An Oracle White Paper
June, 2013

Enterprise Manager Cloud Control 12*c* Infrastructure and Operational Security Best Practices

Executive Overview

Oracle Enterprise Manager Cloud Control (Enterprise Manager) is Oracle's integrated enterprise IT management product line, and provides the industry's only complete cloud lifecycle management solution. Oracle Enterprise Manager creates business value from IT by leveraging the built-in management capabilities of the Oracle stack for traditional and cloud environments, allowing customers to achieve unprecedented efficiency gains while dramatically increasing service levels. Enterprise Manager provides:

- *Best service levels for traditional and cloud applications* through business-driven application management

- *Maximum return on IT management* investment through the best solutions for intelligent management of the Oracle stack and engineered systems with real-time integration of Oracle's knowledgebase with each customer environment

- *A complete cloud lifecycle management solution* allowing you to quickly set up, manage and support enterprise clouds and traditional Oracle IT environments from applications to disk.

- *Unmatched customer support experience* through real-time integration of Oracle's knowledgebase with each customer environment

Introduction

The dynamic and complex nature of today's IT environments, the potential fallout of security breaches in terms of the financial implications and loss of goodwill coupled with stringent regulatory requirements make security a critical area of consideration for both business and IT managers. Whilst security considerations are important for standalone applications, the introduction of distributed system management applications can make it yet more challenging. While standardized security best practices are available for databases and application servers, there aren't any standardized security benchmarks specifically for system management products. However, Enterprise Manager has been evaluated and in the past, has received a third party security certification, by the Common Criteria Recognition Arrangement.

Securing Enterprise Manager requires working closely with System Administrators, Network Administrators, Database Adminstrators, Application Administrators and the Security team. This document can be used by all concerned parties to identify various security considerations and the best practices for securing Oracle Enterprise Manager deployments. The recommendations in this document are based on our experience with both customer deployments and Oracle's own internal usage of Enterprise Manager.

Enterprise Manager Architecture Overview

Enterprise Manager provides a central point for monitoring and administration in the data center. To achieve this, it collects information from a variety of distributed components and consolidates it in a centralized repository. The key Enterprise Manager components must all work in concert for the system to operate correctly. The components involved in collecting, processing and presenting this information to users are as follows:

- **Targets** - A Target, or more specifically, a Target instance, can be defined as any entity that can be monitored within an enterprise. This entity can be an application running on a server, the server itself, the network, or any of its constituent parts.
- **Oracle Management Agent (Agent)** – The Oracle Management Agent is a software component that is installed on every monitored host in the enterprise. Agents collect information from the Targets running on the host and send this information to the Oracle Management Service (OMS). Agents also perform operations against the Targets on behalf of Enterprise Manager users. There are many different types of Targets that Enterprise Manager can manage. Examples include Host, VM Guest, Database, Listener, ASM, WebLogic Server, Service Bus and Fusion Applications components
- **Oracle Management Service (OMS)** – The Oracle Management Service is the central component in Enterprise Manager with which all other components interact. The OMS is deployed on a WebLogic Server and must be available in order for the Agents to upload data and for administrators to access the Enterprise Manager console.
- **Oracle Management Repository (Repository)** – The Oracle Management Repository is used as a persistent data store. Examples of the information stored in the repository include user information, job definitions, monitoring and alerting settings and all configuration and monitoring data related to Targets. The OMS cannot run if the repository is unavailable.
- **Software Library** – The Software Library is a filesystem repository that stores software entities such as software patches, virtual appliance images, reference gold images, application software, and their associated directive scripts. The Software Library is accessed by the OMS and is used extensively by the Enterprise Manager framework for features such as self-update and Agent deployment.
- **Console** – The Console is a browser-based web application that is the main user interface for Enterprise Manager. This console allows the administrator to monitor, manage and report on the Enterprise Manager Targets that have been setup.
- **Certificate Authority** – Issues digital certificates that certify the ownership of a public key.
- **Cipher Suite** - Named combination of authentication, encryption and message authentication code to negotiate settings for a network connection using TLS or SSL.
- **HTTPS** - Hypertext Transfer Protocol Secure (HTTPS) uses SSL/TLS to provide encrypted communication and secure identification.

- **Firewall** - Device that permits or denies network transmission based on ports and protocols to secure network data.

- **SSLv3** - Cryptographic protocol that provides communication security by encrypting segments of network connections..

- **TLSv1** - Next generation SSL, client and server negotiate a stateful connection by using a handshaking procedure in which they agree on various parameters used to establish the connection's security.

Data Confidentiality and Integrity

To ensure data confidentiality and integrity data must not be disclosed to entities unless they are authorized to access. Data must not be changed, destroyed or lost in an unauthorized or accidental manner.

A man-in-the-middle attack is the act of intercepting data or messages intended for someone else, similar to eavesdropping. If your data and network are not protected as they are transferred from client to server, your passwords, personal information and more could be "sniffed" from the network and used maliciously.

The best way to protect data confidentiality and integrity for your Enterprise Manager environment is to secure the communications of all involved components and protect the systems behind a firewall.

Data Availability

Enforcing data availability means to make data available and usable upon demand by an authorized entity. To do this, you must prevent denial-of-service attacks. A DoS attack is an attempt to make a system or service unusable by saturating it with network communications. This can cause the system to reset or deplete its resources such that it cannot process valid transactions.

Enterprise Manager is often the central management system, Repository and console for an organization or company. If the system is made unavailable by a DoS attack, the Target status may be unknown and outages or issues may be missed.

Authenticate

Authentication is the process of validating a subject that is allowed to act on behalf of a given principal (user, computer, etc). The most common form of authentication is login credentials and passwords. There are many ways to implement authentication in a secure manner and to ensure password crack attempts (or hacking) are defeated.

In the Enterprise Manager framework, authentication covers both the authentication to the Enterprise Manager Console and authentication to the managed Targets.

Authorize

Authorization is the act of validating the privileges and permissions of an authenticated subject. To avoid exploiting authorization, you must implement a policy of segregation of duties. This means no one person should be given responsibility for more than one related function.

Enterprise Manager users may vary widely among a company, and they may have very different roles and purposes.

Audit

Auditing is the process of collecting, storing and distributing information about operating requests and the outcome of those requests for the purposes of non-repudiation. This electronic trail of computer activity allows validation of the integrity and reliability of information, including actions performed in Enterprise Manager. To show internal control, you must be able to show who took what action when.

Infrastructure Security

Securing your Enterprise Manager deployment involves securing all layers of the stack starting with the underlying operating system (OS) on which the OMS and Repository reside all the way up to the Enterprise Manager components themselves. These recommendations will increase overall security as well as prevent certain DoS attacks.

Secure the Infrastructure and Operating System

Harden the machines themselves by removing all unsecure services such as rsh, rlogin, telnet, and rexec on Linux platform (for the list of unsecure services and how to remove them on different platforms, please refer to the CIS benchmarks). It is also recommended to stop non-essential services, this minimizes the 'attack footprint' of the host and reduces resource consumption by services that are not required, freeing up system resources to deliver the best performance from the OMS.

Restrict OS access by supporting only indirect or impersonation-based access to all Oracle Homes by using utilities such as sudo or PowerBroker. Protect the WebLogic Server Home directory, especially the domain directory which contains configuration files, security files, log files and other Java EE resources for the WebLogic domain. Grant only one OS user who runs WebLogic Server the access privilege to the directory.

Ensure that all the Oracle Homes are patched with the latest CPU (Critical Patch Update). This is a recommended best practice for securing the Oracle Management Service, Repository, Agents and managed Targets. Setup your My Oracle Support credentials to detect new Security Alerts and CPUs from the Patch Advisor. With the default Security Recommendations for Oracle Products compliance standard, when a Target is missing the latest Security patches, a compliance standard violation will be triggered. In addition, the Secure Configuration for Host should be associated to the hosts of the OMS and Repository. There are additional compliance standards for Database and WLS that can be applied depending on your level of security. Review *Oracle Enterprise Manager Cloud Control Security Guide* section on Compliance for more information on available compliance standards and how to associate Targets.

The OMS runs on top of the Oracle WebLogic Server. Most of the best practices for securing Oracle WebLogic Server are also applicable for securing the OMS. Refer to the *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server* section Securing Oracle WebLogic Server for additional information.

Ensure that the OMS, Repository and Agent are monitored for filesystem space. The OMS writes a lot of information to log and trace files, and proper space needs to be available for successful operation and troubleshooting. The Agent also relies on filesystem space for log and trace files as well as collecting Target metrics.

Best Practices for Securing the Infrastructure and Operating System

- Remove unsecure services and stop non-essential services on all infrastructure components
- Restrict OS access and protect critical files and directories
- Apply latest OS security patches
- Adhere to security Compliance Standards and apply latest Oracle CPU patches to all components (OMS, Repository and Agent)
- Monitor filesystem space for OMS, Repository and Agent

Securing the Oracle Management Repository

In addition to the above recommendations, steps are necessary to secure the Oracle Management Repository. Since the Oracle Management Repository resides within an Oracle database, a number of best practices for securing the Oracle database are also applicable to securing the Repository. For best practices on Oracle database security, please refer to the Oracle Database Security Checklist.

The above document also covers certain Operating System level steps that need to be performed to secure the database. Following are additional recommendations to be implemented in the Enterprise Manager deployment.

Enable Advanced Security Option

Enable Advanced Security Option (ASO) between the OMS and Repository to ensure that the data between the OMS and Repository is secure both from confidentiality and integrity standpoints. In addition to the ASO configuration required on the Repository database, you will need to configure the OMS and Agent to connect to a secure Repository database. The detailed instructions for implementing ASO for Enterprise Manager can be found in the *Oracle Enterprise Manager Cloud Control Security Guide.*

Please refer to the *Oracle Database Advanced Security Administrator's Guide* to obtain detailed information about ASO.

Audit SYS actions

Audit all SYS (schema) operations at the database level by setting AUDIT_SYS_OPERATIONS = TRUE.

Use the operating system syslog audit trail to minimize the risk that a privileged user, such as a database administrator, can modify or delete audit records stored in an operation system trail if the database version of Repository is 10gR2 or after.

- For 10gR2 DB, refer to the Auditing documentation to obtain more information about syslog audit trail.
- For 11g DB, set AUDIT_SYS_LEVEL initialization parameter appropriately to use syslog audit trail. Refer to the 11g documentation for details.

Restrict Network Access

Restrict network access to the host on which the Repository resides by putting the repository database behind a firewall and checking network IP addresses. The Listener should be configured to accept requests only from OMS nodes by adding the following parameters into TNS_ADMIN/protocol.ora file:

- tcp.validnode_checking =YES
- tcp.excluded_nodes = (list of IP addresses)
- tcp.invited_nodes = (list of IP addresses)(list all OMS nodes here)

The first parameter turns on the feature whereas the latter parameters respectively deny and allow specific client IP addresses from making connections to the Oracle listener. Please refer to the Secure the Network Connection section of the *Oracle Database Security Guide* for more information.

Securing User Accounts

Users should log in to the Enterprise Manager Console with their own individual accounts, and not use the SYSMAN user. SYSMAN is the schema owner and is more privileged than Enterprise Manager Super Administrators. Multiple users should be granted Super Administrator privilege to reduce the need for SYSMAN access. One strong reason for creating multiple Super Administrator accounts is to ensure one user maintains account access in case another user becomes locked out by a brute force attack. The Super Administrator privilege should be limited to users who truly need all the permissions that Super Administrator gives them.

In some cases, you may wish to prevent SYSMAN from logging into the console by executing the following SQL statement on the Repository database as the SYSMAN user:

```
UPDATE MGMT_CREATED_USERS
SET SYSTEM_USER='-1'
WHERE user_name='SYSMAN'
```

After disabling SYSMAN from logging into console, you can enable it by executing:

```
UPDATE MGMT_CREATED_USERS
SET SYSTEM_USER='1'
WHERE user_name='SYSMAN'
```

Use password profiles to enforce the password control of Enterprise Manager Administrators while Repository-based authentication is used. There is an out-of-box password profile MGMT_ADMIN_USER_PROFILE with the following parameter settings for Enterprise Manager Administrators:

- FAILED_LOGIN_ATTEMPTS=10

- PASSWORD_LIFE_TIME=180
- PASSWORD_REUSE_TIME=UNLIMITED
- PASSWORD_REUSE_MAX=UNLIMITED
- PASSWORD_LOCK_TIME=1
- PASSWORD_GRACE_TIME=7
- PASSWORD_VERIFY_FUNCTION=MGMT_PASS_VERIFY

The out-of-box password verification function MGMT_PASS_VERIFY will ensure that the password cannot be the same as username, its minimum length is 8, and it must have at least one alphabet, digit and punctuation character.

You can create customized password profiles with different values to meet your special requirements, for example, a new password verification function to meet a stricter password complexity requirement.

Change SYSMAN and MGMT_VIEW users' password on a regular basis using only the method documented in the *Oracle Enterprise Manager Cloud Control Security Guide*. The documented command(update_db_password()) helps you change the SYSMAN related passwords in the OMS and in the Repository database. If you do not execute this command properly, the OMS may fail to start due to inconsistent passwords for one of the many accounts. You will be prompted for the old and new SYSMAN passwords.

When changing the MGMT_VIEW password, you can select "-auto_generate" to generate a random password that no one will know. The MGMT_VIEW password is used only by the Reporting system and should not be used for login, therefore the auto_generate flag can ensure the password is not known.

To avoid the service interruption due to the lockout of internal users, SYSMAN and MGMT_VIEW users are associated with MGMT_INTERNAL_USER_PROFILE upon install. The password parameters are all set to UNLIMITED. In addition, to avoid sessions hanging or taking a long time due to resource consumption limit, MGMT_INTERNAL_USER_PROFILE's kernel parameters are set to default, which is unlimited as well.

Secure and Backup the Encryption Key

The Encryption Key is the master key that is used to encrypt/decrypt sensitive data, such as passwords and preferred credentials, stored in the Repository. The key itself is originally stored in the Repository and removed automatically once the installation is done. It only needs to be in the Repository during an upgrade. By storing the key separately from the Enterprise Manager schema, we ensure that the sensitive data such as Preferred Credentials remain inaccessible to the schema owner and other SYSDBA users (privileged users who can perform maintenance tasks on the database). Keeping the key outside of the Enterprise Manager schema will ensure that sensitive data remain inaccessible while Repository backups are accessed. Further, the Enterprise Manager schema owner (SYSMAN) should not have access to the OMS Oracle Homes to prevent reading or overwriting the emkey. See the *Oracle Enterprise Manager Cloud Control Security Guide* for more detailed information about Enterprise Manager's Cryptographic Support and the emkey. Follow the process outlined below to secure the encryption key.

Backup the encryption key to a file by running the following command and keep the encryption file on a separate machine securely, restrict access to only the OMS software owner. If the encryption key is lost or corrupted, the encrypted data in the repository is unusable.

```
$ emctl config emkey –copy_to_file_from_credstore –emkey_file emkey.ora
```

While the encryption key is required to be in the Repository for some operations such as Enterprise Manager patches and upgrades, if the operation does not automatically copy the emkey back to Repository (or remove it from the Repository afterwards), please copy it back to the Repository and after the operation remove it from the Repository by following the procedure below:

```
$ emctl config emkey –copy_to_repos
```

You will be prompted for SYSMAN password.

Remove the key from the Repository once the operation is done.

```
$ emctl config emkey –remove_from_repos
```

Best Practices for Securing the Oracle Management Repository

- Enable Advanced Security Option on the Repository database and configure OMS and Agent
- Restrict network access to known Targets
- Grant Super Administrator to selective administrators and do not login with SYSMAN account
- Enable strong password profiles and change application related account passwords regularly
- Secure and backup the encryption key

Securing the Oracle Management Agent

For better security during Agent installation, Agents should be deployed using Enterprise Manager's Agent Deploy Method which uses the secure SSH protocol. When manually deploying Agents, to protect against the possibility of users installing unauthorized Agents, use one-time registration passwords that have a reasonable expiry date instead of persistent registration passwords. Registration passwords can be created in the Console or by using the *emctl secure setpwd* command.   Install the Agent as a separate user from OMS installation and support only impersonation based access to this account such as sudo or PowerBroker post installation to prevent unauthorized changes.

Best Practices for Securing the Oracle Management Agent

- Utilize Enterprise Manager Agent Deployment method for Agent installations
- Use one-time registration passwords with expiry dates
- Install Agent as a separate user from OMS or Targets

Secure Communication

There are several ways to secure the communication between OMS and Agent, including firewalls, the OMS secure-lock feature, enabling TLSv1, enabling strong cipher suites and certificates. The following section looks at these in more detail.

Firewalls

Firewalls and Access Control Lists (ACLs) have become common in many organizations. Each component in Enterprise Manager has various protocols and ports that need to be opened for communication to succeed. Collaboration with the network and security administrators will be required to identify ports and protocols for access.

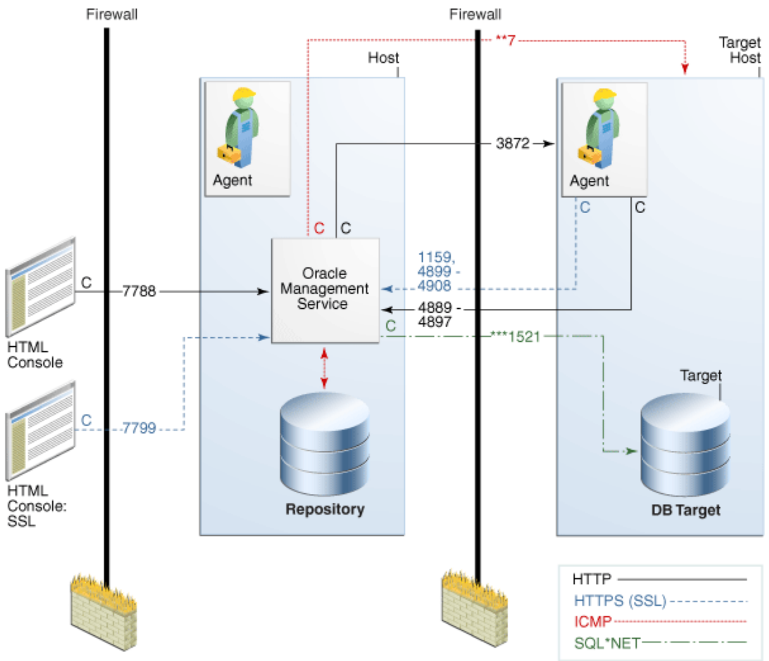


Figure 2. Out-of-the-Box Install network traffic protocols and default ports.

The default port assignments and usage are shown in the table below. Ports are system dependant and can be customized in each installation. This is just a reference of out-of-the-box installations. Additional components will add additional network interfaces and ports of their own.

TABLE 2. DEFAULT PORTS AND PROTOCOLS OF ENTERPRISE MANAGER

Default Port	*Protocol*	*Use*
3872	*HTTP*	*Oracle Management Service to Agent*
4889-4897	*HTTP*	*Agent to Oracle Management Service, used only to secure if running in Secure mode*
1159, 4899-4908	*HTTPS (SSL)*	*Agent to Oracle Management Service used for upload when in Secure*

		mode
7788	*HTTP*	*HTTP Console to Oracle Management Service from any client browser machine*
7799	*HTTPS (SSL)*	*HTTPS Console to Oracle Management Service from any client browser machine*
*1521 ****	*SQL*Net*	*Oracle Management Service to Database Listeners (depends on what port Listeners are configured for), used for Administration and Real-Time connections.*
*1521 ****	*SQL*Net*	*Oracle Management Service to Oracle Management Repository*
7	*ICMP*	*Oracle Management Service to Target Host to validate host status if Agent fails to upload for a preconfigured amount of time*

Enable ICMP

Enterprise Manager uses the industry-standard Internet Control Message Protocol (ICMP) echo request to check status of Target host machines if the Agent has not uploaded or responded in a timely fashion or at expected intervals. If ICMP is disabled, the Target will appear to be down. Firewall should be configured to allow ICMP to prevent false down Target alerts.

ICMP and User Datagram Protocol (UDP) are also used to transfer data between Beacon Targets that allow an Agent to monitor services and the network components you are monitoring. A Beacon is a target that allows the Management Agent to remotely monitor services. A Beacon can monitor one or more services at any point in time.

If there is a firewall or ACL between the web application components and the Beacons you use to monitor those components, you must configure it to allow ICMP, UDP, and HTTP traffic.

Configure Oracle Management Agent for Firewalls

When the host where the Agent resides is protected by a firewall, you need to configure the Agent to use a proxy, or configure the firewall to allow incoming communication from the OMS. To configure the firewall you must determine the port assigned to the Agent and whether communication is HTTP or HTTPS. You can find this information by running *emctl status agent*.

To configure the proxy set the following properties using the Enterprise Manager Console to edit the Agent properties or *emctl setproperty agent* and restart the Agent. The proxy realm, user and password may not be required in all environments.

```
$ emctl setproperty agent -name REPOSITORY_PROXYHOST -value proxy42.acme.com
$ emctl setproperty agent -name REPOSITORY_PROXYPORT -value 80
$ emctl setproperty agent -name REPOSITORY_PROXYREALM –value <value if needed>
$ emctl setproperty agent -name REPOSITORY_PROXYUSER –value <value if needed>
$ emctl setproperty agent -name REPOSITORY_PROXYPWD –value <value if needed>
```

Configure Oracle Management Service for Firewalls

In cases where the Oracle Management Service is behind a firewall, configurations will be needed to allow proxy communications to the Agents or incoming communication through the firewall.

If the Agents that are behind the firewall are in different domains, you can configure the proxy to allow communication for those Agents and use the dontProxyFor parameter to identify the Agents within the firewall. To configure the proxy on the Management Service set the following properties using *emctl set property*. The proxy realm, user and password may not be required in all environments.

```
$ emctl set property -name REPOSITORY_PROXYHOST -value proxy42.acme.com
$ emctl set property -name proxyPort –value 80
$ emctl set property -name dontProxyFor –value “.acme.com, .acme.us.com”
```

To configure the firewall to allow inbound communication from the Agents for metric uploads, the firewall must be configured to accept HTTP/HTTPS traffic on the upload ports. The default ports are 4889 (HTTP) and 1159 (HTTPS). If your ports were customized you'll need to use those ports.

If there is a firewall between your browser and the Enterprise Manager Console, you must configure firewall to allow the console to receive HTTP/HTTPS traffic over port 7788/7799 (defaults). You can validate your port by looking at the URL you access the Console with.

```
https://mgmthost.acme.com:7799/em
```

Additional component installations such as JVMD, APD and BI have additional port requirements. For example, if BI Publisher is installed additional ports may be needed for access to the reporting console. Default ports are 9702/9703 (HTTP/HTTPS). For more information please see the documentation specific to the component.

To manage the database Targets that are configured behind firewalls, you must allow Oracle Net traffic on the listener ports (typically 1521 but often customized). For more information regarding configuring Oracle Databases for firewalls see the *Oracle Database 2 Day + Security Guide.*

Secure and Lock the OMS and Agents

The Oracle Management Service and Oracle Management Agents can run in non-secure (HTTP) or secure (HTTPS) modes. The recommendation is to always use secure mode, hence the default installation will automatically secure-lock the OMS. The secure-lock mode takes security one step further in requiring that Agents communicate only through HTTPS port (HTTP port is locked). This ensures that the OMS-Agent communication is always encrypted and mutually authenticated. All requests from un-secure Agents are rejected by the OMS. Similarly, any un-secure request from the OMS is rejected by the Agent. This helps safe-guard the management system from any malicious 'man-in-the-middle' attack happening from within the infrastructure.

If your installation was done before Oracle Enterprise Manager 10g Release 5, you may be required to secure-lock your OMS manually. In the case of upgrades, if the pre-upgrade environment is secured, the upgrade retains the secure mode but does not secure-lock the OMS. If the pre-upgrade environment is already secure-locked, the upgrade retains the secure-lock mode between OMS and Agent.

To check the secure status of the OMS and secure-lock the communication between OMS and Agent run the command and restart the OMS:

```
$ emctl status oms -details
Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.3.0
Copyright (c) 1996, 2011 Oracle Corporation.  All rights reserved.
Enter Enterprise Manager Root (SYSMAN) Password :
Console Server Host : mgmthost.acme.com
HTTP Console Port   : 7790
```

```
HTTPS Console Port  : 7803
HTTP Upload Port    : 4890
HTTPS Upload Port   : 4904
OMS is not configured with SLB or virtual hostname
Agent Upload is locked.
OMS Console is locked.
Active CA ID: 1
Console URL: https://mgmthost.acme.com:7803/em
Upload URL: https://mgmthost.acme.com:4904/empbs/upload
…
```

```
$ emctl secure lock -upload
Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.3.0
Copyright (c) 1996, 2011 Oracle Corporation.  All rights reserved.
Enter Enterprise Manager Root (SYSMAN) Password :
Agent Upload is locked. Agents must be secure and upload over HTTPS port.
Restart OMS.
```

Note that once OMSs are running in secure-lock mode, unsecure Agents will not able to upload any data to the OMSs. To check the status and secure the Agent issue the following, you will be prompted for the registration password:

```
$ emctl status agent -secure
Oracle Enterprise Manager 12c Cloud Control 12.1.0.3.0
Copyright (c) 1996, 2011 Oracle Corporation.  All rights reserved.
Checking the security status of the Agent at location set in
/scratch/cllamas/oracle/em12/agent/agent_inst/sysman/config/emd.properties...  Done.
Agent is secure at HTTPS Port 3872.
Checking the security status of the OMS at
https://mgmthost.acme.com:4904/empbs/upload/...  Done.
OMS is secure on HTTPS Port 4904
```

```
$ emctl secure agent
Oracle Enterprise Manager 12c Cloud Control 12.1.0.3.0
Copyright (c) 1996, 2011 Oracle Corporation.  All rights reserved.
Agent successfully stopped...   Done.
Securing agent...   Started.
Enter Agent Registration Password :
Agent successfully restarted...   Done.
EMD gensudoprops completed successfully
Securing agent...   Successful.
```

To ensure the console access from the client browser is secure over SSL/TSL, the console must be locked as well. From Oracle Enterprise Manager 10g Release 5 installations are secure-locked by default. In the case of upgrades, if the pre-upgrade environment is not secure-locked, after the upgrade you need to run the following command to secure-lock the console access:

```
$ emctl secure lock -console
```

Configure TLSv1 Protocol

It is recommended to configure OMS and Agents to support only TLS v1 protocol, which is the successor of SSL v3, for the communication.   By default the OMS is configured in mixed-mode, accepting both SSLv3 and TLSv1 protocols.

To configure OMS for TLS v1 protocol only:

```
$ emctl stop oms
```

```
$ emctl secure oms -protocol TLSv1
```

Append the following to the JAVA_OPTIONS in Domain_Home/bin/startEMServer.sh. If this property already exists, update the value to TLS1

```
-Dweblogic.security.SSL.protocolVersion=TLS1
```

```
$ emctl start oms
```

To configure an Agent to support only TLS v1 protocol while the Agent listens as a server, edit the Agent properties in the Enterprise Manager Console or use emctl setproperty at the command line. To edit multiple Agents at a time, go to Setup -> Agents, select the Agents you want to modify, click Properties. This will create a job and you can specify the Agent property changes on the Parameters page that will get applied to all selected Agents. To use the command line, issue the following:

```
$ emctl setproperty agent -name allowTLSOnly -value true
```

Enable Strong Cipher Suites

A cipher suite is a combination of cryptographic parameters that define the security algorithms and key sizes used for authentication, key agreement, encryption, and integrity protection. Cipher suites protect the integrity of a communication. For example, the cipher suite called `RSA_WITH_RC4_128_MD5` uses RSA for key exchange, RC4 with a 128-bit key for bulk encryption, and MD5 for message digest. Enterprise Manager allows strong cipher suites for the communication between OMS and Agent. By default, the following cipher suites will be allowed for the communication on the Agent:

- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA

To see the current Cipher Suites enabled view the Agent properties in the Enterprise Manager Console or run:

```
$ emctl getproperty agent -name SSLCipherSuites
Oracle Enterprise Manager 12c Release 1 12.1.0.3.0
Copyright (c) 1996, 2011 Oracle Corporation.  All rights reserved.
SSLCipherSuites is unset; default value is
SSL_RSA_WITH_RC4_128_MD5:SSL_RSA_WITH_RC4_128_SHA:SSL_RSA_WITH_3DES_EDE_CBC_SHA:SSL_RSA
_WITH_DES_CBC_SHA:SSL_RSA_EXPORT_WITH_RC4_40_MD5:SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
```

To configure the strong cipher suites to be used for Agent SSL/TLS communication edit the Agent properties in the Enterprise Manager Console or use the setproperty command:

```
$ emctl setproperty agent -name SSLCipherSuites -value <values>
```

The following are supported strong cipher suites:

- SSL_RSA_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_AES_256_CBC_SHA
- SSL_DH_anon_WITH_3DEC_EDE_CBC_SHA
- SSL_DH_anon_WITH_RC4_128_MD5
- SSL_DH_anon_WITH_DES_CBC_SHA
- SSL_RSA_WITH_RC4_128_MD5

- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA

To restrict the strong cipher suites used by OMS, please edit SSLCipherSuite parameter in $INSTANCE_HOME/WebTierIH1/config/OHS/ohs1/httpd_em.conf and ssl.conf files with the appropriate values. Here are the default values:

- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

Third Party Certificates

Use a certificate from well-known Certificate Authority (CA) to secure OMS-Agent communication and console access to take advantage of the well-known trusted certificates with different expiry and key size. Please refer to the section Configuring Secure Communications in *Oracle Enterprise Manager Cloud Control Security Guide* for detailed information.

Oracle has introduced the concept of a wallet, which is a password-protected container used to store authentication and signing credentials, including private keys, certificates, and trusted certificates needed by SSL.

To secure the console using a custom certificate authority, you need to create a wallet location and secure the console against that wallet location. For more information on creating a wallet, see *Oracle Fusion Middleware Administrator's Guide.*

Best Practices for Securing Communication

- Enable ICMP for ping check validation
- Configure firewalls as appropriate in your environment
- Secure and lock the OMS and Agents
- Configure strong cipher suites for the OMS and Agent
- Secure upload and console virtual HTTPS hosts with third party certificates

Operational Security

Authentication

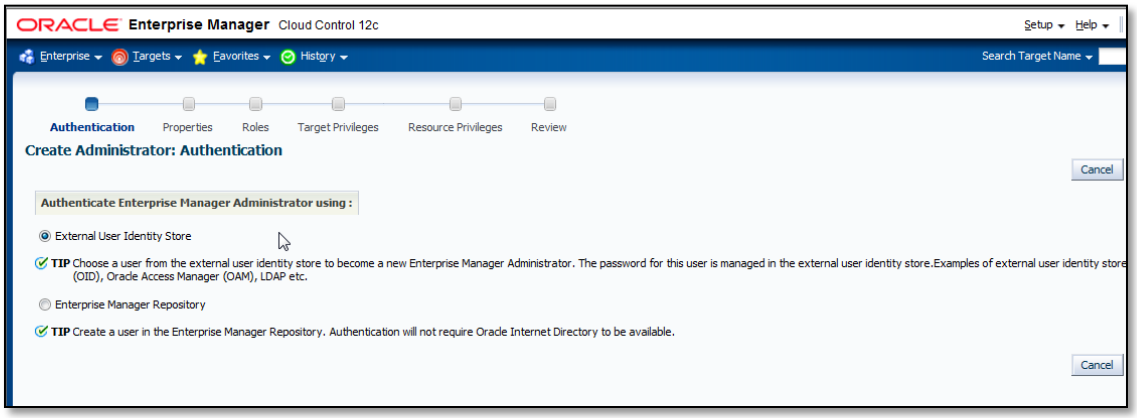
Enterprise Manager offers multiple methods of authentication. In addition to the predefined methods, a customized provider/module can be plugged in to Enterprise Manager. The default system authentication method is the standard Repository based authentication. Additional predefined methods include:

- Oracle Single Sign-On (OSSO)
- Enterprise User Security (EUS)
- Integration with Oracle Access Manager Single Sign-On (OAM SSO)

- Direct LDAP integration (Oracle Internet Directory, Microsoft Active Directory)

Please refer to the Authentication section in the *Oracle Enterprise Manager Cloud Control Security Guide* for detailed information about how to configure Enterprise Manager to use the pre-defined providers.

Using one of the extended authentication modules enables you to take advantage of centralized identity management across the enterprise. Doing this allows you to rely on the external identity management system for password security compliance, password changes and resets. During creation of every new user in Enterprise Manager you are prompted for that users mode of Authentication, via an external Identity store such as Oracle Access Manager(OAM), LDAP or Oracle Internet Directory(OID), or internally via Enterprise Manager Repository. Figure 3. Shows the default window which pops up, during user creation.



Create Administrator: Authentication

Authenticate Enterprise Manager Administrator using :

● External User Identity Store

✓ TIP Choose a user from the external user identity store to become a new Enterprise Manager Administrator. The password for this user is managed in the external user identity store.Examples of external user identity store (OID), Oracle Access Manager (OAM), LDAP etc.

○ Enterprise Manager Repository

✓ TIP Create a user in the Enterprise Manager Repository. Authentication will not require Oracle Internet Directory to be available.

Figure 3. Enterprise Manager New User Authentication

When using external Authentication, Enterprise Manager allows the creation of external roles which map to the identity management systems groups by name (i.e. Enterprise Manager role “DBA” maps to LDAP group “DBA”). Thus allowing synchronized user access and privileges based on external group membership.

Target authentication provides access to the host, database or application Targets managed through Enterprise Manager. Using strong Target authentication methods, named credentials and configuring database password profiles are a few ways to ensure secure Target authentication.

To ensure Target authentication security, choose strong host and database authentication methods. Credentials for Target access are encrypted and stored in Enterprise Manager. With Enterprise Manager, strong authentication such as SSH-keys for host and Kerberos tickets for database are now supported. These credentials can be used by jobs, deployment procedures and other subsystems.

Best Practices for Authentication

- Integrate with corporate identity management system for enterprise wide authentication
- Use external roles to automatically assign privileges to users based on external group membership

- Automate user creation/deletion based on external group membership using EM CLI
- Utilize strong authentication methods (SSH for host, Kerberos for database).

Privilege and Role Management

Enterprise Manager comes with several out-of-the-box roles that provide role based authentication for various operational roles. Segregation of Operator, Designer and Administrator functions for Patching, Provisioning, Cloud, Compliance, and Plug-ins allow more granular authentication for users. Use the Create Like feature to further enhance or restrict as required for your operations. With using Role Based Access Control (RBAC), privilege management becomes easier; managing role grants is simpler than managing privilege grants. For a complete list of the out-of-the-box roles see the Privileges and Roles section of *Oracle Enterprise Manager Cloud Control Security Guide*.

With Enterprise Manager we have the ability to specify Target privileges and resource privileges.

Target privileges allow an administrator to perform operations on a Target. Some of the new Target privileges include Connect to any Viewable Target, Execute Command Anywhere, Execute Command as any Agent and more. The Target privileges can be assigned for all Targets or for specific Targets.

Resource privileges grant access to a function, button or page within Enterprise Manager. Some of the new resource privileges include Backup Configurations, Cloud Policy, Compliance Framework, Enterprise Manager Plug-in, Job System, Patch Plan, Self Update and Template Collection. For a complete list refer to the Privileges and Roles section of *Oracle Enterprise Manager Cloud Control Security Guide*.

With these new privileges, it's much easier to implement the Principal of Least Privilege by creating specific roles with very fine grained privileges assigned that match the job duties.

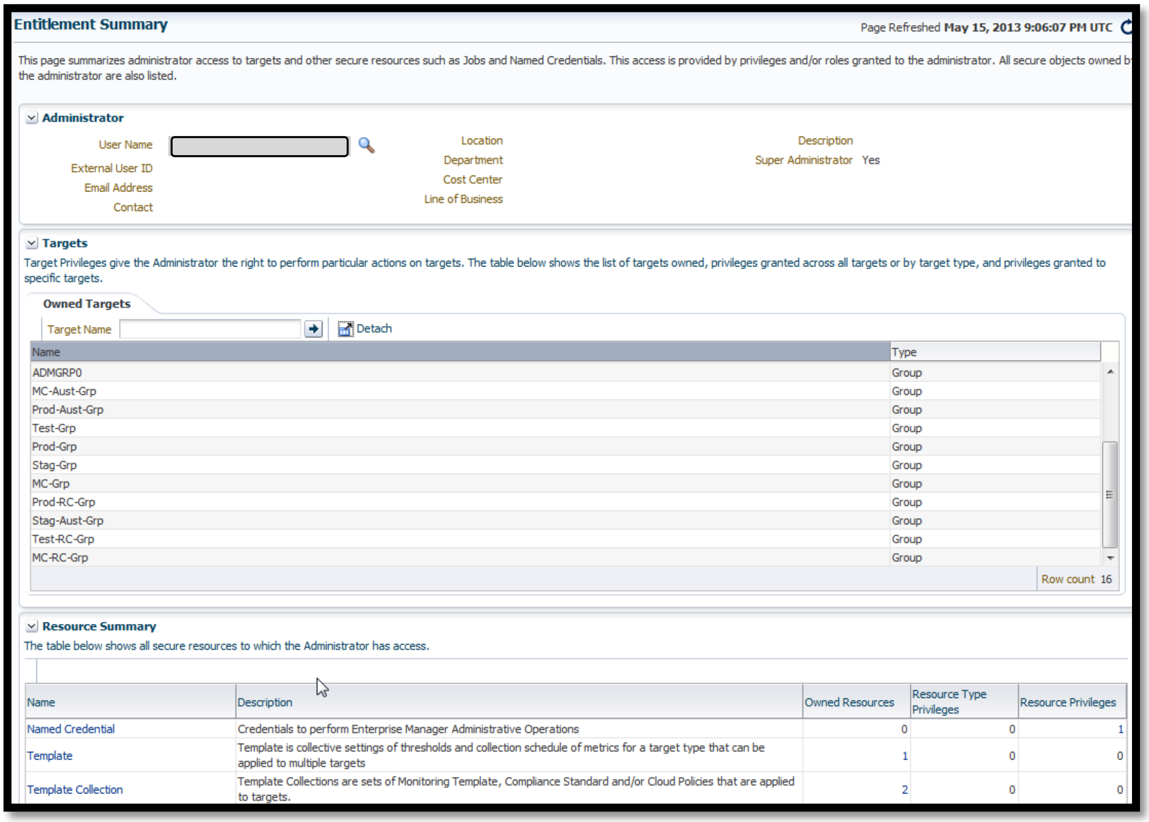
Other key privilege related to auditable actions are listed here:

- Grant job privilege
- Grant privilege
- Grant role
- Grant Target privilege
- Grant system privilege
- Revoke job privilege
- Revoke privilege
- Revoke role
- Revoke Target privilege
- Revoke system privilege

Super Administrators have FULL privileges on Targets/reports/templates/jobs. These are the only users who can create other users and Super Administrators, and grant/revoke privileges to/from other users. Super user privilege should be granted with caution. Using the following query to get the list of super users:

```
SELECT grantee FROM MGMT_PRIV_GRANTS WHERE PRIV_NAME = 'SUPER_USER'
```

The Administrators Entitlement page displays all the privileges and roles granted to that Administrator. This page also summarizes an Administrators access to targets as well as displaying the named credentials and secure resources owned by that Administrator. Figure.4 shows an example of the Enterprise Manager Administrator Entitlement page. You can access this page by clicking on the dropdown menu, beside the Administrators name, and clicking Entitlement Summary.



Entitlement Summary

Page Refreshed **May 15, 2013 9:06:07 PM UTC**

This page summarizes administrator access to targets and other secure resources such as Jobs and Named Credentials. This access is provided by privileges and/or roles granted to the administrator. All secure objects owned b the administrator are also listed.

Administrator

User Name		Location		Description	
External User ID		Department		Super Administrator	Yes
Email Address		Cost Center			
Contact		Line of Business			

Targets

Target Privileges give the Administrator the right to perform particular actions on targets. The table below shows the list of targets owned, privileges granted across all targets or by target type, and privileges granted to specific targets.

Owned Targets

Name	Type
ADMGRP0	Group
MC-Aust-Grp	Group
Prod-Aust-Grp	Group
Test-Grp	Group
Prod-Grp	Group
Stag-Grp	Group
MC-Grp	Group
Prod-RC-Grp	Group
Stag-Aust-Grp	Group
Test-RC-Grp	Group
MC-RC-Grp	Group

Row count 16

Resource Summary

The table below shows all secure resources to which the Administrator has access.

Name	Description	Owned Resources	Resource Type Privileges	Resource Privileges
Named Credential	Credentials to perform Enterprise Manager Administrative Operations	0	0	1
Template	Template is collective settings of thresholds and collection schedule of metrics for a target type that can be applied to multiple targets	1	0	0
Template Collection	Template Collections are sets of Monitoring Template, Compliance Standard and/or Cloud Policies that are applied to targets.	2	0	0

Figure 4. Enterprise Manager New Administrators Entitlement Page

Best Practices for Privilege and Role Management

- Create meaningful roles and grant roles to users instead of granting privileges to users.
- Grant only the minimum set of privileges a user needs for carrying out his/her responsibilities by granting the fine-grained privileges/roles only when needed.
- Audit privilege and role actions for complete monitoring and accountability.
- Limit the number of Super Administrators

Credentials

Preferred Credentials simplify access to managed Targets by storing Target login credentials in the Management Repository. Users can access an Enterprise Manager Target that recognizes those credentials without being prompted to log into the Target. Preferred credentials are set on a per user basis, thus ensuring the security of the managed enterprise environment. Default credentials can be set for a particular Target type as well as Target credentials for a particular Target. The Target credentials override the default credentials.

Do not set preferred credentials for group/common accounts such as SYSMAN. If preferred credentials are set for common accounts, then the accountability of the use of these credentials is lost. The following SQL statements can be used to report the list of users who have the preferred credentials set:

```
SELECT t.target_name,tc.user_name,tc.credential_set_name
FROM MGMT_TARGET_CREDENTIALS tc, MGMT_TARGETS t
WHERE tc.target_guid=t.target_guid
```

```
SELECT t.target_name,tc.user_name, tc.set_name
FROM EM_TARGET_CREDS tc, MGMT_TARGETS t
WHERE tc.target_guid=t.target_guid and tc.user_name = 'SYSMAN'
```

Credentials can be stored as Named Credentials and then privileges granted to other users to use, update or own the credentials. These credentials can be used for jobs, patching or other administration tasks on specific Targets or globally. Eligible credential types include username/password, SSH-key for host and Kerberos for database. This method allows administrators to configure Named Credentials for privileged access and grant to specific users. Auditing tracks Named Credential creation, modification and usage.

Named Credentials provide a secure mechanism in Enterprise Manager to allow for separation of privilege management from privilege delegation for Targets. Using Named Credentials an organization can separate the management of the specific username/password/authentication details from the actual authority to use these credentials. This is an essential tool in modern, secure organizations where there needs to be certainty that a malicious user cannot conduct operations outside Enterprise Manager using a set of known credentials. Additionally, the management of a central set of Named Credentials removes a significant burden on the proliferation of credentials information across many Enterprise Manager Administrators and also therefore reduces the likelihood of these being used outside the Enterprise Manager environment or helps prevent against the accidental publication of credentials.

Best Practices for Credentials

- Use EM CLI to automate routine password changes on privileged named credentials, this allows one administrator to know and update the password for granted users.
- Utilize named credentials when setting preferred credentials to simplify credential management.
- Do not set preferred credentials for group/common accounts such as SYSMAN.

Groups and Systems

Using groups and systems to organize your Targets helps reduce security administration overhead. There are two types of groups available in Enterprise Manager that help simplify privilege management and authorization. By granting roles to groups, instead of users and using privilege propagating groups, you can reduce the direct grants and ensure users have access to the Targets as needed.

Privilege Propagating Groups simplify the privilege assignment, revocation, and administration along with group management by propagating the assigned privileges to all members of the group.   For example, a user can be granted access to a privilege propagating group Sales, and they in turn receive access to all Targets within that group.

Administration Groups are privilege propagating groups that automate the application of monitoring settings to Targets upon joining the group. Targets cannot be assigned directly to the group, rather they are automatically added based on membership criteria.

Systems are also privilege propagating and allow you to group all related Targets of a particular application or function into a system.

Best Practices for Groups and Systems

- Create meaningful roles and grant roles to users instead of granting privileges to users.
- Grant only the minimum set of privileges a user needs for carrying out his/her responsibilities by granting the fine-grained privileges/roles only when needed.
- Utilize privilege propagating groups and systems to reduce administration overhead

Audit

Enterprise Manager has additional auditing that is available for purposes of tracking and validating actions performed in Enterprise Manager, including jobs and credentials accessed. Basic and Infrastructure auditing is enabled by default for Enterprise Manager.

In Enterprise Manager, there are over 150 options for auditing.

An enhanced Auditing page makes it easy to quickly view the privilege grants on a regular basis and also keep track of which users exercised what privileges, this improves user accountability. Infrastructure activities are audited out of the box, these include updates, downloads, OMS password changes and EM key copy and removes from the Repository.

For a list of all auditing commands, please use the following EM CLI command:

```
$ ./emcli show_operations_list
Operation ID                       Operation Name              Infrastructure Operation
ADD_AGENT_REGISTRATION_PASSWORD    Add Registration Password        NO
ADD_CS_TARGET_ASSOC                Add Standard-Target Association  NO
AGENT_REGISTRATION_PASSWORD_USAGE  Registration Password Usage      NO
AGENT_RESYNC                       Resync Agent                     NO
AG_AUD_CREATE                      Create Administration Groups     NO
AG_AUD_DELETE                      Delete Administration Groups     NO
AG_AUD_MODIFY                      Modify Administration Groups     NO
APPLY_TEMPLATE                     Apply Monitoring Template        NO
APPLY_UPDATE                       Apply Update                     YES
```

```
ATTACH_MEXT                     Attach Metric Extension         NO
```

… [Please refer to section Setting up for Auditing System for Enterprise Manager of the *Oracle Enterprise Manager Cloud Control Security Guide* for the complete list]

To show current OMS audit information, please use the following EM CLI command:

```
 $ ./emcli show_audit_settings
User Activity Audit    : Enabled  (For all Operations)
Externalization Switch : Disabled
Directory              : Not configured
File Prefix            : em_audit
File Size              : 5000000 Bytes
Data Retention Period  : 365 Days
*Infrastructure Audit is always enabled
```

To enable audit for a subset of audited operations, please use the following EM CLI verb:

```
$ emcli update_audit_settings -audit_switch="ENABLE/DISABLE"  -
operations_to_enable="name of the operations to enable,for all operations use ALL" -
operations_to_disable="name of the operations to disable, for all operations use ALL"
```

For example to audit only logon/logoff you would issue:

```
$./emcli update_audit_settings -audit_switch="ENABLE" -
operations_to_enable="LOGIN;LOGOUT"
Successfully updated the audit settings.
```

Please refer to section Setting up for Auditing System for Enterprise Manager of the *Oracle Enterprise Manager Cloud Control Security Guide* for the list of operations that are audited by Enterprise Manager.

Once audit is enabled, the audit records are kept in MGMT$AUDIT_LOG view in the Repository. Use Enterprise Manager Console to monitor the audit data as user with Super Administrator, click Setup -> Security -> Audit Data.

The externalization service via EM CLI verb update_audit_settings externalizes the audit data from the Repository to an external file system on a regular basis. Make sure there is enough space in the directory for the audit log files.

```
$ emcli update_audit_settings -file_prefix=<file_prefix> -
directory_name=<directory_name> -file_size = <file size> -data_retention_period=<period
in days>
```

The following example shows that the audit data will be retained in the Repository for 14 days and once exported the data will be stored in the OS directory that corresponds to database directory AUDIT with filenames prefixed with gc12_audit, and the file size will be 50M bytes each:

```
$ emcli update_audit_settings -externalization_switch=ENABLE  -file_prefix=gc12_audit -
directory=AUDIT -file_size=50000000 -data_retention_period=14
```

Achieve separation of duties by restricting the access to the directory where the externalized audit data is stored. No Enterprise Manager users should have access to the externalized audit data.

Best Practices for Auditing

- Formalize the audit process by setting up an Audit Review schedule or integrating with an Audit tool such as Audit Vault for notifications and alerts.
- Externalize the audit service and secure the files created

Conclusion

It is difficult to overstate the importance of security. This is particularly true for Enterprise Manager given its broad footprint in the data center. Oracle Enterprise Manager Cloud Control 12*c* provides a robust set of security features and capabilities starting with secure framework level communication to a secure user model. Wherever possible, we attempt to incorporate best practices learned in the field into the product itself while balancing ultimate security and usability. The rich set of Target security policies shipped out-of-box are an example of this effort. The best practices in this document are designed to enable users to sacrifice some convenience in order to further secure their Enterprise Manager deployments to meet corporate standards.

Referenced Links

Oracle Database Advanced Security Administrator's Guide
Oracle Database Security Guide
Oracle Database Security Checklist
Oracle Database 2 Day + Security Guide
Oracle Enterprise Manager Cloud Control Administrator's Guide
Oracle Fusion Middleware Administrator's Guide
Oracle Fusion Middleware Securing Oracle WebLogic Server
Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server
Oracle Enterprise Manager Cloud Control Security Guide

Oracle is committed to developing practices and products that help protect the environment

Oracle Enterprise Manager Cloud Control 12*c* Infrastructure and Operational Security Best Practices
June, 2013
Author: Oracle
Contributing Authors: Courtney Llamas, Werner De Gruyter, Andrew Bulloch, Ravi Pinnamaneni

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Hardware and Software, Engineered to Work Together