IT service management automation – An automation centric approach leveraging configuration control, audit verification and process analytics

Naga Ayachitula[1], Melissa Buco[1], Yixin Diao[1], Bradford Fisher[2],
David Loewenstern[1], Chris Ward
[1] IBM Thomas J Watson Research Center
Hawthorne, NY 10532
[2] IBM
RTP, NC 27709
{nagaaka, mjbuco, diao, bradfish, davidloe, cw1}@us.ibm.com

Abstract. People, processes, technology and information are the service provider's resources for delivering IT services. Process automation is one way in which service providers can reduce cost and improve quality by automating routine tasks thereby reducing human error and reserving people resources for those tasks which require human skill and complex decision making. In this paper we propose a conceptual methodology for IT service management process automation in the area of configuration control, audit verification, and process analytics. We employ a complexity model to assist in identifying the opportunities for process automation. We recommend and outline an automated approach to the complex task of variance detection of the hierarchically defined Configuration Items in a Configuration Management Database (CMDB) against the Configuration Items in the IT environment. We also recommend the integration of this automated detection with human centric remediation for resolving the variances detected and outline an automated approach to the variance detection.

1 Introduction

Today's IT environments are generally large, complex, distributed, and constantly being changed. Although most changes are intended to fix or improve the environment, they can often have unexpected, undesirable, and costly effects on the environment. Therefore, it is recommended by best practices such as ITIL [1], the recognized standard for IT service management, that configuration of the environment be maintained in a CMDB and be carefully controlled. The CMDB includes attributes of and relationships between the configuration items (CIs) in the IT environment and serves as a source of authorized configuration information that can be used by all of the other ITIL processes. It also maintains relationships between configuration items and other Service Support artifacts (e.g. Change Records and Incident Records). Because the CMDB serves as the source of information for decision making by many other process, the accuracy of the CMDB is important. Therefore, regular audits are needed to verify that the CMDB correctly reflects the environment. This is an opportunity to detect and correct any errors in the CMDB as

well as unauthorized changes that have been made to the IT environment. For an environment of even moderate size, these activities are time consuming and prone to human error which makes them prime candidates for automation.

2 Configuration control, Audit Verification and Remediation

The Configuration Management process ensures accuracy by imposing configuration control, that is, by requiring controlling documentation for changes to information in the CMDB. [2] Thus the CMDB can then be regarded as repository of authorized information about CIs. The intent of configuration control is to prevent unauthorized changes to the IT environment and the CMDB. It is up to the discretion of the Configuration Manager to establish the policies regarding the extent and content of the controlling documentation required for a change. Correctness the contents of the CMDB can be ensured by regularly comparing against the actual IT environment. This requires discovering, either manually, via automated scans, or import from an authorized source information on what is actually in the IT environment. This gathered data may come from a variety of sources. The actual data may then be compared with that which was authorized in accordance with Configuration Management process to detect variances. Before comparison against the authorized data in the CMDB, the gathered data must be normalized and multiple sources reconciled. Based on the type of variance (e.g. unauthorized changed in the environment) an appropriate remediation is enacted.

3 Automation centric remediation leveraging configuration control, audit and remediation and process analytics

The proposed methodology calls for using the IT complexity modeling tool to determine in a given business process which of the activities demand extensive coordination, communication, collaboration and require human interaction versus identifying repeatable patterns of activities that can be effectively automated, as illustrated in Figure 1. Below is an overview of the proposed automation in Figure 1.

1. Define which configuration item types should be part of the audit. Relationships between configuration items can be extensive. In order to make the comparison process feasible some scope for comparison has to be established around which set of CI relationships to compare. The scope in the proposed automation limits the CI relationship comparison to CI relationships which transverse “down” the CI relationship tree as defined in the authorized CI definition template.
2. Define the link rules for Authorized CI types to Actual CI types. A link rule provides a mechanism to uniquely identify CI instances. A link rule is typically one or more sets of attributes and criteria.
3. Search and retrieve all authorized CI instances for identified audit CI types.
4. Search and retrieve all actual CI instances for identified audit CI types.

5. Use the CI definition as a template to compare authorized CI instances with actual CI instances. The authorized CI template defines what CIs and relationship types to compare and how deep the compare should be.
6. Write audit comparison and variance results.

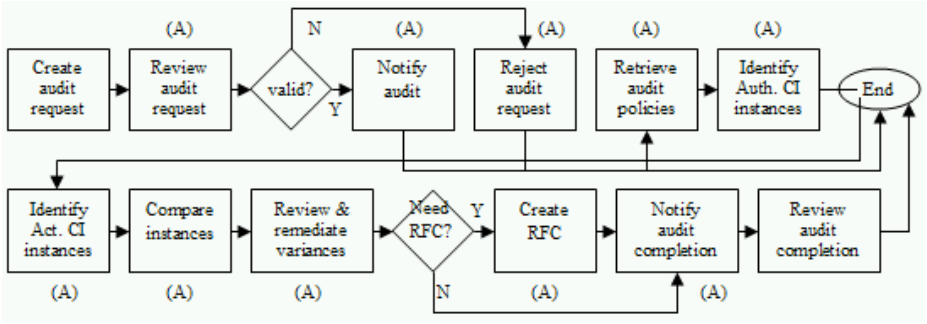

Figure 1. Automation centric remediation process - activities labeled as (A) are automated activities.

For the authorized CI to actual CI comparison, once the auditable CI data set is returned and the links are established between instances, comparison of the relationship and attributes for the CIs returned in the link and for all subsequent lower level CIs down the tree are also compared. For each comparison a result is written to the audit results.

4 Evaluation using IT process complexity model

We conducted a complexity evaluation for the process represented in Fig.1. Our discussion is based on the IT management complexity framework described in [3]. The per-task complexity was computed based on the complexity metrics introduced above along the three complexity dimensions. For example, task 7 compares and identifies variances between authorized and actual CI instances and involves high business item complexity. Once the per-task metrics have been computed, they can be aggregated to produce process-wide views to identify the complexity bottlenecks within this process and process-wide metrics to facilitate cross-process comparison. Per-task views are graphs showing all per-task metrics in bar charts. Fig. 2 provides a per-task view for all 11 tasks. The x axis indicates the tasks and the y axis indicates the metric values. All per-task metrics can be plotted separately or aggregated for three high-level views of execution complexity, coordination complexity, and business item complexity. The overall process complexity metrics are summarized in Table 1. We also conducted complexity evaluation for the automated process. As shown in Figure 2 and Table 1, tasks 2 to 7 and 9 to 10 have been automated and so have zero complexity associated with them. This reduces the number of tasks of this process from 11 to 3. In addition, automation also reduces the number of business items in this process from 8 to 2, since most of the required business items can be acquired and applied automatically in the new process.

5 Conclusions

Configuration control and audit verification exemplify areas which can benefit significantly from integration of as much automation as maturity and technology permit with human centric interactions for tasks such as remediation which are most efficiently handled by a human assisted by appropriate tooling. In this paper, we described a conceptual methodology for IT service management process automation in the area of configuration control, audit verification, and process analytics. We employed a complexity model to assist in identifying the opportunities for process automation. We outlined an automated approach to variance detection between authorized and actual and recommended integration of this automated detection with human centric remediation for resolving the variances detected.

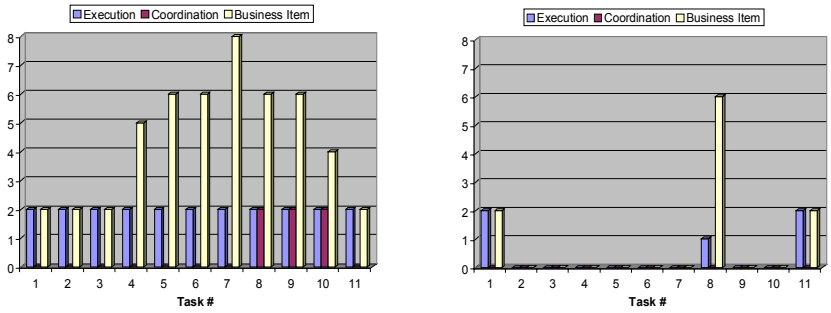

Figure 2: Per Task View of Processes without/with Automation

Table 1: Complexity metrics for audit and remediation process in Figure 1

Complexity Measure	Metric	Value Before	Value After
Execution	Number of Tasks	11	3
Coordination	Number of Shared Tasks	0	0
	Number of Cross-Role Links	2	0
Business Item	Number of Business Items	8	2

References

1. ITIL The Key to Managing IT Services: Service Support Version 2.3, (TSO for OGC), 2000.
2. Information technology — Service management, (ISO/IEC 20000).
3. Diao, Y., Keller, A.: Quantifying the complexity of IT service management processes, Proceedings of the 17th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management, Dublin, Ireland (2006) 61–73.