ORACLE ENTERPRISE MANAGER 12c

Oracle Enterprise Manager 12c: Zero to Manageability

Lessons Learned from the Strategic Customer Programs Fast Track Installation Method

ORACLE WHITE PAPER | JANUARY 2015

ORACLE

Table of Contents

Introduction

Oracle Enterprise Manager (EM) has evolved from the early days of just a database monitoring tool to being a full-scale data center monitoring and management tool. As with any application, you need proper planning to ensure a successful implementation. If you don't take the right approach to planning your environment, the project can become overwhelming. As part of the Enterprise Manager Strategic Customer Programs team, we've worked on over 80 Enterprise Manager 12c installations at various companies across the world. Most of our customers are large enterprise-wide installations, requiring detailed planning and integration. From our experiences, we've outlined a methodology to implementing EM in a phased approach to ensure success. The goal is to complete the basic deployment and monitoring configuration before diving into extended features such as Lifecycle Management and Cloud. If you start with a solid infrastructure, the rest of the feature implementations will also be successful. By following the steps in this whitepaper you will successfully plan and architect the first phase of your deployment with the future usage and growth in mind.

Planning & Architecture

Enterprise Manager is an enterprise application that manages and monitors the other targets in your environment. While monitoring is the core functionality, there are many additional features from performance tuning to patching and provisioning. To properly plan and architect an enterprise-wide Enterprise Manager, you must:

- Identify goals
- Understand the architecture
- Plan capacity for growth
- Identify High Availability requirements

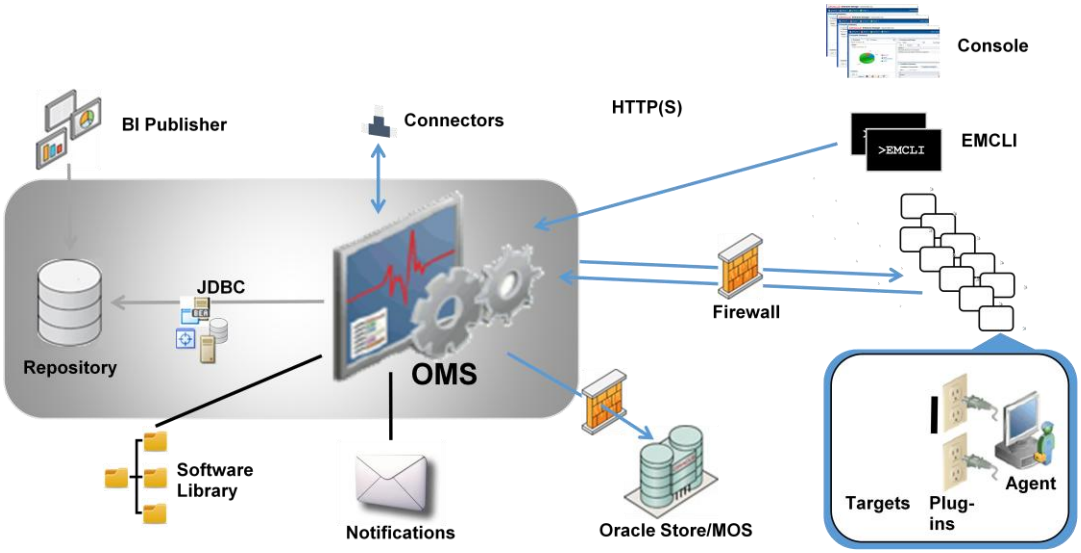


Figure 1. Sample architecture diagram of Oracle Enterprise Manager

Goals

The first step to planning is to determine what your goals are for EM. This includes defining how you will use EM, what targets you will monitor and manage, what additional features will be used now or in the future. Enterprise Manager has such a broad range of capabilities that trying to nail down goals can be quite daunting. The key to successfully accomplishing this is to break the goals down into smaller, more manageable tasks. Examples of tasks that might be identified could include:

- Deliver JVMD instrumentation for UAT applications
- Deliver AWR/ADDM access to Production DBAs
- Provision RAC clusters
- Identify compliance violations

By taking a look at your target environment and evaluating what targets you use, and what you intend to do with them regarding monitoring and management, you can begin to properly plan the type of environment you need. This will also help in the next step of sizing your environment. Now is also a good time to review the EM Certification matrix to ensure that all your targets and operating systems are supported.

Architecture

Once you've identified what type of targets you'll be monitoring and what features of EM you will use or plan to use, the next step is to determine the proper architecture for your deployment.

It's important to note that the OMS and Repository servers should, in networking terms, have very low latency due between them. The recommendation is to have less than 1 ms latency between the OMS and Repository database. For most customers, this typically means the OMS and Repository are located in the same data center. We do not recommend co-locating the OMS and Repository in production environments due to memory and CPU consumption.

It is essential or at the very least strongly recommended to have a development or lab environment where you can test patches, new features and design/develop templates, jobs, deployment procedures and other components that may be moved into Production.

Single or Multiple Installations

One of the most frequently asked questions is should we have one EM installation per data center or country? We do not recommend multiple EM installations in one company for sake of location. There are a few use cases for multiple EM installations in one company, but very limited. Some organizations favor multiple installations to preserve security restrictions, or segregate by functional group. Another common case for multiple EM installations is segregating Non-Production and Production. While this is an acceptable case if complete separation is required, it is not the best practice. The best practice is to have a single Production EM installation for your organization. The benefit of having a single environment is that you will have a single pane of glass for all target information, whether looking at monitoring, inventory, configuration or reporting. By having all your assets in one system you will also have a single system to monitor and manage. EM is an application of its own and requires care and feeding on a regular basis. It is also beneficial to have the entire application stack monitored by the same system so you can take advantage of the many drill-down features of EM.

Physical or Virtual

The recommendation is to place your Repository and OMSes on dedicated hardware for performance and isolation purposes. If you plan to use Virtual servers for ease of maintenance reasons or for scalability, then ensure that your server is not overloaded and that the required resources are available for the EM components. Using virtual servers for the purpose of mass consolidation is not recommended for placement of your EM components.

High Availability

Determining your availability requirements depends on whether you will be monitoring Mission Critical applications and environments and what acceptable downtime and recovery times are for your business. There are various levels of high availability for EM as defined in the table below:

ENTERPRISE MANAGER HIGH AVAILABILITY

	Description	Number of Nodes (Min/Rec)	Load Balancer Requirements
Level 1	OMS and repository database. Each resides on their own host with no failover.	1/2	None
Level 2	OMS installed on shared storage with a VIP based failover. Database is using Local Data Guard.	2/4	None
Level 3	OMS in Active/Active configuration. The database is using RAC + Local Data Guard	3/5	Local Load Balancer
Level 4	OMS on the primary site in Active/Active Configuration. Repository deployed using Oracle RAC. Duplicate hardware deployed at the standby site. DR for OMS and Software Library using Storage Replication between primary and standby sites. Database DR using Oracle Data Guard. Note: Level 4 is a MAA Best Practice, achieving highest availability in the most cost effective, simple architecture.	4/8	Required: Local Load Balancer for each site. Optional: Global Load Balancer

Level 3 is the most common level of availability starting with adding RAC for a repository database, a Data Guard standby, and additional OMSes fronted by a load balancer. All OMSes are active and can balance the load of servers. This level may be required due to availability concerns, but also due to sizing as defined above. The more targets, the more processing power you may need. Keep in mind your sizing requirements when determining the number of active nodes required for availability. For example, if your size dictates 2 OMSes, you will need 3 OMSes for availability. For multiple OMSes, a load balancer is required, as well as a shared Software Library location. For details on this implementation review the Deploying a Highly Available Enterprise Manager 12c Cloud Control whitepaper.

Level 4 takes availability a step further by providing disaster recovery. This involves creating a standby environment for the entire OMS and Repository by using storage replication in a remote data center. There are very unique requirements for network and install locations when using the replicated DR solution, so proper planning before installation is critical. If you think there's a chance you might add a DR in the future, the recommendation is to plan for it during the install time so that moving into a DR solution will be easy. For detailed information on the disaster

recovery implementation review the Enterprise Manager Cloud Control 12c Disaster Recovery with Storage Replication whitepaper.

Once you've defined whether you will need one OMS, multiple OMSes or disaster recovery, you can begin to piece together the rest of the architecture required for your environment including the storage capacity and shared storage.

Installation Planning

The next step is to evaluate your planned installation and forecast capacity required for future growth of your system over the next 12-18 months. The minimum requirements for install are documented in the Basic Installation Guide. By reviewing the Advanced Installation Guide chapter on sizing you can save yourself the time and effort of having to request additional hardware or resources shortly after deployment. The following breakdown of components will help in determining your capacity needs.

Agents

In addition to the agent prerequisites defined in the Basic Installation Guide, you need to consider the Agent install location. The minimum space required for Agent installations is typically 1 GB; however this is just enough for binary installation. The recommendation is to have enough space available to prevent the Agent from stopping collections if it runs out of disk space. It is recommended to have at least 2-4 GB free space for the Agent. Keep in mind, agents will be upgraded out of place from now on, so enough space will be needed for the new agent to be installed before the old Agent can be removed. The agent home is also the default staging location for patches applied from EM and extracts for AWR Warehouse. Our recommendation for agent location is to have the agent installed on its own mount point, e.g. /u01/app/oracle/agent. Isolating the agent ensures that installing, deinstalling and upgrading will not affect non-Agent binaries. If it is shared with other product binaries, you want ensure that there is sufficient space that it does not affect the other products if the agent can't upload or communicate with the OMS temporarily. As a best practice to aid in maintenance planning it would also be a recommendation that the installation location for EM Agents is standardized across your infrastructure. This standardization will assist with debugging, and upgrading in the future.

OMS

The OMS installation will require a binary install location or Oracle Home, as well as the location for the Software Library. For the OMS install, a 64 GB mount point would allow you to install all associated components (EM 12c, BI Publisher, JVMD, ADP, etc) and allow for out-of-place upgrades. The old OMS install can be cleaned up post-upgrade to leave plenty of space for log and dump files needed for any analysis.

For the Software Library, you want to think about what activities you will be performing and how much will be stored in the Software Library. This is where patches, provisioning profiles, cloned Oracle Homes and Database images, Middleware images, and VM images will be store. In a multi-OMS installation, this location must be shared read-write between all OMS servers. The following guidelines derived from multiple customer installations are a starting point based on the planned usage:

- Core Usage - 50 GB
- Patching & Provisioning - 250 GB
- Oracle VM, Cloud - 500 GB

Repository

As defined in the sizing guidelines, the size of the repository space is determined by the size of your installation. You need to identify if you will have a Small, Medium or Large installation as well as if additional features such as

APD and JVMD will be used before determining the appropriate space for your repository database. When requesting disk, keep in mind this includes product installation (Oracle Home), data, archive, flashback, redo logs, temp and undo. The recommendations below are only intended as a starting point. Depending on the type and number of targets, the metrics and frequencies collected as well as the retention policies set, your system may be smaller or larger.

RECOMMENDED REPOSITORY SIZING

	Small	Medium	Large
Data (+temp, undo, redo)	75gb	250gb	350gb
Archive/Flashback	25gb	100gb	150gb
APD (per JVM)	8mb		
JVMD (per JVM)	8mb		
Oracle Home	64 GB		

The nature of the EM Repository is to grow for a period of one year before the daily rollup's start to get purged. If you have a fairly static environment, after one year your repository size should remain consistent all things considered equal. If you increase data retention times, you will need to consider the additional storage required as well. You may also need to give consideration for increased storage usage if the environments you monitor with EM generate substantial event information (for example, lot's of metric threshold violations). This is not often a major impact on sizing but in cases where EM is monitoring large development environments with out of the box default metrics it can have an impact. Consider customizing the metrics to prevent this or increase the storage available in your capacity planning to cater for the additional storage needs.

The space required for the Database binary install is typically 16-20 GB, however database upgrades are going to be out of place upgrades from now on, so the recommendation would be to at least double that space to be prepared for patching or upgrades. A good starting point would be 64 GB.

Network Requirements

Planning out proper network requirements are a key to successful deployment. Obtaining load balancers, virtual IPs and firewall access can take time in many companies. The following considerations should be made when planning your environment.

Load Balancer or VIP

If you are installing multiple OMS servers, you will need a Load Balancer. This will provide a single virtual URL for the agents and users to communicate with to balance the load amongst all servers. If you are not installing a second OMS at this time, you may want to consider using a virtual IP in place of a Load Balancer so that you can easily move towards a multi-OMS scenario at a future time. This will prevent the need to resecure all agents with the new Load Balancer URL. To get details on the required configuration for the load balancer you can review the whitepaper Configuring OMS High Availability with F5 Big-IP Local Traffic Manager or the Administrator's Guide.

Online or Offline Self Update

One of the key features in EM is the integration to My Oracle Support for patch downloads and self-updates. You can specify a proxy server, port, user and password if necessary to enable your OMS servers to communicate with Oracle. If your OMS will not be online, then you can operate in Offline mode which allows you to download patches or updates from an internet connected computer, and import to the Software Library. This method is more tedious,

but may be required for some customers due to security restraints. For details on operating in offline mode see the Oracle Enterprise Manager Cloud Control Administrator's Guide. The best practice is to operate your Enterprise Manager installation in online mode if at all possible.

While operating in online mode, you will need an authorized MOS account and access via HTTPS to the following Oracle websites:

- updates.oracle.com
- support.oracle.com
- ccr.oracle.com
- login.oracle.com
- aru-akam.oracle.com

Some firewalls will also restrict the forwarding to the following Oracle websites and may also be needed:

- servicecentral.sun.oracle
- loginadc.oracle.com

Firewall Ports

Firewalls between intranet components are becoming more and more common. There may be firewalls between your OMS and Repository, OMS and Targets and between the users and the OMS that need to be addressed. If you're installing more than one OMS, you will need a Load Balancer which will also need to be discussed with your networking team. The ports will be needed for each OMS and the VIP or Load Balancer. For additional details on how to change ports see the blog Network Ports Used in Oracle Enterprise Manager 12c.

DEFAULT PORTS FOR BASIC INSTALLATION

Default Port (Range)	Protocol	Source	Destination
3872	HTTPS	OMS	Agent
4889-4897 1159,4899-4908	HTTP HTTPS	Agent	OMS
7788 7799	HTTP HTTPS	Console (End User Browser)	OMS
9702	HTTPS	Console (BI Publisher Interface)	OMS
1521 ***	SQL*Net	OMS	Repository Database
7102	HTTPS	OMS	WLS Admin Console
22	SSH	OMS	Agent Used for agent deploy via Console only.
7	ICMP	OMS	Target Host
		OMS	Target - Additional ports may be required as per target discovery documentation: Oracle Database, GoldenGate, Weblogic, Oracle HTTP Server, Exadata, Exalogic, Exalytics, E-Business Suite, Siebel, PeopleSoft, SOA, BPEL, Service

			Bus, OBIEE, Identity Management, Oracle Data Integrator, TimesTen, DB2, SQL Server, Sybase, WebSphere/JBoss, Tomcat
443	HTTPS	OMS	For online access to MOS or patches: updates.oracle.com support.oracle.com ccr.oracle.com login.oracle.com aru-akam.oracle.com

ICMP

ICMP is also used for checking host status if the agent hasn't updated recently. This needs to be enabled on all UNIX hosts for availability reporting. Without ICMP, if the agent hasn't uploaded in X minutes, the OMS will ping the host and report it as down. While everything will still function without ICMP, the status cannot be accurately detected whether the host is down or agent not uploading. The consequence of being unable to deterministically ascertain correct target status is potentially misleading alerts. For example, receiving a 'target down' message when the actual root cause is a 'network down' issue.

Security

Agent Owner and Root Access

Determining the agent install user can be complicated in some environments. Typically the monitored target user is the agent install user. So for database targets, that would be oracle. For WebLogic, it is typically weblogic. Another approach is to have a single agent install user across the environment. The users must be in the same primary group (i.e. oinstall) for the agent user to have proper permissions to the target and inventory.

Rarely do users have direct password access to the account that they are installing the agent as. In cases such as this, a privilege delegation utility such as pbrun or sudo is often used. This allows administrators to configure access permissions for particular users. Some commands require root access as well, which is often locked down for typical administrators. There are two areas that you will need to configure for privilege delegation, the agent install and post-install usage. Identifying and making the appropriate configuration change requests before install time is highly recommended.

Agent Install

Since the agent has yet to be installed there are additional requirements to be able to push the agent from the OMS to the target server using privilege delegation. This could be used if the install user password is unknown, or for execution the root.sh scripts after install. If direct access to the account is not available, and sudo/pbrun cannot be configured, you will need to look at the AgentPull or Silent Installation methods that run from the target server itself, instead of deploying from the EM console.

CONFIGURING SUDO/PBRUN/SESU FOR AGENT INSTALLATION

	Example
Configuration requirements for sudo, pbrun, su, etc.	If the tool you are using requires a pseudo terminal for remote command execution via SSH (default for prbrun, sesu, su) a. Set the oracle.sysman.prov.agentpush.enablePty property to true in

	$<OMS_HOME>/sysman/prov/agentpush/agentpush.properties or b. use the -enablePty additional parameter in agent push
Sudo config only	Do one of the following: a. Include Defaults visiblepw in the /etc/sudoers file, or enter the sudo command with the -S option for Privileged Delegation Setting on the Installation Details page. or b. Comment out Defaults requiretty in the /etc/sudoers file.
Installing as oracle (or agent owner)	Grant privileges to invoke the id command and the agentdeployroot.sh script as root For example, /etc/sudoers file: `oracle ALL=(root) /usr/bin/id,/<agent_base>/*/agentdeployroot.sh`

Installing as joe sudo to oracle (or agent owner)	a. Grant privileges to invoke /bin/sh as the locked account user
	`joe ALL=(oracle) /bin/sh`
	or
	a. Set the oracle.sysman.prov.agentpush.pdpShellOutEnabled property to false, and ensure that the installing user has the privileges to invoke id, chmod, cp, mkdir, rm, tar, emctl, agentDeploy.sh, runInstaller, and unzip
	`joe ALL=(oracle) /usr/bin/id, /bin/chmod, /bin/cp, /bin/mkdir, /bin/rm, /bin/tar, agent_base>/agent_inst/bin/emctl, <agent_base>/*/agentDeploy.sh, agent_base>/*/prereq_stage/core/*/oui/bin/runInstaller, <agent_base>/*/unzip, agent_base>/*/unzipTmp/unzip`
	Ensure that the locked account user (oracle) has read permission on the home directory of the login user.

Additional details can be found in the agent installation prerequisites.

Post-Install

Once the agent has been installed, privilege delegation requires two steps. First add permissions for nmosudo to the sudoers or pbrun configuration file. Then tell EM what privilege delegating method to use by assigning a default template or assign a template to each agent. These steps must be completed before attempting any action with sudo or pbrun.

Sample SUDOERS File:

```
johndoe ALL=(oracle) /u01/oracle/agent/sbin/nmosudo
johndoe ALL=(root) /u01/oracle/agent/sbin/nmosudo
```

Sample PBRUN Config File:

```
if(user=="johndoe")
if(command=="/u01/oracle/agent/sbin/nmosudo" )
// /u01/oracle/agentis the Agent Home
{
   switch (requestuser
   {
      case "root":
         runuser="root";
         break;
      case "oracle":
         runuser="oracle";
         break;
      default:
      reject;
     }
```

```
 accept;
}
```

Security Certificates

EM supports adding custom certificates to the OMS, WebLogic server and the Agents. Adding a customer certificate to the OMS Console will prevent the "server not trusted" warnings when logging in to the EM 12c Console. To learn more about how to secure EM with custom certificates see EM 12c Cloud Control How to Create a Wallet With Third Party Trusted Certificate that Can Be Imported into the OMS For SSL Communication (Doc ID 1399293.1) Identifying which components should be secured with customer certificates, and how your company produces these before installation time is recommended.

Integrating to Other Applications

While integration with other applications and components can be done at any point after the installation, it is good to start thinking ahead of time what you may be integrating with so you can properly plan for this. The simplest method of notifications is e-mail or pager. Configuring this requires access to a SMTP server from the OMS. EM also has many predefined connectors that can send alerts to 3rd party service desk tools (Remedy, NetCool, etc.) as well as the ability to send SNMP traps. Coordination with your Service Desk/Tools team will be necessary to configure these.

For authentication you might want to integrate with an external authentication system such as Oracle Access Manager, Oracle Internet Directory, or other LDAP systems for simpler user and password management. This is typically managed by a Security team. You will need access to configuration information in order to make these connections. Additional help from your Security team may be required for custom certificates if you wish to load those to EM.

Project Plan

Now that you've identified what you will deploy and how, define a schedule and a plan based on your requirements and company change request processes. Don't forget to include a testing plan. How will you measure success when you've completed the first phase of the installation? What metrics need to be tested? The best method is to implement EM in a phased approach, completing one objective at a time before moving to the next. For example, complete the installation and database monitoring, before proceeding to middleware monitoring. Then start looking at Lifecycle Management, Cloud or other extensions.

Infrastructure Deployment & Configuration

After successful planning, you're ready to being deploying the Enterprise Manager infrastructure. This consists of creating a repository database and installing the Enterprise Manager software on the designated OMS servers.

Repository

When creating the Repository database, we recommend release 11.2.0.4 or later, and apply the latest PSU. Review the Master Index for Cloud Control Oracle Management Service (OMS) and Repository Installation, Upgrade and Patching (Doc ID 1363769.1) on MOS.

Additional notes on setting up the Repository database:

- Be sure to check EM documentation for required patches
- Disable unwanted services (such as XMLDB) and do not install sysman or demo schemas
- Set optimizer parameters in database:

```
ALTER SYSTEM SET OPTIMIZER_CAPTURE_SQL_PLAN_BASELINES=FALSE SCOPE=both;
```

OMS

When you're ready to install, the recommendation is to use VNC to connect to the OMS server. Xterm performance can be unreliable and can leave the install hung if the session disconnects. If you must use Xterm, ensure that the software is staged on a local drive as opposed to NFS share. The performance of the NFS share can severely impact running the Oracle Installer.

Download the latest EM binaries from OTN. The OMS installation wizard will ask you a series of questions about the install location, repository database, plug-ins required and desired ports. The following is an example of the information required during the install:

- Middleware Home Location
- Agent Base Directory
- Host name
- Weblogic user & password
- Nodemanager user & Password
- OMS Instance locations
- Database host, port, sid/service
- Deployment Size
- Sysman pwd, agent registration password,
- Management Tablespace
- Config Tablespaces
- MW Diagnostics
- Software library location
- Ports

After the installation, login to EM as the sysman user using the URL provided at the end of the install. The URL can also be found in the <OMS_HOME>/install/setup.txt file for future reference. You will be prompted to accept the license agreement upon the first login. Verify that the OMS agent and host targets are shown in the All Targets page and that all targets are showing a status of Up (green).

Backups

As with any production application, EM requires backups. The repository database should have regular full and incremental backups, as well as archive log backups per Oracle's best practice. For the OMS, you need to make a backup of the OMS configuration using `emctl exportconfig oms`, and then backup the entire OMS binary location, Software Library location and oraInventory. The exportconfig oms should be run after every configuration change, plug-in deployment or upgrade. The Agent can be recovered from a reinstall and resync from the OMS, but any modifications or customizations to the emd.properties should be backed up or noted for recovery purposes. It is also highly recommended to test your recovery procedure, before you actually need it.

Configure

While the out-of-box configuration is fine for most environments, larger systems will require a few more configurations and customizations for optimal performance. Some of these include increasing heap size, task workers, console timeout value and configuring auditing. Review the MOS note for Oracle Enterprise Manager 12c Configuration Best Practices (Doc ID 1553342.1) to get details on all areas that you might want to optimize your configuration. You may also want to integrate with an external authentication mechanism at this time, such as

Oracle Access Manager or Microsoft Active Directory. This can be done by referencing the Cloud Control Security Guide.

Download Agents and Plug-ins

In Enterprise Manager 12c, all software management is done via the Self-Update page. Software can be downloaded directly from Oracle via https in online mode. If you can't use a proxy and access the required Oracle sites, then you can use offline mode which will walk you through the steps to download files from a browser and import the files to EM using EM CLI. For detailed instructions on configuring and using Self-Update, please refer to the Administrator's Guide Chapter 13 Updating Cloud Control.

For Online Mode you will need to configure your Proxy and set My Oracle Support Credentials for SYSMAN user. Once you've established a connection, go to Self Update and click Check for Updates to ensure the latest content has been downloaded. If running in Offline mode, you will need to follow the steps provided in the console to download the catalog and import using EM CLI.

Once the catalog is up to date, you can begin downloading Agents for additional platforms and any additional Plug-ins that you are licensed for. Only download and apply the Agents and Plug-ins that you require. Maintaining these components adds maintenance overhead and consumes space in the Software Library.

Apply Recommend Patches

As with any software, it is recommended to apply the latest patches. With Enterprise Manager, there are several components that will need to be patched. While some patches may be released monthly, a quarterly patching cycle is typically followed by most customers. You'll want to setup a plan for planned software maintenance in your environment. There's a whitepaper Oracle Enterprise Manager Software Planned Maintenance that will help guide you through the best practices.

OMS Patches

The core Enterprise Manager system is typically patched with the quarterly PSU patches (released Jan, Apr, July, Oct) or a one-off when directed by support for a critical issue. PSU patches will be cumulative, so you need not apply each of them, just apply the latest. The OMSes must be shutdown during patching; however some patches are being released with rolling patch instructions for multi-OMS systems. These patches must be applied at the host level, and cannot be automated via EM. ALWAYS read the readme, yes every time. The patching steps can change from patch to patch so it's critical to read the readme. OPatch or OPatchauto will be used to apply these patches. Did I mention to read the readme for every patch? It's also important to note that there may be additional steps when patching in a multi-OMS or standby environment, so read the output of OPatchauto carefully.

Always download the latest OPatch release for the appropriate version. If you read the readme, you already know this! Download patch 6880880 for 11.1 (the OPatch version used by EM) and unzip into the $ORACLE_HOME. Most errors in patching are related to not updating OPatch.

For more information on PSU Patches and patching EM:
Oracle Enterprise Manager Cloud Control Administrators Guide - Chapter 16 Patching Oracle Management Server and the Repository
EM 12c Cloud Control: List of Available Patch Set Updates PSU (Doc ID 1605609.1)
How to Determine the List of Patch Set Update(PSU) Applied to the Enterprise Manager OMS and Agent Oracle Homes? (Doc ID 1358092.1)

Each plug-in has binaries that will require patches as well. Same downtime requirements apply for plug-in patches as the quarterly PSUs. Starting in 12.1.0.3, the plug-in patches are being released as a monthly bundle. This

means that if you have 6 plug-ins, you may have 6 OMS side patches to apply - 1 for each plug-in. Bundles are not always released for every plug-in every month. They are cumulative, so pick the latest.

Starting with 12.1.0.4, the individual OMS-side plug-in bundles are being grouped into a System Patch each month. So for example, in June 2014 the System patch includes MOS, Cloud, DB, FA, FMW, SMF, and Siebel plug-ins. Non-required patches will be skipped.

For more information on the EM Patch Bundles and Patching EM:
Enterprise Manager 12.1.0.4.0 (PS3) Master Bundle Patch List (Doc ID 1900943.1)
Enterprise Manager 12.1.0.3 Bundle Patch Master Note (Doc ID 1572022.1)

Agent Patches

Agent patches are applied to each agent. They can be applied via EM using the MOS patch plans, which makes it a lot easier when you have 100s or 1000s of Agents to patch! The Patch Plans will start a blackout, validate prerequisites, check for conflicts, and update OPatch for you. If you don't use the Patch Plan you can patch manually with OPatch, don't forget to read the readme! The Agent must be shutdown during the patch application. There are 4 main types of Agent patches you will see:

- Core Agent - Starting with 12.1.0.3.0 the core Agent will have monthly patch bundles. These are also cumulative, so my recommendation is to apply the latest one.
- Agent-side Discovery Plug-in - This is the lightweight piece of the plug-in used for target discovery. Discovery plug-in patches are cumulative with other discovery plug-in patches for that component.
- Agent-side Monitoring Plug-in - This is the more detailed monitoring side of the plug-ins for the required components. Monitoring plug-in patches are cumulative with other monitoring plug-in patches for that component. So if there's a Discovery and Monitoring patch available for the DB Plug-in, you need to apply both of them.
- JDBC patches for the Agent will be JDBC version 11.1.0.7.0. These patches do get applied to the Agent, and can be applied via the Patch Plans.

You can apply the latest Agent bundle, JDBC patch and the plug-in bundles in one patch plan. If there's a conflict, you'll be notified. If the Agents you've selected don't have specified plug-ins, you'll also receive notice during the analyze step.

In previous releases you had to specify Normal Oracle Home preferred credentials for all Agent targets to patch, or select Override and specify the Normal Oracle Home credentials. In 12.1.0.4, the Agent uses its internal credentials to Patch itself, so setting preferred credentials or specifying at run-time is not required. The user patching would require the Manage Target Patch and Patch Plan privileges.

For additional details on Agent patching:
Oracle Enterprise Manager Cloud Control Administrators Guide - Chapter 17 Patching Enterprise Manager Agents
Blog: Simplified Agent and Plug-in Patching

Infrastructure

It's also important to keep the infrastructure stack up to date as well. This includes the Oracle Fusion Middleware and Oracle Database that are used for EM. The recommendation is to follow the best practices for each of these components, and regularly update with the PSU patches available. The following reference notes will help in identifying the current PSU patches. The WebLogic Server version used by EM 12cR4 is 10.3.6.

Oracle Recommended Patches -- Oracle Database (MOS 756671.1)
Master Note on WebLogic Server Patch Set Updates (PSUs) (MOS 1470197.1)

Add Additional OMS

Once configuration is done, you can look at adding an additional OMS and securing against a Load Balancer or VIP. There are three steps to adding an additional OMS. First ensure that your Software Library location is shared between all OMS servers. Second step is to secure the OMS is using the Load Balancer. Third, you are ready to add an additional OMS using the provided deployment procedure. An agent must be deployed on the server you wish to add as an OMS prior to running the deployment procedure. This process is detailed in the Administrator's Guide.

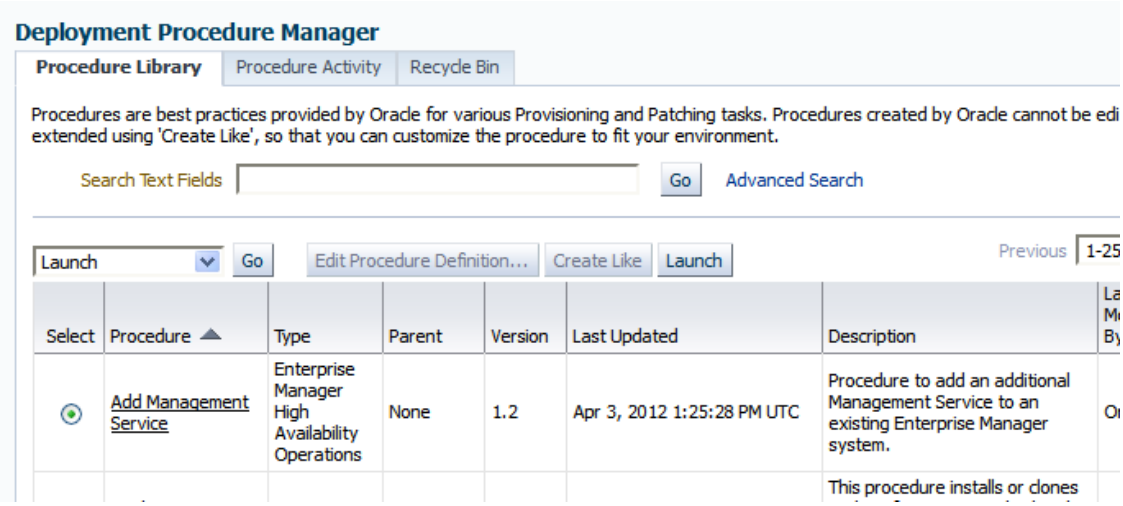


Figure 2. Add Management Service deployment procedure

Setup Monitoring Framework

Before getting too far into installation, it's best to sit down and think about whom your users will be and who your administrators will be. You will need to define groups, roles and users that will function as your organization functions. To do this you can start by asking your team these questions:

- Do the DBAs have access to all databases or just a certain set of them?
- Do the Middleware admins have access to the databases, read-only or additional permissions?
- Who can evaluate performance and run ASH/ADDM reports on the database?
- Who will be installing agents and discovering targets?
- Who will manage/patch/maintain EM?

Most customers will start deploying Agents to all hosts as soon as EM is installed; however if you take some time to set up the monitoring framework and rules before deploying agents and discovering targets, things will fall into place as targets are discovered. This includes setting up Groups, Roles, Users, Templates, Incident Rules and Target Properties. In the following section we will outline some of the considerations when determining how to setup your monitoring framework. The whitepaper Strategies for Scalable, Smarter Monitoring using Oracle Enterprise Manager Cloud Control 12c is an excellent resource for understanding the capabilities of enterprise monitoring with EM.

Groups

Groups are a very powerful feature in EM that helps you align your targets and perform bulk actions on like targets. The key is to group targets with common attributes that can be monitored in the same way. This may mean grouping by Lifecycle Status (Production, Test, Development, etc) or by Department (Sales, Finance, IT, etc.). By

aligning your security roles and incident rules to groups, you can ensure that people have access to the right targets and they receive the notifications important for them. Jobs, including database backups, can be run against a group. There is no one group fits all, but we will try to outline some of the thought areas that need to go into making this decision.

Most customers choose to use the Administration Group to manage their monitoring requirements. Targets become a member of the Administration Group based on their target properties. You will be able to set target properties during target discovery, afterwards, or even using an EM CLI script. Once defined, monitoring template collections can be associated with a tier of the Administration Group and synchronized on a regular basis. For this reason, we recommend that you first define your monitoring requirements and determine which targets will have like metrics and thresholds. One thing to keep in mind is that a target can only be a member of one tier in the Administration Group.

This can be easily accomplished by looking at the way your organization handles support on the targets currently. For this whitepaper we're going to assume you're planning to monitor Databases, Applications and Middleware targets and they each have their own support group. By creating a basic Administration Group that has DB, APP, and MW at the top level, you can easily map your DBAs to the Database targets and notifications, while mapping the Middleware Admins to the Middleware targets and notifications. By adding a 2nd level using the Lifecycle Status, you can further segregate your targets by their lifecycle (Development, Test, Production, etc.).

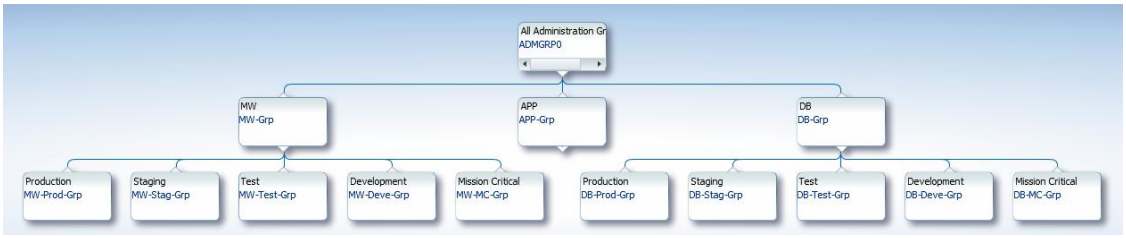


Figure 3. Administration Group Hierarchy

Not all your Group needs may fit nicely into an Administration Group; in that case the recommendation is to create Dynamic Groups. Similar to the Administration Group, the targets are automatically added based on their Target Properties matching the group criteria; however they do not automate any template application or synchronization.

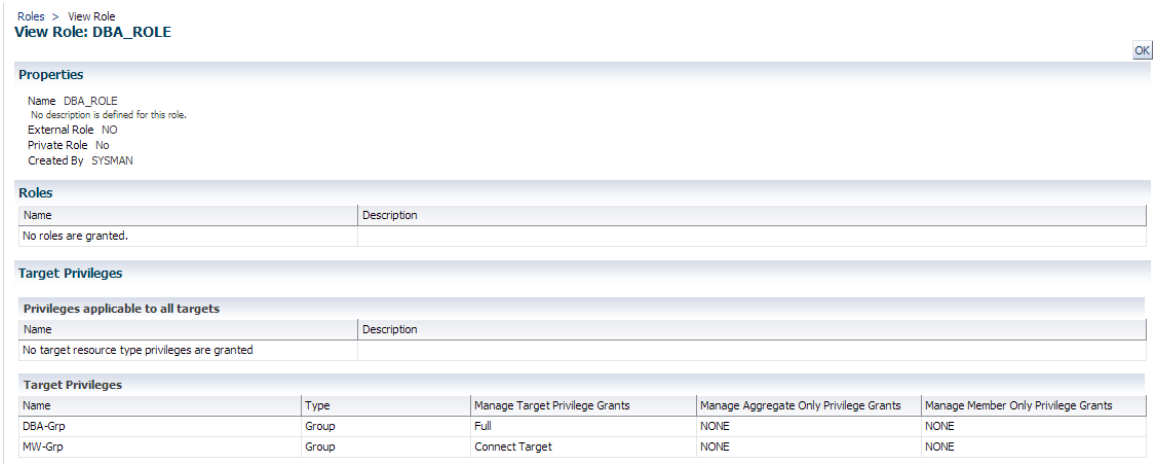
Templates

Templates are a key component to standardizing your monitoring. Create a template for each target type that you plan to monitor. Review the Oracle recommended metrics and determine if these are sufficient for your environment, remove thresholds from metrics you don't want to alert on, and disable metrics you don't want to collect at all. Consider whether you want to receive notifications and perform actions against a particular metric. If not, then a threshold is probably not needed. This is one way to reduce the number of alerts and notifications you support organizations receive. You may need multiple templates per target type, say one for Production Databases and one for Non-Production. The next step is to create a template collection which contains templates for multiple target types (Cluster Database, Database Instance, Host, etc.) and associate the collection to a leaf of the Administration Group. These can be grouped by target function or lifecycle (Sales or Production). By applying these to the Administration Group, you can ensure that targets in those groups will always have consistent metrics and thresholds as the templates are synchronized automatically.

Users & Roles

When granting privileges to users, the recommendation is to grant privileges to roles instead of directly to users. The benefit here is that you can group your users by function, and ensure that they have the same permissions. Once you've set up your Groups (Administration or Dynamic), you can easily grant permissions to a subset of

targets by selecting one of the groups. The following is an example of how you could setup roles for DBAs and Middleware Admins that would grant full permissions to the owning group, and read-only permissions to the non-owning group. In Figure 4 you can see that the DBA_ROLE will grant Full permissions to the DBA-GRP but only Connect and View permissions on the MW-GRP.


Roles > View Role

View Role: DBA_ROLE

OK

Properties

Name DBA_ROLE
No description is defined for this role.
External Role NO
Private Role No
Created By SYSMAN

Roles

Name	Description
No roles are granted.	

Target Privileges

Privileges applicable to all targets

Name	Description
No target resource type privileges are granted	

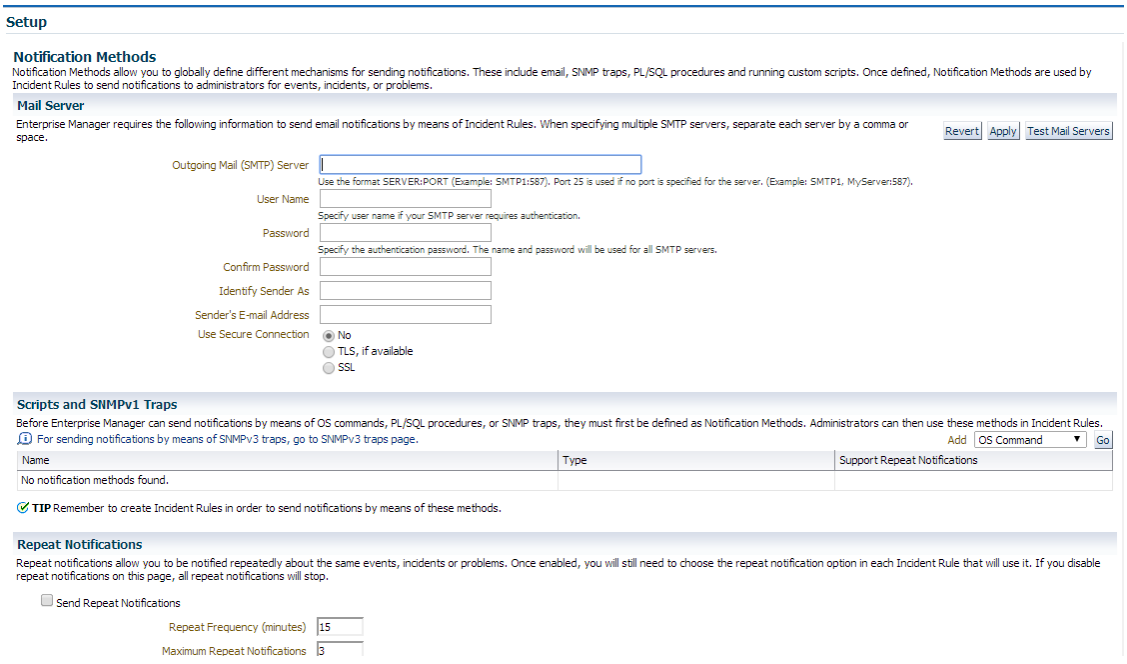
Target Privileges

Name	Type	Manage Target Privilege Grants	Manage Aggregate Only Privilege Grants	Manage Member Only Privilege Grants
DBA-Grp	Group	Full	NONE	NONE
MW-Grp	Group	Connect Target	NONE	NONE

Figure 4. DBA_ROLE with Full on DBA-Grp and Connect Target on MW-Grp

Notifications

Notifications can be as simple as an e-mail to a distribution list, or more complex such as SNMP traps to a monitoring tool, or a custom notification method in which an OS command is called. There are also many connectors available to integrate to some of the available 3rd party service desk applications. To configure the mail server, SNMP or custom notifications, go to **Setup/Notifications/Notification Methods**. These notifications will be available to select when you create an Incident Rule.


Setup

Notification Methods

Notification Methods allow you to globally define different mechanisms for sending notifications. These include email, SNMP traps, PL/SQL procedures and running custom scripts. Once defined, Notification Methods are used by Incident Rules to send notifications to administrators for events, incidents, or problems.

Mail Server

Enterprise Manager requires the following information to send email notifications by means of Incident Rules. When specifying multiple SMTP servers, separate each server by a comma or space.

Revert Apply Test Mail Servers

Outgoing Mail (SMTP) Server
Use the format SERVER:PORT (Example: SMTP1:587). Port 25 is used if no port is specified for the server. (Example: SMTP1, MyServer:587).
User Name
Specify user name if your SMTP server requires authentication.
Password
Specify the authentication password. The name and password will be used for all SMTP servers.
Confirm Password
Identify Sender As
Sender's E-mail Address
Use Secure Connection
No
TLS, if available
SSL

Scripts and SNMPv1 Traps

Before Enterprise Manager can send notifications by means of OS commands, PL/SQL procedures, or SNMP traps, they must first be defined as Notification Methods. Administrators can then use these methods in Incident Rules.

For sending notifications by means of SNMPv3 traps, go to SNMPv3 traps page.

Add OS Command Go

Name	Type	Support Repeat Notifications
No notification methods found.		

TIP Remember to create Incident Rules in order to send notifications by means of these methods.

Repeat Notifications

Repeat notifications allow you to be notified repeatedly about the same events, incidents or problems. Once enabled, you will still need to choose the repeat notification option in each Incident Rule that will use it. If you disable repeat notifications on this page, all repeat notifications will stop.

Send Repeat Notifications
Repeat Frequency (minutes) 15
Maximum Repeat Notifications 3

Figure 5. Setup Notification Methods

Incident Rules

The final step in setting up monitoring is to create Incident Rules which evaluate the events, create incidents and send notifications. Following the same example as before with DBA and Middleware teams, you would create an Incident Rule for each group, and apply it to their targets only by selecting the Database group, or the Middleware group. Then each team would only receive the notifications for the targets they are responsible for. An easy way to create your rules is to do a Create Like on the out of box Incident Rule Set and customize the Rules and Actions as needed. The out of box Rule Set has Rules designated for Metric Alerts, Errors, Unreachable, Down, Availability and more, as well as Rules to clear the stateless Alerts (ORA- errors) that often get left behind after 7 days.

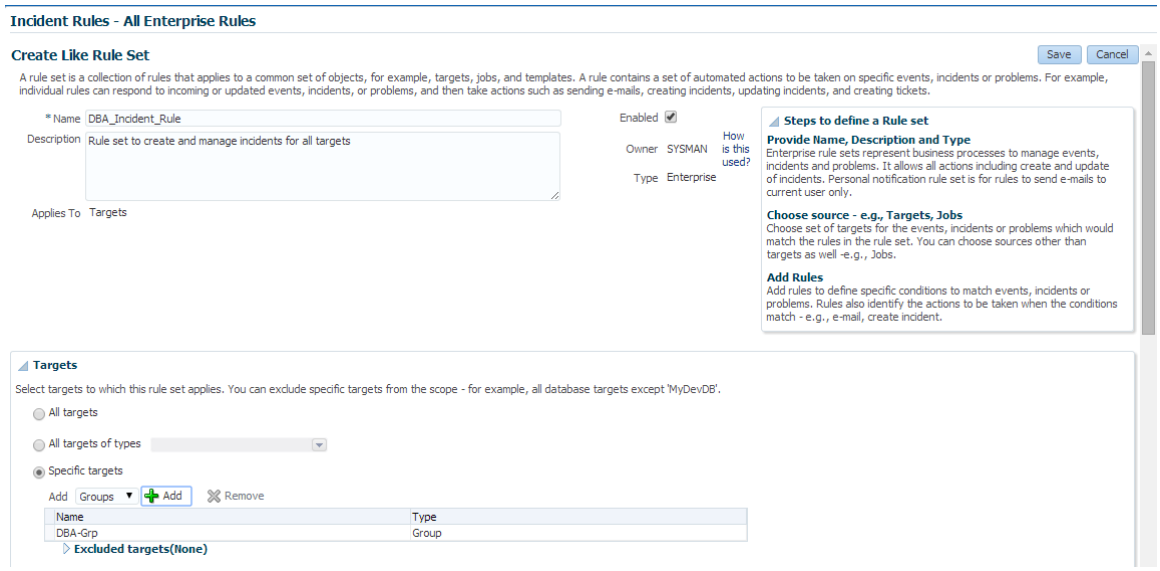


Figure 6. Incident Rules

Agent Deployment & Target Discovery

To monitor and manage targets, all servers will require an Agent. The agent can be deployed in many ways: pushed from EM, pulled from the server, silent install and rpm. Each method has its own requirements and advantages. When deploying your system, the recommendation is to test one or two agents per target type before mass deploying to the rest of your targets. This will help you determine the best method for agent deployment, target discovery and what patches and plug-ins are needed.

Cloning an agent (push or silent install) can be helpful if you want to deploy many agents with the same patches and plug-ins. By designating one agent as your “Golden Image” you can keep this agent updated and use it for deployments to keep the software up to date.

By staging the required patches in the $OMS_HOME/install/oneoffs directory, agents pushed from the console will automatically include the staged patches. Detailed instructions are available in the blog Simplified Agent and Plug-in Deployments. In addition to agent patches, during Agent Upgrades, the plug-in patches will be applied if they are present in the <OMS_HOME/install/oneoffs directory and the agent being upgraded contains those plug-ins.

Target Properties

Target Properties can be used for defining group membership criteria in the Dynamic Groups or Administration Groups, they can also be used in the Incident Rules or Notifications. The target properties are also used in

balancing the workload for the OMS loader processes. If there's a backlog situation, the OMs will process targets in Mission Critical, Production first, then Stage, Test, Development.

If you're using an Administration Group, be sure to populate all the required target properties at discovery time so that the target automatically gets assigned to the right groups. There is a report called Unassigned Targets Report available on the Administration Group Associations tab that can be used to validate all targets have been added to the administration group as required.

Target Discovery

Targets can be discovered many ways. The simplest is by allowing the Auto Discovery mechanism to run on a host, and then promoting the targets for monitoring. From Setup menu, select **Setup/Add Targets/Auto Discovery Results** and the **Targets on Host** tab. From here you can select the targets and click Promote. Be sure to promote the valid Oracle Home targets as well, this becomes critical when patching and provisioning is used later on.

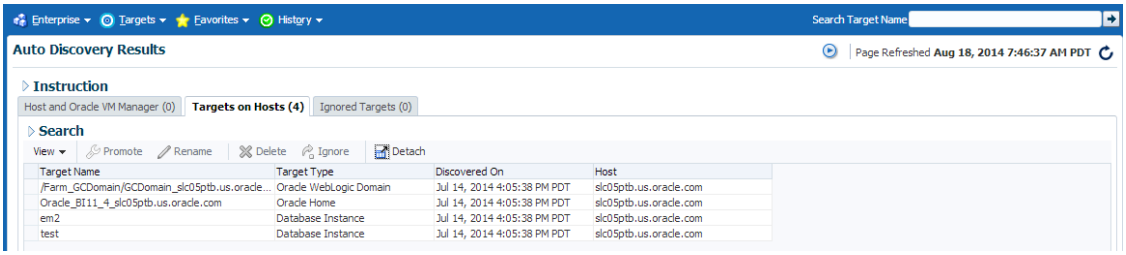


Figure 7. Auto Discovery Results

During promotion, you have options to set Global Target Properties.

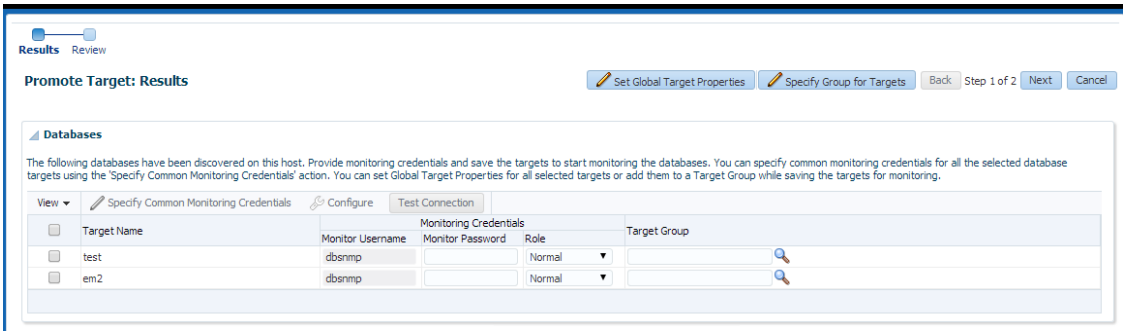


Figure 8. Promote Targets

Auto Discovery is configured automatically when the agent is installed. This is very convenient for new installations or for dynamic hosts. On static hosts, those where targets are not being added or modified, this may cause extra overhead that is not necessary. In this case, it's recommended that you adjust the discovery schedule or disable all together from the **Setup/Add Targets/Configure Auto Discovery** menu. You can adjust the schedule by selecting **Collection Schedule** and then choosing for all hosts or selected hosts.

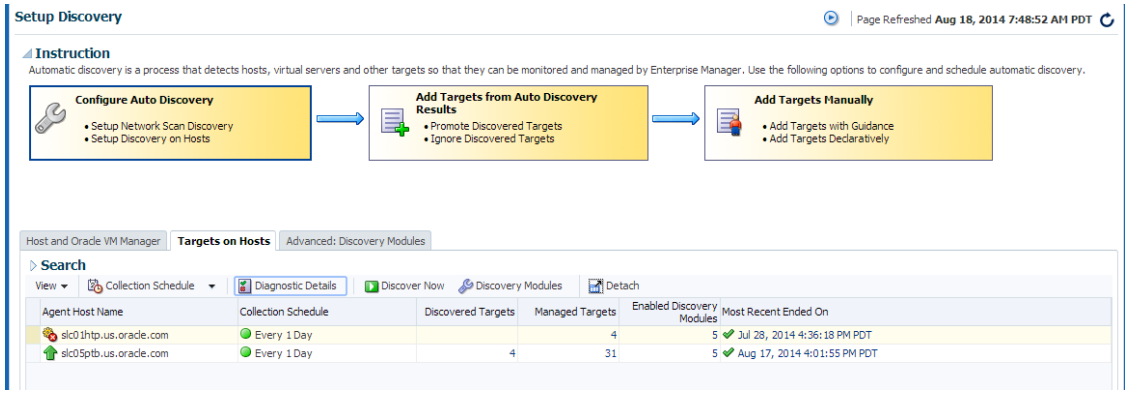


Figure 9. Configuring Auto Discovery

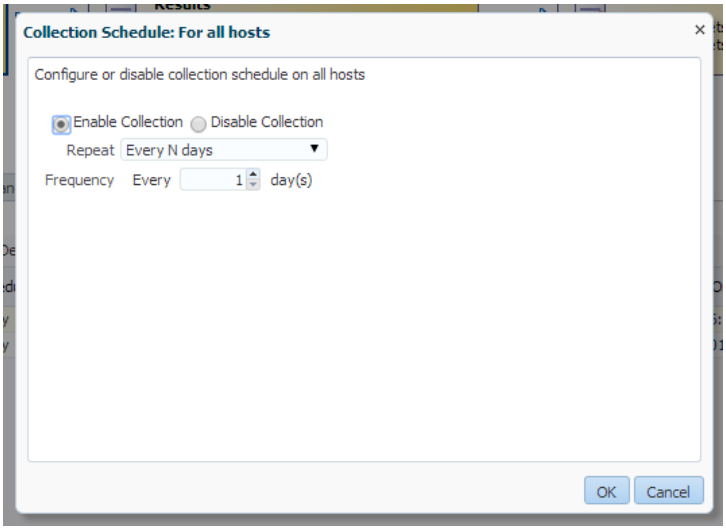


Figure 10. Modify Collection Schedule

During discovery and promotion of the WebLogic Domain, there's a checkbox to setup automatic refresh of the domain. Checking this box will schedule a refresh of the domain targets on a regular basis, since WebLogic Domains tend to be very dynamic. If you miss this during promotion, you can enable it afterwards by going to the WebLogic Domain target, and selecting the **WebLogic Domain Refreshed** timestamp link.

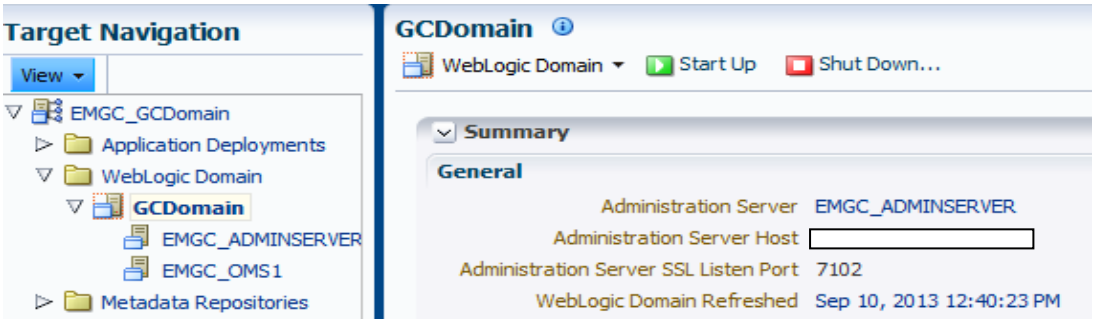


Figure 11. Setup Automatic Refresh for WebLogic Domain

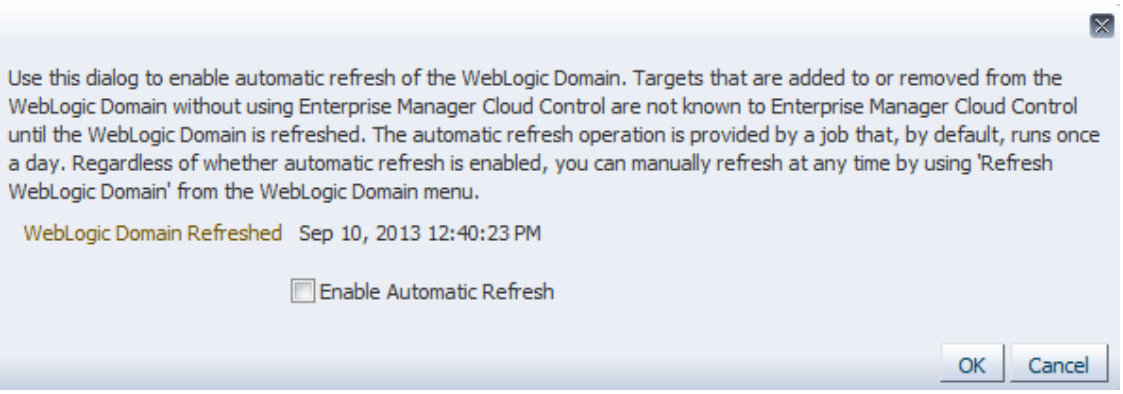


Figure 12. Enable Automatic Refresh for WebLogic Domain

Extending Use

Once you have successfully implemented Enterprise Manager for monitoring your core targets, you'll want to begin extending your usage to more than just monitoring. Whether you want to deploy AWR Warehouse, add additional target types such as E-Business Suite or SOA, or you start developing custom BI Publisher reports, the options are endless. Evaluate and deploy each feature or target type as a separate project so that you can complete one add-on at a time, avoid confusion and ensure a successful deployment. For example, deploying the Database LifeCycle Management pack which includes database configuration, compliance, patching and provisioning. These 4 features themselves are very detailed and require focus. Breaking the projects up into small chunks allows you to test, document and deploy as needed for your installation. Another option could be creating Metric Extensions to collect additional monitoring data not collected by default, or creating Corrective Actions that automatically fix certain metric alerts such as kicking of an RMAN archivelog backup when the Archive % Used metric triggers a Warning.

Maintaining

Enterprise Manager has become a valuable component in monitoring and administrating an enterprise environment. The more critical the application, servers and services that are monitored and maintained via EM, the more critical the EM environment becomes. Therefore, EM must be as available as the most critical target it manages.

There are many areas that need to be discussed when talking about managing Enterprise Manager in a data center. Some of these are as follows:

- Recommendations for staffing roles and responsibilities for EM administration
- Understanding the components that make up an EM environment
- Backing up and monitoring EM itself
- Maintaining a healthy EM system
- Patching the EM components
- Troubleshooting and diagnosing guidelines

When it comes to managing EM, it is recommended to have at least 2 people who are mostly dedicated and know the system very well, to ensure you have backup coverage during vacation or extended illnesses. Someone with knowledge of Oracle Database and WebLogic Server is extremely helpful as these are the main backbones of EM; however they also need to understand your entire enterprise. Integration into authentication and ticketing systems,

placement in network/firewall rules, configuration of the Load Balancer, segregation between support groups and organizations are all areas where the EM Administrator will be required to interface during initial setup and continued operations.

The Operational Considerations and Troubleshooting Oracle Enterprise Manager 12c whitepaper available on the Enterprise Manager Maximum Availability Architecture (MAA) site will help you define administrator requirements and responsibilities. It provides guidance in setting up the proper monitoring and maintenance activities to keep Enterprise Manager healthy and to ensure that EM stays highly available.

Summary

As you can see, Enterprise Manager is a very powerful application and enterprise management tool providing monitoring and management capabilities, to an automated Cloud solution. While you may want to deploy all components immediately, the most successful implementations take things in a phased approach, completing the basics and framework configuration first. By getting your infrastructure and architecture deployed and configured properly, your environment will be situated properly to sustain growth. Once you have your monitoring framework set up, adding targets and getting appropriate notifications becomes easy. Following these steps allows you to successfully add-on to the product with additional components and features without having to go back to make drastic architecture changes and core framework adjustments. If you start with a solid foundation, the possibilities are endless with Enterprise Manager.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oem

facebook.com/oracleenterprisemanager

twitter.com/oracle_em

oracle.com

Hardware and Software, Engineered to Work Together