

? Tanium Patch Blueprint

This page outlines the full configuration blueprint for managing operating system patching in Tanium using standardized scanning, patching, maintenance, and deployment strategies across Windows and Linux platforms.

? Scan Configuration

Windows

[Tanium Scan] - Windows

- Configuration Technique: Tanium Scan
- Scan when new patches are available: ☐
- Frequency: 1 Day
- Groups:
 - All Windows Servers - Physical
 - All Windows Workstations - Physical

[Tanium Scan] - Windows - Virtual

- Configuration Technique: Tanium Scan
- Scan when new patches are available: ☐
- Frequency: 1 Day
- Enable Random Scan Delay: ☐
- Random Scan Delay Value: 120
- Groups:
 - All Windows Servers - Virtual
 - All Windows Workstations - Virtual

[CAB Scan] - Windows Home and Tagged

- Configuration Technique: Offline CAB File
- Download and scan immediately upon new CAB release: ☐
- Groups:
 - Windows Home and Tagged
(Is Windows contains True AND (Operating System contains Home OR Custom Tags equals Patch_Windows_Scan_CAB))

Linux

[Repo Scan] - Linux Repo Scan

- Configuration Technique: Repository Scan
- Use Repositories configured on the endpoint
- Frequency: 1 Day
- Enable Random Scan Delay: ☐

? Patch List

Windows

Patch Tuesday [<Current patch Tuesday mm/dd/yy>]

- Platform: Windows
- Content Set: Patch Content Set
- Rules:
 - Name: Patch Tuesday
 - Conditions:
 - Release Date on or before <The Friday after patch Tuesday>

Linux

Linux Patch List

- Platform: Linux
- Content Set: Patch Content Set
- Rules:
 - Name: First of the Month
 - Conditions:
 - Release Date on or before <First of the current month OR 7 days before the new cycle starts>

? Maintenance Windows

Windows

Windows Workstation - Non-Prod

- Recurrence: Monthly
- Day of week: ☐
 - Starting On: Second Tuesday
 - Day offset: 2
- Duration: 120 hours
- Window Time: Use endpoint local time
- Effective Date and Start Time: 0500
- Target Tag: Patch_Windows_Server_Non-Prod

Windows Workstation - Prod

- Recurrence: Monthly
- Day of week: □
 - Starting On: Second Tuesday
 - Day offset: 6
- Duration: 120 hours
- Window Time: Use the endpoint local time
- Effective Date and Start Time: 0500
- Target Tag: Patch_Windows_Server_Prod

Windows Server - Non-Prod

- Recurrence: Do not repeat
- Window Time: Use the endpoint local time
- Effective Date and Start Time: Sunday after patch Tuesday 0800
- End Time: +8 hours from start
- Target Tag: Patch_Windows_Workstation_Non-Prod

Windows Server - Prod

- Recurrence: Do not repeat
- Window Time: Use the endpoint local time
- Effective Date and Start Time: Second Sunday after patch Tuesday 0800
- End Time: +8 hours from start
- Target Group: All Windows Workstations

Linux

Linux - Non-Prod

- Recurrence: Do not repeat
- Window Time: Use the endpoint local time
- Effective Date and Start Time: Second Sunday of the month 0800
- End Time: +8 hours from start

Linux - Prod

- Recurrence: Do not repeat
- Window Time: Use the endpoint local time
- Effective Date and Start Time: Third Sunday of the month 0800
- End Time: +8 hours from start

? Deployments

Windows

Windows Workstations

- Endpoints to Target: All Windows Workstations
- Deployment Type and Schedule:
 - Ongoing
- Download all package files immediately: ☐
- Patch List: Patch Tuesday
- Restart: ☐
- Post-Notify Users:
 - Duration of Notification Period: 1 Day
 - Final Countdown to Deadline
 - Allow user to postpone: ☐
 - 1 hour
 - 2 hours
 - 4 hours
 - Do not allow user to minimize: ☐
 - Title: **Windows Update - Reboot Required**
 - Body:

“ Critical Windows updates have been installed on this device. To finalize the update, you must reboot within 24 hours. The system will automatically reboot if the update is not completed within this time. You may postpone the reboot by clicking "Postpone" and selecting your preferred time. Any reboot will complete the process.

- Thank you for helping to keep this system secure.

Windows Server - No Reboot

- Endpoints to Target: All Windows Servers
- Deployment Type and Schedule:
 - Ongoing
- Patch List: Patch Tuesday
- Download all package files immediately: ☐

Windows Server - Reboot

- Endpoints to Target: All Windows Servers
- Deployment Type and Schedule:
 - Ongoing
- Patch List: Patch Tuesday
- Download all package files immediately: ☐
- Restart: ☐

Linux

Linux - Reboot

- Content to Deploy: Install All Security Updates
- Endpoints to Target: All Linux
- Deployment Type and Schedule:
 - Ongoing
- Deployment Settings:
 - Download all package files immediately: ☐
 - Restart: ☐

Linux - No Reboot

- Content to Deploy: Install All Security Updates
- Endpoints to Target: All Linux
- Deployment Type and Schedule:
 - Ongoing
- Deployment Settings:
 - Download all package files immediately: ☐

? Reporting

At a minimum, reporting must include the following metrics weekly:

- Current overall compliance by platform (Windows, Linux, Mac)
- Platform compliance by group (non-prod, prod, workstation, server, etc.)
- Mean time to patch

Pre-Patch Audit Criteria

- Patch scan age > 3 days
- Patch scan errors
- System disk free space < 5 GB
- Uptime > 30 days

Revision #2

Created 19 July 2025 02:38:45 by Admin

Updated 16 November 2025 16:32:22 by Admin