Oracle® Enterprise Manager Ops Center

Security

12*c* Release 3 (12.3.2.0.0)

E59968-03

June 2016

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

E59968-03

Primary Author: Krithika Gangadhar

Contents

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.

Related Documents

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

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

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

Describes the product’s purpose.

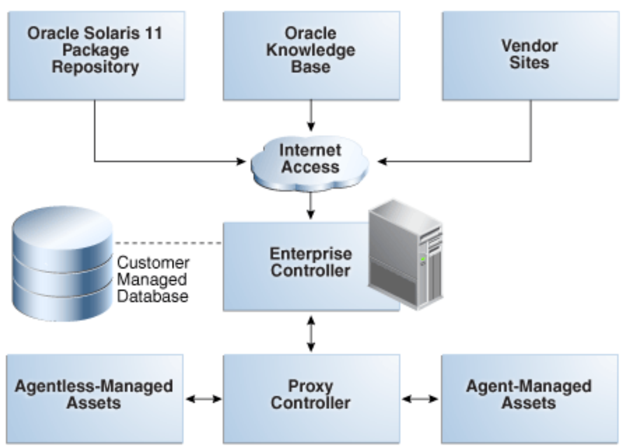
Oracle Enterprise Manager Ops Center is a data center management solution for managing both hardware and software from one console. This document presents good practices for managing the security of Oracle Enterprise Manager Ops Center deployments.

Overview of the Architecture

Describes the components on the product’s solution.

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



About the Knowledge Base (KB) and Package Repository

Describes the components of the product architecture that store images for operating systems.

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.

About the Enterprise Controller

Describes the role of the Enterprise Controller in the product architecture.

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.

About the Proxy Controller

Describes the role of the Proxy Controller in the product architecture.

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.

About the Agent Controllers

Description of the role of the Agent.

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 from the Proxy Controller, performs the required action, and reports results to the Proxy Controller. An agent never communicates directly with the Enterprise Controller and does not initiate operations.

To manage operating systems using agents, an Oracle SE Java Runtime Environment is required. Non-Oracle versions work initially but might exhibit performance and memory issues.

You can choose to manage operating systems without an agent by providing credentials but some product features are not available. See `Using Agent Management for Operating Systems` in the *Oracle Enterprise Manager Operate Reference* for more information about Agent Controllers.

About the Database

Describes the types of databases used in the product.

The Enterprise Controller uses an Oracle Database 12c Enterprise Edition or Oracle Database 11g Enterprise Edition database to store 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.

Security of the Architecture

Description of the locations in the architecture that need to be secured.

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

Table 1-1 Secure Connections

Connection	To Make Secure
From Internet to the Enterprise Controller	About Restricting Network Access About the Connection Mode
Between Enterprise Controller and database	About Database Credentials
Between Enterprise Controller and LDAP server	‘To Add a Directory Server
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 for Oracle Solaris Operating System* and the *Oracle Enterprise Manager Ops Center Installation for Linux Operating Systems*
Between Proxy Controller and assets	Authentication is configured when the asset is discovered and managed as described in About Authentication Between the Proxy Controller and Agents

About Authentication Between the Proxy Controller and Agents

Description of the relationship between Proxy Controllers and Agent Controllers.

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 this section.

For an agentless-managed asset, authentication requires an SSH password as described in About Credentials 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.

About Authentication of Agent-Managed Asset

Describes the result of installing an Agent Controller on an 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
- Authentication of the Proxy Controller

Overview of the Authentication of the Agent

Describes the process of how a Proxy Controller authenticates an Agent Controller.

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.

Overview of the Authentication of the Proxy Controller

Describes the process of how an Agent Controller authenticates a Proxy Controller.

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

About Authenticated Transactions

Description of the authentication process

When 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 handshake.

If the agent does not confirm the Proxy Controller's certificate, the 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

Lists good security practices

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

Topics

- About Keeping Software Up To Date
- About Restricting Network Access
- About the Principle of Least Privilege
- About Monitoring System Activity

About Keeping Software Up To Date

Description of a good practice for security.

Good security is maintained when all software versions and patches are current. This document discusses Oracle Enterprise Manager Ops Center version 12*c* Release 3 (12.3.2.0.0). As new versions or updates of Oracle Enterprise Manager Ops Center become available, install the new software as soon as possible.

About Restricting Network Access

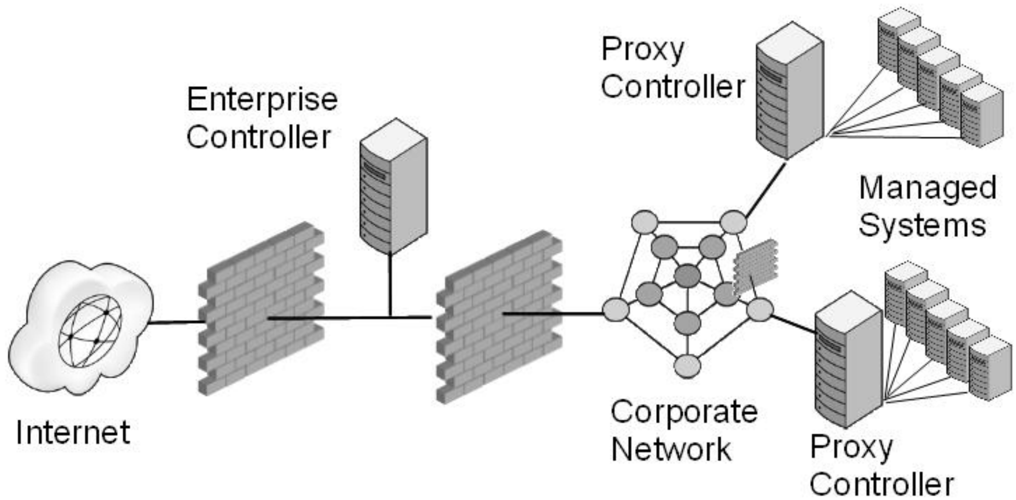
Describes how a firewall adds security to the product architecture.

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 a firewall between the Enterprise Controller and the Internet.

To configure the firewalls, see *Oracle Enterprise Manager Ops Center Ports and Protocols* for information about required URLs, ports, and protocol information.

About the Principle of Least Privilege

Describes the method of securing user access.

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

Lists the role needed to perform each task.

Table 1-2 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 1-3 shows the permissions granted by each role.

Table 1-2 Tasks and Permissions

Tasks	Permission
Read Access	Read Access

Table 1-2 (Cont.) Tasks and Permissions

Tasks	Permission
Add Assets Find Assets	Discover Assets
Manage Assets Delete Assets	Manage Assets
Create Group Edit Group Add Assets to Group Delete Group	Asset Group Management
New Update OS Job Deploy or Update Software Compare System Catalog Create Catalog Snapshot View and Modify Catalog	Update
New Simulated OS Update Job	Update Simulation
Configure and Deploy Server Install Server Configure RAID	Server Deployment
Add or delete storage Assign or detach network Start Guest Shut Down Guest Migrate Guest Clone Guest Lifecycle actions	Virtualization Guest Management
Assign Incidents Add Annotation to incidents Acknowledge incidents Take Actions on Incidents Mark Incidents as Repaired Close Incidents Delete Notifications Take Actions on Notification	Fault Management
Update Management Credentials Any Actions related to changing credentials	Credential Management
Edit Network Domain Edit Network Attributes Edit Network Services	Network Management
Fabric Management	Fabric Management

Table 1-2 (Cont.) Tasks and Permissions

Tasks	Permission
Import ISO Upload image Edit Attributes	Storage Management
Create reports Delete reports	Report Management
Create, delete, and modify profiles and plans	Plan/Profile Management
Create/Update/Delete Instance 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	Cloud Usage
Create/Delete/Update Cloud Create/Delete/Update Cloud Domain Create Public Security Group Share Public Security Group Create VM Instance Type	Cloud Management
Manage Enterprise Controller	Enterprise Controller Management
Unconfigure/Uninstall Proxy Controller Configure Agent Controller Unconfigure Agent Controller DHCP configuration Subnets External DHCP Servers	Proxy Controller Management
Configure/Connect Disconnect/Unconfigure Cloud Control Console	Cloud Control Management
Unconfigure SCCM Configuration	Windows Update Management
Add Users Remove Users	User Management
Assign Roles	Role Management
Asset Management	Asset Management
Write Access	Write Access

Table 1-2 (Cont.) Tasks and Permissions

Tasks	Permission
Open Service Request	Service Request
Power On Power Off Power on with Net Boot Set Power Policy	Power Management
Chassis Management	Chassis Management
Storage Server Management	Storage Server Management
Launch Switch UI	Switch Management
Reset Servers Reset Service Processors Refresh Locator Light On/Off Snapshot Bios Configuration Update Bios Configuration	Server Management
Reboot Upgrade Agent Controller	Operating System Management
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
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

Table 1-2 (Cont.) Tasks and Permissions

Tasks	Permission
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
Create Logical Domains Create zones Create OVM virtual servers	Virtualization Guest Creation
Delete Logic Domain Delete Zones Delete OVM Virtual Servers.	Virtualization Guest Deletion

Table 1-2 (Cont.) Tasks and Permissions

Tasks	Permission
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

Table 1-2 (Cont.) Tasks and Permissions

Tasks	Permission
OVM Manager Usage	OVM Manager Usage
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 1-3 Roles and Permissions

Table 1-3 (Cont.) 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 1-3 (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 1-3 (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 1-3 (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 1-3 (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

Table 1-3 (Cont.) Roles and Permissions

Role	Permissions
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
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

Table 1-3 (Cont.) Roles and Permissions

Role	Permissions
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 1-3 (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 1-3 (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 1-3 (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

Procedure for changing a user’s role and privileges.

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 in About Configuring 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**.

About Monitoring System Activity

Describes the logging features of the product.

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

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. Events are recorded during operations and can provide additional detail about system activity. Log files are protected by file permissions and therefore require a privileged user to get access to them.

About Audit Logs for Performance and Security

Description of the role of audit logs

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

The audit log files record the following types of events:

- Adding and deleting a user account
- Changing the roles for a user account

- Logging in and information about the connection
- Starting and ending jobs

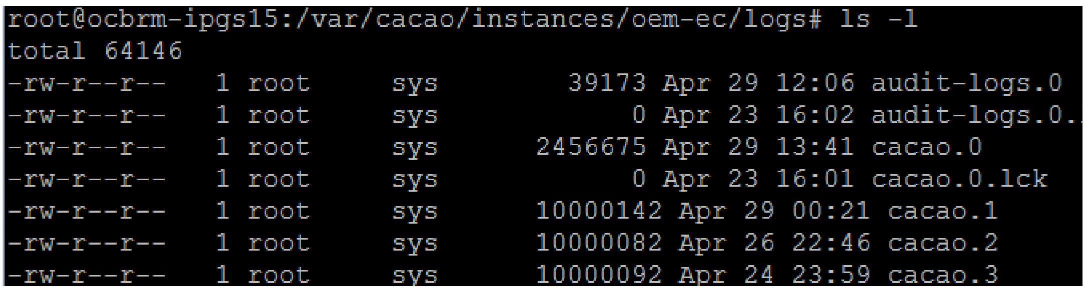
The files are located on the Enterprise Controller in the following location:

- On Oracle Solaris: `/var/cacao/instances/oem-ec/logs/audit-logs.*`
- On Linux: `/var/opt/sun/cacao2/instances/oem-ec/logs/audit-logs.*`

Each audit log file has a maximum size of 10 Mb. When this limit is reached, the file is closed and a new file is created with an incremented file extension. The maximum number of audit log files is 15, accumulating 150 Mb of logged activity. When `audit-logs.14` is closed, the next audit file is `audit-log.0`, overwriting the original `audit-log.0` file.

Figure 1-3 shows the series of log files.

Figure 1-3 Contents of Log Directory on Oracle Solaris 11



```
root@ocbrm-ipgs15:/var/cacao/instances/oem-ec/logs# ls -l
total 64146
-rw-r--r--   1 root     sys        39173 Apr 29 12:06 audit-logs.0
-rw-r--r--   1 root     sys            0 Apr 23 16:02 audit-logs.0.
-rw-r--r--   1 root     sys      2456675 Apr 29 13:41 cacao.0
-rw-r--r--   1 root     sys            0 Apr 23 16:01 cacao.0.lck
-rw-r--r--   1 root     sys     10000142 Apr 29 00:21 cacao.1
-rw-r--r--   1 root     sys     10000082 Apr 26 22:46 cacao.2
-rw-r--r--   1 root     sys     10000092 Apr 24 23:59 cacao.3
```

- User root logs in at 3:06.
- User root creates a new user, stanfield.
- User root gives the OPS_CENTER_ADMIN privilege to user stanfield.
- User root logs out.
- User stanfield logs in at 3:12.
- User stanfield starts a DHCP configuration job.
- Job is completed.
- User stanfield logs out.

Starting with Release 12.3.1, the audit log contains the sessionID to differentiate among multiple sessions of the same user. Also, starting in this release, you have the option to specify the format of the date and time in any of the formats supported by Javadoc's SimpleDateFormat class. You specify the format using the `audit.dateformat` system property.

Syntax of an Audit Log Entry

Lists the components of an event in the audit log file.

The entries in the audit log file have the following syntax:

`datetime action connect_info additional_info`

action

LOGIN
DISCONNECT If a connection expires, the disconnection is not logged.
JOB_START
JOB_END
USER_ADD
USER_DELETE
ROLES_ASSIGN
SCHEDULED_JOB_STARTED
REMOTE_INFO Indicates a connection through the browser interface and includes the IP address and port of the `http` client making the connection, as in the following example:

```
REMOTE_INFO rmi://127.0.0.1 yogi 52, Remote Info: User yogi Session
ID:c2870004d5308069ffbf367fde6b connected from 192.168.134.249:57391 / JMX Session:
com.sun.cacao.sessionrmi://127.0.0.1:9 com.sun.cacao.useryogi
```

connect_info
Unique identifier for the connection, depending on the type of connection:

- Connections through the browser interface or the command line interface: `rmi://`*`ip_address username connection_id`*
- Connections through the API: `jmxmp://`*`ip_address:port username connection_id`*

additional_info

- When the system property `audit.dateformat` is set, a timestamp is included.
- For job actions, the additional information is the job ID, which consists of the Enterprise Controller's name and the job number as listed in the Job pane.
- For user actions, the additional information is the username.

Changing the Date and Time Format of the Audit Log

Procedure for changing the system property that controls the timestamp in audit logs for Oracle Enterprise Manager Ops Center.

1. Select **Administration** in the Asset pane.
2. Select the **Configuration** tab in the center pane.
3. Select **EC Manager** in the drop-down list.
4. Select `audit.dateformat` in the list of properties.
5. Edit the value field to specify the format of the date and time. Use a specification that is supported by Java's SimpleDateFormat class.
6. Click the Save button.
7. Wait at least 10 minutes for the change to take effect and view the current audit log to confirm.

Example of an Audit Log

Sample audit log.

Example 1-1 shows the contents of an audit log for the following operations:

Example 1-1 Example of an Audit Log

```
5/23/14 3:06 PM LOGIN rmi://127.0.0.1 root 13
5/23/14 3:06 PM REMOTE_INFO rmi://127.0.0.1 root 13, Remote Info: User root Session
ID:c2870004d5308069ffbf367fde6b connected from 192.0.2.1:45338 / JMX Session:
com.sun.cacao.session^Armi://127.0.0.1:2 com.sun.cacao.user^Aroot
5/23/14 3:12 PM USER_ADD rmi://127.0.0.1 root 13, Remote Info: User root connected
from Session ID:c2870004d5308069ffbf367fde6b 192.0.2.1:45338 / JMX Session:
com.sun.cacao.session^Armi://127.0.0.1:2 com.sun.cacao.user^Aroot Add user
stanfield: SUCCESS
5/23/14 3:12 PM ROLES ASSIGN rmi://127.0.0.1 root 13 Roles [OPS_CENTER_ADMIN]
granted to user stanfield
5/23/14 3:12 PM DISCONNECT rmi://127.0.0.1 root 13
5/23/14 3:12 PM LOGIN rmi://127.0.0.1 stanfield 18
5/23/14 3:12 PM REMOTE_INFO rmi://127.0.0.1 stanfield 18, Remote Info: User
stanfield Session ID:c2870004d5308069ffbf367fde6d connected from 192.0.2.1:45351 /
JMX Session: com.sun.cacao.session^Armi://127.0.0.1:3 com.sun.cacao.user^Astanfield
5/23/14 3:13 PM JOB_STARTED rmi://127.0.0.1 stanfield 18 sm4170m2-11-
n172.27.immediate - DHCP Server Configuration on sm4170m2-11-n172
5/23/14 3:13 PM JOB_END  Job sm4170m2-11-n172.27 Completed with Status: SUCCESS
5/23/14 3:13 PM DISCONNECT rmi://127.0.0.1 stanfield 18
```

Activity Log Files for Components

Lists the type of event and the type of information about the event that is logged.

The following log files contain detailed information about the same events as the audit log files except for login information. They include the interactions between components of the product software.

- On Oracle Solaris: `/var/cacao/instances/oem-ec/audits/`
- On Linux: `/var/opt/sun/cacao/instances/oem-ec/audits/`

The following log files are specialized for specific events:

- Messages from operating system such as Info and Warning: `/var/adm/messages*`
- Login and connection information: `/var/opt/sun/xvm/logs/audit-logs*`
- Events in the user interface component: `/var/opt/sun/xvm/logs/emoc.log`
- Events between controllers and agents:
  - On an Oracle Solaris Enterprise Controller: `/var/cacao/instances/oem-ec/logs/cacao.`*n*
  - On a Linux Enterprise Controller: `/var/opt/sun/cacao/instances/oem-ec/logs/cacao.`*n*
  - On each Oracle Solaris Proxy Controller: `/var/cacao/instances/scn-proxy/logs/cacao.`*n*
  - On each Linux Proxy Controller: `/var/opt/sun/cacao/instances/scn-proxy/logs/cacao.`*n*
  - On each Oracle Solaris agent: `/var/cacao/instances/scn-agent/logs/cacao.`*n*

– On each Oracle Linux agent: `/var/opt/sun/cacao/instances/scn-agent/logs/cacao.`*n*

High Availability

Lists the Clusterware activity log.

In a High Availability configuration, each Enterprise Controller is a Clusterware node. The Clusterware resource activity is logged each time the active Enterprise Controller's resource action script's `check()` function is executed. The default interval is 60 seconds.

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

Software Updates

Lists the events for 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

Lists the type of event and the type of information about the event that is logged

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

Local Database

Lists the log files for database activity.

- On the Enterprise Controller:
  - For installation events:

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

/var/tmp/opscenter/installer.log.latest

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

  /var/opt/sun/xvm/oracle/diag/rdbms/ocdb/OCDB/alert/log.xml.*

  /var/opt/sun/xvm/oracle/diag/rdbms/ocdb/OCDB/trace/alert_OCDB.log.*

  /var/opt/sun/xvm/oracle/diag/tnslsnr/<hostname>/oclistener/alert/log.xml.*

  /var/opt/sun/xvm/oracle/diag/tnslsnr/<hostname>/oclistener/trace/listener.log.*

- For schema changes:

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

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

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

- For backup, restore, and migrate operations:

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

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

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

- For data files: `/var/opt/sun/xvm/oracle/oradata/OCDB`
- For redo log files: `/var/opt/sun/xvm/oracle/oradata/OCDB`.

  If you used OCDoctor to prepare a zpool directory with Oracle OS user permission, the log files are in: `/var/opt/sun/xvm/oracle/oradata/OCDB/REDO/`
- On the Proxy Controller: `/var/opt/sun/xvm/proxydb/*`
- On each agent: `/var/opt/sun/xvm/agentdb/*`

2 Secure Installation and Configuration

Describes the role of security in the product.

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

Topics

Planning the Deployment

Describes the role of security in the product architecture.

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

Topics

About High Availability

Describes how the product provides 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

Lists the requirements for High Availability.

- Use two or more systems of the same model and configured identically:
  - Processor class
  - Operating system
  - 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 Enterprise Manager Ops Center software.

Limitations of High Availability

Describes the limitations of the High Availability.

- User accounts and data that are not associated with Enterprise Manager Ops Center are not part of the relocate process. Only 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.

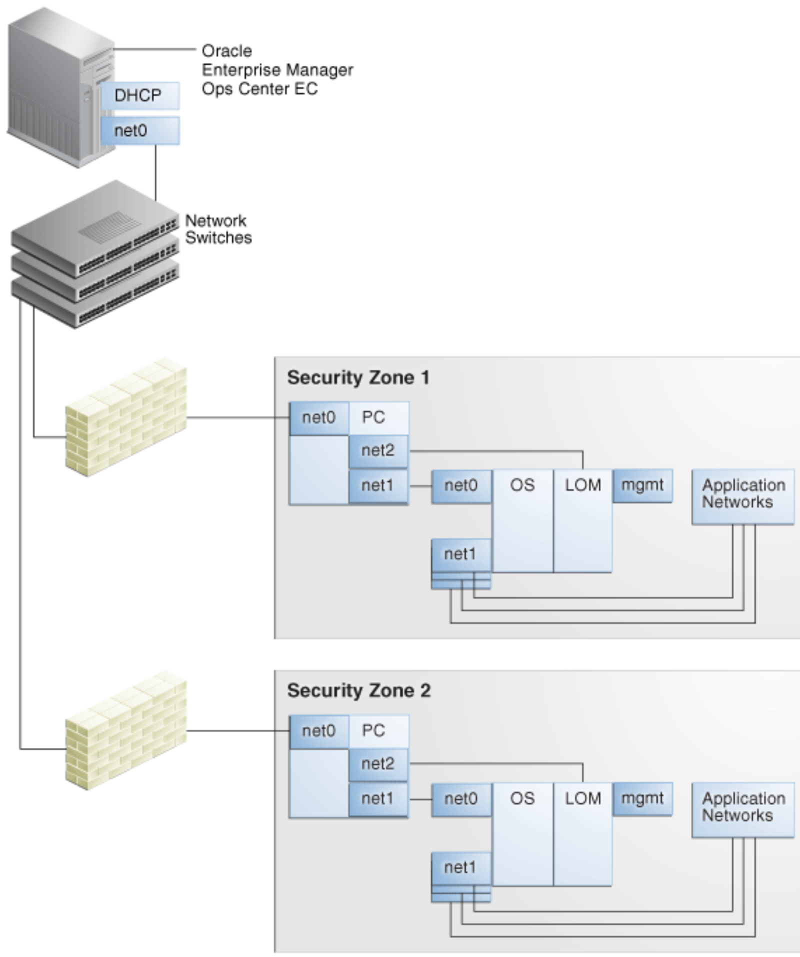
See the *Oracle Enterprise Manager Ops Center Administration* for instructions in configuring and maintaining an High Availability installation.

Overview of Network Configuration

Describes a network configuration in which operations are separated.

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. Network connection (net0) can be physical NIC, a link aggregate, or an IPMP group.

Figure 2-1 Separate Management, Provisioning, Data Networks



About Infrastructure and Operating Systems

Description of the role of various system administrators in the product architecture.

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 the various site system administrators.

About Storage Configuration

Describes how libraries can be configured in the product architecture.

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.

About a Remote Database

Describes the alternative architecture that uses a separate database to support the product.

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.

Starting with Release 12.2.2.0.0, you have the option to prevent the remote database's Enterprise Controller application schema from viewing or executing public database objects.

Note:

Preventing access to public database objects might affect other application schemas if they require public privileges.

To add this security enhancement, use the following procedure to execute the `update_pub_privs_12.2.2.0.sql` script:

1. Copy the `update_pub_privs_12.2.2.0.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:

   - Oracle Solaris OS: `/opt/ORCLsysman-db/sql/update/diamond-update2/oracle/`

   - Linux OS: `/opt/orcl/orcl-dbic/sql/update/diamond-update2/oracle/`

2. On the customer-managed database's system, log into the database administrator account.

3. Execute the script using the following command:

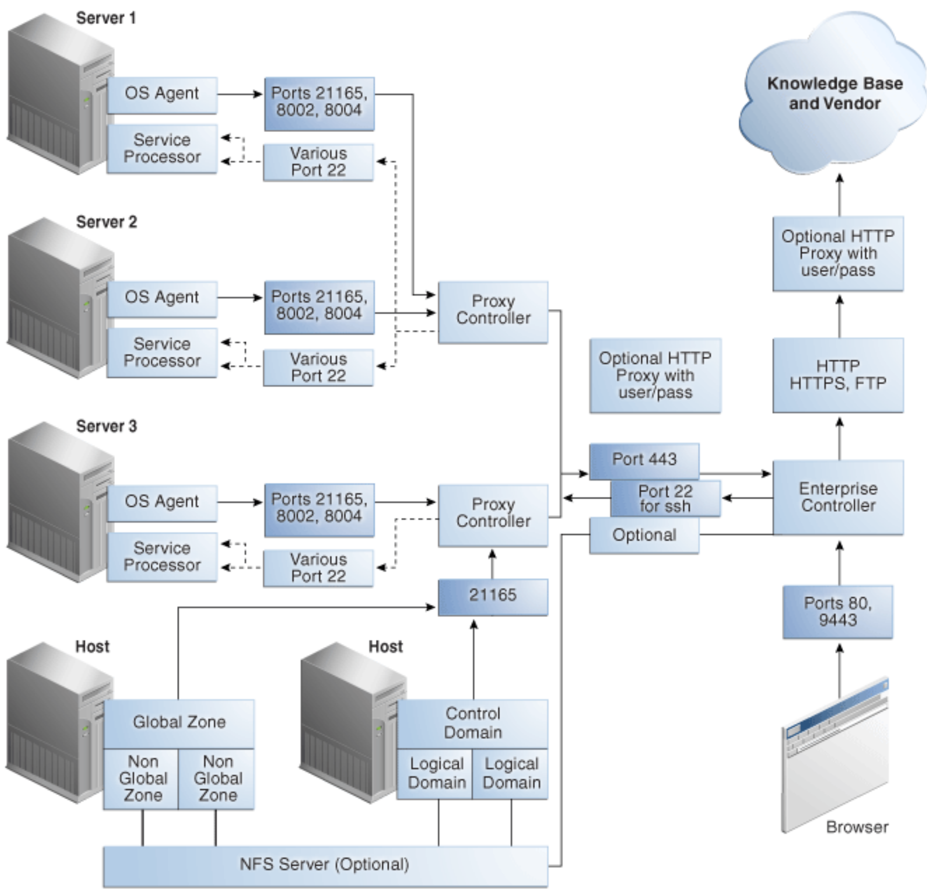
   ```
   sqlplus / as sysdba @update_pub_privs_12.2.2.0.sql
   ```

Typical Deployment

Illustrates a typical product architecture.

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

Describes installation of the product.

Topics

- About Controlling Access
- Obtaining a Certificate Authority's Certificate
- Viewing the Enterprise Controller's Truststore and Keystore
- About Substituting CA Certificates for the Default Certificates
- Verify a Certificate's Expiration Date
- Replace the Certificate for the Enterprise Controller
- Replace the Certificate for the Proxy Controller

- Substituting Certificates for the Glassfish Web Container
- Replace the Certificate for the Apache UCE Container
- About Installing a Remote Proxy Controller Securely

About Controlling Access

Describes the importance of controlling access to the product.

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.

About Substituting CA Certificates for the Default Certificates

Describes the role of certificates in the product architecture.

Oracle Enterprise Manager Ops Center has self-signed certificates that it uses for authentication between its components. Self-signed certificates are certificates that have not been registered with any third-party Certificate Authority (CA), and are therefore not guaranteed by a Certificate Authority. These certificates issue a warning when connecting with a browser and require users to accept the certificate.

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

Oracle Enterprise Manager Ops Center 's internal communication occurs between Java components and between Apache components so both types of certificates must be prepared and substituted for the self-signed certificates.

- Starting in Release 12.3.1.0, use the Command Line Interface's `security` mode to manage certificates. The instructions for invoking and the product's Command Line Interface are in the *Oracle Enterprise Manager Ops Center Command Line Interface*, but to summarize:

  1. Go to the following location:
     - Oracle Solaris: `/opt/SUNWoccli/bin`
     - Linux: `/opt/sun/occli/bin`
  2. Invoke the product CLI:

     ```
     ./oc -e 'connect'
     ```

     If you are connecting to the Enterprise Controller from a remote system, you are prompted for the host name, username, and password.
  3. The procedures in this section use the `security` mode and the `jobs` mode. When you enter a mode, the system prompt changes to indicate the current mode. To enter security mode, type `security` on the command line. You can view the man pages for any mode from the command line or in the *Oracle Enterprise Manager Ops Center Command Line Interface*.

- For Java certificates, use the `keytool` utility, included in the Java Development Kit, to manage the keystore, which stores your server's certificate, and the truststore, which stores the Certificate Authority's certificates.
- For Apache certificates, use the Oracle Solaris's OpenSSL utilities to create certificates for mutual authentication between a server and its clients. OpenSSL is a cryptography toolkit that implements the Transport Layer Security (TLS) network protocol. Oracle Enterprise Manager Ops Center does not use any version of SSL. All transactions with the web browser are in TLS.

Use the procedures in this section to substitute private keys with a Certificate Authority's private keys, signed by the Certificate Authority. By substituting the certificates and keys, you change the trust relationship between components. To ensure authentic communication, substitute the keys on the following:

- The Enterprise Controller's server
- The co-located Proxy Controller
- Each additional Proxy Controller

Obtaining a Certificate Authority's Certificate

Procedure for obtaining a certificate from a Certificate Authority.

To substitute the self-signed certificate with a Certificate Authority's certificate, you must obtain the CA's certificate and communicate with the Certificate Authority during the procedure. The following procedure is the general procedure:

1. Identify the Certificate Authority you want to use and follow their instructions for the specific steps of this general procedure.
2. Submit a request for a certificate to the Certificate Authority, called a certificate signing request (CSR). The Certificate Authority returns a certificate chain, which consists of a root certificate and its signed certificate.
3. Download a Chain Certificate from the Certificate Authority.
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. For a Java certificate, use the following command to see the fingerprints and then communicate with the Certificate Authority to compare the fingerprints:

   ```
   keytool -printcert -file <path/filename>
   ```

5. Replace existing certificates with the CA certificates, as described in the following sections.

Viewing the Enterprise Controller's Truststore and Keystore

Procedure for displaying information about the Enterprise Controller’s certificates and keys.

To configure secure communications, you can configure the Java keystore and truststore. The keystore stores the host server's private keys and local authority certificate, to provide the credentials for secure transactions. The truststore is similar to the keystore, but it stores certificates from remote servers, which allows the remote server to open a secure transaction.

At any time, use the following command to display the content of the Enterprise Controller's keystore:

```
keytool -list -v -keystore /etc/cacao/instances/oem-ec/security/jsse/keystore -
storepass:file /etc/cacao/instances/oem-ec/security/password
```

Use the following command to display the content of the Enterprise Controller's truststore:

```
keytool -list -v -keystore /etc/cacao/instances/oem-ec/security/jsse/truststore -
storepass trustpass
```

Use the CLI `security` mode at any time to display information about the certificates in any Proxy Controller’s truststore or any asset’s truststore. The following commands display information for each certificate on each asset or Proxy Controller: the alias, the owner, the issuer, the serial number, the creation date, and the period during which the certificate is valid.

```
localhost/security > list_proxy [-p|--proxy proxyID]
```

```
localhost/security > list_asset [-a assetname]
```

About CA Certificate Expiration

Description of the expiration of certificates.

The certificates from a Certificate Authority expire after a time period they set, usually between one and two years. Make certain you replace the certificates before they expire. If they expire, access is denied.

Verify a Certificate's Expiration Date

Procedure for displaying information about a certificate.

Use the CLI `security` mode at any time to verify the validity of the certificates in any Proxy Controller’s truststore or any asset’s truststore. You can specify the number of days to check for expiration of the certificate. The following examples check whether the certificate remains valid for the next 180 days.

```
localhost/security > check_proxy -d 180
```

```
localhost/security > check_asset -d 180
```

A result of `OK` means the certificate is valid for at least 180 days.

A result of `Invalid` means the certificate expires in less 180 days.

Replace the Certificate for the Enterprise Controller

Procedure for replacing a certificate on the Enterprise Controller.

You can replace an existing certificate at any time. However, when specifying an alias for a truststore, do not re-use the original alias. You must choose new aliases when replacing certificates because the original certificate and the replacement certificate use the same truststore.

You can change both the certificate and the password for the new keystore or you can change only the certificate and keep the same password for the new keystore.

1. Navigate to the location of the keystore:

- Oracle Solaris OS: `cd /etc/cacao/instances/oem-ec/security/jsse`
- Linux OS: `cd /etc/opt/sun/cacao2/instances/oem-ec/security/jsse/`

2. Create a new password by creating and then editing the following file:

   ```
   /etc/cacao/instances/oem-ec/security/password
   ```

3. Create a new private key in the new keystore. You will be prompted to enter passwords for the key and keystore.

   a. Create a new private key. Use the `keytool -genkey` command, according to its documentation and your site's security policy. The following is an example of the command:

```
keytool -genkey -alias cacao_agent -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity
7300 -keystore keystore_new -storepass:file /etc/cacao/instances/oem-ec/security/password -
dname CN=ec-`uname -n`
```

   where

   `-keyalg` specifies the algorithm to be used to generate the key pair.

   `-sigalg` specifies the algorithm used to sign the self-signed certificate. This algorithm must be compatible with the algorithm specified by the `-keyalg` option, as described in the `keytool` documentation.

   `-validity` specifies the number of days that the certificate remains valid.

   `-dname` specifies the X.500 Distinguished Name to be associated with *alias*, and is used as the issuer and subject fields in the self-signed certificate.

   b. At the prompt to enter the key password for cacao_agent, do not enter any characters. Instead, press the Enter key to set the cacao_agent key password to be the same password as the one used for the keystore. This method is the only way to ensure that the passwords match.

4. Create a signing request (CSR) using the `keytool -certreq` command, according to its documentation and your site's security policy. The following is an example of the command:

   ```
   keytool -certreq -keyalg RSA -sigalg SHA256withRSA -alias cacao_agent -file
   agent.crq -keystore keystore_new -storepass:file /etc/cacao/instances/oem-ec/
   security/password
   ```

   where:

   `SHA256withRSA` specifies the algorithm used to sign the self-signed certificate.

   `agent.crq` is the name of the file containing the signing request.

5. Obtain a new certificate from a Certificate Authority, according to the procedure in Obtaining a Certificate Authority's Certificate.

6. Import the Certificate Authority's root certificate, *`your_ca`*, into the new keystore. The root certificate is in the file `root.cert`.

   ```
   keytool -importcert -alias your_ca -keystore keystore_new -file root.cert -
   storepass:file /etc/cacao/instances/oem-ec/security/password
   ```

7. At the prompt to confirm the certificate, enter `Yes`.

8. Import the signed certificate into the new keystore. The signed certificate is in the file `agent.cert`.

   ```
   keytool -importcert -v -alias cacao_agent -file agent.cert -keystore
   keystore_new -storepass:file /etc/cacao/instances/oem-ec/security/password
   ```

   The output of this command is the message`"Certificate reply was installed in keystore"`, which confirms that the operation completed successfully.

9. Remove the Certificate Authority's root certificate, *`your_ca`*, from the new keystore because it is no longer needed:

   ```
   keytool -delete -alias your_ca -keystore keystore_new -storepass:file /etc/cacao/
   instances/oem-ec/security/password
   ```

10. If you are using the EC-HA High Availability feature, copy the new keystore and the updated truststore to the second node system at the same location. If you are using a new password, copy it to the second node system too.

11. Use the CLI's `security` mode to propagate the new certificate to the truststore of all Proxy Controllers:

    a. View the status of the current certificates:

       ```
       localhost/security > check_proxy
       ```

       The following example shows that two Proxy Controllers have active certificates.

       ```
       Proxy Certificates Status:
           Proxy  |  Alias   |      Serial      |Status|Active|
       ---------------------------------------------------------------
        proxy-1   | cacao_ca |     303b0061     |  OK  |ACTIVE
        proxy-2   | cacao_ca |     303b0061     |  OK  |ACTIVE
        proxy-2   |   sds    | d61bbb3e03e483f9 |  OK  |
       ```

    b. Propagate the new certificates to the Proxy Controllers.

       ```
       localhost/security > push_proxy -k /etc/cacao/instances/oem-ec/security/
       jsse/keystore_new
       -w /etc/cacao/instances/oem-ec/security/password
       ```

       The operation is reported to you as a Job ID that includes the Enterprise Controller's name:

       ```
       Job ID is ec_name.n
       ```

    c. Use the `jobs` mode as a one-line command to follow the progress of the job. This one-line command lets you run a command in a different mode without ending the current mode.

       ```
       localhost/security > cli.jobs.list -C1

       ec_name.n |       SUCCESS       |     root    |     Propagate Satellite
       Certificates to Proxies
       ```

    d. When the job is finished, verify the status of the certificates again. This example shows that all new certificates have been propagated but original certificates are still in use. These certificates remain in use until the active keystore is changed.

```
localhost/security > check_proxy

Proxy Certificates Status:
  Proxy  |     Alias      |      Serial      |Status|Active|
--------------------------------------------------------------------
 proxy-1 | cacao_agent-1 |     2fe12e10     |  OK  |
 proxy-1 |    cacao_ca   |     303b0061     |  OK  |ACTIVE
 proxy-1 | cacao_agent-0 |     a479618c     |  OK  |
 proxy-2 | cacao_agent-1 |     2fe12e10     |  OK  |
 proxy-2 |    cacao_ca   |     303b0061     |  OK  |ACTIVE
 proxy-2 | cacao_agent-0 |     a479618c     |  OK  |
 proxy-2 |      sds      | d61bbb3e03e483f9 |  OK  |
```

12. Stop the Enterprise Controller.
13. Rename the existing keystore to identify it as the previous keystore:

    ```
    mv keystore keystore_old
    ```

14. Rename the new keystore to identify it as the current keystore:

    ```
    mv keystore_new keystore
    ```

15. Set the permissions of the keystore file to 600:

    ```
    chmod 600 keystore
    ```

16. Remove the truststore GF

    ```
    rm truststore_gf
    ```

17. Rename the directories so that `password` is in effect and then change its permissions:

    ```
    mv ../password ../password_old
    mv ../password_new ../password
    chmod 600 ../password_new
    ```

18. Restart the Enterprise Controller. After this start, the new certificates are in use. Remote users of the Command Line Interface must accept the new certificate the first time they connect to the CLI.
19. If you are using the EC-HA High Availability feature, repeat the same commands on the second node system:

    ```
    mv keystore keystore_old
    mv keystore_new keystore
    rm truststore_gf
    mv ../password ../password_old
    mv ../password_new ../password
    chmod 600 ../password_new
    ```

20. Use the `security` mode to remove the original certificates from the Proxy Controllers' truststores.

    a. Verify that all new certificates are now in use and the original certificates are not used.

       ```
       localhost/security > check_proxy
       ```

       The following example shows that the new certificates, starting with `cacao_agent`, are now the active certificates.

```
Proxy Certificates Status:
  Proxy  |     Alias     |      Serial      |Status|Active|
--------------------------------------------------------------------
 proxy-1 | cacao_agent-1 |     2fe12e10     |  OK  |ACTIVE
 proxy-1 |    cacao_ca   |     303b0061     |  OK  |
 proxy-1 | cacao_agent-0 |     a479618c     |  OK  |ACTIVE
 proxy-2 | cacao_agent-1 |     2fe12e10     |  OK  |ACTIVE
 proxy-2 |    cacao_ca   |     303b0061     |  OK  |
 proxy-2 | cacao_agent-0 |     a479618c     |  OK  |ACTIVE
 proxy-2 |      sds      | d61bbb3e03e483f9 |  OK  |
```

b. To remove the old certificates from its truststore, you must remove each one individually. Each operation creates a job with an ID that includes the Enterprise Controller's name.

```
localhost/security > remove_proxy -s 303b0061

Job ID is ec_name.YY
```

c. Verify that each job has been completed.

```
localhost/security > cli.jobs.list -C1

ec_name.YY | SUCCESS | root | Delete Certificate from Proxies | All known
Proxies
```

21. Verify the status of the new certificates:

```
localhost/security > check_proxy

Proxy Certificates Status:
 Proxy   |     Alias     |      Serial      |Status|Active|
--------------------------------------------------------------------
 proxy-1 | cacao_agent-1 |     2fe12e10     |  OK  |ACTIVE
 proxy-1 | cacao_agent-0 |     a479618c     |  OK  |ACTIVE
 proxy-2 | cacao_agent-1 |     2fe12e10     |  OK  |ACTIVE
 proxy-2 | cacao_agent-0 |     a479618c     |  OK  |ACTIVE
 proxy-2 |      sds      | d61bbb3e03e483f9 |  OK  |
```

Because you import the certificates for the new keys into the Proxy Controller truststore before you switch keys, an SSL error occurs in the Proxy Controller. For a Proxy Controller running version 12.3.0.0.0 version or later, the Proxy Controller recovers automatically in a few minutes. The Proxy Controller reads the truststore, detects the new certificates, and restores communication with the Enterprise Controller.

If the Proxy Controller is running a previous version or you experience a delay or other problem, stop and restart the Proxy Controller to force it to re-read its truststore.

Replace the Certificate for the Proxy Controller

Procedure for replacing a certificate on the Proxy Controller.

You must use a different certificate on the Proxy Controller from the certificate used on the Enterprise Controller. You must use a different certificate on each Proxy Controller.

Do not re-use an existing alias when you add a new certificate to a truststore. Each alias in a truststore must be unique.

1. Navigate to the keystore:

- Oracle Solaris OS: `cd /etc/cacao/instances/scn-proxy/security/jsse`
- Linux OS: `cd /etc/opt/sun/cacao2/instances/scn-proxy/security/jsse/`

2. Set the permissions of the keystore file to 0266:

```
# umask 0266
```

3. Create a new private key in the new keystore.

   a. Create a new private key. Use the `keytool -genkey` command, according to its documentation and your site's security policy. Do not include the `-keypass` option so that a prompt for the password will be displayed. The following is an example of the command:

```
keytool -genkey -alias cacao_agent -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity
7300 -keystore keystore_new -storepass:file /etc/cacao/instances/scn-proxy/security/password -
dname CN=ec-`uname -n`
```

   where

   `-keyalg` specifies the algorithm to be used to generate the key pair.

   `-sigalg` specifies the algorithm used to sign the self-signed certificate. This algorithm must be compatible with the algorithm specified by the `-keyalg` option, as described in the `keytool` documentation.

   `-validity` specifies the number of days that the certificate remains valid.

   `-dname` specifies the X.500 Distinguished Name to be associated with *alias*, and is used as the issuer and subject fields in the self-signed certificate. If you do not include the distinguished name in the command, the user is prompted for one.

   b. At the prompt to enter the key password for cacao_agent, do not enter any characters. Instead, press the Enter key to set the cacao_agent key password to be the same password as the one used for the keystore. This method is the only way to ensure that the passwords match.

4. Create a signing request (CSR) using the `keytool -certreq` command, according to its documentation and your site's security policy. The following is an example of the command:

```
keytool -certreq -keyalg RSA -sigalg SHA256withRSA -alias cacao_agent -file
agent.crq -keystore keystore_new -storepass:file /etc/cacao/instances/scn-proxy/
security/password
```

   where:

   `SHA256withRSA` specifies the algorithm used to sign the self-signed certificate.

   `agent.crq` is the name of the file containing the signing request.

5. Obtain a new certificate from a Certificate Authority for each Proxy Controller, according to the procedure in Obtaining a Certificate Authority's Certificate.

6. Import the Certificate Authority's root certificate, *`your_ca`*, into the new keystore. The root certificate is in the file `root.cert`.

```
keytool -importcert -alias your_ca -keystore keystore_new -file root.cert -
storepass:file /etc/cacao/instances/scn-proxy/security/password
```

7. At the prompt to confirm the certificate, enter `Yes`.

8. Import the signed certificate into the new keystore. The signed certificate is in the file `agent.cert`.

```
keytool -importcert -v -alias cacao_agent -file agent.cert -keystore
keystore_new -storepass:file /etc/cacao/instances/scn-proxy/security/password
```

   The output of this command is the message`"Certificate reply was installed in keystore"`, which confirms that the operation completed successfully.

9. Remove the Certificate Authority's root certificate, *`your_ca`*, from the new keystore because it is no longer needed:

```
keytool -delete -alias your_ca -keystore keystore_new -storepass:file /etc/cacao/
instances/scn-proxy/security/password
```

10. Use the CLI's `security` mode to propagate the new certificate to the truststore of all the assets managed by the specified Proxy Controller:

    a. View the status of the current certificates:

```
localhost/security > check_asset -p proxy-1
```

    The following example shows that the two assets managed by this Proxy Controller have active certificates.

```
Asset Certificates Status:
   Proxy |  Asset  |     Alias     |  Serial  |Status|Active|
----------------------------------------------------------------------------
---
 proxy-1 | asset-1 |    cacao_ca   | 70451d3b |  OK  |ACTIVE
 proxy-1 | asset-2 |    cacao_ca   | 70451d3b |  OK  |ACTIVE
```

    b. Propagate the new certificates to the truststore of each asset:

```
localhost/security > push_asset -p proxy-1 -k /etc/cacao/instances/scn-
proxy/security/jsse/keystore_new
```

    The operation is reported to you as a Job ID that includes the Enterprise Controller's name:

```
Job ID is ec_name.n
```

    c. Use the `jobs` mode as a one-line command to follow the progress of the job. This one-line command lets you run a command in a different mode without ending the current mode.

```
localhost/security > cli.jobs.list -C1

ec_name.n | SUCCESS | [Ops Center]| Propagate Proxy Certificates to AC/VC |
Propagate Proxy Certificates to AC/VC
```

    d. When the job is finished, verify the status of the certificates again. This example shows that all new certificates have been propagated but original certificates are still in use. These certificates remain in use until the active keystore is changed.

```
localhost/security > check_asset -p proxy-1
```

```
Asset Certificates Status:
   Proxy |    Asset |      Alias      |  Serial  |Status|Active|
----------------------------------------------------------------------------
-----
 proxy-1 |  asset-1 |  cacao_agent-1  | 2fe12e10 |  OK  |
 proxy-1 |  asset-1 |     cacao_ca    | 70451d3b |  OK  |ACTIVE
 proxy-1 |  asset-1 |  cacao_agent-0  | a4797cad |  OK  |
 proxy-1 |  asset-2 |  cacao_agent-1  | 2fe12e10 |  OK  |
 proxy-1 |  asset-2 |     cacao_ca    | 70451d3b |  OK  |ACTIVE
 proxy-1 |  asset-2 |  cacao_agent-0  | a4797cad |  OK  |
```

11. Place the Proxy Controller in maintenance mode to prevent auto-recovery during the remaining steps of this procedure.
12. Stop the Proxy Controller's internal communication using the following command:
    - Oracle Solaris OS: `/opt/SUNWxvmoc/bin/proxyadm stop -w`
    - Linux OS: `/opt/sun/xvmoc/bin/proxyadm stop -w`
13. Rename the existing keystore to identify it as the previous keystore:

```
mv keystore keystore_old
```

14. Rename the new keystore to identify it as the current keystore:

```
mv keystore_new keystore
```

15. Verify the access rights to the keystore.

```
ls -l /var/opt/sun/xvm/bui/conf/password

-r--------   1 root     root         199 juin 14 08:18 /var/opt/sun/xvm/bui/conf/
password
```

16. Remove the truststore GF.

```
rm truststore_gf
```

17. Restart the Proxy Controller:
    - Oracle Solaris OS: `/opt/SUNWxvmoc/bin/proxyadm start -w`
    - Linux OS: `/opt/sun/xvmoc/bin/proxyadm start -w`
18. Use the `security` mode to remove the original certificates from the assets' truststores.
    a. Verify that all new certificates are now in use and the original certificates are not used.

```
localhost/security > check_asset -p proxy-1

Asset Certificates Status:
   Proxy |   Asset  |                Alias                |  Serial  |
Status|Active|
----------------------------------------------------------------------------
-------------------------
 proxy-1 |  asset-1 |            cacao_agent-1            | 2fe12e10 |  OK
|ACTIVE
 proxy-1 |  asset-1 |               cacao_ca              | 70451d3b |  OK
|
```

```
 proxy-1 |  asset-1 |          cacao_agent-0          | a4797cad |  OK
|ACTIVE
 proxy-1 |  asset-2 |          cacao_agent-1          | 2fe12e10 |  OK
|ACTIVE
 proxy-1 |  asset-2 |             cacao_ca            | 70451d3b |  OK
|
 proxy-1 |  asset-2 |          cacao_agent-0          | a4797cad |  OK
|ACTIVE
```

b. To remove the old certificates from its truststore, you must remove each one individually. Each operation creates a job with an ID that includes the Enterprise Controller's name.

```
localhost/security > remove_asset -p proxy-1 -s 70451d3b

Job ID is ec_name.tt
```

c. Verify that each job has been completed.

```
localhost/security > cli.jobs.list -C1

ec_name.tt | SUCCESS | root | Delete Certificate from assets | All known
Proxies
```

19. Verify the status of the new certificates:

```
localhost/security > check_asset -p proxy-1

Asset Certificates Status:
   Proxy |   Asset  |      Alias      |  Serial  |Status|Active|
---------------------------------------------------------------------------
 proxy-1 | asset-1  |  cacao_agent-1  | 2fe12e10 |  OK  |ACTIVE
 proxy-1 | asset-1  |  cacao_agent-0  | a4797cad |  OK  |ACTIVE
 proxy-1 | asset-2  |  cacao_agent-1  | 2fe12e10 |  OK  |ACTIVE
 proxy-1 | asset-2  |  cacao_agent-0  | a4797cad |  OK  |ACTIVE
```

20. Remove the Proxy Controller from maintenance mode

Because you import the certificates for the new keys into the agent truststore before you switch keystores, an SSL error occurs in the agent. Starting with version 12.3.0.0.0 version, the agent recovers automatically in a few minutes. The agent reads the truststore, detects the new certificates, and restores communication with the Proxy Controller.

If the agent is deployed from a previous version or you experience a delay or other problem, stop and restart the agent to force it to re-read its truststore.

Substituting Certificates for the Glassfish Web Container

Procedure for changing the certificates for Glassfish web container.

Oracle Enterprise Manager Ops Center has self-signed certificates that it uses for authentication for its Glassfish web container. The benefit of substituting the self-signed certificates with certificates from a Certificate Authority is that users do not see a warning from the browser about attempting an untrusted connection and do not have to add a security exception to use the product.

To replace the self-signed certificate on a system that has been running Oracle Enterprise Manager Ops Center, use the following procedure:

1. Stop the Enterprise Controller's internal communication using the following command:

- Oracle Solaris OS: `/opt/SUNWxvmoc/bin/ecadm stop -w`
- Linux OS: `/opt/sun/xvmoc/bin/ecadm stop -w`

2. Navigate to the keystore:

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

3. Delete the keystore. The keystore is re-created automatically when you create a new private key later in this procedure.

```
rm keystore
```

4. Delete the Oracle Glassfish Server truststore used by the product's web server. The truststore is re-created automatically when the Enterprise Controller is restarted.

```
rm keystore_truststore_gf
```

5. Create a new private key, according to your site's security policy. Use the `keytool -genkey` command, according to its documentation and your site's security policy. Do not include the `-keypass` option so that a prompt for the password will be displayed. The following is an example of the command for creating the private key:

```
keytool -genkey -alias `uname -n` -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 7300 -
keystore keystore -storepass password -dname CN=bui-`uname -n`
```

where

`-keyalg` specifies the algorithm to be used to generate the key pair.

`-sigalg` specifies the algorithm used to sign the self-signed certificate. This algorithm must be compatible with the algorithm specified by the `-keyalg` option, as described in the `keytool` documentation.

`-dname` specifies the X.500 Distinguished Name to be associated with *alias*, and is used as the issuer and subject fields in the self-signed certificate. If you do not include the distinguished name in the command, the user is prompted for one.

`-validity` specifies the number of days that the certificate remains valid.

`-password` specifies either the clear text password or the local file named password that contains an arbitrary string used as the keystore password. If you are using a local file named password, then use the `-storepass:file <filename>` format.

Note:

If you are installing Oracle Enterprise Manager Ops Center version 12.3.2, use the `-storepass:file <filename>` for the keystore password.

---

6. At the prompt for the key password, press the Enter key to set the key password to match the keystore password.

7. Create a signing request:

```
keytool -certreq -keyalg RSA -sigalg SHA256withRSA -alias `uname -n` -file
bui.crq -keystore keystore -storepass password
```

8. If you have verified the certificate you received from the Certificate Authority, as described in Step 4 of the procedure in Obtaining a Certificate Authority's Certificate, you are ready to import it.

9. Import the certificate that the CA sent to you into the keystore. The certificate is in the file `root.cert`.

```
keytool -importcert -alias your_ca -keystore keystore -file root.cert -storepass password
```

10. At the prompt to confirm the certificate, enter `Yes`.

11. Import the signed certificate into the keystore. The certificate is in the file `bui.cert`.

```
keytool -importcert -v -alias `uname -n` -file bui.cert -keystore keystore -storepass password
```

The output of this command is the message`"Certificate reply was installed in keystore"`, which confirms that the operation completed successfully.

12. Remove the Certificate Authority's root certificate, *`your_ca`*, from the keystore because it is no longer needed:

```
keytool -delete -alias your_ca -keystore keystore -storepass password
```

13. Restart the Enterprise Controller:

    - Oracle Solaris OS: `/opt/SUNWxvmoc/bin/ecadm start -w`
    - Linux OS: `/opt/sun/xvmoc/bin/ecadm start -w`

Replace the Certificate for the Apache UCE Container

Procedure for replacing a certificate on the Apache UCE Container.

Use the following procedure to replace the certificates by accomplishing the following:

- Create and propagate the new certificates to the clients of the Apache service.
- Stop the Apache service, replace the certificates, and then restart the Apache service.

1. Copy your local Certificate Authority key and certificate files to a secure location on your server. This is a temporary location.

2. Rename the Certificate Authority certificate file to `server.crt`.

3. Rename the Certificate Authority key file to `server.key`.

4. To add the new certificate to the truststore of the client of the Apache Service, define the following variables

```
SMSF_STORE=/var/opt/sun/xvm/security/jsse/smsfacade/jssecacerts
SMSF_PASS=`awk -F= '/^engine.installcert.passphrase/{print $2}' /var/opt/sun/xvm/persistence/scn-satellite/satellite.properties`
NEW_SERVER_SSL_CRT=<your secure temporary location>/server.crt
```

For Oracle Solaris OS, define the following variables:

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

For Linux OS, define the following variables:

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

5. Add the new certificate to the truststore. This example uses `sds-2` and `127.0.0.1-2` to show that the aliases must be different from the original aliases. Specify alias names for your convenience or according to your site policy.

```
keytool -importcert -file $NEW_SERVER_SSL_CRT -alias sds-2 -keystore $TRUST_STORE -storepass $TRUST_PASS -noprompt
keytool -importcert -file $NEW_SERVER_SSL_CRT -alias 127.0.0.1-2 -keystore $SMSF_STORE -storepass $SMSF_PASS -noprompt
```

6. Stop the Enterprise Controller and the Proxy Controllers:
   - Oracle Solaris OS:
     – `/opt/SUNWxvmoc/bin/ecadm stop -w`
     – `/opt/SUNWxvmoc/bin/proxyadm stop -w`
   - Linux OS:
     – `/opt/sun/xvmoc/bin/ecadm stop -w`
     – `/opt/sun/xvmoc/bin/proxyadm stop -w`
7. Navigate to the location of the certificate and key files for the Apache web container:
   - Oracle Solaris OS: `cd /var/opt/sun/xvm/uce/etc.opt/server/uce_server/ssl.crt`
   - Linux OS: `cd /var/opt/sun/xvm/uce/etc/uce_server/ssl.crt`
8. Move the current `server.crt` file and `server.key` file from the `ssl.crt` directory to an alternate, secure location.
9. Copy your local Certificate Authority files from the secure temporary location to the ssl.crt directory.
10. Verify the permissions for the `server.key` file are set to allow only the service user to read the file:

    ```
    chown uce-sds:uce-sds server.key
    chmod 400 server.key
    ```

    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
    ```

11. If the server.key file is encrypted and requires a password, edit the following file to echo the password:

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

12. Restart the Enterprise Controller and Proxy Controllers.
    - Oracle Solaris OS:
      – `/opt/SUNWxvmoc/bin/ecadm start -w`
      – `/opt/SUNWxvmoc/bin/proxyadm start -w`
    - Linux OS:
      – `/opt/sun/xvmoc/bin/ecadm start -w`
      – `/opt/sun/xvmoc/bin/proxyadm start -w`
13. Use the CLI's security mode to propagate the new UCE certificate to each Agent Controller that needs it.

```
localhost/security > push_uce -p <proxy name>
```

About Installing a Remote Proxy Controller Securely

Description of a secure way to install a Proxy Controller on a remote system.

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

Lists the tasks for configuring the product.

A privileged user must be enabled for the Oracle Enterprise Manager Ops Center software. Log in as the privileged user to perform the tasks in this section:

- About the Connection Mode
- Disable Multiple Logins
- About Securing the Log Files
- About Database Credentials
- Disable the Domain Model Navigator
- Secure the Agents
- About Securing the Browsers
- About Strong Cipher Encryption

About the Connection Mode

Describes the differences between Connected mode and Disconnected mode for a set of tasks.

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.

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

Operation	Connected Mode	Disconnected Mode
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.
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 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.

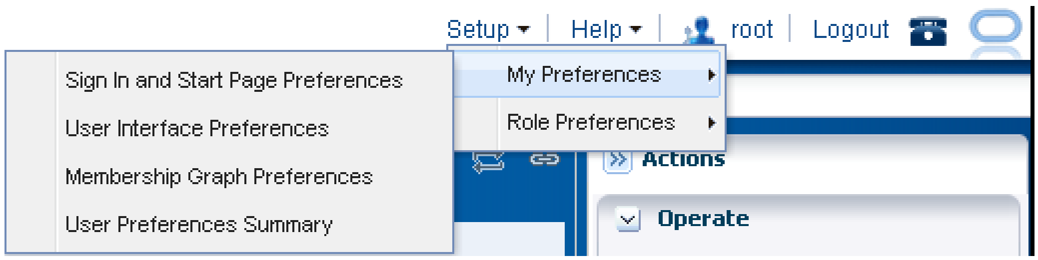
Disable Multiple Logins

Procedure for restricting a user to one login instance.

The default behavior is to allow a user to log in multiple times. This convenience can be a security risk. You can disable simultaneous sessions for an individual user account or for a role, to affect all user accounts that have the role.

1. Click **Setup** in the title bar as shown in Figure 2-3.
2. Click **My Preferences** to change your account or click **Role Preferences** to change the role, which affects all user accounts that have that role.

Figure 2-3 Setting User Preferences



3. Click **User Interface Preferences**.
4. In the Display Preferences section, select the **Disable Multiple Sessions** checkbox.
5. Log out and log in again to make the change take effect.

About Securing the Log Files

Describes the product's 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 the most recent installation or uninstallation: `/var/tmp/opscenter/installer.log.latest`
- Log of previous installation or uninstallation operations: `/var/tmp/opscenter/installer.log.`*`xxxx`*
- Log of a specific installation:

  `/var/opt/sun/xvm/oracle/app/oraInventory/logs/silentInstall<yyyy-mm-dd-hh-mm-sspm>.log`
- Log of an agent installation: `/var/scn/install/log`

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`

About Database Credentials

Describes how the product's database can be secured.

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.

About Securing the Local Database

Describes methods for keeping database secure when it runs on the same system as the Enterprise Controller.

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 Access to 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 About 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.

About Securing a Remote Database

Describes the methods for securing the database when it runs on a different system from the Enterprise Controller's system.

- 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

Procedure for using the SQL script for a customer-managed database.

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:
   - Oracle Solaris OS: `/opt/ORCLsysman-db/sql/update/delta-update1/oracle/refactorOCPrivs_12.1.x.0.sql`
   - Linux OS: `/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

Procedure for changing the credentials of the database that Ops Center uses.

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 secure it with 600 permissions.

   For example:

   ```
   # touch /tmp/password
   # chmod 600 /tmp/password
   # vi /tmp/password
   newpassword
   ```

2. Use the `ecadm` command with the `change-db-password` subcommand and the `-p <password file>` option to change the database password. When prompted, confirm the Enterprise Controller 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 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. Remove the temporary file containing the new password.

   For example:

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

Changing the Database Credentials for the Read-Only User

Procedure for changing the credentials for the database..

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.

   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. Remove the temporary file containing the new password.

   For example:

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

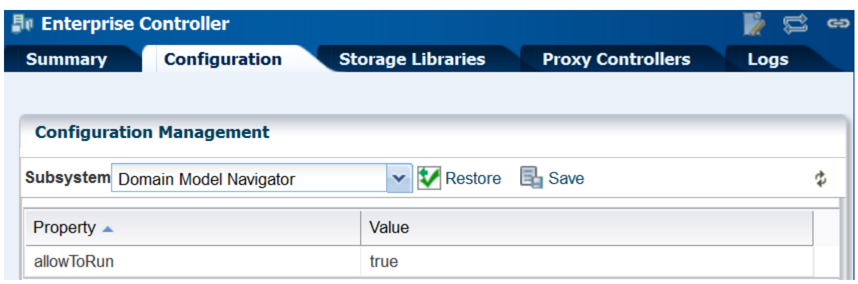
Disable the Domain Model Navigator

Procedure for disabling the interface to the domain model.

Oracle Enterprise Manager Ops Center provides a Domain Model Navigator to allow Oracle support personnel to gather detailed information about the state of the system. This diagnostic interface is enabled by default and requires user authentication for access. However, because the Domain Model Navigator displays an internal view of the product software, disable the interface on the Enterprise Controller and Proxy Controllers using the following procedure. The agents for assets are not part of the Domain Model Navigator.

1. Log in to the Enterprise Controller as the `root` user.
2. Click **Administration** in the Navigation pane.
3. Click **Enterprise Controller.**
4. Click **Configuration** in the center pane.
5. In the Subsystem field, click **Domain Model Navigator.** The `allowToRun` property's default value is `true`, as shown in Figure 2-4.

   Figure 2-4 Property of Domain Model Navigator



6. Click in the **Value** field to edit it. Change the value to `false`.
7. Click the **Save Properties** icon.
8. Perform the following procedure on each Proxy Controller:
   a. Edit the file `/opt/sun/n1gc/lib/XVM_PROXY.properties`
   b. Add the following line to the file:

```
domain.model.navigator.allow=false
```

   c. Stop and restart the Proxy Controller:

```
/opt/SUNWxvmoc/bin/proxadm stop
/opt/SUNWxvmoc/bin/proxadm start
```

9. Stop and restart the Enterprise Controller:

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

To investigate an issue with an asset, My Oracle Support might instruct you to view the Domain Model Navigator. To re-enable the Domain Model Navigator, use the same procedure to set the property values to `true`.

Enable the Domain Model Navigator on the Enterprise Controller

Procedure for enabling the interface to the domain model.

To enable the Domain Model Navigator:

1. Log in to the Enterprise Controller as the `root` user.
2. Click **Administration** in the Navigation pane.
3. Click **Enterprise Controller.**
4. Click **Configuration** in the center pane.
5. Click the **Restore Properties** icon.
6. Repeat the following procedure on each Proxy Controller:
   a. Edit the file `/opt/sun/n1gc/lib/XVM_PROXY.properties`
   b. Add the following line to the file:
      ```
      domain.model.navigator.allow=true
      ```
   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
   ```

Using the Domain Model Navigator

Procedures for locating or changing information in the domain model.

The Domain Model represents Domain Model MBeans, Gear Model MBeans, and Service MBeans and their current states.

To diagnose or correct a problem, you might be directed by My Oracle Support to search for or change information in the domain model. Use the following procedures to complete this task:

- Logging Into the Domain Model
- Searching the Domain Model
- Changing the Domain Model
- Logging Out of the Domain Model Navigator

Logging Into the Domain Model

Procedure for getting access to the domain model.

In the web browser, navigate to the following:

On the Enterprise Controller's system: `https://<hostname>/xvm/`

On the Proxy Controller's system: `https://<hostname>:21165/xvm/`

Log in as the root user of the host system.

Searching the Domain Model

Procedure for locating information about assets in the domain model.

The Domain Model Navigator has two tabs: Domain Model/Gear Model page and the JMX Navigator page. Each page contains the definition of assets and some statistics. To locate a specific asset, use the following search tactics:

- Match JMX patterns in the name. For example, to search for all cache managers, search for: *:type=*Cach*,*
- Use a JMX query:
  - **PowerOff**, which invokes the `PoweredOn = false` query
  - **Status Not OK**, which invokes the `not Status = 'OK'` query
  - **Unreachable**, which invokes the `Reachable = false query`
- Create a JMX query. These queries are case-sensitive.

Changing the Domain Model

Lists the operations you can perform on the domain model.

You can perform the following operations. You must provide the `root` password.

- Refresh
- Set

> **Warning:**
>
> An additional operation, Unregister, is available to Oracle Support engineers. Do not attempt to perform this operation unless you are directed by My Oracle Support.

These operations are recorded in the audit log located at `/var/cacao/instances/oem-ec/logs/audit-logs.0`

Logging Out of the Domain Model Navigator

Procedure for logging out of the domain model securely.

Because you are using the HTTPS protocol, the root credentials are included in each transaction. To log out securely, you must delete the credentials from the browser.

Secure the Agents

Procedure for encrypting the credentials for an Agent Controller.

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
```

About Securing the Browsers

Describes a how to make web browsers secure.

To implement transactions securely, Oracle Enterprise Manager Ops Center supports specific communications and security standards and methods such as HTTP, TLS, 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.

Note:

Oracle Enterprise Manager Ops Center does not use any version of SSL. All transactions with the web browser are in TLS. To verify that SSL is not used, use the following command:

```
openssl s_client -connect IPaddress:port -ssl3
```

The response includes the status:

```
SSL routines:SSL3_WRITE_BYTES:ssl handshake failure
```

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 HTTPS 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.

About Strong Cipher Encryption

Describes the role of encryption in the product architecture.

When Enterprise Manager Ops Center discovers an asset, it encrypts its transactions with the asset using AES-128 encryption. the strongest AES key available to the asset's platform. The default is AES-256 encryption; the alternatives are AES-192 and then AES-128.

By default, Enterprise Manager Ops Center encrypts its transactions with assets using AES-128 encryption. If an asset's `sshd` daemon uses a AES-192 or AES-256 encryption, you must also configure the Proxy Controller's system to manage the asset.

Note:

Some locales do not allow the use of strong ciphers. It is the user's responsibility to verify that this level of encryption is allowed under local regulations.

Verifying the Encryption Type

Procedure for determining information about encryption.

To determine the type of encryption used with an asset, view the asset's `/etc/ssh/sshd_config` file and look for content such as the following in the Ciphers section:

```
Ciphers aes256-cbc
```

Configuring Proxy Controllers to Use a Strong Cipher Suite

Procedure for encrypting credentials for a Proxy Controller.

Use the following procedure to download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files and move them to the systems running a Proxy Controller.

1. On an Internet-facing system, navigate to `http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html`.
2. Click **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 system.

Transport Layer Security (TLS)

These sections describe how to increase the level of security provided by the TLS protocol among components of the Oracle Enterprise Manager Ops Center product.

- About TLS Versions
- Changing the TLS Version for Apache UCE Container
- Changing the TLS Version for Glassfish Web Container

About TLS Versions

The Transport Layer Security protocol provides a foundation for privacy and data integrity between two communicating applications.

The Transport Layer Security protocol now has three versions of increasing security: TLS 1.0, TLS 1.1, and TLS 1.2.

The default version used in Oracle Enterprise Manager Ops Center is TLS 1.0. You can change the version of protocol for all communications if both the communicating application supports the TLS version you want to use. To change the version of protocol for all communications, change the Enterprise Controller's Glassfish server and each remote Proxy Controller's Glassfish Serve and change the Apache UCE Container.

Changing the TLS Version for Apache UCE Container

The Transport Layer Security protocol has three versions.

Starting in 12.3.2, the product's Apache UCE Container supports all three versions of TLS: TLSv1.0, TLSv1.1 and TLSv1.2. Some sites require a higher minimum version. To change the acceptable version of TLS, perform the following procedure on the Enterprise Controller and on each remote Proxy Controller.

1. Login as root.
2. Edit the `conf/extra/httpd-ssl.conf` file.
3. Locate the line: `SSLProtocol -all +TLSv1.2 +TLSv1.1 +TLSv1`
4. To set the protocol to accept only TLS v1.2, change the line to: `SSLProtocol -all +TLSv1.2`
5. Restart the Enterprise Controller.
6. Repeat this procedure on each remote Proxy Controller.

Changing the TLS Version for Glassfish Web Container

The Transport Layer Security protocol has three versions.

Starting in 12.3.2, the product's Glassfish Web Container supports all three versions of TLS: TLSv1.0, TLSv1.1 and TLSv1.2. The default is TLSv1.0, indicating that Version 1.0 is the minimum accepted level for communication. Some sites require a higher minimum version. To change the acceptable version of TLS, perform the following procedure on the Enterprise Controller and on each remote Proxy Controller.

Note:

Before changing the TLS version used by the Proxy Controller, check if all the Agent Controllers managed by the Proxy Controller can use the TLS version. Agent Controllers that use JDK 6 version lesser than 1.6.115 only supports TLSv1.0.

---

1. To see the current minimum version of the TLS protocol, issue the following command:`ecadm get-tls-level`

   ```
   TLS configuration : TLSv1.0 enabled, TLSv1.1 enabled, TLSv1.2
   enabled
   ```

2. To change the minimum version, use the `ecadm set-tls-level -e|--enable 0|1|2` command. The integers refer to the point release of the protocol version, for example, 1 indicates TLSv1.1. To change the minimum version to TLSv1.2, use the following command:

   ```
   ecadm set-tls-level -e 2
   ```

   ```
   TLS configuration : TLSv1.0 disabled, TLSv1.1 disabled,
   TLSv1.2 enabled
   ```

3. Repeat this procedure on each remote Proxy Controller.

Viewing the Enterprise Controller's Configuration

Procedure for displaying information about the Enterprise Controller.

To view the Enterprise Controller's configuration:

1. Select the Enterprise Controller in the **Administration** section of the Navigation pane.
2. Click the **Configuration** tab.
3. 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 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.

About Editing the Configuration

Description of the role for changing the configuration..

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.

Access to Database Data

Lists the parameters needed to use SQL.

The information in this section is also in Access the Product Database.

This section describes how to view the core product data stored in the Oracle Enterprise Manager Ops Center database using or . 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 , 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 Changing the Database Credentials for the Read-Only User 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.example.com where *example* is the string oracle. 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

Procedure for displaying information about the database.

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

Procedure for allowing remote access to the embedded database.

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

Procedure for getting access to the embedded database.

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

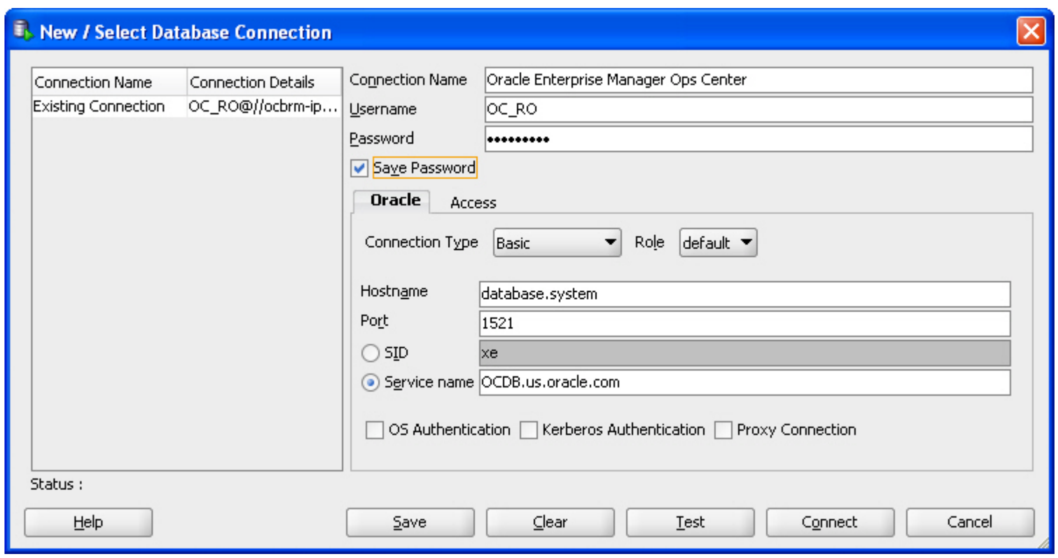
Procedure for configuring access to the database.

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

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 shown in the following figure. For customer-managed databases, the service name is included in the `mgmtdb.dburl` property in the `/var/opt/sun/xvm/db.properties` file.

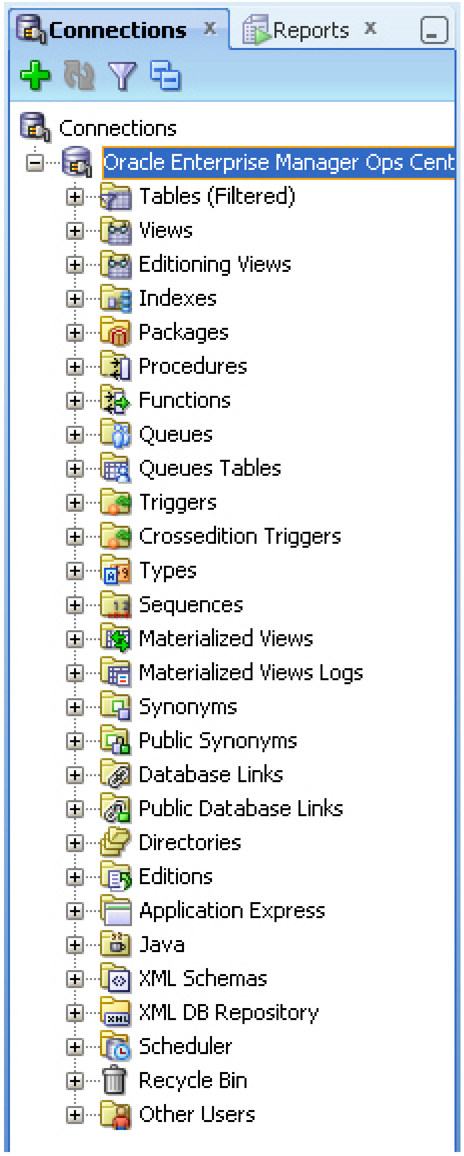


Viewing Data From the Database Using Oracle SQL Developer

Procedure for displaying information in the database.

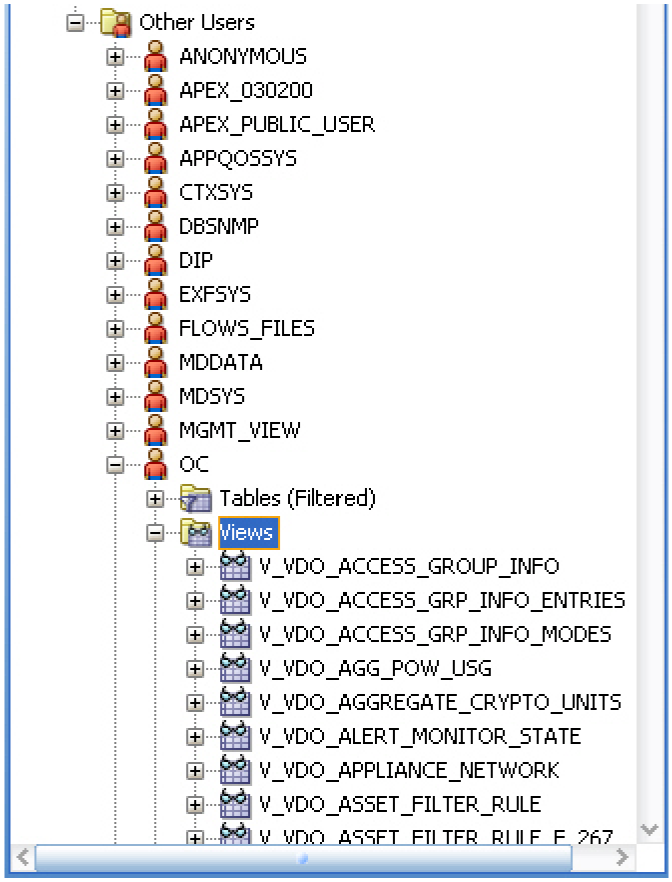
After you create the connection, view product data:

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

Procedure for displaying information in the database about assets.

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

Describes the role of security in the product architecture.

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 TLS 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

Describes 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.

Topics

- About Identity Management for Users
- Credentials for My Oracle Support
- Credentials for IAAS and Cloud Deployments

About Identity Management for Users

Describes how users are authenticated.

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.

About Configuring an LDAP Server

Procedure for changing the 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*.

To grant roles to the users in a directory server, you create groups on the directory server that correspond to the roles in Enterprise Manager Ops Center. You grant a role to a user by adding the user to the corresponding group, and remove a role from a user by removing them from the group. You cannot edit the roles of a directory server user through the user interface.

Users that are added from a directory server begin with complete privileges for each of their roles.

You must configure the remote directory server before adding it to Oracle Enterprise Manager Ops Center.

To Configure the Directory Structure

Procedure for adding a new directory server for Oracle Enterprise Manager Ops Center to use.

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

Procedure for adding a new directory server for Oracle Enterprise Manager Ops Center to use.

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.
   - **Host**: The host name of the directory server.
   - **Port**: The port number to be used to access the directory server.
   - **SSL**: Check this box to use TLS to connect to the directory server.
   - **Anonymous Bind**: Check this box to use anonymous binding to access the directory server.
   - **Username**: The user name used to access the directory server. Username is required only if Anonymous Bind is not checked.
   - **Password**: The password for the given user name. Password is required only if Anonymous Bind is not checked.
   - **Authentication**: Select Use Directory Server for Authentication or Use Ops Center Local Authentication.

   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 tree.
   - **Group search DN**: The container or operational unit in which to search for the role groups.
   - **Group search scope**: The scope of the group search. Select Search One Level or Search Subtree.
   - **User search DN**: The container or operational unit 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**.

About PAM Authentication

Procedure for setting the PAM authentication service.

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 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 the PAM configuration, create a PAM service with a different service name, which uses different PAM modules.

Verifying PAM Authentication

Procedure for displaying the PAM service.

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
```

Changing the PAM Authentication

Procedure for changing the the way PAM authentication is used..

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

Describes access to 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

Describes the protection of the location of the private key.

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.

About Authorization

Describes 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.

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.

About Credentials for Assets

Describes the types of credentials used to manage 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 for the **Protocols** field 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

Procedure for using an SSH key for access to assets.

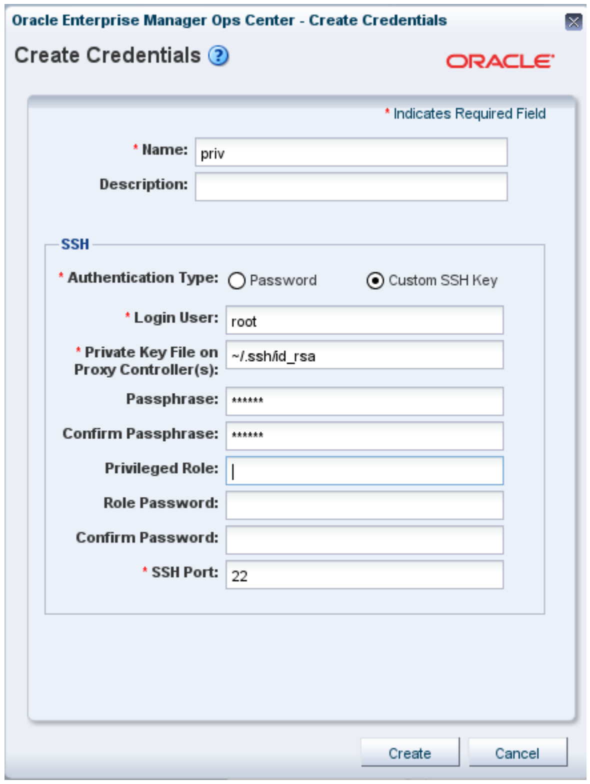
If you prefer not to use password-based SSH credentials, create an SSH key to get access to remote assets, such as operating systems, ILOM service processors, and XSCF service processors. The assets must support the SSH protocol. Oracle Enterprise Manager Ops Center does not protect the SSH keys. If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

Creating Credentials for Access to the Serial Console or SSH Tunnel

Procedure for creating console or SSH credentials.

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

To enable a connection to a service processor or virtual machine, define the user account that Enterprise Manager Ops Center uses to open an SSH tunnel on the Enterprise Controller or to create a serial connection.

Note:

If you do not specify this account, Enterprise Manager Ops Center creates an account each time it accesses a serial console and deletes the account when the connection is no longer needed. This activity might not conform to your site's security policy.

The following types of assets use SSH to connect to a serial console. Create an account for each type and define the same password for each account.

- Proxy Controllers
- Global zones that use agents and require access to the consoles of non-global zones
- Control domains that use agents and require access to the consoles of logical domains

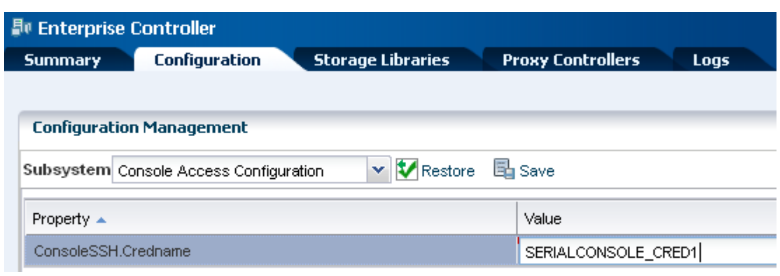
To create the account, define the `ConsoleSSHCredname` system property using the procedure in Defining the system property for console access and then define a user account for that property using either the procedure in Creating the account using Enterprise Manager Ops Center or the procedure in Creating the account using the useradd command.

Defining the system property for console access

Procedure configuring console access.

1. Select the **Administration** section in the Navigation pane.
2. Select the **Configuration** tab in the center pane.
3. In the Subsystem list, select **Console Access Configuration**. The `ConsoleSSH.Credname` system property is displayed.
4. Click in the **Values** column.
5. Enter the name of the new user account. For example, `SERIALCONSOLE_CRED1`.

Figure 3-2 Configuring Console Access



6. Click **Save**.

When the job is completed, define the account using the following procedure.

Creating the account using Enterprise Manager Ops Center

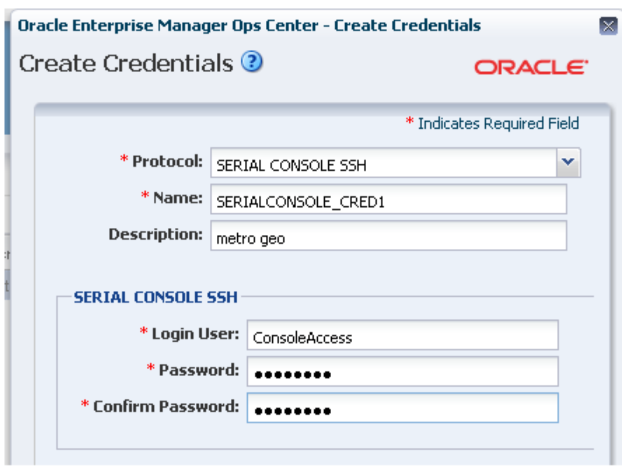
Procedure for creating a new account.

You must have the Security Admin role to perform this procedure.

After you define the user account, the account is created automatically in `/etc/passwd` the first time a job for console access is run. However, if your site's security policy requires that the operating system account must be created outside of Enterprise Manager Ops Center's control or if you prefer to create the account manually, use the procedure described in Creating the account using the useradd command.

1. Select the **Administration** in the Navigation pane.
2. Select **Credentials** in the Navigation pane.
3. Click **Create Credentials** in the Actions pane.
4. Select the **SERIAL_CONSOLE_SSH** protocol and enter the following details:
   - Name of the credential: Enter the value of the `ConsoleSSH.Credname` system property. In this example, `SERIALCONSOLE_CRED1`.
   - Login User: Enter a convenient or descriptive name for the user account, for example, `ConsoleAccess`.
   - Password for the user account and its confirmation.

   Figure 3-3 User Account for Console Access

5. Click **Create** to submit the job.

Creating the account using the useradd command

Procedure for creating a new account.

1. Create the home directory for the account. In the following example, the account is named `consolex`:

   ```
   mkdir /var/tmp/consolex
   ```

2. Add the user account with its shell, `/opt/sun/n1gc/bin/serial_console`:

   ```
   useradd -s "/opt/sun/n1gc/bin/serial_console" -d /var/tmp/consolex -u uid -P
   "profile" -A "solaris.zone.manage" consolex
   ```

   where *uid* is an available user ID on the Enterprise Controller's system and *profile* is either `LDoms Review` for a control domain or `Zone Management` for a global zone. The `-A` option is a feature of Oracle Solaris 11's `useradd(1m)` command that includes an authorization defined in `auth_attr(4)`.

3. Change the ownership of the home directory:

```
/bin/chown consolex /var/tmp/consolex
/bin/chmod 700 /var/tmp/consolex
```

4. Set and confirm the password for the account:

```
passwd consolex
```

About Managing Assets Using the agentadm Command

Describes a method of managing assets without storing credentials.

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

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 Install an Agent Controller

Lists prerequisites for installing an agent.

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

- To configure your Agent Controller software using an administrative user account on the Enterprise Controller you need:
  - User name: the user account provides authentication that supports Agent Controller registration. Use the user name of this account as the argument for the `-u` option of the agentadm command.
  - Password: use this password to populate the `/var/tmp/OC/mypasswd` file. Then use this file name as the argument for the `-p` option of the agentadm command.
- 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 with which you will associate 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 installation installs, or upgrades to, Oracle Java Runtime Environment (JRE) 1.6.0_91. If a later version of JRE is installed, the installation does not downgrade.

Using User Credentials to Install and Configure an Agent Controller Manually

Procedure for installing an Agent Controller manually.

This procedure creates a file that holds the password of the administrative user for your 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 to see the Agent Controller installation archives. For example:

```
# cd /var/opt/sun/xvm/images/agent/
# ls
OpsCenterAgent.Linux.i686.12.2.0.2503.zip
OpsCenterAgent.Linux.i686.12.2.0.2503.zip.sig
OpsCenterAgent.Solaris.i386.12.2.0.2503.zip
OpsCenterAgent.Solaris.i386.12.2.0.2503.zip.sig
OpsCenterAgent.Solaris.sparc.12.2.0.2503.zip
OpsCenterAgent.Solaris.sparc.12.2.0.2503.zip.sig
OpsCenterAgent.SolarisIPS.all.12.2.0.2503.zip
OpsCenterAgent.SolarisIPS.all.12.2.0.2503.zip.sig
#
```

2. Identify the Agent Controller archive that is appropriate for the system where you intend to install the Agent Controller, the target system. See Table 3-1 for a description of the available packages.

Table 3-1 Agent Controller Packages and Their Operating System and Architecture

File prefix	Operating System / Architecture
OpsCenterAgent.Linux.i686	Oracle Linux/x86
OpsCenterAgent.Solaris.i386	Oracle Solaris 10/x86
OpsCenterAgent.Solaris.sparc	Oracle Solaris 10 / Oracle SPARC
OpsCenterAgent.SolarisIPS.all	Oracle Solaris 11 / x86 and Oracle SPARC

3. On the system where you want to install the Agent Controller, create the following directory:

```
# 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. Respond to any authentication or confirmation prompts that are displayed. For example:

```
# scp OpsCenterAgent.Solaris.sparc.12.2.0.2503.zip root@10.0.0.0:/var/tmp/OC
Password:
OpsCenterAgent.S 100% |
**********************************************************************| 187078 KB
00:32
#
```

5. Navigate 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.Solaris.sparc.12.2.0.2503.zip
(output omitted)
```

7. If you are installing the Agent Controller on Oracle Solaris 8-10, 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.
```

   If you are installing the Agent Controller on Oracle Solaris 11, run the `install` command with the `-p` option and specify the IP address. The command configures a local IPS repository using the IP address. For example:

```
# OpsCenterAgent/install -p 10.0.0.1
```

   If you are installing an Oracle VM Server Virtualization Controller Agent, use the `-l` (or `--ldom`) option.

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 to add 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 the 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: `/opt/SUNWxvmoc/bin/agentadm configure`
    - Linux OS: `/opt/sun/xvmoc/bin/agentadm configure`

      The example commands below use the following options:

- `-u`: Specifies the administrative user that exists on the Enterprise Controller to which the Proxy Controller is connected. Be certain that the password that you specified in the `/var/tmp/OC/mypasswd` file is correct for the user that you specify for this option.

Note:

The examples use `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
10.0.0.0
agentadm: Version 1.0.3 launched with args: configure -u droot -p /var/tmp/OC/
mypasswd -x 10.0.0.1
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 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, you can 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
10.0.0.0 -a 10.0.0.1
(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.
```

After the Agent Controller has been unconfigured, correct the problem that was indicated by the error message, 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://10.0.0.0:21165
urn:scn:clregid:abcdef12-6899-4bcc-9ac7-a6ebaf71c1f5:20090420171121805
#
```

Using a Token to Install and Configure an Agent Controller Manually

Procedure to install an Agent Controller.

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 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. See Table 3-1 for a description of the available packages.

3. On the system where you want to install the Agent Controller, create the following directory:

```
# 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. Respond to any authentication or confirmation prompts that are displayed. For example:

```
# scp OpsCenterAgent.Solaris.sparc.12.2.0.2503.zip root@10.0.0.0:/var/tmp/OC
Password:
OpsCenterAgent.S 100% |
*********************************************************************| 187078 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. If you are installing the Agent Controller on Oracle Solaris 8-10, 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.
#
```

   If you are installing the Agent Controller on Oracle Solaris 11, run the `install` command with the `-p` option and specify the IP address. The command configures a local IPS repository using the IP address. For example:

```
# OpsCenterAgent/install -p 10.0.0.1
#
```

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. For example:

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

(output omitted)

trust-store=/var/opt/sun/xvm/security/jsse/scn-proxy/truststore
auto-reg-token=abcdef12-1700-450d-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. For example:

```
# 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 Proxy Controller with the following changes:

    - Remove the `auto-reg-token=`.
    - Remove any backslash characters from the token string. For example:

    ```
    abcdef12-1700-450d-b038-ece0f9482474:1271743200000:T
    ```

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

    - Oracle Solaris OS: `/opt/SUNWxvmoc/bin/agentadm configure`
    - Linux OS: use the `/opt/sun/xvmoc/bin/agentadm configure`

    The example commands use the following options:

    - `-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. For example:

    ```
    # /opt/SUNWxvmoc/bin/agentadm configure -t /var/tmp/OC/mytoken -x 10.0.0.0
    agentadm: Version 1.0.3 launched with args: configure -t /var/tmp/OC/mytoken -
    x 10.0.0.0
    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, you can 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 10.0.0.0 -a
10.0.0.1
(output omitted)
```

12. 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.
```

    After the Agent Controller has been unconfigured, correct the problem that was indicated by the error message, 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://10.0.0.0:21165
urn:scn:clregid:abcdef12-6899-4bcc-9ac7-a6ebaf71c1f5:20090420171121805
#
```

Changing Credentials of Managed Assets

Lists the procedures for managing the credentials for assets.

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

Topics

- Upgrading Management Credentials From a Previous Version
- Updating Management Credentials
- Creating Management Credentials
- Editing Management Credentials
- Copying Management Credentials
- Deleting Management Credentials

Preparing to Use sudo

Procedure to enable escalation of SSH credentials on discovered assets in Oracle Enterprise Manager Ops Center.

1. Log into the asset as root.
2. Enter the `visudo` command to edit the asset's `sudoers` file safely.
3. Edit the sudoers file to conform with the example. Add the command aliases for discovery and provisioning in the following way according to the operating system of the asset and whether it :
   - For agentless Oracle Solaris assets, add the SOLARIS_DISCOVERY section of the file.
   - For agent-managed Oracle Solaris assets, add the SOLARIS_DISCOVERY and SOLARIS_PROVISIONING
   - For agentless Oracle Linux assets, add the LINUX_DISCOVERY section of the file.
   - For agent-managed Oracle Linux assets, add the LINUX_DISCOVERY and LINUX_PROVISIONING
4. In the `## User privilege specification` section, add the name of the new SSH credential that you created or will create using the procedure in "Creating Management Credentials.". Because a password is mandatory, do not add the NOPASSWD parameter.
5. Save and close the file.
6. Repeat this procedure on each asset.

Example 3-1 Format of sudoers File for Ops Center

```
## sudoers file.
##
## This file MUST be edited with the 'visudo' command as root.
## Failure to use 'visudo' may result in syntax or file permission errors
## that prevent sudo from running.
##
## See the sudoers man page for the details on how to write a sudoers file.
##

##
## Host alias specification
```

```
##
## Groups of machines. These may include host names (optionally with wildcards),
## IP addresses, network numbers or netgroups.
# Host_Alias    WEBSERVERS = www1, www2, www3

##
## User alias specification
##
## Groups of users.  These may consist of user names, uids, Unix groups,
## or netgroups.
 User_Alias    OPSCENTER = <username>

##
## Cmnd alias specification
##
## Groups of commands.  Often used to group related commands together.

    Cmnd_Alias SOLARIS_DISCOVERY = /sbin/ifconfig -a, \
                /usr/sbin/virtinfo -ap, \
        /usr/sbin/dladm, \
        /opt/SUNWldm/bin/ldm

    Cmnd_Alias SOLARIS_PROVISIONING = /usr/bin/sc-console, \
                /var/scn/install/uninstall, \
        /usr/sbin/zlogin, \
                /bin/cat */opt/SUNWxvm/xvm_zone_id, \
        /var/tmp/OpsCenterAgent/install, \
                /opt/SUNWxvmoc/bin/agentadm, \
                /usr/lib/cacao/bin/cacaoadm, \
                /usr/bin/unzip -q -o -d /var/tmp/ /var/tmp/OpsCenterAgent*

    Cmnd_Alias LINUX_DISCOVERY = /sbin/ifconfig -a, \
                /usr/sbin/virtinfo -ap

    Cmnd_Alias LINUX_PROVISIONING = /usr/bin/sc-console, \
                /var/scn/install/uninstall, \
        /tmp/OpsCenterAgent/install, \
                /opt/sun/xvmoc/bin/agentadm, \
                /opt/sun/cacao2/bin/cacaoadm, \
                /usr/bin/unzip -q -o -d /tmp/ /tmp/OpsCenterAgent*

##
## Defaults specification
##
## You may wish to keep some of the following environment variables
## when running commands via sudo.
##
## Locale settings
# Defaults env_keep += "LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET"
##
## Run X applications through sudo; HOME is used to find the
## .Xauthority file.  Note that other programs use HOME to find
## configuration files and this may lead to privilege escalation!
# Defaults env_keep += "HOME"
##
## X11 resource path settings
# Defaults env_keep += "XAPPLRESDIR XFILESEARCHPATH XUSERFILESEARCHPATH"
##
## Desktop path settings
# Defaults env_keep += "QTDIR KDEDIR"
##
```

```
## Allow sudo-run commands to inherit the callers' ConsoleKit session
# Defaults env_keep += "XDG_SESSION_COOKIE"
##
## Uncomment to enable special input methods.  Care should be taken as
## this may allow users to subvert the command being run via sudo.
# Defaults env_keep += "XMODIFIERS GTK_IM_MODULE QT_IM_MODULE QT_IM_SWITCHER"
##
## Uncomment to enable logging of a command's output, except for
## sudoreplay and reboot.  Use sudoreplay to play back logged sessions.
# Defaults log_output
# Defaults!/usr/bin/sudoreplay !log_output
# Defaults!/usr/local/bin/sudoreplay !log_output
# Defaults!/sbin/reboot !log_output
 Defaults logfile=/var/log/sudo.log

##
## Runas alias specification
##

##
## User privilege specification
##
 root ALL=(ALL) ALL

## The password of OPSCENTER must be mandatory.
 OPSCENTER ALL=(root) SOLARIS_DISCOVERY,SOLARIS_PROVISIONING

## Uncomment to allow members of group wheel to execute any command
# %wheel ALL=(ALL) ALL

## Same thing without a password
# %wheel ALL=(ALL) NOPASSWD: ALL

## Uncomment to allow members of group sudo to execute any command
# %sudo ALL=(ALL) ALL

## Uncomment to allow any user to run sudo if they know the password
## of the user they are running the command as (root by default).
# Defaults targetpw  # Ask for the password of the target user
# ALL ALL=(ALL) ALL  # WARNING: only use this together with 'Defaults targetpw'

## Read drop-in files from /etc/sudoers.d
## (the '#' here does not indicate a comment)
#includedir /etc/sudoers.d
```

Upgrading Management Credentials From a Previous Version

Procedure for use new credentials to manage assets discovered by an earlier version of Oracle Enterprise Manager Ops Center.

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

If a discovered asset is blacklisted, the same can be removed by updating the management credentials.

To upgrade management credentials, perform the following steps:

1. On the Navigation pane, select **All Assets**.
2. In the Actions pane, click **Upgrade Management Credentials**.

3. Select an asset category: operating systems; servers; or chassis, m-series, and switches.

4. 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

Procedure for updating credentials used to manage an asset.

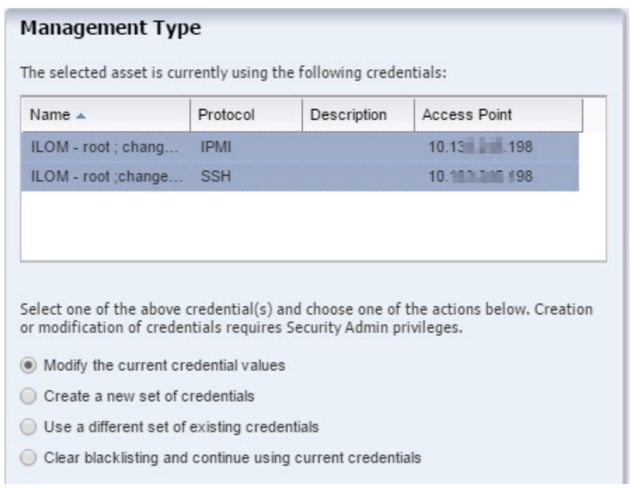
You can change the set of management credentials used by an asset or group of assets.

To update management credentials, perform the following steps:

1. On the Navigation pane, select an asset or group.

2. In the Actions pane, click **Update Management Credentials**.

Figure 3-4 Wizard for Update Management Credentials



3. Select the credentials that you want to change. You can select more than one type of credentials.

4. Click **Modify the current credential values**.

5. Edit the username and/or password.

> **Note:**
>
> If you are modifying the SNMPv3 credentials, then you can edit the username, authentication protocol, authentication password, privacy protocol, or privacy password.

6. Click Finish to submit the change.

Creating Management Credentials

Procedure for creating credentials used to manage an asset.

You can create a new set of management credentials. These credentials can then be used to discover and manage new assets or to manage existing assets.

To create management credentials, perform the following steps:

1. On the Navigation pane, under Administration, select **Credentials**.
2. In the Actions pane, click **Create Credentials**.
3. Click on the drop-down list to see the list of available protocols. Accept the default SSH protocol or select a different protocol. Depending on the type of protocol you select, the remaining fields change to collect the required information for the credentials. For specific examples, see Creating SSH Credentials or Creating SNMPV3 Credentials.
4. Specify a name and description, such as the purpose of the credentials.
5. Select or specify the required information for the type of credential, such as the username and password.
6. Click **Create** to create the management credentials.

The new credentials are now available to be used in discovery profiles.

Creating SSH Credentials

Create a set of SSH credentials to discover and manage new assets or to manage existing assets.

The default protocol for managing assets is SSH. To create SSH credentials, perform the following steps:

1. On the Navigation pane, under Administration, select **Credentials**.
2. In the Actions pane, click **Create Credentials**.
3. Specify a name and description, such as their purpose for the credentials.
4. Specify the username and password.
5. Accept the default authentication type or choose one of the alternatives. Each type has different requirements for authentication.
   - Password: This is the default type of authentication and requires a login username and password.
   - Custom SSH Key: Creates a public SSH key by specifying the Login User name, a Private Key file name, and a passphrase. In the **Private Key File on Proxy Controller(s)** field, accept the default file or change it to refer to other keys. The Proxy Controller installs the SSH public key on the asset's privileged user's authorized SSH key.
   - Ops Center Key: Oracle Enterprise Manager Ops Center generates a new SSH key pair, based on the username you provide, and installs the public key in the asset's login account during discovery. This method requires a set of credentials to begin the discovery. After discovery, the SSH key pair is used. This method does not provide a way to escalate privileges.
6. You can allow the new account to use escalated privileges. The default method is to not allow a change in privileges. The alternatives are to specify a role for the account or to add sudo to the account.

- If you choose the Role method, the Privileged Role field is displayed. Enter the name of an Ops Center role and specify a password. The new account has this level of access.
- If you choose the Sudo method, the Privileged Role field is displayed. Enter the name of an Ops Center account and specify a password. This account must be included in the asset's `/etc/sudoers` file. The privileges defined in the `/etc/sudoers` file will be used by the new account. See "Preparing to Use sudo" for instructions in creating this file. You can edit this file after you complete this procedure, but the Ops Center account must be in the file before the new credentials are effective.

7. Accept the default port for SSH of 22, unless your site has a different requirement.
8. Click **Create** to create the management credentials.

   For more information on creating SSH Credentials, see *Oracle Enterprise Manager Ops Center Configuration Reference*.

Creating SNMPV3 Credentials

Procedure for creating credentials for accessing assets in Oracle Enterprise Manager Ops Center.

Create a set of management credentials to discover and manage new assets or to manage existing assets.

To create credentials that use the SNMPV3 protocol, perform the following steps:

1. On the Navigation pane, under Administration, select **Credentials**.
2. In the Actions pane, click **Create Credentials**.
3. Click on the drop-down list to see the list of available protocols. Click **SNMPV3**.
4. Specify a name and description, such as their purpose for the credentials.
5. Specify the user name with the prefix OC for the credential.

   Note:

   The user name for SNMPV3 protocol is always prefixed with `OC`.

   ---

6. Accept the default authentication protocol, MD5, or choose SHA, which is a stronger authentication protocol.
7. Enter a password for authentication.
8. Accept the default privacy protocol, DES, or choose AES, which is a stronger encryption protocol.
9. Enter a password for encryption.
10. Click **Create** to create the management credentials.

    For more information on creating SSH Credentials, see *Oracle Enterprise Manager Ops Center Configuration Reference*.

Editing Management Credentials

Procedure for changing the credentials that manage and asset.

You can edit an existing set of management credentials to reflect changes to the managed assets.

To edit management credentials, perform the following steps:

1. On the Navigation pane, under Administration, select **Credentials**.
2. In the center pane, select a set of credentials and click the **Edit Credentials** icon.
3. Edit the description and the information required by the protocol, then click **Update** to save the changes.

Copying Management Credentials

Procedure for duplicating credentials used to manage an asset.

You can copy an existing set of management credentials to create a new set.

To copy management credentials, perform the following steps:

1. On the Navigation pane, under Administration, select **Credentials**.
2. In the center pane, select a set of credentials and click the Copy Credentials icon.
3. Edit the name, description, and the information required by the protocol, then click **Copy** to save the new set of credentials.

Deleting Management Credentials

Procedure for removing credentials used to manage an asset.

You can delete an existing set of management credentials. Discovery profiles that use the credentials might no longer function, and Agentless assets that are managed using the credentials must be given a new set.

To delete management credentials, perform the following steps:

1. On the Navigation pane, under Administration, select **Credentials**.
2. In the center pane, select a set of credentials and click the **Delete Credentials** icon.
3. Click **OK** to delete the credentials.

Creating a Credential Plan

Procedure for creating a deployment plan for credentials.

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

Procedure for setting up credentials for an asset.

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.

About Certificates

Describes self-signed certificates.

By default, Oracle Enterprise Manager Ops Center 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 Substituting Certificates for the Glassfish Web Container to replace the self-signed certificate with a certificate from a Certificate Authority.

Configuring and Using Access Control

Lists the procedures for configuring an asset so that it can be managed.

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

Topics

- Verifying Security of Session Cookies
- Setting the Expiration Time for Sessions
- Removing Code Examples

Verifying Security of Session Cookies

Procedure for displaying information about a certificate.

Oracle Enterprise Manager Ops Center uses cookies to store session data for individual users. The cookies are encrypted using JSESSIONID and use the `http-only` flag to deny access to scripting languages.

The HTTP protocol includes the TRACE method to echo input. Because it is possible to use TRACE requests to view session cookies, Oracle Enterprise Manager Ops Center redirects HTTP transactions to HTTPS where the TRACE method is disabled.

To confirm that TRACE is disabled, use the following command on the Enterprise Controller's system or a Proxy Controller's system:

```
# curl -v --insecure -X TRACE https://<hostname>:9443
(output omitted)
HTTP/1.1 405 TRACE method is not allowed
```

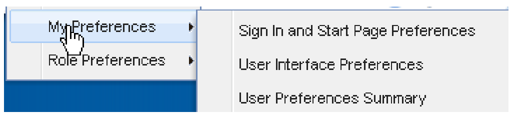
Setting the Expiration Time for Sessions

Procedure for setting the activity timer for a session.

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 3-5.

Figure 3-5 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

Procedure for removing code from the product's command line interface.

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

Lists the procedures for backing up information about the assets.

Topics

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

Using an NFS Server

Procedure for setting up an NFS server for Oracle Enterprise Manager Ops Center.

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`.

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.

About Backing Up and Restoring the Enterprise Controller

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.

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

The `ecadm backup` and `ecadm restore` commands back up and restore the Enterprise Controller. They also back up and restore the co-located Proxy Controller unless otherwise specified. The `proxyadm backup` and `proxyadm restore` commands back up and restore remote Proxy Controllers.

The `ecadm backup` command creates a `tar` file that contains all of the Oracle Enterprise Manager Ops Center information stored by the Enterprise Controller, including asset data, administration data, job history, and the database password, but not including software and storage library contents. The `proxyadm backup` command creates a `tar` file that contains all of the Oracle Enterprise Manager Ops Center information stored by the Proxy Controller, including asset data. You can specify the name and location of the backup file and the log file for each command.

Run the `ecadm backup` and `proxyadm backup` commands regularly and save the backup files on a separate system.

If the Enterprise Controller system fails, you can use the `ecadm restore` command and the backup file to restore the Enterprise Controller to its previous state on the original system or on a new system. The `ecadm restore` command accepts the name of the backup file as input, and restores the Enterprise Controller to the state it had at the time of the backup.

If you are restoring the Enterprise Controller on a new system, you must verify that the new system is compatible.

- The new system must have the same architecture and operating system as the old system. It is recommended that the operating system versions be identical, including updates and SRUs.
- The host name of the new system should be the same as the old system. You can change the host name of the new system, provided the old host name is added as an alias host name in the new system.
- The IP address of the new system can be different. If the new system has a different IP address, the restore process includes a step to configure any remote Proxy Controllers to use the new Enterprise Controller IP address. The MAC address of the new system can be different.
- The new system's Enterprise Controller software version must also match those of the backed up system.

For a regular back up and restore procedure, the IP address and the host name of the new system should match that of the old system. For a disaster recovery procedure, the IP address and the host name of the new system can be different than that of the old system.

If a remote Proxy Controller system fails, you can use the `proxyadm restore` command and the backup file to restore the Proxy Controller. The `proxyadm restore` command accepts the name of the backup file as input, and restores the Proxy Controller to the state it had at the time of the backup.

Some of the procedures described in this section use the `ecadm` and `proxyadm` commands. See the *Oracle Enterprise Manager Ops Center Administration* for more information about these commands.

- On Oracle Solaris systems, these commands are in the `/opt/SUNWxvmoc/bin/` directory.
- On Linux systems, these commands are in the `/opt/sun/xvmoc/bin/` directory.

The following features and topics are covered in this chapter:

- Backing Up an Enterprise Controller
- Restoring an Enterprise Controller

Backing Up an Enterprise Controller

You can create a backup for the Enterprise Controller using the `ecadm` command with the `backup` subcommand.

You can create a backup for the Enterprise Controller using the `ecadm` command with the `backup` subcommand.

Note:

The `ecadm backup` command does not back up the `/var/opt/sun/xvm/images/os` directory because the size of some of the OS image files in this directory can be prohibitively large.

In addition to running the `ecadm backup` command, back up the `/var/opt/sun/xvm/images/os` directory and archive the files to another server, file-share facility, or a location outside of the `/var/opt/sun` directory.

By default, the server data is saved in a backup file in the `/var/tmp` directory with a file name that includes a date and time stamp. You can define the file name and location during the backup, as shown in the example below.

If you are using an embedded database, the backup file includes the product schema from the embedded database. If you are using a customer-managed database, you can back up the database schema using the `--remotedb` option, or you can use the existing backup and recover processes implemented by your database administrator.

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.

   The following options can be used with the `ecadm` command:

   - **-o|--output <backup file>**: Specify the file in which the backup archive is generated. Do not specify a path inside the `/opt/*xvm*` directories. The default output file is `/var/tmp/sat-backup-<date>-<time>.tar`.
   - **-l|--logfile <logfile>**: Save output from command in <logfile>. Log files are stored in the `/var/tmp/` directory.
   - **-d|--description <description string>**: Embed the <description string> as the description of the backup archive.
   - **-r|--remotedb**: If the Enterprise Controller uses a customer-managed database, export the database schema to a `.dmp` file in the Oracle Enterprise Manager Ops Center dump directory on the database server. This directory is `/var/tmp/ocdumpdir` in the examples used in the installation documentation, but any directory can be specified as the dump directory during installation and configuration. The `.dmp` file lets the restore operation restore the database schema. This option only backs up the Oracle Enterprise Manager Ops Center database schema; other schemas and data are not included.
   - **-t|--tag <tag>**: Embed <tag> as a single-word tag in the backup archive
   - **-T|--tempdir <dir>**: Specify the temporary staging directory location.
   - **-v|--verbose**: Increase verbosity level. This option may be repeated.

   For example:

```
ecadm backup -o /var/backup/EC-17December.tar
ecadm: using logFile = /var/opt/sun/xvm/logs/sat-backup-2012-12-17-16:21:12.log
ecadm: *** PreBackup Phase
ecadm: *** Backup Phase
ecadm: *** PostBackup Phase
ecadm: *** Backup complete
ecadm: *** Output in /var/backup/EC-12December.tar
ecadm: *** Log in /var/opt/sun/xvm/logs/sat-backup-2012-12-17-16:21:12.log
```

3. Copy the backup file to a separate system.
4. Start the Enterprise Controller by running the `ecadm` command with the `start` subcommand and the `-w` option.

   For example:

```
ecadm start -w
```

Restoring an Enterprise Controller

You can use a backup file to restore the state of the Enterprise Controller to the state it had at the time of the backup.

This procedure restores the data from the backup file, which is the archive created by the `backup` operation. It also defines the procedure to change the IP address of an Enterprise Controller.

If you are using an embedded database, the restore process restores the product schema from the embedded database. If you are using a customer-managed database, you can use the `--remotedb` option to restore the product schema on the customer-managed database, or do not use this option to restore the Enterprise Controller without restoring the database.

Note:

Before you restore on a system, you must uninstall any previously existing Enterprise Controllers, Proxy Controllers, and Agent Controllers from the system.

---

1. Prepare the Enterprise Controller system.

   - If you are restoring the backup on a new system, then the new system must have the same architecture and operating system as the old system. It is recommended that the operating system versions be identical, including updates and SRUs. The new system's host name and Enterprise Controller software version must also match those of the backed up system. If the host name does not match, add the old host name as an alias to the `/etc/hosts` file.
   - 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
     ```

2. Install the Enterprise Controller to the same version that was running when the backup was made, but do not configure the Enterprise Controller, as the `ecadm restore` command restores your configuration settings.

   - Oracle Solaris OS: See *Oracle Enterprise Manager Ops Center Installation for Oracle Solaris Operating System*.
   - Linux OS: See *Oracle Enterprise Manager Ops Center Installation for Linux Operating Systems*.

Note:

If you are using a customer-managed database which is still functioning, the Enterprise Controller installation procedure indicates several steps that you must skip and an additional option that you must use to avoid overwriting your existing database schema.

---

3. Run the `ecadm` command with the `restore` subcommand and the `-i <backup directory location and file name>` flag.

   The following options may be used with the `ecadm` command:

   - **-i|--input <backup file>**: (Required) Specify the location of the backup file.
   - **-l|--logfile <logfile>**: Save output from command in <logfile>. Log files are stored in the `/var/tmp/` directory.
   - **-r|--remotedb**: If the Enterprise Controller uses a customer-managed database, this option restores the product schema on that database. If you are restoring on a new database system, copy the `.dmp` file from the `/var/tmp/ocdumpdir` directory that corresponds with your backup file to the new system and verify that it is owned by the oracle user on the new system.
   - **-e|--echa**: If the Enterprise Controller is configured in HA mode, this option indicates that the co-located Proxy Controller should not be restored.
   - **-d|--tempdir <dir>**: Specify the temporary staging directory location.
   - **-v|--verbose**: Increase verbosity level (may be repeated)

   For example:

```
 restore -i /var/backup/EC-17December.tar
ecadm: using logFile = /var/opt/sun/xvm/logs/sat-restore-2012-12-17-21:37:22.log
ecadm: *** PreRestore Phase
ecadm: *** Restore Phase
ecadm: *** PostRestore Phase
ecadm: *** Log in /var/opt/sun/xvm/logs/sat-restore-2012-12-17-21:37:22.log
```

4. For an Enterprise Controller with an enabled co-located Proxy Controller, the restore should restore and start the co-located Proxy Controller. The co-located Proxy Controller starts only if the Proxy Controller was enabled during the backup procedure. Check the co-located Proxy Controller's status using the `proxyadm` command with the `status` subcommand. If the Proxy Controller is stopped, restart it using the `proxyadm` command with the `start` subcommand and the `-w` option.

```
# proxyadm status
offline
# proxyadm start -w
proxyadm: Starting Proxy Controller with SMF...
proxyadm: Proxy Controller services have started
```

5. If you restored the Enterprise Controller on a new system, restart each remote Proxy Controller to use the new Enterprise Controller.

   a. Stop the Proxy Controller using the `proxyadm` command with the `stop` subcommand and the `-w` option. For example:

```
# proxyadm stop -w
```

b. On the remote Proxy Controller, update the `/var/opt/sun/xvm/persistence/scn-proxy/connection.properties` URL property to point to the IP address of the new Enterprise Controller. Update this URL property through the command line interface using the `proxyadm` command with the `update` subcommand and the `-s` option:

```
proxyadm update -s|--satellite-ip <ip>
```

c. Restart the Proxy Controller using the `proxyadm` command with the `start` subcommand and the `-w` option. For example:

```
# proxyadm start -w
```

6. Restart the co-located Agent Controllers using the `agentadm` command with the `start` subcommand and the `-w` option. For example:

```
/opt/SUNWxvmoc/bin/agentadm start -w
```

Note:

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

Note:

During the database schema restore, an import log is created. The name of the import log appears in the Enterprise Controller restore log file with the `OC_import<timestamp>.log` format. You can check the progress of the database import status using this import log.

Example: Restoring an Enterprise Controller With an Embedded Database

Sample command for restoring an Enterprise Controller.

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

```
# /opt/SUNWxvmoc/bin/ecadm restore -v -i /var/tmp/OC/server1/EC-17December.tar -l
logfile-restore-15January.log
```

Example: Restoring an Enterprise Controller With a Customer-Managed Database

Sample command for restoring an Enterprise Controller.

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

```
# /opt/SUNWxvmoc/bin/ecadm restore -i /var/tmp/OC/server1/EC-17December.tar -r
```

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

Sample command for restoring an Enterprise Controller.

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

```
# /opt/SUNWxvmoc/bin/ecadm restore -v -i /var/tmp/OC/server1/EC-17December.tar -l
logfile-restore-15January.log
```

Index

Symbols

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P