Driving Database Patch Management with Oracle Enterprise Manager 11g

Configuration Management & Provisioning and Patch Automation Packs
Introduction

Change is inevitable, especially when it comes to management of IT environments. Today, with the widespread rise of worms and malicious code attacks against known vulnerabilities and unpatched systems, increasing concerns with governance and regulatory compliance standards like PCI, HIPAA, etc, and the resultant downtime and cost to the company in terms of resources, time, money and reputation, most organizations are investing heavily in patch management solutions and processes. Unfortunately existing efforts are very manual with sporadic infusion of tools that provide point solutions. The key to efficient patch management is the creation of a good Change Management process, which aims at automating all stages of the patching process.

The primary motive of a patching is to create a consistently configured environment that is secure against known vulnerabilities and product defects. Unfortunately, managing updates for all the databases is a complicated process, especially if it involves complex topologies such as clustered systems. Adding to this, there is an increasing demand from the business to provide higher levels of quality and more service uptime.

A typical Patch Management Process would involve the following phases:

- Identifying vulnerabilities and patches resolving it,
- Analyze the impact and prioritize,
- Test the patches across test environments and schedule rollout,
- Verify for successful application of patches
A Change Management process can not only minimize unplanned changes and reduce unplanned downtime, but also help in audit, compliance, and management reporting. Change Management process ensures effective handling of the patch management process. The four phases of a typical Change Management cycle are:

- **Advise:**
  Recommend changes to resolve vulnerabilities and issues detected based on the rich information about target configurations and the real time incident detection.

- **Plan:**
  Create a suitable plan of action that includes all systems and people involved in the change process.

- **Implement:**
  Deploy the changes in an automated way across the environment as per the planned schedule.

- **Verify:**
  Confirm that the changes were implemented properly on the right systems by the right people.

![Figure 1: Four phases of Change Management Process](image)
Oracle Enterprise Manager with its Configuration Management, and Provisioning and Patch Automation packs provides the essential components required to build and automate a Change Management system to manage the patch management process.

This white paper will outline Oracle Enterprise Manager’s four phased approach towards building a Change Management System for patch management and the various features that can be used to achieve it. We will use the example of patching of Oracle databases to illustrate this process.

**Figure 2: Change Management process in Patch Management**
Advise

In any enterprise the advisories can come from multiple sources - the vendor, from internal security officers and ISVs. The most trusted source for patch advisories happens to be the vendor. In 11g, My Oracle Support is integrated with Enterprise Manager. This integration provides database administrators with a single console that personalizes their support experience along with seamless management of their IT environments. The My Oracle Support integration offers Service Request (SR) Management for cutting down the problem resolution time, Knowledge Management for personalized in-context access to Oracle’s Knowledgebase and Patch Management to get proactive advisories on patches.

My Oracle Support within Enterprise Manager provides comprehensive Patch Recommendations for security and other recommended patches for the managed targets. The patch recommendations are computed daily based on the collected configuration of the targets against the metadata that is automatically downloaded from My Oracle Support.

Figure 3: Patch recommendations by My Oracle Support
The patch recommendations provide proactive alerts on targets affected by security patches (including quarterly Critical Patch Updates) and Oracle’s other patch recommendations like Patch Set Updates (PSUs), Clusterware Bundles and other patches. The dashboard view provides administrator with comprehensive view of vulnerability across their environment.

<table>
<thead>
<tr>
<th>Patch Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Figure 4</strong>: Dashboard view of vulnerabilities across the environment</td>
</tr>
</tbody>
</table>

Users can get detailed information on the patches like bugs fixed, patch readme, and associated Knowledge Base articles. Additionally, the patches are linked with Oracle Forums enabling users to review feedback from other users about the patches, including information on the impact and patch workarounds, if any. The users will also get information on the number of patch downloads and the download trend from the community. In cases of Critical Security Patches, the download trends can be used to gauge best practices across the community, some of which are guided by strict guidelines from governance standards.
Figure 5: Patch details, Download Trends and Oracle Forum

The integration also features Service Requests, through which the users could create/update/monitor Service requests from Enterprise Manager. Users can raise Service Requests in clicks and directly associate the configuration and required logs against incidents on the managed targets. The users review the SRs and directly include the prescribed patches into the Patch Management flow.

Figure 6: Users can monitor service requests and spawn patching from the updates
Plan

Planning phase involves creation of the list of identified patches and vulnerable targets. The patch list is then processed to make sure it can be rolled out across the environment. Typically, this process involves applying the patches on test environment and check for errors in the patch or conflicts against the Oracle Home. In large data centers the planning is typically done by a Lead Administrator, who has the authority to decide on the rollout process and schedule.

Users can consolidate the patches from the various sources like patch recommendations, service requests, and also simple patch search into Patch Plans. Patch Plans provide the user a way to accumulate multiple patches and applicable targets and proceed to rollout across the environments under a single downtime window.

**Figure 7: Create Patch Plans**

Users can associate the patches with targets (say development or QA or production) and do an upfront online validation without actually patching the environment. In this mode, patches are validated for the conflicts amongst the patches selected and with that of the
patches in the Oracle Home of the target based on the information of bugs fixed by the selected patches and of the patches in the Oracle Home inventory.

Upon conflicts users can place a merge patch request, if the patch is readily available it would be replaced directly or an automated merge request will be filed with Oracle. Since the process is completely automated, if there had been multiple merge requests for the same patches from various users, your request would be queued automatically thus reducing the wait time.

Figure 8: Patch Plan validation

The whole merge request process is automated removing the need for the user to raise a Service Request manually with all information and wait for it to be processed.

At the end of the validation process, the Plan would contain set of non-conflicting patches that can be deployed readily on the targets.

After the Patch Plan has been created, one would need to design the patch execution flow. Enterprise Manager comes with out of box Deployment Procedures that automate the application of patches and patchsets. In certain cases, Deployment Procedures would need to be customized to meet specific environmental needs.

The Deployment Procedures are best practices provided by Oracle Enterprise Manager for automated patching of various Oracle products like Oracle Database, Oracle Real Application Clusters, and Oracle Middleware. Users can create a copy of the procedure and customize to incorporate the additional steps required to complete the patching process in their environments. For example, a user integrates custom scripts to handle backup of the environment, or start/stop user cron jobs during their patching process.
Users can enable notifications from Deployment Procedures and integrate with the service desk applications like Remedy to monitor the patching process.

Since the list of patches that need to be applied and the targets to which they are applicable is established, the next step is to track these targets till they comply with the required patch level. The Compliance Management features of Enterprise Manager test the conformance of targets for security standards, and configuration and storage requirements. By continually testing systems, services, and targets, users are ensuring the best possible protection and performance for their systems. Enterprise Manager provides two types of compliance management: Policies and Policy Groups. Policies are rules against which managed entities are evaluated, while Policy Groups are a collection of policies that are managed as a set.

Users can utilize a User-defined Policy (UDP) to test if the desired patches have been applied to all targets. The following screenshot shows a User Defined Policy that tracks the existence of the patches on a continual basis. Policies can also be tied with the notification mechanisms for DBAs to be informed when a violation is detected.

Figure 9: User-defined Policy to test for desired patches on a database instance

1 For more details refer to Chapter 13 in Enterprise Manager Administration Guide.
A User-Defined Group (UDG) needs to be created to include the User-defined Policy for testing of applied patches. This Policy Group will be used to schedule periodic tests against target databases to ensure that they do not violate the required patch level.

![User-defined Group](image)

**Figure 10:** A User-defined Group that includes the applied patches policy

Users can set suitable intervals for Policy Group evaluation.

![Schedule Policy Group evaluation](image)

**Figure 11:** Schedule Policy Group evaluation

---

2 For more details refer to the [User-defined Policy and User-defined Group guide on OTN](https://otn.oracle.com).
Typically, the first evaluation of the Policy Group would return a very low or zero compliance score, but this should increase as more database instances are patched and brought in compliance with the required patch level.

![Policy Groups: Evaluation Results](image)

**Figure 12: First evaluation of the Policy Group**

Enterprise Manager Patch Plans integrate with Deployment Procedures, which automate the entire patching process including pre and post scripts, and the dictionary changes.

The user can select the Deployment Procedure either the out-of-box procedures or the customized procedures and roll out the patches to the targets either in Test or Development environment.
Figure 13: Patch Plan deployment

The Deployment Procedure supports pre-flight check mode – Analyze, through which the user can identify if the targets can be successfully patched.

Figure 14: Pre-flight check mode execution– Analyze

In Analyze mode, the Deployment Procedure runs a set of pre-requisite checks across the target to figure out if the sanity of the target like execution of Inventory sanity tests, OPatch checks, cluster ‘verify’ checks in case of Real Application Clusters (RAC), or execution of dummy SQL to check if dictionary changes could be made on the target.
Upon execution of the procedure in Analyze mode, the results for various tests and failure, if any can be reviewed from the Results tab. The DBA can follow the issues and its recommendations to make sure the target is prepared for the actual patching process.

<table>
<thead>
<tr>
<th>Status</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed</td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td></td>
</tr>
<tr>
<td>Passed</td>
<td></td>
</tr>
<tr>
<td>Error</td>
<td></td>
</tr>
</tbody>
</table>

1. Prerequisite checks: “Check patch readiness” and “Check applicability of the patch on the Oracle home” can be executed using a check option. In both cases the checks are interpreted as success but reported as failed below.
2. Some of the steps would be marked as “Failed” if there are “WARNING” errors. Review the warnings and ignore the step if it fails to continue with Patching.

Figure 15: Plan validation

Once the Analyze mode ran through successfully, pick up the Patch Plan and execute the Deployment Procedure in Deploy mode for the test environments.

Enterprise Manager's Application Quality Management features enables users to execute regression tests on the applications running on the test environment post the patching process.

Upon successful completion of the tests, the lead database administrators, as a best practice in their patch management process before the rollout, can pro-actively check for patchable environments in their enterprise through the EM Target Patchability Report. Through the report, the lead DBA can identify and remediate issues with targets that are marked unpatchable in the environment prior to the rollout schedule.
Figure 16: Target patchability report
Implement

In this phase, typically the user would proceed with the rollout to the production environments, over a period of time. Certain governance standards mandate the application of a patch within a stipulated time after release.

Once the rollout plan is decided, the individual DBAs can select the targets owned by them, against the patches decided and proceed to run them in Analyze mode before a week / few days of the actual maintenance window. Through this they could check and eliminate possible errors and ensure smooth rollout during the maintenance window.

Deployment Procedures support mass deployments by automating application of multiple patches to multiple targets simultaneously. The execution can be scheduled for future date, allowing the user to do automated deployments by selecting targets across the environment and schedule it during pre-scheduled maintenance windows.

Users can also enable notifications and get notified on the status of the execution, thus providing a truly automated unattended process.

Implement

Actions
- Reconcile configuration drifts
- Patch multiple servers and databases in a single window
- Track progress of patch deployment
- Rollback, if required

Features
- MOS Patch Plan
- Deployment Procedures

![Database Patching Deployment Procedure](image-url)

Figure 17: Database patching Deployment Procedure
Users who have access regulations to their environment can configure Deployment Procedure with secure authentication modules like SUDO. Power broker (prun) to enable user impersonation and execute the procedures as a local user.

The Deployment Procedures provides ability to monitor the execution in real-time, the user can drill down on a particular steps of the procedure and verify the execution from the associated logs.

![Job Activity](image)

**Figure 18: Deployment Procedure step logs**

In case of failures during the execution, the Deployment Procedure step can be verified and the procedure can be resumed by either retrying the failed step or ignoring the step based on the failure.

---

3 For more information on how to configure secure authentication with Deployment Procedure refer to section 'Infrastructure Requirements' in the document “Enterprise Manager Administrator’s Guide for Software and Server Provisioning and Patching”
Verify

This phase entails verifying the status of the Deployment Procedure, and ensuring that the right set of changes were made by the right set of people. The phase is supposed to serve IT auditors and Compliance officers so that they have ensured that right changes have been implemented.

Since User-defined Group has been scheduled for periodic evaluation, it will automatically update the compliance score and maintain trend history to track the overall progress of the patching effort.

Additionally, Enterprise Manager features such as, Application Configuration Console (ACC) and Configuration Change Console (CCC) can be leveraged to exercise greater control over the changes being made to the environment and their impact on stability and performance.

*Application Configuration Console (ACC)*\(^4\) provides the ability to collect, compare, and reconcile deep configuration information of complex systems, enabling:

- System alignment with gold standards, and
- Recovery from problems associated with drift

In the current context, Application Configuration Console can discover and compare database parameters, files in Oracle home, database network configuration, and database patch levels across two or more database instances\(^5\). If both target databases have been patched to the same level, the comparison will not flag any differences.

---

\(^4\) For additional details visit the [Application Configuration Console home page on OTN](https://otn.oracle.com).  
\(^5\) For a complete list of supported technologies visit the [Application Configuration Console Blueprints page on OTN](https://otn.oracle.com).
Figure 19: Comparison of database patch levels returns no differences

*Configuration Change Console (CCC)* provides breakthrough capabilities to automate real-time IT configuration Change Management through comprehensive, continuous detection, validation and reporting of authorized and unauthorized configuration change.

CCC can automatically detect and report unauthorized changes made to files and directories, processes, database objects, server resources, and more along with the user who initiated these changes.

In the current context, we can use CCC’s ability to track changes made to files in Oracle Home, database OS processes, and database objects. CCC can also correlate changes against a Change Management System, such as Remedy and flag the changes as “authorized” versus “unauthorized”. If the patch rollout has an RFC associated with it,

CCC can actually lookup that record to mark the change as “authorized”. This information can be viewed via a set of intuitive top-level dashboards that not only provide the ability to inspect any unauthorized changes but also provide a forensic trail of activities that led to this change.

---

6 For additional details visit the [Configuration Change Console home page on OTN](https://otn.oracle.com)
Figure 20: Real-time summary view of a detection policy performance against set thresholds
Summary and Conclusion

Oracle Enterprise Manager provides the components required to create Change Management processes for complex and time consuming activities like patch management. A Change Management process can not only minimize unplanned changes and reduce unplanned downtime, but also help in audit, compliance, and management reporting for database patch management.

Oracle Enterprise Manager Provisioning and Patch Automation Pack provides an end-to-end solution for automated provisioning, patching, and lifecycle management for entire system stacks including physical and virtual infrastructure, servers, databases, middleware and applications.

Oracle Enterprise Manager Configuration Management Pack provides the ability to track system inventory, compare against established baselines or gold standards, guard against configuration drift between environments, and validate compliance settings across the complete stack.

The benefits of these features are well acclaimed by customers. “Oracle Enterprise Manager helped to standardize our process for provisioning and patching in a completely automated, repeatable, and reliable manner. As a result, we have been able to reduce costs, increase staff productivity, and ensure compliance” states Raymond Payne, Principal Architect, Oracle Infrastructure, Johns Hopkins University Applied Physics Laboratory.

Together, these packs can help organizations achieve a positive 124% return on investment (ROI) with a payback period of 15 months\(^7\).

\(^7\) The Total Economic Impact™ Of Oracle Enterprise Manager Configuration Management Pack And Provisioning And Patch Automation Pack, Forrester research
Driving Database Patch Management
with Oracle Enterprise Manager 11g

April 2010
Author: Hari Prasanna Srinivasan and Adeesh Fulay
Contributing Authors: Sudip Datta

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

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

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

Copyright © 2010, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.