
Karsten Bratvogel, Thomas Joos

1. Ausgabe, März 2022

ISBN 978-3-98569-054-1

Windows Server 2022

Netzwerkadministration

W2022N

HERDT

1 Informationen zu diesem Buch und zur virtuellen Testumgebung	4	7 Active Directory installieren	63
1.1 Voraussetzungen und Ziele	4	7.1 Installation vorbereiten	63
1.2 Netzwerk in der Testumgebung	5	7.2 Stammdomäne einrichten	64
1.3 Namensgebung in diesem Buch	6	7.3 Domänencontroller zur Domäne hinzufügen	71
1.4 Aufbau und Konventionen	8	7.4 Active Directory erkunden	73
2 Windows Server 2022	10	8 DNS	78
2.1 Editionen des Windows Servers 2022	10	8.1 Domänennamespace	78
2.2 Virtualisierung	12	8.2 Namensauflösung	80
2.3 Verzeichnisdienste	14	8.3 Global Names	81
2.4 Sicherheitsfunktionen	15	8.4 Dynamisches DNS	81
2.5 Verwaltungsfunktionen	16	8.5 Zonen	82
2.6 Skalierbarkeit, Zuverlässigkeit, Hardwareunterstützung	17	8.6 Zonenübertragung	85
2.7 Netzwerkinfrastruktur	18	8.7 Zonendelegierung verstehen	86
2.8 Dateiverwaltung, Dateisystem	19	8.8 Aufbau der DNS-Datenbank	87
3 Installation	20	9 DNS-Dienst einrichten und konfigurieren	89
3.1 Vorüberlegungen zur Installation	20	9.1 Domänennamespace für die Testumgebung	89
3.2 Informationen für die Installation sammeln und auswerten	22	9.2 TCP/IP konfigurieren für DNS	89
3.3 Die Installation vorbereiten	24	9.3 DNS-Dienst installieren	94
3.4 Windows Server 2022 installieren	26	9.4 DNS-Dienst konfigurieren	95
3.5 Upgrade von Standard- und Testversion auf Datacenter-Edition	28	9.5 Zoneneigenschaften bearbeiten	99
3.6 Erstkonfiguration des Hostrechners	28	9.6 Sekundäre Zone einrichten	101
4 Bedienung und Neuerungen	33	9.7 DNS-Serverdienst testen	101
4.1 Startmenü	33	10 DHCP – Dynamische IP-Konfiguration	104
4.2 Windows Server 2022 mit Tastenkombinationen bedienen	34	10.1 TCP/IP	104
4.3 Server-Manager	34	10.2 Vergabe von IP-Adressen	106
5 Hyper-V-Testumgebung	36	10.3 Dynamic Host Configuration Protocol (DHCP)	107
5.1 Virtualisierung	36	10.4 DHCP-Server installieren	108
5.2 Hyper-V einsetzen	38	10.5 DHCP-Server konfigurieren	109
5.3 Hyper-V installieren	39	11 Physische Struktur von Active Directory	118
5.4 Hyper-V einrichten	41	11.1 Standorte und Standortplanung	118
5.5 Virtuellen Computer einrichten	45	11.2 Replikation innerhalb eines Standorts	119
5.6 Virtuellen Computer verwalten	48	11.3 Replikation zwischen Standorten	120
6 Active Directory	54	11.4 Replikationskomponenten	121
6.1 Überblick Verzeichnisdienst	54	11.5 Replikationstopologie	122
6.2 Domäne, Struktur und Gesamtstruktur	54	12 Active Directory-Objekte verwalten	123
6.3 Funktionsebenen	56	12.1 Container der Domäne erkunden	123
6.4 Domänencontroller, Betriebsmaster und globaler Katalog	58	12.2 Planung einer Domäne	124
6.5 Organisationseinheit – OU	60	12.3 Entwurf für die Domäne <i>firma.intern</i>	126
6.6 Standorte im Active Directory	61	12.4 Organisationseinheiten erstellen	126
6.7 Sysvol – Ressourcen für Anmeldungen	62	12.5 Benutzerkonten	129
		12.6 Benutzerkonto erstellen	131
		12.7 Objektnamen im Active Directory	133
		12.8 Computerkonto erstellen	137

13 Benutzer und Gruppen	139	19 Dateidienste planen	193
13.1 Benutzer und Kontakte	139	19.1 Gründe für zentrale Datenspeicherung	193
13.2 Gruppentypen	139	19.2 Dateistruktur planen	194
13.3 Gruppenbereiche	141	19.3 Verzeichnisstruktur anlegen	195
13.4 Gruppenhierarchien einsetzen	142		
13.5 Gruppenplanung	144	20 Gruppenrichtlinien	197
14 Gruppen verwalten	146	20.1 Einsatzbereiche von Gruppenrichtlinien	197
14.1 Gruppenplanung mit globalen und lokalen Gruppen	146	20.2 Gruppenrichtlinienobjekt	200
14.2 Globale Gruppe erstellen und verwalten	147	20.3 Verarbeitung der Gruppenrichtlinien-einstellungen	200
14.3 Lokale Gruppe erstellen und verwalten	148	20.4 Gruppenrichtlinienberechtigungen	201
14.4 Gruppenplanung mit universalen Gruppen	149	20.5 Vererbung von Gruppenrichtlinien	202
14.5 Universale Gruppen erstellen	150	21 Sicherheitsrichtlinien einsetzen	203
14.6 Gruppen mit einer Batchdatei anlegen	151	21.1 Gruppenrichtlinienverwaltung	203
15 Rechte und Berechtigungen	157	21.2 Sicherheitsrichtlinien für Domänencontroller bearbeiten	205
15.1 Definitionen	157	21.3 Domänenrichtlinien bearbeiten	207
15.2 Vererbung von Berechtigungen	160	21.4 Zusätzliche Kontorichtlinie erstellen	211
16 Active Directory-Berechtigungen verwalten	161	22 Gruppenrichtlinien verwalten	214
16.1 Objektverwaltung	161	22.1 Gruppenrichtlinienimplementierung planen	214
16.2 Berechtigungen und Berechtigungsvererbung überprüfen und verwalten	161	22.2 Test-OU erstellen	215
16.3 Objektverwaltung delegieren	163	22.3 Gruppenrichtlinien implementieren	217
16.4 Verwaltungstools für die Objektverwaltung	166	22.4 Gruppenrichtlinien testen	221
16.5 Konsole mit Aufgabenblock erzeugen	167	22.5 Gruppenrichtlinienergebnisse	223
17 Berechtigungen anpassen	170	22.6 Gruppenrichtlinien bearbeiten	224
17.1 NTFS-Berechtigungen	170	23 Notfallsicherung	225
17.2 Freigabeberechtigungen für Ordner	176	23.1 Strategien und Wiederherstellungsfunktionen	225
17.3 Berechtigungen für Drucker	176	23.2 Fehlertolerante Datenträger	225
17.4 Freigaben und Drucker veröffentlichen	177	23.3 Erweiterte Startoptionen	226
18 Dateidienste	179	23.4 Systemstatusdaten	228
18.1 Ordner-Freigaben	179	23.5 Der Active Directory-Papierkorb	228
18.2 Dateidienste installieren	180	23.6 Windows-Speicherdiagnose	230
18.3 Freigabe- und Speicherverwaltung	182	Stichwortverzeichnis	232
18.4 Ressourcen-Manager für Dateiserver	185		
18.5 Versionierung und Deduplizierung	190		
18.6 Weitere Techniken zur Bereitstellung von Dateien	191		

1 Informationen zu diesem Buch und zur virtuellen Testumgebung

1.1 Voraussetzungen und Ziele

Zielgruppe

Dieses Buch richtet sich in erster Linie an Systembetreuer und Administratoren. Die Kursteilnehmer können neu in die Administration von Netzwerken mit Windows Server 2022 einsteigen oder bereits Erfahrungen im Umgang mit früheren Serverbetriebssystemen von Microsoft gesammelt haben. Das Buch ist jedoch auch für Teilnehmer geeignet, die nachfolgend umrissene Vorkenntnisse anderweitig erworben haben.

Empfohlene Vorkenntnisse

Bei den Kursteilnehmern werden folgende Kenntnisse vorausgesetzt:

- ✓ Erfahrungen in der Betreuung von Client-Computern unter Windows
- ✓ Grundzüge der IP-Adressierung und die Bedeutung des DHCP-Servers für die Vergabe von IP-Adressen an Client-Computer

Lernziele

Nach Durcharbeiten dieses Buches kann der Teilnehmer einen Windows Server 2022 installieren und zum Domänencontroller heraufstufen. Er kann die Aufgaben und Elemente des Active Directory erläutern und die wesentlichen Verwaltungstätigkeiten ausüben. Dazu gehören Benutzer- und Gruppenverwaltung, Ressourcenverwaltung im Netzwerk und der Einsatz von Gruppenrichtlinien. Er kann ferner Methoden für die Notfallabsicherung sowie die Wiederherstellung eines Servers und seiner Daten benennen und anwenden.

Zusätzlich kann der Teilnehmer mittels Hyper-V eine Serverumgebung virtualisieren, sowohl für den Einsatz in Testumgebungen als auch für den Produktiveinsatz.

Hinweise zu Soft- und Hardware

Für den Aufbau der Testumgebung, die diesem Buch zugrunde liegt, benötigen Sie einen Computer mit folgender Hard- und Software:

Computer	Einen 64-Bit-Computer mit mindestens 8 GB Hauptspeicher (je 2 GB für Desktopoberfläche) und 128 GB (4 x 32 GB je Betriebssystem) freier Festplattenkapazität. Das System sollte von DVD-ROM oder USB booten können. Für die Virtualisierung mit Hyper-V muss das System über die Virtualisierungsfunktion AMD-V bzw. Intels VT-x verfügen. Sowohl die CPU als auch das BIOS müssen diese Funktion beherrschen. Alle Computer müssen für Windows Server 2022 geeignet sein (Angaben zu den Systemvoraussetzungen finden Sie in Kapitel 3). Für den Aufbau der Szenarios aus dem HERDT-Buch <i>Windows Server 2022 – Erweiterte Netzwerkadministration</i> benötigen Sie zusätzlichen Speicherplatz von mindestens 80 GB.
Software	Installations-Datenträger Windows Server 2022 (DVD, ISO-Abbild oder bootfähiger USB-Stick)

1.2 Netzwerk in der Testumgebung

Testumgebung mit einem Hostserver und drei virtuellen Maschinen

Die Testumgebung sieht die Einrichtung eines Hostsystems unter Windows Server 2022 vor, auf dem dann über Hyper-V drei virtuelle Maschinen aufgesetzt werden. Der Host ist dabei nicht Teil der virtuellen Firma und auch kein Domänenmitglied. Durch die vollständige Virtualisierung der Testumgebung wird erreicht, dass Sie von allen beteiligten virtuellen Servern Momentaufnahmen (Snapshots) anfertigen können, zu denen Sie später zurückkehren können. Ein weiterer Vorteil ist die vollständige Trennung des virtuellen Netzes von der Außenwelt, sodass mehrere Kursteilnehmer unabhängig voneinander arbeiten können.

Es ist möglich, ein anderes Betriebssystem wie z. B. Linux oder macOS für den Host zu verwenden und Virtualisierungssoftware von anderen Herstellern (z. B. VMware oder VirtualBox von Oracle/Sun) einzusetzen. Diese Alternativen werden jedoch im Buch nicht beschrieben, außerdem gehört der Umgang mit Hyper-V zu den zentralen Inhalten.

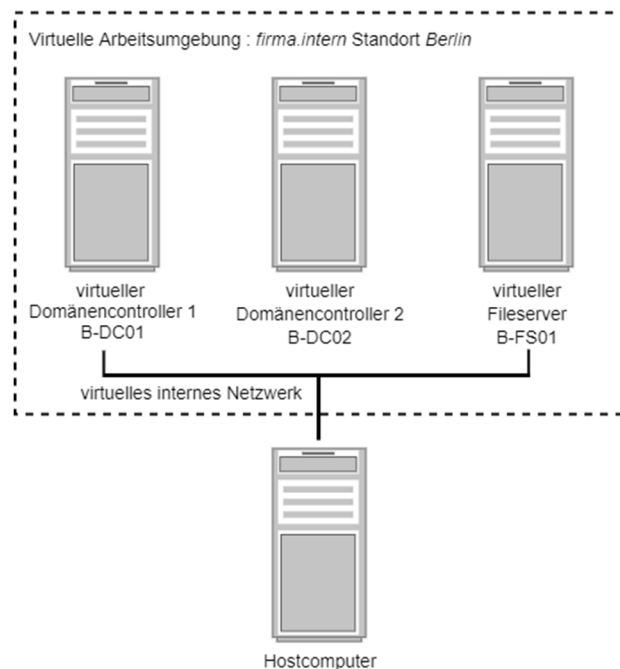


Dieses Buch enthält alles, was Sie für die grundlegende Einrichtung des Netzwerks einer Firma mit einer einzelnen Niederlassung benötigen. In der Testumgebung wird daher eine Domäne am Standort Berlin eingerichtet werden, an dem sich drei Server befinden.

Die Testumgebung wird Schritt für Schritt aufgebaut:

- ✓ Installation des Hosts und Hinzufügen der Serverrolle *Hyper-V*
- ✓ Installation des ersten Domänencontrollers *B-DC01*
- ✓ Einrichtung der Domäne *firma.intern*
- ✓ Installation des zweiten Domänencontrollers *B-DC02*
- ✓ Installation des Dateiservers *B-FS01*

Im HERDT-Buch *Windows Server 2022 – Erweiterte Netzwerkadministration* wird die Testumgebung um weitere Standorte und zusätzliche Serverrollen und Funktionen erweitert, die in diesem Buch erstellten Server werden dabei weiterverwendet.



Testumgebung mit drei virtuellen Servern

Namenskonventionen im Schulnetz

Falls Sie Ihre Testumgebung im Rahmen einer Schulung erstellen, richten Sie sich bei der Wahl von Standorten und IP-Adressen nach den Vorgaben Ihres Kursleiters.

Vorschläge für die Testumgebung

Die virtuellen Umgebungen ermöglichen es jedem Kursteilnehmer, eine identische Versuchsumgebung aufzubauen. Dabei gibt es Folgendes zu bedenken:

- ✓ Alle Teilnehmer sollten bei der Namensvergabe dasselbe Schema benutzen. Durch die konsequente Bezeichnung können alle Ressourcen stets eindeutig zugeordnet werden.
- ✓ Halten Sie den Aufbau der Testumgebung einfach. Eine komplizierte Umgebung schafft zusätzliche Fehlerquellen.

- ✓ Im Buch wird die Domäne *firma.intern* heißen. Jeder Teilnehmer sollte jedoch als Domänennamen seinen Firmennamen, Nachnamen oder einen anderen Namen verwenden, der im Schulungsnetzwerk einmalig ist. Befolgen Sie bei der Auswahl des Domänennamens die Vorgaben des Kursleiters.
- ✓ Achten Sie darauf, dass der Domänenname den Bestandteil *intern* enthält, z. B. *firma.intern*. Da die Domäne *intern* nicht im Internet-DNS registriert werden kann, handelt es sich automatisch um einen internen Domänennamen für das firmeneigene Netzwerk.
- ✓ Beachten Sie die Namenskonventionen. Ein Rechnername sollte maximal 15 Zeichen umfassen. Benennen Sie in Hyper-V die virtuellen Maschinen nach dem Schema *V-<Name des virtuellen Servers>*. So können Sie am Fenstertitel sofort erkennen, in welcher VM Sie sich gerade befinden.

1.3 Namensgebung in diesem Buch

In diesem Buch wird auf eine durchgehende Bezeichnungsweise geachtet. Alle Bezeichnungen sollten **aussagekräftige Namen** enthalten, aus denen die Funktion hervorgeht. Das mag zunächst aufwendig und kompliziert erscheinen, jedoch werden Sie für eindeutige Bezeichnungen sehr dankbar sein, wenn Sie einmal mit einem fremden Active Directory oder Skript arbeiten müssen. Wenn Sie das nachfolgend beschriebene Schema anwenden, können Sie alleine durch die Bezeichnung erkennen, ob es sich um einen Rechnernamen, eine Gruppe oder eine Organisationseinheit handelt, egal in welchem Kontext Sie das Objekt vorfinden.

Am Anfang einer Bezeichnung muss das wichtigste Ordnungsmerkmal stehen, das in einer alphabetisch geordneten Liste dafür sorgt, dass zusammengehörige Einträge auch zusammen aufgeführt werden. Bei Computernamen ist dies der Standort, während es bei Gruppen, Organisationseinheiten und Ressourcen oft sinnvoller ist, sie nach ihrer Funktion zu benennen. Sie können diese Kriterien selbst festlegen, wichtig ist vor allem, dass dabei eine sinnvolle Hierarchie entsteht, an die Sie sich durchgängig halten.

Bindestriche als Trennzeichen

Alle Bezeichnungen werden aus mehreren Bestandteilen zusammengesetzt, die jeweils mit einem Bindestrich (bzw. einem Minuszeichen) voneinander getrennt werden. Verwenden Sie wenn möglich **innerhalb** eines Namensbestandteils keine Minuszeichen.

Keine Leerzeichen

Ersetzen Sie alle Leerzeichen in Bezeichnungen und Namensbestandteilen durch einen Unterstrich. Dadurch sehen Sie auf einen Blick, wo ein Element aufhört und das nächste anfängt, außerdem können Sie so in der Eingabeaufforderung oder der PowerShell und in Skripten auf Anführungszeichen verzichten.

Keine Umlaute

Verzichten Sie grundsätzlich auf die Verwendung von Umlauten und Sonderzeichen, denn so haben Sie auch in internationalen Umgebungen keine Probleme.

Benutzernamen

Die Anmeldenamen werden im Buch durch den Anfangsbuchstaben des Vornamens und den vollen Nachnamen gebildet. Dabei wird auf Umlaute und Sonderzeichen verzichtet. In der Praxis sind aber auch Kombinationen aus Buchstaben und Zahlen üblich (z. B. Personalnummern, generische Namen), die von Namensänderungen (Eheschließung, Scheidung, etc.) unbeeinträchtigt bleiben.

Autokennzeichen als Standortkürzel

Für die Kennzeichnung des Standorts kann, wie in diesem Beispiel, das Autokennzeichen der Stadt verwendet werden, auch wenn dies bei einer Firma mit nur einem Standort zunächst unnötig erscheint. Auf diese Weise sind Sie auf spätere Erweiterungen der Firma vorbereitet. Alternativ kann der Standort beispielsweise auch mit Buchstaben oder Zahlenkombinationen (Abkürzung des Städtenamens/Vorwahlen/Postleitzahlen) kenntlich gemacht werden. Wichtig ist jedoch, dass diese einheitlich und durchgängig verwendet werden.

Rechnernamen

Alle Rechnernamen beginnen mit dem Standortkürzel. Danach kommt eine Abkürzung für die Hauptfunktion des Servers: **DC** für Domain Controller, **FS** für File Server, direkt gefolgt von einer zweistelligen laufenden Nummer. Dabei ergeben sich Bezeichnungen wie z. B. *B-DC02*, *R-FS01* oder *HB-DC01*. Client-Computer werden z. B. als *B-PC01* benannt.

Durch das Voranstellen des Standortnamens werden alle Computer am Standort in einer alphabetisch geordneten Liste zusammenhängend angezeigt. Durch die fortlaufende Nummerierung werden automatisch alle Rechner mit der gleichen Hauptfunktion (DC, FS usw.) an einem Standort untereinander angezeigt.

Namen der virtuellen Maschinen

Die VMs tragen den Namen des virtuellen Computers mit vorangestelltem V für virtuell, z. B. *V-B-DC02*. Dadurch können die Hyper-V-VMs von den Servern in der Testumgebung unterschieden werden.

Organisationseinheiten

Alle Organisationseinheiten (organizational units) beginnen mit OU, damit man sofort erkennt, worum es sich handelt.

Gruppen

Bei allen Gruppen wird die Art der Gruppe vorangestellt:

- ✓ LG für lokale Gruppen
- ✓ GG für globale Gruppen
- ✓ UG für universale Gruppen
- ✓ SG für Sammelgruppen
- ✓ VG für Verteilergruppen
- ✓ SGV für Sammel-Verteilergruppen

Sonstige Abkürzungen

- ✓ Alle Freigaben und Abteilungslaufwerke beginnen mit *LW_* für Laufwerk.
- ✓ Lokale Gruppen für die Laufwerke tragen am Ende des Namens ein Kürzel für die Berechtigungen: L für Lesen, AE für Ändern, VZ für Vollzugriff.

Denkbar sind auch Kombinationen mit englischen Zugriffskennzeichnungen (r, w, rw, f) oder Gruppenzusätze, die die Funktion erkennen lassen (z. B. Access-Groups, Application-Groups, Admin-Groups, u. v. m.)

Abteilungsnamen und Mitarbeitergruppen

Bezeichnungen im Active Directory können ruhig etwas länger sein, daher sollten Sie die Bezeichnung von Abteilungen und Personengruppen ausschreiben. Wenn Sie die vollständige Bezeichnung verwenden, müssen Sie sich auch keine Abkürzung merken. Schreiben Sie also *Buchhaltung* statt *BuchH*, *Verwaltung* statt *Verw* und *Abteilungsleiter* statt *AbtL* oder *AL* (*AL* könnte zum Beispiel auch *Abteilungslaufwerk* bedeuten).

Das soll nicht heißen, dass Sie gar keine Abkürzungen verwenden dürfen, sie müssen bloß eindeutig und unverwechselbar sein.

In diesem Buch werden Abkürzungen zum Beispiel für Städtenamen, Gruppen, Abteilungslaufwerke und Zugriffsberechtigungen verwendet.

Betrachten Sie zum besseren Verständnis die folgenden Beispiele für den Standort *Berlin*:

<i>V-B-DC01</i>	Bezeichnung für die Hyper-V-VM, außerdem Bezeichnung für die virtuelle Festplattendatei
<i>B-DC01</i>	Computername des virtuellen Computers, hier der erste Domänencontroller
<i>OU-Berlin</i>	Dies ist die Organisationseinheit für den Standort <i>Berlin</i> . Darin befinden sich alle weiteren Unter-OUs.
<i>OU-B-Verwaltung</i>	Organisationseinheit für die Verwaltungsabteilung in Berlin; diese ist eine Unter-OU von <i>OU-Berlin</i> .
<i>GG-B-Verwaltung-Abteilungsleiter</i>	Globale Gruppe (GG) für den Standort Berlin (B), für die Abteilungsleitung von Verwaltung
<i>LG-B-LW_Verwaltung-L</i>	Lokale Gruppe (LG) in Berlin (B) für das Abteilungslaufwerk (LW_) der Verwaltung mit Lesen-Berechtigungen (L)
<i>B-LW_Verwaltung</i>	Name des Freigabeordners auf dem Dateiserver für das Abteilungslaufwerk
<i>SG-B-Abteilungsleiter</i>	Sammelgruppe für alle Abteilungsleiter am Standort <i>Berlin</i>
<i>SGV-B-Buchhaltung</i>	Sammel-Verteilergruppe (z. B. für E-Mails) mit allen Mitarbeitern der Buchhaltung

1.4 Aufbau und Konventionen

Aufbau des Buchs

Soweit möglich wechseln sich Theoriekapitel und Kapitel mit praktischen Anweisungen und Übungen ab. Bei einzelnen Kapiteln kann jedoch aus didaktischen Gründen von diesem Prinzip abgewichen werden.

Inhaltliche Gliederung

In diesem Buch wird der schrittweise Aufbau einer Gesamtstruktur mit einer Domäne unter Windows Server 2022 behandelt. Die Domäne verfügt über einen Standort mit drei Servern. Die Installation der Server wird dabei auf virtuellen Maschinen durchgeführt, kann jedoch mit Einschränkungen auch auf mehreren physischen Computern erfolgen. Darüber hinaus werden Strategien und Arbeitsabläufe für ausgewählte Verwaltungsaufgaben vorgestellt.

Theoriekapitel widmen sich dem Aufbau des Netzwerks und stellen die grundlegenden Windows-Konzepte vor. Es folgen Übungskapitel mit detaillierten Arbeitsanleitungen zum Ausführen der zuvor behandelten Konfigurationsmaßnahmen. Zielsetzung dieses Buches ist das Lernen und Üben beim Aufbau einer Windows-Server-2022-Testumgebung.

Typografische Konventionen

Im Text erkennen Sie bestimmte Programmelemente an der Formatierung:

<i>Kursivschrift</i>	kennzeichnet Programmelemente wie Register oder Schaltflächen.
<code>Courier</code>	wird für Benutzereingaben und Systembefehle verwendet.
Spitze Klammern <>	kennzeichnen Platzhalter.

Was bedeuten die Symbole im Buch?



Praxistipp



Warnhinweis

Weitere Medien von HERDT nutzen

Hat Ihnen das vorliegende Buch gefallen, besuchen Sie doch einmal unseren Webshop unter www.herd.com. Sie möchten beispielsweise Ihre ...

- ✓ Administrationskenntnisse erweitern. Hierzu empfehlen wir Ihnen das folgende HERDT-Buch aus der Windows-Server-2022-Reihe, das auf diesem Buch aufbaut:
 - ✓ *Windows Server 2022 – Erweiterte Netzwerkadministration*
- ✓ Netzwerkkennnisse vertiefen. Dazu bietet Ihnen der HERDT-Verlag folgende Bücher an:
 - ✓ *Netzwerke – Grundlagen*
 - ✓ *Netzwerke – Netzwerktechnik*
 - ✓ *Netzwerke – Sicherheit*
 - ✓ *Netzwerke – IPv6 Internet Protocol Version 6*

2 Windows Server 2022

2.1 Editionen des Windows Servers 2022

Unterschiedliche Einsatzbereiche und Anforderungen

Windows Server 2022 ist, ebenso wie seine Vorgängerversionen (z. B. Windows Server 2019, 2016, 2012/2012 R2), ein reines 64-Bit-Betriebssystem. Es ist das Server-Pendant zu Windows 10 / 11 und unterstützt die Funktionen und Oberflächen der Windows Client-Betriebssysteme. Für die volle Unterstützung von Windows 11 müssen entsprechende ADMX Templates nachinstalliert sein. Die Windows 11 Templates finden Sie hier:

- ✓ <https://www.microsoft.com/en-us/download/details.aspx?id=103507>

Auf der offiziellen Webseite (<https://docs.microsoft.com/de-de/windows-server/get-started/editions-comparison-windows-server-2022>) zieht die Firma Microsoft einen Vergleich zwischen den Windows Server 2022 Editionen Standard, Datacenter und Datacenter Azure Edition und verzichtet hierbei auf die Darstellung der Merkmale des ebenfalls erhältlichen Windows Server 2022 Essentials. Die als Editionen bezeichneten Ausführungen des Server-Betriebssystems unterscheiden sich in der maximal unterstützten Hardware und den installierbaren Rollen/Features und sollten nicht mit den Windows-Versionen wie z. B. Windows 7, 10 oder 11 verwechselt werden.

Editionsübersicht von Windows Server 2022 und gemeinsame Anforderungen

Allen Editionen gemeinsam sind die Mindestanforderungen:

- ✓ 64-Bit-Prozessor mit mindestens 1,4 GHz und Unterstützung verschiedener Prozessorfunktionen
- ✓ 512 MB RAM (2 GB für die Installation der grafischen Oberfläche)
- ✓ wenigstens 32 GB freier Festplattenplatz
- ✓ 1 Gbit Netzwerkkarte
- ✓ DVD-Laufwerk oder Boot-Funktion von USB
- ✓ SVGA-Grafik, Tastatur/Maus

Die empfohlenen Hardwarevoraussetzungen richten sich nach den Aufgaben und liegen deutlich darüber. Angaben zu den genauen Anforderungen an die Hardware finden Sie unter dem nachfolgenden Link:

- ✓ <https://docs.microsoft.com/de-de/windows-server/get-started/hardware-requirements>

Edition	Einsatzgebiet
Windows Server 2022 Essentials	<ul style="list-style-type: none"> ✓ Für Firmen bis 25 Benutzer / 50 Geräte (keine Client Access Licences (CALs) erforderlich) ✓ Führt die Reihe von Server Essentials als Ersatz für den früheren Small Business Server fort ✓ Reduzierter Funktionsumfang, keine Virtualisierung, 1 x CPU mit max. 10 Kernen ✓ keine eigene Oberfläche, keine Essentials-spezifischen Funktionen mehr ✓ Vorkonfigurierte Cloud-Anbindung ✓ Keine Exchange-Lizenz inbegriffen
Windows Server 2022 Standard	<ul style="list-style-type: none"> ✓ Variante mit Standardfunktionalität ✓ Lizenzen für zwei Virtualisierungsinstanzen inbegriffen ✓ Unbegrenzte Anzahl von Kernen und max. 48 TB RAM

Edition	Einsatzgebiet
Windows Server 2022 Datacenter	<ul style="list-style-type: none"> ✓ Für den Einsatz in großen Unternehmen und Organisationen mit vielen virtuellen Maschinen konzipiert ✓ Unbegrenzte Anzahl von Lizenzen für Virtualisierungsinstanzen ✓ Keine Einschränkung der Rollen/Feature ✓ Unbegrenzte Anzahl von Kernen und max. 48 TB RAM
Windows Server 2022 Datacenter Azure Edition	<ul style="list-style-type: none"> ✓ Für den Einsatz in großen Unternehmen und Organisationen konzipiert. Betrieb als virtuelle Maschine auf Azure IaaS (Infrastructure as a Service) oder Azure Stack HCI Cluster (Hyper Converged Infrastructure) ✓ Keine Einschränkung der Rollen/Feature ✓ Erweitertes Azure-Netzwerk ✓ Hotpatching ✓ SMB über QUIC

HCI stellt Arbeitsspeicher, Rechenleistung und Massenspeicher auf Basis von Standardhardware in virtuellen Maschinen bereit. Mithilfe intelligenter Steuerungssoftware entstehen optimal passende Systemumgebungen, die über gemeinsam verwendete Speicherlaufwerke gegen Ausfall (z. B. im Failover Cluster) abgesichert werden können (vgl. https://de.wikipedia.org/wiki/Hyperkonvergente_Infrastruktur).

Server Message Blocks (SMB) ist das Standardzugriffsprotokoll für Windows Netzwerkfreigaben. Wird SMB über QUIC (ein IETF-standardisiertes Protokoll) anstelle von TCP transportiert, wird die Verbindung zwischen den Endsystemen verschlüsselt (vgl. <https://de.wikipedia.org/wiki/QUIC>).

Einen vollständigen Vergleich der Editionen Standard, Datacenter und Datacenter für Azure finden Sie hier:

- ✓ <https://docs.microsoft.com/de-de/windows-server/get-started/editions-comparison-windows-server-2022>

SAC- und LTSC-Versionen

Mit der Einführung von Windows Server 2022 hat Microsoft eine Änderung des halbjährlichen Semi-Annual-Channel (SAC) angekündigt. Bisher wurden alle 6 Monate neue Versionen veröffentlicht, die auch häufig neue Funktionen implementierten. Einer der Gründe für diese Bereitstellung waren neue Container- und Microservices, die nun im Azure Stack HCI angesiedelt sind. Hier bleibt es bei den halbjährigen Updates. Somit verfügt Windows Server 2022 nur noch über einen Long Term Servicing Channel (LTSC), der den Support für maximal zehn Jahre (5 Jahre Mainstream Support / 5 Jahre Extended Support) sicherstellt.

Bei Windows Server 2022 handelt es sich um die nächste Vollversion, die Microsoft im Rahmen des LTSC zur Verfügung stellt. Die Veröffentlichung von Windows Server 2022 stellt die Ablösung von Windows Server 2019 als aktuelle LTSC-Version dar.

Standardinstallation mit grafischer Oberfläche

Dies ist die klassische Installationsart mit Windows-Desktop und Startmenü. Durch die grafische Oberfläche sind die Hardwareanforderungen höher, dafür lassen sich sämtliche Einstellungen komfortabel vornehmen. Die Verwaltung erfolgt über den Server-Manager und zahlreiche Tools, Assistenten und Konsolen. Die Steuerung über Eingabeaufforderung oder PowerShell ist ebenfalls möglich.

Server-Core

Server-Core ist die von Microsoft bevorzugte Installationsart. Durch den Verzicht auf die grafische Benutzeroberfläche wird der Ressourcenbedarf reduziert und die Sicherheit erhöht. Dies liegt am reduzierten Umfang der installierten Software, da jeder Programmcode potenzielle Fehler enthält und Angriffsflächen bietet.

Die Verwaltung des Core-Servers erfolgt lokal von der Kommandozeile bzw. PowerShell aus oder von einem anderen System, auf dem der Server-Manager und notwendige Konsolen installiert sind. Für die Remote-Administration von Windows Server 2022 Core wird ein Windows Server 2022 mit grafischer Oberfläche oder Windows 10 / 11 (ab Version Pro) benötigt. Das früher notwendige RSAT-Tool wird seit dem Oktober 2018-Update von Windows 10 bzw. für Windows 11 nicht mehr benötigt. Hier wird die Funktion als „Feature on Demand“ bereitgestellt. Möglich ist auch eine Remoteverbindung per **Remote Desktop Protocol (RDP)**, die jedoch zunächst aktiviert werden muss. Eine Übersicht der installierten bzw. installierbaren Rollen und Feature finden Sie hier:

<https://docs.microsoft.com/en-us/windows-server/administration/server-core/server-core-roles-and-services>

Umschalten zwischen Core und grafischer Oberfläche

In Windows Server 2012/2012 R2 ist es möglich, nachträglich zwischen Core und grafischer Benutzeroberfläche zu wechseln. Diese Funktion wurde mit der Veröffentlichung von Windows Server 2016 eingestellt.

Hyper-V

Ein häufiger Lösungsansatz ist die Installation von Windows Server 2022 in einer virtuellen Maschine. Microsofts virtuelle Umgebung Hyper-V bietet die Möglichkeit, auf einem physischen Server zusätzliche virtuelle Server zu installieren. So können Sie beispielsweise sicherheitsrelevante Server-Dienste (z. B. Domänencontroller, Zertifikatsdienste) auf separaten Servern betreiben, die keine zusätzlichen Angriffsflächen bieten. Der Umzug virtueller Server auf andere Hardware ist selbst im laufenden Betrieb leicht durchzuführen (Live-Migration), da die virtuelle Hardware aller Hyper-V-Instanzen identisch ist. Dadurch ergeben sich interessante Möglichkeiten, die vorhandenen Hardware-Ressourcen besser auszunutzen. Hyper-V ist in den Editionen Standard und Datacenter nutzbar. Die Editionen unterscheiden sich in der Anzahl der integrierten Lizenzen für virtuelle Betriebssysteme. Bei der Standard-Edition ist eine Lizenz für zwei virtuelle Server enthalten, bei Datacenter ist die Anzahl unbegrenzt. Mit Server 2022 wurde für Hyper-V die neue Version 10 eingeführt, außerdem ist der bisherige kostenlose Hyper-V Server entfallen.

2.2 Virtualisierung

Virtuelle Maschinen

Mit Hyper-V lassen sich unter Windows Server 2022 auf einem physischen Server (je nach Betriebssystemversion) mehrere virtuelle Systeme betreiben. Somit können bestimmte Serverrollen an eigene Betriebssysteminstanzen gekoppelt werden und dadurch die vorhandene Hardware besser ausnutzen. Zusätzlich ergeben sich Sicherheitsvorteile. So lässt sich etwa eine Stammzertifizierungsstelle im laufenden Betrieb bei Bedarf an- und abschalten, um sie so vor möglichen Angriffen zu schützen.

Vorteile der Virtualisierung

Die Konsolidierung der Server erlaubt insbesondere eine Verringerung der Betriebskosten, da z. B. redundante Netzteile und Plattensysteme nicht mehrfach angeschafft werden müssen und auch die klimatisierten Serverschränke, unterbrechungsfreie Stromversorgungen (USVs) oder Servergehäuse nicht mehrfach vorhanden sein müssen.

Snapshots/Prüfpunkte

Snapshots (Momentaufnahmen/Prüfpunkte) von virtuellen Servern erlauben das Festhalten unterschiedlicher Konfigurationszustände, was besonders für Testumgebungen ideal ist. So lassen sich bestimmte Konfigurationen mehrfach nacheinander üben, ohne erst eine Deinstallation von Diensten oder gar Betriebssystemen durchführen zu müssen. Außerdem können Sie auf diese Weise verschiedene Konstellationen ausprobieren, die sich ansonsten gegenseitig ausschließen würden. Sie werden im Buch zu den entsprechenden Zeitpunkten aufgefordert, einen Snapshot zu erstellen.

Maximalwerte für Hyper-V-Hostsysteme

- ✓ Bis zu 512 logische Prozessoren und 48 TB RAM
- ✓ 1024 virtuelle Computer je Server
- ✓ Maximale Anzahl virtueller CPUs je Server: 2048

Maximalwerte für virtuelle Computer

Die Maximalwerte der virtuellen Maschinen unterscheiden sich je nach verwendeter Generation und weisen daher auch unterschiedliche Hardwareausstattungen auf. Die aufgeführten Maximalwerte sind teilweise nur mit Maschinen der 2. Generation zu erreichen:

- ✓ 12 TB RAM
- ✓ 64 TB virtuelle Festplattengröße
- ✓ 240 virtuelle Prozessoren
- ✓ Bis zu 50 Prüfpunkte

Eine komplette Übersicht finden Sie unter:

- ✓ <https://docs.microsoft.com/de-de/windows-server/virtualization/hyper-v/plan/plan-hyper-v-scalability-in-windows-server>

Verbesserungen im Zusammenhang mit Hyper-V ab Server 2016

Seit Windows Server 2016 bietet Microsoft im Cluster die Möglichkeit, die lokalen Datenspeicher zu einem Pool zusammenzufassen. Die Technik trägt die Bezeichnung „Storage Spaces Direct“. Die Container-Technologie „Docker“ hielt mit Windows Server 2019 Einzug. Mit dieser Technik lassen sich die Anwendungen virtualisieren, die sich Teile des Betriebssystems mit dem Server teilen. Server 2022 erweitert die Funktionalität von SMB Direct mit einer Verschlüsselung auf Basis von AES-128 und AES-256. Neu ist auch die Nested Virtualization für AMD-Prozessoren, bei der Hyper-V auch auf virtuellen Maschinen aktiviert werden kann. Weitere Informationen hierzu finden Sie auf der Webseite der Firma Microsoft (<https://docs.microsoft.com/de-de/virtualization/hyper-v-on-windows/user-guide/nested-virtualization>). Auch der virtuelle Switch des neuen Hyper-V wurde dahingehend verbessert, dass Netzwerkpakete zu größeren Blöcken zusammengefasst werden, um die Anzahl der CPU-Zyklen zu verringern, was die Netzwerkperformance erhöht. Aufgegeben wurde die Weiterentwicklung der Microsoft Hyper-V Shielded VM, die mit Windows Server 2016 eingeführt wurden. Sichere VM sollen zukünftig in der Azure Stack HCI betrieben werden.

Verbesserungen ab Windows Server 2016

Im Vergleich zu den Vorgänger-Editionen seit Windows Server 2016 gibt es Verbesserungen, vor allem im Bereich der Sicherheit. Windows Server 2022 bietet dabei alle relevanten Funktionen von Windows Server 2016/2019. Erwähnenswert ist sicher die SMB Komprimierung im Zusammenwirken mit Windows 11, bei der die Netzwerkverbindung entlastet wird oder die Leistungsverbesserung von TCP und UDP. Eine komplette Übersicht finden Sie hier:

- ✓ <https://docs.microsoft.com/de-de/windows-server/get-started/whats-new-in-windows-server-2022>

Zusammen mit neuen Versionen seines Windows Servers veröffentlicht Microsoft auch regelmäßig neue Versionen seines neuen webbasierten Server-Managers mit der Bezeichnung Windows Admin Center. Dabei handelt es sich um einen Webdienst, der auch auf Core-Servern mit Windows Server installiert werden kann. Das Windows Admin Center (<https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center>) kann kostenlos bei Microsoft heruntergeladen werden.

Hardwarevoraussetzungen

Um eine Virtualisierung durchführen zu können, werden bestimmte Hardwareanforderungen an das Hostsystem gestellt. So werden neben einer modernen CPU, die Virtualisierung unterstützt, auch eine BIOS-Unterstützung sowie (je nach Anzahl der benötigten Hosts) entsprechende Speicherkapazitäten benötigt. Auch sollten für eine bessere Leistung mehrere Festplatten vorhanden sein, damit die Systeme bei Plattenzugriffen nicht um die Ressourcen konkurrieren müssen.

2.3 Verzeichnisdienste

Aufgabe von Verzeichnisdiensten

Verzeichnisdienste haben die Aufgabe, die **Ressourcen** eines Netzwerks **selektiv verfügbar** zu machen. Eine Ressource ist alles, was zum Netzwerk gehört, z. B. Benutzer, Computer, Dienste, gemeinsam verwendete Anwendungen und gemeinsam verwendete Daten oder Geräte im Netzwerk. Selektiv verfügbar bedeutet dabei, dass eine Steuerung der Verwendung möglich sein soll.

Leistungsfähigkeit von Verzeichnisdiensten

Die Leistungsfähigkeit eines Verzeichnisdienstes bestimmt sich beispielsweise nach ...

- ✓ der Anzahl der verwaltbaren Objekte (Ressourcen wie Benutzer, Geräte, Datenbestände usw.),
- ✓ zahlreichen Sicherheitsanforderungen,
- ✓ der Unterstützung verschiedener Anforderungen für die Verwaltung, z. B. die Delegation von Verwaltungsaufgaben oder die Fernverwaltung,
- ✓ der Erweiterbarkeit des Dienstes, um beispielsweise die Fusion zweier Firmen realisieren zu können,
- ✓ der Flexibilität bei der Gestaltung, um beliebige Firmenstrukturen oder Hierarchien abzubilden,
- ✓ der Performance,
- ✓ dem Maß der Verfügbarkeit auch bei Ausfall eines Teilsystems,
- ✓ der Zusammenarbeit mit Verzeichnisdiensten anderer Hersteller,
- ✓ der Unterstützung und Integration internationaler Standards,
- ✓ der Berücksichtigung der Netzwerkinfrastruktur (schnelle/langsame Datenübertragungswege).

Active Directory

Das **Active Directory (AD)** ist der Verzeichnisdienst in Microsoft-Netzwerken seit Windows Server 2000. Beim AD handelt es sich um eine hierarchische und verteilte Datenbank. Sie basiert weitgehend auf dem Industriestandard X.500 für Datenbanken. Das Active Directory unter Windows Server 2022 ermöglicht das problemlose Klonen von virtualisierten Domänencontrollern.

Leistungsmerkmale des Active Directory

Sicherheit	Windows Server 2022 bietet Sicherheit im Netzwerk durch Einsatz des Authentifizierungsstandards KerberosV5.
Verwaltung	Sowohl die Delegation von Verwaltungsaufgaben als auch die Fernverwaltung werden durch die Active Directory-Verzeichnisdienste unterstützt. Active Directory-Verbunddienste stellen eine zentralisierte Webanmeldung für verteilte webbasierte Anwendungen bereit.

Erweiterbarkeit	Das Erweitern einer vorhandenen Struktur durch Hinzufügen neuer Elemente ist problemlos möglich. Funktionen wie Vertrauensstellungen zwischen Gesamtstrukturen, Authentifizierung zwischen Gesamtstrukturen und die Umbenennung bestehender Gesamtstrukturen und Domänen erleichtern die Integration vorhandener Strukturen. Darüber hinaus liefern die Active Directory Lightweight Directory Services eine Schnittstelle für verzeichnisfähige Anwendungen, die nicht auf eine Domäneninfrastruktur zurückgreifen müssen.
Flexibilität	Hohe Flexibilität und Erweiterbarkeit durch Verschachtelungen. Die Verschachtelungstiefe ist in logischer Hinsicht unbegrenzt, findet ihre Beschränkungen jedoch in den physischen Gegebenheiten.
Performance	Hohe Performance beispielsweise durch Begrenzung der zu übertragenden Datenmengen bei der Replikation (z. B. werden nur Änderungen übertragen)
Verfügbarkeit	Hohe Verfügbarkeit kann durch die Bereitstellung von Redundanz der Verzeichnisinformationen erreicht werden. Weitere Funktionen sind die Fehlertoleranz und die Wiederherstellung der Verzeichnisdienste nach einem Serverausfall.
Interoperabilität	Windows Server 2022 bietet Unterstützung für weitverbreitete Verzeichnisdienste verschiedener Hersteller. Hierzu stellt es die Zugriffe auf alle Active Directory-Funktionen über standardisierte Schnittstellen bereit und beinhaltet außerdem verschiedene Mechanismen zur Synchronisation.
Unterstützung von Standards	Unterstützung für alle internationalen Standards, die momentan für den Netzwerkbetrieb in LAN und WAN etabliert sind
Bezug auf die Netzwerkinfrastruktur	Die Häufigkeit der Übertragungen von Verzeichnisinformationen wird an die Geschwindigkeiten verschiedener Übertragungswege angepasst und kann zeitlich gesteuert werden.

2.4 Sicherheitsfunktionen

Sicherheit durch die Active Directory-Verzeichnisdienste

Der Verzeichnisdienst von Windows Server 2022 gewährt die Sicherheit des Netzwerks auf der logischen Ebene. Zu den Prinzipien gehören Anmeldeauthentifizierung, Gruppenrichtlinien und Zugriffsberechtigungen. Diese können durch die Integration der Active Directory-Zertifikatsdienste verstärkte Sicherheitsmechanismen implementieren. Mit Zertifikaten lässt sich z. B. durch den Einsatz von Smartcards für die Anmeldung eine nochmals verbesserte Sicherheit erreichen.

Verschlüsselung

Verschlüsselung ist eine Methode, Sicherheit für Daten in physischer Hinsicht zu gewähren. Die Verschlüsselung können Sie für Dateien und Ordner nutzen, z. B. durch den Einsatz von EFS (Encrypted File System) oder BitLocker.

Auch Anmeldedaten im Netzwerk können verschlüsselt werden. Hierzu unterstützt Windows verschiedene Authentifizierungsprotokolle, z. B. MS-CHAPv2 und PEAP.

Neben diesen Protokollen, die allein den Datenaustausch für den Anmeldevorgang bewerkstelligen, gibt es zahlreiche Protokolle, die der sicheren Datenübertragung im Allgemeinen dienen. Hierzu gehören beispielsweise IPsec und SSL.