What's new with Windows Server 2025

September 27, 2024

LouMUG

Agenda

- LAPS
- WAC
- SSH
- AD
- dMSA (sMSA, VA, gMSA)
- HP
- FCM
- HV
- Containers
- NVMe
- ReFS
- SR
- S2D
- SMB
- Arc
- Various Things
- Upgrades

Disclaimer

- Information gathered over the last 6 months
- Some may have changed
- Some may change between today and official launch
- I have not been able to personally test all this stuff
- I may have mis-understood what I read/watched
- If something sounds cool, go look it up yourself and make sure you know how it works
- Test before prod
- I may disparage Microsoft off-handedly; don’t sue me.

General idea of Server 2025

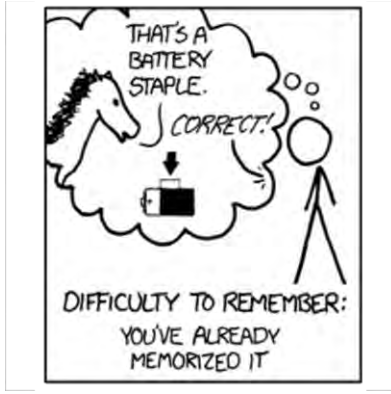
Piecing together from various presentations

- Microsoft has always had 3 core tenants, compatibility, performance, and security.
- It used to be Compatibility, Performance and ‘eh, maybe we’ll get to security.’
- Changed to Performance, Compatibility, Security
- Now it’s solidly Security, Performance, Compatibility
- Key targets:
  - NTLM
  - Mailslots
  - Cryptographic methods

Windows LAPS

Not to be confused with MICROSOFT LAPS

- This isn't exclusive to 2025, you can use it on 2019 and 2022
- Automatically makes a unique password for local admin account
  - Updates frequently and stores password in AD
- Can also set the name of the admin account, or create a random one
- Can backup DSRM account
- Image rollback detection – detects if computer rolled back and automatically updates password
- Can generate passphrases instead of passwords
  - Can set complexity of words and number of words



Windows LAPS

Not to be confused with MICROSOFT LAPS

- New LAPS tab in Active Directory Users and Computers
- Improved readability – can exclude similar characters like I and l or 0 and O
- Font is easier to read
- WAC now has an add-in that makes this SUPER easy to use
- Can even pipe your passwords into RDS or powershell consoles

Windows Admin Center “WAC v2”

Stronger, better, faster [than 2018 technology]

- Also doesn’t require Server 2025
- Upgrade from .NET Core 6 to 8
  - HTTP/2 reduces latency and improves performance
  - Better Security with enhanced cryptography
- Cross-platform support
- “Up to twice as fast” – live demos showed half the load times
- Specific improvements:
  - Micro-service based instead of monolithic
  - VM management improvements
  - Better installer (more customization)

SSH

OpenSSH built in

- ALSO doesn't require Server 2025 (2019 and 2022 can use it)
- Built into server manager on 2025 though (below remote desktop)
- Makes an OpenSSH Users local group like RDS
- Connect to the server
  - Powershell – ssh domain\username@servername
  - Can also sftp to the server
  - Putty like normal
- Can setup an SSH key instead of using a username/password
- Can do automation between windows and Linux easier with unified SSH access
- Can tunnel RDP over SSH

Active Directory

The most interesting things

- 32k page size
  - Can install new DCs with 32k page in backwards compatibility mode
    - Upgraded DCs still use 8k
  - Once all DCs capable, upgrade forest
- New Schema – ‘improvements with EntraID synchronization’
  - First schema update since 2016
- AD Object Repair – Missing SamAccountType and Object Category can now be fixed
- DC Location Algorithm Improvements - aka contoso not corp.contoso.com
  - Allows user defined NETBIOS -> DNS location
  - Caches from trusting domains

Active Directory
Going down the rabbit hole

- New Forest and Domain Functional Levels
  - “Requires Server 2016 or later”
- “Improved algorithms for Name/Sid Lookups”
  - Doesn’t use LSA/netlogon anymore
  - Uses Kerberos and DC locator
- “AD now uses random generated default computer account passwords. Windows 2025 DCs block setting computer account passwords to the default password of the computer account name.”
- DCs and AD LDS instances require encryption (LDAPS) for searching, or changing important fields

Active Directory

Tea with the mad hatter

- “The Kerberos Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) protocol implementation is updated to allow for cryptographic agility by supporting more algorithms and removing hardcoded algorithms.”
- “LAN Manager GPO setting - The GPO setting Network security: Don't store LAN Manager hash value on next password change is no longer present nor applicable to new versions of Windows.”

Active Directory

Coming back to reality

- LDAP encryption by default using SASL (Simple Authentication and Security Layer) and LDAP sealing
- LDAP supports TLS 1.3
- Legacy SAM RPC password change methods are blocked by default
- AD NUMA support – AD previously only used CPUs in NUMA group 0 and no more than 64 cores.
- Extra performance counters in perfmon

Active Directory
Cool stuff again

- Replication Priority Order
  - Currently priority based, hard coded, intra-site has a higher priority
  - Now admins can increase system calculated replication priority for specific partners and naming contexts using replication priority boost
  - Individual DC can be prioritized (such as initial AD sync)
  - This priority addition goes into the overall calculations

Audience Participation!

Question:
How do you make service accounts?

Delegated Managed Service Account

Work our way forward

- Virtual Accounts
  - Introduced in 2008 R2
  - Within a single computer
  - No password managed, creates a virtual account using the format NT SERVICE\SERVICENAME EX: NT SERVICE\MSSQLSERVER
  - In reality these access network resources using the computer account (EX: domainname\computername$
- Standalone Managed Service Account (sMSA)
  - Introduced in 2008 R2
  - Within a single computer
  - Cannot be shared between computers

Delegated Managed Service Account

Work our way forward

- Group Managed Service Accounts (gMSA)
  - Introduced in 2012
  - Used across multiple computers
  - AD Controls password updates
- Delegated Managed Service Accounts (dMSA)
  - Introduced in 2025
  - Uses machine accounts instead of traditional service accounts
  - The server’s machine account has delegated permissions to manage this new service account
  - No other user/computer account can get access to these passwords

Delegated Managed Service Account

Microsoft's comparison

Criterion	sMSA	gMSA	dMSA	Virtual accounts
App runs on a single server	Yes	Yes	Yes	Yes
App runs on multiple servers	No	Yes	No	No
App runs behind a load balancer	No	Yes	No	No
App runs on Windows Server 2008 R2 and later	Yes	No	No	Yes
Requirement to restrict service account to single server	Yes	No	Yes	No
Supports machine account linked to device identity	No	No	Yes	No
Use for high-security scenarios (prevent credential harvesting)	No	No	Yes	No

Service Accounts | Microsoft Learn

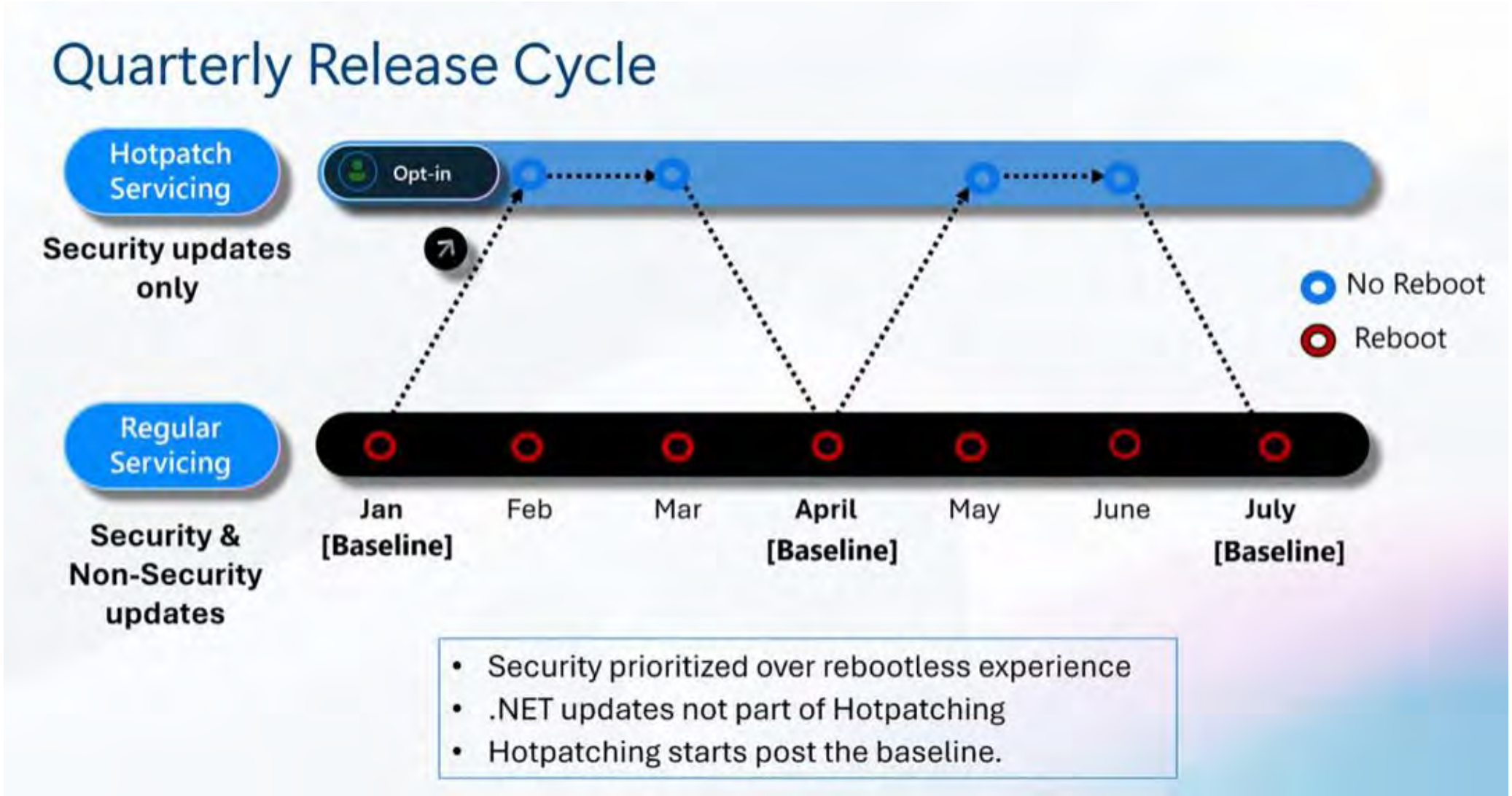
HotPatching

Azure coming down to on-prem… kinda

- Was available in 2022 Azure Edition
- Modify memory code without a reboot
- Quarterly baseline (requires reboot)
- Monthly patches do not
- EX: instead of 12 reboots a year, 4.
- Enable via Azure Portal
  - Requires Azure Edition (no extra costs) on Azure IaaS or Azure Stack HCI
  - Server added to Azure Arc for management

HotPatching

Azure coming down to on-prem… kinda



Failover Clustering

Lot of new tweaks and improvements

- Loads of CAU reliability and performance improvements.
  - Feature updates in Cluster Aware Updates – rolling upgrade to 2025
- “Azure stack features coming to 2025”
  - Single Node clusters
  - S2D Stretch clusters (ex: campus cluster with extra resiliency)
- Workgroup clusters with live migration via certs for auth
- GPU-P VM Live Migration – migrates GPU state as well
- AccelNet (fancy SR-IOV basically)

Hyper-V

- Elden Christensen Principal PM Manager in Core OS group

“First off, I want to say Hyper-V is a critical, foundational technology for Microsoft. We use it everywhere.

It’s the foundation of Azure, the Azure Stack family, Windows Server has Hyper-V, Windows Client has Hyper-V, our container storage is built on top of Hyper-V, and a lot of our platform security features take advantage of technologies in Hyper-V, and Xbox actually uses Hyper-v, when you’re playing games, they’re running on top of Hyper-V.

Hyper-V is critical to Microsoft as a whole.

Sometimes I hear people say these kind of crazy things like ‘oh Hyper-V is dead’ that couldn’t be a more ridiculous statement.

As the leader of Windows Server I’m here to tell you that you should not have any doubts”

Hyper-V
New fun

- GPU Partitioning (GPU-P)
  - Share a GPU using SR-IOV
  - Supports live migration
- GPU Discrete Device Assignment
  - Create a PCI Express resource pool and add GPUs to it
  - Entire GPU assigned to a VM
  - Move VM to another host and it pulls a GPU (VM Stun)
- RemoteFX vGPU did GPU-P functionality
  - Was disabled in 2019
  - Architectural Security Vulnerabilities
  - DDA was only option

Hyper-V
New fun

- Dynamic Processor Compatibility
  - Less draconian on hiding feature sets
  - More granular, only reduces subset not available.
- Increased Scalability
  - 2048 vCPU
  - 240tb of RAM

Audience Participation

My own morbid Curiosity:

Are you using containers?

Containers

If you use Windows containers

- Can move containers from 2022 to 2025 without upgrading the base image
- Reduced image size
- Can add improved application compatibility by installing features on demand (making it bigger again ☺)
- Performance improvements.

SMB

SMB Signing

- Stops relay, attack-in-the-middle and phishing attacks
- Previously only required for DC shares
- Signing required by default in most cases
  - Windows clients require server to be signed
  - Windows servers request client signed
  - Windows server to server not required
- 15% performance hit
  - SMB compression might offset

SMB

Loads of stuff here, some interesting, some boring

- SMB Auth rate limiter
  - Throttles NTLM passwords by default
  - 2 second delay between authentications
- SMB Firewall rule hardening
  - Install file share role opens 445 and 5445
  - No longer opens NetBIOS 137-139 [like it has since XP]
  - In the future won't open ICMP, LLMNR or Spooler RPC
- SMB Dialect Control – can require SMB 2 or 3

SMB

Slowly turning off legacy stuff

- SMB 1 client has finally been disabled on Windows Home edition by default
  - Started with server, then enterprise, then pro, then home
  - 8 Years ago 45% of all SMB traffic was SMB 1, now it's .25%.
  - SMB1 Product Clearinghouse - Microsoft Community Hub
- SMB Guest Auth
  - A lot of NAS allow connection w/o authentication
  - Now off in Server, Enterprise and Pro, only available in home.

SMB

Slowly turning off legacy stuff

- SMB Remote Mailslots disabled
  - A function of SMB1, if you aren't using SMB1, it was already off
  - Even if you are using SMB1 it wasn't inherently using this
  - It's off now.

Audience Participation

Do you know how QUIC works?

SMB

SMB Over QUIC

- The rest of us can finally install it!!!
  - Available in Standard, Datacenter and Azure Edition
- Runs on Port 443
- Uses UDP for file transfer and QUIC handles loss control instead of TCP
- Doesn’t require VPN
- Always encrypted
- TLS 1.3 for authentication
- QUIC already in use by various companies

Storage
ReFS dedup and compression

- Post processing, fully schedulable
- “File servers save 60% of storage”
- “VHD/ISO/Backups save 90% of storage”
- <1ms latency added
- Only runs on new data
- Dedup only, compression only, or both
- Scales up significantly better than previous versions of windows dedup

Storage
Random Stuff

- Storage Replica
  - Performance enhancements with enhanced log
    - Raw format for logging IO to be replicated
    - Allows concurrent IO written to the secondary volume
  - Compression now available
- Storage Spaces Direct
  - Thin provision volumes
  - Adjustable storage repair and resync speed
    - 5 speeds from performance to timeliness

Audience Participation

Do you know what NVMe is?

Storage
NVMe

- Focus on NVMe since both local and remote storage going this direction
- Optimized NVMe in 2025
  - Improved performance up to 70% more IOPs on the same hardware “Expect 90% in an update after GA”
  - Lower CPU utilization
- NVME-OF
  - Supports TCP now
  - RDMA coming in future update
  - Native NVMe Initiator

Various Items

Lot of new tweaks and improvements

- Azure Arc is installed by default.
- Desktop Shell
  - When you first sign in Windows acts like it's windows 11 as far as setting you up.
  - RDS [Windows App] potential nicety, or for Server on Desktop
- Feedback Hub for sharing issues
- New File Compression options – 7z and TAR
- Hyper-V Manager FINALLY defaults to Generation 2
- RRAS doesn't support PPTP and L2TP protocols by default, only SSTP and IKEv2.

Various Items

Lot of new tweaks and improvements

- “Modern Task Manager”
- Windows terminal is now available
- Winget is now installed by default
  - Can control settings via GPO
- Local KDC – Kerberos Key Distribution is built into windows for local accounts now to start getting rid of NTLM
- Credential Guard
  - Uses Secure Boot, Virtualization-based security to protect cached hashes or Kerberos Ticket Granting Tickets
- Can now get your licenses as a subscription
  - Perpetual licenses are not going away

Server on Desktop

I'm saying these are for devs running server on their desktop… I can't think of another legitimate excuse for these features in a server OS

- Dev Drive – separate volume for enhancing dev workload performance
  - Uses ReFS optimizations for greater control over volume settings and security such as AV
  - Supports block cloning - don't have to wait to fully copy stuff, uses less space
- Bluetooth
  - Can be turned on for connecting various devices
  - Most [all real] servers don't have Bluetooth chips
- Wi-Fi – easier to enable than it used to be (installed by default)
  - "maybe you have a branch office where there's no wired connection where the server is"

Server on Desktop

I'm saying these are for devs running server on their desktop… I can't think of another legitimate excuse for these features in a server OS

- Email & Accounts - lets you add accounts to your Server OS
  - EntraID
  - Microsoft Account
  - Work or School Account
  - "It's important to keep in mind that domain join is still required for most situations"
- Windows Insider Program – early access to latest release
- Dtrace – now native tool for debugging running code
- Pin Apps to start menu – defaults to server apps

Upgrading to 2025

Terrifying but works?

- Just use Windows Update
  - Feature Update = in-place upgrade
  - Quality Update = CU
- Telemetry data says 1.5-4% failure rate on in-place upgrades
- Can also do media-based update (setup.exe off ISO)
- 2012 R2, 2016, 2019, 2022 – one-step upgrade
- N-4 feature updates app compatibility tested regularly (96% success rate)
- “Plan for 1 hour per server”
- Don’t forget about activation
- Also, RIP WSUS

Sources!

Branch off from these into a hundred links and ~~Googles~~ Bings. I definitely used Bing.

- What's new in Windows Server 2025 | Microsoft Learn
- Windows Server Summit 2024 - March 26-28, 2024 | Microsoft Event
- SMB1 Product Clearinghouse - Microsoft Community Hub
- The evolution of Windows authentication | Windows IT Pro Blog (microsoft.com)

Thanks! Q&A

Brent Earls
brent.earls@mirazon.com

Join Us at Hack Red Con!

- October 25-26 @ Louisville, KY
- Friday, October 25th @ Churchill Downs
- Saturday, October 26th @ Jefferson Community & Technical College