Quelle: vershininphoto – 123RF

## Neuerungen unter Windows Server 2025

# Aufpoliert

von Dr. Christian Knermann

Mit Windows Server 2025 hat Microsoft einen Nachfolger für die derzeit aktuelle Version 2022 angekündigt. Der kommende Server verspricht, anders als seine letzten beiden Vorfahren, signifikante Neuerungen für lokale Infrastrukturen und auch für das Active Directory. Wir geben einen Überblick über die zu erwartenden neuen Funktionen.

Die Evolution des Windows-Server-Betriebssystems folgt seit einigen Jahren einem gleichbleibenden Schema mit zwei Entwicklungszweigen: den Server-Wartungskanälen (Servicing Channels, SC) [1]. Dazu zählt zum einen der Langzeitwartungskanal (Long-Term Servicing Channel, LTSC). In letzterem erscheinen regelmäßig alle zwei bis drei Jahre die Hauptversionen des Betriebssystems, die Sie an den Jahreszahlen in der Produktbezeichnung erkennen – auf Windows Server 2016 folgte 2019 und daraufhin die gegenwärtig aktuelle Version 2022. Von den R2-Zwischenschritten, wie bei den früheren Versionen Server 2008 und 2012, hatte Microsoft sich zwischenzeitlich verabschiedet.

Der LTSC genießt fünf Jahre Mainstream-Support, in dem die Redmonder neben Sicherheitsupdates auch neue Funktionen versprechen und danach noch fünf Jahre erweiterten Support. Darin erhält das System keine Weiterentwicklungen mehr, aber noch sicherheitsrelevante Updates.

### Keine jährlichen Versionen für DCs

Neben LTSC pflegt Microsoft auch noch den jährlichen Kanal (Annual Channel, AC). Anfänglich hatte das Unternehmen es in diesem Entwicklungszweig als Semi Annual Channel (SAC) mit halbjährlich neuen Versionen versucht, ist dann jedoch analog zum Client-Betriebssystem Windows 10 wieder davon abgerückt. Der frühere SAC gibt aber noch das Namensschema vor, das sich aus zwei Ziffern für das Erscheinungsjahr, gefolgt vom jeweiligen Halbjahr, ergibt. Bis zum Redaktionsschluss war im AC die Version Windows Server 23H2 aktuell.

Im AC erhält das Betriebssystem typischerweise lediglich 24 Monate Unterstützung des Herstellers, davon 18 Monate Mainstream und zusätzliche sechs Monate erweiterten Support. Der AC zielt damit vor allem auf DevOps-Szenarien mit dem Schwerpunkt auf Containern und Microservices. Windows Server unterstützt im AC nur die Server-Core-Installation ohne grafische Benutzeroberfläche und legt den Fokus klar auf den Betrieb als Container-Host, nicht auf die klassischen Anwendungsfälle wie Datei- und Druckdienste oder Domaincontroller (DC). Im Hinblick auf den Schwerpunkt unseres Interesses, das Active Directory (AD), ist folglich nur der LTSC relevant, der mit seinen gegenüber dem AC üppigen Support-Zeiträumen die nötige Sicherheit für einen langfristigen Betrieb bietet.

### Von vNext zum Windows Server 2025

Nun steht im LTSC endlich ein Nachfolger für den Windows Server 2022 in den Startlöchern. Längere Zeit hatte Microsoft die Entwicklung unter dem Arbeitstitel "Windows Server vNext" vorangetrieben, Anfang dieses Jahres dann aber enthüllt, dass das neue Betriebssystem offiziell den Namen Windows Server 2025 tragen wird [2]. Bis zum Redaktionsschluss unseres Sonderhefts war allerdings noch nicht bekannt, wann genau die neue Version erscheinen soll.

Mit den letzten beiden Ausgaben 2019 und 2022 hatte Redmond Funktionen für rein lokale Dienste eher stiefmütterlich behandelt und den Fokus klar erkennbar auf die Anbindung an die hauseigene Azure-Cloud gelegt. Nachdem die Entwicklung neuer Funktionen für den lokalen Betrieb stagnierte, begannen einige Analysten und Marktbeobachter bereits mit dem Abgesang auf das klassische AD und bereiteten Befürchtungen den Boden, dass Microsoft seinen lokalen Verzeichnisdienst zugunsten von Entra ID in der Cloud komplett aufgeben könnte. Doch solche Gerüchte haben sich inzwischen als falsch erwiesen. Über die angekündigten neuen Funktionen dürfen sich auch Admins freuen, die Dienste und Anwendungen weiterhin im lokalen Rechenzentrum betreiben möchten.

So war die Hotpatch-Funktion bislang der Azure-Edition von Windows Server 2022 Datacenter vorbehalten [3]. Das Hotpatching aktualisiert den Code der gerade ausgeführten Prozesse im Arbeits-

speicher direkt zur Laufzeit, ohne dass der jeweilige Prozess oder das System als Ganzes nach einem Neustart verlangt. Microsoft verspricht damit weniger Unterbrechungen von Diensten dank weniger Reboots und somit positive Effekte für die Informationssicherheit, da Updates schneller ihren Weg in den produktiven Betrieb finden [4].

Weniger spezifisch hat das Unternehmen Verbesserungen auch für die Virtualisierung mittels Hyper-V, Unterstützung von Anwendungsfällen künstlicher Intelligenz (KI) sowie Optimierungen beim Daten- und Storage-Management angekündigt. Im Hinblick auf unseren Themenschwerpunkt interessiert uns aber vor allem, dass Microsoft auch signifikante Neuerungen unter der Überschrift "Next Generation Active Directory and SMB" in Aussicht stellt [5].

## Vorerst nur für Insider

Stand September 2024 hatte Microsoft den Windows Server 2025 noch nicht für den produktiven Einsatz freigegeben und auch noch keinen Termin dafür verkündet. Doch solange das neue Betriebssystem noch nicht final verfügbar ist, können Sie bereits im Rahmen des Windows-Insider-Programms vorab einen Blick darauf werfen. Registrieren Sie sich mit einen Unternehmenskonto oder mit einem kostenlosen privaten Microsoft-Konto für das Insider-Programm, erhalten Sie Zugriff auf die laufend aktualisierten Versionen der "Windows Server Insider Preview" [6].

Die Vorabversionen sind zwar keinesfalls für den produktiven Betrieb geeignet, doch je näher die Fertigstellung rückt, desto besser vermitteln sie bereits einen Eindruck davon, was Sie von der neuen Ausgabe von Windows Server erwarten dürfen. Sie finden das System als "Microsoft Server Operating Systems Preview" im Azure-Marketplace. Diese Vorlage können Sie allerdings nur verwenden, wenn das Konto, mit dem Sie sich am Azure-Portal anmelden, auch für das Insider-Programm registriert ist.

Alternativ stellt Microsoft im Rahmen des Insider-Programms ISO-Images sowie virtuelle Festplatten im VHDX-Format für eigenständige Installationen von physischen oder virtuellen Maschinen bereit. Als dieser Artikel entstand, waren Abbilder vom Windows Server vNext mit der Build-Nummer 26257 in Englisch, Deutsch und 16 weiteren Lokalisierungen verfügbar. Das System gibt sich bei der Installation bereits als Windows Server 2025 zu erkennen. Nach dem Setup orientieren sich Desktop, Startleiste und Startmenü am Design von Windows 11.

## Updates für Schema und Funktionsebenen

Die Inbetriebnahme als DC für eine neue Gesamtstruktur unterscheidet sich kaum von früheren Versionen. Auch sämtliche Verwaltungstools können Sie weitestgehend so verwenden wie gewohnt. Allerdings bringt das neue Betriebssystem neue Funktionsebenen mit. Beim Heraufstufen zum DC dürfen Sie für Gesamtstruktur und Domäne zwischen den Funktionsebenen "Windows Server 2016" und "Windows Server 2025" wählen (Bild 1).

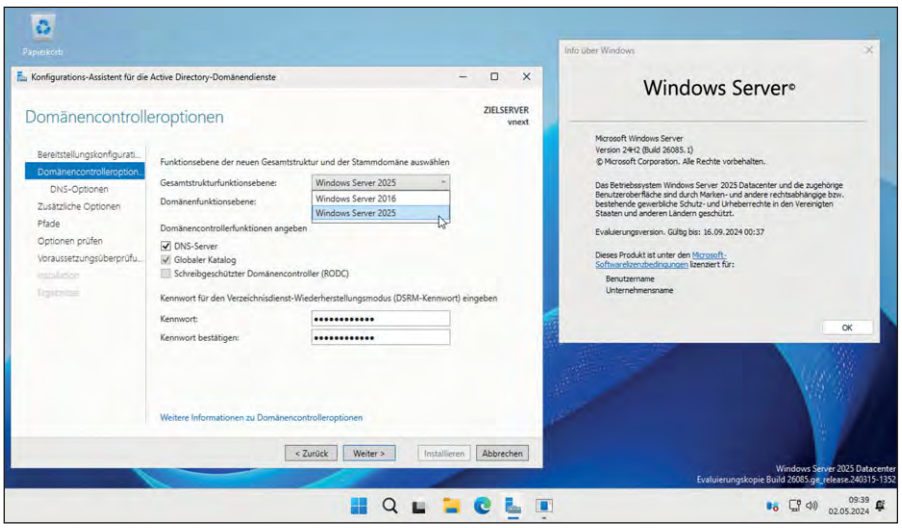
Dies ist auch ein Hinweis auf die Voraussetzungen für Upgrades vorhandener Umgebungen. Möchten Sie einer bereits existierenden AD-Infrastruktur neue DCs unter Windows Server 2025 hinzufügen, müssen alle vorhandenen DCs mindestens unter Windows Server 2016 mit ebendiesen Funktionsebenen laufen.

Die Inbetriebnahme eines DCs unter Windows Server 2025 hebt die Version des AD-Schemas automatisch auf 91, nachdem zuletzt die bereits mit Windows Server 2019 eingeführte Version 88 aktuell war. Mehr zu Upgrades und Migrationen erläutert unser Artikel ab Seite 16. Die Funktionsebenen von Gesamtstruktur und Domänen können Sie erst auf Windows Server 2025 anheben, nachdem Sie sämtliche DCs auf dieses Betriebssystem umgestellt und alle älteren DCs in den Ruhestand verabschiedet haben.

Die neuen Funktionsebenen gilt es auch zu beachten, sofern Sie Systeme mithilfe von Antwortdateien für eine unbeaufsichtigte Installation zum DC heraufstufen möchten. Die Funktionsebenen für Windows Server 2016 entsprachen hierbei den Parametern "ForestLevel=7" und "DomainLevel=7" und dies auch für die Versionen 2019 und 2022 des Betriebssystems. Mit der neuesten Ausgabe des Servers überspringt Microsoft einfach zwei Nummern. Entsprechend lauten die neuen Parameter nun "ForestLevel=10" und "DomainLevel=10". Von weiteren zentralen Neuerungen profitieren vor allem sehr große AD-Infrastrukturen.

## Datenbank aufbohren

Am Fundament der AD-Datenbank, der Microsoft Joint Engine Technology (Jet) in der Variante Jet Blue hatte Microsoft seit der Erstauflage unter Windows 2000 vor über 20 Jahren keine Änderungen vorgenommen. Die auch unter der Bezeichnung Extensible Storage Engine (ESE) bekannte Basis der Datenbank setz-




Windows Server 2025 orientiert sich optisch an Windows 11 und bringt neue Funktionsebenen für Gesamtstruktur und Domänen mit.

te seit jeher auf Datenbankseiten mit einer Größe von maximal 8 KByte. Entsprechend konnten die Datensätze einzelner Objekte im AD ebenfalls nur jeweils 8 KByte groß sein.

Windows Server 2025 hebt dieses Limit auf eine Größe von 32 KByte pro Datenbankseite. Einzelne Objekte dürfen damit deutlich größer werden als bislang, mehrwertige Attribute können jetzt bis zu 3200 Werte enthalten. Neu installierte DCs laufen unter Windows Server 2025 zunächst in einem "8K Simulation Mode", um die Kompatibilität zu älteren Systemen zu gewährleisten.

Sobald Sie alle DCs auf Windows Server 2025 betreiben und auch die Funktionsebenen auf diese Version angehoben haben, lässt sich das optionale Feature mit folgendem Befehl aktivieren:

```
Enable-ADOptionalFeature -Identity
  'Database 32K Pages Feature'
  -Scope ForestOrConfigurationSet
  -Target <Name-der-Gesamtstruktur>
```

Den Namen Ihrer Gesamtstruktur geben Sie dabei wahlweise als Full-Qualified-Domain-Name (FQDN), NetBIOS-Name oder Distinguished Name (DN) des standardmäßigen Namenskontexts an. Die Umstellung auf das 32K-Seitenformat ist irreversibel.

Ebenfalls für sehr große Umgebungen mit typischerweise hoher Last auf den DCs relevant ist der Support für Non-Uniform Memory Access (NUMA). DCs können nun die Vorteile von NUMA-fähiger Hardware nutzen und Prozessorkerne in allen Prozessorgruppen verwenden, um Aufgaben zu parallelisieren. Darüber hinaus profitieren Umgebungen jeglicher Größenordnung von Verbesserungen im Hinblick auf die Informationssicherheit.

## Dienstkonten absichern

Bereits frühere Versionen des Windows Servers hatten das Konzept des Group Managed Service Accounts (gMSA) eingeführt. Windows Server 2025 bringt mit den delegierten verwalteten Dienstkonten (Delegated Managed Service Account, dMSA) nun einen neuen Typ besonders abgesicherter Dienstkonten mit. Doch wie unterscheiden sich gMSA und dMSA?

Bereits mit den gMSA konnten Sie für bestimmte Anwendungsfälle, wie etwa die Ausführung von Diensten oder geplanten Tasks auf Servern, mithilfe von PowerShell Konten einsetzen, deren Passwörter Sie nicht mehr manuell setzen und verwalten mussten. Vielmehr kümmert sich das AD selbst darum, intern sichere Passwörter für die gMSA zu verwenden. Doch obwohl es sich um computergenerierte Passwörter handelt, die das AD noch dazu automatisch rotiert, könnten Angreifer diese Kennwörter theoretisch stehlen.

dMSA verwendet stattdessen verwaltete und zufällig generierte Schlüssel, die zudem mit Geräteidentitäten verknüpft sind. Somit können nur bestimmte im AD zugeordnete Computeridentitäten einen solchen dMSA nutzen. Unter der Haube setzen die dMSA auf aus den Anmeldeinformationen des jeweiligen Computerkontos abgeleitete geheime Schlüssel, die die DCs zum Verschlüsseln von Kerberos-Tickets speichern und verwenden.

Im Unterschied zu gMSA finden sich die geheimen Informationen also ausschließlich auf den DCs. Die Methode hilft somit, das auch als Kerberoasting bezeichnete Sammeln von Anmeldeinformationen mithilfe kompromittierter herkömmlicher Konten zu verhindern. Die Funktion Credential Guard (CG) als Element der virtualisierungsbasierten Sicherheit (VBS) kann die dMSA zusätzlich schützen.

Microsoft beschreibt ein Konzept für den Migrationsprozess und liefert PowerShell-Cmdlets, mit denen Sie herkömmliche Konten sowie auch gMSA auf dMSA umstellen können [7].

## Mehr Sicherheit für Kerberos und LDAP

Weitere Änderungen zielen ebenfalls auf erhöhte Sicherheit. So optimiert Microsoft das Kerberos-Protokoll und fügt die Verschlüsselungsmethoden SHA-256 und SHA-384 hinzu, während der veraltete Algorithmus RC4 nun endgültig auf der Liste der nicht mehr zu verwendenden Verschlüsselungsmethoden landet. Auch an das PKINIT-Protokoll (Kerberos Public Key Cryptography for Initial Authentication in Kerberos) hat Redmond Hand angelegt und die Unterstützung von weiteren Algorithmen hinzugefügt sowie hartcodierte Algorithmen entfernt, um kryptografische Flexibilität zu ermöglichen.

Die gesamte Kommunikation von LDAP-Clients nach einer SASL-Bindung (Simple Authentication and Security Layer) verwendet nun standardmäßig LDAP-Sealing. LDAP unterstützt weiterhin die Verschlüsselung mittels Transport Layer Security (TLS) 1.3.

## Fazit

Nach einer längeren Zeit des Stillstands im Hinblick auf die Funktionen für lokale AD-Infrastrukturen kündigt sich mit dem Windows Server 2025 ein größerer Wurf an. Microsofts neues Server-Betriebssystem orientiert sich optisch an Windows 11 und bringt damit eine überarbeitete Benutzeroberfläche mit. Doch auch unter der Haube stecken einige interessante Neuerungen. Die betreffen vor allem Updates des AD-Schemas, neue Funktionsebenen für Gesamtstruktur und Domänen sowie signifikante Verbesserungen bei der Sicherheit. Insgesamt vollzieht sich die Weiterentwicklung des ADs als sinnvolle Evolution, weniger als Revolution. Und dies bedeutet gleich mehrere gute Nachrichten für Admins. Sie können die gewohnten Tools und bereits vorhandenes Wissen nahtlos weiterverwenden. *(dr)* IT

**Link-Codes**


**[1] Servicing Channels**
os21h

**[2] Ankündigung von Windows Server 2025**
os21i

**[3] Azure Edition**
os21j

**[4] Hotpatching**
os21k

**[5] AD Domain Services**
os21l

**[6] Windows Server Insider Preview**
os21m

**[7] Delegated Managed Service Accounts**
os21n