upload the software to the Local Content section of the product's software library, as illustrated in the following figure.

Figure 1–2 Enterprise Controller in Disconnected Mode



Will You Manage Virtual Assets?

The Enterprise Manager Ops Center software can manage your virtual assets, such as Oracle Solaris Zones or Oracle VM Server for SPARC (logical domains). However, the software provides the most support to those zones and logical domains that are created using Enterprise Manager Ops Center actions.

Using Zones

When you use the Enterprise Manager Ops Center software's browser interface to create a zone, the software has full access to the zone configuration data and can manage the zone. This type of zone is called a greenfield zone. In contrast, any zone created using the `zonecfg` and `zoneadm` commands and later discovered by the Enterprise Manager Ops Center software are called brownfield zones; the product software is not aware of their zone configuration and can manage them in a limited way. Both types of zones are displayed in the product's Asset tree and are labeled by type. You can convert a brownfield zone to greenfield zone.

Do not mix the methods for administering zones. If you use both Enterprise Manager Ops Center actions and zone utility commands to administer zones, the Enterprise Ops Center software no longer recognizes the zone configuration and suspends its management of the zone.

Do not use the product software to create or manage zones if your site uses Live Upgrade to update operating systems of zones. Alternate boot environment (ABE) is not supported for greenfield zones.

Do not install a Proxy Controller in a non-global zone if you intend to use the product to provision operating systems or firmware.

You can install the Enterprise Controller software on a non-global zone but with these constraints:

- The non-global zone must be a whole root zone.
- The Proxy Controller cannot be located in the same zone.
- The Proxy Controller cannot be located in the global zone that supports the Enterprise Controller's non-global zone.
- No Agent software can be installed on the global zone that supports the Enterprise Controller's non-global zone.

Using Logical Domains

Use Oracle VM Server for SPARC to create multiple virtual machines on one physical hardware system. Unlike Oracle Solaris Zones that use the same operating system in all non-global zones, virtual machines can run instances of different operating systems, or different versions of the same operating system. These instances are called logical domains. Each logical domain has its own operating system, resources, and identity.

Although the Enterprise Manager Ops Center software can discover logical domains that were created using the `ldm(1M)` command and display them in the Assets tree, the product softare cannot manage them.

Do not install the Proxy Controller on a Linux system if you intend to provision logical domains. Use an Oracle Solaris x86 or SPARC system to run the Proxy Controller.

What Type of Network Configuration?

If you intend to provision OS or firmware on target systems on a subnet, configure one Proxy Controller on each subnet and then enable DHCP services on the Proxy Controller. Proxy Controllers provide the DHCP services that support the netboot or PXE boot operations of target systems.

Network Requirements

Use these guidelines to configure a network switch for a system running the Enterprise Manager Ops Center software.

- Use an 8-port or 16-port Virtual LAN (VLAN) switch.
- Discover and manage the switch.
- If your site uses VLAN, create a separate VLAN for management and provisioning networks.
- Disable spanning-tree protocols on the switch.

For Ethernet connectivity:

- The management network must be a 10/100 connection.
- The provisioning and data networks must be a 10/100/1000 (1 GB) connection.

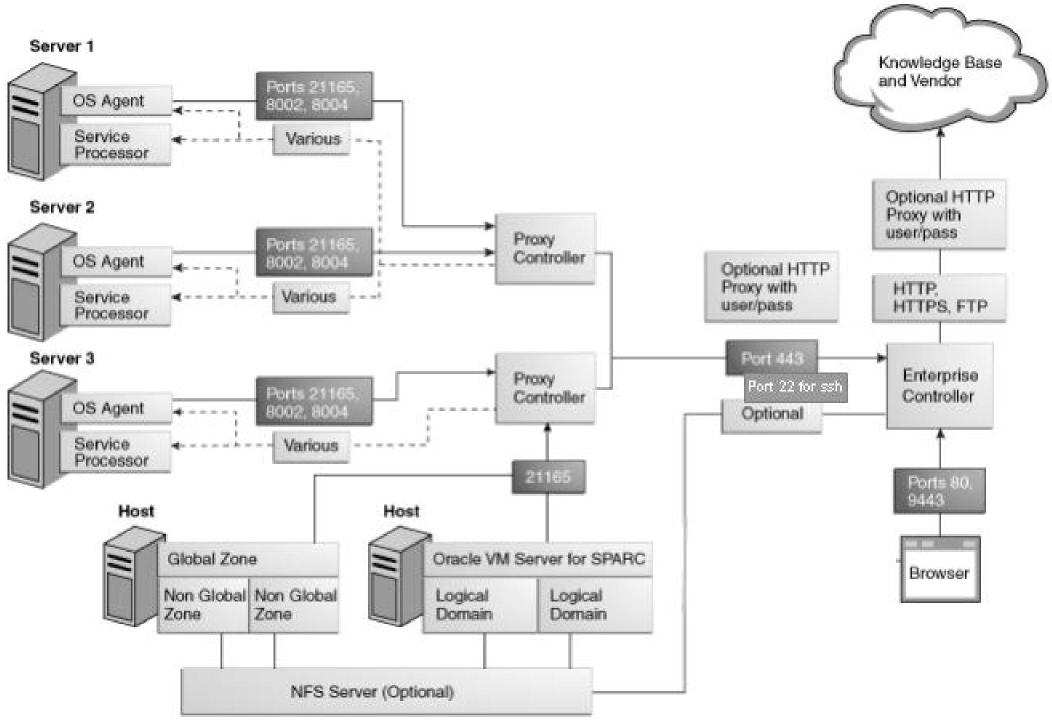
In Connected mode,the Enterprise Controller also needs to get access to vendor Web sites to download updates or other software.

The following sections describe the communication requirements for the Enterprise Manager Ops Center software.

Network Requirements and Data Flow

At least one Proxy Controller must be installed and configured. You use the co-located Proxy Controller installed with the Enterprise Controller software or install one or more Proxy Controllers on separate systems. The following diagram shows a network configuration for a site running the Enterprise Manager Ops Center software in Connected mode and with two Proxy Controllers.

Figure 1–3 Network Ports and Protocols for Enterprise Controller in Connected Mode



Ports and Protocols

The Enterprise Controller's default port is 443. If port 443 is in use, the Enterprise Controller uses Port 11165. The following table describes the required ports and their protocols.

Table 1–1 Required Ports and Protocols

Communication	Protocol and Port	Purpose
Browser to Enterprise Controller	HTTPS, TCP 9443	Web interface
Browser to Enterprise Controller	HTTP, TCP 80	Redirects to port 9443
Proxy Controller to Enterprise Controller	HTTPS, TCP 443	Proxy Controller pushes asset data to Enterprise Controller. Proxy Controller pulls data for jobs, updates, agents, and OS images.
Proxy Controller to Targets	FTP, TCP: Port 21 SSH, TCP: Port 22 Telnet, TCP: Port 23 DHCP, UDP: Ports 67, 68 SNMP, UDP: Ports 161, 162 IPMI, TCP+UDP: Port 623 Service Tags, TCP: Port 6481 ICMP ping: no port	Discovery, bare-metal provisioning, management, and monitoring. For ICMP, proxy controllers send an echo request ping (Type 8) and receive either an echo reply ping (Type 0) or destination unreachable (Type 3).
Enterprise Controller to Proxy Controller	SSH: Port 22	During Proxy Controller installation or updates performed through the UI.
Agent to Proxy Controller	HTTPS, TCP: Port 21165	Agents push asset data to Proxy Controller. Agents pull data for jobs.
Agent to Proxy Controller	HTTPS, TCP: Port 8002	Agents pull updates from Proxy Controller.
OS to Proxy Controller	HTTP, TCP: Port 8004	OS provisioning job's completion status Linux OS provisioning Download of the agent archive file. Upload of the status messages about failed agent installations
Java client to public APIs	Transport Layer Security(TLS): Port 11172	JMX access from clients
WMI to agent	Port 11162	Communication to agent on Windows targets
Proxy Controller to NFS server	Port 2049 (default) See operating system documentation for configuring NFS	Proxy Controller pulls provisioning images.
Enterprise Controller	Port 8005	Enterprise Controller in Disconnected mode

Examples of Network Configurations

This section provides the example configurations and connectivity information for Enterprise Manager Ops Center. Other configurations are possible, such as using separate switches for each network. You can implement your network using any combination of VLANs and switches. Each network, whether management, provisioning, or data, must be assigned to separate VLANs.

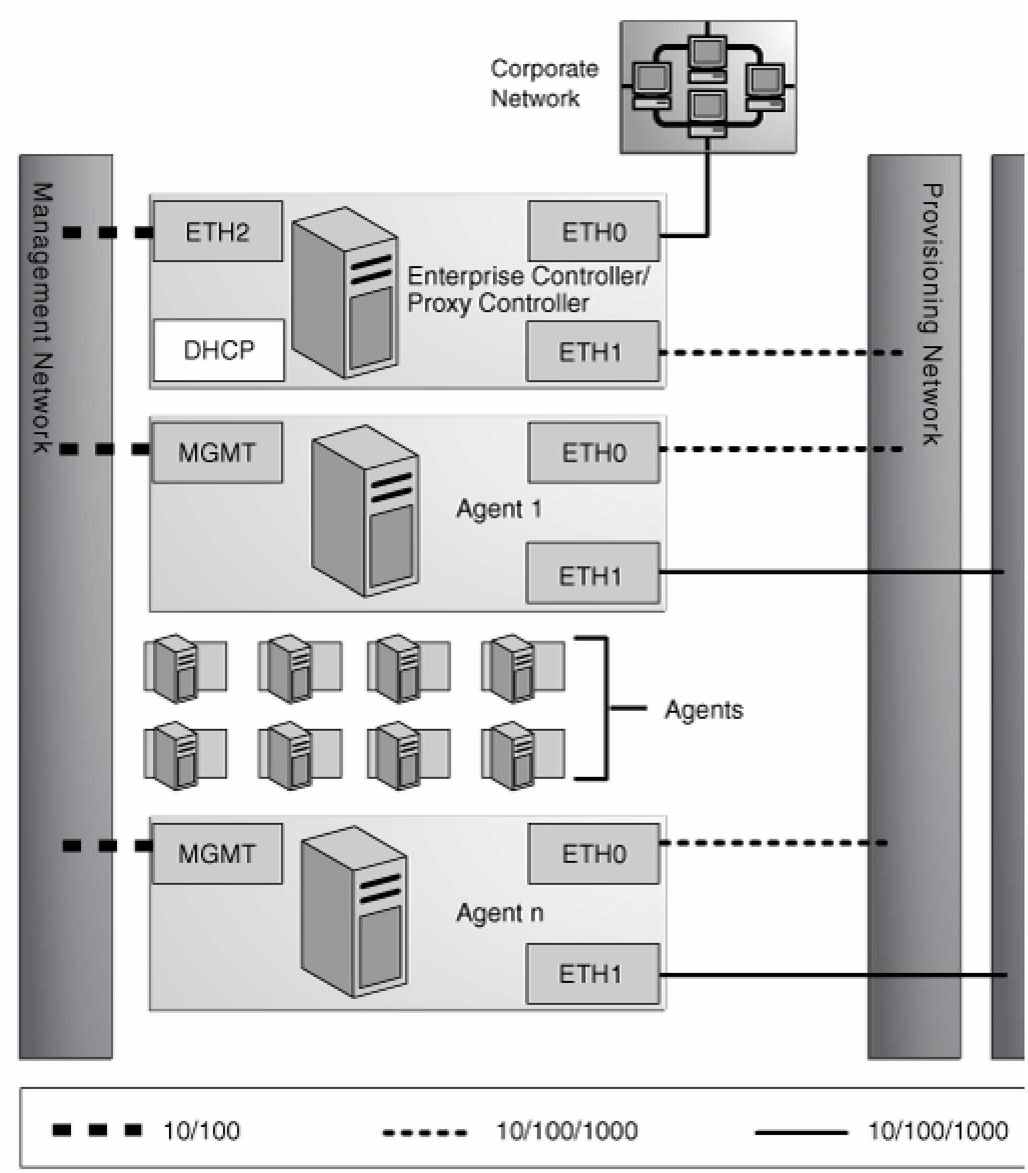
- Separate Management, Provisioning, and Data Networks
- Combined Management and Provisioning Network and a Separate Data Network
- Combined Provisioning and Data Network and a Separate Management Network

- Combined Provisioning, Data, and Management Network

Separate Management, Provisioning, and Data Networks

- Separate networks provide the highest security and the lowest number of points of failure.
- Additional NICs are needed to support this configuration.

Figure 1–4 Separate Management, Provisioning, Data Networks



A configuration with separate management, provisioning, and data networks has the following requirements:

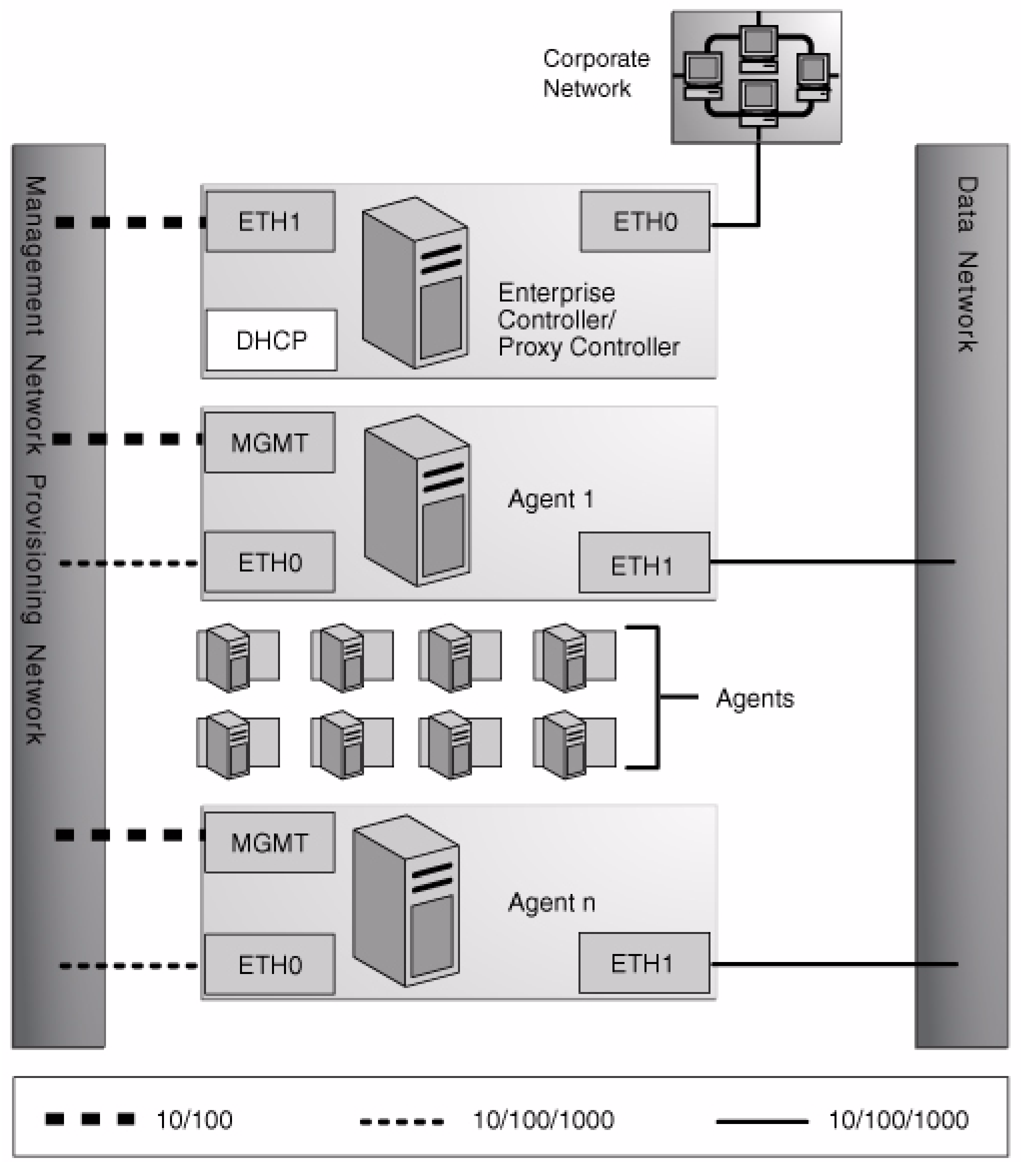
- Enterprise Controller or Proxy Controller
  - ETH0 connects the Enterprise Controller/Proxy Controller to the corporate network for external access. Configure the ETH0 IP address, netmask, and gateway to meet corporate connectivity requirements.

  - ETH1 connects the Enterprise Controller/Proxy Controller to the provisioning network and must be on the same network as the ETH0 connections of the agents. Only the Enterprise Controller/Proxy Controller and the agents must reside on the provisioning network. ETH1 must be a 1 Gb NIC interface.
  - ETH2 connects the Enterprise Controller/Proxy Controller to the management network and must be on the same network as the management port connections of the agents. Configure the ETH2 IP address, netmask, and gateway to enable connectivity to the agents' management port IP addresses. ETH2 must be a 100 Mb NIC interface.
  - The DHCP service allocates IP addresses to the agents for loading operating systems.
- Agents
  - Each agent's management port connects the agent to the management network and must be on the same network as the ETH2 connection of the Enterprise Controller/Proxy Controller. The management port must be a 100 Mb connection.
  - ETH0 connects the agent to the provisioning network and must be on the same network as the ETH1 connection of the Enterprise Controller/Proxy Controller. ETH0 must be a 1 GB connection.
  - ETH1 connects the agent to the data network through the switch to provide corporate network access to the agent. ETH1 must be a 1 GB connection.

Combined Management and Provisioning Network and a Separate Data Network

- Reduced system and network security.
- No additional NIC is needed on the Enterprise Controller or Proxy Controller.

Figure 1–5 Separate Data Network

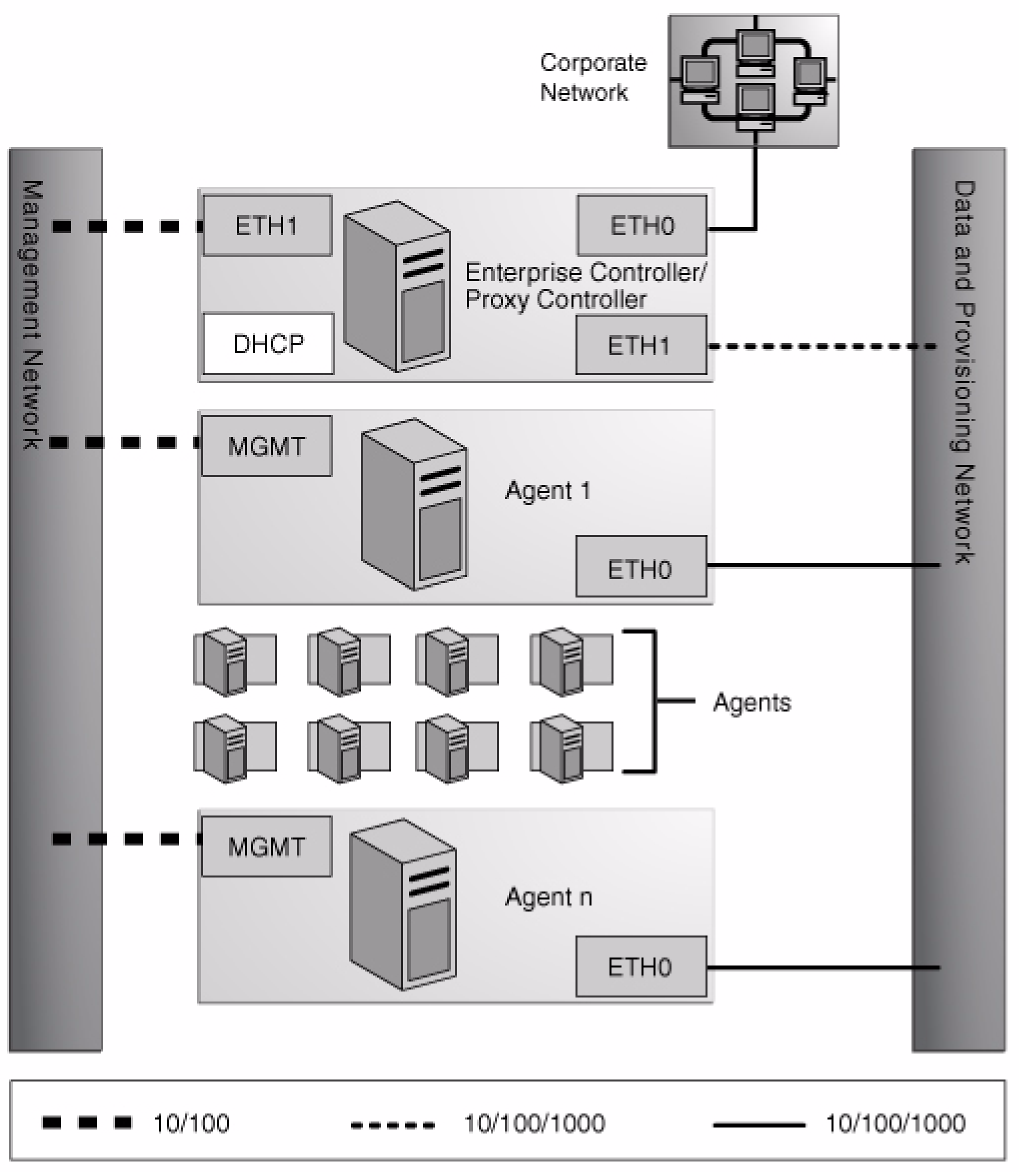


- Enterprise Controller/Proxy Controller
  - ETH0 connects the Enterprise Controller/Proxy Controller to the corporate network to provide external access. Configure the ETH0 IP address, netmask, and gateway to meet corporate connectivity requirements.
  - ETH1 connects the Enterprise Controller/Proxy Controller to the management and provisioning network and must be on the same network as the MGMT and ETH0 connections of the agents. Only the Enterprise Controller/Proxy Controller and the agents must reside on the management and provisioning network. The ETH1 IP address, netmask, and gateway must be configured to enable connectivity to the agent's management port IP addresses. ETH1 must be a 1 Gb NIC interface.
  - The DHCP service allocates IP addresses to the agents for loading operating systems.

- Agents
  - Each agent's management port connects the agent to the management and provisioning network and must be on the same network as the ETH1 connection of the Enterprise Controller/Proxy Controller. The management port must be a 100 Mb connection.
  - ETH0 connects the agent to the management and provisioning network and must be on the same network as the ETH1 connection of the Enterprise Controller/Proxy Controller. ETH0 must be a 1 GB connection.
  - ETH1 connects the agent to the data network through the switch to provide corporate network access to the agent. ETH1 must be a 1-GB connection.

Combined Provisioning and Data Network and a Separate Management Network

Figure 1–6 Separate Management Network

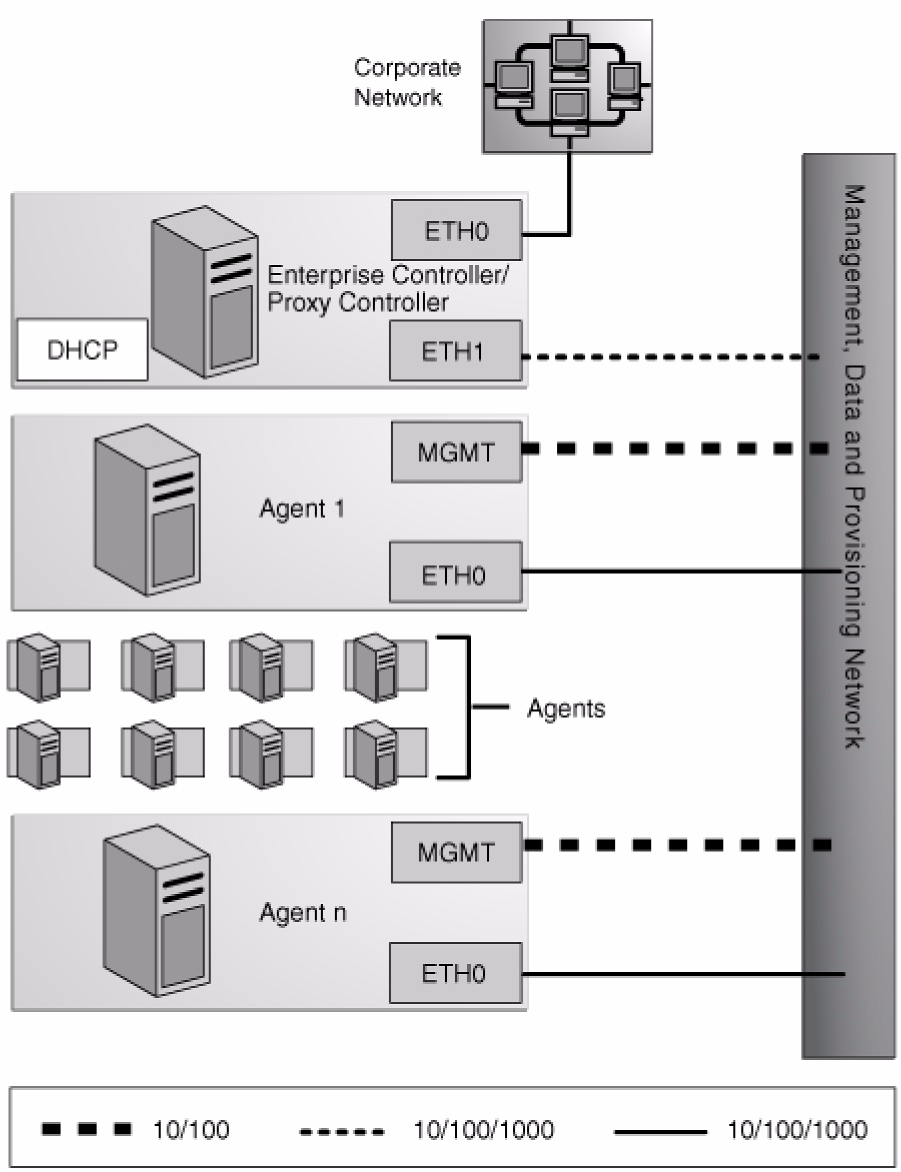


- Enterprise Controller/Proxy Controller
  - ETH0 connects the Enterprise Controller/Proxy Controller to the corporate network to provide external access. Configure the ETH0 IP address, netmask, and gateway to meet corporate connectivity requirements.
  - ETH1 connects the Enterprise Controller/Proxy Controller to the provisioning and data network and must be on the same network as the ETH0 connections of the agents. Only the Enterprise Controller/Proxy Controller and the agents must reside on the data and provisioning network. ETH1 must be a 1 Gb NIC interface.
  - ETH2 connects the Enterprise Controller/Proxy Controller to the management network and must be on the same network as the management port connections of the agents. Configure the ETH2 IP address, netmask, and gateway to enable connectivity to the agent's management port IP addresses. ETH2 must be a 100 Mb NIC interface.
  - The DHCP service allocates IP addresses to the agents for loading operating systems.
- Agents
  - The management port connects the agent to the management network and must be on the same network as the ETH2 connection of the Enterprise Controller/Proxy Controller. The management port must be a 100 Mb connection.
  - ETH0 connects the agent to the data and provisioning network to provide corporate network access to the agent. ETH0 connection must be on the same network as the ETH1 connection of the Enterprise Controller/Proxy Controller. ETH0 must be a 1 GB connection.

Combined Provisioning, Data, and Management Network

- Least secure system and network
- No additional NIC is needed for the Enterprise Controller/Proxy Controller.

Figure 1–7 Combined Networks



- Enterprise Controller/Proxy Controller
  - ETH0 connects the Enterprise Controller/Proxy Controller to the corporate network to provide external access. Configure the ETH0 IP address, netmask, and gateway to meet corporate connectivity requirements.
  - ETH1 connects the Enterprise Controller/Proxy Controller to the combined management, provisioning, and data network and must be on the same network as the MGMT and ETH0 connections of the agents. Only the Enterprise Controller/Proxy Controller and the agents must reside on the combined network. ETH1 must be a 1 GB NIC interface.
  - The DHCP service allocates IP addresses to the agents for loading operating systems.
- Agents

- Each agent's management port connects the agent to the management, provisioning, and data network and must be on the same network as the ETH1 connection of the Enterprise Controller/Proxy Controller. The management port must be a 100 MB connection.
- ETH0 connects the agent to the management, provisioning, and data network, and must be on the same network as the ETH1 connection of the Enterprise Controller/Proxy Controller. ETH0 also connects the agent to the data network through the switch to provide external corporate network access to the agent. ETH0 must be a 1 GB connection.

Does Your Site Require High Availability?

The design for a High Availability (HA) architecture must consider all single points of failure, such as power, storage, and network connectivity in addition to the product software.

High Availability for the Enterprise Controller

For the Enterprise Manager Ops Center environment, high availability applies only to the Enterprise Controller and its co-located Proxy Controller. To avoid a single point of failure in the Enterprise Manager Ops Center software, transfer the `/var/opt/sun/xvm` directory structure manually from the primary Enterprise Controller to a secondary Enterprise Controller. The secondary Enterprise Controller duplicates the primary Enterprise Controller's configuration and takes over much of the primary Enterprise Controller's identity, including its host name, its IP addresses, its ssh keys, and its role. Only one Enterprise Controller, either primary or secondary, can be operational at any time.

In a high-availability configuration, the primary Enterprise Controller is configured and operational. The secondary Enterprise Controller is not configured and not operational. On the primary Enterprise Controller, the `habackup` program saves the data in the `/var/opt/sun/xvm` directory structure. The data that is saved by the `habackup` program is used by the `harestore` program on the secondary Enterprise Controller to duplicate how the primary Enterprise Controller is configured. The `habackup` program also backs up the local `/etc/passwd` file. The `harestore` program uses that information to change the ownership of the files to match the secondary Enterprise Controller's `/etc/passwd` file. However, root user passwords on Enterprise Controllers are not changed.

Requirements for High Availability

- Use two systems of the same model and configured identically:
  - Processor class
  - Operating system
  - Oracle Enterprise Manager Ops Center software version, including updates
  - Network interfaces that are cabled identically to the same subnets
- Add an asset tag to identify the primary Enterprise Controller and to distinguish it from the secondary Enterprise Controller. You can add a tag by using the Edit Asset action.
- Maintain the secondary Enterprise Controller's system in the same way as the primary Enterprise Controller. The primary and secondary Enterprise Controllers must use the same version of Enterprise Manager Ops Center software. If you

cannot use the Enterprise Manager Ops Center's user interface to verify the installed software versions at the time that you need to transfer functions to the secondary system, view the content of the `/n1gc-setup/.version.properties` file. The `product.version` property lists the specific revision of the installed software. For example:

```
# cat /n1gc-setup/.version.properties
#Note: This file is created at build time.
#Wed Jun 30 15:28:45 PDT 2010
version=dev-ga
date=2010/06/30 15\:28
build.variation=xvmopscenter
product.version=2.6.0.1395
product.installLocation=/var/opt/sun/xvm/EnterpriseController_installer_
2.6.0.1395
```

Verify that the product.version property lists the same version on the primary and secondary Enterprise Controllers before you perform a failover procedure.

Limitations

- User accounts and data that are not associated with Oracle Enterprise Manager Ops Center are not part of the failover process. Only Oracle Enterprise Manager Ops Center data is moved between the primary and secondary Enterprise Controllers.
- UI sessions are lost on failover.
- The HA configuration applies only to the Enterprise Controller and its co-located Proxy Controller and not to other standalone Proxy Controllers.

High Availability for Storage Resources

You must configure the `/var/opt/sun/xvm` directory structure on a storage resource that you can move easily between the primary and secondary Enterprise Controllers. Consider dual-ported or SAN storage.

> **Note:** Configure the transferable storage on the system that you intend to use as the primary Enterprise Controller before you install the Enterprise Manager Ops Center software on that system.

Storage devices that you use in an HA configuration must meet these requirements:

- Storage must offer data redundancy capability, such as mirroring or RAID 5.
- Storage must be transferable between the primary and secondary Enterprise Controller systems.
- Storage must offer performance that is sufficient to support operations.
- Storage must have the capacity to hold the data that the Enterprise Manager Ops Center software stores in the `/var/opt/sun/xvm` directory structure.

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

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

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

How Will You Use Enterprise Manager Ops Center?

The Enterprise Manager Ops Center software provides management for hardware, operating systems, firmware and OS updates, for both physical and virtual assets. The number of types of assets, the total number of assets, and the methods you use to manage the assets all affect resource utilization.

Although the Enterprise Controller and the Proxy Controller can run on the same server, this is recommended only for a small-scale site. In most cases, your site benefits from running the Proxy Controller on a separate system. At large-scale sites, deploy a Proxy Controller on each subnet.

Hardware Management

To monitor and manage hardware, the Proxy Controller discovers assets and then polls each asset for status and configuration changes. The Proxy Controller initiates network sessions to the hardtware's systems management Ethernet port, using specific server and chassis-type protocols. Using the product software to manage only hardware assets has a low resource impact on the system running the product software. However, network traffic from the Proxy Controller to the assets can have a high impact. Make sure Proxy Controllers are scaled appropriately.

Hardware Management + OS Provisioning

OS provisioning is executed from the Proxy Controller. The number of OS provisioning jobs that can occur in parallel is metered by the job management system, but OS provisioning also creates a load on the Proxy Controllers and network. Configure a Proxy Controller on each subnet to provision the assets on that subnet. In addition, configure an NFS server close to the Proxy Controllers to store the OS images and firmware images.

Hardware Management + OS Provisioning + Update Management

To update an OS, an agent must be deployed on the operating system and both update and provisioning jobs must be completed. The jobs include several transactions to determine the operating system's required updates and to perform the update operation. These operations increase the network utilization of the Enterprise Controller and Proxy Controllers.

Hardware Management + OS Provisioning + Update Management + Virtualization Management

The assets running Oracle Solaris 10 that you can manage include virtual hosts such as Oracle Solaris Zones and Oracle VM Server for SPARC (Sun Logical Domains.) Managing these virtual hosts exposes significantly large operating system metrics and increases the memory utilization of the Enterprise and Proxy Controllers. For information about deployment considerations and scaling guidelines, contact your Oracle representative.

What Are the System Requirements?

For the current list of hardware, operating systems, and browsers that Enterprise Manager Ops Center supports, see Supported Systems in the *Enterprise Manager Ops Center Reference Guide*.

Cache Requirements

The Enterprise Manager Ops Center software uses a central file cache for the following types of content:

- For provisioning hardware or an OS:
  - Firmware
  - OS Images
- For updating assets:
  - Knowledge Base metadata that specifies the updates for an OS distribution
  - Packages, patches, and RPM files that are a standard part of an OS update distribution
  - Custom content for a site such as software bundles, configuration files, or scripts.

The product software propagates content from the cache. For example, a Proxy Controller downloads content from the Enterprise Controller, and an agent downloads content from the Proxy Controller. After content is cached, it can be re-used without additional download operations.

Cache Recommendations for Connected Mode Configurations

The minimum cache size is 74 GB on Enterprise Controllers and Proxy Controllers. Increase the minimum cache size based on the following guidelines:

- 2 GB for software installation (in `/opt` and `/var/tmp`)
- 4 GB for each OS image used for provisioning
- 10 GB for each distribution for updates

Because agents store only update content for their OS instance, they have reduced caching requirements. Allow 2 GB for both the product software and the update cache.

Example 1–1 Updating Several Operating System Assets

A user runs a job which updates five Oracle Solaris 10 SPARC OS agents managed by a single Proxy Controller. The Proxy Controller downloads and caches all of the patches required by the agents. Each agent downloads and caches the patches it requires. If an agent has cached several updates already, it re-uses those updates and downloads only what it needs from the Proxy Controller.

Example 1–2 Provisioning an Operating System Asset on Several Servers

A user runs a job to provision an OS image to three systems which are managed by two Proxy Controllers. Each Proxy Controller downloads and caches the image. The three systems do not cache the OS image, because they download and install the images from their respective Proxy Controllers.

The installations can use the co-located Proxy Controller, installed on the same OS instance as the Enterprise Controller. The Proxy and Enterprise Controllers share a global file cache so no additional disk space is required for the Proxy Controller's cache.

Example 1–3 Provision and Update Different Operating Systems on Several Servers

A site uses an Enterprise Controller with a co-located Proxy Controller and one other Proxy Controller, which together do the following:

- Provision Oracle Solaris 10 X86 and SPARC (update 6) and Oracle Linux 5.5, using one ISO image for each distribution.
- Update the Oracle Solaris 10 X86, Oracle Solaris 10 SPARC and Oracle Linux 5 32-bit X86 distributions. The remote Proxy Controller provisions and updates Oracle Solaris 10 systems on both SPARC and X86 architectures.

Both the Enterprise Controller with its co-located Proxy Controller and the remote Proxy Controller need a cache size of 74 GB, with 2 GB in `/var/tmp` and `/opt`, and 72 GB in `/var/opt/sun/xvm`. No additional caching is required on the Enterprise Controller because the co-located Proxy Controller shares its cache. The Enterprise Controller must have a minimum cache size of 44 GB:

- 30 GB for the three OS update distributions in `/var/opt/sun/xvm`
- 12 GB for the three OS images in `/var/opt/sun/xvm`
- 2 GB for the product software in `/var/tmp` and `/opt`

The remote Proxy Controller must have a minimum cache of 30 GB:

- 20 GB for the two Oracle Solaris OS update distributions in `/var/opt/sun/xvm`
- 8 GB for the two Oracle Solaris OS images in `/var/opt/sun/xvm`
- 2 GB for the Ops Center software in `/var/tmp` and `/opt`

Cache Requirements for Disconnected Mode Configurations

In Disconnected mode, the Enterprise Manager Ops Center software performs without an Internet connection. Images are managed in the same way as in Connected mode except it is not possible to download Oracle Solaris OS images. Administrators must cache images manually. For OS updates content, administrators must obtain and upload the content:

- The Knowledge Base content is available as an archive file, which users can obtain by running the `harvester` script. Depending on the settings, users can download the KB content only, or they can obtain content for one or more Oracle Solaris baselines.
- Patches, packages, or RPMs must be uploaded to the Enterprise Controller.

Proxy Controllers and agents function the same way in both Connected and Disconnected modes and their cache requirements are the same.

Oracle VM Server for SPARC Requirements

To use Oracle VM Server for SPARC software, the target servers must meet the following requirements.

Hardware Requirements

See Supported Systems in the *Enterprise Manager Ops Center Reference Guide* for specific hardware requirements for the following servers:

- Oracle SPARC T3-1 Server with Oracle VM Server for SPARC 2.0 software

- UltraSPARC T2 Plus based servers
- UltraSPARC T2 based servers
- UltraSPARC T1 based servers only with versions of the Logical Domains software earlier than Version 1.3.

OS Requirements

- Control domain – At least Oracle Solaris 10 10/09
- Logical domain – At least Oracle Solaris 10 5/08

The operating system on all domains must be at least Oracle Solaris 10 9/10 OS.

OS Patch Requirements

- Oracle Solaris 10 5/09: 141778-02 and 139983-04
- Oracle Solaris 10 10/08: 139555-08
- Oracle Solaris 10 5/08: 139555-08

For Oracle VM Server for SPARC 2.0 version, the following patches need to be installed on systems running an OS version earlier than Oracle Solaris 10 9/10:

- Control domain: 141514-02
- Control domain and logical domain: 142909-17

Firmware Requirements

The firmware requirements depend on the hardware that is used for Oracle VM Server for SPARC. The first release of firmware to include Oracle VM Server for SPARC support is System Firmware Version 6.4.x. To enable all the features of Oracle VM Server for SPARC 2.0, the minimum firmware version is 8.0.0.

The following system firmware patches are required:

- For System Firmware Version 6.7.4:
  - Use 139434-03 for Sun Fire and SPARC Enterprise T2000 Servers
  - Use 139435-03 for Sun Fire and SPARC Enterprise T1000 Servers
  - Use 139436-02 for Netra T2000 Server
  - Use 139437-02 for Netra CP3060 ATCA Blade
  - Use 139438-03 for Sun Blade T6300 Server Module
- For System Firmware Version 7.7.2:
  - Use 139439-04 for Sun SPARC Enterprise T5120 and T5220 Servers
  - Use 139440-03 for Sun Blade T6320 Server Module
  - Use 139442-06 for Netra T5220 Server
  - Use 139441 for Sun Netra CP3260 ATCA Blade Server
  - Use 139444-03 for Sun SPARC Enterprise T5140 and T5240 Servers
  - Use 139445-04 for Netra T5440 Server
  - Use 139446-03 for Sun SPARC Enterprise T5440 Server
  - Use 139448-02 for Sun Blade T6340 Server Module

Proxy Controller Requirements

Oracle VM Server provisioning is supported on Proxy Controllers running Solaris SPARC or Solaris x86. The Proxy Controller must be same one used during provisioning.

If the Proxy Controller is remote, the Enterprise Controller can run the Linux or Oracle Solaris OS. If the Proxy Controller is co-located, the Enterprise Controller and co-located Proxy Controller must run on an Oracle Solaris OS.

Oracle Solaris Zones Requirements

Oracle Solaris 10 systems that have non-global zones must have at least the following patches:

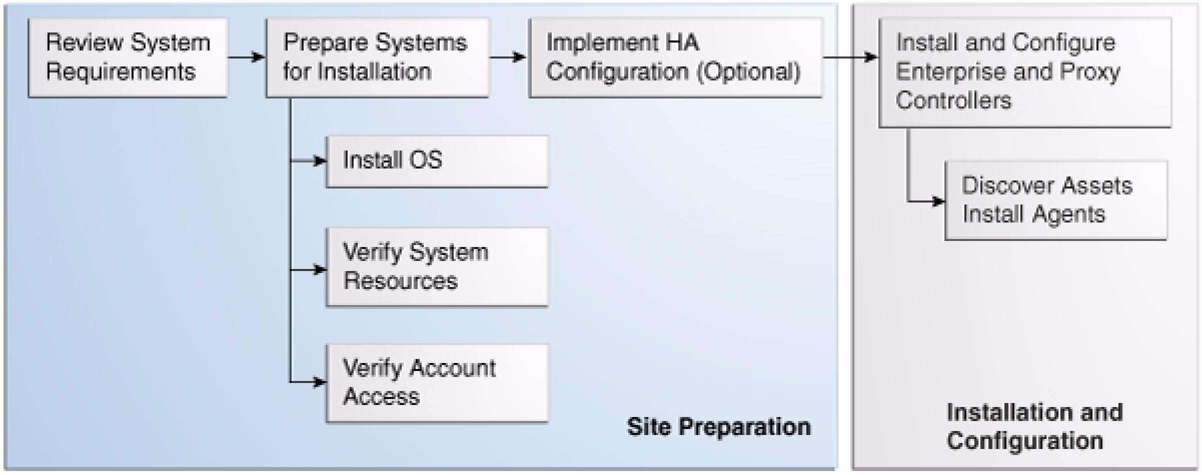
- For SPARC systems:
  - 124630-03: System Administration Applications, Network, and Core
  - 122660-07: Zones patch, obsoleted by Solaris 10 8/07 kernel patch 120011-14
- For x86 systems:
  - 124631-03: System Administration Applications, Network, and Core
  - 122661-07: Zones patch, obsoleted by Solaris 10 8/07 kernel patch 120012-14

Patches 122660-07 and 122661-07 are included on systems that are running at least Solaris 10 8/07.

2 Getting Ready

At this point, the research and decisions you have made complete the Review System Requirements step in the following workflow and you can start to prepare your site and systems.

Figure 2–1 Process for Installing Enterprise Manager Ops Center


Review System Requirements
Prepare Systems for Installation
Implement HA Configuration (Optional)
Install and Configure Enterprise and Proxy Controllers
Install OS
Discover Assets Install Agents
Verify System Resources
Verify Account Access
Site Preparation
Installation and Configuration

The general procedure for preparation is summarized in this section and described in detail in the chapter:

1. Determine System Requirements
   - Determine how many Proxy Controllers your site requires.
   - Identify the servers to use for the Enterprise Controller and for the Proxy Controllers.
   - Determine which operating systems to install.
   - Determine which assets you will monitor and manage and, based on the total, determine your switch requirements.
2. Map Your Network
   - Determine the IP addressing scheme for the management, provisioning, and data networks.
   - Determine whether you will use a single-switch configuration or a two-switch configuration, in which the management network is isolated on one switch and the data and provisioning networks are on the second switch.

- Determine the VLAN assignments.
- Assign an IP address to the management port of each agent. For ILOM, ALOM, and SP-based agents, see the vendor documentation for information about assigning IP addresses to the server's management port.

3. Prepare the Systems
   - Install an operating system.
   - Verify system resources.
   - Verify resources needed for agent installation.
   - Verify accounts and access.

Preparing an Oracle Solaris System for Installation

The system that supports an Enterprise Controller or Proxy Controller requires an operating system that provides all of the resources that the Enterprise Manager Ops Center software requires.

The procedures in this topic describehow to verify that the required system resources exist. The requirements for agent installation and the procedures to verify required account access are also described.

Requirements for Installation on Oracle Solaris OS

The Enterprise Manager Ops Center software requires a full standard installation of the operating system, Oracle Solaris 10 11/06 for SPARC or x86 Systems. Install the OS using either of the following software groups:

- SUNWCXall - Entire Distribution with OEM Support
- SUNWCall - Entire Distribution

For information about installation procedures, see the Additional Resources.

> **Caution:** Do not minimize or harden the operating system until **after** you install the product software. For example, if you remove previously applied SUNWjass changes, the product software installation might fail.

Disk and Swap Space

The Enterprise Manager Ops Center software requires the following minimum values for disk and swap space:

- 2 GB free in `/opt`
- 70 GB free in `/var/opt/sun/xvm`
- 6 GB of swap space

Oracle Solaris Patch Level

To support the product's update capability, a system running Oracle Solaris 10 11/06 or earlier must have these minimum patch levels for specific patches:

- SPARC systems:
  - 125100-04: Kernel Update Patch

  - 120473-05: libc nss ldap PAM zfs Patch
  - 125800-01: Fault Manager Patch
- x86 systems:
  - 125101-04: Kernel Update Patch
  - 120037-15: libc nss ldap PAM zfs Patch
  - 125801-01: Fault Manager Patch

Use the Oracle Solaris `ls`command to verify that the `/usr/lib/extendedFILE.so.1` exists on the system.

Preparing a Non-Global Zone

On servers that run Oracle Solaris 10, you can install the Enterprise Controller in a non-global zone, with the following constraints:

- The non-global zone must be a whole root zone.
- You cannot use a co-located Proxy Controller.
- You cannot install a Proxy Controller or Agent software on the global zone that supports the Enterprise Controller's non-global zone.
- Images stored on an NFS-mounted file system cannot be mounted on the Enterprise Controller. You must configure lofi devices as described in the following procedure. After configuring the devices, you can mount images that reside in the non-global zone.

Configuring the Non-Global Zone for the Enterprise Controller

1. Shut down the non-global zone.

   ```
   root@globalzone# zlogin localzone shutdown -i5 -g0 -y
   ```

2. Use the `zonecfg` command to enter zone configuration mode.

   ```
   root@globalzone# zonecfg -z localzone
   ```

3. Use the `add device` command to add the lofi devices.

   ```
   zonecfg:localzone> add device
   zonecfg:localzone:device> set match=/dev/lofictl
   zonecfg:localzone:device> end
   zonecfg:localzone> add device
   zonecfg:localzone:device> set match=/dev/lofi/*
   zonecfg:localzone:device> end
   zonecfg:localzone> add device
   zonecfg:localzone:device> set match=/dev/rlofi/*
   zonecfg:localzone:device> end
   zonecfg:localzone> exit
   ```

4. Boot the non-global zone.

   ```
   root@globalzone# zoneadm -z localzone boot
   ```

5. Log in to the non-global zone.

   ```
   root@globalzone# zlogin localzone
   [Connected to zone 'localzone' pts/2]
   Last login: Mon Sep 14 12:21:34 on pts/2
   root@localzone#
   ```

6. Use the `lofiadm`a nd `mount` commands to verify that you can create and mount lofi devices.

   ```
   root@localzone# lofiadm -a /root/sampleISO.iso
   /dev/lofi/1
   root@localzone# mount -F hsfs /dev/lofi/1 /mnt
   root@localzone# ls /mnt
   textfile.txt example.bin sampledir/
   root@localzone#
   ```

Verifying System Resources on Oracle Solaris

The Enterprise Manapter Ops Center provides the OC Doctor utility. This utility's pre-installation option checks requirements and identifies issues. If you prefer to check your systems manually, log in as the root user on the system on which you intend to install the Enterprise Controller or Proxy Controller software and use the information in this section. To keep track of your progress, use the checklist in Appendix A.

To Check the Operating System Release

The Enterprise Manager Ops Center software requires at least Oracle Solaris 10 11/06 for SPARC or x86 systems. To check the release, use the following command to display the `/etc/release` file:

```
# cat /etc/release
Solaris 10 5/09 s10x_u7wos_08 X86
Copyright 2009 Sun Microsystems, Inc. All Rights Reserved.
Use is subject to license terms.
Assembled 30 March 2009
```

To Check the Installed Software Group

The Enterprise Manager Ops Center software requires that the Oracle Solaris OS was installed with one of these software groups:

- SUNWCXall - Entire distribution with OEM support
- SUNWCall - Entire distribution

To check the installed software group, use the following command to display the `/var/sadm/system/admin/CLUSTER` file:

```
# cat /var/sadm/system/admin/CLUSTER
CLUSTER=SUNWCall
```

To Check the Zone Identity

The Enterprise Controller can be installed in a non-global zone or the global zone. Use the following command to check the current zone:

```
# zonename
global
```

To Check the Available Disk Space

The Enterprise Manager Ops Center software requires 2 GB of space in`/opt` and 70 GB of space in `/var/opt/sun/xvm`. Use the following command to display the space utilization, and verify that you have at least 70 GB available within the file system that will hold the `/var/opt/sun/xvm` directory structure. In this example, the `/opt` and `/var/opt/sun/xvm` directories are located within the root (/) file system, which has 78 GB of space available.

```
# df -h
Filesystem size used avail capacity Mounted on
/dev/dsk/c1t0d0s0 82G 4.0G 78G 5% /
/devices 0K 0K 0K 0% /devices
ctfs 0K 0K 0K 0% /system/contract
proc 0K 0K 0K 0% /proc
mnttab 0K 0K 0K 0% /etc/mnttab
swap 5.1G 624K 5.1G 1% /etc/svc/volatile
(output omitted)
```

To Check Swap Space

An Enterprise Controller requires 6 GB of configured swap space and Proxy Controllers require at lease 4 GB of configured swap space. Use the following command to display the amount of configured swap space:

```
# swap -l
swapfile dev swaplo blocks free
/dev/dsk/c1t0d0s1 118,1 16 8395184 8395184
```

The values in the blocks and free columns are expressed in 512-byte blocks.

To Verify the Amount of System Memory

An Enterprise Controller requires at least 6 GB of installed memory and each Proxy Controller requires at least 4 GB. Use the following command to display the amount of installed memory on your system:

```
# prtconf | grep -i meg
Memory size: 4096 Megabytes
```

To Verify the Amount of Shared Memory

An Enterprise Controller requires at least 500 MB of shared memory. Use the following command to display the amount of shared memory on your system:

```
# prctl -n project.max-shm-memory -i project 1
project: 1: user.root
NAME PRIVILEGE VALUE FLAG ACTION RECIPIENT
project.max-shm-memory
privileged 1.97GB - deny -
system 16.0EB max deny -
```

If the privileged value is less than 500 MB, use the following command to set it to 500 MB.

```
# projmod -a -K "project.max-shm-memory=(priv,500mb,deny)" default
```

To Verify the webservd User and Group

The Oracle Solaris 10 OS creates the `webservd` user and group. Use the following commands to search the `/etc/passwd`, `/etc/shadow`, and `/etc/group` files to confirm that the `webservd` user and group exist:

```
# grep webservd /etc/passwd
webservd:x:80:80:WebServer Reserved UID:/:
# grep webservd /etc/shadow
webservd:*LK*:::::::
# grep webservd /etc/group
webservd::80:
```

If the webservd user or group does not exist, use the User ID (UID) and Group ID (GID) values in the example to create it.

To Verify an Alternate Administrative User

To designate a user other than root as the administrative user, you must create the user account before you install the product software. This example verifies that the user droot exists as an administrative user:

```
# logins -l droot
droot 0 root 0 Super-User
```

Reviewing Users and Groups

Product installation creates users and groups on the Enterprise Controller and Proxy Controllers. Review the following list of users and groups, and verify that they do not conflict with existing policies. If required by account management policies, add these users and groups before you install the software.

- Enterprise Controller Users: svctag, allstart, scndb, scn, scncon, uce-sds, xvm
- Enterprise Controller Groups: jet, scndb, uce-sds
- Proxy Controller Users: svctag, allstart, uce-sds
- Proxy Controller Groups: jet, uce-sds

The product software creates these users and groups with the following UID and GID values:

```
# cat /etc/group
(output omitted)
uce-sds::98194050:
scndb::98194051:
jet::98194052:
#
# cat /etc/passwd
(output omitted)
svctag:x:95:12:Service Tag UID:/:
scn:x:231796:3::/:/bin/sh
xvm:x:60:60::/:/bin/sh
scncon:x:231798:1::/:/bin/true
uce-sds:x:231799:98194050:UCE Engine:/opt/SUNWuce/server:/bin/sh
scndb:x:231800:98194051:SCS PostgreSQL User:/opt/SUNWscs:/bin/sh
allstart:x:231801:1:AllStart User:/var/opt/sun/xvm/osp/data:/bin/sh
```

All user accounts have locked (*LK*) passwords, except the scncon user. A password is required for the scncon user, but it has no login shell. To create the scncon user before installing the software, edit the /var/opt/sun/xvm/persistence/scn-satellite/satellite.properties file and add the password, in clear text, with the scncon.password parameter. For example:

```
scncon.password=2EzafaJE
```

To Verify the umask Value

Verify that the umask for the root user or equivalent role is set to 0022. Different shells report this value differently. The following examples list output from the umask command for the Bourne shell, the Korn shell, and the C-shell. In all three examples, the umask value is correct.

```
# sh
# umask
0022
# ksh
# umask
022
# csh
# umask
22
```

To Verify the Locations of ssh Binaries

The binary files for ssh operations must be stored in their standard locations, even if OpenSSH is used. Verify that the following files have the following path names:

- /usr/bin/scp
- /usr/bin/ssh
- /usr/bin/ssh-keygen
- /usr/bin/ssh-keyscan

To Verify IP Address Resolution

Verify that the configured naming services resolve the correct IP address for the host name that is assigned to Enterprise Controller's system. For example:

```
# host system.domain
system.domain has address 192.21.26.1337
```

Verify that the /etc/hosts file contains the correct host name and IP address for the system. For example:

```
# grep system /etc/hosts
172.21.26.1337 system loghost
```

To Verify That /usr/local Is Writeable

Some software components of the product software are installed in the /usr/local directory. Verify that the directory is writeable, and is not a mounted remotely, or a read-only directory. For example:

```
# df -h /usr/local
Filesystem size used avail capacity Mounted on
/dev/dsk/c1t0d0s0 82G 4.0G 78G 5% /
# ls -ld /usr/local
drwxr-xr-x 7 root root 512 Feb 23 08:33 /usr/local
```

In this example, the directory is stored in the root (/) file system, and is writeable by the root user and group.

To Verify the Date and Time

Verify that the correct date and time are set on your system. For example:

```
# date
Thu Aug 21 08:31:59 MST 2010
```

To Verify Online cryptosvc and gss Services

The product software requires the the cryptosvc and gss SMF services are online. For example:

```
# svcs cryptosvc gss
```

```
STATE STIME FMRI
online Feb_25 svc:/system/cryptosvc:default
online Feb_25 svc:/network/rpc/gss:default
```

You can use the svcadm command to enable these services if they are not online.

To Remove the SMClintl Package

The SMClintl freeware package conflicts with the product software and must be removed. Use the following command to remove the SMClintl package before you install the software:

```
# pkgrm SMClintl
```

To Verify Network Access to Required Web Sites

Use a web browser to verify that your system can access the following URLs:

https://getupdates.oracle.com
https://a248.e.akamai.net
https://linux.oracle.com

For access to SUSE Linux updates, see http://support.novell.com/linux/registration/ to register your system and then verify you can get access to http://support.novell.com/patches.html.

Use the `wget` command to verify that you can download a sample file from the `getupdates.oracle.com` site.

1. If you use a proxy server to access the Internet, set the `https_proxy` environment variable to point to the proxy server:

   ```
   # export https_proxy="http://myproxy.company.com:8080"
   ```

   where *myproxy.company.com* is the fully-qualified domain name of your proxy server.

2. Download the sample file named `channels.xml` and save it locally as `/tmp/channels.xml`. The following example of the `wget` command show that the command is stored in `/usr/sfw/bin` on Oracle Solaris systems and uses these options:

   - **-O** - Specifies the name of the file to create on the local system
   - **--http-user** - Specifies the My Oracle Support account to use for authentication to `getupdates.oracle.com`
   - **--http-password** - Specifies the password for the My Oracle Support account
   - **--proxy-user** - (Optional) Specifies the user name used for authentication with an HTTPS proxy
   - **--proxy-password** - (Optional) Specifies the password for the user name that you provide for the --proxy-user option In this example, account@xyz.com and password represent the My Oracle Support credentials:

```
# /usr/sfw/bin/wget https://getupdates.oracle.com/channels3/channels.xml -O
/tmp/channels.xml --http-user="account@xyz.com" --http-password="password"
--11:43:41-- https://getupdates.oracle.com/channels3/channels.xml
=> `/tmp/channels.xml'
Resolving getupdates.oracle.com... 198.232.168.136
Connecting to getupdates.oracle.com|198.232.168.136|:443... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
```

```
Location:
https://a248.e.akamai.net/f/248/21808/15m/sun.download.akamai.com/21808/sc/channel
s3/channels.xml?AuthParam=1236019547_
e9120d30e1ac62650c8f9284dfe47663&TUrl=L0QdUQV8Z4i0fdED3QTP3SJDWA8FMyaJsHfIWf4X29kT
WQpKEzIbwqFuyRPZ&TicketId=3qfzk1SIPR9R&GroupName=SWUP&BHost=sdlc3h.sun.com&FilePat
h=/sc/channels3/channels.xml&File=channels.xml [following]
--11:43:42--
https://a248.e.akamai.net/f/248/21808/15m/sun.download.akamai.com/21808/sc/channel
s3/channels.xml?AuthParam=1236019547_
e9120d30e1ac62650c8f9284dfe47663&TUrl=L0QdUQV8Z4i0fdED3QTP3SJDWA8FMyaJsHfIWf4X29kT
WQpKEzIbwqFuyRPZ&TicketId=3qfzk1SIPR9R&GroupName=SWUP&BHost=sdlc3h.sun.com&FilePat
h=/sc/channels3/channels.xml&File=channels.xml
=> `/tmp/channels.xml'
Resolving a248.e.akamai.net... 208.51.221.73, 208.51.221.48
Connecting to a248.e.akamai.net|208.51.221.73|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 66,505 (65K) [application/xml]

100%[=============================================================================>
] 66,505 397.16K/s

11:43:42 (396.55 KB/s) - `/tmp/channels.xml' saved [66505/66505]
```

To Verify Network Port Access

See Ports and Protocols to verify that your systems allow using the required network services and ports.

To Verify ssh Access for the root User

If you intend to use root credentials to discover systems and install the agent, verify that the ssh daemon on your target systems is configured to allow root user logins. If you use a non-root user for ssh access, this configuration is not necessary.

To verify ssh access for the root user, use `ssh` to log in as root to the system. If the attempt succeeds, no further action is necessary. If the attempt fails, check the value of the PermitRootLogin parameter in the `/etc/ssh/sshd_config` file. If PermitRootLogin is set to `no`, edit the file to change the etting to `yes`. Then use the `svcadm` command to restart the `svc:/network/ssh:default` service. For example:

```
# svcadm restart svc:/network/ssh:default
```

Preparing a System for Installation on Linux

The system that supports an Enterprise Controller or Proxy Controller requires an operating system that provides all of the resources that the Enterprise Manager Ops Center software requires.

The procedures in this topic describe how to verify that the required system resources exist. The requirements for agent installation and the procedures to verify required account access are also described.

Requirements for Linux OS Installation

Product installation requires a full installation of Oracle Linux. When you install the operating system, install all optional software components in every software category except the Language category. Set the SELinux security setting to Disabled

Disk and Swap Space

- At least 70 GB of available disk space after the operating system has been installed
- At least 6 GB of swap space

Values for kernel.shmall and kernel.shmmax

If the `/etc/sysctl.conf` file has been modified, the values of kernel.shmall and kernel.shmmax might be too small, which will cause the product installation to fail. The following values are recommended:

- kernel.shmall: 268435456
- kernel.shmmax: 4294967295

Edit Kernel Settings

When you install Linux, the Xen kernel is set as the default kernel. Setting the standard kernel as the default kernel improves performance. Perform the following procedure on each system that will the Enterprise Controller and Proxy Controllers.

1. Edit the `/boot/grub/menu.lst` file.

   ```
   # vi /boot/grub/menu.lst
   ```
2. Set the value of default to 1.

   ```
   default=1
   ```
3. Save the file.
4. Shut down the system.

   ```
   # shutdown -r now
   ```
   The system now uses the standard kernel by default.

Verifying System Resources on Linux

The Enterprise Manapter Ops Center provides the OC Doctor utility. This utility's pre-installation option checks requirements and identifies issues. If you prefer to check your systems manually, log in as the root user on the system on which you intend to install the Enterprise Controller or Proxy Controller software and use the information in this section. To keep track of your progress, use the checklist in Appendix A.

To Check the Operating System Release

Verify that a release of the Linux OS that is compatible with product software is installed.   To check the release, use the following command to display the `/etc/redhat-release` file:

```
# cat /etc/redhat-release
```

To Verify That Required Packages Are Installed

The product software requires specific packages for installation on Linux systems:

- python-2.4.3
- expect-5.43.0
- perl-DBD-Pg
- xinetd
- tftp-server
- dhcp

- gettext
- perl-XML-Parser
- ncompress
- libxml2 (both the 64 bit and 32 bit RPMs are required)

Use the following command to verify that package is installed:

```
# rpm -q dhcp-3.0.5-3.el5
dhcp-3.0.5-3.el5
```

To Check the Available Disk Space

The Enterprise Manager Ops Center software requires 2 GB of space in`/opt` and 70 GB of space in `/var/opt/sun/xvm`. Use the following command to display the space utilization, and verify that you have at least 70 GB available within the file system that will hold the `/var/opt/sun/xvm` directory structure. In this example, the `/opt` and `/var/opt/sun/xvm` directories are located within the root (/) file system, which has 119 GB of space available.

```
# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
131G 5.7G 119G 5% /
/dev/sda1 99M 12M 83M 12% /boot
tmpfs 2.0G 0 2.0G 0% /dev/shm
```

To Verify the Amount of System Memory and Swap Space

You must have at least 6 GB of installed memory and swap space for Enterprise Controller installations and at least 4 GB of installed memory and swap space for Proxy Controller installations. Use the following command to display the amount of installed memory and swap space:

```
# free -m
total used free shared buffers cached
Mem: 3931 1389 2542 0 220 1053
-/+ buffers/cache: 115 3816
Swap: 4096 0 4096
```

The value in the total column indicates the amount of installed memory or configured swap space.

You can also use the `dmesg` command to display the amount of memory installed. For example:

```
# dmesg | grep Memory
Memory: 4022900k/4063168k available (2043k kernel code, 39036k reserved, 846k
data, 232k init, 3145664k highmem)
```

To Verify the SELinux Setting

If you have installed a Security Enhanced Linux OS (SELinux), disable this capability. To check the state of SELinux, either run the `sestatus` command or display the contents of the `/etc/selinux/config` file to verify that the `SELINUX` variable is set to `disabled`. For example:

```
# sestatus
SELinux status: disabled
#
# cat /etc/selinux/config
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
# enforcing - SELinux security policy is enforced.
# permissive - SELinux prints warnings instead of enforcing.
# disabled - SELinux is fully disabled.
SELINUX=disabled
# SELINUXTYPE= type of policy in use. Possible values are:
# targeted - Only targeted network daemons are protected.
# strict - Full SELinux protection.
SELINUXTYPE=targeted
```

If the `SELINUX` state is either `enforcing` or `permissive`, edit the `/etc/selinux/config` file and change the `SELINUX` value to `disabled`. After making this change, reboot your system for the change to take effect.

Users and Groups

Product installation creates users and groups on the Enterprise Controller and Proxy Controllers. Review the following list of users and groups, and verify that they do not conflict with existing policies. If required by account management policies, add these users and groups before you install the software.

- Enterprise Controller Users: `svctag, allstart, scndb, scn, scncon, uce-sds, xvm`
- Enterprise Controller Groups: `jet, scndb, uce-sds`
- Proxy Controller Users: `svctag, allstart, uce-sds`
- Proxy Controller Groups: `jet, uce-sds`

The product software creates these users and groups with the following UID and GID values:

```
# cat /etc/group
(output omitted)
uce-sds::98194050:
scndb::98194051:
jet::98194052:
#
# cat /etc/passwd
(output omitted)
svctag:x:95:12:Service Tag UID:/:
scn:x:231796:3::/:/bin/sh
xvm:x:60:60::/:/bin/sh
scncon:x:231798:1::/:/bin/true
uce-sds:x:231799:98194050:UCE Engine:/opt/SUNWuce/server:/bin/sh
scndb:x:231800:98194051:SCS PostgreSQL User:/opt/SUNWscs:/bin/sh
allstart:x:231801:1:AllStart User:/var/opt/sun/xvm/osp/data:/bin/sh
```

All user accounts have locked (*LK*) passwords, except the `scncon` user. A password is required for the `scncon` user, but it has no login shell. To create the `scncon` user before installing the software, edit the `/var/opt/sun/xvm/persistence/scn-satellite/satellite.properties` file and add the password, in clear text, with the `scncon.password` parameter. For example:

```
scncon.password=2EzafaJE
```

To Verify the umask Value

Verify that the umask in use for the root user or equivalent role is set to 022. Different shells report this value differently. The following examples list output from the umask command for the Bourne shell, the Korn shell, and the C Shell, and bash, in descending order. In all three examples, the umask value is correct.

```
# sh
# umask
0022
# ksh
# umask
0022
# csh
# umask
22
# bash
# umask
0022
```

Check the umask value set in `/etc/bashrc`. The umask value must be set to 022, even for non-root users. For example:

```
# grep umask /etc/bashrc
umask 002
umask 022
```

To Verify the Locations of ssh Binaries

The binary files for ssh operations must be stored in their standard locations, even if OpenSSH is used. Verify that the following files have the following path names:

- `/usr/bin/scp`
- `/usr/bin/ssh`
- `/usr/bin/ssh-keygen`
- `/usr/bin/ssh-keyscan`

To Verify IP Address Resolution

Verify that the configured naming services resolve the correct IP address for the host name that is assigned to your system. For example:

```
# host x4200-brm-13
x4200-brm-13.Central.Sun.COM has address 192.20.25.169
```

To Verify That /usr/local Is Writeable

Some product components are installed in the `/usr/local` directory. Verify that the directory is writeable, and is not mounted remotely, or a read-only directory. For example:

```
# df -h /usr/local
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
131G 5.7G 119G 5% /
# ls -ld /usr/local
drwxr-xr-x 11 root root 4096 Nov 30 2005 /usr/local
```

In this example, the `/usr/local` directory is stored in the root (/) file system and is writeable by the root user and group.

To Verify the Date and Time

Verify that the correct date and time are set on your system. For example:

```
# date
```

```
Thu Aug 21 08:31:59 MST 2010
```

If the date and time are not correct, reset them.

To Verify Network Access to Required Web Sites

Use a web browser to verify that your system can access the following URLs:

```
https://getupdates.oracle.com
https://a248.e.akamai.net
https://linux.oracle.com
```

For access to SUSE Linux updates, see `http://support.novell.com/linux/registration/` to register your system and then verify you can get access to `http://support.novell.com/patches.html`.

Use the `wget` command to verify that you can download a sample file from the `getupdates.oracle.com` site.

1. If you use a proxy server to access the Internet, set the `https_proxy` environment variable to point to the proxy server:

   ```
   # export https_proxy="http://myproxy.company.com:8080"
   ```

   where *myproxy.company.com* is the fully-qualified domain name of your proxy server.

2. Download the sample file named `channels.xml` and save it locally as `/tmp/channels.xml`. The following example of the `wget` command show that the command is stored in `/usr/sfw/bin` on Oracle Solaris systems and uses these options:

   - **-O** - Specifies the name of the file to create on the local system
   - **--http-user** - Specifies the My Oracle Support account to use for authentication to getupdates.oracle.com
   - **--http-password** - Specifies the password for the My Oracle Support account
   - **--proxy-user** - (Optional) Specifies the user name used for authentication with an HTTPS proxy
   - **--proxy-password** - (Optional) Specifies the password for the user name that you provide for the --proxy-user option In this example, account@xyz.com and password represent the My Oracle Support credentials:

```
# /usr/sfw/bin/wget https://getupdates.oracle.com/channels3/channels.xml -O
/tmp/channels.xml --http-user="account@xyz.com" --http-password="password"
--11:43:41-- https://getupdates.oracle.com/channels3/channels.xml
=> `/tmp/channels.xml'
Resolving getupdates.oracle.com... 198.232.168.136
Connecting to getupdates.oracle.com|198.232.168.136|:443... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location:
https://a248.e.akamai.net/f/248/21808/15m/sun.download.akamai.com/21808/sc/channel
s3/channels.xml?AuthParam=1236019547_
e9120d30e1ac62650c8f9284dfe47663&TUrl=L0QdUQV8Z4i0fdED3QTP3SJDWA8FMyaJsHfIWf4X29kT
WQpKEzIbwqFuyRPZ&TicketId=3qfzk1SIPR9R&GroupName=SWUP&BHost=sdlc3h.sun.com&FilePat
h=/sc/channels3/channels.xml&File=channels.xml [following]
--11:43:42--
https://a248.e.akamai.net/f/248/21808/15m/sun.download.akamai.com/21808/sc/channel
s3/channels.xml?AuthParam=1236019547_
e9120d30e1ac62650c8f9284dfe47663&TUrl=L0QdUQV8Z4i0fdED3QTP3SJDWA8FMyaJsHfIWf4X29kT
WQpKEzIbwqFuyRPZ&TicketId=3qfzk1SIPR9R&GroupName=SWUP&BHost=sdlc3h.sun.com&FilePat
```

```
h=/sc/channels3/channels.xml&File=channels.xml
=> `/tmp/channels.xml'
Resolving a248.e.akamai.net... 208.51.221.73, 208.51.221.48
Connecting to a248.e.akamai.net|208.51.221.73|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 66,505 (65K) [application/xml]

100%[============================================================================>
] 66,505 397.16K/s

11:43:42 (396.55 KB/s) - `/tmp/channels.xml' saved [66505/66505]
```

To Verify Network Port Access

See Ports and Protocols to verify that your systems allow using the required network services and ports.

Verifying kernel.shmall and kernel.shmmax Values

If the `/etc/sysctl.conf` file has been modified, the values of kernel.shmall and kernel.shmmax might be too small. The following values are recommended:

- kernel.shmall: 268435456
- kernel.shmmax: 4294967295

1. Verify the values of kernel.shmall and kernel.shmmax.

   ```
    # sysctl -a | grep shm
   vm.hugetlb_shm_group = 0
   kernel.shmmni = 4096
   kernel.shmall = 2097152
   kernel.shmmax = 33554432
   #
   ```

2. If the values for kernel.shmall and kernel.shmmax are lower than the recommended values , edit the file to set the variables equal to the recommended values.

   ```
   # vi /etc/sysctl.conf
   kernel.shmmax = 4294967295
   kernel.shmall = 268435456
   ```

3. Reboot the system.

Prepare the Agents

When Enterprise Manager Ops Center software manages an asset, it installs a small program so that the asset can respond to inquiries and commands from the Enterprise Controller or Proxy Controller. Regardless of the operating system supporting the Enterprise Controller, it can manage assets that use either Linux and Oracle Solaris systems.

Run the `OC Doctor` utility to check requirements and to identify potential issues on each system you intend to manage. The OC Doctor utility performs the following operations. If you prefer, you can perform the same tasks manually and keep track of your progress, using the checklist in Appendix A.

Oracle Solaris OS: To Verify Required Packages and Devices

Use the `pkginfo` command to verify that the following packages are installed on Oracle Solaris assets.

Table 2–1 Required Packages and Devices for Oracle Solaris Systems

All Systems	Oracle Solaris 10	Solaris 9	Solaris 8
SUNWadmap	SUNWbzip	SUNWcpp	SUNWlmsx
SUNWbash	SUNWcpp	SUNWgcmn	SUNWnisr
SUNWctpls	SUNWgcmn	SUNWlibpopt	SUNWnisu
SUNWdtcor	SUNWlibmsr	SUNWlmsx	SUNWtltk
SUNWesu	SUNWlibpopt	SUNWlxml	SUNWxildh
SUNWgzip	SUNWlxml	SUNWpl5u	SUNWxilow
SUNWlibC	SUNWperl584core	SUNWpl5v	SUNWxilrl
SUNWlibms	SUNWperl584usr	SUNWzlibx	SUNWzlibx
SUNWloc	SUNWxwplr		
SUNWmfrun	SUNWxwplr		
SUNWswmt			
SUNWtoo			
SUNWxcu4			
SUNWxwdv			
SUNWxwfnt			
SUNWxwice			
SUNWxwplt			
SUNWxwrtl			
SUNWzip			
SUNWzlib			
/dev/random			
/dev/urandom			

Linux OS: To Verify Required Packages

Use the `rpm -q` *package* command to verify that a specific package has been installed. Use the `rpm -q` *file* command to find the name of the package that installed a file.

Linux systems require the following utilities for agent installation:

coreutils
file
gettext
grep
tar
unzip
xinetd
Agent installation on Linux systems requires the 32-bit versions of the following packages:

Table 2–2 Required Packages for Linux Systems

Oracle Linux	SUSE Linux Enterprise 10/11 64bit
pam	pam-32bit
libxml2	libxml2-32bit
e2fsprogs	e2fsprogs-32bit
	libuuid-32bit

To Verify ssh Installation

Although root ssh access is not required for agent installation, ssh must be available on systems on which you want to provision OS or firmware images.

- Oracle Solaris OS: Use the `pkginfo` command to verify that the SUNWsshu package is installed:

  ```
  # pkginfo SUNWsshu
  system      SUNWsshu SSH Client and utilities, (Usr)
  ```

- Linux OS: Use the `rpm` command to check for ssh installation. For example:

  ```
  # which ssh
  /usr/bin/ssh
  # rpm -qf /usr/bin/ssh
  openssh-clients-4.3p2-16.el5
  ```

To Verify Patches on Oracle Solaris 10 Systems With Non-Global Zones Installed

Oracle Solaris 10 systems that have non-global zones must have the following patches:

- For SPARC systems:
  - 124630-03 - System Administration Applications, Network, and Core
  - 122660-07 - Zones patch, obsoleted by Solaris 10 8/07 kernel patch 120011-14
- For x86 systems:
  - 124631-03 - System Administration Applications, Network, and Core
  - 122661-07 - Zones patch, obsoleted by Solaris 10 8/07 kernel patch 120012-14

Patches 122660-07 and 122661-07 are included on systems that are running at least Solaris 10 8/07. If the system is running an earlier version than Solaris 10 8/07, plan for the following tasks:

1. Take each system offline.
2. Install the patches in single-user mode.
3. Reboot the systems.

To Identify and Remove Duplicate Service Tags

The Enterprise Manager Ops Center software requires unique service tag uniform resource names (URNs) in each operating system instance that it manages. Service tag URNs are stored in the `/var/sadm/servicetag/registry/servicetag.xml` file. However, systems that have been installed using a flash archive (FLar) that contains this file have identical URNs.

1. On each system installed from a FLar file, use the following command to display the service tags that are stored in the /var/sadm/servicetag/registry/servicetag.xml file:

   ```
   # stclient -x
   <?xml version="1.0" encoding="UTF-8"?>
   <registry urn="urn:st:4aa51776-9cea-e85b-ab14-aedd6ca93e49" version="1.0">
     <service_tag>
       <instance_urn>urn:st:c76d9a11-f64b-418b-e9dc-a2fb18e7b76e</instance_urn>
       <product_name>Solaris 10 Operating System</product_name>
       <product_version>10</product_version>
       <product_urn>urn:uuid:5005588c-36f3-11d6-9cec-fc96f718e113</product_urn>
       <product_parent_urn>urn:uuid:596ffcfa-63d5-11d7-9886-ac816a682f92</product_
   ```

```
parent_urn>
    <product_parent>Solaris Operating System</product_parent>
    <product_defined_inst_id/>
    <product_vendor>Sun Microsystems</product_vendor>
    <platform_arch>sparc</platform_arch>
    <timestamp>2009-01-09 22:23:42 GMT</timestamp>
    <container>global</container>
    <source>SUNWstosreg</source>
    <installer_uid>95</installer_uid>
  </service_tag>
</registry>
```

2. Compare the `instance_urn` values on the systems and determine if duplicate URNs exist. If the `instance_urn` value for the Oracle Solaris operating system matches the `instance_urn` value from another system, you can remove the service tag registry and regenerate it to correct the problem.
3. To remove the service tag registry:

```
# rm /var/sadm/servicetag/registry/servicetag.xml
# ls /var/sadm/servicetag/registry/servicetag.xml
/var/sadm/servicetag/registry/servicetag.xml: No such file or directory
```

4. Use the `svcadm` command to restart the stosreg service, then verify that the `/var/sadm/servicetag/registry/servicetag.xml` file exists. For example:

```
# svcadm restart stosreg
# ls /var/sadm/servicetag/registry/servicetag.xml
/var/sadm/servicetag/registry/servicetag.xml
```

5. Use the `stclient -x` command to verify that the new `instance_urn` values are unique. For example:

```
# stclient -x
<?xml version="1.0" encoding="UTF-8"?>
<registry urn="urn:st:fdd576f6-b95c-63e6-ab54-f142ecca360f" version="1.1.4">
  <service_tag>
    <instance_urn>urn:st:cbf9acfb-0c48-c248-fb07-9816382ceb29</instance_urn>
    <product_name>Solaris 10 Operating System</product_name>
    <product_version>10</product_version>
    <product_urn>urn:uuid:5005588c-36f3-11d6-9cec-fc96f718e113</product_urn>
    <product_parent_urn>urn:uuid:596ffcfa-63d5-11d7-9886-ac816a682f92</product_
parent_urn>
    <product_parent>Solaris Operating System</product_parent>
    <product_defined_inst_id/>
    <product_vendor>Sun Microsystems</product_vendor>
    <platform_arch>sparc</platform_arch>
    <timestamp>2009-03-13 23:23:24 GMT</timestamp>
    <container>global</container>
    <source>SUNWstosreg</source>
    <installer_uid>95</installer_uid>
  </service_tag>
</registry>
```

To prevent duplicate service tag entries in future provisioning , create flash archives without the /var/sadm/servicetag/registry/servicetag.xml file.

The `flar` and `flarcreate` commands both accept the `-x` and `-X` options, which enable you to specify files to exclude from flash archives. Use these options to exclude the `/var/sadm/servicetag/registry/servicetag.xml` file from the flash archive of the Oracle Solaris OS you will use to provision the Oracle Solaris OS. Refer to the flar(1M) and flarcreate(1M) man pages for more information about creating Oracle Solaris flash archives.

To Check for Agent Patch Dependencies

The product software installs the following patches as part of agent provisioning:

- Solaris 8 SPARC: 110165-05, 110380-06,110934-26, 112097-08
- Solaris 9 SPARC: 114014-17
- Oracle Solaris 10 SPARC: 119042-09, 119254-63, 120900-04, 121133-02, 121901-02, 137321-01
- Oracle Solaris 10 x86: 119043-09, 119255-63, 120901-03, 121334-04, 121902-02, 137322-01

For systems running Oracle Solaris 10 versions earlier than Oracle Solaris 10 6/06, agent provisioning installs the patchadd patch 119254-52 or 119255-52, which in turn requires patches 120900 and 120901 or 121133 and 121334 respectively. For each system that is running an Oracle Solaris 10 operating system earlier than Solaris 10 6/06, plan to install patches 120900 and 120901 or 121133 and 121334. These patches require a reboot to ensure proper installation.

The patches 119254-63 and 119255-63 correct issues with Oracle Solaris 10 single-user mode operations. Before you provision an agent, verify that no IDR patches have been installed previously to address single-user mode operations.

To Verify the umask Value

Verify that the umask for the root user or equivalent role is set to 0022. Different shells report this value differently. The following examples list output from the umask command for the Bourne shell, the Korn shell, and the C-shell, in descending order. In all three examples, the umask value is correct.

```
# sh
# umask
0022
# ksh
# umask
022
# csh
<host_name># umask
22
```

Oracle Solaris OS: To Verify cryptosvc and gss Services

Use the svcs command to verify that the cryptosvc and gss services are enabled. For example:

```
# svcs cryptosvc gss
STATE          STIME    FMRI
online         Mar_31   svc:/system/cryptosvc:default
online         Mar_31   svc:/network/rpc/gss:default
```

Verifying Account Access

Log into My Oracle Support or register for an account and log in.

To update SUSE Linux systems, you must have a Novell account. Verify that your Novell account allows access to software updates.

Configuring for High Availability

The High Availability configuration uses manual failover procedures to transfer product functions from the primary Enterprise Controller to the secondary Enterprise Controller. Depending on the nature of the failure, different or additional procedures might be required. The procedures follow these general steps:

1. Shut down the primary Enterprise Controller, if possible.
2. Prepare the secondary Enterprise Controller for failover.
3. Transfer the storage asset that holds the `/var/opt/sun/xvm` directory structure from the primary Enterprise Controller to the secondary Enterprise Controller the
4. Run the `harestore` program to configure the Enterprise Manager Ops Center software on the secondary Enterprise Controller.
5. Reboot the secondary Enterprise Controller and start the Enterprise Manager Ops Center operations.

The `harestore` command configures the secondary Enterprise Controller to use the IP addresses of the primary Enterprise Controller. As you repair the primary Enterprise Controller, prevent it from accessing the networks where the secondary Enterprise Controller is operational.

Configuring Storage

The `/var/opt/sun/xvm/osp/share/allstart` directory is configured as an NFS share. If you use ZFS to provide the file system that mounts as `/var/opt/sun/xvm`, do not use the ZFS `sharenfs` command to share `/var/opt/sun/xvm/osp/share/allstart` so that the Enterprise Manager Ops Center software can use legacy NFS sharing tools to share the `/var/opt/sun/xvm/osp/share/allstart` directory.

Obtaining the Product Software

For more information about planning to use the Enterprise Manager Ops Center software, go to:

`http://www.oracle.com/technetwork/oem/ops-center/index.html`

From that page, you can follow links to the product documentation and to the software download site or you can go to the following page and scroll down to the Enterprise Manager section:

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

The following documents guide you through installing the product software on Oracle Solaris and Linux systems:

- *Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System*
- *Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems*

A

Planning Checklist

MY ORACLE SUPPORT Account Name and Password	______________________	______________________
Novell Account Name and Password (optional)	______________________	______________________

Oracle Solaris

Use the OC DOCTOR utility to perform these verifications.

To Check the Operating System Release	Oracle Solaris 10 11/06	____________
To Check the Installed Software Group	SUNWCall or SUNWCXall	____________
To Check the Available Disk Space	2 GB of space in `/opt` 70 GB of space in `/var/opt/sun/xvm`	____________
To Check Swap Space	6 GB for Enterprise Controller 4 GB for Proxy Controller	____________
To Verify the Amount of System Memory	6 GB for Enterprise Controller 4 GB for Proxy Controller	____________
To Verify the Amount of Shared Memory	500 MB	____________
To Verify the webservd User and Group	`/etc/passwd/etc/shadow/etc/`group	____________
To Verify an Alternate Administrative User	Verify or create	____________
Reviewing Users and Groups	-	-
Enterprise Controller Users:	`svctag, allstart, scndb, scn, scncon, uce-sds, xvm`	____________
Enterprise Controller Groups:	`jet, scndb, uce-sds`	____________
Proxy Controller Users:	`svctag, allstart, uce-sds`	____________
Proxy Controller Groups:	`jet, uce-sds`	____________
To Verify the umask Value	0022	____________
To Verify the Locations of ssh Binaries	-	-
--	`/usr/bin/scp`	____________
--	`/usr/bin/ssh`	____________

--	`/usr/bin/ssh-keygen`	____________
--	`/usr/bin/ssh-keyscan`	____________
To Verify IP Address Resolution	Matching host name and IP address	____________
To Verify That /usr/local Is Writeable	`df -h /usr/local`	____________
To Verify the Date and Time	Current timestamp	____________
To Verify Online cryptosvc and gss Services	Online	____________
To Remove the SMClintl Package	rm	____________
Ports and Protocols	-	-
Web interface:	9443, 80 redirects to 9443	____________
Proxy Controllers:	21, 22, 23, 67, 68, 161, 162, 623, 443, 6481, 8004, 8005	____________
Agents:	21165, 8002	____________
Agents for Windows and Java:	11162	____________
To Verify Network Access to Required Web Sites	-	-
--	`https://getupdates.oracle.com` and `https://a248.e.akamai.net`	____________
--	(optional) `https://linux.oracle.com`	____________
--	(optional) `http://download.novell.com` and `http://cdn.novell.com`	____________
To Verify ssh Access for the root User	ssh with root credentials	____________
To Check the Zone Identity	`zonename` command	____________

Linux

Use the OC DOCTOR utility to perform these verifications.

To Check the Operating System Release	Oracle Linux 5.3 or 5.5	____________
To Check the Available Disk Space	2 GB of space in /opt	____________
	70 GB of space in `/var/opt/sun/xvm`	
To Verify the Amount of System Memory and Swap Space	6 GB for Enterprise Controller 4 GB for Proxy Controller	____________
To Verify the Amount of System Memory and Swap Space	6 GB for Enterprise Controller 4 GB for Proxy Controller	____________
To Verify the SELinux Setting	Disabled	____________
To Verify the umask Value	0022	____________
Users and Groups	-	-
Enterprise Controller Users:	`svctag, allstart, scndb, scn, scncon, uce-sds, xvm`	____________
Enterprise Controller Groups:	`jet, scndb, uce-sds`	____________
Proxy Controller Users:	`svctag, allstart, uce-sds`	____________

Proxy Controller Groups:	`jet, uce-sds`	____________
To Verify That Required Packages Are Installed	-	-
--	python-2.4.3	____________
--	expect-5.43.0	____________
--	perl-DBD-Pg	____________
--	xinetd	____________
--	tftp-server	____________
--	dhcp	____________
--	gettext	____________
--	perl-XML-Parser	____________
--	ncompress	____________
--	libxml2 (both 64-bit and 32-bit RPMs)	____________
To Verify IP Address Resolution	Matching host name and IP address	____________
To Verify the Locations of ssh Binaries	-	-
--	`/usr/bin/scp`	____________
--	`/usr/bin/ssh`	____________
--	`/usr/bin/ssh-keygen`	____________
--	`/usr/bin/ssh-keyscan`	____________
To Verify That /usr/local Is Writeable	`df -h /usr/local`	____________
To Verify the Date and Time	Current timestamp	____________
Ports and Protocols To Verify Network Port Access	-	-
Web interface:	9443, 80 redirects to 9443	____________
Proxy Controllers:	21, 22, 23, 67, 68, 161, 162, 623, 443, 6481, 8004, 8005	____________
Agents:	21165, 8002	____________
Agents for Windows and Java:	11162	____________
To Verify Network Access to Required Web Sites	-	-
--	`https://getupdates.oracle.com` and `https://a248.e.akamai.net`	____________
--	(optional) `https://linux.oracle.com`	____________
--	(optional) `http://download.novell.com`	____________
--	(optional) `http://access.redhat.com/downloads`	
Verifying kernel.shmall and kernel.shmmax Values	kernal.shmall = 268435456	____________
Verifying kernel.shmall and kernel.shmmax Values	kernel.shmmax=4294967295	____________

Assets To Be Managed

Oracle Solaris OS: To Verify Required Packages and Devices	-	-
-	SUNWadmap	____________
-	SUNWbash	____________
-	SUNWctpls	____________
-	SUNWdtcor	____________
-	SUNWesu	____________
-	SUNWgzip	____________
-	SUNWlibC	____________
-	SUNWlibms	____________
-	SUNWloc	____________
-	SUNWmfrun	____________
-	SUNWsshu	____________
-	SUNWswmt	____________
-	SUNWtoo	____________
-	SUNWxcu4	____________
-	SUNWxwdv	____________
-	SUNWxwfnt	____________
-	SUNWxwice	____________
-	SUNWxwplt	____________
-	SUNWxwrtl	____________
-	SUNWzip	____________
-	SUNWzlib	____________
-	SUNWbzip	____________
-	SUNWcpp	____________
-	SUNWgcmn	____________
-	SUNWlibmsr	____________
-	SUNWlibpopt	____________
-	SUNWlxml	____________
-	SUNWperl584core	____________
-	SUNWperl584usr	____________
-	SUNWxwplr	____________
-	SUNWxwplr	____________
-	/dev/random	____________
-	`/dev/urandom`	____________
Linux OS: To Verify Required Packages	-	-
Utilities:	`coreutils`	____________

-	file	____________
-	gettext	____________
-	grep	____________
-	tar	____________
-	unzip	____________
-	xinetd	____________
32-bit packages:	libxml2	____________
-	pam	____________
-	e2fsprogs	____________
-	pam-32bit (SuSE Linux Enterprise 10/11 64-bit)	____________
-	libxml2-32bit (SuSE Linux Enterprise 10/11 64-bit)	____________
-	e2fsprogs-32bit (SuSE Linux Enterprise 10 64-bit)	____________
-	libuuid-32bit (SuSE Linux Enterprise 11 64-bit)	____________
-	openssh-clients	____________
SSH	Enabled	____________
To Verify Patches on Oracle Solaris 10 Systems With Non-Global Zones Installed	-	-
For Oracle Solaris SPARC systems:	124630-03 and 122660-07	____________
For Oracle Solaris x86 systems:	124631-03	____________
To Check for Agent Patch Dependencies	120900 and 120901 or 121133 and 121334	___________
To Identify and Remove Duplicate Service Tags	Remove duplicates	____________
{To Verify the umask Value	0022	____________
To Verify Online cryptosvc and gss ServicesS	Online	____________