IT Change Management Tracking Tools

[1]Khalid A. Al-Khathlan, [2]Jumana F. Alturairi, [3]Lamia T. AlSulaiman

Dhahran, The Kingdom of Saudi Arabia

Abstract: As IT services are essential for all business operations, the ability to control the changes implemented in the IT infrastructure is significant in order to maintain the IT availability, reliability and security. The most important key to have a secure and well-defined structure for change management process is to have a mechanism to maintain a record of all changes implemented in the IT infrastructure despite the change type whether its authorized or unauthorized. Several issues encountered without having a tool to detect/ trace IT changes, which might exploit a vulnerability to breach security and thus cause huge impact such as system failure, higher cost, business impact, security threats, undocumented changes and loss of revenue.

This article describes the process of storing, tracking, preventing and detecting configuration changes implemented in the IT infrastructure.

Keywords: Information Technology, IT Change Management, Configuration Changes Tracking Tools, Trace, Unauthorized Changes.

I. INTRODUCTION

Information Technology (IT) services plays a significant role to enable business organization to perform their day-to-day operations. Any unexpected outages in IT services may cause major financial loss due to business disruption. However, there are mandatory alterations executed frequently in IT infrastructure due to introducing, enhancing, modifying, replacing, or removing assets/services. Controlling the lifecycle of all alterations in the IT infrastructure is the responsibility of IT Change Management (ITCM). This is essential to ensure the security, availability, and reliability of the IT Infrastructure by eliminating the disruption of business and maximize IT services readiness towards customer satisfaction. A comprehensive study was conducted to figure out the best practice to detect/trace IT changes.

II. CHANGE MANAGEMENT TRACKING TOOLS

The best approach to automate detecting unauthorized changes is through configuration changes tracking tools. The main functions of these tools are to trace unauthorized changes within the IT infrastructure, validate compliance and store configuration changes. The ultimate goal is to have a well-controlled and secured IT environment with emphasis on availability, security and compliance covering designing, implementing and validating stages through tracking and configuration tools.

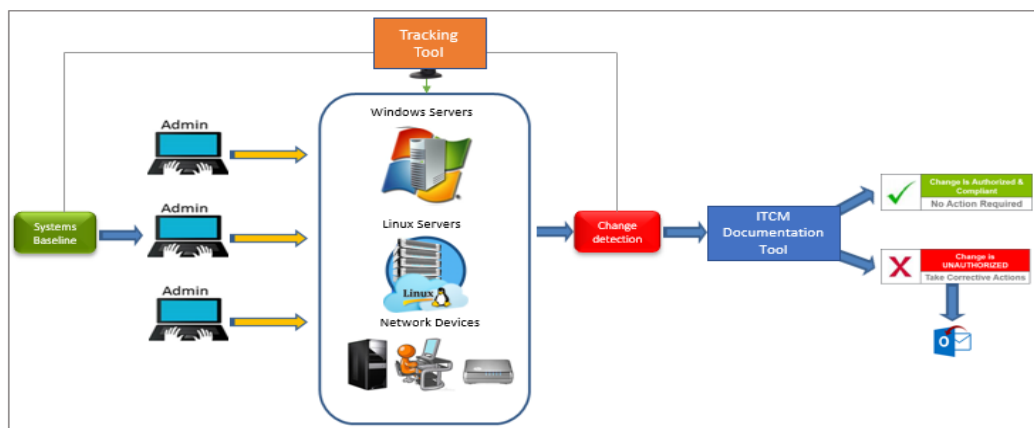### A. Configuration Changes Tracking Tool Mechanism

Figure.1 Tracking Tool Process

Research Publish Journals

Configuration changes tracking tools will detect all changes implemented on IT infrastructure as follow;

• **Step1:** The tool will capture data/configuration within IT infrastructure components and save it in a file as a baseline for that component.

• **Step2:** In the next day, it will check the components data/configuration and compare it with the baselines.

• **Step3:** If there was any modification to the baseline (including add, remove, or change to the configuration), tracking solution will check if there is an approved change request or Trouble Ticket related to this component within the same period:

o If there is a valid change request or incident ticket, this modification is considered as authorized change

o If not, this modification is considered as an unauthorized change

• **Step4:** Tracking tool will send an automation email to the implementer, to justify the unauthorized changes for specified period.

• **Step5:** ITCM should assess and evaluate the case to take the proper action.

B. Evaluation

Feasibility study is essential in order to determine the most appropriate tool based on change management requirements. The following are steps for configuration changes tracking tools evaluation:

• Identify the Scope of IT Infrastructure Components

• Define Solution Evaluation Criteria (Minimum Requirements) such as:

o **Real time tracking and alert:** New solution should provide real time alerts mechanism once an improper change occurs (Immediate Alert)

o **Integrated with ITCM documentation tool:** The key criterion is the integration with ITCM documentation system where it should be capable to check the compliance status of each change

o **Compatible with most industrial systems and devices in IT infrastructure**: Solution must be suited with most industrial system and devices in IT infrastructure covering network devices, applications, databases and servers

o **Reporting feature:** The solution requires reporting feature in order to document all devices information such as Name, Number, and Owner...etc. Also, generate a report for all changes implemented on IT infrastructure components and be able to demonstrate the previous information and compare it with the updated one to identify who made the changes, what changes were made, when the changes were made, and where the information is available

o **Life dashboard mechanism:** Dashboard mechanism is essential in order to provide real-time views of changes and color-coded by priority and even pinpointed on maps to know where to focus attention first.

• Prepare Evaluation Questions such as:

o How much does it utilize the bandwidth?

o Is it user friendly?

o Is there a local vendor?

o Is there a local support and level of support?

o What is the life time cycle of the system?

o What is the total cost of running the system?

o What is the license type and cost?

o Is there any training?

o What is the roadmap of the system?

- Evaluate In-House Products

- Evaluate Initial Market Products

III. CONCLUSION

In conclusion, clear organization requirements along with conducting a benchmark study to determine the best practice and validate the historical record are essentials in order to select the suitable solution and process for storing, tracking, preventing and detecting configuration changes.

REFERENCES

[1] How to Automate Server Provisioning and Configuration Management by Analysts Paul Delory, Gregg Siegfried Published 23 December 2020 - ID G00718850 - 76 min read

[2] ITSM Best Practices: A Guidance Framework for Implementing a Configuration Management Database By Analysts Steve White, published 31 March 2021 - ID G00720852 - 62 min read