

Enhance BMC Change Management with Closed-Loop Control

The Change Control Gap

Unwanted change to infrastructure is a leading cause of IT woes. Service availability outages, increased compliance costs, and the overall time and effort devoted to chasing change are just a few of the many problems faced by IT operations every day.

In an effort to “get in front” of the change problem, many organizations have invested heavily in solutions such as the change management components of BMC Remedy Service Management or BMC IT Service Management for Mid-sized Businesses (formerly “Magic”). These are widely deployed, market-leading products that do a great job of automating the process of managing change. So why do many organizations that have implemented these products fail to fully realize their expectations for control over change, and ultimately ROI?

The fact is that most change management implementations, regardless of vendor, fail to bring all change under control. Invariably, there is a gap between what the change management process says is happening and the change that is actually occurring across the IT infrastructure. This “Change Control Gap” is typically the result of process failure, not product failure. First of all, most processes are designed around the desired, and assumed change practices of the organization. They do not adequately consider actual change behavior, which is often largely unknown. This puts the process at odds with reality from the start. Secondly, the best process, even with a high-degree of automation, must be understood, socialized and religiously followed by the entire organization in order to succeed. This is a very difficult achievement even for mature organizations. Finally, most breakdowns to the process go undetected, at least until a

major problem occurs. Even when detected there is no sustainable accountability mechanism. As a result, the process deteriorates over time and the gap widens.

The change control gap, in turn, creates an ROI gap for change management implementations. Even if 80% of change goes through process, it is the 20% of the change eluding process that keeps organizations from realizing much of their expected ROI. See Figure 1.

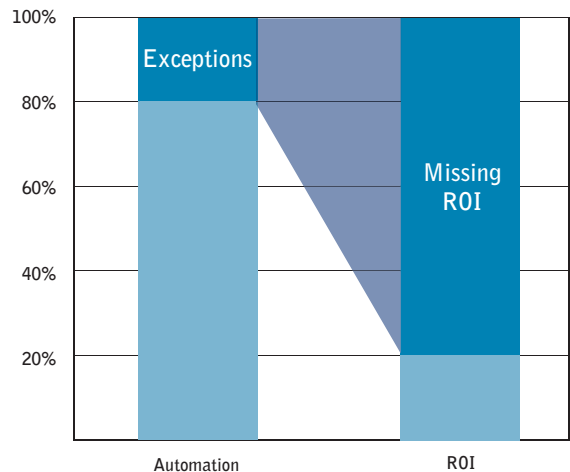


Figure 1: Change management ROI not realized 80% of the time

Closing the Gap

So is implementing a change management solution a waste of time and money? The answer is no. Change management solutions

are absolutely necessary for the achievement of overall IT service management goals. However, to fully meet expectations, a change management implementation needs an additional ingredient: *Closed-loop control*.

Organizations that recognize the need to close the loop on their change management processes often assume the answer is additional process automation combined with periodic checks on the state of the infrastructure. They attempt to link the change management solution with a change provisioning or datacenter automation tool to close the loop between approval and deployment. They may also invest in a configuration management database (CMDB), which helps track the state of the infrastructure and its internal dependencies. Both of these approaches have great value and are recommended practices for achieving ITIL maturity. However, they do not close the change control gap. Change still happens outside of the process and the CMDB, even when fully implemented and fed by surrounding processes, typically has neither timely nor complete information about such change.

What's needed to close the gap is a specific form of closed-loop control at the infrastructure level that is tightly integrated with the change management solution. Closed-loop control starts with three fundamental capabilities:

- 1. Continuous change auditing:** This means capturing each relevant change to the infrastructure as it happens and capturing all the pertinent details regarding that change, including who made the change, what specifically was changed, exactly when the change was made, and what program was used to make the change. Note that continuously auditing *change actions* is fundamentally different from "periodically" auditing the *state* of the infrastructure.
- 2. Change validation against change requests:** This involves using all the information captured about actual change to group changes intelligently and match them against change requests in the change management system.
- 3. Real-time change prevention:** This is the capability to actually prevent change from occurring without a valid change request. This must be fine-grained and flexible to match the needs of different environments.

With these fundamental capabilities in place, it is possible to build highly useful closed-loop control workflows that integrate seamlessly with change management. These workflows include reconciliation of actual changes with the change management system, matching of changes in staging and production environments, and enforcing change policy through the change management system. These capabilities are discussed below in the context of a BMC Remedy Change Management implementation.

Reconciling Changes with Change Management System

Continuous change auditing creates a complete database of detailed change events. Change validation matches groups of changes in the database to corresponding approved and implemented requests for change (RFCs) in the Remedy system. This is based on hostname or configuration item (CI), actual start time, actual end time, and username. After reconciliation, the RFC is updated with detailed information about the change that includes the user who made the change, the CI/hostname that changed, and a link to a detailed report of changes. This information is accessible from the Remedy Worklog field.

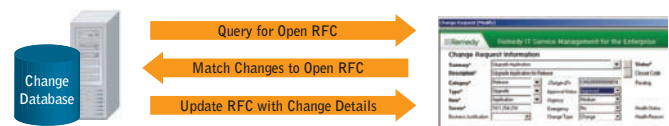


Fig. 2: Reconciling an approved RFC

Matching Staging and Production Environment Changes

Changes are deployed and audited in the staging environment and a manifest ticket is created for production implementation. After the production implementation is complete, the changes in production are audited and reconciled against the manifest ticket created from the staged changes. As Figure 3 illustrates, the RFC is updated with the actual matching changes and an exception report listing extra and missing changes is generated.

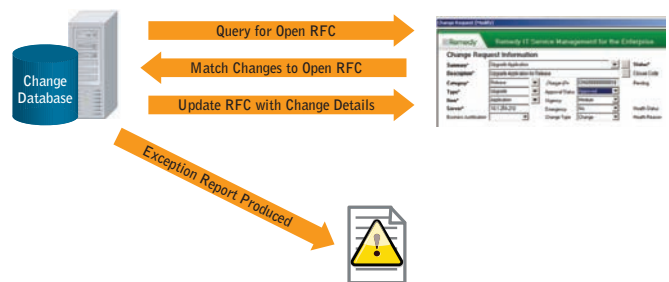


Fig. 3: Comparison between Staging and Production Servers

Enforcing Change Policy via Remedy Change Management Application

The pro-active change prevention capability discussed above can turn the Remedy Change Management application into a system which can technically enforce the enterprise change policy for selected servers and files. The change prevention capability puts the critical objects in a locked state. When the system or software detects that an RFC has been moved to the "work-in-progress" state, the time window specified in the RFC is checked against

the current time to ensure the change is being implemented during the authorized window. If there is a match, the critical objects on the target server for the RFC are unlocked and the change is made. Once the RFC is closed, the objects are locked once again. With this capability in place, any of the constraints in the RFC such as scheduled start time, scheduled end time, approval status, and RFC status, can be enforced at the infrastructure level. See Figure 4.

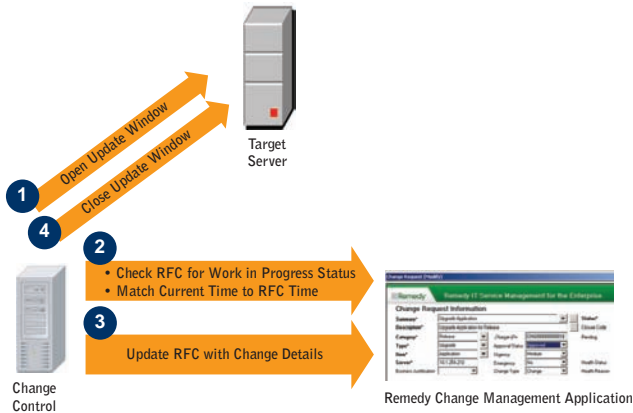


Fig. 4: Enforcing Policy with Remedy Change Management

Summary

Closed-loop control ties change policy directly to the infrastructure. It greatly increases the operational effectiveness of change management applications such as BMC Remedy by ensuring that actual changes are automatically linked to authorized change processes. This is accomplished by:

- Reconciling actual changes to approved, ticketed, and change requests;
- Automatically creating new tickets for un-ticketed changes;
- Creating tickets for changes made to the staging environment, reconciling the ticket with the production environment changes, and reporting the exceptions; and
- Preventing the execution of changes without an approved change request.

Solidcore S3 Control™ provides the only complete, closed-loop change control solution for BMC change management applications. S3 Control integrates easily with both default and customized installations of BMC Remedy and Magic change management applications without requiring any change to existing processes. It verifies that approved changes have been deployed and identifies unapproved/un-ticketed changes (e.g. emergency changes) with very high accuracy to ensure continuous process verification. S3 Control can also be configured to pro-actively prevent changes that do not have a proper RFC. By adding S3 Control to BMC Change Management implementations, organizations can reduce the cost of compliance, improve service availability, and achieve maximum ROI on ITIL change management initiatives.

About Solidcore Systems

Solidcore is a leading provider of change control for critical systems.

Solidcore's S3 Control software is the industry's first and only solution to automate the enforcement of change management policies. Solidcore automatically reconciles infrastructure changes against change tickets, and provides real-time change auditing so enterprises can measure the effectiveness of change management processes and policies.

Customers trust Solidcore to improve service availability, implement ITIL initiatives, and lower costs related to compliance. Solidcore also provides change control for embedded systems and is used by major device manufacturers to securely leverage open systems to meet their business requirements.

Solidcore is headquartered in Cupertino, California. For more information, visit www.solidcore.com.

solidcore®

Solidcore Systems, Inc.
20863 Stevens Creek Blvd, Suite#300
Cupertino, CA 95014

Email: sales@solidcore.com
Web: <http://www.solidcore.com>