Oracle® Enterprise Manager Ops Center

Security Guide

12*c* Release 1 (12.1.4.0.0)

E35102-04

June 2013

ORACLE®

Oracle Enterprise Manager Ops Center Security Guide 12*c* Release 1 (12.1.4.0.0)

E35102-04

Primary Author: Barbara Higgins

Contributor: Jeff Hanson

Contents

3 Security Features

Preface

The *Oracle Enterprise Manager Ops Center Security Guide* describes good practices for managing security of Oracle Enterprise Manager Ops Center deployments.

Audience

This document is intended for system administrators who are responsible for planning the configuration of the software or deploying the software.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the Oracle Enterprise Manager Ops Center documentation library.

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

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
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.

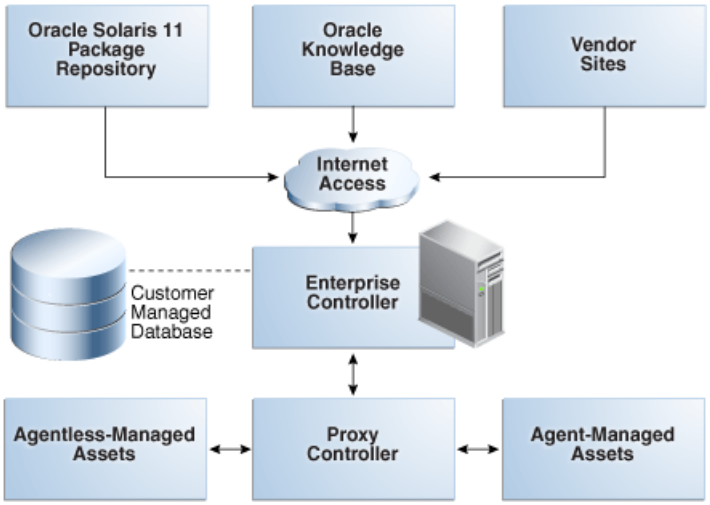
1 Overview

Oracle Enterprise Manager Ops Center is a data center management solution for managing both hardware and software from one console. This document presents good practices for managing the security of Oracle Enterprise Manager Ops Center deployments.

Product Architecture

The Oracle Enterprise Manager Ops Center software has a distributed architecture with a single master controller (Enterprise Controller) and multiple controllers (Proxy Controllers). Each Proxy Controller connects either to multiple Agent Controllers hosted on an Operating System instance or to managed systems or to both. Figure 1–1 shows a deployment with one Proxy Controller, which can be located on the same system as the Enterprise Controller.

Figure 1–1 Basic Deployment



Knowledge Base (KB) and Package Repository

The Knowledge Base is the repository for metadata about Oracle Solaris 10-8 and Linux OS components, which resides on Oracle's website. Oracle Enterprise Manager Ops Center can connect to the Knowledge Base through the Internet to obtain OS updates and updates to the product software itself. In a similar way, the Enterprise Controller can get access to the Oracle Solaris 11 Package Repository for updates to components of Oracle Solaris 11.

Enterprise Controller

The Enterprise Controller is the central server for Oracle Enterprise Manager Ops Center and there is only one Enterprise Controller in each installation. The Enterprise Controller stores firmware and OS images, plans, profiles, and policies. The Enterprise Controller also stores the asset data and site customizations in a database and hosts the web container for the user interface components. The Enterprise Controller handles all user authentication and authorization. All operations are initiated from the Enterprise Controller.

Although the Enterprise Controller stores firmware and OS images, these images are not included in a backup of the Enterprise Controller. As a good practice, create the software library for OS images on networked storage (NAS). Then include the network storage device in your site's backup plan.

Proxy Controller

A Proxy Controller links the managed assets to the Enterprise Controller and acts for the Enterprise Controller in operations that must be located close to managed assets, such as OS provisioning. The Proxy Controller provides fan-out capabilities to minimize network load and to support complex network topologies. The Proxy Controller also contains the logic for agent-less monitoring and management of hardware.

Agent Controller

An Agent is lightweight Java software that represents and manages an OS asset or OS instance and responds to requests from a Proxy Controller. Hardware management does not require an agent. The Agent receives the command, performs the required action, and reports results to the Proxy Controller. An agent never communicates directly with the Enterprise Controller.

Database

The Enterprise Controller uses an Oracle Database 11g Enterprise Edition database to store Oracle Enterprise Manager Ops Center data. The database can be local or remote:

- The local database is embedded in the Enterprise Controller, created during product installation.
- A remote database is a new or existing customer-managed database.

Oracle Enterprise Manager Ops Center provides utilities to help you manage the local database, migrate your data from a local database to a customer-managed database, back up and recover the database schema, and change database credentials.

Securing the Architecture

For a secure deployment, each communication direction must be protected. Use the procedures in Table 1–1to secure each connection.

Table 1–1 Secure Connections

Connection	To Make Secure
From Internet to the Enterprise Controller	Restrict Network Access Set the Connection Mode

Table 1–1 (Cont.) Secure Connections

Connection	To Make Secure
Between Enterprise Controller and database	Secure the Databases
Between Enterprise Controller and LDAP server	Use SSL authorization as described in the To Add a Directory Server procedure
Between Enterprise Controller and the NFS server	Verify that a firewall does not separate the Enterprise Controller and the NFS server. Verify that the NFS server uses the NFSv4 protocol.
Between Enterprise Controller and remote Proxy Controllers	Configure a reverse SSH tunnel when you install the product software. This option is described in the Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System and the Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems
Between Proxy Controller and assets	Authentication is configured when the asset is discovered and managed as described in Authentication Between the Proxy Controller and Agents

Authentication Between the Proxy Controller and Agents

In the normal operation of the product, various Proxy Controllers make requests for asset data or status and receive the response from each asset. For each transaction, the Proxy Controller must authenticate the asset and each asset must authenticate the Proxy Controller, as described in the next section. For an agentless-managed asset, authentication requires an SSH password as described in Credential Management for Assets. An alternative procedure for an OS asset that does not require a password is to install a token manually, also described in that section.

Authentication of Agent-Managed Asset

For an agent-managed asset, authentication is configured when the asset is discovered and managed. The Enterprise Controller installs an agent controller on the asset. This triggers two actions:

Authentication of the Agent

1. Agent creates a public/private key pair
2. Agent saves the key pair in `/var/opt/sun/xvm/persistence/scn-agent/connection.properties`

   Only the root user can read the agent properties file.
3. Agent sends the public key to the Enterprise Controller (through its Proxy Controller)
4. Enterprise Controller creates a unique client registration ID for this agent.
5. Enterprise Controller saves the public key and the client registration ID together in the database
6. Enterprise Controller sends the client registration ID to the agent,

7. Agent saves the client registration ID in t/var/opt/sun/xvm/persistence/scn-agent/connection.properties file.

Authentication of the Proxy Controller

1. Proxy Controller's server-side certificate was prompted to the agent as part of SSL handshake.
2. Agent accepts the certificate.
3. Agent saves the certificate locally in /var/opt/sun/xvm/security/jsse/scn-agent/truststore

Authentication Transactions

Whenever an agent gets an inquiry:

1. Proxy Controller's web server sends its certificate to the agent.
2. Agent confirms this certificate with the already-accepted certificate saved in /var/opt/sun/xvm/security/jsse/scn-agent/truststore. This is the SSL handshake.

If the agent does not confirm the Proxy Controller's certificate, the SSL handshake fails. No data is sent. This protects against an interloper.

When an agent responds to an inquiry:

1. Agent creates a string from the client reg ID and the private key. The string is its signature
2. Agent sends an HTTPS POST of the signature and the requested data to the Proxy Controller.
3. Proxy Controller retrieves the public key for the agent's client reg ID from the database.
4. Proxy Controller verifies that the message's signature was created from the private key that matches the public key.

If the Proxy Controller detects that the message's private key does not match the public key, the Proxy Controller does not allow the connection. This protects against an entity misrepresenting itself as the agent.

General Principles of Security

This section describes the principles fundamental to using the software securely.

Keep Software Up To Date

Good security is maintained when all software versions and patches are up to date. This document discusses Oracle Enterprise Manager Ops Center version 12*c* Release 1 (12.1.4.0.0). As new versions or updates of Oracle Enterprise Manager Ops Center become available, install the new software as soon as possible.

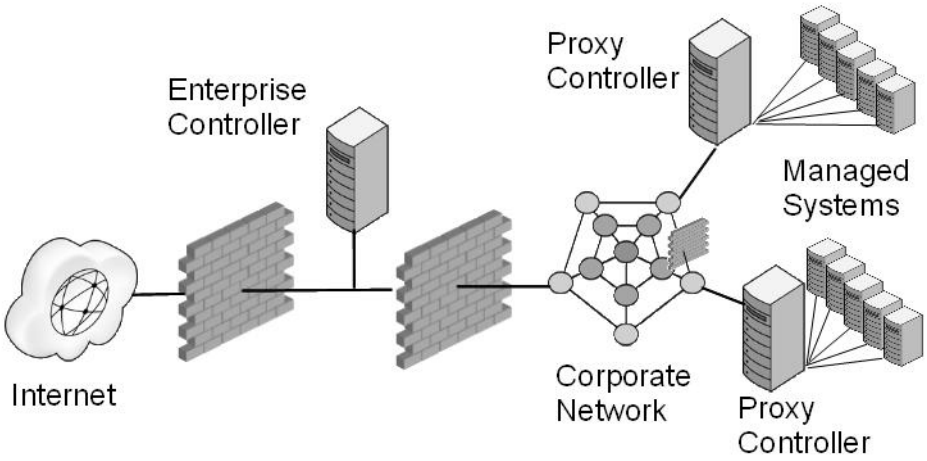
Restrict Network Access

Firewalls restrict access to systems to a specific network route that can be monitored and controlled. When firewalls are used in combination, they create a DMZ, a term for a subnetwork that controls access from an untrusted network to the trusted network. Using firewalls to create a DMZ provide two essential functions:

- Blocks traffic types that are known to be illegal.
- Contains any intrusion that attempts to take over processes or processors.

In your deployment, design an environment that locates the Enterprise Controller's system in a DMZ, that is, with a firewall between the system and the Internet and a firewall between the system and the corporate intranet, as in Figure 1–2. This type of environment allows the Enterprise Controller to get access to the Internet to perform operations while in Connected mode, and restricts access to assets to only those operations that manage the assets. When the Enterprise Controller is in Disconnected mode, it operates without access to the Internet.

Figure 1–2 Firewalls Restrict Access to Enterprise Controller



If your data center includes remote Proxy Controllers, use firewalls between the Enterprise Controller's system and the Proxy Controllers' systems.

To use Oracle Enterprise Manager Ops Center in Connected mode, use the information in Table 1–2 to configure the firewall between the Enterprise Controller and the Internet.

Table 1–2 IP Address and Port Requirements

Site	IP Address	Port	Purpose
`https://java.net/projects/oc-doctor/downloads`	192.9.164.103	Port 443	Updates to OCDoctor utility
`https://java.net/projects/oc-cluster-profiles`	192.9.164.103	Port 443	Access to Oracle Solaris Cluster profiles and scripts.
`login.oracle.com`	141.146.8.119	Port 443	Logging into Oracle sites
`updates.oracle.com`	141.146.44.51	Port 443	Access to Oracle Knowledge Base for OS updates
`inv-cs.oracle.com`	192.18.110.10	Port 443	Product registration
`hs-ws1.oracle.com`	192.18.110.11	Port 443	Product registration
`support.oracle.com`	141.146.54.16	Port 443	My Oracle Support

Table 1–2 (Cont.) IP Address and Port Requirements

Site	IP Address	Port	Purpose
`www.oracle.com`	96.17.111.33 96.17.111.49	Port 80	-
`aru-akam.oracle.com`	na	Port 80	Provides local IP addresses to optimize download speed. Use `nslookup` to resolve the IP address, add the address to the `/etc/hosts` file, and open the firewall for the address.
`a248.e.akamai.net`	na	Port 443	Provides local IP addresses to optimize download speed. Use `nslookup` to resolve the IP address, add the address to the `/etc/hosts` file, and open the firewall for the address.

To configure the firewall between the Enterprise Controller and a Proxy Controller or a corporate network, allow the ports and protocols in Table 1–3.

Table 1–3 Required Ports and Protocols

Communication Direction	Protocol and Port	Purpose
Enterprise Controller	Port 443, then Port 11165 Port 8005	Enterprise Controller in Disconnected mode
Enterprise Controller	Port 443, then Port 11165	Enterprise Controller in Connected mode
Browser to Enterprise Controller	HTTP, TCP: Port 80	Redirects to port 9443
Browser to Enterprise Controller	HTTPS, TCP: Port 9443	Web interface
Enterprise Controller to Local Database	Port 11176	Oracle Listener port
Enterprise Controller to Proxy Controller	SSH, TCP: Port 22 ICMP ping: Type 8 Code 0 (echo request)	Enterprise Controller installs or upgrades a Proxy Controller through the UI.
Proxy Controllers to Enterprise Controller	HTTPS, TCP: Port 443	Proxy Controller pushes data about assets to Enterprise Controller. Proxy Controller pulls data for jobs, updates, Agent Controllers, and OS images from the Enterprise Controller.
Proxy Controllers to Enterprise Controller	HTTP: Port 8004	WAN Boot traffic
Proxy Controllers to Enterprise Controller	ICMP ping: Type 0 Code 0 (echo reply)	During upgrades, Proxy Controllers use ICMP ping.
Remote Proxy Controller to Enterprise Control through an SSH Tunnel	SSH, Port 21161	When a Proxy Controller is deployed on a network outside of the firewall, the SSH Tunnel and Port 21161 change the direction of communication so that the remote Proxy Controller does not initiate communication with the Enterprise Controller.

Table 1–3 (Cont.) Required Ports and Protocols

Communication Direction	Protocol and Port	Purpose
Proxy Controller to ALOM Service Processors	SSH, TCP: Port 22 or Telnet, TCP: Port 23 SNMP, UDP: Port 161 TCP: Port 6481 (for discovery by service tags) ICMP, Type 8 Code 0	Proxy Controller discovers, manages, and monitors the service processor.
Proxy Controller to ILOM Service Processors	SSH, TCP: Port 22 SNMP, UDP: Port 161 IPMI, TCP, UDP: Port 623 TCP: Port 6481 (for discovery by service tags) ICMP, Type 8 Code 0	Proxy Controller discovers, manages, and monitors the service processor.
Proxy Controller to ALOM or XCSF Service Processor	FTP, TCP: Port 21	Proxy Controller provisions firmware on an ALOM service processor. Port 21 transfers the firmware image. A transient random port is opened for the duration of the operation.
Proxy Controller to ILOM Service Processor	TFTP, UDP: Port 69	Proxy Controller provisions firmware on an ILOM service processor. Port 69 transfers the firmware image. A transient random port is opened for the duration of the operation.
Service Processor to Proxy Controller	SNMP, UDP: Port 162 ICMP ping: Type 0 (echo reply)	For monitoring hardware, the service processor sends SNMP traps to the Proxy Controller. For a failed connection, Proxy Controller receives ICMP ping Type 3 (destination unreachable).
Proxy Controller to OS Host	SSH, TCP: Port 22 or Telnet, TCP: Port 23 TCP: Port 6481 (for discovery and monitoring by service tags) ICMP, Type 8 Code 0 (heartbeat)	Proxy Controller discovers, manages, and monitors an asset.
Proxy Controller to OS Host	DHCP, UDP: Port 67	Proxy Controller provisions an OS.
OS Host to Proxy Controller	HTTP, TCP: Port 8004 Oracle Solaris 11 Automated Installer Web Server: Port 5555 to accept requests from the OS Host during provisioning ■ For provisioning by DHCP, the opened port is on the Proxy Controller. ■ For provisioning by WAN Boot, the opened port is on the Enterprise Controller or a Proxy Controller.	OS Host reports status of OS updates and status of Agent Controller installation. OS Host downloads Agent Controller archive file.

Table 1–3 (Cont.) Required Ports and Protocols

Communication Direction	Protocol and Port	Purpose
OS Host to Proxy Controller	DHCP, UDP: Port 68 TFTP, UDP: Port 69 TCP+UDP: Port 37 HTTP, TCP: Port 8004	OS Host responds to Proxy Controller inquiries during bare-metal OS provisioning
Agent Controller to Proxy Controller	HTTPS, TCP: Port 21165	Agent Controllers push asset data to Proxy Controller. Agent Controllers pull data for jobs.
Agent Controller to Proxy Controller	HTTPS, TCP: Port 8002	Agent Controllers pull updates from Proxy Controller.
Agent Controller on Oracle Solaris OS or on Oracle hardware to co-located Proxy Controller	SNMP: Port 1162, or a port in the range of 1100 through 1200	For monitoring assets, the Agent Controller sends trap notifications and fault management alerts (FMA) to the Proxy Controller as local traffic. Because the Proxy Controller is using Port 162, a co-located Agent Controller uses Port 1162, if it is available, or a port in the range of Ports 1100 through 1200.
Java client to public APIs	TLS: Port 11172	JMX access from clients
WMI client on Proxy Controller to Agent Controller	Port 11162	WMI client resides on the Proxy Controller and communicates with the WMI server on the Agent Controller. The Proxy Controller uses the DCOM protocol to monitor a Windows system. The Proxy Controller opens a TCP connection to the Windows DCOM registry port, TCP 135, which provides a lookup service to the WMI scripting DCOM object. The Proxy Controller connects to the DCOM object. The port number for this connection is allocated by the Windows system.
Proxy Controller to NFS server	Use an NFS server that is on the same side of the firewall as the Proxy Controller. Refer to your OS documentation to set up the NFS server.	Proxy Controller pulls provisioning images from NAS Library
Global Zones or Oracle VM Servers to NFS server	Use an NFS server that is on the same side of the firewall as the Proxy Controller. Refer to your OS documentation to set up the NFS server.	Global Zones and Oracle VM Servers push their metadata and virtual host images to NAS Library
OCDoctor to `java.net`	HTTPS, TCP: Port 80	Acquires product updates.

Follow the Principle of Least Privilege

The principle of least privilege states that users are given the lowest level of permissions to perform their tasks. Granting roles or privileges in excess of a user's responsibilities leaves a system open for non-compliance. Review privileges periodically to determine whether they remain appropriate for each user's current job responsibilities.

You give each user a set of roles, which determine the tasks the user can and cannot perform, and a set of privileges which specify the assets, networks, or other objects to which the user's roles apply. This gives you fine-grained control of the actions that users can take.

Role Requirement for Tasks

Table 1–4 shows the permission needed to perform each action. Oracle Enterprise Manager Ops Center groups permissions into roles and assigns one or more roles to a user account. Table 1–5 shows the permissions granted by each role.

Table 1–4 Tasks and Permissions

Tasks	Permission
Read Access	Read Access
Add Assets	Discover Assets
Find Assets	
Manage Assets	Manage Assets
Delete Assets	
Create Group	Asset Group Management
Edit Group	
Add Assets to Group	
Delete Group	
New Update OS Job	Update
Deploy or Update Software	
Compare System Catalog	
Create Catalog Snapshot	
View and Modify Catalog	
New Simulated OS Update Job	Update Simulation
Configure and Deploy Server	Server Deployment
Install Server	
Configure RAID	
Add or delete storage	Virtualization Guest Management
Assign or detach network	
Start Guest	
Shut Down Guest	
Migrate Guest	
Clone Guest	
Lifecycle actions	

Table 1–4 (Cont.) Tasks and Permissions

Tasks	Permission
Assign Incidents	Fault Management
Add Annotation to incidents	
Acknowledge incidents	
Take Actions on Incidents	
Mark Incidents as Repaired	
Close Incidents	
Delete Notifications	
Take Actions on Notification	
Update Management Credentials	Credential Management
Any Actions related to changing credentials	
Edit Network Domain	Network Management
Edit Network Attributes	
Edit Network Services	
Fabric Management	Fabric Management
Import ISO	Storage Management
Upload image	
Edit Attributes	
Create reports	Report Management
Delete reports	
Create, delete, and modify profiles and plans	Plan/Profile Management
Create/Update/Delete Instance	Cloud Usage
Attach/Detach Volume to Instance	
Create/Delete/Update Security Group	
Create/Update/Delete Volume	
Upload/Register/Delete templates	
Create/RollbackTo/Delete Snapshot	
Shutdown All servers	
Link/Launch OVAB	
Create/Delete/Update Cloud	Cloud Management
Create/Delete/Update Cloud Domain	
Create Public Security Group	
Share Public Security Group	
Create VM Instance Type	
Manage Enterprise Controller	Enterprise Controller Management

Table 1–4 (Cont.) Tasks and Permissions

Tasks	Permission
Unconfigure/Uninstall Proxy Controller	Proxy Controller Management
Configure Agent Controller	
Unconfigure Agent Controller	
DHCP configuration	
Subnets	
External DHCP Servers	
Configure/Connect	Cloud Control Management
Disconnect/Unconfigure	
Cloud Control Console	
Unconfigure	Windows Update Management
SCCM Configuration	
Add Users	User Management
Remove Users	
Assign Roles	Role Management
Asset Management	Asset Management
Write Access	Write Access
Open Service Request	Service Request
Power On	Power Management
Power Off	
Power on with Net Boot	
Set Power Policy	
Chassis Management	Chassis Management
Storage Server Management	Storage Server Management
Launch Switch UI	Switch Management
Reset Servers	Server Management
Reset Service Processors	
Refresh	
Locator Light On/Off	
Snapshot Bios Configuration	
Update Bios Configuration	
Reboot	Operating System Management
Upgrade Agent Controller	
Cluster Management	Cluster Management
Aggregate Links	Link Aggregation
IPMP Groups	IPMP Groups
Update Firmware	Update Firmware
Upgrade Proxy Controller	Proxy Controller Upgrade
Execute Operation	Operation Execution
Unconfigure Enterprise Controller	Unconfigure EC

Table 1–4 (Cont.) Tasks and Permissions

Tasks	Permission
Add Product Alias	Add Product Alias
Upgrade Enterprise Controller	EC Upgrade
Set Enterprise Controller Storage Library	EC Storage Library Management
Configure Local Agent Unconfigure Local Agent	EC Local Agent Management
Proxy Deployment Wizard	EC Proxy Management
Set up Connection Mode	EC Connection Mode Management
Register Enterprise Controller	EC Registration
Change HTTP Proxy	EC HTTP Proxy Management
Edit Energy Cost	EC Energy Cost Management
Ops Center Downloads	Ops Center Downloads
Activate Boot Env and Reboot Create New Boot Env. Synchronize Boot Env.	Boot Environment Management
Create Server Pool	Server Pool Creation
Delete Server Pool	Server Pool Deletion
Rebalance Resource Edit Server Pool Attribute Attach Network to Server Pool Associate Library to Server Pool Add/Remove Virtual Host	Server Pool Management
Create OVM virtual Servers Create zone servers Create Logical Domains	Server Pool Usage
Create Virtualization Host	Virtualization Host Creation
Delete Virtualization Host	Virtualization Host Deletion
Add/Remove Virtual Host to/from Server Pool Edit Tags Edit Attributes Reboot Change Routing Configuration Change NFS4 Domain Change Naming Service Change Remote Logging Configuration	Virtualization Host Management
Create Logical Domains Create zones Create OVM virtual servers	Virtualization Host Usage

Table 1–4 (Cont.) Tasks and Permissions

Tasks	Permission
Create Logical Domains Create zones Create OVM virtual servers	Virtualization Guest Creation
Delete Logic Domain Delete Zones Delete OVM Virtual Servers.	Virtualization Guest Deletion
Start Guest Shutdown Guest Migrate Guest Clone Guest	Virtualization Guest Usage
Create Library	Storage Creation
Delete Library	Storage Deletion
Associate Library	Storage Usage
Create Network Domain Create Network	Network Creation
Delete Network Domain Delete Network	Network Deletion
Assign Network Connect Guests	Network Usage
Create Fabric	Fabric Creation
Delete Fabric	Fabric Deletion
Fabric Management	Fabric Usage
Chassis Usage	Chassis Usage
Storage Server Usage	Storage Server Usage
Switch Usage	Switch Usage
Launch LOM Controller Edit Tags	Server Usage
Edit Tags Edit Attributes	Operating System Usage
Create Rack	Rack Creation
Directory Server Management	Directory Server Management
Power Distribution Unit Usage	Power Distribution Unit Usage
Power Distribution Unit Management	Power Distribution Unit Management
Rack Creation	Rack Creation
Rack Deletion	Rack Deletion
Rack Management	Rack Management
Rack Usage	Rack Usage
OVM Manager Usage	OVM Manager Usage

Table 1–4 (Cont.) Tasks and Permissions

Tasks	Permission
OVM Manager Management	OVM Manager Management
Network Domain Creation	Network Domain Creation
Network Domain Deletion	Network Domain Deletion
Network Domain Management	Network Domain Management
Network Domain Usage	Network Domain Usage
Asset Network Management	Asset Network Management
Job Management	Job Management

Table 1–5 Roles and Permissions

Role	Permissions
Asset Admin	Asset Group Management Asset Management Asset Network Management Boot Environment Management Chassis Management Chassis Usage Cluster Management Discover Assets IPMP Groups Link Aggregation Manage Assets Network Management Operating System Management Operating System Usage Power Distribution Unit Management Power Distribution Unit Usage Power Management Rack Creation Rack Deletion Rack Management Rack Usage Read Access Server Management Server Usage Service Request Storage Server Management Storage Server Usage Switch Management Switch Usage Write Access

Table 1–5 (Cont.) Roles and Permissions

Role	Permissions
Cloud Admin	Asset Management Asset Network Management Cloud Management Cloud Usage Fabric Creation Fabric Deletion Fabric Management Fabric Usage IPMP Groups Link Aggregation Manage Assets Network Creation Network Deletion Network Domain Creation Network Domain Deletion Network Domain Management Network Domain Usage Network Management Network Usage Operating System Management Operating System Usage OVM Manager Management OVM Manager Usage Profile Plan Management Read Access Role Management Server Management Server Pool Management Server Pool Usage Server Usage Storage Management Storage Server Management Storage Server Usage Storage Usage Switch Management Switch Usage Virtualization Guest Creation Virtualization Guest Deletion Virtualization Guest Management Virtualization Guest Usage Virtualization Host Management Virtualization Host Usage Write Access

Table 1–5 (Cont.) Roles and Permissions

Role	Permissions
Cloud User	Asset Management Asset Network Management Cloud Usage Fabric Creation Fabric Deletion Fabric Usage Manage Assets Network Creation Network Deletion Network Domain Management Network Domain Usage Network Management Network Usage Operating System Management Operating System Usage OVM Manager Usage Read Access Server Pool Usage Server Usage Storage Management Storage Server Usage Storage Usage Switch Usage Virtualization Guest Creation Virtualization Guest Deletion Virtualization Guest Management Virtualization Guest Usage Virtualization Host Management Virtualization Host Usage Write Access

Table 1–5 (Cont.) Roles and Permissions

Role	Permissions
Exalogic Systems Admin	Asset Management Credential Management Directory Server Management EC Energy Cost Management EC HTTP Proxy Management EC Registration Fabric Creation Fabric Deletion Fabric Management Fabric Usage Job Management Link Aggregation Network Creation Network Deletion Network Domain Creation Network Domain Deletion Network Domain Management Network Domain Usage Network Management Network Usage Operating System Management Operating System Usage Operation Execution OVM Manager Management OVM Manager Usage Power Distribution Unit Management Power Distribution Unit Usage Profile Plan Management Proxy Controller Management Read Access Report Management Role Management Server Deployment Server Management Server Usage Service Request Storage Creation Storage Deletion Storage Management Storage Server Management Storage Server Usage Storage Usage Switch Usage Update Firmware User Management Write Access

Table 1–5 (Cont.) Roles and Permissions

Role	Permissions
Fault Admin	Fault Management Read Access Write Access
Network Admin	Asset Management Asset Network Management Fabric Creation Fabric Deletion Fabric Management Fabric Usage IPMP Groups Link Aggregation Network Creation Network Deletion Network Domain Creation Network Domain Deletion Network Domain Management Network Domain Usage Network Management Network Usage Read Access Write Access
Ops Center Admin	Add Product Alias Discover Assets EC Connection Mode Management EC Energy Cost Management EC HTTP Proxy Management EC Local Agent Management EC Proxy Management EC Registration EC Storage Library Management EC Upgrade Enterprise Controller Management Cloud Control Management Job Management Manage Assets Ops Center Downloads OVM Manager Management OVM Manager Usage Proxy Controller Management Proxy Controller Upgrade Read Access Unconfigure EC Windows Update Management Write Access
Plan/Profile Admin	Plan/Profile Management Read Access Write Access

Table 1–5 (Cont.) Roles and Permissions

Role	Permissions
Read	Read Access
Report Admin	Read Access Report Management Update Simulation Write Access
Role Management Admin	Read Access Role Management Write Access
Security Admin	Credential Management Read Access Write Access
Apply Deployment Plans	Operation Execution Read Access Server Deployment Update Firmware Write Access
Storage Admin	Asset Management Read Access Storage Creation Storage Deletion Storage Management Storage Server Management Storage Server Usage Storage Usage Write Access

Table 1–5 (Cont.) Roles and Permissions

Role	Permissions
Supercluster Systems Admin	Asset Management Cluster Management Credential Management Directory Server Management EC Energy Cost Management EC HTTP Proxy Management EC Registration Fabric Creation Fabric Deletion Fabric Management Fabric Usage Job Management Link Aggregation Network Creation Network Deletion Network Domain Creation Network Domain Deletion Network Domain Management Network Domain Usage Network Management Network Usage Operating System Management Operating System Usage Operation Execution Power Distribution Unit Management Power Distribution Unit Usage Profile Plan Management Proxy Controller Management Read Access Report Management Role Management Server Deployment Server Management Server Usage Service Request Storage Creation Storage Deletion Storage Management Storage Server Management Storage Server Usage Storage Usage Switch Usage Update Firmware User Management Write Access

Table 1–5 (Cont.) Roles and Permissions

Role	Permissions
Update Admin	Boot Environment Management Read Access Update Update Simulation Windows Update Management Write Access
Update Simulation Admin	Read Access Update Simulation Write Access
User Management Admin	Directory Server Management Read Access User Management Write Access

Table 1–5 (Cont.) Roles and Permissions

Role	Permissions
Virtualization Admin	Asset Management Asset Network Management Fabric Creation Fabric Deletion Fabric Management Fabric Usage IPMP Groups Link Aggregation Manage Assets Network Creation Network Deletion Network Domain Creation Network Domain Deletion Network Domain Management Network Domain Usage Network Management Network Usage Operating System Management OVM Manager Management OVM Manager Usage Read Access Server Deployment Server Management Server Pool Creation Server Pool Deletion Server Pool Management Server Pool Usage Storage Creation Storage Deletion Storage Management Storage Server Management Storage Server Usage Storage Usage Virtualization Guest Creation Virtualization Guest Deletion Virtualization Guest Management Virtualization Guest Usage Virtualization Host Creation Virtualization Host Deletion Virtualization Host Management Virtualization Host Usage Write Access

Assigning Roles and Privileges to a User

The user accounts are created from the local authentication subsystem of the Enterprise Controller's operating system or from a separate directory server, as described inConfiguring an LDAP Server.

You must have the Role Admin role to grant roles to user accounts and to change privileges.

1. Select Administration in the Navigation pane.
2. Click the Roles tab. The Roles page is displayed.
3. Select a user from the list of users.
4. Click the Manage User Roles icon.
5. Add or remove one or more roles from the roles list. By default, a user has all the permissions of the assigned role. To control the scope of a user's role, remove a specific permission:
   a. Deselect the Use the default Role associations box. Click Next.
   b. The privileges for each type of target are displayed on separate pages. Select the roles to apply to each target, then click Next.
6. The Summary page is displayed. Review the roles and privileges assigned to the user, then click Finish.

Monitor System Activity

Each Oracle Enterprise Manager Ops Center component has some auditing capability. Follow audit advice in this document and regularly monitor audit records.

Oracle Enterprise Manager Ops Center performs each action as a job. The details of a job show the order of operations in the job and the managed assets that were targets of the job. You can view the details of a job from either the browser or the command-line interface. Oracle Enterprise Manager Ops Center stores each job until the job is deleted explicitly.

In addition to the jobs record, log files can be a source of activity records. Logs are written during operations and can provide additional detail about system activity. Log files are protected by file permissions and therefore requires a privileged user to get access to them.

User Activity

User session activity is included in the BUI log file and in the audit-logs file, which also include activity from the command-line interface.:

- `/var/opt/sun/xvm/logs/emoc.log` has the following format with the timestamp:

```
User login: User <username> logged in.
User logout: User <username> logged out.
User login session expire: User <username> logged in.
```

- `/var/opt/sun/xvm/logs/audit-logs*` has the following format:

```
6/6/13 9:39 AM LOGIN rmi://127.0.0.1 root 7
6/6/13 9:39 AM REMOTE_INFO rmi://127.0.0.1 root 7, Remote Info: User root
connected from 10.166.78.167:54179 / JMX Session:
com.sun.cacao.session^Armi://127.0.0.1:1 com.sun.cacao.user^Aroot
```

General Events

- Messages: `/var/adm/messages*`
- Sessions with IP address and port: `/var/opt/sun/xvm/logs/audit-logs*`

- BUI: `/var/opt/sun/xvm/logs/emoc.log`
- Actions of the BUI and remote clients on the Enterprise Controller:
  - On Oracle Solaris: `/var/cacao/instances/oem-ec/audits/`
  - On Linux: `/var/opt/sun/cacao/instances/oem-ec/audits/`
- Events between controllers and agents:
  - On an Oracle Solaris Enterprise Controller: `/var/cacao/instances/oem-ec/logs/cacao.`*n*
  - On a Linux Enterprise Controller: `/var/opt/sun/cacao/instances/oem-ec/logs/cacao`*n*
  - On each Oracle Solaris Proxy Controller: `/var/cacao/instances/scn-proxy/logs/cacao.`*n*
  - On each Linux Proxy Controller: `/var/opt/sun/cacao/instances/scn-proxy/logs/cacao.`*n*

High Availability

When Oracle Enterprise Manager Ops Center is in a High Availability configuration, each Enterprise Controller is a Clusterware node. The Clusterware resource activity is logged and the following log file is updated each time the active Enterprise Controller's resource action script's `check()` function is executed. The default interval is 60 seconds.

On Oracle Solaris: `/var/opt/sun/xvm/ha/EnterpriseController.log`

Software Updates

The Software Update component has its own server with its own logs. The following logs provide information on the activity for this server:

- Audit Log
  - On Oracle Solaris: `/var/opt/sun/xvm/uce/var.opt/server/logs/audit.log`
  - On Linux: `/usr/local/uce/server/logs/audit.log`
- Errors
  - On Oracle Solaris: `/var/opt/sun/xvm/uce/var.opt/server/logs/error.log`
  - On Linux: `/usr/local/uce/server/logs/error.log`
  - Download jobs: `/opt/SUNWuce/server/logs/SERVICE_CHANNEL/error.log`
- Job Log
  - On Oracle Solaris: `/var/opt/sun/xvm/uce/var.opt/server/logs/job.log`
  - On Linux: `/usr/local/uce/server/logs/job.log`

Agents

- `/var/scn/update-agent/logs` directory.
- `/var/opt/sun/xvm/logs`

Local Database

- On the Enterprise Controller:
  - For installation events:

/var/opt/sun/xvm/oracle/cfgtoollogs/dbca/OCDB/*

/var/tmp/installer.log.latest

- For operational events reported by the `ecadm sqlplus` utility:

```
/var/opt/sun/xvm/oracle/diag/rdbms/ocdb/OCDB/alert/log.xml.*
/var/opt/sun/xvm/oracle/diag/rdbms/ocdb/OCDB/trace/alert_OCDB.log.*
/var/opt/sun/xvm/oracle/diag/tnslsnr/<hostname>/oclistener/alert/log.xml.*
/var/opt/sun/xvm/oracle/diag/tnslsnr/<hostname>/oclistener/trace/listener.
log.*
```

- For schema changes:

  /var/opt/sun/xvm/log/satadmsqlplus.log

  /var/opt/sun/xvm/logs/alter_oracle_schema.out

  /var/opt/sun/xvm/logs/alter_oracle_storage.out

- For backup, restore, and migrate operations:

  /var/opt/sun/xvm/logs/sat-backup-*date-time*.log

  /var/opt/sun/xvm/logs/sat-restore-*date-time*.log

  /var/opt/sun/xvm/logs/migrate.log

- On the Proxy Controller: `/var/opt/sun/xvm/proxydb/*`
- On each agent: `/var/opt/sun/xvm/agentdb/*`

2

Secure Installation and Configuration

This chapter describes how to plan an installation and then how to configure the software so that you use the software securely.

Planning the Deployment

This section outlines the options for a secure installation and describes several recommended deployment topologies for the systems.

High Availability

The simplest deployment architecture is a single-system deployment in which the Enterprise Controller and a Proxy Controller are installed on the same system. Although the simplicity is appealing, this type of deployment creates a single point of failure and cannot provide high availability because all components are stored on the same computer.

The High Availability configuration uses multiple Enterprise Controllers with Oracle Clusterware and a remote database. The active Enterprise Controller is used for all operations. The standby Enterprise Controllers are configured as backups. If the active Enterprise Controller must be taken offline, make another Enterprise Controller active. One of the standby Enterprise Controllers is also activated if the active Enterprise Controller fails.

Each asset is managed by a specific Proxy Controller. If a Proxy Controller fails or is uninstalled, Oracle Enterprise Manager Ops Center gives you the option to migrate the failed Proxy Controller's assets to another Proxy Controller. At any time, move an asset from one functional Proxy Controller to another Proxy Controller. The destination Proxy Controller must either be connected to the networks of the assets being moved, or be associated with those networks and have them enabled.

Requirements for Enterprise Controller High Availability

- Use two or more 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
- Use the **Edit Asset** action to add an asset tag that identifies the active Enterprise Controller and distinguishes it from the standby Enterprise Controller.

- Maintain the standby Enterprise Controller's system in the same way as the active Enterprise Controller. The active and standby Enterprise Controllers must use the same version of Oracle Enterprise Manager Ops Center software.

Limitations of High Availability

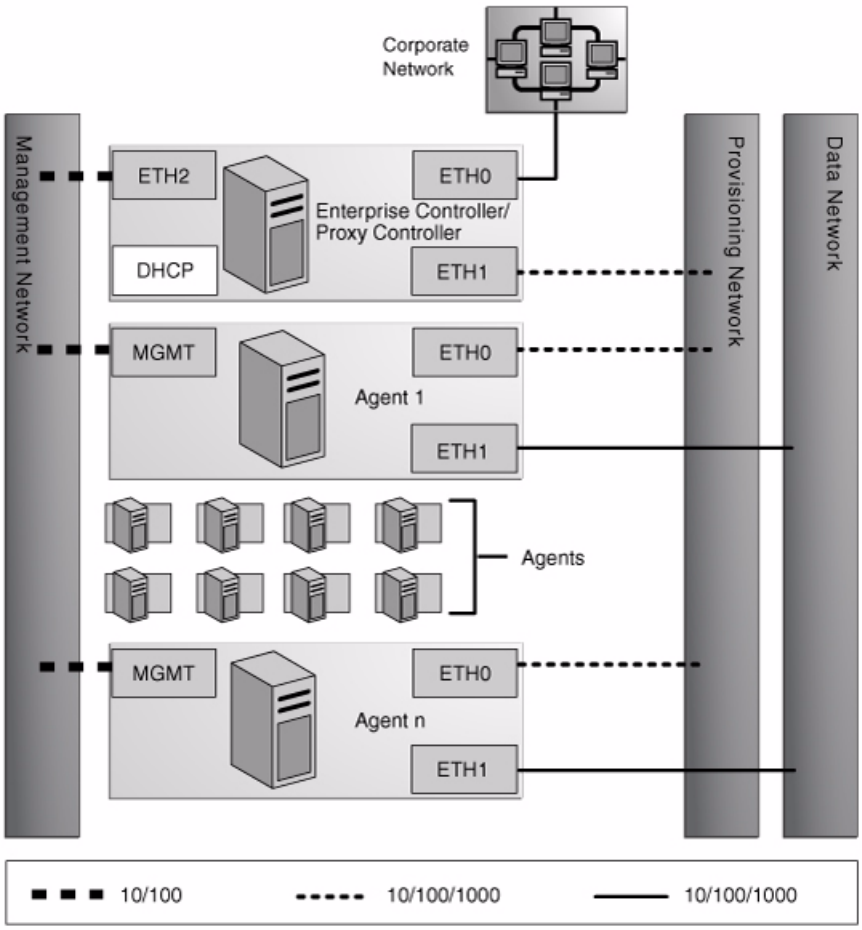
- User accounts and data that are not associated with Oracle Enterprise Manager Ops Center are not part of the relocate process. Only Oracle Enterprise Manager Ops Center data is moved between the active and standby Enterprise Controllers.
- Any customizations of the PAM configuration on the primary node must be repeated on the standby node. Oracle Enterprise Manager Ops Center does not replicate PAM configuration.
- UI sessions are lost in a relocation.
- The Enterprise Controller HA configuration applies only to the Enterprise Controller and not to Proxy Controllers.

See the *Oracle Enterprise Manager Ops Center Administration Guide* for instructions in configuring and maintaining an High Availability installation.

Network Configuration

Network connections are needed for data operations, for management operations, and for provisioning operations. The minimum configuration, but least secure, is to combine all operations on one network. Separate networks, as shown in Figure 2–1, provide the highest security and the lowest number of points of failure. However, additional network interface cards (NIC) are needed to support this configuration.

Figure 2–1 Separate Management, Provisioning, Data Networks



Infrastructure and Operating Systems

Oracle Enterprise Manager Ops Center manages and monitors assets in multiple locations and on multiple platforms. The responsibility for securing the network, hardware, and operating system of the server that runs the Enterprise Controller is that server's system administrator. The responsibility for securing the hardware, network, and operating system of Proxy Controllers and all assets falls on various sites' system administrators.

Storage Configuration

Oracle Enterprise Manager Ops Center stores its data and metadata in Software and Storage Libraries. These libraries can reside in local file systems or on the shares of an NFS server. Because the Enterprise Controller does not mount the NFS share, install the NFS server on a system that is close to the systems that will use the NFS share, that is, the systems that host global zones and Oracle VM Servers.

Remote Database

This version of the product software provides the capability to use a remote, customer-managed database. The Enterprise Controller interacts with the remote, customer-managed database using the Oracle*Net protocol over TCP/IP.

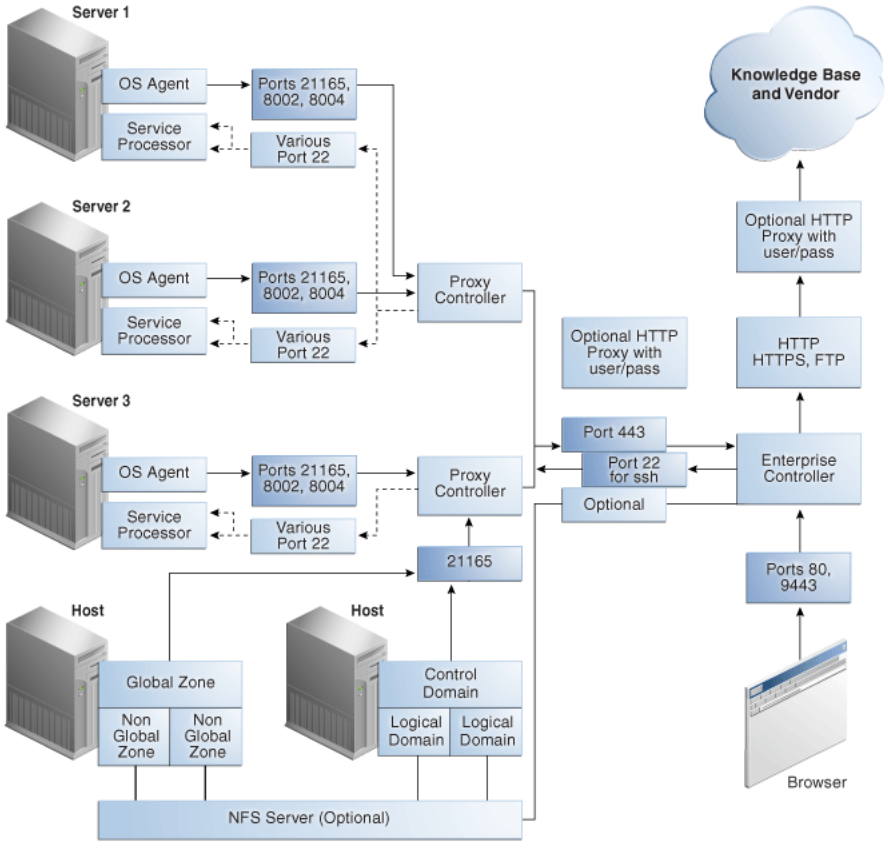
Oracle Enterprise Manager Ops Center provides scripts to create the database schema and users. Before you install Oracle Enterprise Manager Ops Center, your database administrator creates the database and then runs the `createOCSchema_remote.sql`script to create the Ops Center Schema and to grant the CREATE DATABASE privilege. The database administrator provides the database credentials and the connection information to you and you create the `remoteDBCreds.txt` file. The file can be located in a directory of your choice on the system that hosts the Enterprise Controller.

When you install the Oracle Enterprise Manager Ops Center software, you use the `-remoteDBprops` flag and provide the location of the `remoteDBCreds.txt` file. During installation, the connection between the Enterprise Controller and the remote database is created.

Typical Deployment

Figure 2–2 shows a deployment running the product software in Connected mode and with two Proxy Controllers.

Figure 2–2 Deployment Example



Installing Oracle Enterprise Manager Ops Center

- Control Access
- Install a Remote Proxy Controller

Control Access

Install the Enterprise Controller component only on a system where root access is controlled tightly because a root-privileged user must modify or create system services as part of the installation. To install the product on Linux systems, disable the SELINUX setting.

Install a Remote Proxy Controller

When installing a Proxy Controller that is not co-located with the Enterprise Controller, do not use the **Proxy Controller Deploy** action from the browser interface. Instead, copy the Proxy Controller bundle to the target system and then log in as root to install the software. This method removes the need to provide root credentials to the Proxy Controller's system and eliminates the need to enable `ssh` access from the Enterprise Controller's system to the Proxy Controller's system.

Configuring Oracle Enterprise Manager Ops Center

A privileged user must be enabled for the Oracle Enterprise Manager Ops Center software. Log in as the privileged user to configure the software.

Set the Connection Mode

Connection modes provide a way to keep the product software and all of the asset software current. However, Connected mode requires Internet access and if this access cannot be made secure or if a site's policy does not enable Internet access, the alternative is to run Oracle Enterprise Manager Ops Center in Disconnected mode. Although Disconnected mode might seem to provide the most secure environment, its use relies on manual procedures that can are error-prone without rigorous compliance to procedures and policies. Table 2–1 shows how operations are affected by the connection mode.

Table 2–1 Comparison of Functions in Different Connection Modes

Operation	Connected Mode	Disconnected Mode
Obtain a new version of the product software	Use the **Oracle Ops Center Downloads** action to create a job that obtains the latest version.	1. Log in to an Internet-facing system and download the `https://updates.oracle.com/OCDoctor/harvester_bundle-latest.zip` file. 2. Unzip the compressed file and run the `harvester` script to connect to the Oracle Datacenter and create an upgrade bundle. 3. Copy the update bundle to the Enterprise Controller's system.
Upgrade the product software	Use the **Upgrade Enterprise Controller** action. For each Proxy Controller, use the **Update to Latest Available Version** action.	For the Enterprise Controller and each Proxy Controller: 1. Log in to each system as root and create a temporary directory. 2. Move the upgrade software from the Internet-facing system to the new directory. 3. Uncompress the file and install the software, according to the instructions in the appropriate installation guide.
Provision an OS and update an existing OS, using the latest image.	Download the operating system software from `http://updates.oracle.com` to a software library.	Obtain the image. Use a CD or DVD to load the operating system software. Log in to an Internet-facing system and download the operating system software from `http://updates.oracle.com` Then use the **Upload ISO Images** action and the **Import Images** action to update the contents of the Enterprise Controller's software library.
Provision firmware and update existing firmware, using the latest image.	Download firmware from `http://updates.oracle.com` or vendor sites.	Use a CD or DVD to load the software. Then use the **Upload ISO Images** action, the **Upload Firmware** action, and the **Import Images** actions to update the contents of the Enterprise Controller's software library.

Table 2–1 (Cont.) Comparison of Functions in Different Connection Modes

Operation	Connected Mode	Disconnected Mode
Use Automatic Service Requests (ASR)	After you register the assets in the My Oracle Support database and register a user account as the My Oracle Support user, you have the option to create a service request whenever an incident is reported. In an Automated Service Request, the following information is sent from the Enterprise Controller to My Oracle Support: serial number FRU data IP address site location hardware SNMP trap	Contact My Oracle Support to request service.
Create a Services Request	After you register the assets in the My Oracle Support database and register a user account as the My Oracle Support user, select the **Open Service Request** action.	Contact My Oracle Support to request service. The **Open Service Request** action is disabled.
Verify warranties	After you register the assets in the My Oracle Support database and register a user account as the My Oracle Support user, view the warranty of a specific asset or all assets.	Contact My Oracle Support to coordinate warranty records with your own records.

Secure the Log Files

All installation and upgrade log files remain in place to assist in diagnosing any problems with the installation or upgrade. Because their content can be considered sensitive, archive them securely and remove the files after a successful installation or upgrade.

The product installs a diagnostic program,`OCDoctor`, that gathers logged data, analyzes an installation for common errors, and responds to inquiries. To remove the program at any time, delete its files and directories.

The installation logs are found in the following locations:

- Log of a successful installation: `/var/tmp/installer.log.latest`

  Log of a specific installation:

  `/var/opt/sun/xvm/oracle/app/oraInventory/logs/silentInstall<YYYY-MM-DD-HH-MM-SSPM>.log`

- Log of previous installation or uninstallation operations: `/var/tmp/installer.log.`*`xxxx`*
- Log of an agent installation: `/var/scn/install/log`

The log of upgrade actions for the Enterprise Controller and its co-located Proxy Controller is in the file: `/var/opt/sun/xvm/update-saved-state/update_satellite_bundle_12.1.`*`n.xxxx`*`/updatelog.txt`

The log of upgrade actions for a Proxy Controller that is not co-located is in the file: `/var/opt/sun/xvn/update-saved-state/update_proxy_bundle_12.1.`*`n.xxxx`*`/updatelog.txt`

Substitute the Certificates for the Browser

Oracle Enterprise Manager Ops Center has self-signed certificates that it uses for authentication between its web container and a browser client.

- Oracle Glassfish Server is the web container in the current version of the product.
- Apache Tomcat is the web container used in versions of the product prior to Version 12.1.

Self-signed Certificates are site-generated Certificates that have not been registered with any well-known Certificate Authority (CA), and are therefore not guaranteed. These certificates issue a warning when connecting with a browser and require users to accept the certificate.

Java's standard keystore format is JKS, the format created by the `keytool` command-line utility. This tool is included in the JDK and creates the self-signed certificates. The Oracle Enterprise Manager Ops Center keystore for the browser certificates is located in:

```
/var/opt/sun/xvm/bui/conf/keystore
```

The keystore has a password that cannot be configured. The keystore is protected by filesystem permissions.

To ensure that the data being transmitted and received is private and not vulnerable to eavesdropping, a self-signed certificate is sufficient. However, to ensure that connections are authentic, replace the self-signed certificates with Class A or B certificates from an third-party Certificate Authority such as Verisign.

Obtaining a Certificate Authority's Certificate

1. Identify the Certificate Authority you want to use.
2. Submit a request for a certificate to the Certificate Authority, according to their instructions. The Certificate Authority returns a certificate to you.
3. Download a Chain Certificate from the Certificate Authority, according to their instructions.
4. Verify the certificates' fingerprints. When you add a certificate to the keystore, any transactions using that certificate become trusted. You must be certain that the certificates you received are authentic before you import them. Use the keytool's `print` command to see the fingerprints and then communicate with the Certificate Authority to compare the fingerprints. To see a certificate's fingerprint, use the following command:

   ```
   keytool -printcert -file <path/filename>
   ```
5. Replace the self-signed certificate with the CA certificate, as described in the following sections.

Substituting Certificates in the Current Version

To replace the self-signed certificate with a certificate from a Certificate Authority, use the following procedure:

1. Import the Chain Certificate in the Oracle Enterprise Manager Ops Center keystore:

   ```
   keytool -import -alias root -keystore /var/opt/sun/xvm/bui/conf/keystore
   -trustcacerts -file <chain_certificate>
   ```

2. At the prompt for the password to the keystore, enter the following:

```
trustpass
```

3. Confirm the certificate's authenticity.
4. Import the certificate that the CA sent to you into the keystore:

```
keytool -import -alias <hostname>-ca -keystore
/var/opt/sun/xvm/bui/conf/keystore -trustcacerts -file <your_certificate>
```

   where *<hostname>* is the name of the system on which the Enterprise Controller is running and *<your_certificate>* is the name of the file containing the certificate sent from the Certificate Authority.

5. At the prompt, enter the password to the keystore and verify the certificate's authenticity.

Substituting Certificates in Versions Before 12.1.0.0

To replace the self-signed certificate with certificates from a Certificate Authority, use the following procedure on systems running Oracle Solaris 10 and Oracle Linux.

> **Note:** Do not attempt this procedure on systems running Oracle Solaris 11 because it will affect the communication between the agent and the Enterprise Controller.

The procedure is not available for Oracle Solaris 11.

1. Stop the Enterprise Controller and Proxy Controllers.
2. Copy the Certificate Authority certificate files to a directory on your server. This is a temporary location.
3. Rename the Certificate Authority certificate file to `server.crt`
4. Rename the Certificate Authority key file to `server.key`
5. Navigate to the location of the self-signed certificate and key files for the Apache Tomcat web container:
   - Oracle Solaris 10: `/var/opt/sun/xvm/uce/etc.opt/server/uce_server/ssl.crt`
   - Linux: `/var/opt/sun/xvm/uce/etc/uce_server/ssl.crt`
6. Move the current `server.crt` file and `server.key` file from the `ssl.crt` directory to an alternate, secure location.
7. Copy the CA files from the temporary location to the `ssl.crt` directory.
8. Change the permissions so that the files can be ready by only root:

```
chown uce-sds:uce-sds <filename>
chmod 400 <filename>
```

The files now have these permissions:

```
-r--------  1 uce-sds  uce-sds  1751 Jun 13 13:05 server.key
-rw-r--r--  1 uce-sds  uce-sds  1220 Jun 13 13:05 server.crt
```

9. If the `server.key` file is encrypted and requires a passphrase, edit the following file to change the echo output to the passphrase.

- Oracle Solaris 10: `/var/opt/sun/xvm/uce/etc.opt/server/uce_server/.sslphrase`
- Linux: `/var/opt/sun/xvm/uce/etc/uce_server/.sslphrase`

10. Use a script or the command line to define these variables:

```
SDS_KEYS=/path/to/your_certificate
SMSF_STORE=/var/opt/sun/xvm/security/jsse/smsfacade/jssecacerts
SMSF_PASS=`cat /var/opt/sun/xvm/persistence/scn-satellite/satellite.properties
| grep engine.installcert.passphrase |awk -F= '{print $2}'`
```

In addition, define these OS-specific variables:

- Oracle Solaris 10:

```
TRUST_STORE=/etc/cacao/instances/oem-ec/security/jsse/truststore
TRUST_PASS=`cat /etc/cacao/instances/oem-ec/private/cacao.properties | grep
com.sun.cacao.ssl.truststore.password |awk -F= '{print $2}'`
```

- Linux:

```
TRUST_STORE=/etc/opt/sun/cacao2/instances/oem-ec/security/jsse/truststore
TRUST_PASS=`cat
/etc/opt/sun/cacao2/instances/oem-ec/private/cacao.properties | grep
com.sun.cacao.ssl.truststore.password |awk -F= '{print $2}'`
```

11. Remove the old alias from the `cacao` and `smsfacade` truststores and import the new certificates:

```
$LATEST_JDK/bin/keytool -delete -alias sds -keystore $TRUST_STORE -storepass
$TRUST_PASS -noprompt
$LATEST_JDK/bin/keytool -importcert -file $SDS_KEYS -alias sds -keystore
$TRUST_STORE -storepass $TRUST_PASS -noprompt
$LATEST_JDK/bin/keytool -delete  -alias 127.0.0.1-1 -keystore $SMSF_STORE
-storepass $SMSF_PASS -noprompt
$LATEST_JDK/bin/keytool -importcert -file $SDS_KEYS -alias 127.0.0.1-1
-keystore $SMSF_STORE -storepass $SMSF_PASS -noprompt
```

12. Start the Enterprise Controller and Proxy Controllers.

Secure the Databases

Database passwords are encrypted in `/var/opt/sun/xvm/dbpw.properties`, using AES 128-bit encryption. The Advanced Encryption Standard (AES) specification defines one key for both encrypting and decrypting electronic data.

Securing a Local Database

Access to the local database is restricted to processes on the Enterprise Controller. To allow an external host to get access to the database, you must modify the Oracle*Net Listener configuration, as described in Getting Access to the Database Data.

- You must protect the properties file for the database, `/var/opt/sun/xvm/db.properties`, because it contains schema names and passwords. Use the most restrictive permission: read-only by file owner.
- You must protect the compressed file created when you use the `ecadm backup` command, as described in Backing Up and Restoring the Enterprise Controller. This tar file contains the dump of the local database. You must also ensure that the backup file is moved to an alternate location.

Securing a Remote Database

- You must remove the `remoteDBCreds.txt` file after installation. The file contains unencrypted credentials for the schema on the customer-managed database, used to configure the connection between the Enterprise Controller and the remote database. The file is located on the system that hosts the Enterprise Controller in a directory chosen by the administrator who installed the software.
- If you are upgrading from product version 12*c* Release 1 (12.1.0.0.0) to a later version and use a remote database, you must also execute the `refactorOCPrivs_12.1.x.0.sql` script as described in the following section to further tighten security for the schema owner on the remote database.
- /You must protect the properties file for the database, `var/opt/sun/xvm/db.properties`, because it contains schema names and passwords. Use the most restrictive permission: read-only by file owner.
- You must ensure that a remote database is included in your site's routine backup plan so that the Oracle Enterprise Manager Ops Center data can always be recovered.

Using the refactorOCPrivs_12.1.x.0.sql Script

Use a database administrator account for this procedure.

To obtain the schema names for the remote database, view the `/opt/sun/xvm/db.properties` file and search for the `mgmtdb.appuser` and `mgmtdb.roappuser` values.

1. Copy the `refactorOCPrivs_12.1.x.0.sql` script from the Enterprise Controller's system to the Oracle account on the server where the customer-managed database instance is installed. The script is located in the following location of the Enterprise Controller's system:
   - On Oracle Solaris: `/opt/ORCLsysman-db/sql/update/delta-update1/oracle/refactorOCPrivs_12.1.x.0.sql`
   - On Linux: `/opt/orcl-sysman-db/sql/update/delta-update1/oracle/refactorOCPrivs_12.1.x.0.sql`
2. Log in as the database administrator and execute the SQL script, using the following command:

   ```
   sqlplus / as sysdba @refactorOCPrivs_12.1.1.0.sql
   ```

3. At the prompts for Ops Center database login and Read-Only Ops Center database login, enter the schema names created when the remote database was created.
4. Verify the new roles and privileges by running the following SQL statement in a privileged database administrator account:

   ```
   set pages 0
   Select
      lpad(' ', 2*level) ||
      Granted_Role "User, his roles and privileges"
   From
     (
   -- THE USERS
       Select
          null  Grantee,
   ```

```
        UserName Granted_Role
     From
        Dba_Users
    Where
       UserName Like Upper('&_OC_SYSTEM_SCHEMA%')
-- ROLES TO ROLES RELATIONS
Union
    Select
       Grantee,
       Granted_Role
    From
       Dba_Role_Privs
-- THE ROLES TO PRIVILEGE RELATIONS
 Union
    Select
       Grantee,
       Privilege
    From
        Dba_Sys_Privs
  )
Start With
   Grantee is null
Connect By
   Grantee = Prior Granted_Role
/

Enter the value for the OC System Database Login (i.e the value for
mgmtdb.appuser) at the prompt:
    Enter value for _oc_system_schema: OC <cr>
```

The following are the new roles and privileges, in addition to those granted when the original schema was created such as `CREATE DATABASE LINK`.

```
CREATE TABLE
    CREATE VIEW
    OC_SYSTEM_ROLE
      CREATE CLUSTER
      CREATE INDEXTYPE
      CREATE OPERATOR
      CREATE PROCEDURE
      CREATE SEQUENCE
      CREATE SESSION
      CREATE TRIGGER
      CREATE TYPE
```

The following are the Read Only roles and permissions.

```
CREATE SESSION
CREATE SYNONYM
```

Changing the Database Credentials for the Ops Center User

You can change the database password for the Oracle Enterprise Manager Ops Center user on an embedded or customer-managed database. The Enterprise Controller's services must be restarted to use the new password.

Use this procedure to change the credentials:

1. Create a temporary file containing the new password and use the most restrictive permissions for the file. For example:

```
# vi /tmp/password
newpassword
```

```
# chmod 400 /tmp/password
```

2. Use the `ecadm` command with the `change-db-password` subcommand and the `-p <password file>` option to change the database password. At the prompt, confirm that you want the Enterprise Controller to restart. For example:

```
# ./ecadm change-db-password -p /tmp/password
The Enterprise Controller will be restarted after the database password is
changed. Continue? (y/n)
y
ecadm:    --- Changed database password, restarting.
ecadm: shutting down Enterprise Controller using SMF...
ecadm: Enterprise Controller services have stopped
ecadm: Starting Enterprise Controller with SMF...
ecadm: Enterprise Controller services have started
#
```

3. If you have a high availability configuration, the `ecadm` command copies the new database properties to each standby cluster node. Enter the root password for each standby cluster node. For example:

```
ecadm:    --- Changed database password, restarting.
The DB configuration file must now be copied to each remote cluster node.
You will be prompted for the root password for each node to perform the copy.
Copying to node OC-secondary
Password: password
<output omitted>
ecadm:    --- Enterprise Controller successfully started HA
#
```

4. Delete the temporary file containing the new password.

```
# rm /tmp/password
```

Changing the Database Credentials for the Read-Only User

You can change the database password for the read-only user on an embedded or customer-managed database. The Enterprise Controller's services must be restarted to use the new password.

Use this procedure to change the credentials:

1. Create a temporary file containing the new password and use the most restrictive permissions for the file. For example:

```
# vi /tmp/password
newpassword
```

2. Use the `ecadm` command with the `change-db-password` subcommand and the `-p <password file>` and `-r` options to change the database password. When prompted, confirm the Enterprise Controller restart. For example:

```
# ./ecadm change-db-password -r -p /tmp/password
The Enterprise Controller will be restarted after the database password is
changed. Continue? (y/n)
y
ecadm:    --- Changed database password, restarting.
ecadm: shutting down Enterprise Controller using SMF...
ecadm: Enterprise Controller services have stopped
ecadm: Starting Enterprise Controller with SMF...
ecadm: Enterprise Controller services have started
#
```

3. If you have a high availability configuration, the `ecadm` command copies the new database properties to each remote cluster node. Enter the root password for each remote cluster node. For example:

```
ecadm:    --- Changed database password, restarting.
The DB configuration file must now be copied to each remote cluster node.
You will be prompted for the root password for each node to perform the copy.
Copying to node OC-secondary
Password: password
<output omitted>
ecadm:    --- Enterprise Controller successfully started HA
#
```

4. Delete the temporary file containing the new password.

```
# rm /tmp/password
```

Disable the Data Model Navigator

Oracle Enterprise Manager Ops Center provides a Data Model Navigator to allow Oracle support personnel to gather detailed information about the state of the system from a model view of the system. This diagnostic interface is enabled by default and requires user authentication for access. Because it represents an internal view of the system, disable the interface and enable it only when in communication with Oracle support personnel.

Disable the interface using the following procedure:

1. Log in to the Enterprise Controller as the `root` user.
2. For an Oracle Solaris system, copy `/etc/cacao/instances/oem-ec/modules/restfuladaptor.xml` to `/etc/cacao/instances/oem-ec/modules/restfuladaptor.xml.orig`

   For a Linux system, copy `/etc/opt/sun/cacao/instances/oem-ec/modules/restfuladaptor.xml` to `/etc/opt/sun/cacao/instances/oem-ec/modules/restfuladaptor.xml.orig`
3. Edit the new file and locate the line: `ignored-at-startup="No"`
4. Change the value so that the line is: `ignored-at-startup="Yes"`
5. Save the file.
6. Repeat the procedure on each Proxy Controller:
   a. For an Oracle Solaris system, copy the file `/etc/cacao/instances/scn-proxy/modules/com.sun.hss.proxy.restfuladaptor.xml`

      For a Linux system, copy the file `/etc/opt/sun/cacao/instances/scn-proxy/modules/com.sun.hss.proxy.restfuladaptor.xml`
   b. Edit the file to change the value and save it.
   c. Stop and restart the Proxy Controller:

      ```
      /opt/SUNWxvmoc/bin/proxadm stop
      /opt/SUNWxvmoc/bin/proxadm start
      ```
7. Stop and restart the Enterprise Controller:

```
/opt/SUNWxvmoc/bin/satadm stop
/opt/SUNWxvmoc/bin/satadm start
```

Secure the Agents

To encrypt the credentials used to get access to the Agent Controller of an asset:

1. Check the status of the agent:

```
/var/opt/sun/xvm/OCDoctor/OCDoctor.sh --update
/var/opt/sun/xvm/OCDoctor/OCDoctor.sh --troubleshoot
```

2. Check the prerequisites for encryption and then encrypt the agent password:

```
/var/opt/sun/xvm/OCDoctor/OCDoctor.sh --troubleshoot --fix
```

Secure the Web Browsers

To implement transactions securely, Oracle Enterprise Manager Ops Center supports specific communications and security standards and methods such as HTTP, SSL, x.509 certificates, and Java. Most browsers support several of these features but users must configure their browsers properly to take advantage of security capabilities.

Information sent to and from a browser is transmitted in the clear so any intermediate site can read the data and potentially alter it in transit. Oracle Enterprise Manager Ops Center's browsers and servers address this problem in part by using the Secure Sockets Layer to encrypt HTTP transmissions (referred to as HTTP/SSL or HTTPS). This ensures the security of data transmitted from the client to the server. However, because browsers do not ship with client certificates, most HTTP/SSL transmissions are authenticated in only one direction, from server to client. The client does not authenticate itself to the server.

The browser interface uses JavaScript extensively. Take care to protect against JavaScript-based attacks.

Use Strong Cipher Encryption

> **Note:** Some locales do not allow the use of strong ciphers. Use this type of encryption only if local legislation allows it.

If you modify an asset's `sshd` daemon to use a strong cipher such as AES-256 encryption, you must also configure the Proxy Controller to manage the asset. To determine if the `sshd` daemon has been modified, view the `/etc/ssh/sshd_config` file, in the Ciphers section, to see if it contains content such as this:

```
Ciphers aes256-cbc
```

To discover and manage assets that use a strong cipher suite configuration, you must download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files and move them to the Proxy Controller systems.

Configuring Proxy Controllers to Use a Strong Cipher Suite Configuration

1. On an Internet-facing system, navigate to `http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html`.
2. Select Accept License Agreement.
3. Click the `UnlimitedJCEPolicyJDK7.zip` link and download the file.

4. Unzip the `UnlimitedJCEPolicyJDK7.zip` file.
5. Move the `local_policy.jar` and `US_export_policy.jar` files to the `/usr/jdk/jdk<latest version>/jre/lib/security/` directory on the Proxy Controller.
6. Restart the Proxy Controller system.

Viewing the Enterprise Controller's Configuration

To view the Enterprise Controller's configuration, select the Enterprise Controller in the Administration section of the Navigation pane, then click the Configuration tab. Select one of the following subsystems to display its settings.

- Agent Provisioning – Manages the provisioning of Agent Controllers.
- Automated Service Requests – Manages the Automated Service Request (ASR) settings.
- Database – Manages the database used by Oracle Enterprise Manager Ops Center.
- EC Manager – Manages the Enterprise Controller.
- Firmware – Manages firmware downloads.
- Job Manager – Manages the way that jobs are run.
- My Oracle Support (MOS) – Manages Oracle Enterprise Manager Ops Center's communications with MOS.
- Network/Fabric Manager – Manages networks and fabrics.
- OCDoctor – Manages the OCDoctor location and updates.
- OS Provisioning – Manages network and fabric settings.
- Permission Cache – Manages cache sizes.
- Power – Manages energy cost settings.
- Proxy Manager – Manages the interactions between the parts of the infrastructure.
- Quartz Scheduler – Manages the quartz scheduler.
- Role Preferences – Manages role settings.
- Update – Manages the location of update libraries.
- Zone Controller – Manages the zone management settings.

Editing the Configuration

Use roles to control access to the Enterprise Controller's configuration after installation. The Ops Center Admin role is the only role that can modify the configuration properties. Use care in assigning this role to a user.

Note: Editing configuration properties can have an adverse affect on the stability and performance of the product and is done only if directed by My Oracle Support.

Getting Access to the Database Data

The information in this section is also in *Oracle Enterprise Manager Ops Center Accessing Core Product Data* in the How To library.

This section describes how to view the core product data stored in the Oracle Enterprise Manager Ops Center database using Oracle SQL Developer or SQL*Plus. Use this information to integrate this product with other applications such as Oracle Enterprise Manager Cloud Control, or to pull data from the Oracle Enterprise Manager Ops Center datastore for analytical applications. To use Oracle SQL Developer, you need the following information:

- **Database host name** – The name of the database host is listed in the `mgmt.dburl` property of the `/var/opt/sun/xvm/db.properties` file on the Enterprise Controller system. The format for this property is: `jdbc:oracle:thin:@<databasehostname>:<listenerPort>/<OracleServiceName>`.
- **Read-Only User Name** – The Read-Only User name is a schema on the Oracle Enterprise Manager Ops Center Repository that is configured to access Oracle Enterprise Manager Ops Center data using read-only views. When the Enterprise Controller uses an embedded database, the username is `OC_RO`. When the Enterprise Controller uses a customer-managed database, the schema name is included in the `mgmtdb.roappuser` property of the `/var/opt/sun/xvm/db.properties` file.
- **Read-Only Password** – When your Enterprise Controller is configured with the embedded database, the password is randomized at installation. If you do not know the embedded database password, see the Database Management chapter in the *Oracle Enterprise Manager Ops Center Administration Guide* for information about changing the password. If you are using a customer-managed database and you do not know the password, ask your database administrator for assistance.
- **Listener Port** – The listener port number for the database is listed in the `mgmt.dburl` property of the `/var/opt/sun/xvm/db.properties` file on the Enterprise Controller system. The format for this property is: `jdbc:oracle:thin:@<databasehostname>:<listenerPort>/<OracleServiceName>`.
- **Oracle Service Name** – For embedded databases, the service name is `OCDB.us.oracle.com`. For customer-managed databases, the service name is listed in the `mgmt.dburl` property of the `/var/opt/sun/xvm/db.properties` file on the Enterprise Controller system. The format for this property is: `jdbc:oracle:thin:@<databasehostname>:<listenerPort>/<OracleServiceName>`.

Viewing Core Product Data Using Oracle SQL Developer

Using Oracle SQL Developer, you can connect to the database using a read-only account and view the schema structures and data.

Modifying Oracle*Net Listener

To allow an external host to get access to the database, you must modify the Oracle*Net Listener configuration on the Enterprise Controller:

1. Change to Oracle Enterprise Manager Ops Center's user environment:

```
$ su - oracleoc
```

2. Edit the `sqlnet.ora` file:

```
vi $ORACLE_HOME/network/admin/sqlnet.ora
```

3. Disable valid node checking by commenting the following lines:

```
#tcp.validnode_checking = yes
#tcp.invited_nodes = (localhost,x4150-brm-04)
```

4. Save the file and exit.

5. To use the new version of the file, either restart all services on the Enterprise Controller, or reload the Oracle*Net Listener configuration from the `oracleoc` user environment.

```
/opt/SUNWxvmoc/bin/satadm stop -w
/opt/SUNWxvmoc/bin/satadm start -w
```

OR

```
$ lsnrctl reload OCLISTENER
```

Opening Oracle*Net to External Access

If you are using the embedded database, you must open Oracle*Net to enable external access before you can connect to the database.

1. Log in to the Enterprise Controller system.

2. Change to the user that owns the Oracle software. For example:

```
$ su - oracleoc
```

3. Modify the `sqlnet.ora` file to comment out the two lines beginning with `tcp.validnode_checking` and `tcp.invited_nodes`. For example:

```
$ vi $ORACLE_HOME/network/admin/sqlnet.ora
#tcp.validnode_checking = yes
#tcp.invited_nodes = (localhost,<EnterpriseControllerHostname>)
```

4. Use the `lsnrctl reload` command to reload the listener configuration without stopping the Enterprise Controller services. For example:

```
$ lsnrctl reload OCLISTENER
```

Creating the Connection to the Database

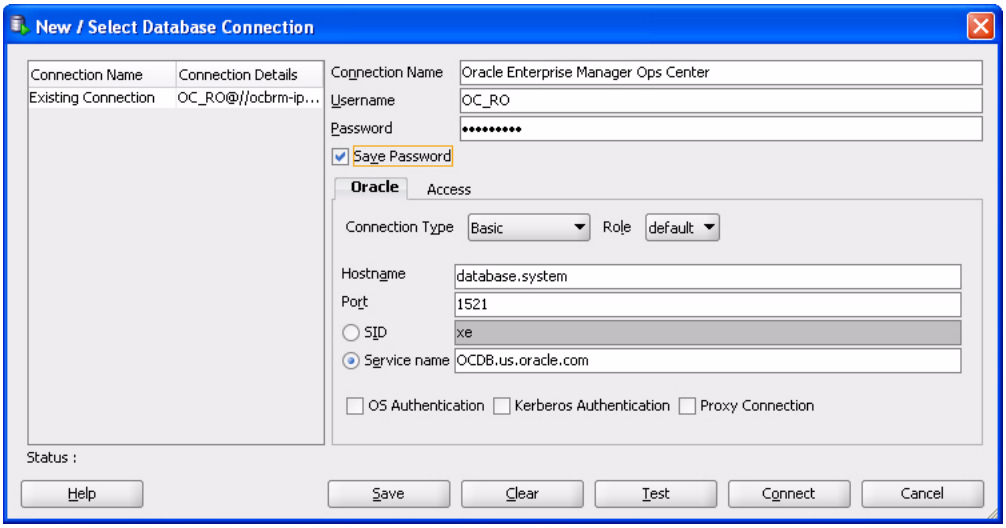
You must create a connection to the Oracle Enterprise Manager Ops Center database in Oracle SQL Developer.

1. In Oracle SQL Developer, click the New Connection icon in the Connections tab.

2. Enter the connection information, then click Save:

   - **Connection Name** – Enter a name. This name is only used in Oracle SQL Developer.
   - **Username** – Enter the schema name for the read-only user.
   - **Password** – Enter the password for the read-only user.
   - **Host name** – Enter the name of the database host.
   - **Port** – Enter the Oracle*Net Listener port number.

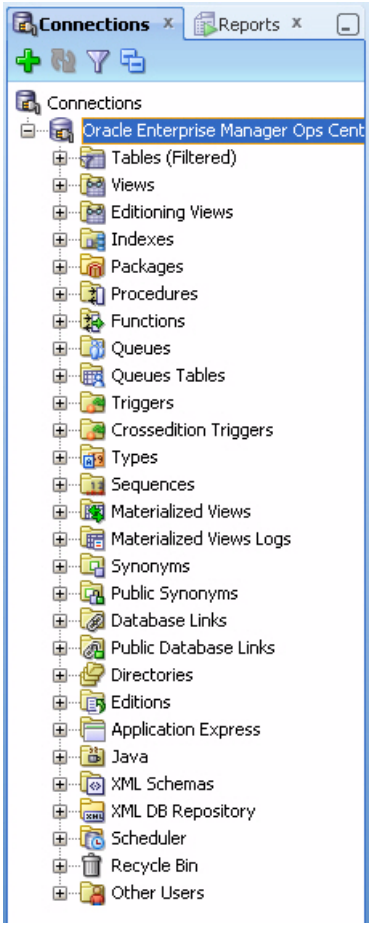
- **Service Name** – Select the service name option and enter the service name. For embedded databases, the service name is `OCDB.us.oracle.com`. For customer-managed databases, the service name is included in the `mgmtdb.dburl` property in the `/var/opt/sun/xvm/db.properties` file.



Viewing Data From the Database Using Oracle SQL Developer

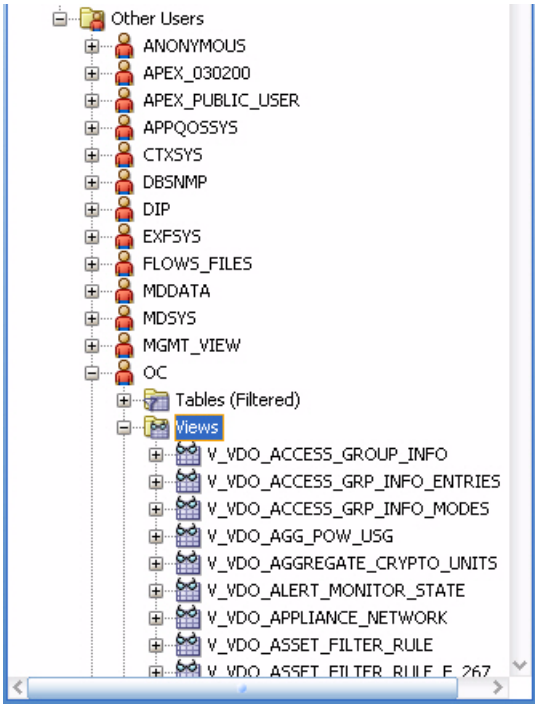
After you create the connection, view product data:

1. Select the connection you created in the previous procedure. The contents of the target database are displayed.



2. Within the database hierarchy, expand the Other Users section, then select the application user and expand the Views section. If you are using an embedded database, the application user is OC. If you are using a customer-managed database, the application user is included in the `mgmtdb.appuser` property of the `/var/opt/sun/xvm/db.properties` file.

   The database columns visible to the application user are displayed.



3. View the comment column to find the location of the Javadoc for each column, which explains the usage of the column.

> **Note:** The `SUNWxvmoc-sdk.pkg` package, which is included with the product installation media, installs Javadoc. If this package is not installed on your system, use the `pkgadd` command to install it for Oracle Solaris systems, or the `rpm` command to install it for Linux systems.

After you get access to the product data, you can integrate the data with other applications, run analytics on the product data, or take other actions that require the data.

Viewing Core Product Data Using SQL*Plus

If you have access to the Enterprise Controller system, you can access the database from the command line.

1. Log in to the Enterprise Controller system.
2. Run the `ecadm sqlplus` command. Use the `-r` option to access the database in read-only mode.

   You are connected to the database using the SQL*Plus interface.
3. Invoke commands using the SQL*Plus syntax.
   - To see a list of views:

     ```
     select view_name from user_views where (view_name like 'V_VMB%' or view_
     name like 'V_VDO%')
     ```

   - To see comments on a specific view:

```
select comments from user_tab_comments where table_name='<view name from
the above list>'
```

- To see comments on all columns of a specific view:

```
select column_name, comments from user_col_comments where table_name='<view
name from the above list>'
```

3

Security Features

Oracle Enterprise Manager Ops Center provides security services for user authentication, custom user authorization, and protection for data in repositories and during network transmissions. Oracle Enterprise Manager Ops Center also provides network authentication between its infrastructure components using standard certificates.

Oracle Enterprise Manager Ops Center uses standard protocols and third-party solutions to secure data and operations, using SSL and X.509v3 certificates, and secure HTTP and PAM (Pluggable Authentication Modules) protocols to provide the following services:

- Authentication
- Authorization
- Access Control
- Data Protection

Configuring and Using Authentication

Authentication allows a system to verify the identity of users and other systems that request access to services or data. In a multi-tier application, the entity or caller can be a human user, a business application, a host, or one entity acting on behalf of another entity.

Identity Management for Users

Users log in to the browser interface to use the product. The credentials must be valid for the Oracle Enterprise Manager Ops Center installation.

Add users to Oracle Enterprise Manager Ops Center from the local authentication subsystem of the Enterprise Controller's operating system or from a separate directory server.

Configuring an LDAP Server

You can add directory servers to Oracle Enterprise Manager Ops Center. Users and roles are added to the product from the directory server. The information in this section is also in the *Oracle Enterprise Manager Ops Center Administration Guide*.

To Configure the Directory Server

1. Create the following user groups on the directory server:
   - ASSET_ADMIN

- CLOUD_ADMIN
- CLOUD_USER
- EXALOGIC_ADMIN
- FAULT_ADMIN
- NETWORK_ADMIN
- OPS_CENTER_ADMIN
- PROFILE_PLAN_ADMIN
- READ
- REPORT_ADMIN
- ROLE_ADMIN
- SECURITY_ADMIN
- SERVER_DEPLOY_ADMIN
- STORAGE_ADMIN
- Update_ADMIN
- Update_SIM_ADMIN
- USER_ADMIN
- VIRT_ADMIN

2. Add users to these groups. The users within each group are given the role corresponding to the group.

To Add a Directory Server

1. Select Administration in the Navigation pane.
2. Click Directory Servers.
3. Click the Add Directory Server icon. The Remote Directory Server Connection Settings page is displayed.
4. Enter the following connection settings:
   - **Name** – The name of the directory server
   - **Hostname** – The name of the host for the directory server
   - **Port** – The port number to be used to access the directory server
   - **Use SSL** – Check this box to use SSL to connect to the directory server
   - **Username** – The user name used to access the directory server
   - **Password** – The password for the given user name

   Click Next. The Remote Directory Server Schema Settings page is displayed.
5. Enter the following schema settings:
   - **Root suffix** – The root node of the directory hierarchy for the user search
   - **User search DN** – The subnode in which to search for users
   - **User search scope** – The scope of the user search. Acceptable values are base, one, subtree, baseObject, singleLevel, wholeSubtree, or subordinateSubtree.

- **User search filter** – An LDAP search filter which users must meet for inclusion.

Click **Next**. The Summary page is displayed.

6. Review the summary, then click **Add Directory Server**.

Configuring PAM Authentication

Oracle Enterprise Manager Ops Center uses Pluggable Authentication Modules (PAM) to validate credentials for user accounts of users who log in to the browser interface. The default PAM service allows Oracle Enterprise Manager Ops Center users to log in to the system in the standard way.

The `pam-service-name` parameter sets the PAM service for the `oem-ec` instance of the `cacao` daemon.

- Oracle Solaris: The default value is `pam-service-name=other`
- Linux: The default value is `pam-service-name=passwd`

If you require control of Oracle Enterprise Manager Ops Center's PAM configuration, create a PAM service with a different service name, which uses different PAM modules.

To see the current value of the `pam-service-name` parameter, use the following `cacaoadm` command:

```
./cacaoadm get-param -i oem-ec pam-service-name
```

To change the authentication service from the operating system's default to a different service name, use the following procedure. If this is a High Availability environment, perform the procedure on both the primary node and on the standby node.

1. On a Linux system, create a configuration file or edit the existing configuration file for the service to use. The configuration file has the same name as the service.

   `/etc/pam.d/`*`filename`*

   On an Oracle Solaris 10 system, edit the following file:

   `/etc/pam.conf`

2. Change the contents of the configuration file. For example:

```
auth       required     pam_warn.so debug
auth       required     pam_safeword.so.1 debug
account    include      system-auth
password   include      system-auth
```

3. To initialize the PAM service with the new configuration, stop the Enterprise Controller:

   ```
   /opt/sun/xvmoc/bin/satadm stop
   ```

4. Change the value of the `pam-service-name` parameter

   ```
   ./cacaoadm set-param -i oem-ec pam-service-name=opscenter
   ```

5. Verify the change:

   ```
   ./cacaoadm get-param -i oem-ec pam-service-name
   ```

6. Restart the Enterprise Controller:

```
/opt/sun/xvmoc/bin/satadm start
```

Note: If you use the SafeNet SafeWord® Agent for PAM software (`pam_safeword.so`), you can use the SafeWord static password mode or single-use dynamic password mode, but you cannot use the dynamic challenge password mode. To use single-use dynamic passwords, you must modify the `pam_safeword.cfg` file to ensure that the User ID source is set to `SYSTEM` and not `USER`. The SYSTEM setting causes the authentication process to get the User ID from the `/etc/passwd` file.

Credentials for My Oracle Support

In Connected mode, the Oracle Enterprise Manager Ops Center software requires the user to provide one or more sets of My Oracle Support credentials. These credentials are used to authenticate and authorize downloading product updates, creating Service Requests, and retrieving warranty information, in addition to the initial authentication between the Enterprise Controller's system and My Oracle Support.

Credentials for IAAS and Cloud Deployments

Some commands for the IAAS platform require a parameter for the location of the private key file. Because the private key authenticates a cloud user, this file is sensitive and must be managed as a security risk:

- The file must be owned by the user running the IAAS command-line interface.
- The file must have the highest restrictive permission: read-only by file owner.

Configuring and Using Authorization

Authorization allows a system to determine the privileges which users and other systems have for accessing resources on that system.

Roles grant users the ability to use the different functions of Oracle Enterprise Manager Ops Center. By giving a role to a user, an administrator can control what functions are available to that user and for which groups of assets.

An Enterprise Controller Admin can grant users different roles for the Enterprise Controller, the All Assets group, and any user-defined groups. A user who is assigned a role for a group receives the same role for all subgroups. See Follow the Principle of Least Privilege for a list of the available roles and their functions.

Caution: A user with the Apply Deployment Plans, Exalogic Systems Admin, or SuperCluster Systems Admin role can apply an operational profile to a managed system using root access. Take care when assigning these roles because the role allows the user to use an operational profile to run scripts.

Credential Management for Assets

Oracle Enterprise Manager Ops Center uses credentials to discover and manage assets and to establish trust between internal components. Examples of the types of credentials managed by Oracle Enterprise Manager Ops Center include:

- SSH credentials for Operating System instances and hardware service processors.
- IPMI credentials for hardware service processors

To see a list of all the types of credentials, select Credentials in the Administration section, then click **Create Credentials** in the Actions pane. The drop-down list shows all of the supported protocols.

Oracle Enterprise Manager Ops Center requires remote network access and administrative privileges to discover and manage an asset. This can be done either by using a privileged account or by combining the credentials of a non-privileged user account with the credentials for the administrative account. In this case, Oracle Enterprise Manager Ops Center uses the non-privileged user account to connect to the system and then uses the administrative account to inquire about the characteristics of the system.

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

Note: IPMI communications from the Proxy Controller to the ILOM system are not encrypted. To protect the transmissions, isolate the ILOM system and the Proxy Controller it uses within your private administrative network.

Using SSH Key-Based Authentication

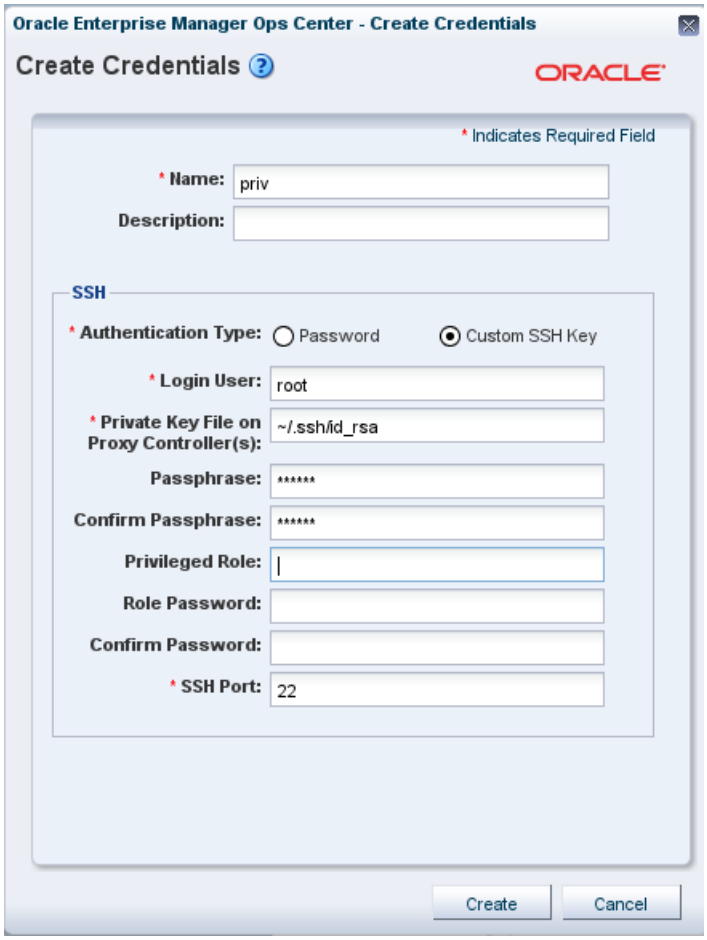
If you prefer not to use password-based SSH credentials, create an SSH key to get access to remote assets, such as operating systems, ILOM service processors, and XSCF service processors. The assets must support the SSH protocol. Oracle Enterprise Manager Ops Center does not protect the SSH keys. If you choose to use this method, you must ensure the following:

- You must create the SSH key on each Proxy Controller that needs to get access to the asset.
- For an OS asset, you must add the SSH public key to the `~/.ssh/authorized_keys` file. For a hardware asset, you must use the asset's Web interface to upload the public SSH key.

To create the SSH key, use the **Create Credentials** action.

1. Enter a name for the key.
2. Click the Custom SSH key button, as shown in Figure 3–1, to enable the remaining fields.

Figure 3–1 Creating an SSH Public Key



3. In Login User, enter the name of the account that uses this key.
4. The location of the key file is set to the default location for the `sshkey-gen` utility. If your site uses a different location, edit this field.
5. (Optional) For OS assets, create a privileged user such as root, or a non-privileged user with keys. Provide a password for the role.

   The passphrase is an optional addition to the password and is created at the same time as the key.
6. Click Create to create the SSH key.

Using the agentadm Command to Manage Assets

The information is this section is also in the *Oracle Enterprise Manager Ops Center Feature Reference Guide*.

Although it is possible to discover assets without providing credentials, Oracle Enterprise Manager Ops Center is limited in its ability to manage or monitor these assets. If you prefer not to store credentials for assets in the product software, install the Agent Controller on each asset manually.

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

Before You Begin

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

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

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

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

Using User Credentials to Install and Configure an Agent Controller Manually This procedure creates a file that holds the password of the administrative user for your Oracle Enterprise Manager Ops Center installation.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    - Oracle Solaris OS – Use the `/opt/SUNWxvmoc/bin/agentadm` command.

- Linux OS – Use the `/opt/sun/xvmoc/bin/agentadm` command

The example commands below use the following options:

- `configure` – Causes an Agent Controller configuration operation to take place.
- `-u` – Specifies the administrative user that exists on the Enterprise Controller to which the Proxy Controller is connected. Be certain that the password that you specified in the `/var/tmp/OC/mypasswd` file is correct for the user that you specify for this option.

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

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

  Error messages similar to *Connection cannot be registered* in the following example typically indicate problems with the user credentials that you specified in the `agentadm` command. In this example, the user `droot` was not authenticated on the Enterprise Controller. If you see this type of error, check

that the user name that you supplied for the `agentadm -u` option, and the password in the file that you specified for the `agentadm -p` option, match an existing administrative user on the Enterprise Controller.

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

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

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

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

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

Correct the connection problem and re-run the `agentadm configure` command.

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

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

Using a Token to Install and Configure an Agent Controller Manually This procedure uses a token to configure your Agent Controller software.

1. On the Enterprise Controller, change to the `/var/opt/sun/xvm/images/agent/` directory and list the contents. This directory contains the Agent Controller installation archives.

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

2. Identify the appropriate Agent Controller archive for the system where you intend to install the Agent Controller, the target system.

3. On the target system, create a directory named `/var/tmp/OC`:

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

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

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

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

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

6. Uncompress the Agent Controller archive:

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

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

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

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

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

(output omitted)

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

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

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

10. Edit the `/var/tmp/OC/mytoken` file so that it contains the auto-reg-token string from the Proxy Controller and make the following changes:
    - Remove the `auto-reg-token=`.
    - Remove any backslash characters from the token string.

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

11. Use the `agentadm` command to associate the Agent Controller with the Proxy Controller.
    - Oracle Solaris OS: Use the `/opt/SUNWxvmoc/bin/agentadm` command.
    - Linux OS: Use the `/opt/sun/xvmoc/bin/agentadm` command.

    The commands have the following options:

    – `configure` – Causes an Agent Controller configuration operation to take place.

    – `-t` – Specifies the absolute path name of the file that contains the registration token.

    – `-x` – Specifies the IP address or host name of the Proxy Controller to which this Agent Controller will connect.

    – `-a` – Specifies the IP address to use during Agent Controller registration. This selects the network interface that the Agent Controller will use for registration. Accept the server's certificate when prompted.

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

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

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

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

```
Added the service tags recreate script successfully.
#
```

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

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

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

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

{output omitted}
End of configuration.
```

Correct the connection problem and re-run the `agentadm configure` command.

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

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

Changing Credentials of Managed Assets

The information is this section is also in the *Oracle Enterprise Manager Ops Center Administration Guide*.

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

To upgrade management credentials, select All Assets and click Upgrade Management Credentials. Select an asset category (operating systems; servers; or chassis, m-series, and switches). Select one or more assets of that category. To assign an existing set of credentials, select Assign existing set and then select an existing set of credentials. To assign a new set of credentials, select Create and assign new set and then enter a protocol, name, and credential information.

Updating Management Credentials To update management credentials, select an asset or group and click **Update Management Credentials** in the Actions pane. Click Select to select an existing set of credentials, or click New to create a new set. Do not change the credentials for an asset in another manner, such as through its own user interface because Oracle Enterprise Manager Ops Center is not updated with new credentials that are added this way.

Creating Management Credentials To create management credentials, select Credentials in the Administration section, then click **Create Credentials** in the Actions pane. Select a protocol, then enter a name for the set of credentials and the protocol's required information.

Editing Management Credentials To edit management credentials, select Credentials in the Administration section, then select a set of credentials and click the Edit Credentials icon. Edit the description and the protocol information, then click OK to save the changes.

Copying Management Credentials Copy an existing set of management credentials to create a new set.

To copy management credentials, select Credentials in the administration section, then select a set of credentials and click the Copy Credentials icon. Edit the name, description, and the protocol information, then click OK to save the new set of credentials.

Deleting Management Credentials When you delete an existing set of management credential, discovery profiles that use the credentials might no longer function, and you must give any Agentless assets that were managed using the credentials a new set.

To delete management credentials, select Credentials in the administration section, then select a set of credentials and click the Delete Credentials icon.

Creating a Credential Plan

As an alternative to using the **Create Credential** and **Edit Credential** actions, create and apply a plan that updates credentials.

1. Expand Plan Management in the Navigation pane.
2. Scroll down to the Credentials section and click it.
3. Click **Create Credentials** in the Action pane.
4. Click the drop-down list of protocols to select the type of protocol. Enter a name and description of the purpose of these credentials, for example, the type of asset they support.
5. Enter the credentials.
6. Click the Create button.

Applying the Credential Plan

To apply a credential plan to an asset:

1. Expand Plan Management in the Navigation pane.
2. Scroll down to the Credentials section and click a plan.

   The window displays the assets that use these credentials and are affected by any change.
3. Click Apply.

Certificate Management

By default, Oracle Enterprise Manager Ops Centers uses self-signed certificates for authentication between the web container and the browser client. Oracle Enterprise Manager Ops Center does not provide certificates signed by a Certificate Authority such as Verisign because an Authority requires the name of the domain where the certificate will be used. The Oracle Enterprise Manager Ops Center software cannot be delivered with a generated signed certificate because the domain where the Web server of the Enterprise Controller runs is unknown until the customer installs the

software. However, after installation, use the procedure in Substitute the Certificates for the Browser to replace the self-signed certificate with a certificate from a Certificate Authority.

Configuring and Using Access Control

Access control allows a system to grant access to resources only in ways that are consistent with security policies defined for those resources.

Protecting Session Data

Oracle Enterprise Manager Ops Center uses cookies to store session data for individual users. The cookies are encrypted using JSESSIONID with the "http-only" flag. The cookies are transmitted using the HTTPS protocol.

The browser controls a session's inactivity timer with a default time of 30 minutes. Consider changing the expiration time to a shorter duration, using the following procedure:

1. Click Setup in the title bar of the browser window.
2. Click My Preferences and then User Interface Preferences, as in Figure 3–2.

Figure 3–2 User Interface Preferences

3. In the Time Intervals section of the User Interface Preferences window, change the value in the Session Timeout field.

Removing Code Examples

The command-line interface includes code examples.If you consider these examples to be a security risk, remove them with the following procedure:

1. Log in as `root` user.
2. Issue the following command:

```
rm -rf /opt/SUNWoccli/doc/examples
```

Configuring and Using Data Protection

- Using an NFS Server
- Backing Up and Restoring the Enterprise Controller

Using an NFS Server

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

The Oracle Enterprise Manager Ops Center software prepares an NFS client to mount the share. Use the following procedure to prepare the NFS server on an Oracle Solaris

10. The same procedure is also supported in Oracle Solaris 11 system, or you can use a new procedure, described in Oracle Solaris Administration: ZFS File Systems.

Setting Up a Share on an NFS Server

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

```
# mkdir -p /export/lib/libX
# chmod 777 /export/lib/libX
```

2. Open the /etc/dfs/dfstab file on the NFS server.
3. Add an entry to share the directory. For example, to share the directory named /export/lib/libX, create the following entry:

```
share -F nfs -o rw,"Share 0" /export/lib/libX
```

   If you want the NFS share to be accessible from other network domains, use the rw option to specify a list of allowed domains:

```
share -F nfs -o rw=IPaddress1,IPaddress2 "Share 0" export/lib/libX
```

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

```
# shareall
# share
export/lib/libX   rw, "Share 0"
```

   The share now allows a root user on the NFS clients to have write privileges.

Backing Up and Restoring the Enterprise Controller

The information is this section is also in the *Oracle Enterprise Manager Ops Center Administration Guide*.

Oracle Enterprise Manager Ops Center has several tools that can be used for disaster recovery. These tools let you preserve Oracle Enterprise Manager Ops Center data and functionality if the Enterprise Controller or Proxy Controller systems fail.

Some of the procedures described in this section use the ecadm and proxyadm commands. See the *Oracle Enterprise Manager Ops Center Feature Reference Guide* for more information about this command.

- On Oracle Solaris systems, this command is in the /opt/SUNWxvmoc/bin/ directory.
- On Linux systems, this command is in the /opt/sun/xvmoc/bin/ directory.

The ecadm backup and ecadm restore commands back up and restore the Enterprise Controller, but they do not back up or restore the co-located Proxy Controller or libraries.

The ecadm backup command creates a backup file that contains all of the Oracle Enterprise Manager Ops Center information stored by the Enterprise Controller, including asset data, administration data, and job history. Specify the name and location of the backup file and its log file.

If the Enterprise Controller system fails, use the ecadm restore command to restore the Enterprise Controller to its previous state. The ecadm restore command uses the backup file to configure the Enterprise Controller and restore the data. The new Enterprise Controller system must have Oracle Enterprise Manager Ops Center installed but not configured.

Backing Up an Enterprise Controller

Create a backup file of the Enterprise Controller using the `ecadm` command with the `backup` subcommand. By default, the server data is saved in the `/var/tmp/sat-backup-`*`date-time`*`.tar` file. You can specify a different name and location during the backup.

> **Note:** The `ecadm backup` command does not back up the software libraries because the size of OS image files can be large. As a good practice, create the software library for OS images on networked storage (NAS) and include the network storage device in your site's backup plan. As an alternative, back up the Enterprise Controller's directory manually and archive the files on another server, file-share facility, or a location outside of the `/var/opt/sun` directory.

If you are using an embedded database, the backup file includes the Ops Center Schema. If you use a customer-managed database, use the `--remotedb` option to perform a logical backup (datapump dump) of the Ops Center Schema and ensure that the database administrator performs routine backups of the customer-managed database according to site policy.

> **Note:** Because the backup procedure includes the database password file, you must back up the Enterprise Controller each time you change the database credentials. If you do not, a restore operation overwrites the new database credentials.

To Back Up an Enterprise Controller

1. From the command line, log in to the Enterprise Controller system.
2. Use the `ecadm` command with the `backup` subcommand to back up the Enterprise Controller. Use the following options with the command:
   - `-o|--output` *backup_filename* – Specify the file for the backup archive. The default output file is the `/var/opt/sun/xvm/logs/sat-backup-`*`date-time`*`.tar` file.
   - `-c|--configdir` *directory* – Specify an alternate backup configuration directory.
   - `-l|--logfile` *logfile* – Save output in a log file with the specified name. Log files are stored in the `/var/opt/sun/xvm/logs/` directory.
   - `-d|--description` *text* – Include the text as the description of the backup archive.
   - `-r|--remotedb` –When the Enterprise Controller uses a customer-managed database, this option exports the database schema to a file in the OC_DUMP_DIR directory on the database's server. This option does not perform a full database backup. The database administrator must perform a full database backup.
   - `-t|--tag` *text* – Include the text as the tag of the backup archive.
   - `-T|--tempdir` *directory* – Specify the location of the temporary staging directory.
   - `-v|--verbose` – Increase verbosity level (can be repeated)

For example:

```
ecadm backup -o /var/tmp/backup-file-name.tar
```

3. Save the contents of the most recent upgrade installation directory. This directory is a child of the `/var/opt/sun/xvm/update-saved-state/` directory, and is named according to the version number.
4. Copy the backup file to a separate system.

Restoring an Enterprise Controller

Use a backup file to return the Enterprise Controller to the state it had at the time of the backup.

If you are using an embedded database, the process restores the Ops Center Schema to the state of the schema as it was at the time of the backup. If you are using a customer-managed database, use the `--remotedb` option to restore the product schema on the customer-managed database.

To Restore an Enterprise Controller

This procedure restores the data from the archive created by the `ecadm backup` operation. See Example 3–1, Example 3–2, and Example 3–3 for variations.

1. Prepare the Enterprise Controller system.
   - If you are restoring the backup on the same system, but the software has become corrupt or an upgrade failed, uninstall the Enterprise Controller software.

     Run the `install` script with the `-e` and `-k` options. The `-e` option uninstalls the Enterprise Controller and co-located Proxy Controller, and the `-k` option preserves the Oracle Configuration Manager software. For example:

     ```
     # cd /var/tmp/OC/xvmoc_full_bundle
     # install -e -k
     ```

   - If you are restoring the backup on the same system, and the software is functioning normally, unconfigure the Enterprise Controller.
2. Install the Enterprise Controller if it has not been installed, but do not configure the Enterprise Controller. The `restore` command includes your configuration settings.
   - Oracle Solaris OS: See the *Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System*.
   - Linux OS: See the *Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems*.
3. If the Enterprise Controller is not at the same version as was running when the backup was made, upgrade the Enterprise Controller using the command line.
4. Invoke the `ecadm restore` command with the `-i` option that identifies the backup archive. The following options can be used:
   - `-i|--input` *backup_filename* – Specify the file for the backup archive. The default file is `/var/tmp/sat-backup-`*`date-time`*`.tar`.
   - `-c|--configdir` *directory* – Specify an alternate configuration directory.
   - `-l|--logfile` *logfile* – Save output in an alternate log file. The default log file is `/var/opt/sun/xvm/logs/sat-restore-`*`date-time`*`.log`.

- `-r|--remotedb` – If the Enterprise Controller uses a customer-managed database, this command restores the product schema on that database.
- `-T|--tempdir` *directory* –Specify the location of the temporary staging directory.
- `-v|--verbose` – Increase verbosity level (can be repeated)

5. For an Enterprise Controller with a co-located Proxy Controller, restart the co-located Proxy Controller using the `proxyadm` command. The `proxyadm` command is in the same directory as the `ecadm` command.

```
proxyadm start -w
```

6. For an Enterprise Controller with a co-located Proxy Controller, use the Add Assets method to rediscover the system. See the *Oracle Enterprise Manager Ops Center Feature Reference Guide* for more information about the Add Assets procedure. You do not need to re-register the assets.

Note: After restoring the Enterprise Controller, the asset details might take several minutes to display completely in the user interface.

Example 3–1 Restoring an Enterprise Controller With an Embedded Database

In this example, the `restore` command includes options to set the restore in verbose mode and to create a log file for debugging purposes. The input option specifies the backup file location.

```
# /opt/SUNWxvmoc/bin/ecadm restore -v -i /var/tmp/OC/server1/backup-May28-1812.tar
-l SiteX_logfile-restore-May28-1812.log
```

Example 3–2 Restoring an Enterprise Controller With a Customer-Managed Database

In this example, the `restore` command includes the option to restore the database schema on a customer-managed database. The input option specifies the backup file location.

```
# /opt/SUNWxvmoc/bin/ecadm restore -i /var/tmp/OC/server1/backup-May28-1812.tar -r
```

Example 3–3 Restoring an Enterprise Controller With a Customer-Managed Database Without Restoring the Database Schema

In this example, the `restore` command includes options to set the restore in verbose mode and to create a log file for debugging purposes. The input option specifies the backup file location. The `-r` option is not included.

```
# /opt/SUNWxvmoc/bin/ecadm restore -v -i /var/tmp/OC/server1/backup-May28-1812.tar
-l SiteX-logfile-restore-May28-1812.log
```

Index

N

O

P

R

S

T

U

V

W