IT/Dev CONNECTIONS

Patch Tuesday: Patching Your Endpoints With ConfigMgr

Harjit Dhaliwal
Technology Evangelist
Twitter: @Hoorge
About Me: https://about.me/harjitdhaliwal
Email: Harjit@techkonnect.net

Delivered by KNect365 TMT an Informa business

Agenda

- Facts
- Planning
- Patching Strategies
  - Microsoft Best Practices
  - Common Patching Strategies
  - Scheduling and Selection
- Patching Issues
- Patching Maintenance
  - Software Update Groups
  - WSUS Catalog
- Reporting
- 3rd Party Application Patching
- Server Groups
- Resources

Update Facts

3 parts to updates:

- Update metadata = Update Catalog
  The metadata consist: description, detection logic, and where to download the binaries from
- Update binaries
  Files used to install an update.
- The EULAs (end user license agreements)

Update Facts

- Software Update Point (SUP) is a management layer on top of WSUS. SUP role is to manage WSUS
- ConfigMgr uses WSUS to download update catalog and EULAs
- WSUS doesn't manage approvals or content download
- Update metadata is stored in the WSUS database and replicated to the ConfigMgr database
- ConfigMgr clients communicate with WSUS to get the update catalog and the EULAs
- Intranet ConfigMgr clients get update binaries from distribution points or Microsoft update
- Internet ConfigMgr clients get update binaries from Microsoft update

The Basics

- Patches released on 2nd Tuesday of each month
- Microsoft releases patches at 10:00 AM Pacific Standard Time (PST)
- Cummulative Updates, .NET updates, etc
- Office Updates are released a week before

Harjit's Process

- ADR runs late on Tuesday night
- Software Update Group(s) and Deployments created
- Pay close attention to patch reports / issues
- Manual check of patches
- Enable Deployments in ConfigMgr
- Server collections setup with Maintenance Windows
- Workstations deployed as "Available" / Mandatory later

Plan For Updates

The software update point can support up to 25,000 clients when WSUS runs on the software update point server
WSUS is used with Configuration Manager, and you configure the following settings:
IIS Application Pools:

- Increase the WsusPool Queue Length to 2000
- Increase the WsusPool Private Memory limit x4 times, or set to 0 (unlimited). For example, if the default limit is 1,843,200 KB, increase it to 7,372,800.
- More information: Configuration Manager support team blog post

Resource: Plan for Software Updates

Plan For Updates

Limit of 1000 software updates in a deployment
Limit the number of software updates to 1000 for each software update deployment. When you create an automatic deployment rule (ADR), specify criteria that limits the number of software updates
The ADR fails when the specified criteria returns more than 1000 software updates. Check the status of the ADR from the **Automatic Deployment Rules** node in the Configuration Manager console
When you manually deploy software updates, don't select more than 1000 updates to deploy
Limit the number of software updates to 1000 in a configuration baseline
More information, see Create configuration baselines

Best Practices

- 1000 updates limit for Software Update Groups
- Create a new Software Update Group every month
- Reuse existing Software Update Group for definition updates (Endpoint Protection/Defender)

Microsoft's Best Practices for software updates in ConfigMgr

Common Strategies

- Sync WSUS Catalog and run Automatic Deployment Rules on Patch Tuesday
- Could separate ADRs for Workstations and Servers if preferred
- Select required updates released since last month
- Create multiple deployments for test, pilot, production rollouts
- Roll up older Software Update Groups into a yearly SUG

Patch Tuesday: Not Always 2nd Tuesday

Update for Windows 10 Version 1511 (KB3150513)	3/15/2017 5:00 PM	"Windows 10"
Update for Windows 10 Version 1511 for x64-based Systems (KB3150513)	3/15/2017 5:00 PM	"Windows 10"
2017-05 Cumulative Update for Windows 10 Version 1703 for x86-based Systems (KB4020102)	5/26/2017 2:00 AM	"Windows 10"
2017-06 Update for Windows 10 Version 1607 for x64-based Systems (KB3150513)	6/8/2017 7:00 PM	"Windows 10"
2017-06 Update for Windows 10 Version 1607 for x86-based Systems (KB3150513)	6/8/2017 7:00 PM	"Windows 10"

Image Courtesy of Bryan Dam

Scheduling - Issues

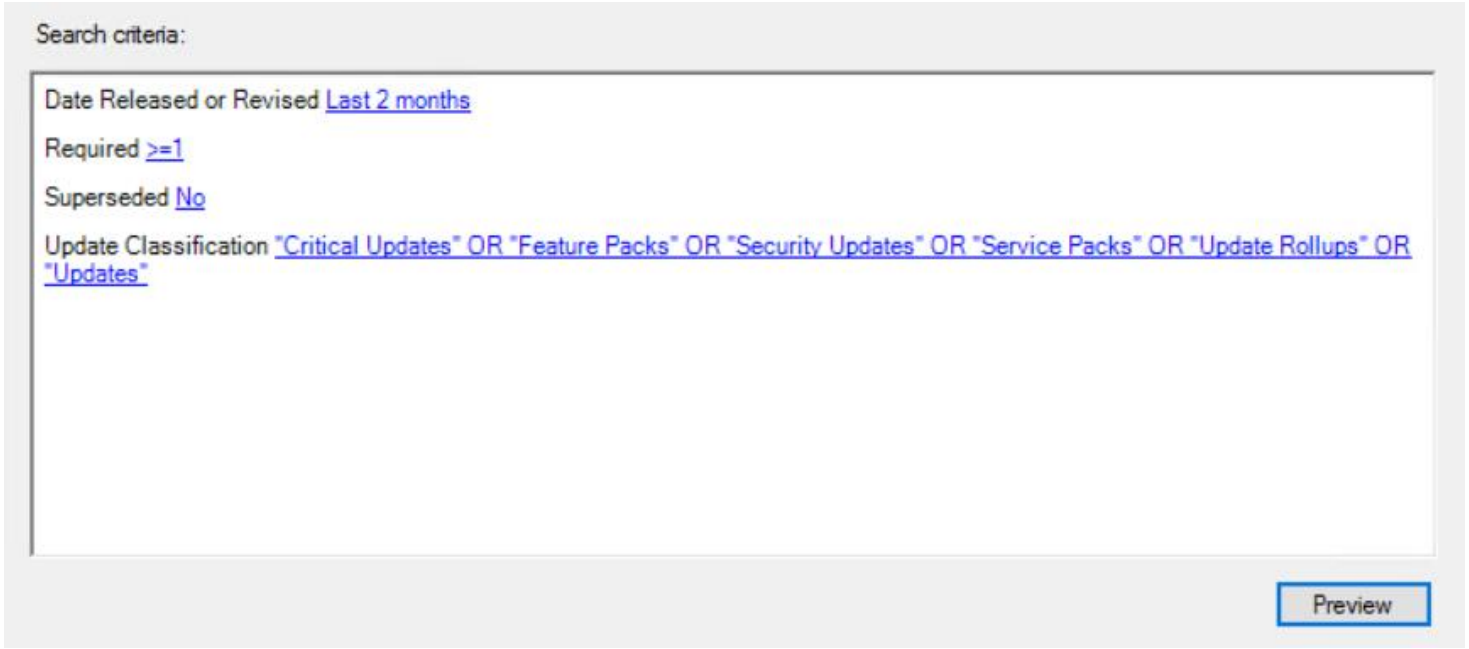
- Running ADRs simultaneously can cause SQL locks
- Schedule ADRs after successful catalog sync
- Update sync fails for example Windows Update is down
- Will retry every 30 minutes but this might not succeed until ADRs have run
- Microsoft messes up the releases (Delta updates)

Scheduling - Considerations

- Manually run update sync and ADRs.
- Deadline schedule is based on ADR run time.
- Offset scheduling since CM 1802
- Use Task Scheduler to run a PowerShell Script (by Bryan Dam):

Run a Configuration Manager Software Update Synchronization
Run a Configuration Manager Automatic Deployment Rule

Updates Selection



Updates Selection

Date Released or Revised: 1 Month

- Subtracts from the date's month (example: October 9 = September 9)
- Don't miss updates released after your last sync
  - Use 2 months

Required: > =1

- Update catalog must sync, client must scan against the latest catalog, and ConfigMgr must process scan results before the ADR runs.
- This can cause significant delays
- You can:
  - Separate your Update Sync from the ADR schedule with amount greater than your Software Update Scan schedule (found in Client Settings)
  - An update might become needed in the future but it won't get deployed because it's older than the date criteria.

Updates Selection

Microsoft's patching strategy:

- Monthly Cummulative Updates (CU)
- Internet Explorer, Servicing Stack, and other updates are separate
- .NET has separate updates

Preview of Monthly Quality Updates.

Early release of the quality updates two weeks ahead of full rollout.

Allows for earlier testing of new features.

Do not deploy alongside of the production rollups.

.Net Framework Cummulative Update

New Update channel – Announced September 19, 2018

The Cumulative Update release schedule for the .NET Framework will have the following characteristics:

- **Independent** – Released separately from the Windows Cumulative Update
- **Cumulative** – The latest patch will fully update all .NET Framework versions on your system
- **Same cadence** – The Cumulative Update for .NET Framework will be released on the same cadence as Windows 10.

Updates Selection

Use Negation Title Filters to fine tune updates selection

Use a minus sign in front of text to exclude from update selection:

-Security Only
-Preview of
-Itanium
-Office 365 Client Update - Monthly Channel
-Office 365 Client Update - Semi-annual Channel (Targeted)

Review the updates selected by your ADRs.
Use the Preview button to validate all changes to your ADRs.

Updates Selection

Search criteria:

Date Released or Revised Last 2 months

Product "Windows Server 2012" OR "Windows Server 2008 R2" OR "Windows Server 2008" OR "Windows Server 2012 R2" OR "Windows Server 2016"

Superseded No

Title -Security Only OR -Preview of OR -Itanium

Update Classification "Critical Updates" OR "Security Updates" OR "Update Rollups" OR "Updates"

Patching Issues

Demystifying "Dual Scan"
Improving Dual Scan on 1607
Using ConfigMgr With Windows 10 WUfB Deferral Policies

Dual scan uses WU for Windows OS products and WSUS for everything else
Triggered by configuring both an internal WSUS server and WUfB deferral policies
This can cause unintended feature updates to Windows 10

Do This:

- Use ConfigMgr to manage Window 10 deployments
- Configure deferral policies via ConfigMgr (Windows 10 v1703+)
- Use new 'Do not allow update deferral policies to cause scans against Windows Update" policy (v1709)

Patching Issues

- Cummulative Updates can have prerequisites
- Buggy patches causing unresponsive systems
- Spectre/Meltdown mitigation required registry key for A/V Compatibility (Introduced in January and eliminated in April)

Patching Issues - Registry

Customers without Antivirus

In cases where customers can't install or run antivirus software, Microsoft recommends manually setting the registry key as described below in order to receive the latest Windows security updates.

Note: Customers will not receive the January 2018 Windows security updates (or any subsequent Windows security updates) and will not be protected from security vulnerabilities unless and until their antivirus software vendor sets the following registry key:

Key="HKEY_LOCAL_MACHINE" Subkey="SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompat"
Value="cadca5fe-87d3-4b96-b7fb-a231484277cc" Type="REG_DWORD"

Data="0x00000000"

Patching Issues - VMs

- Virtual Machines with shared storage are highly susceptible to impact
  Scan and Inventories can be problematic when certain events like power outage can synchronize them instead of randomization
  Reboot storms can take down environments
  Client Settings can randomize the deadline for two hours
  Randomization is always from the deployment deadline, not by the MW
- Use several Maintenance Windows to start at different intervals
- Create collections based on the last digits of the Resource ID for proper spread

WSUS - Issues

WSUS syncs the update catalog and EULAs from Microsoft and delivers to the clients

- Clients contact WSUS to determine catalog version
- If there is no match, then they request a delta catalog
- WSUS generated deltas causes high CPU consumption
- WSUS cached metadata consumes high memory

Fixing WSUS - When the Best Defense is a Good Offense

WSUS - Issues

- CU patching model has increased update metadata
  New version duplicates previous version and adds additional detection methods
- WSUS generates a catalog delta for each client and caches the results for future clients
  Clients fetching new CU metadata can trigger the default 110 second timeout
  WSUS IIS application pool reaches memory threshold, resets, and clears the cache. Then, it must rebuild the metadata cache again

Fixes:

Apply hotfixes
Increase ASP.NET timeout.
Increase the WSUS application pool private memory threshold as high as you can. (0=Unlimited)
Maintain WSUS

High CPU/High Memory in WSUS following Update Tuesdays

WSUS - Issues

Version Next Updates – Updates for Windows Insider builds (massive amount of metadata)

Microsoft Compatibility Analyzer – Gathers data for Windows Analytics

- Caused clients to discard part of cached catalog which triggered a full scan (February 2018)

Fixes:

Decline Version Next updates unless supporting Windows Insider clients

Disable Microsoft Compatibility Analyzer scheduled task

Unexpected high network bandwidth consumption when clients scan for updates from local WSUS server

Patching Issues – Maximum Runtime

Max runtime defaults for Updates depend on update type:

- Normal updates are 10 minutes
- Service Packs are 60 minutes
- CU rollups are 60 minutes

You can manually set the maximum runtime if needed

Can use PowerShell script to change

Patching - Maintenance

Monthly SUGs help with checking a particular month's compliance
Combine monthly SUGs into a yearly groups to minimize deployments and clutter
Search for superseded updates and remove from yearly SUGs

SCCM will recreate the SUG when the ADR results differ from the current SUG.
- Automates SUG cleanup by eliminating declined and superseded updates.

Some Concerns:
- The 1000 limit can force to create more SUGs
- Rollouts longer than a month you will overwrite active deployments
- Built-in reporting is based on SUGs
- Create custom reports for overall compliance

Patching - Maintenance

Supersedence Rules

- Expires superseded updates after x amount of time from when the update was superseded
- This will not expire updates in WSUS
- In WSUS, Microsoft Updates can only be expired by Microsoft in the global Windows Update catalog

Run WSUS cleanup wizard

- Run from WSUS Console
- Will decline updates that Microsoft expired
- When ran from Configuration Manager it will *never* decline updates that are superseded
- The wizard only declines superseded updates whose superseded updates is approved
- Decline updates not used like Itanium, beta, etc

PowerShell Scripts

The complete guide to Microsoft WSUS and Configuration Manager SUP maintenance **WSUS Cleanup for ConfigMgr**

Maintenance – Bryan Dam's Automation

Detect if a synchronization is happening and wait for success before resuming
Declines superseded updates
Declines updates by a list of titles
Declines updates based on external plugin scripts
Output a comma-delimited list of declined updates
Run the WSUS Cleanup Wizard
Initiate a software update synchronization
Remove expired and declined updates from software update groups
Delete software update groups that have no updates
Combine software update groups into yearly groups
Set the maximum run time for updates by title
Remove unneeded files from the deployment package source folder
Update the deployment packages used by ADRs either monthly or yearly

Fully Automate Software Update Maintenance

Reporting - Compliance

The built in reports are not great
The dashboard in ConfigMgr console under /Monitoring/Security/ is not so helpful

Use 3rd party Reports

- Gary Simmons: Software Update Compliance Dashboard
- System Center Dudes: Software Update Reports
- Knowledge is Power: Software Update Groups Compliance Dashboard Revisited
- SCConfigMgr: Patch Compliance Reporting in Configuration Manager with PowerBI
- Enhansoft: https://www.enhansoft.com/product/enhansoft-reporting
- Eswar Koneti: SCCM Reports

Build your own reports

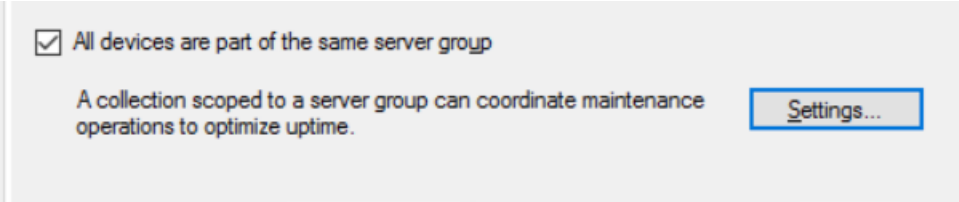
Resources

- The complete guide to Microsoft WSUS and Configuration Manager SUP maintenance
- Microsoft – More on Updates
- Unleash WSUS Performance
- Fixing WSUS: When the best defense is a good offense
- Bryan Dam's Software Update Maintenance Script
- High CPU/High Memory in WSUS following Update Tuesdays
- Re-Index WSUS Database
- WSUS causes high CPU and clients fail update scan
- Ola Hallengren's SQL Server Index and Statistics Maintenance
- Enhancing WSUS database cleanup performance SQL script

Server Groups

Can configure server group settings for a collection to define how many, what percentage, or in what order computers in the collection will install software updates

You can also configure pre-deployment and post-deployment PowerShell scripts to run custom actions



Microsoft Doc – Server Group
ConfigMgr Server Groups – Take Control of Patching

3rd Party Application Patching

3rd party applications need to be patched as well
- Due to vulnerabilities, bugs, exploits

Can patch natively with ConfigMgr and using scripts but a little tedious

Use 3rd party application patching tools such as Patch My PC

Demo!

IT/Dev CONNECTIONS

Thank You!

Delivered by KNect365 TMT an Informa business