

SOLUTION BRIEF

What's in Your CMDB?

Tripwire configuration audit and control ensures that your CMDB reflects the real world



"Through 2008, 75 percent of all CMDB implementations will fail to achieve a comprehensive services view of all consolidated IT domains because of poor control processes."

— Ronni Colville
Research VP
Gartner, Inc.



As companies grow, so do their services and applications. For IT departments, that means expanding infrastructure and corresponding complexity. This has brought IT to a critical stage—the necessity to standardize and control IT processes. In this effort, many organizations, looking to fulfill IT Service Management (ITSM) and IT Infrastructure Library (ITIL) initiatives, are adopting configuration management databases (CMDBs) as a keystone of their IT process framework. The CMDB acts as a repository of configuration items (CI) for business-critical systems, services and components, also becoming a definitive “source of record” that provides a logical model of the relationships among the IT infrastructure for use by IT services. The intent of the CMDB is to provide an accurate overall service view. Unfortunately, the integrity of the CMDB can start to degrade the minute data is loaded into it.

Configuration Drift and Inadequate Change Processes

How a CMDB becomes inaccurate can be best illustrated by using the example of implementing an automated warehouse inventory system. To begin with, a physical account is made of all the goods stored in the warehouse and the data entered into the inventory database. Then, as goods are shipped and received, the tracking system keeps a record, adjusting inventory levels automatically. One year later, another physical account is made, and it is discovered that the inventory is off by several thousands of dollars worth of goods. Why? The system was unable to account for all activity, such as unauthorized or undocumented movement of goods, human error, theft, or unreported breakage. It is only able to record and track the inventory it has been told about.



ITIL and CMDB

ITIL presents the CMDB as an information repository supporting a wide ranging set of management processes; from incident and problem management, to release management, to change management, as well as supporting asset management, service level management, and other more business-oriented disciplines. The value that the CMDB provides to these related ITIL processes is inestimable, and the CMDB data can impact overall service and response.

So, how does ITIL relate to the CMDB? In short, the CMDB becomes for ITIL a trusted resource of configuration information for assuring consistency and efficiency across many IT disciplines in support of ITSM. ITIL does not in any way deal directly with architecture or architectural issues—it is one hundred percent devoted to IT process. ITIL provides the top-down view of processes (the “*what*” not the “*how*”) and the CMDB provides the foundation upon which advanced IT functions are built. The CMDB is, in fact, a concept not necessarily greater or smaller than its parent (ITIL) but in the “real world” represents an overlapping circle where architectural evolution and best practices come together.

Source: Enterprise Management Associates, Inc.

A CMDB is populated with a snapshot of the infrastructure, across all technology domains. Each of the domains is a hub-bub of constant change activity from a variety of sources: automated tools, scripts, and manual changes. If any change is done without authorization or documentation, or made outside of approved configuration tools, the CMDB can either inadvertently record the unauthorized change or simply be unaware that the change was even made. For instance, if a file within a server is upgraded by a well-meaning technician from “version 1.2” to “version 1.3” without authorization or documentation, the CMDB will assume the file is still running at version 1.2. In other words, the CMDB only knows what it knows. Such unauthorized changes, made by different individuals across the infrastructure, can cause information in the CMDB to become out of date and inconsistent with the real state of systems. This is often referred to as “configuration drift.”

In a warehouse, inaccurate inventory reports will continue to be issued, and “untracked goods” will continue to be a costly problem until stronger controls are implemented. Worse, the issue isn’t likely to surface until a critical customer order can’t be delivered or auditors discover the discrepancies. The same situation can occur with the CMDB. Unauthorized and undocumented changes that circumvent controls and processes undermine the accuracy of the CMDB data and IT’s ability to reliably deliver services to the business.

This is a common problem. Gartner Research estimates that through 2008, 75 percent of all CMDB implementations will fail to achieve a comprehensive services view of all consolidated IT domains because of poor control processes.¹ Conventional approaches to change and configuration management, where configuration audit and control processes are not in place or not adhered to, are jeopard-

izing the CMDB’s ability to achieve and maintain “truth.”

The change management process is very important to the success of the CMDB. Accuracy requires that control processes are in place, and if processes are not in place, the result is inaccurate data—and the change management process suffers. It may sound a bit like ‘which comes first, the chicken or the egg,’ but in the case of CMDB, the answer is clear: control processes are fundamental.

Configuration Audit and Control Helps Ensure Success

There are two main issues that can compromise the success of a CMDB: inadequate change processes and unauthorized change. As Gartner puts it, “...[the] CMDB is closely aligned with change management process and policy. Without a rigorous adoption of these processes, the data in a CMDB will be static or old, not reflecting the true current infrastructure. Although configuration management database tools will offer the capability to manage the data for a service view, IT organizations must make preparations to ensure that the data is clean to prevent ‘garbage in, garbage out.’”² Even if you have a good change management process in place, data can become inaccurate if processes are circumvented.

The CMDB, intended to serve simply as a repository of configuration information, has no inherent ability to ensure that changes comply with an organization’s change and configuration management policies. When a change to a production system circumvents these processes, the CMDB will either be unaware of the configuration event and not record the change, or unknowingly record the

¹ Colville, Ronni. “Do All Roads Lead to CMDB?” Gartner 25th Annual Data Center Conference, 2006

² Colville, Ronni. Ibid.

change with the presumption that it was intended and approved. Either way, the CMDB misrepresents the expected configuration state of the infrastructure. When a problem later arises with the affected system, the inaccurate information from the CMDB can lead staff to make wrong decisions and actually create more problems than it is solving. If this happens often enough, the integrity of the CMDB will be questioned and the initiative will fail.

IT organizations can overcome the issues of unauthorized change with the help of Tripwire configuration audit and control solutions. It is strongly recommended to implement Tripwire prior to undertaking a CMDB so that process discipline becomes part of the culture of how changes are managed. But regardless of the point of implementation, Tripwire can enhance CMDB initiatives by ensuring changes meet configuration and change policies, minimizing the effects of poor processes, and providing accurate change detail.

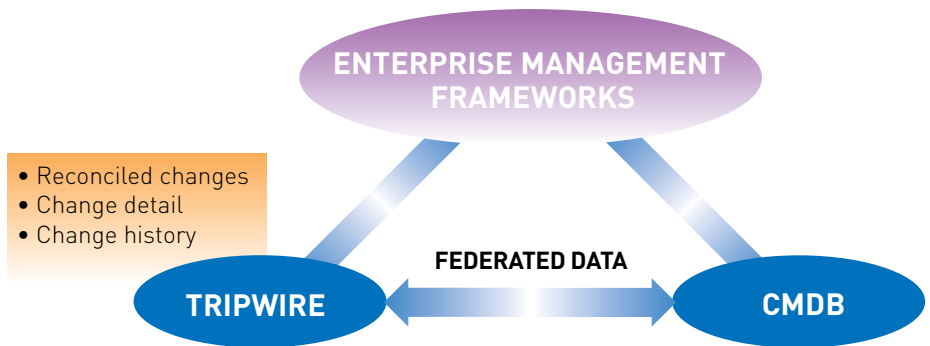


Fig. 1. Configuration Audit and Control Provides Federated Access to CI Change History

A federated CMDB model refines ITIL's idea of a CMDB by extending it with critical information provided by trusted sources to create a comprehensive service management architecture. Tripwire provides detailed change information reconciled with change and configuration management policies to both the CMDB and directly to enterprise management frameworks. In this federated approach, rich change and configuration data across technology domains is made available to increase visibility, accountability and control of configuration changes.

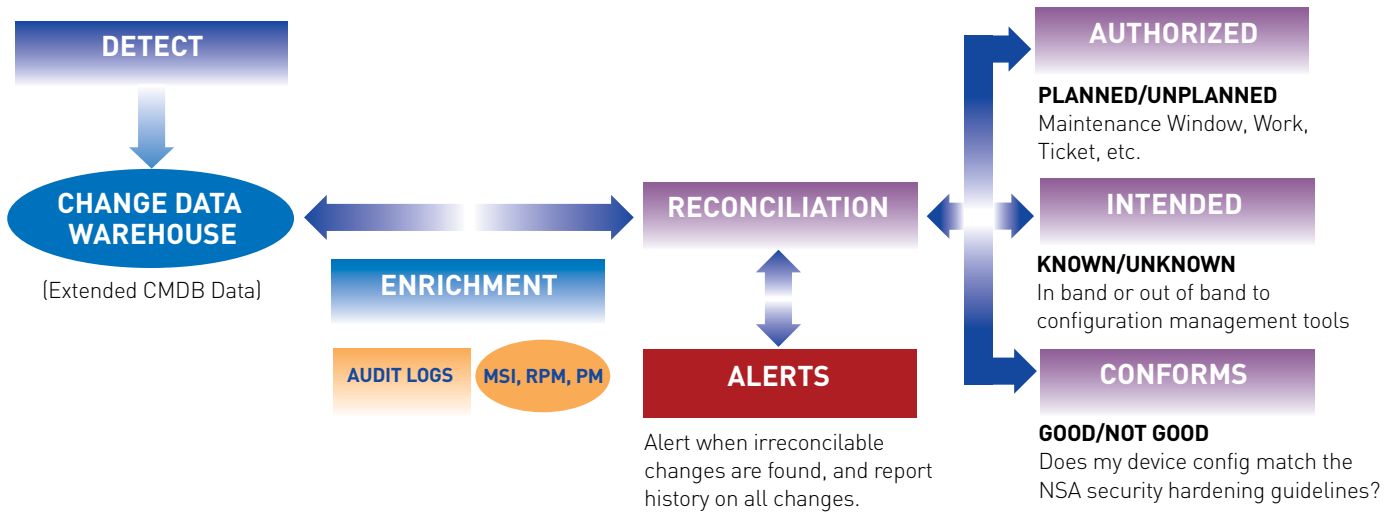


Fig. 2. Configuration Audit and Control Enriches CMDB

Changes are detected and placed in a data warehouse, which extends CMDB data in a federated model. That data is then enriched with information from audit logs and configuration packages. Such information might include who made the changes, user events that occurred to that data before a change was detected, and what packages the files may be part of. Tripwire then reconciles the detected changes to change policies, intended or planned changes, and reference system configurations. Augmenting a CMDB with configuration audit and control not only helps maintain the integrity of your CMDB, but also helps ensure that changes are made in support of the business.

Enforceable Change Processes

Many companies attempt to control change to the infrastructure by declaring a change policy that relies on everyone “remembering” to follow the rules. However, in many data centers, change frequently occurs outside tools and processes, without proper authorization and documentation. Tripwire automatically enforces change policies so that companies do not have to depend on an “honor system.” Tripwire provides:

- automated reconciliation of change based on a variety of user-defined policies and criteria;
- details on the ‘Who, What, Where, and When’ of change that increased accountability and encourages adoption of change processes;
- unauthorized change alerts with actionable reports so that remediation actions can be immediately taken.

Change Accuracy and Confirmation

An organization may have accurate inventory of its physical assets, but it is also necessary to have *accurate configuration data* on those assets. A CMDB can quickly become out of sync with reality unless it is consis-

tently updated with complete and accurate change information as configurations evolve over their life cycle. Tripwire ensures that all changes are properly accounted for and authorized before data enters the CMDB. Tripwire provides the essential ‘glue’ to correlate all changes to the actual state of CIs, and ensures that changes are properly documented, approved and performed in accordance with policy. Tripwire:

- detects all changes made to the infrastructure, regardless of source, including unauthorized, undocumented changes;
- ensures all changes being provided to the CMDB comply and conform to policy;
- ensures changes are reconciled with change and/or configuration policies before entering the CMDB;
- creates an audit trail of successful, validated, and planned changes;
- reports configuration exceptions, and if desired, triggers changes to be rolled back to a desired state;
- discovers changes quickly in a scalable fashion;
- provides reports of changes and records variance as components move through the life cycle; patches, updates, configuration adjustments, repackaging and other necessary changes are documented as components move from one function or team to another.

Tripwire configuration audit and control solutions also provide federated access (across the enterprise and all technology domains) to detailed CI change history through the CMDB. This helps provide management the information needed to realize process and operational improvement.

Summary

The potential benefits of a CMDB are many, among them, a complete picture of the infrastructure and the services it delivers. But potholes will develop on the road to the CMDB success—unless it is built on a foundation of strong change processes enabled by a configuration audit and control solution.

The CMDB will only be valuable when it contains accurate change data. Tripwire adds value to the CMDB by detecting and analyzing all changes made throughout the IT infrastructure, synchronizing changes to change management policy and process while extending CMDB data with change details and history. Tripwire increases the likelihood of success for CMDB initiatives. Plus, the trustworthy data and policies Tripwire make possible also provide broad, bottom line business benefits: a reduction in time to find and remediate problems, and reducing overall infrastructure risks.

Tripwire Professional Services Helps Organizations Develop Change Processes

Ensuring sustainable change and configuration practices requires not only technology, but also people and processes. To provide the whole solution, Tripwire Professional Services helps organizations quickly reap the benefits of Tripwire configuration audit and control solutions. From implementation of Tripwire solutions to core ITIL processes, Tripwire’s consultants offer expertise in network and systems administration, audit and operations, ensuring technology and processes are aligned in order to quickly meet your business objectives.



www.tripwire.com

US TOLL FREE: 1.800.TRIPWIRE MAIN: 503.276.7500 FAX: 503.223.0182
326 SW Broadway, 3rd Floor Portland, OR 97205 USA