Oracle Maximum
Availability Architecture

Oracle Enterprise Manager 12c

Software Planned Maintenance

ORACLE WHITE PAPER | OCTOBER 2015

Table of Contents


ORACLE

Introduction

A critical component of managing an application includes both patching and maintaining the software. Applying patches is not only required for bug fixes, it is also a means of obtaining new and beneficial functionality. Thus it becomes an important task to maintain a healthy and productive Enterprise Manager (EM) solution. The process of patching itself can present different challenges that can potentially increase the work and time involved in each patching exercise. Issues could arise such as patch conflicts; not meeting required prerequisites and even unnecessary downtime. Spending the proper time to setup a patching strategy can save time and effort as well as possible errors and risk when patching a production EM environment. This white paper provides an overview of the recommended patching strategy for Oracle Enterprise Manager. This information is intended to be a guideline for maintaining a patched and highly available EM environment and may need customization to accommodate requirements of an individual organization.

Enterprise Manager Components

Below is a list of the components that may require patching for an EM system.

Oracle Management Service (OMS)

The OMS is a web-based application that communicates with the Oracle Management Agents and Oracle Management Plug-ins to discover, monitor and manage targets as well as store the information in the Oracle Management Repository. It is also responsible for running the user interface for the Enterprise Manager Cloud Control Console.

Oracle WebLogic Server

The OMS application runs on top of Oracle WebLogic Server which is installed on each of the OMS servers.

Oracle Management Plug-ins

The core Enterprise Manager Cloud Control features for managing and monitoring the different Oracle components are now provided via separate components called plug-ins. The required plug-ins will vary by enterprise and according to the components that EM will manage.

Oracle Management Agent

The Oracle Management Agent is deployed on each host to be managed by an EM environment. It is responsible for managing and monitoring all of the targets on that host (including the host itself) and communicating all information to the Oracle Management Service.

Oracle Management Repository

The Oracle Management Repository is used for storing all of the data received from the Oracle Management Agents. It organizes the data so that the Oracle Management Service can retrieve it and display it in the Enterprise Manager Cloud Control Console

Define Business Requirements

Before a proper patching strategy can be defined, it is important to have specific details defined that may vary across companies. These details are part of defining the high availability requirements. This is an important task that

will help in determining the patching strategy and should be defined prior to the definition and documentation of a patching strategy. Defining the high availability requirements of the EM system involves the following:

1. Performing a business impact analysis which consists of categorizing the business processes based on the severity of the impact from an IT-related outage.
2. Identifying and categorizing the critical business processes in EM that have high availability requirements (i.e. monitoring of mission critical systems)
3. Calculating the cost of downtime (both planned and unplanned)
4. Defining the recovery time objective (RTO) and the recovery point objective (RPO). RTO is the maximum amount of time that EM could be down before the company suffers material losses. RPO is the maximum amount of data EM could lose before the company suffers material loses. (i.e. data loss)
5. Understanding the total cost of ownership (TCO) and the return on investment (ROI).

The Oracle Database High Availability Overview Guide provides a good explanation on this process. Once the above items are defined, it is easier to understand the required level of availability for the EM environment. For details on the High Availability levels for EM, refer to the Oracle Enterprise Manager Cloud Control Administrator's Guide.

Patching Strategy Overview

Patches are critical in order to maintain a healthy Enterprise Manager environment. Developing a proactive patch strategy will help in avoiding issues and allow administrators and users to take advantage of new technology and features. Patching is not a one-step process but involves a strategy around timing, testing, the actual patching steps and any possible recovery or fallback options. The list below details some of the tasks involved in developing proper patching strategies.

- Determine the patching strategy that covers the requirements of your organization
- Determine the appropriate timing
- Prepare for the change
- Incorporate sufficient testing

Types of Patches

Patch Sets

A patch set is a full release of the product and is applied via the upgrade process. It is a point release such as upgrading from release 12.1.0.4 to 12.1.0.5. It includes patches for all EM components including WLS and updates to the management repository data. A patch set release of Enterprise Manager could be released as often as every 9 months.

Patch Set Updates / Security Patch Updates (Critical Patch Updates)

Patch Set Updates (PSU) are cumulative patches containing critical recommended bug fixes and security fixes and usually contains updates to all EM components including WLS and the management repository. These patches are intended to be low-risk so they do not include fixes that require re-certification or configuration changes. For more details, please refer My Oracle Support note Patch Set Updates for Oracle Products (Doc ID 854428.1).

The Security Patch Updates (formerly known as Critical Patch Updates) are cumulative patches that limit the included bug fixes to security fixes only. Starting with Oracle Database version 12.1.0.1, Security Patch Updates will no longer be available. The PSU is Oracle's preferred proactive patching mechanism. Both of these patch types are released on a quarterly schedule: the Tuesday closest to the 17th of January, April, July and October.

One-off Patches

One-off patches are bug fixes provided as required for a single bug fix or a collection of bug fixes. They may also be created for customer specific security bug fixes. A one-off patch could also be a diagnostic patch that is created to help diagnose or verify a fix or collection of bug fixes. The recommendation is to apply the bundle patch (described below) and not apply one-off patches unless recommended by Oracle Support. Before applying a one-off patch:

- Make sure that the patch is approved by Oracle Support to work with the current EM release and that it is required to address a current issue/bug.

- Refer to the patch README to carefully set the ORACLE_HOME environment variable to the component that you patch. In some cases it will not be the OMS home (OMS_HOME), but maybe the middleware home (MW_HOME) depending on the patch in question.

Bundle Patches

In order to reduce the number of patches and to assist in the overall availability of the EM system, starting with version 12.1.0.3 Oracle is now releasing patch bundles for the following components:

- Management Agent version 12.1.0.3 and higher
- Cloud Control Plug-ins (both OMS-side and Agent-side)

These bundles will be released on a monthly basis and will contain the latest PSU and any critical one-off patch for that release (up to the cut off window for the patch creation). Each bundle patch will be cumulative for that particular release and will be marked as a "Recommended Patch" on a quarterly basis.

At this time, the bundle patch concept does not apply for the following components and one-off/PSU patches will still be created:

- Enterprise Manager Cloud Control 12.1.0.1 and 12.1.0.2(does not apply for any components prior to release 12.1.0.3, including the OMS, WLS, repository, agent and plug-ins)
- EM 12.1.0.3 Management Server (OMS servers), WLS and EM Repository
- Platform specific patches

For these components, the list of recommended patches can be found in EM under Enterprise / Provisioning and Patching / Patches & Updates. In the Patch Search box, click on "Recommended Patch Advisor". For details on the bundle patch release process, please refer to the My Oracle Support note Enterprise Manager 12.1.0.5.0 (PS4) Master Bundle Patch List (Doc ID 2038446.1).

Plug-in Patches

As mentioned above, Oracle uses plug-ins for managing and monitoring the different Oracle components. The plug-ins therefore may have patches that are released for one-off bug fixes as well as newer plug-in versions. It is important to note that a newer version of a particular plug-in may require a later patch set release of EM. The recommendation is to always apply the latest EM patch set which will not only provide the latest enhancements and bug fixes but will also support the latest plug-in versions. Note that if a plug-in requires a later version of EM, the EM tool itself will not know about the newer plug-in versions. Therefore, always apply the latest EM patch set in order to ensure knowledge of the latest plug-in updates.

Determine Patch List and Required Patching Steps

Although EM provides the ability to provision and patch the majority of an organization's applications and servers, at this point in time, it is not able to patch all of the components that make up EM itself. Therefore, the available patching options may vary for the different EM components and certain patches may require downtime for the entire EM environment.

The table below indicates downtime for the entire EM environment based on the level of availability implemented in the design and assuming application of a patch requiring downtime. For a complete description on the different EM high availability levels, please refer to Oracle Enterprise Manager Cloud Control Administrator's Guide.

TABLE 1. EM DOWNTIME BASED ON AVAILABILITY LEVEL

Component	Level 1	Level 2	Level 3	Level 4
WebLogic Server / OMS	YES	YES	LIMITED*	LIMITED*
Repository	YES	YES	NO	NO

Agent *NOTE: downtime only impacts the agent on that specific server and not the entire EM env.*	NO	NO	NO	NO

* A few patches are now able to be applied in a rolling fashion for the OMS allowing for higher availability when more than one OMS is installed. Also, patching can be orchestrated in such a way as to limit the downtime to the time it takes to apply the patches to the primary OMS.

Best Practice:

- The list of recommended patches for EM can be found in EM under Enterprise / Provisioning and Patching / Patches & Updates. In the Patch Search box, click on "Recommended Patch Advisor". Also, a note is updated quarterly on My Oracle Support with a list of recommended patches for and EM environment. Refer to Applying Enterprise Manger 12c Recommended Patches (Doc ID 1664074.1)
- Set a patch window appropriate to the defined high availability requirements of the EM environment
- Determine the patching procedures/process in advance that will meet the required RTO/RPO for EM.
- Organize the patches according to the component it applies to and the downtime requirements for that patch.

It is important to remember that the patching plan should include back-out steps for any patch as well as a good backup and recovery plan in the event that something should go wrong during a patching window. Each patch includes the back-out steps for that patch. For details on backing up EM, refer to Enterprise Manager Cloud Control Advanced Installation and Configuration Guide.

Planning

What timing works for your organization? It is important to note that some patching may occur out of cycle. For example, there may be a required patch for the database (i.e. security patch) that is not specifically required by EM. In such cases, patching of the EM repository may fall under this patch cycle but not be considered part of the standard EM patching window.

Monthly? This is probably too aggressive for any organization. A monthly patching schedule could be resource intensive as it would require a resource to spend a majority of their time during the month on preparing, testing and patching the test production systems. Once this is done, it would be time to start over again on the next set of patches.

Quarterly? A good strategy however it may not be feasible in some organizations due to resource availability. This timing may be appropriate for companies with smaller EM environments (100 agents or less) or specific company policies requiring more frequent patching.

Semi-annually? Probably the interval that provides the best balance between the TCO and keeping current on patches. This is the recommended patch window. With a semi-annual patch plan, both the test and production environments will be patched twice a year. This actually means patches are applied on a quarterly basis as patches are applied to the test environment first. (see sample table below).

Annually? For most environments, this will most likely be too long and they will find a need to stay more current on the bug fixes and newer plug-in updates.

Best practice:

- Setup a patch window based on patching the production EM environment semi-annually. This will mean patching the test system first and therefore will allow approximately 2 months of testing before application to production. Of course, this window can be shortened if 2 months is not required by moving the production patching window.

Sample Semi-Annual Patch Window

TABLE 2. SAMPLE SEMI-ANNUAL PATCH WINDOW

EM Env	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Test	X						X					
Production				X						X		

Prepare for the Change

Research the patches – understand what is changing, the patch application steps and any required pre or post steps. Oracle's patching options change as more and more patches are able to be applied online or in a rolling fashion. Be sure to leverage these patch application improvements.

Testing the list of required patches on a test EM environment will provide better guidelines as to the amount of downtime to expect (if any), the amount of time for the patching window which may or may not change the list of patches to apply and the exact steps involved in order to meet the required RTO. The test environment should be configured as close to the production system as possible so that the testing will more closely replicate that production environment. The most challenging issue is creating the "load" on the EM environment from the agents. One option for accomplishing this would include having a separate environment for all test and/or development systems. This allows for a staged patch implementation cycle and patches are well tested before affecting production monitoring. For companies that prefer to have all of their systems contained in a single EM environment, the EM test system may not have many agents connecting and therefore will not have the activity/load as the production EM.

Understand the patches that will be applied, the amount of risk or change that will be introduced into the environment and therefore, the amount of testing that should be performed on the test environment. There is a tradeoff between high availability and the overall time it takes to apply patches to an EM environment. For example, depending on the amount of downtime acceptable for your EM environment it may take less time to take the downtime and apply the patches to all OMS servers at the same time. If high availability is a concern, then of course always choose the online or rolling patch method which will therefore extend the time to complete the patching.

Best Practice:

- Understand the amount of change that the patch will introduce into the environment to determine the amount of testing required. This is determined by factors such as components that are being patched, the number of fixes in the patch and the type of patch. For example, understand if the patch contains only bug fixes or includes modified or new functionality. (i.e. an EM patch set will include more change than a simple one-off bug fix)

Testing

Testing patches before going live is critical which is why a test system for the EM environment is so important especially if the environment requires a higher level of availability to meet the required levels for RTO/RPO. Testing should not only check to see how the patch behaves during installation but also when rolled back. It is also important to define a test plan that would test for the all critical processes – technical and functional. It is recommended to define a list of test cases appropriate for that application or organization.

The table below provides some guidelines on the testing level for the different patch types. The application and rollback of the patches should be tested for all patch types. This may involve different levels of testing as described below.

- Bug Verification: If a patch is applied for a specific bug fix, then verify that it does fix that bug.
- Basic testing: This testing includes verifying the overall functionality of EM and/or the application. This would include running the EM Diagnostic Tool called EMDIAG before and after patching, making sure all components stop and start successfully and verifying the health of the EM components in EM after the patch application.
- Full testing: More testing should be involved in the patch set releases as these could include major changes for the EM application. It is important to check as much functionality and performance as possible. This level of testing would include running EMDIAG before and after patching, making sure all components stop and start

successfully, verifying the health of the EM components in EM after patch application, verifying the functionality of the following: notification system, reports, backups, provisioning and patching; verifying the application performance and performance of the job systems.

NOTE: See EMDIAG Troubleshooting Kits Master Index (Doc ID 421053.1) for more information on the EMDIAG tool kit. For more information on confirming the functionality of the EM environment, refer to the whitepaper Operational Considerations and Troubleshooting Oracle Enterprise Manager 12.1.0.4.

TABLE 3. EM PATCH TESTING

	Patch set	PSU/SPU	Bundle Patches	Plug-in patches	one-off patches
Install/Rollback	Yes				
Bug Verification	Where applicable and possible				
EM Admin Activities	Full	Basic	Basic	Basic	Specific for that bug
Application Function	Full	Basic	Basic	Basic	If Applicable

Best Practice:

- Maintain a copy of EM for test purposes (maybe one that hosts dev/test systems for the environment).
- Ensure the test system has the same patches as production prior to testing the new patches.
- Backup the environment before applying the patches. Refer to Oracle Enterprise Manager Cloud Control Administrator's Guide for details on backing up EM.
- Pre-Patch check: Run EMDIAG (see NOTE below) tests and verify the status of the EM components before applying patches. The whitepaper Operational Considerations and Troubleshooting Oracle Enterprise Manager 12.1.0.4 provides guidance for verifying the health of EM.
- Download the patches and apply to the test environment checking for any patch conflicts. If conflicts exit, request merge or overlay patches
- Post-Patch check: Run EMDIAG (see NOTE below) tests and verify the status of the EM components after applying patches. Create test alerts to test the notification system. Perform any necessary application related tests if applicable.
- Use the patch testing and patch apply details to decide the method for the patch application (high availability vs. patch window duration)
- Apply the patches to production repeating the pre and post patch checks.

NOTE: The EM Diagnostic Toolkit (EMDIAG) is a set of utilities that collect data from the OMS, Repository and Agents to assist in troubleshooting and maintenance. See EMDIAG Troubleshooting Kits Master Index (Doc ID 421053.1) for more information.

Example Patching Steps

This process does not cover the application of patch sets as those are done via the upgrade process which is well defined in Oracle's Upgrade Guide (i.e. 12.1.0.5 Upgrade Guide). The patching steps are broken down by component as a patch window may not always contain patches for all EM components. Note: This example assumes the EM environment was configured with the replicated storage solution and not with the deprecated standby domain solution.

1. Create list of patches required. A list of recommended patches is maintained quarterly on My Oracle Support. Refer to MOS note Applying Enterprise Manger 12c Recommended Patches (Doc ID 1664074.1) for more details. Note that if a special one-off patch was applied, it may conflict with a patch on this list but any conflict should have been discovered during the testing phase and therefore an overlay or merge patch added to the list to resolve the conflict.
2. Document each patch to apply and the corresponding patch application steps. If applying patches from the MOS note 1664074.1, then the patch apply steps are also detailed in this note.
3. Create a recovery plan and be sure to document the patch back out or rollback steps for each patch. Refer to the README file to determine steps for backing out each patch.
4. Organize and group the patches by component (i.e. db, oms, agent, etc). This is done in the MOS note 1664074.1 for you.
5. Download all patches and stage patches on servers
6. Within the categories above, group together according to the patch apply requirements (rolling vs. downtime)
7. Before patching begins, stop the standby for the repository database.
8. WebLogic patches should be included in the list of patches for the OMS servers
9. Backup the environment by taking a backup of the Oracle inventory location, Middleware home and instance home on each OMS server and either take a full backup or a restore point for the repository database.
10. Be sure to follow the patch application steps including any prerequisite checks. For agent patches, this will be the analyze mode in the EM patching tool and the –analyze option for the opatchauto command used to patch the OMS.
11. Follow the steps below when applying OMS, WLS and OMS plug-in patches. These steps are organized in a way to provide the highest uptime for EM.
    a. Execute all patch analyze steps prior to shutting down the OMS servers
    b. Execute the patch apply for the Bundle patches for the OMS server (PSU patch and plug-in bundle patch). This will provide the scripts required to apply the patch to each OMS server
    c. Shutdown all OMS servers
    d. Apply all patches to the primary OMS server. This will include running the scripts generated in step b above, all other OMS patches and WLS patches.
    e. Restart the primary OMS server but leave all other OMS servers down.
    f. Repeat step d above on all other OMS server
    g. Restart all additional OMS servers
12. Follow the steps below when applying Repository patches.
    Before applying patches to the repository database, if flashback database has been enabled, it is recommended to take a restore point to be used in the event that a recovery is required. Please refer to the Oracle Database Backup and Recovery User's Guide for further details on using flashback database and setting restore points.
    a. If the recovery on the standby repository database was not stopped in step 7 above, stop the recovery before applying patches to the primary repository database (if applicable).
    b. Apply the latest PSU to the standalone or RAC primary repository database as per the patch README instructions. Note that these patches can be applied in a rolling fashion so the database does not have to be shutdown.
    c. Apply any required one-off database patches.
    d. Execute all required post patch scripts for the repository patches.
    e. Once the primary database is patched, apply the PSU and any required one-off patches to the standby database if applicable.
    f. Restart the recovery process for the standby repository database.
13. Follow the steps below when applying Agent patches. For details on how to patch agents using EM, refer to the Oracle Enterprise Manager Cloud Control Administrator's Guide.
    a. Create a patch plan in EM containing all required agent patches for each patch in the agent patch list. This patch plan can contain patches for different agent components such as the agent bundle patch, any agent one-off patches and all agent plug-in patches. EM is able to determine the patches applicable to each agent during the analyze phase. This allows the same patch plan to be used for all agents.
    b. Select a list of agents to add into this patch plan. It is best to include a maximum of 200 agents per execution.
    c. Execute the analyze option in the patch plan before applying the patches and correct any issue found. If issues are found during the analyze phase, the plan is split into two plans. One plan will contain all of the failed targets and the other plan will contain all of the successful targets. The

successful plan can be executed while the failed plan can be reanalyzed, issues fixed and deployed separately.

d. Apply the patches to the agents.
e. Repeat the above steps for each group of agents.

If desired/required, test the disaster recovery site by performing a switch over to the standby site and confirming the functionality. Depending on the company's strategy/requirements, the systems can stay running there or a switchback can be performed. For details steps on how to switch over to the standby servers, refer to Enterprise Manager Cloud Control Advanced Installation and Configuration Guide

For any issues encountered during the patch application or found after patching the environment, a partial or full recovery of the environment may be required. Follow the defined back out plan.. If specific patches fail then they can be rolled back individually. For an entire environment restore, follow these high level steps: (for detailed steps, refer to the Enterprise Manager Cloud Control Advanced Installation and Configuration Guide)

- Restore the backup of each OMS server
- Restore the database to the point in time prior to the start of the patching via a flashback restore point or from the database backup.
- For agents, it is easier to just reinstall from a clone of another "good" agent.

Conclusion

Although patching an enterprise environment is one of the benefits obtained via Oracle Enterprise Manager Cloud Control, patching the "patching tool" is required to keep the tool current on fixes, enhancements and functionality. EM is an application that becomes more critical as its dependency grows for managing the most critical systems. Therefore, this implies that tasks such as patching need to be well thought out and planned. Developing the right patching strategy will ensure a smoother patching experience while adding to the higher availability and dependability of the environment.

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services

White Paper Title
October 2015
Author: [OPTIONAL]
Contributing Authors: [OPTIONAL]