

O'REILLY®

Thomas Joos

Microsoft Windows Server 2025

Von der Planung und Migration bis zur
Konfiguration und Verwaltung

DAS HANDBUCH



Kapitel 1

Neuerungen und Lizenzierung

In diesem Kapitel widmen wir uns u.a. den Neuerungen in Windows Server 2025 gegenüber Windows Server 2022. Die Neuerungen im Vergleich zum direkten Vorgänger halten sich in Grenzen. Der größte Unterschied ist sicherlich die Basis von Windows 11 als Kernel, während Windows Server 2022 noch Windows 10 nutzt. Windows Server 2025 zeigt eine überarbeitete Benutzeroberfläche im Stil von Windows 11. Das neue Windows-Terminal ersetzt die bisherigen PowerShell- und Eingabeaufforderungsfenster. Darüber hinaus gibt es das Azure Arc-Management in der grafischen Benutzeroberfläche, das eine optionale Verbindung zu Azure ermöglicht und Unternehmen eine hybride Cloud-Integration bereitstellt. Ein klassischer Betrieb ohne Cloud-Anbindung bleibt aber weiterhin möglich.

Windows Server 2025 lässt sich sowohl als Mitgliedsserver als auch als Domänencontroller in gemischten Netzwerken mit Windows Server 2019/2022 betreiben. Es gibt aber einen neuen Betriebsmodus für Active Directory. Nach dessen Aktivierung dürfen nur noch Domänencontroller mit Windows Server 2025 vorhanden sein. Der Betriebsmodus spielt für Mitgliedsserver wie immer keine Rolle. Alle Vorteile erhalten Sie, wenn Sie alle Server auf die neue Version umstellen. Natürlich können Sie Windows Server 2025 auch zusammen mit älteren Versionen, zum Beispiel Windows Server 2019 oder 2022, betreiben.

Von Windows Server 2025 gibt es die Editionen Standard und Datacenter. In Windows Server 2025 ermöglichen alle Editionen »Hotpatching«, also das Aktualisieren des Servers im laufenden Betrieb, zumindest von großen Teilen. Das ist mit den anderen Editionen in Windows Server 2022 nicht möglich, sondern der Azure-Edition vorbehalten. Mit Windows Server 2025 sind alle Server-Editionen dazu in der Lage. Hotpatching ermöglicht eine Installation von Sicherheitsupdates ohne Neustart. Dieses Feature bietet für viele Anwendungsfälle erhebliche Vorteile, da Neustarts auf ein Minimum reduziert werden und nur noch alle drei Monate eine »Baseline« für Updates erforderlich ist. Die Integration erfordert eine Verbindung zu Azure Arc, da das Feature als Azure-Dienst angeboten wird und nur optional aktiviert werden kann.

1.1 Die wichtigsten Neuerungen in Windows Server 2025

Windows Server 2025 entspricht in großen Teilen den Möglichkeiten von Windows Server 2022. Die Grenzen der maximal unterstützten Hardware sind mittlerweile so hoch, dass diese ohnehin kaum Unternehmen betreffen. Es gibt ein paar Neuerungen in Windows Server 2025, deren Einsatz durchaus relevant sein kann. Auf diese gehen wir nachfolgend genauer ein.

In-Place-Upgrades werden von älteren Windows Server-Versionen bis hin zu Windows Server 2012 R2 unterstützt. Windows Server 2022-Installationen können über Windows Update direkt auf Windows Server 2025 aktualisiert werden, was die Migration deutlich vereinfacht. Auch für Hyper-V-Migrationen gibt es zahlreiche Werkzeuge und Optionen, die je nach Anforderung eine Live-Migration oder den Einsatz des System Center Virtual Machine Managers unterstützen.

1.1.1 Neuerungen in Windows Server 2025

Mit dem Nachfolger von Windows Server 2022 verbessert Microsoft auch nachhaltig die Sicherheit von Dateiservern. SMB-over-QUIC ist bei allen Editionen dabei und SMB/NTLM werden weiter abgesichert. Bei SMB over QUIC verbinden sich Client und Server mit Server Quick UDP Internet Connections (QUIC) für die SMB-Verbindung. Aufseiten des Servers können das nur Windows Server 2022 Datacenter: Azure Edition und Windows Server 2025 in allen Editionen. Diese Verbindungen sind schneller und sicherer. Dadurch lassen sich sogar SMB-Zugriffe über die Cloud sicher und schnell durchführen. Die Daten werden bei SMB-over-QUIC mit TLS 1.3 verschlüsselt. Gleichzeitig sind die Verbindungen sehr viel schneller als herkömmliche Verbindungen.

Es gibt noch Szenarien, in denen das unsichere NTLM zum Einsatz kommen muss. Aus diesem Grund schaltet Microsoft das Authentifizierungsverfahren noch nicht ganz ab. Wenn die Dateiserver aber optimal in Active Directory integriert sind, braucht man dieses veraltete Verfahren nicht mehr. Es lässt sich daher in Windows Server 2025 blockieren. Die Einstellungen dazu lassen sich über Gruppenrichtlinien im Pfad *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Netzwerk/LanMan-Arbeitsstation* umsetzen. Hier kann NTLM für alle Zugriffe blockiert werden. Auch das Hinterlegen von Ausnahmen ist an dieser Stelle möglich. Ohne Gruppenrichtlinien lassen sich die Einstellungen in der PowerShell mit dem folgenden Befehl umsetzen:

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

Die Einstellung kann mit dem folgenden Befehl überprüft werden:

```
Get-SmbClientConfiguration | Select BlockNTLM
```

Für die Replikation von VMs zwischen lokalen VMs zu Azure Stack HCI oder zu Azure-VMs kann SMB-over-QUIC interessant sein. Diese Technologie ist für alle Editionen von Windows Server 2025 verfügbar. Ideal ist das auch für Dateifreigaben, die über das Internet schnell und sicher zur Verfügung stehen sollen. SMB über QUIC ist eine signifikante Erweiterung in Windows Server 2025, die das Server Message Block (SMB)-Protokoll über das

Quick UDP Internet Connections (QUIC)-Protokoll transportiert. Diese Technologie stellt eine sichere Verbindung bereit, indem sie TLS 1.3 für die Verschlüsselung nutzt und somit Identitätsdiebstahl sowie Man-in-the-Middle-Angriffe verhindert.

Eine der Schlüsselfunktionen von SMB über QUIC ist die Flexibilität in der Port-Auswahl, wodurch Administratoren nicht länger auf den standardmäßig festgelegten UDP/443-Port beschränkt sind, sondern diesen anpassen können. Diese Anpassungsfähigkeit erweitert die Möglichkeiten für sichere und flexible Netzwerkkonfigurationen. Darüber hinaus gilt SMB über QUIC als »SMB VPN« für Remotearbeiter, mobile Gerätenutzer und Organisationen mit hohen Sicherheitsanforderungen.

1.1.2 Neuerungen in Hyper-V und der Virtualisierung

Microsoft verbessert auch Hyper-V. Die Grundstruktur bleibt ähnlich und die Verwaltung erfolgt weiterhin über den Hyper-V-Manager, System Center Virtual Machine Manager oder das Windows Admin Center. Bei Hyper-V gibt es einige Neuerungen, zum Beispiel die neue Konfigurationsversion 12.0. VMs mit dieser Version laufen nur auf Hyper-V-Hosts, auf denen Windows Server 2025 installiert ist, da diese die neuen Funktionen der neuen Serverversion nutzen. Ältere Konfigurationsversionen lassen sich aber auch mit Windows Server 2022/2019 nutzen. Hier müssen Sie jedoch darauf achten, dass die jeweils gesetzte Konfigurationsversion kompatibel mit den Vorgängern von Windows Server 2025 ist.

Mit der Einführung des Delegated Managed Service Account (dMSA) wird darüber hinaus die Migration von Dienstkonto vereinfacht, indem verwaltete und vollständig zufällige Schlüssel bereitgestellt werden, ohne dass umfangreiche Anwendungsänderungen erforderlich sind. Für VMs und Workloads kann das effektive Verbesserungen mit sich bringen.

Die Skalierbarkeit von Hyper-V wurde massiv gesteigert: Virtuelle Maschinen können bis zu 240 TB RAM und 2048 virtuelle Prozessoren nutzen, was die Eignung für hochskalierbare und speicherintensive Anwendungen deutlich erhöht. Zudem wird GPU-Partitionierung unterstützt, die eine flexible Nutzung von Grafikkarten in virtuellen Maschinen ermöglicht. Dies gilt jedoch nur für bestimmte NVIDIA-Modelle und setzt kompatible Treiber voraus.

Windows Server 2025 kann GPUs virtualisieren und gruppieren

Mit Windows Server 2025 ist es möglich, GPUs zu virtualisieren, und auch die Deduplizierung von Daten funktioniert mit Windows Server 2025 besser, vor allem auf dem empfohlenen Dateisystem ReFS. Ab jetzt ist es einfacher, VMs mit der Live-Migration zwischen Hosts zu verschieben, auch ohne dass die Server Mitglied in einer Active Directory-Umgebung sind. Generell sind zukünftig keine AD-Umgebungen mehr notwendig, um alle Funktionen in Hyper-V zu nutzen, zum Beispiel die Live-Migration.

Mit Windows Server 2025 können GPUs auf einem Host mehreren VMs zugewiesen werden. Das erfolgt über die Partitionierung. Sinnvolles Einsatzgebiet ist das Verwenden von KI-Anwendungen in den VMs. Die Aufteilung der physischen GPUs funktioniert mit Windows Server 2025 darüber hinaus auch in Clustern, zusammen mit der Live-Migration. Damit die neue Technologie funktioniert, müssen GPU und CPU hiermit kompatibel sein. Hier sind also moderne Prozessoren notwendig. Als Betriebssystem muss in den VMs Windows 10/11 oder Windows Server 2022/2025 zum Einsatz kommen oder ausgewählte Linux-Distributionen, wie zum Beispiel Ubuntu.

Neben der Aufteilung von GPUs auf verschiedene VMs kann Windows Server 2025 mehrere GPUs zu einem Pool zusammenfassen. Auch das ist für die Bereitstellung von KI-Anwendungen sinnvoll. Pools lassen sich auf Cluster- und Host-Ebene erstellen und sind auch für den Bereich des Failovers wichtig.

Generation 2-VMs werden in Windows Server 2025 zum Standard

Erstellen Admins im Hyper-V-Manager, dem Windows Admin Center oder der PowerShell eine neue VM, dann wird diese ab Windows Server 2025 standardmäßig als Generation-2-VM erstellt. Hier wird die Hardware paravirtualisiert, was die Leistung moderner Betriebssysteme deutlich verbessert. Dazu kommt die Unterstützung für UEFI, Secure Boot und die Einbindung von virtuellen TPMs. Damit kommen aber nur Windows und aktuelle Linux-Distributionen zurecht.

Windows Server 2025 soll mit NVMe fast doppelt so schnell werden

Setzen Unternehmen in Windows Server 2025 auf NVMe zum Speichern von VMs, können sich Schreib- und Leseleistung teilweise fast verdoppeln, verspricht Microsoft. Davon profitieren natürlich vor allem große Dateien, zum Beispiel virtuelle Festplatten von VMs. Zusammen mit den verbesserten Dedup-Funktionen, die den benötigten Speicherplatz nach der Angabe von Microsoft fast halbieren können, bietet hier Windows Server 2025 einiges an Potenzial für große Workloads.

Der Bereich »Storage Spaces Direct« (S2D) wurde umfassend weiterentwickelt, um hyperkonvergente Infrastrukturen effizienter zu unterstützen. Unternehmen können Storage-Konfigurationen auf Basis von NVMe nutzen, wodurch eine signifikante Leistungssteigerung erreicht wird. NVMe over Fabrics wurde ergänzt, um das Speichernetzwerk zu entlasten. Ebenso wurde die Verwaltung und Bereitstellung von Speicher optimiert, beispielsweise durch Funktionen wie Thin Provisioning und eine verbesserte Datendeduplizierung, die nun zu 60 % bis 80 % Speicherplatz einspart.

1.1.3 Verbesserungen und Neuerungen in Active Directory

Mit Windows Server 2025 gibt es erstmals seit Windows Server 2016 wieder wesentliche Änderungen und Neuerungen im Active Directory. So gibt es einen neuen Betriebsmodus für Gesamtstruktur und Domäne, der speziell für Windows Server 2025 und die darin enthaltenen Neuerungen reserviert ist. Active Directory bleibt aber weiter lokal und es findet keine Zusammenführung mit Azure AD/Entra ID statt. Das Active Directory in Windows Server 2025 ist weiterhin vollständig verfügbar, wird aber von Microsoft an die aktuellen Herausforderungen angepasst, zum Beispiel durch die Vergrößerung der Datenbankseiten.

Obwohl es einen neuen Betriebsmodus für Windows Server 2025 gibt, ist dieser nicht zwingend erforderlich. Sie können weiterhin den Windows Server 2016-Betriebsmodus für Domänencontroller in Windows Server 2025 verwenden. In diesem Fall können Sie die neue Serverversion als Domänencontroller in bestehende AD-Strukturen ab Windows Server 2016 integrieren.

Wenn Sie jedoch den Betriebsmodus auf Windows Server 2025 umstellen, können in dieser Active Directory-Umgebung nur Domänencontroller mit Windows Server 2025 verwendet werden. Bei den Mitgliedsservern können Sie aber wie in den Vorgängerversionen weiterhin ältere Windows-Versionen sowie Linux und andere Geräte einbinden. Diese funktionieren mit Windows Server 2025 genauso wie mit seinen Vorgängern.

Neue Versionen von Funktionsebenen und Schema

Im Rahmen der Einrichtung von Active Directory mit Windows Server 2025 muss die Funktionsebene mindestens auf Windows Server 2016 gesetzt sein, ältere Versionen sind nicht mehr verfügbar. Die interne Versionsnummer für die neue Funktionsebene beträgt 10. In Windows Server 2016 war die Version noch 7. Die Versionen 8 und 9 waren für Windows Server 2019 und Windows Server 2022 vorgesehen. Diese beiden Funktionsebenen gab es mangels Neuerungen aber nie. Zwar hat Microsoft das Schema von Active Directory immer mal wieder aktualisiert, aber keine neuen Funktionen integriert. In Version 10 hat Microsoft die Replikation zwischen Domänencontrollern mit Windows Server 2025 verbessert und ermöglicht flexiblere Einstellungen.

Das Active Directory-Schema hat in Windows Server 2025 die neue Version 90. Diese können Sie in der PowerShell mit dem Befehl `Get-ADObject (Get-ADRootDSE).schemaNamingContext -property objectversion` anzeigen. Windows Server 2019 und 2022 verwenden noch die Schema-Version 88 und Windows Server 2016 Version 87.

```
PS C:\Users\Administrator> Get-ADObject (Get-ADRootDSE).schemaNamingContext -property objectversion

DistinguishedName : CN=Schema,CN=Configuration,DC=vnext,DC=lab
Name              : Schema
ObjectClass       : dMD
ObjectGUID        : 5e981e4c-83a1-42d9-8ca3-ce9e3439c993
objectversion     : 90
```

Abb. 1.1 Das Active Directory-Schema bekommt in Windows Server 2025 eine neue Version.

Die Neuerungen von Active Directory verstehen

Die Neuerungen in Active Directory betreffen vor allem die Active Directory-Datenbank, die neuen Funktionsebenen für die Gesamtstruktur und die Domäne sowie mehr Sicherheitsfunktionen, die Benutzer und Geräte vor Angriffen schützen sollen. Gleichzeitig bleibt die neue Version mit früheren Serverversionen kompatibel. Sie können Windows Server 2025 also in bestehende Netzwerke integrieren und die neuen AD-Funktionen nutzen, indem Sie alle Domänencontroller auf die neue Version aktualisieren.

Die Mitgliedsserver können weiterhin mit Windows Server 2019/2022 oder auch mit Windows Server 2016 und anderen Betriebssystemen installiert werden. Die letzten Neuerungen für Active Directory gab es mit Windows Server 2016. In Windows Server 2019 und Windows Server 2022 gab es keine größeren Neuerungen, die eine neue Funktionsstufe rechtfertigen würden.

Bessere AD-Datenbank, neue Funktionsschicht, mehr Sicherheit im AD

Windows Server 2025 kommt mit einer neuen Funktionsebene für die Gesamtstruktur und die Domäne. Diese kann während der Installation und Einrichtung oder nach der Installation ausgewählt werden, sobald keine älteren Domänencontroller vor Windows Server 2025

mehr in der Umgebung vorhanden sind. In einer Testumgebung ist es in der Regel sinnvoll, gleich die neue Version zu verwenden, da so alle neuen Funktionen im Active Directory von Windows Server 2025 genutzt werden können.

Datenbankseiten können in Active Directory mit Windows Server 2025 nun eine Größe von 32KB erreichen und verwenden 64-Bit-Long-Value-IDs (LIDs). Bisher waren die Seiten nur maximal 8KB groß. Dies ermöglicht eine flexiblere Skalierbarkeit, es können mehr Daten gespeichert werden, Gruppen können mehr Mitglieder enthalten und es gibt weitere Vorteile, die große Datenbankseiten bieten. Beim direkten Upgrade von Windows Server 2019/2022 auf Windows Server 2025 bleibt die Größe der Datenbankseiten bei 8KB. Hier muss manuell nachkonfiguriert werden. Ein neuer Domänencontroller wird mit einer 32k-Seiten-Datenbank installiert, verwendet 64-Bit-Long-Value-IDs und läuft aus Kompatibilitätsgründen mit früheren Versionen im 8k-Seiten-Modus. Wenn ein Domänencontroller direkt auf Windows Server 2025 aktualisiert wird, verwendet er weiterhin sein aktuelles Datenbankformat und 8k-Seiten. Die Umstellung auf 32k-Datenbankseiten erfolgt auf Basis der Gesamtstruktur und erfordert, dass alle Domänencontroller in der Struktur über eine 32k-Seiten-fähige Datenbank verfügen. Um die 32k-Datenbankseiten zu aktivieren, müssen Sie die Forest-Funktionsstufe auf die neue Stufe für Windows Server 2025 anheben. Die 32k-Datenbankseitengröße ist auch ein optionales Feature für AD LDS. Active Directory ist immer noch eine ESE-Datenbank, wie in früheren Versionen.

Verbessertes NUMA und Monitoring in Windows Server 2025

Eine weitere Neuerung ist die verbesserte Unterstützung von Non-Uniform Memory Access (NUMA) in Windows Server 2025. Hier können Domänencontroller künftig alle NUMA-Gruppen nutzen. Diese Verbesserung hat Windows Server 2022 inzwischen auch per Update erhalten, in Windows Server 2025 ist sie von Haus aus integriert. NUMA spielt eine Schlüsselrolle in der Serverarchitektur. NUMA teilt den Speicher in verschiedene Blöcke auf, wobei jeder Prozessor direkten Zugriff auf einen ihm zugewiesenen Speicherblock hat. Diese Konfiguration verbessert die Leistung, da die Prozessoren schneller auf den Speicher zugreifen können, der ihnen räumlich am nächsten liegt.

In Windows Server-Umgebungen, insbesondere bei der Verwendung von Active Directory, bietet NUMA verschiedene Vorteile. Active Directory, das aufgrund der Verarbeitung großer Datenmengen für seinen hohen Speicherbedarf bekannt ist, profitiert von der geringeren Speicherlatenz, die NUMA bietet. Dies führt zu schnelleren Antwortzeiten und einer effizienteren Datenverarbeitung. Insbesondere bei der Nutzung der neuen, vergrößerten Datenbankseiten ergeben sich vor allem in großen Umgebungen einige Leistungsverbesserungen.

Mit NUMA kann die Serverleistung effizient skaliert werden. Dies ist besonders wichtig für Active Directory-Umgebungen, die mit dem Wachstum des Unternehmens mitwachsen. NUMA ermöglicht eine effizientere Nutzung der Server-Ressourcen. Durch schnellere Speicherzugriffe können NUMA-basierte Windows-Server mehr Aufgaben gleichzeitig ausführen, was für Active Directory-Umgebungen mit hohem Durchsatz unerlässlich ist. Durch die Implementierung von NUMA in Windows Server-Umgebungen mit Active Directory können somit signifikante Leistungsvorteile erzielt werden, die zur Steigerung der Effizienz und Skalierbarkeit beitragen.

NUMA-Gruppen, eine Kernkomponente der Non-Uniform Memory Access Architecture, strukturieren den physischen Speicher eines Computers in separate Segmente. Jedes Segment, auch NUMA-Knoten genannt, ist einem bestimmten Prozessor oder einer Gruppe

von Prozessoren zugeordnet. Diese Zuordnung ermöglicht es jedem Prozessor, effizienter auf seinen eigenen lokalen Speicher zuzugreifen als auf den entfernten Speicher anderer Knoten.

In der Praxis führt dies zu einer Optimierung des Speicherzugriffs. Wenn ein Prozessor auf Daten im lokalen Speicher zugreift, ist die Latenz geringer als beim Zugriff auf Speicher, der einem anderen NUMA-Knoten zugeordnet ist. Diese Speicherverteilung trägt erheblich zur Gesamtleistung des Systems bei, insbesondere in Umgebungen mit hohem Speicherbedarf und mehreren Prozessoren.

Betriebssysteme und Anwendungen, die für NUMA optimiert sind, können diese Architektur nutzen, indem sie Prozesse und Speicheranforderungen intelligent auf die verschiedenen NUMA-Knoten verteilen. Dies erhöht die Systemeffizienz und -leistung, da Verzögerungen durch entfernte Speicherzugriffe minimiert werden. Dies ist insbesondere in Serverumgebungen wie Windows Server relevant, da hier häufig Anwendungen mit hohen Leistungsanforderungen laufen, die von den verbesserten Speicherzugriffszeiten profitieren.

Für die Überwachung von Domänencontrollern stehen in diesem Zusammenhang neue Leistungsindikatoren wie »Local Security Authority (LSA) Lookups«, »DC Locator« und »LDAP Client« zur Verfügung. Dies ermöglicht eine bessere Überwachung von AD-Umgebungen, insbesondere wenn diese ausgelastet sind und an ihre Leistungsgrenzen stoßen. AD unterstützt daher in Windows Server 2025 mehrere Kerne mit mehreren CPUs. Insgesamt können bis zu 64 Cores mit AD in Windows Server 2025 verwendet werden.

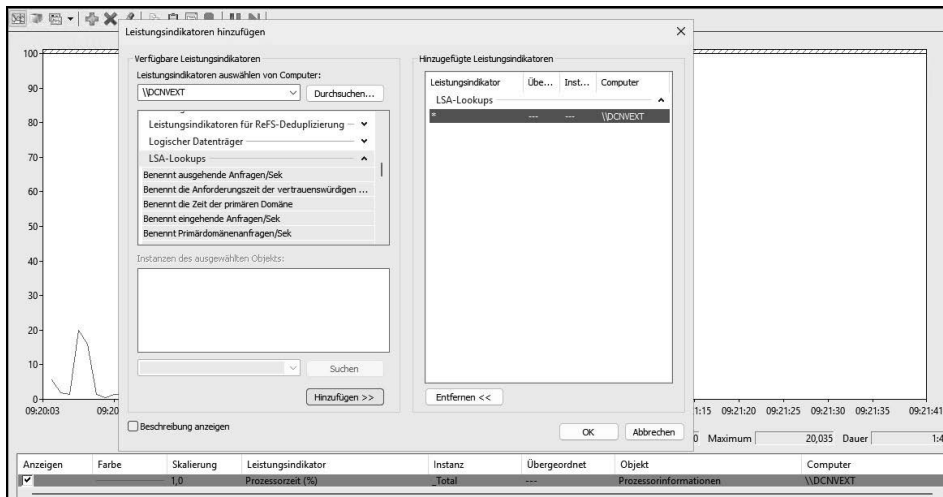


Abb. 1.2 Active Directory kann in Windows Server 2025 mit neuen Leistungsindikatoren überwacht werden.

Mehr Sicherheit im Active Directory mit Windows Server 2025

Microsoft verbessert die Kommunikation zwischen Domänencontrollern und gestaltet diese sicherer. LDAP verwendet jetzt TLS 1.3 mit LDAP over TLS. Außerdem wird LDAP-Sealing verwendet, was die Sicherheit von AD-Sitzungen erhöht. LDAP-Sealing verschlüsselt LDAP Payload-Daten für die Übertragung sensibler Daten. Darüber hinaus erfolgt die Änderung von Passwörtern mit SAM-RPC unter Verwendung von AES. Es ist auch möglich, die Remote-Änderung von Passwörtern für bestimmte Konten zu verbieten. Diese

müssen dazu Mitglied der Gruppe *Protected Users* sein. Dies können Sie in den Gruppenrichtlinien bei *Administrative Vorlagen/System/Sicherheitskontenverwaltung* konfigurieren. Kerberos unterstützt in Windows Server 2025 AES SHA256/384, was zeigt, dass sich Microsoft viele Gedanken gemacht hat, das Active Directory zu modernisieren, ohne die Administration unnötig kompliziert zu machen.

1.2 Windows Server 2025 lizenzieren

Eines ändert sich auch mit Windows Server 2025 nicht: die Komplexität der Lizenzierung. Es gibt zahlreiche Verträge und viele Möglichkeiten, Windows 10/11 und Windows Server 2025 zu lizenzieren. Verantwortliche im Unternehmen sollten sich darüber informieren, welche Lizenzverträge und Möglichkeiten es gibt.

Generell ist davon auszugehen, dass der Einsatz von Windows Server 2025 teurer wird. Das liegt vor allem an der Prozessor-Kern-Lizenzierung. Der CAL-Zugriff der Anwender bleibt in Windows Server 2025 generell gleich zu den Vorgängern. Die unterschiedlichen Windows-Editionen bieten für Unternehmen verschiedene Möglichkeiten und Auswahlkriterien.

1.2.1 Editionen und Lizenzen im Vergleich

Microsoft hat mit Windows Server 2025 Unterschiede in den Storage-Funktionen integriert. So unterstützt nur die Datacenter-Edition alle Funktionen. In der Standard-Edition gibt es weder Storage Spaces Direct noch Storage Replica. Die Lizenzierung erfolgt auf Basis der CPU-Kerne. In Hyper-V werden die logischen Prozessoren lizenziert, da diese das Pendant zu den physischen Prozessorkernen darstellen.

Beide Editionen decken immer nur zwei Prozessorkerne des Hosts oder zwei logische CPUs ab. Die erforderliche Mindestanzahl von Betriebssystemlizenzen für jeden Server wird durch die Anzahl der physischen Prozessorkerne des Hosts sowie die Anzahl an virtuellen Servern bestimmt, die Sie auf dem Hyper-V-Host installieren. Setzen Unternehmen also Server mit mehreren Prozessoren ein, ist pro Kern-Paar eine Lizenz notwendig, egal welche Edition im Einsatz ist.

Sie müssen für jeden Server mindestens vier Lizenzen erwerben, also für acht Kerne. Setzen Sie einen Dual-Prozessor mit je acht Kernen ein, müssen Sie also acht Lizenzen für diese 16 Kerne erwerben. Für jeden Kern mehr müssen Sie ein Core-Pack kaufen, damit alle Kerne lizenziert sind. In Windows Server 2025 Standard dürfen Sie pro Lizenz zwei VMs installieren, Windows Server 2025 Datacenter kennt kein Limit. Hier müssen Sie lediglich alle Prozessorkerne des Servers lizenzieren.

1.2.2 Clientzugriffslizenzen beachten

Für die Editionen Standard und Datacenter benötigen Sie weiterhin Clientzugriffslizenzen (CALs). Auch in Windows Server 2025 können Sie diese benutzerbasiert oder pro Gerät erwerben, dürfen sie aber nicht aufsplitten. Clientzugriffslizenzen (CALs) und Remotedesktop-Clientzugriffslizenzen (RDCALs) sowie Lizenzen für die Active Directory-Rechteverwaltung (ADRMS) sind auch in Windows Server 2025 weiterhin notwendig, aber nur in

den Editionen Standard und Datacenter. Hier gibt es gleichfalls Gerätelizenzen oder Benutzerlizenzen für den Zugriff. Sie müssen bereits bei der Bestellung Ihrer Lizenzen im Voraus planen, welchen Lizenztyp Sie einsetzen wollen.

Sie können die verschiedenen Lizenzen miteinander mischen. Es ist jedoch nicht erlaubt, die einzeln erhältlichen Lizenzpakete in Geräte- und Benutzerlizenzen aufzusplitten. Sie dürfen also ein 5er-Paket Gerätelizenzen und ein 5er-Paket Benutzerlizenzen für einen Server kaufen und lizenzieren. Es ist aber nicht erlaubt, diese Pakete aufzusplitten und zum Beispiel als 2er-Gerätelizenz und 8er-Benutzerlizenz zu verwenden. Genauso ist nicht zulässig, mit CALs von Vorgängerversionen auf Server mit Windows Server 2025 zuzugreifen.

1.2.3 Geräte-CALs und Benutzer-CALs

Wenn Sie mit Geräte-CALs lizenzieren, müssen Sie für jeden PC, der auf diesen Server zugreift, eine Lizenz kaufen, unabhängig davon, wie viele Benutzer an diesem PC arbeiten. Wenn Sie PCs betreiben, zum Beispiel im Schichtbetrieb, an denen zu unterschiedlichen Zeiten unterschiedliche Benutzer arbeiten, benötigen Sie für diese PCs nur jeweils eine Geräte-CAL. Im umgekehrten Fall, wenn also ein Benutzer mit mehreren PCs, Notebooks oder Smartphones auf den Server zugreift, benötigen Sie für diesen Benutzer mehrere Geräte-CALs, da dieser Benutzer mit mehreren PCs auf den Server zugreift. Alternativ können Sie auch eine Benutzer-CAL kaufen.

CALs sind bei Microsoft an die Version gebunden. Sie dürfen daher CALs für Windows Server 2019/2022 nicht für Windows Server 2025 nutzen. Allerdings ist es erlaubt, mit CALs für Windows Server 2025 auf Server mit Windows Server 2019/2022 zuzugreifen. Sie sollten daher möglichst immer die aktuellen CALs verwenden.

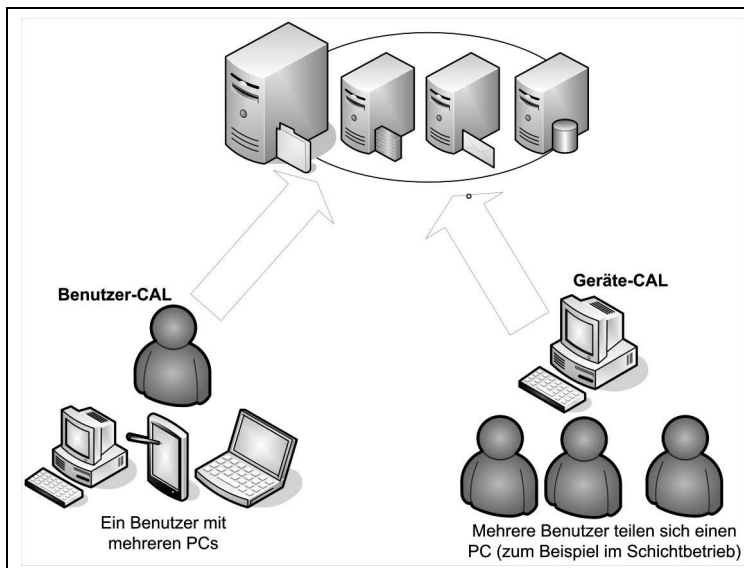


Abb. 1.3 Benutzer-CALs und Geräte-CALs verstehen

Jeder Benutzer mit einer Benutzer-CAL kann an beliebig vielen PCs eine Verbindung mit einem Server aufbauen. Die CALs müssen eindeutig zugewiesen sein. Sie können daher nicht nur so viele CALs kaufen, wie gleichzeitig Benutzer arbeiten, sondern müssen die Gesamtzahl Ihrer Arbeitsstationen, Smartphones und sonstiger Geräte lizenzieren, wenn Sie Geräte-Lizenzen kaufen.

Bei Benutzer-Lizenzen müssen diese genau der Anzahl der Benutzer zugewiesen werden, die insgesamt mit dem Server arbeiten. Es ist nicht erlaubt, auf einem Server Lizenzen von Standard und Datacenter zu mischen. Sie dürfen eine Lizenz auch nicht auf mehrere Server aufsplitten.

In Ihrem Unternehmen sind beispielsweise 100 Mitarbeiter beschäftigt, von denen jedoch lediglich 63 mit PCs am Server arbeiten. Wenn Sie Geräte-CALs kaufen, wird jede gekaufte Lizenz einem bestimmten PC zugeordnet. Mit diesen PCs können sich jetzt beliebig viele Mitarbeiter mit Servern verbinden, wenn sich diese zum Beispiel PCs im Schichtbetrieb teilen. Wenn neue PCs hinzukommen, müssen Sie für diese weitere Gerätelizenzen kaufen.

Im nächsten Beispiel gehen wir von einer IT-Firma aus, in der 40 Mitarbeiter beschäftigt sind. Von diesen 40 Mitarbeitern arbeiten 25 mit der Windows-Domäne. Jeder dieser Mitarbeiter hat einen PC und ein Notebook, mit denen er am Server arbeitet. Obwohl in diesem Unternehmen nur 40 Mitarbeiter beschäftigt sind, verbinden sich 50 PCs mit dem Server. Es müssen in diesem Beispiel daher 50 Gerätelizenzen erworben werden. Wenn das Unternehmen seine Lizenzen jedoch als Benutzerlizenz erwirbt, werden lediglich 25 Lizenzen benötigt, da nur 25 Benutzer mit dem Server arbeiten.

1.2.4 Wie Unternehmen Windows und Office kostengünstig lizenzieren können

Unternehmen oder auch kleine Büros und Freiberufler können bei der Lizenzierung von Windows und Office oft einiges an Kosten sparen, indem gebrauchte Lizenzen zum Einsatz kommen. Grundsätzlich ist es für KMU in den meisten Fällen nicht notwendig, teure Serviceverträge mit Microsoft abzuschließen, auch wenn sie parallel Microsoft 365 einsetzen. Häufig reichen günstige OEM- und Retail-Lizenzen völlig aus. Es ist daher sinnvoll, sich mit dem Thema Lizenzierung in Microsoft-Umgebungen auseinanderzusetzen, um Investitionen zu sparen und teure Lizenzstreitigkeiten zu vermeiden. Allerdings lauern auch viele Fallstricke und es gibt unseriöse und illegale Angebote für günstige Microsoft-Software. In diesem Abschnitt zeigen wir, worauf Sie achten sollten, um Windows, Office und auch Windows Server günstig und legal zu lizenzieren. Microsoft informiert außerdem auf seiner Website darüber, was Unternehmen beim Kauf von Software beachten sollten (<https://www.microsoft.com/de-de/aktionen/piraterie/sicheres-einkaufen>).

PCs und Notebooks ohne Betriebssystem sind teilweise günstiger

Nicht immer ist es sinnvoll, PCs oder Notebooks mit Windows-Lizenzen zu kaufen. Gerade KMU können hier einiges an Kosten sparen, wenn sie die Geräte ohne Betriebssystem kaufen und die jeweilige Windows-Version unabhängig erwerben. Auf Portalen wie Lizensio oder UsedSoft erhalten Sie beispielsweise Windows 11 Pro für unter 20 Euro und Microsoft Office 2021/2024 Home & Student (Word, Excel, PowerPoint und Outlook) für knapp 60 Euro. Wer Microsoft Office 2021/2024 Professional Plus (Word, Excel, PowerPoint, Outlook, Publisher, Access) benötigt, findet Lizenzen bei Lizenzguru für rund 230 Euro.

Wenn Sie solche günstigen Lizenzen erwerben wollen, achten Sie darauf, dass Sie sie bei einem seriösen Händler kaufen. In den meisten Fällen erhalten Sie einen Produktschlüssel, den Sie für die Installation verwenden können. Windows 11 selbst können Sie bei Microsoft herunterladen, zum Beispiel unter <https://www.microsoft.com/de-de/software-download/Windows11>. Wichtig ist dabei aber, dass Sie eine Lizenz mit erwerben, nicht nur den Produktschlüssel. Das ist beim Kauf des Produkts eindeutig ersichtlich. Lizenzguru ist ebenfalls ein bekanntes Portal für gebrauchte Lizenzen (<https://lizenzguru.de>). Achten Sie beim Kauf darauf, dass Sie Windows 11 Pro erwerben, auch wenn Sie kein Active Directory einsetzen. Windows 11 Home ist zwar oft günstiger, aber in der Funktionalität vor allem für den professionellen Einsatz eingeschränkt. Bei Lizenzguru gibt es Windows 10 Professional für etwa 15 Euro, während Windows 11 Professional 50 Euro kostet. Sie können Ihre Windows 10 Pro-Version aber jederzeit auf Windows 11 Pro upgraden, ohne zusätzliche Lizenzen erwerben zu müssen.

Es ist auch möglich, gebrauchte (defekte) Hardware zu kaufen, wenn sich die Lizenzaufkleber darauf befinden. Denn diese Lizenzen können Sie mit anderer Hardware weiter nutzen. In diesem Fall haben Sie den Vorteil, dass Sie die Lizenz komplett erwerben, da Sie auch die entsprechende Hardware besitzen. Natürlich müssen Sie sich vergewissern, dass der Verkäufer seine Lizenz nicht weiternutzt. Kaufen Sie daher vor allem aus seriösen Quellen. Beachten Sie, dass ein Produktschlüssel keine Lizenz ist. Sie können auch einen Produktschlüssel ohne Lizenz kaufen, zum Beispiel bei Volumenlizenzen. Das ist aber nicht legal. Wenn Sie eine Lizenz besitzen, dann haben Sie auch den dazugehörigen Produktschlüssel, aber nicht umgekehrt. Wenn jemand seinen Produktschlüssel mehrfach verkauft, behält er seine Lizenz, die Käufer erhalten nur die Produktschlüssel der Lizenz. Das ist nicht legal und Sie sollten aufpassen, dass Sie nicht in diese Falle tappen. Viele unseriöse Händler vermeiden beim Verkauf den Begriff »Lizenz« und sprechen nur von »Produktschlüssel« oder »Product Key«. Solche Angebote sollten Sie nicht kaufen, sie kommen oft aus dem Ausland. Hier haben Sie kaum rechtliche Handhabe, wenn eine gekaufte Lizenz nicht legal ist. Vor allem aus Russland oder China ist mit illegalen Lizenzen zu rechnen. Hier hilft ein Blick ins Impressum des Webshops, der die Lizenzen verkauft.

Keine Volumenlizenzen kaufen

Achten Sie beim Kauf von günstigen Lizenzen darauf, dass Sie keine Volumenlizenzen erwerben, sondern einen OEM- oder besser noch einen Retail-Schlüssel. Bei Volumenlizenzen kann die Lizenz des Verkäufers jederzeit auslaufen. Solche Verträge sind für große Unternehmen und Bildungseinrichtungen gedacht. In der Regel dürfen diese Lizenzen nur von Mitarbeitern oder Nutzern des Unternehmens oder der Bildungseinrichtung verwendet werden. Wenn solche Unternehmen die Produktschlüssel weiterverkaufen, funktionieren diese zwar für eine gewisse Zeit, aber Microsoft kann sie jederzeit sperren und damit unbrauchbar machen. Der Kauf dieser Lizenzen ist illegal, auch wenn Microsoft in den letzten Jahren nicht gegen Kunden vorgegangen ist. Allerdings sperrt Microsoft regelmäßig Produktschlüssel, die negativ auffallen.

Kündigt der Verkäufer den Vertrag oder verkauft er mehr Lizenzen als vertraglich vereinbart, verfallen die zugehörigen Produktschlüssel oder Sie können Ihren Produktschlüssel nicht mehr verwenden. Sie als Käufer haben darauf keinen Einfluss, da Sie selbst den zum Produktschlüssel gehörenden Volumenlizenzvertrag nicht abgeschlossen haben, sondern nur aus einem solchen Vertrag einen Schlüssel verwenden. Volumenlizenzen gibt es für

Windows und Office, sie sind günstig, bergen aber das Risiko, dass sie von einem Tag auf den anderen nicht mehr funktionieren. Lassen Sie lieber die Finger davon, auch wenn solche Produktschlüssel durch ihren geringen Preis oft verlockend sind.

Besser ist es, OEM-Lizenzen oder Retail-Lizenzen zu erwerben. Fragen Sie daher vor dem Kauf eines Schlüssels nach, ob es sich um einen OEM- oder Volumenlizenzschlüssel handelt, beziehungsweise überzeugen Sie sich, dass es sich bei dem Angebot um eine Lizenz handelt, nicht nur um einen Produktschlüssel einer Lizenz. Das ist bei unseriösen Angeboten oft nur aus dem Kleingedruckten erkennbar. Retail-Keys sind in diesem Fall noch besser, da sie nicht an Hardware gebunden sind. Somit ist die Gefahr, dass Microsoft den Produktschlüssel sperrt, sehr gering. Wenn Sie also auf Nummer sicher gehen wollen, kaufen Sie am besten (gebrauchte) Retail-Keys. Aus diesen Gründen sind Volumenlizenzschlüssel besonders günstig und Retail-Lizenzen im Vergleich teurer, dafür aber legal und dauerhaft einsetzbar.

Lizenzart auslesen

Um welche Office-Lizenz es sich auf einem Computer handelt, können Sie nach der Installation von Microsoft Office 2021/2024 überprüfen, indem Sie in das Installationsverzeichnis von Microsoft Office wechseln. Standardmäßig ist dies `C:\Programme (x86)\Microsoft Office\Office16`. Hier können Sie mit folgendem Befehl überprüfen, ob es sich um eine Volumenlizenz, eine OEM-Lizenz oder eine herkömmliche Einzelhandelslizenz handelt:

```
cscript ospp.vbs /dstatus
```

Den Lizenztyp von Windows können Sie auch über die Befehlszeile überprüfen. Dazu verwenden Sie den Befehl `slmgr -dli`. Erscheint hier die Meldung, dass Sie keine Retail- oder OEM-Lizenz verwenden, sondern einen Volumenschlüssel, sollten Sie aktiv werden. Bei Volumenlizenzen innerhalb der eigenen Firma spielt dies keine Rolle, wenn Sie aber einen Multiple Activation Key (MAK) erworben haben, gehört diese Lizenz der Firma mit dem Volumenlizenzvertrag. Läuft dieser aus, wird auch Ihr MAK ungültig. Das kann auch passieren, wenn Microsoft diesen sperrt. Außerdem stellt sich bei diesen Keys die Frage nach der Rechtmäßigkeit und damit nach der Beziehung Ihres Unternehmens zu diesem Volumenlizenzinhaber. Wenn Sie keine Volumenlizenz abgeschlossen haben, sollten Sie die Gültigkeit der Lizenz überprüfen und gegebenenfalls auf eine OEM- oder Retail-Lizenz umsteigen. Die Kosten halten sich in Grenzen, aber Sie vermeiden potenziellen und teuren Lizenzärger und Probleme mit Windows oder Office, wenn Microsoft den Produktschlüssel sperrt.

Gebrauchte OEM-Lizenzen können bares Geld sparen

OEM-Lizenzen sind zwar direkt an die Hardware gebunden, dürfen aber in Deutschland separat verkauft werden. Der Bundesgerichtshof hat in einem Urteil (BGH, 06.07.2000 - I ZR 244/97) die Entkopplung von der Hardware für rechtmäßig erklärt. Sie können also ohne Bedenken gebrauchte OEM-Lizenzen kaufen und verwenden, jedoch keine Volumenlizenzen. Allerdings müssen Sie darauf achten, dass Sie zwar legal OEM-Lizenzen kaufen und verwenden können, Microsoft aber mit dieser Vorgehensweise nicht einverstanden ist, da sie gegen die eigenen Lizenzbedingungen verstößt. Es ist daher möglich, dass Microsoft einzelne Produktschlüssel sperrt, sodass die Aktivierung nicht funktioniert oder Windows und Office die Aktivierung verlieren. Es kann daher nicht schaden, eine oder zwei Ersatzli-

enzen zu haben, um für diesen Fall gewappnet zu sein, oder besser gleich auf Retail-Lizenzen zu setzen. Als Alternative ist der bereits beschriebene Weg denkbar, gebrauchte oder defekte Hardware zu kaufen, bei der die Lizenzen für das jeweilige Produkt dabei sind.

Durch den Kauf von gebrauchten Lizenzen können Sie günstig an Lizenzen von Software kommen, die der ursprüngliche Besitzer nicht mehr benötigt. Zugriffslizenzen (CALs) können mit beliebigen Lizenzen kombiniert werden. Wenn Sie also in Ihrem Unternehmen bereits CALs erworben haben, können Sie diese auch mit OEM-Lizenzen – auch gebrauchten – kombinieren. Es ist außerdem erlaubt, einen Produktschlüssel und ein Installationsmedium zu verwenden, das für einen anderen Computer verwendet wird. Der Produktschlüssel und das Installationsmedium stellen nicht die Lizenz dar. Sie müssen jedoch darauf achten, dass Sie über eine Lizenz verfügen, wenn Sie einen Produktschlüssel und ein Lizenzmedium für ein Produkt verwenden. Mit welchem Produktschlüssel und Medium Sie die Installation durchführen, spielt keine Rolle. Wichtig ist die Lizenz.

Lizenzierung von Windows-Servern mit OEM-Lizenzen

Die Lizenzierung von Windows-Servern kann wie bei Windows 10/11 und Office über OEM-Lizenzen erfolgen. Sie können hier ebenfalls auf gebrauchte Lizenzen zurückgreifen. Beachten Sie aber, dass Sie mindestens Lizenzen für 16 CPU-Kerne benötigen, auch wenn der Server weniger Kerne hat. Hat der Server mehr CPU-Kerne, benötigen Sie natürlich auch für diese eine Lizenz. Das können problemlos OEM-Lizenzen sein. Hier gibt es verschiedene Varianten, Direct OEM (DOEM), Reseller Option Kit (ROK) und Channel OEM for System Builder (COEM). Grundsätzlich haben alle diese Lizenzen den gleichen Funktionsumfang, es gibt keine eingeschränkten OEM-Lizenzen. Wenn Sie eine OEM-Lizenz erwerben, können Sie innerhalb von 90 Tagen einen Software-Assurance-Vertrag mit Microsoft abschließen. OEM-Lizenzen ermöglichen also durchaus moderne Support-Szenarien. Allerdings lohnt sich das vermutlich eher nicht. Darüber hinaus haben OEM-Lizenzen auch ein umfassendes Downgrade-Recht. Wenn Sie eine OEM-Lizenz von Windows Server 2025 erwerben, können Sie damit auch Windows Server 2019/2022 installieren.

DOEM wird häufig für PCs verwendet, auf denen Windows 11 bereits vorinstalliert ist. Sie können also DOEM-Lizenzen erwerben, sollten sich aber vergewissern, dass diese Lizenz nicht bereits verwendet wird. ROK ist eine flexible Art, Windows Server zu lizenzieren. Hier kann sich ein Preisvergleich lohnen. Wenn Sie selbst Server zusammenstellen, können Sie COEMS verwenden. Sie müssen aber darauf achten, was die Lizenz abdeckt, insbesondere die Anzahl der Cores. Wenn Sie kein Installationsmedium haben, können Sie bei Microsoft ein Downgrade-Kit kaufen. Es ist auch ausdrücklich erlaubt, die Installationsmedien eines Servers für einen anderen Server zu verwenden. Wichtig ist, dass Sie die richtige Edition verwenden, also Windows Server 2025 Standard oder Datacenter.

BIOS-Lock OEM-Medien beachten

Die von Ihnen erworbene Lizenz hat in der Regel nichts mit dem von Ihnen verwendeten Installationsmedium zu tun. Wenn Sie ein anderes Installationsmedium der gleichen Edition vorliegen haben, können Sie es verwenden. Die Lizenz ist weder an den Produktschlüssel noch an das Installationsmedium gebunden. Es gibt jedoch auch Installationsmedien, die an ein bestimmtes BIOS gebunden sind. Das bedeutet, dass Sie die Lizenz nicht mit diesem Medium verwenden können. Das macht aber nichts, Sie können einfach ein anderes Medium verwenden. Microsoft selbst hat keine BIOS-Lock-Klausel in seinen Lizenzverträgen. Sie dürfen jedoch den BIOS-Lock des Datenträgers nicht entfernen, sondern müssen einen anderen Datenträger verwenden.

OEM-Lizenzen in Volumenlizenzen umwandeln

Wenn Sie OEM-Lizenzen erworben haben, können Sie diese in eigene Volumenlizenzen umwandeln, wenn sich das preislich für Sie lohnt. Hier kann es sinnvoll sein, ein Angebot einzuholen. Sie können bei Microsoft eine Software Assurance abschließen und erhalten dadurch verschiedene Vorteile wie Zugriff auf das Volume Licensing Service Center (VLSC) und die Möglichkeit, Windows und Office mit Multiple Activation Keys (MAK) zu aktivieren. Außerdem können Sie immer die aktuelle Version des jeweiligen Produkts verwenden. Dies vereinfacht auch die Aktivierung. In den meisten Fällen ist Software Assurance für KMU jedoch nicht sinnvoll. Gebrauchte Lizenzen sind in den meisten Fällen günstiger.

Microsoft bietet auf seiner Website ein Portal an, auf dem die jeweiligen Lizenzbestimmungen der einzelnen Produkte abgerufen werden können (<https://www.microsoft.com/de-de/useterms>). Darüber hinaus ist auch die Lizenzierungsseite (<https://www.microsoft.com/de-de/licensing>) von Microsoft eine wichtige Informationsquelle zu den einzelnen Produkten und den Lizenzbestimmungen, die Sie einhalten müssen.

Um die genauen Bedingungen für OEM-Lizenzen zu berücksichtigen, wählen Sie unter *Wie wird die Software erworben?* die Option *Vom Computerhersteller auf dem Computer vorinstalliert?*. Diese Auswahl beschreibt die OEM-Lizenzen. Bei *Version* wählen Sie das Produkt aus, zum Beispiel *Windows Server 2022 Datacenter und Standard*. Bei *Sprache* ist die Auswahl *Deutsch* wichtig. Nach der Auswahl werden die Lizenzbedingungen angezeigt.

1.2.5 CALs und Editionen beachten: Datacenter und Standard

CALs gibt es übrigens sehr häufig recht günstig über OEM-Kanäle. Bei der Lizenzierung von Hyper-V-Hosts sind keine CALs für den Virtualisierungs-Host notwendig, wenn die Clients auf die VMs zugreifen. Für den Zugriff auf VMs sind CALs natürlich notwendig. Betreiben Unternehmen aber neben Hyper-V weitere Serverdienste auf einem Server, sind wiederum CALs notwendig. Admins und Consultants, die ein System verwalten, benötigen für das System keine CAL. Arbeiten Admins aber mit Serverdiensten auf einem Server, dann sind CALs dafür notwendig.

Wenn Nutzer mit einer Middleware arbeiten oder mit einem System, das wiederum im Hintergrund mit einem Windows-Server kommuniziert, zum Beispiel mit Multiplexing oder Pooling, dann braucht jeder dieser Benutzer eine CAL, auch wenn nur die Middleware selbst mit dem Windows-Server arbeitet. Spezielle Dienste wie Remote Desktop Services (RDS) und Active Directory Rights Management Services (AD RMS) brauchen ebenfalls CALs. Diese ersetzen die herkömmlichen CALs allerdings nicht, sondern sind immer zusätzlich. Auch bei RD-CALs und AD RMS-CALs gibt es ein Downgrade-Recht.

Bei der Lizenzierung von Windows Server 2025 Standard/Datacenter spielen die CPU-Kerne der Hardware eine wichtige Rolle. Dabei müssen mindestens 16 CPU-Kerne pro Server und mindestens 8 Kerne pro Prozessor lizenziert werden. Hat ein Prozessor weniger Kerne, müssen dennoch 8 Kerne lizenziert werden. Hat eine CPU mehr Kerne, dann sind auch mehr Lizenzen notwendig. Einfach ausgedrückt: Auf einem Server müssen alle Prozessoren und Kerne lizenziert werden, aber mindestens 16 CPU-Kerne. Bei dieser Art der Lizenzierung zählen die physischen CPU-Kerne, Hyperthreading spielt in diesem Fall keine Rolle.

Wenn es aber möglich ist, auf einem Server Prozessoren oder Kerne zu deaktivieren, sind für die deaktivierten Kerne keine Lizenzen notwendig. Das bringt jedoch nur bei Servern etwas, bei denen mehr als 16 CPU-Kerne vorhanden sind, da 16 Kerne ohnehin immer li-

zenziert werden müssen. Diese Lizenzvorschriften kommen vor allem bei OEM-Lizenzen zum Einsatz. Es ist sinnvoll, in diesem Szenario die Deaktivierung der Kerne durch den OEM-Lieferanten durchführen zu lassen und das auch zu dokumentieren.

Bei Windows Server 2025 Standard dürfen zwei VMs auf einem Server betrieben werden. Um mehr virtuelle Server zu betreiben, sind mehr Lizenzen für Windows Server 2025 Standard notwendig. Die Lizenzen lassen sich dadurch stapeln. Auf dem Server dürfen sich keinerlei andere Workloads befinden. Betreiben Unternehmen aus irgendwelchen Gründen auf einem Hyper-V-Server noch Active Directory oder einen anderen Workload, geht dadurch das Recht des Betriebs einer VM verloren. Auch hier gilt, dass alle CPU-Kerne lizenziert werden müssen, mindestens aber 16.

Wenn die Software auf einem Server nicht mehr benötigt wird, dürfen die Lizenzen an einem anderen Server genutzt werden. Interessant ist das bei Hyper-V-Replika. Fällt der Quell-Server aus, lassen sich die Lizenzen des Quell-Servers mitsamt der VMs auf den Replikat-Server übertragen und hier nutzen. Allerdings müssen solche Vorgänge richtig dokumentiert werden.

In diesem Fall darf der Quell-Server nicht mehr laufen und der neue Server muss natürlich korrekt lizenziert sein. 90 Tage nach dem Erwerb von OEM-Lizenzen lassen sich diese als Software Assurance mitnutzen.

Um Windows-Server-Lizenzen in hybriden Umgebungen zu nutzen, kommt Azure Stack HCI zum Einsatz. Die Abrechnung erfolgt über Azure, es lassen sich aber auch eigene Lizenzen für VMs nutzen, die auf einem lokalen Azure Stack HCI-Server laufen. Die Preise für Azure Stack HCI stehen auf der Microsoft-Seite zur Verfügung (<https://azure.microsoft.com/de-de/pricing/details/azure-stack/hci>). Bei Azure Stack HCI sind Extended Security Updates (ESU) standardmäßig mit dabei. Läuft der Support für ein Produkt ab, erhält es auf Azure Stack HCI weitere Updates.

1.2.6 Windows 11 und Windows Server 2025

Windows Server 2025 lässt sich mit Windows 10 und Windows 11 betreiben. Windows 11 ist für Windows Server 2025 optimiert und wird auch in Zukunft das bevorzugte Client-Betriebssystem für Windows Server 2025 sein. Es ist aber problemlos möglich, im Netzwerk Windows 10 mit Windows Server 2025 zu betreiben oder eine gemischte Umgebung mit Windows 10, Windows Server 2019/2022 und Windows 11 mit Windows Server 2025. Die Oberfläche von Windows Server 2025 orientiert sich an der von Windows 11.

1.2.7 Windows Server 2025 versus Azure Stack HCI

Windows Server 2025 und Azure Stack HCI bieten umfassende Plattformen zur Virtualisierung und Verwaltung moderner IT-Infrastrukturen, unterscheiden sich jedoch deutlich in der Zielsetzung und Funktionalität. Beide Systeme setzen auf Hyper-V, Storage Spaces Direct und Software Defined Networking (SDN), die durch die Verwaltung über Tools wie das Windows Admin Center (WAC) und, bei Azure Stack HCI, das Azure-Portal unterstützt werden. Der Windows Server 2025 eignet sich dabei besonders für klassische On-Premises-Infrastrukturen ohne zwingenden Cloud-Bezug, während Azure Stack HCI stark auf hybride und cloudnahe Funktionen ausgelegt ist.

Zielgruppen und Einsatzszenarien

Windows Server 2025 richtet sich primär an Unternehmen, die eine lokale Infrastruktur betreiben und Workloads isoliert ohne Cloud-Integration verwalten möchten. Im Gegensatz dazu fokussiert Azure Stack HCI auf hybride Szenarien, die eng mit Azure-Diensten verknüpft werden. Ein zentrales Unterscheidungsmerkmal liegt in den Vorteilen durch die Azure-Anbindung. Azure Stack HCI bietet durch die Einbindung in das Azure-Portal beispielsweise die Möglichkeit, Azure Virtual Desktop (AVD) und das Azure Update Management nahtlos zu integrieren. Während Windows Server 2025 die bewährten RDS-Lizenzen für Remotedesktop-Services nutzt, bietet AVD eine moderne, zentralisierte Desktop- und Applikationsbereitstellung, die jedoch Lizenzkosten pro vCPU-Stunde verursacht.

Funktionsumfang: Storage und Hotpatching

Im Bereich Storage ermöglicht Azure Stack HCI seit der Version 23H2 Thin Provisioning für Storage Spaces Direct, eine Funktion, die bei Windows Server 2025 neu ist. Thin Provisioning erlaubt eine flexible Speicherzuweisung und unterstützt dabei, die Speicherressourcen effizienter zu nutzen. Für Sicherheit und kontinuierliche Verfügbarkeit bietet Azure Stack HCI das Hotpatching, ein Feature, das Sicherheitsupdates ohne Neustart ermöglicht. Dieses Feature ist im Windows Server 2025 ebenfalls enthalten, jedoch nur, wenn er über das Azure-Portal lizenziert wird oder über eine entsprechende Software Assurance (SA) verfügt. Bei einer Standardlizenzierung von Windows Server bleibt diese Funktion ungenutzt.

Administration und Lizenzierung

Administrativ bietet Windows Server 2025 das bekannte Ökosystem der Microsoft-Tools wie Hyper-V Manager, Failover Cluster Manager und PowerShell. Azure Stack HCI hingegen fordert eine hybride Administrationsstruktur, bei der zentrale Funktionen über das Azure-Portal ablaufen. Dies ermöglicht die Nutzung von Azure-Funktionalitäten wie das Azure Update Management und die Verwaltung über das sogenannte Azure Arc für hybride Infrastrukturen. Azure Stack HCI erfordert mindestens eine monatliche Verbindung zum Azure-Portal, während Windows Server 2025 diese Verbindung lediglich als Option für hybride Funktionen sieht. Ein weiteres Unterscheidungsmerkmal zeigt sich in der Lizenzierung: Azure Stack HCI wird in Form eines Abonnements pro Host lizenziert, das zusätzliche Azure-Dienste und -Features inkludiert. Diese Lizenzierung enthält keine Windows-Server-Lizenz, weshalb auf den virtuellen Maschinen entweder separate Windows-Lizenzen oder Linux-Distributionen eingesetzt werden müssen.

Bei Windows Server 2025 sind hingegen Client Access-Lizenzen (CALs) erforderlich, was insbesondere in größeren Umgebungen die Kosten erhöht. Azure Stack HCI hingegen benötigt für die Nutzerzugriffe in der Azure-Edition keine CALs, was die Lizenzierungskosten in einigen Umgebungen reduziert. Es ist jedoch wichtig, die Netzwerkanforderungen bei der Auswahl zu berücksichtigen: Windows Server 2025 unterstützt eine flexible Architektur, die nicht zwingend einen Domain-Controller verlangt. Bei Azure Stack HCI hingegen ist in den meisten Fällen eine Azure-AD-Integration notwendig, um die volle Funktionalität sicherzustellen.

Fazit: Flexibilität und Fokus auf hybrides Management

Die Wahl zwischen Windows Server 2025 und Azure Stack HCI hängt von den individuellen Anforderungen an die Infrastruktur ab. Unternehmen, die lokale Workloads isoliert ohne Anbindung an die Cloud betreiben wollen, finden in Windows Server 2025 eine flexible und vielseitige Lösung. Azure Stack HCI hingegen bietet sich vor allem für hybride Szenarien an, bei denen die Vorteile der Azure-Integration, wie etwa Azure Virtual Desktop, Hotpatching und das Update Management, voll zum Tragen kommen. Während Windows Server 2025 die bewährten, lokal installierten Microsoft-Tools zur Verwaltung nutzt, forciert Azure Stack HCI eine gemischte Verwaltungsstruktur über Azure und lokale Tools, was eine intensivere Einbindung in die Cloud-Welt bedeutet. In einer zunehmend hybriden IT-Landschaft erlaubt Azure Stack HCI eine engere Verzahnung von lokalen und Cloud-Workloads, bleibt jedoch für Unternehmen, die auf vollständige On-Premises-Kontrolle setzen, optional.

1.3 Zusammenfassung

In diesem Kapitel haben wir Ihnen die wichtigsten Neuerungen von Windows Server 2025 gezeigt, damit Sie einen Überblick haben, welche neuen Funktionen es gibt. Wir sind in diesem Kapitel auch auf die Editionen und die Lizenzierung eingegangen. In den weiteren Kapiteln des Buches vertiefen wir die Neuerungen und zeigen die Verwaltung von Windows Server 2025. Im nächsten Kapitel erfahren Sie, wie Sie Windows Server 2025 installieren und einrichten.

Inhaltsverzeichnis

Vorwort	27
 Teil I Grundlagen und Installation	
Kapitel 1 Neuerungen und Lizenzierung	31
1.1 Die wichtigsten Neuerungen in Windows Server 2025	32
1.1.1 Neuerungen in Windows Server 2025	32
1.1.2 Neuerungen in Hyper-V und der Virtualisierung	33
1.1.3 Verbesserungen und Neuerungen in Active Directory	34
1.2 Windows Server 2025 lizenzieren	38
1.2.1 Editionen und Lizenzen im Vergleich	38
1.2.2 Clientzugriffslizenzen beachten	38
1.2.3 Geräte-CALs und Benutzer-CALs	39
1.2.4 Wie Unternehmen Windows und Office kostengünstig lizenzieren können	40
1.2.5 CALs und Editionen beachten: Datacenter und Standard	44
1.2.6 Windows 11 und Windows Server 2025	45
1.2.7 Windows Server 2025 versus Azure Stack HCI	45
1.3 Zusammenfassung	47
 Kapitel 2 Installation und Grundeinrichtung	49
2.1 Grundlagen zur Installation	49
2.1.1 Windows Server 2025-Installation verstehen	50
2.1.2 Installation von Windows Server 2025 vorbereiten	51
2.2 Windows Server 2025 neu installieren	52
2.2.1 Windows Server 2025-Installation durchführen	52
2.2.2 USB-Stick für Windows Server 2025 erstellen	57
2.3 Zu Windows Server 2025 aktualisieren	58
2.3.1 Aktualisierung zu Windows Server 2025 durchführen	59
2.3.2 Upgrade von Standard- und Testversion auf Datacenter-Edition	61
2.4 Nacharbeiten zur Installation von Windows Server 2025	62
2.4.1 Windows Server 2025 aktivieren	62
2.4.2 Treiberinstallation überprüfen	64
2.4.3 Netzwerkverbindung testen	64
2.4.4 Windows Update aktivieren	64
2.4.5 Sprachpakete installieren	65
2.4.6 Media Player deaktivieren	66
2.4.7 Computernamen und Domänenmitgliedschaft festlegen	67
2.4.8 Aktivieren von Remotedesktop	68
2.5 Zusammenfassung	70

- Kapitel 3 Erste Schritte mit Windows Server 2025** 71
 - 3.1 Erste Schritte nach der Installation 71
 - 3.1.1 Windows Server 2025 mit Windows 10/11 verwalten 71
 - 3.2 Core-Server verwalten 76
 - 3.2.1 Hardware und Treiber auf Core-Servern installieren 80
 - 3.2.2 Windows Updates auf Core-Servern steuern 80
 - 3.3 Erweiterte Startoptionen nutzen 81
 - 3.3.1 Starten der automatischen Reparatur von Windows Server 2025 81
 - 3.3.2 Windows Server 2025 im abgesicherten Modus starten 82
 - 3.3.3 Abgesicherter Modus über msconfig.exe 82
 - 3.3.4 Abgesicherten Modus in das Bootmenü einbinden 82
 - 3.3.5 Abgesicherter Modus über automatische Reparatur starten 83
 - 3.4 Remote-Management aktivieren 83
 - 3.5 Windows Admin Center in der Praxis 84
 - 3.5.1 Admin Center Gateway installieren und aktualisieren 85
 - 3.5.2 Windows Admin Center: Modernized Gateway basiert auf Microservices 86
 - 3.5.3 Verbindungsaufbau zu Servern herstellen 89
 - 3.5.4 Fehler bei der Verbindung beheben 90
 - 3.5.5 Server im Windows Admin Center verwalten 91
 - 3.5.6 Mit Markierungen arbeiten und Objekte suchen 93
 - 3.5.7 Datei-Explorer, Registry-Editor, PowerShell und Remotedesktop nutzen 93
 - 3.5.8 Gatewayzugriff steuern 94
 - 3.5.9 Zertifikat für das Windows Admin Center steuern 94
 - 3.5.10 Erweiterungen für das Windows Admin Center 95
 - 3.5.11 Windows Admin Center und Microsoft Azure 95
 - 3.5.12 Hyper-V mit dem Windows Admin Center verwalten 102
 - 3.6 Zusammenfassung 103
- Kapitel 4 Serverrollen und Features installieren und einrichten** 105
 - 4.1 Installieren von Serverrollen und Features auf einem Server 106
 - 4.1.1 Rollen installieren 106
 - 4.1.2 Installation von Rollen und Features abschließen 120
 - 4.2 Rollen in der PowerShell installieren 121
 - 4.2.1 Serverrollen und Features in der PowerShell verwalten 121
 - 4.2.2 Unbeaufsichtigte Installation von Rollen und Features 122
 - 4.3 Rollen und Features mit DISM installieren 122
 - 4.3.1 Webserver mit Dism.exe remote verwalten und Serverrollen auf Core-Servern installieren 122
 - 4.4 Serverrollen mit dem Best Practices Analyzer überprüfen 123
 - 4.4.1 Überprüfen von Servern über das Netzwerk 124
 - 4.4.2 BPA in der PowerShell starten 125
 - 4.4.3 Ergebnisse exportieren 127
 - 4.4.4 BPA für Hyper-V nutzen 127
 - 4.4.5 BPA auswerten 128
 - 4.5 Zusammenfassung 128

Teil II Einrichtung des Servers

Kapitel 5	Datenträger und Speicherpools verwalten	131
5.1	Wichtige Funktionen im Storage-Bereich	132
5.1.1	Storage Spaces Direct und Storage Replica	133
5.1.2	Datendeduplizierung erweitert	134
5.1.3	ReFS und Speicherpools	134
5.2	Datenträger erstellen und anpassen	138
5.2.1	Einrichten von Datenträgern	138
5.2.2	Konfigurieren von Laufwerken	141
5.2.3	Komprimieren von Datenträgern und Ordern	143
5.2.4	Festplattenverwaltung in der PowerShell und Eingabeaufforderung	145
5.2.5	Mit GPT-Partitionen und ReFS arbeiten	150
5.2.6	Verkleinern und Erweitern von Datenträgern	151
5.2.7	Software-RAIDs in Windows Server nutzen	153
5.3	Verwalten von Datenträgern	154
5.3.1	Defragmentierung verwalten	155
5.3.2	Hardware und Richtlinie von Datenträgern verwalten	156
5.4	BitLocker-Laufwerkverschlüsselung	158
5.4.1	Grundlagen zu BitLocker und Trusted Platform Module (TPM)	158
5.4.2	BitLocker schnell und einfach aktivieren	160
5.4.3	BitLocker mit der PowerShell steuern	162
5.4.4	Troubleshooting für BitLocker	164
5.4.5	Verschlüsselndes Dateisystem (EFS) – Daten einfach absichern	164
5.5	Speicherpools einsetzen	166
5.5.1	Speicherpools erstellen	167
5.5.2	Speicherplätze in Speicherpools erstellen	168
5.5.3	Volumes auf virtuellen Datenträgern in Speicherpools erstellen	170
5.5.4	Speicherpools verwalten und physische Festplatten hinzufügen	172
5.5.5	Virtuelle und physische Datenträger verwalten, trennen und löschen	173
5.5.6	Speicherpools und virtuelle Festplatten mit der PowerShell verwalten	173
5.5.7	Erstellen eines Storage Spaces mit SSD-/NVMe-Festplatten	175
5.6	Verwenden von Schattenkopien	178
5.7	Erstellen und Verwalten von virtuellen Festplatten	180
5.7.1	Virtuelle Festplatten in der Datenträgerverwaltung erstellen	180
5.7.2	VHD(X)-Festplatten konvertieren und in der PowerShell verwalten	181
5.7.3	VHD-Dateien in den Boot-Manager einbinden	182
5.7.4	iSCSI-Ziele über virtuelle Festplatten zur Verfügung stellen	183
5.7.5	iSCSI-Ziele sicher zur Verfügung stellen	184
5.7.6	iSCSI-Festplatten verbinden	185
5.8	Datendeduplizierung einrichten	187
5.8.1	Einstieg in die Deduplizierung	188
5.8.2	Datendeduplizierung im Server-Manager und der PowerShell	189
5.9	Speicher-Replikation – Daten in Netzwerken replizieren	191
5.9.1	Storage Replica verstehen	191
5.9.2	Ablauf der Replikation	192
5.9.3	Storage Replica in der Praxis	192
5.9.4	Storage Replica auf alleinstehenden Servern in der PowerShell steuern	193
5.9.5	Storage Spaces Direct und Storage Replica	194
5.10	Zusammenfassung	195

- Kapitel 6 Windows Server 2025 im Netzwerk betreiben** 197
 - 6.1 Grundlagen zur Netzwerkanbindung 197
 - 6.1.1 Installation der Netzwerkhardware 197
 - 6.1.2 Anbindung des Computers an das Netzwerk 198
 - 6.1.3 Erweiterte Verwaltung der Netzwerkverbindungen 198
 - 6.1.4 Eigenschaften von Netzwerkverbindungen und ihre erweiterte Verwaltung 200
 - 6.1.5 DNS über HTTPS – DoH 201
 - 6.2 Netzwerkkarten zusammenfassen – NIC-Teaming 204
 - 6.2.1 NIC-Team erstellen 204
 - 6.2.2 NIC-Teams auf Core-Server und in der PowerShell 207
 - 6.2.3 NIC-Teams testen und konfigurieren 207
 - 6.2.4 Eigenschaften von TCP/IP und DHCP 208
 - 6.3 Erweiterte Netzwerkeinstellungen – Routing und IPv6 212
 - 6.3.1 IP-Routing unter Windows Server 2025 212
 - 6.3.2 Routen verfolgen in der Eingabeaufforderung – Pathping und Tracert 214
 - 6.3.3 Internetprotokoll Version 6 – IPv6 215
 - 6.4 Mit der PowerShell Netzwerkprobleme lösen 220
 - 6.4.1 Get-NetIPAddress und Get-NetIPConfiguration 220
 - 6.4.2 Test-NetConnection: Routen nachverfolgen und Verbindungen überprüfen 220
 - 6.4.3 Get-NetTCPConnection: Ports und TCP-Verbindungen testen 221
 - 6.4.4 Get-NetFirewallRule: Windows-Firewallregeln überwachen 223
 - 6.4.5 Aufgaben im Netzwerk mit der PowerShell durchführen 223
 - 6.4.6 Mit der PowerShell nach geöffneten Ports suchen 224
 - 6.4.7 Daten in der PowerShell mit der Zwischenablage austauschen 226
 - 6.5 Windows Server 2025 Active Directory 227
 - 6.5.1 Netzwerkeinstellungen für die Domänenaufnahme konfigurieren 227
 - 6.5.2 Domänenaufnahme durchführen 227
 - 6.5.3 Domänenaufnahme testen 228
 - 6.6 Zusammenfassung 231

Teil III Virtualisierung mit Hyper-V

- Kapitel 7 Hyper-V – Installation und Server virtualisieren** 235
 - 7.1 Neuerungen in der Virtualisierung 236
 - 7.1.1 Neue VM-Version 12 in Windows Server 2025 238
 - 7.1.2 Generation-1-VMs versus Generation-2-VMs 239
 - 7.1.3 Hyper-V-Switches verstehen 240
 - 7.1.4 Microsoft sieht den Schwerpunkt von Hyper-V in Azure Stack HCI 242
 - 7.2 So funktioniert Hyper-V 242
 - 7.2.1 Optimale Hochverfügbarkeit 243
 - 7.2.2 Sicherheit und Bandbreitenverwaltung 243
 - 7.2.3 Schnellerer Datenfluss in Rechenzentren mit SAN 245
 - 7.2.4 Weitere wichtige Funktionen in Hyper-V 245
 - 7.2.5 Verzeichnisse in Hyper-V 247
 - 7.2.6 Hyper-V in Windows Server 2025 nutzen 247
 - 7.3 Hyper-V installieren und verwalten 249
 - 7.3.1 Voraussetzungen für den Einsatz von Hyper-V 249
 - 7.3.2 Hyper-V installieren 250
 - 7.3.3 Erste Schritte mit Hyper-V 252
 - 7.3.4 CPU-Last überwachen und Daten zu VMs anzeigen 253

7.4	Virtuelle Switches in Windows Server 2025	254
7.4.1	Hyper-V-Netzwerke planen	254
7.4.2	Erstellen und Konfigurieren von virtuellen Switches	256
7.4.3	MAC-Adressen für Hyper-V konfigurieren	259
7.4.4	Virtuelle LANs (VLAN) und Hyper-V	260
7.4.5	Switch Embedded Teaming – NIC-Teams für Hyper-V	261
7.4.6	NAT in Hyper-V konfigurieren	262
7.5	Virtuelle Server erstellen und installieren	262
7.5.1	IDE oder SCSI – Welcher virtuelle Controller ist besser?	263
7.5.2	Laufwerke mit der PowerShell hinzufügen	264
7.5.3	Virtualisierung von Domänencontrollern	264
7.5.4	Per Hyper-V-Manager virtuelle Maschinen erstellen	267
7.5.5	Virtuelle Server steuern	271
7.6	Einstellungen von virtuellen Servern anpassen	272
7.6.1	Hardware zu virtuellen Computern hinzufügen	272
7.6.2	Virtuelle Festplatten zu Servern hinzufügen	274
7.6.3	Speicher-Migration – Virtuelle Festplatten verschieben	276
7.6.4	USB-Festplatten an Hyper-V anbinden	278
7.6.5	Virtuelle Festplatten von Servern verwalten und optimieren	279
7.6.6	Dynamic Memory – Arbeitsspeicher anpassen	279
7.6.7	Prozessoren in Hyper-V steuern	281
7.6.8	Allgemeine Einstellungen von virtuellen Computern verwalten	283
7.6.9	Virtuelle Server in der PowerShell steuern – PowerShell Direct nutzen	284
7.6.10	Daten von virtuellen Servern aus Hyper-V auslesen	285
7.7	Hyper-V-Host absichern	287
7.7.1	Updates installieren und Lücken schließen	287
7.7.2	Sicherheitsempfehlungen von Microsoft mit Richtlinien absichern	288
7.7.3	BPA für Hyper-V nutzen	288
7.7.4	Sichere virtuelle Maschinen mit Secure Boot	289
7.8	Migration zu Hyper-V	290
7.8.1	Direkte Aktualisierung von Hyper-V-Hosts und VMs	290
7.8.2	Side-by-Side-Migration von Hyper-V-Hosts zu Windows Server 2025	291
7.8.3	Prozessorkompatibilität bei der Migration berücksichtigen	292
7.8.4	Vorhandene VM in Windows Server 2025 importieren	293
7.8.5	Windows Server-Migrationstools nutzen	293
7.8.6	Neue VM-Version mit der PowerShell steuern	295
7.8.7	Eingebettete Virtualisierung in Windows Server 2025	295
7.8.8	Festplattendateien migrieren	297
7.9	Zusammenfassung	297
Kapitel 8	Hyper-V – Datensicherung und Wiederherstellung	299
8.1	Hyper-V und virtuelle Server richtig sichern	299
8.2	Prüfpunkte von virtuellen Servern erstellen	300
8.2.1	Produktionsprüfpunkte in Windows Server 2025 nutzen	301
8.2.2	Prüfpunkte verstehen	302
8.2.3	Produktionsprüfpunkte erstellen	304
8.2.4	Snapshots von virtuellen Servern erstellen	305
8.2.5	Verwalten der Snapshots von virtuellen Servern	307
8.2.6	Datensicherung und Snapshots bei Hyper-V im Cluster	308
8.3	Sicherung durch Export	309

8.4	VMs per Skript sichern	310
8.4.1	Snapshots erstellen in Hyper-V mit »Checkpoint-VM«	311
8.5	Virtuelle Server gruppieren	312
8.6	Zusammenfassung	313
Kapitel 9	Hyper-V – Hochverfügbarkeit	315
9.1	Einstieg in die Hochverfügbarkeit in Hyper-V	316
9.1.1	Hyper-V-Replikation und Cluster	316
9.1.2	Arten der Hochverfügbarkeit in Hyper-V	318
9.2	Hyper-V-Replikation in der Praxis	318
9.2.1	Hyper-V-Hosts für Replikation aktivieren	318
9.2.2	Hyper-V-Replikation mit SSL konfigurieren	320
9.2.3	Virtuelle Server zwischen Hyper-V-Hosts replizieren	321
9.2.4	Failover mit Hyper-V-Replica durchführen	324
9.3	Livemigration ohne Cluster	324
9.4	Hyper-V im Cluster – Livemigration in der Praxis	328
9.4.1	Clusterknoten vorbereiten	329
9.4.2	Cluster mit Windows Server 2025 installieren	330
9.4.3	Cluster Shared Volumes aktivieren	334
9.4.4	Virtuelle Server im Cluster verwalten	338
9.4.5	MAC-Adressen im Cluster konfigurieren	338
9.4.6	Nacharbeiten: Überprüfung des Clusters und erste Schritte mit der Clusterverwaltung oder der PowerShell	339
9.5	Zusammenfassung	341

Teil IV Active Directory

Kapitel 10	Active Directory – Grundlagen und erste Schritte	345
10.1	Einstieg in Active Directory mit Windows Server 2025	345
10.1.1	Die Neuerungen in Active Directory im Detail	345
10.1.2	Active Directory im Detail	350
10.1.3	Active Directory-Systemrollen nutzen	350
10.1.4	Active Directory mit dem Verwaltungscenter verwalten	352
10.1.5	Active Directory für Einsteiger	353
10.1.6	PowerShell und Active Directory	355
10.1.7	Migration zu Active Directory mit Windows Server 2025	356
10.1.8	Sicheres DNS-System in Windows Server 2025	356
10.1.9	Active Directory remote verwalten	357
10.2	Active Directory mit Windows Server 2025 installieren und verstehen	357
10.2.1	Aufbau von Active Directory	358
10.3	Active Directory remote mit der PowerShell verwalten	360
10.3.1	Remote-PowerShell aktivieren und Verbindungsprobleme beheben	360
10.3.2	Cmdlets für die Remoteverwaltung und Abrufen der Hilfe	361
10.4	Verwalten der Betriebsmasterrollen von Domänencontrollern	362
10.4.1	PDC-Emulator verwalten	363
10.4.2	RID-Master – Neue Objekte in der Domäne aufnehmen	364
10.4.3	Infrastrukturmaster – Auflösen von Gruppen über Domänen hinweg	365
10.4.4	Schemamaster – Active Directory erweitern	365
10.4.5	Domänennamenmaster – Neue Domänen hinzufügen	366

10.4.6	Der globale Katalog	366
10.4.7	Verwaltung und Verteilung der Betriebsmaster	369
10.5	Schreibgeschützte Domänencontroller (RODC)	373
10.6	Zusammenfassung	375
Kapitel 11	Active Directory – Installation und Betrieb	377
11.1	Tipps für die Verwaltung von Active Directory	377
11.2	DNS für Active Directory installieren	379
11.2.1	Vorbereitungen für DNS treffen und DNS installieren	379
11.3	Active Directory von Installationsmedium installieren	395
11.3.1	Vorbereiten des Active Directory-Installationsmediums	395
11.3.2	Domänencontroller mit Medium installieren	396
11.4	Active Directory mit der PowerShell installieren	396
11.4.1	Beispiel: Erstellen einer neuen Active Directory-Gesamtstruktur in der PowerShell	398
11.4.2	Die neuen Features in Windows Server 2025 aktivieren	399
11.5	Virtuelle Domänencontroller betreiben – Klonen und Snapshots	400
11.5.1	Möglichkeiten zur Virtualisierung von Domänencontrollern	401
11.5.2	Bereitstellung virtueller Domänencontroller vorbereiten – XML-Dateien erstellen	401
11.5.3	Quelldomänencontroller vor dem Klonen überprüfen und vorbereiten	403
11.5.4	Festplatten von virtuellen Domänencontrollern kopieren	403
11.5.5	Geklonten Domänencontroller für die Aufnahme in Active Directory vorbereiten	404
11.6	Domänencontroller entfernen	405
11.6.1	Herabstufen eines Domänencontrollers in der PowerShell	405
11.6.2	Entfernen von Active Directory über den Server-Manager	406
11.7	Migration zu Windows Server 2025-Active Directory	406
11.7.1	Domänen zu Windows Server 2025 aktualisieren	406
11.8	Das Active Directory-Verwaltungscenter und die PowerShell	407
11.8.1	Active Directory und die PowerShell	409
11.8.2	Objekte schützen und wiederherstellen	411
11.8.3	Andere Objekte schützen – Active Directory-Standorte und -Dienste	412
11.8.4	Löschschutz in der PowerShell abfragen und setzen	412
11.9	Sicherheit in LDAP für Domänencontroller nutzen	412
11.9.1	Microsoft empfiehlt die Aktivierung von LDAPS	413
11.9.2	Probleme nach Aktivierung von LDAPS erkennen	413
11.9.3	LDAP-Signierung und LDAP Channel Binding für mehr Sicherheit in Active Directory	414
11.9.4	LDAP over SSL in Active Directory nutzen	416
11.9.5	LDAPS zusammen mit LDAP-Signatur und LDAP Channel Binding einsetzen	417
11.9.6	LDAP-Prioritäten und -Gewichtung konfigurieren – DCs entlasten	417
11.10	Zeitsynchronisierung in Windows-Netzwerken	418
11.10.1	Grundlagen zur Zeitsynchronisierung in Active Directory	419
11.10.2	Das NTP-Protokoll und Befehle zur Zeitsynchronisierung	421
11.10.3	Net Time versus W32tm	422
11.10.4	Funkuhr versus Internetzeit – Zeitsynchronisierung konfigurieren	422
11.10.5	Zeitsynchronisierung bei der Virtualisierung beachten	424
11.11	Zusammenfassung	425

- Kapitel 12 Active Directory – Erweitern und Absichern** 427
 - 12.1 Offline-Domänenbeitritt – Djoin 427
 - 12.1.1 Vorteile und technische Hintergründe zum Offline-Domänenbeitritt 427
 - 12.1.2 Voraussetzungen für die Verwendung des Offline-Domänenbeitritts 428
 - 12.1.3 Durchführen des Offline-Domänenbeitritts 428
 - 12.1.4 Offline-Domänenbeitritt bei einer unbeaufsichtigten Installation über Antwortdatei 429
 - 12.2 Verwaltete Dienstkonten – Managed Service Accounts 430
 - 12.2.1 Verwaltete Dienstkonten – Technische Hintergründe 430
 - 12.2.2 Verwaltete Dienstkonten – Produktiver Einsatz 431
 - 12.2.3 Verwaltete Dienstkonten in der grafischen Oberfläche anlegen 432
 - 12.2.4 Einen Delegated Managed Service Account anlegen 434
 - 12.3 Der Active Directory-Papierkorb im Praxiseinsatz 435
 - 12.3.1 Active Directory-Papierkorb verstehen und aktivieren 435
 - 12.3.2 Objekte aus dem AD-Papierkorb mit Bordmitteln wiederherstellen 436
 - 12.3.3 Organisationseinheiten und Objekte in AD absichern und sichern 438
 - 12.3.4 Erweiterte Optionen für Organisationseinheiten einblenden 439
 - 12.4 Zusammenfassung 441
- Kapitel 13 Active Directory – Neue Domänen und Domänencontroller** 443
 - 13.1 Core-Server als zusätzlichen Domänencontroller betreiben 443
 - 13.1.1 Vorbereitungen in der PowerShell durchführen 444
 - 13.1.2 Active Directory auf dem Core-Server installieren und einrichten 445
 - 13.2 Schreibgeschützter Domänencontroller (RODC) 446
 - 13.2.1 Vorbereitungen für die Integration eines zusätzlichen Domänencontrollers in eine Domäne 446
 - 13.2.2 Einstieg in schreibgeschützte Domänencontroller – RODC 447
 - 13.2.3 Integration eines neuen Domänencontrollers 448
 - 13.2.4 Delegierung der RODC-Installation 453
 - 13.2.5 Kennwortreplikationsrichtlinien auf RODCs steuern 454
 - 13.2.6 RODC löschen 454
 - 13.2.7 Notwendige Nacharbeiten nach der Integration eines zusätzlichen Domänencontrollers 455
 - 13.3 Erstellen einer neuen untergeordneten Domäne 456
 - 13.3.1 Anpassen der DNS-Infrastruktur an untergeordnete Domänen 457
 - 13.3.2 Heraufstufen eines Domänencontrollers für eine neue untergeordnete Domäne .. 462
 - 13.4 Einführen einer neuen Domänenstruktur in einer Gesamtstruktur 463
 - 13.4.1 Erstellen der DNS-Infrastruktur für eine neue Domänenstruktur 464
 - 13.4.2 Optimieren der IP-Einstellungen beim Einsatz von mehreren Domänen 465
 - 13.4.3 Erstellen der neuen Domänenstruktur 466
 - 13.5 Das Active Directory-Schema erweitern 466
 - 13.6 Zusammenfassung 468
- Kapitel 14 Active Directory – Replikation** 469
 - 14.1 Grundlagen zur Replikation 469
 - 14.2 Konfiguration der Routingtopologie in Active Directory 471
 - 14.2.1 Erstellen von neuen Standorten über Active Directory-Standorte und -Dienste ... 472
 - 14.2.2 Erstellen und Zuweisen von IP-Subnetzen 474
 - 14.2.3 Erstellen von Standortverknüpfungen und Standortverknüpfungsbrücken 475
 - 14.2.4 Zuweisen der Domänencontroller zu den Standorten 476
 - 14.2.5 Die Konsistenzprüfung (Knowledge Consistency Checker) 477

14.3	Fehler bei der Active Directory-Replikation beheben	480
14.3.1	Suche mit der Active Directory-Diagnose	480
14.3.2	Ausschließen der häufigsten Fehlerursachen	480
14.3.3	Nltest zum Erkennen von Standortzuweisungen eines Domänencontrollers	481
14.3.4	Repadmin zum Anzeigen der Active Directory-Replikation	481
14.3.5	Replikation in der PowerShell testen	483
14.3.6	Netzwerkverbindungen zwischen DCs überprüfen	484
14.3.7	Secure Channel überprüfen – Test-ComputerSecureChannel	484
14.3.8	Kerberos-Test mit Dcdiag ausführen	485
14.3.9	Überprüfung der notwendigen SRV-Records im DNS unter <i>_msdcs</i>	485
14.4	Zusammenfassung	485
Kapitel 15	Active Directory – Fehlerbehebung und Diagnose	487
15.1	Bordmittel zur Diagnose verwenden	488
15.1.1	Schneller Überblick zu Domänen und Gesamtstrukturen in der PowerShell – inklusive Betriebsmaster	488
15.1.2	Informationen aus Active Directory mit der PowerShell auslesen	489
15.1.3	Daten zu Computer und Benutzerkonten anzeigen	489
15.1.4	Microsoft Active Directory Documentation Script	490
15.1.5	Verwenden der Domänencontrollerdiagnose	490
15.1.6	Testen der Namensauflösung mit Nslookup	492
15.1.7	Standard-OUs per Active Directory-Benutzer und -Computer überprüfen	495
15.1.8	Überprüfen der Active Directory-Standorte	495
15.1.9	Überprüfen der Domänencontrollerliste	496
15.1.10	Überprüfen der Active Directory-Dateien	496
15.1.11	Domänenkonto der Domänencontroller überprüfen und Kennwort zurücksetzen	497
15.1.12	Überprüfen der administrativen Freigaben	498
15.1.13	Überprüfen der Gruppenrichtlinien	498
15.1.14	DNS-Einträge von Active Directory überprüfen	499
15.1.15	Testen der Betriebsmaster	499
15.1.16	Leistungsüberwachung zur Diagnose nutzen	500
15.1.17	LDAP-Zugriff auf Domänencontrollern überwachen	501
15.1.18	Zurücksetzen des Kennworts für den Wiederherstellungsmodus in Active Directory	501
15.2	Konfiguration der Ereignisprotokollierung von Active Directory	502
15.3	Einbrüche in Active Directory effizient erkennen	503
15.3.1	Aktivieren der einfachen Überwachung	503
15.3.2	Erweiterte Überwachung nutzen	504
15.3.3	Anmeldungen im Netzwerk überwachen	506
15.3.4	Mit Tools für mehr Sicherheit sorgen	506
15.4	Computerkonten in Active Directory verwalten und reparieren	508
15.4.1	Computerkonten in Active Directory-Benutzer und -Computer verwalten	509
15.4.2	Fehlerbehebung von Computerkonten	509
15.4.3	Veraltete Computer finden und bei Bedarf entfernen	510
15.5	Bereinigung von Active Directory und Entfernen von Domänencontrollern	511
15.5.1	Vorbereitungen beim Entfernen eines Domänencontrollers	511
15.5.2	Herabstufen eines Domänencontrollers	512
15.5.3	Bereinigen der Metadaten von Active Directory	513
15.6	Zusammenfassung	514

- Kapitel 16 Active Directory – Sicherung, Wiederherstellung und Wartung** 515
 - 16.1 Active Directory sichern und wiederherstellen 516
 - 16.1.1 Active Directory mit der Windows Server-Sicherung sichern 516
 - 16.1.2 Wiederherstellen von Active Directory aus der Datensicherung 517
 - 16.2 Active Directory-Datenbank warten 522
 - 16.2.1 Verschieben der Active Directory-Datenbank 522
 - 16.2.2 Offlinedefragmentation der Active Directory-Datenbank 523
 - 16.2.3 Reparieren der Active Directory-Datenbank 524
 - 16.2.4 Erstellen von Snapshots der Active Directory-Datenbank 525
 - 16.3 Cleanup Best Practices für Active Directory 525
 - 16.3.1 Nicht mehr benötigte Benutzer und leere Gruppe identifizieren und löschen 526
 - 16.3.2 Veraltete SIDs erkennen und löschen 527
 - 16.3.3 Identifizierung und Änderung von Benutzern mit der Option »Passwort läuft nie ab« 527
 - 16.4 Zusammenfassung 528
- Kapitel 17 Active Directory – Vertrauensstellungen** 529
 - 17.1 Wichtige Grundlagen zu Vertrauensstellungen in Active Directory 529
 - 17.2 Varianten der Vertrauensstellungen in Active Directory 531
 - 17.3 Einrichtung einer Vertrauensstellung 533
 - 17.3.1 Fehler mit Vertrauensstellungen von Computern zur Domäne beheben 536
 - 17.4 Automatisch aktivierte SID-Filterung 536
 - 17.5 Zusammenfassung 537
- Kapitel 18 Benutzerverwaltung und Profile** 539
 - 18.1 Grundlagen zur Verwaltung von Benutzern 539
 - 18.1.1 Active Directory-Benutzerverwaltung 541
 - 18.1.2 Benutzerkonten in der PowerShell anlegen, verwalten und löschen 542
 - 18.1.3 Verwalten von Benutzerkonten 544
 - 18.1.4 Benutzerverwaltung für Remotedesktopbenutzer 547
 - 18.2 Benutzerprofile nutzen 548
 - 18.2.1 Benutzerprofile lokal und im Profieinsatz verstehen 548
 - 18.2.2 Servergespeicherte Profile für Benutzer in Active Directory festlegen 550
 - 18.2.3 Anmelde- und Abmeldeskripts für Benutzer und Computer 556
 - 18.3 Gruppen verwalten 558
 - 18.3.1 Gruppen anlegen und verwenden 558
 - 18.3.2 Berechtigungen für Benutzer und Gruppen verwalten 559
 - 18.3.3 Szenario: Delegierung zum administrativen Verwalten einer Organisationseinheit 562
 - 18.4 Zusammenfassung 563
- Kapitel 19 Richtlinien im Windows Server 2025-Netzwerk** 565
 - 19.1 Erste Schritte mit Richtlinien 565
 - 19.1.1 Verwaltungswerkzeuge für Gruppenrichtlinien 566
 - 19.1.2 Wichtige Begriffe für Gruppenrichtlinien 566
 - 19.1.3 Gruppenrichtlinien-Preferences effizient einsetzen 569
 - 19.1.4 Registry-Einstellungen von Gruppenrichtlinien herausfinden 571
 - 19.1.5 BSI bietet Hilfe bei der Absicherung von Windows 572
 - 19.1.6 Windows 10/11 mit Microsoft-Sicherheitsempfehlungen konfigurieren 573

19.2	Gruppenrichtlinien verwalten	577
19.2.1	Neue Gruppenrichtlinie erstellen	578
19.2.2	GPO mit einem Container verknüpfen	579
19.2.3	Gruppenrichtlinien erzwingen und Priorität erhöhen	581
19.2.4	Vererbung für Gruppenrichtlinien deaktivieren	582
19.2.5	Administration von domänenbasierten GPOs mit ADMX-Dateien	583
19.3	Sicherheitseinstellungen mit Richtlinien steuern	585
19.3.1	Default Domain Controllers Policy mit Microsoft Baseslines analysieren und verbessern	585
19.3.2	Sicherheit in Windows 10 und Windows 11 steuern	592
19.3.3	Benutzer und Kennwörter mit Gruppenrichtlinien absichern	594
19.4	Gruppenrichtlinien testen und Fehler beheben	595
19.4.1	Einstieg in die Fehlerbehebung von Gruppenrichtlinien	595
19.4.2	Vorgehensweise bei der Fehlerbehebung von Gruppenrichtlinien	596
19.4.3	Policy Analyzer zur Fehlerbehebung nutzen	597
19.4.4	Datensicherung und Wiederherstellung von Gruppenrichtlinien	598
19.4.5	Gruppenrichtlinien mit der PowerShell sichern und wiederherstellen	601
19.4.6	Gruppenrichtlinienmodellierung	601
19.5	Softwareverteilung über Gruppenrichtlinien	602
19.6	Geräteinstallation mit Gruppenrichtlinien konfigurieren	603
19.6.1	Geräteidentifikationsstring und Gerätesetupklasse	604
19.6.2	So funktionieren die Steuerungen in Geräteinstallationen über Gruppenrichtlinien	606
19.6.3	Konfiguration von Gruppenrichtlinien für den Zugriff auf Wechselmedien	606
19.6.4	Layered Group Policies – Mehrschichtige Gruppenrichtlinien nutzen	606
19.6.5	Konfiguration von Gruppenrichtlinien für den Zugriff auf Wechselmedien	608
19.7	Mit AppLocker Desktop- und Windows-Apps in Netzwerken steuern	609
19.7.1	AppLocker in Unternehmen nutzen	609
19.7.2	Gruppenrichtlinien für AppLocker erstellen	609
19.7.3	Erstellen von Regeln für AppLocker	611
19.7.4	Automatisches Erstellen von Regeln und Erzwingen von AppLocker	612
19.7.5	Benutzerkontensteuerung über Richtlinien konfigurieren	612
19.7.6	Erstellen einer neuen Gruppenrichtlinie für sichere Kennwörter	613
19.7.7	Firewalleinstellungen über Gruppenrichtlinien setzen	613
19.8	Zusammenfassung	614

Teil V Datei- und Druckserver mit Windows Server

Kapitel 20	Dateiserver und Daten im Netzwerk freigeben	617
20.1	SMB 3.x in Windows Server 2025 nutzen	617
20.1.1	Mehr Sicherheit und Leistung in SMB 3.x	618
20.1.2	SMB 1.0 und 2.0 im Netzwerk ausfindig machen und deaktivieren	620
20.1.3	SMB-Verschlüsselung im Netzwerk erzwingen	621
20.2	Berechtigungen für Dateien und Ordner verwalten	626
20.2.1	Erweiterte Berechtigungen auf Ordner	627
20.2.2	Berechtigungen verstehen	629
20.2.3	Effektive Berechtigungen	631
20.2.4	Tools zur Überwachung von Berechtigungen	632
20.2.5	Dateien und Ordner in der PowerShell erstellen und verwalten	634

- 20.3 Überwachung von Dateien und Ordnern 638
 - 20.3.1 Einstieg in die Überwachung von Verzeichnissen 638
 - 20.3.2 Überwachung mit Richtlinien steuern 639
- 20.4 Die Freigabe von Ordnern 639
 - 20.4.1 Freigaben erstellen 640
 - 20.4.2 Der Assistent zum Erstellen von Freigaben 641
 - 20.4.3 Dateifreigaben in der PowerShell erstellen und verwalten 641
 - 20.4.4 Anzeigen geöffneter Dateien über das Netzwerk – PsFile 645
 - 20.4.5 Versteckte Freigaben 645
 - 20.4.6 Anzeigen aller Freigaben 646
 - 20.4.7 Auf Freigaben über das Netzwerk zugreifen 646
 - 20.4.8 Offlinedateien für den mobilen Einsatz unter Windows 10/11 647
- 20.5 Storage Quality of Services (QoS) – Richtlinien für Datenspeicher 651
 - 20.5.1 Einstieg in Speicherrichtlinien 651
 - 20.5.2 Storage QoS in der PowerShell verwalten 652
 - 20.5.3 Neue Richtlinien in der PowerShell erstellen und verwalten 653
 - 20.5.4 Aggregated Policies nutzen 653
 - 20.5.5 Storage QoS im Cluster überwachen 655
 - 20.5.6 Speicherrichtlinien in System Center Virtual Machine Manager 655
- 20.6 Dateien und Freigaben auf Windows Server 2025 migrieren 656
 - 20.6.1 Daten mit Robocopy übernehmen 656
 - 20.6.2 Nur Freigaben und deren Rechte übernehmen 659
 - 20.6.3 Windows Server Storage Migration Service 660
- 20.7 Zusammenfassung 664
- Kapitel 21 Ressourcen-Manager für Dateiserver und DFS 665**
 - 21.1 Kontingentverwaltung in Windows Server 2025 666
 - 21.1.1 Kontingentverwaltung mit FSRM 666
 - 21.1.2 Datenträgerkontingente für Laufwerke festlegen 670
 - 21.2 Dateiprüfungsverwaltung nutzen 671
 - 21.2.1 Erstellen einer Dateiprüfung 671
 - 21.2.2 Dateiprüfungsausnahmen 673
 - 21.2.3 Dateigruppen für die Dateiprüfung 673
 - 21.3 Speicherberichteverwaltung in FSRM 674
 - 21.4 Dateiklassifizierungsdienste einsetzen 675
 - 21.4.1 Klassifizierungseigenschaften und Klassifizierungsregeln verstehen und einsetzen 676
 - 21.4.2 Dateiverwaltungsaufgaben bei der Dateiklassifizierung einsetzen 677
 - 21.5 So schützen Unternehmen ihre Dateiserver vor Ransomware 678
 - 21.5.1 Allgemeine Tipps für den Schutz vor Ransomware 678
 - 21.5.2 Generelle Vorgehensweise beim Befall gegen Ransomware 678
 - 21.5.3 Schattenkopien helfen bei Windows-Servern 679
 - 21.6 Organisieren und Replizieren von Freigaben über DFS 679
 - 21.6.1 Einführung und wichtige Informationen beim Einsatz von DFS 679
 - 21.6.2 DFS-Namespace und DFS-Replikation 681
 - 21.6.3 Voraussetzungen für DFS 683
 - 21.6.4 Installation und Einrichtung von DFS 683
 - 21.6.5 Einrichtung eines DFS-Namespace 684
 - 21.6.6 Einrichten der DFS-Replikation 686
 - 21.7 Zusammenfassung 687

Kapitel 22	BranchCache	689
22.1	BranchCache im Überblick – Niederlassungen effizient anbinden	689
22.2	Gehosteter Cache (Hosted Cache) nutzen	691
22.3	Verteilter Cache (Distributed Cache) nutzen	694
22.4	BranchCache auf dem Hosted-Cache-Server konfigurieren	696
22.4.1	Feature für Hosted Cache installieren	696
22.4.2	Zertifikate auf dem Hosted-Cache-Server betreiben	697
22.4.3	Einstellungen auf dem Hosted-Cache-Server anpassen	697
22.4.4	Content-Server konfigurieren	698
22.5	BranchCache auf Clients konfigurieren	698
22.5.1	Clientkonfiguration mit Gruppenrichtlinien konfigurieren	699
22.5.2	Firewalleinstellungen für BranchCache setzen	699
22.6	Leistungsüberwachung und BranchCache	700
22.7	Zusammenfassung	700
Kapitel 23	Druckerserver betreiben	701
23.1	Drucken im Netzwerk und mit Smartphones oder Tablets	701
23.1.1	Drucker in Windows freigeben	702
23.1.2	Drucker über WLAN und LAN anbinden	703
23.1.3	Eigenen Netzwerkanschluss konfigurieren	703
23.1.4	Drucken mit iPhone und iPad – AirPrint	704
23.2	Freigegebene Drucker verwalten	705
23.2.1	Anpassen der Einstellungen von Druckern	705
23.2.2	Der Zugriff auf freigegebene Drucker	705
23.2.3	Eigenschaften von Druckern in der PowerShell ändern	706
23.2.4	Druckaufträge in der PowerShell erzeugen	707
23.2.5	Druckberechtigungen mit Skripts setzen – SetACL.exe	708
23.3	Verwaltung von Druckjobs	708
23.3.1	Druckverwaltungs-Konsole – Die Zentrale für Druckerserver	709
23.3.2	Benutzerdefinierte Filteransichten erstellen	709
23.3.3	Drucker exportieren und importieren	710
23.3.4	Drucker verwalten und über Gruppenrichtlinien verteilen lassen	710
23.4	Steuerung von Druckern über Gruppenrichtlinien in Netzwerken	712
23.4.1	Druckerverteilung über GPO ist nicht immer sinnvoll	712
23.4.2	Alternative zur Druckerverteilung mit GPOs	712
23.4.3	PrintNightmare und andere Lücken mit Gruppenrichtlinien bekämpfen	713
23.4.4	Druckerbereitstellung per GPO	714
23.4.5	Drucker abhängig vom Active Directory-Standort zuordnen	715
23.5	Druckprobleme im Netzwerk lösen	715
23.5.1	Generelle Vorgehensweise beim Lösen von Druckproblemen	716
23.5.2	Druckjobs überprüfen und löschen	716
23.5.3	Problembehebung mit Assistenten durchführen	717
23.5.4	Druckeinstellungen zur Fehlerbehebung überprüfen	717
23.5.5	Berechtigungen und Sicherheitseinstellungen überprüfen	718
23.5.6	Drucker mit WMI ansprechen	718
23.6	Druckerserver mit Microsoft Universal Print in der Cloud betreiben	720
23.6.1	Lizenzierung und Einstieg in Universal Print	720
23.7	Zusammenfassung	722

Teil VI Infrastrukturen mit Windows Server

Kapitel 24 DHCP- und IPAM-Server einsetzen 725

 24.1 DHCP-Server einsetzen 725

 24.1.1 Installation eines DHCP-Servers 725

 24.1.2 Grundkonfiguration eines DHCP-Servers 726

 24.1.3 DHCP-Server mit Tools testen und Fehler finden 734

 24.1.4 DHCP-Verkehr mit WireShark überprüfen 735

 24.1.5 Core-Server – DHCP mit Netsh über die Eingabeaufforderung verwalten 736

 24.1.6 Konfigurieren von DHCP mit der richtlinienbasierten Zuweisung 736

 24.1.7 MAC-Filterung für DHCP in Windows Server 2025 nutzen 738

 24.2 Migration – Verschieben einer DHCP-Datenbank auf einen anderen Server 739

 24.3 Ausfallsicherheit von DHCP-Servern 740

 24.3.1 DHCP für Failover konfigurieren 741

 24.3.2 Ausfallsicherheit mit 80/20-Regel 745

 24.3.3 Bereichsgruppierung (Superscopes) 746

 24.3.4 Ausfallsicherheit bei DHCP-Servern durch verschiedene Bereiche herstellen 746

 24.3.5 Standby-Server mit manueller Umschaltung 747

 24.4 IPAM im Praxiseinsatz 748

 24.4.1 IPAM-Grundlagen 748

 24.4.2 IPAM einrichten 749

 24.4.3 Fehlerbehebung der Anbindung von IPAM-Clients 751

 24.4.4 Infrastrukturüberwachung und -verwaltung 752

 24.4.5 IP-Adressblöcke mit IPAM 753

 24.5 Zusammenfassung 753

Kapitel 25 DNS einsetzen und verwalten 755

 25.1 Erstellen von Zonen und Domänen 755

 25.1.1 Erstellen von neuen Zonen 755

 25.1.2 Erstellen von statischen Einträgen in der DNS-Datenbank 758

 25.1.3 Einstellungen und Verwalten von Zonen 760

 25.2 Verwalten der Eigenschaften eines DNS-Servers 767

 25.2.1 Schnittstellen eines DNS-Servers verwalten 767

 25.2.2 Erweiterte Einstellungen für einen DNS-Server 767

 25.2.3 Zonendaten beim Start des DNS-Servers einlesen 768

 25.2.4 Protokollierung für DNS konfigurieren 769

 25.2.5 Ereignisprotokollierung konfigurieren 770

 25.3 DNS-Weiterleitungen verwenden 770

 25.4 Konfiguration sekundärer DNS-Server 771

 25.5 DNS-Troubleshooting 772

 25.5.1 Überprüfung und Fehlerbehebung der DNS-Einstellungen 773

 25.5.2 Ipconfig für DNS-Diagnose verwenden 775

 25.5.3 Domänencontroller kann nicht gefunden werden 776

 25.5.4 Namensauflösung von Mitgliedsservern 776

 25.5.5 Erweiterte Namensauflösung sicherstellen 777

 25.5.6 Nslookup zur Auflösung von Internetdomänen verwenden 778

 25.5.7 Mit Nslookup SRV-Records oder MX-Records anzeigen 778

 25.5.8 Komplette Zonen mit Nslookup übertragen 779

 25.5.9 Dnscmd zur Verwaltung eines DNS-Servers in der Eingabeaufforderung 779

25.6	DNSSEC – Sicherheit in DNS	782
25.6.1	DNSSEC verstehen	782
25.6.2	DNS sicher betreiben – DNSSEC in der Praxis	783
25.6.3	DNS-Abfragen mit Richtlinien steuern	787
25.6.4	Response Rate Limiting – Schutz vor Denial of Service	789
25.7	Zusammenfassung	789
Kapitel 26	Windows Server Container, Docker und Hyper-V-Container	791
26.1	Einstieg in Container und Docker	791
26.1.1	Container im Vergleich zu virtuellen Servern	792
26.1.2	Container-Feature installieren	792
26.1.3	Erste Schritte mit Docker in Windows Server 2025	794
26.1.4	Hyper-V-Container-Host	796
26.1.5	Container im Windows Admin Center verwalten	797
26.2	Erweiterte Konfiguration von Containern	798
26.2.1	Neues Containerimage für Windows Server 2025 verfügbar	798
26.2.2	Container erstellen und Serverdienste verwalten	799
26.2.3	Container und eigene Images erstellen	800
26.2.4	Dockerfiles für eigene Images erstellen	801
26.2.5	Docker Push – Container in die Cloud laden	802
26.3	Hyper-V-Container in Windows Server 2025	802
26.3.1	Einstieg in Hyper-V-Container	802
26.3.2	Hyper-V-Container erstellen und konfigurieren	804
26.3.3	Docker, Hyper-V-Container und VMs parallel einsetzen	804
26.3.4	Windows Server Container in der PowerShell verwalten	805
26.4	Windows-Subsystem für Linux in Windows Server 2025 und Windows 10/11	805
26.4.1	Linux und Windows gemeinsam betreiben	806
26.4.2	Windows Subsystem for Linux installieren	806
26.5	Zusammenfassung	809
Kapitel 27	Webserver – Internetinformationsdienste (IIS)	811
27.1	Installation, Konfiguration und erste Schritte	812
27.1.1	Anzeigen der Websites in IIS	814
27.1.2	Hinzufügen und Verwalten von Websites	815
27.1.3	Starten und Beenden des Webserver	817
27.1.4	Systemdateien von IIS verstehen	818
27.1.5	Verwalten der Webanwendungen und virtuellen Ordner einer Website	819
27.1.6	Entwicklungstools in Microsoft Edge	820
27.1.7	Proxy-Einstellungen im Windows-Netzwerk mit WPAD und PAC konfigurieren	821
27.2	Verwalten von Anwendungspools	823
27.2.1	Erstellen und Verwalten von Anwendungspools	824
27.2.2	Zurücksetzen von Arbeitsprozessen in Anwendungspools	825
27.3	Verwalten von Modulen in IIS 2025	825
27.4	Delegierung der IIS-Verwaltung	825
27.4.1	Vorgehensweise bei der Delegierung von Berechtigungen	826
27.4.2	Verwalten von IIS-Manager-Benutzern	826
27.4.3	Berechtigungen der IIS-Manager-Benutzer verwalten	826
27.4.4	Verwalten der Delegierung	828
27.4.5	Aktivieren der Remoteverwaltung	829

27.5	Sicherheit in IIS 2025 konfigurieren	830
27.5.1	Konfiguration der anonymen Authentifizierung	830
27.5.2	Konfiguration der Standardauthentifizierung	831
27.5.3	Konfiguration der Windows-Authentifizierung	831
27.5.4	Einschränkungen für IP-Adressen und Domänen	832
27.5.5	Sicherheitseinstellungen von IIS anpassen	833
27.5.6	IP-Adressen, Domänen, SSL und URL Rewrite	833
27.5.7	IIS mit kostenlosen Tools absichern	835
27.5.8	Zed Attack Proxy Project (ZAP) und Deft-Linux – Webanwendungen testen	835
27.5.9	Freigegebene Konfiguration	836
27.6	Konfigurieren der Webseiten, Dokumente und HTTP-Verbindungen	836
27.6.1	Festlegen des Standarddokuments	836
27.6.2	Das Feature »Verzeichnis durchsuchen« aktivieren und verwalten	837
27.6.3	Konfigurieren der HTTP-Fehlermeldungen und -Umleitungen	838
27.7	IIS 2025 überwachen und Protokolldateien konfigurieren	840
27.7.1	Ablaufverfolungsregeln für Anforderungsfehler	841
27.7.2	Allgemeine Protokollierung aktivieren und konfigurieren	841
27.7.3	Überprüfen der Arbeitsprozesse der Anwendungspools	843
27.8	Optimieren der Serverleistung	843
27.8.1	Komprimierung aktivieren	843
27.8.2	Ausgabezwischen Speicherung verwenden	844
27.9	FTP-Server betreiben	845
27.9.1	Konfiguration des FTP-Servers	846
27.9.2	Schritt für Schritt-Anleitung zum FTP-Server in IIS 2025	846
27.10	Zusammenfassung	849
Kapitel 28	Remotedesktopdienste – Anwendungen virtualisieren	851
28.1	Einstieg in die Remotedesktopdienste	851
28.2	Konfigurieren von RDP-Verbindungen in Windows Server 2025	853
28.2.1	Remotedesktop aktivieren	854
28.2.2	RDP im Windows Admin Center und in der PowerShell	855
28.2.3	Gruppenrichtlinien und Firewall-Einstellungen für den Remotedesktop	857
28.2.4	RDP-Port und Firewallregeln über Registry und PowerShell ändern	857
28.2.5	RDP nutzt TCP und UDP	858
28.3	Installation eines Remotedesktopservers	859
28.3.1	Installation und Verteilen der notwendigen Rollendienste	859
28.3.2	Einrichten einer neuen Sitzungssammlung	865
28.3.3	RemoteApp – Anwendungen bereitstellen	868
28.3.4	Remotedesktoplizenzierung	870
28.3.5	Remotedesktopsitzungen spiegeln	874
28.3.6	Nacharbeiten zur Installation	879
28.4	Drucken mit Remotedesktop-Sitzungshosts	880
28.4.1	Einstieg in das Drucken mit den Remotedesktopdiensten	881
28.4.2	Druckerprobleme auf Remotedesktop-Sitzungshosts lösen	882
28.4.3	Berechtigungs-Probleme auf Remotedesktop-Sitzungshosts lösen	883
28.5	Installation von Applikationen	884
28.5.1	RDS-Server und Microsoft Office	885
28.5.2	Lizenzierung von Office auf RDS-Servern	886
28.6	Remotedesktopclient	887
28.6.1	Befehlszeilenparameter für den Remotedesktopclient	888
28.6.2	Umleitung von Digitalkameras und Mediaplayer	888
28.6.3	RDP-Dateien mit einem Zertifikat signieren	889

28.7	Verwaltung eines Remotedesktop-Sitzungshosts	890
28.7.1	Remotedesktopdienste verwalten	892
28.7.2	Single Sign-On (SSO) für Remotedesktop-Sitzungshosts	893
28.7.3	Connection Broker an Microsoft Azure anbinden	894
28.8	RemoteApps verwalten	894
28.8.1	Konfiguration von Remotedesktopdienste-RemoteApp	896
28.8.2	Mit Windows 10/11 auf RemoteApps zugreifen	896
28.8.3	Remotedesktopdienste-Webzugriff	897
28.9	Remotedesktopgateway	898
28.9.1	Einrichtung und Konfiguration eines Remotedesktopgateways	899
28.9.2	Ressourcenautorisierungsrichtlinien erstellen und verwalten	900
28.10	Remotedesktop-Verbindungsbroker	901
28.11	Zertifikate installieren und einrichten	901
28.11.1	RDS-Zertifikate im Überblick	901
28.11.2	Zertifikate von den Active Directory-Zertifikatdiensten abrufen	902
28.11.3	Eigene Zertifikate-Vorlagen für die Anmeldung an RDS verwenden	903
28.12	Zusammenfassung	905
Kapitel 29	Virtual Desktop Infrastructure – Arbeitsstationen virtualisieren	907
29.1	Einstieg in VDI	907
29.2	Windows 10/11 als virtuellen Computer in einer VDI-Struktur einsetzen	908
29.2.1	Installieren des Remotedesktop-Sitzungshosts	908
29.2.2	VDI-Umgebung verwalten	910
29.2.3	Virtuelle Computer installieren und für VDI vorbereiten	911
29.2.4	System mit Sysprep vorbereiten	912
29.3	Konfiguration des virtuellen Desktop-Pools	912
29.3.1	Sammlung virtueller Pools im Server-Manager erstellen	913
29.3.2	Desktop testen und verwenden	914
29.3.3	Personalisierte virtuelle Rechner verwenden	914
29.3.4	Eigenes Hintergrundbild für gehostete Desktops aktivieren	914
29.4	Zusammenfassung	915
Teil VII	Sicherheit, Verfügbarkeit und Skripting	
Kapitel 30	Active Directory-Zertifikatdienste	919
30.1	Installation einer Zertifizierungsstelle	920
30.1.1	Serverrolle für Active Directory-Zertifikatdienste installieren	920
30.1.2	Zertifizierungsstelle einrichten	922
30.1.3	Eigenständige Zertifizierungsstellen	926
30.1.4	Installieren einer untergeordneten Zertifizierungsstelle	927
30.1.5	Migrieren des Active Directory-Zertifikatdienstes	927
30.1.6	Migration beginnen	928
30.1.7	Zielserver konfigurieren	928
30.1.8	Troubleshooting für Active Directory-Zertifikatsdienste	929
30.2	Zertifikate zuweisen und installieren	930
30.2.1	Zertifikate mit Assistenten aufrufen	930
30.2.2	Zertifikate im IIS-Manager abrufen	931
30.2.3	Zertifikate über Webinterface ausstellen	932
30.2.4	Zertifikate mit Gruppenrichtlinien verteilen	933

- 30.3 Zertifizierungsstelle verwalten 933
 - 30.3.1 SSL für Zertifikatdienste einrichten 933
 - 30.3.2 Zertifikate von Stammzertifizierungsstellen verwalten 935
 - 30.3.3 Die Zertifizierungsstellentypen und -Aufgaben 936
 - 30.3.4 Verteilung der Zertifikateinstellungen über Gruppenrichtlinien 937
- 30.4 Sicherheit für Zertifizierungsstellen verwalten 937
 - 30.4.1 Zertifizierungsstellenverwaltung delegieren 937
 - 30.4.2 Sichern von Active Directory-Zertifikatdiensten 938
- 30.5 Let's Encrypt-Zertifikate in Windows mit Certbot anfordern und als PFX exportieren 939
 - 30.5.1 Windows-Subsystem für Linux installieren 939
 - 30.5.2 Wildcard-Zertifikate in Let's Encrypt mit Certbot abrufen 939
 - 30.5.3 Erstellen eines Zertifikats 940
 - 30.5.4 Zertifikat exportieren 940
- 30.6 Zusammenfassung 940
- Kapitel 31 Firewall, Defender und IPsec im Netzwerk einsetzen 941**
 - 31.1 Microsoft Defender für den Malware-Schutz nutzen 941
 - 31.1.1 Microsoft Defender in der GUI und Befehlszeile steuern 942
 - 31.1.2 Definitionsdateien automatisiert herunterladen und installieren 943
 - 31.1.3 Microsoft Defender in der PowerShell verwalten 944
 - 31.1.4 Microsoft Defender in den Einstellungen und Gruppenrichtlinien anpassen 945
 - 31.1.5 Malware-Schutz aus der Cloud heraus steuern 946
 - 31.1.6 Microsoft Defender for Business 948
 - 31.1.7 Ausnahmen für Serverrollen verwalten – Hyper-V 949
 - 31.1.8 Malware-Suche mit dem Sysinternals Process Explorer 952
 - 31.2 Windows Defender Credential Guard und Hypervisor-Protected Code Integrity 954
 - 31.2.1 Windows Defender Credential Guard aktivieren 954
 - 31.2.2 Kernisolierung: Hypervisor-Protected Code Integrity 956
 - 31.3 Windows Defender-Firewall nutzen 956
 - 31.3.1 Windows Defender-Firewall in der PowerShell steuern 956
 - 31.3.2 IPsec mit der Windows Defender-Firewall nutzen 957
 - 31.3.3 Firewallregeln steuern 960
 - 31.4 Zusammenfassung 964
- Kapitel 32 Active Directory-Rechteverwaltungsdienste nutzen 965**
 - 32.1 Active Directory-Rechteverwaltung im Überblick 966
 - 32.1.1 ADRMS und dynamische Zugriffssteuerung 966
 - 32.2 Rechteverwaltung installieren und einrichten 967
 - 32.2.1 SQL-Server für ADRMS vorbereiten 968
 - 32.2.2 Konfigurieren von ADRMS 971
 - 32.2.3 ADRMS nach der Installation verwalten und überprüfen 973
 - 32.3 Dynamische Zugriffssteuerung nutzen 974
 - 32.4 Zusammenfassung 976
- Kapitel 33 Hochverfügbarkeit und Lastenausgleich 977**
 - 33.1 Grundlagen zum Lastenausgleich 977
 - 33.2 Notwendige Vorbereitungen für NLB-Cluster 978
 - 33.3 Netzwerklastenausgleich installieren 979
 - 33.4 NLB-Cluster erstellen 979
 - 33.5 NLB versus DNS-Roundrobin 983

33.6	Storage Spaces Direct nutzen	985
33.6.1	Einstieg in Storage Spaces Direct	986
33.6.2	So funktioniert Storage Spaces Direct	986
33.6.3	Storage Spaces Direct in der Praxis	987
33.6.4	Ausfallsicherheit bei Storage Spaces Direct	995
33.6.5	Speicherpools in Storage Spaces Direct optimieren	998
33.7	Scale-Out File Server erstellen	998
33.7.1	Cluster sind auch in kleinen Netzwerken sinnvoll einsetzbar	999
33.7.2	Scale-Out File Server und Storage Spaces Direct	1000
33.7.3	Scale-Out File Server im Cluster nutzen	1001
33.7.4	Vorteile beim Einsatz eines Scale-Out File Servers: SMB-Version beachten	1002
33.7.5	Dateiserver und das Cluster Shared Volume	1003
33.8	Cluster Operating System Rolling Upgrade	1004
33.8.1	So aktualisieren Sie einen Cluster zu Windows Server 2025	1004
33.8.2	Node Fairness – Lastenausgleich aktivieren	1006
33.8.3	Startreihenfolge der VMs nach der Migration anpassen	1008
33.8.4	Compute Resiliency – Ausfallsicherheit steuern	1008
33.9	Cluster Aware Update nutzen und einrichten	1009
33.9.1	Grundlagen für die Einführung von Cluster Aware Update	1009
33.9.2	Firewalleinstellungen und mehr für CAU	1010
33.9.3	CAU für den Cluster aktivieren	1011
33.9.4	CAU in der PowerShell steuern	1013
33.9.5	Fehlerbehebung der Einrichtung	1013
33.9.6	Updates mit CAU planen	1013
33.10	Zusammenfassung	1014
Kapitel 34	Datensicherung und Wiederherstellung	1015
34.1	Grundlagen zur Datensicherung	1015
34.2	Windows Server-Sicherung installieren und konfigurieren	1016
34.2.1	Sicherung in der Eingabeaufforderung und PowerShell konfigurieren	1021
34.2.2	Daten mit dem Sicherungsprogramm wiederherstellen	1022
34.2.3	Kompletten Server mit dem Sicherungsprogramm wiederherstellen	1024
34.3	Azure Backup	1026
34.3.1	Azure Backup mit dem Windows Admin Center einrichten	1027
34.3.2	Windows Admin Center kostenlos bei Azure registrieren	1027
34.3.3	Azure Backup einrichten	1028
34.3.4	Manuelle Einrichtung und Verwaltung von Azure Backup	1029
34.3.5	Sicherungsplan für die Datensicherung in Azure Backup erstellen	1030
34.3.6	Daten mit Azure Backup wiederherstellen	1032
34.4	Erweiterte Wiederherstellungsmöglichkeiten	1033
34.4.1	Schrittaufzeichnung – Fehler in Windows nachvollziehen und beheben	1033
34.4.2	Datensicherung über Ereignisanzeige starten	1033
34.5	Windows-Abstürze analysieren und beheben	1035
34.6	Zusammenfassung	1039
Kapitel 35	Active Directory-Verbunddienste und Workplace Join	1041
35.1	Installieren und Einrichten der Active Directory-Verbunddienste	1042
35.1.1	Einstieg in die Installation von ADFS	1042
35.1.2	Vorbereitungen für die ADFS-Infrastruktur	1043
35.1.3	SSL-Zertifikate als Vorlage in Active Directory-Zertifikatdiensten festlegen	1043
35.1.4	ADFS als Serverrolle installieren	1044

- 35.1.5 ADFS einrichten 1046
 - 35.1.6 Geräteregistrierung konfigurieren 1048
 - 35.1.7 Vertrauensstellung zwischen Webanwendung und ADFS einrichten 1049
- 35.2 Fehlerbehebung und Überwachung bei einem ADFS-Server 1050
- 35.3 Single Sign-On mit ADFS – auch mit Microsoft 365 1051
- 35.4 Zusammenfassung 1052
- Kapitel 36 Updates in Microsoft-Netzwerken mit WSUS und Azure steuern 1053**
 - 36.1 Checkpoint-Updates und Hotpatching 1054
 - 36.1.1 Checkpoint-Updates mit Hotpatching kombinieren 1055
 - 36.1.2 Hotpatching in Windows Server 2025 1055
 - 36.2 WSUS installieren 1057
 - 36.2.1 WSUS nach der Installation einrichten 1058
 - 36.2.2 WSUS-Grundeinrichtung über Gruppenrichtlinien 1060
 - 36.2.3 Upstreamserver in WSUS nutzen 1060
 - 36.2.4 Mehr Sicherheit für WSUS: SSL aktivieren 1061
 - 36.3 Updates im Griff behalten und steuern 1068
 - 36.3.1 Steuerung von Windows-10/11-Updates mit Gruppenrichtlinien 1070
 - 36.3.2 Konfiguration der Übermittlungsoptimierung 1070
 - 36.3.3 Update-Funktionen in Windows 10/11 verstehen 1072
 - 36.3.4 Windows-Updates in Windows 10/11 steuern 1072
 - 36.3.5 Windows 10/11 und WSUS 1073
 - 36.3.6 Probleme bei der Installation von Updates beheben 1074
 - 36.4 Patchverwaltung mit WSUS 1075
 - 36.4.1 Clientcomputer über Gruppenrichtlinien anbinden 1076
 - 36.4.2 Einstellungen für Windows 10/11 korrekt setzen 1079
 - 36.4.3 Updates genehmigen und bereitstellen 1081
 - 36.4.4 Berichte mit WSUS abrufen 1083
 - 36.5 WSUS in Windows Server 2025 überwachen 1083
 - 36.5.1 Überprüfung der Gruppenrichtlinien 1083
 - 36.5.2 In der Befehlszeile nach Problemen suchen 1084
 - 36.5.3 SSL-Port beachten 1084
 - 36.5.4 Diagnostic Tool for the WSUS Agent 1085
 - 36.5.5 WSUS mit der PowerShell verwalten 1085
 - 36.6 Azure Update Management für das Patchmanagement nutzen 1086
 - 36.7 Zusammenfassung 1087
- Kapitel 37 Diagnose und Überwachung 1089**
 - 37.1 Fehlerbehebung in Windows Server – Ereignisanzeige 1089
 - 37.1.1 Ereignisanzeige nutzen 1089
 - 37.1.2 Ereignisprotokolle im Netzwerk einsammeln 1093
 - 37.2 Überwachung der Systemleistung 1099
 - 37.2.1 Die Leistungsüberwachung 1100
 - 37.2.2 Indikatorendaten in der Leistungsüberwachung beobachten 1103
 - 37.2.3 Sammlungssätze nutzen 1104
 - 37.2.4 Speicherengpässe beheben 1104
 - 37.2.5 Prozessorauslastung messen und optimieren 1107
 - 37.2.6 Der Task-Manager als Analysewerkzeug 1108
 - 37.2.7 Laufwerke und Datenträger überwachen – Leistungsüberwachung und Zusatztools 1110

37.3	Serverüberwachung mit dem Windows Admin Center	1111
37.3.1	Neuen Arbeitsbereich erstellen	1112
37.3.2	Workspace speichern, herunterladen und hochladen	1113
37.4	Aufgabenplanung – Windows automatisieren	1114
37.4.1	Aufgabenplanung verstehen	1114
37.4.2	Erstellen einer neuen Aufgabe	1117
37.5	Prozesse und Dienste überwachen	1118
37.5.1	Dienste in der PowerShell verwalten	1118
37.5.2	Dateisystem, Registry und Prozesse überwachen – Sysinternals Process Monitor ..	1122
37.5.3	Laufende Prozesse analysieren – Process Explorer	1125
37.5.4	Wichtige Informationen immer im Blick – BgInfo	1129
37.5.5	Systeminformationen in der Eingabeaufforderung anzeigen – PsInfo	1131
37.6	Zusammenfassung	1132
Kapitel 38	Windows PowerShell	1133
38.1	PowerShell 7 für Windows, macOS und Linux	1133
38.1.1	Kompatibilität der PowerShell 7 mit der PowerShell 5.x	1134
38.1.2	PowerShell 7 installieren	1135
38.1.3	Pipelines mit der PowerShell 7 und weitere neue Funktionen	1136
38.2	Wissenswertes zur PowerShell in Windows Server 2025	1136
38.2.1	Einstieg in die PowerShell und Eingabeaufforderung	1138
38.3	PowerShell und PowerShell ISE – Eine Einführung	1140
38.3.1	Mit der PowerShell ISE effizient arbeiten	1141
38.3.2	Einstieg in die PowerShell	1141
38.3.3	Die PowerShell über das Netzwerk nutzen	1142
38.4	Die grundsätzliche Funktionsweise der PowerShell	1143
38.4.1	Einstieg in die Befehle der PowerShell	1143
38.4.2	Patches und Datensicherungen verwalten	1144
38.4.3	Registry und Co. mit der PowerShell verwalten	1144
38.4.4	Die PowerShell-Laufwerke verwenden	1145
38.4.5	Skripts mit der PowerShell erstellen	1147
38.5	Mit PowerShell Desired State Configuration Windows-Server absichern	1148
38.5.1	MOF-Dateien für DSC erstellen und umsetzen	1149
38.5.2	MOF-Dateien erweitern	1150
38.6	Windows PowerShell zur Administration verwenden	1151
38.6.1	PowerShell Direct – Virtuelle Betriebssysteme steuern	1151
38.6.2	Software im Netzwerk verteilen	1152
38.6.3	Software mit Chocolatey installieren und aktuell halten	1153
38.6.4	Chocolatey installieren, aktualisieren und nutzen	1153
38.6.5	Software mit der ChocolateyGUI installieren	1154
38.6.6	Grundlagen zur Verwaltung von Servern mit der PowerShell	1154
38.6.7	Mit Variablen arbeiten	1155
38.6.8	Systemprozesse verwalten	1155
38.6.9	Dateien und Objekte kopieren, löschen und verwalten	1156
38.6.10	Dienste in der PowerShell und Befehlszeile steuern	1158
38.6.11	Aus der PowerShell E-Mails schreiben	1158
38.6.12	Windows-Firewall in der PowerShell steuern	1159
38.7	Eingabeaufforderung verwenden	1162
38.8	Batchdateien für Administratoren	1166
38.8.1	Grundlagen zu Batchdateien	1166
38.8.2	Netzwerkverwaltung in der Befehlszeile	1166

38.8.3 Sprungmarken und Warte-Befehle	1167
38.8.4 Wenn/Dann-Abfragen nutzen	1167
38.8.5 Informationen zum lokalen Server abrufen	1168
38.8.6 Schleifen und Variablen	1169
38.9 WMI-Abfragen nutzen	1170
38.10 Zusammenfassung	1172
Index	1173

Microsoft Windows Server 2025

Diese komplett überarbeitete und aktualisierte Auflage des Klassikers zu Windows Server gibt Ihnen einen tiefgehenden Einblick in den praktischen Einsatz von Windows Server 2025. Das Buch richtet sich sowohl an Neueinsteiger*innen in Microsoft-Servertechnologien als auch an Umsteiger*innen von Vorgängerversionen. Planung und Migration, Konzepte und Werkzeuge der Administration sowie die wichtigsten Konfigurations- und Verwaltungsfragen werden praxisnah behandelt.

Alle wichtigen Funktionen werden ausführlich vorgestellt, ebenso die effiziente Zusammenarbeit mit Windows 10/11-Clients. Es erwarten Sie über 1000 Seiten praxisnahes und kompetentes Insiderwissen mit vielen hilfreichen Anleitungen und Profitipps.

Aus dem Inhalt:

- Alle Neuerungen von Windows Server 2025 und Änderungen im Vergleich zu Windows Server 2022
- Lizenzierung und Installation
- Verwalten von Datenträgern und Speicherpools, Hochverfügbarkeit, Datensicherung und -wiederherstellung
- Secured Core Server, Secure DNS und weitere Sicherheitsneuerungen in der Praxis
- Lokale Rechenzentren an Microsoft Azure anbinden
- Betreiben und Erweitern von Active Directory
- Verwaltung mit dem Windows Admin Center
- Hochverfügbarkeit und Lastenausgleich
- Windows Server Update Services (WSUS)
- Diagnose und Überwachung für System, Prozesse und Dienste
- Viele neue PowerShell-Befehle für die Verwaltung von Windows Server 2025
- Windows Server Container, Docker und Hyper-V-Container
- Virtualisierung mit Hyper-V
- Fehlerbehebung und Troubleshooting

Thomas Joos

ist selbstständiger IT-Consultant und seit über 20 Jahren in der IT-Branche tätig. Er schreibt Fachbücher und berät Unternehmen in den Bereichen Active Directory, Exchange Server und IT-Sicherheit. Durch seinen praxisorientierten und verständlichen Schreibstil sind seine Fachbücher für viele IT-Profis eine wichtige Informationsquelle geworden. Neben vielen erfolgreichen Büchern schreibt er für zahlreiche IT-Publikationen wie z. B. c't, Computerwoche und IT-Administrator sowie für LinkedIn. Seinen Blog finden Sie auf

thomasjoos.wordpress.com.



9 783960 092520

www.dpunkt.de

Euro 69,90 (D)
ISBN 978-3-96009-252-0



Gedruckt in Deutschland
Mineralölfreie Druckfarben
Zertifiziertes Papier