Windows Server 2025

Mikael Nystrom, Truesec

About Me

- Microsoft MVP for 20 years

- Started with 8" floppy's and Winchester drives

- Currently working in Cyber Security Incident Response Team as a lead infrastructure responder at Truesec

- Written 7 books regarding OS Deployment

- Also knows as "The Deployment Bunny"

MVP

Windows Server 2025 – What is gone?

Windows Server 2025 – Hardware Req?

Limitations ☺

Locks and limits	Windows Server 2025 Datacenter
Maximum SMB connections	16,777,216
Maximum RRAS connections	Unlimited
Maximum IAS connections	2,147,483,647
Maximum RDS connections	65,535
Maximum number of 64-bit sockets	64
Maximum number of cores	Unlimited
Maximum RAM (5 level paging)	4 Petabyte
Maximum RAM (4 level paging)	256 Terrabyte
Number of vCPUs	2048

Licensing

Licensing

- Perpetual Licensing

  - OEM

  - EA

- Pay As You Go

  - Azure Arc

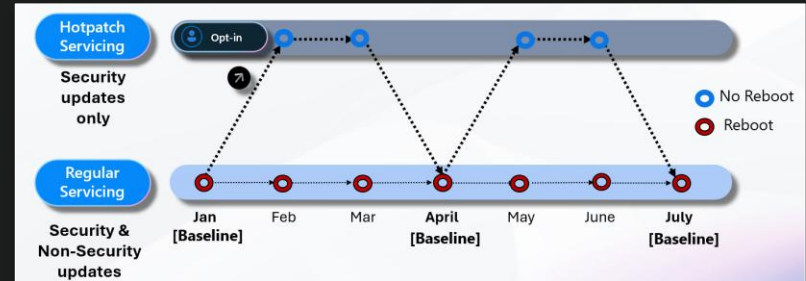# Let's geek around for a while...

Windows Server 2025 Features

Arc-enabled Hotpatching

- Reduce reboots from 12x per year down to 4x per year

- Enable Hotpatching via Azure Portal
  - Monthly subscription

- No additional cost with Azure Edition
  - Azure and Azure Stack HCI

Hyper-V enhancments

- GPU partitioning (GPU-P)

- Share a GPU across multiple VMs

- Assign a VM to each partition

- VM can Live Migrate to another node on the cluster maintaining integrity

- GPU DDA pools

- Live migrating between servers with different processor capabilities

- Improved performance, increased granularity on processor compatibility

- Support for 240 TB of RAM

- Support for 2048 virtual processors

Storage

- Optimized NVMe Drivers

  - Improved performance

- Optimized Dedup and Compression for ReFS

  - File Server: Save ~60% storage

  - VHD/ISO/Backups: Save ~90% of storage

- Storage Spaces

  - Thinly provisioned storage spaces

  - Supported on Failover Clustering

Failover clustering

- GPU-P VM live migration on a failover cluster

  - VM live migration on a workgroup cluster

  - Workgroup cluster does not need an Active Directory Domain Controller (Only DNS)

  - Uses self-signed certificates instead of Kerberos tokens

  - Requires NTLM accounts to configure and manage

- Cluster-aware updating

  - Reliability and performance improvements

  - Upgrade from Windows Server 2022 to Windows Server 2025
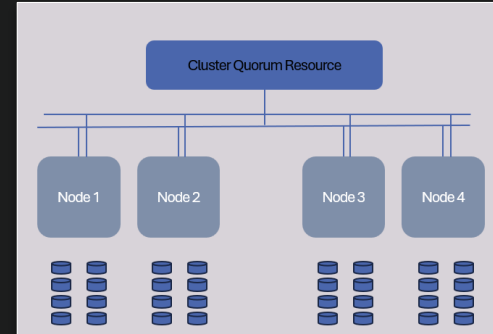
Networking

- Network ATC

  - One-click deployment and drift remediation of host network configuration across the cluster

  - Network HUD

  - Always-on alerting & remediation of operational network issues & inefficiencies

- SDN Multisite

  - Native L2 & L3 Connectivity for workloads in multiple locations.

- SDN Gateway Performance Improvements

  - Hosted natively on Failover Cluster as a GenSvc

  - Empowering Modern AKS Applications

  - Hybrid AKS workloads can now be put on SDN networks for Windows Server

Upgrade

- Media based In-place Upgrade from Windows Server 2012 R2

- Windows Update Update from Windows Server 2019/2022

File services

- SMB over QUIC

  - Secure and reliable transport built on UDP

  - SMB for telecommuters, mobile devices, cloud

  - Does not require VPN – mostly replaces VPN, runs over port 443

  - Encryption always enabled

  - Handshake authenticated with TLS 1.3

  - Available in all editions: Standard, Datacenter, Datacenter Azure Edition

File services

- SMB Security Improvements

- Secure by default

- SMB Signing

  - Signing required by default (Stop relay, attacker-in-the-middle, phishing)

- Auth Rate Limiter

  - Throttles bad NTLM passwords by default (Brute force attack prevention)

- SMB Firewall Rule Hardening (No longer opens NetBIOS ports)

- SMB NLTM Disable Option (Granular control of remote NTLM)

- SMB Dialect Control (Allow/Refuse a range of SMB 2 & 3)

Active Directory

- New functional level (forest and Domain)

    - Minimum functional level is 2016 for a DC running 2025

- New installed DCs can be upgraded to 32k JET pages instead of 8k pages

    - In place upgrades will not be able to switch, need new install

- NUMA support

Active Directory

- New performance Counters

  - Local Security Authority (LSA) Lookups

  - DC Locator

  - LDAP Client

- Priority of replication partners

  - You can "boost" replication

- Security stuff

  - RC4 is now added to the "don't use list"

  - LDAP now supports TLS 1.3