

An Oracle White Paper
April 2010

Oracle Enterprise Manager 11g Configuration Management Pack

*Delivering Open, Integrated and Application Aware
Configuration Management*

Disclaimer

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

Table of Content

Contents

Disclaimer	2
Table of Content	3
Executive Overview	4
Introduction	4
Simplify Management	5
Key Benefits	5
Key Features	6
Improving Level of Service	16
Key Benefits	16
Key Features	16
Enforcing Compliance	22
Configuration Change Console	23
Configuration Change Console Architecture	23
Key Features	24
Conclusion	32
Contact Us	33

Executive Overview

Oracle Enterprise Manager 11g Configuration Management Pack supports Oracle and Non-Oracle software enabling management of IT configurations through a broad and deep coverage of configuration items coupled with industry-leading, powerful automation capabilities. Businesses now depend so much on IT that IT is a key source of competitive advantage. But, with today's tough economic conditions, IT is being asked to do more with less. These two trends are converging on IT forcing them to deliver improved quality of service, better agility, lower risk, and lower operational costs. Now IT organizations have the tools and capabilities to succeed with Oracle Enterprise Manager 11g Configuration Management Pack—giving IT the pressure relief it so desperately needs.

Introduction

In order to better manage IT configurations, enterprises seek strategic solutions that enable comprehensive management of the IT stack across the lifecycle of enterprise applications. Configuration management lies at the heart of the solutions facilitating the day-to-day tasks of IT operations while providing C-level executives with the 360° operational and compliance views they require. Configuration management solutions should provide IT organizations deep, relevant information on widely deployed assets while being extensible and scalable as enterprises invest in new applications and businesses processes. IT organizations also require multiple modes of information collection such as agentless, low overhead periodic collections as well as agent-based real-time configuration change detection. Oracle Configuration Management Pack fulfills these strategic and tactical needs with unmatched capabilities for the Oracle software stack while offering competitive solutions for all IT configuration management needs.

This paper takes a three-pronged approach to Configuration Management.

- Simplifying the management of your IT infrastructure by providing asset discovery and tracking, managed baseline configurations and configuration policies
- Improving the level of service you provide your end users by managing the application lifecycle, configuration provisioning and extending applications management to custom and third-party applications
- Enforcing compliance with real-time change detection for files, database objects, users and processes, and detecting unauthorized and authorized changes

Configuration Management Benefits

Simplify Management	Improve Service	Enforce Compliance
<ul style="list-style-type: none"> • Automate discovery of assets • Control configuration drift • Configuration item search and reporting • Configuration policies for security and best practices 	<ul style="list-style-type: none"> • Manage configurations across the deployment lifecycle • Manage the application stack configuration • Gain visibility into changes • Accelerate cross-tier root-cause analysis to reduce unplanned downtime 	<ul style="list-style-type: none"> • Manage configuration compliance with automated IT controls • Control unauthorized changes • Meet IT compliance with out-of-box policy frameworks and drill-down reports

Simplify Management

Oracle Enterprise Manager 11g Configuration Management Pack forms the centerpiece of Enterprise Manager’s ability to manage assets, configurations, compliance and automate IT processes. It captures and centralizes the information about all hardware and software resources in the enterprise, thereby facilitating the diagnosis of problems, manage configuration drift through comparison, automation of processes and compliance with regulatory and industry standards like Sarbanes-Oxley and ITIL. The proactive evaluation of configuration against best practices, aided by policy-based exception management and comprehensive reporting, ensure a more efficient use of IT resources with demonstrable ROI, faster problem resolution and an improved quality of service.

Key Benefits

- ***Discovery and asset tracking***

Discover and track all IT assets within the data center. Search, report and find assets with specific custom attributes or configuration properties. Reduce exposure by ensuring patching and security settings are in compliance with your best practices.

- ***Manage configuration complexities***

The Pack provides a real-time or near-real-time view of configuration items, services and their dependencies within and across each other. Manage configuration drift through comparison with “gold configurations” and saved baselines. Enable the tracking, analysis and reporting of configurations while capturing configuration data that is used for the administration of the entire change management process, including change automation and active system diagnostics.

- ***Reduce Cost of Achieving Compliance***

Automate security assessments using policy and policy groups for detection of critical security vulnerabilities and compliance to best practice standards.

- ***Managing unplanned downtime: Faster problem resolution and root cause analysis***

Detect, document, alert and continuously maintain system configuration “shift and drift” resulting from planned and unplanned events. Reduce the risks involved in rolling out changes to production environments by identifying the impact of changes on deployed applications and users. Enable faster mean-time-to-repair through root cause analysis by isolating and correlating problems to the exact infrastructure or application component that is causing failure and by auditing change history for all targets and parameters.

Key Features

- ***Automated Centralized Inventory Tracking and Configuration Baselineing***

For years, IT departments have relied upon the knowledge of key individuals who kept track of all the software and hardware assets in documents and spreadsheets. As businesses expand or get more complicated, these manual methods are no longer viable from a quality of service standpoint. A centralized tool to track the assets becomes imperative.

The Oracle Configuration Management Pack collects deep configuration information about hardware and software components across the enterprise.

This information includes:

- Hardware (CPU, memory, storage, network, and so forth)
- Operating system packages, patches and kernel parameter settings
- Oracle software (operating system, database, middleware and applications) installed including interim patches, patch sets and other configuration settings, components
- Systems, Services and Groups
- Topologies
- Third-party software including, databases like SQL Server and DB2, storage like NetApp and EMC, networking solutions like Juniper and Cisco and middleware like IBM WebSphere

The configurations are automatically collected at regular intervals and stored in Oracle Enterprise Manager CMDB. Ad hoc collections are also supported and the configuration can be saved as a baseline for configuration comparison. Oracle Enterprise Manager offers a comprehensive view of all heterogeneous components in a data center from a central console. For example, the snapshot below shows a view of all Oracle Database installations in an enterprise.

Deployments Summary
View Database Installations

Software Targets Without Inventory 31 of 332 Collection Problems 7

Database Installations	Targets	Installations	Interim Patches Applied
Oracle Database 10g 10.1.0.2.0	0	3	No
Oracle Database 10g 10.1.0.3.0	6	13	Yes
Oracle Database 10g 10.1.0.3.1	1	1	No
Oracle Database 10g 10.1.0.4.0	13	16	Yes
Oracle Database 10g 10.1.0.5.0	20	22	No
Oracle Database 10g 10.2.0.1.0	16	19	Yes
Oracle Database 10g 10.2.0.2.0	14	3	No
Oracle8i Server 8.1.6.3.1	22	7	No
Oracle8i Server 8.1.7.0.0	0	1	No
Oracle8i Server 8.1.7.2.0	7	1	No
Oracle8i Server 8.1.7.4.0	60	37	No
Oracle9i 9.0.1.4.0	0	1	No
Oracle9i 9.0.1.5.0	6	5	No
Oracle9i 9.2.0.1.0	16	12	Yes
Oracle9i 9.2.0.4.0	30	24	Yes
Oracle9i 9.2.0.5.0	28	19	Yes
Oracle9i 9.2.0.6.0	48	53	Yes
Oracle9i 9.2.0.7.0	14	11	No

Figure 1, Deployment Summary view of Oracle Database Installations

The Client System Analyzer (CSA) functionality collects and analyzes data from Windows client machines such as desktops and laptops. Using an agentless technology, CSA uploads client data such as hardware, software, and OS versions and configurations, and compares it against reference configurations to verify if the client is configured as desired.

- **Ad hoc Search and Analysis**

Oracle Enterprise Manager possesses the ability to search for specific configuration values across all targets to verify drift from a gold standard. This can help in finding out if problem configurations are in use. Out-of-box searches can determine:

- Which servers have a particular version of a product installed
- Which Oracle installations are missing a particular patch or a patch set
- Which Oracle Databases have a particular init.ora parameter set
- Which Oracle Databases are using a particular feature, say, partitioning
- Which hosts have a specific kernel parameter value set
- Which hosts have a specific operating system patch installed

Oracle Enterprise Manager schema definition is published and is extensible to accommodate custom search and reporting.

- **Configuration Comparison**

Oracle Enterprise Manager also provides tools for comparing systems enterprise-wide in great detail, allowing an administrator to quickly and easily pinpoint any potential differences. The comparison spans the entire stack from the hardware to the application. This helps to keep systems synchronized and to reduce configuration drift. It also simplifies investigations into why systems that are presumed to be identical may behave differently, for example the nodes in a RAC cluster.

Administrators often need to create new systems that are equivalent in performance to existing systems. One way to do this is to capture point in time information for an existing system. This information can then be used as a blueprint for creating new systems. The Oracle Configuration Management Pack allows users to easily capture, store and view such information. Configuration comparison is extremely useful in change management. By comparing configuration baselines before and after a change or patch is applied, an administrator can verify that all configuration changes introduced as a result of the patch were planned and expected.

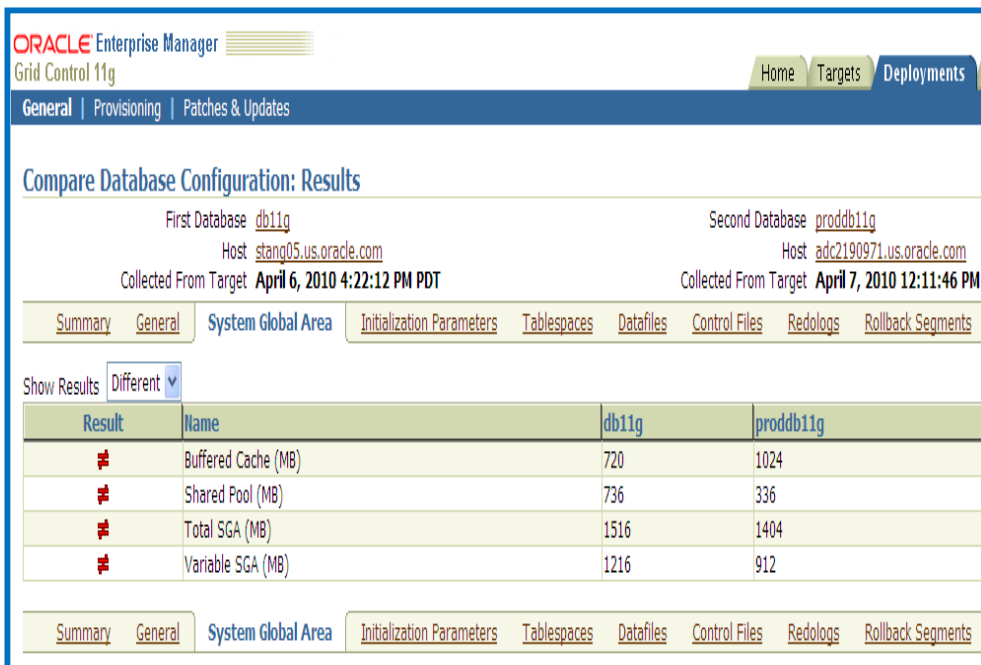


Figure 2, Comparison of Oracle Database Parameters Between Two Database Instances

The scheduled comparison between selected multiple (1-n) targets and gold configuration can be against reference configuration, a saved configuration baseline or a live configuration. Comparison results can be saved to a file for further analysis.

- **Configuration Updates**

A key feature of a configuration management solution is to allow for configuration updates across one or more targets. Configuration compare identifies configuration drift and the configuration update feature allows for remediation of the drift.

Oracle Enterprise Manager allows for viewing database initialization parameters and

application of updates of these parameters to multiple targets with a single request. Initialization parameters can be set to particular values to initialize many of the memory and process settings of an Oracle instance.

For example, by default, the PMON process registers service information with its local listener on the default local address of TCP/IP port 1521. To ensure the listener configuration is synchronized with the database configuration, the protocol address of the listener needs to be specified in the listener.ora file and the location of the listener in the initialization parameter file. Some customers have a requirement to use an alias for the location instead of using hard coded file location parameters. Using the init parameter configuration update feature, customers can point to the initialization parameter LOCAL_LISTENER=listener_alias across all database instances with one command.

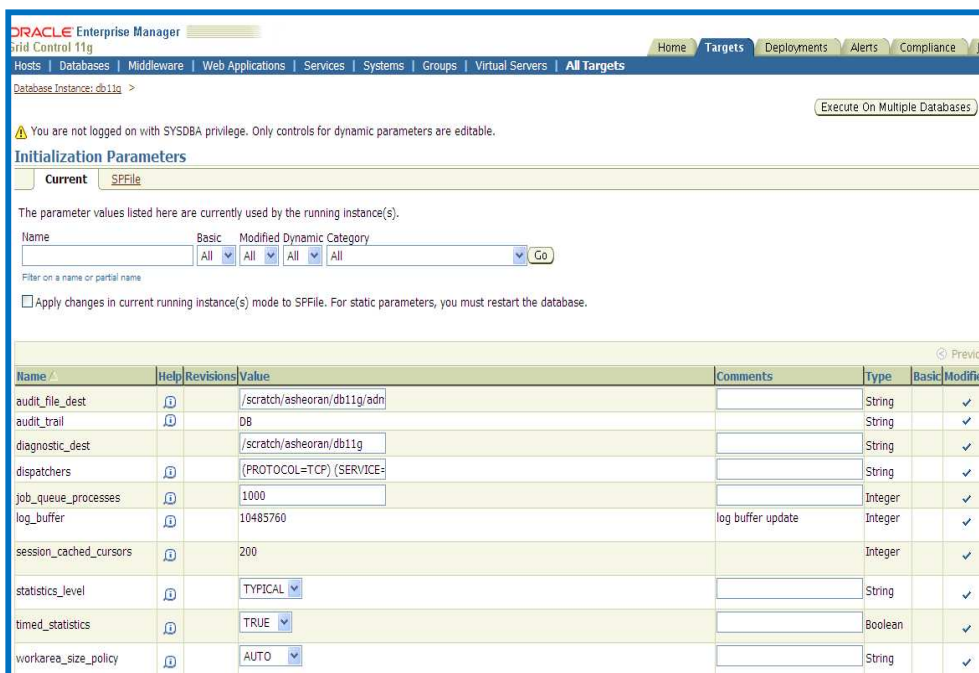


Figure 3, Configuration Update of Database Initialization Parameters

The Configuration Management solution discovers and collects hundreds of configuration parameters. However, not all configuration parameters are automatically discovered. For example, ITIL requires the tracking of CI lifecycle status from one state to another, such as *development*, *test*, and *production*. For non-discoverable parameters, Enterprise Manager allows for user-entered properties for each CI.

These target properties are optional descriptive attributes that can be associated with any target. Properties include:

- o Comment
- o Line of Business: Business Unit
- o Deployment Type: CI Status- Development, Test, Production, Withdrawn, etc.

- Location
- Contact/Owner

Target properties extend the search capabilities of Oracle Enterprise Manager by allowing administrators to use the aforementioned property values as search parameters.



Figure 4, Target Properties as Search Parameters

- **Configuration History and Tracking**

Administrators are faced with situations where a system that once worked well is suddenly not performing at an acceptable level. Did someone make a change to a configuration parameter? Apply an operating system patch? Remove memory? Trying to determine the exact change responsible for the decrease in system performance could take hours if the administrator had to go through each of the possible scenarios by hand. Oracle Enterprise Manager makes it simple by tracking all changes to hardware and software installations and configurations across multiple tiers.

This makes it quick and easy for the administrator to view changes that have been made since the last time the machine was functioning appropriately, and apply the appropriate solution to get the system back to an acceptable level.

This feature is critical in managing compliance, since it facilitates “who changed, what, when and why” analysis

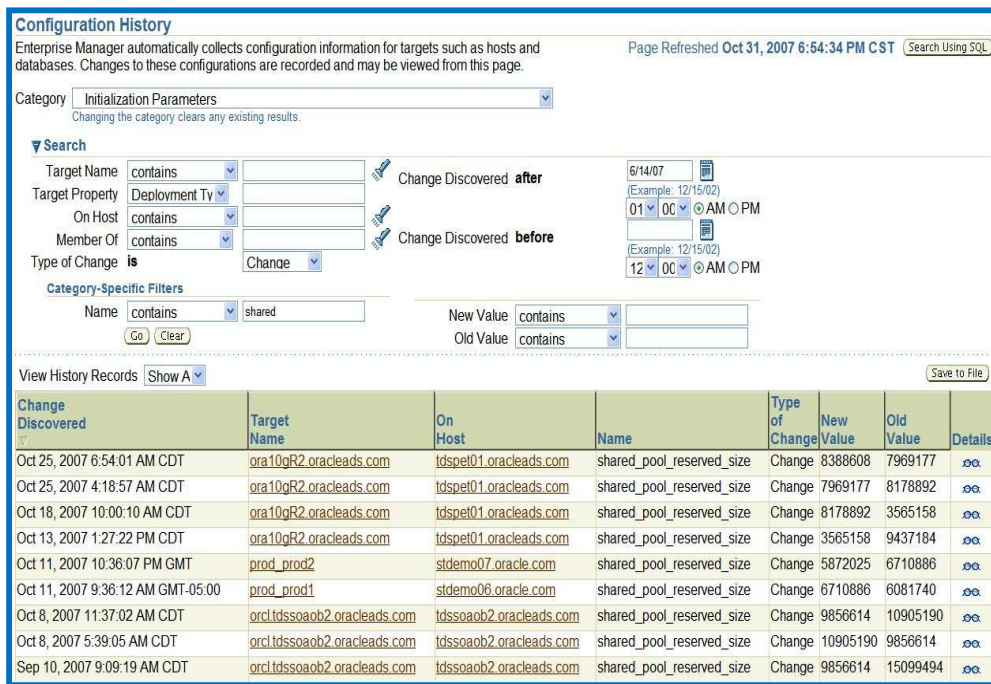


Figure 5, Viewing Change History

One of the key benefits of a true configuration management solution is the ability to manage unplanned downtime through impact analysis and root cause analysis. By capturing associations and relationships between configuration items, services and systems and displaying the topology in a chart allows for easy “what is affected, what is impacted” analysis. The topological view not only visually indicates the impact of a single CI on a specific service availability and resulting impact on overall business service availability, but also allows for drilling into specific configurations to view the out of band parameters.

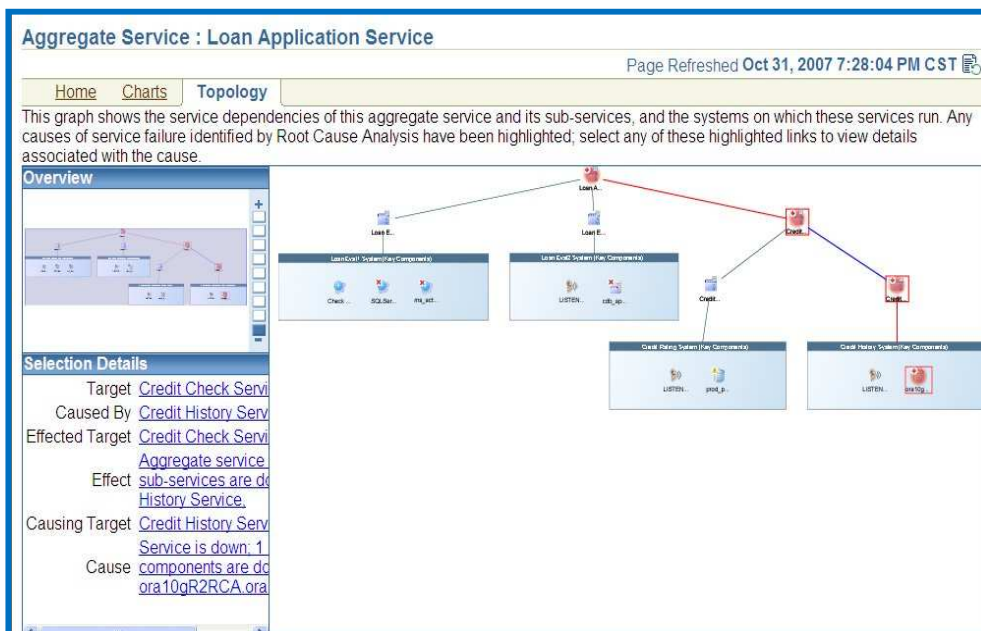


Figure 6, Topology View: Configuration and Service Dependencies

- **Out-of-Box Best Practice and User Defined Policies**

Oracle Enterprise Manager ships with more than 250 best practices policies in the areas of security, configuration, and storage. Policies help in continuous security assessment by automatically detecting critical security vulnerabilities.

Policies are effective in managing configuration drift (through installation of patches, adding files and directories, changing settings and ports, editing its dependencies, and so forth) by continually auditing against prescribed configurations.

This drift is tracked so that administrators know when they are happening, what changes are acceptable, and what changes must be corrected. This level of security and compliance, through proactive auditing and enforcement, is necessary to keep control in the continual flux that defines most of today’s data centers. Policies can be scheduled and applied across targets. Example policies include:

- o Database SPFILE not used
- o Unchanged default passwords
- o Insufficient number of Control Files
- o Detect open host ports

Oracle Enterprise Manager tracks violations of these policies in a manner similar to performance metrics. Notification rules can be applied and corrective actions can be assigned. For example, if well-known usernames/passwords are present in a database, a corrective action can be defined to automatically disable that account.

Compliance reports that denote the compliance score for the targets over a period of time supplement proactive enforcement of policies. It is possible to inspect the compliance score and drill down at each target level to detect the violations and the possible impact. Integration with problem ticketing solutions allow for policy violation information to be automatically sent without the need for manual intervention.

The screenshot shows the Oracle Enterprise Manager interface for the Policies Library. It includes a search bar and a table of policies. The table has the following columns: Select Policy, Severity, Category, Type, Description, Owner, Used in Monitoring Templates, and Used by Targets. The table lists various security policies related to database access and user groups.

Select Policy	Severity	Category	Type	Description	Owner	Used in Monitoring Templates	Used by Targets
<input type="checkbox"/> Domain Users' Group Member of local 'Users' Group	Warning	Security	Database Instance	Ensures domain server local Users group does not have Domain Users group	<SYSTEM>	1	2
<input type="checkbox"/> Access to % CATALOG_% Roles	Critical	Security	Database Instance	Ensure grant of %_CATALOG_% is restricted	<SYSTEM>	0	0
<input type="checkbox"/> Access to ALL_SOURCE View	Informational	Security	Database Instance	Ensures restricted access to ALL_SOURCE view	<SYSTEM>	0	0
<input type="checkbox"/> Access to DBA_* Views	Warning	Security	Database Instance	Ensures Select privilege is never granted to any DBA_* view	<SYSTEM>	1	2
<input type="checkbox"/> Access to DBA_ROLES View	Informational	Security	Database Instance	Ensures restricted access to DBA_ROLES view	<SYSTEM>	0	0
<input type="checkbox"/> Access to DBA_ROLE_PRIVS View	Informational	Security	Database Instance	Ensures restricted access to DBA_ROLE_PRIVS view	<SYSTEM>	0	0
<input type="checkbox"/> Access to DBA_SYS_PRIVS View	Informational	Security	Database Instance	Ensures restricted access to DBA_SYS_PRIVS view	<SYSTEM>	0	0
<input type="checkbox"/> Access to DBA_TAB_PRIVS View	Informational	Security	Database Instance	Ensures restricted access to DBA_TAB_PRIVS view	<SYSTEM>	0	0
<input type="checkbox"/> Access to DBA_USERS View	Informational	Security	Database Instance	Ensures restricted access to DBA_USERS view	<SYSTEM>	0	0
<input type="checkbox"/> Access to ROLE_ROLE_PRIVS View	Informational	Security	Database Instance	Ensures restricted access to ROLE_ROLE_PRIVS view	<SYSTEM>	0	0
<input type="checkbox"/> Access to STATSPACT Table	Informational	Security	Database	Ensures restricted access to STATSPACT table	<SYSTEM>	0	0

Figure 7, Example of Rich Out-of-Box Policy Library

As an extension of the out-of-box policies, customers can also create custom policies or “User Defined Policies” (or UDP) with the User Defined Policy wizard. Policies can also be grouped into User Defined Policy Groups providing the flexibility to define and group specific best practices for your IT infrastructure.

A policy tests data retrieved from a query performed against the Oracle Management Repository. A policy rule is a conditional expression that tests values from a target against a condition, for example, verifying that database profile limits are set as expected. A policy is said to be compliant if it is determined that the managed targets do, in fact, meet the desired state; that is, the test of the policy failed to identify any violations. Otherwise, a policy is said to be non-compliant when it has one or more policy violations.

To create a UDP, you must identify the name of the policy, data that is to be evaluated, the policy rule test (optionally parameterized) that is used to test the current state of the data and what, if any, default parameter values should be substituted into the test.

Upon creation, the policy is automatically stored in the Policy Library and is available to be viewed, incorporated into User Defined Groups, and associated with targets.

- ***Compliance Dashboards and Policy Groups***

Policy Group compliance dashboards enable administrators and CIO’s to get at-a-glance views on how their systems are complying with security best practices specified in their environment. Increasing regulatory compliance demands that IT systems are secure and have not been compromised. Ensuring that IT systems are behaving in line with security best practices is critical for any IT shop. Administrators define Policy Groups (a collection of security and configuration policies) against which each selected target is evaluated. Policy Groups are out-of-box best practices collections of policies for security, configuration management. Validated configurations can be mapped to industry standards like CIS and Cobit.

The evaluation results are converted into compliance scores (based on a weighted average) and the overall scores can be presented in the Compliance Dashboard. The dashboard presents summaries of key indicators, with ability to drilldown to details, allowing users to continuously monitor and verify their compliance posture. Support for trend analysis provides the ability to track progress towards compliance over time for the entire IT environment.

Exceptions and violations can be remediated to bring systems back into compliance with policy groups.

Out-of-box Policy Groups include security best practices for Oracle Database, Oracle Real Application Clusters (RAC), and Oracle Listener.



Figure 8, Secure Configuration for Oracle Database Policy Group

- **Critical Patch Advisory**

The Critical Patch Advisory alerts users to critical patches issued by Oracle and immediately identifies those systems across the enterprise that may require the new critical patch. The Critical Patch Advisory also supports an offline mode for data centers that lack connection to the Internet. The Critical Patch Advisory can automatically assess all targets for violations, report deviations and offer multiple remediation paths for fixing a particular vulnerability.

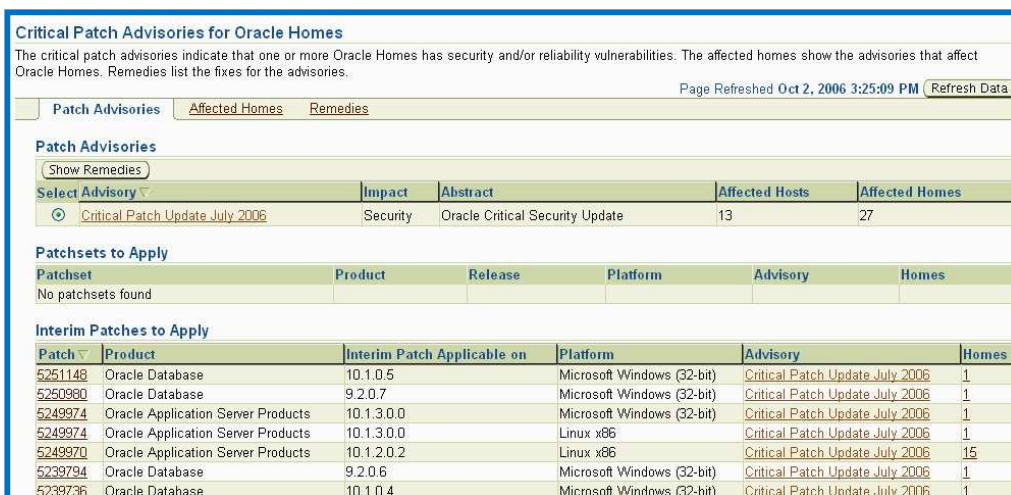


Figure 9, Critical Patch Advisory for Detecting Security Patch Violations

- **Configuration Reporting**

Oracle Enterprise Manager provides ready-to-use reports on hardware and software configurations and for compliance. Information Publisher, Enterprise Manager's powerful reporting framework, is pre-installed and ready to use and comes with a comprehensive library of predefined out-of-box reports. Standard reports include Hardware Summary, Operating System Summary, Oracle Database Configuration Summary, Affected Oracle Homes, Most Common Policy Violations, Policy Violations History, and Compliance Evaluation Summary etc.

Information Publisher also provides the ability to easily create customized reports, as well as create new reports using an intuitive graphical user interface. These HTML-based reports can be viewed interactively, generated on a schedule, and sent to selected recipients via e-mail. Additionally, reports can be shared among Oracle Enterprise Manager administrators and made available to non-credentialed users via the Enterprise Manager Reporting website.

- **Integrated Support Experience**

My Oracle Support is integrated with Oracle Enterprise Manager providing Database and System administrators a unified systems management and support experience. This integration provides a single console that personalizes the support experience along with seamless management of 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 provide proactive advisories on patches.

In addition to the My Oracle Support Integration, Oracle Enterprise Manager 11g will maintain a central repository for all your configurations. Configuration Information can be uploaded to Oracle from Oracle Enterprise Manager 11g by a function call the Harvester. This function eliminates the need to deploy the Oracle Configuration Manager on the hosts you want to manage with My Oracle Support.

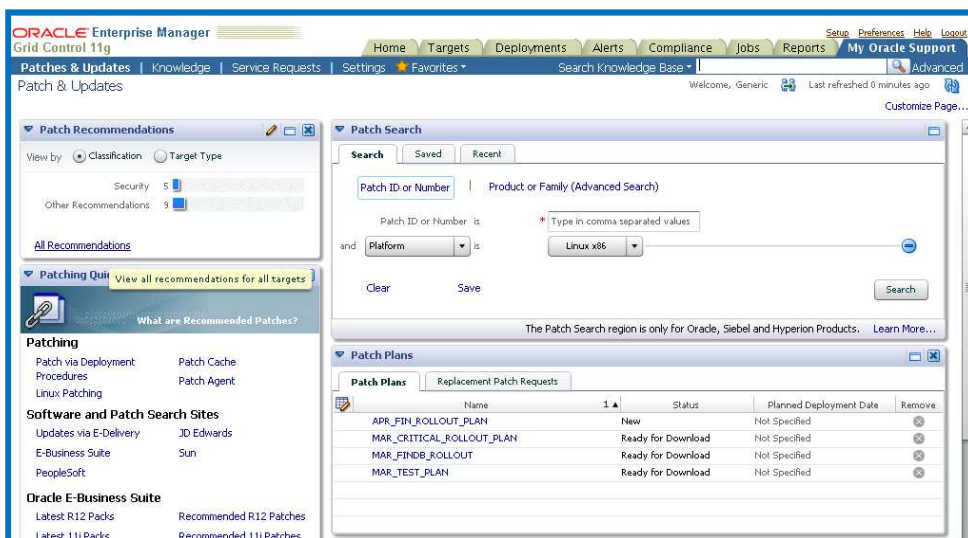


Figure 10, My Oracle Support integration with Oracle Enterprise Manager 11g

Improving Level of Service

As IT infrastructures continue to expand configuration management has become one of the most critical components of day-to-day IT operations. Simply put, failure to effectively control application and system architecture erodes the value of technology investments. To address this need for control, Oracle Configuration Management Pack includes a feature set called Application Configuration Console that is designed for the specific needs of IT infrastructure teams within large enterprises. These teams require a comprehensive solution for managing the application infrastructure underlying their mission-critical applications — the multi-tiered, distributed architecture that includes application servers, Web servers, databases and middleware. This environment typically includes tens of thousands of configuration properties that need to be set, tuned and controlled for the infrastructure to work reliably across all environments, geographies and software assets.

Application Configuration Console provides IT infrastructure teams with an automated “gold master” approach to application infrastructure configuration management that enables smooth delivery and support of mission-critical business applications. Through use of the capabilities, IT infrastructure personnel can capture the current state of configuration settings for IT assets, monitor them for changes, and automate processes for provisioning changes as well as setting up new environments throughout the application lifecycle — from development to testing and into production.

Key Benefits

- ***Manage the application infrastructure***

Improve IT productivity through automating routine tasks associated with building, managing, changing, troubleshooting, provisioning and auditing the application infrastructure that can consume up to 75% of an IT team’s time.

- ***Accelerate time-to value for new applications***

Accelerate the time-to value of new applications, migrations and upgrades by dramatically reducing the configuration errors and complexity that contribute to application downtime.

- ***Increase application uptime***

Enhance application uptime and quality through rigorous control of configuration consistency across all environments.

Key Features

- ***Centralized Application Infrastructure Configuration Data Repository***

At the core of Application Configuration Console is a centralized configuration data repository that stores fine-grained configuration settings for all managed application infrastructure assets. Data is automatically collected at an individual property level via an agentless, deep-dive approach using out-of box signatures for more than 100

software assets, providing the foundation for change tracking, audit reporting and versioning/rollback.

The software includes a built-in wizard that allows users to rapidly create new signatures for extracting configuration data from nearly any packaged or custom software component. Application Configuration Console also enables users to create standardized templates of configuration settings that can be used to quickly create and deploy new instances of application infrastructure assets.

- **Flexible, User-Defined Views**

Application Configuration Console's user-defined views provide IT with detailed insight into large, complex infrastructures by allowing them to view visual representations of managed assets across multiple environments and drill down into configuration details as needed. Users can easily customize their views to highlight only those configuration details for which they are responsible (for example, application servers only or assets by specific location).

In the following example a customer can configure their view for a specific technology such as viewing and managing all their databases, E-Business Suites, Oracle Application Server or Weblogic. Or define a service such as Employee Portal and define the application stack across the different development, test and production centers.

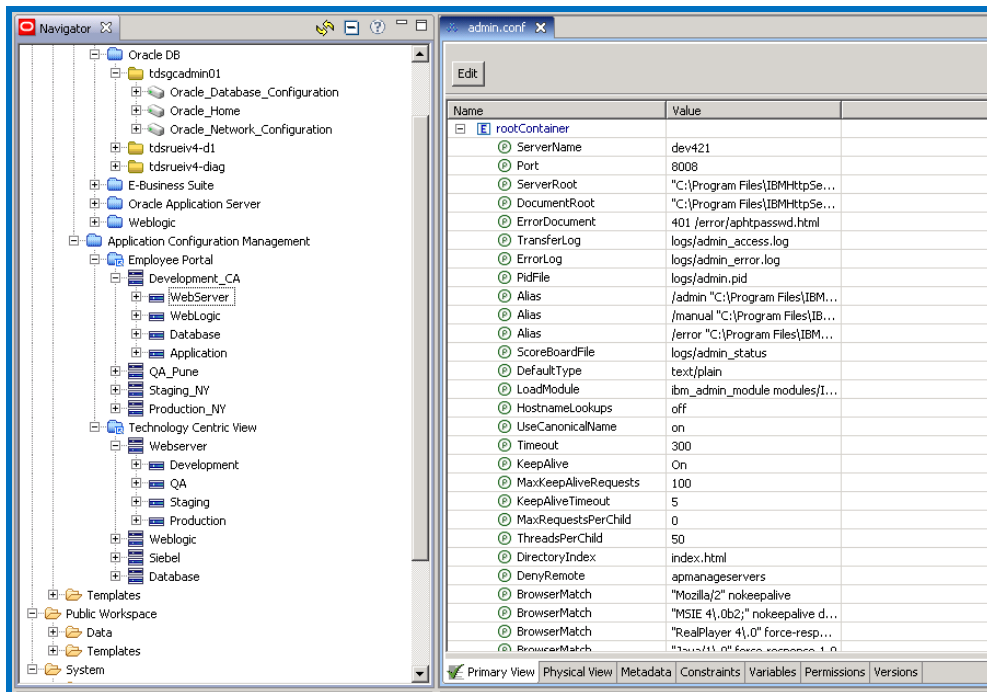


Figure 11, Flexible, user defined views

- **Powerful “Compare” Feature**

Application Configuration Console’s unique compare feature enables users to instantly compare fine-grained configuration setting differences across time, among similar assets or among entire environments by intelligently identifying only unexpected differences. This powerful capability enables users to quickly pinpoint the “needle in a haystack” differences that would otherwise take hours or days to find. Detailed change detection and analysis can be set to execute on a pre-determined schedule or an ad hoc basis.

You can select if you want to compare a single asset type or compare the application stack across different IT Centers or the deployment lifecycle (Development – Production).

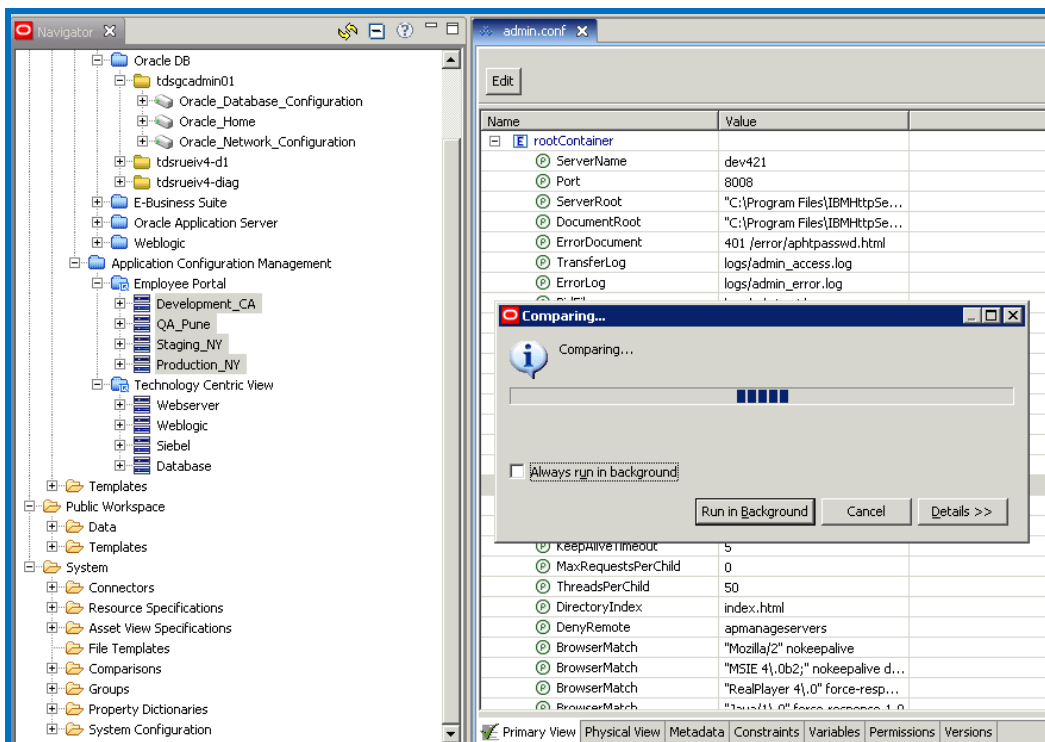


Figure 12, Comparing the application stack across IT centers

Ability to eliminate known differences and compare fine-grained configuration settings, across time, among like assets or across entire environments by intelligently identifying only unexpected differences

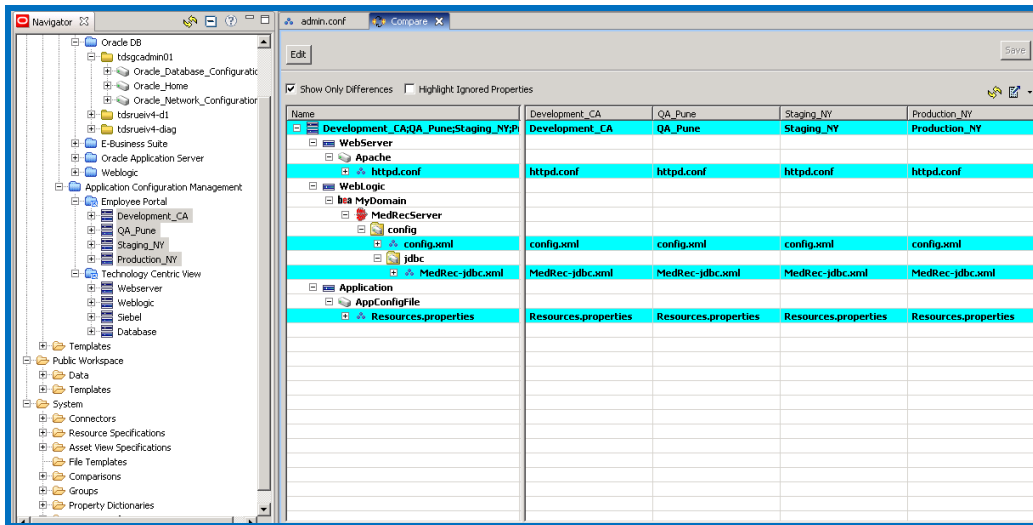


Figure 13, Only meaningful differences are displayed

- **Change Tracking**

Application Configuration Console facilitates a centralized approach to change tracking by maintaining a running record of changes across application environments. IT can create and enforce policies for managing configuration changes and automatically capture and catalog every change as a separate version for simplified comparison and reporting. Versions show who changed what, when, and provide a fast means of rollback in the event of system downtime.

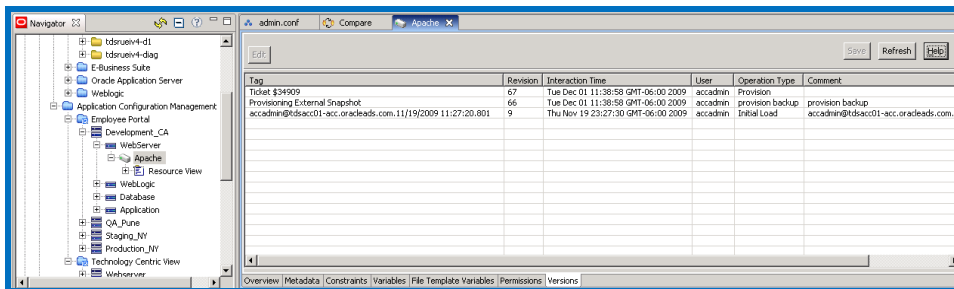


Figure 14, Versions of all changes maintained for roll-back if needed

- **Configuration Provisioning**

Using “gold master” configuration templates, Application Configuration Console can instantly provision application configuration settings to a virtually unlimited number of target host systems. This can be done for any single element in the application infrastructure or across the entire software stack. Additionally, Application Configuration Console can provision configuration setting changes at an extremely fine-grained level when only specific anomalies need to be corrected across distributed environments. Prior to provisioning changes, users can confirm accuracy

by comparing proposed changes in Application Configuration Console's data model to the live environment.

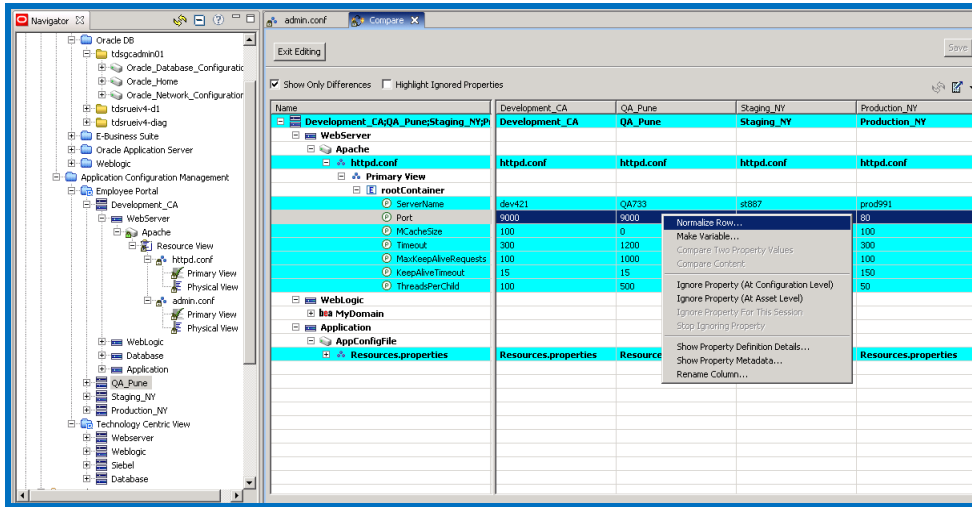


Figure 15, Provisioning a single change by Normalizing Row

- **Alerts**

Application Configuration Console's sophisticated tracking and comparison alerts allow IT to become immediately aware of differences detected based on scheduled events. IT also gains insight into which users resolve specific alerts and associated resolution details. Users can set one of several states for alerts to track progress as well as associate alerts to an external ticketing application for closed-loop change compliance.

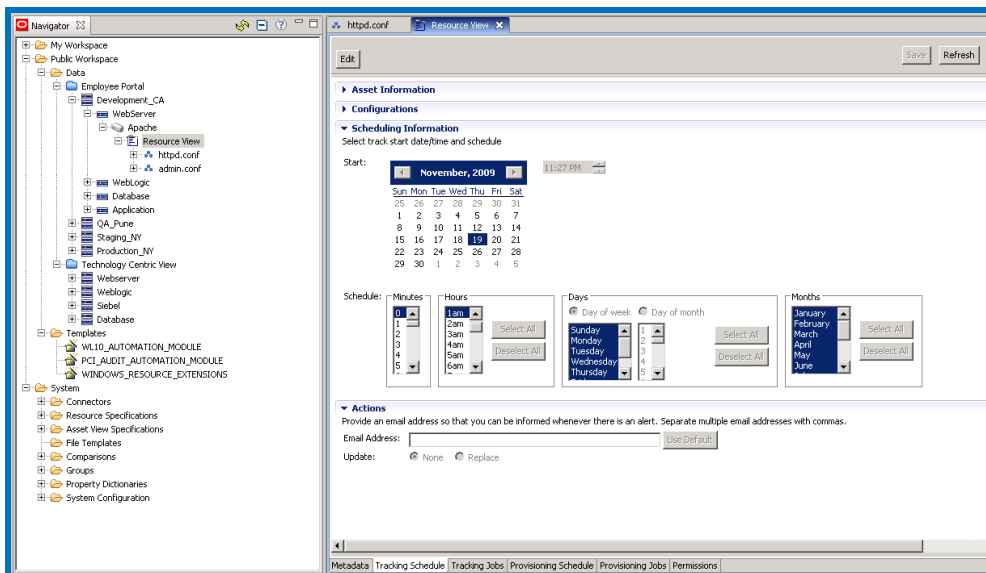


Figure 16, Scheduling comparison and alerts

- **Reporting**

The foundation of Application Configuration Console's powerful reporting capabilities is a dashboard that highlights total assets and configurations under management, recent activity, change volume and change compliance and provides easy access to more than a dozen detailed reports related to Audit, Activity, Planning, Comparison, Administration and System categories. Reports can be generated automatically and saved as PDFs, distributed via e-mail and scheduled to run on a recurring basis.

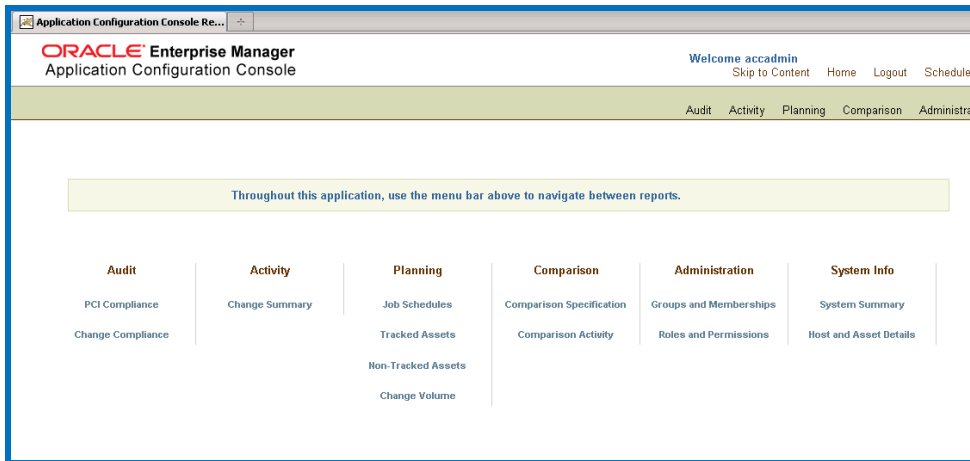


Figure 17, Rich suite of reporting options

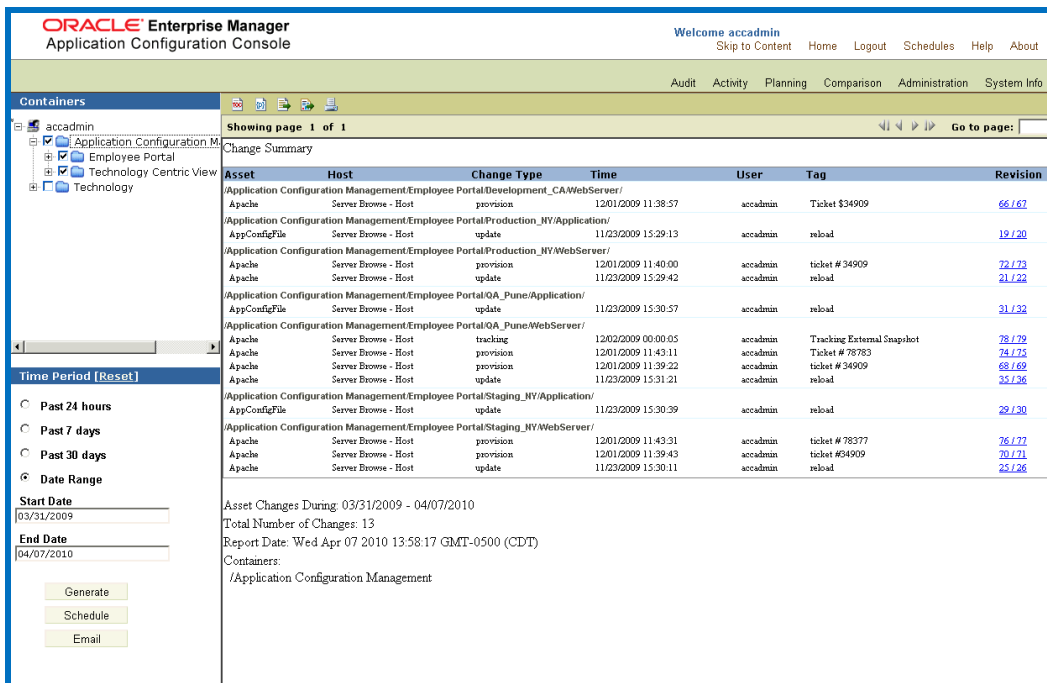


Figure 18, Change summary report

- **Extensibility and out-of-box support for major business applications**

Oracle Enterprise Manager Configuration Management Pack Application Configuration Console provides out-of-box support for over 100 technologies including all major business applications from Oracle and third-party products. As an agentless technology, Application Configuration Console can easily be extended to support custom and third-party applications.

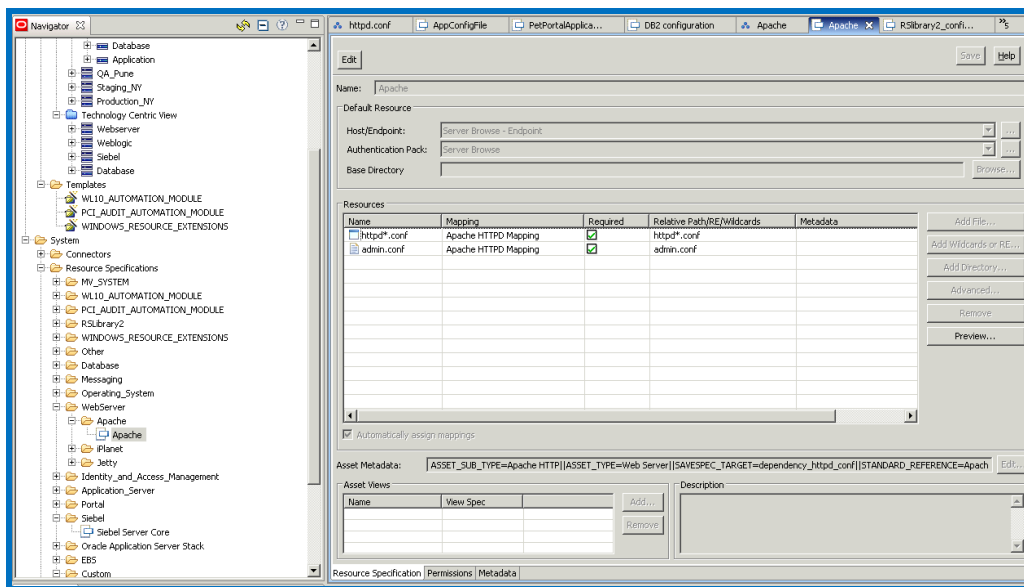


Figure 19, Flexible framework for ease of extensibility

Enforcing Compliance

Although many IT organizations have developed and documented operational policies, many are still finding these inadequate to meet the constant pressure for managing their configuration compliance. One of the main issues customers are experiencing is the inability to develop policies into processes and procedure that produce real-time measurable metrics. This can result in insufficient internal controls to manage today's complexity and changes.

The issue becomes magnified with the introduction of regulatory requirements such as the Sarbanes-Oxley Act, where public companies are required to comply. One of the key strategies used by IT organizations to meet these internal controls is to adopt standards such as PCI, ITIL, ISO 17799, and ISO 20000 which are recognized as industry best practices.

These guidelines not only help IT organizations meet their regulatory requirements, but the IT Governance Institute has also found that adopting these best practices results in lowering IT operational cost and improved alignment with business needs. Consequently, organizations

today are finding it necessary to develop best practices and tools that map their IT strategies, technologies and management practices to their business objectives.

To ensure these best practices comply with regulatory, security and service quality requirements, you need to have metrics in place that determine if your IT goals are being met. An automation process that links company policies to best practices and implements a real-time automated method for measuring compliance is the best way to achieve this end.¹

The Configuration Management Pack includes a feature set called Configuration Change Console that provides breakthrough capabilities to automate real-time IT configuration change management through comprehensive, continuous detection, validation and reporting of authorized and unauthorized configuration change. This white paper discusses the unique capabilities of Configuration Change Console to help you define, track and enforce IT policies; automate IT compliance processes; and reduce the effort and cost of managing business applications.

Configuration Change Console

Configuration Change Console is designed to help organizations by providing an out-of-the-box IT framework that connects IT policies and controls directly to the data collection. This includes tracking and recording both manual and automated actions and events against configuration items, applications and IT components as part of normal daily operations. Configuration Change Console also provides a centralized repository to manage IT policies, and controls where it maps the detected actions and events against it.

Configuration Change Console is designed to provide improved reliability, security, performance and meet compliance requirements that will result in bottom-line savings and peace of mind.

Configuration Change Console Architecture

To understand how this is achieved, let's review Configuration Change Console architecture.

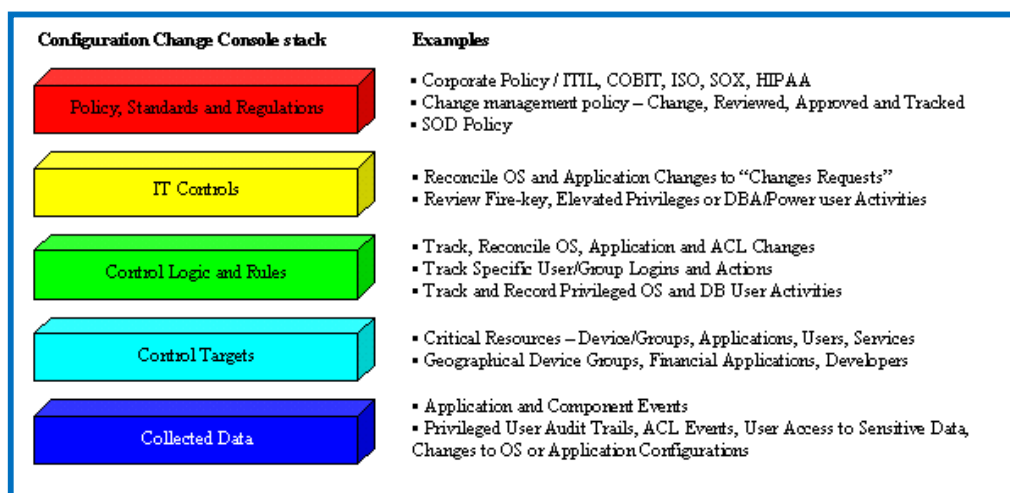


Figure 20, Configuration Change Console stack

The Configuration Change Console is deployed in a distributed architecture, using lightweight agents on managed devices to populate a time-based information model in a back-end database. All data capture is exposed to the user via a Web-based user interface where you are able to perform real-time data analysis, reporting, policy configuration, change notification, administration, and integration with change management systems.

Configuration Change Console is designed to provide real-time configuration change tracking and be highly scalable and capable of monitoring thousands of servers. Often, the scalability is achieved by adding additional application servers accessing the same back-end database.

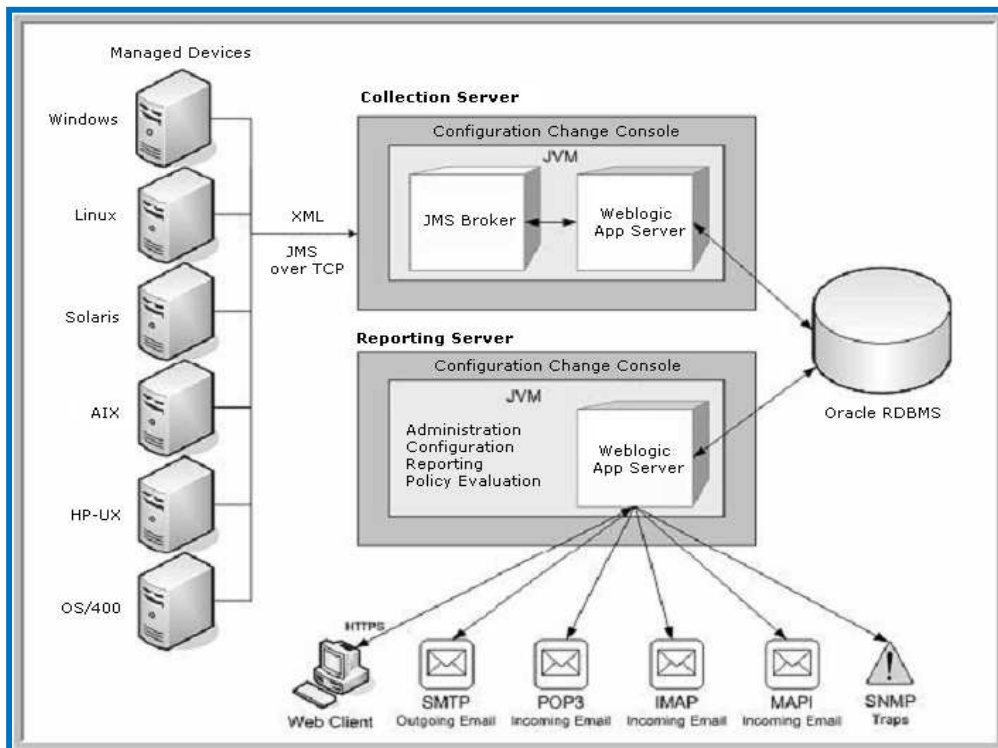


Figure 21, Configuration Change Console overview

Key Features

- **Agents and Data Collection**

Configuration Change Console has the unique ability to track configuration changes for a vast array of IT components in real-time, ranging from OS files and processes to individual point of sale devices. To provide this level of complete, accurate and real-time configuration change reporting, Configuration Change Console's change detection methodology is based upon a lightweight agent installed on each managed device that interacts directly with the IT infrastructure.

The agent operates passively in the background and is continuously monitoring the environment for change activity. As changes are detected on the managed devices, the agent reports changes back to the centralized Configuration Change Console

application server. This requires minimal resources on the monitored target. All CPU intensive analysis and activities take place on Configuration Change Console server and not the managed devices.

- **Monitored Components**

The configuration items that represent the key elements within the IT infrastructure are stored in the central repository database. The information stored is used as a basis to support other service management processes and to verify configuration information against the infrastructure in order to remediate deviations quickly.

As changes are often the leading cause of downtime, most compliance frameworks such as ITIL and SOX require some kind of change management to be in place. The objective of change management is to ensure that standardized methods and procedures are used to efficiently handle all changes, resulting in minimal impact of any change to the service delivered to end users.

Configuration Change Console can automatically detect changes on the components monitored. These include:

Monitored Component	Detected and Reported Events
Files and directories	Creation, deletion, modification, renaming, reading, browsing and attributes change. Data collected includes date/time, event type, MD5 and user ID of the account, depending on the OS
Processes	Start and stop events and CPU utilization. Data collected includes process name, process id, process user, event type, and date/time
User Accounts	User login/logout for local and remote users, source IP, activity level, and user-initiated processes
Server Resources	CPU utilization, memory utilization, file system/storage utilization
Database	Detect application configuration object changes
Network Devices	Capture SNMP traps from devices with configuration changes
Active Directory & LDAP	User, group, and computer adds, deletes, modifications, and membership changes
Windows Registry	Creation, deletion, modification. Data collected includes user and before / after values

- **Operating System-specific Data Collection Information**

As every operating system detects and records change activity differently, this may influence how much data can be collected based on the compliance framework. As a result, Configuration Change Console has architected its agent to detect and report configuration change activity based upon each operating system's uniqueness. The following table details some of the methods used:

Platform	File Change Events	Process Events	User Logon/off Events
Windows	Win32 API and Security Log monitoring	Operating System polling every 3 seconds	Audit/security log monitoring (must be enabled)
Solaris	Audit Log monitoring	Operating System polling every 3 seconds	WTMP file monitoring (can detect type: e.g. telnet, FTP, SSH, Samba, and source hostname of remote logon)
HP-UX	Audit Log monitoring	Operating System polling every 3 seconds	WTMP file monitoring
AIX	Audit Log monitoring	Operating System polling every 3 seconds	WTMP file monitoring
Linux (Red Hat)	Kernel module	Operating System polling every 3 seconds	WTMP file monitoring

In a compliance environment, the tracking of file changes to individual users is a mandatory requirement. To correlate users to file changes, the agent needs to communicate with the operating system to retrieve this information. The following table describes the OS-specific mechanisms for retrieving user information.

Operating System	Mechanism for Retrieving User Information for File or Object Changes
Windows	Audit/Security logging enabled
Solaris	Audit logging enabled using the Basic Security Module (BSM)
HP-UX	Host Intrusion Detection System (HIDS) enabled
Red Hat Linux	Reloadable kernel audit module retrieves information about file change events
IBM AIX	Audit logging enabled

When enabling OS auditing is not possible, Configuration Change Console also provides a mechanism for detecting file changes using snapshots; this is independent from the auditing and logging system of the OS. Users can select which version to use during installation.

- **Application-specific Data Collection Information**

In order to accurately detect and report changes to specific applications such as databases or Active Directory systems, Configuration Change Console leverages various data collection methodologies and sources. The following table summarizes the various application-specific changes detected by Configuration Change Console and their source.

Change Detection Type	Detected Changes	Source of Change Data
Database	Detect application configuration object changes	For all supported databases, changes can be detected by real-time auditing, or diffing snapshots collected at a user specified interval.
Registry Key	Creation, deletion, modification. Data collected includes user and before / after values.	Configuration Change Console leverages a kernel module that traces all system calls in real-time to the Registry.
Active Directory	User, Group, and Computer adds, deletes, modifications, and membership changes.	Configuration Change Console uses two approaches: <ul style="list-style-type: none"> • The proxy method uses LDAP to generate snapshot every 5 minutes of the domain controller, and compares snapshots to report change events (no user name is reported). • The trace method reads account management events in real time in the security log (user name is reported).

- **Agent Communications and Network Utilization**

After the data collection process the Configuration Change Console agent aggregates the data and report change activity using a compressed XML format in 1 to 5-minute intervals. The transmission can be configured to encrypt the data from the agents to the application server over a JMS/SSL connection.

The average transmission size from each agent is about 10 KB every five minutes; this gives you some idea how negligible the network bandwidth is. Based on an

average of 25,000 changes per month, one managed server would generate approximately 100MB of data per month, after normalizing for XML compression.

In the event the communication is broken, all data is queued and sent once the communication is up and running. The agent uses a message broker client to queue data and save it to disk if the connection to the Configuration Change Console application server or database is unavailable or if the agent is suspended in local mode. The data can be queued using cached disk space on the managed server. Cache size is configurable by both the maximum amount of disk space and maximum amount of time to queue data. When the connection is reestablished, the message broker will send the data to the Configuration Change Console server.

- ***Agent CPU Consumption***

The Configuration Change Console agent has been engineered to have minimal impact on the performance of the managed device. All CPU intensive analysis and reporting are conducted on the centralized Configuration Change Console server. For each managed server, the Configuration Change Console agent consumes less than 1% of server CPU over an extended period of time.

- ***Configuration Operations Management***

With an understanding of the monitoring and data capturing process, the next step is to link the infrastructure components with Configuration Change Console and to define how these components are interrelated and will be monitored. This is an important step because most components are interdependent with each other. When one component fails, it will most probably affect the service level of another component impacting the service level or creating a system outage.

Defining the overall interrelationships and how each component is monitored provides complete end-to-end monitoring and with it, operational stability. To do this, use Configuration Change Console to define the components and applications.

- ***Establishing Configuration Change Console Components***

Components basically serve as a blueprint for the important elements that are involved in an application used within your ecosystem. They represent the elements that make up your infrastructure. Examples of components are files, processes, OS users and application-specific internal objects such as database objects.

Configuration Change Console provides a set of predefined components (that also include rules) out-of- box to expedite this creation process within the system. These predefined components can be used as a starting point and later customized to suit the organization's monitoring, compliance and auditing needs.

Defining components include the following steps:

Step 1: Specifying the rules set for each component

Once the components are defined, specify the monitoring rules for these components. In this step, configure what the kind of controls required for the components to meet your compliance framework. The rule set within Configuration Change Console covers a list of components types that include: file event, process event, user event, Active Directory, database (such as DB2, Oracle SQL Server), and Windows registries.

Step 2: Mapping the Components to the managed devices

After configuring the components for the application, specify the device on which each component is running: create what is called the component instance. In this step Configuration Change Console links the components with your infrastructure.

Step 3: Defining audit actions

Once you have established the component rule sets and mapped the component to managed devices, the next step is to specify the actions required when an event occurs. When an unauthorized change is detected, Configuration Change Console can be defined to trigger an email notification, perform a report generation, send SNMP traps, and Change Management Reconciliation.

These event triggers enable the organization to notify the appropriate personnel so that they can analyze changes and make any corrective actions if necessary.

- ***Creating an application to simplify management and reporting***

With the component instance defined, you can logically group the component instances into an application within Configuration Change Console. This application should map directly to your actual business application to provide linkage from Configuration Change Console with your business services.

This allows you to model your real business applications and to be able to report issues that are in line with your business needs. In most cases, a business application relies on multiple IT infrastructure components, such as the Web server, application server and the database, which are all running on different servers.

With Configuration Change Console, you can now easily view the change events that affect the application as a whole rather than only looking at the individual component. This view is not only more effective, but also gives you the ability to view the inter-dependency of one component with another as it relates to a business application.

- ***Policy Management***

As explained earlier, frameworks and best practices are used to manage complexity and cost containment. With an understanding of the architecture and how Configuration Change Console can help improve operations, you now need to understand how to meet required compliance frameworks, policies and controls such as ITIL, SOX and PCI. To do this, use the component configuration defined earlier to

employ the policy management within Configuration Change Console, as described in the following four steps:

Step 1: Planning the compliance requirements

In establishing an overall compliance strategy, it is helpful to consider the relevance of the various control frameworks that are being used within the industry. Every framework has a different emphasis and may be implemented differently across organizations.

Decide which framework best meets your organization's requirements. Based on a particular framework, there are also policies and controls that you may want to fine-tune and customize based on your organization's requirements.

Configuration Change Console provides out-of-box predefined frameworks, policies and controls. These provide some general guidelines that will help you expedite the implementation and the adoption.

Step 2: Defining the controls and assign controls to components

Once you have outlined the desired controls, you can start using Configuration Change Console to map directly with the granular controls that you are using in your organization. For example, you may define the "Restricted File Access" control that monitors read and write accesses to protected/restricted files.

To link the compliance controls within your infrastructure, associate the controls with the components in Configuration Change Console. You can assign multiple components to a particular control. You can create as many controls as necessary to map to your compliance structure.

Step 3: Defining the policy

Once you have defined the controls, assign the controls to a policy. Policies are basically a plan or a course of action that are designed to define issues and influence decision-making that relates to your compliance requirements.

For example, you might create a policy called "Managing Performance Levels" that includes "Capacity Monitoring" and "Problem Tracking" controls within that policy. This means that if there is a violation within the "Capacity Monitoring" control, the "Managing Performance Levels" policy would also be flagged.

Step 4: Defining the framework

A framework within Configuration Change Console is a representation of the compliance framework that your organization has adopted. In this step, define the framework in Configuration Change Console that will be used within your organization. You can specify multiple frameworks if necessary.

For example, you may want to monitor both the ITIL and PCI framework in your organization.

- **Monitoring And Controlling**

Once you have set up the framework within Configuration Change Console, you are able to use a series of dashboards that will provide a high-level view where you can quickly monitor and be alerted of any real-time unauthorized change based on your organizations compliance framework, policies and controls. This includes the capability to control and inspect whether there has been any unauthorized access to your infrastructure. Also provided is the capability for the forensic trail of activities that reduces the mean time to repair of a system crash or a service level agreement violation.

The top-level dashboard shows a series of real-time dials that relate to the framework. Each dial represents a policy defined within that framework. These dials provide a real-time summary view of a policy's performance as defined by per-configured thresholds.

If a control has a violation, the dial for that policy will provide a status view as defined by the configured threshold for that control. For example, if you experience an unauthorized access to a password file, a notification would be sent and the dial for the “Implement Detect application configuration object changes Strong Access Controls” policy will provide an indicator that that particular control has been violated.

To provide a more in-depth view of the issue, you can drill down to the respective dial providing an at-a-glance view with forensic information of the event. Through this understanding, you can then analyze the activities and perform corrective actions as needed.

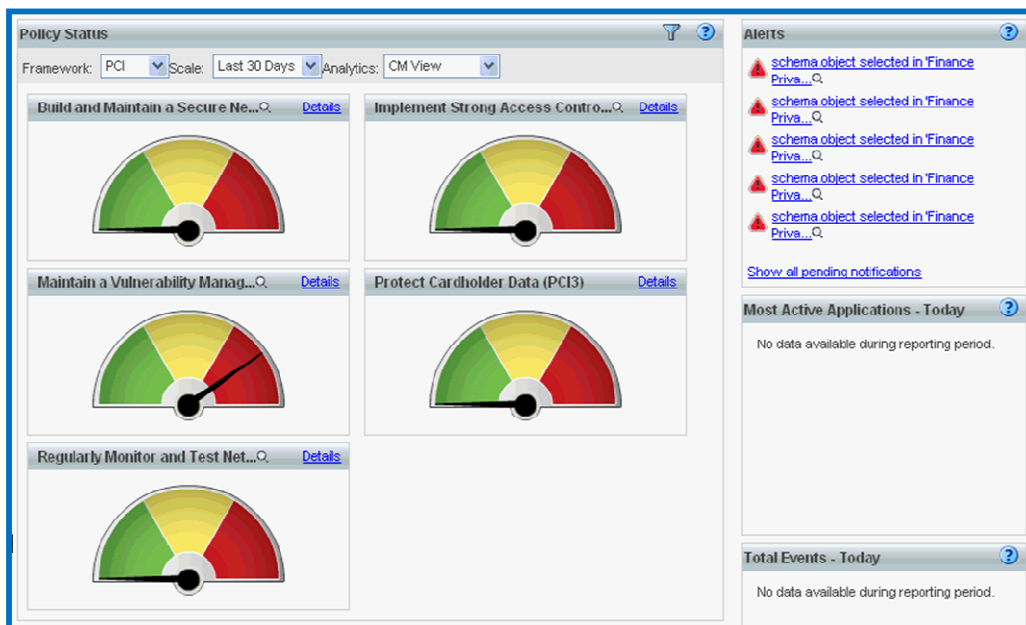


Figure 22, Configuration Change Console Dashboard

Conclusion

The goal of Oracle Enterprise Manager 11g Configuration Management Pack is to increase administrator productivity, improve efficiency, and reduce IT management costs through industry-leading automation. Oracle Configuration Management Pack allows IT organizations to free up administrator's time and resources for higher value-added tasks like proactive maintenance and capacity planning, which results in a more stable, more efficient IT environment.

Managing a data center requires broad and deep automation for scalability, high availability and standardization. Oracle Configuration Management Pack achieves these objectives by first discovering the Oracle IT environment and then managing it through change tracking, search, and powerful configuration comparison capabilities. Lastly Oracle's policy management helps enforce best practices; in particular, it acts as the underpinning of several security capabilities for Oracle Enterprise Manager 11g. This leads to a more proactive and secure environment helping you avoid the high costs associated with compromised security.

Oracle Enterprise Manager 11g Configuration Management Pack provides businesses the industry's most comprehensive end-to-end solution for managing system configurations—from application-to-disk, at the lowest possible cost and with proven measureable ROI.

For additional Return On Investment information reference the Total Economic Impact™ Of Oracle Enterprise Manager Configuration Management Pack and Provisioning and Patch Automation Pack from Forrester Consulting. This study demonstrated that by *“using Oracle Enterprise Manager **Configuration Management Pack** and Provisioning and Patch Automation Pack achieved a risk-adjusted and a **very favorable 124% ROI** (130% non risk-adjusted ROI) over a three-year period with a risk adjusted **payback period of 15 months**”*

You can access the complete report on Oracle.com or from the following link:

<http://www.oracle.com/corporate/analyst/reports/infrastructure/em/forrester-tei-em-config-provision.pdf>

Contact Us

For more information about [insert product name], please visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative



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

White Paper Title

April 2010

Author: Andy Oppenheim

Contributing Authors: CMP Team

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

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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd. 0110