Raising the Ante on Security with Oracle Enterprise Manager

Angeline Janet Dhanarani
Senior Product Manager
Oracle Enterprise Manager
October 29, 2015

Joe Kopilash
Architect and Director
Database Administration
EPSILON
Total Cloud Control

Superior Enterprise-Grade Management

Integrated Cloud Stack Management

Complete Cloud Lifecycle Management

Scalable, Secure | Optimized, Efficient | Agile, Automated
Next Release Builds on a Solid Foundation

Superior Enterprise-Grade Management

Integrated Cloud Stack Management

Complete Cloud Lifecycle Management

NEW: Continuous Monitoring

NEW: Infrastructure Management

NEW: Improved Hybrid Cloud Management

Scalable, Secure | Optimized, Efficient | Agile, Automated
Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Program Agenda

1. Security Framework Overview
2. Infrastructure Security
3. Operational Security
Enterprise Manager : Security Framework Overview

- **Infrastructure Security**
- **Operational Security**

Secure Communication

Enterprise Manager Authentication

Target Authentication

Enterprise Manager Authorization

Administrators

Oracle Management Repository

Targets

Agent

Database

Agent

Application Server

Agent

Applications

Oracle Management Service

Console

EMCLI

Backup/Recovery Jobs, SQL Script Jobs, Monitoring Templates, Provisioning and Patching, etc
Program Agenda with Highlight

1. Security Framework Overview
2. Infrastructure Security
3. Operational Security
Infrastructure Security

Common Questions

- Secured Communication using Third party CA certificates
- Secured Communication over Corporate Firewall
- Secured Communication on TLS Protocol
Infrastructure Security
Secure protocol for communication

Can Enterprise Manager components be configured to accept only TLS?
TLS protocol is supported

• EM 12c: Follow MOS Note: 1938799.1 to configure EM12c to accept only TLS

• EM 13c: TLS enabled out-of-box

  • OMS → 13c Agent
  • 13c Agent → 13c Agent
  • EMCLI → OMS
  • 13c Agent → FMW Targets
  • OMS → FMW Targets
  • Browser → Console
  • OMS → Server Load Balancer
  • 13c Agent → DB Targets
  • OMS → DB Targets

• OMS can be restricted to any specific version

  • emctl secure oms -protocol TLSv1.2
Infrastructure Security

Working with corporate firewalls

What network flows and port directions do I need to configure on the firewall to enable secure communication between Enterprise Manager Components?
Default Ports with direction that need to be opened in the Firewall

- Cloud control console HTTPS Port (7799)
- Admin Server Console HTTPS Port (7101)
- Weblogic Node Manager HTTPS Port (7401)
- BIP Reports Console HTTPS Port (9801)
- Management Repository Database SQL * Net Port (1521)
- Management Agent HTTPS Port (3872)
- Enterprise Manager Upload HTTPS Port (1159, 4899)
- Host Status ICMP (0) Echo reply, ICMP (8) Echo Request
- Target Database SQL *Net Port (1521)
- Secure Admin SSH 22
Infrastructure Security
Certificates for encryption

I configured communications using Oracle-provided certificates. Is this secure?
Communication secure only with Third party CA certificates

• Oracle-provided self-signed certificates are not secure enough
• For truly secure environment
  • **DO NOT**
    • Use the Self-signed certificates of Enterprise Manager
    • Use the default WebLogic Server demonstration certificates
  • **DO**
    • Get your own third party CA certificate
• Popular Browsers have restricted access to use self-signed certificates

• Configure Third party CA certificates for:
  • Console to OMS
  • Agent to OMS
  • OMS to Agent
  • OMS to target database
Configuring Third party CA certificates

**Configuring OMS**
- Create a wallet and import third party certificates into it.
- Secure the **HTTPS Console access**
  - `emctl secure console -wallet`
- Secure the **HTTPS Upload access**
  - Copy certificates to trust store and repository using **“emctl secure oms -trust_certs_loc”**
  - Secure all agents with **“emctl secure agent”**
  - Import certificates into OMS using **“emctl secure oms –wallet -trust_certs_loc”**

**Configuring WebLogic Server components**
- SSL certificates to be generated with the physical host name of the OMS machine and not the SLB host name.
- Import CA certificates into the trust store of the Agent which is monitoring the OMS with **“emctl secure add_trust_cert_to_jks -trust_certs_loc”**
- **Configure OMS and WLS using “emctl secure wls -wallet”**

**Configuring Agents**
- Copy the cwallet.sso file to `<AGENT_INST>/sysman/config/server` directory.
- If the OMS SSL certificate has been signed by different CA than Agent, import the root certificates of Agent’s new SSL certificate to the OMS trust store using **“emctl secure oms –wallet -trust_certs_loc”**

Refer Security Guide for samples and details
Configuring secured access to Target Databases

- **Configure TCPS connection protocol for monitoring target databases securely**
  - Enables data transport encryption via TCPS (Default: TLS 1.0)
    - between OMS and database server target
    - between Agent and database server target

- **Configuration Steps**
  - Enable Oracle Advanced Security TLS setting on the target database
  - Configure Secure wallets with third party CA certificates
  - Configure wallets for OMS and Agent communication
    - Refer Appendix for configuration
  - Set the connection protocol to TCPS in the monitoring configuration properties of target database
Infrastructure Security

Securing access to Repository

What are the best practices to secure access to the Enterprise Manager Repository
Secured Access to Enterprise Manager Repository

• Secure and backup the Encryption Key
  – Encryption Key: Used by OMS to access sensitive data (e.g., Target credentials) in repository
  – After any Enterprise Manager upgrade/patching,
    • Ensure encryption key is removed from repository using `emctl status emkey`
    • If present, secure the encryption key using `emctl config emkey -remove_from_repos`
  – Backup the encryption key to a file, restrict access to only the OMS software owner
    • `emctl config emkey -copy_to_file_from_credstore -emkey_file emkey.ora`

• DO NOT use SYSMAN
  – Only the OMS should be using SYSMAN to access the repository
  – Grant Super Administrator privilege to selective administrators accounts
  – Disable SYSMAN from logging into Enterprise Manager Console
    • Use new EMCLI verb `emcli lock_user_account -name=SYSMAN`
Program Agenda with Highlight

1. Security Framework Overview
2. Infrastructure Security
3. Operational Security
Operational Security
Common Questions

Target Authentication is the process of enabling access to target

Authentication is the process of determining the validity of a user

Authorization is the action of determining who has access to do what.
Enterprise Manager Authentication

Corporate LDAP Server

How can I configure Enterprise Manager to work with our corporate LDAP server?
Working with Corporate LDAP Servers

• **Step1:** Configure underlying WebLogic Server to work with the LDAP server
  - OMS delegates user authentication to WebLogic Server (in OMS Stack) for external authentication

• IF LDAP Server is Microsoft Active Directory / Oracle Internet Directory / Oracle Access Manager
  - Native Support with One-step configuration `emctl config auth`

• IF any other external authentication providers
  - Manually configure with the out-of-box WebLogic Security Provider OR
  - Create and configure Custom Security providers through WebLogic service provider interface (APIs)
Simplify User and Role administration for LDAP Users

**Step 2:** Configure External Roles
- Auto-assigns Enterprise Manager roles to users based on LDAP group membership
  - Define Enterprise Manager Role and mark it “External”
  - `<Enterprise Manager external role name>` = `<LDAP_group_name>`

**Step 3:** Enable auto provisioning
- Automate the provisioning of Enterprise Manager user-accounts upon first login
  - Set OMS property `oracle.sysman.core.security.auth.autopropvisioning = true`
  - Apply auto-provisioning to all users or restrict to a particular LDAP group

**Benefit:** Simply administration with External Roles and auto provisioning
- Auto-creates Enterprise Manager user accounts
- Provides Enterprise Manager users with defined privileges on first login
Enterprise Manager Authorization
Differentiate access to database target

How do I give application developers read-only access to view the performance management report for a production database target?
Different personas of database users

• **Application Developer**

  **Authorized:**
  - Performance, SQL Monitor
  - SQL Plan Control, Top Activity
  - Top Consumers, SPA
  - Read Only access to Sessions, Database Schema

  **Not Authorized:**
  - Database Startup/Shutdown
  - Run SQL, SQL Worksheet
  - Security Pages, View Table Data
  - Tablespaces
  - Init Parameters
  - Any write access to database

• **Application DBA**

  **Authorized:**
  - Performance, SQL Monitor
  - SQL Plan Control, SQL Tuning Sets
  - Sessions (including Kill Session)
  - Top Activity, Top Consumers
  - Database Schema (View and modify)
  - Optimizer Statistics, Init Parameters

  **Not Authorized:**
  - Database Startup/Shutdown
  - Run SQL, SQL Worksheet
  - Security Pages (Users, Roles, Profiles)
  - Data Guard, Backup/Recovery
  - Storage

• **Database Administrator**

  **Authorized:**
  - Backup/Recovery
  - Storage
  - Database Startup/Shutdown
  - Database Patching/Upgrade
  - Performance (Top Activity, SQL Monitor, etc.)
  - Replication
  - Init Parameters
  - Resource Manager

  **Not Authorized:**
  - None
Flexible DB Access Control for Database

- Flexible DB Access Control privileges
  - Very granular database target privileges available for target types – Database Instance, Cluster Database and Pluggable Database
  - Privileges restrict access
    - Menu items (Disabled if no access)
    - Database home page regions (not visible if no access)
    - Separate View and Manage privileges for all areas in DB management (~150)
- Out-of-box Aggregated Privileges also available. Eg:

<table>
<thead>
<tr>
<th>Database Application DBA</th>
<th>Manage Database Performance Privilege Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Can manage application schema, application objects and application performance in the database]</td>
<td>Manage Database Schema Privilege Group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Database Application Developer</th>
<th>View Database Performance Privilege Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Can view DB performance but cannot make changes to DB]</td>
<td>View Database Schema Privilege Group</td>
</tr>
</tbody>
</table>
Flexible DB Access Control for Database

Application DBA Role
Database Application DBA privilege
On DB1, DB2, DB3, DB4

Application Developer Role
Database Application Developer privilege
On DB1, DB2, DB3, DB4

Application DBAs

Application Developers

Database Targets

Application DBAs have access to “SQL Performance Analyzer Setup” and “SQL Access Advisor”.

Example, “SQL Performance Analyzer Setup” and “SQL Access Advisor”
Enterprise Manager Authorization

Propagating privileges to New target

When a new target is added, how do my administrators automatically get the right set of privileges on the newly discovered target?
Privilege Propagating Groups

- Privilege propagating group
  - Enables privileges to be propagated to members of a group
  - Existing members of a group
  - Automatically propagates to any new members

- Enhances target group management
  - Allows granting of privileges to thousands of targets
  - Allow grants to various teams different levels of access to target group
  - On-boarding new administrator becomes simpler
Enterprise Manager Authorization
Sharing Named Credentials

Since I cannot add Named Credential to a role, how can I share Named credentials with some of my users?
Share Named Credentials using Private Roles

– Some sensitive privileges cannot be added to a System Role
  • Any Super administrator has access and can grant to any user
  • Any Super administrator could grant a role without knowledge of the owner
– To grant these sensitive privileges to many users, use Private Roles
– Private Roles:
  • Only Role owners or role grantees can grant role to other users
  • Only Role owner has access to modify/delete the private role
– Share restricted Named Credentials between administrators by assigning it to Private Role, then granting that role to your users.
Enterprise Manager Authorization

Sharing credentials with ALL users

How can I easily share and manage credentials with all users?
Global Preferred Credential

• Preferred credential for ALL users
  – Applies to specific targets instances / all targets of a type

• Benefits:
  – Reduced administrative overhead of maintaining lesser privileged credentials
  – New targets can automatically be accessed by many users if global preferred credential is already set for its target type
  – Enable new users to automatically access many targets
Enterprise Manager Authorization
User administration

Is there a way I can delegate user management responsibility to an Enterprise Manager user without requiring the user to be a super administrator?
Delegated User Administration

- New System resource privilege “User Management”
  - Allows non-super administrators to be responsible for user creation and deletion
  - Can add, update, delete users
  - Avoid unnecessary granting of super administrator privilege for user management
How do I know my database passwords are going to expire and change?
New Metrics to monitor DBSNMP account password expiry

– **Monitoring User Expiry**
  - Monitors potential expiry of DBSNMP user password
  - Alert threshold: Hours before user account expires
  - Default values: Warning: 72 hours
  - Enables proactive management of DBSNMP password, preventing password expiration and lapse in DB monitoring

– **Monitoring User Connectivity Issue**
  - Monitors DBSNMP user that is already expired, locked
  - Raises critical alert (Threshold default: Critical: ORA-*)
  - Alert message will include the ORA message from failed connection attempt
  - Provides visibility into problems with DBSNMP user, preventing lapse in monitoring
Configuration extension to monitor DB account password expiry

• Create custom compliance rules to monitor database user password expiry

• Register compliance violations
  – Create Configuration extension for database instance target type
    • Refer SQL Query from Appendix
  – Create Agent-side Compliance Standard Rule and select the configuration extension created.
  – Create Agent-side Compliance Standard and add the Compliance standard rule
  – Associate the database instance targets to the compliance standard

• Alternate Option
  – EMCLI Scripting with verb `get_db_account` passing in “-expire_in_hours” parameter
Making Password Changes Easier

• For host credentials: Two step configuration process
  – Change OS user password at the host
  – Change in Enterprise Manager using EMCLI verb: update_host_password
  – Sample: emcli update_host_password –target_name=myHost –user_name=Admin1 –change_all_references=yes

• For DB credentials: One step configuration process
  – EMCLI verb update_db_password changes at DB target and all Enterprise Manager credential references
  – Supports changing password for ALL users, including SYS/SYSDBA users
  – Sample: emcli update_db_password –target_name=mydb –user_name=dbsnmp –target_type=oracle_database –change_all-references=yes –change_at_target=yes

• All other targets: Two step configuration process
  – Change at target
  – Change in the credential with EMCLI verb -update_named_credentials
Enterprise Manager: Security Best Practices Summary

Vigilant security solutions for protecting infrastructure communications

Scalable security management solution encompassing robust access control

Strong password management practices reducing risk
Appendix
Configuration extension to monitor DB account password expiry

• SQL Query:

```
SELECT USERNAME || ' going to expire in next 24 hours' FROM SYS.DBA_USERS WHERE ACCOUNT_STATUS not like '%EXPIRED%' AND ROUND((EXPIRY_DATE - SYSDATE)*24,0) <= 24
```
Configuring Third party CA certificates for communication to target databases

- Properties to be set at OMS
  - #Client authority
    - `emctl set property -sysman_pwd sysman -name em.targetauth.db.pki.KeyStore -value <...wallet..>`
    - `emctl set property -sysman_pwd sysman -name em.targetauth.db.pki.KeyStorePassword -value <...>`
    - `emctl set property -sysman_pwd sysman -name em.targetauth.db.pki.KeyStoreType -value <..>`
  - #Server authority
    - `emctl set property -sysman_pwd sysman -name em.targetauth.db.pki.TrustStorePassword -value <...>`
    - `emctl set property -sysman_pwd sysman -name em.targetauth.db.pki.TrustStore -value <...wallet..>`

- Properties to be set at Agent
  - #Client authority
    - `emctl setproperty agent -name connectionKeyStoreLocation -value <...wallet..>`
    - `emctl setproperty agent -name connectionKeyStoreType -value <..>`
    - `emctl setproperty agent -name connectionKeyStorePassword -value <..>`
  - #Server authority
    - `emctl setproperty agent -name connectionTrustStoreLocation -value <...wallet..>`
    - `emctl setproperty agent -name connectionTrustStorePassword -value <..>`
    - `emctl setproperty agent -name connectionTrustStoreType -value <..>`
Raising the Ante on Security with Oracle Enterprise Manager [CON9719]

Joe Kopilash – Architect and Director, Database Administration
Super Administrators

- Only a small subset of DBAs are SA within OEM
- Main reason is we can’t enforce standards if everyone can do anything they like.
- Are responsible for the operations of OMS
- Assist regular administrators if they run into issues
User Roles/Permissions

- Regular DBA Administrators (the bulk of the users in OEM)
  - DBAs are responsible for installing their own agents via OEM Console
  - DBAs are given full permissions on their targets
  - DBAs are allowed to discover, add, and drop their own targets
  - DBAs are responsible for their own agent patching and operations
User Roles/Permissions

Application Users With Access To EM
- Read only permissions on EM targets
- Granted “Connect Target Read-only” for some users
- If required to view top activity and/or other info we grant them view on a named credential they can use that has the required DB roles.
Named Credentials

- Database Access From EM
  - Named Credentials are an object in 12c that you can create, modify, and grant permissions on.
  - Our normal DBA users have the ability to create their own named credentials for most activities.
  - When multiple DBAs work on the same DB, common users needed in EM can be easily shared by granting permissions on them like SYS or OS users.
  - For many of our Application users if they need to see things they don’t have or we don’t want them to see outside of EM, we setup named credentials for them and grant them view access to it along with “Connect Target Read-only” to their account.
  - Credentials can be used made as Global to be used across multiple targets such as data guard.
Security Setup

- **Targets**
  - All targets are added to groups

- **Groups**
  - Are created as **propagating privilege** groups and are granted to roles
  - Are nested
  - Used for Reporting
  - Used by notification PL/SQL procedures to send out alerts by populating custom target properties on the groups

- **Roles** – Are granted to users with required privileges on groups
EM Auditing

- Basic Auditing is enabled by default and includes the following on named credentials:
  - Creating
  - Deleting
  - Editing
  - Associating
  - Accessing
- Can update with “emcli update_audit_settings”
- We enabled all auditing and find it very useful
Security Setup

- Authentication
  - Currently using repository authentication for users
  - LDAP/AD authentication
    - Setup has improved in 12.1.0.5 and we are currently reviewing implementing it.
    - We are looking to use EM roles instead of external roles
Safe Harbor Statement

The preceding is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Integrated Cloud
Applications & Platform Services