Automating IT Configuration Controls with Oracle Enterprise Manager Configuration Change Console

An Oracle Technical White Paper
October 2008

ORACLE

Automating IT Configuration Controls with Oracle Enterprise Manager Configuration Change Console

INTRODUCTION

Today Oracle offers Oracle Enterprise Manager a complete application management solution. Oracle Enterprise Manager allows you to manage your applications top-down from a business perspective. This allows you to identify business exceptions rapidly, pinpoint root cause issues using drilldowns in the underlying technologies, infrastructure, and remediate the issues automatically before they become emergencies. A key component of Oracle Enterprise Manager is the Configuration Management Pack. The Configuration Management Pack provides discovery, asset tracking, analytics, change detection and compliance assessments and reporting. Included with the Configuration Management Pack is the Configuration Change Console. Configuration Change Console 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 the Configuration Change Console, helping you define, track and enforce IT policies; automate IT compliance processes; and reduce the effort and cost of managing business applications.

Security is only as strong as the weakest link. Methods that applications use to interact with the database are often an overlooked link that's improperly secured.

POLICY-BASED IT MANAGEMENT AND GOVERNANCE

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.

This issue is even more magnified with the entry 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.

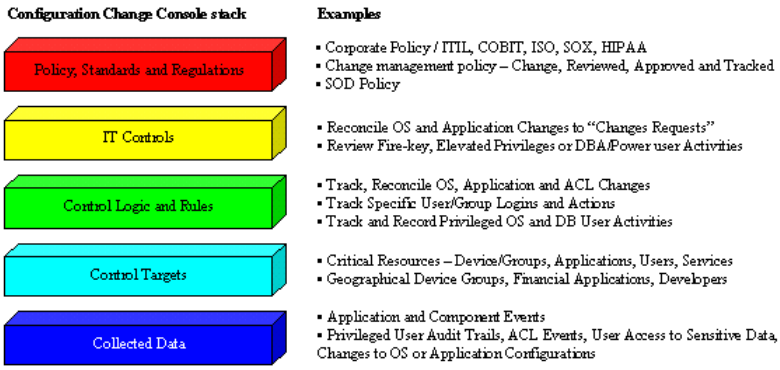
These guidelines not only help IT organizations meet their regulatory requirements but IT Governance Institute has also found that adopting these best practices has also resulted in lowering IT operational cost and improved alignment with business needs[1]. As a result, organizations today are finding 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, metrics need to be in place that determines if the IT goals are being met. To successfully provide this, it is highly recommended to have an automation process that links company policies to best practices and implement a real-time automated method for measuring compliance[2]

Configuration Change Console helps organizations ensure regulatory compliance as well as implement internally mandated controls. Configuration Change Console delivers these benefits by providing a library of policies coupled with real-time change detection and change reconciliation.

CONFIGURATION CHANGE CONSOLE

The 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 the 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.



The 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 the Configuration Change Console's architecture.

---

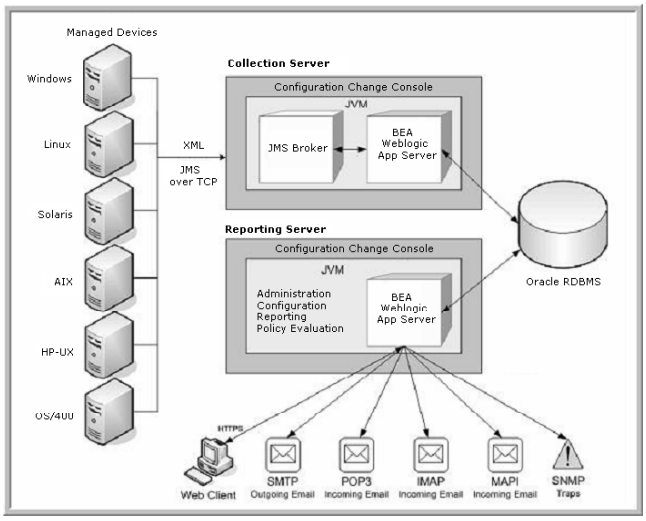
[1] IT Governance Institute (2005): Aligning COBIT, ITIL and ISO 17799 for business benefit

[2] Gartner Research (2006), Security Controls and Policy Management Defined

The Configuration Change Console is deployed in a distributed architecture, using lightweight probes 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 collects real-time event information through a probe installed on each managed device. The probe can capture events on objects such as files, processes, users (and so on) on these devices.

The probe is light-weight and requires minimal resources on the managed devices.



Configuration Change Console is designed to provide real-time configuration change tracking, 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.

PROBES AND DATA COLLECTION

One of the unique capabilities of the Configuration Change Console is its ability to track configuration changes for a vast array of IT components in real-time; ranging from OS Files and processes t 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 probe installed on each managed device that interacts directly with the IT infrastructure.

The probe operates passively in the background and is continuously monitoring the environment for change activity. As changes are detected on the managed devices, the probe 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 the 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 use as a basis to support other service management processes and is used 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 for efficiently handling of all changes, resulting in minimal impact of any change to the service delivered to end users.

The 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 probe 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 probe 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, CCC also provides a mechanism of detecting file changes using snapshotting, 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,	Configuration Change Console utilizes two approaches. The proxy method uses LDAP to generate snapshot every 5 minutes of the domain

	and membership changes.	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).

PROBE COMMUNICATIONS AND NETWORK UTILIZATION

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

The average transmission size from each probe is about 10 KB every five minutes hence this would give 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.

Probe has been designed to consume as little resources as possible. For example:

Network: Average transmission size for each probe is 10 Kb every 5 minutes.

CPU: Average CPU utilization for probes has been found to be less than 1% over long periods.

In the event the communication is broken, all data would be queued and sent once the communication is up and running. The probe 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 probe 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.

PROBE CPU CONSUMPTION

The Configuration Change Console probe 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 probe consumes less than 1% of server CPU over an extended period of time.

CONFIGURATION OPERATIONS MANAGEMENT

With the understanding of monitoring and data capturing process, the next step is to link the infrastructure components with the Configuration Change Console and to defining 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.

By defining the overall interrelationships and how each component is monitored, we will have complete end-to-end monitoring that will provide operational stability.

To do this, we need to define the components and applications with Configuration Change Console.

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.

The Configuration Change Console provides a set of predefined components (that also include rules) out-of-the-box to expedite this creation process within the system. These predefined components can be used as a starting point and be 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, we then specify the monitoring rules for these components. In this step, we configure what kind of controls is required for the components to meet your compliance framework. The rule set within the 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.

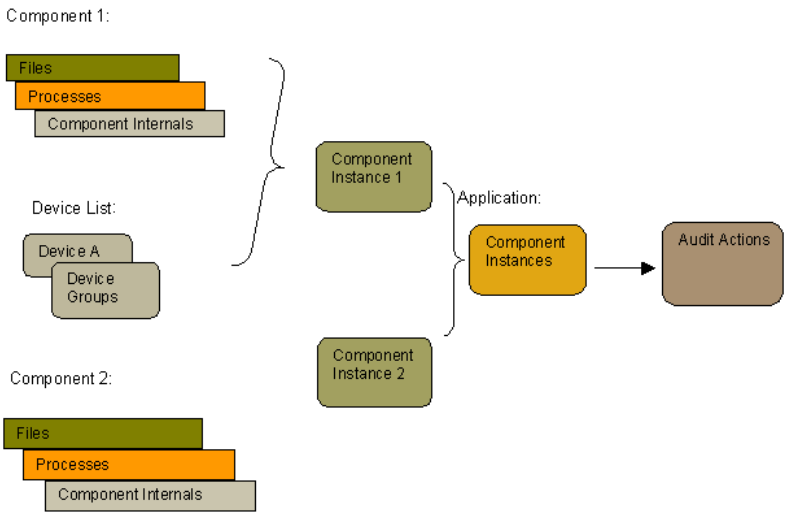
Step 2: Mapping the Components to the managed devices

After configuring the components for the application, then specify the device on which each component is running. This is creating what is called the component instance. In this step the 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 what actions would be 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 where they can analyze changes and make any corrective actions if necessary.



CREATING AN APPLICATION TO SIMPLIFY MANAGEMENT AND REPORTING

Configuration Change Console allows logical grouping of components into applications. This enables users to easily view change events affecting their business applications.

With the component instance defined, we then logically group the component instances into an application within Configuration Change Console. This application in the Configuration Change Console should map directly with your actual business application where it provides a 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 does rely 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 is also very empowering because you are now able to view the inter-dependency of one component with another that relates to a business application.

POLICY MANAGEMENT

As explained in the beginning of this paper, frameworks and best practices are used to manage complexity and cost containment. So far, this paper has defined the architecture and how the Configuration Change Console can help improve operations.

Now we need to understand how we can meet required compliance frameworks, policies and controls such as ITIL, SOX and PCI. To do this, we need to employ

the policy management within Configuration Change Console by using the component configuration that was defined earlier. This is done in 4 main 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 emphases and across organizations may be implemented slightly different.

You would need to decide which framework would best meet your organization's requirements. Based on a particular framework, there are also policies and controls that you may want to fine-tune and customized based on your organization's requirements.

The Configuration Change Console provides out of the box predefined frameworks, policies and controls. These will 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, you would need to 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, you would then need to assign it 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 may create a policy that is called "Managing Performance Levels" and included "Capacity Monitoring" control 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 the Configuration Change Console is a representation of the compliance framework that your organization has adopted. In this step, you would need to 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.

Configuration Change Console dashboards provide a quick snapshot of the complete monitored environment.

Users can drill down further to investigate problem areas – Configuration Change Console provides rich details about each event, facilitating problem resolution.

MONITORING AND CONTROLLING

Once you have setup the framework within Configuration Change Console, you are able to use a series of dashboards that will provide you 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 onto 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 one of your controls has a violation, the dial for that policy will provide you 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 drilldown 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.

CONCLUSION

A leading cause of failures in IT systems and applications is unauthorized and unexpected configuration change. This often results in costly downtime and violations of compliancy and service level objectives. The Configuration Change Console provides a unique solution to address these challenges through automated management and enforcement of IT policies for configuration change management. It helps connect people, process and technology to automate IT controls and governance through comprehensive recordings and forensic trails. What sets the Configuration and Change Console apart is its exhaustive coverage for IT components; comprehensive integration with leading IT change management solutions; and integration with Oracle's top-down application management. By using Configuration Change Console, organizations will have a better control of the IT infrastructure; meet regulatory compliance and statutory requirements using an automated IT control that will then result in lowering your operation cost.

Automating IT Configuration Controls with Oracle Enterprise Manager Configuration Change Console
October 2008
Author: Andy Oppenheim
Contributing Author: Zia Hydari

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