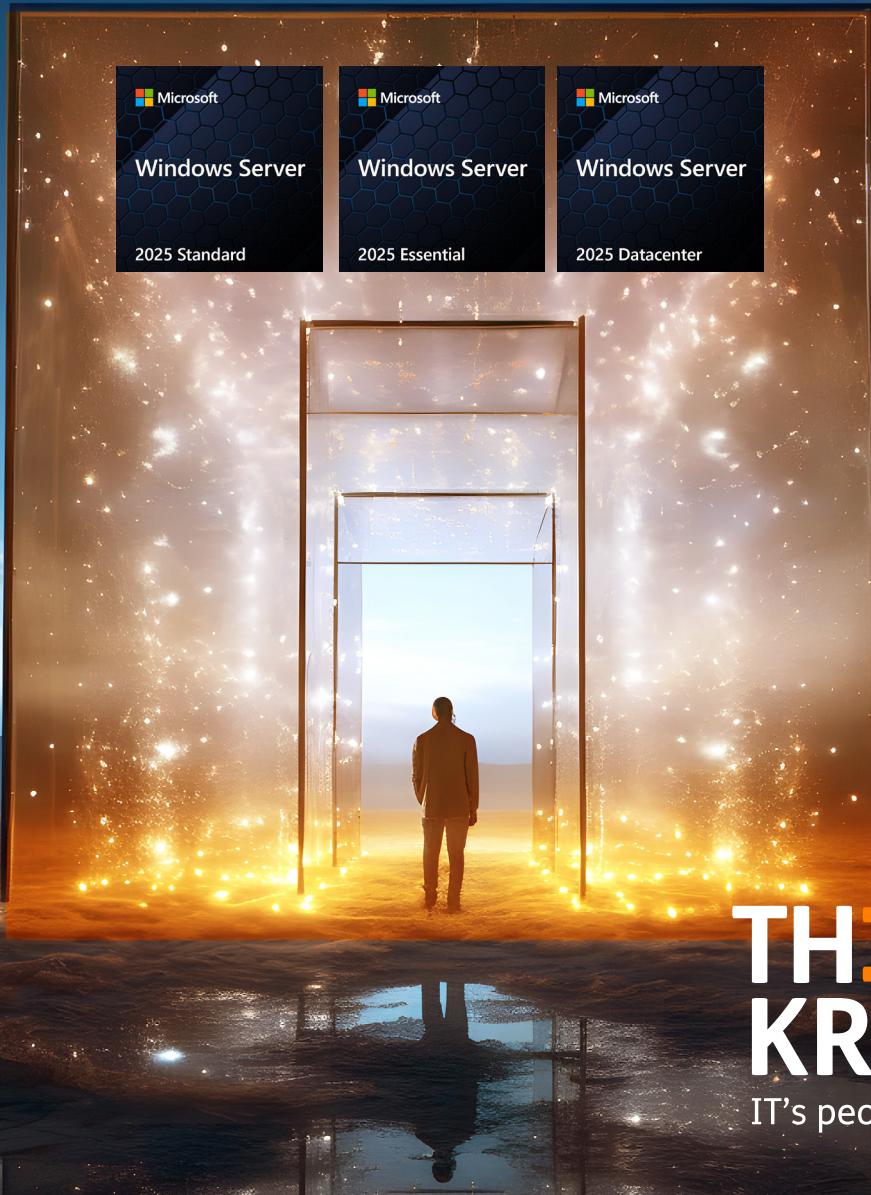


Windows Server 2025

Die wichtigsten neuen Features



**THEMAS
KRENN®**

IT's people business

Inhaltsverzeichnis

Einleitung	4
1. Active Directory	5
1.1 Neue Funktionsebene	
1.2 Leistungsfähigere Datenbank	6
1.3 NUMA-Support	
1.4 Neue Performance-Counter	
1.5 Priorität für Replikationspartner	7
1.6 Neuer Algorithmus zum Auffinden von DC	
1.7 Security-Verbesserungen	8
1.8 Methoden für den Kennwortwechsel	
2. File-Service	8
2.1 SMB over QUIC in allen Editionen	
2.2 SMB over QUIC künftig als bevorzugtes Protokoll	9
2.3 QUIC Client Access Control	10
2.4 Aktivierung von SMB over QUIC	
2.5 Sicherheitsfunktionen für SMB	11
2.6 NTLM-Authentifizierung für SMB-Verbindungen blockieren	
2.7 Zahl der NTLM-Anmeldeversuche begrenzen	12
2.8 Intervalle zwischen den Logins	13
2.9 Bestimmte SMB-Versionen erzwingen	14
2.10 SMB-Signing standardmäßig aktiviert	16
2.11 Standardmäßig aktivierte Firewall-Regeln	17
3. Storage	18
3.1 Vollwertige Unterstützung für NVMe	
3.2 Storage Spaces Direct	
3.3 Dedup und Kompression für ReFS	19
4. Update-Management	20
4.1 Migration über Inplace-Upgrade oder Neuinstallation	
4.2 Vor- und Nachteile beider Methoden	21
4.3 Update-Quellen	
4.4 Voraussetzungen für ein Upgrade	23
4.5 Verfahren abhängig von Server-Rollen	
4.6 Hotpatching	24
4.7 Cloud-Anbindung über Azure Arc erforderlich	
4.8 Für alle Editionen und Installationsoptionen	25

5. Hyper-V	25
5.1 GPU zwischen VMs teilen	
5.2 Pooling von Grafikprozessoren	26
5.3 Live Migration in Workgroup-Cluster	
5.4 Gemischte CPUs in Cluster	27
5.5 VMs der Gen2 als Vorgabe	
6. Network ATC	28
6.1 Gängige Aufgaben beim Einrichten von Netzwerken	
6.2 Automatisierung durch Network ATC	29
6.3 Network ATC installieren	
6.4 Vorbereitungen	30
6.5 Konfiguration mittels Intent	
6.6 Intent mit Override anpassen	32
6.7 Intents entfernen	34
7. Neue Komponenten	34
7.1 OpenSSH-Server	
7.2 Software-Installation mit winget	35
7.3 Windows Terminal	36
8. Editionen und Lizenzen	38
8.1 Zwei Haupteditionen	
8.2 Essentials Edition nur über OEMs	39
8.3 Lizenzoptionen	
8.4 Separate Lizenz für Hotpatching	
8.5 Pay-as-you-go-Option	40
8.6 Lizenzierung auf VM-Ebene	41
8.7 Höhere Preise	
9. Fazit	42

Einleitung

Seit Windows Server 2016 sparte Microsoft sichtlich mit Innovationen für sein Server-Betriebssystem. Der Tenor war, dass man mit neuen Releases primär jenen Kunden entgegenkomme, die „noch nicht“ bereit wären, vollständig in die Cloud zu migrieren. Windows Server sollte in der Zwischenzeit die Rolle zukommen, „Legacy-Dienste“ wie Active Directory oder File- und Print-Services bereitzustellen. Die Infrastrukturdiene sten sollten dagegen von Azure Stack HCI kommen, einem OS, das im Prinzip als Außenstelle der Microsoft-Cloud fungiert. Windows Server sollte darauf in virtuellen Maschinen laufen.

Ob Microsoft diese Strategie grundsätzlich geändert hat, lässt sich derzeit schwer beurteilen. Auf der einen Seite baut Microsoft nämlich wesentliche Features in Windows Server ab oder verweigert ihnen eine weitere Entwicklung.

Bereits Windows Server 2022 reduzierte die Szenarien für die Windows Deployment Services (WDS), und mit der Version 2025 erklärt Microsoft Windows Server Update Services (WSUS) als „deprecated“. Der SMTP-Server verschwindet ganz aus dem Produkt und die Remote Desktop Services befinden sich schon lange auf dem Abstellgleis.

Auf der anderen Seite entschloss sich Microsoft jedoch nun, einige bisher exklusive Features von Azure Stack HCI auf Windows Server 2025 zu portieren. Dies betrifft sowohl den Software-definierten Speicher mit Storage Spaces Direct (S2D) als auch die automatische Konfiguration von Netzwerken im Server-Cluster mit Network ATC.

Darüber hinaus erhält Windows Server 2025 eine ganze Reihe genuiner Neuerungen. Viele davon bringen deutliche Fortschritte für Technologien, die zum Teil schon seit Jahrzehnten an Bord sind.

Dazu gehört allen voran das Active Directory, das seit Windows Server 2016 keine nennenswerten Verbesserungen bekam und auf der Funktionsebene dieser Version stehen blieb. Dies ändert sich nun mit Windows Server 2025, wobei die interne Versionsnummer von bisher 7 auf 10 steigt.

Zu den Fortschritten des AD zählen zudem die überarbeitete Datenbank Jet Blue mit einer auf 32K erweiterten Seitengröße, NUMA-Support, zusätzliche Performance-Counter und Security-Funktionen.

Eine gründliche Renovierung erhält zudem das File-Sharing, das nun auch on-prem SMB over QUIC unterstützt, nachdem dies bis dato der Azure Edition vorbehalten war. Hinzu kommen mehrere Verbesserungen für die SMB-Sicherheit, die zum Teil durch striktere Default-Einstellungen erzielt werden.

Nach einer Phase geringer Innovationen bekommt auch Hyper-V in Windows Server 2025 einige interessante Neuerungen. Dazu gehört die Virtualisierung von GPUs, die besonders für AI-Applikationen von Bedeutung ist. Das OS unterstützt sowohl die Partitionierung als auch das Pooling von GPUs.

Neu ist zudem der Support von Live Migration in einem Cluster, der nicht Mitglied im AD ist. Die Dynamic Processor Compatibility erlaubt künftig ein Nebeneinander von Xeon-CPU's der dritten und vierten Generation in einem Cluster.

Vor allem Hyper-V-Hosts kommen die neuen Storage-Features zugute. Dazu zählen der verbesserte NVMe-Support inklusive eines integrierten Initiators für NVMe-OF. Storage Spaces Direct erhalten mit Thin Provisioning ein wichtiges Feature. Es erlaubt eine dynamische Nutzung des vorhandenen Speicherplatzes inklusive dessen Überbuchung.

Außerdem erweitert Microsoft das Deduplizierungs-Feature in ReFS, das nun auch mit virtuellen Laufwerken zureckkommt. Bei VHD(X) ist das Einsparungspotenzial besonders hoch.

Ein von Microsoft besonders gehyptes Feature ist Hotpatching, das ein Installieren von Updates ohne Neustart des Servers erlaubt. Es war ebenfalls schon in der Azure Edition von Windows Server 2022 enthalten und ist künftig auch on-prem verfügbar. Dazu müssen Server allerdings über Azure Arc verwaltet werden und es fallen dafür zusätzliche Kosten an.

Die folgenden Abschnitte beschreiben die Neuerungen im Detail.

1. Active Directory

Windows Server 2025 erhält eine Reihe interessanter Neuerungen für die Active Directory Domain Services (AD DS) und die Lightweight Domain Services (AD LDS). Dazu gehören eine neue Funktionse-

bene für Domänen und Forests, eine Vergrößerung der Datenbank-Seiten auf 32 KB, ein Schema-Update und mehrere Security-Verbesserungen.

1.1 Neue Funktionsebene

Das Anheben der Funktionsebene für Domänen oder Forests dient in der Regel dazu, neue Funktionen der betreffenden Server-Version nutzen zu kön-

nen. Das Update der AD DS sowie der AD LDS trägt die interne Versionsnummer 10, während Windows Server 2016 noch Version 7 enthielt.

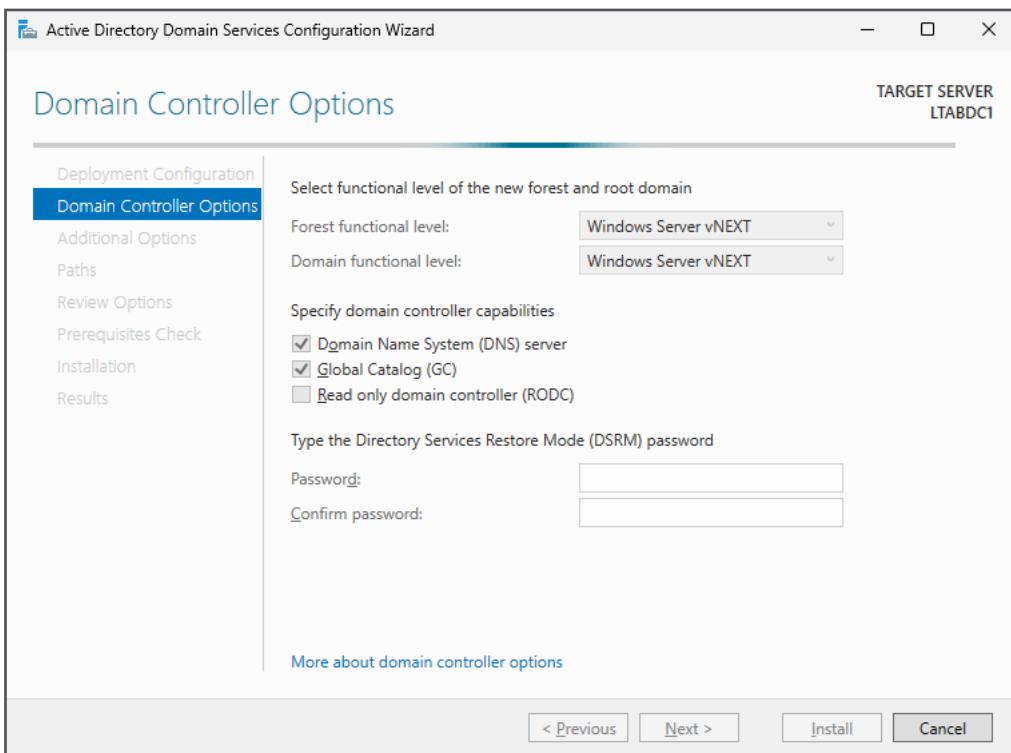


Abb. 1: Mit der neuesten LTSC-Version von Windows Server erhält das AD eine höhere Funktionsebene.

Microsoft überspringt somit die Versionen 8 und 9, die eigentlich Windows Server 2019 und 2022 zu stehen und die beide auf dem Level von 2016 stecken blieben. Laut [Ankündigung](#) gibt es keine Pläne, diese ungenutzten Versionen nachträglich an die beiden älteren Server zu vergeben.

Neu eingerichtete AD-Forests müssen unter Windows Server 2025 mindestens die Funktionsebene von Server 2016 erhalten. Wenn man einen Server 2025 in einer bestehenden Domäne zu einem DC promoten möchte, dann muss sich diese ebenfalls mindestens auf Level 2016 befinden.

1.2 Leistungsfähigere Datenbank

Der wichtigste Grund für das Update der Gesamtstruktur auf die neue Funktionsebene 10 besteht darin, dass man dadurch in den Genuss der aufgebohrten Datenbank-Engine kommt. Sie nutzte seit der Einführung des AD in Windows Server 2000 eine Seitengröße von 8K. Daraus ergab sich eine Reihe von Limitierungen, etwa dass ein einzelnes Objekt nicht größer als 8K sein konnte.

Die überarbeitete Jet Blue erweitert die Seitengröße auf 32K, so dass auch die maximale Größe von Objekten diesen Wert erreichen darf. Attribute vom Typ Multi-Value können dann bis zu 3200 Werte aufnehmen.

Neue Domänen-Controller werden mit 32K-Seitengröße installiert und verwenden 64-bit Long Value

IDs. Für die Kompatibilität mit bestehenden Umgebungen beherrschen sie einen so genannten 8K Page Mode.

Bei einem Upgrade vorhandener DCs auf Server 2025 nutzen diese weiterhin das bisherige Datenbankformat und damit eine 8K-Seitengröße. Die globale Umstellung auf 32K erfolgt auf Forest-Ebene durch Anheben des Functional Levels und setzt voraus, dass sämtliche DCs über eine 32K-fähige Datenbank verfügen. Außerdem muss man das Feature zusätzlich aktivieren.

Das neue Release erweitert zudem das Active-Directory-Schema um zwei neue LDF-Dateien. Das äquivalente Schema-Update für AD LDS ist in der Datei `MS-ADAM-Upgrade3.ldf` enthalten.

1.3 NUMA Support

Der Skalierbarkeit und der Performance kommt auch die neue NUMA-Unterstützung zugute. Bis dato konnten die AD DS nur CPUs in Gruppe 0 nutzen, künftig stehen ihnen alle Prozessorgruppen zur Verfügung.

Diese Verbesserung bleibt jedoch nicht Server 2025 vorbehalten, sondern wurde auch mit dem kumulativen Update für August 2022 an Windows Server 2022 ausgeliefert.

1.4 Neue Performance-Counter

Microsoft hat in der Leistungsüberwachung mehrere neue Indikatoren hinzugefügt, mit denen sich die Performance verschiedener AD-Operationen überwachen lassen. Dabei handelt es sich um Performance-Counter für folgende Funktionen:

- **Local Security Authority (LSA) Lookups**
- **DC Locator**
- **LDAP Client**

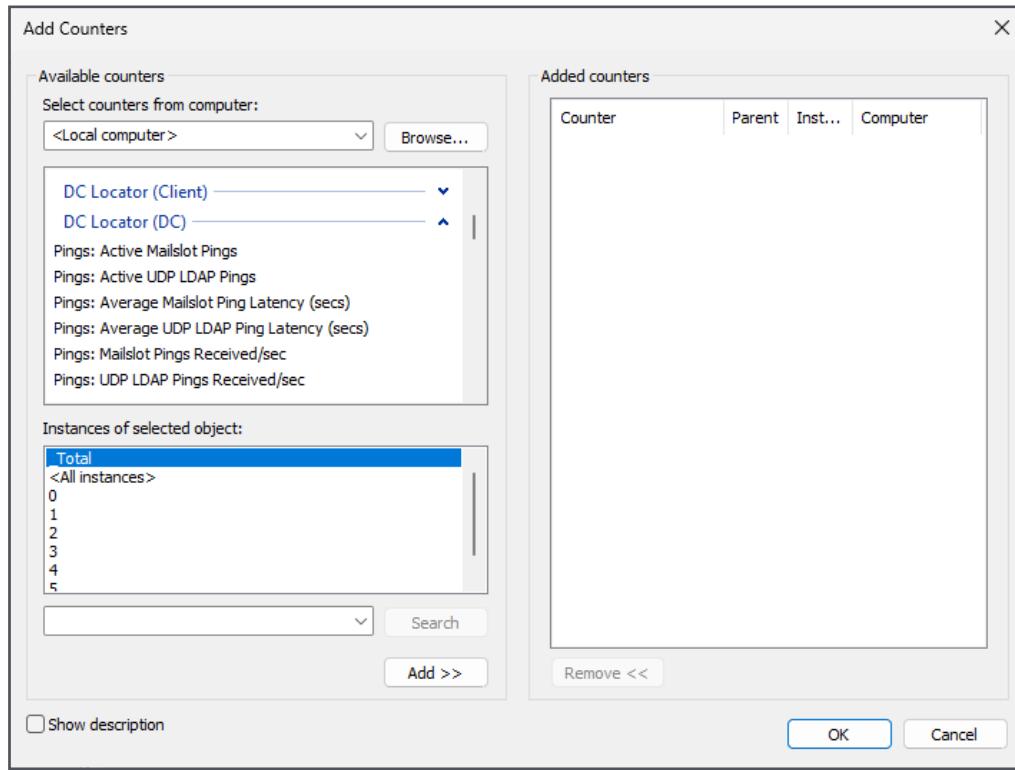


Abb. 2: Neuer Indikator für die Performance des LDAP-Clients.

1.5 Priorität für Replikationspartner

Das System berechnet normalerweise automatisch, mit welcher Priorität die Daten zwischen den verschiedenen DCs repliziert werden sollen. Server 2025 erlaubt es Admins aber nun, diese Priorität für bestimmte Replikationspartner zu erhöhen.

Dies soll die Replikation für bestimmte Szenarios flexibler gestalten.

1.6 Neuer Algorithmus zum Auffinden von DC

Microsoft hat [WINS und Mailslots als Verfahren deaktiviert](#), mit denen Mitglieder der Domäne einen DC lokalisieren können. Der neue Discovery-Algo-

rithmus erlaubt es, DCs anhand der NetBIOS-Namen zu entdecken, ohne dieses veraltete Protokoll zu verwenden.

1.7 Security-Verbesserungen

Die nächste Version des Active Directory bringt einige Fortschritte in puncto Sicherheit, von denen sich einige schon durch Probleme in der Vergangenheit abgezeichnet haben.

Dies betrifft die Kerberos-Unterstützung für den RC4-Algorithmus, von dem Microsoft spätestens nach dem Auftreten von CVE-2022-37966 abgeraten hatte. Er wird nun in die Cipher-Liste für die Verfahren aufgenommen, die man nicht nutzen sollte.

Die LDAP-Kommunikation unterstützt nun TLS 1.3 bei LDAP over TLS. Außerdem wird nach einer [SASL-Authentifizierung](#) automatisch LDAP-Sealing aktiviert.

Wenn man LDAP Channel Binding über eine strengere Richtlinie erzwingt, dann können besonders auf älteren Geräten Fehler auftreten. Zwei neue Events (3074 und 3075) sollen dabei helfen, solche Probleme aufzuspüren. Diese Option gibt es mittlerweile auch schon unter Windows Server 2022.

1.8 Methoden für den Kennwortwechsel

Änderungen gibt es auch im Standardverhalten beim Wechsel von Passwörtern. Die aktuelle SAM-RPC-Methode für das Ändern von Kennwörtern verwendet eine AES-Verschlüsselung und wird als Standard akzeptiert. Microsoft blockiert künftig aber mehrere ältere SAM-RPCs.

Für Mitglieder der Gruppe *Protected Users* („Geschützte Benutzer“) und für lokale Konten von Domänen-Computern wird das SAM-RPC-Interface standardmäßig blockiert. Dies lässt sich bei Bedarf über eine Gruppenrichtlinie ändern.

2. File-Service

Seit der Einführung der Version 3 in Windows Server 2012 entwickelte Microsoft SMB zu einem leistungsfähigen Protokoll, das sich etwa auch für das Storage von virtuellen Maschinen eignet. Die älteren und somit auch vergleichsweise unsicheren Versionen sind aber immer noch im Einsatz.

Mit Windows Server 2025 setzt Microsoft einige Maßnahmen, um die Risiken durch veraltete SMB-Varianten zu entschärfen. Hinzu kommt mit QUIC ein performanter und sicherer Transportmechanismus.

2.1 SMB over QUIC in allen Editionen

Eine der wesentlichen Neuerungen von Windows Server 2022 war SMB over QUIC, aber es blieb bisher der Azure Edition vorbehalten. Dieses Protokoll basiert auf UDP und TLS 1.3, was die Sicherheit und Performance von File-Shares erhöht. Windows Server 2025 wird es in allen Editionen enthalten, und dazu das neue QUIC Client Access Control.

QUIC ist als Alternative zu TCP und RDMA gedacht, um eine sichere Verbindung zu einem File-Server über nicht vertrauenswürdige Netze herzustellen. Ein wesentlicher Vorteil von QUIC ist nämlich die obligatorische Zertifikat-basierte Verschlüsselung.

SMB over QUIC bietet somit eine Art SMB-VPN für Benutzer, die von unterwegs arbeiten. Das Server-Zertifikat erstellt einen TLS 1.3-verschlüsselten Tunnel

über den UDP-Port 443. Der SMB-Verkehr einschließlich der Authentifizierung wird gegenüber dem zugrundeliegenden Netzwerk nicht offengelegt.

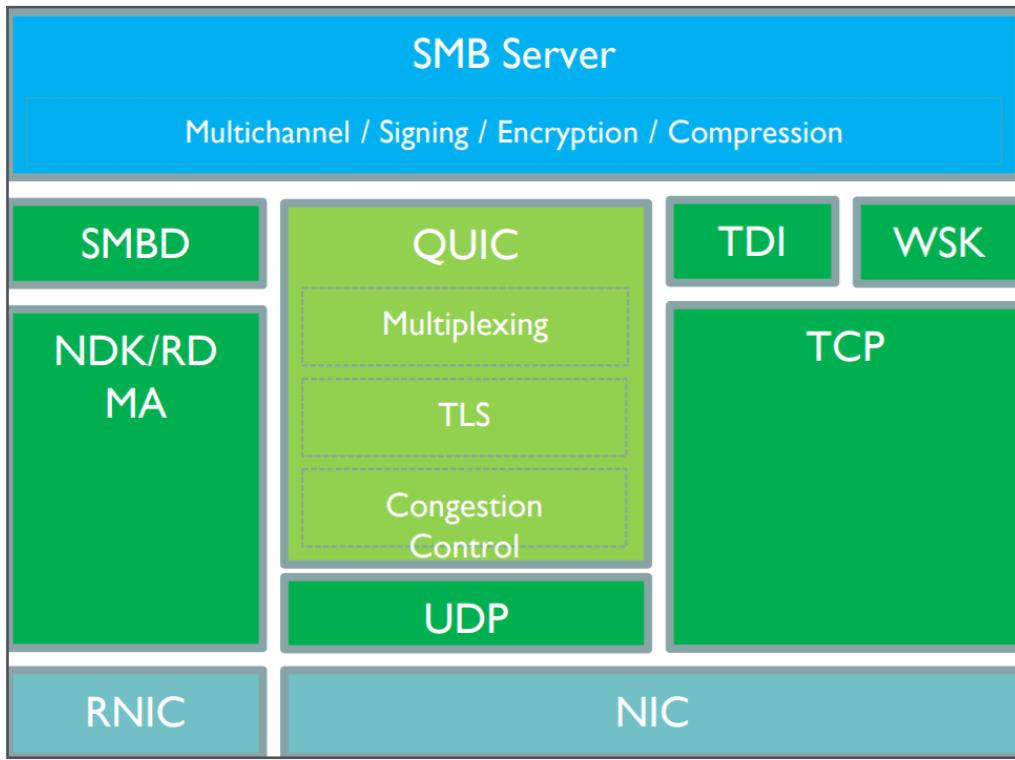


Abb. 3: Transportoptionen für Server Message Block (SMB).

SMB verhält sich innerhalb des QUIC-Tunnels aus der Sicht der Benutzer wie gewohnt, und Funktionen wie Multi-Channel und Komprimierung sind weiterhin verfügbar.

2.2 SMB over QUIC künftig als bevorzugtes Protokoll

Aufgrund dieser Eigenschaften positionierte Microsoft SMB over QUIC bis dato als Feature für so genannte Edge-Server, also File-Server, die in der Cloud oder der DMZ laufen und über das Internet erreichbar sein müssen.

Diese Einschätzung diente auch als Begründung dafür, die QUIC-Unterstützung auf die Azure Edition zu beschränken. Diese läuft in der Microsoft-Cloud oder on-prem auf Azure Stack HCI.

Die [Ankündigung](#) von SMB over QUIC für Windows Server 2025 geht einher mit der generellen Neupositionierung des Features als sichere Alternative zu SMB über TCP. Sie härtet File-Server auch bei der internen Nutzung gegen den Zugriff auf NTLM-Credentials. Daher wird QUIC künftig zum bevorzugten Transportmechanismus für SMB.

2.3 QUIC Client Access Control

Gegenüber der Implementierung in Windows Server 2022 kommt eine weitere Neuerung hinzu, die es erlaubt, den Zugriff auf File-Server via QUIC auf bestimmte Clients zu beschränken. Aktuell akzeptiert ein Server alle Clients, deren Zertifikat auf das gleiche Root-Zertifikat zurückgeht wie jenes für QUIC am Server.

Die Einschränkung erfolgt ebenfalls auf Basis von Zertifikaten. Dazu hinterlegen Admins den Fingerabdruck der Client-Zertifikate in einer Liste mit ver-

trauenswürdigen Geräten am Server. Wenn sich ein Rechner mit dem Server verbindet, dann kann dieser anhand der übertragenen Zertifikatsinformationen entscheiden, ob der Client für den Zugriff berechtigt ist.

In großen Umgebungen könnte es mit viel Aufwand verbunden sein, die Thumbprints aller Client-Zertifikate am Server zu pflegen. Daher unterstützt QUIC Client Access Control auch SAN-Zertifikate, welche die Namen mehrerer Hosts enthalten können.

2.4 Aktivierung von SMB over QUIC

Die Windows Server Insider Preview Build 25997 enthält erstmalig SMB over QUIC für alle Editionen, also auch für Standard und Datacenter. Per Voreinstellung ist das Feature deaktiviert und muss vom Server-Admin freigeschaltet werden. Clients können die Nutzung des Protokolls nicht erzwingen.

Die Tools für die Aktivierung von SMB over QUIC bleiben wie gehabt das Windows Admin Center (WAC) und PowerShell. Die aktuelle Version von WAC ist bei dieser Aufgabe derzeit noch auf die Azure Edition limitiert und verweigert die QUIC-Konfiguration bei anderen Ausführungen des OS.

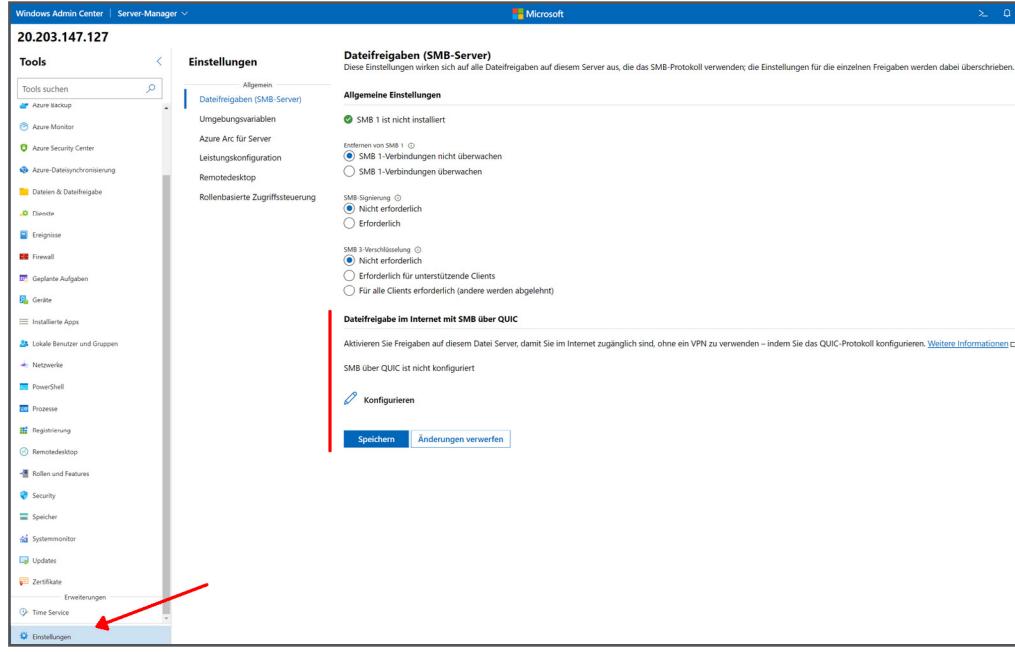


Abb. 4: SMB over QUIC im Windows Admin Center aktivieren.

In PowerShell sind dafür die Cmdlets `New-SmbServerCertificateMapping` und `Set-SmbServerConfiguration` zuständig.

```

Administrator: Windows PowerShell

PS C:\Users\wolf> Get-SmbServerConfiguration |
>> select EnableSMBQUIC, RestrictNamedPipeAccessViaQuic, DisableSmbEncryptionOnSecureConnection

EnableSMBQUIC RestrictNamedPipeAccessViaQuic DisableSmbEncryptionOnSecureConnection
----- ----- -----
True True True

```

Abb. 5: Status von SMB over QUIC in PowerShell abfragen.

2.5 Sicherheitsfunktionen für SMB

Daneben bringt das neueste Server-Release im LTSC eine ganze Reihe von neuen Mechanismen, die das herkömmliche SMB über TCP oder RDMA gegen Angriffe absichern.

Auch wenn SMB over QUIC nach Microsofts Aussagen die Zukunft gehört, so wird es die herkömmlichen Transportmechanismen weiterhin geben.

Windows Server 2025 führt einige Funktionen ein, um auch diese besser zu schützen.

2.6 NTLM-Authentifizierung für SMB-Verbindungen blockieren

Standardmäßig handeln Client und Server über den SPNEGO-Mechanismus das Protokoll für die Authentifizierung aus. Bei einer Verbindung zwischen Rechnern, die einer Domäne angehören, kommt normalerweise Kerberos zum Zug.

In einigen Situationen erfolgt die Anmeldung jedoch über NTLM, nämlich wenn:

- **der Client eine Verbindung über eine IP-Adresse herstellt;**
- **der Kerberos CIFS Service Principal Name für den SMB-Server im Active Directory fehlt;**
- **für die Anmeldung am SMB-Server ein lokales Benutzerkonto verwendet wird.**

Diese Notwendigkeit zur NTLM-Authentifizierung soll mittel- bis langfristig durch Erweiterungen von Kerberos entfallen. Bis dahin sieht Microsoft die Möglichkeit vor, NTLM für SMB zu blockieren. Eine Verbindung scheitert dann jedoch, wenn einer der obigen Gründe für die Verwendung von NTLM gegeben ist.

Windows 11 und Server 2025 erhalten für diesen Zweck eine Gruppenrichtlinie namens **NTLM blockieren (LM, NTLM, NTLMv2)** („Block NTLM (LM, NTLM, NTLMv2)“). Diese existiert allerdings nur für den SMB-Client. Sie findet sich unter *Computerkonfiguration => Richtlinien => Administrative Vorlagen => Netzwerk => LanMan-Arbeitsstation*.

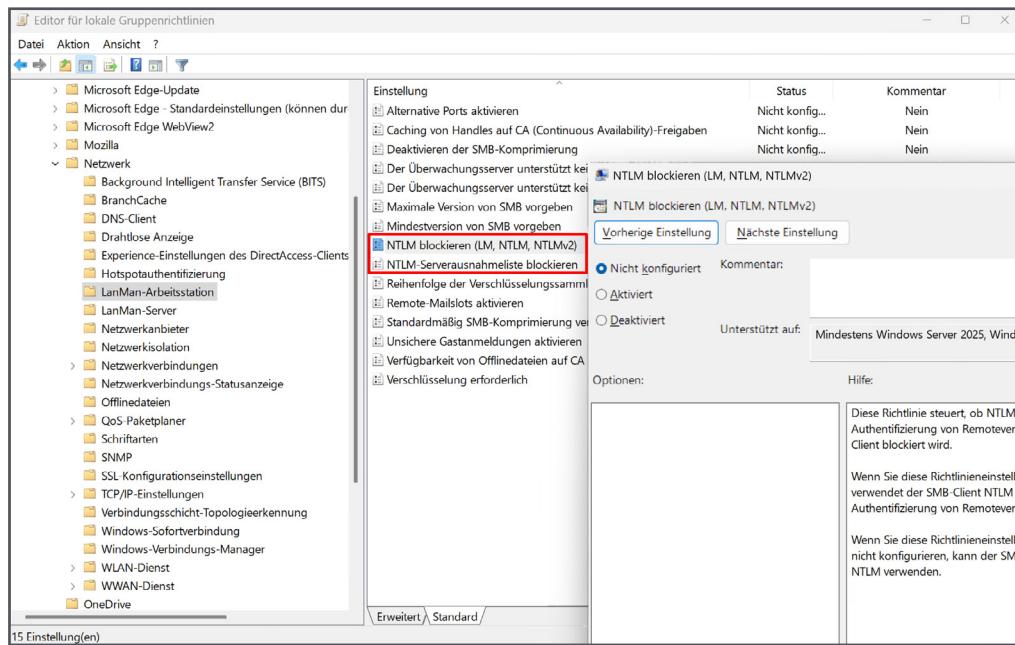


Abb. 6: Die Gruppenrichtlinien für das Blockieren der SMB-Authentifizierung mittels NTLM.

Wenn sich diese Hürden für einzelne Server nicht beseitigen lassen, dann kann man aktuell für sie Ausnahmen definieren. Diesem Zweck dient die Gruppenrichtlinie *Block NTLM Server Exception List*.

Zusätzlich besteht die Möglichkeit, NTLM mit PowerShell für alle oder nur bestimmte Verbindungen mit einem SMB-Server zu deaktivieren:

```
Set-SmbClientConfiguration -BlockNTLM $true
```

Dieser Aufruf ändert die Konfiguration des SMB-Clients global, während man nur eine bestimmte Verbindung folgendermaßen anpasst:

```
New-SmbMapping -RemotePath \\server\share
-BlockNTLM $true
```

2.7 Zahl der NTLM-Anmeldeversuche begrenzen

Wenn es einem Hacker gelingt, Benutzernamen zu erraten oder aus dem Active Directory auszulesen, dann kann er NTLM-Anmeldeversuche in sehr kurzen Abständen an einen SMB-Server schicken.

Um Passwörter der verwendeten Konten zu knacken, kommen typischerweise Dictionaries oder Listen mit kompromittierten Kennwörtern zum Einsatz. Wenn sich in automatisierten Angriffen meh-

Den jeweiligen Status dieser Eigenschaft kann man dann mit

```
Get-SMbClientConfiguration | select BlockNTLM
```

und

```
Get-SmbMapping | select BlockNTLM
```

abfragen. Auch das alte *net use* verfügt nun über einen Schalter */blockntlm*.

rere hundert Login-Versuche pro Sekunde absetzen lassen, dann bestehen gute Chancen für eine erfolgreiche Anmeldung nach kurzer Zeit.

Unternehmen können sich bisher dagegen schützen, indem sie Konten nach einer bestimmten Zahl an gescheiterten Anmeldeversuchen sperren. Dieses Feature lässt sich jedoch für Denial-of-Service-Attacken missbrauchen.

2.8 Intervalle zwischen den Logins

Windows Server 2025 erhält einen alternativen Mechanismus zum Schutz gegen missbräuchliche SMB-NTLM-Authentifizierungen. Der so genannte *SMB NTLM Authentication Rate Limiter* erlaubt die Definition von Intervallen, die zwischen zwei Anmeldeversuchen vergehen müssen. Diesen kann man etwa dann einsetzen, wenn das Blockieren von SMB-NTLM nicht praktikabel ist.

Dadurch werden automatisierte Angriffe ausgebremst und es würde um ein Vielfaches länger dauern, ein Passwort zu knacken.

Die Zahl der Anmeldeversuche innerhalb eines bestimmten Intervalls lässt sich mit Hilfe der Gruppenrichtlinie *Begrenzer für Authentifizierungsrate aktivieren* („Enable Authentication Rate Limiter“) reduzieren. Die Einstellung ist unter *LanMan-Server* verfügbar.

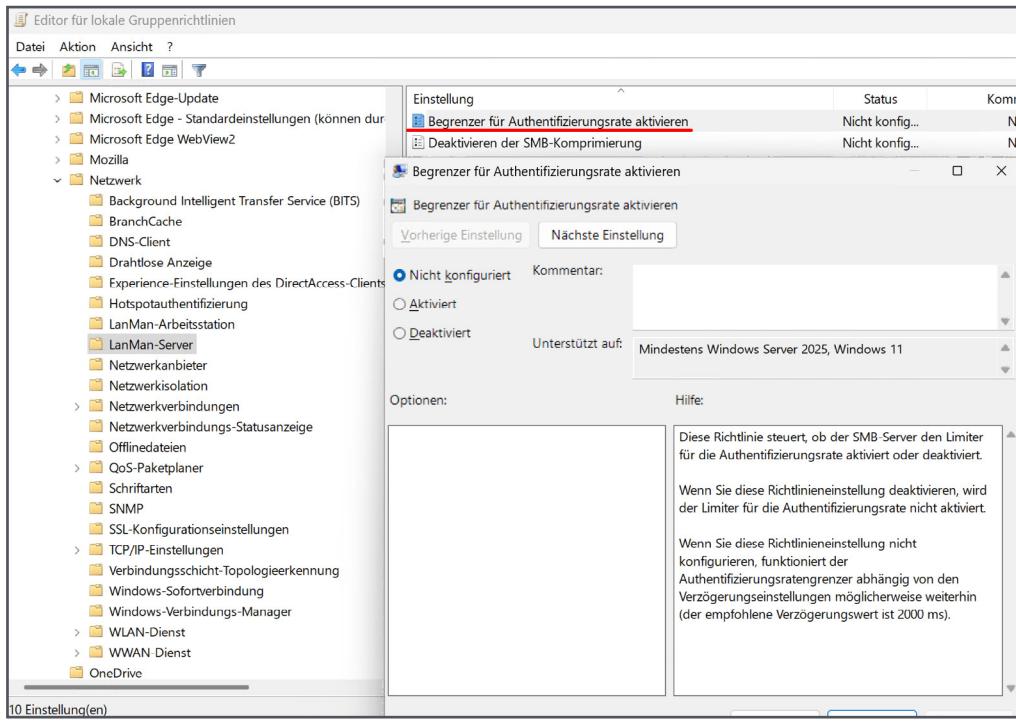


Abb.7: Zu häufige Anmeldeversuche und damit Brute-Force-Angriffe per Gruppenrichtlinie unterbinden.

Die Gruppenrichtlinie lässt jedoch keine Konfiguration der Intervalle zu, die nach einem ungültigen Anmeldeversuch vergehen müssen. Dies geht nur mit PowerShell.

Um die aktuelle Einstellung in PowerShell abzufragen, verwendet man dieses Kommando:

```
Get-SmbServerConfiguration | select InvalidAuthenticationDelayTimeInMs
```

```

Administrator: Windows PowerShell

PS C:\WINDOWS\system32> Get-SmbServerConfiguration | select InvalidAuthenticationDelayTimeInMs
InvalidAuthenticationDelayTimeInMs
-----
0

PS C:\WINDOWS\system32> Set-SmbServerConfiguration -InvalidAuthenticationDelayTimeInMs 1000
Confirm
Are you sure you want to perform this action?
Performing operation 'Modify' on Target 'SMB Server Configuration'.
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
PS C:\WINDOWS\system32> Get-SmbServerConfiguration | select InvalidAuthenticationDelayTimeInMs
InvalidAuthenticationDelayTimeInMs
-----
1000

PS C:\WINDOWS\system32>

```

Abb. 8: Konfiguration des SMB NTLM Authentication Rate Limiter mittels PowerShell.

Um das Intervall zwischen zwei Anmeldeversuchen festzulegen, geht man folgendermaßen vor:

`Set-SmbServerConfiguration -InvalidAuthenticationDelayTimeInMs <Millisekunden>`

2.9 Bestimmte SMB-Versionen erzwingen

Bei SMB handeln Client und Server standardmäßig die höchste, von beiden Seiten unterstützte Version des Protokolls aus. Mit zwei neuen Gruppenrichtlinien erhalten Admins aber nun die Möglichkeit, eine minimale und eine maximale Version von SMB festzulegen.

Auf diese Weise lassen sich ältere und weniger sichere Ausführungen ausschließen. Die niedrigste verfügbare Version ist dabei die 2.0.2. Wenn sich eine Organisation hier beispielsweise auf die jüngs-

te Variante 3.1.1 festlegt, dann lassen sich alle älteren nicht mehr nutzen.

Die Gruppenrichtlinie zur Festlegung einer minimalen und maximalen SMB-Version existiert sowohl für den Client (ausgehende Verbindung) als auch den Server (eingehende Verbindung). Sie befindet sich unter *Computerkonfiguration => Richtlinien => Administrative Vorlagen => Netzwerk => LanMan-Arbeitsstation bzw. LanMan-Server*.

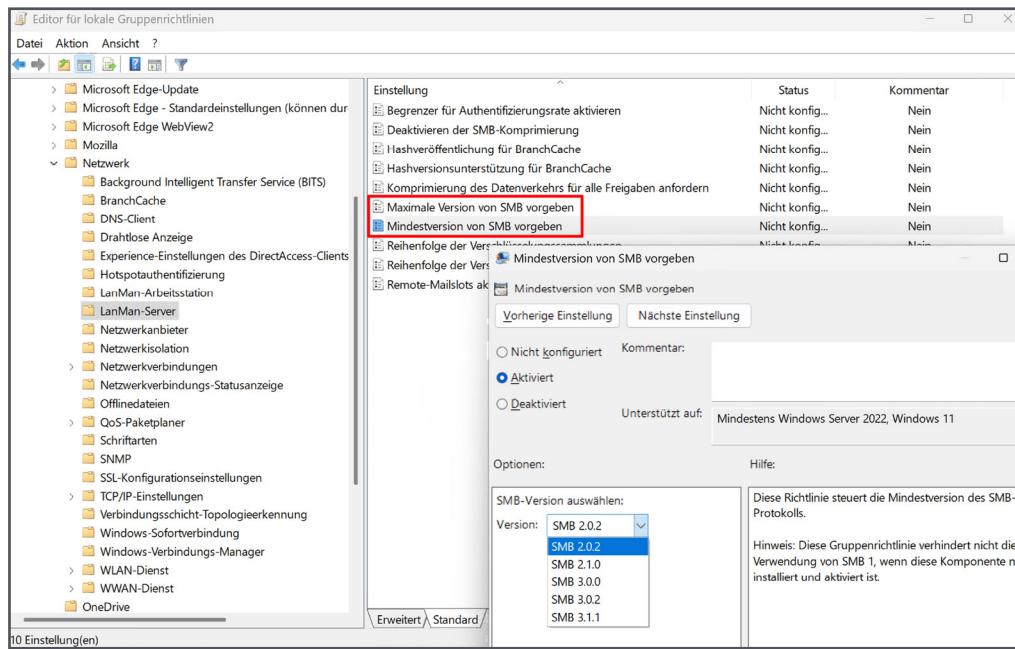


Abb. 9: Auswahl der minimalen und maximalen SMB-Versionen mittels Gruppenrichtlinien.

Auch hier sieht Microsoft eine Konfiguration mittels PowerShell vor. Die Cmdlets

- `Set-SmbClientConfiguration`
- `Set-SmbServerConfiguration`

erhielten dafür die neuen Parameter `Smb2DialectMin` und `Smb2DialectMax`. Als Werte kommen analog zu den Gruppenrichtlinien `SMB202` bis `SMB311` in Frage.

Abfragen kann man die aktuellen Einstellungen über `Get-SmbClientConfiguration` und `Get-SmbServerConfiguration`.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Lernen Sie das neue plattformübergreifende PowerShell kennen - https://aka.ms/pscore6

PS C:\Users\wolf> Get-SmbClientConfiguration | FL requiresecuritysignature

requiresecuritysignature : False

PS C:\Users\wolf> Get-SmbServerConfiguration | FL requiresecuritysignature

requiresecuritysignature : False

PS C:\Users\wolf>
```

Abb. 10: Einstellungen für minimale und maximale SMB-Versionen abfragen.

Wie man obiger Abbildung entnehmen kann, sind standardmäßig alle SMB-Versionen zulässig.

2.10 SMB-Signing standardmäßig aktiviert

Bislang erforderten nur Verbindungen zu einem Domänen-Controller eine SMB-Signatur. Künftig aktiviert Microsoft generell die SMB-Signierung per Voreinstellung, und zwar sowohl auf dem Client als auch auf dem Server.

Der Hersteller hat länger mit dieser Maßnahme gezögert, weil sie zu Kompatibilitätsproblemen mit älteren Systemen führen kann. Admins sollten sich daher auf die bevorstehende Änderung vorbereiten.

Mit folgenden PowerShell-Befehlen lassen sich die aktuellen Client- und Server-Einstellungen für SMB-Signierung abfragen:

`Get-SmbClientConfiguration | Format-List RequireSecuritySignature`

`Get-SmbServerConfiguration | Format-List RequireSecuritySignature`

```

Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Lernen Sie das neue plattformübergreifende PowerShell kennen – https://aka.ms/pscore6

PS C:\Users\wolf> Get-SmbClientConfiguration | FL requiresecuritysignature

requiresecuritysignature : False

PS C:\Users\wolf> Get-SmbServerConfiguration | FL requiresecuritysignature

requiresecuritysignature : False

PS C:\Users\wolf> ■

```

Abb. 11: Bis dato war die SMB-Signierung standardmäßig deaktiviert.

Falls ein unverzichtbares Legacy-System die SMB-Signierung nicht zulässt, dann kann man sie für ausgehende Client-Verbindungen deaktivieren. Dazu führt man diesen Befehl in einer PowerShell mit Admin-Rechten aus:

`Set-SmbClientConfiguration -RequireSecuritySignature $false`

Und um die SMB-Signaturanforderung auf dem Server zu deaktivieren, gibt es den folgenden PowerShell-Befehl:

`Set-SmbServerConfiguration -RequireSecuritySignature $false`

Für diese Aufgabe gibt es auch Einstellungen in den Gruppenrichtlinien. Sie heißen *Microsoft-Netzwerk (Client bzw. Server): Kommunikation digital signieren*. Sie existieren in Ausprägungen für den Client und den Server sowie für immer oder bei Zustimmung der Gegenseite.

Sie finden sich unter *Computerkonfiguration => Richtlinien => Windows-Einstellungen => Sicherheitseinstellungen => Lokale Richtlinien => Sicherheitsoptionen*.

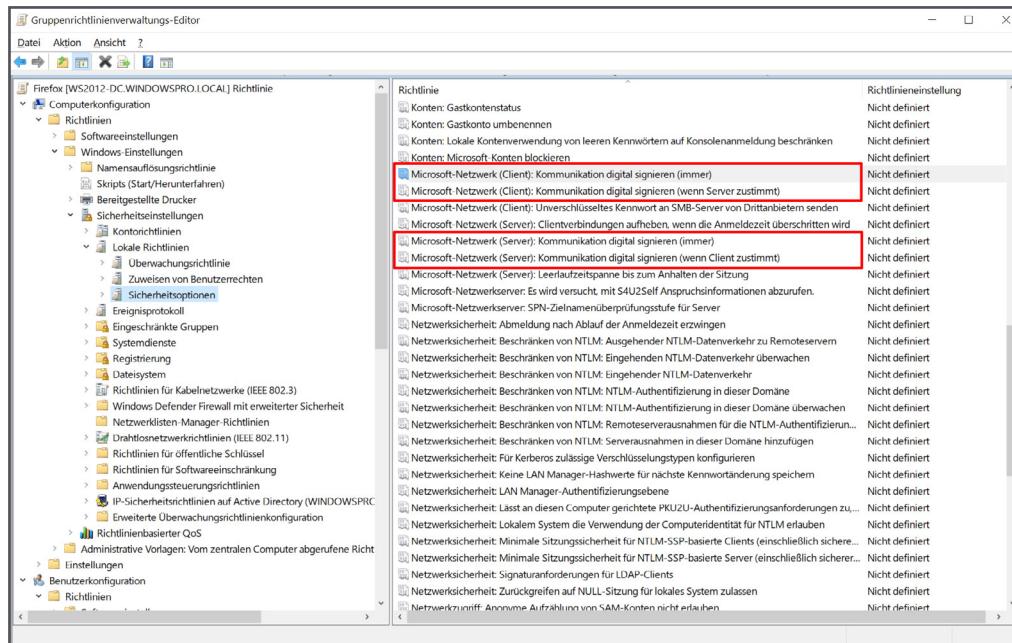


Abb. 12: Die vorgegebene SMB-Signierung lässt sich über Gruppenrichtlinien deaktivieren.

2.11 Standardmäßig aktivierte Firewall-Regeln

Wenn man die File-Server-Rolle installiert, dann aktiviert dies bisher nicht nur automatisch die Firewall-Regeln für SMB oder den Spooler-Service, sondern öffnet auch die NetBIOS-Ports. In Windows

Server 2025 ist dies nicht mehr der Fall. Die Regeln existieren aber weiterhin, so dass man diese bei Bedarf aktivieren kann.

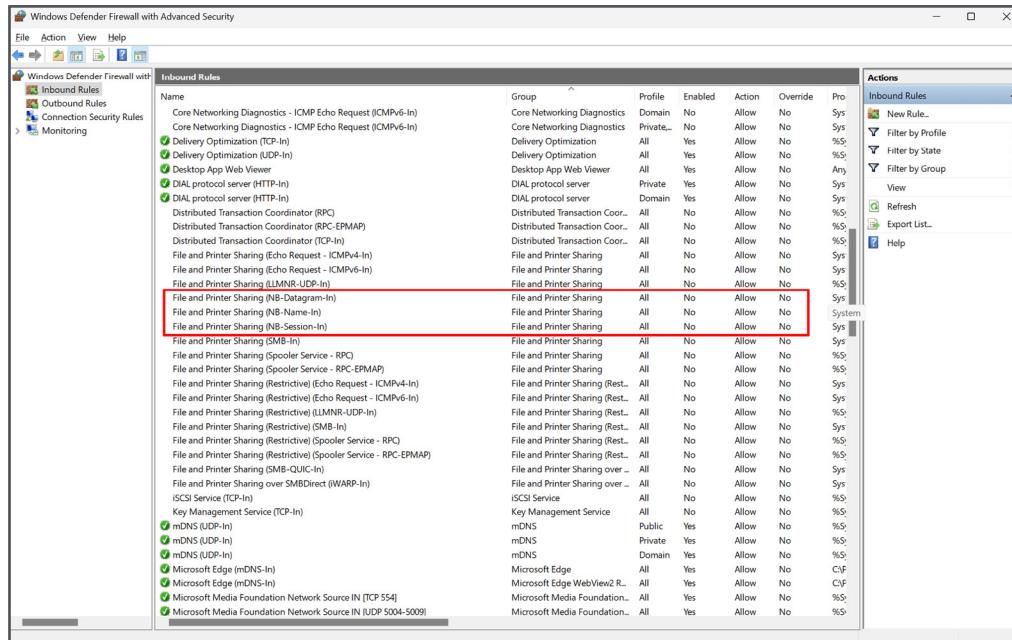


Abb. 13: Das Installieren der File-Server-Rolle öffnet in Server 2025 die NetBIOS-Ports in der Firewall nicht mehr.

3. Storage

Zu den Fortschritten beim Storage-Subsystem zählen ein besserer NVMe-Support, ein überarbeitetes Storage Spaces Direct (S2D) für hyperkonvergen-

te Infrastrukturen sowie ein erweitertes Dedup für ReFS.

3.1 Vollwertige Unterstützung für NVMe

SANs lassen sich an Hyper-V-Cluster weiterhin wie gewohnt über iSCSI oder Fibre Channel anbinden, und in Windows Server 2025 kommt dafür ein integrierter Initiator für NVMe over Fabrics (NVMe-OF) hinzu. Dieser unterstützt vorerst nur TCP, aber später soll für Workloads, die eine geringere Latenz erfordern, der Support für RDMA ergänzt werden.

Insgesamt verspricht Microsoft für die nächste Version seines OS eine deutlich höhere Performance auf NVMe-Storage mit bis zu 90 Prozent mehr IOPS. Das Ganze soll sich mit einer geringeren Auslastung der CPUs erzielen lassen, so dass den VMs mehr Prozessorleistung verbleibt.

3.2 Storage Spaces Direct

Zur wichtigsten Neuerung in S2D gehört die Unterstützung für Thin Provisioning. Damit lässt sich der physische Speicher nun überbuchen und wird erst dann belegt, wenn er tatsächlich für Daten benötigt wird. Volumes mit fixer Größe kann man konvertieren, so dass sie ihren maximalen Speicherplatz nicht gleich verbrauchen.

Thin Volumes lassen sich als Vorgabe für einen Storage Pool festlegen. Alternativ können Benutzer beim Anlegen von Volumes entscheiden, welchen Typus sie erstellen möchten.

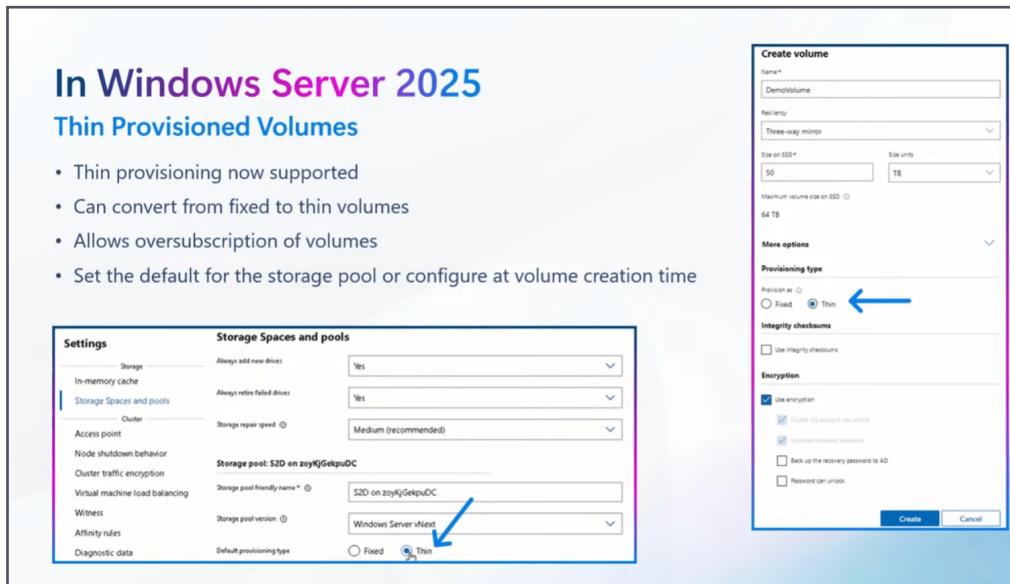


Abb. 14: Thin oder fixed Volumes lassen sich als Standard für Storage Pools vorgeben oder man wählt den Typ beim Anlegen aus.

Verbesserungen bringt S2D in Windows Server 2025 auch bei der Reparatur und bei der Resynchronisierung der Laufwerke. Muss eine defekte Disk ersetzt werden, dann stellt S2D die Daten auf der neuen Platte automatisch wieder her, nachdem diese in einem Pool redundant vorgehalten werden.

Eine Synchronisierung steht auch dann an, wenn ein Knoten offline war und wieder online gebracht wird.

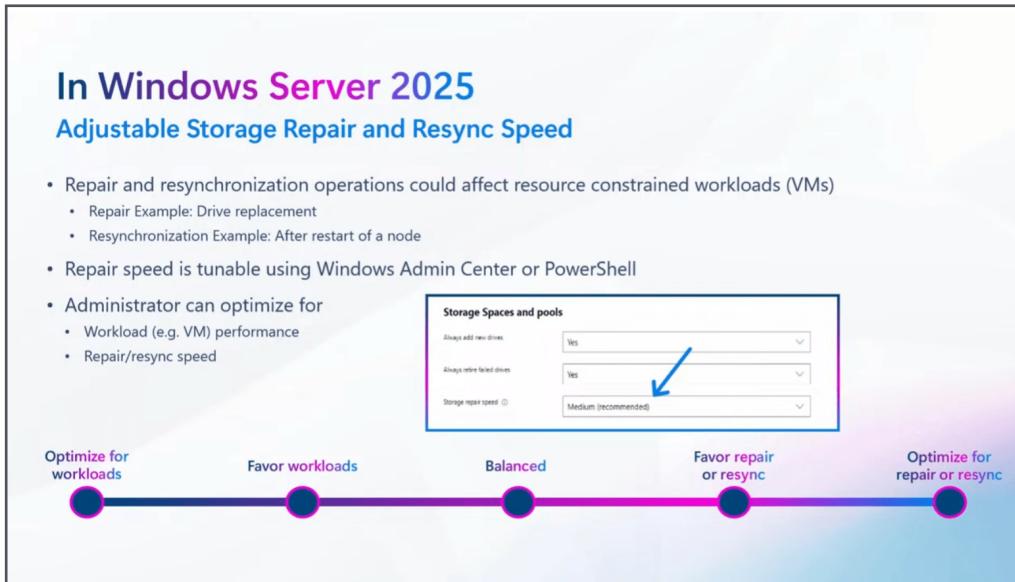


Abb. 15: Die Ressourcenzuteilung zu S2D-Sync und -Reparatur lässt sich in fünf Stufen priorisieren.

Admins können diese S2D-Operationen auf Kosten der Workloads priorisieren oder die VMs bevorzugen, was die S2D-Synchronisierung verzögert. Insgesamt

sieht Windows Server 2025 fünf Stufen für die Verteilung der Ressourcen zwischen diesen beiden Aufgaben vor.

3.3 Dedup und Kompression für ReFS

Das Resilient File System (ReFS) bietet schon seit Windows Server 2016 die Möglichkeit, Daten zu deduplizieren. Dieses Feature war bisher aber auf Cold Data beschränkt, also auf solche Daten, die sich nur relativ wenig ändern, etwa freigegebene Laufwerke auf einem File-Server.

Windows Server 2025 unterstützt Dedup explizit auch für ReFS-Laufwerke, auf denen virtuelle Maschinen gespeichert werden. Das gilt in Azure Stack HCI 24H2 sogar für die Images von Azure Virtual Desktop. Bei VHD(X) sind die Einsparungsmöglichkeiten aufgrund der hohen Redundanz besonders signifikant.

In Windows Server 2025

ReFS Deduplication and Compression

- ✓ Significant savings
 - Over 60% storage savings in virtualization, backups file server workloads
 - Includes Azure Virtual Desktop on Azure Stack HCI
- ✓ Easy to manage
 - Use Windows Admin Center or PowerShell cmdlets
 - Schedule, monitor and start optimizations
- ✓ Smart and efficient
 - Cluster-aware, low overhead
 - Deduplicates only new or changed data
- ✓ Multiple modes
 - Choose from deduplication only, compression only, or both (default)
 - Compression has two separate algorithms enable choice of aggression
- ✓ Administrator enablement required

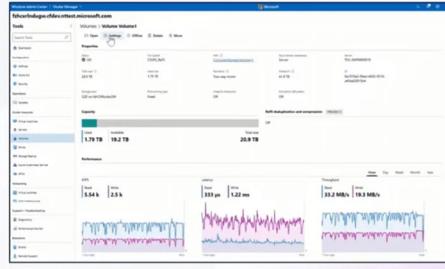


Abb. 16: Dedup und Komprimierung für ReFS lässt sich über das Windows Admin Center steuern.

Sowohl Deduplizierung als auch Komprimierung lassen sich über das Windows Admin Center oder mittels PowerShell verwalten. Letztere verfügt nun

über zwei verschiedene Algorithmen, die auf höhere Verdichtung oder größere Geschwindigkeit optimiert sind.

4. Update-Management

Dieser Abschnitt bespricht zwei Aspekte des Update-Managements: Zum einen, wie Anwender mittels Feature-Updates auf die neueste Version von Windows Server migrieren können, und zum ande-

ren, wie sie das Betriebssystem auf dem aktuellen Stand halten. Zu den bisher bekannten Verfahren gesellt sich nun das aus der Azure Edition bekannte Hotpatching.

4.1 Migration über Inplace-Upgrade oder Neuinstallation

Microsoft unterstützt bei der Migration auf Windows Server 2025 neben der Neuinstallation des Betriebssystems („Wipe and Load“) auch ein Feature-Update von älteren OS-Versionen. Es verursacht weniger Aufwand und geht schneller über die Bühne, lässt sich aber nicht mehr rückgängig machen und birgt die Gefahr eines Fehlschlags.

Windows Server 2025 orientiert sich bei den Upgrade-Optionen an Windows 11, wobei Microsofts Prä-

ferenzen am Client beim Inplace-Update liegen. Dabei bedeuten die Bezeichnungen *Feature-Update*, *Upgrade* und *Inplace-Update* das Gleiche.

Dies gilt es etwa zu berücksichtigen, wenn man Feature-Updates über WSUS beziehen möchte. Dafür muss man die Klassifizierung *Upgrade* auswählen.

4.2 Vor- und Nachteile beider Methoden

Bei Windows Server gibt der Hersteller keiner der beiden Methoden den Vorzug, sondern nennt nur die jeweiligen Pros und Contras. So lässt sich der *Clean OS Install* besser automatisieren, erfordert aber die erneute Einrichtung von Apps, Bibliotheken und Frameworks.

Diese Arbeit kann man sich bei einem Feature-Update sparen, muss aber mit einem gewissen Risiko für das Scheitern dieser Operation rechnen. Microsoft zufolge schlagen bis zu vier Prozent der Inplace-Updates fehl. Entsprechend ist es wichtig, vorher ein Backup zu erstellen.

Strong Recommendation:

Backup Your Windows Server Before Feature Update

We want your Feature Update to be successful !!!

- Telemetry data shows a failure rate between 1.5% and 4% for Feature Updates
- It is NOT 100% successful – and we are continuing to improve reliability every day
- If there is a recoverable error, installation will rollback automatically
- Note that Windows Server cannot be uninstalled after Feature Update – unlike Windows 11 Feature Updates, which can be uninstalled for 10 days
- Error logs can be captured to discover the cause of Feature Update failures
- Best practice is to test your backups with a restore test



Abb. 17: Microsoft weist auf die Einschränkungen und das mögliche Scheitern von Inplace-Updates hin.

Dieses braucht man auch, wenn man die alte Version wiederherstellen möchte. Im Unterschied zu

Windows 11 erlaubt Server 2025 die Deinstallation eines Feature-Updates nämlich nicht.

4.3 Update-Quellen

Anwender können Feature-Updates über die gewohnten Quellen beziehen. Das sind neben der Setup-ISO Windows Update (für Business) und WSUS. Für letzteres gibt es aktuell unter *Produkte und Klassifizierungen* den Eintrag *Microsoft Server Operating System 24H2*, was konsistent mit Windows Server 2022 ist.

Eine Präsentation im Rahmen des Windows Server Summit zeigte jedoch die Option *Windows Server 2025*. Es bleibt abzuwarten, ob Microsoft das Namensschema in WSUS erneut ändert.

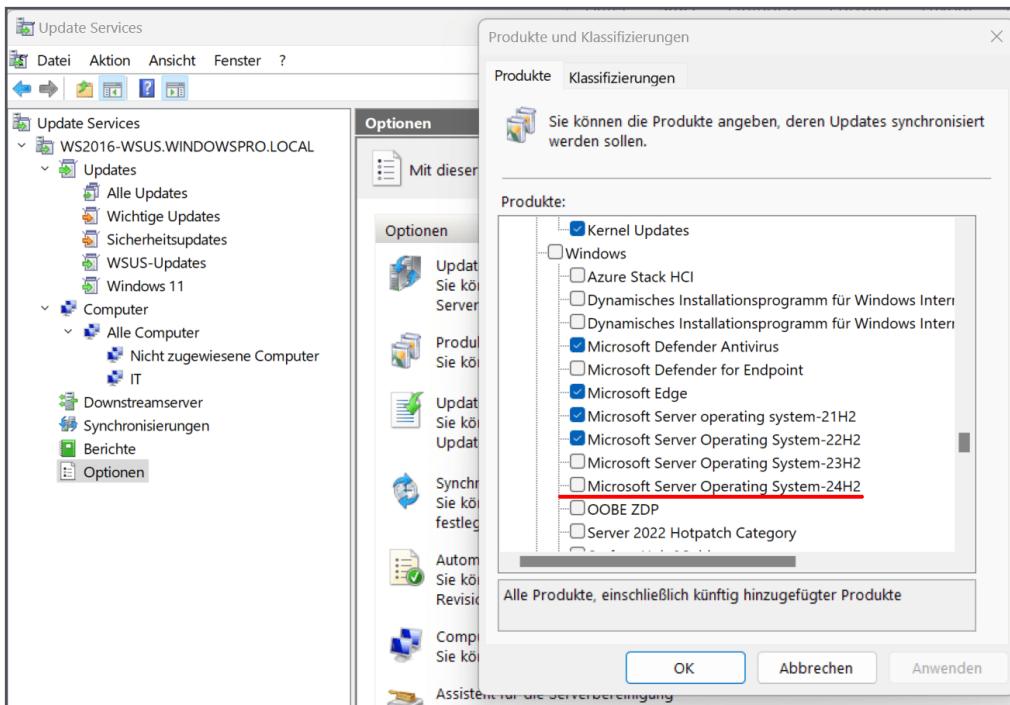


Abb. 18: Updates für Windows Server 2025 erhält man voraussichtlich über die Option Microsoft Server Operating-System 24H2.

Die Installation von Upgrades über Windows Update lässt sich über die entsprechenden Gruppenrichtlinien steuern. Sobald dies für den betreffenden Server genehmigt wurde, bietet es die App *Einstellungen*

unter *Windows Update* zur Installation an. Unter Server Core kann man ein Upgrade dagegen über *sconfig* starten.

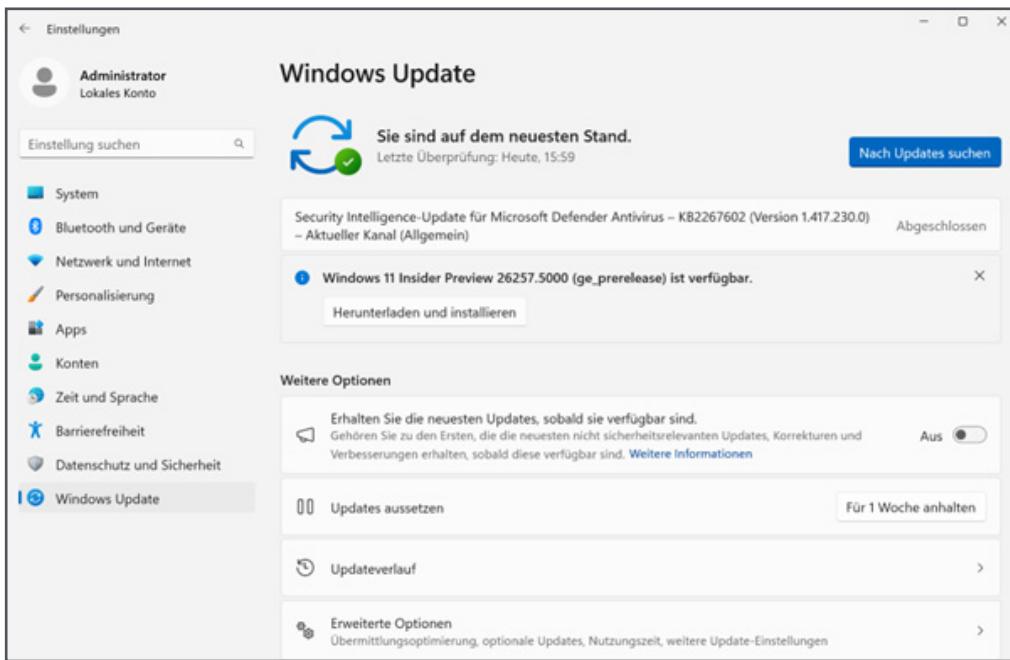


Abb. 19: Die Preview zeigt (irrtümlich?) ein Upgrade für Windows 11 an. Nach dem gleichen Muster wird die GA-Version verfügbar sein.

Dagegen funktioniert ein Wipe and Load nur mittels der Installationsmedien, wobei man *setup.exe* wie in der Vergangenheit über eine Antwortdatei auto-

matisieren kann. Abhängig von der verwendeten Lizenz ist bei diesem Verfahren die Eingabe eines Product Key erforderlich.

4.4 Voraussetzungen für ein Upgrade

Während ein Clean OS Install nur eine kompatible Hardware voraussetzt, gelten für das Inplace-Update Einschränkungen bezüglich der Server-Version, auf die das Upgrade installiert werden kann. Microsoft unterstützt für dieses Szenario so genannte N-4 Media-Based Feature-Updates.

Es bedeutet, dass man die letzten vier Versionen des Betriebssystems mit Hilfe der Installationsmedien direkt auf Windows Server 2025 aktualisieren kann. Das älteste dafür geeignete Release ist somit Server 2012 R2.

Upgrade from / to	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server 2022	Windows Server 2025 (preview)
Windows Server 2012	Yes	Yes	-	-	-
Windows Server 2012 R2	-	Yes	Yes	-	Yes
Windows Server 2016	-	-	Yes	Yes	Yes
Windows Server 2019	-	-	-	Yes	Yes
Windows Server 2022	-	-	-	-	Yes
Windows	-	-	-	-	Yes

Abb. 20: Windows Server 2025 erlaubt im Unterschied zu Server 2022 ein Upgrade von der Version 2012 R2.

4.5 Verfahren abhängig von Server-Rollen

Microsoft empfiehlt ganz allgemein, das Upgrade-Verfahren zu wählen, das für die Anforderungen bestimmter Server am besten passt, ohne sich in Einzelheiten zu ergehen. Ein entscheidendes Kriterium dabei sind die Rollen und Features, die ein Server ausführt.

So ist es eine Best Practice, bei einem Domänen-Controller auf ein Inplace-Update zu verzichten und

stattdessen einen neuen DC aufzusetzen, gegebenenfalls die FSMO-Rollen dorthin zu übertragen und den alten DC herunterzustufen.

Dagegen sind File-, Web- oder DHCP-Server gute Kandidaten für ein Feature-Update, auch wenn es etwa für DHCP auch eine bewährte Methode zu Migration des Dienstes auf einen anderen Server gibt.

4.6 Hotpatching

Eine wesentliche Neuerung in Windows Server 2022 war Hotpatching, aber es blieb der Azure Edition vorbehalten. Dieses Feature beschleunigt nicht nur das Einspielen von Updates, sondern vermeidet auch den Neustart des Servers. Mit der Version 2025 wird es auch on-prem verfügbar sein, allerdings nicht ohne Cloud-Anbindung und zusätzliche Kosten.

Updates werden dabei gleich in den Arbeitsspeicher der gepatchten Prozesse eingeschleust, so dass ein Neustart nicht erforderlich ist, um den aktualisierten Code von Platte zu laden.

Darüber hinaus verwendet Hotpatching kleinere Pakete, so dass die Installation deutlich schneller vonstattengeht. Alle Workloads laufen dabei ohne Unterbrechung weiter.

Das Hotpatching hält das System stets auf dem gleichen Stand wie die regulären Security-Updates. Als Baseline dient immer ein kumulatives Update, wobei dieses alle drei Monate aktualisiert wird. Eine solche Erneuerung der Baseline erfordert dann aber einen Reboot.

Das gilt auch bei der Veröffentlichung einer ungeplanten Baseline nach einem kritischen Update (Zero-day Fix), falls sich dieses nicht als Hotpatch ausliefern lässt. Schließlich werden auch sonst nicht alle Updates als Hotpatch verfügbar sein, so dass in diesem Fall ebenfalls ein Neustart fällig ist.

4.7 Cloud-Anbindung über Azure Arc erforderlich

Die Implementierung von Hotpatching in Windows Server 2025 sieht jedoch kein lokales Management vor. Vielmehr lässt es sich nur über das Azure Portal

verwalten. Dazu muss man die betreffenden Server über Azure Arc mit der Microsoft-Cloud verbinden.

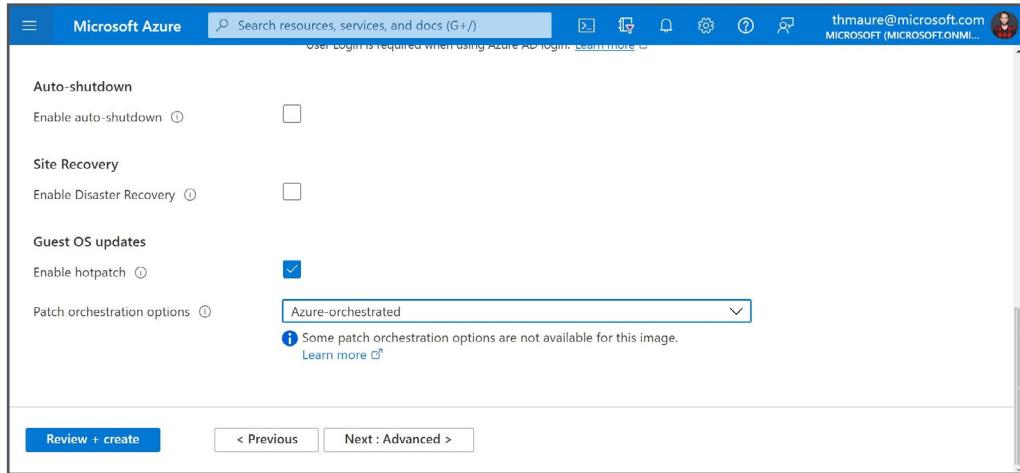


Abb. 21: Das Management von Hotpatching erfolgt auch für on-prem-Server über das Azure Portal.

Hinzu kommt eine monatliche Gebühr für den Service. Das Unternehmen bewirbt Azure und Azure

Stack HCI als Alternative, wo man über die Azure Edition das Hotpatching ohne Aufpreis bekommt.

4.8 Für alle Editionen und Installationsoptionen

Die Installation von Updates ohne Reboot bleibt nicht der Datacenter Edition vorbehalten, sondern wird auch in der Standard Edition verfügbar sein.

Microsoft bekräftigte zudem, dass nicht nur Server Core in den Genuss von Hotpatching kommt, sondern auch die Installation mit Desktop Experience.

5. Hyper-V

Da Hypervisoren mittlerweile ausgereifte Produkte sind, gab es in den letzten Jahren nicht mehr allzu viele Innovationen für diese Software. Microsoft hatte hier mittlerweile jedoch einige Nachholbedarf.

5.1 GPU zwischen VMs teilen

Mit der steigenden Bedeutung von Grafikprozessoren, vor allem aufgrund ihrer zentralen Rolle bei AI-Anwendungen, reicht die bisherige Unterstützung von GPUs in Hyper-V nicht mehr aus. Sie beschränkte sich bis dato auf das Durchreichen einer GPU an eine virtuelle Maschine mittels Direct Device Assignment (DDA). Sie steht dann exklusiv für diese eine VM zur Verfügung.

Das betrifft unter anderem die Virtualisierung von GPUs oder Live Migration von VMs auf Clustern, die nicht Mitglied einer AD-Domäne sind.

Angesichts der hohen Leistungsfähigkeit und der Kosten für moderne Grafikprozessoren ist eine solche Nutzung ineffizient. Windows Server erlaubt es daher zukünftig, GPUs zu partitionieren und auf mehrere VMs aufzuteilen.

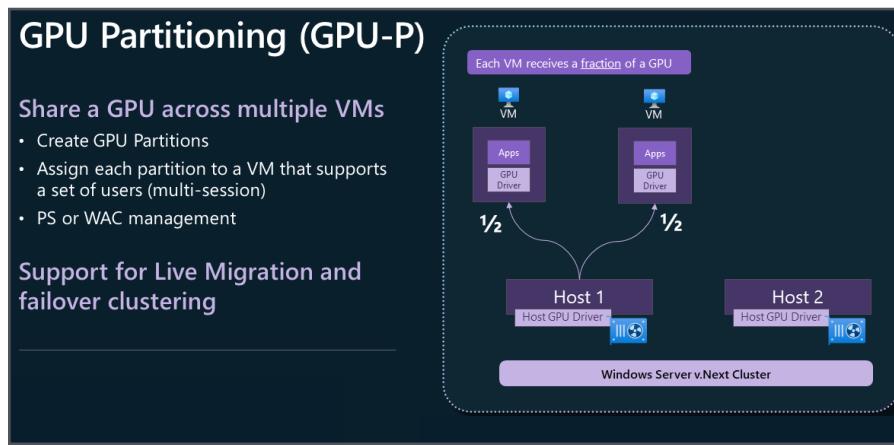


Abb. 22: GPUs auf mehrere virtuelle Maschinen aufteilen.

Neben einer besseren Ressourcennutzung unterstützt diese GPU-Virtualisierung auch die Live Migration, und zwar sowohl innerhalb eines Clusters als auch zwischen Standalone-Hosts. Das bisherige Konzept einer direkten Zuordnung der physischen Hardware an eine VM stand dem unterbrechungs-

freien Transfer einer VM auf einen anderen Host entgegen.

Entsprechendes gilt auch für die Hochverfügbarkeit von VMs, die bei der Nutzung von GPU-Partitionen nun unterstützt wird.

Voraussetzung für das neue Feature sind der Support für SR-IOV, Prozessoren der Serie AMD Milan oder Intel Sapphire Rapids sowie die nVidia-GPUs A2, A10, A16 und A40. Als Gäste kommen Windows 10 / 11, Windows Server 2019 / 2022 sowie Linux Ubuntu 18.04 / 20.04 LTS in Frage.

5.2 Pooling von Grafikprozessoren

Neben der Partitionierung von GPUs beherrscht Windows Server 2025 auch den gegenteiligen Prozess, nämlich das Zusammenfassen mehrerer Grafikprozessoren zu einer virtuellen GPU. Dieses Pool-

ling dient ausschließlich dem Failover; Live Migration unterstützt es nicht, da es auf DDA beruht.

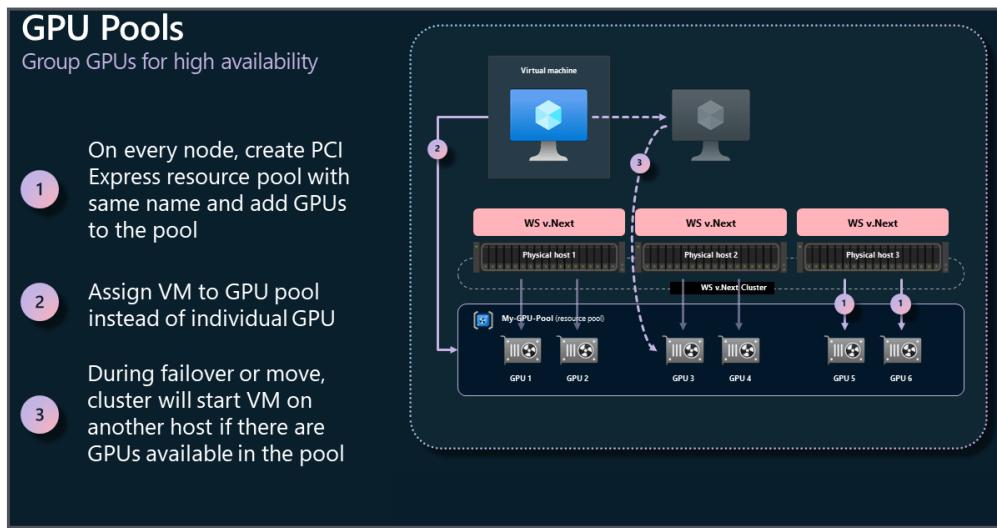


Abb. 23: GPU-Pools für das Failover von VMs.

Admins müssen dazu auf jedem Cluster-Knoten einen Pool mit dem gleichen Namen erstellen und die VMs an diesen zuweisen. Beim Ausfall eines Knotens

startet der Cluster die VM auf einem anderen Server und verbindet sie mit dem entsprechenden Pool.

5.3 Live Migration in Workgroup-Cluster

Hinsichtlich Live Migration bringt Windows Server 2025 eine weitere Neuerung. Das Betriebssystem erlaubt seit der Version 2016 die Einrichtung eines Clusters in einer Workgroup. Eine solche Konfiguration eignet sich primär für kleinere Deployments, etwa in Außenstellen, wo man die Infrastruktur möglichst schlank halten möchte.

Ein Cluster, der nicht Mitglied in einem Active Directory ist, unterstützt nicht alle Workloads und bei Hyper-V bis dato nur eine Quick Migration. Dies ändert sich mit Server 2025, der eine Zertifikat-basierte Live Migration auf einem AD-losen Cluster erlaubt.

5.4 Gemischte CPUs in Cluster

Ein Update gibt es zudem bei der Dynamic Processor Compatibility. Sie macht es möglich, Rechner mit Prozessoren unterschiedlicher Generationen eines Herstellers zu einem Cluster zusammenzuschließen.

Dabei nutzt Windows nur den kleinsten gemeinsamen Nenner bei den CPU-Funktionen.

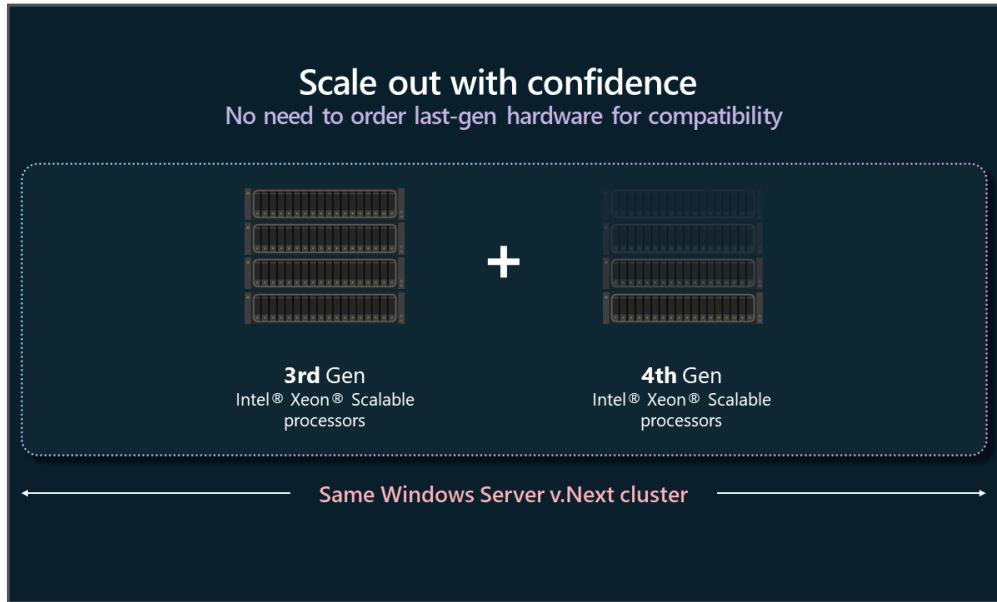


Abb. 24: Die Dynamic Processor Compatibility erlaubt verschiedene Xeon-CPU's in einem Cluster.

In der Version 2025 ist es möglich, Intel Xeon-Prozessoren der dritten und vierten Generation in einem Cluster zu mischen.

5.5 VMs der Gen2 als Vorgabe

Eine weitere Neuerung besteht darin, dass VMs der zweiten Generation künftig zum Standard werden. Wenn man derzeit eine VM mit dem Hyper-V Manager oder dem Windows Admin Center anlegt, dann lautet die Vorgabe immer noch Gen1.

Die zweite Generation bietet nicht nur eine höhere Skalierbarkeit, sondern auch Support für Secure Boot, TPM und UEFI.

6. Network ATC

Die Konfiguration der Management-, Compute- und Storage-Netzwerke in einem Windows-Cluster ist aufwändig und entsprechend fehleranfällig. Mit Network ATC lässt sich diese Arbeit automatisieren. Dieses Feature gibt es in Azure Stack HCI bereits seit 21H2, und findet nun seinen Weg in Windows Server 2025.

Für das Networking in einem Windows-Cluster gelten relativ hohe Anforderungen. So sollen die Kno-

ten nicht nur aus weitgehend identischen Servern bestehen, sondern auch nach Möglichkeit für die jeweiligen Traffic-Typen baugleiche Netzadapter verwenden.

Idealerweise werden die NICs auf jedem Rechner gleich benannt, so dass etwa für die Storage-Anbindung gleichnamige Adapter auf allen Servern zum Einsatz kommen. Dies vereinfacht die Administration.

6.1 Gängige Aufgaben beim Einrichten von Netzwerken

Wenn sich verschiedene Traffic-Typen einen oder mehrere Adapter teilen, dann definiert man für sie jeweils eigene VLANs und man kann dann über QoS-Einstellungen festlegen, wie viel der verfügbaren Bandbreite sie maximal bekommen.

Umgekehrt bündelt man Adapter, wenn mehrere von ihnen für bestimmte Traffic-Typen zur Verfügung stehen, wahlweise über NIC-Teaming oder Switch-Embedded Teaming (SET). Dabei können

natürlich auch mehrere Traffic-Typen über ein NIC-Team laufen und über QoS ihren jeweiligen Anteil an der Bandbreite zugeteilt bekommen.

Zur Konfiguration des Networking in einem Cluster gehört auch meistens das Erstellen von mehreren vSwitches und ihre Zuordnung zur physischen NICs.

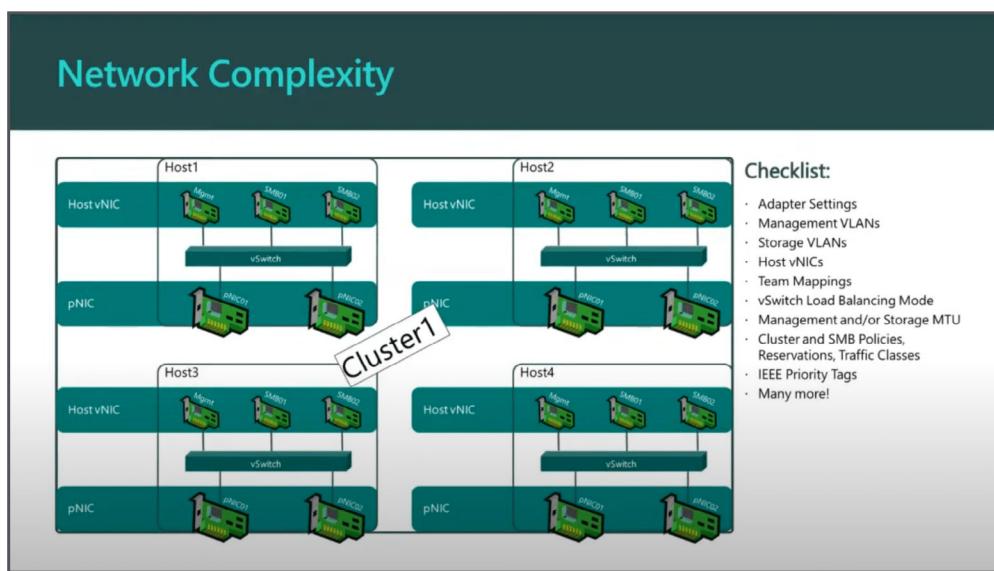


Abb. 25: Microsofts (unvollständige) Checkliste für die Netzwerkkonfiguration in einem Windows-Cluster.

Es liegt auf der Hand, dass der Aufwand für all diese Aufgaben mit der Zahl der Cluster-Knoten steigt. Entsprechendes gilt später auch für die Wartung und die Suche nach möglichen Abweichungen von

der ursprünglichen Konfiguration. Network ATC kümmert sich auch um diesen Aspekt und korrigiert Änderungen, die manuell an den Netzwerken einzelner Knoten vorgenommen wurden.

6.2 Automatisierung durch Network ATC

Ziel von Network ATC ist es, Admins von der manuellen Konfiguration der Netzwerke in einem Cluster zu entlasten. Der Hersteller wendet dabei die von ihm empfohlenen Best Practices automatisch an, wobei sich bestimmte Einstellungen jedoch über so

genannte Overrides überschreiben lassen. Die Standardwerte, die Microsoft beispielsweise für Storage-VLANs verwendet, findet man [hier in der Dokumentation](#).

6.3 Network ATC installieren

Network ATC ist ein Feature in Windows Server 2025. Es lässt sich wie gewohnt über den Server Manager

oder PowerShell installieren.

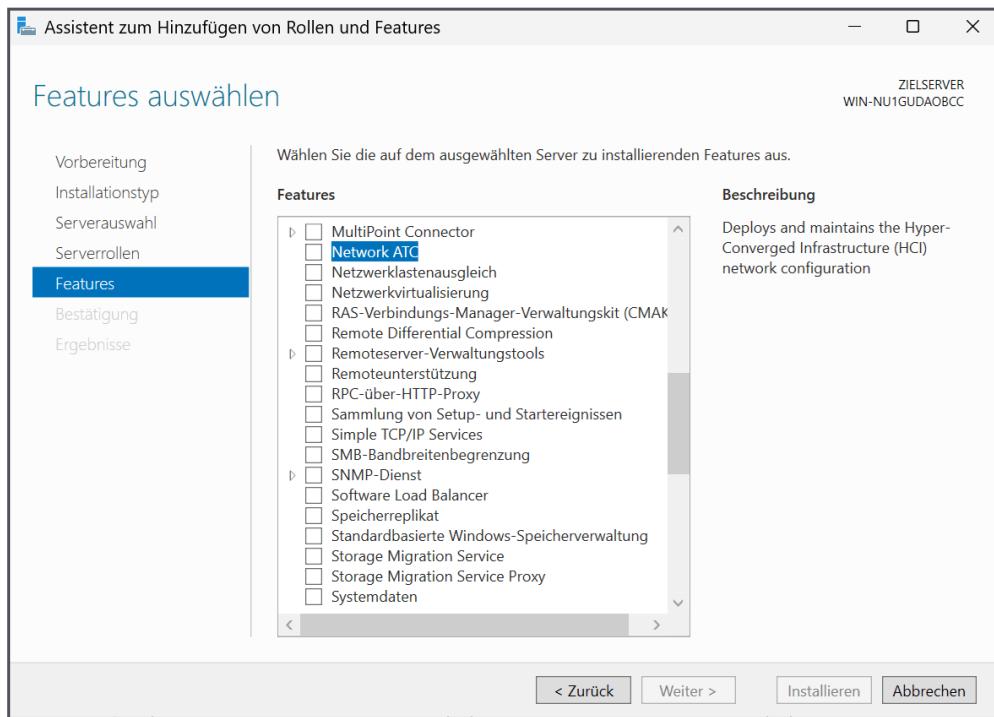


Abb. 26: Installation von Network ATC über den Assistenten des Server Managers.

Mit PowerShell erledigt der folgende Befehl diese Aufgabe:

```
Install-WindowsFeature -Name NetworkATC -IncludeManagementTools
```

Als Tools für das Management von Network ATC kommen Windows Admin Center, das für diesen Zweck eine eigene Extension bietet, sowie Power-

Shell in Frage. Nachdem sich das Feature mit PowerShell relativ unkompliziert verwalten lässt, bietet das notorisch langsame und von Remote-Management-Problemen geplagte WAC hier keinen wesentlichen Vorteil.

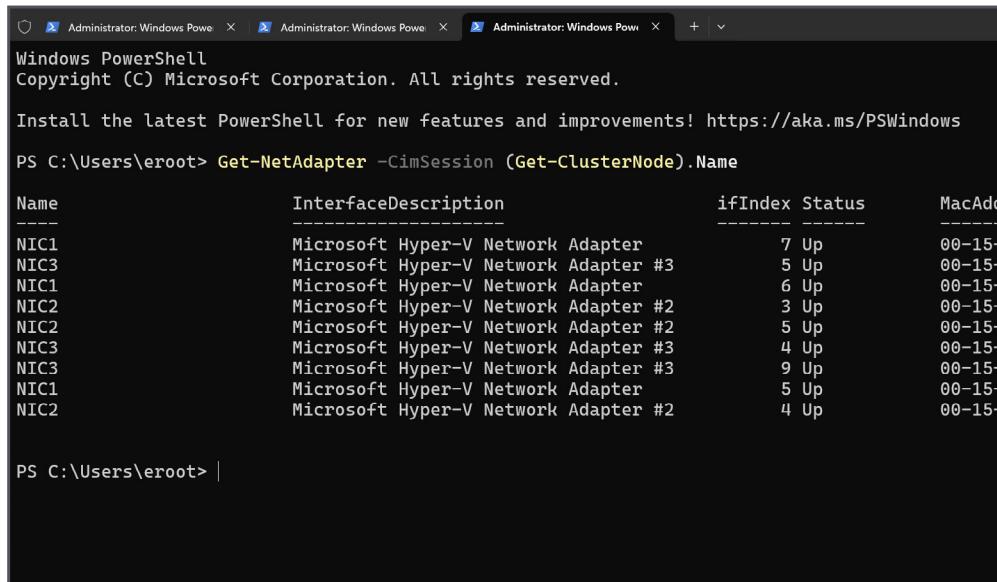
6.4 Vorbereitungen

Zu den Vorarbeiten gehört, dass die NICs, die auf allen Knoten die gleiche Aufgaben erfüllen, auch den gleichen Namen bekommen.

Außerdem muss man sicherstellen, dass jeder Adapter den Status Up anzeigt. Dies lässt sich mit Po-

werShell verifizieren, indem man folgenden Befehl auf einem Knoten des Clusters ausführt:

```
Get-NetAdapter -CimSession (Get-ClusterNode).Name
```



The screenshot shows three separate Windows PowerShell windows. The first window has a title bar 'Administrator: Windows Powe'. The second and third windows also have 'Administrator: Windows Powe' in their title bars. All three windows show the same command and its output. The command is:

```
PS C:\Users\eroot> Get-NetAdapter -CimSession (Get-ClusterNode).Name
```

The output is a table with the following data:

Name	InterfaceDescription	ifIndex	Status	MacAddress
NIC1	Microsoft Hyper-V Network Adapter	7	Up	00-15-
NIC3	Microsoft Hyper-V Network Adapter #3	5	Up	00-15-
NIC1	Microsoft Hyper-V Network Adapter	6	Up	00-15-
NIC2	Microsoft Hyper-V Network Adapter #2	3	Up	00-15-
NIC2	Microsoft Hyper-V Network Adapter #2	5	Up	00-15-
NIC3	Microsoft Hyper-V Network Adapter #3	4	Up	00-15-
NIC3	Microsoft Hyper-V Network Adapter #3	9	Up	00-15-
NIC1	Microsoft Hyper-V Network Adapter	5	Up	00-15-
NIC2	Microsoft Hyper-V Network Adapter #2	4	Up	00-15-

Abb. 27: Die Namen und den Status der NICs im Cluster mit PowerShell ausgeben.

6.5 Konfiguration mittels Intent

Die Konfiguration der Netzwerke erfolgt über so genannte Intents („Absichten“), also die Definition der beabsichtigten Verwendung. Dabei darf jede physische NIC nur in einem einzigen Intent vorkommen.

Um existierende Intents anzuzeigen, setzt man diesen Befehl ab:

```
Get-NetIntent | select IntentName, IntentType, NetAdapterNameCsv
```

Anfangs ist diese Liste erwartungsgemäß leer und man kann mit der Definition eigener Intents beginnen. Diesem Zweck dient das Cmdlet `Add-NetIntent`. Um beispielsweise das Management-Netzwerk zu konfigurieren, führt man auf einem der Cluster-Knoten einen Befehl nach diesem Muster aus:

```
Add-NetIntent -Name Mgmt -Management -AdapterName NIC1
```

```

Administrator: Windows Powershell C:\Users\eroot> Get-NetAdapter -CimSession (Get-ClusterNode).Name
Name           InterfaceDescription      ifIndex Status     MacAddress          LinkSpeed
--           Microsoft Hyper-V Network Adapter    7 Up      00-15-5D-00-40-10   1 Gbps
NIC1          Microsoft Hyper-V Network Adapter    6 Up      00-15-5D-00-40-16   1 Gbps
NIC1          Microsoft Hyper-V Network Adapter #3   5 Up      00-15-5D-00-40-12   1 Gbps
NIC3          Microsoft Hyper-V Network Adapter #3   4 Up      00-15-5D-00-40-11   1 Gbps
NIC2          Microsoft Hyper-V Network Adapter #2   3 Up      00-15-5D-00-40-17   1 Gbps
NIC2          Microsoft Hyper-V Network Adapter #2   5 Up      00-15-5D-00-40-18   1 Gbps
NIC3          Microsoft Hyper-V Network Adapter #3   9 Up      00-15-5D-00-40-15   1 Gbps
NIC3          Microsoft Hyper-V Network Adapter #3   8 Up      00-15-5D-00-40-13   1 Gbps
NIC1          Microsoft Hyper-V Network Adapter #2   4 Up      00-15-5D-00-40-14   1 Gbps
NIC2          Microsoft Hyper-V Network Adapter #2   4 Up      00-15-5D-00-40-19   1 Gbps

PS C:\Users\eroot> Add-NetIntent -Name Mgmt -Management -AdapterName NIC1
-- Creating a new Intent with name Mgmt
-- Management intent was submitted
-- WARNING: Forcing Compute intent when only Management is specified
-- Checking if exact intent request 'mgmt' already exists
-- Checking if specified physical adapters conflict with an existing intent
-- Validating if physical NICs with the name exist on node ws2025-node1 and have status 'Up'
-- Found NIC1 on ws2025-node1
-- Validating physical NICs on ws2025-node1 are symmetric
-- Validating if physical NICs with the name exist on node WS2025-Node2 and have status 'Up'
-- Found NIC1 on WS2025-Node2
-- Validating physical NICs on WS2025-Node2 are symmetric
-- Validating if physical NICs with the name exist on node WS2025-Node3 and have status 'Up'
-- Found NIC1 on WS2025-Node3
-- Validating physical NICs on WS2025-Node3 are symmetric
-- The specified Storage Vlan for NIC1 was: 711
-- Submitting Intent request for mgmt
-- SUCCESS: Intent request for mgmt submitted
-- Checking for existing global intent
-- No existing global intent. Putting global intent with default parameters

Please check Get-NetIntentStatus to see provisioning status. Deployment can take several minutes to complete.
PS C:\Users\eroot>

```

Abb. 28: Management-Netzwerk mittels PowerShell konfigurieren.

In diesem einfachen Beispiel würde auf allen Knoten der Adapter NIC1 für das Management des Clusters konfiguriert. Der Vorgang kann etwas dauern, und mit

Get-NetIntentStatus -Name Mgmt

kann man seinen Fortschritt beobachten.

Es wäre aber auch möglich, zwei NICs für diese Aufgabe heranzuziehen, wobei Network ATC dann automatisch das Teaming konfiguriert:

Add-NetIntent -Name Mgmt -Management -AdapterName NIC1, NIC2

Eine andere denkbare Converged-Variante könnte Management und Compute auf zwei NICs zusammenfassen:

Add-NetIntent -Name CompMgmt -Management -Compute -AdapterName NIC1, NIC2

Stehen genügend Netzadapter zur Verfügung, kann man eine eigene NIC oder ein Team für jeden Traffic-Typ reservieren.

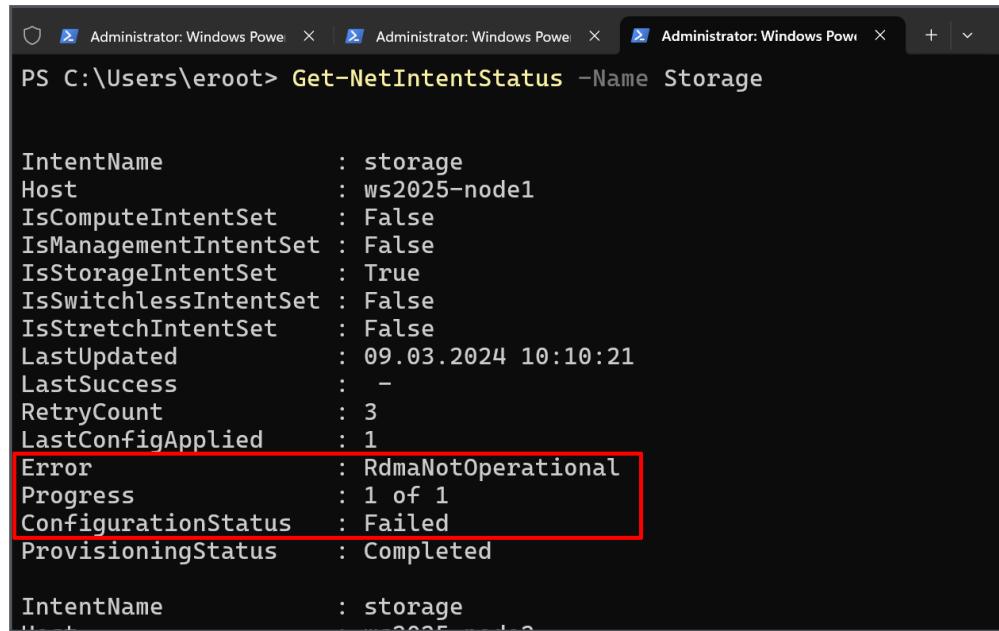
Ein Intent vom Typ Storage konfiguriert automatisch auch die IP-Adressen für die zugewiesenen Adapter. Er verifiziert dabei, dass diese nicht bereits im Netzwerk vergeben sind. Ein einfaches Beispiel für das Erstellen eines Storage-Intent könnte so aussehen:

Add-NetIntent -Name Storage -Storage -AdapterName NIC2

6.6 Intent mit Override anpassen

Führt man obigen Befehl für das Anlegen eines Storage-Intents in einer Lab-Umgebung aus, in der die Cluster-Knoten in einer VM laufen, dann wird der

Vorgang mit dem Fehler *RdmaNotOperational* scheitern. Der Grund dafür ist, dass die virtuellen NICs RDMA nicht unterstützen.



```
PS C:\Users\eroot> Get-NetIntentStatus -Name Storage

IntentName      : storage
Host            : ws2025-node1
IsComputeIntentSet : False
IsManagementIntentSet : False
IsStorageIntentSet : True
IsSwitchlessIntentSet : False
IsStretchIntentSet : False
LastUpdated     : 09.03.2024 10:10:21
LastSuccess      :
RetryCount       : 3
LastConfigApplied : 1
Error           : RdmaNotOperational
Progress         : 1 of 1
ConfigurationStatus : Failed
ProvisioningStatus : Completed

IntentName      : storage
Host            : ws2025-node1
```

Abb. 29: Wenn die NICs RDMA nicht unterstützen, scheitert der Storage-Intent aufgrund der standarmäßigen Anforderungen.

Diese Anforderung kann man durch einen Override übergehen. Dieser sieht so aus:

```
$override = New-NetIntentAdapterPropertyOverrides
```

```
$override.NetworkDirect = 0
```

```
Add-NetIntent -Name Storage -Storage -AdapterName NIC2 -AdapterPropertyOverrides $override
```

```

PS C:\Users\eroot> $override = New-NetIntentAdapterPropertyOverrides
PS C:\Users\eroot> $override.NetworkDirect = 0
PS C:\Users\eroot>
PS C:\Users\eroot> Add-NetIntent -Name Storage -Storage -AdapterName NIC2 -AdapterPropertyOverrides $override
  -- Creating a new intent with name Storage
  -- Storage intent was submitted
  -- Override found for Adapter Properties
  -- Checking if exact intent request 'storage' already exists
  -- Checking if specified physical adapters conflict with an existing intent
  -- Validating if physical NICs with the name exist on node ws2025-node1 and have status 'Up'
  - Found NIC2 on ws2025-node1
  - Validating physical NICs on ws2025-node1 are symmetric
  - Validating if physical NICs with the name exist on node WS2025-Node2 and have status 'Up'
  - Found NIC2 on WS2025-Node2
  - Validating physical NICs on WS2025-Node2 are symmetric
  - Validating if physical NICs with the name exist on node WS2025-Node3 and have status 'Up'
  - Found NIC2 on WS2025-Node3
  - Validating physical NICs on WS2025-Node3 are symmetric
  -- The specified Storage Vlan for NIC2 was: 711
  -- Submitting Intent request for storage
  -- SUCCESS: Intent request for storage submitted
  -- Checking for existing global intent

Please check Get-NetIntentStatus to see provisioning status. Deployment can take several minutes to complete.

PS C:\Users\eroot> Get-NetIntentStatus -Name Storage

IntentName      : storage
Host           : ws2025-node1
IsComputeIntentSet : False
IsManagementIntentSet : False
IsStorageIntentSet : True
IsSwitchlessIntentSet : False
IsStretchIntentSet : False
LastUpdated     : 09.03.2024 12:10:03
LastSuccess     : 09.03.2024 12:10:03
RetryCount      : 0
LastConfigApplied : 1
Error          :
Progress       : 1 of 1
ConfigurationStatus : Success
ProvisioningStatus : Completed

```

Abb. 30: Hinzufügen eines Storage-Intent auf einem Adapter ohne Support für RDMA.

Neben dem Override für Adaptereigenschaften bietet das PowerShell-Modul eine Reihe weitere Cmdlets für die Anpassung anderer Einstellungen, etwa für Switches oder Storage. Diese kann man so anzeigen:

```
Get-Command -Noun NetIntent*Over* -Module NetworkATC
```

Ruft man eines dieser Cmdlets auf, dann erhält man eine Liste aller Eigenschaften, die man damit ändern kann. Zum Beispiel erlaubt `New-NetIntentSiteOverrides` das Anpassen der VLANs für Storage- und Management-Netzwerke.

```

PS C:\Users\eroot> Get-Command -Noun NetIntent*Over* -Module NetworkATC

 CommandType      Name          Version   Source
 ----          ----          -----   -----
 Function        New-NetIntentAdapterPropertyOverrides    1.0.0.0  NetworkATC
 Function        New-NetIntentAdapterRssOverrides    1.0.0.0  NetworkATC
 Function        New-NetIntentGlobalClusterOverrides  1.0.0.0  NetworkATC
 Function        New-NetIntentGlobalProxyOverrides   1.0.0.0  NetworkATC
 Function        New-NetIntentQoSPolicyOverrides   1.0.0.0  NetworkATC
 Function        New-NetIntentSiteOverrides      1.0.0.0  NetworkATC
 Function        New-NetIntentStorageOverrides   1.0.0.0  NetworkATC
 Function        New-NetIntentSwitchConfigurationOverrides 1.0.0.0  NetworkATC

PS C:\Users\eroot> New-NetIntentSiteOverrides

Name      :
StorageVLAN  :
StretchVLAN :
ManagementVLAN :
InstanceId   : 807a2987-4f74-4fb7-9112-8e83898b93bd
ObjectVersion : 1.0.0.10

```

Abb. 31: Cmdlets für das Definieren von Overrides.

Um etwa die Bandbreite für SMB auf 25 Prozent zu beschränken, definiert man einen Override folgendermaßen:

```
$QosOverride = New-NetIntentQosPolicyOverrides
```

```
$QosOverride.BandwidthPercentage_SMB = 25
```

6.7 Intents entfernen

Die Anpassung von existierenden Intents beschränkt sich auf das Anwenden von Overrides. Ein anderweitiges Bearbeiten ist nicht möglich, vielmehr muss man ihn in diesem Fall entfernen und neu anlegen.

Diese Aufgabe übernimmt das Cmdlet *Remove-NetIntent*. Zu beachten ist dabei allerdings, dass

Wenn man den Intent bereits angelegt hat, ohne den Override anzugeben, kann man diesen nachträglich anwenden:

```
Set-NetIntent -Name ComputeStorage -QosPolicy-Overrides $QosOverride
```

es zwar den Intent löscht, aber nicht die von ihm vorgenommene Konfiguration des Netzwerks. Somit ist es notwendig, entsprechende Switches oder Net-QoS-Einstellungen selbst aufzuräumen.

7. Neue Komponenten

Microsoft entwickelt eine Reihe von Windows-Features parallel zum regulären OS-Development. Es handelt sich dabei oft um Open-Source-Projekte auf GitHub oder um die Portierung derartiger Software von Linux auf Windows.

7.1 OpenSSH-Server

Bis dato war der OpenSSH-Server nur als optionales Feature verfügbar, das man selbst hinzufügen musste. Das ändert sich mit Server 2025, den Microsoft auf dem System vorinstalliert.

Darüber hinaus lässt sich der SSHD nun über den Server Manager aktivieren und deaktivieren. Wenn der SSH-Server aktiv ist, dann kommuniziert er nur

Sie gehören dann oft nicht oder erst spät zum Lieferumfang des Betriebssystems. Beispiele dafür sind PowerShell 7, Windows Terminal, curl, OpenSSH oder winget. Die beiden Letzten sind nun bei Windows Server 2025 an Bord.

in privaten Netzwerken und nutzt standardmäßig Port 22. Das OS enthält zudem eine Gruppe namens *OpenSSH Users*.

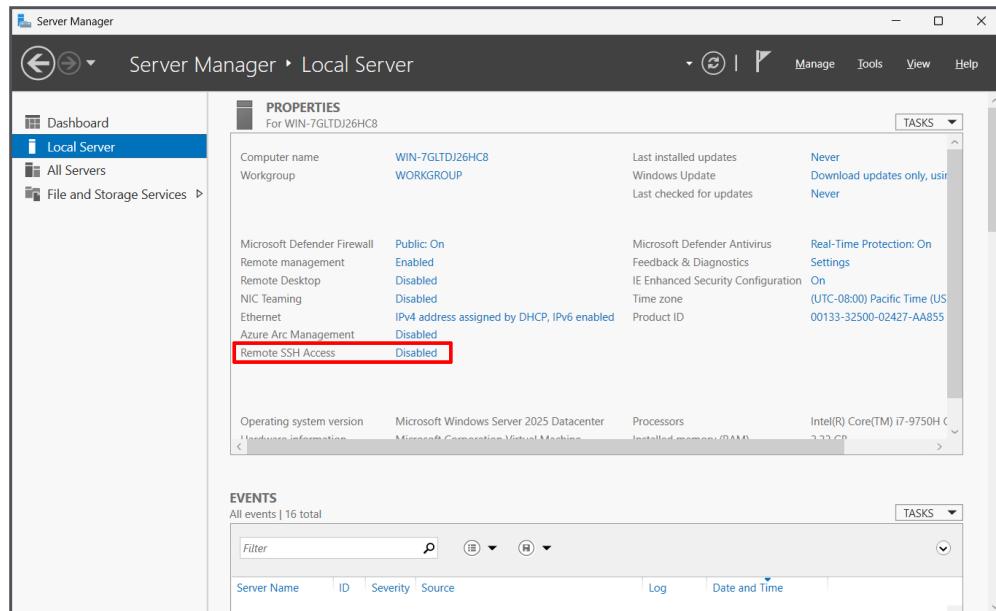


Abb. 32: Der OpenSSH-Server ist zwar vorinstalliert, aber nicht aktiviert. Dies lässt sich im Server Manager ändern.

7.2 Software-Installation mit winget

Der Paket-Manager winget ist beim Client-OS schon länger an Bord, während man ihn unter Windows Server 2022 mit einigem manuellen Aufwand nachinstallieren kann, ohne dass er jedoch offiziell unterstützt wird.

In Windows Server 2025 ist winget dagegen nun offiziell an Bord. Obwohl es sich dabei um ein Tool für die Kommandozeile handelt, setzt es die Desk-

top-Version des Servers voraus. Der Grund dafür dürfte sein, dass es sich bei winget um eine Komponente von App Installer handelt, der seinerseits als Store App implementiert ist.

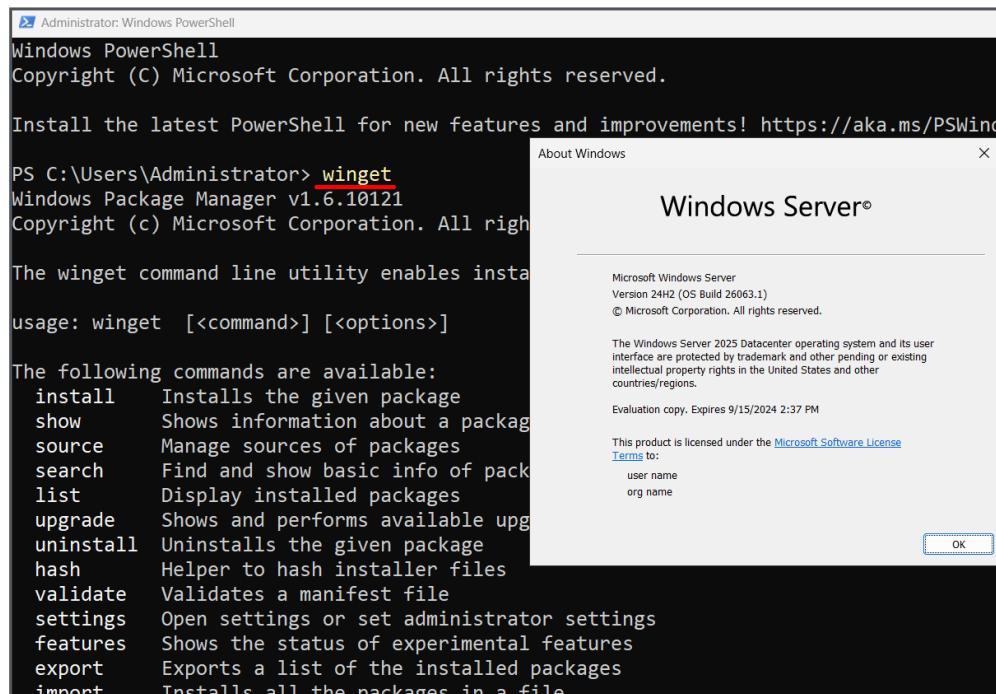


Abb. 33: Der Paket-Manager winget ist in Windows Server 2025 vorinstalliert.

7.3 Windows Terminal

Eine andere Anwendung aus dieser Kategorie ist Windows Terminal, das sich unter Windows 2022 mit einigen Klimmzügen nachinstallieren lässt. Es ist in Server 2025 nun ebenfalls an Bord.

Es handelt sich dabei um eine moderne Konsole, die mehrere Kommandozeilen in verschiedenen Regis-

terkarten eines Fensters ausführen kann. Zusätzliche Flexibilität beim Layout bietet es dadurch, dass man Fenster vertikal und horizontal in Abschnitte teilen kann.

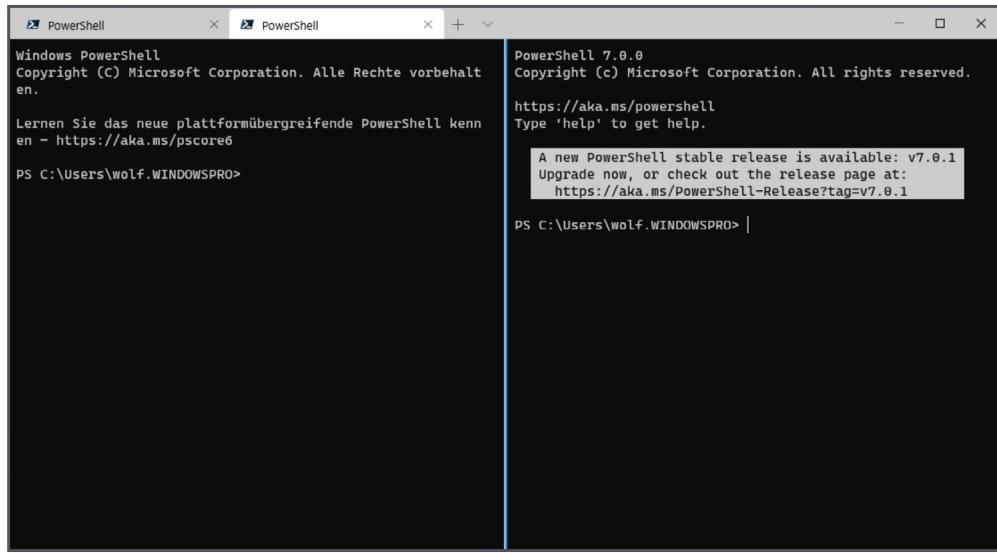


Abb. 34: Windows Terminal unterstützt Tabs und teilbare Fenster.

Windows Terminal integriert sich automatisch mit cmd.exe, Windows PowerShell und PowerShell 6.x und 7. Installiert man das Subsystem for Linux 2,

dann hängt es die bash als weitere Shell in das Terminal ein.

7.3 Windows Terminal

Eine andere Anwendung aus dieser Kategorie ist Windows Terminal, das sich unter Windows 2022 mit einigen Klimmzügen nachinstallieren lässt. Es ist in Server 2025 nun ebenfalls an Bord.

Es handelt sich dabei um eine moderne Konsole, die mehrere Kommandozeilen in verschiedenen Regis-

terkarten eines Fensters ausführen kann. Zusätzliche Flexibilität beim Layout bietet es dadurch, dass man Fenster vertikal und horizontal in Abschnitte teilen kann.

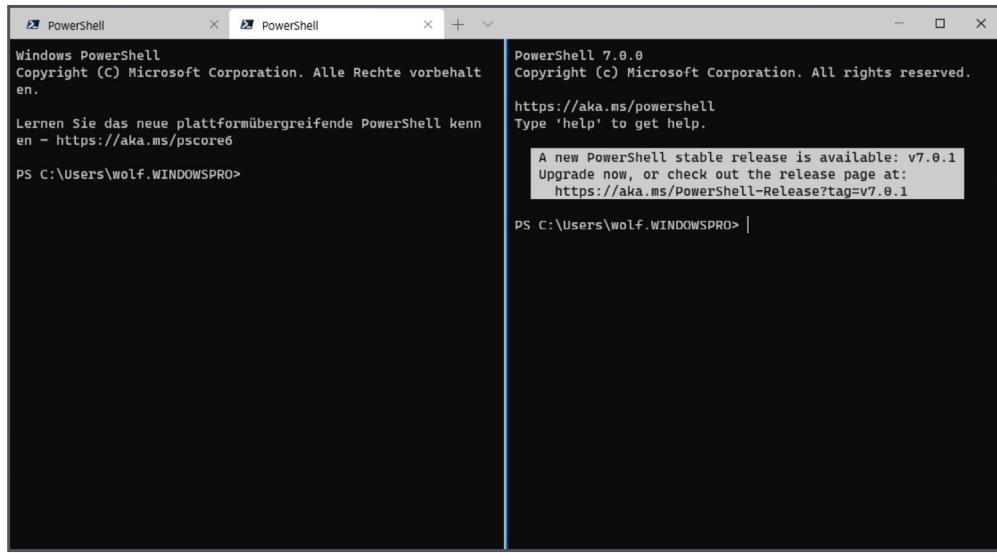


Abb. 34: Windows Terminal unterstützt Tabs und teilbare Fenster.

Windows Terminal integriert sich automatisch mit cmd.exe, Windows PowerShell und PowerShell 6.x und 7. Installiert man das Subsystem for Linux 2,

dann hängt es die bash als weitere Shell in das Terminal ein.

8. Editionen und Lizenzen

Ohne viel Aufhebens gab Microsoft den Build 26100.1742 am 1. November 2024 offiziell als GA frei. Da es sich dabei um das neueste Release im Long Term Service Channel (LTSC) handelt, erhält es fünf Jahre Mainstream- und fünf Jahre Exten-

ded-Support, also wie gewohnt insgesamt 10 Jahre. Der Mainstream-Support währt somit bis zum 09. Oktober 2029, und die erweiterte Unterstützung endet am 10. Oktober 2034.

8.1 Zwei Haupteditionen

Wie bereits die Vorgänger, so gibt es auch die Version 2025 in zwei Haupteditionen, nämlich Standard und Datacenter. Der wichtigste Unterschied zwischen den beiden besteht in den Virtualisierungsrechten.

Während Anwender auf der Datacenter Edition beliebig viele virtuelle Instanzen mit Windows Server ausführen dürfen (Virtual Operating System Environment, VOSE), bleibt die Standard Edition auf zwei VOSEs beschränkt.

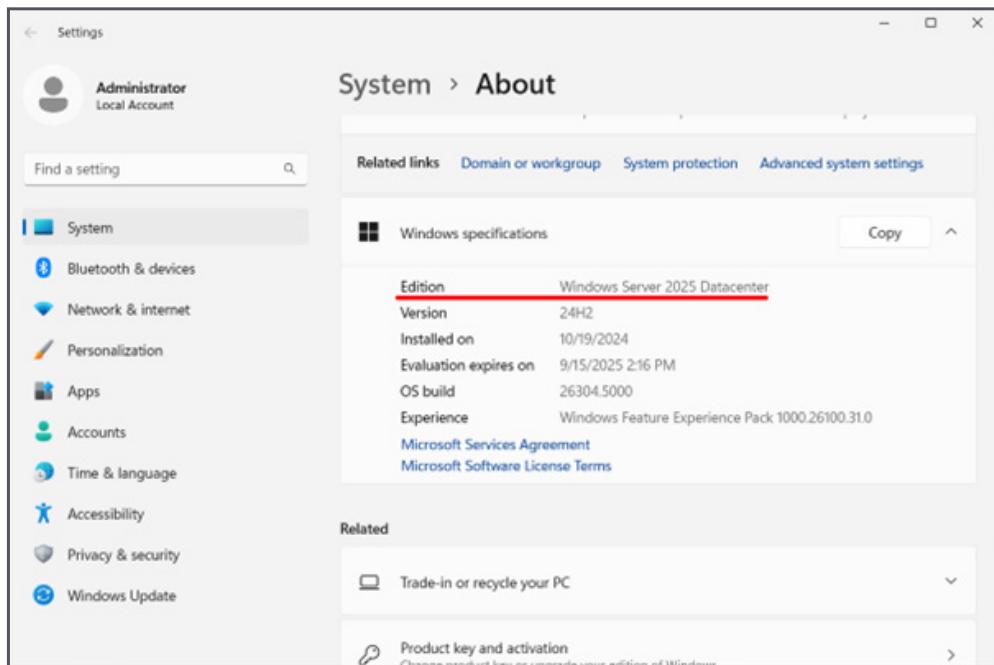


Abb. 35: Die Datacenter Edition erlaubt die Ausführung von beliebig vielen VOSEs mit Windows Server 2025.

Zudem fehlen der Network Controller und der Host Guardian Service. Darüber hinaus ist Storage Replica in der Standard-Ausführung auf Volumes mit 2 TB limitiert.

Die Azure Edition basiert auf der Datacenter Edition, weist gegenüber dieser jedoch einige Einschränkungen auf. So darf sie nur auf Azure oder Azure Stack

HCI genutzt werden und umfasst keine Virtualisierungsrechte, mit denen man Windows Server in VMs ausführen könnte.

Ihr fehlen zudem die Rolle als KMS-Server für die Aktivierung von Windows und die Funktionen für den Betrieb als Container-Host. Ein detaillierter Vergleich der drei Editionen findet sich auf [Microsofts Website](#).

8.2 Essentials Edition nur über OEMs

Die Essentials-Variante ist eigentlich nur noch eine Installations- und Lizenzoption, seit Microsoft in Server 2019 alle ihre exklusiven Features und die dazugehörige Rolle eliminiert hat. Sie kann zudem nur über OEMs bezogen werden.

Diese Ausführung richtet sich an kleinere Umgebungen und lässt wie bisher maximal 25 Benutzer und 50 verbundene Geräte zu. Clients Access Licenses (CALs) benötigen diese jedoch nicht. Außerdem berechtigt sie zur Ausführung einer OS-Instanz in einer VM, wobei sich dann das Host-System auf die Virtualisierung beschränken muss.

8.3 Lizenzoptionen

Für die permanenten Lizenzen bietet Microsoft seit mehreren Generationen des Betriebssystems eine Lizenzierung pro Core an, wobei pro Server mindestens 16 Kerne lizenziert werden müssen. Verfügt ein

Weitere Limitierungen betreffen die Hardware. Ein Essentials-Server darf höchstens mit einem Prozessor mit maximal 10 CPU-Kernen sowie 128 GB RAM ausgestattet sein.

Die Remote Desktop Services wurden auf einem Essentials-Server nie mit allen Rollen unterstützt, aber nun schließen die neuen Use Terms den Einsatz als Terminal-Server explizit aus. Die Nutzungsbedingungen untersagen in der Version 2025 zudem die Verwendung der Rights Management Services (RMS).

8.4 Separate Lizenz für Hotpatching

Ein Novum ist die separate Bepreisung einzelner Features. Dies gilt für Hotpatching, das mit Windows Server 2025 auch in den On-prem-Versionen verfügbar ist. Diese Features müssen jedoch an Azure Arc angebunden werden und benötigen eine Software Assurance, damit sie diese Technologie nutzen können.

Rechner über mehr als 16 Cores, dann muss man weitere Lizenzen über zusätzliche Packages erwerben, wobei dies in Schritten von zwei, vier oder 16 Cores erfolgen kann.

Aktuell finden sich auf Microsofts Website noch keine Preise für das Hotpatching, aber im Vorfeld ließ Microsoft durchblicken, dass dafür ein eigenes Abonnement vorgesehen ist.

8.5 Pay-as-you-go-Option

Die neue verbrauchsabhängige Lizenzierung richtet sich an Anwender, die mit der Standard Edition über keine unlimitierten Virtualisierungsrechte verfügen und vorübergehend zusätzliche Kapazitäten benötigen. Sie können auf diesem Weg zusätzliche VMs mit Windows Server 2025 betreiben.

Voraussetzung dafür ist, dass sie über Azure Arc an Microsofts Cloud angebunden werden. Das Lizenzmodell und die Preise sind identisch wie bei der Ausführung von Windows Server in einer Azure-VM.

Das bedeutet unter anderem, dass die Preise für die Editionen Standard und Datacenter gleich sind, außerdem benötigen Unternehmen dafür keine CALs. Nutzt man die VM indes als Terminal-Server, müssen RDS-CALs erworben werden.

Um die Pay-as-you-go-Option in Anspruch nehmen zu können, darf die Installation von Windows Server nicht für eine andere Lizenz aktiviert sein. Außerdem lässt sie sich nur mit der Retail-Version des OS nutzen.

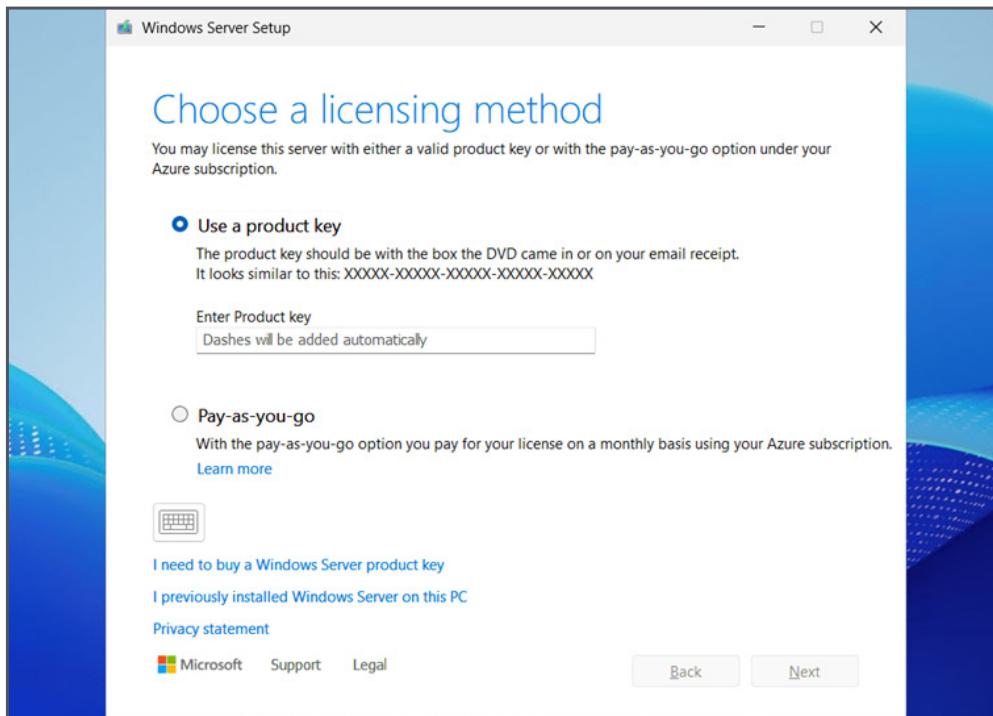


Abb. 36: Das Setup von Windows Server 2025 bietet die Auswahl zwischen Eingabe eines Product Keys und Pay-as-you-go.

Ein Wechsel zwischen der verbrauchsabhängigen und konventionellen Lizenzierung ist ohne Weiteres möglich. Um Erstere zu beenden, muss man nur einen Produktschlüssel für eine permanente Lizenz eingeben.

Wenn man die VM herunterfährt oder dauerhaft entfernt, ohne vorher Pay-as-you-go zu deaktivieren, dann läuft die Abrechnung weiter und es ent-

stehen unerwünschte Kosten. Diese Aufgabe lässt sich über das Azure Portal oder PowerShell erledigen, alternativ entfernt man das Gerät aus Azure Arc.

8.6 Lizenzierung auf VM-Ebene

Seit dem Q4 2002 besteht mit der vCore-Lizenzerung die Möglichkeit, Windows Server unabhängig von der physischen Hardware nur für einzelne VMs zu erwerben. Dabei müssen Anwender ein Minimum von acht virtuellen Prozessorkernen lizenziieren.

Zurzeit gibt es keinen expliziten Hinweis darauf, dass Microsoft diese Lizenzoption für Server 2025 beibehalten wird, aber nachdem es sich dabei um ein relativ neues Modell handelt, gilt dies als wahrscheinlich.

8.7 Höhere Preise

Anlässlich der [Ankündigung von Windows Server 2025](#) nennt Microsoft keine Preise. Auf der Website des Herstellers finden sich jedoch [Angaben zu den beiden Haupteditionen](#), wobei es sich dabei nur um empfohlene Preise handelt.

Demnach kostet die Datacenter Edition 6.771 USD und die Standard Edition 1.176 USD. Beide Preise beziehen sich auf die Basisausstattung mit 16 Cores.

Für den deutschen Markt lässt sich folgende Preiserhöhung feststellen:

- **Windows Server 2025 Essentials: 15 Prozent**
- **Windows Server 2025 Standard, Datacenter und CALs: 10 Prozent**
- **Windows Server 2025 RDS-CALs: 20 Prozent**

Diese Entwicklung beschränkt sich nicht auf Windows Server 2025, sondern zeigt sich auch bei anderen Produkten. Ein aktuelles Beispiel ist System

Center 2025, das gleichzeitig mit Server 2025 freigegeben wurde und dessen Preis ebenfalls um 10 Prozent stieg.

9. Fazit

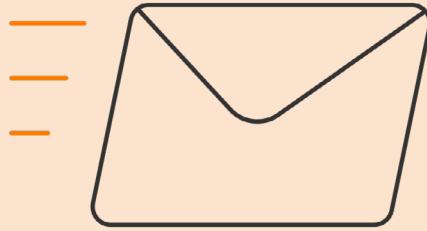
Mit Windows Server 2025 lässt Microsoft dem Betriebssystem eine ganze Reihe von neuen Funktionen und Verbesserungen angedeihen, nachdem die Entwicklung des OS über die letzten acht Jahre weitgehend stagnierte.

Ob sich daraus ein grundlegender Kurswechsel ableiten lässt, der on-prem-Lösungen wieder mehr Aufmerksamkeit gewährt, ist jedoch unklar. Microsoft sendet in dieser Hinsicht unterschiedliche Signale aus.

Zum einen haben wichtige Rollen wie WDS, WSUS oder RDS keine Zukunft, stattdessen sollen Unternehmen für deren Funktionen in die Cloud ausweichen.

Zum anderen erhält Windows Server jedoch einige Features, die bisher der Azure Edition und Azure Stack HCI vorbehalten waren. Das gilt besonders für SMB over QUIC, Hotpatching, fortgeschrittene Funktionen in Storage Spaces Direct oder Network ATC.

Insgesamt profitiert Server 2025 von zahlreichen Verbesserungen in vielen Bereichen und erhält zudem neue Komponenten in Form von OpenSSH-Server, winget und Windows Terminal. Das wohl wichtigste Lebenszeichen des Server-Betriebssystems ist aber wohl das signifikante Update für das Active Directory.



Sie möchten keine **Neuheiten, Trends oder wichtigen Tipps** verpassen? Dann abonnieren Sie unseren **Newsletter** und wir halten Sie auf dem Laufenden!

[Newsletter abonnieren](#)



**Sie haben Fragen/Anregungen/Feedback zu unserem E-Book?
Wir freuen uns auf den Austausch mit Ihnen - [Schreiben Sie uns gerne an!](#)**

Ihnen gefällt, was Sie lesen?
Mehr E-Books gibt's hier:
www.thomas-krenn.com/ueberblick_ebooks

Thomas-Krenn.AG
Speltenbach-Steinäcker 1
D-94078 Freyung
thomas-krenn.com

THOMAS
KRENN[®]
IT's people business