SOFTWARE UPDATE PATCH MANAGEMENT

PATCH MANAGEMENT

Windows patch management is the process of managing patches for Windows, from scanning for and detecting missing patches to downloading and deploying them. Also generate reports for you to confirm whether Windows patches have been deployed properly.

SCCM SUP Pre-requisites & configurations

In SCCM **"Software Update Point (SUP)"** must be installed and configured to patch required machines O.S.

Prerequisites of SUP installation:-

1. IIS
2. WSUS(Window server update service)
3. WSUS Admin Console
4. WUA(Windows update Agent)
5. Port 8530(http) & 8531(https), we can also use 80 and 443 but prefer to use custom ports because it is self -updating all virtual directory information in default IIS websites.

NOTE: - The software update point site system role must be created on a server that has WSUS installed. The software update point interacts with the WSUS services to configure the software update settings and to request synchronization of software updates metadata.

Types of windows updates:-

Microsoft release patches by every 2nd Tuesday of month.

Critical update

A widely released fix for a specific problem that addresses a critical, non-security-related bug.

Definition update

A widely released and frequent software update that contains additions to a product's definition database. Definition databases are often used to detect objects that have specific attributes, such as malicious code, phishing websites, or junk mail.

Driver

Software that controls the input and output of a device.

Feature pack

New product functionality that is first distributed outside the context of a product release and that is typically included in the next full product release.

Security update

A widely released fix for a product-specific, security-related vulnerability. Security vulnerabilities are rated by their severity. The severity rating is indicated in the Microsoft security bulletin as critical, important, moderate, or low.

Additional information

Microsoft security updates are available for customers to download and are accompanied by two documents: a security bulletin and a Microsoft Knowledge Base article.

Service pack

A tested, cumulative set of all hotfixes, security updates, critical updates, and updates. Additionally, service packs may contain additional fixes for problems that are found internally since the release of the product. Service packs may also contain a limited number of customer-requested design changes or features.

Tool

A utility or feature that helps complete a task or set of tasks.

Update

A widely released fix for a specific problem. An update addresses a noncritical, non-security-related bug.

Update rollup

A tested, cumulative set of hotfixes, security updates, critical updates, and updates that are packaged together for easy deployment. A rollup generally targets a specific area, such as:

- Security
- A component of a product, such as Internet Information Services (IIS).

Software Update Management can be broken down in to four main components:

- **Synchronization**
- **Compliance**
- **Deployment**
- **Reporting (will not covered in this document)**

Synchronization

Software updates synchronization starts. Synchronization can be initiated either manually or on a schedule.

When synchronization is initiated on a schedule, WSUS Synchronization Manager (**WSyncMgr**) wakes up on the configured schedule and initiates synchronization: you can check **WSyncMgr.log.**

Apply filter and create SUG (software update group):- Once Metadata is synchronized we need to filter the required update create software update group and then download the patches available in group for Distribution purpose: **you can check PatchDownloader.log.**

Compliance

Software update scan process on client side

Step 1: Scan Agent requests the scan and WUAHandler initiates the scan

Step 2: Windows Update Agent (WUA) starts the scan against the WSUS computer

Step 3: WUAHandler receives the results from the Windows Update Agent and marks the scan as complete

Step 4: WUAHandler parses the scan results

Step 5: Update store records the status and raises a state message for each update in WMI

Step 6: State messages are sent to the management point

LOGS you can check: - scanagent.log, ccmMessage.log, updatestore.log, locationservices.log

For complete details check: - https://docs.microsoft.com/en-us/troubleshoot/mem/configmgr/track-software-update-compliance-assessment#software-update-scan-on-clients

DEPLOYMENT

Distribute and Deploy patches: - Once patch downloaded & scan completed you need to place the deployment and mention important information in deployment like:

i. Maintenance windows
ii. Reboot Suppress for prevention of servers and workstations
iii. After maintenance window behaviour

1. **Policy Agent receives the policy after deployment: -** retrieval automatic or on schedule. When policy is received, the following are logged in **PolicyAgent.log.**

2. After the policy is evaluated, the scheduler for the deadline is evaluated. This operation is done by the Scheduler component. **You can check: - Scheduler.log file.**

   ALSO, at the scheduled deadline, Scheduler notifies the Updates Deployment Agent to start the deployment evaluation process.

3. Updates Deployment Agent starts the deployment evaluation process by requesting a software update scan. The scan ensures that the deployed updates are still applicable. **You can check: - UpdatesDeployment.log.**

4. At this point, the scan request is handled by Scan Agent component. Scan Agent calls WUAHandler to perform a scan and then hands the results back to Updates Handler and Updates Deployment Agent. **You can check: - updatehandler.log and WUA handler.log.**

5. Updates Deployment Agent raises state messages for the deployment to update the current **Evaluation** and **Compliance** state. Here's what we see in **UpdatesDeployment.log.**

6. Updates Deployment Agent now starts a job to download the software update files from the distribution point. Here's what we see in **Updateshandler.log.**

7. Updates Handler starts the download request from Content Access service for the three actionable updates.

8. Content Access service starts a download job for each update and creates a Content Transfer Manager (CTM) job. A CTM job is created for each update separately, and **CAS.log** entries resemble the following for each update: you can check: - **CAS.LOG.**

9. Content Transfer Manager starts working on the download job. It first requests the location for the content that must be downloaded. You can check: - **ContentTransferManager.log & Locationservices.log.**

10. After the download is complete, CTM and Content Access service are notified, and they mark the download jobs as completed. You can check: - **CAS.log.**

11. Windows Update Agent Handler then copies the downloaded binaries to the Windows Update Agent cache (C:\Windows\SoftwareDistribution\Download) directory and instructs Windows Update Agent to start the installation process. We see in **WUAHandler.log.**

12. After the updates are installed, Updates Deployment Agent checks whether any updates require a reboot.

13. After the computer restarts, a post-reboot detection scan is started for the deployment. The scan verifies that updates are installed and raises state messages for the update and deployment to indicate that updates are installed and that enforcement was successful. Check **updatedeployment.log.**

URL Reference for troubleshooting: - https://docs.microsoft.com/en-us/troubleshoot/mem/configmgr/troubleshoot-software-update-management