American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-11, Issue-10, pp-44-47
www.ajer.org
Research Paper Open Access

Simplification of Security Update Deployment for IT Services

Premanandh Devarajan
Senior Program Manager, Wipro Limited
7529 Rhyner Way, Fort Worth, Texas, United States

ABSTRACT : *Deployment of Microsoft Security update to Windows Servers requires the use of custom deployment tool for simplifying the process, avoiding humanerrors and to have better control of its deployment with 4-eye principal which helps in avoiding mistakes leading to unplanned deployments. In this paper, the topologies for how to deploy security updates and how to implement custom deployment control tool in larger infrastructure are presented.*

KEYWORDS:*security updates, impact, monitoring.*

Date of Submission: 07-10-2022 Date of acceptance: 19-10-2022

I. INTRODUCTION

Security updates are nothing but pieces of software code that are written to fix a bug in a windows operating system that might lead to vulnerability. Such vulnerabilities in any operating system are loop holes for attackers to get their hands on business-critical data and information. So it is highly crucial to keep all the windows servers in a network updated to its latest security updates.

Microsoft releases security updates on the second Tuesday of each month. Predominantly security patch updates of varying severity like Critical, Important, Moderate & Low are labeled and released. It is always a best practice to prioritize your patching based on the severity level mentioned.

When managing larger IT infrastructure with **25,000** windows servers including factory managed systems through SCCM (System Center Management System), highest care should be taken when creating custom collections and scheduling deployment of security updates. If any miscalculation of date time conversion from one time zone to another, selecting wrong date can lead to unplanned downtime to business-critical servers. To avoid human errors, custom deployment tool is developed with 4-eye processes (Doer-Checker), where one user (Doer) will create collections in SCCM and another user (Checker) will verify and approve the collections in deployment system. Same process is followed for creating deployments. Second user will verify the members in collection and verify the date/time and approve the deployment.

II. SCCM DEPLOYMENT CONTROL SYSTEM

The main goal of this deployment control system is to automate and include 4-eye processes (Doer-Checker) in below tasks where there is high risk involved in large infrastructure environments.

The main objectives:

- Creating custom collections
- Validating collections list
- Restrict members count in collections
- Creating deployments
- Monitoring the deployment status
- Monitor system performance over time
- Analyze errors and their causes

Doer (SCCM Analyst) will create custom collections by providing the list of servers in the tool. Checker (Approver) will validate the collections created by doer.Every deployment on production servers should have a valid incident or change request ticket associated with it. Custom Deployment tool will not allow creation of Collections/Deployment without ticket. Once approved by Checker, tool will send communication to stakeholders.

Summary of Deployment control tool is,

- For every task, it will save & send notification mail with authorization code to approvers
- Will alert the user with warning messages and also it will limit the scope of collections
- Once approver verified and approved, the tasks can be executed from control system
- Logging is enabled for every action

Fig.1 shows the connectivity between SCCM servers and the deployment control system. The system is capable of performing real-time monitoring of deployment that can be monitored via intranet website.

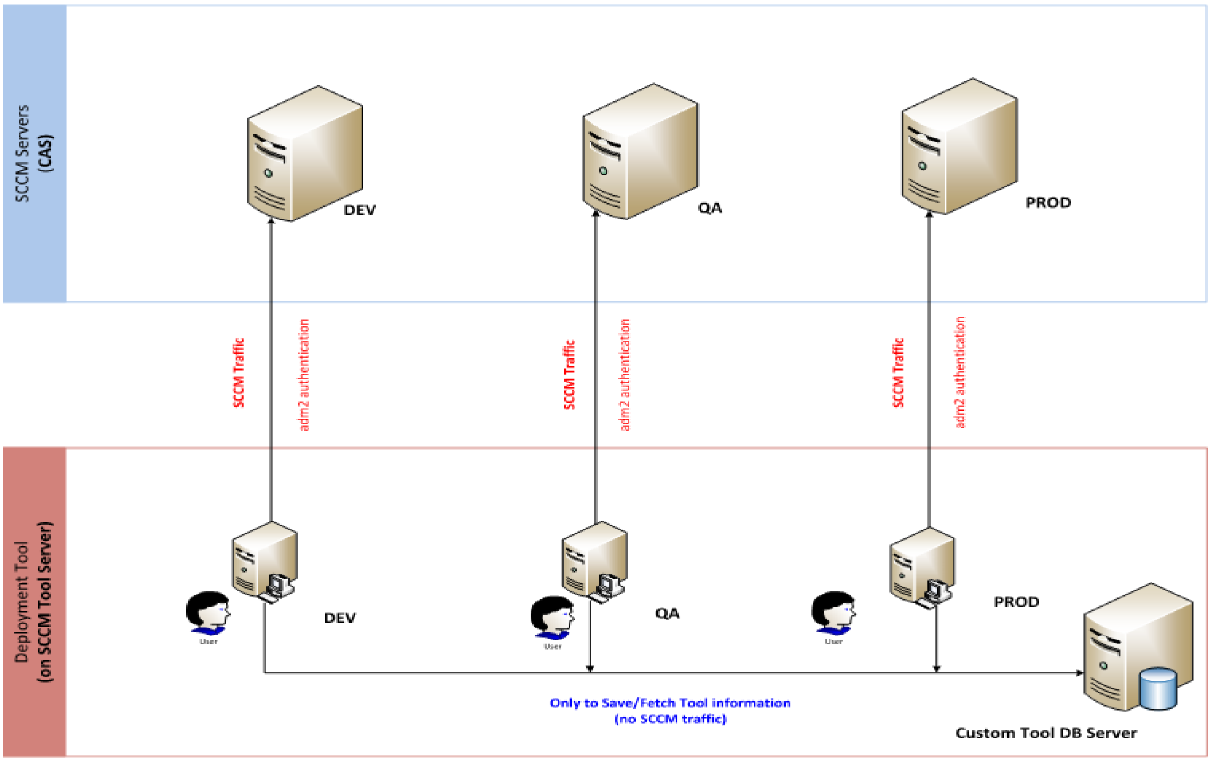

Fig.1. Connectivity and Traffic flow

Fig. 2 shows the general workflow of deployment control system.

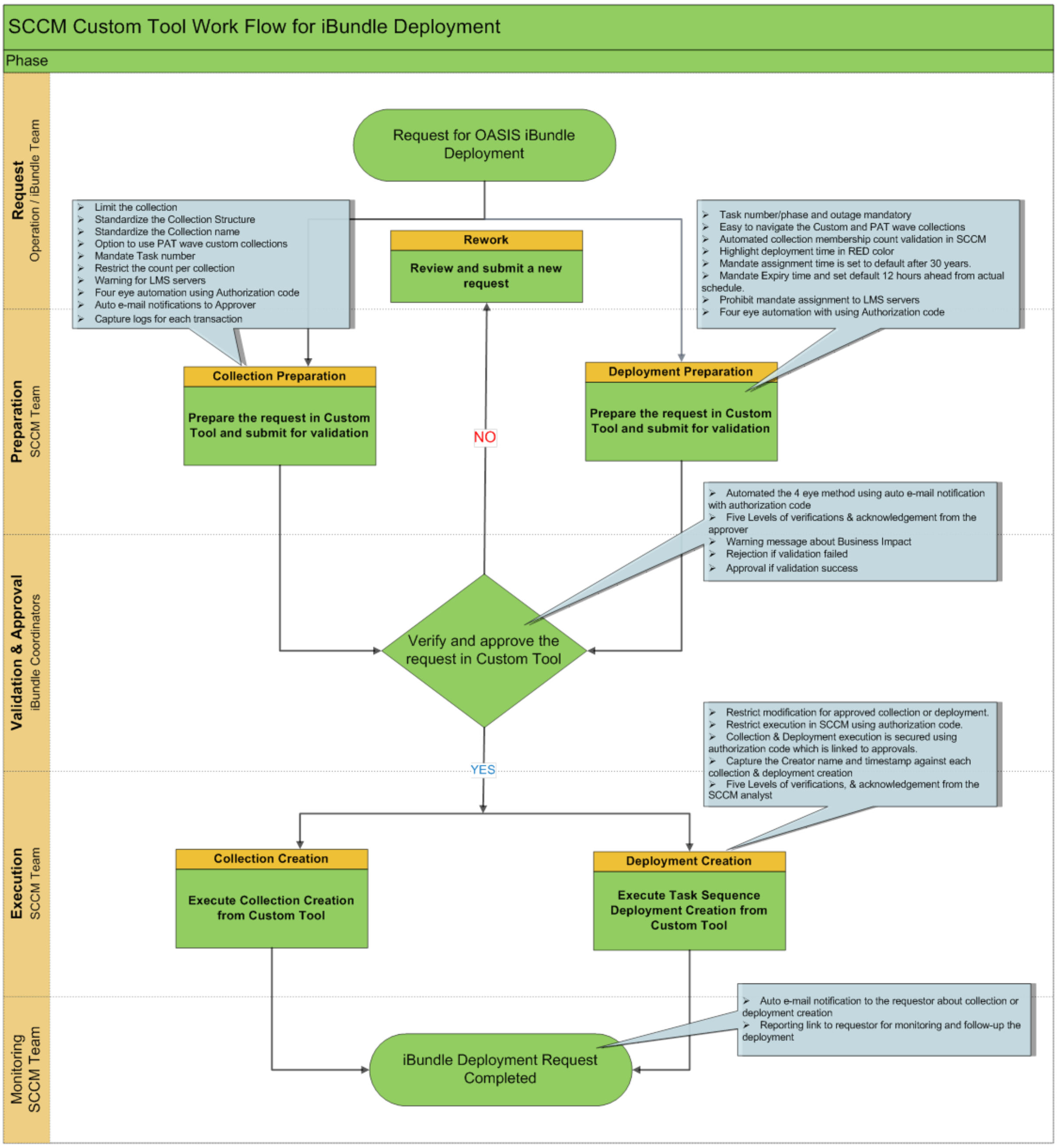
SCCM Custom Tool Work Flow for iBundle Deployment
Phase
Request
Operation / iBundle Team
Preparation
SCCM Team
Validation & Approval
iBundle Coordinators
Execution
SCCM Team
Monitoring
SCCM Team
Request for OASIS iBundle Deployment
Limit the collection
Standardize the Collection Structure
Standardize the Collection name
Option to use PAT wave custom collections
Mandate Task number
Restrict the count per collection
Warning for LMS servers
Four eye automation using Authorization code
Auto e-mail notifications to Approver
Capture logs for each transaction
Rework
Review and submit a new request
Task number/phase and outage mandatory
Easy to navigate the Custom and PAT wave collections
Automated collection membership count validation in SCCM
Highlight deployment time in RED color
Mandate assignment time is set to default after 30 years.
Mandate Expiry time and set default 12 hours ahead from actual schedule.
Prohibit mandate assignment to LMS servers
Four eye automation with using Authorization code
Collection Preparation
Prepare the request in Custom Tool and submit for validation
NO
Deployment Preparation
Prepare the request in Custom Tool and submit for validation
Automated the 4 eye method using auto e-mail notification with authorization code
Five Levels of verifications & acknowledgement from the approver
Warning message about Business Impact
Rejection if validation failed
Approval if validation success
Verify and approve the request in Custom Tool
YES
Restrict modification for approved collection or deployment.
Restrict execution in SCCM using authorization code.
Collection & Deployment execution is secured using authorization code which is linked to approvals.
Capture the Creator name and timestamp against each collection & deployment creation
Five Levels of verifications, & acknowledgement from the SCCM analyst
Collection Creation
Execute Collection Creation from Custom Tool
Deployment Creation
Execute Task Sequence Deployment Creation from Custom Tool
Auto e-mail notification to the requestor about collection or deployment creation
Reporting link to requestor for monitoring and follow-up the deployment
iBundle Deployment Request Completed

Fig.2 General Workflow

III. ADMIN MODEL

Deployment control system has three types of user roles (User, Approver, and Administrator). User can able to create custom collections, deployments. Approver can able to Approve/Reject the collection/deployments. Administrator can able to create new users and also have approver rights.

Approver can be a Peer, Shift Lead, L3 Analyst, Coordinators, and Manager.

Activities	**User (Doer - SCCM Analyst)**	**Approver (Checker)**	**Administrator**
Create/View SCCM Collections	X		
Create/View SCCM Deployments	X		
Approve / Reject Collections & Deployments		X	X
Create/Modify/Delete Users			X

Report the summary of deployment			X
Perform SCCM agent client health	X		
Site configuration SCCM settings			X
Initiate OTP re-send			X

IV. CONCLUSION

There are many benefits to installing a SCCM deployment control system — some of which strongly interrelate with each other. A properly designed deployment system offers a safe and controlled deployment of security updates to all Windows servers in a very large environment.

Benefits of using custom deployment control system

1. Avoids business loss
2. Reduces downtime
3. Saves time and resource utilization
4. Ensures better customer satisfaction

REFERENCES

[1]. Microsoft Reference
https://msdn.microsoft.com/en-us/library/cc145320.aspx

[2]. Creating Applications in Configuration Manager
https://learn.microsoft.com/en-us/mem/configmgr/apps/deploy-use/create-applications

[3]. Deploying Applications with Configuration Manager
https://learn.microsoft.com/en-us/mem/configmgr/apps/deploy-use/deploy-applications