RC24915 (C0912-005) December 3, 2009
Computer Science

IBM Research Report

Knowledge-Enhanced Change Audit for Configuration Management

Bo Yang
IBM Research Division
China Research Laboratory
Building 19, Zhouguancun Software Park
8 Dongbeiwang West Road, Haidian District
Beijing, 100193
P.R.China

Research Division
Almaden - Austin - Beijing - Cambridge - Haifa - India - T. J. Watson - Tokyo - Zurich

Knowledge-Enhanced Change Audit for Configuration Management

Bo Yang

Department of Distributed Computing and Service Management, IBM Research - China
Tower A, Bld. 19 Zhongguancun Software Park, Beijing, 100193, China
yangbbo@cn.ibm.com

***Abstract*—IT infrastructure is highly complex and changeable for reacting to business update with market change. Unfortunately, change is not always successful. Managing change effectively and reducing the negative effects of day-to-day operations has become one of the most important tasks in IT service management. Beyond recording all configuration items used in the provision of operational services, analysis and audit for the operations on configuration items are more important. One needs to scale or respond to special domain knowledge, collaboration and the right data for helping IT professionals to improve their configuration management. In this paper, a sync audit with Request for Change (RFC) ticket and knowledge-enhanced audit analysis services is proposed to improve change & configuration management quality. The essential contribution of this work is to organize the highly complex IT configuration information with RFC ticket and to build a knowledge repository for accumulating and reusing experts' knowledge for audit. In addition, a prototype is implemented to explore this knowledge-enhanced audit analysis services framework. Finally, a real use case of change management is used for evaluating the effectiveness and efficiency of the knowledge-enhanced audit analysis services framework.**

***Index Terms*—IT service management; change management; configuration management database; knowledge database; audit**

I. Introduction

THE economic downturn forces businesses to be aware of changes in their organizations, re-think their strategies and operating plans. However, organizations are managing increasingly complex IT environments. They have to deliver more services to respond to increasing business requirements, with a greater number and variety of applications, personal computers (PCs), laptops, servers, printers, mobile devices and network cables. Most organizations do not have the information, processes and experts needed to make informed, responsive decisions due to lack of rich knowledge and experience in system management.

A key challenge here for dynamic enterprise-scale IT system management is that IT infrastructure is highly complex and configurable, and business requirements often have a dynamic impact on IT component configurations. Administrators managing these systems are not only expected to keep them running with those changes, but in addition, many such systems must meet certain Service Level Agreements (SLAs). Even the occurrence of seemingly routine events like software patches, load changes, or modifications of certain environmental parameters can cause such systems to behave in unexpected ways, often resulting in their business application failing to meet current objectives [1]. At the same time, IT departments have to face the requirements of improving the alignment of IT efforts to business needs and managing the efficient provisioning of IT services with guaranteed quality [2].

Many methods have been proposed to leverage information technology for supporting this work, which trying to provide a platform to collect and store significant components information of the IT infrastructure that helps an organization understand the overall landscape for an enterprise’s IT services, such as Configuration Management Database (CMDB) in IT Service Management [3] and CMDB products including IBM CCMDB and HP Mercury Universal CMDB etc.

Configuration management provides diverse information to users or other service components in an IT service management (ITSM) environment [4]. Its purpose is to show what makes up the infrastructure and illustrate the physical locations and links between each item, which are known as configuration items. The technician can then make a more informed decision about an upgrade needed.

However, even if all the information of the systems and operations are captured, IT management professionals can be hazed and confused by the trivial details. According to Gartner, 50 to 80 percent of unplanned downtime is caused by people and process issues that result in unstable configuration changes. And 40 percent of downtime by operator errors, including not performing a required operations task or performing a task incorrectly [5]. A recent Enterprise Management Association report concurs,

Bo Yang is with the Department of Distributed Computing and Service Management, IBM Research - China, BJ 100193 China. (e-mail: yangbbo@cn.ibm.com).

indicating that more than 60 percent of IT infrastructure problems are the direct result of change [6]. How to control the risk of change and negative effect is an open question.

Our work focuses on improving change & configuration management quality in a change process which is enhanced by introducing sync audit with RFC ticket and knowledge database (KDB). It provides analysis essential to configuration management in a complex IT infrastructure environment including change history, change impact assessment, and differentia between expected change and actual change. This information is organized in relational models based on a sync audit with RFC ticket. It works with data capture and analysis systems to support resource discovery, job scheduling, and management visibility.

II. Problem Analysis

ITSM has received growing attention from both the academia and the industry. An important and challenging subject in ITSM is configuration management.

Configuration management is characterized by configuration items' wide distribution, changeable and dynamic functions as well as diversified forms. It works closely with change management for providing the entire collection of systems landscape to make sure any changes made to one system do not adversely affect any of the other systems.

A recent survey by IDC with corporate executives reveals that the executives require access to trusted and reliable information in a timely manner [7]. However, most enterprises are flooded with large scale data and content scattered in many systems and sources, and in multiple forms. The volume and variability of such information continues to increase, including application configurations, network configurations, OS configurations, service status, CPU usage, memory usage, transaction workload, transaction response time, etc. Sharing information and ensuring that the most appropriate views are discovered and used for their intended and changing purposes can be daunting given the many layers of hard-coded and semantic dependencies built within typical applications and systems. Furthermore, it is quite inefficient and disconcerting that different applications apply their respective approaches in a very fragmented, redundant, and inconsistent manner.

For centralizing configurations control, the CMDB [3, 8] has been proposed that focuses on how organizations are positioned to extract value and raise competencies to address their unique information requirements. The concepts underlying CMDB include information governance, change management, as well as the development and maintenance of a flexible information infrastructure. CMDB is intended to be an infrastructure approach to coordinating data-oriented service and integration functions in a dedicated fashion. It provides connectivity to a vast amount of data and delivers relevant information, consolidating these functions in a unified fashion.

However, in fact, beyond recording all configuration items and change history of hardware and software used in IT environment, differentia between authorized change and actual change is more important for change risk control.

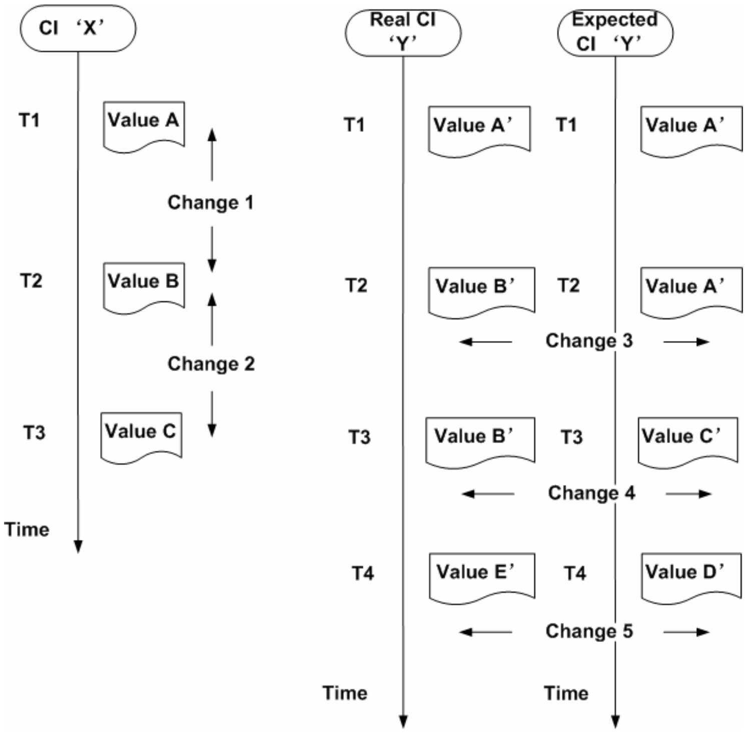

Fig.1. Gap in existing configuration management

Gap between existing configuration management and requirement of risk control on change is shown as Fig.1. Besides traditional change history 'change 1' & 'change 2' in CMDB, the differentia between real change and expected change for risk control can be divided into three classes:

- **Unauthorized change.** Those changes (e.g. 'change 3') on the configuration items are illegal without change improvements. With the change, there is a change track in change history of the unauthorized changed CI, and there is no record in related change process.

- **Unimplemented change.** Executants did not perform a required operations task for authorized change (e.g. 'change 4'). It results in there is a record in change process indicates that an CI has been changed to updated value, however, the value of the CI is same as before in real environment.

- **Incorrectly change.** Executants did a change for authorized change, but performed a task incorrectly (e.g. 'change 5'). The result is that value of a CI is not the expected as authorized one in request for change.

All of the differentia will lead ITSM administrator to make improper decision with inaccurate information.

Furthermore, it is not sufficient simply to record all the information on systems and operations in CMDB. Without the assistance of change impact assessment with domain knowledge, change audit can easily get confused and be lost in low-level redundant details.

III. Sync Audit for CMDB

When studying how to provide trusted and reliable information for configuration management, we must consider how to satisfy change management demands from ITSM applications. Since information from a complicated IT infrastructure discovery is not the only data needed for configuration management, in this paper, we advocate a sync audit strategy with RFC ticket and knowledge-enhanced audit analysis services. The RFC ticket represents the record of request for change in change management. To organize authorized change and actual change on configuration items (CI), sync audit introduces authorized CI and actual CI for indicating the target CI in authorized change process and the one in real IT environment. Sync audit of configuration management is for ensuring that board-approved change directives are implemented, and checking the unauthorized change by comparing authorized CI with actual CI.

Information of CI is classified into a version according to its capture time. As shown in Fig. 2, all information around a RFC ticket lifecycle is regarded as a version of related system description.

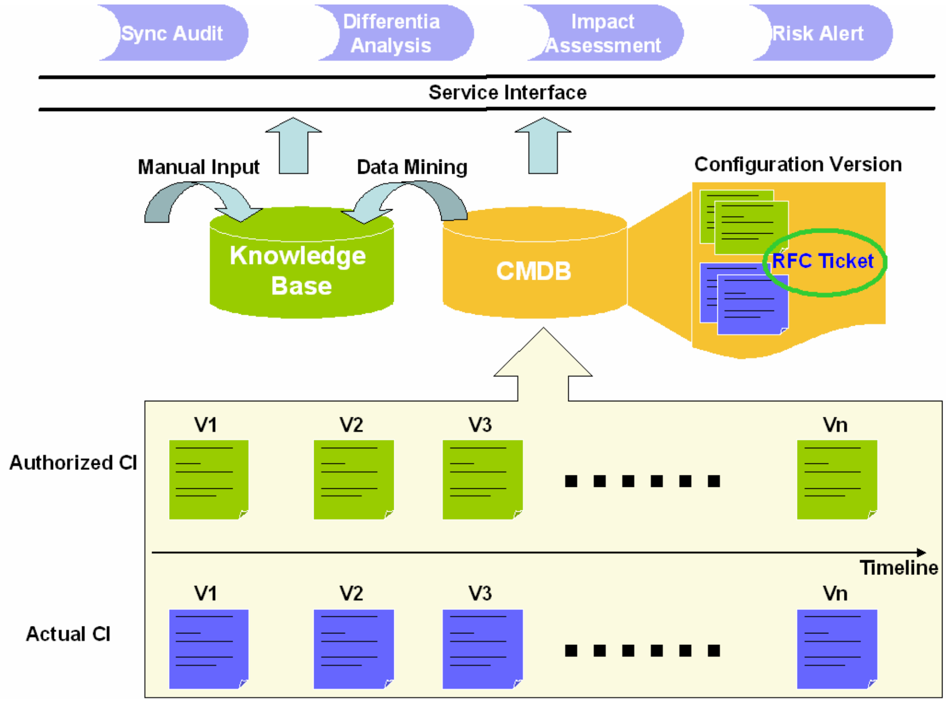

Fig.2. Sync audit with RFC ticket and knowledge-enhanced audit analysis services

Sync audit strategy provides the differentia analysis between authorized CI and actual CI in the version after the RFC ticket lifecycle. The conflicting CI will invoke an impact assessment for any potential affect on other CIs with knowledge base. Owner of those impacted CI will be notified for potential risk control.

After differentia analysis, the authorized CI will be sync with actual CI to reflect the real situation, which is to provide accurate information to change approver for subsequent RFC assessment.

In particular, for a version, sync audit with RFC ticket of the configuration change provides tremendous added value to other application services such as conflict detection, performance analysis and problem diagnosis etc. It is almost impossible for a traditional CMDB containing only CI change history to provide such added value. Sync audit with RFC ticket also provides the audit trace of change management, which can indicate what configurations have been used to meet special business requirements when the RFC ticket is combined with configuration information.

Moreover, a knowledge database is introduced to store not only the risk rank of differentia, but also extended patterns and rules that ITSM operators define in the course of their work. In a distributed environment, this strategy enables ITSM operators to share their domain knowledge for different application services. The reuse of experts' knowledge will be effective in reducing the labor cost for complicated IT service management.

IV. Implementation of the Sync Audit

In this section, a proof of concept (PoC) project SA is developed to validate the sync audit for change & configuration management. It is built on Eclipse Toolkit with Java technology, and implements a container for information capture, data organization, differentia analysis, impact assessment, rule and policy definition, risk alert and the GUI of using knowledge. The architecture of SA is shown in Fig.3.

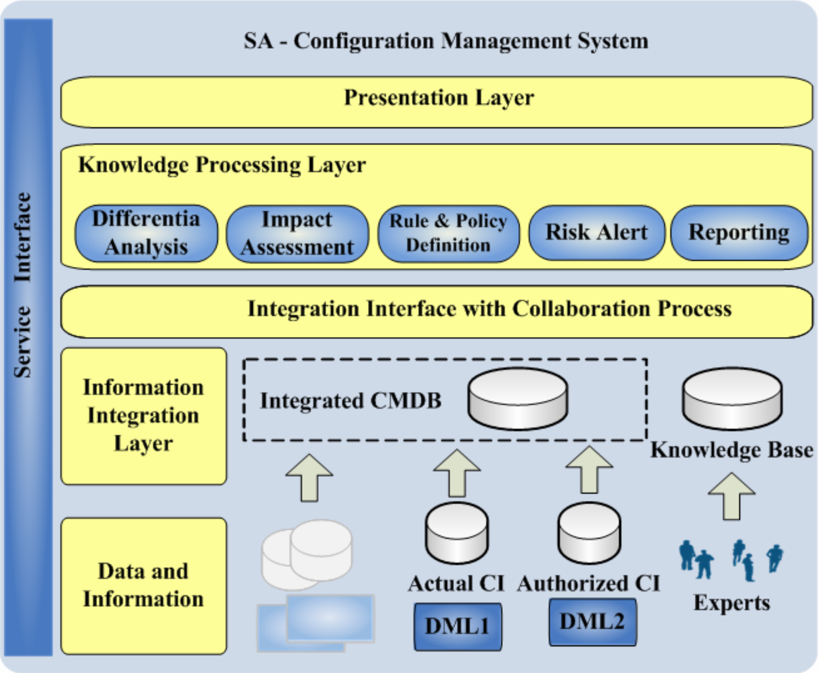

Fig.3. Prototype framework about Sync audit for configuration management system

A. *Sync Audit Strategy for Information Coordination*

The framework of SA is shown in Fig. 3, in which a data capture platform, a data integration & knowledge processing layer, and a data presentation platform are constructed to provide information services.

After data is captured from target systems, it needs to be coordinated to represent the target systems. For data coming from diverse sources with different capture schedule, a loose composite data model is proposed to synchronize data by RFC ticket, compose the diverse CI data, and store the composed data in a CMDB. A synchronized data model in xml is introduced in the prototype. All of the data in a version represents the system status after the RFC implemented. Thus it provides a comprehensive, synchronized view of the target business-IT infrastructure by aligning diverse information.

B. Knowledge-Enhanced Change Audit

Moreover, and most importantly, the knowledge processing layer provides fundamental functions upon the synchronization of data to facilitate change & configuration management. Frequently used data analysis functions such as comparison and change tracking, change impact assessment and reporting, rule and policy definition, risk alert and RFC ticket are provided as utility libraries. Comparison makes it possible to discover what differentia between all authorized CIs and actual CIs is, in which the system can meet the SLA requirement, based on configuration versions with RFC ticket. Impact assessment helps to risk analysis when RFC is coming or an illegal change has been detected. Rule & policy definition constitute risk category, rank and reaction for potential risk. When an expert diagnoses or solves a problem successfully, he can use "Rule & policy definition" to file his solution in knowledge base. Risk alert will notify the owners of impacted CIs result from change impact assessment. And reporting provides fact track for system health check and audit process requirement.

V. Experiment Result and Analysis

We selected a use case that coming from real environment to demonstrate the sync audit with RFC ticket and knowledge database (KDB) for multi-business applications change & configuration management. SA provides a platform for IT change management in a complex IT infrastructure, defines a management domain, and delivers the related data to its manager. Then, with knowledge integration on various impact rules of business impact by impact assessment, an audit analysis services is invoked to analyze a illegal change, such as a database server outage, operation system patch, etc. It returns the impact scope including hardware, software, service, application and so on. Moreover, the reason can be attached to the report automatically because of the shared knowledge repository.

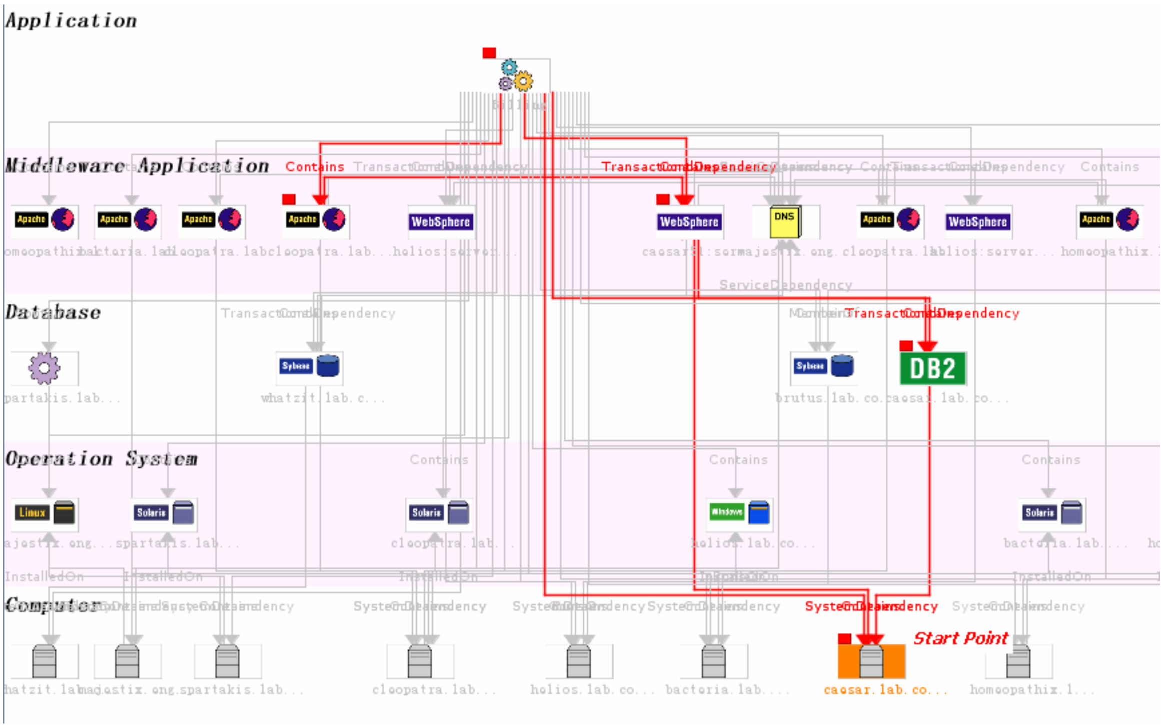

Fig.4. Impact assessment from a specified starting point in target management domain for a detected illegal change

As shown in Fig. 4, an illegal change of IP address has been detected on computer Caesar.lab that will cause the computer inaccessible, expected components that will be impacted are marked with red cubes and lines when the "Impact Assessment" is invoked.

Four components will be impacted because of the illegal change on starting point in the target application domain with 33 components. From the starting point, a DB2 instance will be impacted because it runs on the host Caesar.lab while the computer will be inaccessible. A Websphere server that depends on the DB2 instance will be impacted because of the effect on the database. Then an Apache server will be impacted because it depends on the Websphere server. Furthermore, a business application "Billing" in the top layer will be impacted because its components have been affected. The assessment result shows the impacted scope for a configuration change on computer Caesar.lab, which beyond the database expert concerns that focus on the database issue when "Billing" manager combined with experts' knowledge on Hardware, Database, Middleware etc. After impact assessment, risk alert is invoked to notify the owner of the impacted CIs for risk control.

This case provides a whole picture for a user to review what is potential risk (impacted CIs) when a illegal change is detected by SA, which will help him to make an appropriate decision more quickly, more accurately, less expensively, and with more visibility than silos of management model might be able to achieve the management purpose.

VI. Conclusion

In this paper, we have presented a sync audit with RFC ticket and knowledge-enhanced audit analysis services to improve change & configuration management quality. From the risk analysis experiments on the distributed application system, we can conclude that knowledge-enhanced change audit is effective and efficient, and provides significant improvement on change & configuration management quality. This paper represents our initial effort. Further investigation will be conducted and reported in the future.

References

[1] Vibhore Kumar, Brian F. Cooper, Greg Eisenhauer, Karsten Schwan: iManage: Policy-Driven Self-management for Enterprise-Scale Systems. Middleware 2007: 287-307

[2] HP BTO software: Optimize the business outcome of IT, White paper, 4AA0-8911ENW, Nov. 2006, Available: http://www.hp.com.

[3] H Madduri, SSB Shi, R Baker, N Ayachitula, L Shwartz, M Surendra, C Corley, M Benantar, S Patel, "A configuration management database architecture in support of IBM Service Management," IBM Systems Journal 46:33, 441-457, Jul., 2007.

[4] Van Bon, J., Kemmerling,G., Pondman, D., IT Service Management: An Introduction, Van Haren Publishing, September 1, 2002.

[5] Scott, Donna. "Making Smart Investments to Reduce Unplanned Downtime", Tactical Guidelines Research Note TG-07-. 4033, Gartner Group, Stamford, CT, March 19 1999.

[6] Enterprise Management Associates Inc., EMA Product Brief, 2007

[7] Rogers, S.: Information as a Service to the Enterprise. White paper, December, 2006.

[8] Berkhout, M., Harrow, R., Johnson, B., Lacy, S., Lloyd, V., Page, D., van Goethem, M., van den Bent, Welter, G.: Service Support: Service Desk and the Process of Incident Management, Problem Management, Configuration Management, Change Management and Release Management, London: The Stationery Office. 2000.