gibb Berufsfachschule Bern

In Kooperation mit dem HERDT-Verlag stellen wir Ihnen eine PDF inkl. Zusatzmedien für Ihre persönliche Weiterbildung zur Verfügung. In Verbindung mit dem Programm HERDT-Campus ALL YOU CAN READ stehen diese PDFs nur Lehrkräften und Schüler*Innen der oben genannten Lehranstalt zur Verfügung. Eine Nutzung oder Weitergabe für andere Zwecke ist ausdrücklich verboten und unterliegt dem Urheberrecht. Jeglicher Verstoß kann zivil- und strafrechtliche Konsequenzen nach sich ziehen.

# Windows Server 2019

## Netzwerkadministration

Thomas Joos, Martin Dausch

1. Ausgabe, März 2019

ISBN 978-3-86249-851-2

W2019N

Schulversion

**1 Informationen zu diesem Buch und zur virtuellen Testumgebung 4**

1.1 Voraussetzungen und Ziele 4
1.2 Netzwerk in der Testumgebung 5
1.3 Namensgebung in diesem Buch 6
1.4 Aufbau und Konventionen 8

**2 Windows Server 2019 10**

2.1 Editionen von Windows Server 2019 10
2.2 Virtualisierung 12
2.3 Verzeichnisdienste 13
2.4 Sicherheitsfunktionen 15
2.5 Verwaltungsfunktionen 16
2.6 Skalierbarkeit, Zuverlässigkeit, Hardware-Unterstützung 17
2.7 Netzwerkinfrastruktur 18
2.8 Dateiverwaltung, Dateisystem 18

**3 Installation 20**

3.1 Vorüberlegungen zur Installation 20
3.2 Informationen für die Installation sammeln und auswerten 23
3.3 Die Installation vorbereiten 24
3.4 Windows Server 2019 installieren 27
3.5 Upgrade von Standard- und Testversion auf Datacenter-Edition 29
3.6 Erstkonfiguration des Hostrechners 29

**4 Bedienung und Neuerungen 34**

4.1 Startmenü 34
4.2 Windows Server 2019 mit Tastenkombinationen bedienen 35
4.3 Server-Manager 36

**5 Hyper-V-Testumgebung 37**

5.1 Virtualisierung 37
5.2 Hyper-V einsetzen 40
5.3 Hyper-V installieren 41
5.4 Hyper-V einrichten 42
5.5 Virtuellen Computer einrichten 47
5.6 Virtuellen Computer verwalten 50

**6 Active Directory 55**

6.1 Überblick Verzeichnisdienst 55
6.2 Domäne, Struktur und Gesamtstruktur 56
6.3 Funktionsebenen 57
6.4 Domänencontroller, Betriebsmaster und globaler Katalog 58
6.5 Organisationseinheit – OU 60
6.6 Standorte im Active Directory 61
6.7 Sysvol – Ressourcen für Anmeldungen 62

**7 Active Directory installieren 63**

7.1 Installation vorbereiten 63
7.2 Stammdomäne einrichten 65
7.3 Domänencontroller zur Domäne hinzufügen 71
7.4 Active Directory erkunden 73

**8 DNS 78**

8.1 Domänennamespace 78
8.2 Namensauflösung 80
8.3 Global Names 81
8.4 Dynamisches DNS 82
8.5 Zonen 83
8.6 Zonenübertragung 85
8.7 Zonendelegierung verstehen 86
8.8 Aufbau der DNS-Datenbank 87

**9 DNS-Dienst einrichten und konfigurieren 89**

9.1 Domänennamespace für die Testumgebung 89
9.2 TCP/IP konfigurieren für DNS 90
9.3 DNS-Dienst installieren 95
9.4 DNS-Dienst konfigurieren 96
9.5 Zoneneigenschaften bearbeiten 99
9.6 Sekundäre Zone einrichten 101
9.7 DNS-Serverdienst testen 102

**10 DHCP – Dynamische IP-Konfiguration 105**

10.1 TCP/IP 105
10.2 Vergabe von IP-Adressen 107
10.3 Dynamic Host Configuration Protocol (DHCP) 108
10.4 DHCP-Server installieren 109
10.5 DHCP-Server konfigurieren 111

**11 Physische Struktur von Active Directory 119**

11.1 Standorte und Standortplanung 119
11.2 Replikation innerhalb eines Standorts 120
11.3 Replikation zwischen Standorten 121
11.4 Replikationskomponenten 122
11.5 Replikationstopologie 123

**12 Active Directory-Objekte verwalten 124**

12.1 Container der Domäne erkunden 124
12.2 Planung einer Domäne 126
12.3 Entwurf für die Domäne *firma.intern* 127
12.4 Organisationseinheiten erstellen 128
12.5 Benutzerkonten 130
12.6 Benutzerkonto erstellen 132
12.7 Objektnamen im Active Directory 134
12.8 Computerkonto erstellen 138




Schulversion

© HERDT-Verlag

**13 Benutzer und Gruppen 140**
13.1 Benutzer und Kontakte 140
13.2 Gruppentypen 141
13.3 Gruppenbereiche 142
13.4 Gruppenhierarchien einsetzen 143
13.5 Gruppenplanung 145

**14 Gruppen verwalten 147**
14.1 Gruppenplanung mit globalen und lokalen Gruppen 147
14.2 Globale Gruppe erstellen und verwalten 148
14.3 Lokale Gruppe erstellen und verwalten 149
14.4 Gruppenplanung mit universalen Gruppen 150
14.5 Universale Gruppen erstellen 151
14.6 Gruppen mit einer Batchdatei anlegen 152

**15 Rechte und Berechtigungen 158**
15.1 Definitionen 158
15.2 Vererbung von Berechtigungen 161

**16 Active Directory-Berechtigungen verwalten 162**
16.1 Objektverwaltung 162
16.2 Berechtigungen und Berechtigungsvererbung überprüfen und verwalten 163
16.3 Objektverwaltung delegieren 165
16.4 Verwaltungstools für die Objektverwaltung 168
16.5 Konsole mit Aufgabenblock erzeugen 169

**17 Berechtigungen anpassen 172**
17.1 NTFS-Berechtigungen 172
17.2 Freigabe-Berechtigungen für Ordner 178
17.3 Berechtigungen für Drucker 178
17.4 Freigaben und Drucker veröffentlichen 179

**18 Dateidienste 181**
18.1 Ordner-Freigaben 181
18.2 Dateidienste installieren 183
18.3 Freigabe- und Speicherverwaltung 184
18.4 Ressourcen-Manager für Dateiserver 187
18.5 Versionierung und Deduplizierung 192
18.6 Weitere Techniken zur Bereitstellung von Dateien 193

**19 Dateidienste planen 195**
19.1 Gründe für zentrale Datenspeicherung 195
19.2 Dateistruktur planen 197
19.3 Verzeichnisstruktur anlegen 197

**20 Gruppenrichtlinien 199**
20.1 Einsatzbereiche von Gruppenrichtlinien 199
20.2 Gruppenrichtlinienobjekt 202
20.3 Verarbeitung der Gruppenrichtlinien-einstellungen 202
20.4 Gruppenrichtlinienberechtigungen 203
20.5 Vererbung von Gruppenrichtlinien 204

**21 Sicherheitsrichtlinien einsetzen 205**
21.1 Gruppenrichtlinienverwaltung 205
21.2 Sicherheitsrichtlinien für Domänencontroller bearbeiten 207
21.3 Domänenrichtlinien bearbeiten 209
21.4 Zusätzliche Kontorichtlinie erstellen 213

**22 Gruppenrichtlinien verwalten 215**
22.1 Gruppenrichtlinienimplementierung planen 215
22.2 Test-OU erstellen 217
22.3 Gruppenrichtlinien implementieren 218
22.4 Gruppenrichtlinien testen 223
22.5 Gruppenrichtlinienergebnisse 224
22.6 Gruppenrichtlinien bearbeiten 225

**23 Notfallsicherung 226**
23.1 Strategien und Wiederherstellungsfunktionen 226
23.2 Fehlertolerante Datenträger 227
23.3 Erweiterte Startoptionen 228
23.4 Systemstatusdaten 229
23.5 Der Active Directory-Papierkorb 230
23.6 Windows-Speicherdiagnose 231

**Stichwortverzeichnis 232**

© HERDT-Verlag
Schulversion

# 1 Informationen zu diesem Buch und zur virtuellen Testumgebung

**In diesem Kapitel erfahren Sie**

- wie Sie dieses Buch einsetzen können
- welche Vorkenntnisse Sie mitbringen sollten
- welchen Aufbau die virtuelle Testumgebung für dieses Buch hat
- welche Namenskonventionen in diesem Buch verwendet werden

## 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 2019 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 2019 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 und mindestens 120 GB freier Festplattenkapazität. Die Systeme sollten 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 2019 geeignet sein (Angaben zu den Systemvoraussetzungen finden Sie in Kapitel 3). Für den Aufbau der Szenarios aus dem HERDT-Buch *Windows Server 2019 – Erweiterte Netzwerkadministration* benötigen Sie zusätzlichen Speicherplatz von mindestens 80 GB. |
| Software | Installations-Datenträger Windows Server 2019 (DVD, ISO-Abbild oder bootfähiger USB-Stick) |


Schulversion
© HERDT-Verlag

## 1.2 Netzwerk in der Testumgebung

### Testumgebung mit einem Hostserver und drei virtuellen Maschinen

Die Testumgebung sieht die Einrichtung eines Hostsystems unter Windows Server 2019 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.

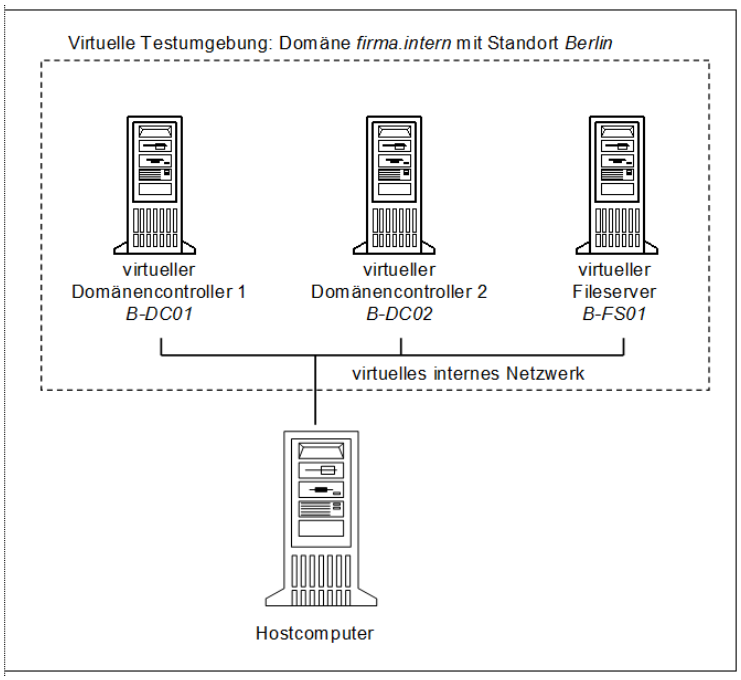
Es ist möglich, ein anderes Betriebssystem wie z. B. Linux oder macOS für den Host zu verwenden und Virtualisierungssoftware von anderen Herstellern (z. B. VMware oder VirtualBox von Oracle/Sun) einzusetzen. Diese Alternativen werden jedoch im Buch nicht beschrieben, außerdem gehört der Umgang mit Hyper-V 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 2019 – 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 sollen **aussagekräftige Namen** sein, aus denen die Funktion hervorgeht. Das mag zunächst aufwendig und kompliziert erscheinen. Wenn Sie jedoch einmal mit einem fremden Active Directory oder Skript arbeiten müssen, werden Sie für eindeutige Bezeichnungen sehr dankbar sein. 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 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 stets 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.


Schulversion
© HERDT-Verlag

### Benutzernamen

Die Anmeldenamen werden durch den Anfangsbuchstaben des Vornamens und den vollen Nachnamen gebildet. Dabei wird auf Umlaute und Sonderzeichen verzichtet.

### Autokennzeichen als Standortkürzel

Für die Kennzeichnung des Standorts wird jeweils das Autokennzeichen der Stadt verwendet, auch wenn dies bei einer Firma mit nur einem Standort zunächst unnötig erscheint. Auf diese Weise sind Sie auf spätere Erweiterungen der Firma vorbereitet.

### 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 und KZ für kein Zugriff.

### 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*:

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

## 1.4 Aufbau und Konventionen

### Aufbau des Buchs

- Am Anfang jedes Kapitels finden Sie die Lernziele.
- 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 2019 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, die detaillierte Arbeitsanleitungen zum Ausführen der vorher behandelten Konfigurationsmaßnahmen enthalten. Zielsetzung dieses Buches ist das Lernen und Üben beim Aufbau einer Windows-Server-2019-Testumgebung.


Schulversion
© HERDT-Verlag

## Typografische Konventionen

Im Text erkennen Sie bestimmte Programmelemente an der Formatierung:

| | |
|---|---|
| *Kursivschrift* | kennzeichnet Programmelemente wie Register oder Schaltflächen. |
| `Courier` | wird für Benutzereingaben und Systembefehle verwendet. |
| Spitze Klammern `<>` | kennzeichnen Platzhalter. |

## Was bedeuten die Symbole im Buch?

Hilfreiche Zusatzinformation

Praxistipp

Warnhinweis

## Weitere Medien von HERDT nutzen

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

- Administrationskenntnisse erweitern. Hierzu empfehlen wir Ihnen das folgende HERDT-Buch aus der Windows-Server-2019-Reihe, das auf diesem Buch aufbaut:
  - *Windows Server 2019 – Erweiterte Netzwerkadministration*
- Netzwerkkenntnisse vertiefen. Dazu bietet Ihnen der HERDT-Verlag folgende Bücher an:
  - *Netzwerke – Grundlagen*
  - *Netzwerke – Netzwerktechnik*
  - *Netzwerke – Sicherheit*
  - *Netzwerke – IPv6 Internet Protocol Version 6*

Wir wünschen Ihnen viel Spaß und Erfolg mit diesem Buch.

Ihr Redaktionsteam des HERDT-Verlags

# 2 Windows Server 2019

**In diesem Kapitel erfahren Sie**

- einen Überblick über die verschiedenen Editionen des Servers
- eine kurze Einführung in Virtualisierung mittels Hyper-V
- einen Überblick über die Leistungsfähigkeit der Verzeichnisdienste
- einen Überblick über einige Sicherheitsfunktionen
- einen Überblick über einige Verwaltungsfunktionen
- einen Einblick in die Konzepte zur Unterstützung der Netzwerkinfrastruktur

**Voraussetzungen**

- Erfahrung mit Windows-Installationen, z. B. als Systembetreuer
- Grundlagen des Netzwerkbetriebs

## 2.1 Editionen von Windows Server 2019

### Unterschiedliche Einsatzbereiche und Anforderungen

Windows Server 2019 ist ebenso wie seine Vorgänger Windows Server 2008 R2 und 2012/2012 R2/2016 ein reines 64-Bit-Betriebssystem. Es ist das Server-Pendant zum neuen Windows 10 und unterstützt dessen neue Funktionen und die neue Oberfläche. Vier verschiedene Ausführungen des Betriebssystems stehen zur Verfügung, die sich in der Unterstützung verschiedener Betriebssystemkomponenten und der maximal unterstützten Hardware unterscheiden. Die verschiedenen Betriebssystemausführungen werden als **Editionen** bezeichnet, nicht zu verwechseln mit Windows-**Versionen** wie z. B. Windows Vista, 7/8/8.1 oder 10.

### Editionen von Windows Server 2019

Für unterschiedliche Einsatzgebiete werden verschiedene Editionen von Windows Server 2019 angeboten.
Sie unterscheiden sich hinsichtlich der unterstützten Hardware sowie der enthaltenen Funktionen.

Windows Server 2019 ist nur als 64-Bit-Version erhältlich. Die Mindestanforderungen für alle Editionen sind ein 64-Bit-Prozessor mit mindestens 1,4 GHz, 512 MB RAM und wenigstens 32 GB freier Festplattenplatz.
Die empfohlenen Hardwarevoraussetzungen richten sich nach den Aufgaben und liegen **erheblich** darüber.

| Edition | Einsatzgebiet |
|---|---|
| **Windows Server 2019 Essentials** | ✔ Für Firmenumgebungen bis 25 Benutzer<br>✔ Ersetzt den Small Business Server<br>✔ Reduzierter Funktionsumfang, keine Virtualisierung<br>✔ Keine eigene Oberfläche mehr, wie noch in Windows Server 2016 Essentials<br>✔ Vorkonfigurierte Cloud-Anbindung<br>✔ Keine Exchange-Lizenz inbegriffen |
| **Windows Server 2019 Standard** | ✔ Standardvariante mit eingeschränkter Funktionalität<br>✔ Lizenzen für zwei Virtualisierungsinstanzen inbegriffen<br>✔ Max. 512 Prozessoren und max. 24 TB RAM |


Schulversion
© HERDT-Verlag

| Edition | Einsatzgebiet |
|---|---|
| **Windows Server 2019 Datacenter** | ✔ Für den Einsatz in großen Unternehmen und Organisationen konzipiert<br>✔ Volle Funktionalität<br>✔ Unbegrenzte Anzahl von Lizenzen für Virtualisierungsinstanzen<br>✔ Max. 512 Prozessoren und max. 24 TB RAM |

Bei den Limitierungen werden physische CPUs gezählt, nicht CPU-Kerne innerhalb eines Prozessors. Es wird daher die Anzahl der CPU-Sockel auf dem Mainboard angegeben.

## SAC- und LTSC-Versionen

Seit Windows Server 1709, dem ersten Nachfolger von Windows Server 2016, veröffentlicht Microsoft halbjährlich neue Server-Versionen, die auch über neue Funktionen verfügen. Diese tragen auch die Bezeichnung „Semi-Annual-Channel-Versionen“ (SAC). Im Gegensatz zu den Hauptversionen von Windows Server tragen die SAC-Versionen nicht nur die Jahreszahl der Veröffentlichung im Namen sondern auch den Monat. SAC-Versionen stehen nur Kunden zur Verfügung, die einen Software-Assurance-Vertrag mit Microsoft geschlossen haben. Auch Kunden in Microsoft Azure können, mit etwas Verzögerung, auf die SAC-Versionen setzen.

Mit dem neuen Semi Annual Channel (SAC) stellt Microsoft neue Server-Version schneller zur Verfügung, wie Windows Server 1709/1803/1809 und neuer. Die SAC-Versionen von Windows Server werden keine grafische Oberfläche erhalten. Windows Server 1709 und Windows Server 1803/1809 werden ausschließlich als Core-Server installiert. Neben der Core-Version erscheinen die SAC-Versionen, also auch Windows Server 1803/1809, als Container-Image. Hier stehen das Core-Image und das Nano-Image zur Verfügung.

Bei Windows Server 2019 handelt es sich um die nächste Vollversion, die Microsoft im Rahmen des Long Term Servicing Channel (LTSC) zur Verfügung stellt. Die Veröffentlichung von Windows Server 2019 stellt die Ablösung von Windows Server 2016 als aktuelle LTSC-Version dar. Die wichtigsten Neuerungen von Windows Server 2019 drehen sich um die Unterstützung von Linux und Containern, inklusive Kubernetes.

Mit dem Long Term Servicing Channel erhalten Unternehmen für 5 Jahre grundlegenden und erweiterten Support. Außerdem lassen sich optional zusätzlich 6 Jahre Premium Assurance dazubuchen. Neue Funktionen werden in dieser Zeit aber nicht in die Serverversion integriert.

Unternehmen, die Ihren Server mit Windows Server 2016 zu Windows Server 1709/1803/1809 aktualisieren, wechseln automatisch in den Semi Annual Channel. Das bedeutet, für den Server gibt es nur noch 18 Monate Support nach der Veröffentlichung. Danach muss die nächste SAC-Version oder eben die nächste LTSC-Version installiert werden.

## Standardinstallation mit grafischer Oberfläche

Dies ist die klassische Installationsart mit Windows-Desktop und dem Startmenü. Durch die grafische Oberfläche sind die Hardwareanforderungen geringfügig 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 durch weniger Angriffspunkte auch die Sicherheit erhöht. Die Verwaltung des Servers erfolgt lokal von der Kommandozeile bzw. PowerShell aus oder von einem anderen Server aus über den Server-Manager und diverse Konsolen. Möglich ist auch eine Remoteverbindung. Für die Fernsteuerung von Windows Server 2019 Core werden Windows Server 2019 oder Windows 10 Pro bzw. Enterprise benötigt.

Die Core-Variante ist nur bei den Editionen Standard und Datacenter möglich. Im Gegensatz zu Server 2008 R2 ist das .NET-Framework stets verfügbar, sodass auch folgende Webserver-Rollen möglich sind:

- IIS-ASPNET
- IIS-NetFxExtensibility
- IIS-ManagementConsole
- IIS-ManagementService
- IIS-LegacySnapIn
- IIS-FTPManagement
- WAS-NetFxEnvironment
- WAS-ConfigurationAPI

### Umschalten zwischen Core und grafischer Oberfläche

In Windows Server 2012/2012 R2 ist es möglich, nachträglich zwischen Core und grafischer Benutzeroberfläche zu wechseln. Diese Möglichkeit gibt es seit Windows Server 2016 und auch in Windows Server 2019 nicht mehr.

### Hyper-V

Eine Sonderinstallationsform ist die Installation von Windows Server 2019 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, 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, beim Datacenter ist die Anzahl unbegrenzt.

## 2.2 Virtualisierung

### Virtuelle Maschinen

Mit Hyper-V lassen sich unter Windows Server 2019 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

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

Zusätzlich erlauben Snapshots (Momentaufnahmen/Prüfpunkte) von virtuellen Servern 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.


Schulversion
© HERDT-Verlag

### Neue Maximalwerte im Vergleich zu Windows Server 2012 R2

Seit Windows Server 2016 hat Microsoft an den Maximalwerten nichts verändert:

- Bis zu 512 logische Prozessoren und 24 TB RAM pro Host
- Erhöhung des Hauptspeichers pro VM auf 16 TB
- Maximale Anzahl an virtuellen CPUs pro VM: 240

### Verbesserungen ab Windows Server 2012 R2

In Windows Server 2019 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“ hält in Windows Server 2019 Einzug. Mit dieser Technik lassen sich die Anwendungen virtualisieren, die sich Teile des Betriebssystems mit dem Server teilen. In Hyper-V gibt es einige Verbesserungen bezüglich der Systemdateien und der Erstellung von Snapshots. Das virtuelle Betriebssystem in den VMs lässt sich bei der Erstellung von Snapshots mit einbeziehen.

### Verbesserungen ab Windows Server 2016

Im Vergleich zu Windows Server 2016 gibt es ebenfalls Verbesserungen. Windows Server 2019 bietet alle relevanten Funktionen von Windows Server 2016 und zahlreiche interessante neue Funktionen. Dazu gehört die verbesserte Container-Technologie auf Basis von Docker und eine weitere Bereitstellungsvariante mit der Bezeichnung „Nano“. Die Nano-Installation ist in Windows Server 2019 nur noch als Container-Image verfügbar. Dafür unterstützt Windows Server 2019 jetzt auch die effektivere Bereitstellung von Containern, vor allem auf Basis von Linux. Auch Kubernetes wird in Windows Server 2019 unterstützt.

Zusammen mit neuen Versionen seines Windows Servers veröffentlicht Microsoft auch regelmäßig neue Versionen seines neuen webbasierten Server-Managers mit der Bezeichnung Windows Admin Center (Projektname Honolulu). 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 Verzeichnisdiensts 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 Delegierung 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 ist der Verzeichnisdienst in Microsoft-Netzwerken seit Windows 2000 Server. Beim Active Directory 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 2019 ermöglicht das problemlose Klonen von virtualisierten Domänencontrollern.

## Leistungsmerkmale des Active Directory

| | |
|---|---|
| Sicherheit | Windows Server 2019 bietet Sicherheit im Netzwerk durch Einsatz des Authentifizierungsstandards KerberosV5. |
| Verwaltung | Sowohl die Delegierung von Verwaltungsaufgaben als auch die Fernverwaltung werden durch die Active Directory-Verzeichnisdienste unterstützt.<br>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.<br>Funktionen wie Vertrauensstellungen zwischen Gesamtstrukturen, Authentifizierung zwischen Gesamtstrukturen und die Umbenennung bestehender Gesamtstrukturen und Domänen erleichtern die Integration vorhandener Strukturen.<br>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 |
| 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. |


Schulversion
© HERDT-Verlag

| | |
|---|---|
| Interoperabilität | Windows Server 2019 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. |

## 2.4 Sicherheitsfunktionen

### Sicherheit durch die Active Directory-Verzeichnisdienste

Der Verzeichnisdienst von Windows Server 2019 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 einrichten.

### 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 von 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.

### BitLocker-Laufwerksverschlüsselung

Mit der BitLocker-Laufwerksverschlüsselung lassen sich komplette Datenträger verschlüsseln. Dabei wird auf der TPM-Technik (Trusted Platform Module) basierend eine Integritätsprüfung für Startkomponenten durchgeführt, bevor der Zugriff auf Datenträger gewährt wird. So kann ein Datenträger nicht mehr in einen anderen Rechner eingebaut werden, um seinen Inhalt zu lesen.

Dadurch ergeben sich einerseits Sicherheitsvorteile, da der Diebstahl eines Datenträgers weniger Auswirkungen auf die Unternehmenssicherheit hat. Andererseits wird bei einem Hardwaredefekt der Zugriff auf Informationen erschwert, da es nicht mehr möglich ist, auf Festplattendaten schnell zuzugreifen, indem das Laufwerk in einen anderen Rechner eingebaut wird. In der Praxis ist es meist einfacher, den Zugang zu Servern zu beschränken, und dadurch die Sicherheit zu gewährleisten. Anders verhält sich dies bei tragbaren Rechnern, die einem höheren Diebstahlrisiko ausgesetzt sind.

### Read-only Domain Controller (RODC)

Mit Read-only Domain Controllers stehen schreibgeschützte Versionen der Active Directory-Datenbank zur Verfügung, die an Standorten mit eingeschränkter Replikation und ohne administratives Personal verwendet werden können.

Administratoren können festlegen, dass nur bestimmte Objekte und Attribute an einen RODC übermittelt werden, sodass bei Diebstahl der Festplatten oder unerwünschten Zugriffen sicherheitsrelevante Informationen nicht in falsche Hände gelangen können.

## 2.5 Verwaltungsfunktionen

### Windows Bereitstellungsdienste

Die Windows-Bereitstellungsdienste (Windows Deployment Services, WDS) ermöglichen eine schnelle Installation von Workstations und Servern im Netzwerk. Wesentliche Elemente dieses Verfahrens sind die Speicherung eines Betriebssystem-Abbildes mit der gewünschten Konfiguration auf einem Bereitstellungsserver sowie die Installation des Betriebssystems über das Netzwerk mittels Transportserver. Beide Funktionen können auf einem Server installiert werden.

### Gruppenrichtlinien

Die Gruppenrichtlinien sind ein mächtiges Verwaltungsinstrument unter Active Directory. Mit ihnen können beispielsweise die Desktops der verschiedenen Benutzer verwaltet und Anwendungen von zentraler Stelle aus auf Workstations verteilt werden. Unter Windows Server 2019 wurde die Anzahl der verfügbaren Gruppenrichtlinien weiter erhöht. Daneben bieten administrative Vorlagen die Möglichkeit, bei Bedarf zusätzliche Gruppenrichtlinien zu erstellen. Windows Server 2019 enthält einige Detailverbesserungen und Updates, stellt aber im Wesentlichen die gleichen Funktionen zur Verfügung wie seine Vorgänger.

### Microsoft Management Console

Die MMC ist eine Verwaltungsplattform, mit der die verschiedenen Programme (als „Snap-In“ bezeichnet) zur Verwaltung aufgerufen werden können. Sie können die MMC anpassen, indem Sie nur solche Snap-Ins aufnehmen, die Sie zur Ausführung der Verwaltungsarbeiten benötigen. Zusätzlich lassen sich über Aufgabenblockansichten Verwaltungsaufgaben vereinfacht vorbereiten. Damit können Verwaltungsaufgaben leichter zugewiesen werden.

### Windows Script Host

Der Windows Script Host (WSH) ist ein sprachunabhängiger Script Host. Mit ihm können Sie Skripts vom Desktop oder von der Befehlszeile ausführen. Er ist damit ein Instrument zum Automatisieren von Verwaltungsaufgaben.

### Windows PowerShell

Die Windows PowerShell stellt in ihrer vierten Version eine mächtige Befehlszeilen- und Programmierschnittstelle dar, die mittels Hunderter sogenannter Cmdlets (Commandlets gesprochen) komplexe Befehle für die Konfiguration sämtlicher Systembestandteile bereitstellt. Mit den cmdlets lassen sich unter anderem differenzierte Operationen an der Registry sowie an WMI-Klassen und COM-Objekten ausführen. Windows Server 2019 bietet einige zusätzliche Cmdlets.


Schulversion
© HERDT-Verlag

### Windows Management Interface

Das WMI ist eine Software-Schnittstelle, mit der Verwaltungsinformationen standardisiert abgefragt werden können. Sie entspricht dem Standard WBEM (Web-Based Enterprise Management) und erlaubt die Abfrage und den Zugriff sowohl auf lokalen Systemen als auch über das Netzwerk. So erlauben z. B. WMI-Abfragen auf verfügbaren Festplattenspeicher, Anwendungen nur dann über Richtlinien zu installieren, wenn auch ausreichend Speicherplatz zur Verfügung steht.

### Windows Admin Center

Das Windows Admin Center ist eine webbasierte Verwaltungsoberfläche für Windows-Server. Dazu installieren Sie auf einem Server oder einer Arbeitsstation das Gateway des Windows Admin Centers. Administratoren verbinden sich mit einem Webbrowser mit dem Gateway und können dann über einen Browser die Server im Netzwerk mit einer grafischen Weboberfläche verwalten. Hier lassen sich auch Core-Server anbinden und die Vorgänger von Windows Server 2019.

### Remotedesktopdienste

Remotedesktopdienste ermöglichen Benutzern den Fernzugriff auf einen Computer. Sie übertragen nur die Benutzeroberfläche eines Programms auf den Arbeitsplatz des Benutzers. Der Remotedesktopserver übernimmt die gesamte Rechenleistung für die Datenverarbeitung. Die Remotedesktopdienste sind in Windows Server integriert. Benutzer können sich beispielsweise über VPN mit dem Netzwerk verbinden und komplexe Anwendungen auf dem Remotesystem ausführen.

Die Remotedesktopdienste stellen auch Anwendungen isoliert auf dem Client bereit. Der Anwender startet scheinbar eine lokale Anwendung, in Wirklichkeit läuft diese jedoch auf dem Remoteserver.

## 2.6 Skalierbarkeit, Zuverlässigkeit, Hardware-Unterstützung

### Unterstützung für symmetrisches Multiprocessing

Die Unterstützung des Symmetric Multiprocessing ermöglicht den Betrieb eines Servers – abhängig von der Serverversion und der Art der Installation. Die Prozessoren nutzen denselben physischen Speicher.

### Unterstützung von Clustering für Lastenausgleich und Fehlertoleranz

Mit Windows Server 2019 Standard und Datacenter können mehrere einzelne Server (Nodes, Knoten) zu einem **Cluster** zusammengefasst werden. Der Cluster kann sowohl mehr Rechenleistung als auch Fehlertoleranz bieten, indem mehrere Knoten gleichzeitig eingehende Anfragen bearbeiten. Besonders in Kombination mit virtuellen Maschinen kann beim Einsatz von Clustern sehr flexibel auf Veränderungen in den Anforderungen reagiert werden.

### Treibermodell

Das aktuelle Treibermodell trägt in erheblichem Umfang dazu bei, Abstürze zu verhindern. Windows Server 2019 kann sowohl den Code des Betriebssystems als auch den des Treibers mit einem Schreibschutz versehen. Unzulässige Zugriffe auf den geschützten Speicherbereich werden erkannt, und ein Administrator kann fehlerhafte Treiber schnell entdecken. Hilfestellung bei der Diagnose bietet auch der Treiberüberprüfungs-Manager *verifier.exe*. Dies ist ein Tool, mit dem Sie die Speichernutzung eines Treibers analysieren können, bevor Sie ihn einsetzen.

### Hardware-Unterstützung

Windows Server 2019 unterstützt aktuelle Hardware und Spezifikationen, z. B. Plug & Play, iSCSI, USB 3.x, Firewire und mit Zusatzsoftware auch Thunderbolt. Daneben bringt es eine Vielzahl an Treibern mit. Die Treiber für Windows 7, 8/8.1 und 10 verwenden dasselbe Treibermodell wie Windows Server 2019, allerdings unterscheiden sich manche Treiber in Funktionsumfang und möglichen Energiespareinstellungen, um den Anforderungen an einen Server besser gerecht zu werden.

## 2.7 Netzwerkinfrastruktur

### DHCP

DHCP-Server vergeben an Workstations eindeutige IP-Adressen. Unter Windows Server 2019 müssen DHCP-Server im Active Directory autorisiert werden, damit der DHCP-Dienst starten kann. So wird verhindert, dass versehentlich mehrere DHCP-Server identische Adressbereiche mehrfach im Netz vergeben. Windows Server 2019 unterstützt dabei sowohl IPv4- als auch IPv6-Adressvergabe und ermöglicht somit eine vollwertige Integration von neuen Standards.

Seit Windows Server 2012 ist es mit der neuen Funktion *DHCP-Failover* leichter, mehrere DHCP-Server zu betreiben, um die Ausfallsicherheit und Lastverteilung zu erhöhen.

### DNS

DNS ist Voraussetzung für das Active Directory und spielt bei Windows Server Betriebssystemen eine zentrale Rolle. DNS unterstützt dynamische Aktualisierungen, bei dem ein Computer seine IP-Adresse automatisch im DNS registriert. Bei Bedarf kann diese Aufgabe auch ein DHCP-Server übernehmen.

In der DNS-Datenbank werden außer der Zuordnung von Workstation-Namen zu IP-Adressen auch Informationen über die vorhandenen Netzwerkdienste gespeichert. Damit können Workstations DNS nutzen, um beispielsweise einen Server zu ermitteln, der die Benutzeranmeldung durchführen kann. Für die Auflösung bekannter Adressen zu unbekannten Namen werden Reverse-Lookupzonen sowohl für IPv4 als auch für IPv6 unterstützt.

Windows Server 2019 bietet eine verbesserte Unterstützung von DNSSEC, um die Vertrauenswürdigkeit von DNS-Servern mittels Zertifikaten überprüfen zu können.

## 2.8 Dateiverwaltung, Dateisystem

### Distributed File System (DFS)

Das Distributed File System ermöglicht, eine einzige Verzeichnisstruktur für die Datenbestände einer Organisation oder Abteilung oder der gesamten Firma zu erstellen. Im Vergleich zu den Vorgängern besitzen Windows Server 2012/2012 R2 und Windows Server 2019 eine verbesserte Integration des DFS in DirectAccess, mehrere PowerShell-Cmdlets zur Verwaltung der DFS-Namespaces und eine aktualisierte WMI-Schnittstelle.

### NTFS-Datenträgerkontingente

Auf NTFS-Datenträgern können Sie die Speicherplatzbelegung über Kontingente (Quotas) verwalten, bei denen Sie einem Benutzer Speicherplatz zuweisen, den er auf dem Datenträger zum Speichern seiner Dateien verwenden kann. Die NTFS-Quotas gibt es seit zwei Jahrzehnten, inzwischen lassen sich solche Aufgaben jedoch viel effektiver über den Ressourcenmanager verwalten.


Schulversion
© HERDT-Verlag

## Ressourcen-Manager

Unter Windows Server 2019 besteht mit dem Ressourcen-Manager die Möglichkeit, festzulegen, welche Dateitypen auf einem bestimmten Laufwerk gespeichert werden dürfen. Wenn ein Benutzer versucht, verbotene Dateitypen zu speichern, lassen sich verschiedene Reaktionen vorgeben, etwa das Verbot der Speicherung oder eine E-Mail-Benachrichtigung an den Administrator. Die dynamische Zugriffssteuerung (Dynamic Access Control, DAC) ermöglicht durch die Klassifizierung von Dateien nach verschiedenen Kriterien (wie beispielsweise Speicherort, Zeitpunkt, Größe und Dateityp) eine effiziente Verwaltung von Dateiservern inklusive einer intelligenten Kontingentverwaltung. Die Klassifizierung kann sowohl automatisch durch die festgelegten Regeln erfolgen als auch manuell für bestimmte Ordner eingerichtet werden.

## Datenträgerdeduplizierung

Unter Windows Server 2012 wurde die Datenträgerdeduplizierung eingeführt. Mit dieser können Dateien, die mehrfach auf einem Datenträger liegen, erfasst werden. Dabei werden binär die Daten erfasst und die Unterschiede getrennt für jede Version eines Dokuments gespeichert. Hierdurch lassen sich die gespeicherten Datenmengen auf einer Festplatte z. T. erheblich reduzieren.

Seit Windows Server 2012 R2 wird Datenträgerdeduplizierung auch auf VHDX unterstützt, was die Verwendung mit Hyper-V möglich macht. So können z. B. die Systemdatenträger mehrerer VMs dedupliziert werden.

## NTFS

NTFS ist das Standard-Dateisystem unter Windows und ist seit Windows Vista weitgehend unverändert geblieben. Unter Windows Server 2019 sind alle vorhandenen NTFS-Funktionen nutzbar und keine weiteren dazugekommen.

## ReFS

Seit Windows Server 2012 ist mit dem **Re**silient **F**ile **S**ystem (robustes Dateisystem, ReFS) ein neues Dateisystem hinzugekommen, das vor allem für die Bereitstellung von Dateien im Netzwerk geeignet ist. Bei ReFS wird die traditionelle Trennung von lokaler NTFS-Zugriffsberechtigung und Freigabeberechtigung in einem neuen Konzept zusammengeführt. ReFS wird zunächst parallel zu NTFS eingesetzt, soll es langfristig jedoch vollständig ersetzen. ReFS wird ständig weiterentwickelt und wird im Funktionsumfang noch zulegen.

Die Maximalwerte für Dateigröße, Partitionsgröße und Dateianzahl entsprechen mindestens denen von NTFS oder übertreffen sie deutlich, z. B. dürfen Dateinamen statt 255 Zeichen nun 32.785 Zeichen lang sein.

ReFS baut auf NTFS auf, verzichtet jedoch auf einige wenig genutzte Funktionen von NTFS. In absehbarer Zukunft soll NTFS von ReFS ersetzt werden, bisher ist es jedoch noch nicht möglich, von ReFS-Partitionen zu booten. Auch für die Systempartition wird weiterhin NTFS benötigt.

# 3 Installation

**In diesem Kapitel erfahren Sie**

- was Sie vor einer Installation von Windows Server 2019 beachten sollten
- wie Sie die Installation durchführen

**Voraussetzungen**

- Installieren und Konfigurieren eines PCs
- Grundlagen des Netzwerkbetriebs

## 3.1 Vorüberlegungen zur Installation

### Hardware-Voraussetzungen

Windows Server 2019 ist nur als 64-Bit-Version erhältlich. Die Mindestanforderungen für alle Editionen sind ein 64-Bit-Prozessor mit mindestens 1,4 GHz, 512 MB RAM und wenigstens 32 GB freier Festplattenplatz. Die **empfohlenen** Hardwarevoraussetzungen richten sich nach den Aufgaben und liegen in der Regel **erheblich** darüber.

Der minimale freie Speicherplatz kann erheblich über den 32 GB liegen, wenn das System über mehr Arbeitsspeicher verfügt, da dieser die Größe der Auslagerungsdatei bestimmt.

| Hardware | Minimale Ausstattung |
|---|---|
| Prozessor | x64-CPU ab 1,4 GHz, empfohlen ab 2 GHz |
| Hauptspeicher | 512 MB, empfohlen 2 GB RAM |
| Freier Speicherplatz | 32 GB |
| Dateisystem | NTFS |
| Netzwerkadapter | mindestens 1 |
| DVD-ROM | alternativ von USB bootfähig |

Auf die Hardwarevoraussetzungen für den Hostcomputer der Testumgebung dieses Buches wird im Folgenden noch eingegangen.

### Vor- und Nachteile von Aktualisierung und Neuinstallation

| Aktualisierung einer früheren Windows-Version | Neuinstallation |
|---|---|
| **Vorteil:**<br>Bereits installierte Software wird automatisch erkannt und integriert. Dies ist z. B. bei Datenbanken von Vorteil.<br>Lokale Benutzerkonten, Benutzereinstellungen und die Konfiguration werden übernommen. | **Vorteil:**<br>Eine saubere Neuinstallation bereinigt das System von Altlasten wie temporären Dateien oder alten Treibern.<br>Eine neue Berechtigungsstruktur lässt sich leichter implementieren.<br>Für eine virtualisierte Umgebung ist es von Vorteil, wenn das Hostsystem außer Hyper-V keine weiteren Dienste und Rollen ausführt. |
| **Nachteil:**<br>Eine Installation mit einer älteren Betriebssystemversion entspricht nur selten den heutigen Anforderungen. Insbesondere für die Virtualisierung werden aktuelle Hardwarekomponenten mit modernen Funktionen benötigt. | **Nachteil:**<br>Ihre gesamte Software muss unter Windows Server 2019 neu installiert werden.<br>Benutzer und andere Ressourcen einer Domäne müssen zu Windows-Server-2019-Domänen migriert werden. |


Schulversion
© HERDT-Verlag

Sehen Sie in einer Produktivumgebung davon ab, Windows Server 2019 mit einem anderen Betriebssystem in Multiboot-Konfiguration zu betreiben, denn daraus ergeben sich zusätzliche Fehlerquellen und Sicherheitslücken. Kompatibilitätsprobleme lassen sich außerdem mit virtuellen Maschinen meist leichter beheben.

Die Migration einer Domäne lässt sich deutlich vereinfachen, indem der neue Server als zusätzlicher Domänencontroller installiert wird und anschließend die erforderlichen Dienste konfiguriert werden. Dies geht mit Windows Server 2019 bei Domänen ab Windows Server 2008 R2.

## Installationsverfahren anhand der Serverrolle auswählen

Abhängig von der Rolle (allein stehender Server, Mitgliedsserver oder Domänencontroller), die der Server im Netzwerk übernehmen soll, und dem Vorhandensein eines älteren Betriebssystems auf Ihrem Rechner müssen Sie das geeignete Installationsverfahren auswählen:

| Ausgangssituation und Zielsetzung | Installationsverfahren |
|---|---|
| Ein Netzwerk unter einer Vorgängerversion von Windows ist nicht vorhanden. Mit der Installation des Windows Servers 2019 wird der Aufbau eines Windows-Netzwerks begonnen. | Neuinstallation von Windows Server 2019 auf einem geeigneten Computer |
| Ein Netzwerk unter einer Vorgängerversion von Windows ist vorhanden. Die Station verwendet einen 64-Bit-Prozessor und soll ihre bisherige Rolle im Netzwerk beibehalten. Windows Server 2019 soll Vorgängerversionen von Windows Server ersetzen. Das Windows-Netzwerk soll bleiben, wie es ist. | Aktualisierung des Servers |
| Der Server war bisher Domänencontroller unter einer Vorgängerversion von Windows. Gleichzeitig soll das Netzwerk zu Windows Server 2019 migriert werden. Windows Server 2019 soll Vorgängerversionen von Windows Server ersetzen. | Migration; diese sehr komplexe Aufgabe wird am besten in Teamarbeit von erfahrenen Administratoren der vorhandenen Systeme durchgeführt. |

## Dateisystem auswählen

Als Dateisystem kommt zur Installation eines Servers ausschließlich NTFS infrage. Ältere Dateisysteme sind nicht empfehlenswert oder werden nicht mehr unterstützt.

Das neue Dateisystem ReFS kann für die Windows-Installation nicht verwendet werden. Auch unterstützt ReFS einige Besonderheiten von Windows Server 2019 noch nicht (zum Beispiel Schattenkopien) und ist somit derzeit nur eingeschränkt empfehlenswert. Für einzelne Serverdienste empfiehlt Microsoft aber ReFS. Hier sollte vor der Installation die Dokumentation des entsprechenden Serverdienstes zu Rate gezogen werden.

ReFS (Resilient File System, unverwüstliches Dateisystem) ist in der Lage, defekte Dateien automatisch zu reparieren. Außerdem gilt ReFS im Vergleich zu NTFS als wesentlich unempfindlicher gegenüber Abstürzen des Betriebssystems oder dem Ausschalten des Servers ohne vorheriges Herunterfahren. Sie können auch in der Befehlszeile oder der PowerShell die Formatierung durchführen und ReFS verwenden. Dazu nutzen Sie den Befehl

`Format /fs:ReFS <Laufwerksbuchstabe>:` oder

`Format-Volume -DriveLetter <Buchstabe> -FileSystem ReFS -Full` in der PowerShell.

Eine Schnellformatierung führen Sie in der Befehlszeile mit `Format /fs:ReFS /q <Buchstabe>:` durch.

Sie können für Software-RAIDs in Windows Server 2019 auch das ReFS-Dateisystem verwenden. Die Erstellung und Verwaltung ist identisch mit der Verwendung von NTFS.

## Größe der Installationspartition

Für eine Neuinstallation von DVD-ROM sollten Sie in der Praxis mindestens 40 GB freien Speicherplatz zur Verfügung stellen und nicht nur das von Microsoft vorgegebene Minimum von 32 GB verwenden (siehe Tabelle oben). Einige Serverrollen wie z. B.

- die Windows-Bereitstellungsdienste (WDS),
- die Windows Server Update Services (WSUS) oder
- Datenbanken

benötigen viel zusätzlichen Speicherplatz, den Sie jedoch bevorzugt auf einem anderen Datenträger bereitstellen sollten.

In der Testumgebung erhalten die virtuellen Maschinen dynamische virtuelle Datenträger mit 127 GB (Standardwert), die während der Installation partitioniert werden. Die Systempartition erhält 40.000 MB, der restliche Speicherplatz wird später partitioniert. Da sich die VHDX-Datei dem Füllstand der virtuellen Festplatte dynamisch anpasst, wird auf dem physischen Datenträger des Hosts wesentlich weniger Speicherplatz benötigt.

## Lizenzierung

Die Lizenzierung erfolgt nicht mehr auf Basis der CPUs, sondern 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 2019 Standard dürfen Sie pro Lizenz zwei VMs installieren, Windows Server 2019 Datacenter kennt kein Limit. Hier müssen Sie lediglich alle Prozessorkerne des Servers lizenzieren.

Lizenzen von Windows Server 2019 sind direkt auf die physische Hardware gebunden. Jede Lizenz deckt zwei physische Prozessorkerne ab. Sie dürfen mit der Standard Edition außerdem bis zu zwei virtuelle Server auf dem lizenzierten Host betreiben. Beim Einsatz der Datacenter Edition dürfen Sie so viele virtuelle Server auf dem Host betreiben, wie die Hardware hergibt.

Unter Windows Server 2019 können Sie für Client-Zugriffslizenzen zwischen dem Modus **pro Gerät oder pro Benutzer** und **pro Server** wählen:

| | |
|---|---|
| Pro-Gerät- oder Pro-Benutzer-Lizenz (CALs) | Wählen Sie diesen Lizenzmodus, um **Client-Computer** oder **Benutzer** in Ihrem Netzwerk mit einer Client-Zugriffslizenz auszustatten. Dieser Modus ersetzt die bisherigen Pro-Arbeitsplatz-Lizenzen.<br>Sie können Zugriffslizenzen entweder für jeden Benutzer oder für jeden Client-Computer erwerben, je nachdem, welches Modell besser zu Ihrem Unternehmen passt. |
| Pro-Server-Lizenz | Bei dieser Lizenzierungsart werden Client-Zugriffslizenzen den jeweiligen Servern zugeteilt. Damit erlaubt der einzelne Server die betreffende Zahl gleichzeitiger Verbindungen. Jeder weitere Server erfordert erneut die betreffende Anzahl an Client-Zugriffslizenzen. |
| Server-Lizenz:<br>je zwei CPU-Sockel | Bei den Editionen Standard und Datacenter sind die Lizenzen für Windows Server 2019 in Paketen erhältlich. Jede Lizenz gilt für bis zu zwei physische Prozessoren auf einem physischen Server. Bei der Standard-Edition dürfen pro Lizenz insgesamt zwei Instanzen von Windows Server 2019 auf einem Server laufen, bei der Datacenter-Edition ist die Anzahl der (virtuellen) Instanzen unbegrenzt. |


Schulversion
© HERDT-Verlag

Je größer das Netzwerk ist und je mehr Server vorhanden sind, desto größer ist der Preisvorteil der Lizenzierung nach dem Modell pro Gerät bzw. Benutzer. Für jeden Client oder Benutzer wird dann unabhängig von der Anzahl der Server im Netzwerk nur eine CAL benötigt. Sie können deshalb vom Pro-Server-Modus einmalig zum Modus pro Gerät oder pro Benutzer wechseln.

Für größere Unternehmen besteht darüber hinaus die Möglichkeit, über das Volume Licensing Program von Microsoft die Lizenzverwaltung zu vereinfachen und wirtschaftlich zu optimieren.

Da es bei Windows Server 2019 keine Web-Server-Edition mehr gibt, sind zum Ausgleich für den Betrieb einer Standard- oder Datacenter-Edition als Webserver keine weiteren CALs erforderlich.

## 3.2 Informationen für die Installation sammeln und auswerten

### Hardware-Informationen sammeln

Stellen Sie sicher, dass die Hardware Ihres Rechners von Windows Server 2019 unterstützt wird. Nicht unterstützte Geräte können Probleme verursachen. Verwenden Sie möglichst nur Hardware, die für Windows Server 2019 zertifiziert ist. Wenn Sie neue Hardware für Windows Server 2019 beschaffen, sollten Sie Ihren Händler darauf hinweisen.

Halten Sie für Festplatten-Controller (SATA-RAID oder SAS beispielsweise) die notwendigen Treiber bereit!

Beachten Sie, dass

- für neuere Hardware unter Umständen noch keine passenden Treiber verfügbar sind. In vielen Fällen können Sie Treiber für Vorgängerbetriebssysteme verwenden. Achten Sie stets darauf, die jeweiligen 64-Bit-Treiber zu verwenden. Besonders bei älteren Treibern leistet hier der Kompatibilitätsassistent wertvolle Dienste. Falls dies nicht ausreicht und Windows den Treiber nicht akzeptiert, können Sie als letztes Mittel die Konfigurationseinträge in den INF- und INI-Dateien verändern.
- Windows Server 2019 keine Installation auf Datenträgern unterstützt, die zu einem Speicherpool zusammengefasst sind. Dieser muss zuvor aufgelöst werden.

### Informationen zum bestehenden Netzwerk sammeln

Für die Installation eines Windows Server 2019 in einem bestehenden Netzwerk benötigen Sie Folgendes:

- Einen Computernamen, der in der Domäne einmalig ist. Erfragen Sie den Namen gegebenenfalls bei Ihrem Administrator. Der Name wird erst nach Abschluss der Installation angepasst.
- Typ und Einstellungen der installierten Netzwerkkarte
- Für die Nutzung der Windows-Update-Funktion schon während der Installation benötigen Sie DHCP. Nach der Installation ist es empfehlenswert, dem Server eine statische IP-Adresse zuzuweisen, die im Netzwerk noch nicht vergeben ist. Dazu benötigen Sie die IP-Adressen von DNS-Server und Standardgateway. Dies gilt sowohl für die IPv4- als auch für die IPv6-Adressen.
- Für die Anbindung an eine bestehende Windows-Domäne benötigen Sie den Namen der Domäne und die Anmeldeinformationen eines Domänenbenutzers. Falls Sie den Server zum Domain Controller machen wollen, benötigen Sie die Anmeldeinformationen eines Domänen-Admins.
- Für die Anbindung an andere Netzwerksysteme wie Linux sollten Sie über gültige Accounts im jeweiligen System verfügen. Zusätzlich müssen Sie nach der Installation darauf achten, die entsprechende Client-Software bzw. die entsprechenden Netzwerkprotokolle zu installieren.

### Installationsart auswählen

Je nach Ausstattung des Rechners, der installiert werden soll, und seiner Umgebung können Sie aus verschiedenen Datenträgern für die Installation den geeigneten auswählen:

Die Installation von einer DVD-ROM ist die einfachste Methode. Dabei booten Sie den Rechner von DVD und das Setup-Programm wird direkt von der DVD ausgeführt. Diese Installationsart wird in Kapitel 4 ausführlich beschrieben.

Noch schneller geht es, wenn Sie den Inhalt der DVD auf einen schnellen USB-Stick kopieren und von diesem aus booten. Die Erstellung eines USB-Sticks lohnt sich vor allem bei häufigen Windows-Installationen.

### Installation über das Netzwerk vorbereiten

Eine Installation über das Netzwerk ist nur in größeren Netzwerken mit zahlreichen Servern sinnvoll, in kleineren Umgebungen ist es effizienter, die wenigen Server per DVD oder USB-Stick zu installieren. Für eine Installation über das Netzwerk werden folgende Gegebenheiten benötigt:

- Windows-Bereitstellungs-Server (Windows Distribution Services, WDS)
- DHCP-Server
- PXE-fähiger Netzwerkadapter
- BIOS-Unterstützung für das Booten vom Netzwerk
- ISO-Abbild oder Installations-DVD Windows Server 2019

## 3.3 Die Installation vorbereiten

### Hardwareanforderungen für den Host der Testumgebung

Für die Testumgebung in diesem Buch werden drei virtuelle Hyper-V-Maschinen benötigt, die gleichzeitig laufen sollen. Um die Testumgebung aufbauen und in angemessener Geschwindigkeit betreiben zu können, benötigen Sie einen Rechner mit folgender Ausstattung:

- Prozessor mit zwei oder mehr Kernen,
- Virtualisierungsfunktion **AMD-V** bzw. Intels **VT-x** verfügbar und im BIOS aktiviert,
- 8 GB Hauptspeicher,
- wenigstens 120 GB freie Festplattenkapazität,
- eine SSD oder mehrere herkömmliche Festplatten zur Verteilung der Daten für die VMs.

Leistungsfähige Notebooks mit SSD sind ebenso gut geeignet wie Workstations mit ausreichender Speicher- und Festplattenausstattung. Mit weniger als 8 GB Hauptspeicher und nur einer herkömmlichen Festplatte wird das Arbeiten zur Geduldsprobe, die Prozessorgeschwindigkeit ist hingegen zweitrangig.

Wenn Sie über mehrere Festplatten verfügen, sollten Sie in Erwägung ziehen, die schnellsten Festplatten nicht für das Hostsystem zu verwenden, sondern für die virtuellen Maschinen. Im Betrieb greifen vor allem die VMs auf die Festplatte zu, währen das beim Host nur der Fall ist, wenn der Hauptspeicher zur Neige geht.

Sie benötigen für die VMs keine separaten Festplattenpartitionen, da Sie mit virtuellen Festplattendateien im VHD- oder VHDX-Format arbeiten, die Sie an beliebigen Orten anlegen können. Im Idealfall verfügen Sie über vier Festplatten: eine für den Host und eine für jede VM. Noch komfortabler und schneller ist der Einsatz einer SSD. Für jede Server-Installation werden etwa 30 GB benötigt, eine SSD mit 120 GB ist also knapp ausreichend, optimal wäre allerdings die doppelte Größe. Ein modernes Notebook mit Intel i3 oder vergleichbarem Prozessor mit 8 GB Speicher und einer SSD ist für die Testumgebung gut geeignet.


Schulversion
© HERDT-Verlag

Für die Erweiterung der Testumgebung im HERDT-Buch *Windows Server 2019 – Erweiterte Netzwerkadministration* ist zusätzlicher Speicherplatz von etwa 80 GB erforderlich. Sie können durch das Löschen von nicht mehr benötigten Snapshots einen Teil des zusätzlichen Speicherplatzes zurückgewinnen, dennoch reichen 120 GB definitiv nicht aus. Mit 200 GB freiem Speicherplatz sind Sie gut versorgt.

Die Virtualisierungsfunktionen müssen im BIOS freigeschaltet sein. Bei manchen PCs und Notebooks kann die Virtualisierung nicht aktiviert werden, obwohl die CPU alle Funktionen beherrschen würde.

Bei Neuanschaffungen sollten Sie darauf achten, dass die Systeme auch die erweiterte Speicheradressierung (Second Level Address Translation, SLAT) beherrschen. Diese Funktion ist zwar für die Virtualisierung unter Windows Server 2019 nicht zwingend erforderlich, erhöht aber die Geschwindigkeit und Zukunftssicherheit. Bei Intel wird SLAT als Extended Page Table (EPT) bezeichnet, AMD verwendet den Begriff Rapid Virtualization Indexing (RVI). Bei Intel verfügen alle aktuellen Xeon-Server-CPUs und Desktop-CPUs der Reihen i3, i5 und i7 über SLAT. Bei AMD besitzen alle Desktop-Prozessoren ab 2009 und alle Barcelona-basierten Opteron-Server-CPUs ab Mitte 2007 diese Funktion.

### Multiboot-Umgebung

Wenn Sie ein bereits installiertes Betriebssystem behalten möchten, können Sie auch eine Multiboot-Umgebung in Erwägung ziehen. Für eine Testumgebung kann eine Parallelinstallation sinnvoll sein, bei einem Server in einer Produktivumgebung sollten Sie jedoch möglichst kein Multiboot verwenden.

Greifen Sie in Multiboot-Konfigurationen später nicht auf die Systempartition des bereits vorhandenen Betriebssystems zu und legen Sie dort auch keine Daten ab. Denken Sie auch an eine Sicherung der wichtigen Daten vor der Installation.

## Auswahl der Serverversion für die Übungen

Für die Testumgebung ist es am sinnvollsten, mit einer Testversion des Servers zu arbeiten. Die Nutzung ist auf einen Testzeitraum von 180 Tagen beschränkt. Sie können den Testzeitraum übrigens nicht mehr mit dem altbekannten Befehl `slmgr.vbs -rearm` verlängern!

Die 180-Tage-Testversion ist kostenlos als ISO-Image zum Download erhältlich unter

*https://www.microsoft.com/de-de/evalcenter/evaluate-windows-server-2019*

Sie benötigen ein Microsoft-Konto für die Registrierung.

Wenn Sie in der Übungsumgebung eine Virtualisierung durchführen möchten, empfiehlt sich der Einsatz der Windows Server 2019 Datacenter-Edition, damit Sie alle Funktionen zur Verfügung haben.

Der Server muss weiterhin innerhalb der ersten Tage aktiviert werden. Hierzu benötigen Sie keinen gültigen Produktschlüssel, es reicht aus, dass das Betriebssystem Verbindung zum Internet herstellen kann.

## Anfertigen eines Installationsmediums

Um einen bootfähigen Datenträger zu erstellen, benötigen Sie folgende Dinge:

- einen DVD-Rohling oder einen USB-Stick mit 8 GB Speicherkapazität,
- ein ISO-Abbild der Windows-Server-2019-Installations-DVD, das Sie bei Microsoft herunterladen können,
- das Windows USB/DVD Download Tool, das Sie bei Microsoft kostenlos herunterladen können.

- Installieren und starten Sie die Software.
- Geben Sie den Pfad zum ISO-Abbild an.
- Legen Sie einen DVD-Rohling in Ihr optisches Laufwerk ein und wählen Sie dieses als Ziel aus.
  Die Software brennt daraufhin eine bootfähige Installations-DVD.

Alternativ können Sie als Ziel auch einen USB-Stick mit mindestens 8 GB auswählen. Alle Daten gehen bei der Formatierung verloren. Nach der Formatierung werden die Installationsdateien automatisch kopiert.

Bedenken Sie, dass Sie die virtuellen Maschinen der Testumgebung nicht von einem USB-Stick installieren können, da Hyper-V keine USB-Laufwerke kennt. DVD-Laufwerke und ISO-Abbilder können Sie dagegen in die Hyper-V-Umgebung einbinden.

## Windows Server 2019 von DVD-ROM installieren

Um das Betriebssystem zu installieren, müssen Sie einmalig vom Installationsmedium booten. Für solche Fälle verfügen die meisten Systeme über eine Taste, mit der Sie für den nächsten Bootvorgang das Bootmedium auswählen können. Oft sind dies die Tasten F11 oder F12, möglich sind auch F8 oder Esc. Alternativ können Sie auch die Bootreihenfolge im BIOS dauerhaft verändern:

- Starten Sie den Rechner und betätigen Sie die entsprechende Taste, um in das BIOS-Setup zu gelangen.
- Je nach BIOS kann dies Entf, F1, F2, Esc oder F10 sein. Achten Sie auf Einblendungen während des Bootvorgangs oder konsultieren Sie die Dokumentation des Mainboard- oder System-Herstellers.
- Legen Sie die Windows-Server-2019-DVD in Ihr optisches Laufwerk ein.
- Bestimmen Sie das Laufwerk mit der eingelegten DVD zum Boot-Datenträger und speichern Sie die Einstellungen ab.

  Die Schritte dazu unterscheiden sich je nach BIOS und Mainboard. Der Rechner startet automatisch neu.
- Falls Sie dazu aufgefordert werden, betätigen Sie eine beliebige Taste, um das Windows-Setup von DVD zu starten.

  Eine Minimalversion von Windows wird geladen und der Setup-Bildschirm erscheint.

Im BIOS-Setup ist die Tastatur meistens auf amerikanische Tastaturbelegung eingestellt. Sie müssen also für eine Bestätigung mit *Y* die Taste Z betätigen.

## Windows Server 2019 von USB-Stick installieren

- Stecken Sie den Installations-Stick in einen USB-Anschluss.
- Starten Sie den Rechner neu und stellen Sie, wie oben beschrieben, im BIOS oder Bootmenü *USB* als Bootmedium ein.
- Booten Sie vom USB-Datenträger.

### USB-Stick vorbereiten

Die Installationsdateien belegen etwa einen Platz von 3,5 GB.

- Starten Sie eine Eingabeaufforderung über das Kontextmenü im Administratormodus.
- Geben Sie `diskpart` ein.
- Geben Sie `list disk` ein.
- Geben Sie den Befehl `select disk` <Nummer des USB-Sticks aus list disk> ein.

  Sie erkennen den Stick an dessen Größe
- Geben Sie `clean` ein.
- Geben Sie `create partition primary` ein.
- Geben Sie `active` ein, um die Partition zu aktivieren.

  Dies ist für den Bootvorgang notwendig, denn nur so kann der USB-Stick booten.
- Formatieren Sie den Datenträger mit `format fs=fat32 quick`.
- Geben Sie den Befehl `assign` ein, um dem Gerät im Explorer einen Laufwerksbuchstaben zuzuordnen.
- Beenden Sie Diskpart mit `exit`.


Schulversion
© HERDT-Verlag

- Kopieren Sie den kompletten Inhalt der Windows Server 2019-DVD/ISO-Datei in den Stammordner des USB-Sticks. Anstatt der Datei „install.wim“ aus dem Verzeichnis „sources“ kopieren Sie aber die beiden erstellten SWM-Dateien.

  Der Installationsassistent erkennt die Dateien, und verwendet Sie, wie die „install.wim“.
- Booten Sie einen Computer mit diesem Stick, startet die Windows Server 2019-Installation.

## 3.4 Windows Server 2019 installieren

### Überblick

Die Installation von Windows Server 2019 ist sehr einfach, denn es müssen nur wenige Abfragen beantwortet werden. Nach Abschluss der Installation können Sie weitere Einstellungen vornehmen. Im Folgenden wird beschrieben, wie Sie eine Neuinstallation auf einem Rechner ohne vorhandenes Betriebssystem mit einer DVD durchführen.

### Die erste Stufe der Installation

Eine Standardinstallation umfasst die im Folgenden beschriebenen Schritte. Je nachdem, welche Art der Installation Sie durchführen bzw. welche Einstellungen Sie im Verlauf der Installation vornehmen, kann die Zahl der eingeblendeten Dialogbildschirme und Dialogfenster jedoch variieren.

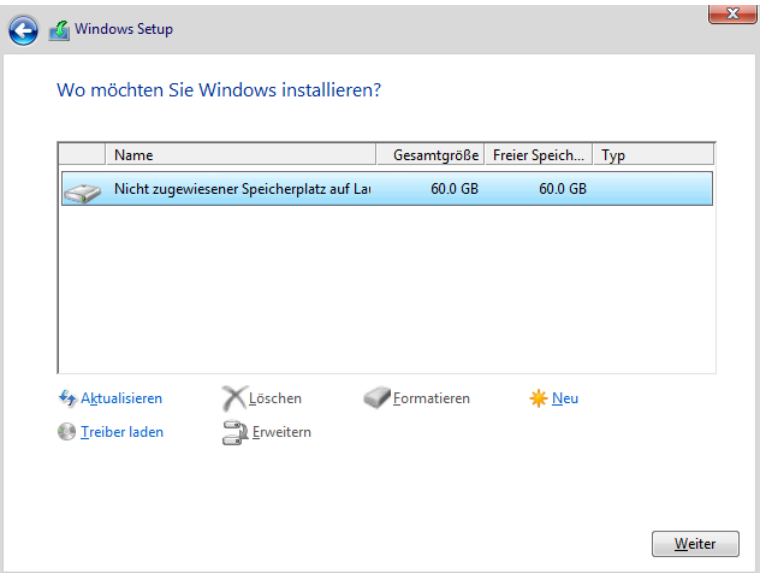
- Kontrollieren Sie die Spracheinstellungen und klicken Sie dann auf *Weiter*.
- Nehmen Sie die Spracheinstellungen in Österreich oder der Schweiz vor, dann verwenden Sie als Spracheinstellung DE – DE (nicht DE – AT), um Problemen, z. B. mit dem SQL-Server, vorzubeugen.
- Klicken Sie auf *Jetzt installieren*.
- Wählen Sie für die Testumgebung den Eintrag *Windows Server 2019 Datacenter (Server mit grafischer Benutzeroberfläche)* und klicken Sie auf *Weiter*.

  Stellen Sie später bei der Installation der Verkaufsversion für den Produktiveinsatz sicher, dass Sie zur gewählten Variante den benötigten Lizenzschlüssel besitzen! Eine spätere Korrektur ist nicht möglich und Sie müssen eine Neuinstallation vornehmen.
- Akzeptieren Sie die Lizenzbedingungen und klicken Sie auf *Weiter*.
- Wählen Sie als Installationsart *Benutzerdefiniert (erweitert).*

Setup zeigt Ihnen jetzt eine Liste der Partitionen bzw. Volumes, die unpartitionierten Bereiche sowie deren Gesamtgröße und freien Speicherplatz.

Wenn Sie sofort auf *Weiter* klicken, legt Windows neben der primären versteckten aktiven Startpartition in dem restlichen gesamten verfügbaren Speicherbereich auf dem Datenträger eine weitere Partition an, die zur Installation des Betriebssystems genutzt wird.

Unter *Laufwerkoptionen (erweitert)* können Sie Partitionen erstellen, löschen und formatieren.




*Auswahl des Installationsortes*

Sollte Windows den Festplattencontroller nicht erkennen, können Sie unter *Treiber laden* den vom Hersteller gelieferten Treiber installieren. Diesen benötigen Sie vor allem bei modernen Servern.

Für ein Produktivsystem kann es vorteilhaft sein, den Datenträger in System- und Datenpartitionen zu unterteilen. Beachten Sie, dass Windows standardmäßig alle Dateien auf der Systempartition abspeichert. Sie müssen also für jede Anwendung den Speicherort angeben.

In der Testumgebung ist es nicht nötig, auf der Systemfestplatte des Hostrechners mehrere Partitionen für die einzelnen virtuellen Maschinen anzulegen. Bei großen Festplatten kann es jedoch vorteilhaft sein, eine zusätzliche Backup-Partition für Serversicherungen oder ISO-Images anzulegen.

- Klicken Sie auf *Laufwerkoptionen (erweitert)* und dann auf *Neu*.
- Geben Sie die Größe der Partition in MB ein und klicken Sie auf *Übernehmen*.
- Bestätigen Sie die Meldung zur automatischen Einrichtung der kleinen Bootpartition mit *OK*.
- Markieren Sie die Partition, auf der Windows installiert werden soll, und klicken Sie auf *Weiter*.

  Die Partition wird automatisch mit NTFS formatiert und die Installation beginnt.

Das Installationsprogramm überprüft jetzt die Festplatten, kopiert die notwendigen Daten vom Datenträger auf die Festplatte und speichert die Konfigurationsdaten. Der Vorgang dauert einige Minuten.

## Abschluss der Installation

Nach einem Neustart fordert Windows Sie auf, ein Kennwort für das Konto *Administrator* zu setzen.

- Geben Sie zweimal ein gültiges Kennwort ein und klicken Sie auf *Fertig stellen*.

  Die Windows-Installation ist damit beendet.

In einer Testumgebung ist es sinnvoll, stets dasselbe Passwort zu verwenden. Das Passwort sollte acht Zeichen lang sein und muss den Komplexitätsrichtlinien entsprechen. Dazu muss es drei der folgenden vier Kategorien enthalten: Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen.

Verwenden Sie möglichst nur Zeichen, die Ihnen auch bei einer englischen Tastaturbelegung zur Verfügung stehen. Wenn Sie den Rechner ohne Tastaturtreiber hochfahren, werden Sie andernfalls Probleme bei der Passworteingabe bekommen.

Das Passwort muss mindestens drei Zeichen lang sein. Die Mindestlänge ist zwar noch auf null gesetzt, aber wegen der Komplexitätsanforderung muss das Passwort mindestens drei verschiedene Zeichen enthalten.

## Als Administrator lokal anmelden

Nach einer Neuinstallation ist der Computer noch nicht Mitglied einer Domäne. Das Konto des lokalen Administrators ist das einzig gültige Konto.

- Betätigen Sie Strg Alt Entf, um den Anmeldedialog anzuzeigen.
- Geben Sie das Kennwort des Administrator-Kontos ein.

  Sie werden angemeldet, gelangen auf den Desktop und der Server-Manager wird geöffnet.


Schulversion
© HERDT-Verlag

## 3.5 Upgrade von Standard- und Testversion auf Datacenter-Edition

Haben Sie Windows Server 2019 Standard installiert, können Sie auf die Datacenter-Edition aktualisieren. Sie müssen dazu Windows nicht neu installieren, die Aktualisierung kann im laufenden Betrieb erfolgen. Nach der Aktualisierung müssen Sie lediglich den Server neu starten.

Zunächst geben Sie in der Befehlszeile den u. a. Befehl ein, um zu überprüfen, ob eine Aktualisierung möglich ist.

Um die Aktualisierung von Standard zu Datacenter durchzuführen, geben Sie den Befehl `Dism /Online /Set-Edition:ServerDatacenter /AcceptEula /ProductKey:xxxxx-xxxxx-xxxxx-xxxxx-xxxxx` ein. Nach der Aktualisierung starten Sie den Server neu.

Sie haben auch die Möglichkeit, die Testversionen von Windows Server 2019 zu einer vollwertigen Version umzuwandeln. Ob es sich bei der Version um eine Testversion handelt, sehen Sie durch Eingabe des Befehls `slmgr.vbs /dlv`. Auch in der Testversion sehen Sie mit *`dism /online /Get-TargetEditions`*, auf welche Edition Sie aktualisieren können. Die aktuelle Edition lassen Sie mit `dism /online /Get-CurrentEdition` anzeigen.

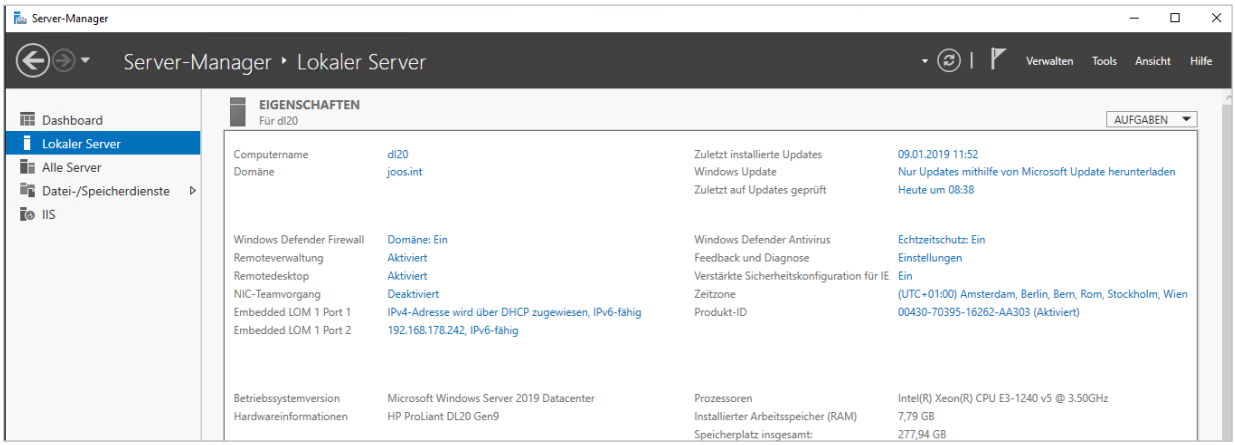
## 3.6 Erstkonfiguration des Hostrechners

### Die Erstkonfiguration vorbereiten

Windows Server fragt während der Installation keine Informationen ab, sondern ermöglicht die Anpassung nach der Installation. Dies sorgt für eine schnellere und unbeaufsichtigte Installation, da währenddessen keine Eingaben erforderlich sind.

Nach der erfolgreichen Anmeldung wird automatisch der Server-Manager geöffnet. In der linken Spalte können Sie durch die verfügbaren Seiten navigieren. Sie befinden sich auf der ersten Seite, dem **Dashboard**.

- Klicken Sie im Server-Manager in der linken Spalte auf *Lokaler Server*.

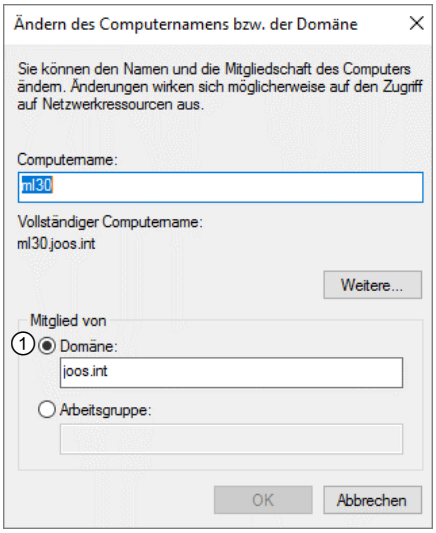



Zum Abschluss der Installation müssen am Hostrechner noch folgende Einstellungen vorgenommen werden:

- Computername und Arbeitsgruppe festlegen,
- IP konfigurieren,
- Windows Update konfigurieren,
- Windows aktivieren und ggf. Produktschlüssel eingeben.

## Computername und Arbeitsgruppe oder Domäne festlegen

Das Windows-Setup generiert bei der Installation automatisch einen Computernamen und macht den Rechner zum Mitglied der Arbeitsgruppe *WORKGROUP*. Im Server-Manager wird der Name des lokalen Servers angezeigt.




- Klicken Sie auf den Link neben *Computername*.
- Geben Sie einen in der Domäne bzw. Arbeitsgruppe eindeutigen Computernamen ein.

  Er darf maximal 15 Zeichen lang sein und sollte nur aus englischen Buchstaben, Ziffern und dem Bindestrich bestehen.
- Benennen Sie in der Testumgebung den Hostrechner.
- Unter *Weitere* können Sie das primäre DNS-Suffix des Rechners angeben.

  Beim Domänenbeitritt wird dort automatisch der Domänenname eingetragen.
- Ändern Sie bei Bedarf die Arbeitsgruppe.

  Beachten Sie die Vorgaben des Kursleiters.
- Für einen Domänenbeitritt aktivieren Sie Option ① und geben Sie den Namen und Anmeldeinformationen der Domäne ein.

Alle Veränderungen in diesem Fenster erfordern einen Neustart, den Sie sofort oder später durchführen können.

Für einen Domänenbeitritt müssen einige Voraussetzungen erfüllt sein:

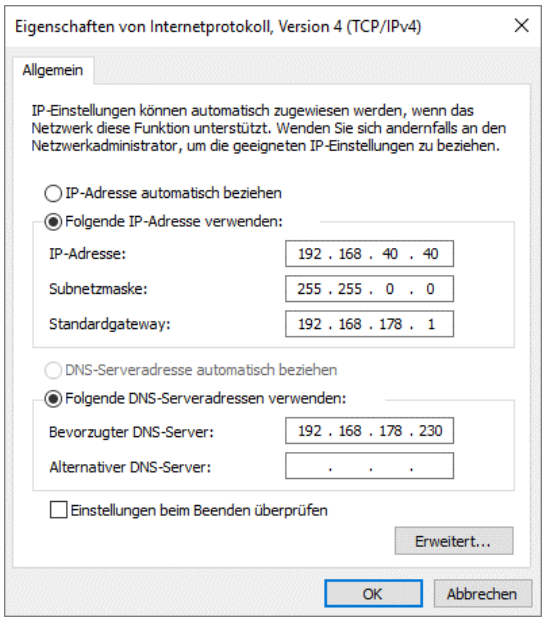
- ✔ Die IP-Konfiguration muss stimmen. Der Rechner muss mit einem passenden DNS-Server konfiguriert sein und Kontakt zu einem Domänencontroller herstellen können.
- ✔ In der Domäne muss entweder ein Computerkonto für den Rechner vorbereitet sein oder Sie benötigen ein Benutzerkonto, das über das Recht verfügt, Computerkonten der Domäne hinzuzufügen.

  In den Standardeinstellungen kann jeder Domänenbenutzer 10 Computer zur Domäne hinzufügen.

In der Testumgebung wird der Hostrechner nicht Mitglied einer Domäne. Er stellt lediglich die Ressourcen für die virtuellen Server zur Verfügung.

## IP konfigurieren

Wenn der Server kein DHCP-Client sein soll, müssen Sie dem Server jetzt eine IP-Adresse zuweisen. Die aktuelle IP-Konfiguration können Sie in der Eingabeaufforderung mit `ipconfig /all` anzeigen lassen. Befolgen Sie bei der Auswahl die Vorgaben des Kursleiters oder des zuständigen Administrators.




- Öffnen Sie die Netzwerkverbindungen, indem Sie im Server-Manager auf den Link neben *Ethernet* klicken.
- Öffnen Sie per Rechtsklick die Eigenschaften der angezeigten Verbindung.
- Öffnen Sie dort *Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)*.
- Aktivieren Sie *Folgende IP-Adresse verwenden* und geben Sie die IP-Adresse ein.
- Kontrollieren Sie die vorgeschlagene Subnetzmaske im Eingabefeld.
- Geben Sie die IP-Adresse des Routers ein.


Schulversion
© HERDT-Verlag

- Geben Sie in das Eingabefeld die IP-Adresse des bevorzugten DNS-Servers ein.
- Geben Sie optional in das Eingabefeld die IP-Adresse eines alternativen DNS-Servers ein.

Über *Erweitert* kommen Sie zu den erweiterten TCP/IP- Einstellungen. Dazu gehören:

- einem Netzwerkadapter mehrere IP-Adressen zuweisen,
- Verwendung mehrerer Router oder DNS-Servern,
- Verwendung verbindungsspezifischer DNS-Namen (bei mehrfach vernetzten Computern),
- Festlegen, ob und wie dynamische DNS-Aktualisierungen erfolgen.

## Windows Update konfigurieren

Da die VMs in der Testumgebung im Normalfall keinen Internetzugang haben, ist es vertretbar, dort auf Updates zu verzichten. Für den Host und alle VMs, die dauerhaften Internetzugang besitzen, sollten Sie manuell nach Sicherheitsupdates suchen und diese installieren.

- Klicken Sie neben *Windows Update* auf den Link und stellen Sie den gewünschten Modus ein.

## Verstärkte Sicherheitskonfiguration für den Internet Explorer ausschalten

Im Produktivbetrieb ist es sinnvoll, den Internet Explorer als potenzielles Einfallstor für Viren und Trojaner stark einzuschränken. In einer Testumgebung ist es vertretbar, wegen der zügigeren Internetrecherche auf die verstärkte Sicherheitskonfiguration zu verzichten.

- Klicken Sie neben *Verstärkte Sicherheitskonfiguration für IE* auf den Link *Ein*.

  Wählen Sie bei Administratoren und Benutzern die Option *Aus* und klicken Sie auf *OK*.

  Möglicherweise dauert es eine Weile, bis die Anzeige aktualisiert wird.

## Windows aktivieren

Beachten Sie, dass Sie für die Aktivierung einen Internetzugang benötigen. Bei der Verkaufsversion erhalten Sie bereits nach 2 Tagen die Aufforderung, Windows zu aktivieren, die 180-Tage-Testversion muss spätestens nach 10 Tagen aktiviert werden. wobei hier kein Produktschlüssel erforderlich ist. Sie müssen also auch bei den VMs dafür sorgen, dass diese wenigstens kurzzeitig bei der Einrichtung Zugang zum Internet haben.

- Klicken Sie neben *Produkt-ID* auf den Link.
- Geben Sie einen gültigen Produktschlüssel ein und klicken Sie auf *Aktivieren*.

  Nach wenigen Sekunden wird ein gültiger Schlüssel akzeptiert und Ihr Windows ist aktiviert.

### Ausführliche Erläuterung zur Aktivierung

Nach der Installation müssen Sie die Aktivierung von Windows Server 2019 durchführen. Mehr Informationen erhalten Sie auch, wenn Sie im Startmenü nach *slui* suchen. Sie können Windows Server 2019 entweder über das Internet aktivieren oder per Telefon. Bei der Aktivierung per Telefon werden Sie mit einem automatischen Telefonsystem verbunden.

Sollten Sie Probleme bei der Aktivierung bekommen, überprüfen Sie die Uhrzeit und die Zeitzone Ihres Servers. Sind die entsprechenden Einstellungen nicht korrekt, können Sie Windows nicht aktivieren.

### Mit `slui` und `slmgr` die Aktivierung steuern

Über den Befehl `slui 3` wird ein Dialogfeld geöffnet, um einen neuen Produktschlüssel einzugeben. Starten Sie das Tool über die Suchfunktion des Startmenüs mit Administratorrechten über das Kontextmenü. In diesem Bereich aktivieren Sie Windows Server 2019 dann mit dem neuen Key.

Der Befehl `slui 4` öffnet die Auswahl der Aktivierungshotlines. Wollen Sie sich die aktuelle Windows Server 2019-Edition anzeigen lassen, die auf dem Computer installiert ist, öffnen Sie eine Eingabeaufforderung mit Administratorrechten und geben den Befehl `dism /online /Get-CurrentEdition` ein. Sie erhalten daraufhin die Edition und weitere Information zur Installation angezeigt.

Wollen Sie anzeigen, zu welchen Editionen Sie die installierte Version aktualisieren können, verwenden Sie den Befehl `dism /online /Get-TargetEditions`.

Für die Verwaltung und die Abfrage von Lizenzinformationen auf Windows Server 2019-Computern stellt Microsoft das Skript *slmgr.vbs* zur Verfügung, welches Sie über die Eingabeaufforderung oder das Dialogfeld *Ausführen* aufrufen. Dieses starten Sie mit der Tastenkombination [⊞] [R]. Das Tool kennt verschiedene Optionen:

- `/ato` Windows online aktivieren
- `/dli` zeigt die aktuellen Lizenzinformationen an
- `/dlv` zeigt noch mehr Lizenzdetails an
- `/dlv all` zeigt detaillierte Infos für alle installierten Lizenzen an

Möchten Sie den Status der Aktivierung von Windows Server 2019 anzeigen, geben Sie in der Befehlszeile den Befehl `slmgr.vbs /dli` ein, und führen diesen aus. Anschließend werden der Name und die Beschreibung des Betriebssystems, aber auch ein Teil des Product Key und der Lizenzstatus angezeigt.

Haben Sie den Produktschlüssel eingetragen, fügen Sie die Aktivierung über die beschriebenen Wege durch. Verfügt der Computer über eine Internetverbindung, führt der Assistent die Aktivierung automatisch aus, sobald der korrekte Product Key eingegeben wurde. Sie können den Status der Aktivierung anschließend direkt einsehen, indem Sie `slui` eingeben. Hier wird auch das Datum der Aktivierung angezeigt.

## Aktivierung auf Core-Servern verstehen

Sie können den Product Key einer Windows Server 2019-Installation anpassen. Über diesen Weg aktivieren Sie Windows Server 2019 auch auf einem Core-Server:

Geben Sie zum Löschen des alten Product Key in der Eingabeaufforderung den Befehl `slmgr /upk` ein. Zwar ersetzen die nächsten Punkte den vorhandenen Product Key. Allerdings funktioniert das nicht immer, wenn nicht zuvor die alte Nummer gelöscht wurde. Bestätigen Sie das Löschen.

Den neuen Product Key geben Sie dann mit `slmgr /ipk xxxxx-xxxxx-xxxxx-xxxxx-xxxxx` ein. Mit `slmgr /ato` aktivieren Sie Windows Server 2019.

Da ein Core-Server über keine grafische Oberfläche verfügt, müssen Sie einen solchen Server über die Eingabeaufforderung aktivieren. Verwenden Sie zur lokalen Aktivierung des Servers den Befehl `slmgr.vbs -ato`. Nach Eingabe des Befehls wird die Aktivierung durchgeführt. Sie können Windows Server 2019 auch remote über das Netzwerk aktivieren. Verwenden Sie dazu den Befehl `slmgr.vbs <ServerName> <Benutzername> <Kennwort> -ato`.

Um einen Server lokal über das Telefon zu aktivieren, verwenden Sie den Befehl `slmgr -dti`. Notieren Sie sich die ID, die generiert wird, und rufen Sie die Aktivierungsnummer von Microsoft an. Geben Sie über die Telefontasten die ID ein und Sie erhalten vom Telefoncomputer eine Aktivierungs-ID. Diese geben Sie mit dem Befehl `slmgr -atp <Aktivierungs-ID>` ein.

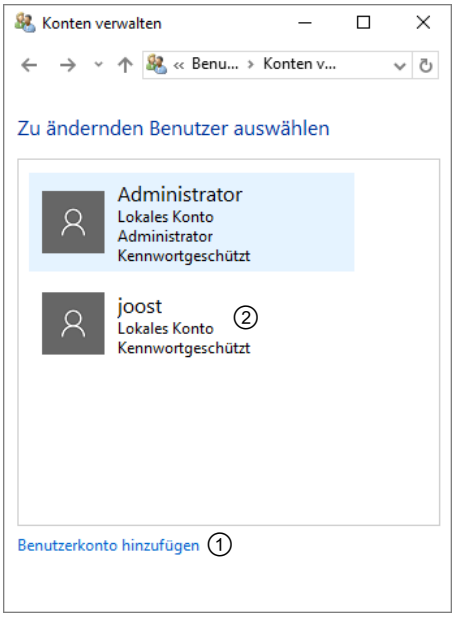
Sie können die Edition eines Core-Servers auch aktualisieren, indem Sie in der Eingabeaufforderung Änderungen vornehmen:

- Anzeigen der aktuell installierten Edition -- *dism /online /Get-CurrentEdition*
- Mögliche Editionen zur Aktualisierung -- *dism /online /Get-TargetEditions*
- Aktualisierung zur Zielversion durchführen -- *dism /online /Set-Edition:<edition ID> /ProductKey:<Seriennummer>*


Schulversion
© HERDT-Verlag

## Neues Administratorkonto erstellen

Sie sollten so wenig wie möglich mit dem Standardkonto *Administrator* arbeiten, daher benötigen Sie ein neues lokales Benutzerkonto mit Administratorrechten.




- Rufen Sie die Systemsteuerung auf und klicken Sie auf *Benutzerkonten\Benutzerkonten\Anderes Konto verwalten*.

  Die Systemsteuerung finden Sie am schnellsten, wenn Sie „Systemsteuerung“ im Suchfeld des Startmenüs eingeben.

  Der Dialog *Konto verwalten* wird geöffnet.
- Klicken Sie auf den Link *Benutzerkonto hinzufügen* ①.
- Geben Sie Ihren Namen für das Konto ein.

  Es ist sinnvoll, das Wort *Admin* anzuhängen, damit Sie ein zweites Konto mit Ihrem Namen erstellen können, das nur über normale Benutzerrechte verfügt.
- Geben Sie zweimal ein Passwort, das den Komplexitätsrichtlinien entspricht, und einen Kennworthinweis ein.
- Klicken Sie auf das neu erstellte Konto ②.
- Klicken Sie auf *Kontotyp ändern*.
- Wählen Sie als Kontotyp *Administrator* und klicken Sie auf *Kontotyp ändern*.
- Melden Sie sich mit dem neuen Konto an.

  Verwenden Sie das Konto *Administrator* ab sofort nur noch in Ausnahmefällen.

## Abschluss der Konfiguration

Nachdem Sie den Computernamen und die IP-Konfiguration geändert und alle anderen Einstellungen vorgenommen haben, müssen Sie den Computer neu starten.

- Überprüfen Sie, ob Namen und IP-Konfiguration korrekt sind und ob der Internet- und der Netzwerkzugang funktionieren.

Falls alles richtig eingestellt ist, können Sie mit der Installation der Hyper-V-Testumgebung fortfahren.

# 4 Bedienung und Neuerungen

**In diesem Kapitel erfahren Sie**

- wie Sie das Startmenü im Windows 10-Stil bedienen
- wie Sie Ihre Arbeitsgeschwindigkeit mit Tastenkürzeln steigern können
- welche Funktion der Server-Manager hat
- welche Neuerungen es sonst noch gibt

**Voraussetzungen**

- Grundkenntnisse in der Installation und Konfiguration eines PCs
- Installationsplanung und Vorbereitung für Windows Server 2019

## 4.1 Startmenü

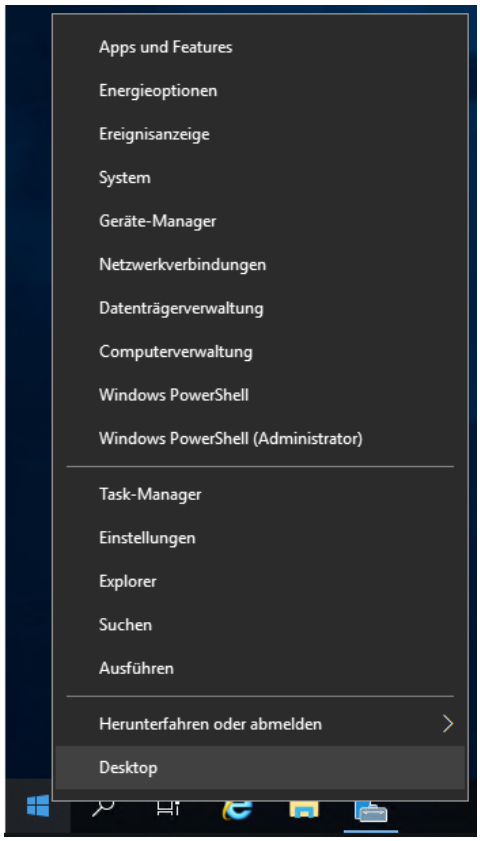
Das Startmenü von Windows Server 2019 entspricht im Wesentlichen dem von Windows 10 bekannten Stil.

### Bedienung des Startmenüs

Den Desktop gibt es auch bei Windows Server 2019 noch. Mit einem Klick auf das Desktop-Icon kann der Desktop angezeigt werden. Standardmäßig sind auf dem Server 2019 keine Windows-Apps, wie aus Windows 10 bekannt, verfügbar.

Auf dem Desktop befindet sich der Start-Button, über den auch ein **Schnellzugriffsmenü** gestartet werden kann. Dieses starten Sie über einen Rechtsklick auf die Start-Schaltfläche oder über ⊞ X. Von hier aus haben Sie Zugriff auf die wichtigsten Einstellungen von Windows Server 2019.

Die farbigen Rechtecke im Startmenü werden seit Windows Server 2012 R2 als **Kacheln** oder **Tiles** bezeichnet. Jede farbige Kachel repräsentiert dabei eine App, während alle Kacheln mit einem Desktop-Icon für eine Desktop-Anwendung stehen. Viele Kacheln zeigen wechselnde Inhalte, daher werden sie auch **Live-Kacheln** oder **Live Tiles** genannt. Diese werden aber vor allem in Windows 10 verwendet.

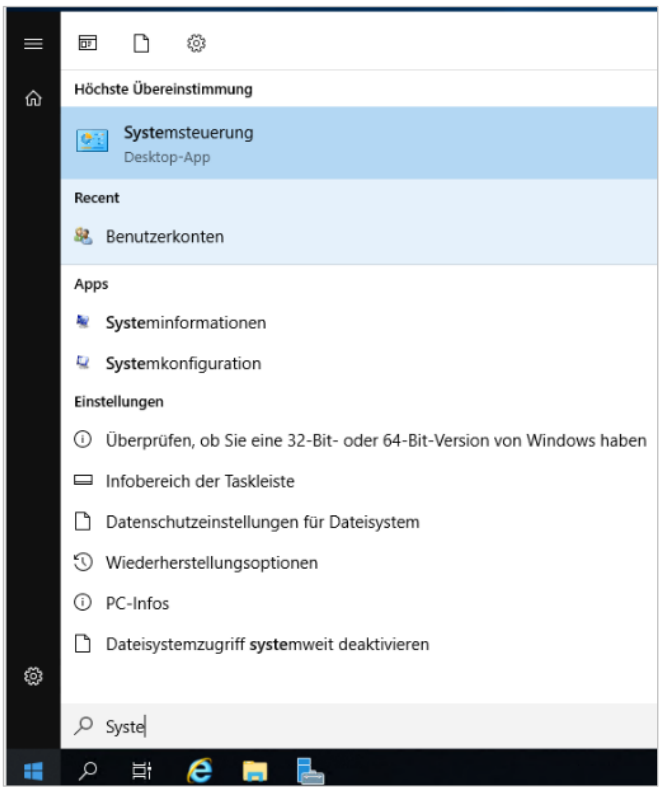



*Schnellzugriffsmenü*


Schulversion
© HERDT-Verlag

### Suchfunktion

Um nach Apps zu suchen, geben Sie im Startmenü sozusagen blind die ersten Buchstaben des gesuchten Programms oder den kompletten Namen ein. Noch während der Eingabe öffnet sich die Anzeige aller Apps, die dem Suchbegriff entsprechen. Jede geeignete App und jedes Windows-Programm meldet sich bei Windows an und wird dann in der Liste der durchsuchbaren Apps angezeigt.




*Suchen mit geeigneten Apps*

## 4.2 Windows Server 2019 mit Tastenkombinationen bedienen

Nach kurzer Zeit werden Sie in der Lage sein, relativ flüssig mit dem neuen System umzugehen und sich mit etwas Mühe wieder zurechtzufinden. Das neue Bedienungskonzept bietet möglicherweise die Chance, Ihre Produktivität zu steigern. Mit Tastenkombinationen kommen Sie direkt ans gewünschte Ziel. Zentraler Bestandteil ist dabei die Windows-Taste [⊞], die noch nie so nützlich war wie bei Windows Server 2019.

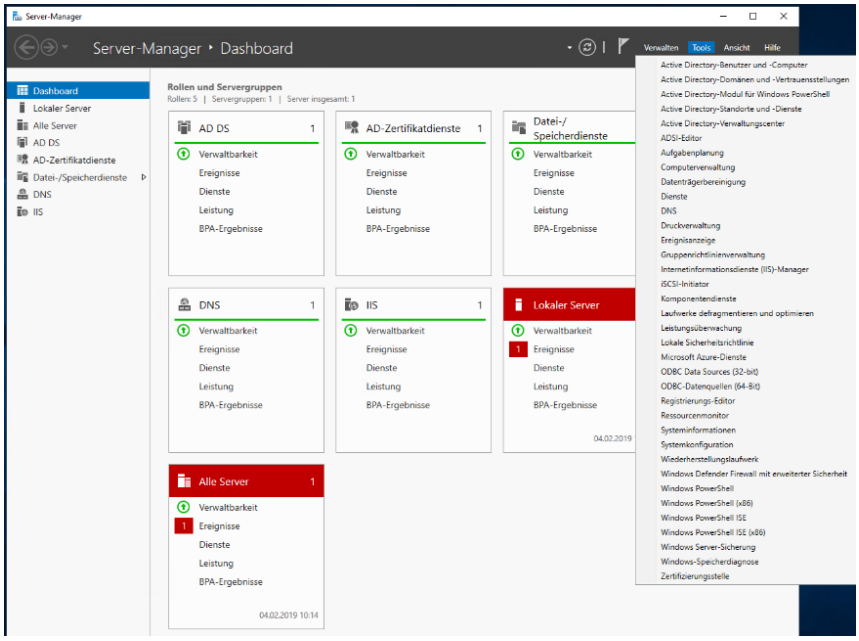
Mit Tastenkombinationen kommen Sie direkt ans gewünschte Ziel. Sie sollten die folgenden Tastenkombinationen ausprobieren und sich so viele wie möglich merken:

| Tastenkombination | Ergebnis |
|---|---|
| [⊞] [I] | Öffnet die Einstellungen |
| [Alt] [⇥] | Umschalten zwischen allen Anwendungen |
| [Alt] [F4] | Schließen von Desktop-Anwendungen |
| [⊞] [P] | Öffnet Einstellungen für Präsentation und zwei Monitore |
| [⊞] [X] | Öffnet das Schnellzugriffsmenü |
| [⊞] [K] | Öffnet die Seite zum Verbinden von Geräten |
| **Suchen** | |
| [⊞] [Q] | Nach Dateien und Anwendungen suchen |

| Tastenkombination | Ergebnis |
|---|---|
| **Sonstiges** | |
| ⊞ D | Zeigt den Desktop |
| ⊞ Druck | Speichert einen Screenshot im PNG-Format in *Bilder* |
| ⊞ Pause | Öffnet die Systemeigenschaften |
| ⊞ R | Befehl ausführen |
| ⊞ E | Öffnet ein Explorer-Fenster |

## 4.3 Server-Manager

Der Server-Manager dient zur Überwachung eines oder mehrerer Server und ist geeignet, neue Rollen (z. B. DNS-Server, Hyper-V, Domänencontroller) und Features (z. B. Bitlocker, BranchCache) hinzuzufügen und grundlegende Einstellungen vorzunehmen. Der Server-Manager erfordert für Umsteiger von Windows Server 2008 R2 etwas Eingewöhnungszeit. Viele erweiterte Einstellungen lassen sich nur noch über separate Anwendungen vornehmen, die über das Menü *Tools* erreichbar sind.




*Server-Manager mit dem Dashboard*

Der Server-Manager soll dem Administrator einen Überblick über die gesamte Serverinfrastruktur verschaffen, indem frei konfigurierbare Meldungen und Protokolle, Status- und Leistungsanzeigen nach Serverrollen gegliedert werden. Dies ist im täglichen Betrieb wichtiger als Einstellungen, die nur während der Einrichtung des Servers durchgeführt werden müssen.

### Zentrale Verwaltungsschnittstelle

Der Server-Manager ist jetzt deutlich stärker auf die Überwachung ausgerichtet als sein Vorgänger. So gibt er auf dem **Dashboard** einen schnellen Überblick und auf den einzelnen Seiten für jede Serverrolle einen genaueren Einblick in die Funktion, den Ressourcenverbrauch und mögliche Probleme. Manche Einstellungen lassen sich nur im Server-Manager ändern, andere erfordern den Aufruf der entsprechenden Konsole aus dem Menü *Tools* heraus. Die Konsolen lassen sich auch über die Eingabe eines Suchbegriffs oder des Dateinamens im Startbildschirm aufrufen. Über den Server-Manager lassen sich Remoteserver genauso überwachen wie der lokale Server.


Schulversion
© HERDT-Verlag

# 5 Hyper-V-Testumgebung

**In diesem Kapitel erfahren Sie**

- was Virtualisierung ist
- welche Voraussetzungen für eine Virtualisierung erfüllt sein müssen
- welche Vor- und Nachteile eine Virtualisierung mit sich bringt
- welche Serverrollen für die Virtualisierung geeignet sind
- wie Sie die Rolle *Hyper-V* auf einem Server hinzufügen
- wie Sie virtuelle Computer erstellen und einrichten
- wie Sie virtuelle Netzwerkumgebungen erstellen
- wie Sie die Testumgebung für die folgenden Übungen bereitstellen können

**Voraussetzungen**

- Hardwarekenntnisse
- Installation von Windows Server 2019
- Verständnis von Serverrollen

## 5.1 Virtualisierung

### Grundlagen der Virtualisierung

Virtualisierung bedeutet, eine reale Komponente durch ein virtuelles Abbild darzustellen. Dies kann in der IT eine Anwendung, eine bestimmte Funktion oder ein komplettes Betriebssystem sein. Bei der Anwendungsvirtualisierung wird z. B. eine Instanz einer Anwendung mit virtualisierten Eigenschaften ausgeführt. Dazu werden etwa temporäre Dateien, DLLs (Dynamic Link Library, dynamische Bibliotheken) oder Treiber in einen temporären Cache geladen und erlauben so einen stabilen Betrieb für mehrere unterschiedliche Instanzen der Anwendung, die andernfalls Konflikte verursachen würden.

### Servervirtualisierung

Die Virtualisierung von Servern beruht auf einer Trennung von Hardware und Betriebssystem. Die eigentliche Hardware wird von einem Server ausgeführt, der über seine HAL (Hardware Abstraction Layer) die physischen Komponenten des Systems steuert. Auf diesem Server werden nun virtuelle Systeme installiert, denen das Gastsystem eine scheinbare Hardwareumgebung vorspielt. So benötigen diese keine eigenen Treiber für die spezifische Hardware, sie können gemeinsam auf Komponenten zugreifen und im Bedarfsfall schneller gestartet werden. Durch sehr hardwarenahe Virtualisierung im Zusammenspiel mit den modernen Prozessoren können zahlreiche virtuelle Maschinen auf effiziente Weise auf einem Server laufen.

### Prüfpunkte

Mit Hyper-V können Sie jederzeit eine Momentaufnahme des Zustands einer virtuellen Maschine anfertigen. Momentaufnahmen werden auch als Snapshots und Prüfpunkte bezeichnet. Diese Prüfpunkte umfassen sowohl den Speicherinhalt als auch den Zustand der virtuellen Festplatte. Bei Bedarf können Sie jederzeit zu diesem Zustand zurückkehren. Diese Funktion macht die Verwendung virtueller Maschinen für Testumgebungen sehr attraktiv, weil sich etwa Konfigurationsprozesse oder Software-Installationen leicht wieder rückgängig machen lassen, wenn sie nicht das gewünschte Ergebnis bringen.

Bedenken Sie beim Umgang mit Prüfpunkten in Domänen, dass durch die Rückkehr zu einem früheren Zeitpunkt das Active Directory in einen inkonsistenten Zustand geraten kann. Fertigen Sie daher für alle beteiligten Server gleichzeitig einen Prüfpunkt an und vergeben Sie für alle Prüfpunkte Namen, aus denen hervorgeht, dass sie zusammenhängen. Falls dies versäumt wurde, können Sie die zusammengehörigen Prüfpunkte auch über das Erstellungsdatum identifizieren. In Windows Server 2019 hat Microsoft die neuen Produktions-Prüfpunkte integriert. Diese erfassen nicht nur die Konfiguration der VM, sondern auch den Zustand des virtuellen Betriebssystems. Dadurch lassen sich auch Prüfpunkte für virtuelle Datenbankserver und Domänencontroller einfacher erstellen.

## Live-Migration

Mit der aktuellen Hyper-V-Version ist es möglich, virtuelle Maschinen im laufenden Betrieb auf einen anderen Host zu verschieben. Dieser Vorgang ist für die Benutzer völlig transparent und erfordert weder Abschalten und Neustart noch irgendwelche Konfigurationsänderungen am virtuellen Server.

Trotz aller Fortschritte im Bereich der Live-Migration von VMs ist es immer noch nicht möglich, eine VM zwischen Hosts mit AMD-Prozessoren und Intel-Systemen zu migrieren. Eine neue Prozessor-Kompatibilitätsfunktion erlaubt immerhin den Wechsel zwischen verschiedenen Prozessorversionen des gleichen Herstellers. In produktiven Umgebungen sollten Sie aber ohnehin besser auf identische Server setzen.

## Server wiederherstellen

Sicherungen von Servern werden im VHD/VHDX-Format unterstützt. Da dieses auch von Hyper-V verwendet wird, können gesicherte Server als virtuelle Maschinen wiederhergestellt werden. So kann bei Ausfall von systemrelevanter Hardware (z. B. Mainboard) der Server trotzdem schnell wieder verfügbar gemacht werden.

## Cluster

Von besonderer Bedeutung ist die Virtualisierung auf Clustern. Cluster sind Verbünde von Rechnern, die auf ein gemeinsames Speichermedium (Quorum) zugreifen. Hierdurch können auch Komponenten wie Mainboard, Prozessor und Speicher redundant ausgelegt werden. Die einzelnen Rechner, aus denen sich ein Cluster zusammensetzt, werden hierbei als Knoten bezeichnet. Bei Failover-Clustern wird nun eine Anwendung auf einem Knoten betrieben, die Zustandsinformationen werden dabei auf das Quorum geschrieben. Fällt der aktive Knoten aus, so kann der zweite Knoten auf das Quorum zugreifen und anhand der Informationen an der Stelle weiterarbeiten, an der der ursprüngliche Knoten ausgefallen ist. Werden virtuelle Server im Cluster betrieben, kann der Zugriff auf die virtuellen Maschinen scheinbar ununterbrochen weitergehen, ohne dass verbundene Benutzer von einem Hardwareausfall betroffen sind.

Der Einsatz von Clustern ist allerdings mit erheblichen Kosten verbunden. Es müssen nicht nur die normalen Rechnerkomponenten doppelt vorhanden sein, sondern clusterfähige Systeme und ein Quorum angeschafft werden. Zusätzlich werden Lizenzen für den Betrieb von Clustern und die Betriebssysteme benötigt. In der Praxis ergeben sich damit ca. die zehnfachen Kosten bei vergleichbarer Hardwareleistung.

## Serverrollen

Server können unterschiedliche Rollen im Netzwerk übernehmen. Manche davon sind besser, andere weniger für eine Virtualisierung geeignet. Die folgende Tabelle gibt einige Beispiele für bestimmte Serverrollen und beschreibt dabei die Eignung für eine Virtualisierung und den Einsatz im Cluster:


Schulversion
© HERDT-Verlag

| Serverrolle | Geeignet für Virtualisierung | Geeignet für Cluster |
|---|---|---|
| **Domänencontroller (DCs) und DNS-Server** | Da Domänencontroller nur zu bestimmten Zeiten eine hohe Auslastung haben, kann es sinnvoll sein, sie zu virtualisieren, um während der Geschäftszeiten Prozessorkapazitäten für andere Anwendungen bereitzustellen. In aller Regel wird der DNS-Server als zusätzliche Rolle auf dem Domänencontroller betrieben. Für ihn gelten dieselben Regeln. | Da Domänencontroller in der Lage sind, auf mehreren Rechnern gleichzeitig in einem Netz betrieben zu werden, sind die Mehrkosten für den Clusterbetrieb nicht gerechtfertigt. In aller Regel sollten an einem Standort mindestens zwei DCs betrieben werden. |
| **DHCP-Server** | DHCP-Server werden vor allem während der Anmeldezeiten belastet und sind während der Geschäftszeiten weniger aktiv. Somit kann durch eine Virtualisierung Prozessorzeit für andere Aufgaben im Netzwerk verfügbar gemacht werden. | DHCP-Server verwenden eine hochdynamische Datenbank, die nicht zweimal identisch vorhanden sein darf. Zudem können mehrere DHCP-Server Konflikte im Netzwerk verursachen. Indem der DHCP-Server auf einem Cluster betrieben wird, kann Redundanz für die automatische Adressvergabe erreicht werden. |
| **Dateiserver** | Dateiserver belasten vor allem massiv den Festplattenbus und die Netzwerkadapter. Durch eine Virtualisierung werden diese Komponenten jedoch zusätzlich vom Gastsystem belastet. Daher ist es nicht sinnvoll, den Dateiserver zu virtualisieren. | Der Betrieb eines Dateiservers im Cluster würde die Kosten in den meisten Fällen sprengen, da Quorum-Datenträger erhebliche Mehrkosten verursachen. Stattdessen empfiehlt sich der Einsatz von speziellen netzwerkfähigen autonomen Systemen. |
| **Webserver** | Webserver werden in aller Regel in einem eigenen Netz betrieben, auf das von außen zugegriffen werden kann. Um mögliche Angriffspunkte zu vermindern, sollten auf ihnen nur die benötigten Dienste betrieben werden. Damit sind sie für eine Virtualisierung nicht geeignet, da das Hostsystem seinerseits einen zusätzlichen Angriffspunkt bietet. | Da Webserver in aller Regel statische Datenbestände verwenden, ist der Einsatz von Clustern nicht nötig. Stattdessen können sie auf sogenannten NLB-Clustern (**N**etwork **L**oad **B**alancing, Netzwerklastenausgleich) eingesetzt werden. Diese stellen für statische Datenbestände eine ausreichende Ausfallsicherheit und Lastenverteilung bereit. |
| **Datenbankserver** | Datenbankserver haben eine hohe Prozessorbelastung während der Geschäftszeiten. Sie können virtualisiert werden und so zusätzliche Prozessorkapazitäten verwenden, die von anderen Servern während des Tages nicht benötigt werden. | Datenbankserver können aufgrund der dynamischen Datenbestände nicht redundant installiert werden und sind somit für den Einsatz in Clustern geeignet. |

## 5.2 Hyper-V einsetzen

### Vor- und Nachteile von Hyper-V

Bei Hyper-V handelt es sich um die Software, die Microsoft als Bestandteil von Windows Server für die Servervirtualisierung bereitstellt. In Windows Server 2019 ist Hyper-V in einer neuen Version enthalten. Im Vergleich zu den kommerziellen Konkurrenzprodukten hat Microsoft mit Hyper-V deutlich aufgeholt, was die Flexibilität und die Einsatzmöglichkeiten angeht. Ob sich der Einsatz von Hyper-V in Ihrem Unternehmen lohnt, kann jeweils nur eine detaillierte Betrachtung aller Faktoren ergeben.

Für die Testumgebung in diesem Buch ist Hyper-V bestens geeignet.

### Hardwarevoraussetzungen

Damit Sie auf Ihrem Rechner Hyper-V und Windows Server 2019 einsetzen können, müssen folgende Bedingungen erfüllt sein:

- Sie verwenden einen X64-kompatiblen Prozessor, der mindestens zwei (besser vier) Kerne unterstützt.
- Der Prozessor unterstützt hardwareunterstützte Virtualisierung, entweder über Intel Virtualization Technology (Intel VT) oder AMD Virtualization (AMD-V).
- Das BIOS des Mainboards unterstützt Datenausführungsverhinderung (Data Execution Prevention, DEP).
- Sie verfügen über mindestens 512 MB (empfehlenswert sind 1500 MB) Arbeitsspeicher pro virtuellem System und Gastsystem.

### Status der Datenausführungsverhinderung überprüfen

Bevor Sie Hyper-V installieren, sollten Sie überprüfen, ob DEP aktiviert ist. Falls das nicht der Fall ist, müssen Sie möglicherweise im BIOS die Datenausführungsverhinderung (Data Execution Prevention, DEP) einschalten.

Den aktuellen DEP-Status können Sie am einfachsten über folgenden Kommandozeilenbefehl abrufen:

```
wmic OS get DataExecutionPrevention_SupportPolicy
```

Als Ergebnis erhalten Sie einen Wert zwischen 0 und 3. Sie müssen nur bei einem Rückgabewert von 0 etwas unternehmen. Überprüfen Sie in diesem Fall die BIOS-Einstellungen.

| Wert | DEP-Status |
|---|---|
| 0 | DEP ausgeschaltet |
| 1 | DEP für alle Software eingeschaltet |
| 2 | DEP nur für Systemkomponenten von Windows eingeschaltet |
| 3 | DEP für alle Software eingeschaltet, es können vom Administrator Ausnahmen erstellt werden. |


Schulversion
© HERDT-Verlag

## 5.3 Hyper-V installieren

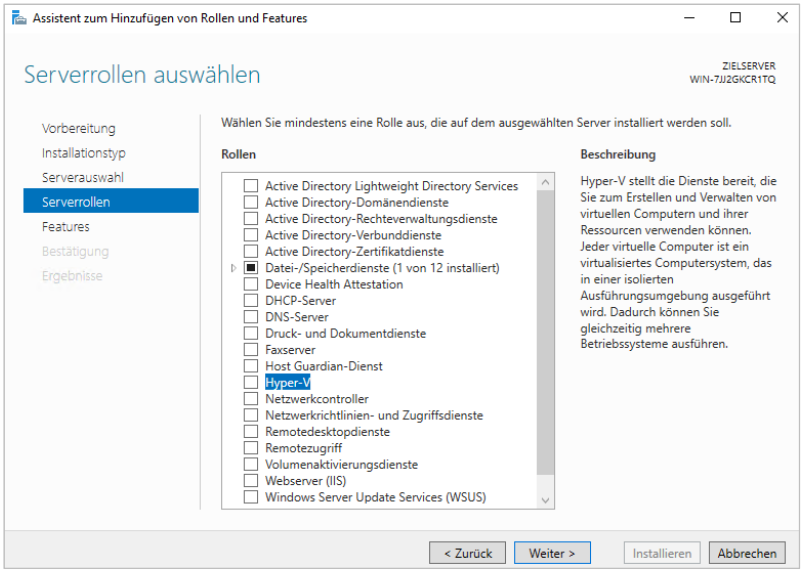
### Die Rolle *Hyper-V* hinzufügen

Die im Folgenden beschriebenen Schritte dienen dazu, den Dienst Hyper-V zu installieren. Die Schritte, die Sie dabei durchführen, sind die Grundlage für die Installation zusätzlicher Serverrollen. Beachten Sie die Möglichkeit, zu den jeweiligen Serverrollen zusätzliche Informationen abzurufen, bevor Sie eine Installation durchführen.

- Öffnen Sie den Server-Manager, indem Sie auf das Icon in der Taskleiste klicken.
- Lesen Sie die Vorbemerkungen und klicken Sie auf *Weiter*.

  Optional können Sie hier aktivieren, dass diese Seite ab sofort übersprungen werden soll.
- Wählen Sie die Option *Rollenbasierte Installation* und klicken Sie auf *Weiter*.
- Wählen Sie den Zielserver aus und klicken Sie auf *Weiter*.
- Aktivieren Sie auf der Seite *Serverrollen* im Listenfeld die Rolle *Hyper-V*.

  Es öffnet sich ein weiterer Dialog.
- Bestätigen Sie das Hinzufügen der für die Serverrolle *Hyper-V* erforderlichen Features, indem Sie auf *Features hinzufügen* klicken.
- Klicken Sie für eine Beschreibung der markierten Rolle auf der rechten Seite auf den Link. Klicken Sie auf *Weiter*.
- Klicken Sie auf der Seite *Features* auf *Weiter*.
- Lesen Sie die Hinweise auf der Seite *Hyper-V* durch und klicken Sie auf *Weiter*.

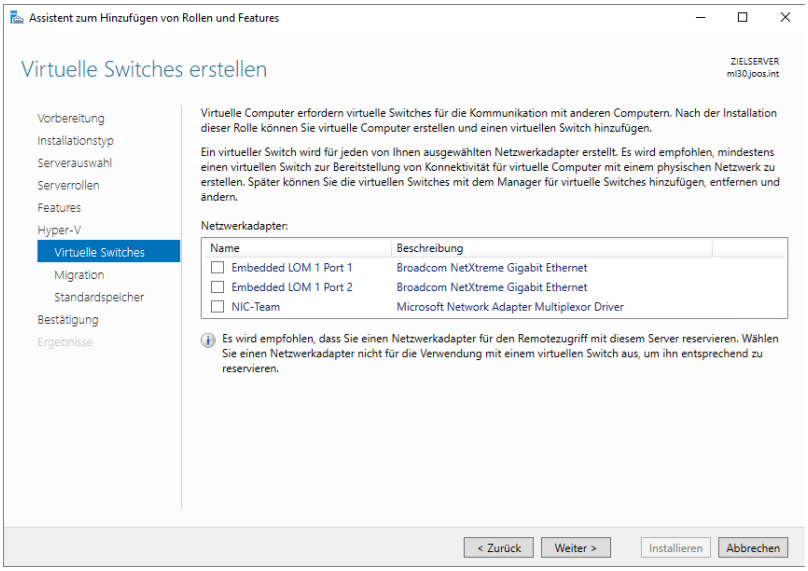



*Serverrollen hinzufügen*

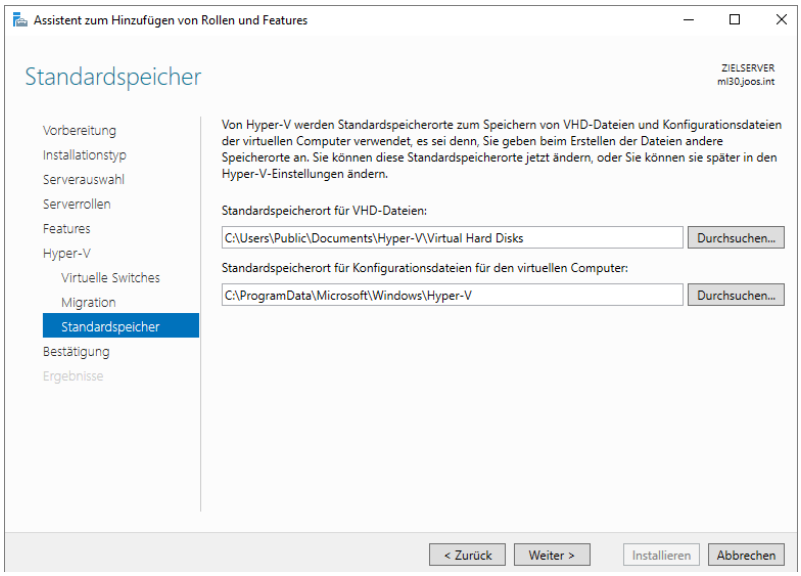
Auf der Seite *Virtuelle Switches* können Sie eine Netzwerkkarte auswählen, an die der virtuelle Switch von Hyper-V gekoppelt werden soll.

- Wählen Sie jetzt noch **keine** Karte an, sondern klicken Sie auf *Weiter*. Sie können die Einstellungen für die virtuellen Netzwerke später verändern.
- Klicken Sie auf der Seite *Migration* auf *Weiter*.

  Hier können Sie die Live-Migration für diesen Server einschalten und das Authentifizierungsprotokoll für diese festlegen. Dies wird für die Testumgebung jedoch nicht benötigt und kann jederzeit eingestellt werden.



- Wählen Sie auf der Seite *Standardspeicher* die Standardspeicherorte für die virtuellen Festplattendateien (VHD bzw. VHDX) und die Konfigurationsdateien aus und klicken Sie auf *Weiter*.




Als Standardspeicherort sollten Sie die schnellste Festplatte mit ausreichend freiem Speicherplatz wählen, Sie können aber bei der Erstellung jeder neuen virtuellen Maschine den Speicherort der VHD-Datei verändern. Wichtig ist, dass Sie die VMs möglichst auf die vorhandenen Datenträger verteilen.

Wenn Sie alle virtuellen Datenträger auf einem Datenträger anlegen möchten, sollten Sie eine SSD verwenden. Andernfalls muss der Lese-/Schreib-Kopf ständig zwischen den verschiedenen VHDs wechseln. Dies kann das System erheblich ausbremsen.

Auf der letzten Seite werden Sie aufgefordert, die Installationsauswahl zu bestätigen. Auf Wunsch können Sie eine Option aktivieren, die den Rechner automatisch neu startet, wenn dies für die Installation erforderlich ist.

- Aktivieren Sie die Option für den automatischen Neustart. Klicken Sie auf *Installieren*, nachdem Sie die Installationsmeldung überprüft haben.
- Nehmen Sie gegebenenfalls Änderungen im BIOS vor, um Hyper-V zu unterstützen.

Im Verlauf der Installation von Hyper-V muss Ihr Rechner mehrmals neu starten. Unterbrechen Sie diese Startvorgänge nicht.

## 5.4 Hyper-V einrichten

### Installationserfolg von Hyper-V überprüfen

Nach der ersten Anmeldung mit der neuen Serverrolle wird diese auf dem Dashboard des Server-Managers angezeigt. Falls Sie bei der Installation die Option *Automatisch neu starten* aktiviert hatten, wird im Assistenten der Installationsstatus angezeigt. Außerdem haben Sie auf dieser Seite die Möglichkeit, die Konfigurationseinstellungen zur späteren Wiederverwendung in eine Datei zu exportieren.

### Mit anderem Hostserver verbinden

Standardmäßig verbindet sich der Hyper-V-Manager mit dem lokalen Server, Sie können jedoch auch eine Verbindung mit einem anderen Hyper-V-Host herstellen:

- Klicken Sie im Menü *Tools* des Server-Managers auf *Hyper-V-Manager*.

  *oder* Geben Sie im Startmenü `Hyper` ein und wählen Sie *Hyper-V-Manager*.

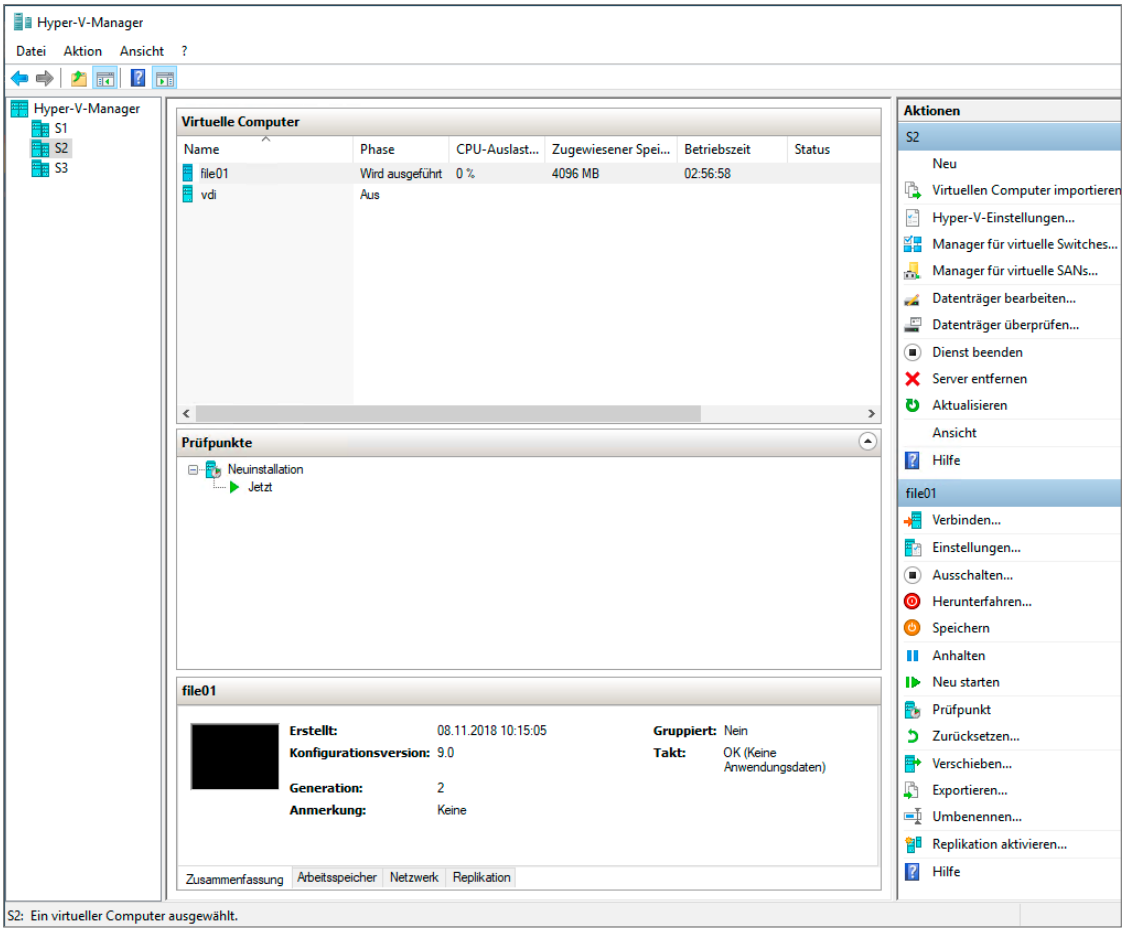
  Der Hyper-V-Manager wird geöffnet und automatisch mit dem lokalen Hostrechner verbunden.


Schulversion
© HERDT-Verlag

- Klicken Sie in der linken Spalte mit der rechten Maustaste auf *Hyper-V-Manager.*
- Klicken Sie dann auf *Verbindung mit dem Server herstellen*.
- Wählen Sie einen anderen Hostserver und klicken Sie auf *OK*.

Der Hyper-V-Manager kann im Startmenü auch über `virtmgmt.msc` aufgerufen werden.

## Hyper-V-Manager




*Hyper-V-Manager für Hostserver*

### Navigationsspalte

In der linken Spalte können Sie sehen, mit welchem Hostserver Sie gerade verbunden sind.

### Virtuelle Computer

Im zentralen Bereich *Virtuelle Computer* sehen Sie eine Auflistung aller vorhandenen virtuellen Computer. Zu jeder VM werden neben ihrem Namen auch der momentane Zustand, die prozentuale Auslastung der Host-CPU, der momentan zugewiesene Hauptspeicher sowie die Betriebszeit seit dem Einschalten angezeigt.

### Prüfpunkte

In der Mitte des Hyper-V-Managers werden alle Prüfpunkte der markierten VM angezeigt. Das Standard-Benennungsschema ist der Name der VM, gefolgt von Datum und Uhrzeit in Klammern. Sie können die Bezeichnung bei der Erstellung oder später ändern. Über das Kontextmenü oder den Aktionsbereich können Sie den markierten Prüfpunkt löschen, umbenennen oder anwenden, d. h. die VM auf den Stand des Prüfpunkte zurückversetzen.

### Weitere Informationen

Unter den Prüfpunkten werden unter dem Namen der markierten VM weitere Informationen angezeigt. Hier können Sie sich auf vier Registerkarten eine Zusammenfassung sowie Details zum Arbeitsspeicher, Netzwerk und zur Replikation anzeigen lassen. In der Zusammenfassung sehen Sie eine Miniaturabbildung des Bildschirminhalts.

### Aktionen

Im rechten Teil des Hyper-V-Managers sehen Sie unter *Aktionen* die möglichen Verwaltungspunkte, die in der folgenden Tabelle erläutert werden:

| | |
|---|---|
| *Neu* | Verwenden Sie *Neu,* um virtuelle Computer, Festplatten oder Disketten zu erstellen. |
| *Virtuellen Computer importieren* | Wenn Sie vorhandene virtuelle Computer, die zuvor auf diesem oder einem anderen Hostserver erstellt worden sind, in den verbundenen Server importieren wollen, müssen Sie den Speicherort der Abbilddateien angeben. |
| *Hyper-V-Einstellungen* | Hier können Sie die virtuellen Festplatten, Computer und die Einstellungen für die Benutzeraktion festlegen. |
| *Manager für virtuelle Switches* | Verwalten Sie die Sicherheitseinstellungen für vorhandene virtuelle Netzwerke oder erstellen Sie neue virtuelle Netzwerke. Außerdem können Sie den Adressbereich festlegen, in dem MAC-Adressen vom System vergeben werden sollen, und VLAN-IDs für zusätzliche virtuelle Adapter vergeben.<br>VLAN-IDs erlauben auf Switches das Einrichten virtueller Netze, indem nur die Adapter miteinander kommunizieren können, die eine identische VLAN-ID verwenden. |
| *Manager für virtuelle SANs* | Stellen Sie physisch vorhandene Fibre-Channel-Ports zu einem virtuellen Speichernetzwerk (Storage Area Network, SAN) zusammen. |
| *Datenträger bearbeiten* | Hier können Sie einen virtuellen Datenträger komprimieren, verkleinern und vergrößern oder zwischen VHD und VHDX konvertieren. |
| *Datenträger überprüfen* | Hiermit können Sie die virtuellen Datenträger untersuchen lassen. Ihnen wird angezeigt, wie groß der virtuelle Datenträger ist, ob er dynamisch erweiterbar ist und unter welchem Pfad er vorliegt. |
| *Dienst beenden* | Beendet den Hyper-V-Dienst und damit auch alle VMs. Anschließend können Sie den Dienst über das Aktionsmenü wieder starten. |
| *Server entfernen* | Entfernt einen Virtualisierungsserver aus dem Hyper-V-Manager, ohne ihn zu löschen |
| *Aktualisieren* | Aktualisiert die Ansicht im zentralen Bereich des Hyper-V-Managers |

Im unteren Teil des Bereichs *Aktionen* werden für Server, VMs oder Prüfpunkte unterschiedliche Aktionen angezeigt.

## Externen virtuellen Switch einrichten

Bevor Sie mit der Installation von VMs beginnen, müssen Sie einen virtuellen Switch einrichten, über den die VMs untereinander, mit dem Host und mit dem Netzwerk kommunizieren können. Es gibt drei verschiedene Typen von virtuellen Switches:

- **Extern:** Die VMs sind im Netzwerk sichtbar und haben Netzwerk- und Internetzugang.
- **Intern:** Die VMs können untereinander und mit dem Host kommunizieren, sind im Netzwerk unsichtbar und haben weder Netzwerk- noch Internetzugang.
- **Privat:** Die VMs können nur untereinander kommunizieren, sind für den Host unsichtbar und haben weder Netzwerk- noch Internetzugang.


© HERDT-Verlag

Für die Aktivierung von Windows wird kurzzeitig eine Internetverbindung benötigt, später laufen die VMs jedoch in einem internen Netz. Daher werden für die Testumgebung zwei Switches erstellt, einer ist extern, der andere intern.

Sie könnten auch mit einem Switch auskommen, den Sie später umstellen, es ist jedoch praktischer und weniger fehlerträchtig, zwei Switches zu verwenden. So haben Sie außerdem später noch die Möglichkeit, zusätzliche VMs zu erstellen und Windows über das Internet zu aktivieren, ohne die Konfiguration der anderen VMs zu stören.

Falls Sie bei der Installation von Hyper-V bereits einen virtuellen Switch erstellt haben, fällt der folgende Schritt weg, denn dann haben Sie bereits einen **externen** Switch. Nehmen Sie in diesem Fall keine nachträgliche Namensänderung des virtuellen Switches vor, um Probleme zu vermeiden.

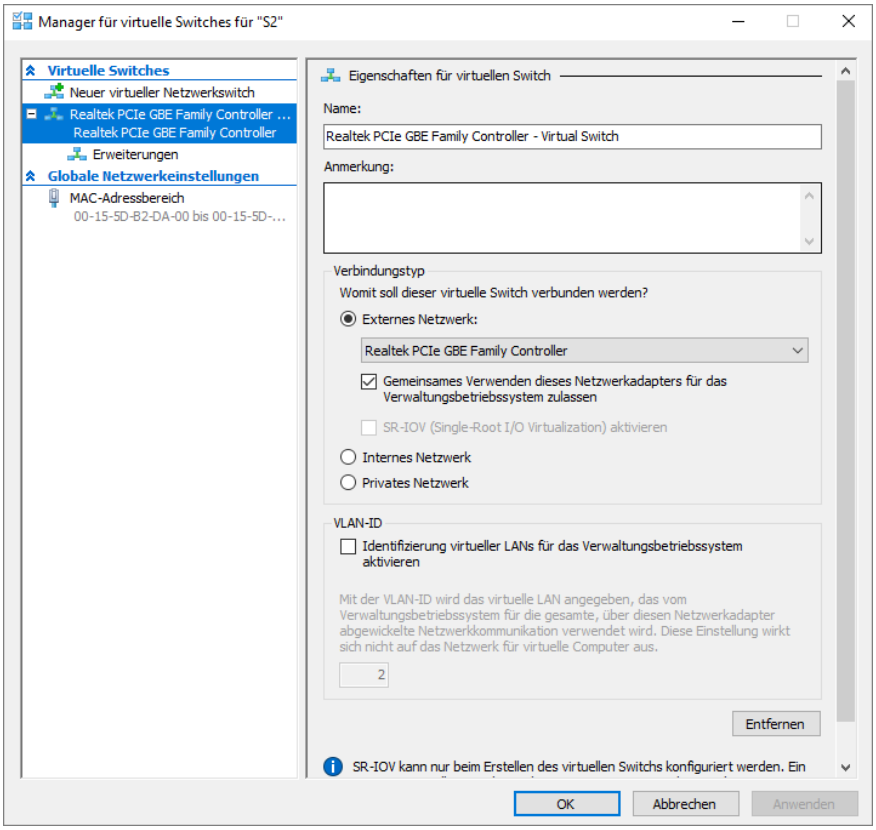
- Klicken Sie im Aktionsbereich des Hyper-V-Managers auf *Manager für virtuelle Switches*.
- Wählen Sie als Switch-Typ *Extern* und klicken Sie auf *Virtuellen Switch erstellen*.
- Geben Sie dem Switch einen aussagekräftigen Namen, z. B. *Extern*.
- Klicken Sie auf *Anwenden*, bestätigen Sie die Warnmeldung mit *Ja* und klicken Sie auf *OK*.

Sie können beim externen Netzwerk einstellen, an welchen physischen Netzwerkadapter der virtuelle Switch gebunden ist.

Das gemeinsame Verwenden des Netzwerkadapters ermöglicht den gleichzeitigen Internetzugriff für Host und VMs und sollte aktiviert sein.

Mit *SR-IOV* erscheinen Netzwerkadapter mit mehreren Ports nach außen hin wie ein einzelner Adapter. Diese Option kann nur beim Erstellen eines neuen virtuellen Switches konfiguriert werden.

Sie können den Switch später von *extern* auf *intern* oder *privat* umstellen, dies ist jedoch nicht ratsam, weil dabei Fehlkonfigurationen auftreten können. Unter *VLAN-ID* können Sie VLANs verwenden und eine ID zuweisen.




## Internen Switch erstellen

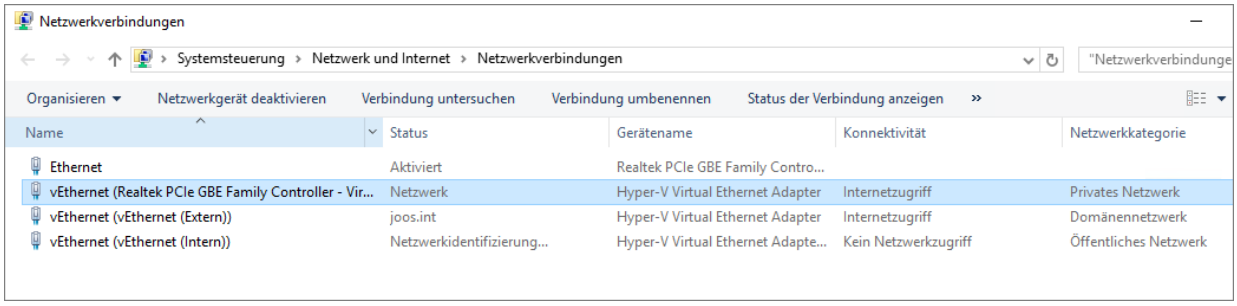
Für die Testumgebung wird ein weiterer Switch benötigt, der nur interne Kommunikation zulässt.

- Erstellen Sie einen zweiten Switch, der nur mit dem internen Netzwerk verbunden ist.
- Nennen Sie den Switch z. B. *Intern.*

## Resultat auf dem Hostcomputer

Nach Einrichtung der beiden virtuellen Switches ist die Netzwerkverbindung unterbrochen und Sie müssen auf dem Hostcomputer noch einige Einstellungen vornehmen. Öffnen Sie dazu die Netzwerkverbindungen.

- Suchen Sie im Startmenü nach *ncpa.cpl*.
  *oder* Klicken Sie im Server-Manager auf der Seite *Lokaler Server* auf eine Netzwerkverbindung.
  Die Netzwerkverbindungen werden geöffnet.




Sie sehen nun drei Netzwerkverbindungen. Das erste Gerät *Ethernet* ist der physische Netzwerkadapter, der nun die Funktion eines virtuellen Switches übernimmt und somit auch keine IP-Adresse mehr hat. Das zweite Gerät *vEthernet (Extern)* ist aus Sicht des Hosts der Netzwerkadapter, der mit dem LAN und dem Internet verbunden ist. Er verfügt über die IP-Einstellungen, Standardgateway und DNS-Server, die für das physische lokale Netzwerk benötigt werden. Das dritte Gerät *vEthernet (Intern)* ist über das interne Netzwerk mit den VMs verbunden. Dieser zweite virtuelle Netzwerkadapter soll das Standardgateway für die VMs sein und erhält daher die IPv4-Adresse 192.168.1.1.

- Klicken Sie mit der rechten Maustaste auf eine Netzwerkverbindung und wählen Sie *Einstellungen*.
- Überprüfen Sie bei allen drei Verbindungen, ob die Einstellungen mit der folgenden Tabelle übereinstimmen.
  Als Subnetzmaske ist jedes Mal 255.255.255.0 einzutragen.

## Netzwerkverbindungen des Hosts

| Name | Funktion | IP-Eigenschaften |
|---|---|---|
| Ethernet | virtueller Switch | Hyper-V erweiterbarer virtueller Switch, kein IPv4/IPv6 |
| vEthernet (Extern) | virtueller Netzwerkadapter | IPv4-Adresse, DNS-Server und Standardgateway passend für das physische Netzwerk, in dem der Host sich befindet |
| vEthernet (Intern) | virtueller Netzwerkadapter | IPv4-Adresse internes virtuelles Netzwerk: 192.168.1.1<br>DNS IPv4: 192.168.1.2; alternativer DNS 192.168.1.3<br>Standardgateway bleibt leer, Subnetzmaske unverändert.<br>IPv6-Adresse: fc01::192:168:1:1<br>DNS IPv6: fc01::192:168:1:2; alternativer DNS: fc01::192:168:1:2<br>(siehe auch die IP-Konfigurationstabelle in Kapitel 9) |

Verwenden Sie bei der IP-Konfiguration die in Kapitel 9 vorgegebenen IP-Adressen. Tragen Sie sorgfältig für IPv4 und IPv6 die IP-Adressen, Standardgateway und DNS-Server ein.

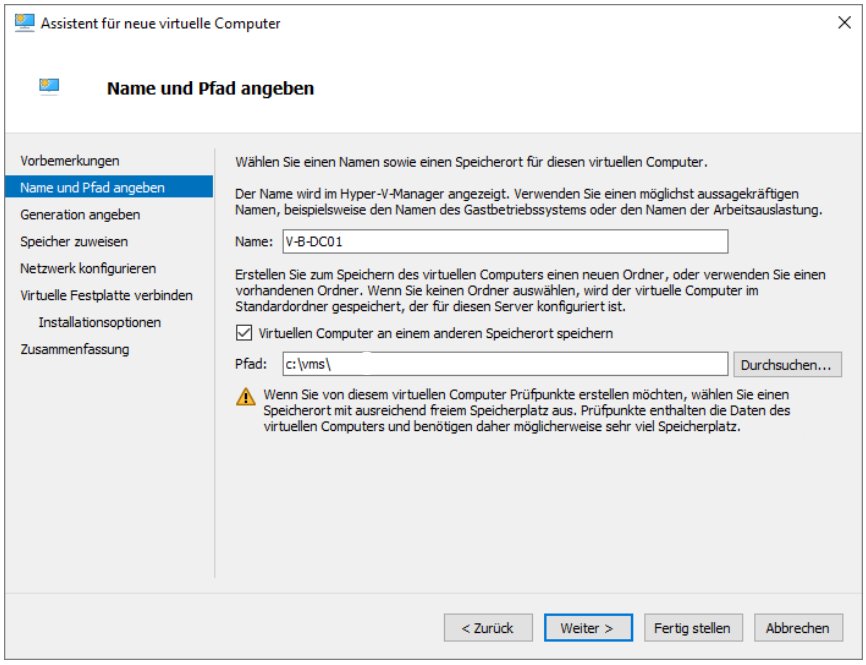
Verändern Sie anschließend, wenn möglich, nichts mehr an den Einstellungen der virtuellen Netzwerkadapter für das interne Netzwerk, denn sonst ergeben sich schwer nachvollziehbare Probleme im Zusammenspiel der VMs.


© HERDT-Verlag

## 5.5 Virtuellen Computer einrichten

Sie werden nun durch die Schritte geleitet, die Sie benötigen, um den ersten virtuellen Rechner auf Ihrem Hostserver einzurichten. Am Ende der Einrichtung haben Sie den ersten virtuellen Computer namens *V-B-DC01* erstellt, der über folgende Eigenschaften verfügt:

- virtuelle Festplatte mit 127 GB im VHDX-Format auf einer physischen Partition des Hosts mit 30 GB freiem Speicherplatz,
- Konfigurationsdateien und Prüfpunkte auf derselben Partition wie die VHDX-Datei,
- 1500 MB Hauptspeicher für die VM,
- dynamische Speicherverwaltung aktiviert,
- Netzwerkverbindung über den eingerichteten externen virtuellen Switch,
- Bootmedium ist die ISO-Datei für die Installations-DVD.




- Starten Sie den Hyper-V-Manager und verbinden Sie sich mit Ihrem Hostserver.
- Klicken Sie im Bereich *Aktionen* auf *Neu* und wählen Sie *Virtueller Computer,* um den Assistenten für neue virtuelle Computer zu starten.
- Geben Sie als Namen `V-B-DC01` ein .

Beachten Sie, dass der Name der Hyper-V-Maschine den späteren Namen des Servers enthält, dem ein '*V*' vorangestellt wurde. Dies erleichtert die spätere Zuordnung enorm.

Wenn Sie die Standardeinstellungen für virtuelle Abbilddateien, virtuelle Laufwerke und Speicherkonfigurationen übernehmen möchten, können Sie nun auf *Fertig stellen* klicken.

- Zum Ändern des Speicherorts aktivieren Sie die Option *Virtuellen Computer an einem anderen Speicherort speichern* und geben Sie den Ordnerpfad ein.
- Klicken Sie auf *Weiter*.

Am eingestellten Speicherort werden die Konfigurationsdateien und die Prüfpunkte der VM abgelegt. Während die Konfigurationsdateien recht klein sind, können zahlreiche Prüfpunkte mit vielen Änderungen an der Serverkonfiguration sehr viel Platz einnehmen. Es ist sinnvoll, hier den gleichen Speicherort anzugeben wie für die virtuelle Festplattendatei. Im Idealfall werden die Dateien für jede VM auf einer eigenen Festplatte gespeichert. Alternativ ist auch eine ausreichend große SSD geeignet, um alle VMs darauf zu speichern.

- Legen Sie die Generation der virtuellen Maschine fest, die Sie verwenden möchten. Für die Übungen in diesem Buch sollten Sie VMs der ersten Generation wählen.
- Klicken Sie auf *Weiter*.

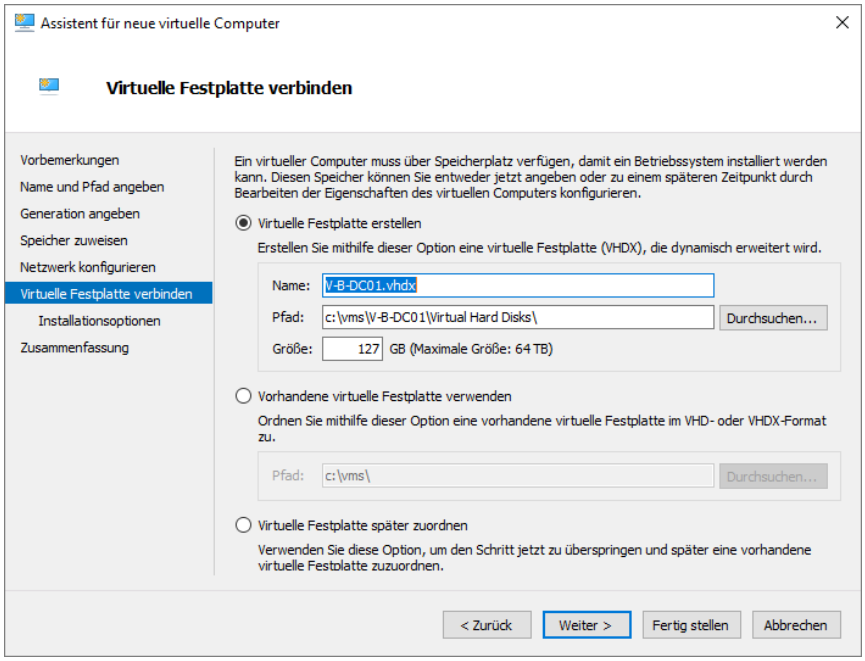
Die zweite Generation von VMs stellt eine der Neuerungen von Hyper-V unter Windows Server 2019 dar. So werden nun neue Arten des Starts unterstützt (PXE-Boot von neuen Netzwerkadaptern, Secure Boot und SCSI-Start). Dafür ist die Unterstützung von virtuellen IDE-Geräten nicht mehr möglich.

- Legen Sie auf der Seite *Speicher zuweisen* fest, wie viel Arbeitsspeicher der virtuelle Computer erhalten soll. Geben Sie als Wert *1024* ein.
- Aktivieren Sie den dynamischen Arbeitsspeicher und klicken Sie auf *Weiter*.

Der angegebene Speicher ist für das virtuelle System reserviert und steht dem Host nicht mehr zur Verfügung, wenn das virtuelle System ausgeführt wird. Innerhalb der VM zeigt Windows diesen Wert als Speicherausstattung an. Für einen Domänencontroller in der Testumgebung sind Werte zwischen 1024 und 2000 MB geeignet. Der dynamische Arbeitsspeicher sorgt dafür, dass die VM im Betrieb nur so viel Speicher belegt wie nötig. Für die Testumgebung ist diese Option optimal. Sie können die Einstellungen später bei ausgeschalteter VM verändern.

- Wählen Sie auf der Seite *Netzwerk konfigurieren* eine Verbindung für die VM aus. Wählen Sie den virtuellen externen Switch aus und klicken Sie auf *Weiter*.
- Belassen Sie die Option *Virtuelle Festplatte erstellen* unverändert, um eine neue virtuelle Festplatte im VHDX-Format zu erstellen. Der Name der Datei entspricht dem Namen der VM und sollte nicht geändert werden.
- Passen Sie den *Pfad* so an, dass die VHDX-Datei auf derselben Partition liegt wie die Konfigurationsdateien und Prüfpunkte.
- Belassen Sie die *Größe* der virtuellen Festplatte für die Testumgebung bei 127 GB.

  Beachten Sie, dass im Produktiveinsatz das virtuelle Laufwerk nicht größer sein sollte als der verfügbare Speicherplatz auf dem realen Datenträger. In dieser Testumgebung benötigt jede VM nur etwa 30 GB physisch auf dem Host vorhandenen Speicherplatz.
- Klicken Sie auf *Weiter*.




Als Alternative zum Erstellen einer neuen VHDX-Datei können Sie auch eine vorhandene Festplatte verwenden, die Sie unter *Pfad* auswählen können. Oder Sie verzichten zunächst auf die Erstellung des virtuellen Datenträgers und holen dies später nach.

Verwenden Sie nach Möglichkeit eine SSD oder separate Festplatten für jede VM. Andernfalls verlangsamen die konkurrierenden Zugriffe Ihr System stark und magnetische Festplatten werden mechanisch extrem beansprucht.


Schulversion
© HERDT-Verlag

## Installationsoptionen

Die Installation eines virtuellen Computers kann von unterschiedlichen Orten aus erfolgen:

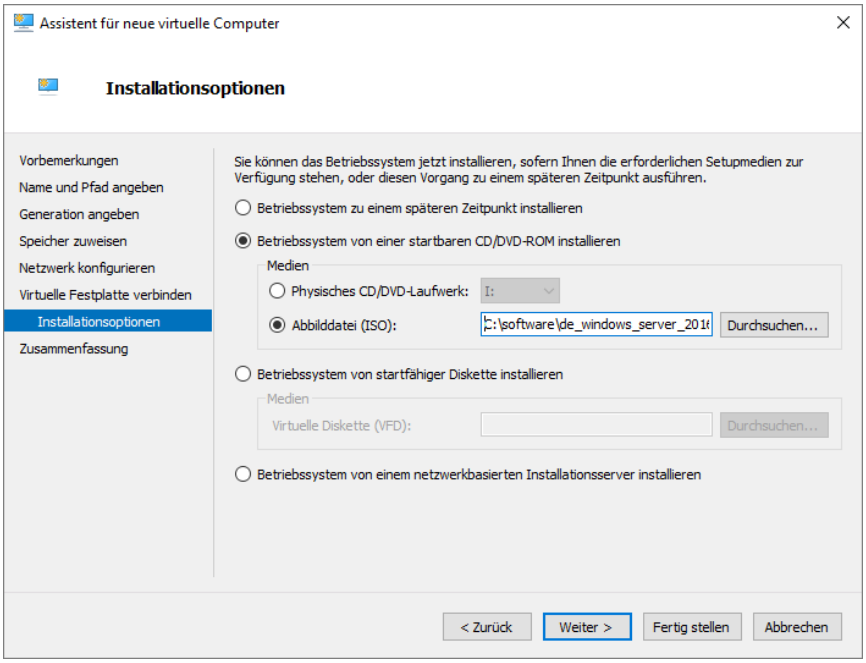
- physische Windows-Server-2019-Installations-DVD
- ISO-Abbild der Windows-Server-2019-Installations-DVD

  Die ISO-Datei kann an einem beliebigen Ort liegen, der vom Host aus ansprechbar ist (z. B. interne Festplatte, USB-Stick oder Netzwerkfreigabe).
- Netzwerkinstallation über DHCP/BOOTP und die Windows-Bereitstellungsdienste (WDS) in einer Domäne

Der schnellste Weg zur Installation ist ein ISO-Image auf einem anderen Datenträger als die VM. Im Idealfall verwenden Sie hierfür zwei SSDs. Da Hyper-V keine USB-Medien einbinden kann, fällt der USB-Stick als Installationsmedium weg, Sie können allerdings das ISO-Abbild auf einen schnellen USB-3.0-Stick kopieren und so die Installation möglicherweise erheblich beschleunigen.

- Aktivieren Sie auf der Seite *Installationsoptionen* die Option *Betriebssystem von startfähiger CD/DVD-ROM installieren* und wählen Sie im Bereich *Medien* die Option *Abbilddatei* aus.
- Geben Sie den Pfad zur ISO-Datei an und klicken Sie auf *Weiter*.

Alternativ können Sie das Betriebssystem auch später installieren, eine Installations-DVD oder ein startfähiges Diskettenabbild verwenden oder über das Netzwerk installieren.




*Auswahl des Installationsmediums*

- Lesen Sie auf der letzten Seite des Assistenten die Zusammenfassung Ihrer Konfigurationseinstellungen und bestätigen Sie diese mit *Fertig stellen*.

  Nach wenigen Sekunden ist die virtuelle Maschine erstellt.
- Richten Sie auf die gleiche Weise für den zweiten DC und den Fileserver zwei weitere VMs mit den Namen *V-B-DC02* und *V-B-FS01* ein.

  Geben Sie wenn möglich als Speicherort für jede VM eine separate Festplatte an.

Es gibt zahlreiche Möglichkeiten und Tricks, eine bestehende VM zu vervielfältigen. Sie können z. B. die VHDX-Datei kopieren und bei der Erstellung einer neuen VM einbinden. Sie können ebenfalls die Export-/Import-Funktionen verwenden. Keine dieser Kopiermethoden ist frei von Problemen und es besteht die Gefahr, die eingesparte Zeit bei der Fehlersuche wieder einzubüßen. Das Kopieren von VMs wird daher nicht empfohlen.

## 5.6 Virtuellen Computer verwalten

### Virtuellen Computer starten

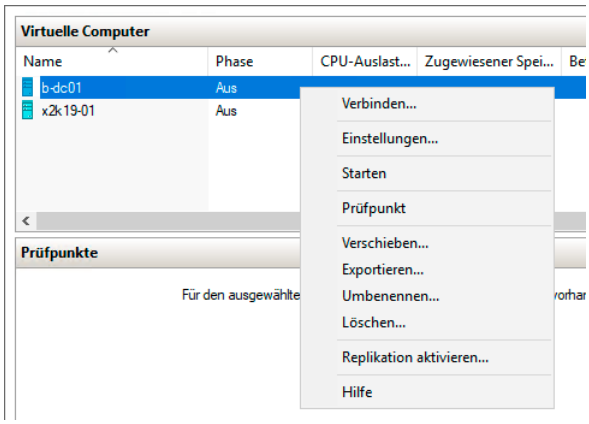
- Öffnen Sie den Hyper-V-Manager und wählen Sie den von Ihnen verwalteten Server.

  Es werden die erstellten VMs angezeigt, die alle noch ausgeschaltet sind.
- Klicken Sie mit der rechten Maustaste auf *V-B-DC01* und wählen Sie *Starten*.

  Alternativ können Sie auch die VM markieren und dann im Aktionsbereich auf *Starten* klicken.

  Die VM wird nun im Hintergrund gestartet.
- Um das Fenster mit der VM zu öffnen, klicken Sie doppelt auf die VM.

  Sie können auch im Kontextmenü der VM oder im Aktionsbereich auf *Verbinden* klicken.




*Starten der VM*

### Virtuellen Server installieren

Sie befinden sich nun im Fenster für die Verbindung mit dem virtuellen Computer. In der Titelzeile des Fensters steht die Bezeichnung der VM, was bei mehreren VMs sehr hilfreich ist.

Neben zahlreichen Menüpunkten verfügt jedes VM-Fenster über eine Reihe von farbigen Bedienungselementen, die ihre Funktion anzeigen, wenn Sie mit der Maus darauf zeigen.

| | |
|---|---|
| | Tastenkombination Strg Alt Entf an die VM senden |
| | VM starten |
| | VM ohne Herunterfahren oder Speichern ausschalten (entspricht dem Ziehen des Netzsteckers) |
| | VM herunterfahren (entspricht dem normalen Beenden von Windows) |
| | Momentanen Zustand der VM speichern, ähnlich dem Ruhezustand |
| | VM pausieren. Die VM wird eingefroren und kann anschließend über wieder fortgesetzt werden. |
| | VM zurücksetzen (entspricht dem Betätigen des Reset-Schalters) |
| | Prüfpunkt erstellen |
| | Setzt die VM auf den Stand des letzten Prüfpunkts zurück |

Da Sie schon bei der Einrichtung die ISO-Datei als Installationsmedium angegeben haben, startet die neue VM nach dem Einschalten automatisch das Windows-Setup.

- Führen Sie wie gewohnt eine Installation des Betriebssystems durch. Verwenden Sie dabei eine vollständige Datacenter-Version mit grafischer Benutzeroberfläche.
- Klicken Sie in der Datenträgerauswahl auf *Neu* und geben Sie unter *Größe* `40000` ein (also knapp 40 GB, was für die Testumgebung und viele Produktivserver ausreichend ist). Klicken Sie auf *Übernehmen*.
- Starten Sie die Installation.
- Melden Sie sich am virtuellen Server an.


Schulversion
© HERDT-Verlag

Mit [Strg] [Alt] [Entf] senden Sie einen Tastatur-Interrupt an das Hostsystem. Um sich am virtuellen System anmelden zu können, müssen Sie [Strg] [Alt] [Ende] betätigen. Alternativ können Sie auch im VM-Fenster auf klicken.

Falls in Ihrem Netzwerk DHCP vorhanden ist, haben Sie bereits eine Verbindung zum Internet und müssen vorerst nichts an der IP-Adresse ändern. Ohne DHCP benötigen Sie eine in Ihrer Netzwerkumgebung verfügbare IP-Adresse. Sie müssen außerdem die Adresse für das Standardgateway und einen DNS-Server eintragen. Beachten Sie hier die Vorgaben des Kursleiters.

- Passen Sie die IP-Einstellungen an die Gegebenheiten des physischen Netzwerks an.

## Windows aktivieren

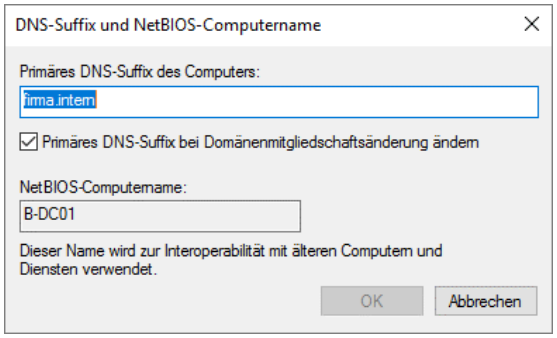
- Sobald Sie über eine funktionierende Internetverbindung verfügen, öffnen Sie den Server-Manager und klicken auf *Lokaler Server*.
- Klicken Sie neben *Produkt-ID* auf den Link *Nicht aktiviert*.

  Bei Windows-Server-2019 erfolgt die Aktivierung automatisch, kurz nachdem die Internetverbindung zustande gekommen ist. Es dauert allerdings eine Weile, bis die erfolgreiche Aktivierung im Server-Manager angezeigt wird. Mit [F5] können Sie die Anzeige aktualisieren.
- Bei der Vollversion geben Sie den Produktschlüssel ein und klicken Sie auf *Aktivieren*.

  Nach wenigen Sekunden wird ein gültiger Schlüssel akzeptiert und Ihr Windows ist aktiviert.
- Betätigen Sie [⊞] [Pause] und klicken Sie auf *Einstellungen ändern*.

## Computernamen und DNS-Suffix festlegen

- Klicken Sie auf der Registerkarte *Computername* auf *Ändern*.
- Benennen Sie den Computer um und klicken Sie auf *Weitere*.
- Tragen Sie als DNS-Suffix *firma.intern* ein. Stellen Sie sicher, dass die Option *Primäres DNS-Suffix bei …* aktiviert ist, und klicken Sie auf *OK*.
- Starten Sie den Rechner neu, wenn Sie dazu aufgefordert werden.
- Führen Sie diese Schritte auch für die beiden anderen VMs durch: Geben Sie *V-B-DC02* den Namen *B-DC02* und verwenden Sie für *V-B-FS01* den Namen *B-FS01*.




## Virtuelles Netzwerk von Extern auf Intern umschalten

Wenn Sie auf allen drei virtuellen Computern Windows erfolgreich aktiviert haben, können Sie die VMs von externem auf internes Netzwerk umschalten. Die folgenden Handlungen müssen für jede VM durchgeführt werden. Der Betriebszustand der VM ist dabei unerheblich.

- Öffnen Sie den Hyper-V-Manager.
- Klicken Sie mit der rechten Maustaste auf eine VM und wählen Sie *Einstellungen*.

  Der Einstellungsdialog für die VM wird geöffnet.
- Klicken Sie in der linken Spalte auf *Netzwerkkarte*.
- Wählen Sie in der rechten Spalte im Listenfeld *Virtueller Switch* den internen Switch.
- Klicken Sie auf *Anwenden*, dann auf *OK*.
- Wiederholen Sie den Vorgang für alle anderen VMs.

Ihre VMs können jetzt nur noch untereinander und mit dem Host kommunizieren. Dadurch können sich mehrere Testumgebungen nicht gegenseitig stören, außerdem können Sie wegen der Trennung vom übrigen Netzwerk gefahrlos experimentieren.

Beachten Sie, dass Sie in den Netzwerkeinstellungen des Hosts bei dem internen Switch als IPv4-Adresse 192.168.1.1 und als IPv6-Adresse fc01::192:168:1:1 eintragen müssen, damit dieser als Standardgateway für die VMs dienen kann.

## IP-Adressen zuweisen

Für die Testumgebung sind feste IP-Adressen vorgesehen, die Sie nun auf jeder VM einstellen müssen.

- Starten Sie alle drei VMs und klicken Sie jeweils im Server-Manager auf der Seite *Lokaler Server* auf die IP-Adresse.
- Weisen Sie nun den VMs folgende IPv4-Adressen zu:
  - *B-DC01* erhält 192.168.1.2
  - *B-DC02* erhält 192.168.1.3
  - *B-FS01* erhält 192.168.1.4
- Alle drei VMs erhalten die folgenden IPv4-Einstellungen:
  - Standardgateway 192.168.1.1
  - DNS-Server 192.168.1.2
  - alternativer DNS-Server 192.168.1.3
- Weisen Sie den VMs folgende IPv6-Adressen zu:
  - *B-DC01* erhält fc01::192:168:1:2
  - *B-DC02* erhält fc01::192:168:1:3
  - *B-FS01* erhält fc01::192:168:1:4
- Alle drei VMs erhalten die folgenden IPv6-Einstellungen:
  - Standardgateway fc01::192:168:1:1
  - DNS-Server fc01::192:168:1:2
  - alternativer DNS-Server fc01::192:168:1:3

Am Anfang von Kapitel 9 finden Sie eine Tabelle, in der sämtliche Einstellungen für den Host und die VMs dokumentiert sind. Wenn Sie hier bei der Einrichtung sorgfältig arbeiten, können Sie sich anschließend aufs Lernen konzentrieren und müssen nicht ständig Probleme bekämpfen. Dies gilt selbstverständlich nicht nur für die Testumgebung, sondern erst recht für das Aufsetzen eines Firmennetzwerks im Produktiveinsatz.

## Optisches Laufwerk freigeben

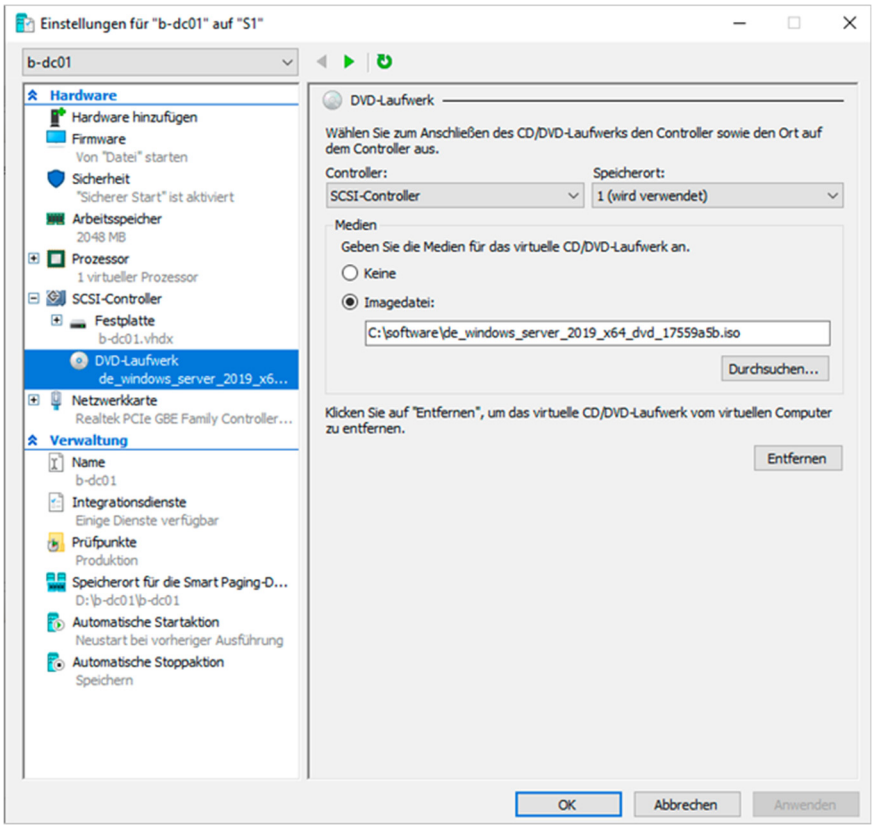
Falls Sie während der Installation das physische DVD-Laufwerk verwendet haben, müssen Sie es wieder freigeben, bevor es in einer anderen VM benutzt werden kann. ISO-Dateien erfordern zwar keinen exklusiven Zugriff, es ist jedoch auch hier sinnvoll, die virtuelle DVD „auszuwerfen“, da sonst bei jedem Startvorgang der VM davon gebootet wird.


Schulversion
© HERDT-Verlag

Gehen Sie wie folgt vor:

- Wählen Sie im Hyper-V-Manager den virtuellen Computer, den Sie verwalten möchten, und klicken Sie unter *Aktionen* auf *Einstellungen.*
- Wählen Sie im Listenbereich unter *Hardware* das DVD- Laufwerk aus.
- Wählen Sie unter *Medien* die Option *Keine*.
- Klicken Sie auf *Anwenden* und *OK*.

  Das optische Laufwerk steht nun den anderen VMs wieder zur Verfügung und es ist auch kein ISO-Abbild mehr eingelegt.




*Optisches Laufwerk entfernen*

Sie können bei laufender VM das physische DVD-Laufwerk auch wieder freigeben, indem Sie im Menü *Medien - DVD-Laufwerk* auf *<Laufwerksbuchstabe> freigeben* klicken. Falls Sie eine ISO-Datei geladen haben, klicken Sie auf *<ISO-Datei> auswerfen*.

## Prüfpunkt erstellen

Um für weitere Übungen stets zu diesem Systemzustand zurückkehren zu können, sollten Sie nun einen Prüfpunkt von allen virtuellen Maschinen erstellen. Rufen Sie hierzu im Hyper-V-Manager die entsprechende Aktion auf. Das System generiert daraufhin eine Datei, die den Namen des Rechners mit Datum und Uhrzeit trägt und am Speicherort der Systemabbilddatei im Unterverzeichnis *Prüfpunkte* abgelegt wird.

Zum Verwalten der Prüfpunkte stehen Ihnen im Bereich der Aktionen im Hyper-V-Manager die folgenden Befehle zur Verfügung:

| | |
|---|---|
| *Einstellungen* | Mit *Einstellungen* können Sie die Systemzuordnungen eines Abbildes bearbeiten. Hier können Sie z. B. virtuelle Laufwerke, Arbeitsspeicher oder Prozessoren einem Prüfpunkt eines Systems zuordnen. |
| *Anwenden* | Mit *Anwenden* ersetzen Sie den momentanen Betriebszustand eines virtuellen Computers durch einen Prüfpunkt. Das System muss dafür neu gestartet werden. |
| *Umbenennen* | Verwenden Sie aussagekräftige Namen für Ihre Prüfpunkte und nennen Sie z. B. den eben erstellten Prüfpunkt *Frisch installiert*. |
| *Prüfpunkt löschen* | Sie können einzelne Prüfpunkte löschen, wenn Sie diese nicht mehr benötigen oder der Speicherplatz knapp wird. Die anderen Prüfpunkte werden dadurch nicht beeinträchtigt und funktionieren weiterhin. |
| *Prüfpunkt-unterstruktur löschen* | Prüfpunkte werden nach einem hierarchischen System ab dem Zeitpunkt des Erstellens organisiert. Klicken Sie hier, um einen Prüfpunkt mit seiner Unterstruktur zu löschen. Auch dieser Vorgang beeinträchtigt die Funktion der verbleibenden Prüfpunkte nicht. |

## Prüfpunkte verwenden

Die Anfertigung von Prüfpunkten dauert nicht sehr lange. Prüfpunkte speichern jeweils nur die Änderungen seit dem letzten Prüfpunkt, also ist es ratsam, häufig einen Prüfpunkt anzufertigen. Sie sollten den Zustand der gesamten Testumgebung regelmäßig sichern, indem Sie zeitnah von **allen** VMs einen Prüfpunkt anfertigen. Benennen Sie diese Prüfpunkt-Sets so, dass Sie später erkennen können, welche Prüfpunkte zusammengehören. Nur durch diese Sets können Sie sicherstellen, dass sich Ihre Testumgebung nach der Rückkehr zu einem früheren Zeitpunkt wieder in einem konsistenten Zustand befindet. Ist dies nicht der Fall, treten nach einiger Zeit merkwürdige Probleme auf, die kaum zu orten und nur schwer zu beseitigen sind.

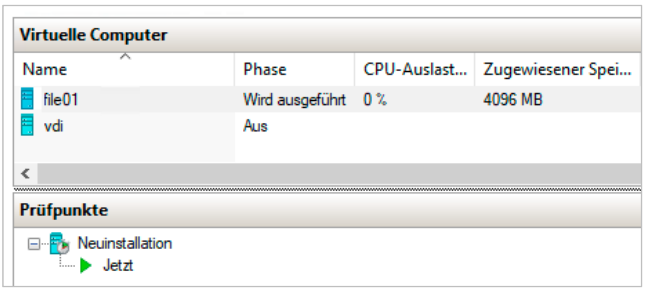
Verwenden Sie Prüfpunkte, um Zwischenstadien Ihrer Übungen festzuhalten. So kann z. B. ein Server vor der Installation einer zusätzlichen Rolle abgebildet werden. Wenn Sie anschließend die Rolle entfernen möchten, können Sie stattdessen einfach auf den Prüfpunkt des Systems ohne die Rolle wechseln. Sie können auch Konfigurationen rückgängig machen, die das System nur einmalig erlaubt, etwa das Hochstufen der Domänenfunktionsebene.

Bedenken Sie dabei jedoch, dass bestimmte Änderungen auf allen Servern der Domäne gleichzeitig erfolgen müssen. In einem solchen Fall müssten Sie auch die Prüfpunkte sämtlicher Server in der Version laden, die die benötigte Umgebung darstellen.

## Testumgebung überprüfen

Überprüfen Sie die folgende Checkliste:

- Sie haben virtuelle Maschinen eingerichtet, auf denen Windows Server 2019 installiert und aktiviert wurde.
- Alle VMs befinden sich in einem internen Netz ohne Verbindung nach außen.
- Von allen VMs wurden Prüfpunkte angefertigt.
- Falls alles zutrifft, sind Sie nun bereit für die folgenden Kapitel.




## Datenaustausch zwischen VMs und Host ermöglichen

Beim Einsatz von VMs ist es praktisch, wenn man eine Möglichkeit hat, Daten zwischen den VMs und dem Host auszutauschen. Hierfür bietet es sich an, eine Netzwerkfreigabe auf dem Host zu erstellen, die Sie dann auf jeder VM als Netzlaufwerk einbinden. Auf diese Weise können Sie z. B. Skripte und Screenshots zentral abspeichern.


Schulversion
© HERDT-Verlag

# 6 Active Directory

**In diesem Kapitel erfahren Sie**

- Grundlagen über den Verzeichnisdienst Active Directory
- was Domänen, Strukturen, Gesamtstrukturen und Vertrauensstellungen miteinander zu tun haben
- was Funktionsebenen sind
- was Betriebsmaster und globaler Katalog bedeutet
- wie Active Directory strukturiert werden kann

**Voraussetzungen**

- Grundkenntnisse im Aufbau von Computer-Netzen

## 6.1 Überblick Verzeichnisdienst

Das Active Directory (AD) ist der Verzeichnisdienst in Windows-Netzen, mit dem alle Ressourcen hierarchisch gespeichert, identifiziert und zugänglich gemacht werden. Der Aufbau der dahinterliegenden Datenbank orientiert sich am sogenannten X.500-Standard. Zur Abfrage und Modifikation der Datenbankinhalte wird das **L**ightweight **D**irectory **A**ccess **P**rotocol (**LDAP**) genutzt, weshalb beim Active Directory auch von einem LDAP-Verzeichnis gesprochen wird. Das Active Directory ist die Kernkomponente der Active Directory-Domänendienste (Active Directory Domain Services, AD DS).

Das Schema definiert die Struktur bzw. den Aufbau einer LDAP-Datenbank. Im Schema werden zunächst Attribute (z. B. SamAccountName) definiert, die u. a. den Typ eines Eintrags festlegen (z. B. Text, ganze Zahl). Attribute werden dann in Klassen (z. B. Account) zusammengefasst. Als Verzeichnis-Eintrag wird ein Objekt gespeichert, das zu mindestens einer Klasse gehören muss. Jedes Objekt wird eindeutig durch den Distinguished Name (DN) gekennzeichnet.

Active Directory ermöglicht es, die Struktur eines Unternehmens abzubilden. Dazu dienen verschiedene Objekte (z. B. Benutzer, Gruppe, Computer), die Sie an verschiedenen Orten (Organisationseinheit, Domäne) speichern können. Grundsätzlich ist die AD-Datenbankdatei *NTDS.dit* in drei Teile gegliedert:

- Die Schema-Partition enthält das Schema.
- Die Konfigurations-Partition enthält Informationen über vorhandene Domänen und die Vertrauensstellung.
- Die Domänen-Partition enthält alle Objekte einer bestimmten Domäne.

Der Inhalt der Schema- und der Konfigurations-Partition ist auf allen Domänencontrollern in einem AD identisch.

Das AD wird durch die AD-Domänendienste (ADDS, Active Directory Domain Services) verwaltet, die als eine Serverrolle hinzugefügt werden.

## 6.2 Domäne, Struktur und Gesamtstruktur

### Planung der Verzeichnisstruktur

Eine Verzeichnisstruktur sollte den Bedürfnissen der Firma, der Verwalter und der Benutzer gerecht werden. Vor der Implementierung des Verzeichnisdiensts müssen Sie daher die Firmenstruktur und Geschäftsbereiche im Hinblick auf logische Zusammenhänge zwischen Geschäftsprozessen, Abhängigkeiten und Hierarchien sowie die Funktion und Aufgabenteilung untersuchen. Geografische Gegebenheiten haben in der Regel keinen Einfluss auf die Domänenplanung.

### Domäne

Eine Domäne ist ein zentral verwaltbarer Sicherheitsbereich, der eine administrative Grenze im Active Directory bildet. Zur strukturierten Speicherung der Objekte dienen Organisationseinheiten.

Viele Active Directory-Implementierungen bestehen aus einer einzelnen Domäne. Mehrere Domänen sollten Sie nur dann einsetzen, wenn Sie Millionen von Objekten verwalten müssen, administrative Grenzen benötigen, z. B. bei mehreren Gruppen von Domänen-Admins oder bei einzelnen Standorten mit sehr langsamen Verbindungen untereinander. Schon seit Windows Server 2008 sind unterschiedliche Kennwortrichtlinien kein Grund mehr, zusätzliche Domänen einzurichten.

Eine Domäne erstellen Sie durch die entsprechende Installation eines Domänencontrollers. Die Namensgebung für Domänen orientiert sich am DNS-Namespace – dazu später mehr.

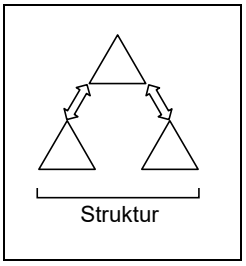
Ein Domänencontroller (DC) speichert immer sämtliche Objekte seiner Domäne. Er kann niemals DC für mehrere Domänen sein.

### Struktur

Eine Struktur entsteht, wenn Sie in Ihrem Active Directory weitere Domänen erstellen und ihnen den Namen einer Subdomäne (zu einer bestehenden Domäne) geben.

Ein Beispiel: Ihre erste Domäne heißt *Firma.intern* und Sie erstellen eine zusätzliche Domäne mit dem Namen *Forschung.Firma.intern*. Um die Abbildung umzusetzen, könnten Sie eine dritte Domäne erstellen und ihr den Namen *Produktion.Firma.intern* geben.

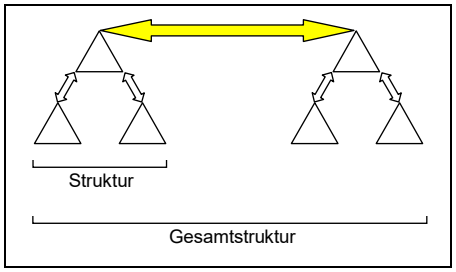
Eine Struktur wird in der Literatur oft auch als Baum oder **Tree** bezeichnet.




*Struktur*

### Gesamtstruktur

Eine Gesamtstruktur entsteht, wenn Sie im Active Directory eine zusätzliche Domäne erstellen und als Bezeichnung einen anderen Namen als die bestehende Domäne *Firma.intern* wählen, z. B. *Unternehmen.intern*. Die Domänen *Unternehmen.intern* und *Firma.intern* liegen dann neben- und nicht untereinander.




*Gesamtstruktur*

Die Abbildung zeigt eine Gesamtstruktur, die aus zwei Strukturen à drei Domänen besteht. Gesamtstruktur bezeichnet immer alle Domänen, die zu einem Active Directory gehören, auch wenn es sich dabei nur um eine einzelne Domäne handelt. Gesamtstrukturen werden auch als Wald oder **Forest** bezeichnet.

Jede Domäne muss sich in einer Gesamtstruktur befinden, daher wird beim Anlegen der ersten Domäne in einer Firma gleichzeitig eine neue Gesamtstruktur erstellt.


Schulversion
© HERDT-Verlag

### Vertrauensstellungen

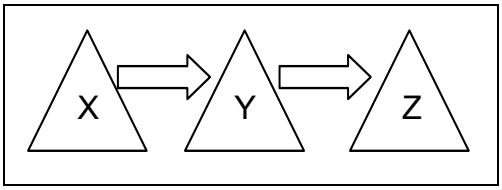
Innerhalb eines Active Directory werden automatisch Vertrauensstellungen zwischen Domänen angelegt – symbolisiert durch die Pfeile in den beiden Abbildungen oben. Vertrauensstellungen ermöglichen es, dass Benutzer einer Domäne auf Ressourcen einer anderen Domäne zugreifen können.

Eine Vertrauensstellung beschreibt die Beziehung zwischen zwei Domänen. Die vertrauende Domäne (Pfeilspitze) lässt Anmeldeauthentifizierungen aus der vertrauten Domäne zu; sie vertraut den Benutzern der vertrauten Domäne.

### Unidirektionale, nichttransitive Vertrauensstellung

Aus der Annahme „Domäne X vertraut Domäne Y und Domäne Y vertraut Domäne Z“ ergeben sich folgende Konsequenzen:

- Domäne X vertraut nicht automatisch Domäne Z.
- Domäne Y vertraut nicht automatisch Domäne X.
- Domäne Z vertraut nicht automatisch Domäne Y.




*Unidirektionale, nichttransitive Vertrauensstellungen*

Wären die Vertrauensstellungen transitiv, dann würde Domäne X auch der Domäne Z vertrauen.

### Bidirektionale, transitive Vertrauensstellungen

Alle automatisch erstellten Vertrauensstellungen innerhalb eines Active Directory sind bidirektional (gegenseitig) und transitiv (durchlässig). Dadurch vertraut jede Domäne jeder anderen – eventuell über einige dazwischenliegende Domänen hinweg.

Sie können auch Vertrauensstellungen zu Domänen aufbauen, die nicht zum selben Active Directory gehören. Die Funktionsweise ist weitgehend identisch mit der eben beschriebenen.

## 6.3 Funktionsebenen

### Überblick

Funktionsebenen sind Betriebsmodi des Active Directory, die festlegen, welche Funktionen zur Verfügung stehen und welche Betriebssystem-Versionen Sie für Domänencontroller einsetzen können. Funktionsebenen gibt es auf Domänen- und Gesamtstruktur-Ebene.

Die Betriebssystem-Version sämtlicher betroffener DCs darf nicht kleiner sein als die Funktionsebene. Wenn Sie z. B. versuchen, in der Funktionsebene *Windows Server 2019* einen Windows Server 2008 zum DC hochzustufen, so wird das fehlschlagen.

Sind die Voraussetzungen erfüllt, können Sie Funktionsebenen heraufstufen. Ein Herunterstufen ist nicht möglich.

### Domänenfunktionsebenen

Es folgt eine Auflistung wichtiger Erweiterungen, die in den einzelnen Funktionsebenen dazukommen. Für Windows Server 2019 wird es keine eigene Funktionsebene geben.

- Windows Server 2008 – mehrere Kennwortrichtlinien in einer Domäne, DFS-Replikation von SYSVOL
- Windows Server 2008 R2 – verbesserte Kerberos-Authentifizierung
- Windows Server 2012/2012 R2 – dynamische Zugriffskontrolle (Dynamic Access Control, DAC)
- Windows Server 2016 – keine zusätzlichen Funktionen

Bei Windows Server 2012/2012 R2 wird als Domänen- und Gesamtstrukturfunktionsebene ebenfalls Windows Server 2012/2012 R2 vorgeschlagen. Bedenken Sie hier, dass es später nicht mehr möglich ist, die Funktionsebene herabzustufen!

Die Domänenfunktionsebene heraufstufen können Sie nach einem Rechtsklick auf den Domänennamen in Active Directory-Benutzer und -Computer. Alternativ können Sie dies auch in der Konsole Active Directory.

### Gesamtstrukturfunktionsebenen

- Windows Server 2008 – keine zusätzlichen Funktionen
- Windows Server 2008 R2 – AD-Papierkorb
- Windows Server 2012/2012 R2 – keine zusätzlichen Funktionen
- Windows Server 2016 – keine zusätzlichen Funktionen

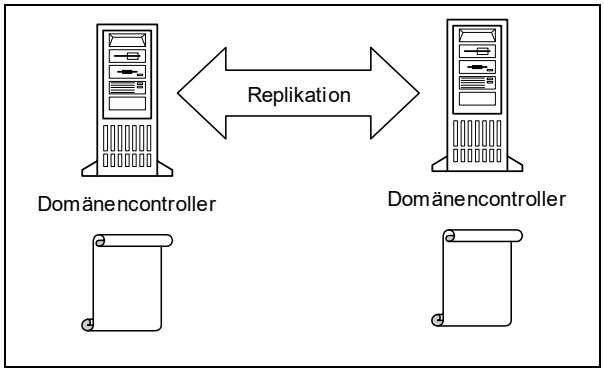
Fügen Sie Ihrem Active Directory neue Domänen hinzu, entspricht deren Domänenfunktionsebene der Gesamtstrukturfunktionsebene. Zum Heraufstufen der Gesamtstrukturfunktionsebenen benötigen Sie das MMC-Snap-In *Active Directory-Domänen und -Vertrauensstellungen*. Klicken Sie mit der rechten Maustaste direkt auf das Snap-In und wählen Sie den entsprechenden Eintrag im Kontextmenü. Wenn Sie das Snap-In aufklappen und mit rechts auf eine Domäne klicken, können Sie dort auch die Domänenfunktionsebene heraufstufen.

Sie dürfen die Gesamtstrukturfunktionsebene erst heraufstufen, wenn alle Domänen die entsprechende Funktionsebene erreicht haben.

## 6.4 Domänencontroller, Betriebsmaster und globaler Katalog

### Multimaster-Replikationsmodell

Um die Ausfallsicherheit zu erhöhen, sollte jede Domäne über mehrere Domänencontroller verfügen. Da alle DCs einer Domäne gleichberechtigt sind, können Verwaltungsaufgaben auch auf jedem DC erfolgen. Verändern Sie ein Objekt, müssen diese Informationen natürlich auch auf die anderen Domänencontroller übertragen werden. Dieser Vorgang wird als Replikation bezeichnet. Active Directory bestimmt über die Replikationstopologie automatisch (welcher DC aktualisiert seine Informationen von welchen DCs). Manuelles Eingreifen ist hier nur in Spezialfällen notwendig.




*Replikation zwischen Domänencontrollern*

Die sogenannten Betriebsmaster-Rollen stellen eine Ausnahme von dieser Gleichberechtigungsregel dar.

### Read-Only Domain Controller – schreibgeschützter DC

Mit Windows Server 2008 wurde der sogenannte Read-only Domain Controller (RODC) eingeführt. RODCs zielen auf den Einsatz in kleinen Filialen, in denen eine physische Sicherung des Servers (Zugangs- und Diebstahlschutz) nicht gegeben ist. Sie können festlegen, welche Benutzerkonten zu einem RODC repliziert werden. Die fehlenden Schreibrechte stellen einen weiteren Schutz gegen Missbrauch dar.


Schulversion
© HERDT-Verlag

Voraussetzungen für den Einsatz eines Read-only Domain Controllers sind:

- Gesamtstruktur-Funktionsebene mindestens Windows Server 2003
- Mindestens ein beschreibbarer Domänencontroller mit einem Betriebssystem ab Windows Server 2008 in der Domäne des RODC
- Ein Domänen-Admin muss den Befehl `adprep /rodcprep` ausgeführt haben.

## Betriebsmaster (FSMOs)

Der Betriebsmaster (Flexible Single Master Operation, FSMO) ist eine Funktion auf einem Domänencontroller, die so sensibel für das Funktionieren des Active Directory ist, dass diese Aufgabe nicht von mehreren DCs übernommen werden darf.

Insgesamt gibt es fünf Betriebsmaster-Rollen. Die ersten beiden sind einmalig in einer Gesamtstruktur, die folgenden drei sind einmalig in jeder Domäne.

| | |
|---|---|
| Schema-Master | Veränderungen am Schema können nur auf diesem Rollen-Inhaber vorgenommen werden; notwendig z. B. bei einer Exchange-Installation. |
| Domain-Name-Master, auch DNS-Master genannt | Stellt beim Erstellen neuer oder beim Löschen vorhandener Domänen sicher, dass Active Directory in einem funktionsfähigen Namensraum arbeitet |
| Infrastruktur-Master | Verantwortlich für die korrekte Namenszuordnung bei domänenübergreifenden Gruppenmitgliedschaften |
| RID-Master (Relative ID) | Stellt die Eindeutigkeit von Domänen-Objekten sicher (SID-Generierung) |
| PDC-Emulator (Primärer DC) | Verschiedene Aufgaben im Zusammenhang mit Kennwortänderungen, zentrale Zeit-Quelle für alle Domänen-Computer |

Standardmäßig werden dem ersten Domänencontroller einer neuen Gesamtstruktur alle fünf FSMO-Rollen zugewiesen. Dem ersten DC einer zusätzlichen Domäne werden standardmäßig die drei domainweiten Funktionen übertragen.

Betriebsmaster-Rollen können zwischen Domänencontrollern derselben Domäne übertragen werden.

Wollen Sie die Anzeige von Domänencontrollern in der PowerShell filtern lassen, zum Beispiel, um die PDC-Master anzeigen zu lassen, verwenden Sie:

```
Get-ADDomainController -Filter {OperationMaster-Roles -like "PDC*"}
```

Wollen Sie nur die Namen und die installierten Betriebsmaster anzeigen, ergänzen Sie das CMDlet noch mit `|fl Hostname, OperationMasterroles`

Sie können in der PowerShell auch Daten einzelner Domänen abfragen. Dazu verwenden Sie das CMDlet *Get-ADDomain*. Das CMDlet *Get-ADForest* zeigt Informationen zu Gesamtstrukturen an. In jeder Domäne gibt es die drei FSMO-Rollen, die Sie mit dem folgenden Befehl anzeigen lassen:

```
Get-ADDomain | Select InfrastructureMaster, RID-Master, PDCEmulator
```

Schema-Master und Domänennamen-Master gibt es nur einmal pro Gesamtstruktur. Diese Informationen lassen sich wiederum mit dem CMDlet *Get-ADForest* anzeigen:

```
Get-ADForest | Select-Object DomainNamingMaster, SchemaMaster
```

Um sich einen Überblick über alle Betriebsmaster einer Gesamtstruktur zu verschaffen, können Administratoren den Befehl `netdom query fsmo` in der Eingabeaufforderung aufrufen.

Betriebsmasterrollen lassen sich in der PowerShell auf andere Domänencontroller verschieben. Das passende CMDlet dazu ist:

```
Move-ADDirectoryServerOperationMasterRole
```

Mit `get-help Move-ADDirectoryServerOperationMasterRole` lassen Sie sich die umfassende Syntax und einige Beispiele für das CMDlet anzeigen.

### Globaler Katalog

Der globale Katalog (Global Catalog, GC) stellt eine domänenübergreifende Suchfunktion für AD-Objekte zur Verfügung. Im GC werden ausgewählte Attribute aller Objekte aus allen Domänen gespeichert. Diese Funktion kann nur ein Domänencontroller übernehmen. GC-Server spielen eine wichtige Rolle, ohne die manche AD-Funktionen nicht funktionieren. Sie sollten jeden Domänencontroller auch zu einem globalen Katalog-Server machen.

An jedem Standort in Active Directory sollte ein globaler Katalog-Server installiert sein. Der globale Katalog ist eine weitere Rolle, die ein Domänencontroller einnehmen kann. Im Gegensatz zu den beschriebenen FSMO-Rollen kann (und sollte) die Funktion des globalen Katalogs mehreren Domänencontrollern zugewiesen werden.

### Verwaltung und Verteilung der Betriebsmaster

Die Stabilität und Performance der Betriebsmaster spielt für die Stabilität der Gesamtstruktur eine nicht unerhebliche Rolle. Aus diesem Grund sollten die Rollen auch möglichst optimal verteilt und verwaltet werden. Standardmäßig besitzt der erste installierte Domänencontroller einer Gesamtstruktur alle fünf FSMO-Rollen seiner Domäne und der Gesamtstruktur. Jeder erste Domänencontroller weiterer Domänen verwaltet die drei Betriebsmasterrollen seiner Domäne (PDC-Emulator, RID-Master, Infrastrukturmaster). Vor allem in größeren Active Directorys empfiehlt Microsoft jedoch die Verteilung der Rollen auf verschiedene Domänencontroller.

#### Empfehlungen zur Verteilung von Betriebsmastern

Zur optimalen Verteilung der FSMO-Rollen gibt es folgende Empfehlungen:

- Der Infrastruktur-Master sollte nicht auf einem globalen Katalog liegen, da ansonsten Probleme bei der Auflösung von Gruppen, die Mitglieder aus verschiedenen Domänen haben, auftreten können.
- Domänennamen-Master und Schema-Master sollten auf einem gemeinsamen Domänencontroller liegen, der auch globaler Katalog ist.
- PDC-Emulator und RID-Master kommunizieren viel miteinander und sollten daher auf einem gemeinsamen Domänencontroller liegen, der auch globaler Katalog ist.

Um sich einen Überblick über alle Betriebsmaster einer Gesamtstruktur zu verschaffen, können Administratoren den Befehl `netdom query fsmo` in der Eingabeaufforderung aufrufen.

## 6.5 Organisationseinheit – OU

### Sinn von Organisationseinheiten

Eine OU (Organizational Unit) ist ein Objekt in einer Domäne, das verschiedenen Zwecken dient:

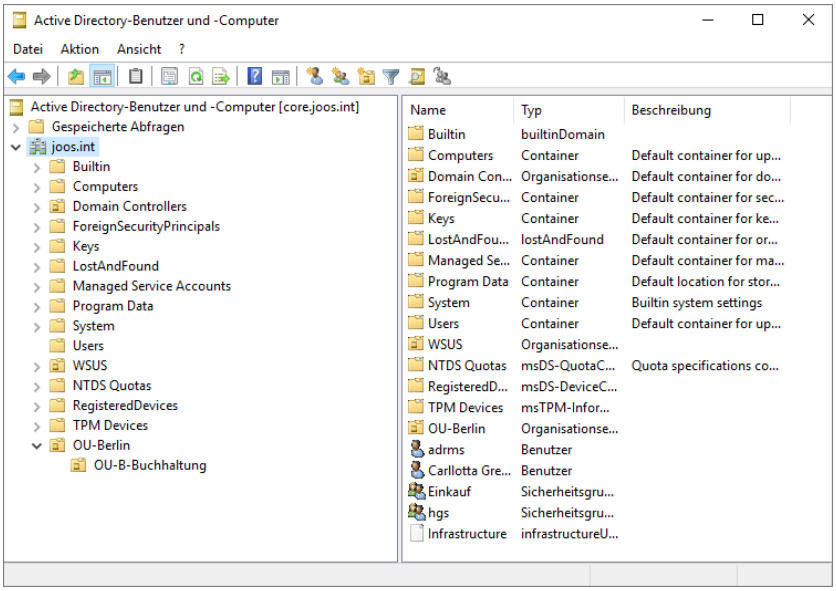
- Strukturiertes Speichern von Objekten, vergleichbar mit dem Speichern von Dateien in Ordnern
- Delegierung von Verwaltung; u. a. die Benutzer- und Gruppenverwaltung kann auf OU-Ebene an Nicht-Administratoren delegiert werden. Dadurch werden weniger Benutzerkonten mit hohen Rechten benötigt.
- Gezieltes Zuweisen von Gruppenrichtlinien. Den überwiegenden Teil der Computer- und Benutzerkonfiguration sollten Sie mit Gruppenrichtlinien (Group Policy Objects, GPOs) erledigen.


© HERDT-Verlag

In den Aufbau Ihrer OU-Struktur sollten Sie einige Überlegungen stecken. Entwerfen Sie ein Schema und halten Sie es anschließend konsequent ein. Besonders wichtig ist hier die sinnvolle und einheitliche Benennung der einzelnen OUs. Das beginnt mit scheinbar trivialen Dingen wie der Benennung von Organisationseinheiten. Alle OUs sollten aussagekräftige Namen erhalten, sodass Sie allein durch den Namen Hierarchie, Standort und Funktion erkennen können (vgl. Abschnitt 1.3). Der Name jeder Organisationseinheit sollte mit den Buchstaben *OU* beginnen, z. B. *OU-Berlin*. So können Sie z. B. den Standort *Berlin* klar von der ihn repräsentierenden Organisationseinheit unterscheiden.

In der Abbildung wird das Grundmuster vieler größerer Domänen dargestellt. Dabei wurde die Domäne um den Standort Regensburg erweitert, um den Aufbau zu verdeutlichen. Im Buch *Erweiterte Netzwerkadministration* werden Sie mit mehreren Standorten arbeiten.

Zunächst werden alle geografischen Standorte abgebildet. Deren Inhalt wird dann weiter untergliedert. Je nach Anzahl der zu verwaltenden Objekte und Ihren Bedürfnissen kann diese Gliederung auch anders aussehen, z. B. können einzelne Abteilungen eingefügt werden, auf die die Benutzer und PCs verteilt werden.




*OU-Struktur*

Bei einer zentralen Verwaltung kann es sinnvoll sein, Standort-OUs erst auf der zweiten Ebene zu verwenden und auf der ersten Ebene z. B. nach Abteilung oder Funktion zu gliedern.

Sollte bei Ihnen z. B. der Container *LostAndFound* nicht angezeigt werden, können Sie im Menü *Ansicht - Erweiterte Features* einschalten. Ohne diese Einstellung sind auch manche Objekt-Eigenschaften nicht sichtbar.

## 6.6 Standorte im Active Directory

Wächst Ihr Active Directory über den Umfang eines einzelnen LANs hinaus, dann arbeiten Sie an unterschiedlichen geografischen Standorten, die Sie über teure und vergleichsweise langsame Weitverkehrsverbindungen (Wide Area Network, WAN) zusammenschließen müssen. Das ist immer mit verschiedenen IP-Netzen und Routing verbunden.

Wenn Sie bezüglich der AD-Replikation und der Domänenanmeldung auf den standortübergreifenden Datenverkehr Einfluss nehmen wollen, müssen Sie Active Directory-Standorte definieren. Das prinzipielle Vorgehen dabei ist:

- Sie definieren **Standortnamen**, z. B. *Berlin*, *Bremen*, *Regensburg*.
- Sie geben die verwendeten **IP-Netze** an, z. B. 10.10/16, 10.20/16, 10.30/16, und verknüpfen diese mit den zugehörigen Standortnamen.
- Sie verschieben Domänencontroller in die entsprechenden Standorte. Im Regelfall sollte an jedem Standort auch ein globaler Katalog-Server verfügbar sein.
- Sie definieren **Standortverknüpfungen** und geben an, welche Standorte zu dieser Verknüpfung gehören. Bei den Standortverknüpfungen geben Sie u. a. ein Replikationsintervall und einen Kostenfaktor an.

Bei AD-bezogenem Datenverkehr versuchen Clients nun, zunächst standortlokale Ressourcen zu nutzen. Ist die Ressource nicht lokal vorhanden, wird diejenige genutzt, die über die billigste Standortverknüpfung (Kostenfaktor) erreichbar ist. Erfolgt der Zugriff dabei über mehrere Standortverknüpfungen hinweg, addieren sich die einzelnen Kostenfaktoren auf. Auch verteilte Dienste wie z. B. DFS (Distributed File System) nutzen diesen Mechanismus.

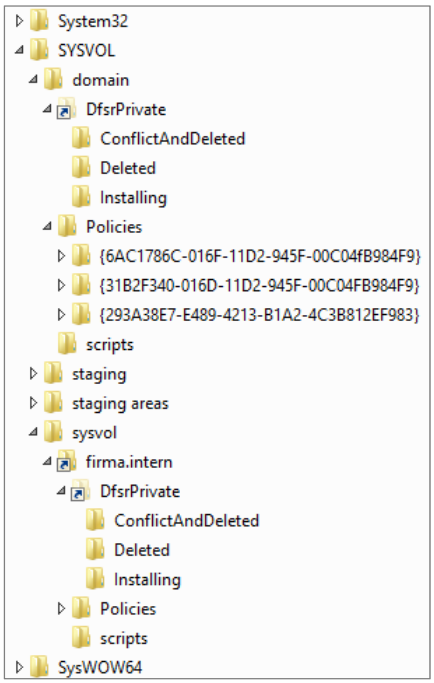
An jedem Standort sollte ein globaler Katalog vorhanden sein.

Ein Active Directory-Standort hat nichts mit Domänen oder Organisationseinheiten zu tun. Prinzipiell handelt es sich dabei nur um ein oder mehrere IP-Netze, die mit einem Namen versehen wurden.

## 6.7 Sysvol – Ressourcen für Anmeldungen

Jeder Domänencontroller stellt bei der Anmeldung Gruppenrichtlinien zur Verfügung. Für die Benutzeranmeldung ist zusätzlich ein Anmeldescript möglich. Diese Informationen werden nicht in der Datei *NTDS.dit* gespeichert, sondern im Ordner *SYSVOL*, dessen Speicherort beim Installieren des Domänencontrollers gewählt wurde (standardmäßig ist es *C:\Windows\SYSVOL*). Er enthält die Ordner *domain*, *staging*, *staging areas* und *sysvol*.

Der Ordner *SYSVOL\sysvol* ist auf jedem DC vorhanden und entspricht der Freigabe SYSVOL. Darin befindet sich ein Ordner mit dem Namen Ihrer Domäne. Das Pfeilsymbol signalisiert, dass es sich dabei um eine Verbindung handelt. Dieser Link zeigt auf den Ordner *SYSVOL\domain*, deshalb sind die angezeigten Inhalte auch identisch.




Die Ordner *SYSVOL\staging* und *SYSVOL\staging areas* werden für die Verwaltung der Replikation benötigt.

In den Ordnern *SYSVOL\domain\Policies* und *SYSVOL\sysvol\<Domänenname>\Policies* finden Sie mehrere Ordner, deren Namen mit einer geschweiften Klammer beginnen. Jeder dieser Ordner enthält ein Gruppenrichtlinienobjekt.

Der Ordner *SYSVOL\sysvol\<Domänenname>\scripts* entspricht der Freigabe *NETLOGON*, wo Benutzer-Anmeldeskripte gespeichert werden.

Der Inhalt der Freigabe *SYSVOL* wird vom File Replication Service (FRS) zwischen den DCs einer Domäne repliziert. Die Replikation kann auch über das DFS erfolgen. Aus dem Ordner *SYSVOL* wird dann der Ordner *SYSVOL_DFSR*.

Die Freigaben *SYSVOL* und *NETLOGON* werden vom Anmeldedienst *netlogon* benötigt.


Schulversion
© HERDT-Verlag

# 7 Active Directory installieren

**In diesem Kapitel erfahren Sie**

- wie Sie Active Directory-Verzeichnisdienste installieren
- wie Sie eine Gesamtstruktur einrichten
- wie Sie eine Stammdomäne einrichten
- wie Sie einen neuen Domänencontroller zu einer vorhandenen Domäne hinzufügen
- wie Sie die Domänenfunktionsebene heraufstufen
- wie Sie eine DNS-Zone ins Active Directory integrieren können
- wie Sie Objekte im Active Directory erkunden können

**Voraussetzungen**

- DNS-Dienst einrichten und konfigurieren
- Konzepte von Active Directory

## 7.1 Installation vorbereiten

### Logische Struktur für die Testumgebung

Die Gesamtstruktur für das Unternehmen *Firma GmbH* besteht aus einer Domäne. Dies entspricht der gängigen Praxis. Es gilt, so wenige Domänen wie möglich zu installieren, da jede zusätzliche Domäne einen deutlichen administrativen und finanziellen Mehraufwand bedeutet.

Falls Sie Ihre Testumgebung um zusätzliche untergeordnete Domänen erweitern möchten, vergessen Sie nicht, dass Sie nur als Organisationsadministrator Standorte verwalten, DHCP-Server autorisieren oder Gesamtstruktur-funktionsebenen hochstufen können.

Wollen Sie Domänencontroller zu Windows Server 2019 aktualisieren, müssen Sie zunächst das Schema der Gesamtstruktur erweitern. Dazu führen Sie den Befehl `adprep /forestprep` auf einem Domänencontroller aus. Sie finden das Tool im Ordner *support\adprep* auf der Windows Server 2019-DVD.

Damit Sie das Schema erweitern können, müssen Sie zuvor noch mit `c` die Erweiterung bestätigen. Diese Maßnahmen lassen sich nicht mehr rückgängig machen. Nach der Aktualisierung des Schemas sollten Sie mit `adprep /domainprep` noch die einzelnen Domänen aktualisieren. Installieren Sie neue Domänencontroller, lassen sich diese problemlos in Active Directory aufnehmen. Auch Mitgliedsserver mit Windows Server 2019 können Sie in bestehende Domänen aufnehmen.

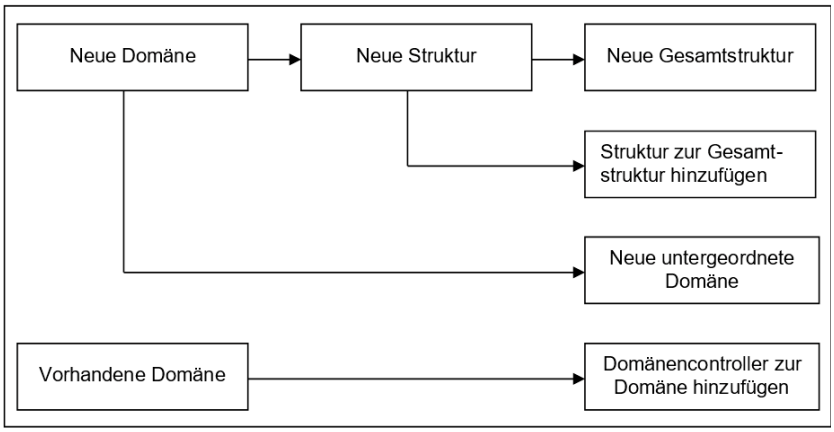
Bei Migrationen können Sie Betriebsmasterrollen von Vorgängerversionen auf die neuen Domänencontroller mit Windows Server 2019 übernehmen. Die Vorgänge dazu sind identisch mit der Übernahme in Windows Server 2008 R2 sowie Windows Server 2012/2012 R2.

### Planung der Implementierung

Benötigte Informationen über die Gesamtstruktur:

- DNS-Domänennamen
- NetBIOS-Namen
- Domänenfunktionsebene

Je nach geplanter struktureller Maßnahme müssen Sie für den jeweiligen Server unter Windows Server 2019 entscheiden, welche Position in der Domänenhierarchie er einzunehmen hat. Außerdem müssen Sie die dafür benötigten Informationen wie DNS-Domänenname oder Kennwörter eines Administrators parat haben.




## Voraussetzungen

Folgende Voraussetzungen müssen im Netzwerk bzw. auf den Servern unter Windows Server 2019 erfüllt sein:

- Für jede Windows-Domäne muss mindestens ein Windows Server vorhanden sein.
- Ein Netzwerkadapter muss installiert und mit einer funktionierenden Gegenstelle verbunden sein. Als Netzwerkprotokoll muss TCP/IP verwendet werden. Es sollte eine statische IP-Adresse verwendet werden.
- In jeder Domäne muss ein DNS-Server vorhanden sein, der SRV-Ressourceneinträge unterstützt. Soweit noch nicht vorhanden, kann der DNS-Serverdienst auch bei der Installation des Active Directorys installiert und konfiguriert werden.
- Zusätzliche Domänencontroller müssen einen DNS-Server abfragen können, um die Domänendienste zu lokalisieren.
- Für alle Server, die als Domänencontroller fungieren sollen, müssen Uhrzeit und Zeitzone korrekt eingestellt sein.
- Sie benötigen die Anmeldeinformationen eines Organisations- oder Domänenadministrators, um eine neue Domäne zu einer Gesamtstruktur oder um einen weiteren Domänencontroller zu einer Domäne hinzuzufügen.

## Verzeichnisdienste deinstallieren

Sie können Active Directory auch wieder deinstallieren. Dadurch wird der betreffende Domänencontroller zu einem Mitgliedsserver in der Domäne oder zu einem alleinstehenden Server, falls er der letzte Domänencontroller war. Diese Maßnahme kann sinnvoll sein, wenn mehrere Domänencontroller in einer Domäne vorhanden sind, einer wiederholt ausfällt und Sie einen anderen Server zum Domänencontroller machen wollen. Ein anderes Beispiel wäre, dass Sie mehrere Domänen zusammenlegen möchten.

Beachten Sie jedoch, dass Sie die Domäne verlieren, falls Sie die Verzeichnisdienste vom einzigen Domänencontroller Ihrer Domäne entfernen. Das Herabstufen des letzten Domänencontrollers muss im Assistenten explizit angegeben werden.

## Rolle *DNS-Server* entfernen

- Klicken Sie im Server-Manager im Menü *Verwalten* auf *Rollen und Funktionen entfernen.*
- Klicken Sie auf *Weiter*.
- Deaktivieren Sie das Kontrollkästchen für *DNS-Server* und bestätigen Sie das Entfernen der dazugehörigen Features mit *Features entfernen*.

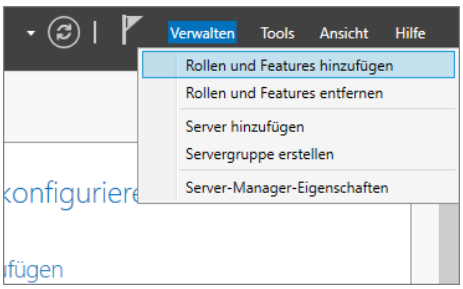
  Falls Sie von diesem Server aus einen entfernten DNS-Server verwalten möchten, deaktivieren Sie die Option *Verwaltungstools entfernen*.
- Klicken Sie auf *Weiter* und dann auf *Entfernen*.
- Starten Sie den Server anschließend neu.


Schulversion
© HERDT-Verlag

## 7.2 Stammdomäne einrichten

### Aufgabenstellung

In der Testumgebung soll die Gesamtstruktur für die *Firma GmbH* aufgebaut werden. Hierzu richten Sie die Stammdomäne *firma.intern* ein. Domänencontroller für die Stammdomäne der Gesamtstruktur wird der Server *B-DC01*. Die DNS-Zone *firma.intern* soll in das Active Directory integriert werden.



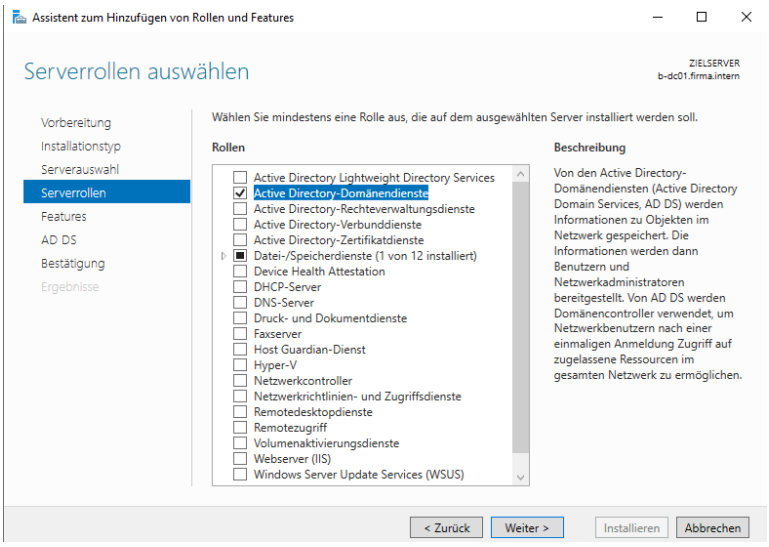

*Rolle hinzufügen über das Menü „Verwalten“*

### Domänencontroller installieren

Der Assistent zum Installieren der AD-Domänendienste befindet sich nun im Server-Manager. Das bisher verwendete **dcpromo** ist nicht mehr verfügbar.

- Melden Sie sich am Server *B-DC01* an und starten Sie den Server-Manager.
- Klicken Sie im Server-Manager in der Menüzeile auf *Verwalten*.
- Klicken Sie auf *Rollen und Funktionen hinzufügen*.
- Wählen Sie als Installationstyp *Rollenbasiert* aus.
- Wählen Sie den Server aus.
- Aktivieren Sie die Serverrolle *Active Directory-Domänendienste* und bestätigen Sie das Hinzufügen der dafür benötigten Features mit *Features hinzufügen*.

  Daraufhin werden die Remoteserver-Verwaltungstools und die AD-Domänendienste (AD DS) der Installationsliste hinzugefügt.




*Auswahl der Serverrolle AD-Domänendienste*

Neben dem Server-Manager können Sie die Binärdateien von Active Directory inklusive der Verwaltungstools auch in der PowerShell installieren. Dazu verwenden Sie den Befehl `Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools`.

Ob die Binärdateien für Active Directory installiert sind, können Sie mit dem CMDlet *get-windowsfeature* anzeigen. Auf diesem Weg lässt sich in der PowerShell anzeigen, welche Serverdienste bereits installiert sind.

Alle Befehle, die für Active Directory zur Verfügung stehen, erhalten Sie über `Get-Command -Module ADDSDeployment` angezeigt. Hilfestellungen rufen Sie mit `Get-Help <Cmdlet>` ab.

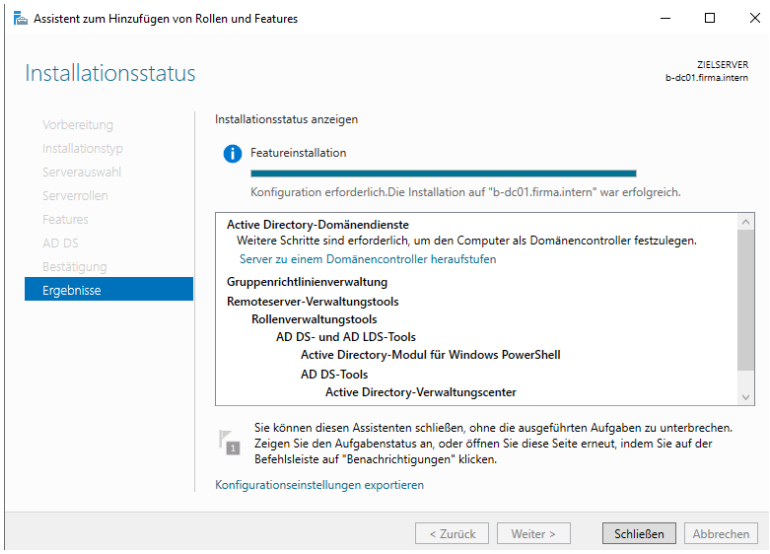
- Bestätigen Sie die Dialoge *Serverrollen*, *Features* und *AD DS* mit *Weiter.*

- Klicken Sie im Dialog *Bestätigung* auf *Installieren*.

  Die Installation der Serverrolle und der Features wird nun durchgeführt.

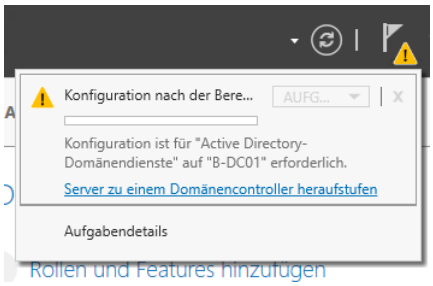
Nach Abschluss der Installation zeigt der Installationsstatus an, dass alle Komponenten erfolgreich installiert wurden, dass jedoch noch weitere Schritte erforderlich sind, um den Server zum Domänencontroller heraufzustufen.

- Klicken Sie auf den Link, um den Server zum Domänencontroller heraufzustufen.




*Heraufstufen zum DC aus dem Assistenten heraus*

*oder* Falls Sie den Assistenten während der Installation geschlossen haben, klicken Sie im Server-Manager auf das Fähnchen mit den aktuellen Aufgaben. Klicken Sie anschließend auf *Server zu einem Domänencontroller heraufstufen*.




*Heraufstufen aus dem Menü heraus*

## Voraussetzungen in der PowerShell testen

Das Cmdlet *Test-ADDSDomainControllerInstallation* ermöglicht das Testen der Voraussetzungen für die Installation eines Domänencontrollers.

Die Voraussetzungen für schreibgeschützte Domänencontroller testen Sie mit *Test-ADDSReadOnlyDomainControllerAccountCreation.*

Mit *Test-ADDSDomainInstallation* testen Sie die Voraussetzungen für die Installation einer neuen Domäne in Active Directory, *Test-ADDSForestInstallation* testet das gleiche für eine neue Gesamtstruktur auf Basis von Windows Server 2019.

Ein Beispiel für den Befehl ist: `Test-ADDSDomainControllerInstallation -DomainName <DNS-Name der Domäne> -SafeModeAdministratorPassword (Read-Host -Prompt Kennwort -AsSecureString).`

## Server zum Domänencontroller hochstufen

Im Konfigurations-Assistenten für die Active Directory-Domänendienste müssen Sie zunächst entscheiden, welche Art von Domänencontroller Sie benötigen.

- Treffen Sie eine Auswahl:

  ① erstellt einen zusätzlichen DC in einer vorhandenen Domäne.

  ② erstellt den ersten DC einer neuen Domäne in einer vorhandenen Gesamtstruktur. Wenn diese Option aktiviert ist, können Sie anschließend zwischen einer untergeordneten Domäne (Subdomain) und einer Strukturdomäne auswählen.

*Auswahl beim Erstellen des Domänencontrollers*


Schulversion
© HERDT-Verlag

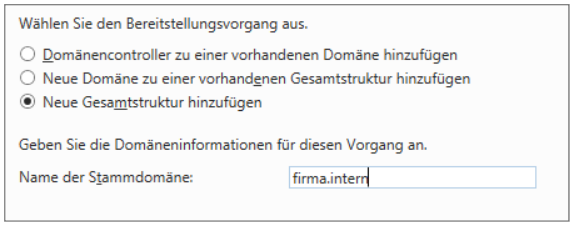
③ erstellt den ersten DC einer neuen Gesamtstruktur, eine Gesamtstruktur-Stammdomäne. Damit etablieren Sie ein neues Active Directory.

Die weiteren Schritte hängen von der gewählten Option ab.

## Neue Gesamtstruktur hinzufügen

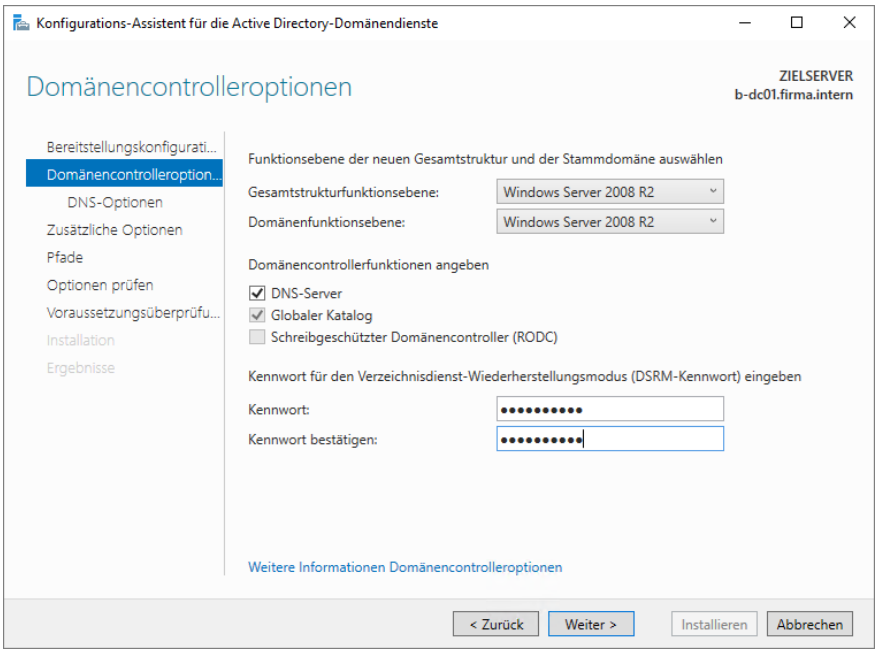
In der Testumgebung gibt es bisher keine Gesamtstruktur und keine Domänen, also benötigen Sie eine neue Gesamtstruktur.

- Wählen Sie auf der Seite *Bereitstellungskonfiguration* die Option *Neue Gesamtstruktur hinzufügen*.
- Geben Sie den vollqualifizierten Namen (FQDN) der neuen Gesamtstruktur-Stammdomäne ein. Wählen Sie hier (mindestens) eine Second-Level-Domain, z. B. *firma.intern,* und klicken Sie auf *Weiter*. Setzen Sie für *Firma* den Namen Ihres Unternehmens ein.




Auf der nächsten Seite können Sie die Domänencontrolleroptionen festlegen.

- Stellen Sie für die Testumgebung jeweils *Windows Server 2008 R2* ein, denn so können Sie anschließend in einer Übung die Ebenen heraufstufen.
- Legen Sie als Gesamtstrukturfunktionsebene anhand des ältesten DCs fest, der in der Gesamtstruktur verwendet werden soll. Bedenken Sie, dass es nicht möglich ist, die Funktionsebenen nachträglich abzusenken.
- Legen Sie anschließend die Domänenfunktionsebene fest.
- Stellen Sie sicher, dass die Optionen *DNS-Server* und *Globaler Katalog* aktiviert sind, denn jeder DC sollte auch DNS-Server sein. Der erste DC einer Gesamtstruktur **muss** globaler Katalog-Server sein, alle weiteren **sollten** es sein. Einen schreibgeschützten Domänencontroller können Sie nur installieren, wenn in der Domäne bereits ein Domänencontroller ab Windows Server 2008 vorhanden ist.
- Geben Sie zweimal das Verzeichnisdienst-Wiederherstellungskennwort ein. Dieses Kennwort benötigen Sie, wenn Sie gelöschte AD-Objekte nach einem Booten in den Verzeichnisdienst-Wiederherstellungsmodus zurückspielen wollen.

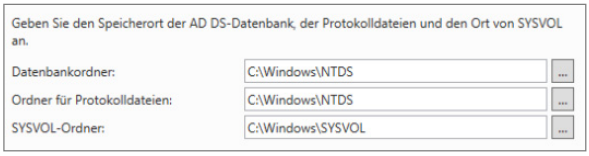


Verwenden Sie hier ein komplexes Kennwort. Dieses sollte 7 oder mehr Zeichen lang sein und mindestens ein Zeichen aus drei der vier folgenden Gruppen enthalten: *a–z, A–Z, 0–9, nicht alphanumerische Zeichen*. Komplexe Kennwörter sind die Standardeinstellung in neuen Domänen.

Das DSRM-Kennwort wird auf jedem Domänencontroller lokal gespeichert und muss für jeden DC getrennt verwaltet werden. Häufig wurde das Kennwort vor längerer Zeit festgelegt und nachträglich nicht mehr aktualisiert. Wenn Sie in einem neuen Firmennetz tätig werden, sollten Sie beizeiten eine Aktualisierung der DSRM-Kennwörter auf allen DCs einplanen, um nicht während einer Notfallwiederherstellung vor unbekannten Kennwörtern zu stehen.

- Klicken Sie auf *Weiter*. Sie erhalten auf der Seite *DNS-Optionen* eine Fehlermeldung, die Sie jedoch in diesem Fall ignorieren können. Klicken Sie auf *Weiter*.
- Überprüfen Sie auf der Seite *Zusätzliche Optionen* den NetBIOS-Domänennamen. Der Assistent schlägt Ihnen den linken Bestandteil des FQDN vor, in unserem Beispiel also *FIRMA*. Klicken Sie auf *Weiter*.
- Ändern Sie bei Bedarf auf der folgenden Seite die Pfade zur AD DS-Datenbank, zu den Protokolldateien und zum SYSVOL. Klicken Sie auf *Weiter*.

Für die Testumgebung ist keine Änderung erforderlich.

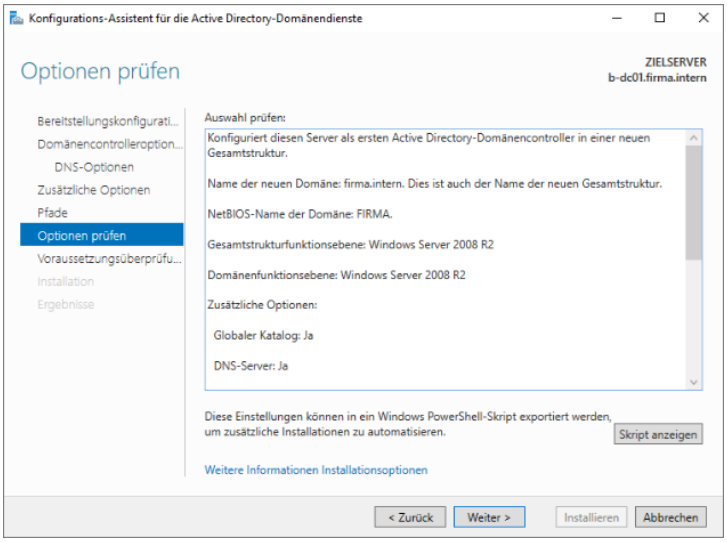



*Pfade zum NTDS und SYSVOL*

Standardmäßig wird die Active Directory-Datenbank in einem Ordner namens *NTDS* (NT Directory Service) auf der Systempartition *C:* abgelegt. Da Windows aus Sicherheitsgründen für das Active Directory-Laufwerk den Schreibcache ausschaltet, empfiehlt sich in der Praxis die Verwendung eines separaten Datenträgers für den Datenbankordner. Die Protokolldateien sollten wiederum nicht auf dem gleichen Datenträger liegen wie die Datenbank, damit Sie bei Ausfall der Datenbankplatte aus einer Sicherung und den Änderungsprotokollen eine aktuelle Version der Datenbank erstellen können. Den Speicherort des Ordners *SYSVOL* sollten Sie nicht verschieben, da sich Replikationsprobleme ergeben können, wenn dieser nicht am Standardspeicherort liegt.

Auf der Seite *Optionen prüfen* erhalten Sie eine Zusammenfassung Ihrer Einstellungen, die Sie mit einem Klick auf *Skript anzeigen* im Texteditor öffnen und abspeichern können. Diese Datei kann später bei unbeaufsichtigten Installationen wiederverwendet werden.

- Überprüfen Sie die Auswahl und klicken Sie auf *Weiter*.



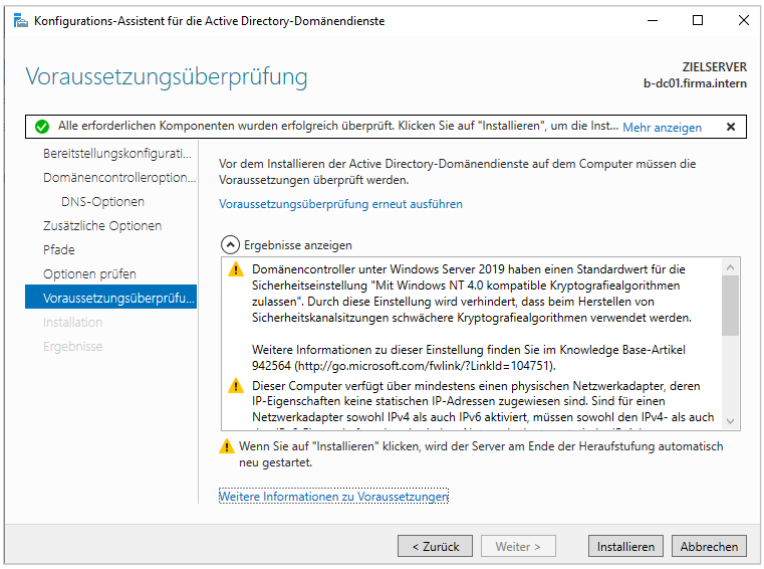

*Übersicht aller Optionen*


Schulversion
© HERDT-Verlag

Im letzten Schritt vor der Ausführung der Installation werden alle beteiligten Komponenten überprüft. Auch bei einer fehlerfreien Konfiguration werden stets mehrere Warnmeldungen angezeigt. Falls Sie als Endergebnis ein grünes Häkchen angezeigt bekommen, sind alle Bedingungen erfüllt. Falls die Überprüfung jedoch Fehler ergeben hat, müssen diese vor der Fertigstellung erst beseitigt werden.

- Klicken Sie auf *Installieren*.

  Der Installationsvorgang wird nun ausgeführt und der Server automatisch neu gestartet.




*Überprüfung vor der Hochstufung zum DC.*

Das Konto *Administrator* dieses Rechners wird automatisch Mitglied der Gruppen *Organisations-*, *Schema-* und *Domänen-Admins*. Als Kennwort wird das bestehende Administratorkennwort verwendet.

Die IP-Konfiguration wird bei der Installation angepasst. Als primärer DNS-Server ist jetzt 127.0.0.1 (localhost) eingetragen. War vorher ein primärer DNS-Server konfiguriert, so fungiert er jetzt als sekundärer. Das gilt auch für die folgenden Beschreibungen.

## In der Domäne anmelden

Windows hat ein neues Konto für den Domänenadministrator angelegt und dafür die Kennwörter (Benutzername und Passwort) vom Konto des lokalen Administrators verwendet. Der erste Domänenadministrator in einer neuen Struktur ist verantwortlich für die Gesamtstruktur der Firma oder Organisation. Er wird deshalb auch als **Organisations-** oder als **Enterprise-Admin** bezeichnet und verfügt über alle Berechtigungen.

- Melden Sie sich am Server *B-DC01* als Domänenadministrator in der Domäne *firma.intern* an.

Das lokale Administratorkonto existiert auf einem Domänencontroller nicht mehr. Künftig wird jede Anmeldung durch die Domäne *firma.intern* autorisiert.

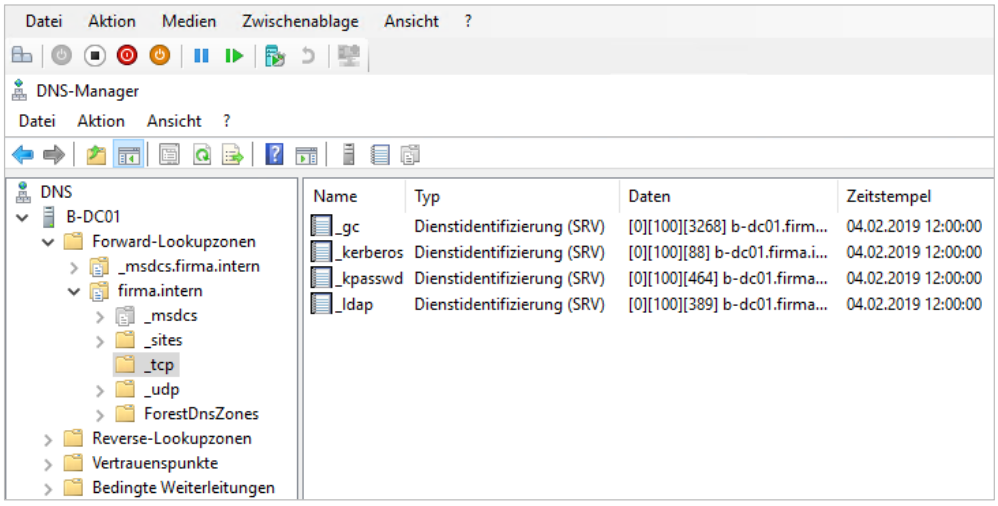
## Registrierung neuer DNS-Einträge überprüfen

Domänencontroller und ihre Dienste werden im DNS mit Service-Ressourceneinträgen (Service Resource Records, SRV) identifiziert. Diese SRV-Einträge werden automatisch angelegt. Dies sollten Sie überprüfen, bevor Sie mit der Einrichtung der Testumgebung fortfahren:

- Geben Sie im Startbildschirm `DNS` ein und klicken Sie auf *DNS*.
- Erweitern Sie im DNS-Manager in der linken Spalte *Forward-Lookupzonen* und dann *firma.intern*.

Hier sind einige neue Ordner hinzugekommen, wenn DNS richtig installiert wurde. Falls dies nicht der Fall ist, sollten Sie in Erwägung ziehen, DNS zu entfernen und erneut zu installieren. Ohne korrekt funktionierendes DNS kann Ihre Testumgebung nicht richtig arbeiten.

Sie können sich die SRV-Einträge ansehen, beispielsweise im Ordner *_tcp*. Falls vorher schon Reverse-Lookupzonen und Stubzonen existierten, sind sie vom DNS-Serverdienst bei der Einrichtung übernommen worden, da die Zonendatendateien bereits an entsprechender Stelle im Dateisystem vorhanden waren.



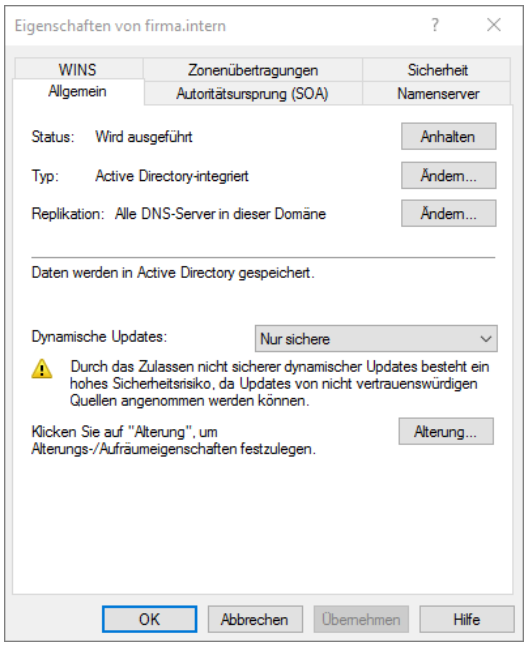

*SRV-Einträge zur Dienstidentifizierung ansehen*

## DNS-Zone ins Active Directory integrieren

Wenn die Zone beim Hochstufen des Servers vom System erstellt wurde, wurde sie automatisch ins Active Directory integriert. Sie können dies wie folgt überprüfen:

- Klicken Sie mit der rechten Maustaste im DNS-Manager auf die Zone *firma.intern*. Wählen Sie im Kontextmenü *Eigenschaften*.

Auf der Registerkarte *Allgemein* wird angezeigt, ob die Zone ins Active Directory integriert ist. Bei Bedarf können Sie dies auch nachträglich ändern.




*Zone in das Active Directory integrieren*

### Erstellung der Registrierungseinträge erzwingen

Die SRV-Einträge werden vom System bei jedem Start des Anmeldedienstes automatisch angelegt. Sollte dies einmal nicht der Fall sein, können Sie die Registrierung durch einen Neustart des Dienstes manuell erzwingen. Zusätzlich können Sie noch in der Befehlszeile mit *ipconfig /registerdns* die Einträge hinzufügen.

- Öffnen Sie die Eingabeaufforderung.
- Beenden Sie den Anmeldedienst mit dem Befehl
  `net stop netlogon` ↵.
- Starten Sie den Dienst erneut. Geben Sie dazu folgenden Befehl ein:
  `net start netlogon` ↵.


Schulversion
© HERDT-Verlag

## 7.3 Domänencontroller zur Domäne hinzufügen

### *B-DC02* zum zusätzlichen DC machen

Der Server *B-DC02* soll zum zusätzlichen Domänencontroller in der Domäne *firma.intern* heraufgestuft werden. Dafür ist eine funktionierende Netzwerkverbindung erforderlich. Es vereinfacht die Sache, wenn Sie in den Netzwerkeigenschaften von *B-DC02* als DNS-Server *B-DC01* eintragen. Die Serverrolle AD DS haben Sie bereits hinzugefügt.

- Melden Sie sich am virtuellen Server *B-DC02* als lokaler Administrator an.
- Klicken Sie im Server-Manager auf das Fähnchen und anschließend auf *Server zu einem Domänencontroller heraufstufen*.

### Domänencontroller zu einer vorhandenen Gesamtstruktur hinzufügen

Das Hinzufügen eines zusätzlichen Domänencontrollers verläuft ähnlich wie das Erstellen einer neuen Gesamtstruktur.

- Wählen Sie die Option Domänencontroller zu einer vorhandenen Gesamtstruktur hinzufügen.
- Wählen Sie als Namen der Domäne `firma.intern` und geben Sie die Anmeldeinformationen eines Domänenadministrators ein.
  Verwenden Sie dabei die Form `firma.intern\Administrator`.
- Klicken Sie auf *Weiter*.
- Aktivieren Sie die Optionen *DNS-Server* und *Globaler Katalog*.

  Das Deaktivieren des globalen Katalogs ist nur in Sonderfällen sinnvoll, z. B. bei kleinen Filialen mit schlechter WAN-Anbindung in großen Domänen. Im Normalfall sollte jeder DC diese beiden Funktionen ausüben.

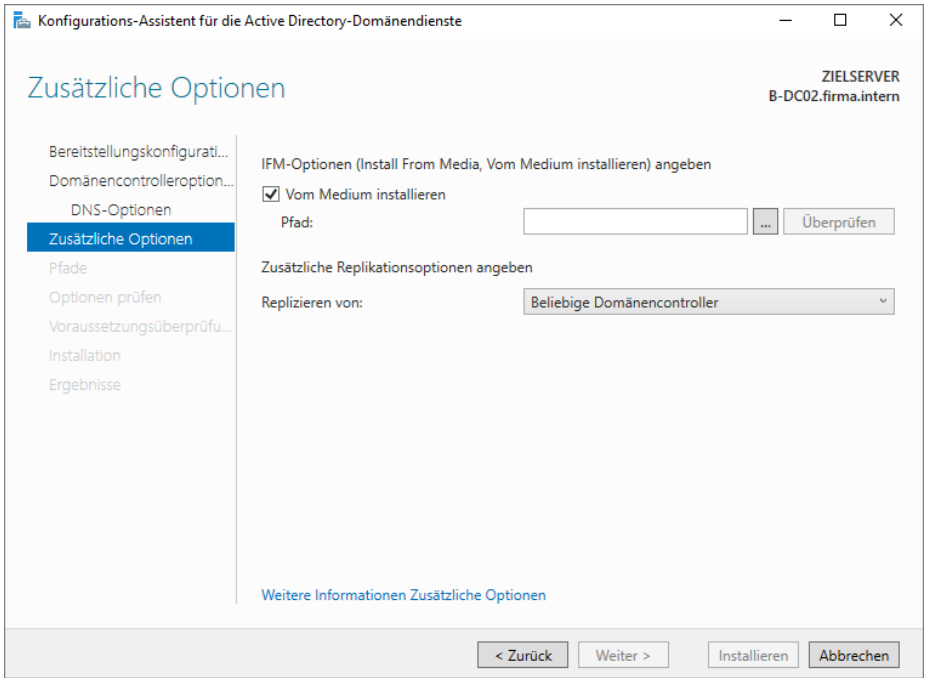
  Für kleine Außenstellen, an denen der Server nicht ausreichend gegen Zugriff gesichert werden kann und wo das Personal keine Änderungen am AD vornehmen soll, aktivieren Sie die Option *Schreibgeschützter Domänencontroller (RODC)*.
- Legen Sie den Standort fest. Falls kein passender Standort eingerichtet wurde, verwenden Sie *Default-First-Site-Name*. Klicken Sie auf *Weiter*.

Auf der Seite *DNS-Optionen* können Sie die Option *DNS-Delegierung aktualisieren* einschalten und gültige Anmeldeinformationen für diesen Vorgang eingeben. Dabei wird ein zusätzlicher Nameserver-Eintrag in der DNS-Delegierung der übergeordneten Domäne erstellt.

- Klicken Sie auf *Weiter*.

Falls Sie einen zusätzlichen DC in einem Struktur-Stamm erstellen, erscheint ein Hinweis über eine nicht erfolgreiche DNS-Delegierung. Bestätigen Sie mit *Ja*, dass Sie den Vorgang fortsetzen wollen.

Auf der Seite *Zusätzliche Optionen* haben Sie die Möglichkeit, das Active Directory nicht über das Netzwerk zu replizieren, sondern von einem Datenträger. Dieses Verfahren heißt **Install From Media** (IFM).




*DNS-Delegierung einstellen und Anmeldeinformationen eingeben*

- Falls Sie IFM verwenden möchten, aktivieren Sie die Option *Vom Medium installieren* und geben Sie den Pfad zur Datei `ntds.dit` ein, der auf einem lokalen Laufwerk liegen muss. Klicken Sie auf *Überprüfen*.
- Wählen Sie aus, von welchem DC das Active Directory repliziert werden soll, oder überlassen Sie dies dem Assistenten.
- Klicken Sie auf *Weiter*.
- Legen Sie die Speicherorte für die AD-Daten fest.
- Geben Sie zweimal ein komplexes Kennwort für den Verzeichnisdienst-Wiederherstellungsmodus DSRM (Directory Services Restore Mode) ein. Klicken Sie auf *Weiter*.
- Überprüfen Sie die Auswahl und klicken Sie auf *Weiter*.

  Es wird eine Überprüfung der Einstellungen durchgeführt. Falls Probleme auftreten, müssen diese vor der Installation beseitigt werden.
- Klicken Sie auf *Installieren*.

  Der Installationsvorgang wird nun ausgeführt und der Server automatisch neu gestartet.

## Zusammenspiel der Domänencontroller unter Hyper-V

Sobald Sie in der Hyper-V-Testumgebung den zweiten DC in die Domäne gehoben haben, sollten Sie von nun an die beiden DCs als untrennbare Zwillinge betrachten.

- Schalten Sie nie für längere Zeit einen der beiden DCs aus, während der andere weiterläuft.
- Bevor ein virtueller Domänen-Computer eingeschaltet wird, muss stets ein DC gestartet werden.
- Fertigen Sie stets Snapshot-Sets von allen VMs zum gleichen Zeitpunkt an.
- Falls Sie bei einem DC zu einem früheren Zeitpunkt zurückkehren wollen, müssen Sie dies bei allen anderen VMs ebenfalls tun.

Falls Sie sich nicht an diese Regeln halten, werden Sie sich erhebliche Probleme im Active Directory und DNS einhandeln, die sich schwer auffinden und noch schwerer beheben lassen. Im schlimmsten Fall haben Sie in Ihrem Testnetzwerk zwei Domänen gleichen Namens, die nicht miteinander kommunizieren.


Schulversion
© HERDT-Verlag

## 7.4 Active Directory erkunden

### Active Directory-Verwaltungsprogramme verwenden

Mit dem Heraufstufen zum Domänencontroller werden auf einem Server auch Programme zur Verwaltung des Active Directorys installiert. Die folgenden Programme stellen Standardschnittstellen für die Verwaltung von Active Directory dar:

- *Active Directory-Modul für Windows PowerShell*
- *Active Directory-Domänen und -Vertrauensstellungen*
- *Active Directory-Benutzer und -Computer*
- *Active Directory-Standorte und -Dienste*
- *Active Directory-Verwaltungscenter*

Sie können die Werkzeuge rund ums Active Directory über das Tools-Menü im Server-Manager aufrufen oder durch Eingabe von `Active` im Startmenü. Wie üblich lassen sich zahlreiche Aufgaben an mehreren Stellen erledigen, einige Handlungen können jedoch nur in einer bestimmten Konsole ausgeführt werden. Die Konsole *Active Directory-Benutzer und -Computer* können Sie über das Suchfeld des Startmenüs oder aus der Befehlszeile auch mit „dsa.msc“ aufrufen. Das Active Directory-Verwaltungscenter starten Sie mit „dsac“.

Um Active Directory zu testen, starten Sie eine Eingabeaufforderung, zum Beispiel durch Eingabe von *cmd* im Startmenü. Das Startmenü starten Sie mit der ⊞-Taste oder einem Klick mit der Maus unten links im Bildschirm. Geben Sie dann *dcdiag* ein.

Mit `nltest /dclist:<NetBIOS-Domänennamen>` lassen Sie sich den Namen des Domänencontrollers anzeigen, mit `nslookup <Vollständiger Name des DC>` muss der Name und die IP-Adresse verfügbar sein.

### Active Directory-Modul für Windows PowerShell

Die Module für die Windows PowerShell erlauben eine Reihe von umfangreichen Eingriffen in die Struktur und Funktionalität des Active Directorys und würden den Rahmen des Buches sprengen, da sie eine eigene Programmierumgebung darstellen. In vertiefenden Büchern dieser Reihe finden Sie jedoch Beispiele für Aufgaben, die mit der PowerShell durchgeführt werden können.

Mit Windows Server 2019 haben Sie die Möglichkeit, von einer lokalen PowerShell-Sitzung von Arbeitsstationen aus remote auf Domänencontroller zuzugreifen, um Active Directory zu verwalten. Das ist oftmals wesentlich bequemer und effizienter als mit Remotedesktopsitzungen.

Um Server im Netzwerk über Arbeitsstationen mit Windows 10 zu verwalten, sind die Remoteserver-Verwaltungstools notwendig. Damit sich Active Directory remote über die PowerShell verwalten lässt, müssen Sie *Rollenverwaltungstools/AD DS-/AD LDS-Tools/Active Directory-Modul für Windows PowerShell* installiert haben. Die Installation überprüfen Sie, wenn Sie „optionalfeatures“ im Startmenü auf dem Windows 10-Compuer eingeben.

Die Installation erfolgt im Server-Manager über die Auswahl von *Remoteserver-Verwaltungstools/ Rollenverwaltungstools/AD DS- und AD LDS-Tools/Active Directory-Modul für Windows PowerShell*.

Damit sich ein Server in der PowerShell remote verwalten lässt, muss die Funktion auf dem Zielserver zunächst aktiviert werden. Dazu geben Sie in einer PowerShell-Sitzung auf dem Ziel-Server den Befehl `Enable-PSRemoting -Force` ein. Der Befehl richtet die entsprechenden Ausnahmen in der Firewall ein und aktiviert die notwendigen Funktionen. Rückgängig machen lässt sich der Vorgang mit `Disable-PSRemoting -Force`.

## Active Directory-Domänen und -Vertrauensstellungen

Mit dieser Konsole können Sie die Gesamtstruktur und die einzelnen Strukturen, Domänen und Unterdomänen anzeigen und die Vertrauensstellungen verwalten. Außerdem können Sie hier die Funktionsebenen für Domäne und Gesamtstruktur heraufstufen und den Betriebsmaster ändern.

## Active Directory-Benutzer und -Computer

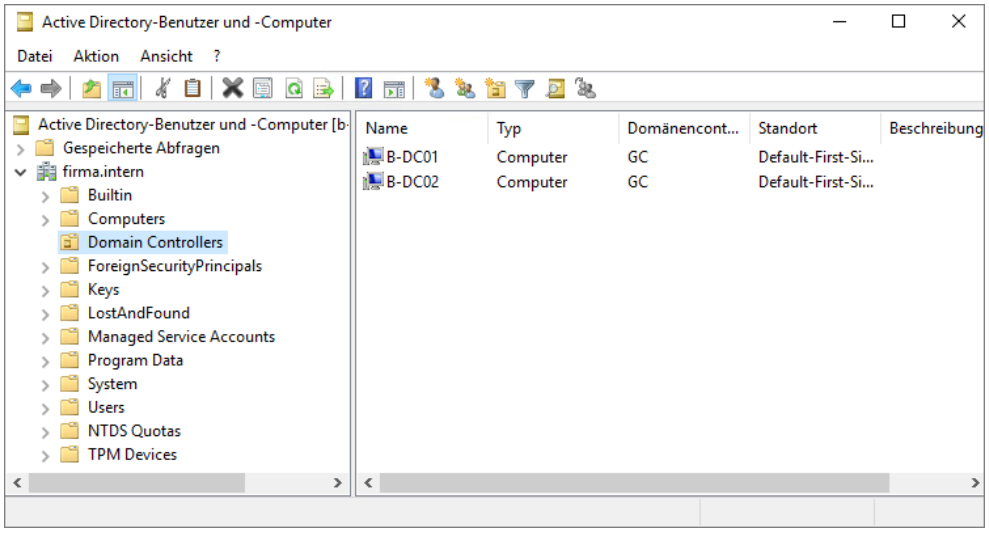
In der seit vielen Jahren nahezu unveränderten Konsole können Sie einen Großteil der Einstellungen rund um das Active Directory vornehmen. Hier legen Sie neue Organisationseinheiten, Benutzer, Gruppen und andere Objekte wie Computer und Drucker an. Sie können auch Benutzer kopieren, was bei der Einrichtung und Verwaltung der Benutzer sehr hilfreich ist.

Sie sollten im Menü *Ansicht* den Eintrag *Erweiterte Ansicht* aktivieren, um alle AD-Bestandteile sehen zu können. Ebenfalls im Menü *Ansicht* können Sie unter *Anpassen* z. B. den Aktionsbereich aktivieren wie unten abgebildet.

## Computer anzeigen

Sie können sich in *Active Directory-Benutzer und -Computer* unter anderem die vorhandenen Domänencontroller anzeigen lassen:

- Geben Sie auf einem der virtuellen Domänencontroller im Startmenü `active` ein und klicken Sie auf *Active Directory-Benutzer und -Computer.* Alternativ starten Sie das Tool durch Eingabe von „dsa.msc“.
- Erweitern Sie die Domäne *firma.intern* und öffnen Sie beispielsweise die Organisationseinheit *Domain Controllers*.




*Domänencontroller in der Domäne „firma.intern“ anzeigen*

Wenn Sie der Anleitung zur Testumgebung gefolgt sind, sehen Sie die beiden installierten Server im Bereich *Domain Controllers*. Auf beiden ist der globale Katalog (GC) installiert.

## Active Directory-Standorte und -Dienste

In dieser Konsole können Sie Standorte, Standortverknüpfungen und Subnetze für Ihre Domäne einrichten. In diesem Buch gibt es nur den Default-Standort und ein Subnetz, das Thema wird jedoch im HERDT-Buch *Windows Server 2019 – Erweiterte Netzwerkadministration* ausführlich behandelt.


Schulversion
© HERDT-Verlag

## Verwaltungsprogramme auf Client-Computern installieren

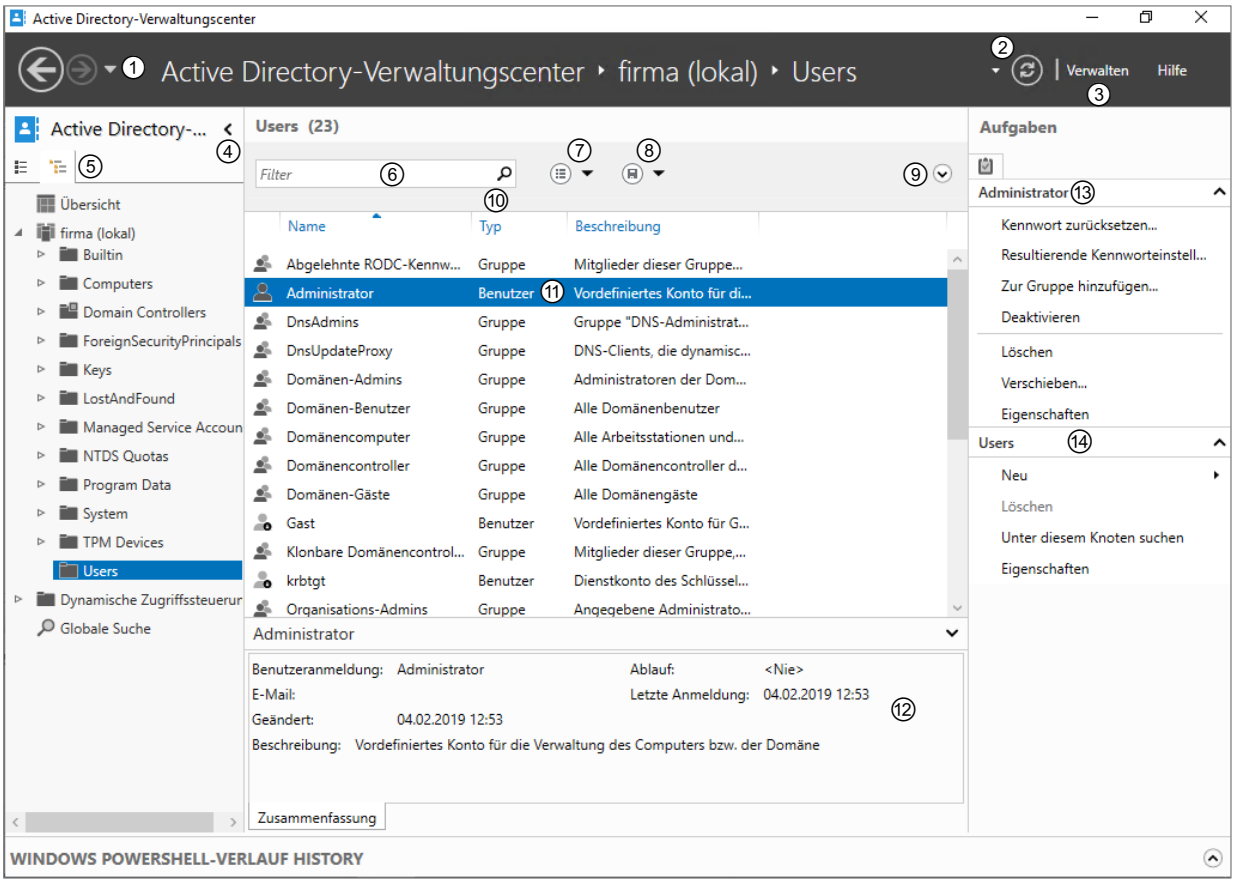
Auf Client-Computern und Mitgliedsservern sind die Verwaltungsprogramme standardmäßig nicht vorhanden. Wollen Sie Domänen von einer Arbeitsstation aus verwalten, müssen Sie diese Programme installieren.

Zur Fernadministration von Windows Server 2019 sind nur Systeme mit Server 2019 und Windows 10 geeignet. Alternativ installieren Sie im Netzwerk das Windows Admin Center. Allerdings enthält das Windows Admin Center keine Werkzeuge für die Verwaltung von Active Directory. Bei Computern mit Server 2019 können Sie sich im Server-Manager und den Konsolen auf andere Server einloggen und Änderungen vornehmen. Unter Windows 10 benötigen Sie die Remoteserver-Verwaltungstools (Remote Server Administration Tools, RSAT), die nicht im Lieferumfang enthalten sind. Die Tools sind kostenlos als x86- und x64-Version bei Microsoft zum Download erhältlich. Suchen Sie im Internet nach *RSAT Windows 10.*

Im Wesentlichen erhalten Sie mit den Remoteserver-Verwaltungstools den Server-Manager und dieselben Konsolen wie bei Server 2019. Mit RSAT können Sie auch ältere Server-Versionen wie Windows Server 2008 R2 und Windows Server 2012/2012 R2/2016 administrieren, umgekehrt können Sie jedoch keine älteren Betriebssystemversionen für die Fernadministration einsetzen. Achten Sie darauf, jeweils die aktuellste RSAT-Version zu installieren.

## Active Directory-Verwaltungscenter

Das Active Directory-Verwaltungscenter ist die zentrale Verwaltungsschnittstelle unter Windows Server 2019, mit der sich typische Routineaufgaben ausführen lassen. Das Verwaltungscenter verfügt über eine Vielzahl von vordefinierten Filtern, die in komplexen Umgebungen die Suche nach Objekten anhand bestimmter Kriterien vereinfachen.



| Schematische Darstellung des Active Directory-Verwaltungscenters | | |
|---|---|---|
| Die Titelzeile zeigt an, wo Sie sich gerade befinden. Bei ① werden die zuletzt besuchten Orte angezeigt. ② aktualisiert die Anzeige und ③ bietet weitere Optionen, z. B. *Hinzufügen eines Navigationsknotens*. | | |
| Die Navigationsspalte kann mit ④ ausgeblendet werden. ⑤ schaltet zwischen einfacher Listendarstellung und Baumstruktur um. | Schränken Sie die Anzeige über Filter ein ⑥. Bei ⑦ werden gespeicherte Filter angezeigt, die Sie unter ⑧ abspeichern können. Mit ⑨ erweitern Sie die Ansicht, um dann unter ⑩ weitere Filterkriterien angeben zu können. | Hier werden alle für die ausgewählten Objekte verfügbaren Aktionen angezeigt ⑬. |
| | Die Objekte, die anhand der Filterung im gewählten Container gefunden wurden, erscheinen in einer Liste und lassen sich auswählen ⑪. Über einen Doppelklick öffnen Sie die Eigenschaftsseite, das Kontextmenü enthält weitere Optionen. | Hier werden die für den Container verfügbaren Aktionen angezeigt ⑭. |
| | Hier werden Informationen zu den ausgewählten Objekten angezeigt ⑫. | |

Leider ist es auch in der neuesten Version des AD-Verwaltungscenters nicht möglich, Benutzer zu kopieren. Diese Funktion ist weiterhin der Konsole AD-Benutzer und -Computer vorbehalten.

## Funktionsebenen heraufstufen

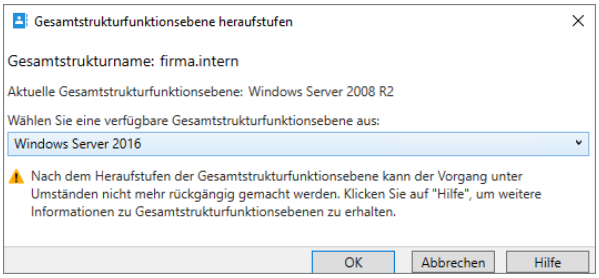
Im AD-Verwaltungscenter haben Sie die Möglichkeit, die Funktionsebenen für Gesamtstruktur und Domäne heraufzustufen. Beide Funktionsebenen Ihrer Testumgebung sind zurzeit noch auf Server 2008 R2 eingestellt, dies soll nun auf Windows Server 2016 geändert werden. Für Windows Server 2019 gibt es keine eigenen Funktionsebenen für Domänen und Gesamtstruktur. Fertigen Sie zuerst einen Snapshot/Prüfpunkt von allen virtuellen Servern an.

In der Praxis sollten Sie die Funktionsebenen nur dann heraufstufen, wenn dafür ein wichtiger Grund vorliegt. Aus diesem Grund wird in der Übung auch nicht auf den Modus Windows Server 2016 hochgestuft, da dieser keine zusätzliche Funktionalität bereitstellt, aber den Einsatz von Windows Server 2012-Domänencontrollern verhindert.

Bedenken Sie vor einer Heraufstufung:

- Heraufstufungen der Funktionsebenen können nicht wieder rückgängig gemacht werden.
- Die Gesamtstrukturfunktionsebene Windows Server 2012 wird für Dynamic Access Control (DAC) benötigt. Die Technik ist auch in der Funktionsebene Windows Server 2016 dabei.
- Die Domänenfunktionsebene kann nicht niedriger sein als die Gesamtstrukturfunktionsebene und wird automatisch angehoben.
- Wenn die Domänenfunktionsebene auf Windows Server 2016 gesetzt wurde, ist es nicht mehr möglich, ältere Server mit Windows Server 2008 R2 als Domänencontroller einzusetzen.
- Zum Heraufstufen der Gesamtstrukturfunktionsebene müssen Sie Organisations-Admin sein, zum Heraufstufen der Domänenfunktionsebene genügt ein Domänenadministrator.
- Die Replikation zwischen den beiden Domänencontrollern dauert einige Minuten.

- Klicken Sie im AD-Verwaltungscenter auf *firma (lokal)*.
- Klicken Sie im Kontextmenü von *firma (lokal)* oder im Aufgabenbereich auf *Gesamtstrukturfunktionsebene heraufstufen*.
- Klicken Sie auf das Listenfeld und wählen Sie *Windows Server 2016* aus. Klicken Sie auf *OK*.





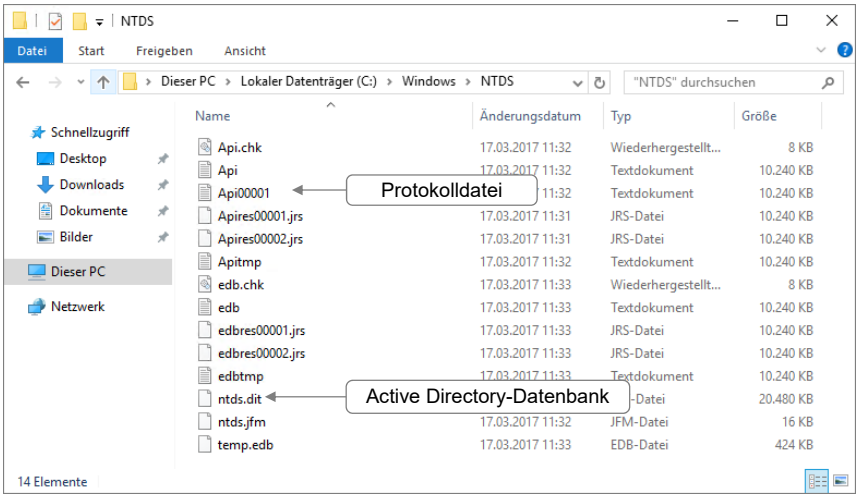
© HERDT-Verlag

Da die Domänenfunktionsebene automatisch mit angehoben wird, müssen Sie diese nicht mehr heraufstufen. Sie können die Domänenfunktionsebene anpassen, indem Sie bei beiden VMs zum vorhin angelegten Snapshot zurückkehren und diesmal *Domänenfunktionsebene heraufstufen* wählen.

## Active Directory-Datenbank ansehen

- Erweitern Sie im Windows-Explorer `%WINDIR%\NTDS`.

  Die Systemvariable `%WINDIR%` verweist auf den Windows-Ordner auf der Systempartition.




*Den Ordner „NTDS“ einsehen*

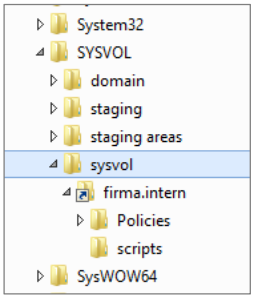
## Freigegebenen Systemdatenträger ansehen

- Erweitern Sie im Windows-Explorer `%WINDIR%\SYSVOL\Sysvol`.

Jeder Domänencontroller ist Anmeldeserver. Die Dateien, die in der gesamten Domäne verfügbar sein müssen, werden im freigegebenen Verzeichnis *SYSVOL* gespeichert und vom File Replication Service auf die übrigen Domänencontroller repliziert.

Der Unterordner *scripts* ist unter dem Namen *Netlogon* freigegeben. Er kann die folgenden Dateien aufnehmen:

- ✔ Vorlagen für Gruppenrichtlinien
- ✔ Anmeldeskripte




*SYSVOL einsehen*

Die Ressourcen *SYSVOL* und *Netlogon* werden vom Anmeldedienst *netlogon* verwendet, um Benutzeranmeldungen durchzuführen.

# 8 DNS

**In diesem Kapitel erfahren Sie**

- das Konzept des Domänennamespace
- die Funktionsweise der Namensauflösung
- die Funktionsweise des dynamischen DNS
- das Konzept von Zonen und Zonenübertragung
- den Aufbau der DNS-Datenbank

**Voraussetzungen**

- Windows Server 2019 installieren
- IP-Adressierung

## 8.1 Domänennamespace

### IP-Adressen und Namen

TCP/IP greift auf andere Computer auf der Netzwerkebene über die IP-Adresse zu. Diese ist bei IPv4 eine 32 Bit lange Adresse, die in vier Blöcken dezimal ausgedrückt wird (z. B. 192.168.15.144), bei IPv6 eine 128-Bit-Adresse in hexadezimaler Schreibweise (z. B. fe80:0:0:0:5043:5d10:be95:c32a).

TCP/IP wurde für den Vorläufer des Internets entwickelt und ermöglicht Benutzern heutzutage, mit einfachen Mitteln auf Ressourcen im weltweiten Web zuzugreifen. Da sich die meisten Menschen solche langen Zahlenkombinationen wie IP-Adressen nur schlecht merken können, sind Konzepte entwickelt worden, um diesen IP-Adressen einprägsame und eindeutige Namen (Fully Qualified Domain Names, FQDN) zuzuordnen. Windows Server 2019 verwendet dazu DNS, aus Kompatibilitätsgründen wird auch noch der ältere Standard WINS unterstützt.

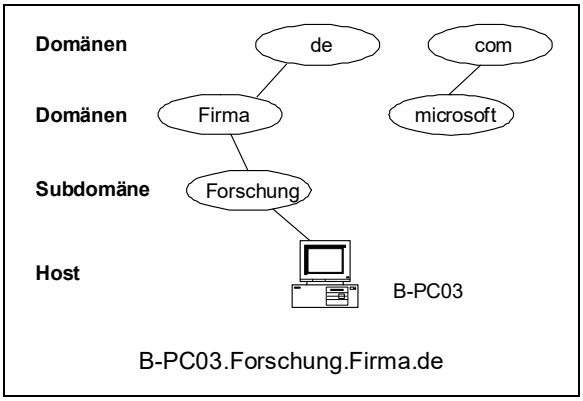
### Domain Name System

DNS ist das im Internet verwendete Konzept zur Namensauswertung. Es basiert auf einer verteilten Datenbank. In einer hierarchischen Anordnung pflegen DNS-Server Datenbanken, in denen Hostnamen innerhalb von Domänen IP-Adressen zugeordnet sind.

### DNS-Domänenname

**DNS** ist ein hierarchischer Namensraum für Computer, Dienste und DNS-Subdomänen eines Netzwerks. Die DNS-Domäne selbst besitzt auch einen Namen. Aus der Tatsache, dass eine Domäne eine oder mehrere Domänen der nächsten Ebene registriert, ergibt sich die Hierarchie. Die Namensräume sind hierarchisch angeordnet.

DNS-Domänennamen werden von zentralen Institutionen an Länder, Organisationen und Unternehmen vergeben. Der DNS-Domänenname besteht aus zwei oder drei Teilen (Suffixe). Davon ist der letzte Teil eine Abkürzung, die beispielsweise die Art des Unternehmens oder ein Land bezeichnen kann.




*Hierarchie des Domänennamespace*

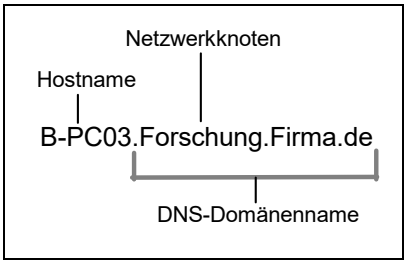

Schulversion
© HERDT-Verlag

## Hostnamen

Der komplette DNS-Name (Fully Qualified Domain Name; FQDN) für einen Host besteht aus dem **Hostnamen** und dem **DNS-Domänennamen**.

Beispiel:

Der Computer *B-PC03* ist ein Host in der DNS-Domäne *Forschung.Firma.de.* Der FQDN dieses Computers ist *B-PC03.Forschung.Firma.de.* Anhand des FQDN wird die Position des Hosts in der Domänenhierarchie bestimmt.




*Der vollständige DNS-Name FQDN*

Soll ein einzelner Computer mehrere IP-Adressen oder Hostnamen erhalten, beispielsweise ein Webserver im Internet, können Sie das Konzept der **virtuellen Hosts** verwenden. Dabei werden mehrere Hostnamen vergeben, die im DNS entweder auf die gleiche oder auf verschiedene IP-Adressen des Computers verweisen können.

## Primäres DNS-Suffix

Der Bestandteil des FQDN, der vom DNS-Domänennamen gebildet wird, heißt bei Microsoft-Betriebssystemen primäres DNS-Suffix. Jeder Microsoft-Host muss ein primäres DNS-Suffix besitzen. Das heißt, der DNS-Domänenname muss für jeden Host angegeben werden.

Dem primären DNS-Suffix steht ein verbindungsspezifisches DNS-Suffix gegenüber. Ein solches gilt unter Microsoft-Betriebssystemen ab Windows 2000 nur für eine im Computer installierte Netzwerkkarte. Sinnvoll sind verbindungsspezifische DNS-Suffixe nur, wenn mehr als eine Netzwerkkarte in einem Computer (Server) vorhanden sind.

## Hostname und Computername

Ein Computer kann einen Hostnamen und einen Computernamen (NetBIOS-Name) besitzen. Die beiden Namen stimmen oft überein. Unterstriche sind z. B. im NetBIOS-Namen erlaubt, im Hostnamen jedoch nicht. Bei der Benennung eines Computers mit einem NetBIOS-Namen ersetzt Windows unzulässige Zeichen automatisch. So wird *server_1* beispielsweise ersetzt durch *server-1*. Auf diese Weise entsteht ein Computername, der auch als Hostname verwendet werden kann.

In der Praxis empfiehlt es sich, Computernamen zu verwenden, die keine für DNS unzulässigen Zeichen enthalten, um eine homogene Namensstruktur zu erzielen. Auch sollten Sie keine Sonderzeichen oder Umlaute verwenden, die bei fremdsprachlicher Tastaturbelegung nicht eingegeben werden können.

## Richtlinien für die Erstellung des Domänennamespace

- Eine DNS-Struktur darf bis zu fünf Ebenen enthalten.
- Eindeutige Namen für Subdomänen einer Domäne
- Die Verwendung von kurzen, aussagekräftigen Namen wird empfohlen.
- Die maximale Länge der einzelnen Domänennamenskomponente beträgt 63 Zeichen einschließlich des Punktes.
- Gesamtlänge eines FQDN maximal 255 Zeichen
- Die DNS-Standardzeichen sind: a – z, 0 – 9 und der Bindestrich

  Großbuchstaben können eingegeben werden, werden aber automatisch durch Kleinbuchstaben ersetzt.

  Unicodezeichen wie z. B. Umlaute können Sie zwar verwenden, falls **alle** DNS-Server und -Clients Ihres Netzwerks Unicode unterstützen, Sie sollten dennoch darauf verzichten.

Der Domänenname sollte nicht dem Namen der Internetpräsenz entsprechen. Verwenden Sie z. B. *firma.de* für die Internetpräsenz und *firma.intern* für die Domäne. Dadurch wird die Verwaltung der DNS-Datenbanken vereinfacht, da interne Namen nicht im Internet bekannt werden dürfen, externe Informationen aber auch durch interne Benutzer abrufbar sein sollten.

## 8.2 Namensauflösung

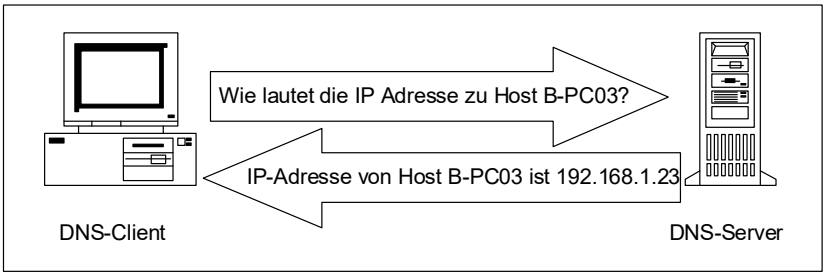
### Wie DNS funktioniert

Damit ein Host mit einem anderen Kontakt aufnehmen kann, benötigt er dessen IP-Adresse. Vor dem Aufbau einer Verbindung zu einem Zielhost muss deshalb praktisch immer eine **Namensauflösung** durchgeführt werden. Diese Namensauflösung ist normalerweise der Vorgang, bei dem ein DNS-Namenserver zu einem angegebenen FQDN die zugehörige IP-Adresse ermittelt. Aber auch der umgekehrte Weg ist möglich: Der DNS-Namenserver ermittelt zu einer IP-Adresse den zugehörigen FQDN.

Je nach der Richtung der Namensauflösung wird zwischen **Forward-Lookup** und **Reverse-Lookup** unterschieden.

### Forward-Lookup

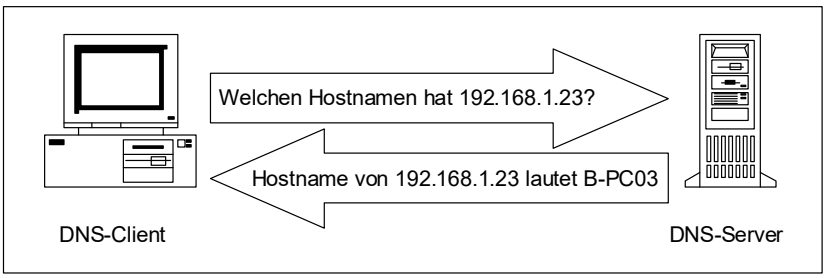
In einer Forward-Lookup-Anfrage sendet ein DNS-Client-Computer den FQDN des Empfängers an den DNS-Server und erhält daraufhin die zugehörige IP-Adresse der Empfängerstation. Windows Server 2019 unterstützt hierbei sowohl IPv4-Adressen (Host-Einträge vom Typ A) als auch IPv6-Adressen (Host-Einträge vom Typ AAAA). Forward-Lookup-Anfragen müssen vom DNS-Server beantwortet werden können, damit eine Verbindung zu einem namentlich angegebenen Host hergestellt werden kann.




*Forward-Lookup-Abfrage: Zu einem Hostnamen wird die zugehörige IP-Adresse ermittelt*

### Reverse-Lookup

In einer Reverse-Lookup-Abfrage sendet ein DNS-Client die IP-Adresse des Empfängers an den DNS-Server und erhält daraufhin den zugehörigen FQDN der Empfängerstation. Die Einrichtung eines DNS-Servers zur Beantwortung von Reverse-Lookup-Abfragen ist nicht zwingend erforderlich.




*Reverse-Lookup-Abfrage: Zu einer IP-Adresse wird der zugehörige Hostname ermittelt*

Unter Windows Server 2019 werden sowohl IPv4- als auch IPv6-Reverse-Lookupzonen unterstützt. Die Arbeitsweise der beiden Reverse-Zonentypen ist dabei identisch.


Schulversion
© HERDT-Verlag

### Client-/Servermodell der Namensauflösung

Die Namensauflösung folgt dem Client-/Servermodell, wie in den gezeigten Beispielen ersichtlich wird: DNS-Namenserver übernehmen die Rolle des Servers. Zum DNS-Client wird ein Computer, indem die IP-Adresse eines zuständigen DNS-Namenservers bei der Konfiguration des TCP/IP-Protokollstacks auf dem betreffenden Computer eingetragen wird.

Danach kann der DNS-Client Abfragen an den DNS-Namenserver schicken. Ein Namenserver kann nur solche Hostnamen und IP-Adressen auflösen, für die er autorisiert ist, d. h. für die er Einträge in seiner DNS-Datenbank besitzt. Erhält ein Namenserver eine Client-Abfrage, die er selbst nicht auflösen kann, übergibt er die Anfrage an einen übergeordneten DNS-Namenserver.

Alternativ dazu lässt sich eine Weiterleitung an einen anderen DNS-Server konfigurieren. In diesem Fall arbeitet der DNS-Server seinerseits wie ein Client. Die Weiterleitung wird in aller Regel eingesetzt, um so mehrfache Anfragen zu sparen, indem der DNS-Server des Internetanbieters (Internet Service Provider, ISP) die eigentliche Auflösung im Internet übernimmt.

### Namenservercaching

Namenserver speichern Ergebnisse von Abfragen im Cache. Die Lebensdauer zwischengespeicherter Abfrageergebnisse ist begrenzt (TTL, Time To Live). Die Zeitspanne des Zwischenspeicherns beträgt bei Microsoft-Servern standardmäßig 24 Stunden. Clients dagegen erhalten standardmäßig Antworten mit einer Lebensdauer von 60 Minuten.

## 8.3 Global Names

### Problemstellung

DNS-Clients unter Windows-Betriebssystemen senden Anfragen, in denen nach einer Ressource automatisch das eigene primäre DNS-Suffix angehängt wird. Wenn also ein Benutzer von *firma.intern* im Browser *B-FS01* eingibt, wird automatisch eine DNS-Anfrage nach *B-FS01.firma.intern* gesendet.

Wenn nun in einem Firmennetzwerk mehrere Domänen verfügbar sind, kann dies dazu führen, dass eine Hostabfrage durch unpassende DNS-Suffixe ergänzt wird. Dies ist kein Problem, solange zusätzlich NetBIOS im Einsatz ist, da dann der WINS-Server vom DNS abgefragt werden kann, um über den Computernamen eine eindeutige Auflösung durchzuführen.

Ist aber NetBIOS deaktiviert oder der DNS-Server nicht in der Lage, einen WINS-Server abzufragen, so kann der Name nicht aufgelöst werden.

### Die GlobalNames-Zone

Seit Windows Server 2008 steht mit der Zone *GlobalNames* ein weiterer Datentyp im DNS zur Verfügung. Darin können Hostnamen gespeichert werden, die unabhängig von dem DNS-Suffix aufgelöst werden sollen. Es handelt sich um eine spezielle Forward-Lookupzone, die auf eine DNS-Suffix-Erweiterung verzichtet. Der Mechanismus muss gesondert aktiviert werden.

## 8.4 Dynamisches DNS

### Dynamische Aktualisierung

Die dynamische Aktualisierung ist eine erweiterte Funktion für DNS: Beim Start eines Netzwerkadapters oder bei Änderungen an der IP-Adresse oder dem Hostnamen teilt ein Computer dies standardmäßig seinem primären DNS-Server automatisch mit. Dadurch verringert sich der Verwaltungsaufwand für Einträge in den DNS-Datenbanken, die ohne Einsatz von dynamischer Aktualisierung jeweils manuell aktualisiert werden müssten.

Von besonderem Vorteil ist die dynamische Aktualisierung bei Computern (Notebooks etc.), die innerhalb des Netzwerks an unterschiedlichen Orten eingesetzt werden. Solche Computer sollten im Idealfall ihre IP-Konfiguration über DHCP zugeteilt bekommen. Dynamisches DNS und DHCP können so eingerichtet werden, dass die Zuordnung von Hostnamen zu IP-Adressen vom DHCP-Server an DNS mitgeteilt wird. Dadurch können auch Systeme dynamisch in die DNS-Datenbank integriert werden, die selbst kein dynamisches DNS unterstützen, wie etwa Rechner unter Windows NT4.0.

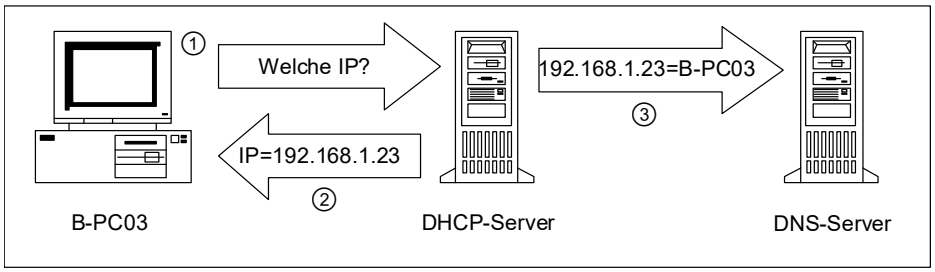
### Das Zusammenspiel von DynDNS und DHCP

Voraussetzung ist, dass DHCP für die automatische Registrierung in der DNS-Datenbank konfiguriert wurde.

① Die Workstation fordert vom DHCP-Server eine IP-Adresse an.

② Der DHCP-Server weist der Workstation eine IP-Adresse zu.

③ Der DHCP-Server übergibt den Hostnamen und die IP-Adresse zur Registrierung an DNS.




DNS-Clients können dem DNS-Server ihren Hostnamen sowie ihre IPv4- und IPv6-Adresse auch selbst mitteilen. Ob die Registrierung durch den DHCP-Server erfolgen soll, kann in den Eigenschaften eines Bereiches oder für das gesamte Protokoll (IPv4 oder IPv6) festgelegt werden.

Damit auf diese Weise nicht beliebige Computer die DNS-Datenbank aktualisieren können, sind im DNS unter Windows Server 2019 zusätzliche Sicherheitsmechanismen implementiert.

### Sichere dynamische Aktualisierung

Üblicherweise wird unter Windows der DNS-Dienst von einem Domänencontroller angeboten und das DNS ist in das Active Directory integriert. Der DNS-Server kann in diesem Fall überprüfen, ob der angegebene Rechnername auch den Konteninformationen in der Active Directory-Datenbank entspricht. Nur wenn der Client, der um Registrierung ersucht, auch über ein passendes Dienstticket für die Domäne verfügt, wird der Eintrag in der Datenbank aktualisiert.


Schulversion
© HERDT-Verlag

## 8.5 Zonen

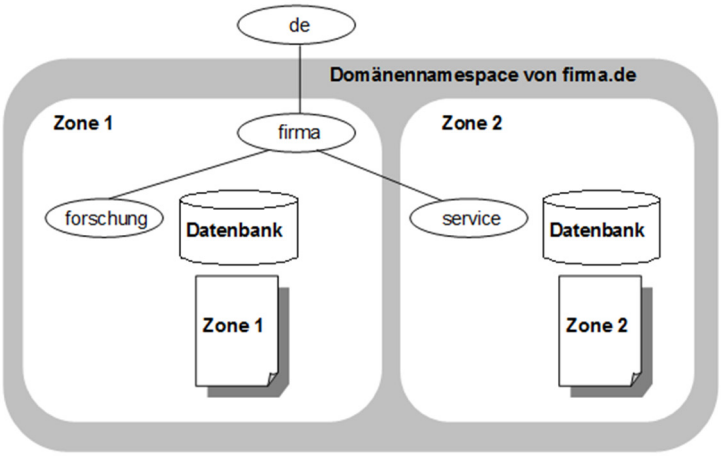
### Zonen und Zonendateien

Die Anzahl der IP-Adressen und Namen in großen Netzwerken wie dem Internet macht eine zentrale Verwaltung der DNS-Datenbank unmöglich. Deshalb wird der Domänennamespace in **Zonen** aufgeteilt. Der Vorgang der Namensauflösung kann dadurch beschleunigt werden, denn der DNS-Namenserver muss nicht eine umfangreiche Datenbank durchsuchen, sondern eine kleinere, wenige Einträge umfassende Datenbank. Die Verwaltung des Domänennamespace kann durch die Aufteilung in Zonen beispielsweise auch auf mehrere Administratoren verteilt werden.

Eine Zone kann umfassen:

- eine Domäne, gegebenenfalls mit Subdomänen,
- eine einzelne Subdomäne,
- einen Teil einer Domäne.

Jede Zone hält die DNS-Namen von IP-Adressen in einer **Zonendatei**. Diese ist in der Zonendatenbank gespeichert.




*Zonen eines Domänennamespace*

Das Unterteilen einer Domäne in mehrere Teildatenbanken ist mit erheblichem Mehraufwand verbunden, und eine saubere Auflösung von Anfragen durch Clients kann nicht sicher gewährleistet werden. Daher sollten Sie stattdessen auf eine Segmentierung in Subdomänen zurückgreifen, wann immer dies möglich ist.

### Domänenstamm einer Zone

Der Domänenstamm einer Zone ist die Domäne, die innerhalb der Zone in der Hierarchie an oberster Stelle steht. Im gezeigten Beispiel ist *firma.de* der Domänenstamm für die Zone 1, *service.firma.de* ist der Domänenstamm für die Zone 2.

Für die Domäne *firma.de* und die Subdomäne *forschung.firma.de* sind die Namenszuordnungen von IP-Adressen in der Zonendatei der Zone 1 gespeichert. Für die Subdomäne *service.firma.de* sind die Namenszuordnungen in der Zonendatei der Zone 2 gespeichert.

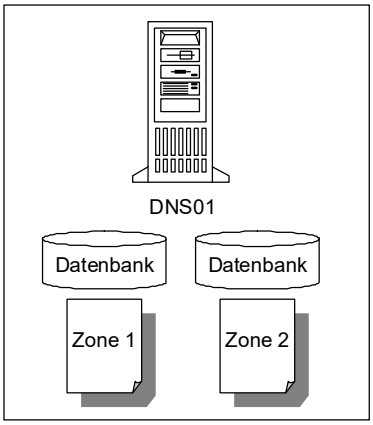
### DNS-Stamm

DNS-Stamm eines Netzwerks ist die DNS-Domäne, die innerhalb des Netzwerks in der Hierarchie an oberster Stelle steht. Im Internet ist der DNS-Stamm die Domäne "**.**". Der oder die DNS-Server, die den DNS-Stamm pflegen, sind **Stammnamenserver** des Netzwerks (Root Name Server).

In dem gezeigten Beispiel darf der DNS-Server für *firma.de* nicht als Stammnamenserver konfiguriert sein. Er würde sonst keine Anfragen mehr an die übergeordneten Domänen *de* und "**.**" im Internet weiterleiten. Nur wenn Unternehmen für die interne Vernetzung einen separaten, nicht mit dem Internet verbundenen Domänennamespace verwenden, darf es einen Stammnamenserver für diesen Namespace im Unternehmen geben.

## Namenserver

Der Server, der die Zonendatenbank hält, ist **DNS-Namenserver** für die betreffende Zone. Er ist für diese Zone **autorisiert**. Jede Zone muss einen DNS-Namenserver besitzen. Ein Server kann DNS-Namenserver für mehrere Zonen sein.



*Primärer Namenserver*

### Beispiel

Im Netzwerk der *Firma GmbH* könnte ein einzelner Server die DNS-Dienste ausführen, der Server *DNS01*. Er pflegt in diesem Fall zwei Zonendatenbanken, nämlich die für die Zone 1 und die für die Zone 2. Das bedeutet auch: Namenserver für die Zone 1 ist *DNS01*, und Namenserver für Zone 2 ist ebenfalls *DNS01*.

Die Nachteile dieser Positionierung sind:

- Fällt der Server *DNS01* aus, ist keine Namensauflösung im Netzwerk mehr möglich.
- Die Auslastung von *DNS01* kann sehr hoch sein, denn er muss alle Abfragen zur Namensauflösung bearbeiten.

## Positionierung mehrerer Namenserver

Für jede Zone sollten deshalb mehrere DNS-Namenserver zur Verfügung gestellt werden. Dabei ist einer der Namenserver ein **primärer Namenserver**. Er pflegt die **primäre Zonendatenbank**. Die übrigen Namenserver (sekundäre Namenserver) erhalten Kopien der primären Zonendatei. Änderungen an den Zonendaten werden nur in die primäre Zonendatei eingetragen. Im Zuge von **Zonenübertragungen** erhalten die sekundären Namenserver der betreffenden Zone aktualisierte Zonendaten. So können die Probleme mit einem einzigen Namenserver vermieden werden. Allerdings registrieren sich Clients mit dynamischem DNS nur bei dem für sie eingetragenen ersten DNS-Server. Wenn dieser nun über eine sekundäre Zone verfügt, können sich die Clients bei ihm nicht registrieren.

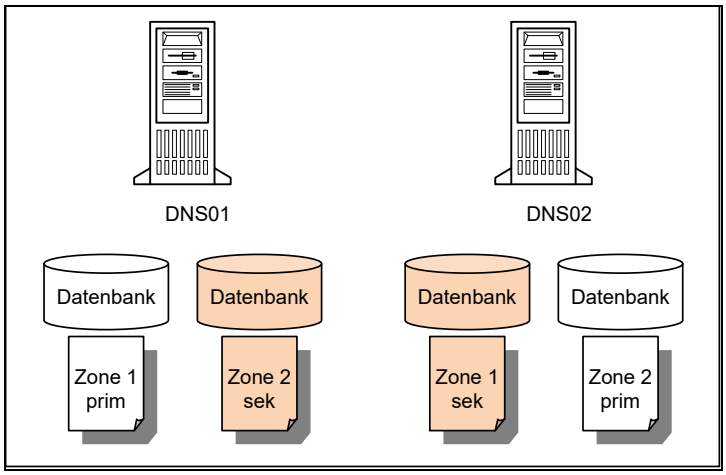
### Beispiel

Eine akzeptable Lösung für *Firma GmbH* wäre z. B. die Aufstellung von zwei Servern, die beide den DNS-Dienst ausführen.

Der Server *DNS01* könnte primärer Namenserver für die Zone 1 und sekundärer Namenserver für die Zone 2 sein.

Ein anderer Server, *DNS02*, wäre dann als primärer Namenserver für die Zone 2 und als sekundärer Namenserver für die Zone 1 einzurichten.

Eine weitere mögliche Alternative bei Einsatz von DNS auf Domänencontrollern seit Windows Server 2003 ist die Einrichtung von Active-Directory-integrierten Zonen.



*Primärer und sekundärer Namenserver*


Schulversion
© HERDT-Verlag

### Active-Directory-integrierte Zonen

Domänencontroller unter Microsoft-Serversystemen ab Windows 2000 können DNS-Zonendaten für den Namespace der eigenen Windows-Domäne in das Active Directory einbeziehen. Dies geschieht, wenn Sie anstelle einer primären oder sekundären Zone auf einem DNS-Server eine Active-Directory-integrierte Zone einrichten, wie in den vorigen Kapiteln beschrieben wurde. Die Konfiguration der nachfolgend beschriebenen Zonenübertragung wird dadurch erheblich vereinfacht.

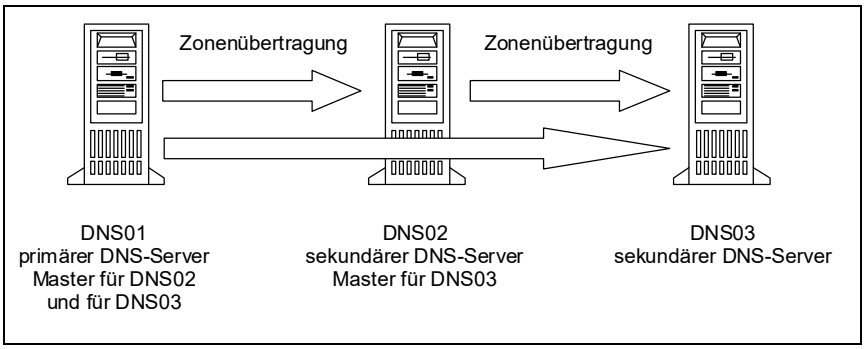
## 8.6 Zonenübertragung

### Klassische Replikation der Zonendatei

Die Zonendatei einer Zone wird vom primären auf die sekundären Namenserver kopiert. Der Informationsfluss erfolgt nur in diese Richtung. Dadurch wird die Zonendatei repliziert.

Es ist nicht erforderlich, dass alle sekundären Namenserver die Kopie direkt vom primären Namenserver erhalten. Auch ein sekundärer Namenserver kann als Quelle von Zonendaten dienen (Master-DNS-Server).

Außerdem kann für einen sekundären Namenserver Zonenübertragung von mehr als einem Masterserver konfiguriert werden. Damit kann sichergestellt werden, dass ein sekundärer Namenserver auch dann die aktuellen Daten erhält, wenn ein Masterserver ausfällt oder nicht erreichbar ist.




### Replikationsmethoden

Je nach Umfang der replizierten Daten und des DNS-Servers, der eine Replikation von Zonendaten auslöst, kann zwischen folgenden Replikationsmethoden unterschieden werden:

- **Vollständige Zonenübertragung** (AXFR): Die gesamte Zonendatei wird vom primären Namenserver aus auf die sekundären Namenserver übertragen.
- **Inkrementelle Zonenübertragung** (IXFR): Nur die Änderungen an den Zonendaten werden vom primären zum sekundären Namenserver übertragen.
- **Vom primären Namenserver veranlasste Zonenübertragungen**: Wenn die Zonendaten geändert wurden, benachrichtigt der primäre Namenserver die sekundären Namenserver über die Änderung. Die sekundären Namenserver fordern daraufhin eine Zonenübertragung an.
- **Vom sekundären Namenserver veranlasste Zonenübertragung**: Ein sekundärer Namenserver fragt seinen Masterserver nach Änderungen in der Zonendatei ab, wenn ...
  - der DNS-Serverdienst auf dem sekundären Namenserver neu gestartet wird;
  - das Intervall für die Serveraktualisierung abläuft.

### Replikation Active-Directory-integrierter Zonen

Durch Integration einer Zone in das Active Directory geht die Replikation der Zonendaten in den Replikationsplan der Domänencontroller der betreffenden Active Directory-Domäne über. Zonendaten müssen deshalb nicht mehr separat an andere DNS-Server repliziert werden.

Die Replikation Active-Directory-integrierter Zonen wird dabei über Verzeichnispartitionen gesteuert. Verzeichnispartitionen sind Teile der Active Directory-Datenbank, die für bestimmte Replikationsräume eingerichtet werden. Unter Windows Server 2019 stehen für die DNS-Replikation die folgenden Verzeichnispartitionen zur Verfügung:

| Verzeichnispartition | Replikationsraum |
|---|---|
| **Forest-DNS-Partition** | Die Replikation erfolgt an alle Domänencontroller der Gesamtstruktur, auf denen der DNS-Dienst installiert ist. |
| **Domain-DNS-Partition** | Die Replikation erfolgt an alle Domänencontroller der Domäne, auf denen der DNS-Dienst installiert ist. |
| **Domainpartition** | Die Replikation erfolgt an alle Domänencontroller der Gesamtstruktur, unabhängig davon, ob der DNS-Dienst installiert ist. |
| **Anwendungs-verzeichnispartitionen** | Möchte man die Datenbankinformationen nur auf bestimmte Domänencontroller übertragen, so können spezielle Anwendungsverzeichnispartitionen erstellt werden, die nur auf ausgesuchte Domänencontroller der Gesamtstruktur repliziert werden. |

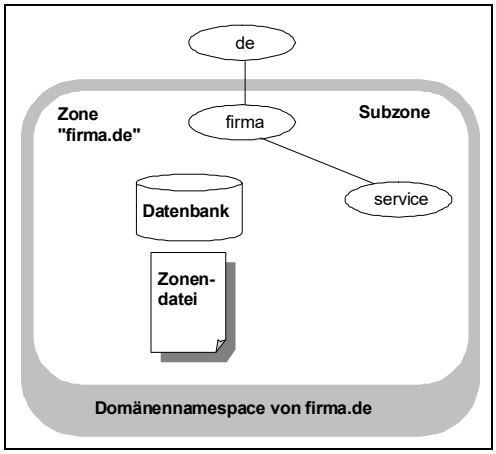
Wenn in einer gemischten Umgebung DNS-Server unter Windows Server 2000 an der Replikation der DNS-Datenbank teilnehmen sollen, müssen Sie die Domainpartition als Replikationsraum angeben, da Windows 2000 keine anderen Verzeichnispartitionen unterstützt. Dieser Hinweis erscheint im System, ist aber rein akademisch, da kein geringerer Gesamtstrukturbetriebsmodus als Windows Server 2008 unterstützt wird.

## 8.7 Zonendelegierung verstehen

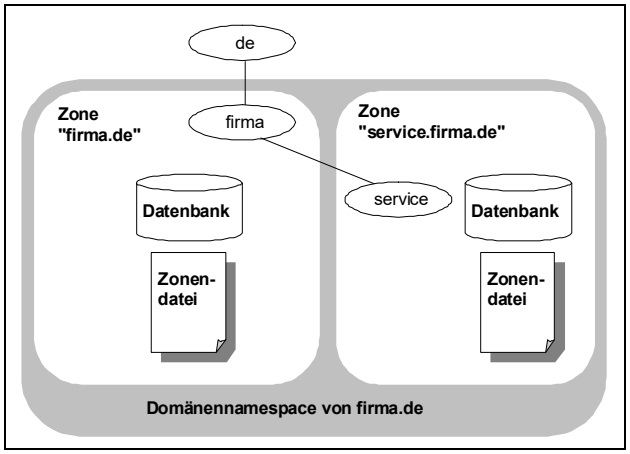
### DNS-Subdomäne und delegierte Zone

Beim Erstellen einer DNS-Subdomäne übernimmt der Domänenstamm der Zone zunächst einmal die Erfassung und die Pflege der betreffenden Ressourceneinträge. Eine Subdomäne bleibt zunächst in der Zone der übergeordneten Domäne. Eine solche Zone heißt **Subzone**. Bei der Integration der DNS-Zone in Active Directory sehen Sie auch die Möglichkeit, eine **Stubzone** zu erstellen. Eine **Stubzone** ist die Kopie einer Zone, die nur die für diese Zone erforderlichen Ressourceneinträge zum Identifizieren der autorisierenden DNS-Server enthält.

Erst durch das **Delegieren** einer Subzone an einen anderen als den bisherigen DNS-Server oder das Anlegen einer eigenen untergeordneten Zone wird der Domänennamespace in mehrere Zonen aufgeteilt.




*Zone mit DNS-Domäne und Subdomäne*




*Zonendelegierung von „service.firma.de“*


Schulversion
© HERDT-Verlag

### Vorteile der Delegierung

- Ein Teil des DNS-Namespaces kann einer anderen Abteilung bzw. einem anderen Administrator überantwortet werden.
- Die Auslastung der für die übergeordnete Zone autorisierenden DNS-Server wird verringert.

### Delegierungseinträge

Die übergeordnete Zone enthält Ressourceneinträge (Delegierungseinträge, Verbindungsdatensätze), die auf die untergeordnete Zone verweisen. Solche Ressourceneinträge enthalten zonenexterne Daten:

- einen Ressourceneintrag, der auf den Namenserver der delegierten Zone verweist,
- einen Hosteintrag, der zum FQD-Namen des für die delegierte Zone autorisierenden Servers die IP-Adresse nennt.

Delegierungen können nur für Subzonen eingerichtet werden, wenn der Server selber über die übergeordnete Zone verfügt. Es ist nicht möglich, mittels Delegierung auf einen Namenserver für beliebige andere DNS-Zonen zu verweisen. Diese Aufgabe können Sie jedoch unter Windows Server 2019 mithilfe von **Stubzonen** erfüllen.

### Stubzonen

Eine Stubzone (Stub = englisch für Stumpf/Stummel) ist ein Auszug aus der Kopie einer DNS-Zone von einem anderen DNS-Server. Die Stubzone erhält den Namen der kopierten Zone, den Autoritätsursprung sowie eine Liste der Namenservereinträge für diese Zone. Der befragte DNS-Server kann daraufhin lokale Anfragen für die Stubzone direkt an einen zuständigen Namenserver weiterleiten und ist nicht gezwungen, zuerst bei den übergeordneten DNS-Servern nachzufragen.

Beispielsweise kann nach einer Fusionierung von ***firma*** mit ***superfirma*** der Wunsch bestehen, Hostnamen bei *superfirma* von *firma* aus direkt aufzulösen. In diesem Fall kann eine Stubzone ***superfirma.de*** auf den DNS-Servern von *firma* eingerichtet werden.

Außerdem wird der DNS-Server, der die Stubzone hält, durch regelmäßige Replikation mit dem Master-DNS-Server über Änderungen informiert. Somit lernt er, wenn neue Namenserver hinzugefügt oder bestehende aus der Struktur entfernt werden.

## 8.8 Aufbau der DNS-Datenbank

### Dateien des DNS

Der DNS-Dienst auf einem Windows Server 2019 legt Daten zur Konfiguration, beispielsweise die Zonendaten, in verschiedenen Dateien ab. Diese Dateien befinden sich unter folgendem Pfad und besitzen verschiedene Funktionen:

| `%WINDIR%\System32\dns\` | |
|---|---|
| `service.firma.de.dns` | Zonendatenbankdatei für Forward-Lookup-Abfragen in der Zone *service. firma*. Die Datenbank ist nach Hostnamen indiziert. |
| `1.168.192.in-addr.arpa.dns` | Zonendatenbankdatei für Reverse-Lookup-Abfragen im Netzwerk 192.168.1.0. Die Datenbankdatei ist nach IP-Adressen indiziert. |
| `cache.dns` | In dieser Datei sind die Einträge der Stammserver des Internets gespeichert. |

### DNS-Aliaseinträge

Aliaseinträge ermöglichen die Verwendung eines zusätzlichen Namens, über den ein Computer im Netzwerk angesprochen werden kann. Mit solchen Einträgen können Sie z. B. den Server *B-FS01.firma.intern* als Fileserver ansprechen. Noch wichtiger sind Aliaseinträge für das Internet, um etwa einen Webserver nicht nur unter seinem Hostnamen *Webserver.firma.de*, sondern auch unter *www.firma.de* erreichbar zu machen. Der Alias wird auch als CNAME (Canonical Name) oder kanonischer Namenseintrag bezeichnet. Er wird in die Zonendatenbankdatei eingetragen.

## Einträge in der Zonendatenbankdatei

Einträge in den Zonendatenbanken heißen Ressourceneinträge. In der folgenden Tabelle werden die verschiedenen Typen von Einträgen aufgeführt:

| Objekt und Kürzel | Erklärung |
|---|---|
| **Autoritätsursprung, SOA** | Ressourceneintrag für den Stammnamenserver der jeweiligen Zone |
| **Namenserver, NS** | Jeder DNS-Server einer Zone wird anhand eines solchen Ressourceneintrags in der Zonendatenbank vermerkt. |
| **Host, A** | Ressourceneintrag für Forward-Lookup-Abfragen nach IPv4-Adressen<br>Diese Ressourceneinträge können dynamisch aktualisiert werden. |
| **Host AAAA** | Ressourceneintrag für Forward-Lookup-Abfragen nach IPv6-Adressen<br>Diese Ressourceneinträge können dynamisch aktualisiert werden. |
| **Zeiger, PTR** | Ressourceneintrag für die Namensauflösung im Reverse-Lookup-Verfahren<br>Die Werte eines Zeigers sind der Hostanteil einer IP-Adresse und der Hostname. Diese Ressourceneinträge können dynamisch aktualisiert werden. |
| **Dienst, SRV** | Mit einem Serviceressourceneintrag können Netzwerkressourcen und Netzwerkdienste vermerkt und von Clients gefunden werden. Mit diesen Diensteinträgen werden beispielsweise Domänencontroller ab Windows 2000 lokalisiert. Diese Ressourceneinträge können dynamisch aktualisiert werden. |
| **Alias, CNAME** | Ressourceneintrag für einen alternativen Hostnamen |
| **Mail-Exchanger, MX** | Ressourceneintrag für einen Mail-Server, der E-Mails für die lokale DNS-Domäne annehmen kann |
| **Hostinfo, HINFO** | Ressourceneintrag für das Betriebssystem und die CPU des Hosts |


Schulversion
© HERDT-Verlag

# 9 DNS-Dienst einrichten und konfigurieren

**In diesem Kapitel erfahren Sie**

- wie Sie den Domänennamespace einrichten
- wie Sie TCP/IP für DNS konfigurieren
- wie Sie den DNS-Dienst installieren und konfigurieren
- wie Sie Forward-Lookupzonen und Reverse-Lookupzonen einrichten
- wie Sie primäre und sekundäre Namenserver konfigurieren
- wie Sie den DNS-Serverdienst testen
- wie Sie die Eigenschaften der Zonen überprüfen

**Voraussetzungen**

- IP-Adressierung
- Konzepte von DNS

## 9.1 Domänennamespace für die Testumgebung

### Ausgangslage nach der Einrichtung der beiden Domänencontroller

In der Testumgebung haben Sie das Active-Directory-integrierte DNS während der Installation der Domänencontroller für *firma.intern* mit eingerichtet. Die beiden DCs *B-DC01* und *B-DC02* sind nun zu DNS-Servern der Zone *firma.intern* geworden und DNS ist grundsätzlich funktionstüchtig. Die Integration des DNS in das AD ist in den meisten Fällen der klassischen DNS-Installation mit primären und sekundären Zonen vorzuziehen, da sie wesentlich einfacher einzurichten und zu administrieren ist.

Für die Testumgebung und auch für die meisten Firmennetzwerke ist eine einzige AD-integrierte DNS-Zone vollkommen ausreichend, daher wird in diesem Buch auf die Einrichtung von Subdomänen und weiteren Zonen verzichtet.

### IP-Protokollauswahl

Damit DNS korrekt funktionieren kann, muss die IP-Konfiguration stimmen. Die Domänencontroller und DNS-Server sollten über eine feste IPv4-Adresse verfügen. Die Clients erhalten ihre IP-Adresse zusammen mit den Informationen über den DNS-Server und den Standardgateway üblicherweise über DHCP zugeteilt, was im nächsten Kapitel beschrieben wird.

Windows Server 2019 unterstützt sowohl IPv4 als auch IPv6. Die Adressierung von Rechnern mittels IPv6 spielt im normalen Geschäftsumfeld immer noch eine untergeordnete Rolle und ist meist auf den Einsatz im Internet beschränkt. Dort herrscht inzwischen ein weltweiter Mangel an IPv4-Adressen, sodass langfristig kein Weg an IPv6 mit seiner schier unbegrenzten Zahl von IP-Adressen vorbeiführt. Im LAN gibt es dagegen nur wenige Anwendungen und Funktionen, die zwingend auf IPv6 angewiesen sind, daher bleiben viele Unternehmen bisher bei IPv4. Gründe hierfür sind vor allem der erhöhte Verwaltungs- und Lernaufwand, aber auch die Kosten für IPv6-fähige Router und Layer-3-Switche.

## 9.2 TCP/IP konfigurieren für DNS

### IP-Konfiguration in der Testumgebung

Sie haben die Server nach deren Installation bereits mit festen Adressen für IPv4 und IPv6 versorgt.

Falls kein DHCPv6 im Netzwerk vorhanden ist, vergibt ein IPv6-Client sich selbst eine verbindungslokale Adresse aus dem Bereich fe80::/10. Die so entstandenen IPv6-Adressen sind stets eindeutig innerhalb des eigenen Netzwerksegments, werden jedoch von Routern nicht weitergeleitet. Dieser Modus ist für die hier beschriebene Testumgebung jedoch ungeeignet, weil die Domänencontroller und DNS-Server über eine statische IP-Adresse verfügen müssen. Auch bei Mitgliedsservern wie *B-FS01* ist dies ratsam.

Sie können sich die IP-Konfiguration auf Ihrem Server ansehen, indem Sie in einer Eingabeaufforderung folgenden Befehl eingeben:

```
ipconfig /all ↵
```

### Aufgabenstellung

Zunächst sollen alle Server mit statischen Adressen und dem DNS-Domänennamen *firma.intern* konfiguriert werden. Anschließend wird auf dem Server *B-DC01* der DNS-Server-Dienst für den Domänennamespace des Netzwerks eingerichtet.

Die folgende Tabelle enthält noch einmal die IP-Konfiguration für die Testumgebung. Alle virtuellen Server sind über ein internes Netz mit dem jeweiligen Host verbunden. Ersetzen Sie also *firma* und den Namen des Hosts durch einen eigenen Namen. Sprechen Sie Ihre Einstellungen gegebenenfalls mit dem Kursleiter und den anderen Teilnehmern ab, um Adressenkonflikte zu vermeiden.

Alle VMs und der interne Netzwerkadapter des Hosts haben die folgenden IPv4-Einstellungen gemeinsam:

- Subnetzmaske: 255.255.255.0
- DNS-Server: 192.168.1.2
- alternativer DNS-Server: 192.168.1.3
- Standardgateway: 192.168.1.1
- DNS-Suffix bzw. DNS-Domänenname: *firma.intern*

Alle VMs und der interne Netzwerkadapter des Hosts haben die folgenden IPv6-Einstellungen gemeinsam:

- Subnetzpräfixlänge: 64
- DNS-Server: fc01::192:168:1:2
- alternativer DNS-Server: fc01::192:168:1:3
- Standardgateway: fc01::192:168:1:1
- DNS-Suffix bzw. DNS-Domänenname: *firma.intern*

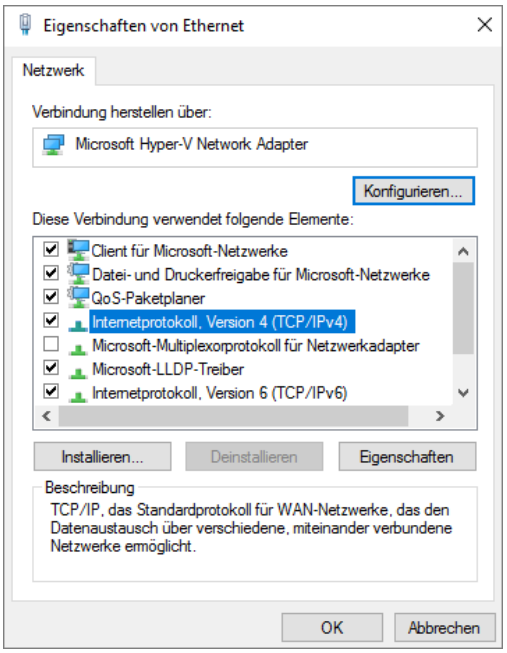

Schulversion
© HERDT-Verlag

| | |
|---|---|
| *HOST-DAUSCH*<br>Physischer Netzwerkadapter<br>Name: *Ethernet* | Übernimmt die Funktion eines virtuellen Switches und hat daher keine IP-Adresse. Der Host verwendet nun den virtuellen Ethernetadapter *vEthernet (Extern)*, um sich mit dem physischen LAN und dem Internet zu verbinden. |
| *HOST-DAUSCH*<br>Hyper-V-Netzwerkadapter<br>Name: *vEthernet (Extern)* | Wählen Sie IPv4-Adresse, DNS-Server und Standardgateway Ihrer physischen Netzwerkumgebung entsprechend, z. B. wie folgt:<br>IPv4-Adresse: 192.168.178.104<br>Standardgateway:192.168.178.1<br>DNS-Server: 192.168.178.1 |
| *HOST-DAUSCH*<br>Hyper-V-Netzwerkadapter<br>Name: *vEthernet (Intern)* | IPv4-Adresse: 192.168.1.1<br>IPv6-Adresse: fc01::192:168:1:1 |
| *B-DC01* | IPv4-Adresse: 192.168.1.2<br>IPv6-Adresse: fc01::192:168:1:2 |
| *B-DC02* | IPv4-Adresse: 192.168.1.3<br>IPv6-Adresse: fc01::192:168:1:3 |
| *B-FS01* | IPv4-Adresse: 192.168.1.4<br>IPv6-Adresse: fc01::192:168:1:4 |

Auf dem Hostserver dürfen Sie auf keinen Fall die Konfiguration auf dem physischen Netzwerkadapter *Ethernet* verändern, da andernfalls die Konnektivität für die virtuellen Computer verloren geht. Der reale Adapter dient im System nur noch als virtueller Netzwerk-Switch für die virtualisierten Adapter!

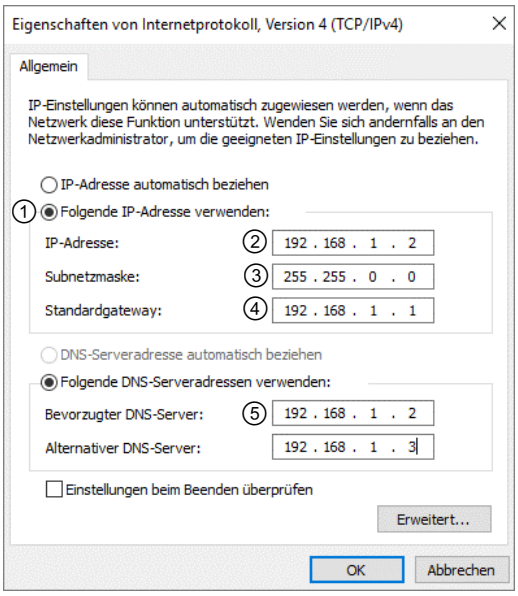
## IPv4 konfigurieren

Die IP-Einstellungen werden stellvertretend auf dem virtuellen Server *B-DC01* durchgeführt. Bei der Erstkonfiguration des Servers *B-DC01* verwenden Sie noch das externe Netz und damit den DNS-Server des physischen Netzwerks, in dem Sie sich befinden. Sobald Sie Windows Online aktiviert haben, schalten Sie in den Hyper-V-Einstellungen jeder VM die Netzwerkverbindung auf den internen Switch um. Die folgende Beschreibung geht davon aus, dass Sie Windows bereits aktiviert haben und mit dem internen Netzwerk verbunden sind. Ob die Domäne bereits eingerichtet wurde, ist für die IP-Konfiguration zweitrangig.




- Melden Sie sich am Server *B-DC01* als Administrator an.
- Öffnen Sie den Server-Manager und wählen Sie in der Serverübersicht *Computerinformationen - Netzwerkverbindungen anzeigen.*
- Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung, die Sie verwalten wollen, und wählen Sie *Eigenschaften*.
- Klicken Sie doppelt auf den Eintrag *Internetprotokoll Version 4 (TCP/IPv4)*.

## Feste IPv4-Adresse angeben




- Im Dialogfenster *Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)* aktivieren Sie die Option ①.
- Geben Sie die eindeutige IP-Adresse in das Eingabefeld ② ein. Durch Betätigen von [.] bzw. [⇥] setzen Sie den Cursor in das nächste Oktett.
- Klicken Sie in das Feld *Subnetzmaske* ③.

Standardmäßig veranschlagt Windows als Subnetzmaske die Maske, die direkt aus der Klasse der in ② eingegebenen IP-Adresse resultiert. Wenn Ihr Netzwerk nicht in Subnetzwerke unterteilt ist, können Sie die vorgeschlagene Subnetzmaske akzeptieren.

- Ändern Sie die Subnetzmaske ③ ab, wenn IP-Subnetzwerke vorhanden sind bzw. wenn Subnetting oder Supernetting vorgesehen ist.

## Standardgateway angeben

Das Standardgateway ist der für Ihren Rechner nächstgelegene zuständige IP-Router, der die Verbindung zu beliebigen anderen Netzen und zum Internet herstellt.

- Geben Sie die IP-Adresse des zuständigen IP-Routers ein ④.

In der virtuellen Testumgebung gibt es keinen IP-Router, Sie sollten hier jedoch den Host mit 192.168.1.1 eintragen. Wenn Sie den Eintrag leer lassen, werden die Stammhinweise nicht verwendet, sondern durch das Anlegen einer eigenen Root-Zone ersetzt. Diese später durch geeignete Stammhinweise zu ersetzen, macht zusätzliche Arbeitsschritte nötig. Geben Sie lieber eine fiktive Adresse an als gar keine.

## Bevorzugte DNS-Server angeben

- Geben Sie in das Eingabefeld ⑤ die IP-Adresse eines primären oder sekundären DNS-Namenservers Ihrer Zone ein.

  Für *B-DC01* können Sie hier die eigene IP-Adresse 192.168.1.2 eingeben.

Falls ein weiterer DNS-Server vorhanden ist, können Sie dessen IP-Adresse als alternativen DNS-Server eingeben. Dabei kann es sich auch um einen DNS-Server einer anderen Zone handeln. Für den zweiten DNS-Server ist es wichtig, dass Sie hier die IP-Adresse des ersten DNS-Servers eingeben. Bei der Einrichtung von *B-DC02* geben Sie also als DNS-Server 192.168.1.2 an.

Wenn Sie den Server *Hostserver* erstmals konfigurieren, gibt es in der Testumgebung noch keine DNS-Server. Der virtuelle Server *B-DC01* selbst soll anschließend der erste DNS-Server im Netzwerk werden. Sie können also in der Testumgebung auf allen Rechnern die IP-Adresse von *B-DC01* eingeben, auch wenn dies ins „Leere“ läuft, solange der DNS-Dienst auf dem Server noch nicht eingerichtet ist.

Wenn Sie jedoch in der Praxis an einem Standort mehrere DNS-Server mit Active-Directory-integrierten Zonen einsetzen, sollten diese sich gegenseitig als primären DNS-Server eingetragen haben. Dadurch können beim Startvorgang Einträge effizienter abgefragt und aktualisiert werden.


© HERDT-Verlag

## Erweiterte Einstellungen

- Klicken Sie im Dialogfenster *Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)* auf die Schaltfläche *Erweitert*.

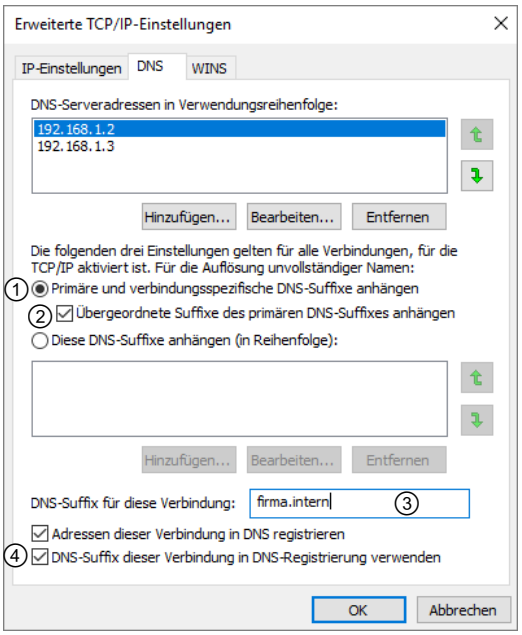
Die Einstellungen in diesem Dialogfenster beziehen sich auf weiterführende TCP/IP-Konfigurationen für den Computer und die komplexe Serverpositionierung im Netzwerk:

- Multihoming (Mehrfachvernetzung, ein Host besitzt mehrere Netzwerkkarten und/oder IP-Adressen)
- Verwendung von mehr als zwei IP-Routern mit Angabe von Metriken (Kosteninformationen der Routen)
- Verwendung von mehr als zwei DNS-Servern
- Verwendung von verbindungsspezifischen DNS-Namen bei mehrfach vernetzten Computern
- Festlegung, ob und wie dynamische Aktualisierung erfolgen soll
- Festlegung, ob und wie die Auflösung von NetBIOS-Namen erfolgen soll

## Erweiterte TCP/IP-Einstellungen

Die folgenden Einstellungen sollten Sie sowohl auf dem Hostserver als auch bei den VMs durchführen. Besonders wichtig sind sie für alle (zukünftigen) DNS-Server, also *B-DC01* und *B-DC02*.

- Wählen Sie im Dialogfenster *Erweiterte TCP/IP-Einstellungen* das Register *DNS*.
- Stellen Sie sicher, dass die Option ① und das Kontrollfeld ② aktiviert sind. Im Feld ③ können Sie nun das DNS-Suffix *firma.intern* eintragen.
- Aktivieren Sie das Kontrollfeld ④.




Dies bewirkt, dass für die Anfrage zur Namensauflösung die DNS-Client-Komponente DNS-Namen bildet, indem sie das angegebene Suffix anhängt, statt den computereigenen DNS-Domänennamen zu verwenden.

Beachten Sie, dass der DNS-Domänenname noch nicht festgelegt worden ist. Um aber trotzdem eine Registrierung mit dem verbindungsspezifischen DNS-Suffix zu ermöglichen, sollten Sie in der Testumgebung einen Eintrag in ③ vornehmen und ④ aktivieren.

Wenn der Computer bereits Mitglied einer Domäne ist, sollten Sie das Feld ③ frei und das zugehörige Kontrollfeld ④ deaktiviert lassen, außer Sie möchten eine alternative Registrierung konfigurieren, die vom Rechnernamen abweicht.

- Schließen Sie alle Dialogfenster.

Erst wenn Sie das Dialogfenster *Eigenschaften von Ethernet* schließen, erfolgt ein Neustart des Netzwerkadapters und die Einstellungen werden übernommen.

## IPv6 konfigurieren

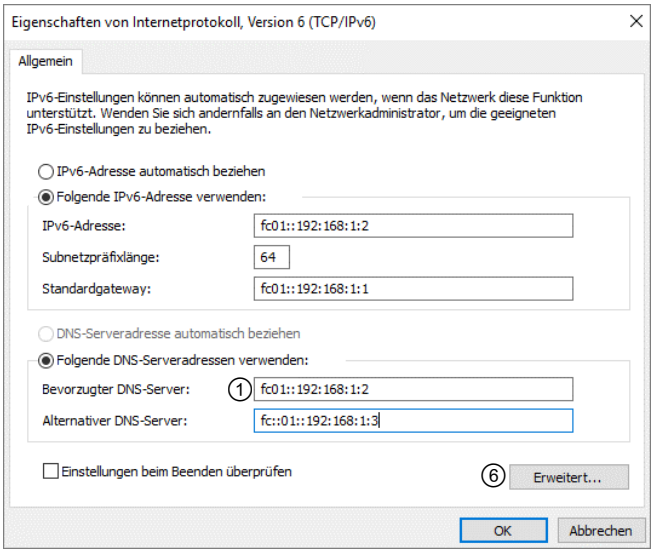
- Öffnen Sie entsprechend die Eigenschaften der Ethernet-Verbindung, die Sie für IPv6 konfigurieren möchten.
- Klicken Sie doppelt auf den Eintrag *Internetprotokoll Version 6 (TCP/IPv6).*

## Feste IPv6-Adresse angeben

- Im Dialogfenster *Eigenschaften von Internetprotokoll Version 6 (TCP/IPv6)* aktivieren Sie die Option *Folgende IPv6-Adresse verwenden*.
- Geben Sie die eindeutige IP-Adresse ein.

  Wählen Sie wegen der leichten Lesbarkeit `fc01::` gefolgt von Ihrer IPv4-Adresse.
- Klicken Sie in das Feld *Subnetzpräfixlänge*.

  Der Standard ist 64. Nur wenn Sie eine abweichende Subnetzkonfiguration verwenden, müssen Sie die Subnetzpräfixlänge anpassen.




## Standardgateway angeben

- Geben Sie die IP-Adresse des zuständigen IP-Routers ein. Für die Testumgebung können Sie hier `fc01::192:168:1:1` eintragen.

## Bevorzugte DNS-Server angeben

- Geben Sie in das Eingabefeld ① die IP-Adresse eines primären oder sekundären DNS-Namenservers Ihrer Zone ein.

  Falls ein weiterer DNS-Server vorhanden ist, können Sie dessen IP-Adresse in das Eingabefeld eingeben. Dabei kann es sich auch um einen DNS-Server einer anderen Zone handeln. In der Testumgebung ist es hilfreich, hier stets auch den zweiten DNS-Server einzutragen.

## Erweiterte Einstellungen

- Klicken Sie im Dialogfenster *Eigenschaften von Internetprotokoll Version 6 (TCP/IPv6)* auf die Schaltfläche *Erweitert*.
- Überprüfen Sie Ihre Einstellungen analog zu IPv4.

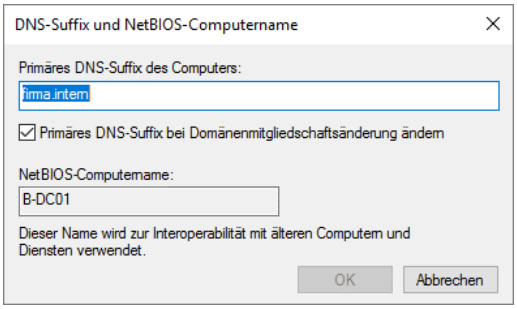
## Serverkonfiguration abschließen

Verfahren Sie bei allen drei virtuellen Computern entsprechend den in der Tabelle festgelegten Adressen.

## DNS-Server vorbereiten

Bevor Sie den DNS-Serverdienst auf dem virtuellen Computer *B-DC01* einrichten, müssen Sie dafür sorgen, dass dieser sich selbst im DNS sauber einträgt und auflösen kann. Sonst werden DNS-Clients nicht in der Lage sein, sich auf ihm zu registrieren. Diesen Vorgang müssen Sie auch für *B-DC02* durchführen.

- Öffnen Sie im Server-Manager die Seite *Lokaler Server*.
- Klicken Sie auf den Computernamen.
- Betätigen Sie im Register *Computername* die Schaltfläche *Ändern* und klicken Sie anschließend auf *Weitere.*
- Geben Sie das primäre DNS-Suffix für Ihren Computer an und bestätigen Sie mit *OK*.




Würden Sie stattdessen den Rechner in eine Domäne aufnehmen, würde dieses Feld automatisch ausgefüllt werden.

- Starten Sie den Rechner nach Aufforderung neu.


© HERDT-Verlag

## 9.3 DNS-Dienst installieren

### Aufgabenstellung

Obwohl Sie bereits im Kapitel 7 das DNS im Zuge der Active Directory-Einrichtung installiert haben, geht es jetzt darum, DNS ohne AD-Integration zu installieren. Dabei sollen die Funktionsweise von DNS und mögliche Probleme bei der Einrichtung gezeigt werden, die Ihnen bei der AD-integrierten Zone weitgehend abgenommen werden. Nutzen Sie dazu die Vorteile einer virtuellen Testumgebung:

- Fertigen Sie von allen drei VMs einen Snapshot an, damit Sie nach Beendigung der folgenden Übungen zu DNS wieder zum vorigen Stand zurückkehren können.
- Kehren Sie bei allen VMs zum ersten Snapshot zurück, der nach der Windows-Installation, aber vor der Installation des AD angefertigt wurde. Klicken Sie dazu mit der rechten Maustaste auf den Snapshot und wählen Sie *Anwenden*.

  Es erscheint eine Warnmeldung.
- Falls Sie gerade einen Snapshot erstellt haben, klicken Sie auf *Anwenden*, ansonsten klicken Sie auf *Momentaufnahme erstellen und anwenden*.

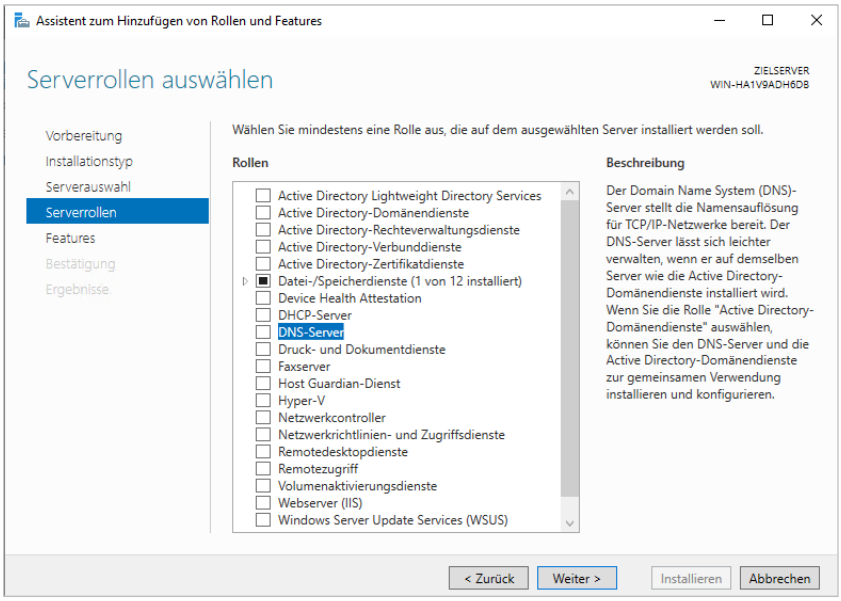
Beachten Sie die in diesem Kapitel beschriebenen Schritte zur IP-Konfiguration und vergessen Sie nicht, das DNS-Suffix *firma.intern* einzutragen.

### DNS-Dienst installieren

- Verbinden Sie sich mit dem virtuellen Computer *V-B-DC01* und melden Sie sich am Server *B-DC01* als Administrator an.
- Klicken Sie im Dashboard des Server-Managers auf *Rollen und Features hinzufügen*.

  Es öffnet sich der Assistent.
- Klicken Sie auf *Weiter*, bis Sie die Seite *Serverrollen hinzufügen* erreichen.
- Klicken Sie auf *DNS-Server*.
- Bestätigen Sie das Hinzufügen zusätzlicher benötigter Features mit *Features hinzufügen*.

  Achten Sie dabei darauf, dass die Option *Verwaltungstools einschließen* aktiviert ist.
- Klicken Sie mehrmals auf *Weiter* und dann auf *Installieren*. Die Serverrolle *DNS-Server* wird nun installiert.




*Rollenstatus des DNS-Servers*

Sie erhalten im Server-Manager eine Übersicht über den Status des DNS-Servers. Hier können Sie die beteiligten Rollen und Features sowie den DNS-Serverdienst sehen. Außerdem werden im Server-Manager noch Warnungen, Fehler und die Auslastung des DNS-Servers angezeigt.

Die DNS-Konfiguration führen Sie nicht im Server-Manager durch, sondern über den DNS-Manager.

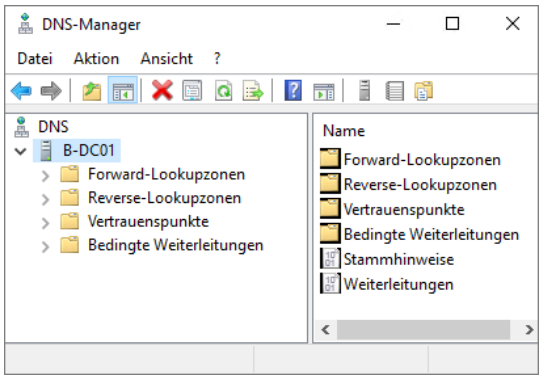
### DNS-Manager aufrufen

- Klicken Sie im Menü *Tools* des Server-Managers auf *DNS.*

  Alternativ können Sie auch im Startmenü `dnsmgmt.msc` eingeben.

  Der DNS-Manager wird geöffnet.

Im DNS-Manager können Sie sämtliche Einstellungen rund um DNS vornehmen. Direkt nach der Installation gibt es noch keine DNS-Zone, es sei denn, Sie verwenden AD-integriertes DNS.




*DNS-Konsole*

## 9.4 DNS-Dienst konfigurieren

Der DNS-Dienst soll folgendermaßen konfiguriert werden:

- *B-DC01* soll primärer Namenserver für die DNS-Domäne *firma.intern* sein.
- Er soll Namensauflösungsanfragen für übergeordnete DNS-Domänen an Stammserver im Internet weitergeben.
- Eine Forward-Lookupzone für die DNS-Domäne soll erstellt werden.
- Eine IPv4-Reverse-Lookupzone soll erstellt werden.
- Eine IPv6-Reverse-Lookupzone soll erstellt werden.
- Forward-Lookup- und Reverse-Lookupzone sollen für unsichere und sichere dynamische Aktualisierung aktiviert sein.

### Die Datei *cache.dns*

Zur Einrichtung des DNS-Servers wird ein Assistent angeboten. Dieser Assistent wird versuchen, Hinweise auf Stammnamenserver im Internet einzurichten. Dies gelingt automatisch, wenn bei der Konfiguration des Netzwerkadapters ein Standardgateway angegeben wurde und eine Internetverbindung besteht. Falls dies nicht der Fall ist, erfolgt die Standardkonfiguration mithilfe der Datei *%systemroot%\system32\dns\samples\cache.dns*, die bei der Installation von DNS eingerichtet wurde. Sie sollten überprüfen, ob deren Informationen noch dem aktuellen Stand entsprechen.

- Öffnen Sie die Datei mit dem Editor und schauen Sie sich den Aufbau an.
- Überprüfen Sie die Aktualität der Version, indem Sie auf die in der Datei angegebene Internetadresse zugreifen. Öffnen Sie dort die Datei *db.cache*.

Die lokale Datei enthält die gleichen Stammhinweise (A Resource Records) wie die neuere Version im Internet, diese verfügt zusätzlich über die Stammhinweise für IPv6 (AAAA Resource Records). Eine Aktualisierung ist in der Praxis nicht zwingend notwendig.

Die Datei *cache.dns* ist schreibgeschützt. Um sie zu verändern, müssen Sie so vorgehen:

- Schließen Sie den DNS-Manager und beenden Sie den DNS-Dienst entweder im Task-Manager oder im Server-Manager.
- Speichern Sie die Datei *cache.db* in einer Freigabe ab, auf die von den VMs aus zugegriffen werden kann. Markieren Sie den gesamten Inhalt der Datei *cache.db* und ersetzen Sie damit den Inhalt der lokalen Datei *cache.dns*. Speichern Sie die Datei. Stellen Sie sicher, dass Sie dabei keine Endung .txt angefügt haben.
- Starten Sie den DNS-Dienst im Server-Manager neu.


Schulversion
© HERDT-Verlag

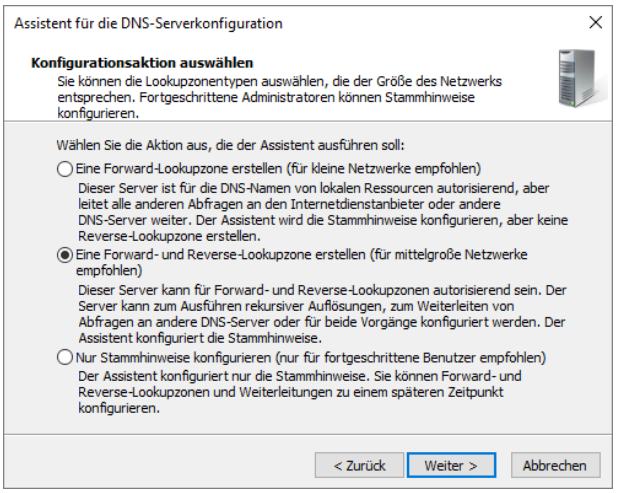
## Aktion des Assistenten auswählen

- Klicken Sie im Menü *Aktion* des DNS-Managers auf *DNS-Server konfigurieren.*

Der gestartete Assistent für die DNS-Serverkonfiguration bietet drei unterschiedlich komplexe Optionen für den Einsatz des Servers an.

- Wählen Sie die mittlere Option zur Einrichtung einer Forward- und Reverse-Lookupzone.

  Diese Option wird für die meisten Konstellationen empfohlen.

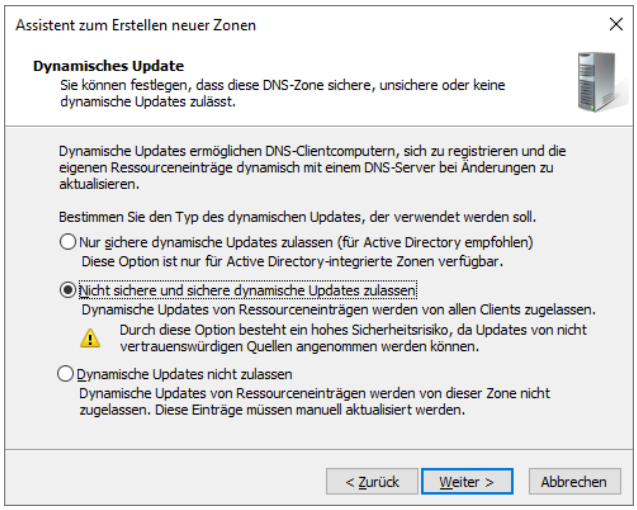



*Aktion auswählen*

Die folgenden 5 Dialogfenster führen Sie durch die Erstellung einer Forward-Lookupzone.

## Forward-Lookupzone erstellen

- Bestätigen Sie die Erstellung einer neuen Forward-Lookupzone.
- Wählen Sie als Zonentyp die primäre Zone aus.
- Geben Sie als Zonennamen *firma.intern* an.
- Lassen Sie eine neue Zonendatendatei mit dem vorgeschlagenen Namen *firma.intern.dns* erstellen.
- Lassen Sie die nicht sichere und sichere dynamische Aktualisierung der Zonendaten zu. Sie können später die DNS-Zonen in das Active Directory integrieren und dann nur noch gesicherte Aktualisierungen zulassen.
- Bestätigen Sie Ihre Angaben mit *Weiter.*



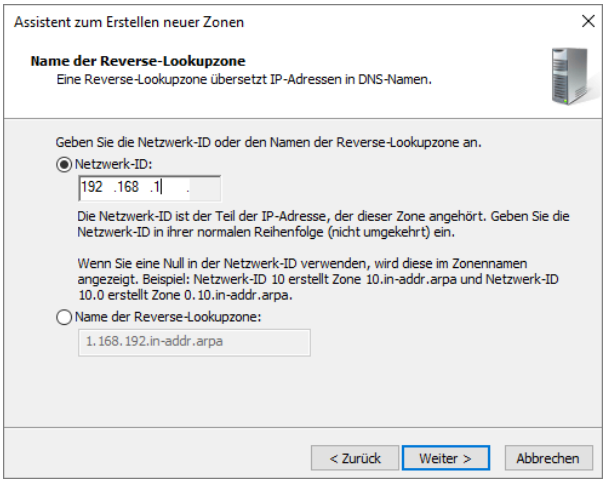

*Zonentyp auf primär festlegen*

Sie werden nun gefragt, ob Sie eine Reverse-Lookupzone erstellen möchten.

## Reverse-Lookupzone erstellen

Sie können mit dem Assistenten nur eine Reverse-Lookupzone erstellen. Erstellen Sie primär die IPv4-Reverse-Lookupzone und später manuell die IPv6-Reverse-Lookupzone.

- Bestätigen Sie die Einrichtung einer Reverse-Lookupzone.
- Legen Sie den Zonentyp mit primär fest.
- Legen Sie fest, dass Sie eine IPv4-Reverse-Lookupzone erstellen möchten, und bestätigen Sie mit *Weiter.*
- Tragen Sie die Netzwerkkennung Ihres IP-Subnetzes ein, für die Testumgebung ist das *192.168.1*.



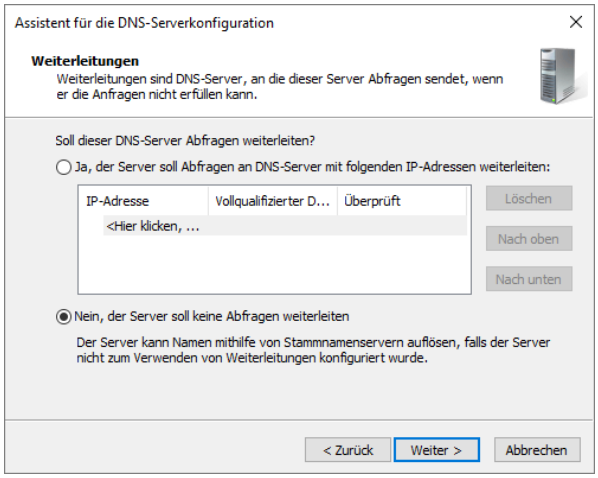

*Netzwerkkennung für IPv4-Reverse-Lookupzone angeben*

Die Subnetz-IP findet sich in umgekehrter Reihenfolge im Namen der Zone wieder.

- Übernehmen Sie den vorgeschlagenen Namen *1.168.192.in-addr.arpa.dns* für die Zonendatei.
- Erlauben Sie wiederum die unsichere dynamische Aktualisierung der Zonendatei.

## Weiterleitungen und Stammhinweise konfigurieren

Wenn ein DNS-Server Anfragen zur Namensauflösung nicht selbst beantworten kann oder soll, muss er diese an andere Namenserver weitergeben. Übergeordnete Namenserver erreicht er dabei entweder über eine **Weiterleitung** an definierte Server oder mittels Abfrage der **Stammnamenserver** einer DNS-Hierarchie, beispielsweise des Internets. Bei einer **Weiterleitung** wird eine **iterative Abfrage** (entspricht einer einfachen Clientanfrage) an einen Server gesendet, der seinerseits die **rekursive Abfrage** an das Internet sendet. Bei einer Abfrage an die **Stammnamenserver** wird eine eigene rekursive Abfrage durchgeführt.




*Weiterleitung einrichten*

- Aktivieren Sie das Optionsfeld *Nein, der Server soll keine Abfragen weiterleiten*, da für die Testumgebung noch keine DNS-Server zur Weiterleitung verfügbar sind.
- Stellen Sie den Assistenten fertig.

Sofern eine Internetverbindung besteht, wird DNS jetzt konfiguriert, während der Assistent die Konfiguration der Stammhinweise aus der Datei oder dem Internet durchführt.

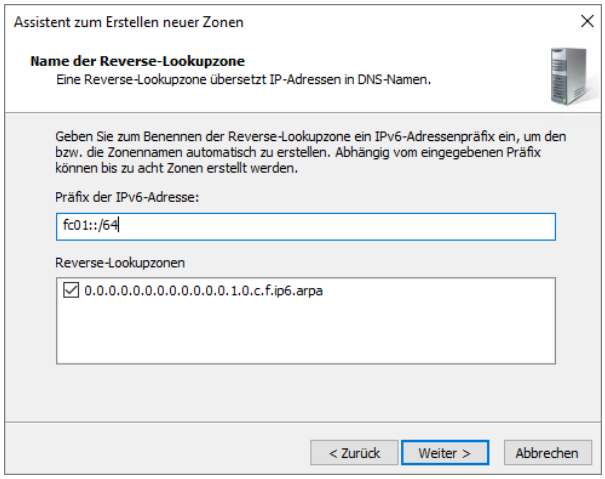
Da Sie in der Testumgebung keine Internetverbindung verwenden, erhalten Sie eine Warnmeldung. Diese weist Sie darauf hin, dass Ihre Stammhinweise konfiguriert werden müssen. Das System nimmt anschließend eine Konfiguration mit den vorhandenen Einträgen der Datei `Cache.dns` vor.

Der Server *B-DC01* ist jetzt als **primärer Namenserver** für die Zone *firma.intern* eingerichtet.

## Einrichten der IPv6-Reverse-Lookupzone

Bevor Sie nun die Rechner auf dem DNS-Server registrieren, sollten Sie noch eine Reverse-Lookupzone für IPv6 einrichten.

- Erweitern Sie im DNS-Manager den Knoten *Reverse-Lookupzonen*.
- Klicken Sie im Kontextmenü auf *NEUE ZONE*, um den Assistenten für das Erstellen neuer Zonen zu starten.
- Klicken Sie auf *Weiter* und wählen Sie eine primäre Zone. Bestätigen Sie die Auswahl.
- Erstellen Sie nun eine IPv6-Reverse-Lookupzone und klicken Sie auf *Weiter*.
- Geben Sie eine korrekte IPv6-Adresse einschließlich der Bit-Maske ein und bestätigen Sie mit *Weiter*. Tragen Sie als Präfix in der Testumgebung `fc01::/64` ein.




*IPv6-Adressenpräfix angeben*

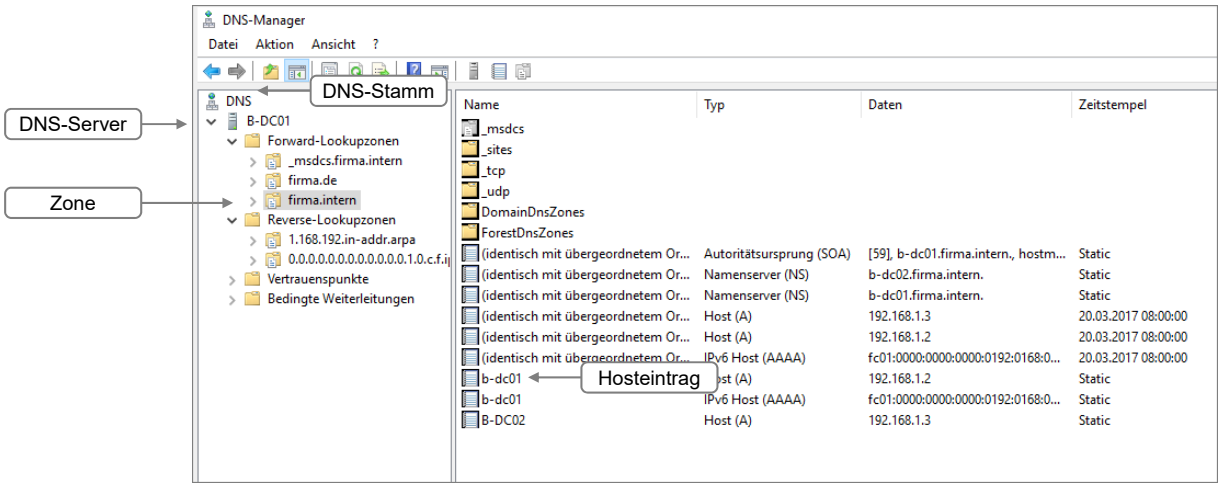

Schulversion
© HERDT-Verlag

- Geben Sie einen beliebigen Namen für die Datei ein, z. B. `ipv6.firma.dns`, und bestätigen Sie mit *Weiter*.
- Wählen Sie nicht sichere und sichere dynamische Updates zulassen und klicken Sie auf *Weiter*.
- Beenden Sie den Assistenten mit *Fertig stellen*.

### Registrieren des eigenen DNS-Servers in der DNS-Zone

- Öffnen Sie eine Eingabeaufforderung mit Administratorrechten und geben Sie den Befehl `ipconfig -registerdns` ein.

  Der Befehl bewirkt, dass sämtliche Netzwerkadapter Ihres Rechners sofort auf dem DNS-Server registriert werden.
- Wiederholen Sie diesen Schritt auf allen Servern der Testumgebung.




*Primärer Namenserver der DNS-Domäne „firma.intern“*

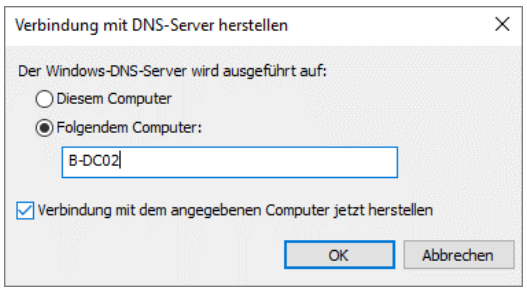
## 9.5 Zoneneigenschaften bearbeiten

### Fernen DNS-Server im DNS-Manager anzeigen

Sofern die Kennwörter der lokalen Administratorkonten der Server gleich lauten und die Firewall-Einstellungen dies zulassen, können Sie auch ferne DNS-Server im DNS-Manager der Verwaltung anzeigen.

- Klicken Sie auf dem Server *B-DC01* im DNS-Manager mit der rechten Maustaste auf den Knoten *DNS* und wählen Sie im Kontextmenü *Mit DNS-Server verbinden*.
- Aktivieren Sie die Option *Folgendem Computer* und geben Sie den Namen des Servers ein, in diesem Fall *B-DC02*. Klicken Sie auf *OK*.

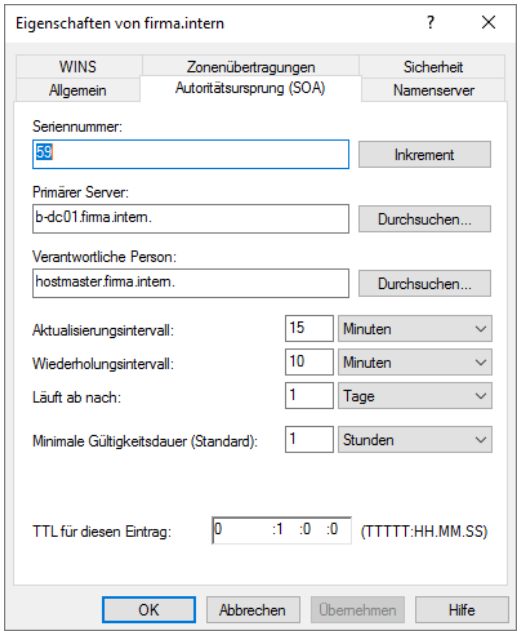
  Der Server *B-DC02* erscheint nun im DNS-Manager.




Die Einstellungen werden gespeichert, sodass beim nächsten Start des DNS-Managers wieder alle hinzugefügten DNS-Server verfügbar sind.

## Eigenschaften des Autoritätsursprungs anzeigen

- Klicken Sie im DNS-Manager unter dem Server *B-DC01* mit der rechten Maustaste auf die Zone *firma.intern* und wählen Sie den Kontextmenübefehl *Eigenschaften*.
- Öffnen Sie das Register *Autoritätsursprung (SOA)*.




*Autoritätsursprung anzeigen*

### Seriennummer

Die Seriennummer dient zur Identifikation der Version einer Zonendatendatei, die im Moment von einem Server verwendet wird. Durch Betätigen der Schaltfläche *Inkrement* wird die Seriennummer der Zonendatendatei erhöht und so eine Replikation vom primären an sekundäre DNS-Server initialisiert. Voraussetzung hierfür ist, dass Benachrichtigungen konfiguriert sind. In der Standardeinstellung sind diese für Server im Register *Namenserver* aktiviert.

### Zusammenfassung

Die Eigenschaften des Autoritätsursprungs (die Zonendatenbank) können nur auf dem primären Namenserver einer Zone verändert werden. Die sekundären Namenserver erhalten eine schreibgeschützte Kopie der Datei.

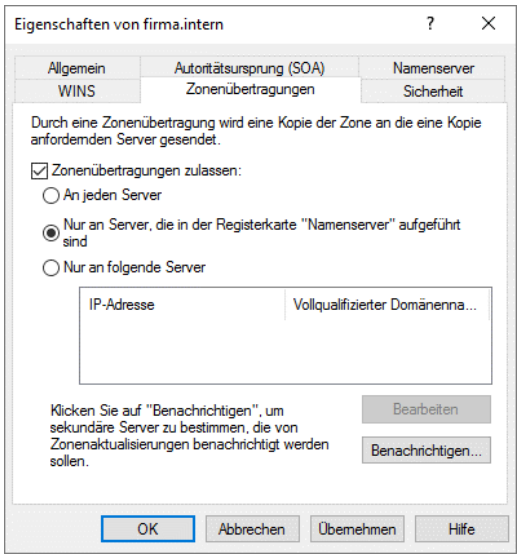
## Einstellungen für die Zonenübertragung überprüfen

Die Zonenübertragungen gelten für jede Zone einzeln. Das bedeutet, dass Sie die Einstellungen für beide Forward-Lookupzonen (IPv4 und IPv6) und beide Reverse-Lookupzonen ändern müssen. In den Standardeinstellungen werden Zonenübertragungen zwar zugelassen, jedoch nur an Server, die auf der Registerkarte *Namenserver* eingetragen sind. Dort ist standardmäßig nur der primäre DNS-Server zu finden.

- Lassen Sie die Zonenübertragungseigenschaften der primären Zone für den Server *B-DC01* anzeigen. Klicken Sie hierzu im Dialogfenster *Eigenschaften von firma.intern* auf das Register *Zonenübertragungen.*
- Kontrollieren Sie, ob die Zonenübertragung stattfinden kann. Belassen Sie die momentan aktive Option und fügen Sie alle sekundären Server auf der Registerkarte *Namenserver* hinzu.

  Alternativ können Sie auch die Option *An jeden Server* aktivieren.
- Führen Sie diesen Vorgang für jede einzelne primäre Zone durch.

Unter *Benachrichtigen* können Sie sekundäre Server eintragen, die bei Zonenänderungen automatisch informiert werden sollen.




*Einstellungen zur Zonenübertragung einsehen*

### Zusammenfassung

Zonenübertragungen werden vom primären DNS-Server (Master) angestoßen und gehen hin zum sekundären DNS-Server (Push-Mechanismus). Zonenübertragungen erfolgen standardmäßig ausschließlich an DNS-Server, die im Register *Namenserver* in eine Liste eingetragen sind.

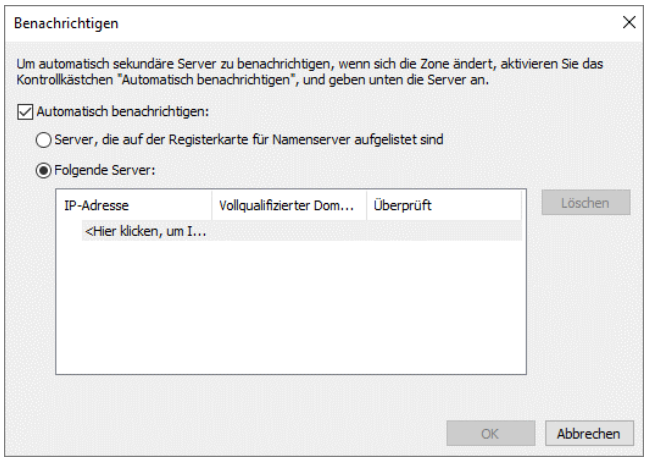

Schulversion
© HERDT-Verlag

### DNS-Benachrichtigung in der Zone *firma.intern* überprüfen

Damit DNS innerhalb der Zone korrekt funktioniert, müssen die sekundären DNS-Server über alle Änderungen informiert werden. Dies wird mithilfe von DNS-Benachrichtigungen erreicht, die standardmäßig an alle in der Registerkarte *Namenserver* versendet werden.

- Klicken Sie im Dialogfenster *Eigenschaften von firma.intern* im Register *Zonenübertragungen* auf die Schaltfläche *Benachrichtigen.*

  Interpretieren Sie die Wirkung der abgebildeten Standardeinstellungen.




*Benachrichtigungseinstellungen einsehen*

Sie sehen hier erneut, wie wichtig es ist, dass die sekundären Server in der Liste der Namenserver eingetragen wurden.

Sie sollten die Einstellungen für die automatische Benachrichtigung nicht grundlos ändern.

Denken Sie daran, dass diese Einstellungen für jede einzelne Zone stimmen müssen, damit DNS reibungslos funktioniert.

### Zusammenfassung

Die DNS-Benachrichtigung ist standardmäßig aktiviert. Sie sieht die Benachrichtigung der sekundären DNS-Namenserver einer Zone vor, die in die Liste der Namenserver aufgenommen sind.

Diese Benachrichtigungseinstellungen bleiben so lange relevant, wie Sie DNS nach dem klassischen Verfahren mit primären und sekundären Zonen betreiben. Wenn Sie die DNS-Zonen jedoch später ins Active Directory integrieren, werden Zonendaten über die Replikationsmechanismen des Active Directory repliziert. Sie können die klassischen Benachrichtigungen dann deaktivieren.

## 9.6 Sekundäre Zone einrichten

### Zonenreplikation vorbereiten

Sie werden nun eine Kopie der Zone *firma.intern* für die Replikation auf *B-DC02* vorbereiten. Vergewissern Sie sich, dass Sie das DNS-Suffix manuell hinzugefügt haben, sonst kann der DNS-Server nicht richtig arbeiten.
Den ersten Teil der Einrichtung führen Sie auf *B-DC01* durch:

- Klicken Sie mit der rechten Maustaste auf die Zone *firma.intern* und wählen Sie im Kontextmenü *Eigenschaften*.
- Wechseln Sie auf die Registerkarte *Namenserver* und klicken Sie auf *Hinzufügen*.
- Geben Sie den vollen FQDN des Servers ein, also `B-DC02.firma.intern`, und klicken Sie auf *OK*.

Sie können die Meldung ignorieren, dass der Server im Moment für die Zone nicht autorisierend ist. Dieser Fehler wird behoben, sobald Sie die Zone eingerichtet haben.

- Klicken Sie in *Eigenschaften* auf *OK*.

### Sekundäre Zone hinzufügen

Sie können die sekundäre Zone auch über den Assistenten für das Erstellen neuer Zonen erstellen, doch der Weg über die Kommandozeile ist hier deutlich schneller:

- Verbinden Sie sich mit dem Server *B-DC02* und öffnen Sie dort eine Kommandozeile mit Administratorrechten.
- Geben Sie `dnscmd /zoneadd firma.intern /secondary 192.168.1.2` ↵ ein.
- Verwenden Sie die IP-Adresse des primären Namenservers für die Zone. In der Testumgebung ist dies *B-DC01*.
- Erstellen Sie nun die verbleibende Forward-Lookupzone für IPv6 und die sekundären Reverse-Lookupzonen.

## 9.7 DNS-Serverdienst testen

### Testen mit dem Befehl `nslookup`

*Nslookup.exe* ist ein Diagnoseprogramm, das zusammen mit dem Protokoll TCP/IP installiert wird. Verwenden Sie dieses Programm, um DNS-Server zu testen.

- Öffnen Sie die Eingabeaufforderung.

Sie haben die Möglichkeit, *nslookup* interaktiv zu starten. Geben Sie dazu `nslookup` ein. Nun können Sie mehrere Abfragen nacheinander durchführen. Den interaktiven Modus beenden Sie mit dem Befehl `exit`.

Sie können *nslookup* auch starten, indem Sie im DNS-Manager in der Navigationsspalte mit der rechten Maustaste auf einen DNS-Server klicken und im Kontextmenü auf *nslookup starten* klicken.

Möchten Sie nur eine Abfrage durchführen, geben Sie den Befehl `nslookup` mit Parametern ein.

| `nslookup [option] <computer> <server>` | |
|---|---|
| `option` | Ein oder mehrere `nslookup`-Befehle. Die Liste der verfügbaren Befehle können Sie durch Eingabe von `?` anzeigen lassen. |
| `computer` | Hostname oder IP-Adresse des Hosts, für den Sie die Namensauflösung testen möchten |
| `server` | Hostname oder IP-Adresse des Namenservers, der die DNS-Abfrage bearbeiten soll |


Schulversion
© HERDT-Verlag

## Übung: Den DNS-Serverdienst mit `nslookup` testen

- Führen Sie auf dem Server *B-DC01* folgende Abfragen durch:
  1. `nslookup` ↵
  2. `B-DC01.firma.intern` ↵
  3. `B-DC02` ↵
  4. `fc01::192:168:1:4` ↵
  5. `192.168.1.2` ↵
- Schließen Sie das `nslookup`-Eingabefenster noch nicht.

```
C:\>nslookup
Standardserver:  b-dc01.firma.intern
Address:  fc01::192:168:1:2

> b-dc01.firma.intern
Server:  b-dc01.firma.intern
Address:  fc01::192:168:1:2

Name:    b-dc01.firma.intern
Addresses:  fc01::192:168:1:2
          192.168.1.2

> b-dc02
Server:  b-dc01.firma.intern
Address:  fc01::192:168:1:2

Name:    b-dc02.firma.intern
Addresses:  fc01::192:168:1:3
          192.168.1.3

> fc01::192:168:1:4
Server:  b-dc01.firma.intern
Address:  fc01::192:168:1:2

Name:    b-fs01.firma.intern
Address:  fc01::192:168:1:4

> 192.168.1.2
Server:  b-dc01.firma.intern
Address:  fc01::192:168:1:2

Name:    b-dc01.firma.intern
Address:  192.168.1.2

> 192.168.1.21
Server:  b-dc01.firma.intern
Address:  fc01::192:168:1:2

Name:    b-pc01.firma.intern
Address:  192.168.1.21

> dateiserver
Server:  b-dc01.firma.intern
Address:  fc01::192:168:1:2

Name:    b-fs01.firma.intern
Addresses:  fc01::192:168:1:4
          192.168.1.4
Aliases:  dateiserver.firma.intern
```

*`nslookup` im interaktiven Modus ausführen*

## Neuen Host erstellen

- Klicken Sie im DNS-Manager mit der rechten Maustaste auf die Zone *firma.intern* und wählen Sie den Kontextbefehl *Neuer Host (A oder AAAA)*.
- Geben Sie den Hostnamen und die IPv4-Adresse an, z. B. *B-PC01* mit 192.168.1.21 als IP-Adresse.
- Aktivieren Sie die Option *Verknüpften PTR-Eintrag erstellen*, um einen Eintrag in der Reverse-Lookupzone zu erstellen, und klicken Sie auf *Host hinzufügen.*

## Neuen Alias erstellen

- Klicken Sie im DNS-Manager mit der rechten Maustaste auf die Zone *firma.intern* und wählen Sie den Kontextbefehl *Neuer Alias (CNAME)*.
- Geben Sie als Aliasnamen z. B. *Dateiserver* ein und verknüpfen Sie diesen Alias mit *B-FS01.firma.intern*.
- Klicken Sie auf *OK*.

## Weitere `nslookup`-Abfragen

- Führen Sie nun auf dem Server *B-DC01* weitere Abfragen durch:
  6. `192.168.1.21` ↵
  7. `dateiserver` ↵
  8. `exit` ↵
- Führen Sie auch `nslookup`-Abfragen auf den Servern *B-DC02* und *B-FS01* durch.

## Fehlersuche

- Probleme können auftreten, wenn noch keine sekundäre Reverse-Lookupzone eingerichtet wurde. Holen Sie dies nun nach. Sie können dies von beiden DNS-Servern aus erledigen.
- Eine andere wahrscheinliche Ursache sind fehlende DNS-Benachrichtigungen.
- Allgemeine Störungen des DNS können durch Netzwerkprobleme verursacht werden, vor allem, wenn Sie auf dem Host die Einstellungen des virtuellen Netzwerkadapters für das interne Netz nachträglich verändert haben. Wechseln Sie in solchen Fällen probeweise für jede VM die Netzwerkverbindung nach extern und wieder zurück auf intern. Vermeiden Sie Änderungen an den Netzwerkverbindungen des Hosts.
- Firewall-Einstellungen können dafür sorgen, dass die Ping-Abfragen nicht funktionieren. Deaktivieren Sie in solchen Fällen testweise die Firewall.
- Falls Sie Ihre VMs zu Snapshots mit unterschiedlichen Zeitpunkten zurückgesetzt haben, können die seltsamsten Effekte auftreten. Kehren Sie bei Problemen einfach zu einem bekanntermaßen funktionierenden Stand zurück.
- Manchmal dauert es einfach einige Minuten, bis neue Einträge im DNS bekannt gemacht werden.
- Überprüfen Sie, ob eventuell veraltete Einträge im DNS vorhanden sind, und löschen Sie diese.

Verwenden Sie stets AD-integriertes DNS. Arbeiten Sie nur dann mit primären und sekundären Zonen, wenn es sich nicht vermeiden lässt. Damit schalten Sie zahlreiche Fehlerquellen und potenzielle Probleme zuverlässig aus.


Schulversion
© HERDT-Verlag

# 10 DHCP – Dynamische IP-Konfiguration

**In diesem Kapitel erfahren Sie**

- wie IP-Adressen aufgebaut sind
- wie das Konzept der dynamischen IP-Adressierung aufgebaut ist
- wie Sie den DHCP-Serverdienst installieren und konfigurieren
- wie DHCP Namenszuordnungen im dynamischen DNS bekannt macht
- wie Sie DHCP-Failover einrichten

**Voraussetzungen**

- DNS und Namensauflösung
- Kenntnisse in der IP-Konfiguration von Windows-Rechnern
- Domänencontroller installieren und neue Domänen erstellen

## 10.1 TCP/IP

Ohne Grundlagenwissen zur IP-Adressierung fällt es schwer, die Funktionsweise von DHCP zu verstehen, daher folgt hier eine kurze Einführung ins Thema.

TCP/IP bezeichnet einen Protocol-Stack (Protokoll-Stapel), eine Ansammlung verschiedener zusammengehöriger Protokolle, die unterschiedliche Aufgaben übernehmen, z. B. TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol).

IP (Internet Protocol) übernimmt dabei die Adressierungsfunktion (Telefonnummer) und kann in den Versionen 4 und 6 genutzt werden. IPv6 ist seit Vista ein fester Bestandteil von Windows und kann für ältere Versionen nachinstalliert werden.

Bei der Konfiguration der Server wird in diesem Buch IPv4 eingesetzt. Im europäischen Raum entspricht das den Gegebenheiten im normalen Geschäftsumfeld. Gründe dafür sind u. a. die höheren Kosten für Router und Layer-3-Switches (Neuanschaffungen), die Notwendigkeit zum Umdenken beim Einsatz von IPv6 und vor allem die noch fehlende Notwendigkeit zur Umstellung (siehe auch den aktuellen Stand diesbezüglich bei den Providern).

### IPv4-Adressen

IPv4-Adressen sind 32 Bit lang und werden aus Gründen der Lesbarkeit in der „**dotted decimal notation**“ dargestellt:

4 Gruppen zu 8 Bit, getrennt durch einen Punkt. Diese 4 Zahlen (Bytes, Oktette) können Werte zwischen 0 und 255 annehmen.

| | |
|---|---|
| IP-Adresse: | 192.168. 24.105 |
| Subnetzmaske: | 255.255.255. 0 |
| Netzwerkadresse: | 192.168. 24. 0 |
| Rechneradresse: | 105 |

Eine IP-Adresse besteht aus zwei Teilen:

- Netzwerkadresse (Netz-ID)
- Rechneradresse (Hostadresse, Host-ID)

Die Subnetzmaske ist ebenfalls 32 Bit lang und legt fest, wie viele Bits der IP-Adresse zur Netz-ID gehören. Sie trennt die Netzwerkadresse von der Rechneradresse und bestimmt so, ob zwei Netzwerkgeräte im selben Teilnetz liegen oder nicht. Binär geschrieben ist eine Subnetzmaske eine Folge von Einsen, die irgendwann umschlägt in eine Folge von Nullen. Die Anzahl an Einsen entspricht den Bits der IP-Adresse, die zur Netzwerkadresse gehören. Die Standard-Subnetzmaske `255.255.255.0` für ein Klasse-C-Netz lässt sich z. B. binär als eine Folge von 24 Einsen darstellen: `11111111.11111111.11111111.00000000`.

### CIDR-Schreibweise

Die Angabe der IP-Adresse und der Netzmaske in der oben beschriebenen Schreibweise ist recht lang, daher wurde mit der CIDR-Notation (Classless Inter-Domain Routing) eine kürzere Schreibweise eingeführt. Hier wird die Anzahl der binären Einsen der Subnetzmaske mit einem Schrägstrich an die IP-Adresse angehängt, im obigen Beispiel wäre das 192.168.24.105/24.

Sobald das letzte Oktett einer IP-Adresse den Wert 0 hat, handelt es sich um einen Adressbereich. Adressbereiche lassen sich noch weiter abkürzen, da alle zusammenhängenden Oktette am Ende der IP-Adresse mit dem Wert 0 weggelassen werden dürfen. So kann z. B. der Adressbereich 128.0.0.0 mit Subnetzmaske 255.255.0.0 auch als 128/16 geschrieben werden.

### Private IPv4-Adressen

Öffentliche, vom Internet aus erreichbare IP-Adressen werden von verschiedenen Gremien verwaltet, die diese Adressen an Internet-Provider weitergeben, die sie dann an die Endkunden verteilen.

Die sogenannten privaten IP-Adressen sind aus diesem Verteilungsverfahren ausgeschlossen, d. h., sie werden im Internet niemals genutzt und sind von dort auch nicht erreichbar.

Für Ihr LAN sollten Sie immer private IP-Adressen aus einem der folgenden Bereiche wählen:

- 10.0.0.0 bis 10.255.255.255 (10.0.0.0/8 bzw. 10/8)
- 172.16.0.0 bis 172.31.255.255 (172.16.0.0/12 bzw. 172.16/12)
- 192.168.0.0 bis 192.168.255.255 (192.168.0.0/16 bzw. 192.168/16)

## IPv6-Adressen

IPv6-Adressen sind 128 Bit lang und werden in der Doppelpunkt-Hexadezimal-Notation geschrieben. Im englischen Sprachraum wird diese Schreibweise weniger umständlich als „colon hex“ bezeichnet. Jeweils 2 Bytes werden zu einem 4-stelligen Block hexadezimaler Zahlen zusammengefasst, die durch einen Doppelpunkt getrennt sind, z. B.:

2001:0db8:85a3:08d3:1319:8a2e:0370:7344

Subnetzmasken gibt es bei IPv6 nicht mehr. Stattdessen wird zur Angabe von Präfixen und Netzwerkbereichen die modernere CIDR-Schreibweise genutzt, die nach dem Schrägstrich die Anzahl der gültigen Netz-Bits angibt.

In Adressen, in denen mehrere Gruppen von Nullen vorkommen, ist es erlaubt, eine Gruppe von Nullen durch aufeinanderfolgende Doppelpunkte zu kürzen. Statt: `2001:0db8:0000:0000:0000:0000:1428:57ab` können Sie einfach `2001:0db8::1428:57ab` schreiben.

Eine Aufteilung in verschiedene Netzwerkklassen, wie man sie aus IPv4 kannte, gibt es in IPv6 nicht mehr. Üblicherweise stellen die ersten 64 Bit die Netzwerk-ID und die letzten 64 Bit die Host-ID dar. Es gibt jedoch, ähnlich wie in IPv4, spezielle Adressen mit Sonderfunktionen:

| | |
|---|---|
| ::/128 | ist eine undefinierte IPv6-Adresse – entspricht der IPv4-Adresse 0.0.0.0 |
| ::1/128 | ist das lokale Interface – entspricht der IPv4-Adresse 127.0.0.1 (localhost) |


© HERDT-Verlag

| | |
|---|---|
| fe80::/10 | sind linklokale Adressen, die im Rahmen einer Autokonfiguration verwendet werden und die nicht geroutet werden sollen |
| ff00/8 | stellen Multicast-Adressen dar |
| 0:0:0:0:0:ffff::/96 | sind sogenannte Mapped IPv6-Adressen. Die letzten 32 Bit enthalten hier die IPv4-Adressen von konvertierten IPv4-Paketen. Auf diese Weise können Router IPv4-Pakete auch durch IPv6-Netzwerke befördern. |
| fc00::/7 | stehen für sogenannte ULA – Unique Local Addresses. Adressen mit dem Präfix **fc** sind global zugewiesene, eindeutige ULAs, während Adressen mit dem Präfix **fd** lokal generierte ULAs anzeigen.<br>Nach dem Präfix folgt eine 40-Bit-Site-ID, die den Standort angibt, gefolgt von 16 Bit für die Subnet-ID. Die letzten 64 Bit sind die Host-ID.<br>Dieses System tritt die Nachfolge der privaten IP-Adressen aus dem IPv4-Bereich an, da es eine unkomplizierte lokale Vergabe von Adressen ermöglicht. Im Gegensatz zum IPv4 wären diese IP-Adressen allerdings aus den öffentlichen Netzwerken ohne NAT-Probleme direkt adressierbar. |

### Netzwerkadresse

Die Netz-ID dient der Lokalisierung eines Rechners. In einer Firma können mehrere Netzwerke vorhanden sein, die sich durch unterschiedliche Netzwerkadressen auszeichnen. Will ein Computer eine Verbindung zu einer anderen Netzwerkadresse aufbauen, muss diese Verbindung über einen Router vermittelt werden. Diese Art der Netzwerk-Segmentierung benötigen Sie spätestens dann, wenn Sie unterschiedliche Standorte über öffentliche IP-Netze zusammenschließen wollen.

Der Router hat dabei die Aufgabe, Datenpakete auf den richtigen Weg zu einer Netzwerkadresse weiterzuleiten. Die dazu benötigten Informationen hält er in einer internen Routing-Tabelle, die angibt, welcher Router-Anschluss zu welchem Ziel-Netz führt. Dazu benötigt der Router Netzwerkkarten in mindestens zwei Netzen. Diese Netze können physikalisch (z. B. Glasfaser, Twisted-Pair-Kabel und Funknetz) unterschiedlich sein.

### Standardgateway

Das Standardgateway ist der Default-Router, den ein PC benutzt, wenn er Datenpakete an Rechner mit einer anderen Netz-ID senden will und über keine Informationen bezüglich der zu benutzenden Wege verfügt.
Am häufigsten wird das Standardgateway die Verbindung zum Internet zur Verfügung stellen.

## 10.2 Vergabe von IP-Adressen

### Identifikation im Netzwerk

Generell werden zur Identifikation eines Rechners im Netzwerk drei Informationen benötigt:

- Die MAC-Adresse ist eine vom Hersteller direkt der Netzwerkkarte zugewiesene, 6 Bytes lange Identifikationsnummer. Rechner mit derselben Netz-ID kommunizieren letztlich über MAC-Adressen miteinander.
- Der MAC-Adresse wird eine IP-Adresse zugeordnet.
- Benutzer können den Rechner auch über einen Namen ansprechen. Dieser wird in die IP-Adresse aufgelöst.

  Windows-Rechner haben eigentlich zwei Namen: einen NetBIOS-Namen, den Sie bei der Installation angeben, und einen Host-Namen, der aus dem NetBIOS-Namen abgeleitet wird. Wenn Sie für Computer-Namen nur englische Buchstaben, Ziffern und den Bindestrich verwenden, sind beide Namen identisch.

### Dynamische IP-Adressierung – DHCP (Dynamic Host Configuration Protocol)

Jeder Computer benötigt eine eindeutige IP-Adresse. Müssen Sie viele Rechner verwalten, dann wird die Verwaltung und Dokumentation der verwendeten IP-Adressen immer aufwendiger. Ein DHCP-Server nimmt Ihnen diese Aufgabe ab. Sie konfigurieren den DHCP-Server mit einem oder mehreren IP-Adressbereichen nebst zusätzlich notwendigen Informationen (z. B. Standardgateway, DNS-Server) und die Clients holen sich ihre IP-Konfiguration vom DHCP-Server. Der DHCP-Client erhält seine IP-Konfiguration üblicherweise beim Hochfahren aus dem Adresspool des DHCP-Servers.

Die Nutzung von DHCP ist die Standard-Einstellung bei einem neu installierten Windows-Rechner. Findet ein DHCP-Client keinen DHCP-Server, nutzt er stattdessen APIPA (Automatic Private IP Addressing). Dabei weist er sich nach einer Überprüfung selbstständig eine freie IP-Adresse aus dem Bereich 169.254.0.0/16 zu.

### Adressierung mit statischer IP-Adresse – manuelle Konfiguration

Die Vergabe einer statischen IP-Adresse ist in erster Linie für Server vorgesehen. Vor allem Rechner, die das Netzwerk an sich begründen oder zentrale Adressierungsfunktionen für das Netzwerk bereitstellen, müssen immer die gleiche IP-Adresse haben.

- Domänencontroller
- DNS-Server
- DHCP-Server

DHCP unterstützt auch sogenannte Reservierungen. Dabei wird einer MAC-Adresse eine IP-Adresse fest zugeordnet. So erhalten Computer dynamisch immer dieselbe IP-Adresse. Reservierungen sind nicht für alle Server-Typen geeignet, beispielsweise darf ein DHCP-Server nicht gleichzeitig DHCP-Client sein.

### DNS-Server

DNS-Server (Domain Name System) sind eine Art automatisches Telefonbuch, das zu einem Host-Namen die passende IP-Adresse liefert. Besonders wichtig wird DNS, wenn die Kommunikation mit dem Internet hergestellt werden soll.

In Windows-Domänen werden wichtige Dienste (z. B. Domänencontroller) über DNS gesucht. Dynamisches DNS ermöglicht es, dass ein Rechner seinen Host-Namen nebst IP-Adresse selbstständig auf dem DNS-Server verwaltet. Sie müssen die Einträge im DNS-Server dann nicht mehr selber pflegen. Bei DHCP-Clients kann diese dynamische Aktualisierung auch der DHCP-Server übernehmen.

### WINS-Server

Der Windows Internet Naming Service ist ein automatisches Telefonbuch für NetBIOS-Namen. Obwohl WINS inzwischen als überholter Dienst zur Namensauflösung gilt, existieren noch erstaunlich viele Anwendungs- und Dienstimplementationen, die zuverlässiger laufen, wenn im Netzwerk auch ein WINS-Server vorhanden ist. Wollen Sie die Netzwerkumgebung im Windows-Explorer in Netzen mit unterschiedlichen Netz-IDs nutzen, kommen Sie an WINS nicht vorbei.

## 10.3 Dynamic Host Configuration Protocol (DHCP)

### Dynamische IP-Konfiguration mit DHCP

Jeder Rechner muss über eine eindeutige IP-Adresse verfügen. Bei manueller Konfiguration steigen Verwaltungsaufwand und Fehleranfälligkeit mit der Anzahl der Clients schnell an. Abhilfe schaffen DHCP-Server, die IP-Konfigurationen (Leases) aus vorkonfigurierten Adressbereichen dynamisch an anfragende Clients verleihen.


Schulversion
© HERDT-Verlag

### Ablauf einer dynamischen Adresszuweisung

Die folgende Darstellung geht von einem Windows DHCP-Client aus, der erstmalig bootet. Zu diesem Zeitpunkt verfügt er noch über keine IP-Konfiguration, der Netzwerkverkehr wird über MAC-Broadcasts abgewickelt.

1. Der DHCP-Client schickt einen **DHCP-Discover**-Broadcast (Entdecken) ins Netz.
2. Alle DHCP-Server, die ein Angebot machen können, antworten mit einer **DHCP-Offer** (Angebot). Diese Offer beinhaltet bereits die IP-Konfiguration.
3. Der Client wählt das erste Angebot und verschickt an diesen DHCP-Server einen **DHCP-Request**. Auch der Request (Anfrage) enthält die IP-Konfiguration.
4. Der Server bestätigt die Anfrage mit einem **DHCP-ACK** (Acknowledgement, Bestätigung).

Die erhaltene IP-Konfiguration ist mit einer **Leasedauer** versehen. Nach Ablauf von 50 % der Leasedauer versucht der Client über einen DHCP-Request, seine Nutzungsfrist wieder auf den vollen Wert zu setzen. Reagiert der DHCP-Server nicht, versucht es der Client in zunehmend kürzeren Abständen erneut. Ist die Lease abgelaufen, muss der Client diese IP-Konfiguration aufgeben. Er startet dann wieder bei 1.

Sollte sich der DHCP-Server in einem anderen IP-Netz befinden als der Client, muss im Netz des Clients ein sogenannter **DHCP-Relay-Agent** vorhanden sein. Dieser nimmt den Broadcast auf, leitet ihn an den DHCP-Server weiter, empfängt die Antwort und gibt sie an den Client zurück. An der IP-Adresse des Relay-Agent erkennt der DHCP-Server auch, welche IP-Adresse der Client benötigt.

DHCP-Relay wird auch als BootP-Relay bezeichnet, denn hier wird dasselbe Verfahren angewendet. Alle RFC-1542-kompatiblen Router beherrschen diese Funktion.

Hat ein Windows-Client bereits einmal eine DHCP-Konfiguration erhalten, so speichert er diese in der Registry und wird beim nächsten Mal direkt mit einem DHCP-Request starten. In folgenden Fällen erhält der Client als Antwort **DHCP-NACK** (Non Acknowledgement):

- ✔ Der DHCP-Server hat die angeforderte IP-Konfiguration inzwischen anderweitig vergeben.
- ✔ Die angeforderte IP-Adresse passt nicht zum Subnetz des Clients.

  Nach einem DHCP-NACK muss der Client wieder bei Schritt 1 beginnen.

## 10.4 DHCP-Server installieren

### Einsatz von DHCP in der Testumgebung

### Aufgabenstellung

In der Testumgebung soll es zwei DHCP-Server geben. Dafür werden *B-DC02* und *B-FS01* ausgewählt. Der DHCP-Bereich soll die IPv4-Adressen 192.168.1.20 bis 192.168.1.254 umfassen, der Bereich von 192.168.1.100 bis 192.168.1.110 soll ausgespart werden. Es wird kein DHCP-Bereich für IPv6 eingerichtet. Da es nur einen Standort mit einem Subnetz gibt, ist die DHCP-Konfiguration in der Testumgebung einfach gehalten. Die beiden Server sollen als Team im DHCP-Failover für Ausfallsicherheit bzw. Lastverteilung sorgen. Komplexere Konstellationen und weitere Informationen zur Funktionsweise von DHCP finden Sie im HERDT-Buch *Windows Server 2019 – Erweiterte Netzwerkadministration*.

- ▶ Fertigen Sie von allen Servern der Testumgebung einen Snapshot an.

Vor der Einrichtung von DHCP müssen Sie sicherstellen, dass Ihre Testumgebung über den internen Switch miteinander verbunden und von außen nicht erreichbar ist. Mehrere unkoordinierte DHCP-Server können zu erheblichen Problemen für die Kursumgebung und das gesamte physische Netzwerk führen.

## Rolle hinzufügen

DHCP können Sie auf jedem Server innerhalb der Domäne installieren, dessen IP-Konfiguration manuell erfolgt ist.

Wählen Sie für die Testumgebung den Server *B-DC02* aus und führen Sie denselben Vorgang anschließend für *B-FS01* durch.

- Klicken Sie im Server-Manager auf *Verwalten - Rollen und Funktionen hinzufügen*.
- Wählen Sie im Assistenten als Installationstyp *Rollenbasiert* und klicken Sie auf *Weiter*.
- Wählen Sie den Server aus und klicken Sie auf *Weiter*.
- Wählen Sie als Serverrolle *DHCP-Server* aus.
- Bestätigen Sie die Installation der benötigten Tools mit *Features hinzufügen* und klicken Sie mehrmals auf *Weiter*, bis die Schaltfläche *Installieren* verfügbar ist.
- Klicken Sie auf der Seite *Bestätigung* auf *Installieren*.

  Die Installation wird durchgeführt.

## DHCP konfigurieren und DHCP-Server autorisieren

Nach dem Hinzufügen der Serverrolle und der dazugehörigen Tools muss DHCP konfiguriert werden. Hierbei wird der DHCP-Server im Active Directory autorisiert, um Konflikte mit anderen DHCP-Servern auszuschließen und festzulegen, welcher DHCP-Server zur Vergabe von Adressen berechtigt ist. Dazu ist die Berechtigung eines Organisations-Admins erforderlich.

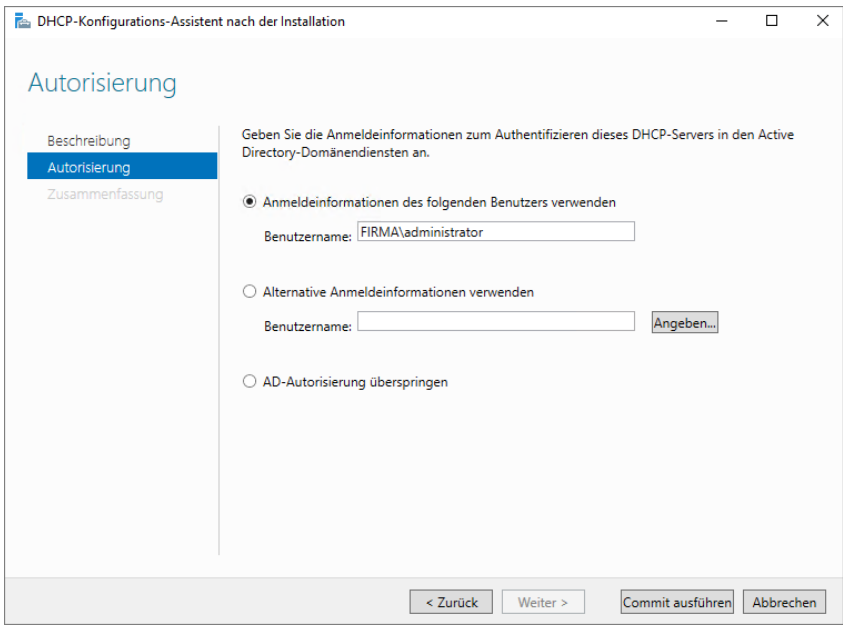
Falls mehrere DHCP-Server in einem Netzwerk vorhanden sind, müssen diese sorgfältig aufeinander abgestimmt sein. Fehlkonfigurationen und unbemerkt eingeschaltete DHCP-Server können schwere Störungen hervorrufen.

- Klicken Sie im Assistenten oder im Menü *Verwalten* auf *DHCP-Server konfigurieren*.

  Der DHCP-Konfigurations-Assistent wird gestartet.
- Klicken Sie auf *Weiter*.

Auf der Seite *Autorisierung* können Sie auswählen, ob Sie für die Autorisierung den aktuellen Benutzer verwenden oder andere Anmeldeinformationen eingeben möchten. In diesem Fall klicken Sie auf *Angeben* und geben Sie die Informationen ein. Sie können die AD-Autorisierung auch überspringen, was jedoch nicht empfehlenswert ist.

- Schließen Sie den Assistenten mit *Commit ausführen* ab. Der DHCP-Server wird nun aktiviert.




*Autorisierung des DHCP-Servers*


Schulversion
© HERDT-Verlag

## 10.5 DHCP-Server konfigurieren

### Überblick

Nach der erfolgreichen Installation und Autorisierung des DHCP-Servers werden alle weiteren Einstellungen in der DHCP-Konsole durchgeführt. Verwenden Sie dafür in der Testumgebung den Server *B-DC02*.

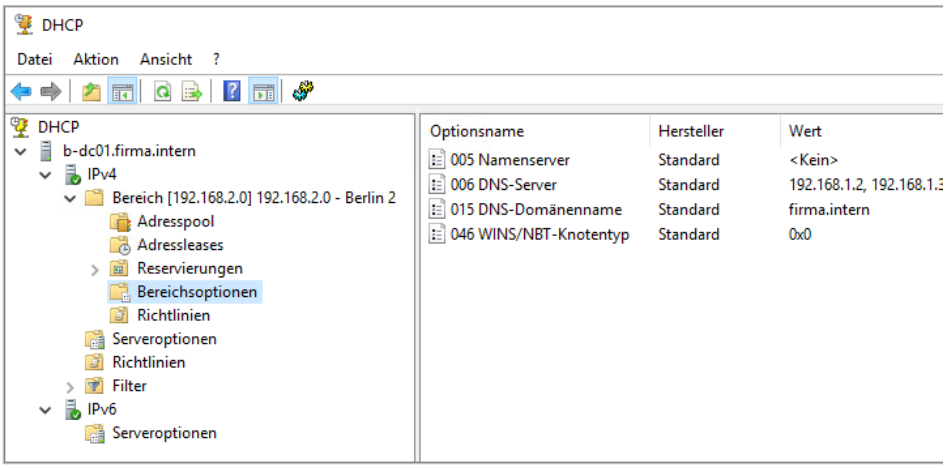
- Geben Sie im Startmenü `dhcpmgmt.msc` ein.
  Alternativ können Sie auch im Server-Manager auf *Tools - DHCP* klicken.

Im Snap-In *DHCP* werden alle Einstellungen für den lokalen Server nach IPv4 und IPv6 getrennt angezeigt. Hier können Sie außerdem weitere DHCP-Server hinzufügen, neue Bereiche erstellen und zahlreiche Optionen, Richtlinien und Filter einstellen. Ohne die DHCP-Bereiche ist DHCP noch nicht aktiv.

Die Abbildung zeigt den Zustand nach Abschluss aller Einstellungen.

Es sind zwei DHCP-Server vorhanden und es wurden die Bereiche *Berlin* und *Berlin2* eingerichtet. Der Bereich *Berlin2* ist verfügbar und aktiv. Auch nicht aktive Bereiche werden angezeigt.

Im Bereich *Berlin 2* wurden die Bereichsoptionen um die Einträge für WINS ergänzt.

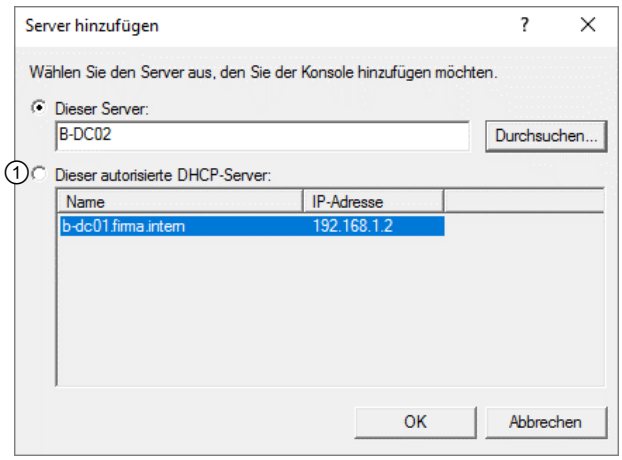



### Weitere DHCP-Server verwalten

#### Server hinzufügen

In Ihrem Firmennetzwerk sollten sich stets mehrere DHCP-Server befinden. Diese werden jedoch nicht automatisch angezeigt, sondern müssen manuell in die Konsole aufgenommen werden.

- Klicken Sie in der linken Spalte der DHCP-Konsole auf den obersten Eintrag *DHCP*.
- Klicken Sie im Menü auf *Aktion - Server hinzufügen*.
- Aktivieren Sie das Optionsfeld ① und wählen Sie alle Server aus, die hinzugefügt werden sollen.
  Fügen Sie in der Testumgebung den Server *B-FS01* hinzu. Dieser wird nicht automatisch angezeigt, da er kein Domänencontroller ist.
  Falls der Server nicht aufgeführt ist, können Sie den Namen des Servers eingeben oder auf *Durchsuchen* klicken, um die erweiterten Suchmöglichkeiten zu nutzen.
- Klicken Sie auf *OK*.



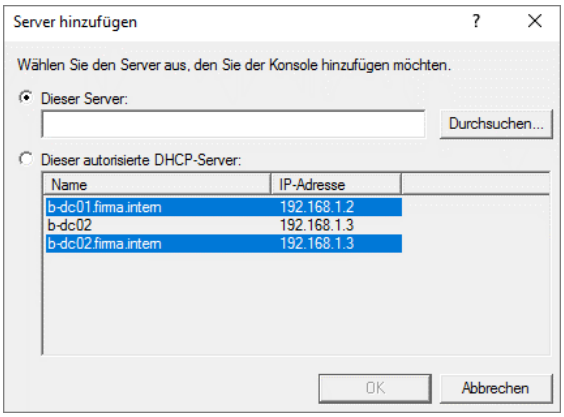

*Hinzufügen weiterer DHCP-Server*

## Server nachträglich autorisieren

Die Autorisierung im AD sollte während der Einrichtung des DHCP-Servers stattfinden, kann aber auch übersprungen und zu einem späteren Zeitpunkt nachgeholt werden. Die folgenden Schritte sind auch für DHCP-Server ohne Microsoft-Betriebssystem geeignet, z. B. für Internetrouter.

- Klicken Sie in der linken Spalte der DHCP-Konsole auf den obersten Eintrag *DHCP*.
- Klicken Sie im Menü auf *Aktion - Autorisierte Server verwalten*.

  Im Dialog werden alle autorisierten Server angezeigt.
- Um weitere DHCP-Server zu autorisieren, klicken Sie auf *Durchsuchen*.
- Geben Sie den Namen oder die IP-Adresse des zu autorisierenden DHCP-Servers ein.
- Falls der Server gefunden wird, bestätigen Sie die Autorisierung mit *OK*.



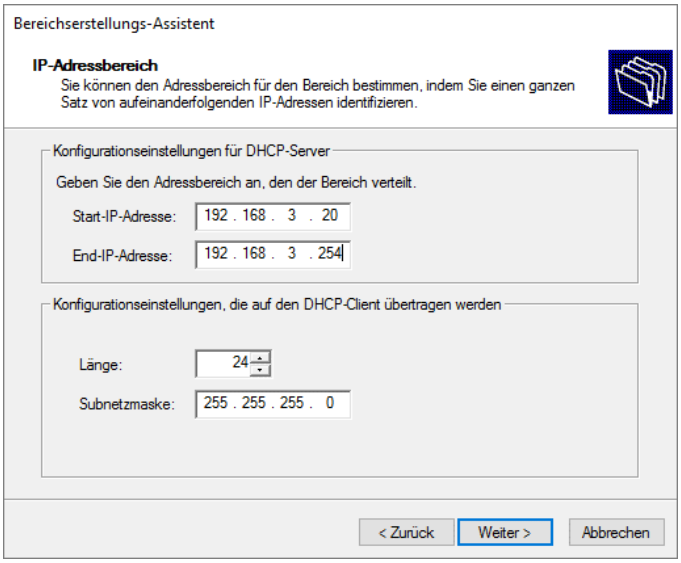

*Hinzufügen weiterer DHCP-Server*

## Neuen IPv4-Bereich erstellen

Welche IP-Adressen ein DHCP-Server vergibt, legen Sie durch die Definition von Bereichen fest. Sie können auf einem DHCP-Server nur einen Bereich je Subnetz erstellen. Die Bereichskonfiguration von IPv4 und IPv6 geschieht auf gleiche Weise, deshalb wird hier nur IPv4 beschrieben. Wählen Sie für die Testumgebung den IP-Bereich von 192.168.1.20 bis 192.168.1.254, Länge 24 und Subnetzmaske 255.255.255.0.

- Erweitern Sie im Snap-In *DHCP* den DHCP-Server und klicken Sie dann mit rechts auf *IPv4*. Wählen Sie im Kontextmenü *Neuer Bereich*.
- Klicken Sie auf der Willkommensseite des Bereichserstellungs-Assistenten auf *Weiter*.
- Geben Sie Bereichsnamen (z. B. `Berlin`) und Beschreibung ein und klicken Sie auf *Weiter*.
- Geben Sie den IP-Adressbereich an, aus dem Adressen vergeben werden.

  Dazu legen Sie die kleinste und größte IP-Adresse fest.
- ✔ Sie können einen Teil des IP-Netzes für statische IP-Adressen (z. B. für Server und Druckgeräte) reservieren. Alternativ geben Sie hier das gesamte IP-Netz an und können später einen oder mehrere Adressbereiche ausschließen.



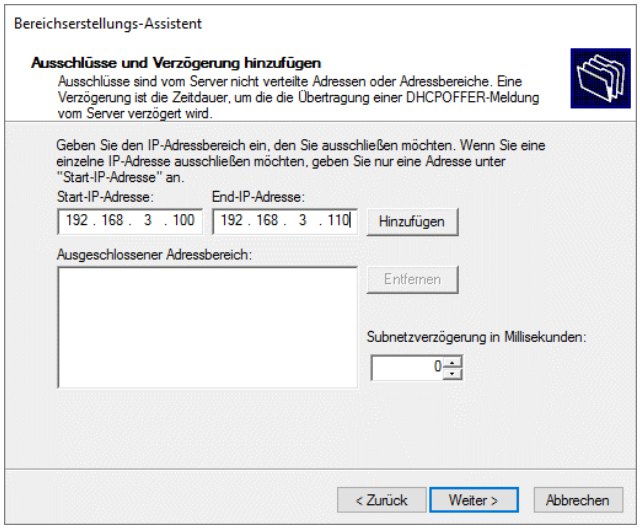

*IP-Adressbereich und Subnetz festlegen*

- ✔ Die Subnetzmaske können Sie entweder durch die Anzahl der gesetzten Bits festlegen oder direkt eingeben. Diesen Wert können Sie später nicht mehr verändern!
- Klicken Sie auf *Weiter*.


Schulversion
© HERDT-Verlag

Auf der nächsten Seite können Sie Ausschlüsse und Verzögerungen hinzufügen und entfernen. Ausschlüsse sind IP-Adressen, die der DHCP-Server nicht vergibt. Diese Adressen können Sie z. B. für die manuelle Konfiguration von Geräten benutzen. Schließen Sie in der Testumgebung den Bereich zwischen 192.168.1.100 und 192.168.1.110 aus.

Über die Subnetzverzögerung legen Sie fest, wie lange der DHCP-Server wartet, bevor er einen Request mit einer DHCP-Offer beantwortet. Das kann sinnvoll sein, wenn dieser DHCP-Server erst antworten soll, wenn der Hauptserver ausgefallen oder überlastet ist. Eleganter lässt sich so etwas allerdings durch DHCP-Failover lösen, das am Ende des Kapitels beschrieben wird.




*Ausschlüsse und Verzögerung festlegen*

- Klicken Sie auf *Weiter*.

Auf der nächsten Seite können Sie die Leasedauer verändern. Die Leasedauer legt fest, wie lange ein Client seine IP-Adresse behalten darf. Windows-Clients geben beim Herunterfahren ihre Lease nicht frei. Mit der Leasedauer legen Sie deshalb fest, wie lange eine IP-Adresse von einem Windows-Client belegt bleibt, bevor sie der DHCP-Server anderweitig vergeben kann. Der Standardwert von 8 Tagen ist brauchbar.

- Stellen Sie die Leasedauer ein und klicken Sie auf *Weiter*.

Der Assistent fragt, ob Sie die DHCP-Optionen konfigurieren wollen, und schlägt *Ja* als Antwort vor. Wenn Sie hier *Nein* wählen, entfallen die nächsten drei Schritte. Tragen Sie für die Testumgebung als Router 192.168.1.1 ein, als Domänennamen *firma.intern* und als DNS-Server 192.168.1.2 und 192.168.1.3. Als WINS-Server können Sie 192.168.1.2 verwenden.

- Fügen Sie die IP-Adresse von mindestens einem Router (Standardgateway) hinzu.
- Legen Sie das primäre DNS-Suffix (den Domänennamen) fest.
  Die DNS-Server können Sie entweder über den FQDN oder die IP-Adresse angeben.
- Geben Sie die zu benutzenden WINS-Server an, entweder als FQDN oder über die IP-Adresse.
- Falls Sie keine weiteren Konfigurationen mehr vorzunehmen haben, aktivieren Sie den Bereich und klicken Sie auf *Weiter*. Klicken Sie andernfalls auf *Nein, diesen Bereich später aktivieren* und *Weiter*.
- Klicken Sie auf der letzten Seite des Assistenten auf *Fertig stellen*.

## Bereichseinstellungen ändern

Sie können bestehende Bereiche nachträglich konfigurieren. Hier können Sie zusätzliche Einstellungen vornehmen, die während der Erstellung nicht verfügbar waren.

- Klicken Sie mit der rechten Maustaste auf den Bereich und wählen Sie *Eigenschaften*.

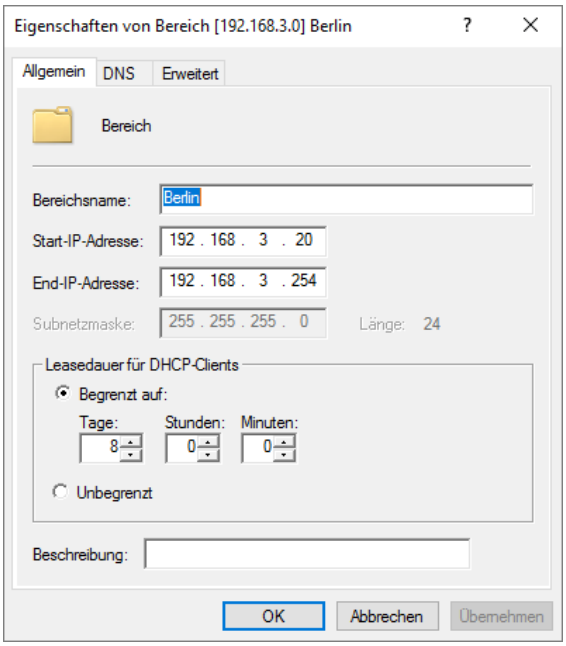
Der Eigenschaftendialog eines Bereichs verfügt über drei Registerkarten, auf denen Sie alle Einstellungen des Bereichs einsehen und ändern können.

## Leasedauer anpassen

Auf der Registerkarte *Allgemein* können Sie den Bereichsnamen, die IP-Adressen und die Leasedauer einstellen. Beachten Sie, dass das Subnetz nachträglich nicht geändert werden kann.

Wichtig wird die Leasedauer, wenn die zur Verfügung stehenden Adressbereiche klein sind (im Verhältnis zur Anzahl der Clients) oder die Rechner häufig ihr Subnetz ändern, z. B. Außendienstmitarbeiter, die ihre Laptops in verschiedenen Filialen anschließen, oder Funknetzbenutzer, die durch verschiedene Funknetzbereiche wandern.

In solchen Fällen können Sie Leasedauern von einigen Stunden in Betracht ziehen. Diese können Sie mit eigenen Geräteklassen und WMI-Filtern so kombinieren, dass mobile Benutzer eine kürzere Lease erhalten als Arbeitsplatzrechner. Beachten Sie, dass eine kürzere Leasedauer beim Ausfall der DHCP-Server entsprechend schneller zu Problemen führt.




*Leasedauer einstellen*

Die Standardleasedauer von 8 Tagen ist in den meisten Fällen brauchbar. Es kann sich aber auch bei stationären Clients lohnen, die Leasedauer deutlich herabzusetzen, etwa auf 12 Stunden. Der Vorteil dabei ist, dass Änderungen, die abends nach der Kernarbeitszeit gemacht wurden, am nächsten Morgen bereits umgesetzt sind. Bei Leasedauern von mehreren Tagen müsste man entsprechend länger warten. Bei einem sauber aufgebauten Netzwerk mit mehr als einem DHCP-Server ergeben sich durch die verkürzte Leasedauer keine Nachteile und die Administration vereinfacht sich enorm.

`ipconfig /release` in einer Eingabeaufforderung auf dem Client sorgt dafür, dass der Client seine DHCP-Lease sofort freigibt.

## Dynamische DNS-Aktualisierungen anpassen

Der DHCP-Server kann beim Vergeben einer Lease entsprechende Einträge im DNS erstellen. Wenn Sie DNS-Einträge ausschließlich für Rechner ab Windows XP benötigen, sollten Sie die Einstellungen im Register *DNS* nicht verändern. Für die Testumgebung müssen Sie hier nichts verändern.

## Weitere Bereichseigenschaften

Im Register *Failover* werden bei eingeschaltetem Failover die aktuellen Einstellungen angezeigt, Sie können hier jedoch keine Einstellungen vornehmen. Im letzten Register *Erweitert* können Sie wählen, ob IP-Adressen an DHCP-Clients, BOOTP-Clients oder beide vergeben werden. Außerdem können Sie hier die Subnetzverzögerung erhöhen, was vor allem bei sekundären DHCP-Servern sinnvoll ist.

## Eigenschaften von IPv4 oder IPv6 anpassen

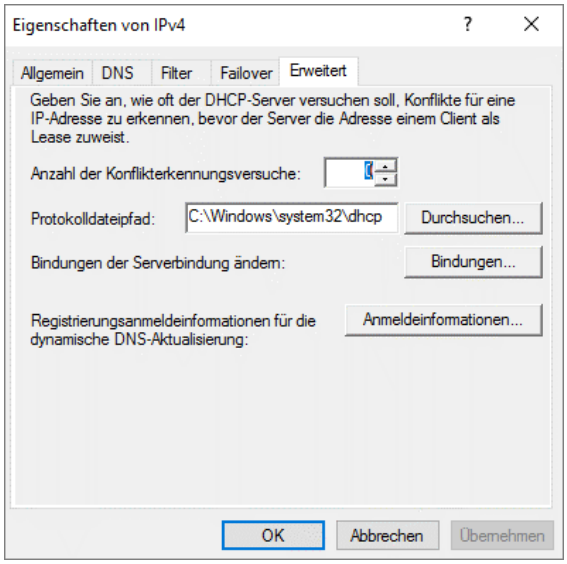
Sie können neben den Einstellungen für den Bereich auch globale Einstellungen für IPv4 bzw. IPv6 vornehmen.

- Klicken Sie mit der rechten Maustaste auf *IPv4* und wählen Sie *Eigenschaften*.


Schulversion
© HERDT-Verlag

Der Eigenschaftendialog verfügt über fünf Registerkarten:

- Im Register *Allgemein* können Sie die automatische Statistikerstellung und die Überwachungsprotokollierung ein- und ausschalten.
- Im Register *DNS* können Sie dieselben Einstellungen vornehmen wie bei den Bereichseigenschaften.
- Im Register *Filter* können Sie bestimmte MAC-Adressen von DHCP aus- oder einschließen.
- Im Register *Failover* können Sie eine bestehende Failover-Partnerschaft konfigurieren oder löschen.
- Im Register *Erweitert* können Sie einstellen, wie oft der DHCP-Server versucht, IP-Adresskonflikte zu erkennen. Außerdem können Sie hier den Pfad zur Protokolldatei oder die Bindungen des Servers an vorhandene Netzwerkadapter ändern und die Anmeldeinformationen für die dynamische DNS-Aktualisierung eintragen.




*Erweiterte Eigenschaften von IPv4 einstellen*

## Serveroptionen und Bereichsoptionen anpassen

Die DHCP-Serveroptionen legen fest, welche IP-Konfiguration der DHCP-Client zusätzlich zur IP-Adresse erhält. Die Einstellungen gelten für alle Bereiche auf diesem Server. Die Serveroptionen finden Sie unter *IPv4* bzw. *IPv6*, während sich die Bereichsoptionen im jeweiligen Bereich befinden. Die Dialoge für beide Optionsarten sind identisch aufgebaut. Die Einstellungen aus den Bereichsoptionen überschreiben den Inhalt der Serveroptionen.

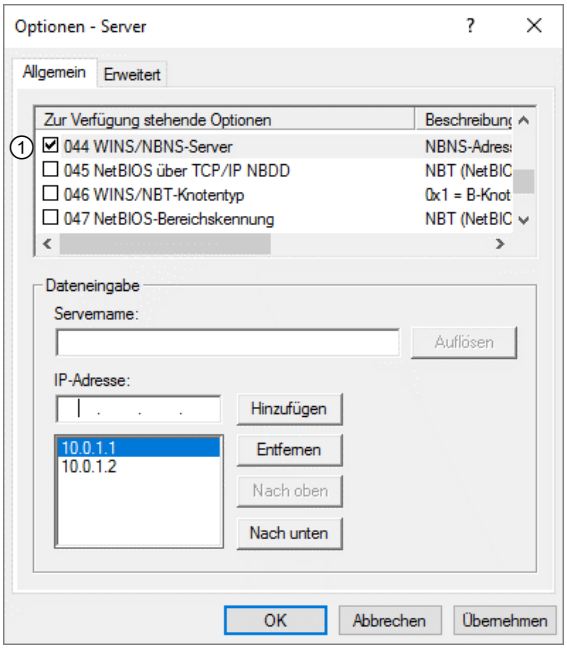
- Um die **Serveroptionen** zu öffnen, klicken Sie mit der rechten Maustaste auf *IPv4* bzw. *IPv6* und wählen Sie *Optionen konfigurieren*.

  *oder* Um die **Bereichsoptionen** zu öffnen, klicken Sie im Kontextmenü eines DHCP-Bereichs auf *Bereichsoptionen* und wählen Sie *Optionen konfigurieren*.

Im Register *Allgemein* werden alle DHCP-Standardoptionen angezeigt, im Register *Erweitert* haben Sie bei der Herstellerklasse die Möglichkeit, zusätzliche Microsoft-Optionen sowie Optionen für Windows 2000 zu aktivieren.

- Aktivieren Sie eine Option ① und geben Sie die Parameter wie z. B. Servername und IP-Adresse ein.

  Die möglichen Eingabewerte unterscheiden sich je nach Option.
- Schließen Sie die Eingabe mit *Übernehmen* und *OK* ab.

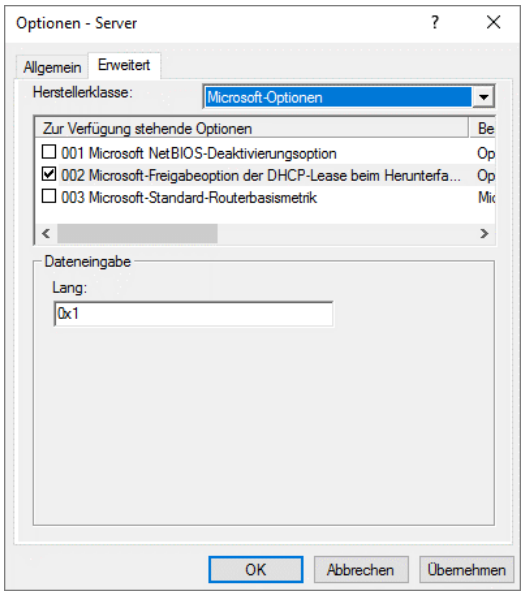



Bei der Eingabe mehrerer IP-Adressen steht die bevorzugte IP-Adresse stets oben. Sie können Einträge hinzufügen oder entfernen. Die Abbildung zeigt die Konfiguration von zwei WINS-Servern. Der primäre WINS-Server steht an erster Stelle in der Liste. Die Reihenfolge ändern Sie mit *Nach oben* und *Nach unten*.

Wenn Sie WINS-Server (Option 044) angeben, müssen Sie auch den WINS/NBT-Knotentyp (Option 046) konfigurieren. Hier sollten Sie als Wert `0x8` eintragen.

## Lease beim Herunterfahren freigeben

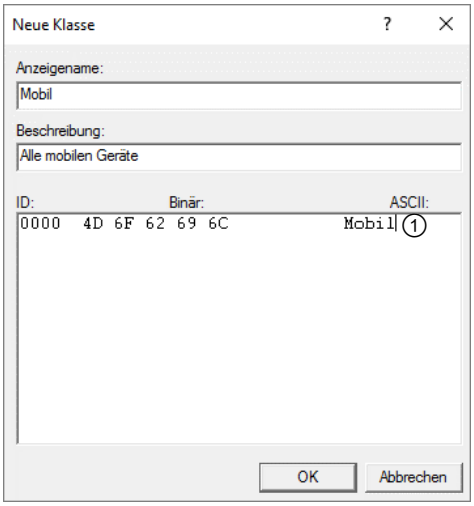
Falls Sie möchten, dass die Clients ihre DHCP-Lease beim Herunterfahren wieder freigeben, wählen Sie die Herstellerklasse *Microsoft-Optionen* und aktivieren Sie die Option *002*.




Bei älteren Microsoft-Server-Versionen wurden in den Dialogen für die Server- und Bereichsoptionen neben den Herstellerklassen auch die Benutzerklassen angezeigt. Diese können Sie jetzt erreichen, indem Sie im Kontextmenü von IPv4 bzw. IPv6 auf *Benutzerklassen definieren* klicken.

## Benutzerklassen erstellen

Benutzerklassen bieten Ihnen die Möglichkeit, DHCP-Clients mit anderen Optionen zu konfigurieren. Vordefiniert ist beispielsweise die Standardrouting- und RAS-Klasse für Clients, die diesen Microsoft-Dienst nutzen. Solche Klassen können Sie auch selbst definieren. Das kann sinnvoll sein, um z. B. mobilen Geräten eine deutlich kürzere DHCP-Leasedauer zuzuweisen als stationären Rechnern. Diese Ein-stellungen können Sie dann mithilfe von WMI-Filtern in Gruppenrichtlinien umsetzen.




- Klicken Sie mit der rechten Maustaste auf *IPv4* und wählen Sie im Kontextmenü *Benutzerklassen definieren*.

  Es öffnet sich ein Fenster, das die vorhandenen Benutzerklassen anzeigt.
- Klicken Sie auf *Hinzufügen*, um eine neue Klasse zu definieren.
- Geben Sie einen Anzeigenamen und eine Beschreibung der Benutzerklasse ein.
- Geben Sie unter *ASCII* ① dieselbe Bezeichnung ein wie unter *Anzeigename* und bestätigen Sie mit *OK*.

Nun können Sie für alle Mitglieder der neuen Benutzerklasse eigene Optionen definieren. Dazu müssen Sie den Client noch in die entsprechende Klasse versetzen.

- Öffnen Sie auf dem Client eine Eingabeaufforderung und geben Sie ein:

  `ipconfig /SetClassID <LAN-Verbindung> <Klasse>`

`LAN-Verbindung` ist die Bezeichnung der Netzwerkverbindung und `Klasse` ist der ASCII-Wert ①.

Mit `ipconfig /SetClassID` entfernen Sie den Client wieder aus der zugewiesenen Klasse.

## Herstellerklassen erstellen

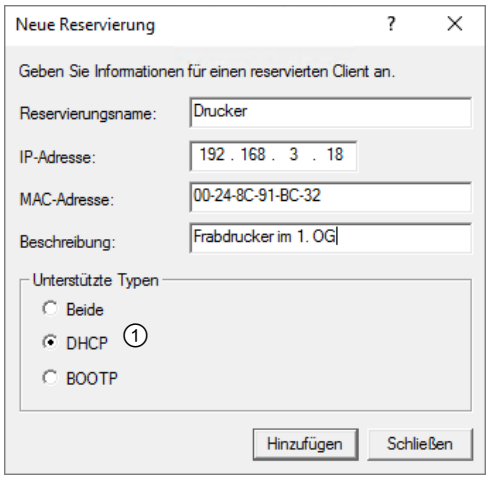
- Klicken Sie mit rechts auf *IPv4* und wählen Sie im Kontextmenü *Herstellerklassen definieren*.

Der weitere Vorgang entspricht dem Hinzufügen von Benutzerklassen.


Schulversion
© HERDT-Verlag

## Reservierungen hinzufügen

Um sicherzustellen, dass bestimmten Clients (z. B. Druckern) immer dieselbe IP-Adresse zugewiesen wird, können Sie eine Reservierung erstellen:




- Erweitern Sie in der Konsolenstruktur den betreffenden DHCP-Bereich.
- Klicken Sie mit der rechten Maustaste auf *Reservierungen* und wählen Sie den Kontextmenübefehl *Neue Reservierung*.
- Legen Sie den Reservierungsnamen fest; der Name des Netzwerkknotens bietet sich dafür an.
- Ergänzen Sie im Feld die IP-Adresse.
- Geben Sie die MAC-Adresse des Clients ein.
- Aktivieren Sie die entsprechende Option ①.

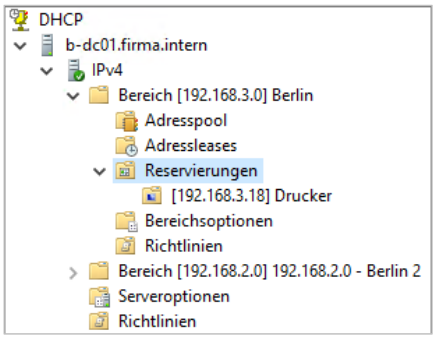
Mit *Hinzufügen* bestätigen Sie die Reservierung und können eine weitere Reservierung eingeben. Mit *Schließen* beenden Sie den Reservierungsvorgang.

Die MAC-Adresse ist auf vielen Netzwerkkomponenten aufgedruckt. Auf einem Windows-Rechner können Sie die MAC-Adressen aller Netzwerkadapter mit `ipconfig /all` auflisten. Sie werden als „physische Adresse“ angezeigt.

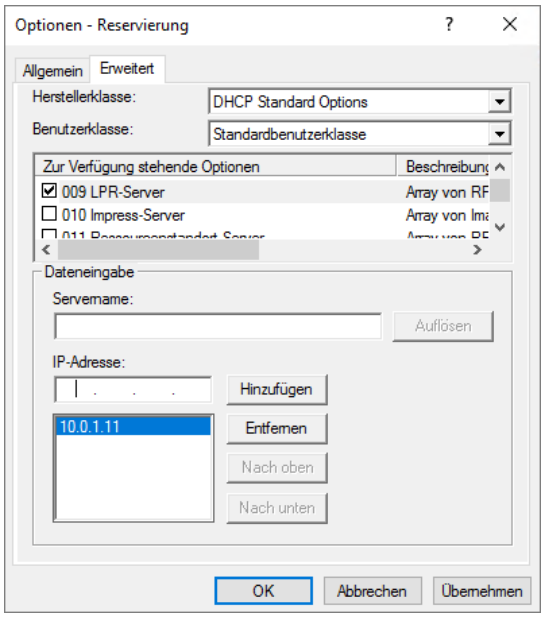
Sie können auch `ping <Netzwerkknoten>` eingeben, um und sich dann die MAC-Adresse mit `arp -a <IP-Adresse>` anzeigen zu lassen.

## Optionen für Reservierung hinzufügen

Sobald Sie eine Reservierung erstellt haben, können Sie dafür spezielle Optionen konfigurieren, die alle Server- und Bereichsoptionen überschreiben.




- Klicken Sie mit der rechten Maustaste auf die Reservierung und wählen Sie *Optionen konfigurieren*.




- Klicken Sie auf das Register *Erweitert* und wählen Sie die Optionen aus.
- Geben Sie die nötigen Daten ein und klicken Sie auf *OK*.

Bei den Optionen für die Reservierung können Sie aus verschiedenen Hersteller- und Benutzerklassen wählen, Sie können jedoch keine selbst erstellten Klassen verwenden.

## DHCP-Failover einrichten

Falls ein DHCP-Client eine neue IP-Konfiguration benötigt und keinen DHCP-Server erreichen kann, gibt er sich über die IP-Autokonfiguration APIPA selbst eine IP-Adresse aus dem Bereich 169.254.y.z. Mit einer solchen IP-Adresse kann er jedoch in der Domäne nicht arbeiten.

Um den Ausfall von Arbeitsstationen durch fehlgeschlagene IP-Konfiguration über DHCP zu vermeiden, muss ständig ein DHCP-Server mit freien Adressen verfügbar sein.

Normalerweise werden dafür im Netzwerk mehrere DHCP-Server eingesetzt. Vor einigen Jahren war die Konfiguration und Koordination der beteiligten DHCP-Server noch aufwendig und schwierig, jetzt verfügen die DHCP-Server über leicht zu verwaltende Funktionen für Redundanz und Lastverteilung.

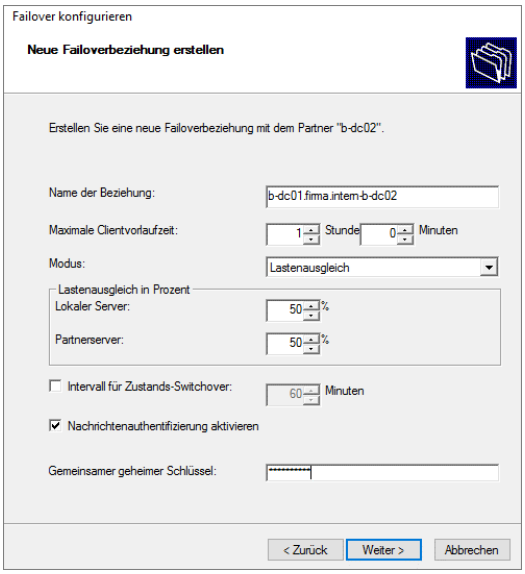
Windows Server 2019 kann mit dem DHCP-Failover die Zusammenarbeit mehrerer DHCP-Server in einem Verbund (Cluster) erheblich vereinfachen. Das Failover sorgt für erhöhte DHCP-Verfügbarkeit, denn falls der DHCP-Server ausfällt, übernimmt sein Partner die Aufgabe. Dieser Modus wird auch als **Hot Standby Mode** bezeichnet. Failover kann außerdem im Modus **Lastenausgleich** (Load Balance) die Belastung variabel auf beide Server verteilen. Durch den regelmäßigen Abgleich aller vergebenen Leases zwischen den Partnern können keine IP-Adressen doppelt vergeben werden. Beide Server merken sich, wann die Leases ablaufen, sodass selbst bei Ausfall und Neustart eines DHCP-Servers alles konsistent bleibt. Wählen Sie für die Testumgebung den Modus *Lastenausgleich* mit gleichmäßiger Verteilung.

- Klicken Sie im Snap-In *DHCP* mit der rechten Maustaste auf *IPv4* und wählen Sie *Failover konfigurieren*.
- Wählen Sie auf der ersten Seite des Assistenten die Bereiche aus, die im Failover enthalten sein sollen, oder übernehmen Sie alle verfügbaren Bereiche (Standard). Klicken Sie auf *Weiter*.
- Geben Sie auf der nächsten Seite den FQDN oder den Namen des Partnerservers ein und klicken Sie auf *Weiter*.

- Wählen Sie für die Failoverbeziehung eine eindeutige Bezeichnung.
- Stellen Sie im Feld *Maximale Clientvorlaufzeit* (Maximum Client Lead Time, MCLT) eine zusätzliche Leasedauer ein, die beim Ausfall eines DHCP-Servers dafür sorgt, dass zwischenzeitlich vergebene Leases nicht erneut vergeben werden können.

  Der Standard ist eine Stunde.
- Wählen Sie bei *Modus* zwischen *Lastenausgleich* (Load Balance) und *Hot Standby* aus.
- Stellen Sie für den Modus *Lastenausgleich* die Last-verteilung ein.

  *oder* Stellen Sie für den Modus *Hot Standby* hier ein, wie viel Prozent der im Bereich vorhandenen IP-Adressen für den Stand-by-Server reserviert werden sollen (nicht abgebildet).




- Aktivieren Sie bei Bedarf die Option *Intervall für Zustands-Switchover* (Auto State Switchover Interval) und stellen Sie ein, wie viel Zeit nach dem letzten Lebenszeichen verstreichen darf, bevor ein DHCP-Server annimmt, dass sein Partner ausgefallen ist.
- Aktivieren Sie bei Bedarf die Nachrichtenauthentifizierung und geben Sie einen geheimen Schlüssel ein, durch den sich die Partnerserver gegenseitig identifizieren können.
- Klicken Sie auf *Weiter* und auf der folgenden Seite auf *Fertig stellen*.

Das Failover wird nun eingerichtet und Sie werden über den Fortschritt informiert. Nach Abschluss des Vorgangs erhalten Sie die Meldung, dass das Failover erfolgreich konfiguriert wurde.


Schulversion
© HERDT-Verlag

# 11 Physische Struktur von Active Directory

**In diesem Kapitel erfahren Sie**

- Grundlagen zu Active Directory-Standorten
- wie die Replikation innerhalb eines Standorts und zwischen Standorten verläuft
- wie die Geschwindigkeit der Datenübertragung die Replikation beeinflusst
- wie eine Replikationstopologie die schnellen und langsamen Datenübertragungswege der Active Directory-Replikation beschreibt

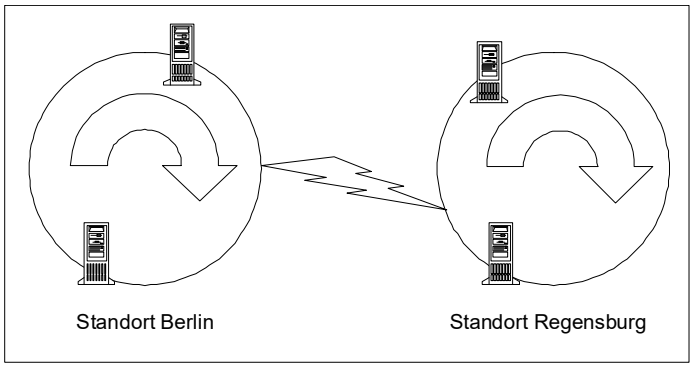
**Voraussetzungen**

- Konzepte von Active Directory
- Grundlagen der IP-Subnetzadressierung

## 11.1 Standorte und Standortplanung

### Standorte

Ein Standort ist eine Ansammlung von Computern, die alle über schnelle und zuverlässige Datenübertragungswege miteinander in Verbindung stehen. Die Datenübertragung innerhalb eines Standorts erfolgt zuverlässig und mit hoher Geschwindigkeit. Als Hochgeschwindigkeit ist eine Datenübertragungsrate von mindestens 500 Kbit/s (Kilobit/Sekunde) definiert. Für die Datenübertragung zwischen Standorten werden oft langsame Verbindungen verwendet, z. B. WAN-Verbindungen mit 128 Kbit/s.




- Ein Standort entspricht in den meisten Fällen einem LAN.
- Ein Standort umfasst ein IP-Subnetz oder mehrere IP-Subnetze.
- Ein Standort umfasst immer ganze IP-Subnetze. Das heißt, ein IP-Subnetz kann nur an einem einzigen Standort vorkommen.

Falls Sie mehrere IP-Subnetze an einem Standort haben, muss die Datenübertragung zwischen den IP-Subnetzen ebenfalls mit hoher Geschwindigkeit erfolgen, um die Subnetze zu einem Standort zusammenfassen zu können.

Durch das Definieren von Standorten haben Sie die Möglichkeit, die Datenübertragungswege gemäß ihrer Geschwindigkeit, Kosten und Zuverlässigkeit einzustufen. Dabei weisen Sie den bevorzugten Verbindungen einen niedrigen Kostenwert zu und den langsamen, teuren und unzuverlässigen Verbindungen hohe Kosten. So können Sie eine Replikationstopologie konfigurieren, die vorhandene Datenübertragungswege optimal ausnutzt und stets den günstigsten Weg durch das Firmennetzwerk verwendet. Zur Einrichtung von Standorten und zur Erstellung einer Replikationstopologie benötigen Sie die Berechtigungen eines Organisationsadministrators.

Die Testumgebung in diesem Buch verfügt zwar nur über einen Standort, dennoch sind Kenntnisse über Standorte und Replikation unverzichtbar. Im HERDT-Buch *Windows Server 2019 – Erweiterte Netzwerkadministration* wird eine Testumgebung mit mehreren Standorten eingerichtet, bei der Sie die hier erworbenen Kenntnisse einsetzen können.

### Planungsfaktoren

Neben Geschwindigkeiten spielen vor allem Kosten eine Rolle, wenn es um die Planung von Standorten geht. Aktuelle Übertragungsgeschwindigkeiten werden in aller Regel auch bei standortübergreifendem Verkehr über 500 Kbit/s betragen. Aber die Kosten für WAN-Strecken sind immer noch erheblich höher als innerhalb eines LANs. Daher sollte die standortübergreifende Replikation minimiert werden, um Bandbreite für andere Daten vorzuhalten.

### Der erste Standort in einer Gesamtstruktur

Wenn Sie den ersten Domänencontroller in einer neuen Gesamtstruktur erstellen, wird gleichzeitig eine physische Struktur erstellt. Sie umfasst einen einzigen Standort mit dem Namen *Default-First-Site-Name*. Der erste und alle weiteren Domänencontroller werden standardmäßig diesem Standort zugeordnet. Dieser Standort umfasst am Anfang damit auch alle IP-Subnetze, ohne dass diese definiert werden müssen.

### Ziele beim Einrichten von Standorten

- Lokale Dienste sollen z. B. für die Anmeldung und Abfragen des globalen Katalogs bevorzugt werden.
- Durch Berücksichtigung langsamer Verbindungen soll der Replikationsverkehr optimiert werden.
- Jeder Benutzer soll stets über die schnellste und kostengünstigste Verbindung mit einem Domänencontroller verbunden werden.
- Abfragen an einen Server des globalen Katalogs sollen möglichst über eine schnelle und kostengünstige Verbindung erfolgen.

### Standorte und der Namespace

Standorte tauchen im Namespace der Active Directory-Verzeichnisdienste nicht auf. Es besteht keinerlei Zusammenhang zwischen Standorten und dem Namespace.

Ein Benutzer findet ein Objekt, z. B. einen bestimmten Drucker, indem er in einer Domäne oder einer Organisationseinheit nach dem Drucker sucht („Der Drucker gehört zur Domäne *Firma*“ bzw. „Der Drucker gehört zur Organisationseinheit *Verwaltung*“). Er kann den Drucker nicht anhand der Tatsache „Der Drucker steht in *Köln*“ finden.

Sollen Drucker auch über ihre Standortzugehörigkeit gefunden werden können (was durchaus sinnvoll ist), so müssen die entsprechenden Eigenschaften der Druckerobjekte konfiguriert werden. Dann ist eine Suche nach Druckerobjekten über den Namen des ausgewählten Standortattributs möglich.

### Standort und Domäne

Es gibt keinen direkten Zusammenhang zwischen Standorten und Domänen.

- Eine Firma mit nur einer Domäne kann an mehreren Standorten präsent sein.
- An einem Standort können mehrere Domänen vorhanden sein.

Daraus ergibt sich, dass die Standorte domänenübergreifend definiert werden. Standorte können daher nur von Organisationsadministratoren eingerichtet und verändert werden.

## 11.2 Replikation innerhalb eines Standorts

### Häufige Replikation

Innerhalb eines Standorts erfolgt die Replikation zwischen Domänencontrollern automatisch und mit relativ hoher Frequenz. Mindestens einmal pro Stunde wird repliziert, selbst wenn es zwischendurch keine Änderungen am AD-Verzeichnis gegeben hat.


Schulversion
© HERDT-Verlag

Dieses Intervall lässt sich für einen Standort (NTDS Site Settings) oder eine einzelne Replikationsverknüpfung anpassen. Das Replikationsintervall kann gewählt werden zwischen: *keine Replikation*, *einmal pro Stunde*, *zweimal pro Stunde* oder *viermal pro Stunde*.

Die standortinterne Replikation findet immer über das schnelle synchrone RPC-over-IP statt. Dabei wird ein entfernter Funktionsaufruf (Remote Procedure Call, RPC) über eine TCP/IP-Verbindung transportiert. Dem schnellen synchronen Modus steht der langsame synchrone Punkt-zu-Punkt-Modus gegenüber, der für die Replikation zwischen verschiedenen Standorten verwendet wird.

### Änderungsbenachrichtigungen

Innerhalb eines Standorts benachrichtigen Domänencontroller ihre Replikationspartner über eine Änderung nach 15 Sekunden und leiten so einen Replikationszyklus ein. Diese Verzögerung sorgt dafür, dass auf weitere Änderungen, die direkt im Anschluss durchgeführt werden, gewartet wird, bevor eine Replikation erfolgt. Damit werden Replikationen im Sekundentakt vermieden.

### Dringende Replikation

Besonders kritische Änderungen im Active Directory werden sofort repliziert. Dabei wird das gleiche Übertragungsverfahren wie bei den Änderungsbenachrichtigungen verwendet, es gibt jedoch keine 15 Sekunden Wartezeit. Eine dringende Replikation wird ausgelöst durch:

- Benutzerkontosperrungen, z. B. nach mehrmaliger Eingabe eines falschen Kennworts;
- Bearbeitung der Kontosperrungsrichtlinie;
- Bearbeitung der domänenweiten Kennwortrichtlinie;
- Änderungen am RID-Master, z. B. das Verschieben der FSMO-Rolle auf einen anderen DC;
- Änderung eines LSA-Schlüssels (Local Security Authority, lokale Sicherheitsautorität), z. B. bei Kennwortänderung eines DC-Computerkontos.

### Weitergabe von Kennwortänderungen

Kennwortänderungen von Domänenbenutzern werden nicht nur über die normale Replikation an jeden DC in der Domäne weitergegeben, hier wird ein weiterer Mechanismus eingesetzt:

Der DC, auf dem die Kennwortänderung erfolgt, teilt diese umgehend dem PDC-Emulator (PDC = Primary Domain Controller) mit. Dazu verwendet er einen sicheren Kanal über eine RPC-over-IP-Verbindung wie bei allen standortinternen Replikationen. Kann der DC den PDC-Emulator nicht erreichen, wird eine Kennwortänderung mit einer Fehlermeldung verweigert.

Wenn nun der Benutzer vor der nächsten Replikation versucht, sich an einem DC an einem anderen Standort zu authentifizieren, erkennt der DC ein unbekanntes Kennwort und fragt beim PDC-Emulator nach, ob zwischenzeitlich eine Kennwortänderung stattgefunden hat.

Bis zur nächsten turnusmäßigen Replikation kann der Benutzer sich noch mit seinem alten Kennwort anmelden, da dann der DC das Passwort akzeptiert, ohne den PDC-Emulator zu fragen.

## 11.3 Replikation zwischen Standorten

### Seltene Replikation

Die Replikation zwischen Domänencontrollern an unterschiedlichen Standorten erfolgt nicht mit derselben Häufigkeit wie innerhalb eines LANs. Bei langsamen oder teuren WAN-Verbindungen besteht die Notwendigkeit, Kosten und Netzwerklast zu minimieren und die Replikation auf Zeiten zu verlegen, in denen die Verbindungen kostengünstiger sind. Standardmäßig findet alle drei Stunden (180 Minuten) eine standortübergreifende Replikation statt. Sie können diesen Wert über die Eigenschaften der Verbindung im Attribut-Editor verändern. Es kann in der Praxis durchaus sinnvoll sein, den Wert z. B. auf 60 oder sogar 30 Minuten herabzusetzen.

### Keine Änderungsbenachrichtigungen zwischen Standorten

Standardmäßig ist die Änderungsbenachrichtigung (und damit auch die dringende Replikation) zwischen Standorten deaktiviert, sie kann jedoch auch standortübergreifend aktiviert werden. Dies ist über den ADSI-Editor möglich und soll hier nicht erläutert werden, da es sich um einen schwerwiegenden Eingriff in die Funktionsweise des Active Directory handelt und nur in seltenen Fällen Vorteile bietet.

## 11.4 Replikationskomponenten

### Konsistenzprüfung

Die Konsistenzprüfung KCC (Knowledge Consistency Checker) läuft als Dienst auf allen Domänencontrollern. Sie erstellt eine Replikationstopologie für die Active Directory-Replikation, indem sie Replikationspfade einrichtet. In bestimmten Zeitintervallen prüft die Konsistenzprüfung die vorhandenen Pfade und erstellt gegebenenfalls neue Pfade, wenn keine Datenübertragung möglich ist. Auf diese Weise wird sichergestellt, dass die Replikationstopologie jederzeit intakt ist und die aktuellen Verzeichnisdaten überall im Netzwerk vorhanden sind.

Sie können die Replikation beeinflussen, indem Sie Standorte erstellen und die Wege zwischen den Standorten mit individuellen Kosten belegen. Das System wird stets versuchen, den Weg mit den niedrigsten Kosten zu verwenden. So können Sie die Replikation gezielt den Erfordernissen anpassen. Wie das geht, wird im HERDT-Buch *Windows Server 2019 – Erweiterte Netzwerkadministration* beschrieben.

### Serverobjekt

Jeder Domänencontroller wird anhand eines Computerobjekts und anhand eines Serverobjekts repräsentiert. Das Computerobjekt repräsentiert den Domänencontroller im Active Directory-Verzeichnis und entspricht der Position des Domänencontrollers in der logischen Struktur innerhalb des Verzeichnisses.

Das Serverobjekt dagegen bezieht sich auf die Rolle des Domänencontrollers in der physischen Struktur, also seine Zugehörigkeit zu einem Standort und seine Stellung innerhalb der Replikationstopologie.

### NTDS-Settings

Dieser Container gehört zum jeweiligen Serverobjekt. Er enthält alle Verbindungsobjekte des Serverobjekts.

### Verbindungsobjekt

Ein Verbindungsobjekt ist ein unidirektionaler Replikationspfad zwischen zwei Serverobjekten. Es gehört zum Serverobjekt, das Daten erhält, und nennt das Serverobjekt, das als Quelle der Verzeichnisinformationen dient.

### Standortverknüpfung

Dieses Objekt repräsentiert einen Replikationspfad zwischen zwei Standorten. Es enthält …

- einen Wert für die Kosten der Verbindung (ein Zahlenwert zwischen 1 und 32767, Standard ist 100),
- eine Intervalleinstellung (Häufigkeit der Replikation in Minuten; Standard ist 180 min, mindestens 15 min, höchstens 10.080 min = eine Woche),
- einen Zeitplan (Wochentage und Tageszeiten, in denen Replikation erfolgen kann).

### Standortverknüpfungsbrücke

Dieses Objekt verbindet Standortverknüpfungen, die das gleiche Protokoll verwenden.

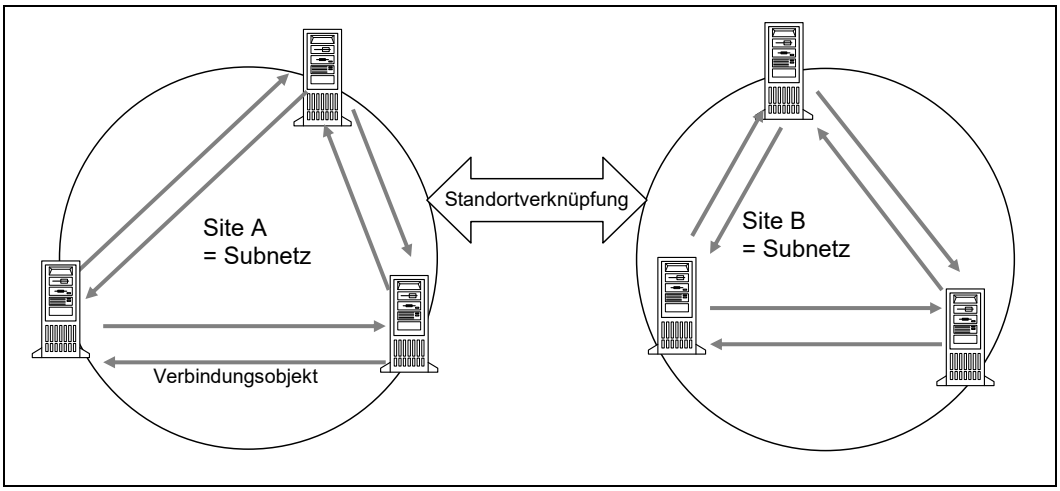
Standortverknüpfungsbrücken müssen Sie in einem Netzwerk, das durchgängig geroutet ist, nicht erstellen, denn Standortverknüpfungen gelten als transitiv. Dann gehören alle Standortverknüpfungen zu einer einzigen Standortverknüpfungsbrücke, die vom System selbst erstellt wird. Solange Sie nicht diesen Automatismus deaktivieren, müssen Sie keine Standortverknüpfungsbrücken errichten.


Schulversion
© HERDT-Verlag

Beispiele und Vorgehensweisen zu manuell erstellten Standorten und Standortverknüpfungsbrücken entnehmen Sie bitte dem Buch *Windows Server 2019 – Erweiterte Netzwerkadministration* sowie weiterführenden HERDT-Büchern zu Active Directory.

## 11.5 Replikationstopologie

### Replikationstopologie für ein Netzwerk mit zwei Standorten




### Zusammenfassung

| | Replikation innerhalb eines Standorts | Replikation zwischen Standorten |
|---|---|---|
| AD-Objekt | Verbindungsobjekt | Standortverknüpfung |
| Geschwindigkeit, Verfügbarkeit | Hohe Geschwindigkeit, hohe Verfügbarkeit | Langsame Verbindung, zeitweise verfügbar |
| Häufigkeit der Replikation | In der Regel stündlich;<br>nach 15 Sekunden, falls eine Änderung am AD-Verzeichnis vorgenommen wird | Durch den Administrator zu definieren,<br>Standard ist 180 Minuten |
| Kritische Änderung | Dringende (quasi sofortige) Replikation | Nur turnusmäßige Replikation |
| Protokoll | Schneller Remote Procedure Call auf IP-Basis (High Speed RPC over IP) | Langsamer Remote Procedure Call auf IP-Basis (Low Speed RPC over IP) oder SMTP.<br>Beim langsamen RPC over IP werden die Replikationsdaten vor dem Versenden komprimiert.<br>Das Simple Mail Transfer Protocol (SMTP) kommt nur für besondere Konstellationen infrage. |
| Erstellung, Überprüfung, Aufrechterhaltung | Automatisch | Durch den Administrator |

# 12 Active Directory-Objekte verwalten

**In diesem Kapitel erfahren Sie**

- wie Sie Organisationseinheiten erstellen
- wie Sie eine logische Hierarchie mit Organisationseinheiten aufbauen
- wie Sie Benutzerkonten erstellen
- wie Sie Computerkonten erstellen
- wie Sie Benutzer und Computerobjekte in Organisationseinheiten organisieren

**Voraussetzungen**

- Active Directory installieren
- Active Directory-Objekte

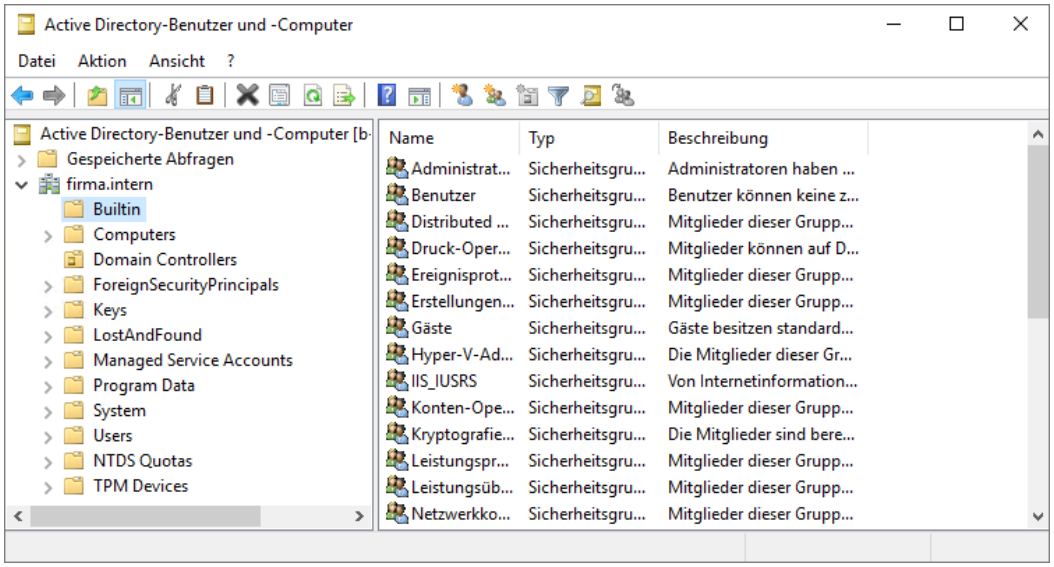
## 12.1 Container der Domäne erkunden

### Aufgabenstellung

Erkunden Sie, welche Container und Objekte nach der Erstellung der Domäne standardmäßig vorhanden sind. Für diesen Zweck ist das Snap-In *Active Directory-Benutzer und -Computer* gut geeignet.

### Snap-In *Active Directory-Benutzer und -Computer* aufrufen

- Melden Sie sich als Domänenadministrator (Domäne *firma*) an.
- Geben Sie Suchfeld des Startmenüs „dsa.msc“ ein und klicken Sie auf *Active Directory-Benutzer und -Computer*.
- Aktivieren Sie im Menü *Ansicht - Erweiterte Features*.




*Snap-In „Active Directory-Benutzer und -Computer“*


Schulversion
© HERDT-Verlag

## Vordefinierte Container in einer Domäne

- ***Builtin***: Der Inhalt entspricht am ehesten den Gruppen, die Sie auf einem Mitgliedsserver oder Client finden und dort über das Snap-In *Lokale Benutzer und Gruppen* bearbeiten können. Zur Gruppe *Administratoren* gehören der ursprünglich lokale Administrator des Servers sowie die Gruppen *Domänen-Admins* und *Organisations-Admins*. Nur in der Gesamtstruktur-Stammdomäne existiert die Gruppe *Erstellung eingehender Gesamtstrukturvertrauensstellungen*.
- ***Computers***: Hier befinden sich alle Computerkonten, die beim Hinzufügen eines Rechners zur Domäne automatisch erstellt wurden.
- ***Domain Controllers***: Alle Domänencontroller dieser Domäne, dies ist die einzige standardmäßig eingerichtete Organisationseinheit. Sie sollten die Einstellungen oder den Inhalt dieser OU nicht verändern.
- ***ForeignSecurityPrincipals***: Container für SIDs vertrauter Domänen einer anderen Gesamtstruktur.
- ***LostAndFound***: Hier werden alle AD-Objekte aufbewahrt, die nicht zugeordnet werden können. Dies können z. B. Objekte sein, die in eine bereits gelöschte OU verschoben wurden, was jedoch noch nicht im AD repliziert wurde. In der Praxis wird dieser Mechanismus selten benötigt.
- ***Managed Service Accounts***: Ab Windows-Server-2008-R2-Domänen können hier Dienste-Konten (z. B. für Exchange-, SQL- oder Internet Information Server) und virtuelle Konten einfacher verwaltet werden. Die Verwaltung erfolgt ausschließlich über die PowerShell.
- ***Selbst erstellte OUs***: An dieser Stelle erscheinen alle Organisationseinheiten, die innerhalb der Domäne erstellt wurden. Sie bilden die logische Struktur des Active Directory.
- ***Program Data***: Container, in dem Anwendungen ihre Daten im AD speichern können.
- ***System***: Bei der Installation von Microsoft-Applikationen werden hier Informationen abgelegt.
- ***Users***: Benutzer- und Gruppenkonten der Windows-Domäne. Das Gastkonto ist standardmäßig deaktiviert. Benutzerkonten, die über die Kommandozeile ohne Angabe einer Ziel-OU erstellt wurden, sind hier gespeichert. In der Gesamtstruktur-Stammdomäne liegen hier die Gruppen *Organisations-Admins* und *Schema-Admins*.
- ***NTDS Quotas***: Werden auch als Active Directory-Kontingente bezeichnet. Mit den Quotas lässt sich festlegen, wie viele Objekte in einer Active Directory-Domäne ein Benutzer erstellen bzw. besitzen darf. Auf diese Weise kann z. B. ein normaler Benutzer ohne Admin-Rechte in die Lage versetzt werden, eigenverantwortlich Benutzer in einer OU hinzuzufügen. Für die Verwaltung von NTDS Quotas müssen Sie die Tools *DSAdd*, *DSMod* und *DSQuery* verwenden.
- ***TPM Devices***: Seit Windows Server 2012 neu eingeführter Container, der die Wiederherstellungsinformationen für TPM-Geräte (Trusted Platform Module) enthält.

Verwenden Sie stets die erweiterte Ansicht von *Active Directory-Benutzer und -Computer,* denn nur so erreichen Sie alle verfügbaren Objekte und Optionen. In den Eigenschaftendialogen der einzelnen Objekte erscheinen dann zusätzliche Registerkarten, auf denen Sie weitere Einstellungen vornehmen können und mehr Informationen erhalten. Im Active Directory-Verwaltungscenter ist dieser Schritt nicht notwendig.

Beachten Sie die unterschiedlichen Symbole von *Computers* und *Domain Controllers*. Nur *Domain Controllers* ist eine Organisationseinheit, und nur OUs können mit Gruppenrichtlinien verknüpft werden oder zum Zuweisen von Verwaltungsaufgaben dienen!

## 12.2 Planung einer Domäne

### Vorüberlegungen

Die Organisation einer Firmenumgebung basiert in erster Linie darauf, vorhandene Abläufe und Strukturen zu virtualisieren. Daneben müssen IT-spezifische Aufgaben in die Planung integriert werden.

### Standorte abbilden

Häufig werden Organisationseinheiten (Organisational Units, OUs) verwendet, um Standorte abzubilden. Dies bezeichnet man als den geografischen Ansatz in der OU-Strukturierung. Gründe dafür können vielfältig sein; die häufigsten sind in der folgenden Tabelle zusammengefasst:

| | |
|---|---|
| Lokaler Datenverkehr | Indem Gruppenrichtlinien an standortbezogene OUs gebunden werden, ist es möglich, in Pfaden auf lokale Ressourcen zu verweisen. So können etwa für die Softwareverteilung oder für Ordnerumleitungen und Updates WAN-Verbindungen geschont und Anmeldevorgänge beschleunigt werden. |
| Dezentrale Administration | Mit OUs kann die Verantwortung für bestimmte Unternehmensbereiche auf Standortebene delegiert werden, ohne deshalb zusätzliche Domänen einrichten zu müssen oder Benutzern administrative Berechtigungen an anderen Standorten zu gewähren. |
| Verstecken von Objekten | Durch die Vergabe von Berechtigungen auf OU-Ebene ist es möglich, den Benutzern nur die Ressourcen am Standort anzuzeigen. So kann z. B. verhindert werden, dass einem Benutzer bei der Suche Drucker angezeigt werden, die sich an anderen Standorten befinden. |
| Übersichtlichkeit | Indem Benutzer und Computer einem Standort zugeordnet werden, kann auch die geografische Lage des Unternehmens dargestellt werden. Je größer eine Domäne wird, desto schwieriger wird es andernfalls, noch effektiv nach Objekten zu suchen. |
| Standortspezifische Rechte | Wenn an bestimmten Standorten Benutzer besondere Einschränkungen von Rechten erhalten sollen, bietet es sich an, Gruppenrichtlinien an OUs zu koppeln. So können etwa unterschiedliche rechtliche Bestimmungen berücksichtigt werden. Ein Beispiel hierfür wäre die Verschlüsselung von Datenverkehr, die mancherorts bestimmte Schlüsselstärken nicht übersteigen darf. |
| Sprachliche oder lizenzrechtliche Besonderheiten | Unter Umständen sollen an bestimmten Standorten besondere Versionen von Programmen eingesetzt werden. Auch dazu ließen sich standortbezogene Richtlinien an passende OUs koppeln. |

### Abteilungen abbilden

In einem administrativen OU-Modell werden Abteilungen durch sie repräsentierende OUs dargestellt. Dies bezeichnet man als den administrativen Ansatz in der OU-Strukturierung. Beispiele und mögliche Gründe dafür können Sie der Tabelle entnehmen:

| | |
|---|---|
| Abteilungsspezifische Verwaltungsaufgaben | In manchen Unternehmen arbeiten Abteilungen relativ autark, z. B ist eine Personalabteilung für die Einstellung von Mitarbeitern zuständig. Hier können Sie das Recht zum Verwalten von Benutzerkonten entsprechend unterwiesenen Fachkräften der Abteilung zuweisen, um die zentrale Verwaltung zu entlasten.<br>Ein weiteres typisches Beispiel ist das Zurücksetzen von Kennwörtern. Die Abteilungsleiter kennen ihre Mitarbeiter in aller Regel und sind dafür besser geeignet als ein Domänenadministrator aus dem Rechenzentrum. Dieser kann gar nicht beurteilen, ob der Mitarbeiter wirklich derjenige ist, der er zu sein vorgibt. So lassen sich unnötige Verzögerungen in der Anmeldung des Benutzers vermeiden und zusätzlich wird die Sicherheit erhöht. |


Schulversion
© HERDT-Verlag

| | |
|---|---|
| Abteilungsspezifische Software einsetzen | Wenn in bestimmten Abteilungen besondere Programme verwendet werden sollen, bietet sich deren Installation über abteilungsspezifische Gruppenrichtlinien an. |
| Spezifische Rechte | In manchen Abteilungen werden oft weiter reichende Rechte benötigt als in anderen. So müssen etwa in einer Grafikabteilung die Benutzer große Dateien lokal speichern. In der Personalabteilung kann der Datenzugriff auf Netzlaufwerke beschränkt sein, um den Datenschutzbestimmungen zu entsprechen. So kann verhindert werden, dass sensible Personaldaten auf Wechselmedien gespeichert werden.<br>Ein weiteres Beispiel sind der Zugriff auf USB-Schnittstellen und die Installation von Treibern, die in den meisten Abteilungen unterbunden werden, für die Dokumentationsabteilung zum Anschließen von Digitalkameras beispielsweise jedoch unverzichtbar sind. |
| Übersichtlichkeit | Auch auf Abteilungsebene kann es die Übersicht verbessern, wenn Benutzer der Abteilung in der zugehörigen OU organisiert werden. So ist auf einen Blick sichtbar, wer etwa in der Abteilung arbeitet, und es müssen nicht umständliche Suchen nach Gruppenzugehörigkeiten oder Abteilungsattributen durchgeführt werden. |

### Mischformen

In der Praxis ist es oft sinnvoll, den geografischen mit dem administrativen Ansatz zu verknüpfen. Meist werden auf oberster Ebene die Standorte abgebildet und unterhalb finden sich dann Abteilungen, die an den Standorten vertreten sind. Diese Aufteilung ist sogar dann sinnvoll, wenn es bisher nur einen Standort gibt, denn so sind Sie für eine zukünftige Erweiterung gerüstet.

Durch so eine OU-Hierarchie werden z. B. Softwareverteilungsrichtlinien auf lokale Netze beschränkt, es kann aber trotzdem eine abteilungsspezifische Unterscheidung zwischen den benötigten Programmen stattfinden.

## 12.3 Entwurf für die Domäne *firma.intern*

### Vorbedingungen

Bevor Sie mit dem Konzipieren einer Unternehmensstruktur beginnen können, müssen Sie folgende Informationen sammeln:

- Welche Standorte gibt es?
- Welche Abteilungen werden definiert?
- Existieren besondere administrative Vorgaben?

Für die *Firma GmbH* in der Testumgebung sind die folgenden Informationen vorgegeben:

Es gibt nur den Standort Berlin. Dieser umfasst folgende Abteilungen:

- Buchhaltung
- IT
- Kundenbetreuung
- Management
- Softwareentwicklung
- Support
- Vertrieb
- Verwaltung

### Auftrag

Die Unternehmensstruktur muss die folgenden Anforderungen erfüllen:

- Als oberste OU soll der Standort abgebildet werden.
- In *Firma GmbH* sollen Workstations auf einen lokalen WSUS-Server zugreifen, um Updates einzuspielen.
- Die Mitarbeiter der Softwareentwicklung und der IT-Abteilung sollen in der Lage sein, auf ihren Rechnern unterschiedliche Bildschirmauflösungen zu verwenden. Alle anderen Mitarbeiter erhalten keinen Zugriff auf die Anzeige-Einstellungen der Systemsteuerung.

- Die Kennwörter anderer Benutzer werden von den Abteilungsleitern und den IT-Mitarbeitern verwaltet.
- Die Support-Mitarbeiter sollen die Kennwörter von Verwaltungsmitarbeitern zurücksetzen können.
- Die IT-Abteilung soll in einer OU außerhalb der Standort-OU untergebracht werden, da sie standortübergreifend arbeiten soll.
- Alle OUs sollen nach den in Kapitel 1 festgelegten Konventionen benannt werden.

Nehmen Sie sich vor dem Weiterlesen die Zeit und notieren Sie die Struktur, die das Unternehmen korrekt abbildet und die alle Anforderungen erfüllt. Da diese nur wenig Spielraum lässt, müssten Sie zum gleichen Ergebnis kommen wie im weiteren Verlauf dieses Kapitels beschrieben.

## 12.4 Organisationseinheiten erstellen

### Aufgabenstellung

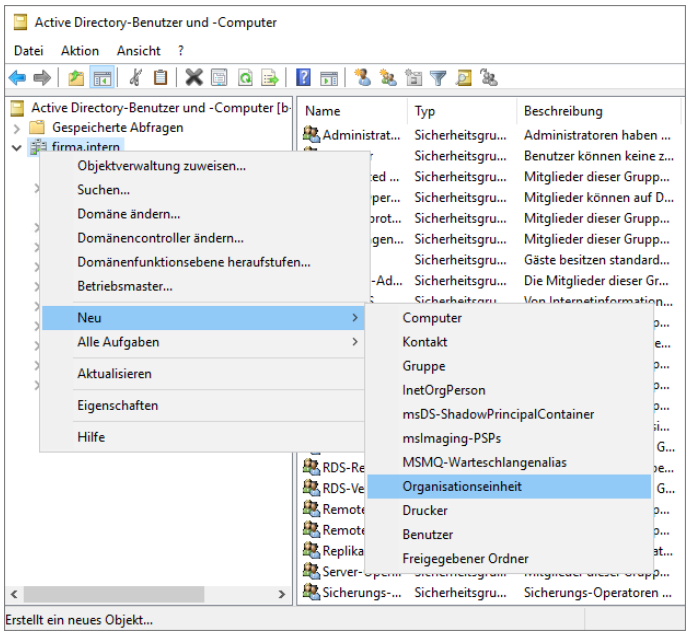
Entsprechend der Aufgabenstellung ergibt sich eine OU-Struktur, die auf der ersten Ebene einen geografischen Ansatz erfordert. Auf einer zweiten Ebene werden die Abteilungen abgebildet.

### Organisationseinheit erstellen

Beginnen Sie nun damit, den Standort *Berlin* abzubilden, indem Sie die Toplevel-OU *OU-Berlin* und unterhalb die Abteilungs-OUs für den Standort anlegen. Sie können hierzu verschiedene Werkzeuge verwenden, die Ihnen im Folgenden vorgestellt werden.

### Active Directory-Benutzer und -Computer verwenden

- Klicken Sie im Menü *Tools* des Server-Managers auf *Active Directory-Benutzer und -Computer*.
- Wählen Sie im Kontextmenü von *firma.intern* den Befehl *Neu - Organisationseinheit*.
- Geben Sie den Namen für die Organisationseinheit ein. Für die Testumgebung ist dies *OU-Berlin*.



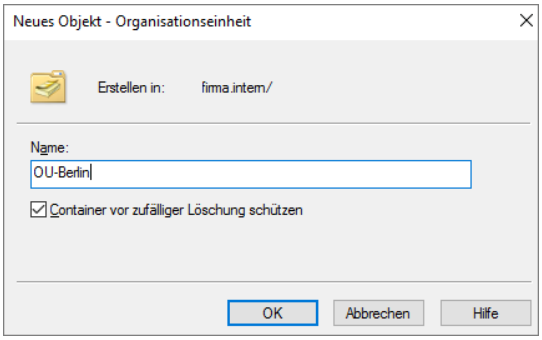

*Neue Organisationseinheit im Server-Manager anlegen*

- Deaktivieren Sie bei Bedarf die Option *Container vor zufälliger Löschung schützen* und klicken Sie auf *OK*.

### Schutz vor zufälliger Löschung nachträglich deaktivieren

Standardmäßig werden neue OUs vor dem versehentlichen Löschen oder Verschieben geschützt. Um später eine OU löschen oder verschieben zu können, müssen Sie diese Option deaktivieren:

- Stellen Sie sicher, dass im Menü *Ansicht* die Option *Erweiterte Features* aktiviert wurde.
- Klicken Sie im Kontextmenü einer OU auf *Eigenschaften*.
- Deaktivieren Sie auf der Registerkarte *Objekt* die Option *Objekt vor zufälligem Löschen schützen*.
- Klicken Sie auf *Übernehmen* und *OK*.





Schulversion
© HERDT-Verlag

Objekte können Sie mit dem Kontextmenübefehl *Verschieben* in der Hierarchie neu einordnen. Sie können ein Objekt auch mit der Maus verschieben.

Probieren Sie einmal aus, was passiert, wenn Sie eine geschützte OU erst verschieben und dann löschen wollen. Schalten Sie dann die Option in *Eigenschaften - Objekt* aus und wiederholen Sie den Vorgang.

## Steuerelemente in Active Directory-Benutzer und -Computer

Am schnellsten geht die Erstellung von OUs, Gruppen und Benutzern, wenn Sie die Steuerelemente verwenden:

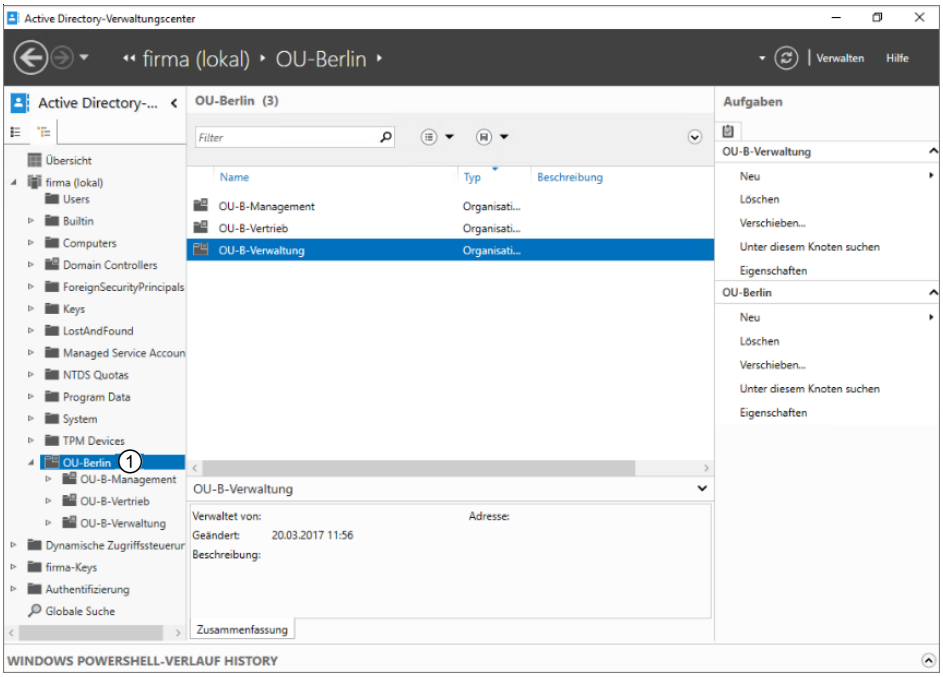
| Symbol | Funktion |
|---|---|
| | Erstellt einen neuen Benutzer am aktuellen Ort |
| | Erstellt eine neue Gruppe am aktuellen Ort |
| | Erstellt eine neue OU am aktuellen Ort |
| | Öffnet die Filteroptionen, mit denen Sie nur bestimmte Objekte anzeigen lassen können |
| | Sucht Objekte im Active Directory |
| | Fügt die markierten Objekte (Benutzer, Gruppen, Computer etc.) einer Gruppe Ihrer Wahl hinzu |

## Untergeordnete OU mit dem Active Directory-Verwaltungscenter erstellen

Damit Sie die Unterschiede zwischen den verschiedenen Werkzeugen kennenlernen, werden die folgenden Schritte im Active Directory-Verwaltungscenter durchgeführt.

- Starten Sie im Startmenü das *Active Directory-Verwaltungscenter*.
- Markieren Sie in der Strukturanzeige die Organisationseinheit, in der Sie eine neue OU erstellen wollen ①.
- Klicken Sie rechts im unteren Aufgabenbereich auf *Neu - Organisationseinheit.*

  Der Befehl ist auch im Kontextmenü der OU zu finden.

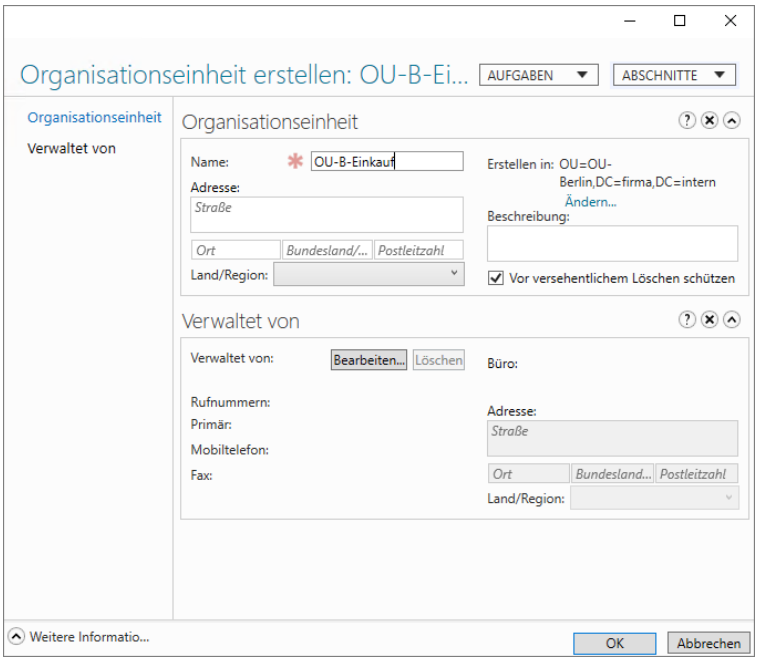



*Neue OU im Active Directory-Verwaltungscenter erstellen*

Es öffnet sich ein Assistent, in dem Sie zusätzlich zur Namensvergabe und dem Schutz vor zufälligem Löschen eine Reihe weiterer Einstellungen vornehmen können.

- Geben Sie den Namen für die neue Organisationseinheit ein. Halten Sie sich dabei an das Benennungsschema *OU-B-<Abteilungsname>*, also z. B. *OU-B-Verwaltung*.
- Geben Sie optional Adressinformationen und eine Beschreibung für die OU ein.
- Wählen Sie, ob die OU vor zufälligem Löschen geschützt werden soll.
- Wenn bereits der Benutzer erstellt wurde, der die OU verwalten soll, können Sie mit *Bearbeiten* einen Auswahl-Assistenten öffnen und den Benutzer auswählen.

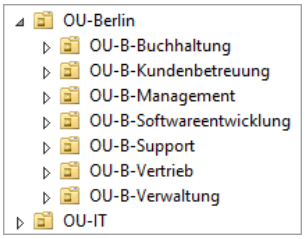
  Die weiteren Informationen werden anhand der Eigenschaften des Benutzerkontos ergänzt.
- Bestätigen Sie Ihre Auswahl mit *OK*.




*Eigenschaften für neue Organisationseinheit festlegen*

### Die OU-Struktur vervollständigen

Erstellen Sie die restlichen OUs, bis Ihre Struktur der Abbildung rechts entspricht.




Die IT-Abteilung ist nicht in der *OU-Berlin* enthalten, weil Sie so für das IT-Personal auf einfache Weise Richtlinien erstellen können, die unabhängig vom Standort und den normalen Benutzern sind. Diese Trennung ist hauptsächlich in Unternehmen mit mehreren Standorten wichtig, erweist sich aber auch bei kleinen Domänen als vorteilhaft.

## 12.5 Benutzerkonten

### Eigenschaften von Benutzerkonten

Benutzerkonten verfügen über eine Reihe von grundlegenden Eigenschaften, die sie von anderen Objekten unterscheiden. Von besonderer Bedeutung sind dabei die folgenden Kategorien:

- Kennwortoptionen
- Anmeldezeiten
- erlaubte Anmeldestationen
- Kontosperrung
- Ablaufdatum
- Profilpfad und Basisordner
- Gruppenmitgliedschaften

### Kennwortoptionen

Die Kennwortoptionen steuern die Einstellungen von Benutzerkennwörtern. Da diese von großer Bedeutung für die Sicherheit im Netzwerk sind, werden die wichtigsten Optionen in der folgenden Tabelle erläutert:

| | |
|---|---|
| Benutzer muss Kennwort bei der nächsten Anmeldung ändern | Dadurch, dass Benutzer sofort ihr Kennwort ändern müssen, kann durch Protokolleinträge nachgewiesen werden, dass der Administrator das Passwort nicht mehr kennt. Nur der Benutzer kann sich jetzt noch anmelden. |
| Benutzer kann Kennwort nicht ändern | Für öffentlich zu verwendende Konten (z. B. in einem Internetcafé) sollten die Kennwörter nicht änderbar sein. |


Schulversion
© HERDT-Verlag

| | |
|---|---|
| Kennwort läuft nie ab | Normalerweise müssen Kennwörter in einstellbaren Intervallen geändert werden. Für manche Konten (z. B. Dienstkonten) ist diese Option deaktivierbar. |
| Kennwort mit umkehrbarer Verschlüsselung speichern | Aktivieren Sie diese Option nur im Ausnahmefall, sie stellt ein Sicherheitsrisiko dar.<br>Normalerweise speichert die Active Directory-Datenbank bei Kennwörtern nur das Resultat einer irreversiblen (nicht umkehrbaren) Verschlüsselung. Wenn nun das System für Authentifizierungen bei veralteten Einwahldiensten das Kennwort im Klartext übertragen soll, muss vorher diese Option aktiviert werden. Anschließend muss der Benutzer sein Kennwort ändern, da das System das Kennwort erst lernen muss. |
| Konto ist deaktiviert | Wenn ein Mitarbeiter das Unternehmen verlässt, sollte sein Konto zuerst nur deaktiviert werden. Der Mitarbeiter könnte z. B. seine Stelle einklagen und müsste dann wieder auf sein Konto zugreifen können.<br>Auch wenn neue Mitarbeiter ihre Stelle antreten sollen, wird in der Regel im Voraus ein Konto erstellt. Erst wenn der Mitarbeiter die IT-Nutzungsbedingungen unterschrieben hat, wird sein Konto aktiviert und er wird zur Eingabe des vordefinierten Kennwortes mit anschließender Kennwortänderung aufgefordert. |
| Benutzer muss sich mit einer Smartcard anmelden | Wenn Benutzer für die Anmeldung Smartcards verwenden müssen, ist diese zusätzliche Option zu konfigurieren. Die Netzwerksicherheit wird dadurch erhöht.<br>Sie können die Option auch über eine Richtlinie für bestimmte Computer konfigurieren. |

## Anmeldezeiten und erlaubte Anmeldestationen

Sie können festlegen, dass bestimmte Benutzer sich nur zu vorgegebenen Zeiten und/oder auf bestimmten Arbeitsplatzrechnern anmelden dürfen. Dies erhöht die Sicherheit im Netzwerk. In den Default-Einstellungen dürfen sich Benutzer zu allen Zeiten an sämtlichen Arbeitsstationen und Mitgliedsservern anmelden.

## Kontosperrung

Wenn ein Benutzer sein Kennwort öfter als erlaubt falsch eingibt, wird das Konto vom System gesperrt. Diese Sperrung muss von einem berechtigten Benutzer aufgehoben werden, damit der Benutzer sich wieder anmelden kann. In aller Regel wird bei dieser Gelegenheit auch das Kennwort zurückgesetzt und muss anschließend vom Benutzer neu eingegeben werden.

## Ablaufdatum

Sie können ein Konto mit einem Ablaufdatum ausstatten. Wenn z. B. die Konten von Praktikanten mit einem automatischen Ablaufdatum versehen werden, können sie ohne weitere Eingriffe eines Administrators nach Beendigung des Praktikums nicht mehr verwendet werden.

## Profilpfad und Basisordner

Wenn Sie servergespeicherte Profile verwenden, muss im Konto des Benutzers festgelegt werden, wo das Profil gespeichert werden soll. Dies hat zusätzlich zur Folge, dass das System für den Benutzer auf das eigene Profil exklusive Zugriffsrechte vergibt. Verwenden Sie an dieser Stelle die Systemvariable *%username%*, um den Pfad zu konfigurieren. Dadurch ist sichergestellt, dass beim Kopieren des Benutzerkontos die Informationen zum jeweiligen Konto passen. Dasselbe gilt für den Basisordner des Benutzers.

## Gruppenmitgliedschaften

Zentrale Bedeutung hat für jeden Benutzer die Mitgliedschaft in Gruppen. Erst indem der Benutzer zu bestimmten Gruppen gehört, sind ihm auch bestimmte Rechte und Berechtigungen zugeordnet.

## 12.6 Benutzerkonto erstellen

### Aufgabenstellung

Erstellen Sie folgende Mitarbeiter in der Abteilung *Buchhaltung* am Standort Berlin:

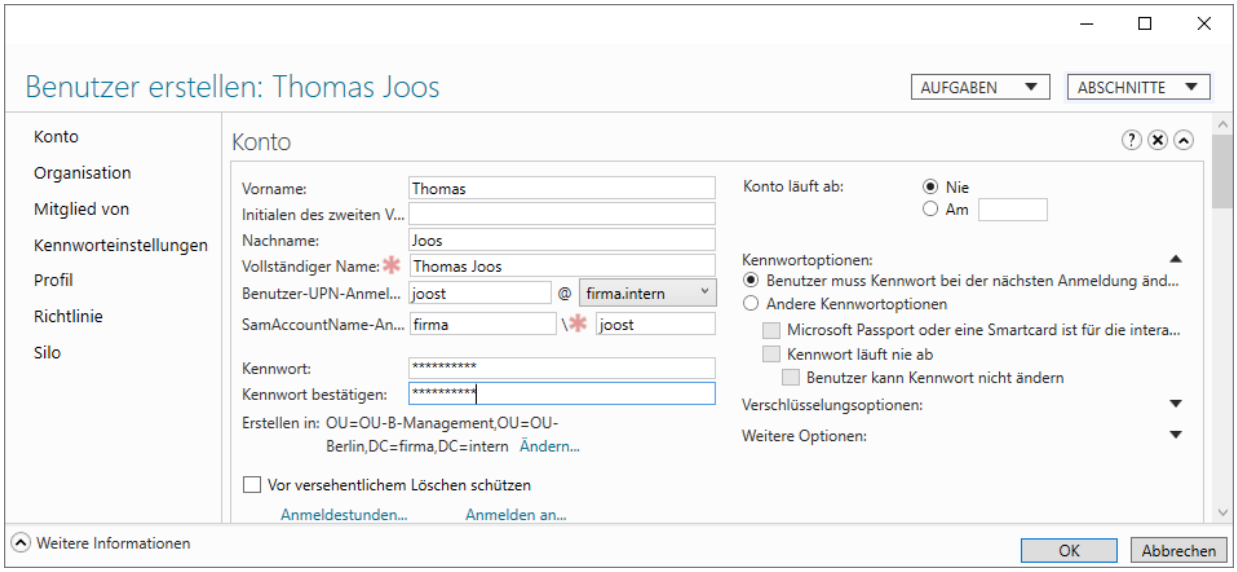
- *Andrea Baumann* *ABaumann*
- *Bernhard Betz* *BBetz*
- *Claudia Beck* *CBeck*

Dabei gelten die folgenden Konventionen:

- Verwenden Sie als Anmeldenamen den Anfangsbuchstaben des Vornamens und den vollen Nachnamen.
- Ersetzen Sie Umlaute und andere Sonderzeichen durch einen ähnlichen Standardbuchstaben.
- Überlegen Sie sich, wie der Anmeldename gebildet wird, wenn mehrere Mitarbeiter den gleichen Anfangsbuchstaben des Vornamens und den gleichen Nachnamen haben.
- Überlegen Sie, wie identische Namen gehandhabt werden könnten. Es ist zwar im AD kein Problem, wenn mehrere Mitarbeiter den gleichen Namen haben, dennoch kann es z. B. sinnvoll sein, ein fiktives Initial zu verwenden.

### Benutzer erstellen

- Öffnen Sie das Active Directory-Verwaltungscenter.
- Klicken Sie im Kontextmenü der *OU-B-Buchhaltung* auf *Neu - Benutzer*. Es öffnet sich der Dialog *Benutzer erstellen*.




*Benutzer im AD-Verwaltungscenter erstellen*

Sie können nun eine Vielzahl von Feldern ausfüllen. Es müssen nur Felder ausgefüllt werden, die mit einem roten Stern gekennzeichnet sind, alle anderen sind optional.

- Geben Sie den Vornamen und den Nachnamen ein. Tragen Sie optional das Initial des zweiten Vornamens ein.
- Editieren Sie bei Bedarf den vollständigen Namen entsprechend den Namenskonventionen.
- Geben Sie den Benutzer-UPN-Anmeldenamen ein und wählen Sie die Domäne aus, zu der das Benutzerkonto gehören soll. Beachten Sie, dass hier stets die Domäne angezeigt wird, die im Alphabet vorne steht.


Schulversion
© HERDT-Verlag

Der Benutzer-Prinzipalname (User Principal Name, UPN) dient zur Anmeldung in einer Active Directory-Domäne. Er besteht aus zwei Teilen, die durch das @ getrennt werden, dem Anmeldenamen und dem UPN-Suffix. Das Suffix ist üblicherweise der Name der Domäne, kann aber auch eine Kurzform sein.

- Passen Sie gegebenenfalls den SamAccountName-Anmeldenamen an.

Die Anmeldung über den SamAccountName-Anmeldenamen dient als Kompatibilitätsmodus für die Anmeldung an der Domäne unter Windows NT, wird aber auch heute noch von vielen Benutzern verwendet. Diese Art der Anmeldung funktioniert nur, wenn im Netzwerk NetBIOS aktiviert ist.

- Geben Sie das Kennwort zweimal ein. Beachten Sie dabei die erforderliche Mindestlänge und die Komplexitätsanforderung des Kennwortes.
- Legen Sie fest, ob das Konto vor zufälligem Löschen geschützt werden soll.

Beachten Sie, dass die Option *Vor versehentlichem Löschen schützen* standardmäßig deaktiviert ist. Dies ermöglicht das unkomplizierte Verschieben von Benutzern in andere Abteilungs-OUs oder Gruppen.

- Legen Sie unter *Kennwortoptionen* fest, ob der Benutzer sein Kennwort ändern kann oder muss und ob es nie ablaufen soll.

In der Praxis sollten Sie einstellen, dass der Benutzer das Kennwort sofort ändern muss. Für die Testumgebung ist es praktischer, wenn Sie unter *Andere Kennwortoptionen* die Option *Kennwort läuft nie ab* aktivieren.

Sie können noch eine Vielzahl von weiteren Eigenschaften des Kontos bearbeiten, z. B. erlaubte Anmeldezeiten, Angaben zur Organisation, Gruppenmitgliedschaften und Profilpfad, die an dieser Stelle nicht beschrieben werden. Scrollen Sie im Fenster weiter nach unten und schauen Sie sich die einzelnen Felder links an, damit Sie einen Eindruck von den Möglichkeiten erhalten.

- Klicken Sie auf OK.

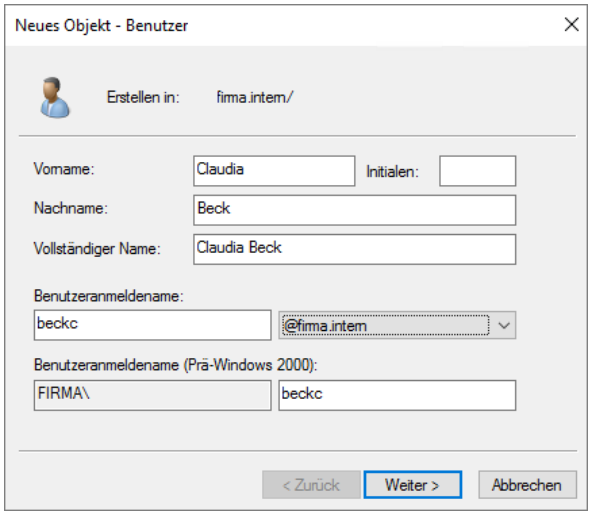
  Der Benutzer wird im Active Directory angelegt.

## Benutzer im Snap-In *Active Directory-Benutzer und -Computer* erstellen

Erstellen Sie nun den Benutzer *Bernhard Betz* in *Active Directory-Benutzer und -Computer*. Vergleichen Sie dabei die Anzahl von Optionen, die Sie beim Erstellen angeben können.

## Benutzerkonto kopieren

Vergleichen Sie die Möglichkeiten, die das Kontextmenü für Benutzerobjekte im AD-Verwaltungscenter bereitstellt, mit denen, die Sie im Snap-In *AD-Benutzer und -Computer* zur Auswahl haben. Sie werden feststellen, dass man im AD-Verwaltungscenter Benutzer zwar verschieben, nicht jedoch kopieren kann.



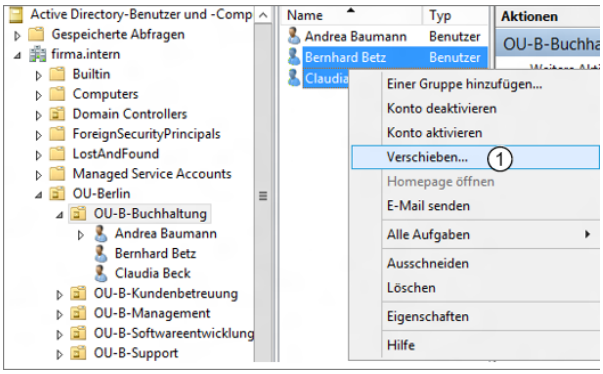

Erstellen Sie nun das Benutzerkonto für *Claudia Beck*, indem Sie das Konto von *Andrea Baumann* im Snap-In *AD-Benutzer und -Computer* kopieren. Hierdurch werden Eigenschaften des Kontos wie Kennwortoptionen, erlaubte Anmeldezeiten und -stationen, Profilpfadangaben, Basisordner und Gruppenmitgliedschaften ebenfalls übernommen. Wenn Basisordner und Profilpfad mit Variablen konfiguriert wurden, werden diese entsprechend ausgewertet.

- Klicken Sie in *AD-Benutzer und -Computer* mit der rechten Maustaste auf das Benutzerkonto von *Andrea Baumann* und wählen Sie im Kontextmenü den Befehl *Kopieren*.
- Geben Sie den Vornamen und den Nachnamen sowie den Benutzeranmeldenamen ein. Beachten Sie, dass die Domänenzugehörigkeit aus dem vorhandenen Konto übernommen wurde.
- Vergeben Sie ein Kennwort und klicken Sie auf *OK*.

### Benutzerkonto verschieben

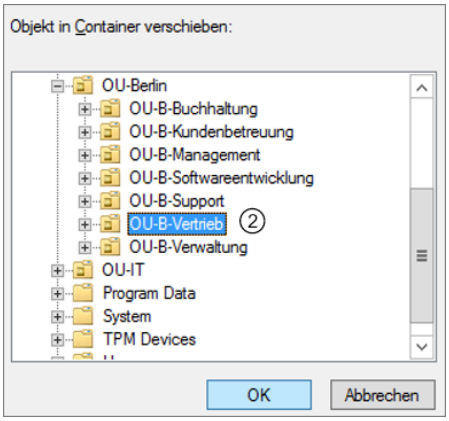
Aufgabenstellung: *Bernhard* und *Claudia* wechseln nun ihr Tätigkeitsfeld. Sie werden künftig Vertriebstätigkeiten übernehmen, deshalb sollen ihre Benutzerkonten in die Organisationseinheit *OU-B-Vertrieb* verschoben werden.

- Klicken Sie auf die Organisationseinheit, um den Inhalt anzeigen zu lassen.




*Benutzer verschieben*

- Markieren Sie die Benutzerkonten, die Sie verschieben wollen (Mehrfachauswahl durch Betätigen von ⇧ oder Strg).
- Klicken Sie mit der rechten Maustaste auf die Markierung und wählen Sie den Kontextbefehl *Verschieben* ①.
- Wählen Sie den Zielcontainer aus ② und klicken Sie auf *OK*. Die Benutzer werden verschoben. Betätigen Sie F5, um die Anzeige zu aktualisieren.




Sie können Objekte übrigens auch verschieben, indem Sie sie mit der Maus woanders hinziehen.

## 12.7 Objektnamen im Active Directory

### Definierte Namen (Distinguished Names)

Objekte im Active Directory verfügen über mehrere Namensattribute wie Vor- und Nachname, Initialen, Anzeigename, UPN-Anmeldename usw. Der einzige Name, der geeignet ist, um das Objekt im Active Directory eindeutig zu identifizieren, ist der **LDAP-Objektname**, auch bekannt unter seiner englischen Bezeichnung **Distinguished Name** (eindeutiger Name). Der Distinguished Name wird von Microsoft auf Deutsch etwas unglücklich als „definierter Name“ bezeichnet. Der LDAP-Objektname unterscheidet die Objekte innerhalb der Hierarchie des Verzeichnisses. Für Frau Baumann aus der Buchhaltung sieht das in der Testumgebung so aus:

*CN=Andrea Baumann, OU=OU-B-Buchhaltung, OU=OU-Berlin, DC=firma, DC=intern*

Der Name ist aus den Pfadbestandteilen des AD zusammengesetzt. Standardmäßig gibt es drei Schlüsselwörter:

- CN (Common Name): Dies ist der Objektname, unter dem das Objekt in der AD-Verwaltung angezeigt wird. Der CN ohne den restlichen LDAP-Pfad wird auch als **Relative Distinguished Name** (RDN) bezeichnet.
- OU (Organizational Unit): Dies bezeichnet eine Organisationseinheit oder Unter-OU, die im Active Directory-Benutzer und -Computer so dargestellt werden: .
- DC (Domain Component): Dies ist der Name einer Domäne oder Unterdomäne.

Zusätzlich zum Distinguished Name (DN) werden weitere Informationen benötigt, damit ein Benutzer sich in der Domäne anmelden und arbeiten kann:

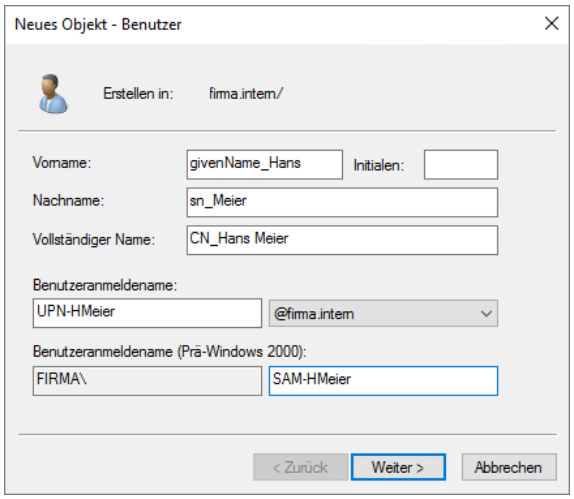

Schulversion
© HERDT-Verlag

- Die Objekt-GUID für den Benutzer als eindeutige ID im Active Directory. Die GUID wird automatisch für jedes Objekt generiert und intern für die Verwaltung des AD verwendet.
- Der Benutzerprinzipalname (User Principal Name, UPN), z. B. *HMeier@firma.intern*. Der UPN besteht aus dem Anmeldenamen (HMeier1) und dem UPN-Suffix (*firma.intern*). Alternativ kann auch die Prä-Windows-2000-Anmeldung (z. B. *FIRMA\HMeier*) verwendet werden, die aus der Kurzform der Domäne *FIRMA* und dem Sam-Account-Namen *HMeier* besteht.
- Die Sicherheits-ID (Security Identifier, SID) ist zwar für die Benutzeranmeldung in der Domäne nicht erforderlich, jedoch kann der Benutzer ohne SID nicht auf Dateien zugreifen, bei denen er Ersteller/ Besitzer ist. Der Zugriff über Gruppenmitgliedschaften ist auch weiterhin möglich. Jeder Benutzer und Computer verfügt über eine SID, aber nicht jedes Objekt im AD.

Der UPN-Anmeldename und der Prä-Windows-2000-Anmeldename sind standardmäßig gleich, können aber auch unterschiedlich vergeben werden. Sie haben nichts miteinander gemeinsam.

## Testbenutzer erstellen

Um die Funktionsweise des Active Directory zu verdeutlichen, wird ein neuer Benutzer benötigt. Bei der Benennung werden den einzelnen Namensbestandteilen Attribute vorangestellt, um sie später besser identifizieren zu können.

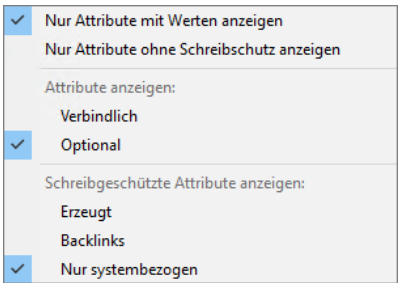



- Starten Sie im Startmenü *Active Directory-Benutzer und -Computer*.
- Erstellen Sie in *OU-Berlin/OU-B-Management* einen neuen Benutzer. Geben Sie Folgendes ein:
  - *Vorname*: `givenName_Hans`
  - *Nachname*: `sn_Meier`
  - *Vollständiger Name*: `CN_Hans Meier`
  - *Benutzeranmeldename*: `UPN-HMeier`
  - *Anmeldename (Prä-Windows 2000)*: `SAM-HMeier`
- Weisen Sie ein Kennwort zu und schließen Sie die Erstellung ab.
- Öffnen Sie über das Kontextmenü die Eigenschaften des Benutzers *CN_Hans Meier*.
- Öffnen Sie die Registerkarte *Allgemein* und ändern Sie den Anzeigenamen in *displayName_Hans Meier* um. Klicken Sie auf *Übernehmen*. Schließen Sie den Dialog noch nicht.

Sie haben nun alle wichtigen Einstellungen für den Benutzer vorgenommen. Jetzt können Sie sich im Attribut-Editor das Ergebnis ansehen.

## Attribut-Editor verwenden

Im Attribut-Editor können Sie sich alle Objektattribute anzeigen lassen:




- Öffnen Sie in *Active Directory-Benutzer und -Computer* über das Kontextmenü die Eigenschaften des Objekts.
- Wechseln Sie zur Registerkarte *Attribut-Editor*. Dort werden zahlreiche Attribute in alphabetischer Reihenfolge angezeigt. Klicken Sie auf die Schaltfläche *Filter*.
- Aktivieren Sie die Option *Nur Attribute mit Werten anzeigen* und deaktivieren Sie die Option *Verbindlich*, um nur die relevanten Attribute anzuzeigen.

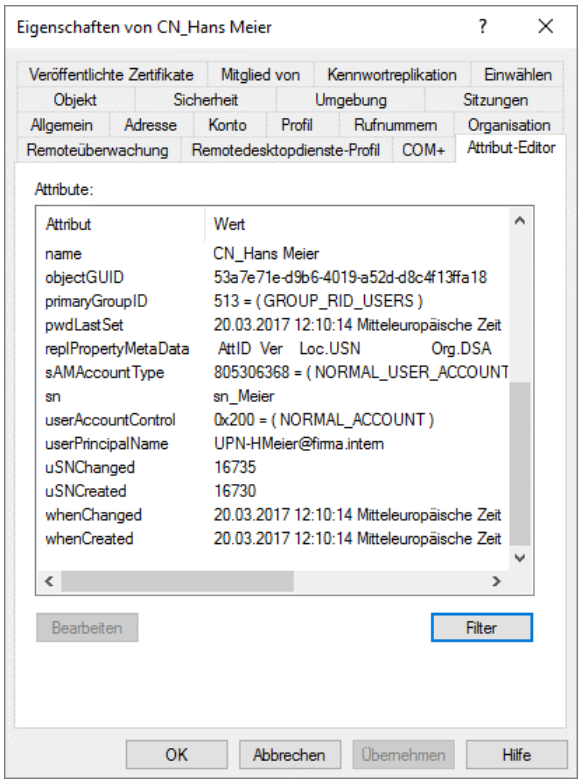
Für das Benutzerobjekt *CN_Hans Meier* gibt es folgende wichtige Attribute:

- CN (Common Name), auch als RDN bekannt
- name (entspricht immer CN)
- distinguishedName (DN, definierter Name)
- objectGUID (Globally Unique Identifier)
- objectSid (Security Identifier)
- sAMAccountName (für Prä-2000-Anmeldung)
- userPrincipalName (UPN Anmeldename)

Weniger wichtige Attribute, die nachträglich ohne Folgen für das Active Directory geändert werden können:

- displayName (Anzeigename)
- givenName (Vorname)
- initials (Initial des zweiten Vornamens)
- sn (Surname, Nachname)

Bei der ungewöhnlichen Schreibweise von *sAMAccount-Name* und *-Type* handelt es sich vermutlich um einen Tippfehler. Da im LDAP nicht zwischen Groß- und Kleinschreibung unterschieden wird, ist die Schreibweise eines Attributs letztlich unwichtig.



*Benutzerattribute im Attribut-Editor*

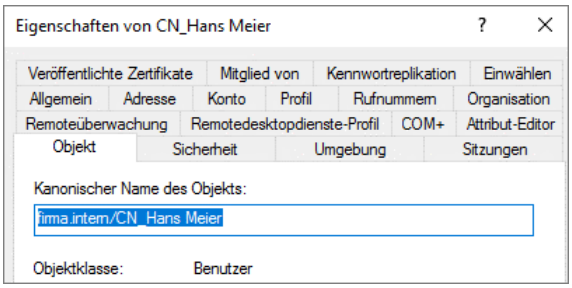
## Der Kanonische Name

In *Active Directory-Benutzer und -Computer* können Sie sich einen weiteren Namenstyp anzeigen lassen: den **kanonischen Namen**. Dieser Name enthält alle Bestandteile des DN in anderer Schreibweise:

- Öffnen Sie über das Kontextmenü die Eigenschaften eines Objekts.
- Öffnen Sie die Registerkarte *Objekt*.

  Dort wird der kanonische Name angezeigt.

Aus dem kanonischen Namen können Sie den Distinguished Name ableiten, indem Sie die Reihenfolge umkehren.




## Der ADSI-Editor

Definierte Namen (Distinguished Names) verwenden Sie hauptsächlich in der PowerShell und bei zahlreichen Kommandozeilentools rund ums Active Directory. Es gibt jedoch auch ein Werkzeug mit grafischer Oberfläche, wo direkt mit Distinguished Names gearbeitet wird: der ADSI-Editor (Active Directory Service Interface, AD-Dienst-Schnittstelle).

Der ADSI-Editor ist ein Werkzeug zur fortgeschrittenen Administration und sollte nur mit großer Umsicht verwendet werden. Sie werden ihn für die meisten Aufgaben nicht benötigen. Er wird hier kurz vorgestellt, um die Struktur des Active Directory besser zu verdeutlichen.

- Rufen Sie im Startmenü bei den Verwaltungsprogrammen den ADSI-Editor auf.
- Erweitern Sie in der linken Strukturansicht die Knoten und klicken Sie auf *DC=firma, DC=intern - OU=OU-Berlin - OU=OU-B-Management*.

  Der Benutzer wird mit seinem definierten Namen (Distinguished Name) angezeigt.


Schulversion
© HERDT-Verlag

Im Kontextmenü eines Objekts oder über den Aktionsbereich können Sie ein Objekt verschieben, löschen, umbenennen oder sich die Eigenschaften anzeigen lassen. Über die Eigenschaften wird der Attribut-Editor geöffnet.

## Übersicht der wichtigsten Namen und Attribute von Benutzern

| Bezeichnungen | Attributname | Beispiel |
|---|---|---|
| Vorname | givenName | *givenName_Hans* |
| Initialen | initials | --- |
| Nachname | sn | *sn_Meier* |
| Anzeigename | displayName | *displayName_Hans Meier* |
| CN, Common Name, relativer definierter Name, RDN, Relative Distinguished Name | cn | *CN=CN_Hans Meier* |
| DN, Distinguished Name, definierter Name, LDAP-Objektname | distinguishedName | *CN=CN_Hans Meier, OU=OU-B-Management, OU=OU-Berlin, DC=firma, DC=intern* |
| Kanonischer Name | --- | *firma.intern/OU-Berlin/OU-B-Management/ CN_Hans Meier* |
| UPN, User Principal Name, Benutzerprinzipalname | userPrincipalName | *UPN-HMeier@firma.intern* |
| Benutzeranmeldename | --- | *UPN-HMeier* |
| UPN-Suffix | --- | *firma.intern* |
| Prä-Windows-2000-Anmeldename | --- | *firma\SAM-HMeier* |
| Kontoname | sAMAccountName | *SAM-HMeier* |

## Übung: Eindeutige Namen

Probieren Sie einmal aus, wie sich das Active Directory beim Umbenennen und Verschieben von Benutzerkonten verhält. Diese Übung hilft beim Verstehen der Zusammenhänge zwischen den verschiedenen Objektattributen und wie Objekte im AD eindeutig zugeordnet werden. Erkunden Sie schrittweise, welche Namen unter Windows eindeutig sein müssen und an welchen Stellen Sie erstaunliche Freiheiten haben.

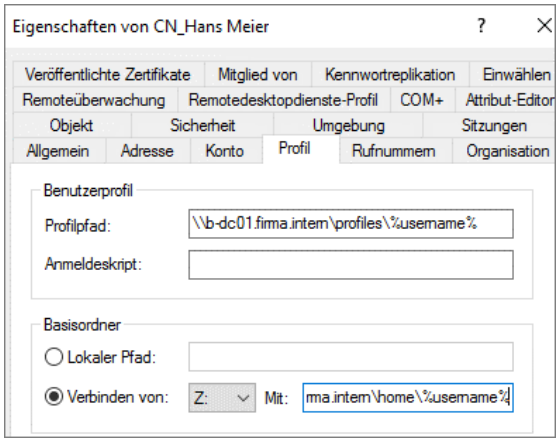
- Erstellen Sie zunächst ein neues Benutzerkonto in der Organisationseinheit *OU-B-Verwaltung*:
  - Vorname: *Hans*
  - Nachname: *Meier*
  - vollständiger Name: *Hans Meier*
  - Benutzermeldename: *HMeier1*
  - Prä-Windows-2000-Anmeldename: *HMeier2*
- Versuchen Sie, ein identisches zweites Konto *Hans Meier* in der gleichen OU zu erstellen.
- Versuchen Sie, ein identisches zweites Konto *Hans Meier* in der gleichen OU zu erstellen, jedoch tragen Sie als vollständigen Namen ***Herbert*** *Meier* ein.
- Versuchen Sie, ein zweites Konto *Hans Meier* in der *OU-B-Buchhaltung* zu erstellen. Die Anmeldenamen sind dabei vertauscht. Benutzermeldename: *HMeier2* und Prä-Windows-2000-Anmeldename: *HMeier1*.
- Versuchen Sie, den Benutzer *Hans Meier* aus der *OU-B-Verwaltung* nach *OU-B-Management* zu verschieben.
- Ändern Sie den Anzeigenamen eines der Benutzer in *Heinz Müller*.
- Ändern Sie den vollständigen Namen eines der Benutzer in *Heinz. Müller*.
- Experimentieren Sie weiter, wenn Sie noch weitere Kombinationen überprüfen wollen.

### Einstellungen zum Benutzerprofil

Den Profilordner, das Anmeldeskript und den Basisordner eines Benutzers können Sie in den Eigenschaften unter *Profile* definieren.

- Erstellen Sie vor der Einrichtung des Benutzerprofils alle Ordner, auf die das Profil später verweisen soll.
- Öffnen Sie in *Active Directory-Benutzer und -Computer* über das Kontextmenü die Eigenschaften des Objekts.
- Wechseln Sie auf die Registerkarte *Profil* und geben Sie die Pfade für das Benutzerprofil (*profiles*), ein optionales Anmeldeskript und den Basisordner (*home*) des Benutzers ein.

  Wenn Sie die Variable *%username%* am Ende des Pfades einsetzen, wird ein Ordner mit dem UPN-Anmeldenamen des Benutzers erstellt.




Alle Ordner, auf die die Pfade verweisen, müssen bereits existieren, sonst können die Benutzerordner darin nicht automatisch erstellt und verrechtet werden.

Im Active Directory-Verwaltungscenter können Sie diese Informationen schon beim Erstellen eines Benutzerkontos eingeben. Falls Sie durch Kopieren eines Benutzers die Einstellungen für weitere Benutzer übernehmen möchten, müssen Sie das Snap-In *AD-Benutzer und -Computer* verwenden, da das Kopieren von Benutzern im AD-Verwaltungscenter nicht möglich ist.

## 12.8 Computerkonto erstellen

### Computerkonten

Wenn der Domäne ein Rechner hinzugefügt wird, für den noch kein Konto erstellt wurde, wird dieses automatisch im Container *Computer* angelegt. Der Ordner *Computer* erlaubt nicht, bestimmte Gruppenrichtlinien an das Objekt zu koppeln. Dies ist nur mit Organisationseinheiten möglich. Daher sollten Computerkonten in entsprechenden Organisationseinheiten erstellt oder in die entsprechenden Organisationseinheiten verschoben werden. Dann können auch Einstellungen über Gruppenrichtlinien vorgenommen werden. Es ist vorteilhaft, neue Computer schon vor dem Beitritt zur Domäne im Active Directory bekannt zu machen, denn so erhält der Computer schon bei der Einrichtung die passende Softwareausstattung und die entsprechenden Einstellungen.

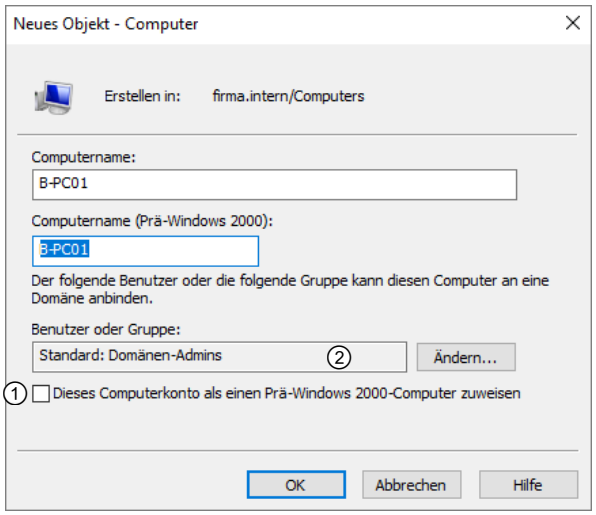

Schulversion
© HERDT-Verlag

## Computerkonto erstellen

In der Organisationseinheit *OU-B-Buchhaltung* soll das Computerobjekt für Andreas Workstation erstellt werden.

- Klicken Sie mit der rechten Maustaste auf die gewünschte Organisationseinheit und wählen Sie den Kontextbefehl *Neu - Computer*.
- Geben Sie einen Namen für den Computer ein. Berücksichtigen Sie dabei die Namenskonventionen für DNS-Namen und Ihr Unternehmensnetzwerk.

  Windows bildet automatisch den NetBIOS-Namen.
- Falls es sich um eine Windows-NT-Workstation handelt, aktivieren Sie die Option ①.




*Computerkonto anlegen*

### Autorisierte Personen

Die Gruppe der Domänen-Admins ist berechtigt, beliebig viele Computer zur Domäne hinzuzufügen ②.

Daneben darf standardmäßig jeder in der Domäne authentifizierte Benutzer der Domäne zehn Computer hinzufügen. Sie können zusätzlich eine bestehende Gruppe mit dieser Aufgabe betrauen oder eine neue Gruppe erstellen, für die Sie das Limit höhersetzen oder ganz weglassen können.

Active Directory sieht für solche Maßnahmen eigentlich die Gruppe der Kontenoperatoren vor. Die Kontenoperatoren sollten für diese Aufgabe nicht verwendet werden, da sie über weitreichende Rechte wie die Verwaltung aller Benutzerkonten der Domäne außer den Administratorkonten verfügen. Stattdessen bietet es sich an, diese Aufgabe einer Gruppe von Workstation-Betreuern für den jeweiligen Standort zuzuweisen.

# 13 Benutzer und Gruppen

**In diesem Kapitel erfahren Sie**

- was Benutzer und was Kontakte sind
- welche Gruppentypen es gibt und welche Gruppenbereiche zu unterscheiden sind
- die AGDLP-Regel
- wie Sie Gruppen planen

**Voraussetzungen**

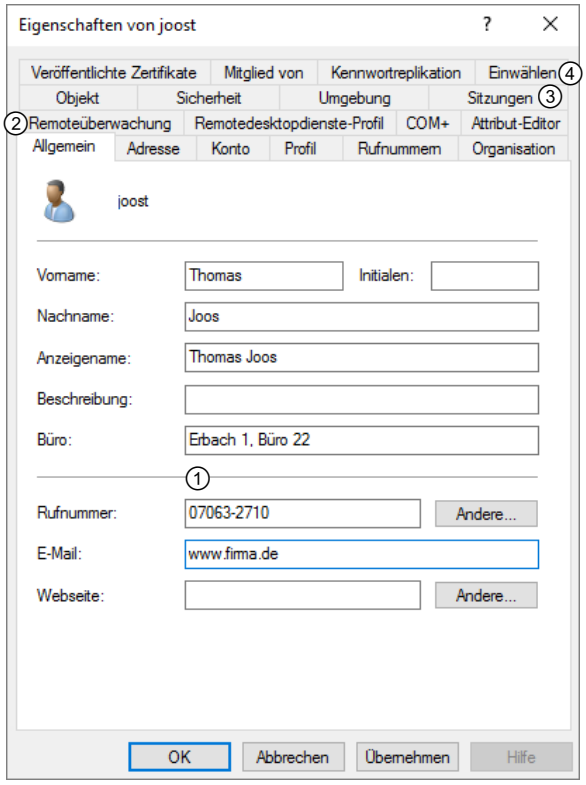
- Active Directory installieren
- Active Directory-Objekte verwalten
- Rechte und Berechtigungen

## 13.1 Benutzer und Kontakte

### Benutzer

Das Objekt *Benutzer* dient dazu, Personen im Active Directory zu virtualisieren. Zentrale Komponenten des Benutzerobjektes sind dabei die Sicherheits-ID (Security Identifier, SID) und die global eindeutige ID (Globally Unique Identifier, GUID), über die das Objekt eindeutig in der Domäne und der Gesamtstruktur identifiziert werden kann. Das Benutzerkonto repräsentiert meist eine einzelne Person, in Sonderfällen kann eine Person aber auch über mehrere Benutzerkonten verfügen, etwa um die normale Funktion als Benutzer von administrativen Tätigkeiten zu trennen. So soll verhindert werden, dass ein Benutzer versehentlich mit administrativen Berechtigungen auf Funktionen von Windows zugreift.

Benutzer haben eine Vielzahl an möglichen Eigenschaften, die eine virtuelle Abbildung in einer Vielzahl von Zusammenhängen ermöglichen. Dazu gehören Kontaktinformationen ①, die bei einer Suche im Active Directory die anschließende Kontaktaufnahme erleichtern. Daneben gibt es auch Berechtigungen, die die Remoteüberwachung ②, den Zugriff auf Terminalserver ③ oder das Einwählen ④ ermöglichen.




*Eigenschaften eines Benutzerobjektes*

### Kontakte

Kontakte dienen dazu, Personen im Active Directory zu erfassen, die selbst keine Anmeldeberechtigungen in der Domäne besitzen. Die Kontaktdaten können von Anwendungen wie Exchange verwendet werden, die auf das Active Directory zugreifen können.

Kontakte verfügen über deutlich weniger Eigenschaften, da sie ja keine Zugriffe erhalten können. Sie verfügen nur über Adressinformationen, organisatorische Zusammenhänge und Objekteigenschaften.


Schulversion
© HERDT-Verlag

## 13.2 Gruppentypen

### Sicherheitsgruppen und Verteilergruppen

Analog zu Benutzern und Kontakten existieren Sicherheits- und Verteilergruppen. Allerdings unterscheiden sich diese nicht durch die Eigenschaften, die ihnen zugewiesen werden können, sondern durch die Möglichkeiten, wie Sie sie einsetzen können.

### Sicherheitsgruppe

Mit Sicherheitsgruppen steuern Sie den Zugriff auf Ressourcen. Dabei wird die SID der Gruppe in die Zugriffssteuerungsliste (Access Control List, ACL) eines Objektes aufgenommen. Diesem Eintrag werden anschließend bestimmte Zugriffsberechtigungen zugeordnet.

### Zugriffskontrolle über Access Control Lists (ACL)

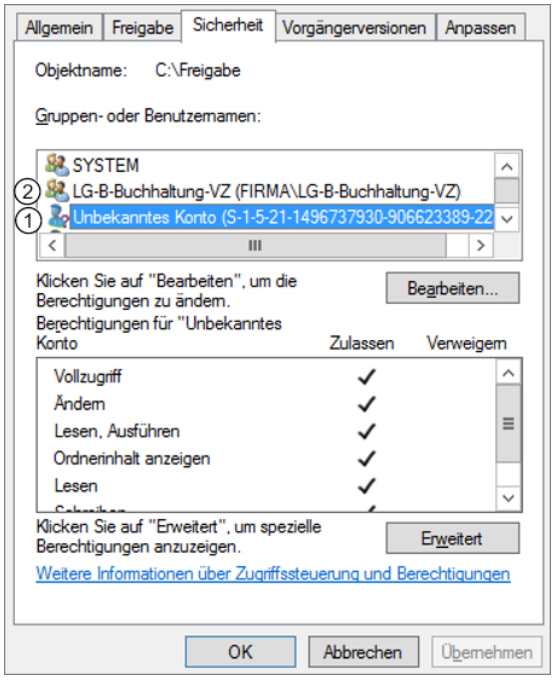
Alle Objektzugriffe auf einem Windows-System werden über die ACLs geregelt, die einem Objekt zugeordnet sind. Dies betrifft z. B. Dateizugriffe auf NTFS- oder ReFS-Partitionen, gilt aber auch für alle anderen Objekte. Die ACL ist eine Liste, mit deren Hilfe überprüft werden kann, ob ein Benutzer auf das Objekt zugreifen darf. Jedem Objekt kann eine ACL angefügt werden, sie muss aber nicht zwingend vorhanden sein. Falls keine ACL vorhanden ist, gibt es keinerlei Zugriffskontrolle und jeder darf nach Belieben auf das Objekt zugreifen. Dies ist z. B. bei FAT-formatierten Datenträgern der Fall. Eine leere ACL ohne Einträge bewirkt, dass niemand auf das Objekt zugreifen darf. Es muss also immer ein Eintrag vorhanden sein, der den Zugang über eine Gruppenmitgliedschaft oder direkt erlaubt. Zur Überprüfung der Identität wird ein Zugriffstoken verwendet. Das Zugriffstoken umfasst zahlreiche Daten, die zur Überprüfung der Zugriffsberechtigung nötig sind. Dazu gehören neben der Benutzer-SID unter anderem auch die SIDs aller Gruppen, in denen der Benutzer Mitglied ist. Die ACL-Einträge werden in den Eigenschaften eines Objekts auf der Registerkarte *Sicherheit* angezeigt.

Da die ACL direkt am Objekt hängt, sind die Informationen darin nicht im Active Directory erfasst. Dies führt dazu, dass in der ACL verwaiste Einträge entstehen, wenn ein dort eingetragener Benutzer im AD kopiert oder gelöscht wird.

In der Abbildung sehen Sie so einen Fall. Nachdem ein zugriffsberechtigter Benutzer gelöscht wurde, kann nur noch *Unbekanntes Konto* und eine SID angezeigt werden ①. Diese Einträge sind nur mühsam wieder zu entfernen oder wiederherzustellen. Um solche Probleme zu vermeiden, sollten Sie Zugriffsberechtigungen stets über Mitgliedschaften in lokalen Gruppen regeln ②. Einzige Ausnahmen sind das Profil und der Basisordner des Benutzers, auf die nur er allein Zugriff haben sollte.

Sie sollten außerdem keine in der ACL eingetragenen Gruppen löschen, sonst erhalten Sie ebenfalls einen Eintrag *Unbekanntes Konto*. Löschen Sie nicht die Gruppe, sondern entfernen Sie stattdessen alle Mitglieder aus der Gruppe.

Beachten Sie, dass es vorteilhaft ist, ausgeschiedene Benutzer nicht sofort zu löschen, sondern erst einmal zu deaktivieren und später zu löschen.




*Einträge in der ACL*

Die ACL wird auch als DACL bezeichnet (Discretionary Access Control List). Sie unterscheidet sich in ihrer Funktion von der SACL (System Access Control List). Während die (D)ACL den Objektzugriff begrenzt, wird die SACL zur Protokollierung aller Zugriffe eingesetzt.

### Verteilergruppen

Über Verteilergruppen können E-Mails an die Gruppenmitglieder versendet werden. Verteilergruppen sind nicht geeignet, um darüber Berechtigungen auf Objekte zu erteilen. Verteilergruppen können sowohl Benutzer als auch Kontakte enthalten. Die Verteilergruppe erhält beim Anlegen eine E-Mail-Adresse und wird im Active Directory-Adressbuch angezeigt. Sie kann wie ein einzelner Empfänger adressiert werden. Da Verteilergruppen für dieses Buch keine Rolle spielen, werden sie hier nicht weiter behandelt.

## 13.3 Gruppenbereiche

### Gültigkeitsbereiche von Gruppen

Sicherheits- und Verteilergruppen werden charakterisiert nach folgenden Bestimmungen:

- Wen kann eine Gruppe enthalten (Herkunft der Gruppenmitglieder)?
- Wo kann die Gruppe im Netzwerk eingesetzt werden (Wirkungsradius des Zugriffs)?
- Wie wird die Gruppe verwendet (Einsatzspektrum der Gruppe)?

Alle Gruppen erhalten bei ihrer Erstellung eine SID.

### Globale Gruppe

| | | |
|---|---|---|
| Verfügbarkeit und Einschränkungen | Früher durften unter Windows 2000 globale Gruppen maximal 5000 Benutzer enthalten. | Seit Windows Server 2003 ist die Anzahl der Mitglieder unbeschränkt. |
| Mitglieder | Benutzer und globale Gruppen der eigenen Domäne | |
| Wirkungsradius der Berechtigungen | Globale Gruppen können Mitglieder beliebiger domänenlokaler Gruppen und universaler Gruppen in der eigenen oder vertrauten Gesamtstruktur sein. | |
| Verwendungszweck | Globale Gruppen dienen dazu, Benutzer nach Art ihrer Tätigkeit zusammenzufassen. Daneben können sie andere globale Gruppen unter funktionellen Gesichtspunkten erfassen. So könnten z. B. alle globalen Gruppen einer Abteilung in einer Abteilungs-Sammelgruppe zusammengefasst werden oder alle globalen Gruppen der Abteilungsleiter in einer Abteilungsleiter-Sammelgruppe für den Standort. | |

### Domänenlokale Gruppe

| | |
|---|---|
| Verfügbarkeit | Unter allen Domänenfunktionsebenen |
| Mitglieder | Benutzer, globale Gruppen und universale Gruppen aus einer beliebigen vertrauten Domäne der eigenen Gesamtstruktur oder vertrauter Domänen oder Gesamtstrukturen. In der Praxis sollten domänenlokale Gruppen jedoch nur in Ausnahmefällen einzelne Benutzer enthalten.<br>Domänenlokale Gruppen der eigenen Domäne |
| Wirkungsradius der Berechtigungen | Beliebige Ressourcen der eigenen Domäne |
| Verwendungszweck | Domänenlokale Gruppen dienen dazu, bestimmte Arten von Zugriffen auf Ressourcen zu bündeln. Sie werden in der Regel für jede Ressource einzeln generiert. |

Domänenlokale Gruppen werden meist nur „lokale Gruppen“ genannt. Sie müssen aber die domänenlokale Gruppe von lokalen Gruppen unterscheiden, die lokal auf einem Rechner angelegt werden. Diese können auch nur auf dem einzelnen Rechner verwaltet werden.


Schulversion
© HERDT-Verlag

### Universale Gruppe

| | |
|---|---|
| Verfügbarkeit | Unter allen Domänenfunktionsebenen |
| Mitglieder | Benutzer, globale Gruppen und universale Gruppen aus beliebiger Domäne der Gesamtstruktur oder vertrauter Domänen oder Gesamtstrukturen |
| Wirkungsradius der Berechtigungen | Beliebige lokale Gruppen in beliebigen Domänen der Gesamtstruktur oder vertrauter Domänen oder Gesamtstrukturen |
| Verwendungszweck | Universale Gruppen dienen dazu, den Einsatz vieler globaler Gruppen unterschiedlicher Domänen in vielen domänenlokalen Gruppen unterschiedlicher Domänen zu bündeln. |

### Einschränkungen bei universalen Gruppen

Die Verwendung von universalen Gruppen wirkt sich auf die Netzwerkleistung und die Sicherheit aus:

- Universale Gruppen vergrößern den globalen Katalog, weil Mitgliedschaften im Katalog gespeichert werden.
- Das Zugriffstoken ist bei universalen Gruppen größer als bei globalen oder lokalen Gruppen. Dies sorgt für erhöhtes Datenaufkommen bei der Replikation.
- Mitgliedschaften in universalen Gruppen mit dem Bereich *Universal* sollten möglichst selten geändert werden, da die gesamte Mitgliedschaft der Gruppen auf alle globalen Kataloge in der Gesamtstruktur repliziert werden muss. Dies führt zu erhöhtem Netzwerkverkehr zwischen den Standorten und Domänen.
- Sie können Domänencontroller die Mitgliedschaft in universalen Gruppen zwischenspeichern lassen, damit Benutzer auch ohne verfügbaren Global Catalog (GC) angemeldet werden können. In diesem Fall wirken sich jedoch sicherheitsrelevante Änderungen der Mitgliedschaft eines Benutzers in einer universalen Gruppe nicht sofort auf die Anmeldung des Benutzers aus.

### Empfehlungen

- Setzen Sie universale Gruppen nur bei mehreren Domänen ein. Beschränken Sie den Einsatz von universalen Gruppen auf die Fälle, in denen Zugriffe auf mehrere verschiedene Ressourcen in verschiedenen Domänen benötigt werden.
- Machen Sie nach Möglichkeit ausschließlich globale Gruppen zu Mitgliedern in der universalen Gruppe und nicht einzelne Benutzer. Mit diesem Zwischenschritt können Sie die Zugehörigkeit eines Benutzers in der universalen Gruppe verändern, indem Sie ihm die Mitgliedschaft in einer entsprechenden globalen Gruppe geben oder entziehen. Dadurch verringert sich der Replikationsaufwand, da ja die Eigenschaften der universalen Gruppe unverändert bleiben.

Die Empfehlungen zur Verwendung von Sicherheitsgruppen lassen sich als AGDLP-Regel zusammenfassen, die weiter unten erläutert wird.

## 13.4 Gruppenhierarchien einsetzen

### Gruppen schachteln

Die Benutzer sollten Mitglieder in globalen Gruppen sein, die ihren Aufgabenbereich möglichst exakt abbilden, z. B. die Gruppe der Sachbearbeiter in der Buchhaltung oder die Gruppe der Abteilungsleiter. Dadurch wird der Benutzer bei einer Veränderung (Abteilungswechsel, Beförderung zum Abteilungsleiter) ohne größeren Aufwand seiner neuen Funktion zugeordnet.

Domänenlokale Gruppen werden verwendet, um bestimmte Zugriffsberechtigungen auf Objekte zusammenzufassen, z. B. auf einen Drucker oder ein Abteilungslaufwerk. Folgendes Beispiel soll die Vorgehensweise erläutern:

*Andrea Baumann* ist Sachbearbeiterin in der Abteilung *Buchhaltung* in Berlin. Als solche ist sie Mitglied in der globalen Gruppe *GG-B-Buchhaltung-Sachbearbeiter*. Sie wird zur Abteilungsleiterin befördert. Entsprechend wird ihr Benutzerkonto in die globale Gruppe *GG-B-Buchhaltung-Abteilungsleiter* verschoben. Sämtliche Zugriffsberechtigungen werden dadurch erfasst, dass die globale Gruppe Mitglied in den entsprechenden domänenlokalen Gruppen ist, die z. B. den Zugang auf das Buchhaltungslaufwerk regeln. Allein durch ihre Mitgliedschaft in der Gruppe der Abteilungsleiter könnte Andrea z. B. die Fähigkeit erworben haben, Kennwörter von Mitarbeitern ihrer Abteilung zurückzusetzen. Dazu waren keine manuellen Anpassungen erforderlich.

Bei einer sinnvoll aufgebauten Struktur reicht das Verschieben des Benutzers in seine neue „Rolle“ aus, um alle erforderlichen Zugriffsberechtigungen automatisch anzupassen. Damit wird der Verwaltungsaufwand minimiert und die Wahrscheinlichkeit von falsch gesetzten Berechtigungen reduziert.

Dieses wichtige Prinzip wird durch die AGDLP-Regel abgedeckt, die Ihnen beim Aufbau Ihrer Struktur wertvolle Orientierungshilfe bietet.

## AGDLP-Regel

Diese englischsprachige Regel ist Teil der Erfolgsmethoden (Best Practice) für Windows-Administratoren. Sie erklärt die sinnvolle Verschachtelung von Gruppen. Die Buchstaben stehen dabei für A = Account (Benutzerkonto), G = globale Gruppe, DL = domänenlokale Gruppe und P = Permission (Erlaubnis).

### 1. Schritt:

Im ersten Schritt erhält der Benutzer (A = ACCOUNTS) eine Mitgliedschaft in einer globalen Gruppe (G = GLOBAL GROUP).

**Beispiel:** *Andrea* und *Hans* werden Mitglied von *GG-B-Buchhaltung*.

### 2. Schritt:

Im zweiten Schritt wird die globale Gruppe in eine lokale Gruppe (DL = DOMAIN LOCAL GROUP) platziert.

**Beispiel:** *GG-B-Buchhaltung* wird Mitglied von *LG-B-LW_Buchhaltung-VZ*.

### 3. Schritt:

Im dritten Schritt erfolgt die Vergabe von Zugriffsberechtigungen (P = PERMISSION) an die lokale Gruppe. Dadurch erhält jedes Mitglied der GG automatisch Zugriff auf die mit der LG verbundenen Ressourcen.

**Beispiel:** Die LG soll allen Buchhaltern den Vollzugriff (VZ) auf das Abteilungslaufwerk (LW_) der Buchhaltung erlauben. Dazu werden der Abteilungsordner und die dazugehörige Freigabe für die lokale Gruppe mit Vollzugriff freigegeben.

## Sinn der AGDLP-Regel

Der Vorteil dieser Vorgehensweise liegt in der Flexibilität des Systems. Wenn ein neuer Mitarbeiter in die Buchhaltungsabteilung kommt, reicht es aus, den Benutzer in die GG zu verschieben, und schon verfügt er über alle für einen Buchhalter notwendigen Berechtigungen. Wechselt jemand die Abteilung, wird der Benutzer einfach in die entsprechende GG verschoben. Dabei werden die bisher geltenden Berechtigungen entzogen und durch die Berechtigungen der neuen Gruppe ersetzt. Es gibt keinerlei Berechtigungen, die von Hand gesetzt werden müssen.


Schulversion
© HERDT-Verlag

Wenn Sie diesen Zusammenhang verstanden haben, sind Sie der erfolgreichen Erstellung und Verwaltung einer AD-Domäne einen Riesenschritt näher gekommen.

Ein weiterer Riesenvorteil ist die Übersichtlichkeit, denn auf diese Weise können Sie sofort erkennen, über welche Berechtigungen ein Benutzerkonto verfügt. Es wird nicht nur angezeigt, in welcher Funktion an welchem Standort der Benutzer tätig ist, sondern über die lokale Gruppe auch jede einzelne Freigabe und die Art des Zugriffs. Durch die sinnvolle und durchgehende Benennung aller Gruppen können Sie jederzeit ablesen, was die Mitgliedschaft in einer Gruppe bedeutet. Dies ermöglicht es neuen Mitarbeitern und Vertretungen im Administrationsteam, sich schnell zurechtzufinden.

## 13.5 Gruppenplanung

### Fallbeispiel 1

Die Benutzer *Bernhard Betz* und *Claudia Beck* aus der Domäne *firma.intern* sollen damit beginnen, die Umsatzzahlen von 2012 statistisch auszuwerten. Auf dem Server *B-FS01* befinden sich die Umsatzzahlen, die in einer Freigabe namens *LW_Umsatz2012* mit Lesezugriff zugänglich gemacht werden sollen.

#### 1. Schritt:

- Erstellen Sie in der Domäne *firma.intern* die globale Gruppe *GG-B-Statistiker*.
  Diese Gruppe soll alle Statistiker am Standort Berlin enthalten.
- Machen Sie Bernhard und Claudia zu Mitgliedern dieser globalen Gruppe.

#### 2. Schritt:

- Erstellen Sie in der Domäne *firma.intern* die lokale Gruppe *LG-B-LW_Umsatz2012-L*.
  Dieser lokalen Gruppe soll Lesezugriff (L) auf die Freigabe *LW_Umsatz2012* ermöglicht werden.
- Machen Sie die Gruppe *GG-B-Statistiker* zu Mitgliedern der Gruppe *LG-B-LW_Umsatz2012-L*.

#### 3. Schritt:

- Erstellen Sie auf dem Fileserver *B-FS01* einen Ordner *Freigaben/Statistik/Statistik2012*.
- Geben Sie den Ordner *Statistik2012* unter dem Namen *LW_Umsatz2012* frei. Beachten Sie, dass der Freigabename vollkommen anders sein kann als der Ordnername.
- Geben Sie der lokalen Gruppe *LG-B-LW_Umsatz2012-L* den Lesen-Zugriff auf die Freigabe \\ *B-FS01.firma.intern\LW_Umsatz2012* und auf den Ordner *Freigaben/Statistik/Statistik2012*.

### Fallbeispiel 2

Das folgende Beispiel soll den Einsatz universaler Gruppen illustrieren, die Konstellation wird jedoch nicht in der Testumgebung nachgestellt. Diese Übung würde den Rahmen des Buches sprengen.

Eine Firma verfügt über eine deutsche Domäne *firma.intern* und eine englische Domäne *company.internal*. Deutschland und England verfügen je über einen Filialleiter und seinen Stellvertreter. Alle vier Personen sollen Zugriff auf alle Kundendaten der Firma erhalten. Die Kundendatenbank liegt verteilt auf Servern in Deutschland und England, in jeder Domäne werden Teile der Datenbank gespeichert.

In einem solchen Fall kommt eine universale Gruppe (UG) zum Einsatz.

### 1. Schritt:

- Erstellen Sie in jeder Domäne eine globale Gruppe, z. B. *GG-Filialleiter_Deutschland* und *GG-Filialleiter_ England*, und machen Sie jeweils den Filialleiter und den Stellvertreter zu Mitgliedern.

### 2. Schritt:

- Erstellen Sie eine universale Gruppe mit dem Namen *UG-Kundendaten*.
- Machen Sie die beiden globalen Gruppen der Filialleiter aus Deutschland und England zu einem Mitglied der universalen Gruppe.

### 3. Schritt:

- Erzeugen Sie in *firma.intern* eine lokale Gruppe mit dem Namen *LG-LW_Kundendaten-Deutschland-L*.
- Erzeugen Sie in *company.internal* eine lokale Gruppe mit dem Namen *LG-LW_Kundendaten-England-L*.
- Machen Sie die Gruppe *UG-Kundendaten* zum Mitglied in beiden lokalen Gruppen *LG-Kundendaten-Deutschland-L* und *LG_Kundendaten-England-L*.

### 4. Schritt:

- Vergeben Sie Zugriffsberechtigungen für die lokalen Gruppen auf die betreffenden Verzeichnisse, z. B. *Filer-London.company.internal**customerdata* und *B-FS01.firma.intern**Kundendaten.*

Nun können über die Domänengrenzen hinweg alle Mitglieder der universalen Gruppe auf beide Freigaben zugreifen. Auch hier gilt wieder: Wenn z. B. den Posten des Abteilungsleiters jemand anderes übernimmt, reicht es aus, den Benutzer der globalen Gruppe *GG-Abteilungsleiter_Deutschland* bzw. *GG-Abteilungsleiter_ England* hinzuzufügen.


Schulversion
© HERDT-Verlag

# 14 Gruppen verwalten

**In diesem Kapitel erfahren Sie**

- wie Sie globale, lokale und universale Gruppen erstellen
- wie Sie Mitgliedschaften in Gruppen verwalten

**Voraussetzungen**

- Active Directory-Objekte
- Gruppen

## 14.1 Gruppenplanung mit globalen und lokalen Gruppen

### Abteilung analysieren

In einem ersten Schritt muss eine Analyse der typischen Abteilungsstruktur eines Unternehmens erfolgen. Die folgende Tabelle soll dabei die Abteilung von *Firma GmbH* und die sich daraus ableitenden globalen Gruppen darstellen:

| Benutzer | Funktion | Gruppe |
|---|---|---|
| Andrea Baumann | Abteilungsleiterin | *GG-B-Buchhaltung-Abteilungsleiter* |
| Bernhard Betz | Sachbearbeiter | *GG-B-Buchhaltung-Sachbearbeiter* |
| Claudia Beck | Sachbearbeiterin | |
| Diego Baldosa | Sachbearbeiter | |
| Ella Burton | Praktikantin | *GG-B-Buchhaltung-Praktikant* |

### Lokale Gruppen mit Standardzugriffsberechtigungen einrichten

Die Abteilung *Buchhaltung* verwendet ein gemeinsames Netzlaufwerk mit diversen Unterverzeichnissen. Dieses Laufwerk wird gemäß den in Kapitel 1 festgelegten Konventionen als *LW_Buchhaltung* bezeichnet. Für das Abteilungslaufwerk werden vier verschiedene lokale Gruppen (LG) angelegt, die den Standardzugriffsberechtigungen *Lesen (L)*, *Ändern (AE)*, *Vollzugriff (VZ)* und *Kein Zugriff (KZ)* entsprechen:

- LG-B-LW_Buchhaltung-L
- LG-B-LW_Buchhaltung-AE
- LG-B-LW_Buchhaltung-VZ
- LG-B-LW_Buchhaltung-KZ

Dieses Verfahren sollten Sie grundsätzlich für sämtliche Abteilungslaufwerke und sonstigen Freigaben anwenden, denn so erfassen Sie sämtliche unterschiedlichen Berechtigungsstufen. Damit sind Sie für alle Fälle und Konstellationen gerüstet, wenn es um Zugriffsberechtigungen auf Ordnerfreigaben geht. Wenn Sie später die Gruppenmitgliedschaften eines Benutzers ansehen, können Sie dort ablesen, welche Zugriffsberechtigungen der Benutzer auf welche Ressourcen hat. Wenn Sie diese Struktur für alle Freigaben verwenden, ergibt dies stets den gleichen Aufbau: Der Benutzer ist Mitglied einer globalen Gruppe, die seiner Funktion in einer Abteilung entspricht, und diese globale Gruppe ist Mitglied einer lokalen Gruppe, die den benötigten Zugriffsberechtigungen entspricht.

Die Erstellung der lokalen Gruppe *Kein Zugriff* hat folgenden Sinn: Nur so können Sie erkennen, dass eine globale Gruppe **keinen** Zugriff auf eine Ressource hat. Dies ist wesentlich übersichtlicher als die Abwesenheit einer lokalen Gruppe, vor allem wenn Sie es mit zahlreichen Freigaben zu tun haben.

### Zugriffsbedürfnisse ermitteln

In unserer Firma sollen die Abteilungsleiter Vollzugriff (VZ) auf das Abteilungslaufwerk erhalten, für die Sachbearbeiter reicht die Berechtigung Ändern (AE) aus. Praktikanten erhalten nur Lesezugriff (L).

### Vorbereitungen für die Übungen

- Erzeugen Sie folgende Active Directory-Objekte, soweit diese noch nicht vorhanden sind:
  /DC=intern/DC=firma/OU=OU-Berlin
  /DC=intern/DC=firma/OU=OU-Berlin/OU=OU-B-Buchhaltung
  /DC=intern/DC=firma/OU=OU-Berlin/OU=OU-B-Buchhaltung/CN=ABaumann
  /DC=intern/DC=firma/OU=OU-Berlin/OU=OU-B-Buchhaltung/CN=BBetz
  /DC=intern/DC=firma/OU=OU-Berlin/OU=OU-B-Buchhaltung/CN=CBeck
  /DC=intern/DC=firma/OU=OU-Berlin/OU=OU-B-Buchhaltung/CN=DBaldosa
  /DC=intern/DC=firma/OU=OU-Berlin/OU=OU-B-Buchhaltung/CN=EBurton
- Veranlassen Sie die Active Directory-Replikation über das gesamte Netzwerk.

## 14.2 Globale Gruppe erstellen und verwalten

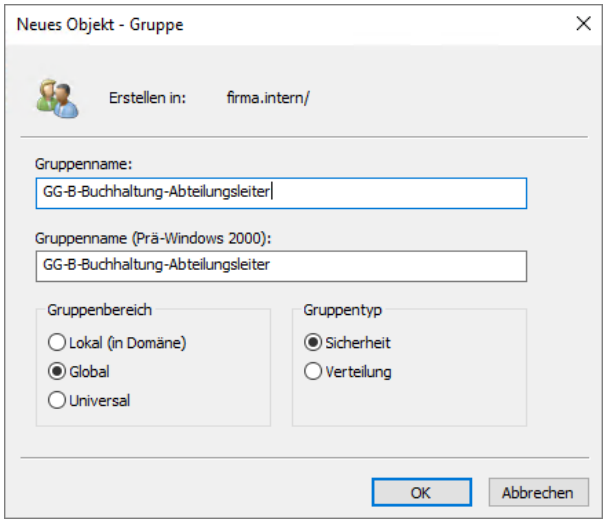
### Aufgabenstellung

Für die Buchhaltungsabteilung soll in der Organisationseinheit *OU-B-Buchhaltung* die globale Gruppe *GG-B-Buchhaltung-Abteilungsleiter* erstellt werden. Die Benutzerin *ABaumann* soll Mitglied dieser globalen Gruppe werden.

### Globale Gruppe erstellen

Teilaufgabe 1: Erzeugen Sie in *OU-B-Buchhaltung* die globale Gruppe *GG-B-Buchhaltung-Abteilungsleiter*.

- Klicken Sie im Snap-In *Active Directory-Benutzer und -Computer* mit der rechten Maustaste auf die gewünschte Organisationseinheit und wählen Sie im Kontextmenü den Befehl *Neu - Gruppe*.
- Geben Sie den Gruppennamen ein.
  Windows erzeugt automatisch einen Gruppennamen für die Anzeige auf Windows-NT-Workstations.
- Legen Sie als Gruppenbereich *Global* fest.
- Legen Sie als Gruppentyp *Sicherheit* fest.




*Neue globale Gruppe anlegen*

### Benutzer zu Mitgliedern einer globalen Gruppe machen

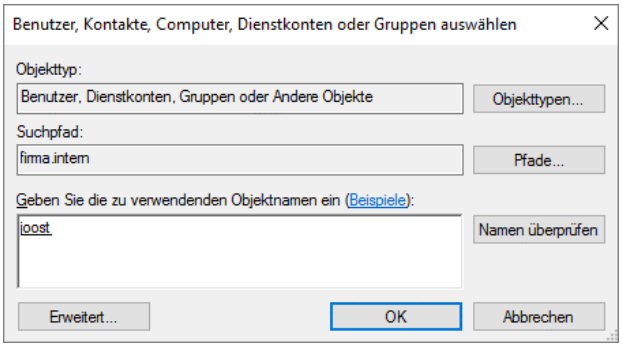
Teilaufgabe 2: *ABaumann* wird zum Mitglied in der globalen Gruppe *GG-B-Buchhaltung-Abteilungsleiter*.

- Klicken Sie mit der rechten Maustaste auf die globale Gruppe und wählen Sie im Kontextmenü *Eigenschaften*.
- Wechseln Sie auf die Registerkarte *Mitglieder* und klicken Sie auf *Hinzufügen*.
  Das Dialogfenster *Benutzer, Kontakte, Computer oder Gruppen wählen* wird geöffnet.


Schulversion
© HERDT-Verlag

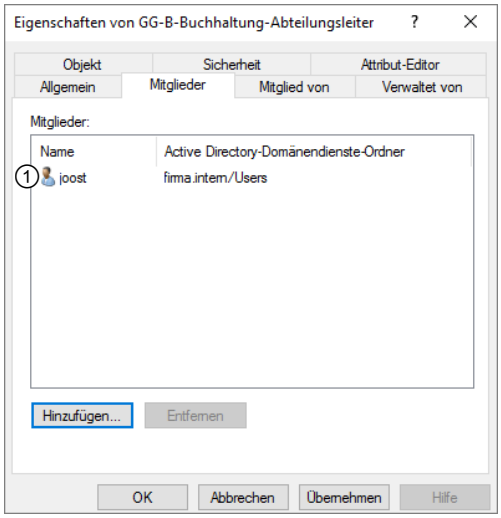
- Um dem Listenfeld einen Benutzer hinzuzufügen, geben Sie den Anmeldenamen oder den vollen Namen des Benutzers ein und klicken Sie auf *Namen überprüfen*.

Der Anfang des Vornamens oder Teile des Anmeldenamens, wie z. B. `joost` oder `Thomas`, reichen aus, um Benutzer schnell zu finden. Wenn mehrere Benutzer den Suchkriterien entsprechen, wird eine Liste angezeigt, aus der Sie auswählen können, anderenfalls wird der Benutzer sofort in das Listenfeld eingetragen. Durch die Eingabe des Nachnamens kann der Benutzer hier nicht gefunden werden. Sie müssen mit dem Vornamen beginnen.




*Mitglieder zum Hinzufügen auswählen*

- Über die Schaltfläche *Erweitert* erreichen Sie ein Dialogfenster für die erweiterte Objektsuche.
- Möchten Sie eine Benutzerwahl revidieren, klicken Sie auf den Eintrag in der Liste ① und betätigen Sie Entf.
- Klicken Sie auf *Übernehmen* und anschließend auf *OK*.




*Mitglieder einer globalen Gruppe hinzufügen*

Unter *Objekttypen* können Sie auswählen, nach welcher Art von Objekten gesucht werden soll. Unter *Pfade* können Sie für die Suche eine andere Domäne auswählen.

Sie können Gruppenmitgliedschaften viel schneller erstellen, indem Sie ein Objekt mit der Maus über eine Gruppe ziehen und loslassen. Verwenden Sie dieses Verfahren, um den folgenden Gruppen ihre Mitglieder zuzuweisen.

- Legen Sie nun die restlichen globalen Gruppen *GG-B-Buchhaltung-Sachbearbeiter* und *GG-B-Buchhaltung-Praktikant* an und fügen Sie den Gruppen die Mitglieder hinzu.

## 14.3 Lokale Gruppe erstellen und verwalten

### Lokale Gruppe erstellen

Teilaufgabe 3: Erzeugen Sie für die Buchhaltungsabteilung in Berlin für das Abteilungslaufwerk *LW_Buchhaltung* in der Organisationseinheit *OU-B-Buchhaltung* die lokale Gruppe *LG-B-LW_Buchhaltung-L*.

- Klicken Sie im Snap-In *Active Directory-Benutzer und -Computer* mit der rechten Maustaste auf die gewünschte Organisationseinheit.
- Wählen Sie im Kontextmenü den Befehl *Neu - Gruppe*.
- Geben Sie den Gruppennamen ein.

Markieren Sie den Gruppennamen und kopieren Sie ihn in die Zwischenablage, dann können Sie ihn beim Erstellen der restlichen Gruppen wiederverwenden.

- Wählen Sie als Gruppenbereich die Option *Lokal (in Domäne)*.
- Legen Sie als Gruppentyp *Sicherheit* fest.

- Erstellen Sie die lokalen Gruppen mit den Endungen *AE*, *VZ* und *KZ* für die Zugriffe „Ändern“, „Vollzugriff“ und „Kein Zugriff“.

Sie können diese Gruppen auch zeitsparender einrichten, indem Sie dafür ein Skript verwenden. Wie das geht, wird am Ende des Kapitels beschrieben.

### Globale Gruppen in lokale Gruppen aufnehmen

Teilaufgabe 4: Für den Zugriff auf das Abteilungslaufwerk sollen folgende Zugriffsberechtigungen eingerichtet werden: Die Abteilungsleiterin erhält Vollzugriff, Sachbearbeiter erhalten Ändern-Zugriff und Praktikanten soll Lesen-Zugriff erteilt werden.

- Klicken Sie mit der rechten Maustaste auf die lokale Gruppe und wählen Sie im Kontextmenü *Eigenschaften*.
- Wechseln Sie auf die Registerkarte *Mitglieder* und klicken Sie auf *Hinzufügen*.

  Das Dialogfenster *Benutzer, Kontakte, Computer oder Gruppen wählen* wird geöffnet.
- Klicken Sie auf *Erweitert*.

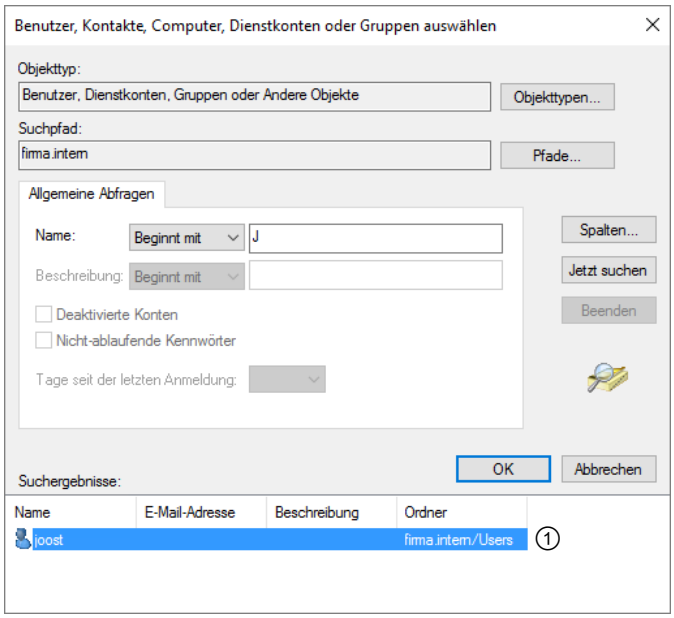
### Globale Gruppen auswählen

Wenn Sie eine Multidomänen-Umgebung verwenden, können Sie über *Pfade* den Eintrag *Gesamtes Verzeichnis* wählen, um alle verfügbaren Objekte aller Domänen der Gesamtstruktur auflisten zu lassen.

- Verwenden Sie im Listenfeld *Name* die Suchbedingung *Beginnt mit* und geben Sie `GG-B-B` ein.
- Klicken Sie auf *Jetzt suchen*.

  Die gefundenen Objekte werden unter *Suchergebnisse* angezeigt.
- Markieren Sie die gewünschten Gruppen und klicken Sie auf *OK*.

  Achten Sie auf die korrekte Domänen- und OU-Zugehörigkeit der einzelnen Objekte ①, um Irrtümer bei der Auswahl zu vermeiden.
- Wiederholen Sie den Vorgang für die verbleibenden lokalen Gruppen.




*Globale Gruppen zur lokalen Gruppe hinzufügen*

## 14.4 Gruppenplanung mit universalen Gruppen

### Universale Gruppen in Multidomänen-Umgebungen

Universale Gruppen werden nur in Gesamtstrukturen mit mehreren Domänen benötigt, die sich gegenseitig einen Zugriff auf ihre Daten ermöglichen sollen. Hier müssen allen globalen Gruppen aus allen Domänen über lokale Gruppen in jeder Domäne Zugriffsberechtigungen erteilt werden. Dieser Vorgang lässt sich durch die Zwischenschaltung einer universalen Gruppe vereinfachen.

Sollen stattdessen nur in einer Domäne Zugriffe berechtigt werden, so ist der Aufwand mit universalen Gruppen höher, als wenn Sie die globalen Gruppen aus der anderen Domäne direkt in die lokale Gruppe aufnehmen. Dasselbe gilt, wenn nur eine globale Gruppe in mehreren Domänen Zugriffe benötigt.


Schulversion
© HERDT-Verlag

Generell ist der Einsatz universaler Gruppen nur in Umgebungen mit mindestens drei Domänen erforderlich. Das folgende Beispiel soll dies verdeutlichen.

### Beispiel für universale Gruppen

Stellen Sie sich ein Unternehmen mit zehn Domänen vor. Jede dieser Domänen enthält eine Buchhaltungsabteilung und ein eigenes Abteilungslaufwerk. Jede Domäne verfügt außerdem über eine globale Gruppe für Buchprüfer, die Zugriff auf die Buchhaltungslaufwerke aller Domänen benötigt.

Sie könnten in jeder der zehn Domänen zehn globale Gruppen in die jeweilige lokale Gruppe für den Laufwerkszugriff aufnehmen, aber das sind dann 100 Gruppenmitgliedschaften, die Sie verwalten müssen.

Wenn Sie jedoch eine universale Gruppe erstellen und ihr die zehn globalen Buchprüfer-Gruppen hinzufügen, ist das zunächst mehr Aufwand. Anschließend müssen Sie jedoch nur eine einzige Gruppenmitgliedschaft verwalten, wenn Sie in jeder Domäne jeweils der lokalen Zugriffsgruppe die universale Buchprüfer-Gruppe hinzufügen. Damit kommen Sie insgesamt nur auf 10 + 10 + 1 = 21 Gruppenmitgliedschaften, die Sie verwalten müssen.

## 14.5 Universale Gruppen erstellen

### Universale Gruppe mit dem Active Directory-Verwaltungscenter erstellen

Wie oben beschrieben sind universale Gruppen bei nur einer Domäne eigentlich unnötig und die Erstellung wird hier nur zu Übungszwecken demonstriert. Dieses Mal erstellen Sie die Gruppen im Active Directory-Verwaltungscenter.

Bevor die universale Gruppe erstellt wird, müssen folgende Objekte eingerichtet werden:

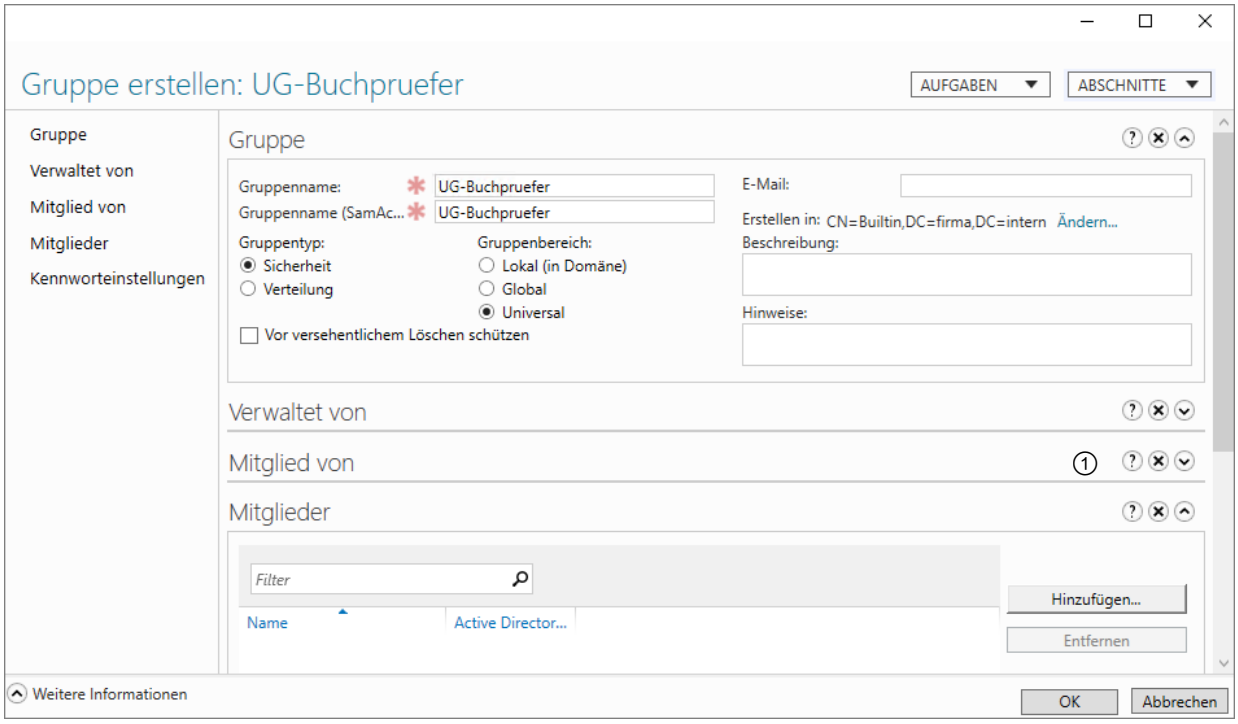
- Erstellen Sie in *firma.intern* die OU *OU-Buchpruefung*.
- Erstellen Sie in *OU-Buchpruefung* die globalen Gruppen *GG-Buchpruefer_Domaene1*, *GG-Buchpruefer_Domaene2* und *GG-Buchpruefer_Domaene3*.

In der Testumgebung soll in der OU *OU-Buchpruefung* die universale Gruppe *UG-Buchpruefer* erstellt werden, der bei der Erstellung schon die drei globalen Gruppen als Mitglieder hinzugefügt werden.

- Geben Sie im Startbildschirm `active` ein und wählen Sie das Active Directory-Verwaltungscenter aus.
- Wählen Sie im Active Directory-Verwaltungscenter die Organisationseinheit, in der Sie die Gruppe erstellen möchten.

  Verwenden Sie für diese Übung die OU *OU-Buchpruefung*.
- Klicken Sie im Bereich *Aufgaben* auf *Neu - Gruppe*.

  Das Fenster *Gruppe erstellen* wird geöffnet.




*Universale Gruppe erstellen und konfigurieren*

- Geben Sie als Namen für die Gruppe *UG-Buchpruefer* ein.
- Wählen Sie für diese Übung *Sicherheit* als *Gruppentyp* und *Universal* als *Gruppenbereich*.
- Geben Sie optional eine Beschreibung der Gruppe und weitere Hinweise ein.
- Geben Sie an, in welchen lokalen Gruppen ① die universale Gruppe Mitglied werden soll.
- Klicken Sie auf *Hinzufügen*, um neue Mitglieder zur universalen Gruppe hinzuzufügen.
- Wählen Sie im Dialog die globalen Gruppen aus, die Sie zu Mitgliedern der universalen Gruppe machen wollen. Wählen Sie für diese Übung die *GG-Buchpruefer_Domaene1*, *2* und *3* aus.
- Klicken Sie auf *OK*.

## 14.6 Gruppen mit einer Batchdatei anlegen

### Vorteile und Gefahren von Skripten

Skripte sind für zahlreiche Verwaltungsaufgaben bestens geeignet, die immer wiederkehrende komplexe Abläufe umfassen. Dabei sparen sie bei mehrfacher Verwendung nicht nur viel Zeit ein, sondern sie sorgen für weniger Probleme, z. B. durch versehentliches Verrutschen beim Klicken oder Tippfehler. Besonders bei stupider Wiederholung ist es nur eine Frage der Zeit, wann bei manuellen Eingaben Fehler auftreten.

Der Nachteil an Skripten ist, dass sie die enthaltenen Befehle ohne Rückfrage ausführen. Durch einen einzigen fehlerhaften Befehl kann das gesamte Active Directory in Mitleidenschaft gezogen werden und im schlimmsten Fall funktionsuntüchtig werden. Besonders verschachtelte Skripte mit rekursiven Befehlsfolgen, die aufeinander aufbauen, sowie die Verwendung von Variablen können durch kleinste Unachtsamkeiten unvorhergesehene Ergebnisse liefern.

Testen Sie Ihre Skripte und die darin enthaltenen Befehle zunächst in einer Testumgebung, bevor Sie sie in der Praxis einsetzen!


Schulversion
© HERDT-Verlag

## Die Kommandozeilentools der DS-Familie

Sie können Objekte im Active Directory auch auf der Kommandozeile verwalten. Dafür steht die Directory-Service-Befehlszeilenfamilie zur Verfügung, zu der die folgenden Befehle gehören:

- `dsadd`: Hinzufügen eines Objekts (Benutzer, Gruppe, Computer, OU oder Quota)
- `dsget`: Anzeige der Eigenschaften eines Objekts
- `dsmod`: Bearbeiten der Eigenschaften eines Objekts
- `dsmove`: Verschieben oder Umbenennen eines Objekts
- `dsquery`: Suche nach Objekten mithilfe von Suchkriterien

## Der Befehl `dsadd`

Um detaillierte Informationen zu dem Befehl zu erhalten, geben Sie in einer Eingabeaufforderung `dsadd /?` ein. Daraufhin werden eine Befehlsbeschreibung sowie die Befehlssyntax mit allen Parametern und Optionen angezeigt. Mehr Details erhalten Sie, wenn Sie den Befehl zusammen mit einer Option eingeben, z. B. `dsadd group /?`

Die Parameter und Optionen unterscheiden sich je nach Befehl, die Schreibweise für den Distinguished Name (also der eindeutige Name eines Objekts im Active Directory) ist jedoch immer gleich:

| Namensbestandteil | Beispiel eines Distinguished Names (DN) |
|---|---|
| CN=<Objektname> | *LG-B-LW_Buchhaltung-L* |
| OU=<Unter-OU> | *OU-Buchhaltung* |
| OU=<Stamm-OU> | *OU-Berlin* |
| DC=<Domäne> | *firma* |
| DC=<Domäne> | *intern* |

Der gesamte Pfad muss in Anführungszeichen gesetzt werden, wenn ein Bestandteil Leerzeichen enthält. Gewöhnen Sie sich an, jeden Pfad in Anführungszeichen zu setzen. Damit sind Sie in jedem Fall auf der sicheren Seite, z. B. wenn Sie fremde Skripte oder Active Directory-Strukturen bearbeiten müssen, die von anderen erstellt wurden. Besonders wichtig ist dies, falls Sie in den Skripten mit Variablen arbeiten, denn möglicherweise ist einmal eine Variable mit Leerzeichen dabei. Außerdem können Sie so optisch schneller erfassen, wo der Pfad zu Ende ist.

Sie sollten keine Leerzeichen **innerhalb** von Bezeichnungen verwenden. Ersetzen Sie wie in Kapitel 1 beschrieben alle Leerzeichen durch Unterstriche.

Die einzelnen Pfadbestandteile werden durch Kommas voneinander abgetrennt. Nach dem Pfad folgen weitere Optionen und Parameter. Für das Beispielskript wird nur die Option `-scope l` benötigt, die die Art der Gruppe festlegt (`l` = lokal, `g` = global, `u` = universal).

## Batchdatei für Abteilungslaufwerk erstellen

Für das Anlegen lokaler Gruppen bietet es sich an, eine Batchdatei zu erstellen, die mithilfe des Befehls `dsadd group` jeweils vier Gruppen erstellt, wenn eine Freigabe im Netz angelegt wird.

- Öffnen Sie den Editor und erstellen Sie folgende Datei:

```
Datei  Bearbeiten  Format  Ansicht  ?
dsadd group "CN=LG-B-LW_Verwaltung-L, OU=OU-B-Verwaltung, OU=OU-Berlin, DC=firma, DC=intern" -scope l
dsadd group "CN=LG-B-LW_Verwaltung-AE, OU=OU-B-Verwaltung, OU=OU-Berlin, DC=firma, DC=intern" -scope l
dsadd group "CN=LG-B-LW_Verwaltung-VZ, OU=OU-B-Verwaltung, OU=OU-Berlin, DC=firma, DC=intern" -scope l
dsadd group "CN=LG-B-LW_Verwaltung-KZ, OU=OU-B-Verwaltung, OU=OU-Berlin, DC=firma, DC=intern" -scope l
```

*Batchdatei für das Anlegen lokaler Gruppen*

- Speichern Sie die Datei unter einem aussagekräftigen Namen mit der Endung *.cmd* ab.

In der Praxis ist es sinnvoll, sich einen speziellen Ordner für Skripte zu erstellen. Ihre Skripte werden im Lauf der Zeit immer komplexer werden und Sie viel Arbeitszeit investieren. Die Skripte müssen also jederzeit auffindbar sein und eine unkomplizierte Sicherung ermöglichen.

Wenn Sie nun ein Abteilungslaufwerk für eine andere Abteilung erstellen wollen, müssen Sie nur mit *Suchen und Ersetzen* das Wort "Verwaltung" durch den entsprechenden Abteilungsnamen austauschen und die Batchdatei aufrufen.

## Einsatz von Variablen

Noch eleganter ist es, wenn Sie mit Variablen arbeiten. So können Sie am Anfang der Batchdatei mit `Set Abteilung=Marketing` die Variable `Abteilung` erstellen und ihr den Wert `Marketing` zuweisen. Im Skript müssen Sie jetzt nur noch in den Befehlen den Abteilungsnamen (Konstante) durch den Variablennamen (`%Abteilung%`) ersetzen.

```
Set Abteilung=Marketing
dsadd OU "OU=OU-B-%Abteilung%, OU=OU-Berlin, DC=firma, DC=intern"
```

Leider müssen Sie immer noch im Editor etwas ändern, also wäre es wünschenswert, wenn Sie die Variablen beim Aufruf des Skriptes eingeben könnten. Dies lässt sich einrichten, indem Sie im Skript eintragen:

```
Set Abteilung=%1
```

Beim Aufruf des Skriptes wird nun der Variablen `%Abteilung%` das erste Wort zugewiesen, das Sie nach dem Skriptnamen eingegeben haben. %2 ist das zweite Wort, %3 das dritte usw. Dies ist übrigens ein gutes Beispiel, warum Leerzeichen in Skripten problematisch sind.

Schauen Sie sich diesen Anfang eines Skriptes an:

```
set Standort=%1
set Kurz=%2
set Abteilung=%3
set DC1=firma
set DC2=intern
```

Hier werden beim Aufruf des Skriptes der Standort (*Berlin*), die Kurzform davon (*B*) und der Abteilungsname (*Marketing*) übergeben. Der Domänenname ändert sich nicht jedes Mal, daher ist er fest im Skript als Konstante eingetragen.

Der Aufruf des Skriptes sieht z. B. so aus:

```
NeueAbteilung.cmd Berlin B Marketing
```


Schulversion
© HERDT-Verlag

## Gruppen zu Mitgliedern anderer Gruppen machen

Sie können eine neue Gruppe einer bestehenden Gruppe hinzufügen:

```
dsadd group <Gruppe> -memberof <Gruppe>
```

Dies ist vor allem für Sammelgruppen interessant. Hier einige Beispiele für Sammelgruppen:

- alle Abteilungsleiter einer Domäne
- alle Mitarbeiter einer Abteilung
- alle Sachbearbeiter eines Standorts
- alle Praktikanten

Im folgenden Beispiel wird eine globale Gruppe für die Abteilungsleiter der Abteilung erstellt, die außerdem Mitglied der Sammelgruppe aller Abteilungsleiter ist. Die Sammelgruppe wird in einer bereits vorhandenen *OU-Sammelgruppen* in *OU-Berlin* erstellt.

```
dsadd group "CN=GG-B-Marketing-Abteilungsleiter, OU=OU-B-Marketing, OU=OU-
Berlin, DC=firma, DC=intern" -memberof "CN=SG-Abteilungsleiter, OU=OU-
Sammelgruppen, OU=OU-Berlin, DC=firma, DC=intern"
```

Das Gegenstück zu `-memberof` ist `-member`, mit dem Sie einer Gruppe Mitglieder hinzufügen können. Mehrere Objekte werden mit Kommas voneinander abgetrennt.

Sie können dieses Skript immer weiter ausbauen, um Vorgänge zu automatisieren. So benötigen Sie beim Erstellen einer neuen Abteilung stets die gleichen Objekte:

- die neue OU;
- globale Gruppen für Abteilungsleiter, Sachbearbeiter, Praktikanten, Azubis und Sonstige;
- einen Freigabeordner für das Abteilungslaufwerk;
- vier lokale Gruppen für das Abteilungslaufwerk, Mitgliedschaft der entsprechenden GGs;
- eine Verteilergruppe für alle Mitarbeiter der Abteilung;
- einen Standardbenutzer für die Abteilung, der schon Mitglied einer globalen Gruppe ist;
- die Mitgliedschaft in Sammelgruppen, z. B. alle Abteilungsleiter eines Standorts.

Verteilergruppen werden durch die Option `-secgrp no` erstellt. Da hier der Standard auf `yes` gesetzt ist, kann die Option beim Erstellen einer Sicherheitsgruppe weggelassen werden.

Das Skript lässt sich prinzipiell beliebig erweitern. So können Sie hinzufügen, dass die Informationen der Benutzer, die der Abteilung hinzugefügt werden sollen, aus einer Textdatei entnommen werden. Dann werden die Benutzer automatisch in der richtigen OU erstellt und auch gleich den entsprechenden Gruppen hinzugefügt. Alles, was Sie noch angeben müssen, sind der Name der OU, ein Speicherort für das Abteilungslaufwerk und eine Liste mit den Benutzerdaten.

## Erweitertes Beispielskript

Das folgende Skript bekommt beim Aufruf den Standort *Berlin* ①, das Standortkürzel *B* ② und den Abteilungsnamen *Marketing* ③ übergeben. Daraufhin wird Folgendes automatisch ausgeführt:

- *OU-Marketing* wird in *OU-Berlin* erstellt ④.
- *GG-B-Marketing-Abteilungsleiter* wird erstellt und Mitglied in *SG-B-Abteilungsleiter* ⑤ in *SG-B-Sammelgruppen,* analoges Vorgehen für Sachbearbeiter ⑥ und Praktikanten ⑦.
- Die Sammel-Verteilergruppe *SGV-B-Marketing* wird in *SG-Sammelgruppen* erstellt ⑧ und die GGs für Abteilungsleiter, Sachbearbeiter und Praktikanten werden hinzugefügt ⑨.
- Die lokalen Gruppen *LG-B-LW_Marketing-L*, *-AE*, *-VZ* und *-KZ* werden in *OU-B-Lokale_Gruppen* erstellt ⑩ und die GGs für Abteilungsleiter, Sachbearbeiter und Praktikanten werden hinzugefügt.

NeueAbteilung - Editor

Datei Bearbeiten Format Ansicht ?

```
@echo off
REM Die Variablen für Standort, Standortkürzel und Abteilung werden beim Aufruf übergeben, die Domäne ist fest eingetragen

set Standort=%1 ①
set Kurz=%2     ②
set Abteilung=%3 ③
set DC1=firma
set DC2=intern

REM Abteilungs-OU erstellen: ④
dsadd ou "OU=OU-%Kurz%-%Abteilung%, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%"

REM GG für Abteilungsleiter, Sachbearbeiter und Praktikanten, Mitgliedschaft in Sammelgruppen (SG):

dsadd group "cn=GG-%Kurz%-%Abteilung%-Abteilungsleiter, OU=OU-%Kurz%-%Abteilung%, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%" ⑤
-memberof "cn=SG-%Kurz%-Abteilungsleiter, OU=OU-%Kurz%-Sammelgruppen, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%"

dsadd group "cn=GG-%Kurz%-%Abteilung%-Sachbearbeiter, OU=OU-%Kurz%-%Abteilung%, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%"  ⑥
-memberof "cn=SG-%Kurz%-Sachbearbeiter, OU=OU-%Kurz%-Sammelgruppen, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%"

dsadd group "cn=GG-%Kurz%-%Abteilung%-Praktikant, OU=OU-%Kurz%-%Abteilung%, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%"  ⑦
-memberof "cn=SG-%Kurz%-Praktikant, OU=OU-%Kurz%-Sammelgruppen, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%"

REM Einrichten einer Sammel-Verteilergruppe (SGV) für alle Mitarbeiter der Abteilung: ⑧

dsadd group "cn=SGV-%Kurz%-%Abteilung%, OU=OU-%Kurz%-Sammelgruppen, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%" -secgrp no -scope g
-member "cn=GG-%Kurz%-%Abteilung%-Abteilungsleiter, OU=OU-%Kurz%-%Abteilung%, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%", ⑨
"cn=GG-%Kurz%-%Abteilung%-Sachbearbeiter, OU=OU-%Kurz%-%Abteilung%, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%",
"cn=GG-%Kurz%-%Abteilung%-Praktikant, OU=OU-%Kurz%-%Abteilung%, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%"

REM Einrichten der lokalen Gruppen L, AE, VZ und KZ für das Abteilungslaufwerk in OU Lokale_Gruppen ⑩
REM Hinzufügen der entsprechenden GGs, z.B. Lesen für Praktikanten, Vollzugriff für Abteilungsleiter etc.

dsadd group "cn=LG-%Kurz%-LW_%Abteilung%-L, OU=OU-%Kurz%-Lokale_Gruppen, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%" -scope l
-member "cn=GG-%Kurz%-%Abteilung%-Praktikanten, OU=OU-%Kurz%-%Abteilung%, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%"

dsadd group "cn=LG-%Kurz%-LW_%Abteilung%-AE, OU=OU-%Kurz%-Lokale_Gruppen, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%" -scope l
-member "cn=GG-%Kurz%-%Abteilung%-Sachbearbeiter, OU=OU-%Kurz%-%Abteilung%, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%"

dsadd group "cn=LG-%Kurz%-LW_%Abteilung%-VZ, OU=OU-%Kurz%-Lokale_Gruppen, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%" -scope l
-member"cn=GG-%Kurz%-%Abteilung%-Abteilungsleiter, OU=OU-%Kurz%-%Abteilung%, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%"

dsadd group "cn=LG-%Kurz%-LW_%Abteilung%-KZ, OU=OU-%Kurz%-Lokale_Gruppen, OU=OU-%Standort%, DC=%DC1%, DC=%DC2%" -scope l
```

## Cmdlets für die Remoteverwaltung und Abrufen der Hilfe

Mit der PowerShell können Sie ebenfalls Benutzer verwalten, auch über das Netzwerk. Befehle in der PowerShell tragen die Bezeichnung „Cmdlets“. Nicht alle Cmdlets eignen sich für eine Remoteverwaltung von Servern. Sie können vor allem die Cmdlets nutzen, welche über die Option *-ComputerName* verfügen. Um sich alle Cmdlets anzeigen zu lassen, die diese Option unterstützen, also Server auch über das Netzwerk verwalten können, hilft der Befehl `Get-Help * -Parameter ComputerName`.

Wollen Sie ausführliche Hilfen anzeigen, bietet das *Get-Help*-Cmdlet noch die Möglichkeit, ausführliche Hilfen und Beispiele anzuzeigen, beispielsweise mit den Optionen `-Examples`, `-Detailed` und `-Full`.

Geben Sie `Get-Command` ein, sehen Sie alle Befehle, welche die Shell zur Verfügung stellt.

Haben Sie nur den Teil eines Befehls in Erinnerung, können Sie mit dem Platzhalter `*` arbeiten. Der Befehl `Get-Command *user` zeigt zum Beispiel alle Cmdlets an, deren Namen mit *user* endet. Ist der gesuchte Befehl nicht dabei, können Sie auch mehrere Platzhalter verwenden, zum Beispiel den Befehl `Get-Command *user*`. Dieser Befehl zeigt alle Befehle an, in denen das Wort »user« vorkommt.

Wurde das gewünschte Cmdlet gefunden, unterstützt die PowerShell mit weiteren Möglichkeiten. Für nahezu alle Cmdlets gilt die Regel, dass diese in vier Arten vorliegen: Es gibt Cmdlets mit dem Präfix *New-* um etwas zu erstellen, zum Beispiel *New-ADUser*. Das gleiche Cmdlet gibt es dann immer noch mit *Remove-*, um etwas zu löschen, zum Beispiel *Remove-ADUser*.


Schulversion
© HERDT-Verlag

Wollen Sie das Objekt anpassen, gibt es das Präfix *Set-*, zum Beispiel *Set-ADUser*. Als Letztes gibt es noch das Cmdlet *Get-*, zum Beispiel *Get-ADUser*, um Informationen zum Objekt abzurufen. Neben dieses Cmdlets gibt es natürlich noch viele andere, zum Beispiel Start- und Stop-Cmdlets, oder Export- und Import-Cmdlets. Geben Sie nur diesen Befehl ein, passiert entweder überhaupt nichts, das Cmdlet zeigt alle Objekte an, oder Sie werden nach der Identität des Objekts gefragt. So listet das Cmdlet *Get-ADUser -Filter **  alle Benutzer der Organisation auf.

Mit dem Befehl `Help <Cmdlet>` erhalten Sie eine Hilfe zum entsprechenden Cmdlet, zum Beispiel `Help New-ADUser`. Für viele Cmdlets gibt es noch die Option `Help <Cmdlet> -Detailed`. Dieser Befehl bietet noch mehr Informationen. Mit dem Befehl `Help <Cmdlet> -Examples` lassen sich Beispiele für den Befehl anzeigen. Auch das funktioniert für alle Befehle in der PowerShell.

Rufen Sie eine Hilfe zu Cmdlets auf, kann sich die PowerShell selbstständig aktualisieren. Das funktioniert auch, wenn Sie für das Cmdlet *Get-Help* die Option *-Online* verwenden, zum Beispiel mit *Get-Help Get-Command-Online*. Die PowerShell bietet das Cmdlet *Update-Help*, welches die Hilfedateien der PowerShell aktualisieren kann.

Dazu muss der Server über eine Internetverbindung verfügen. Der Befehl ruft die Hilfe direkt aus dem Internet ab. Ebenfalls eine interessante Funktion in der PowerShell ist das Cmdlet *Show-Command*. Dieses blendet ein neues Fenster mit allen Befehlen ein, die in der PowerShell verfügbar sind. Sie können im Fenster nach Befehlen suchen und sich eine Hilfe zum Befehl anzeigen lassen, sowie Beispiele dazu.

Mit *Get-Cmdlets* lassen Sie sich Informationen zu Objekten anzeigen. Die Option `|fl` formatiert die Ausgabe. Wollen Sie aber nicht alle Informationen, sondern nur einzelne Parameter anzeigen, können Sie diese nach der Option `|fl` anordnen. Wollen Sie zum Beispiel für Benutzer nur den Distinguished Name und den Status anzeigen lassen, verwenden Sie den Befehl `Get-ADUser -Filter * |fl DistinguishedName, Enabled`. Groß- und Kleinschreibung spielen für die Cmdlets keine Rolle.

Sie können in der PowerShell auch eine Remotesitzung auf einem Server starten. Am besten verwenden Sie dazu die PowerShell Integrated Scripting Environment (ISE). Nach dem Start können Sie eine Verbindung mit *Datei - Neue Remote-PowerShell-Registerkarte öffnen*. Hier geben Sie einen Servernamen und einen Benutzernamen ein, mit dem Sie sich verbinden wollen.

Um eine Remotesitzung in der normalen PowerShell aufzubauen, verwenden Sie das Cmdlet *New-PSSession*. Mit `Enter-PSSession <Servername>` bauen Sie eine Verbindung auf. Mit `Exit-Session` beenden Sie diese Sitzung wieder. Neu ist die Möglichkeit, Sitzungen zu unterbrechen und neu aufzubauen. Bei unterbrochenen Sitzungen laufen die Cmdlets weiter, auch wenn Sie sich vom Server getrennt haben. Dazu nutzen Sie die neuen Cmdlets *Disconnect-PSSession, Connect-PSSession* und *Receive-PSSession*.

## Ausblick

Dieses Beispielskript zeigt nur einen kleinen Teil der Möglichkeiten, die Ihnen mit den Kommandozeilenbefehlen zur Verfügung stehen. Es soll die Nützlichkeit dieser Administrationsweise demonstrieren. Sie können das Skript beliebig erweitern und an Ihre Bedürfnisse anpassen. Hilfe und Anregungen dazu finden Sie im Internet.

# 15 Rechte und Berechtigungen

**In diesem Kapitel erfahren Sie**

- was Rechte sind
- was Berechtigungen sind

**Voraussetzungen**

- wie Sie Rechte und Berechtigungen einsetzen können
- Gruppen verwalten

## 15.1 Definitionen

### Was sind Rechte?

Ein Recht ist die Erlaubnis oder ein Verbot, auf einem System bestimmte Handlungen durchzuführen. Rechte gelten stets systemweit. Sie werden in den lokalen Sicherheitseinstellungen oder durch Gruppenrichtlinien definiert.

Typische Beispiele für Rechte betreffen Tätigkeiten wie das Installieren von Treibern, lokale Anmeldungen, den Zugriff auf bestimmte Bereiche der Registry, das Ändern der Systemzeit oder das Anlegen von Benutzerkonten.

Rechte werden für bestimmte Benutzer oder Gruppen definiert, wobei bestimmte Gruppen von Rechten bestimmten vom System angelegten Konten in Paketen zugewiesen werden. So gibt es etwa die Gruppe der Sicherungsoperatoren, die unter anderem das Recht haben, Daten zu sichern und wiederherzustellen. Der Unterschied zum Benutzer, der Berechtigungen auf einige Ordner oder Dateien hat, ist, dass die Berechtigung nur an das Objekt gekoppelt ist, während das Recht für ein ganzes System gilt. Entweder darf ein Benutzer Sicherungen anfertigen oder nicht. Es ist nicht möglich, jemandem das Recht zum Sichern oder Wiederherstellen auf Objektebene zu gewähren.

### Was sind Berechtigungen?

Berechtigungen werden an Objekte gekoppelt. Sie definieren, dass ein Benutzer, eine Gruppe oder ein Computer bestimmte Handlungen an einem Objekt durchführen darf. Die Berechtigungen werden auch in den Eigenschaften des Objektes gespeichert. So gibt es die Berechtigung zum Drucken, die in der Discretionary Access Control List (DACL) des Druckers gespeichert ist und nur für dieses Druckerobjekt gilt.

#### Berechtigungen verweigern

Berechtigungen können gewährt oder verweigert werden. Dabei ist das Verweigern stets stärker als das Gewähren. Entnehmen Sie dies dem folgenden Beispiel:

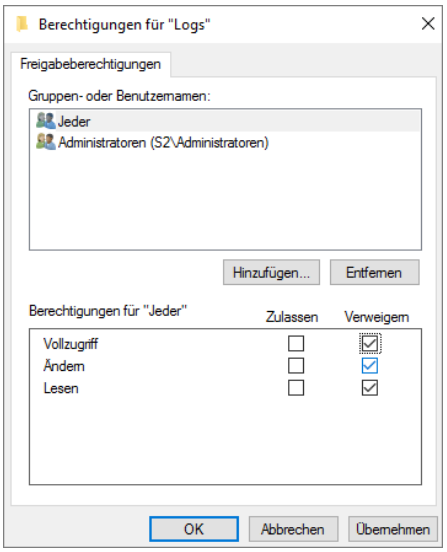
Im Netzwerk gibt es ein freigegebenes Verzeichnis *LW_Buchhaltung*. Über die lokale Gruppe *LG-B-LW_Buchhaltung-AE* hat die globale Gruppe *GG-B-Buchhaltung* Ändern-Berechtigungen auf das Verzeichnis und alle untergeordneten Objekte erhalten. Unterhalb des Verzeichnisses gibt es aber auch das Verzeichnis *Lohn- und Gehaltslisten*. Dieses darf nicht von Mitarbeitern eingesehen werden, die sich noch in der Ausbildung befinden. Daher wird für dieses Verzeichnis der Gruppe *GG-B-Buchhaltung-Azubis* über die Mitgliedschaft in der lokalen Gruppe *LG-B-LW_Buchhaltung-KZ* das Recht Vollzugriff verweigert. Obwohl die Auszubildenden also über die Mitgliedschaft in der Gruppe *GG-B-Buchhaltung* Zugriff erhalten, werden sie explizit ausgeklammert, indem ihnen das Recht an anderer Stelle genommen wird.


Schulversion
© HERDT-Verlag

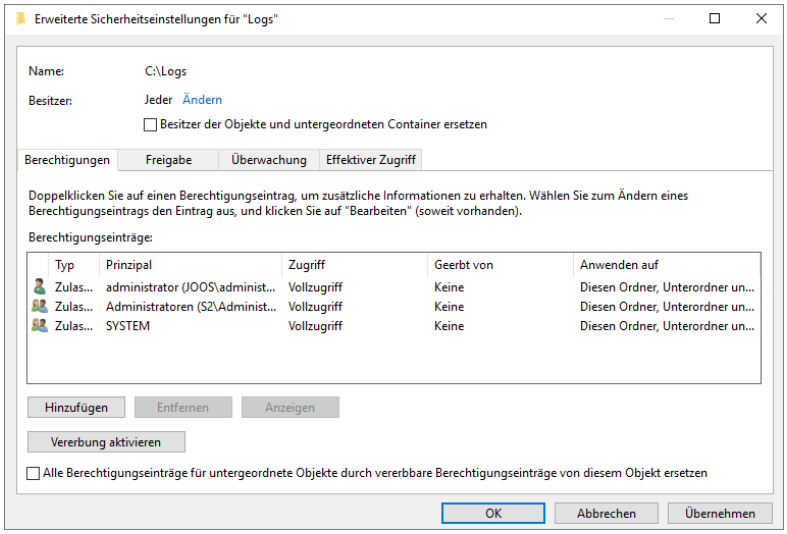
## Arten von Berechtigungen

Berechtigungen unterscheiden sich je nach Art des Objektes, an das sie gebunden sind. Die wichtigsten Arten von Berechtigungen für bestimmte Objekttypen zeigt die folgende Tabelle:

| | |
|---|---|
| Freigabeberechtigungen | Freigabeberechtigungen gelten bei Zugriff auf ein Verzeichnis über den Netzwerkpfad.<br>Auf Freigaben können generell die maximalen Berechtigungen vergeben werden, die ein Benutzer anschließend auf Dateien oder Verzeichnisse erhalten kann, die sich unterhalb dieser Freigabe befinden. Mögliche Freigabeberechtigungen sind:<br>✔ Lesen<br>✔ Ändern<br>✔ Vollzugriff |
| NTFS-Berechtigungen | NTFS-Berechtigungen gelten bei jedem Zugriff auf ein Verzeichnis, egal ob er über das Netzwerk oder lokal erfolgt.<br>Mit NTFS-Berechtigungen kann ein sehr differenzierter Zugriff auf Dateien oder Verzeichnisse und deren Eigenschaften gesteuert werden. Dabei kann auch festgelegt werden, ob dies nur für den Speicherort selbst, nur für Dateien, nur für Unterordner oder für eine Kombination aus diesen gelten soll. |
| Berechtigungen auf Drucker | Auf Drucker lassen sich drei Standard-Berechtigungen vergeben:<br>✔ Drucken<br>✔ Drucker verwalten<br>✔ Dokumente verwalten<br>Daneben können noch spezielle Berechtigungen vergeben werden. Diese betreffen das Lesen und Ändern von Berechtigungen und den Besitz am Druckerobjekt. |
| Berechtigungen auf Objekte im Active Directory | Im Active Directory lassen sich auf jedes Objekt eine Vielzahl von fein abgestimmten Berechtigungen vergeben. Sie können den Lese- und Schreibzugriff auf fast jedes einzelne Attribut eines Objektes differenziert steuern.<br>In aller Regel wird davon allerdings kein expliziter Gebrauch gemacht. Stattdessen werden mit dem Assistenten für das Zuweisen von Verwaltungsaufgaben bestimmten Gruppen typische Aufgaben wie etwa das Zurücksetzen von Kennwörtern zugeteilt. |




*Freigabeberechtigungen*




*Erweiterte NTFS-Berechtigungen*

### Modell für Freigabe- und NTFS-Berechtigungen

Da das Verständnis von Freigabe- und NTFS-Berechtigungen erfahrungsgemäß etwas schwierig ist, soll das folgende Modell versuchen, den Unterschied zu erklären:

Sie möchten ein Gebäude (die Freigabe) über den Eingang 1 betreten. Bevor Sie eintreten dürfen, werden Ihre Personalien überprüft. Die Kontrolle ergibt, ob Sie überhaupt hereinkommen dürfen, und wenn ja, welche Ausstattung Sie beim Eintritt erhalten. Sie erhalten eine Brille zum Lesen, jedoch keinen Stift zum Schreiben. Sie dürfen eintreten und sich im Gebäude frei bewegen, es mag jedoch bestimmte Bereiche und Räume geben, die für Sie gesperrt sind. Dies entspricht einer Freigabeberechtigung.

An den Türen zu allen Räumen wird durch Wachpersonal kontrolliert, was Sie in dem Raum tun und ob Sie Ihre Brille verwenden dürfen. Die Prüfung ergibt keinerlei Beschränkungen und Sie können eintreten und mit Ihrer Brille alle möglichen Dokumente ansehen. Dies entspricht der NTFS-Berechtigung.

Auch wenn Ihnen der Wächter beliebige Änderungen im Raum erlaubt hat, könnten Sie diese nicht ausführen, da Sie ja beim Eintritt nur eine Brille und keinen Stift erhalten haben.

Die Freigabeberechtigungen (Kontrolle am Eingang 1) definieren also das Maximum, das Sie an Berechtigungen im NTFS-Dateisystem (den Räumen) ausüben können.

## Indirekte Steuerung des Zugriffs

Berechtigungen können vererbt werden. Das bedeutet, dass ein Benutzer Zugriff auf ein Objekt bekommt, ohne dass Sie diesen Zugriff für ihn explizit erteilen.

## Effektive Berechtigungen

Welche Berechtigung ein Benutzer tatsächlich auf das Objekt hat, ergibt sich aus der Summe aller Berechtigungen, die ihm …

- direkt gewährt oder verweigert werden,
- durch Vererbung gewährt oder entzogen werden.

### Regeln für effektive Berechtigungen

| | |
|---|---|
| Gewährende Berechtigungen addieren sich auf. | Wenn ein Benutzer drucken darf, weil er in der lokalen Gruppe *LG-Abteilungsdrucker-Drucken* ist, und Drucker verwalten darf, weil er in der lokalen Gruppe *LG-B-DruckerSupport* ist, darf er sowohl drucken als auch Drucker verwalten. |
| Verweigernde Berechtigungen werden abgezogen. | Restriktiver Charakter der Zugriffsverweigerung<br>Wenn festgelegt wurde, dass ein Benutzer auf einem bestimmten Drucker nicht drucken darf, ändert sich das auch nicht dadurch, dass er Mitglied in einer Gruppe ist, die drucken darf. |

## Empfehlungen für die Vergabe von Berechtigungen

### Keine Berechtigungen an Einzelbenutzer vergeben

Weisen Sie Berechtigungen nie einzelnen Benutzern zu, sondern verwenden Sie hierfür stets domänenlokale Gruppen. Wenn sich der Aufgabenbereich eines Benutzers ändert, wird dieser aus seinen globalen Gruppen entfernt und die Zugriffe auf die alten Objekte verschwinden automatisch. Steht der Benutzer aber als Einzelobjekt in einer Zugriffsliste (Access Control List, ACL), so kann das Active Directory ihn nicht aus dieser entfernen, da es ja nichts davon weiß. Auch beim Kopieren von Benutzern gehen diese Informationen verloren.


Schulversion
© HERDT-Verlag

### Nur globale Gruppen in lokale Gruppen aufnehmen

Wenn Sie Benutzer anderer Domänen direkt in domänenlokale Gruppen oder beliebige Benutzer in lokale Gruppen aufnehmen, kann das Verzeichnis dies ebenfalls nicht verwalten. Daher sollten Sie streng der Regel folgen, nur globale oder universale Gruppen in lokale Gruppen aufzunehmen.

### Ausnahmen: Benutzerprofil und Basisordner

Das servergespeicherte Benutzerprofil und der Basisordner eines Benutzers stellen die einzigen Ausnahmen von diesen Regeln dar. Bei ihnen wird der Zugriff vom System automatisch auf den einzelnen Benutzer verrechtet, und nur in Ausnahmefällen sollte eine händische Korrektur erfolgen. Solch eine Ausnahme könnte z. B. vorliegen, wenn alle Benutzer ein identisches Profil verwenden sollen, das nicht geändert werden darf.

### Vollzugriff

Für jedes Objekt gibt es die Standardberechtigung Vollzugriff. Sie gewährleistet, dass das jeweilige Objekt in vollem Umfang verwaltet werden kann. Es sollte nach Möglichkeit immer eine Benutzergruppe oder ein Benutzer den Vollzugriff auf ein Objekt haben. Auch ein Administrator kann ein Objekt nicht in vollem Umfang verwalten, wenn er den Vollzugriff selbst nicht innehat. Er kann sich aber den Vollzugriff stets erteilen, indem er den Besitz an dem Objekt übernimmt.

## 15.2 Vererbung von Berechtigungen

### Übertragung von Berechtigungen

Berechtigungen können ausgehend vom übergeordneten Objekt auf untergeordnete Objekte übertragen werden. Diese Vererbung wird jeweils am untergeordneten Objekt festgelegt. Sie können beim Verändern von Berechtigungen jedoch festlegen, ob die neuen Berechtigungen auf untergeordnete Objekte vererbt werden sollen.

### Standardeinstellungen für die Berechtigungsvererbung

Die Berechtigungsvererbung ist für alle Objekte standardmäßig aktiviert.

Gleichzeitig sind Standardberechtigungen für die unterschiedlichen Objekttypen definiert: Verschiedene originale Benutzergruppen haben die erforderlichen Berechtigungen, um ein bestimmtes Objekt nutzen oder verwalten zu können. Damit ist sichergestellt, dass ein neu erstelltes Objekt sowohl verwaltet (Administratoren) als auch generell in Betrieb genommen werden kann (Systemkomponenten).

### Vererbung von Berechtigungen verhindern

Sie haben die Möglichkeit, die Vererbung auszuschließen. Die Konfiguration nehmen Sie jeweils am betreffenden untergeordneten Objekt vor.

Anschließend gewähren Sie Zugriffe auf das Objekt für die verschiedenen Benutzergruppen explizit. Hierfür stehen zwei Vorgehensweisen zur Verfügung.

### Vererbung von Berechtigungen für ein Objekt komplett unterbinden

Hierzu müssen Sie die Übernahme von Berechtigungen beim untergeordneten Objekt ausschalten. Anschließend bestimmen Sie, ob die Berechtigungen, so wie sie ursprünglich vererbt werden sollten, in das Objekt kopiert werden sollen. Der so erstellte Satz von Berechtigungen bildet die Grundlage für Ihre individuellen Anpassungen. Sie können allerdings auch beim Ausschalten der Vererbung festlegen, dass alle Berechtigungen entfernt werden sollen. Dann müssen Sie die Berechtigungen komplett neu vergeben.

### Einzelne Berechtigungen ausschalten

Nach dem Kopieren der Berechtigungen haben Sie die Möglichkeit, Berechtigungen, die durch Kopieren der vererbten Einstellungen auf das Objekt übergegangen sind, durch Deaktivieren von Kontrollfeldern zu revidieren.

# 16 Active Directory-Berechtigungen verwalten

**In diesem Kapitel erfahren Sie**

- wie Sie mit Berechtigungen die Zugriffe auf Objekte steuern können
- wie Berechtigungen auf untergeordnete Objekte vererbt werden
- wie Sie die Verwaltung von Objekten an andere Personen delegieren
- welche Vorteile der Einsatz angepasster Verwaltungstools hat
- wie Sie eine Verwaltungskonsole erstellen
- wie Sie Aufgabenblöcke erstellen und verwalten
- die Bedeutung des Objektbesitzes

**Voraussetzungen**

- Active Directory-Objekte
- Gruppen verwalten

## 16.1 Objektverwaltung

### Delegierung der Objektverwaltung

Sie haben die Möglichkeit, einzelne Benutzer oder Benutzergruppen mit der Verwaltung von Objekten oder Attributen zu betrauen. Jedoch ist es wenig sinnvoll, Verwaltungsaufgaben für einzelne Objekte zu erteilen. Vielmehr empfiehlt es sich, gleich die Verwaltung mehrerer Objekte zu übertragen, beispielsweise vieler gleichartiger Objekte oder aller Objekte, die im Zusammenhang mit einem bestimmten Geschäftsbereich stehen.

In der Praxis werden bestimmten Benutzergruppen Zuständigkeiten für einige Objekttypen oder Objektattribute an einem Standort oder in einer Abteilung zugewiesen. Typische Beispiele hierfür sind:

- Verwaltung von Computerkonten an fernen Standorten durch einen lokalen Workstation-Betreuer,
- Kontenoperationen wie das Zurücksetzen des Kennworts durch den Abteilungsleiter,
- Mitgliedschaften von Projektgruppen ändern,
- Verwalten von Personaldaten durch Mitarbeiter der Personalabteilung,
- Verwalten von Kontaktdaten durch Mitarbeiter der Kundendienstabteilung.

### Delegierbare Verwaltungsaufgaben

- Objekte erstellen, bearbeiten, löschen
- Spezielle Berechtigungen für Attribute von Objekten bearbeiten


Schulversion
© HERDT-Verlag

## 16.2 Berechtigungen und Berechtigungsvererbung überprüfen und verwalten

### Aufgabenstellung

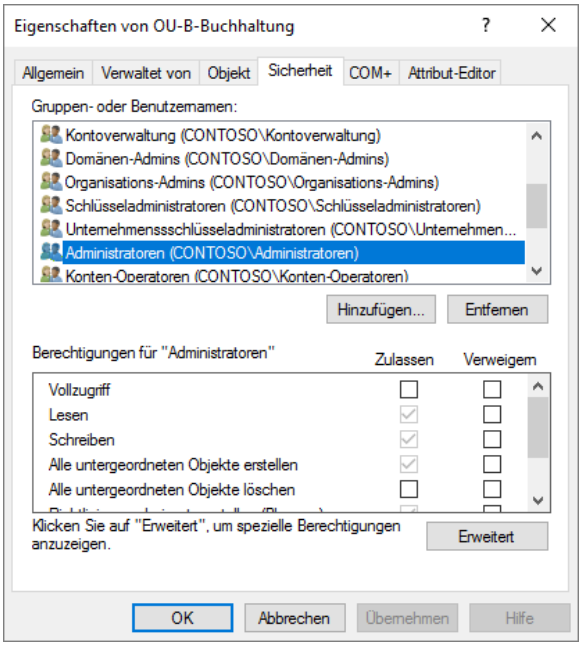
Am Beispiel der Organisationseinheit *OU-B-Buchhaltung* sollen die standardmäßigen Berechtigungen, die speziellen Berechtigungen und die Berechtigungsvererbung überprüft werden.

### Active Directory-Standardberechtigungen anzeigen

- Rufen Sie im Startmenü bei den Verwaltungsprogrammen *Active Directory-Benutzer und -Computer* auf. Sie können das Programm auch durch Eingabe von „dsa.msc“ im Suchfeld des Startmenüs starten.
- Aktivieren Sie den Menüpunkt *Ansicht - Erweiterte Features*.
- Klicken Sie mit der rechten Maustaste auf *OU-B-Buchhaltung* und wählen Sie den Kontextbefehl *Eigenschaften*.
- Wählen Sie das Register *Sicherheit*.

### Berechtigte und Berechtigungen

Das Register *Sicherheit* zeigt für ein Objekt die in der Access Control List (ACL) festgelegten ACEs (Access Control Entries, wörtlich übersetzt: Zugriffskontrolleinträge) an. Dabei ist es unerheblich, ob es sich bei dem Objekt um einen Dateiordner, einen Drucker oder wie hier eine OU handelt. Im oberen Bereich sind die Gruppen und Benutzer aufgeführt, die Berechtigungen für den Objektzugriff besitzen. Im unteren Bereich werden die Standardberechtigungen für die markierte Gruppe angezeigt, die über je ein Kontrollfeld zum Zulassen und Verweigern verfügen. Mit einem Klick auf *Erweitert* ③ öffnen Sie den Dialog *Erweiterte Sicherheitseinstellungen*, wo Sie die einzelnen Berechtigungen anzeigen und ändern können.



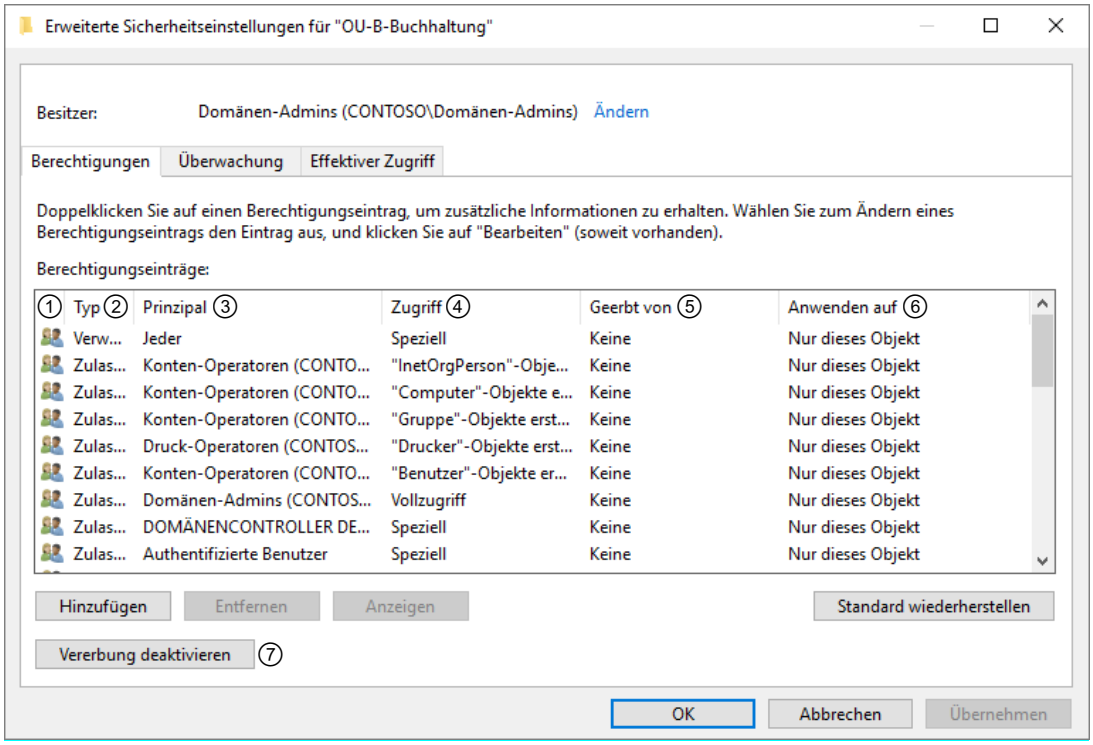

### Berechtigungsvererbung

Die durch Vererbung wirksamen Berechtigungen erkennen Sie an der grauen Färbung. Berechtigungen, die nicht ererbt, sondern direkt erteilt wurden, werden mit schwarz markierten Kontrollfeldern angezeigt.

### Aufgabe 1 – Berechtigungseinträge anzeigen

- Zeigen Sie die standardmäßigen Berechtigungen für die Gruppe *Domänen-Administratoren* an.
  Welche gewährenden und welche verweigernden Standardberechtigungen sind definiert?
  Wie sind diese Berechtigungen offenbar zustande gekommen?
- Klicken Sie auf *Erweitert*, um die erweiterten Sicherheitseinstellungen zu öffnen.

Die erweiterten Sicherheitseinstellungen verfügen über drei Registerkarten. Hier werden die Berechtigungen, die Überwachung und die effektiven Zugriffsberechtigungen angezeigt. Im oberen Bereich des Fensters werden der Datei- oder Ordnername und der Besitzer angezeigt. Über den Link *Ändern* können Sie den Besitz übertragen.




In der Liste werden die Berechtigungseinträge aus der ACL aufgelistet. Falls einer Gruppe verschiedene Berechtigungen erteilt wurden, sind mehrere Einträge zu sehen. So sind die Berechtigungseinträge aufgebaut:

- Das Symbol ① zeigt, ob es sich um eine Gruppe oder ein Einzelkonto handelt.
- Der *Typ* ② kann *Zulassen* oder *Verweigern* sein.
- Der *Prinzipal* ③ ist der Name des Benutzers oder der Gruppe.
- Unter *Zugriff* ④ wird die Art der Berechtigung angezeigt (Vollzugriff, Lesen, Ausführen, Ändern etc.).
- Unter *Geerbt von* ⑤ wird angezeigt, von wo die Zugriffsrechte vererbt wurden.
- *Anwenden auf* ⑥ zeigt, für welche Dateien, Ordner und Unterordner die Berechtigung gilt.

Der Eintrag *Speziell* unter *Zugriff* ④ bedeutet, dass hier eine Kombination von Berechtigungen vergeben wurde, die nicht mit einer Standardberechtigung abgedeckt werden konnte. Mit einem Doppelklick auf einen Eintrag können Sie die einzelnen Berechtigungen anzeigen lassen.

## Vererbung deaktivieren

Solange Sie nicht die Vererbung deaktivieren ⑦, können Sie keine Veränderungen an bestehenden Einträgen durchführen oder zusätzlich Einträge hinzufügen. Während der Deaktivierung können Sie wählen, ob Sie die vererbten Berechtigungen in explizite Berechtigungen umwandeln oder alle vererbten Berechtigungen entfernen möchten. Eine Umwandlung ist in vielen Fällen empfehlenswert, da überzählige Berechtigungen schnell gelöscht werden können.


Schulversion
© HERDT-Verlag

### Aufgabe 2 – Spezielle Berechtigungen anzeigen

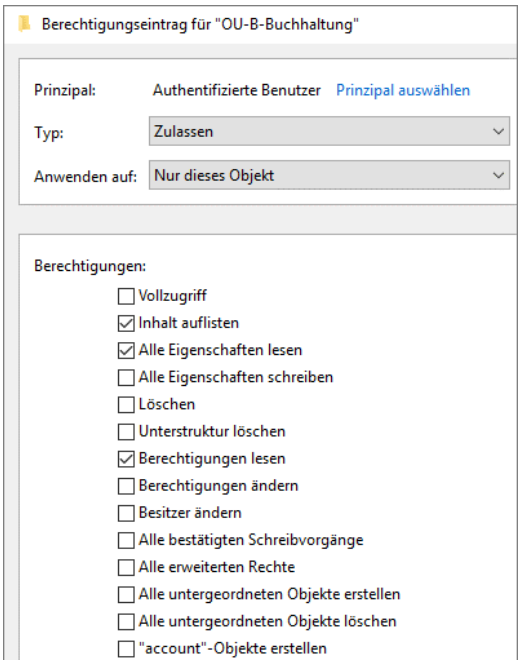
- Klicken Sie doppelt auf den gewünschten Berechtigungseintrag (z. B. *Authentifizierte Benutzer*).

  Das Fenster *Berechtigungseintrag* wird geöffnet.

Im oberen Teil des Fensters wird angezeigt, für welchen Prinzipal dieser Berechtigungseintrag gilt. Sie können den Benutzer oder die Gruppe unter *Prinzipal auswählen* wechseln. Unter *Typ* kann mit *Zulassen* und *Verweigern* bestimmt werden, welche Einträge angezeigt werden. Bei *Anwenden auf* können Sie auswählen, ob die Einstellungen nur für dieses Objekt, für alle untergeordneten Objekte oder für beides gelten sollen.

Darunter wird eine lange Liste von speziellen Berechtigungen angezeigt, gefolgt von einer ebenso langen Auflistung von Eigenschaften.

In den Berechtigungseinträgen müssen Sie selten etwas verändern, dennoch ist es wichtig, von ihrer Existenz zu wissen.




*Spezielle Berechtigungen ansehen*

## 16.3 Objektverwaltung delegieren

### Aufgabenstellung

Andrea Baumann ist Leiterin der Buchhaltungsabteilung. Sie soll künftig die Möglichkeit haben, Mitarbeitern ein neues Kennwort zu geben, wenn diese ihres vergessen haben.

Die Objektverwaltung für *OU-B-Buchhaltung* soll über die Gruppe *GG-B-Buchhaltung-Abteilungsleiter* an *ABaumann* delegiert werden. Die delegierte Aufgabe ist: Kennwörter zurücksetzen.

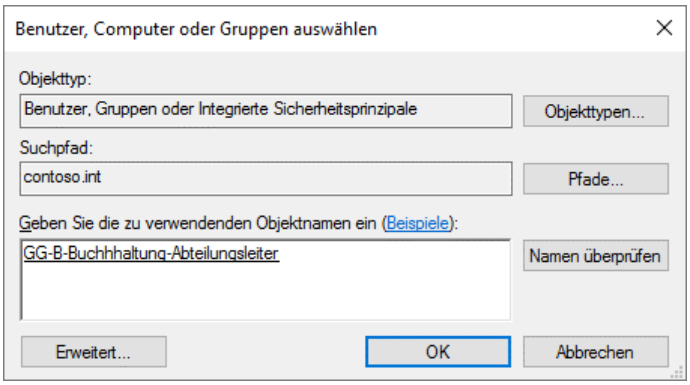
Achten Sie darauf, die Aufgabe der Gruppe *Abteilungsleiter* zuzuweisen. Andernfalls müssten Sie bei einer Personalveränderung die ACL der OU von Hand prüfen, um den entsprechenden Berechtigungseintrag zu korrigieren. Durch die Gruppenverknüpfung wird die Berechtigung automatisch auf den jeweiligen Abteilungsleiter übertragen.

### Objektverwaltung delegieren

- Klicken Sie mit der rechten Maustaste auf *OU-B-Buchhaltung* und wählen Sie den Kontextmenüpunkt *Objektverwaltung zuweisen*.
- Klicken Sie auf *Weiter*.

### Benutzer oder Gruppen auswählen

- Wählen Sie die Gruppe oder den Benutzer aus, an den/die Sie die Verwaltung des Objekts delegieren möchten. Klicken Sie hierzu auf die Schaltfläche *Hinzufügen* und geben Sie den Gruppennamen `GG-B-Buchhaltung-Abteilungsleiter` ein oder suchen Sie ihn im AD.



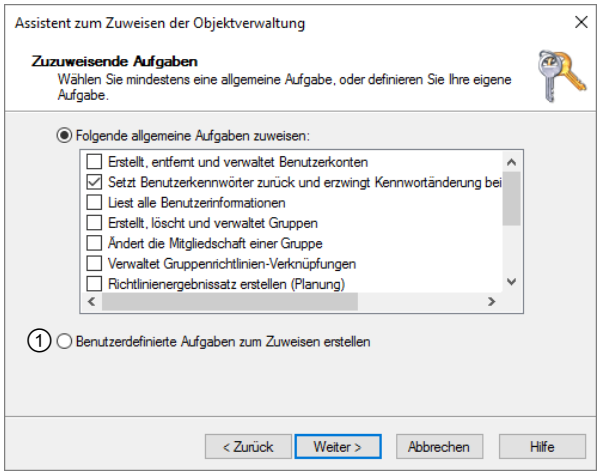

*Gruppe auswählen*

## Delegierte Aufgaben festlegen

- Wählen Sie die Verwaltungsaufgaben aus, die die Person ausführen soll.

Der Assistent listet mehrere allgemeine Aufgaben auf, die häufig delegiert werden. Es empfiehlt sich, wenn möglich, die zu delegierenden Aufgaben anhand dieser Liste auszuwählen.

Sie können die Aufgaben auch selbst definieren ①, müssen dann allerdings die erforderlichen Berechtigungen gegebenenfalls einzeln auswählen. Von dieser Vorgehensweise ist eher abzuraten, denn sie erfordert ein hohes Maß an Wissen und Erfahrung, Umsicht sowie eine Dokumentation der vergebenen Berechtigungen.




*Delegierte Aufgabe festlegen*

- Klicken Sie auf *Weiter*.

  Die Delegierung wird eingerichtet und der Assistent zeigt eine Zusammenfassung.
- Beenden Sie den Assistenten mit *Fertig stellen*.

## Aufgabe 1

Angenommen, Sie möchten die Delegierung der Objektverwaltung wieder aufheben.

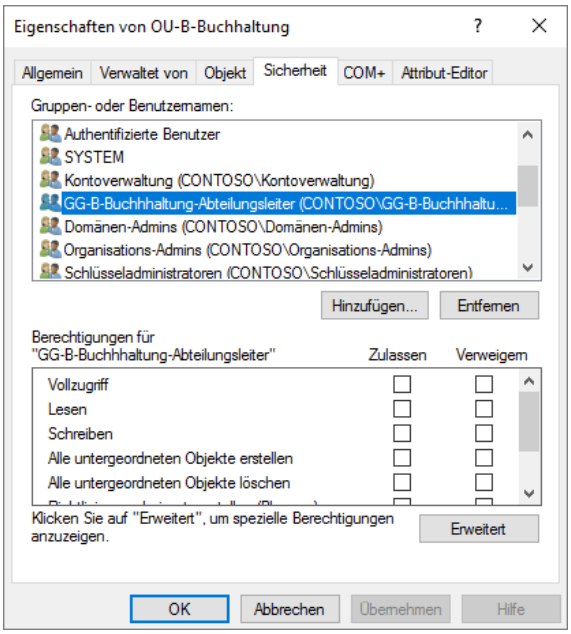
- Suchen Sie das Objekt, das Sie löschen müssten, wenn Sie *ABaumann* die Ausführung der Verwaltungsaufgaben wieder untersagen wollten.

Hier zeigt sich der Vorteil, wenn statt einer Einzelperson einer Gruppe die Berechtigungen zugewiesen werden.

*Die Delegierung finden Sie in den Berechtigungseinträgen.*

## Delegierung entfernen

Bestehende Delegierungen lassen sich mit dem Assistenten zum Zuweisen der Objektverwaltung nicht mehr verändern und werden dort auch nicht angezeigt. Falls Sie den Assistenten mehrmals aufrufen und weitere Gruppen auswählen, werden diese den bestehenden Einträgen hinzugefügt.




- Öffnen Sie über einen Rechtsklick die Eigenschaften der OU *OU-B-Buchhaltung*.
- Wechseln Sie auf das Register *Sicherheit* und markieren Sie dort die delegierten Konten.
- Um zu überprüfen, welche Delegierung für diesen Eintrag gilt, klicken Sie auf *Erweitert*. Mit einem Doppelklick auf einen Berechtigungseintrag können Sie sich im folgenden Dialog alle Berechtigungen anzeigen lassen und anpassen.
- Um eine Gruppe zu entfernen, klicken Sie auf *Entfernen* und dann auf *Übernehmen*.
- Klicken Sie auf *OK*.


Schulversion
© HERDT-Verlag

### Vorbereitung für die nächste Übung

Erstellen Sie nun ein Benutzerkonto in *OU-B-Vertrieb*. Dies wird für die nächste Übung benötigt.

## Delegierte Objektverwaltung testen

- Melden Sie sich als Administrator ab.
- Versuchen Sie sich mit dem Benutzerkonto von *ABaumann* an dem Domänencontroller *B-DC01* in der Domäne *firma.intern* anzumelden.

Sie können sich am Domänencontroller mit dem Konto eines Domänenbenutzers nicht in der Domäne anmelden.

Zum Schutz der Domänencontroller vor unbefugten Zugriffen gibt es eine vordefinierte Sicherheitsrichtlinie für Domänencontroller (Default Domain Controllers Policy), die lokale Anmeldungen von Benutzern unterbindet.

Nur Personen mit bestimmten Verwaltungsaufgaben ist die Anmeldung in der Domäne direkt am Domänencontroller erlaubt. Hierzu zählen die Domänenadministratoren und Operatorengruppen, die Server oder Drucker konfigurieren und verwalten oder sich um die Sicherung von Datenbeständen zu kümmern haben.

## Aufgabe 2

Damit Sie die Objektverwaltung in der Testumgebung überprüfen können, muss *ABaumann* die Berechtigung erhalten, sich von einem Domänencontroller aus in der Domäne anzumelden. Am besten regeln Sie das über eine Gruppenmitgliedschaft.

- Erzeugen Sie eine globale Sicherheitsgruppe mit dem Namen *GG-B-Anmeldung_DC*.
- Nehmen Sie die globale Gruppe *GG-B-Anmeldung_DC* in die lokale Gruppe der Serveroperatoren auf.
- Machen Sie *ABaumann* zum Mitglied in der Gruppe *GG-B-Anmeldung_DC*.

  Erinnern Sie sich an die Regel, nach der diese Gruppierung aufgebaut ist?

  Können Sie begründen, warum diese Vorgehensweise sinnvoll ist?

Sie können auch künftig die Gruppe *GG-B-Anmeldung_DC* in einer Testumgebung für weitere Tests mit Benutzerkonten verwenden. Hierzu platzieren Sie nach Erfordernis globale Benutzergruppen oder einzelne Benutzer in die globale Gruppe *GG-B-Anmeldung_DC*, die durch ihre Mitgliedschaft in der lokalen Gruppe der Serveroperatoren die benötigten Rechte erhält. Bedenken Sie allerdings, dass Serveroperatoren zusätzlich über weitreichende Rechte auf dem System verfügen: Sie dürfen z. B. Daten sichern, Festplattenkonfigurationen ändern und Software installieren.

In der Praxis sollten Sie diese Lösung nicht verwenden, sondern bei Bedarf eine neue Gruppe erstellen und ihr die entsprechenden Rechte zuweisen, indem Sie die Default Domain Controllers Policy entsprechend anpassen. Sie sollten daher die globale Gruppe zu einem Mitglied in einer neu zu erstellenden lokalen Gruppe *LG-B-DCLogon* machen, die den Zugang zur Ressource ermöglicht. Lesen Sie hierzu in diesem Buch die Kapitel über Gruppenrichtlinien.

## Aufgabe 3

Lernen Sie die Möglichkeiten kennen, die ein Benutzer durch die Delegierung erhalten hat, indem Sie Folgendes ausprobieren:

- Melden Sie sich mit dem Konto von *ABaumann* vom Domänencontroller aus in der Domäne an.
- Öffnen Sie das Snap-In Active Directory-Benutzer und -Computer.
- Ändern Sie das Kennwort von *CBeck.*
- Versuchen Sie, das Benutzerkonto von *DBaldosa* zu löschen.
- Erweitern Sie die OU *OU-B-Vertrieb*. Versuchen Sie, das Kennwort des dortigen Benutzers zu ändern.

## 16.4 Verwaltungstools für die Objektverwaltung

### Microsoft Management Console

Die Microsoft Management Console ist ein Instrument, mit dem Sie mehrere Verwaltungsprogramme (Snap-Ins) in einer Plattform (Konsole) zusammenstellen können. Damit können Sie Werkzeuge (Konsolen) für häufig durchzuführende Verwaltungsaufgaben individuell erstellen.

Konsolen sind Dateien mit der Dateinamenerweiterung *.MSC*.

### Verwaltungstools für delegierte Objektverwaltung

Haben Sie die Verwaltung einer OU an eine andere Person delegiert, können Sie eine individuelle Konsole für diese Person erzeugen. Die Konsole sollte ausschließlich jene Verwaltungsprogramme enthalten, die für die Verwaltung der OU erforderlich sind.

Um die erstellte Konsole für die betreffende Person verfügbar zu machen, speichern Sie sie beispielsweise in einem freigegebenen Ordner. Alternativ können Sie die Konsole auch als Dateianhang in einer E-Mail versenden oder auf einem Webserver zur Verfügung stellen. Zusätzlich müssen allerdings die entsprechenden Remoteserver-Verwaltungstools auf dem Rechner installiert sein, auf dem die Konsole aufgerufen werden soll.

### Konsolenmodi

#### Autorenmodus

Eine Konsole hat standardmäßig den Autorenmodus. Das bedeutet, dass derjenige, der die Konsole öffnen darf, den Vollzugriff auf die Konsole hat. Der Vollzugriff befugt dazu, die Konsole selbst zu verändern, beispielsweise dadurch, dass Snap-Ins hinzugefügt oder entfernt werden können.

#### Benutzermodus

Für die Delegierung der Objektverwaltung empfiehlt sich jedoch, Konsolen zu erstellen und zu verteilen, die von der betreffenden Person nicht mehr verändert und auch nicht gespeichert werden können. So ist sichergestellt, dass nicht durch eine unbeabsichtigte Veränderung die Konsole beschädigt wird.

Für den Benutzermodus einer Konsole gibt es drei verschiedene Stufen. Sie bestimmen den Handlungsspielraum für denjenigen, der die Konsole verwendet.

- **Vollzugriff**
  Der Konsolenbenutzer darf zwischen den Verwaltungsprogrammen wechseln, neue Fenster öffnen und alle Elemente der Konsolenstruktur erweitern.
- **Beschränkter Zugriff, mehrere Fenster**
  Der Konsolenbenutzer darf mehrere Fenster anzeigen, jedoch keine neuen Fenster öffnen.
  Er darf nicht alle Elemente der Konsolenstruktur erweitern.
- **Beschränkter Zugriff, Einzelfenster**
  Der Konsolenbenutzer darf nur ein Fenster anzeigen und auch keine neuen Fenster öffnen.
  Er darf nicht alle Elemente der Konsolenstruktur erweitern.

#### Aufgabenblockansichten verwenden

Sie können für jeden Befehl aus dem Kontextmenü eines Objektes auch eine entsprechende Aufgabe definieren, die anschließend von dem Benutzer mit einem einfachen Mausklick aufgerufen werden kann. Dies vereinfacht die Durchführung von Verwaltungsaufgaben für Benutzer erheblich und reduziert mögliche Fehlerquellen.

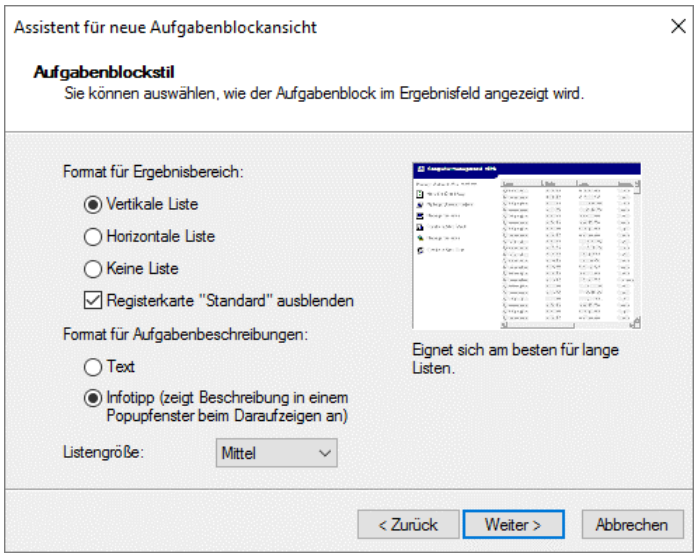

Schulversion
© HERDT-Verlag

## 16.5 Konsole mit Aufgabenblock erzeugen

### Neue Konsole anlegen

- Geben Sie im Startmenü `mmc` ein und klicken auf Sie *mmc*, um eine neue Konsole zu erzeugen.
- Betätigen Sie Strg M oder klicken Sie auf den Menübefehl *Datei - Snap-In hinzufügen/entfernen*.
- Wählen Sie das Snap-In *Active Directory-Benutzer und -Computer*. Bestätigen Sie Ihre Auswahl mit *OK*.
- Erweitern Sie den Listenbereich, bis er den gewünschten Knoten anzeigt.
- Klicken Sie nun im Kontextmenü der OU, für die Sie die Aufgabe vergeben möchten, auf *Neue Aufgabenblockansicht.*
- Klicken Sie im Willkommensbildschirm auf *Weiter*.

- Wählen Sie nun das Format der Listendarstellung, die Listengröße und das Format der Aufgabenbeschreibung.
  - Vertikale Listen sind geeignet für lange Listen, bei denen wenig Details angezeigt werden.
  - Horizontale Listen sind vorzuziehen, wenn die Details im Vordergrund stehen.
  - Die Einstellung *Keine Liste* erlaubt Verwaltungstätigkeiten an der Organisationseinheit, aber keine Befehle aus dem Kontextmenü von Objekten, die in der OU gespeichert sind.
  - Die Listengröße sollte nicht zu groß sein, damit noch genug Platz für Aufgabensymbole bleibt.
  - Für das Darstellungsformat haben sich Infotipps bewährt.




*Aufgabenblockstil festlegen*

- Bestätigen Sie Ihre Auswahl mit *Weiter.*
- Legen Sie fest, ob nur das ausgewählte Strukturelement diesem Format entsprechen soll oder ob Sie in Zukunft alle Strukturelemente so darstellen möchten. Klicken Sie auf *Weiter*.

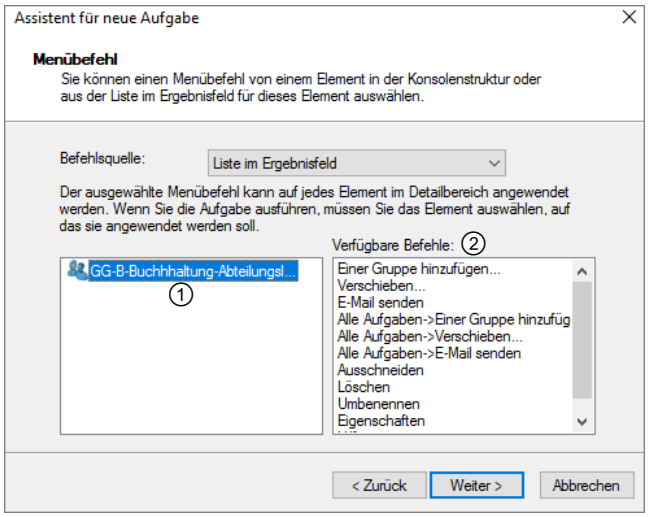
Belassen Sie nach Möglichkeit die Auswahl bei dem ausgewählten Strukturelement, damit Sie in Zukunft frei in Ihrer Entscheidung bleiben. Zwar können Sie auch nachträglich die Art der Aufgabenblockdarstellung anpassen, dies erfordert aber einen größeren Konfigurationsaufwand.

- Vergeben Sie einen Namen und eine Beschreibung und bestätigen Sie Ihre Auswahl.
- Stellen Sie den Assistenten fertig.

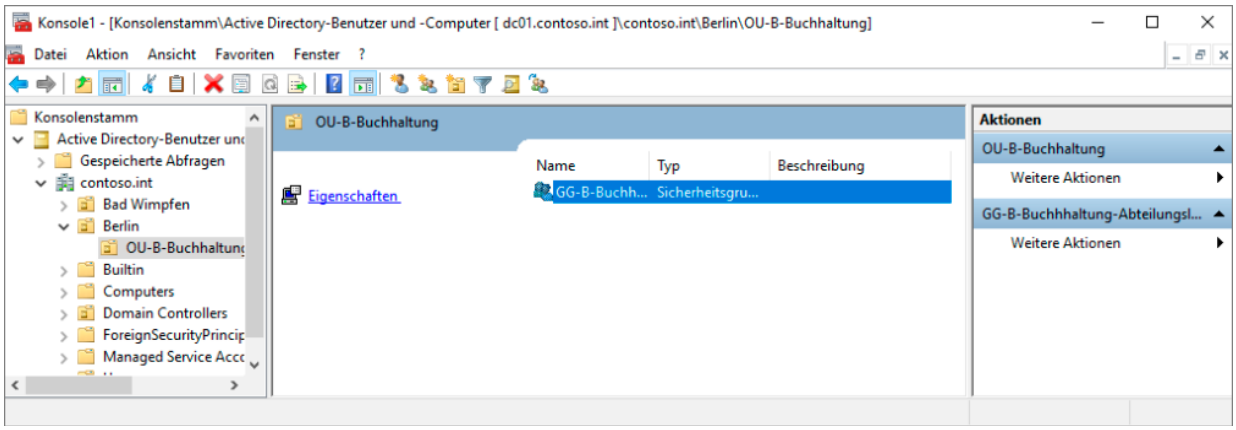
  Achten Sie darauf, dass das Kontrollkästchen *Neue Aufgaben* aktiviert ist.

## Assistent für neue Aufgaben

- Klicken Sie im Willkommen-Fenster auf *Weiter*.
- Wählen Sie unter Befehlstyp *Menübefehl* aus, wenn Sie eine Aufgabe aus dem Kontextmenü auswählen möchten. Bestätigen Sie mit *Weiter*.
- Wählen Sie nun im Listenfeld *Befehlsquelle* den Eintrag *Liste im Ergebnisfeld* und markieren Sie den gewünschten Objekttyp ① sowie einen verfügbaren Befehl ②. Bestätigen Sie Ihre Auswahl wie gewohnt.
- Sie können einen Aufgabennamen und eine Beschreibung eingeben oder die vorgeschlagenen Einstellungen übernehmen. Klicken Sie auf *Weiter*.
- Wählen Sie ein Symbol, das der Aufgabe zugeordnet wird. Für das Zurücksetzen von Kennwörtern könnten Sie z. B. den Schlüsselbund wählen. Sie können auch selbst Symbole definieren, die Sie mit *Durchsuchen* im Dateisystem auffinden. Klicken Sie anschließend auf *Weiter*.
- Bevor Sie den Assistenten fertigstellen, sollten Sie überlegen, ob Sie eine weitere Aufgabe definieren möchten, und das entsprechende Kontrollfeld gegebenenfalls markieren.




*Neue Aufgabe auswählen*




*Erstellte Aufgabe anzeigen*

Wenn Sie nun die von Ihnen erstellte Aufgabe aufrufen möchten, müssen Sie nur den entsprechenden Objekttyp im Listenbereich markieren, und Ihnen wird das Symbol mit dem Namen der Aufgabe angezeigt.

## Aufgaben hinzufügen

- Um nachträglich Einstellungen an der Aufgabenblockansicht zu verändern oder neue Aufgaben hinzuzufügen, klicken Sie im Kontextmenü der OU auf *Aufgabenblockansicht bearbeiten.*
- Im Register *Allgemein* können Sie die Aufgabenblockansicht nachträglich verändern.
- Im Register *Aufgaben* können Sie die Reihenfolge der Aufgaben anpassen, neue Aufgaben hinzufügen oder vorhandene bearbeiten oder entfernen.


Schulversion
© HERDT-Verlag

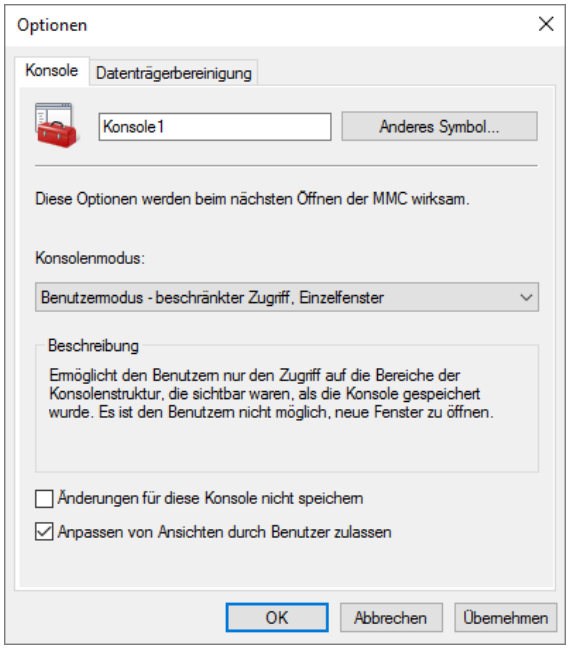
## Konsole speichern

Es ist empfehlenswert, zwei Versionen der Konsole abzuspeichern, eine im Autorenmodus zur späteren Bearbeitung und eine im Benutzermodus. Auch Administratoren können Konsolen im Benutzermodus später nicht mehr bearbeiten.

Bevor Sie die Konsole speichern, sollten Sie über *Datei - Optionen* den Konsolenmodus festlegen und konfigurieren, welche Änderungen zugelassen oder gespeichert werden dürfen. Im Autorenmodus können Sie die Konsole beliebig verändern, während die Benutzermodi eingeschränkter sind. Im beschränktesten Modus kann der Benutzer nicht einmal die voreingestellte Ansicht verändern.

Sie können einen Namen für die Konsole vergeben, der später in der Kopfzeile des Konsolenfensters angezeigt wird.

- Bestätigen Sie Ihre Auswahl mit *OK*.
- Klicken Sie auf *Datei - Speichern unter* und geben Sie einen Pfad und einen Namen für die Konsole an.
- Stellen Sie die Konsole den entsprechenden Benutzern zur Verfügung und weisen Sie diese in deren Gebrauch ein.




*Konsolenoptionen konfigurieren*

# 17 Berechtigungen anpassen

**In diesem Kapitel erfahren Sie**

- wie Sie mit Berechtigungen die Zugriffe auf Objekte steuern können
- wie Sie NTFS-, Freigabe- und Druckerberechtigungen verwalten

**Voraussetzungen**

- Active Directory-Objekte
- Active Directory-Konten verwalten

## 17.1 NTFS-Berechtigungen

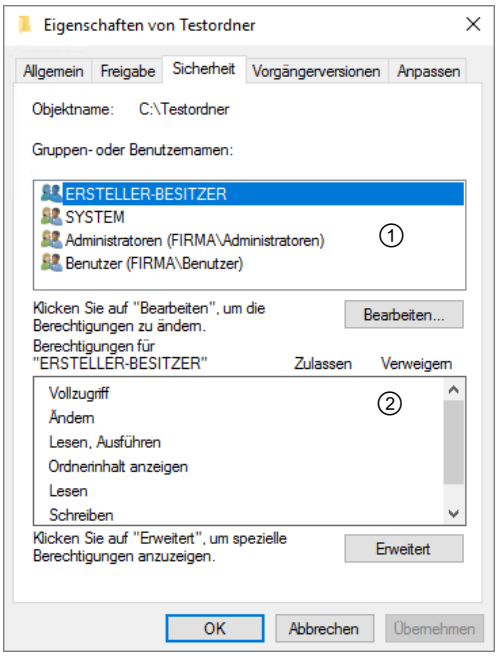
### Einführung zu Berechtigungen

Wenn in einem Unternehmen differenzierte Berechtigungsstrukturen in einer komplexen Verzeichnisstruktur benötigt werden, kann die Verwaltung von Berechtigungen einen erheblichen Aufwand verursachen. Gerade für die Berechtigungsverwaltung ist es dringend geboten, ein sauberes Gruppenkonzept anzuwenden, damit über die Mitgliedschaft in lokalen Gruppen stets eindeutig zu erkennen ist, wer welche Berechtigungen hat.

Wie auch Active Directory-Objekte erben Dateien und Verzeichnisse die Berechtigungen von übergeordneten Strukturen. Betrachten Sie nun zuerst die Standard-NTFS-Berechtigungen eines Verzeichnisses auf einer vom System konfigurierten Partition. Erstellen Sie hierzu auf *B-DC01* einen Ordner unter C:\.

### NTFS-Berechtigungen konfigurieren

- Klicken Sie mit der rechten Maustaste auf einen Ordner und wählen Sie *Eigenschaften*.
- Wechseln Sie in das Register *Sicherheit*.




Der obere Bereich ① zeigt die Liste der Konten mit zugewiesenen Berechtigungen. Wer hier nicht erfasst ist, kann nicht auf das Objekt zugreifen.

*ERSTELLER-BESITZER* können Sie für die Zuweisung von Berechtigungen nutzen, falls verschiedene Benutzer Objekte im Ordner erstellen und Sie dem jeweiligen Objekt-Ersteller andere Rechte zuweisen wollen als dem Rest. Die Objekte werden die Berechtigungen des jeweiligen Ordners erben.

Wenn Ordner oder Dateien mit dem Konto *Administrator* erstellt wurden, so wird dieses Konto in der Liste nicht aufgeführt. Jedes andere Konto wird eingetragen.

Für den markierten Eintrag sehen Sie im unteren Bereich ②, welche Standardberechtigungen ihm zugewiesen sind. Graue Häkchen zeigen ererbte Berechtigungen, schwarze Häkchen zeigen direkt zugewiesene Berechtigungen an.

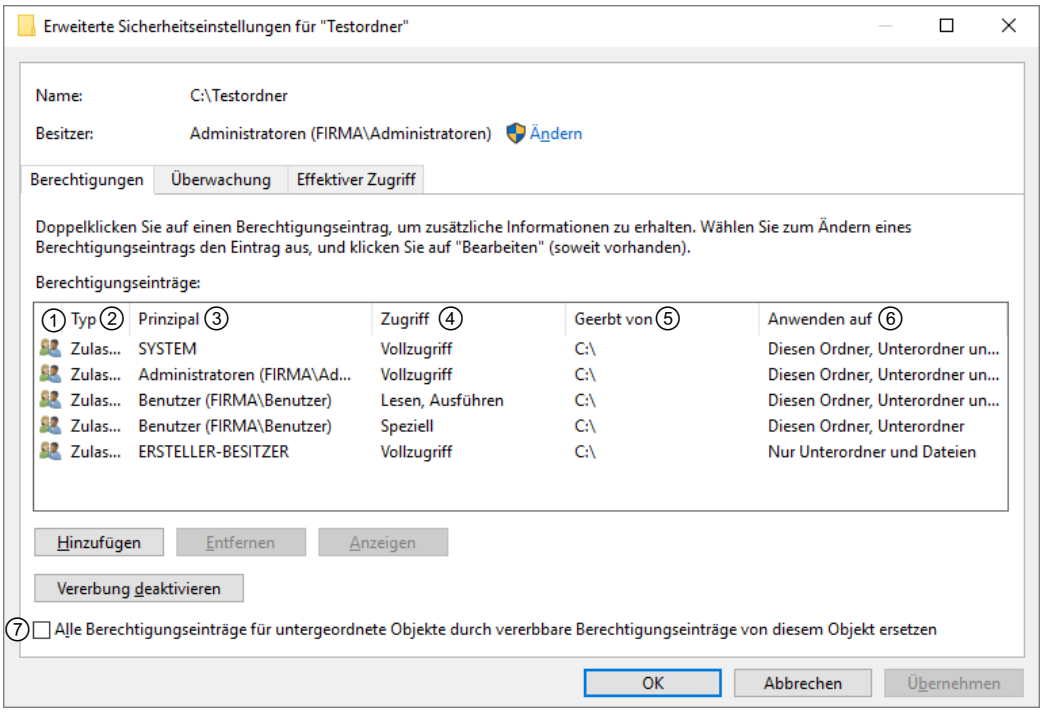
Nach einem Klick auf *Bearbeiten* können Sie sowohl Konten hinzufügen als auch zusätzliche Berechtigungen vergeben. Geerbte Einträge können Sie dort nicht verändern.


Schulversion
© HERDT-Verlag

Dies ist die schnellste und einfachste Möglichkeit, Standardberechtigungen zu ändern.

Mit *Erweitert* (vgl. vorherige Abbildung) kommen Sie zu den erweiterten Sicherheitseinstellungen, wo Sie spezielle Berechtigungen einsehen und vergeben können.

Die erweiterten Sicherheitseinstellungen verfügen über drei Registerkarten: *Berechtigungen*, *Überwachung* und *Effektiver Zugriff*. Im oberen Bereich des Fensters werden der Datei- oder Ordnername und der Besitzer angezeigt. Über den Link *Ändern* können Sie den Besitz übertragen.




So sind die Berechtigungseinträge in den erweiterten Sicherheitseinstellungen aufgebaut:

- Das Symbol ① zeigt, ob es sich um eine Gruppe oder ein Einzelkonto handelt.
- Der *Typ* ② kann *Zulassen* oder *Verweigern* sein.
- Der *Prinzipal* ③ ist der Name des Benutzers oder der Gruppe.
- Unter *Zugriff* ④ wird die Art der Berechtigung angezeigt (Vollzugriff, Lesen, Ausführen, Schreiben etc.).
- Unter *Geerbt von* ⑤ wird angezeigt, von wo die Zugriffsrechte vererbt wurden.
- *Anwenden auf* ⑥ zeigt, für welche Dateien, Ordner und Unterordner die Berechtigung gilt.

Der Eintrag *Speziell* in der Spalte *Zugriff* ④ bedeutet, dass hier Berechtigungen vergeben wurden, die nicht mit einer Standardberechtigung abgedeckt werden können.

Mit einem Doppelklick auf einen Eintrag können Sie die einzelnen Berechtigungen anzeigen lassen.

## Vererbung deaktivieren

Solange Sie nicht die Schaltfläche *Vererbung deaktivieren* betätigen, können Sie keine Veränderungen an bestehenden Einträgen durchführen oder zusätzlich Einträge hinzufügen. Während der Deaktivierung können Sie wählen, ob Sie die vererbten Berechtigungen in explizite Berechtigungen umwandeln oder alle vererbten Berechtigungen entfernen möchten. Eine Umwandlung ist in vielen Fällen empfehlenswert, da überzählige Berechtigungen schnell gelöscht werden können.

Mithilfe des Kontrollfelds ⑦ stellen Sie sicher, dass alle untergeordneten Objekte exakt diejenigen Berechtigungen aufweisen, die Sie hier einstellen. Das kann wichtig sein, wenn der Ordner bereits Dateien oder andere Ordner enthält.

## Überwachung einschalten

Im Register *Überwachung* können Sie festlegen, wer hinsichtlich welcher Zugriffe überwacht wird. Die Konfiguration entspricht dem Zuweisen von Berechtigungen. Für Überwachungen bietet sich die Gruppe *Jeder* an.

Sie müssen zusätzlich die Überwachung für den gesamten Rechner aktivieren, damit Überwachungseinträge ins Sicherheitsprotokoll der Ereignisanzeige geschrieben werden. Näheres dazu erfahren Sie im Kapitel zu den Gruppenrichtlinien.

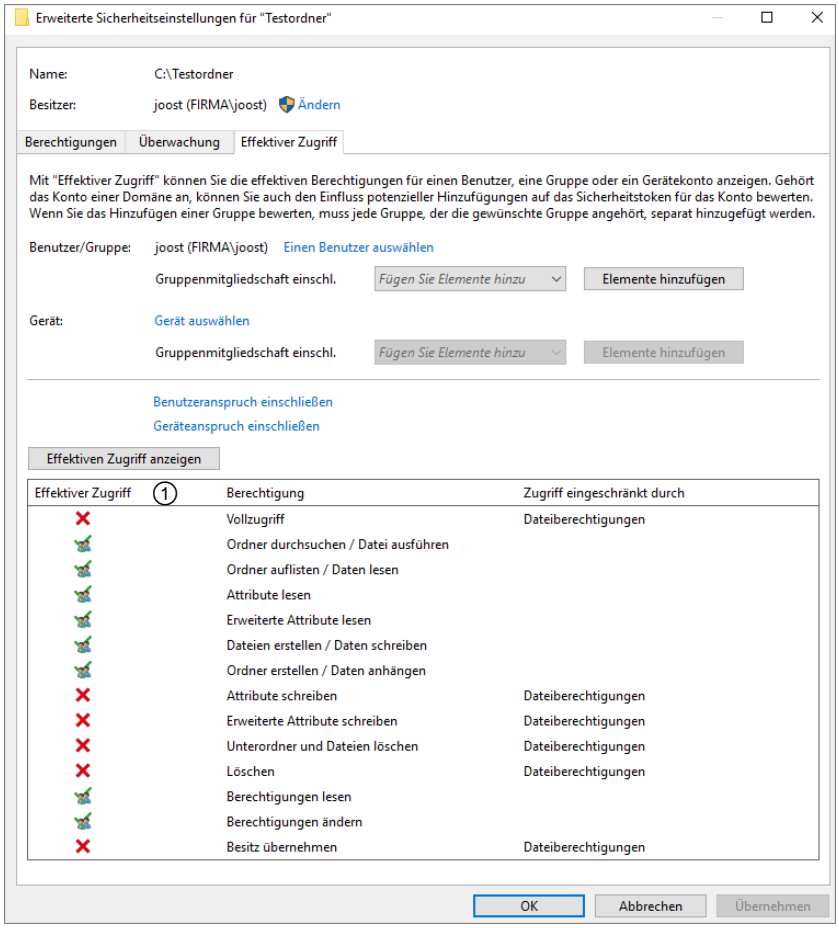
## Effektiven Zugriff einsehen

Auf der Registerkarte *Effektiver Zugriff* können Sie sich die tatsächlichen Berechtigungen für eine Gruppe oder einen Benutzer anzeigen lassen.

- Klicken Sie auf *Einen Benutzer auswählen* und wählen Sie eine Gruppe oder einen Benutzer aus.
- Klicken Sie auf *Effektiven Zugriff anzeigen*.

  Der effektive Zugriff wird für die gewählte Gruppe oder den Benutzer angezeigt ①.

Interessant ist die Möglichkeit, durch einen Klick auf *Elemente hinzufügen* Gruppenmitgliedschaften einzuschließen, denn so können Sie prüfen, was sich durch eine andere Gruppenmitgliedschaft verändern würde. Sie können hier auch mehrere Gruppenmitgliedschaften eintragen.




Vergessen Sie nicht, die Anzeige nach allen Änderungen zu aktualisieren, indem Sie auf *Effektiven Zugriff anzeigen* klicken.

## Besitz an einer Ressource übernehmen

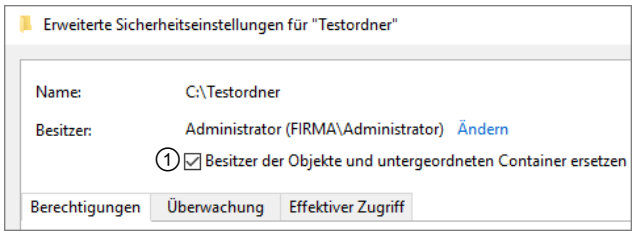
In einigen Fällen ist es möglich, dass Sie als Administrator nicht die Berechtigung haben, die NTFS-Berechtigungen einer Ressource anzuzeigen oder zu verändern. Dann müssen Sie zunächst den Besitz an der Ressource übernehmen, bevor Sie Berechtigungseinstellungen vornehmen können.

Besitzer eines Objekts ist zunächst derjenige Benutzer, der es erstellt hat. Nur der Besitzer kann die Berechtigungen verändern und so auch Administratoren vom Zugriff ausschließen. Das ist beispielsweise erforderlich für private Benutzerordner. Ein Administrator kann jedoch unabhängig von den vorhandenen Berechtigungen den Besitz an einem Objekt übernehmen. Anschließend kann sich der Administrator die nötigen Leserechte verschaffen, die zur Anzeige und Änderung der Berechtigungen nötig sind.

- Klicken in den Dateieigenschaften des Objekts, dessen Besitz Sie übernehmen wollen, im Register *Sicherheit* auf *Erweitert*.
- Klicken Sie im Dialog *Erweiterte Sicherheitseinstellungen* auf *Besitzer: Ändern* (folgende Abbildung).


Schulversion
© HERDT-Verlag

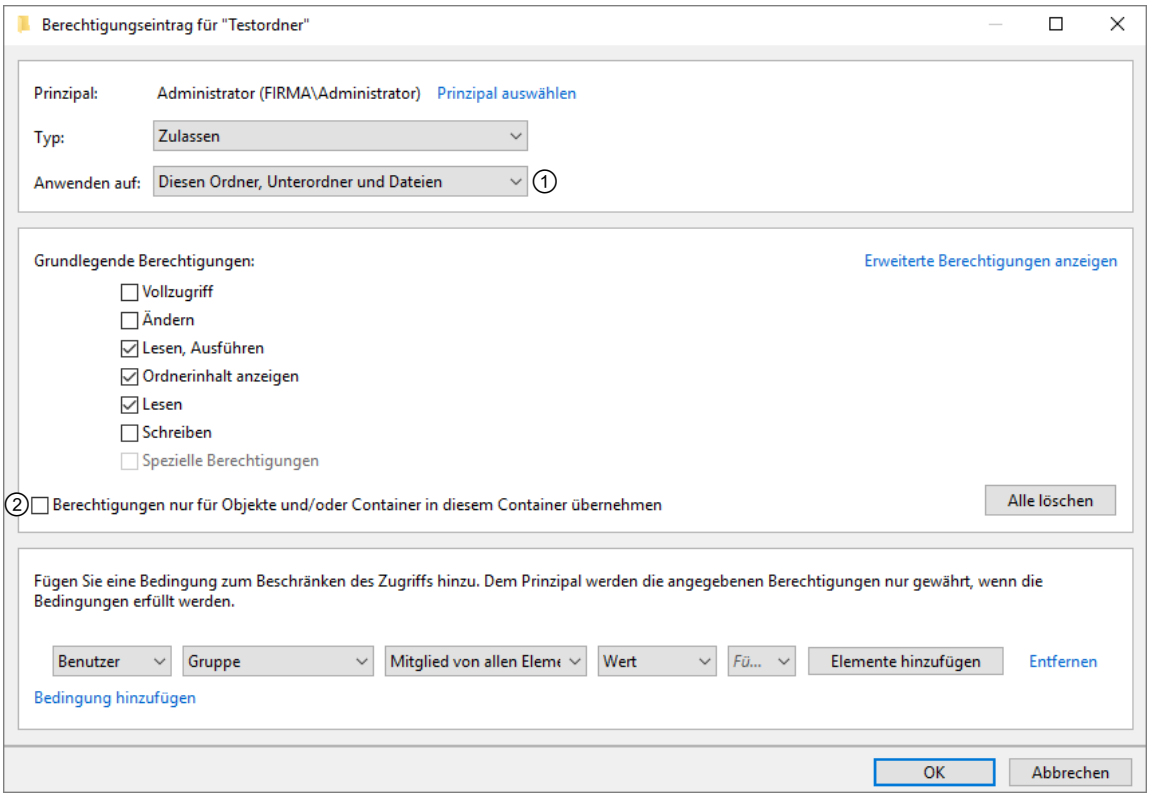
- Geben Sie den Namen des neuen Besitzers ein oder suchen Sie unter *Erweitert* nach Benutzerobjekten. Bestätigen Sie Ihre Auswahl mit *Übernehmen* und *OK*.
- Aktivieren Sie die neu erschienene Option ①, um den Besitzer für alle Dateien und Ordner zu ändern.
- Klicken Sie auf *OK*.




## Konto hinzufügen

Sie können einer Ressource weitere Prinzipale hinzufügen. Bedenken Sie die AGDLP-Regel und verwenden Sie als Prinzipale stets lokale Gruppen. Einzelne Benutzer sollten Sie nicht verwenden.

- Klicken Sie auf der Registerkarte *Berechtigungen* auf *Hinzufügen*, um einen Prinzipal (ein Konto) hinzuzufügen. Das Fenster *Berechtigungseintrag* wird geöffnet.
- Klicken Sie auf *Prinzipal auswählen*.
- Fügen Sie ein Konto hinzu und klicken Sie auf *OK*.
- Stellen Sie die gewünschten Berechtigungen ein und klicken Sie auf *OK*.




Unter *Typ* können Sie die Berechtigung zwischen *Zulassen* und *Verweigern* umschalten. Im Listenfeld *Anwenden auf* können Sie alle möglichen Varianten einstellen und damit die Standardvererbung umgehen. Sie werden das nur in seltenen Fällen benötigen, z. B. bei servergespeicherten Benutzerprofilen.

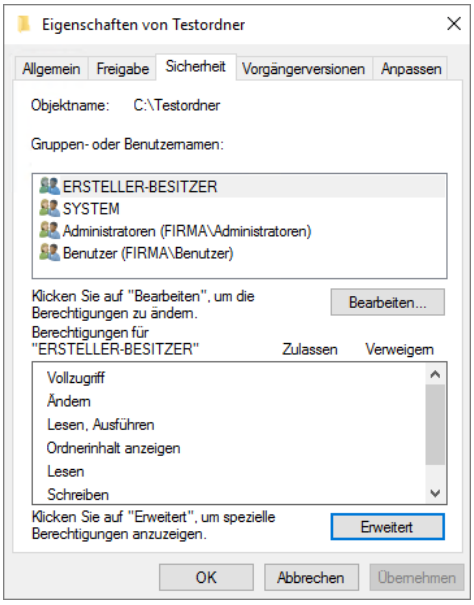
Darunter sehen Sie die Berechtigungen, die Sie verändern können. Über den Link *Erweiterte Berechtigungen anzeigen* können Sie die Anzeige zwischen grundlegenden und erweiterten Berechtigungen umschalten. Wenn Sie das Kontrollfeld ② aktivieren, entspricht das dem Eintrag *Nur Unterordner und Dateien* bei ①.

Im unteren Bereich des Fensters können Sie Bedingungen hinzufügen, die erfüllt sein müssen, damit die Berechtigungen angewendet werden.

Gewöhnungsbedürftig ist, dass hier keine Standardberechtigungen angezeigt werden, Sie werden mit den eigentlichen NTFS-Berechtigungen konfrontiert. Falls Sie lieber mit Standardberechtigungen arbeiten, können Sie es sich einfacher machen:

- Aktivieren Sie beliebige Berechtigungen und klicken Sie auf *OK*.
- Schließen Sie auch die erweiterten Sicherheitseinstellungen, indem Sie auf *OK* klicken.
- Wenn Sie zurück sind in den *Eigenschaften* des Ordners, klicken Sie dort auf *Bearbeiten*.

  Das Konto ist jetzt vorhanden und Sie können ihm Standardberechtigungen zuweisen. Damit aktivieren Sie auch die Standardvererbung.
- Nach dem Deaktivieren der Vererbung können Sie auch gleich in die Eigenschaften zurückgehen und dort weiterarbeiten.




*Standardberechtigungen bearbeiten*

## Verschieben von Dateien und Ordnern

Das Verschieben von Dateien verursacht immer wieder Probleme, weil dabei in einigen Fällen die Berechtigungen nicht an den neuen Ort angepasst werden. Das führt zu Problemen beim Öffnen der Dateien. Mit Verschieben ist der Vorgang gemeint, bei dem die Datei vom alten Ort an den neuen Ort verlegt wird. Dabei ist für den Benutzer nicht immer ersichtlich, welche Technik dabei angewendet wird. Beim Verschieben von Dateien ist es wichtig, drei Fälle zu unterscheiden:

- Verschieben zwischen Volumes, z. B. von *E:* nach *F:*

  Dieser Vorgang ist eigentlich ein Kopieren mit anschließendem Löschen. Das merkt man auch an der benötigten Zeit, denn der Vorgang dauert mit steigender Dateigröße immer länger. Dabei werden die Objekte neu erstellt und erben die Berechtigungen vom übergeordneten Objekt.
- Verschieben innerhalb eines Volumes, z. B. von *E:\Ordner1* nach *E:\Ordner2*

  Dies ist der Problemfall, denn hier kann es passieren, dass die Berechtigungen nicht geändert werden. Es werden nur Verwaltungseinträge umgeschrieben, was Sie auch daran merken, dass das Verschieben sehr schnell geht. Bei Verwendung des Windows-Explorers werden die Berechtigungen seit Windows Vista richtig an den Zielordner angepasst. Wenn jedoch andere Software wie z. B. der Kommandozeilenbefehl `move` zum Verschieben genutzt wird, bleiben die Berechtigungen unangetastet und verursachen Probleme. Es obliegt also der Software, die Berechtigungen korrekt anzupassen. Deshalb müssen Sie besonders bei älterer Software davon ausgehen, dass dies nicht der Fall ist.
- Verschieben von einer Freigabe in eine andere Freigabe

  Unabhängig davon, wo die freigegebenen Ordner liegen, findet beim Zugriff über Freigaben immer ein Kopiervorgang statt. Wenn also alle Benutzer über Dateifreigaben auf den Dateiserver zugreifen, gibt es keine Probleme.

Im Normalfall sollten Sie also dafür sorgen, dass kein Benutzer direkt auf dem Dateiserver auf die Daten zugreifen und Dateien verschieben kann. Dem Administrator muss das Problem bekannt und bewusst sein, wenn beim Verschieben von Dateien nicht der Windows-Explorer verwendet wird.

### Fehlerhafte Berechtigungen anpassen

Falls das Problem der unangepassten Berechtigungen einmal auftauchen sollte, bietet das Kommandozeilentool `icacls.exe` die Lösung, das die Berechtigungen in *Ordnername* durch die vererbbaren Berechtigungen von *Ordnername* ersetzt:

```
icacls <Ordnername>\*.* /reset /T /C /Q
```

`<Ordnername>` ersetzen Sie durch den Ordnerpfad der Freigabe.


Schulversion
© HERDT-Verlag

Mit einer Batchdatei können Sie auch mehrere betroffene Freigaben von dem Problem befreien. Testen Sie solche Skripte, bevor Sie sich darauf verlassen!

## Standardisierte Vorgehensweise

Sie sollten in Ihrer Netzwerkstruktur eine standardisierte Vorgehensweise mit vier Standardgruppen pro Freigabe verwenden. Erstellen Sie für jede Freigabe vier lokale Gruppen für die Berechtigungen „Lesen“, „Ändern“, „Vollzugriff“ und „Kein Zugriff“ und ordnen Sie diesen die entsprechenden einfachen Berechtigungen zu. Schauen Sie sich dazu noch einmal die Namenskonventionen aus dem ersten Kapitel an.

In aller Regel wird zwar die Gruppe *Kein Zugriff* leer bleiben, doch ist im Vergleich der Aufwand nur unbedeutend, wenn Sie die Gruppen mit einer Batchdatei erstellen. Und der Vorteil einer stringenten Struktur ergibt sich daraus, dass Sie keine Entscheidungen von Fall zu Fall mehr vornehmen müssen, sondern stets nach einem nachvollziehbaren Schema arbeiten können. Dies ist insbesondere von Bedeutung, wenn mehrere Administratoren mit der Betreuung einer gemeinsamen Struktur beauftragt sind.

## Tipps und Hinweise zur NTFS-Verrechtung

- Verrechten Sie Ordner, keine Dateien.
- Weisen Sie Berechtigungen nie einzelnen Benutzern zu, sondern stets domänenlokalen Gruppen.
- Nehmen Sie nur globale oder universale Gruppen in domänenlokalen Gruppen auf, niemals Benutzer. Die Benutzer befinden sich in den globalen Gruppen.
- Seien Sie sparsam mit dem Verweigern von Berechtigungen. Bei einem sauberen Aufbau der Gruppenstruktur werden Sie nur in Sonderfällen mit einer Verweigerung arbeiten müssen.
- Geben Sie möglichst nur einer Gruppe (z. B. die Gruppe *Administratoren*) Vollzugriff auf einen Ordner. Normale Benutzer sollten niemals Vollzugriff erhalten. Ändern reicht fast immer aus.
- Ändern Sie die Berechtigungen des Kontos *System* nicht.

**Für Fileserver:** Typischerweise verfügen Sie über folgende Einträge in der Berechtigungsliste:

- Administratoren mit Vollzugriff; erleichtert in vielen Fällen die Arbeit;
- System mit Vollzugriff;
- die standardisierten vier domänenlokalen Gruppen (LG) mit den Berechtigungen L, AE, VZ und KZ, die Sie für jede Ressource einrichten.

Manchmal ist es notwendig, das Löschen von Ordnern zu verhindern. Über komplizierte Berechtigungen kommen Sie in der Regel ans Ziel, das geht aber auch einfacher. Erstellen Sie in dem Ordner eine beliebige Datei und weisen Sie ihr folgende Berechtigungen zu: Gruppe *Jeder - Vollzugriff verweigern*. Da die Datei nicht entfernt werden kann, kann auch der Ordner nicht gelöscht werden.

Taucht eine SID (S-1-5-…) in einer Berechtigungsliste auf, kann das zwei Ursachen haben. Entweder ist der Domänencontroller, der die Auflösungen leisten muss, nicht erreichbar oder es handelt sich um ein Konto, das gelöscht wurde. Im zweiten Fall können Sie den Eintrag löschen, da sich die Einträge sowieso nicht mehr rekonstruieren lassen.

## Warum Benutzer keinen NTFS-Vollzugriff erhalten sollten

Der Unterschied zwischen *Vollzugriff* und *Ändern* besteht aus nur zwei NTFS-Berechtigungen, die ein Benutzer nicht benötigt: Berechtigungen ändern und Besitz übernehmen. Mit Vollzugriff kann ein Benutzer dafür sorgen, dass der ursprüngliche Besitzer ausgesperrt wird. Das willkürliche Ändern von Berechtigungen kann als dummer Streich betrachtet werden oder auch als Mobbing. In jedem Fall können Sie durch das Zuweisen der Ändern-Berechtigung so einen Unfug zuverlässig unterbinden.

## 17.2 Freigabe-Berechtigungen für Ordner

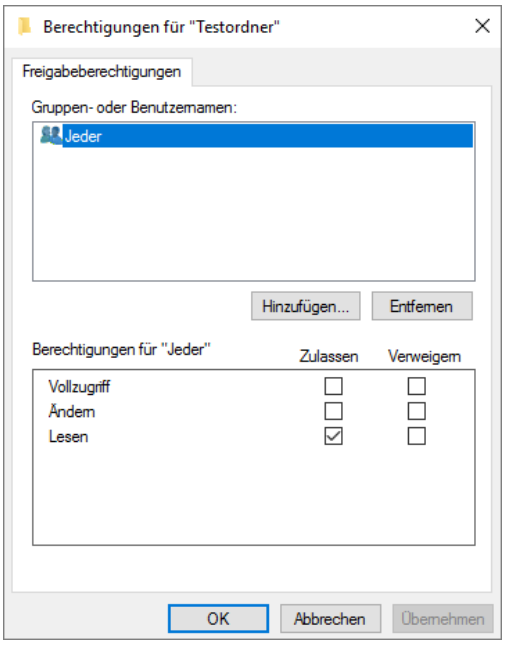
### Voraussetzung für Zugriffe über das Netz

Um auf den Inhalt eines Ordners über das Netzwerk zugreifen zu können, muss dieser Ordner (oder ein übergeordneter) freigegeben werden. Näheres zur Verwaltung solcher Freigaben erfahren Sie im Kapitel *Dateidienste einrichten*, hier werden nur die Freigabe-Berechtigungen erklärt. Die Freigaben können Sie in der Computerverwaltung einsehen.

- Geben Sie im Startmenü „compmgmt.msc“ ein und wählen Sie *Computerverwaltung*.
  Alternativ können Sie mit [⊞] [X] das Schnellzugriffsmenü öffnen und *Computerverwaltung* auswählen.
- Klicken Sie in der linken Spalte auf *System - Freigegebene Ordner - Freigaben*.
- Klicken Sie mit der rechten Maustaste auf eine Freigabe und wählen Sie *Eigenschaften*.

Freigabe-Berechtigungen greifen nur beim Zugriff über das Netzwerk. Auf einen lokal angemeldeten Benutzer haben sie keinerlei Wirkung. Deshalb die allgemeine Empfehlung: Seien Sie großzügig beim Zuweisen von Freigabe-Berechtigungen und regeln Sie die Zugriffe mit NTFS-Berechtigungen. Es gibt nur drei Freigabeberechtigungen: *Vollzugriff*, *Ändern* und *Lesen*.
Der Unterschied zwischen *Vollzugriff* und *Ändern* entspricht den Angaben bei NTFS oben.

Wenn Sie hier für die Gruppe *Jeder* den Vollzugriff zulassen, müssen Sie sich gar nicht mehr um eventuell fehlende Freigabe-Berechtigungen kümmern. Sie verlassen sich dann vollkommen auf die NTFS-Berechtigungen. Wenn Sie nur *Ändern* wählen, schließen Sie damit die NTFS-Berechtigungen *Berechtigungen ändern* und *Besitz übernehmen* aus. Auch der Besitzer einer Datei kann dann über das Netzwerk die Berechtigungen nicht mehr verändern.




### Zusammenspiel von Freigabe- und NTFS-Berechtigungen

Bei Zugriffen über das Netzwerk gilt: Die eingeschränkteren Berechtigungen gelten. Anders ausgedrückt:
Bei Zugriffen über das Netz erhalten Sie direkt an der Freigabe Ihre maximal möglichen Berechtigungen für den Inhalt der Freigabe. Durch NTFS können diese Berechtigungen nur noch reduziert werden, niemals erweitert.

Standardmäßig weist Windows Server 2019 beim Erstellen einer Freigabe nur Leseberechtigung zu. Über das Netzwerk kann niemand den Inhalt der Freigabe verändern.

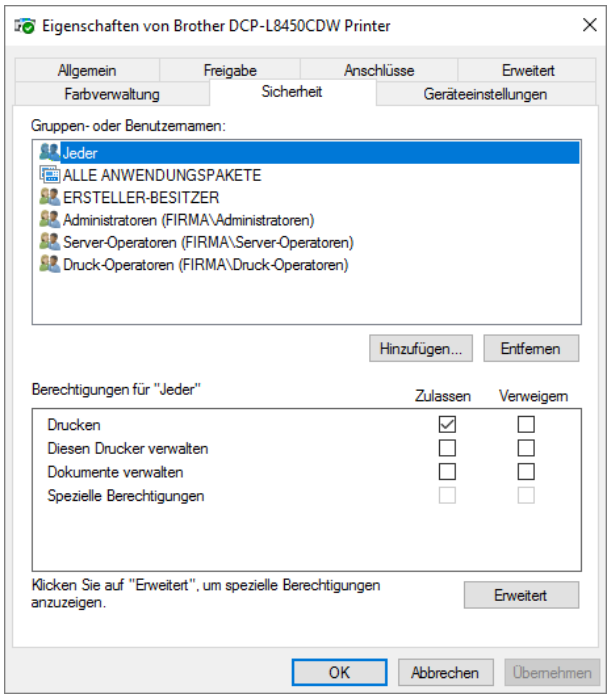
## 17.3 Berechtigungen für Drucker

### Voraussetzung für das Drucken

Um Druckaufträge auf einem Drucker ausgeben zu können, müssen Sie über entsprechende Berechtigungen verfügen. Die Abbildung zeigt, welche Berechtigungen Windows Server standardmäßig beim Installieren eines neuen Druckers einrichtet. Hier werden nur die Berechtigungen erklärt, Näheres zur Druckerverwaltung erfahren Sie im Kapitel *Druckdienste einrichten*.


Schulversion
© HERDT-Verlag

- Öffnen Sie die Systemsteuerung und navigieren Sie zu *Hardware\Geräte und Drucker*.
- Klicken Sie mit der rechten Maustaste auf einen Drucker und wählen Sie *Druckereigenschaften*.
- Klicken Sie auf die Registerkarte *Sicherheit*.




Für Drucker gibt es folgende Berechtigungen:

- ***Drucken*** ermöglicht es, einen Druckauftrag an den Drucker zu schicken und die Berechtigungen aller Druckaufträge anzuzeigen.
- ***Diesen Drucker verwalten*** beinhaltet alle Berechtigungen außer *Dokumente verwalten*. Damit können Sie z. B. die Berechtigungsliste verändern, den Drucker für das Netzwerk freigeben, neue Druckertreiber installieren oder den Drucker löschen.
- ***Dokumente verwalten*** ermöglicht es, Druckaufträge anzuhalten, neu zu starten, zu löschen oder deren Eigenschaften zu verändern. Sowohl der *ERSTELLER-BESITZER* als auch *ALLE ANWENDUNGSPAKETE* verfügen standardmäßig über diese Berechtigung.

Windows richtet die Druckerberechtigungen so ein, dass *Jeder* Druckaufträge an einen Drucker schicken kann und die *ERSTELLER-BESITZER* Dokumente verwalten dürfen. Das sendende Konto ist Besitzer seines Druckauftrags. Dadurch kann *Jeder* drucken und jeder seine eigenen Druckaufträge verwalten. Für die Verwaltung der Drucker sind die Administratoren, Server-Operatoren und Druck-Operatoren vorgesehen.

Bei Netzwerkdruckern werden Sie im praktischen Alltag wahrscheinlich die Gruppe *Jeder* durch eine andere Gruppe ersetzen.

## 17.4 Freigaben und Drucker veröffentlichen

### Veröffentlichung von Freigaben und Druckern in Active Directory

Sie haben die Möglichkeit, freigegebene Ordner oder Drucker im Active Directory zu veröffentlichen. Durch diese zentrale Sammlung der Informationen ist ein einfacherer Zugriff auf verteilte Ressourcen möglich. So wird auch ohne NetBIOS eine Suche nach freigegebenen Ressourcen im Netzwerk unterstützt. Daneben bietet dies den Vorteil, dass bestimmte Schlüsselbegriffe an die Freigabe vergeben werden und die Suche nach bestimmten Druckereigenschaften durchgeführt werden kann. So können Sie etwa alle Drucker anzeigen lassen, die beidseitigen Druck mit einer Mindestgeschwindigkeit von 4 Seiten pro Minute unterstützen. Außerdem kann im Kontextmenü des gefundenen Objekts z. B. gleich eine Verbindung zum Drucker aufgebaut oder auf dessen Treiber zugegriffen werden.

### Erleichterte Suche nach Ressourcen

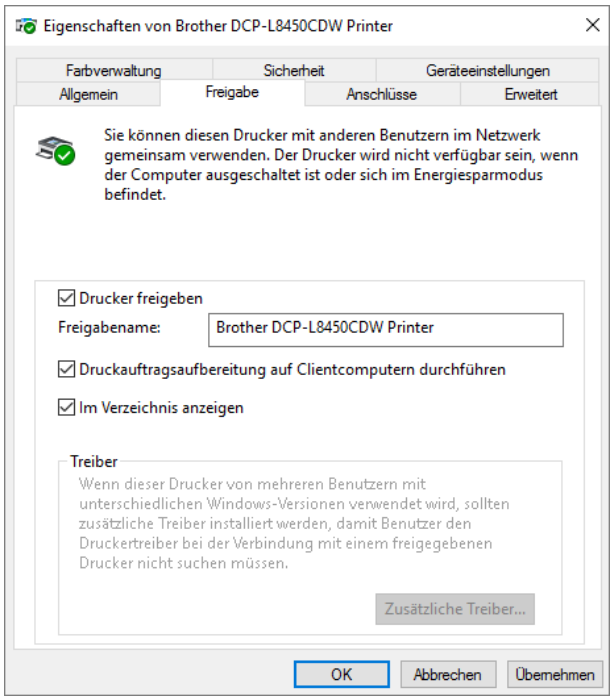
Die Suche nach einem veröffentlichten Objekt erfolgt zentral. Die hierzu benötigten Informationen werden auch im globalen Katalog gespeichert. Allerdings erfordert der effektive Einsatz dieser domänenübergreifenden Suchfunktion, dass ein globaler Katalogserver am Standort des Benutzers verfügbar ist. Wurde stattdessen auf das Zwischenspeichern der universalen Gruppenmitgliedschaften zurückgegriffen, um die Server und die Replikation zu entlasten, findet die Suche über eine WAN-Verbindung statt und im Endeffekt wird die Netzwerkleistung dadurch verschlechtert.

## Druckersuche vorbereiten

Um im nächsten Schritt einen Drucker finden zu können, müssen Sie erst einen lokalen Drucker installieren. Verfahren Sie hierzu wie gewohnt und geben Sie den Drucker im Netzwerk frei, wenn der Assistent Sie dazu auffordert. Anschließend müssen Sie den freigegebenen Drucker im Netzwerk veröffentlichen.

## Drucker veröffentlichen

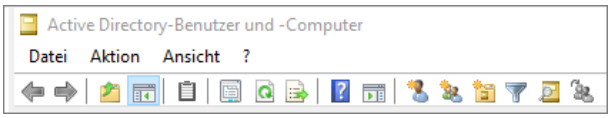
- Rufen Sie die Druckereigenschaften des Druckers auf, den Sie im Verzeichnis anzeigen möchten.
- Wechseln Sie zum Register *Freigabe* und aktivieren Sie das Kontrollfeld *Im Verzeichnis anzeigen*.
- Bestätigen Sie Ihre Einstellung mit *OK*.

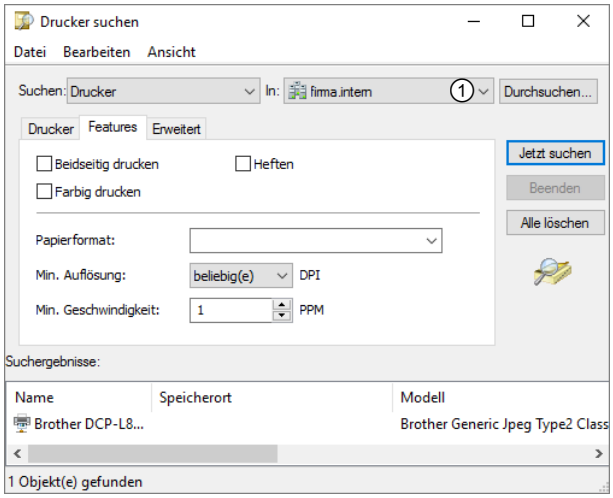



*Drucker im Verzeichnis anzeigen lassen*

## Drucker suchen

- Rufen Sie *Active Directory- Benutzer und -Computer* auf.
- Klicken Sie in der Symbolleiste auf die Lupe , um die Suche aufzurufen.
- Wählen Sie im Listenfeld *Suchen* den Eintrag *Drucker* und als Speicherort *Gesamtes Verzeichnis* ①.
- Geben Sie im Register *Drucker* Name, Aufstellungsort oder Modell des gesuchten Druckers ein.
- Stellen Sie im Register *Features* ein, welche Funktionen der gesuchte Drucker mindestens unterstützen muss.
- Geben Sie im Register *Erweitert* zusätzliche Suchoptionen an, wie z. B. Besitzer, verfügbares Papier, Kommentare oder maximale Auflösung.
- Klicken Sie auf *Jetzt suchen*.




Sie erhalten nun eine Übersicht über die ersten 1500 Drucker, die im Netzwerk gefunden wurden und die gewünschten Features aufweisen. Schränken Sie gegebenenfalls den Suchradius entsprechend ein. Sie können die Suchergebnisse filtern, indem Sie den Menüpunkt *Ansicht - Filter* aktivieren.

Über das Register *Erweitert* können Sie zahlreiche Parameter abfragen, die als Eigenschaft des Druckerobjektes im Active Directory gespeichert sind. Diese Eigenschaften werden allerdings nicht von Administratoren festgelegt, sondern vom System anhand der Treiberinformationen und erweiterten Druckereigenschaften abgefragt.


© HERDT-Verlag

# 18 Dateidienste

**In diesem Kapitel erfahren Sie**

- wie Sie Ordner freigeben
- wie Sie die Dateidienste installieren
- wie Sie mit dem Ressourcen-Manager für Dateiserver Kontingente und Dateiprüfungen verwalten und Speicherberichte erstellen
- wie Sie Datendeduplizierung und Schattenkopien aktivieren
- wie DFS, DAC und Speicherpools perspektivisch die Verwaltung von Dateidiensten erleichtern können

**Voraussetzungen**

- Active Directory-Konten verwalten
- Berechtigungen

## 18.1 Ordner-Freigaben

### Überblick

Eine zentrale Dateiablage mit der Möglichkeit, von beliebigen Rechnern aus auf den Datenbestand zuzugreifen, ist ein Grundbedürfnis in jedem Netzwerk. Die Datensicherung und Verwaltung wird dadurch deutlich vereinfacht. Fileserver bzw. Dateidienste stellen diese Möglichkeit zur Verfügung. In Windows-Netzen werden dazu Ordner für den Netzwerkzugriff freigegeben. Wird das Netz größer, so steigt die Anzahl an Fileservern und Freigaben und die Übersicht geht zunehmend verloren. Das Distributed File System (DFS) kann verschiedenste Freigaben in einem Stamm zusammenfassen und hilft so, den Überblick zu behalten.

Im Folgenden werden zunächst Freigaben mit dem Windows-Explorer erstellt. Dann werden die Dateidienste installiert und es wird gezeigt, welche zusätzlichen Möglichkeiten zur Verwaltung von Fileservern damit zur Verfügung stehen. Zum Abschluss wird gezeigt, welche Vorteile ein DFS bieten kann, wenn die Anzahl an Freigaben steigt.

Mit Windows Server 2012/2012 R2/2016 und 2019 hat sich in der Dateiserver-Verwaltung vieles verändert. Einige Auf gaben können mit dem Server-Manager erledigt werden, andere nur noch mit dem Ressourcen-Manager für Dateiserver oder der DFS-Verwaltung. Und schließlich gibt es auch Tätigkeiten, die nur in der Computerverwaltung oder in der Active Directory-Verwaltung ausgeführt werden können.

Verwenden Sie in der Testumgebung für die folgenden Aufgaben den Dateiserver *B-FS01*. Sie können in einer Testumgebung aber auch den Domänencontroller verwenden, den Sie installiert haben.

### Freigabe-Assistenten deaktivieren

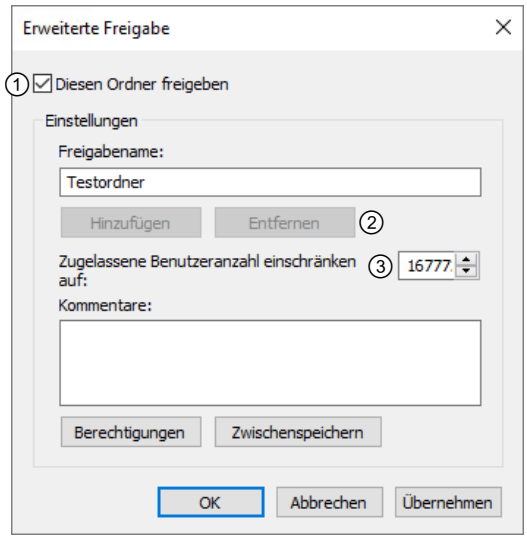
Die folgenden Schritte können Sie auf jedem Windows-Betriebssystem seit Windows Server 2003 nachvollziehen. Stellen Sie als Erstes sicher, dass der Freigabe-Assistent deaktiviert ist.

- Öffnen Sie ein Explorer-Fenster. Klicken Sie im Menü *Ansicht* auf *Optionen* und dann auf *Ordner- und Suchoptionen* ändern.
- Wechseln Sie auf die Registerkarte *Ansicht*.
- Deaktivieren Sie die Option *Freigabe-Assistent verwenden (empfohlen)* und klicken Sie auf *OK*.

## Freigaben mit dem Windows-Explorer erstellen

- Klicken Sie mit der rechten Maustaste auf den Ordner, den Sie freigeben möchten, und wählen Sie im Kontextmenü *Eigenschaften*.
- Wechseln Sie ins Register *Freigabe* und klicken Sie auf *Erweiterte Freigabe*.

Mit ① aktivieren Sie das Freigeben des Ordners.




Als Freigabename wird der Ordnername vorgeschlagen. Wenn Sie an den Freigabenamen ein Dollarzeichen $ anhängen, machen Sie daraus eine versteckte Freigabe, die standardmäßig im Windows-Explorer nicht angezeigt wird. Freigabenamen müssen auf einem Rechner eindeutig sein.

Sie können Ordner unter mehreren verschiedenen Freigabenamen freigeben ② und den Freigaben so unterschiedliche Freigabeberechtigungen zuweisen.

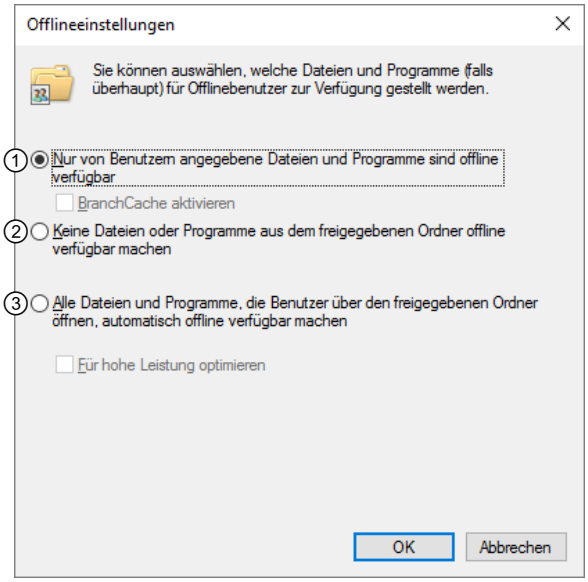
*Berechtigungen* wurden im vorigen Kapitel erläutert.

Unter *Zwischenspeichern* können Sie die Offlineeinstellungen des Ordners festlegen.

Unter ③ können Sie festlegen, wie viele Benutzer gleichzeitig auf diese Freigabe zugreifen können. Auf Client-Betriebssystemen ist 10 als Maximum vorgegeben.

Im Windows-Explorer können Sie nicht alle Optionen für Freigaben einstellen. Die restlichen Einstellungen können Sie entweder im Server-Manager oder im Ressourcen-Manager für Dateidienste vornehmen.

## Offlineeinstellungen – Zwischenspeichern




Offlineeinstellungen zielen in erster Linie auf Laptop-Benutzer, die außerhalb des Firmennetzwerks Zugriff auf den Freigabeninhalt benötigen. Bei entsprechender Client-Konfiguration kann ein Benutzer überall fast so arbeiten, als wäre sein Rechner am Firmennetz angeschlossen.

Die Abbildung zeigt, welche Einstellungen Windows standardmäßig beim Erstellen einer neuen Freigabe setzt:

- Durch ① kann ein Benutzer mit der rechten Maustaste auf eine Freigabe oder Datei in der Freigabe klicken und diese offline verfügbar machen.
- Mit ② deaktivieren Sie die Möglichkeit der Offlinespeicherung. Für Freigaben mit sensiblen Daten sollten Sie diese Einstellung in Erwägung ziehen, denn Laptops können verloren gehen.
- Mit ③ wird jede geöffnete Datei einer Freigabe automatisch offline verfügbar gemacht.


Schulversion
© HERDT-Verlag

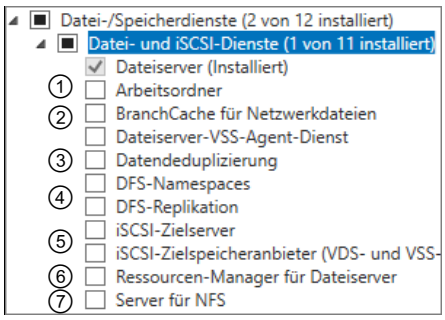
## 18.2 Dateidienste installieren

Soll ein Rechner als Fileserver dienen, empfiehlt es sich, die Rolle *Dateidienste* zu installieren. Dadurch stehen zusätzliche Möglichkeiten für die Verwaltung der Freigaben zur Verfügung. Verwenden Sie dafür in der Testumgebung den Server *B-FS01*. Wenn Sie nur einen Testserver installiert haben, können Sie dazu aber auch den Domänencontroller der Umgebung verwenden.

Sobald Sie auf dem Rechner eine Freigabe erstellt haben, wird die Serverrolle *Dateidienste* automatisch im Server-Manager installiert, aber keines der zusätzlichen Features aktiviert. Falls nötig fügen Sie die Rollen *Dateiserver-VSS-Agent-Dienst*, *Datendeduplizierung* und *Ressourcenmanager* hinzu.

- Öffnen Sie den Assistenten zum Hinzufügen von Rollen und Features.
- Wählen Sie als Installationstyp *Rollenbasiert* und anschließend den Server aus.
- Aktivieren Sie auf der Seite Serverrollen auswählen die Option *Datei- und Speicherdienste*.
- Klicken Sie auf das Pfeilsymbol vor *Datei- und Speicherdienste* und *Datei- und iSCSI-Dienste,* um die Ansicht zu erweitern.

Folgende Dienste können Sie zusätzlich installieren:



*Dateidienste-Rollen*

- *Arbeitsordner* ① können Sie nur mit Clients unter Windows 8.1 nutzen. Mit ihnen können Dateien zwischen verschiedenen Geräten synchronisiert werden. So kann der Benutzer etwa mit dem Tablet von unterwegs auf seine Arbeitplatzdaten zugreifen.
- *BranchCache* ② können Sie nur mit Clients unter Windows 7 Enterprise/Ultimate und 8 Enterprise nutzen. Damit können Dateien von anderen Fileservern automatisch zwischengespeichert werden, was den Netzwerkverkehr zwischen Standorten reduzieren kann.
- *Datendeduplizierung* ③ erlaubt Ihnen, Datenträger nach identischen und ähnlichen Dateien zu durchsuchen. Mit der Deduplizierung werden identische Inhalte erfasst und über Differenzdateien die doppelten Datensätze eliminiert. Dadurch kann erheblich Speicherplatz eingespart werden.
- Sobald Sie mehr als ein paar Ordnerfreigaben benötigen, bietet DFS ④ interessante Möglichkeiten. Bei mehreren Dateiservern sollten Sie *DFS-Namespaces* und *DFS-Replikation* sowie alle erforderlichen Features installieren.
- *iSCSI-Zielserver* und *Zielspeicheranbieter* ⑤ benötigen Sie nur, wenn dieser Server iSCSI-Speicher zur Verfügung stellen soll.
- Der *Ressourcenmanager für Dateiserver* ⑥ sollte in jedem Fall installiert werden.
- *Server für NFS* ⑦ benötigen Sie, wenn Sie Speicherplatz für UNIX-Clients über das Network File System zur Verfügung stellen.

- Aktivieren Sie alle benötigten Dienste und klicken Sie auf *Weiter*.
- Stellen Sie den Assistenten fertig und klicken Sie auf *Installieren*.

Alle gewählten Rollen und Features werden nun installiert. Im Server-Manager finden Sie nun die Seite *Datei- und Speicherdienste*, auf der Ereignismeldungen, der aktuelle Status und die Auslastung angezeigt werden.

Für den Praxiseinsatz bietet es sich an, den Ressourcen-Manager und die Verwaltungstools für Dateidienste auch auf anderen Servern, z. B. *B-DC01*, zu installieren, um von dort aus den Dateiserver zentral zu verwalten. Dies hat vor allem den Vorteil, dass Sie Zugriff auf sämtliche Gruppenverwaltungswerkzeuge und das Active Directory selbst haben. Dies ist auf dem Fileserver nicht der Fall, da er nur ein einfacher Mitgliedsserver ist.

### Freigaben im Server-Manager

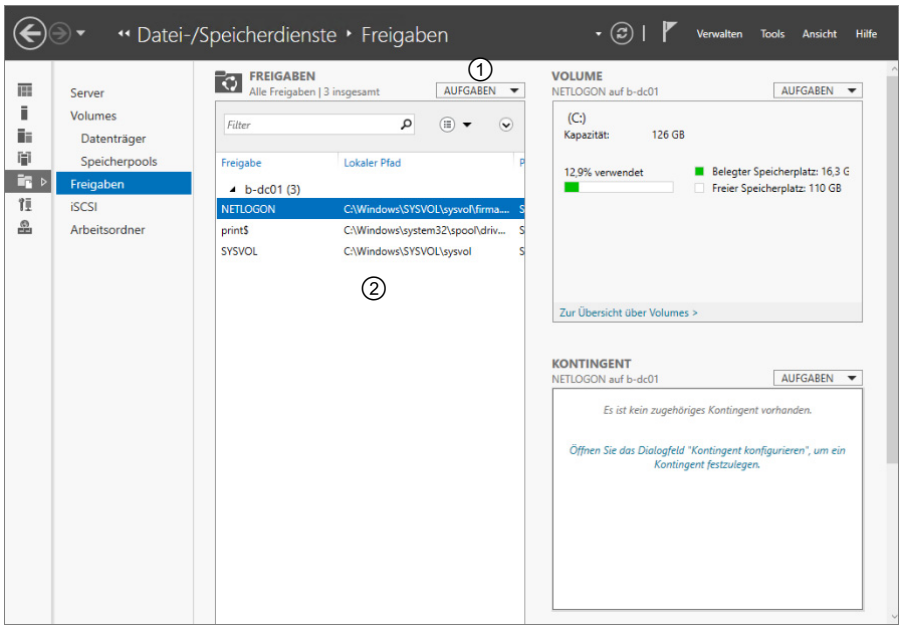
Zahlreiche Einstellungen finden Sie im Ressourcen-Manager für Dateiserver. Sie können aber auch im Server-Manager Einstellungen vornehmen.

Auf der Seite *Freigaben* können Sie folgende Aufgaben ausführen:

Unter *FREIGABEN - AUFGABEN* ① können Sie neue Freigaben erstellen.

Im Kontextmenü einer Freigabe ② können Sie Kontingente konfigurieren, die Freigabe beenden und die Eigenschaften aufrufen.

Im Bereich *VOLUME* sehen Sie einen Überblick über den Füllgrad des Volumes, auf dem sich die Freigabe befindet. Unter *Aufgaben* finden Sie u. a. eine Fehlerüberprüfung und eine Volume-Erweiterung.




Im Bereich *KONTINGENT* sehen Sie einen Überblick über die Kontingenteinstellungen, die Sie über *Aufgaben* auch verändern können.

## 18.3 Freigabe- und Speicherverwaltung

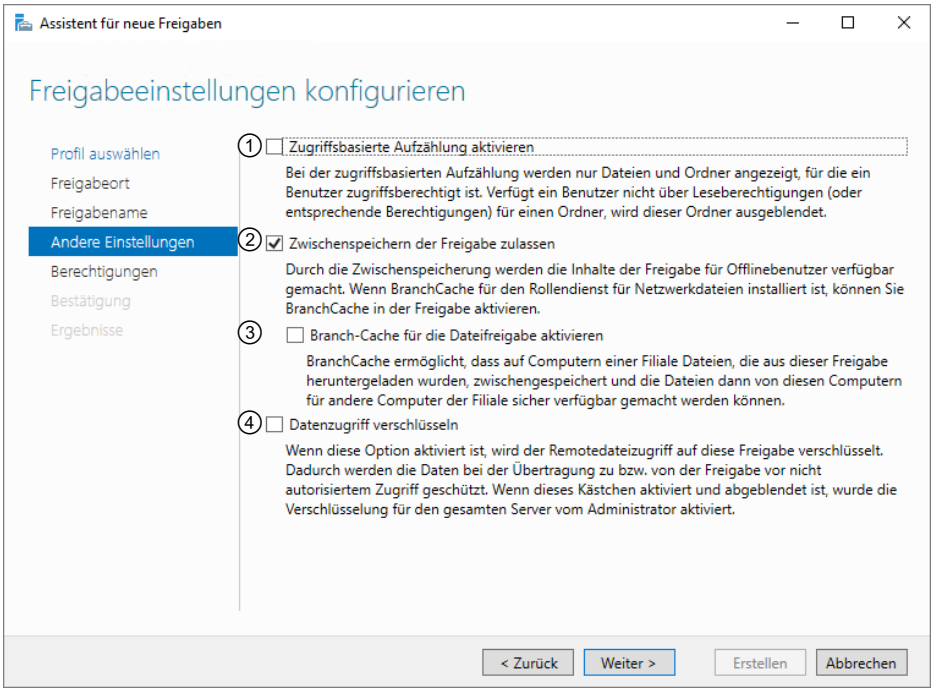
### Neue Freigabe mit Assistenten erstellen

Das Erstellen von Freigaben im Server-Manager erfolgt assistentengesteuert. Dadurch haben Sie die Möglichkeit, alle Konfigurationsschritte in einem Durchlauf zu erledigen. Sie können auch eine Freigabe mit dem Windows-Explorer erstellen und anschließend hier die Eigenschaften der erstellten Freigabe bearbeiten.

- Klicken Sie im Server-Manager in *Freigaben - Aktionen* auf *Neue Freigabe*.
- Wählen Sie das Profil der SMB- oder NFS-Freigabe aus.

  Unter *Erweitert* können Sie mehr Einstellungen vornehmen als beim Standardprofil *Schnell. Anwendungen* erstellt eine Freigabe für Hyper-V oder Datenbanken.
- Wählen Sie als Freigabeort Server und Volume bzw. Pfad für die Freigabe aus und klicken Sie auf *Weiter*.
- Wählen Sie Freigabenamen und optional eine Beschreibung. Ändern Sie, wenn nötig, den lokalen Pfad und Remotepfad zur Freigabe und klicken Sie auf *Weiter*.

Schulversion
© HERDT-Verlag




- Wählen Sie aus den folgenden Freigabeeinstellungen das Gewünschte aus und klicken Sie auf *Weiter*.
  - *Zugriffsbasierte Aufzählung aktivieren* ① zeigt dem Benutzer nur Ordner und Dateien an, für die er mindestens Leseberechtigung hat.
  - *Zwischenspeichern der Freigabe zulassen* ② erlaubt die Speicherung durch Offlinebenutzer.
  - *Branch-Cache* ③ ist eine Art der Datei-Zwischenspeicherung, die nur bei Windows 7/8/8.1 Enterprise/ Ultimate und Windows 10 Enterprise verfügbar ist.
  - *Datenzugriff verschlüsseln* ④ bedeutet, dass die Daten für die Netzwerkübertragung verschlüsselt werden.
- Passen Sie die Zugriffsberechtigungen über einen Klick auf *Berechtigungen anpassen* in den erweiterten Sicherheitseinstellungen an. Klicken Sie auf *OK* und dann auf *Weiter*.
- Wählen Sie in den Ordnerverwaltungseigenschaften die Verwendungszwecke des Freigabeordners aus (Benutzer-, Gruppen-, Anwendungs- und Sicherungs-/Archivierungsdateien).

  Die hier getroffene Auswahl wird von den Datenverwaltungsrichtlinien wie eine Klassifizierungsregel verwendet.
- Geben Sie optional für Hilfeanforderungen von Benutzern eine E-Mail-Adresse oder Verteilerliste an und klicken Sie auf *Weiter*.
- Weisen Sie auf Wunsch eine bestehende Kontingentrichtlinie zu und klicken Sie auf *Weiter*.

  (Kontingentrichtlinien werden im folgenden Unterkapitel erklärt.)
- Überprüfen Sie die Einstellungen und klicken Sie auf *Erstellen*.

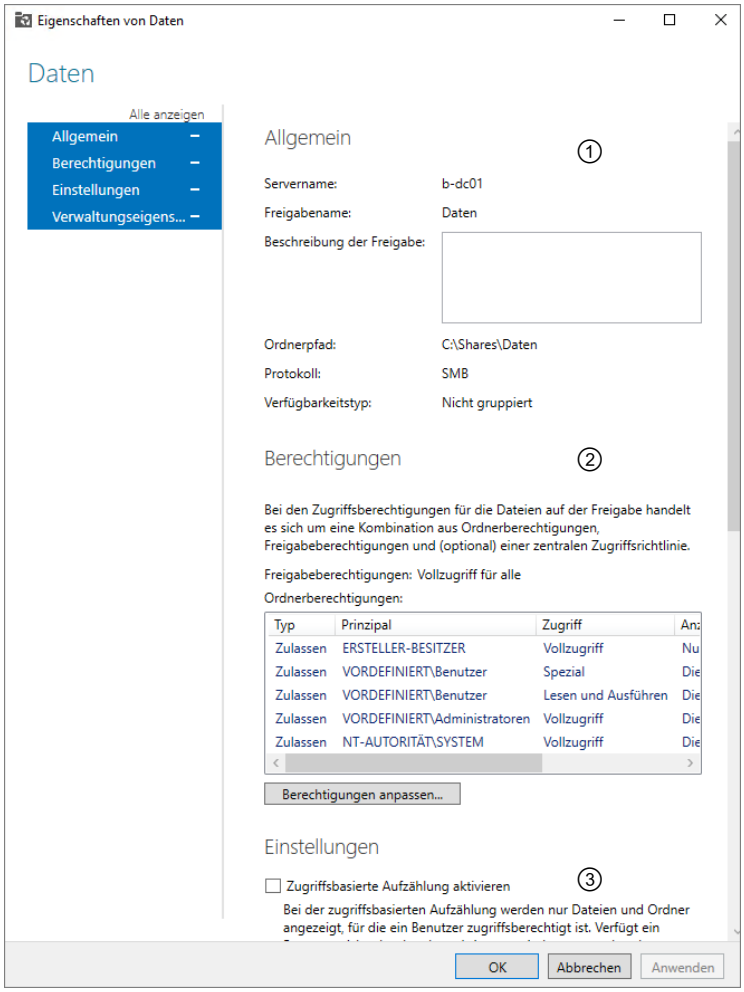
  Auf der letzten Seite wird angezeigt, ob alle Konfigurationsschritte erfolgreich waren. Fehler werden auf einem eigenen Register dargestellt.

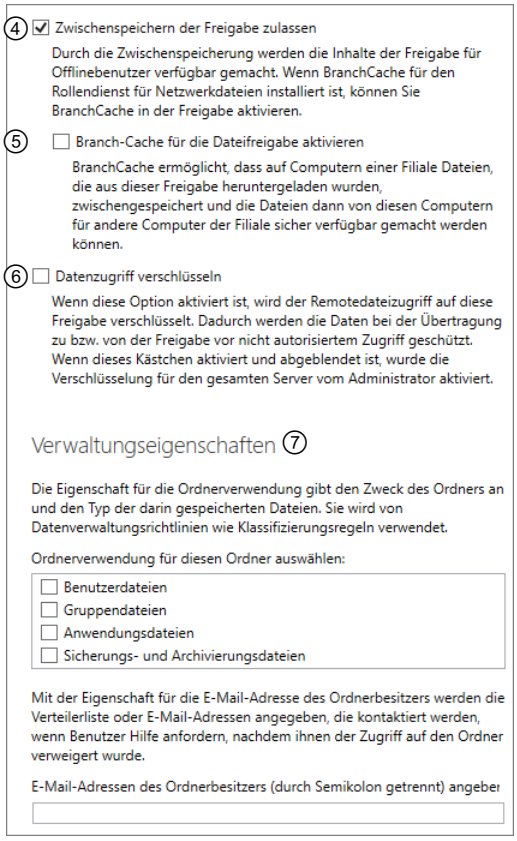
## Eigenschaften einer Freigabe bearbeiten

Den Eigenschaftendialog für Freigaben erreichen Sie über das Kontextmenü einer Freigabe im Server-Manager.

In den Eigenschaften finden Sie:

① allgemeine Daten zur Freigabe,
② Zugriffsberechtigungen (Resultat aus Freigabeberechtigung, NTFS-Berechtigungen und Zugriffsrichtlinien),
③ zugriffsbasierte Aufzählung,
④ Zwischenspeichern (offline),
⑤ Branch-Cache,
⑥ Übertragungsverschlüsselung,
⑦ Verwaltungseigenschaften.




*Freigabe-Eigenschaften im Server-Manager*


Schulversion
© HERDT-Verlag

## 18.4 Ressourcen-Manager für Dateiserver

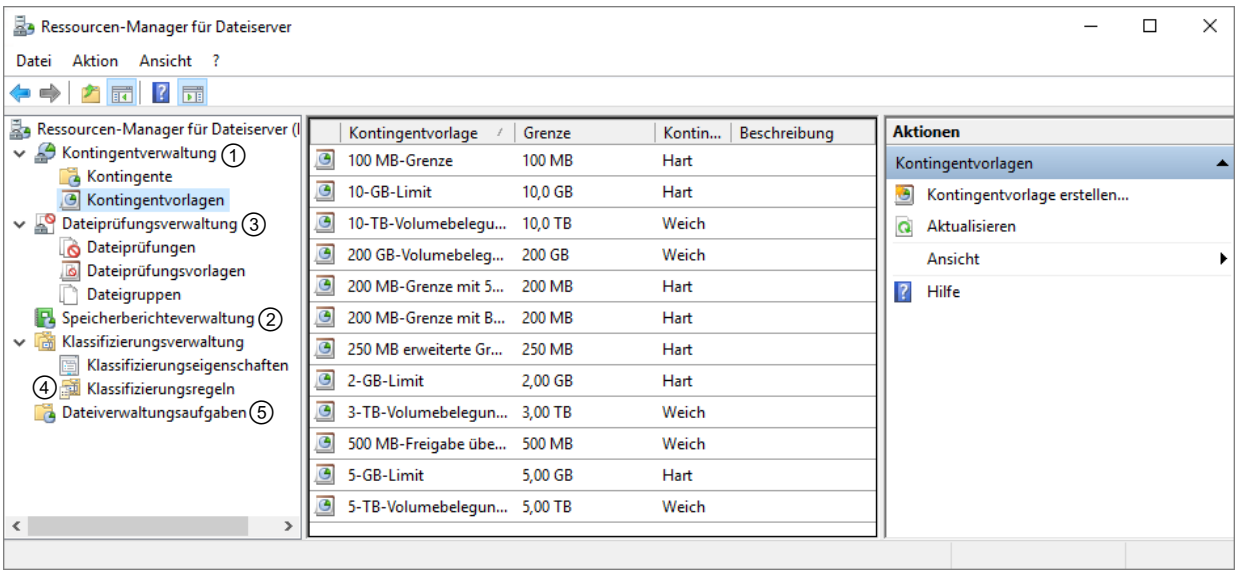
### Überblick

Auf Dateiservern sammeln sich schnell unglaubliche Mengen an Dateien an, wenn die Speicherung nicht geregelt wird. Von kopierten Datenträgerinhalten bis hin zu Video-, Foto- und Musiksammlungen ist hier alles vertreten, außerdem speichern Mitarbeiter gerne den letzten Jahresbericht in ihrem persönlichen Ordner und viele erhalten per Massen-E-Mail dieselben humoristischen Anhänge.

Der Ressourcen-Manager bietet einige Werkzeuge, die das Arbeiten mit Dateiservern angenehmer machen und helfen, oben genannte Auswüchse einzudämmen. Mit der Kontingentverwaltung beispielsweise können Sie die Speichernutzung von Benutzern für einzelne Ordner überwachen. Die Dateiprüfungsverwaltung ermöglicht dasselbe für Dateitypen. Außerdem können Sie Berichte generieren, die zeigen, wie bzw. womit von wem Speicherplatz belegt wird.

### Ressourcen-Manager für Dateiserver

Sie können den Ressourcen-Manager für Dateiserver über das Menü *Tools* des Server-Managers oder über die Eingabe von `fsrm.msc` im Startmenü starten.




Im Ressourcen-Manager können Sie folgende Aufgaben ausführen:

① Kontingente verwalten;

② Speicherberichte nach eigenen Kriterien erstellen und anzeigen lassen; Berichte werden in *C:\StorageReports\Interactive* gespeichert;

③ nach Dateitypen und -gruppen filtern, um ihnen bestimmte Handlungen zuzuordnen (z. B. Speicherverbot);

④ Klassifizierungsregeln erstellen, um z. B. Dateien anhand ihres Inhalts zu kategorisieren;

⑤ Dateiablaufaufgaben erstellen, um anhand von Erstellungszeitpunkt und -ort sowie Zugriffszeit bestimmte automatische Handlungen auszulösen, z. B. um veraltete Dateien in ein Sicherungsverzeichnis zu kopieren.

### Optionen konfigurieren

- Klicken Sie in der linken Spalte auf den Eintrag *Ressourcen-Manager für Dateiserver*.
- Öffnen Sie im Menü *Aktion - Optionen konfigurieren*.

  Der Optionsdialog wird geöffnet.

Sie können auf mehreren Registerkarten zahlreiche Einstellungen zu folgenden Themen vornehmen:

- Speicherorte für verschiedene Berichte,
- Parameter der verschiedenen Speicherberichte,
- Benachrichtigungslimits (Intervalle) in Minuten,
- E-Mail-Benachrichtigungen, SMTP-Server und E-Mail-Konto,
- Zeitplan für automatische Klassifizierung nach Dateiarten,
- E-Mail-Unterstützung nach Zugriffsverweigerung,
- Aufzeichnung von Dateiprüfungsaktivitäten.

## Kontingentverwaltung

Die Kontingentverwaltung ermöglicht eine einfache Überwachung von Benutzern, die mehr als eine festgelegte Menge an Speicherplatz belegen (weiches Kontingent). Ein hartes Kontingent beschränkt den verfügbaren Speicherplatz eines Benutzers auf einen definierten Wert. Zur Durchführung dieser Aufgabe weisen Sie einem Ordner eine Kontingentvorlage zu. Die Kontingentberechnungen erfolgen über den Besitzer der Datei.

Kontingente werden auch als Quotas bezeichnet. Vor Windows Server 2008 konnten Sie Kontingente nur für ganze Volumes vergeben, daher mussten damals viele Volumes angelegt werden. Dies ist heute unnötig.

### Kontingentvorlagen

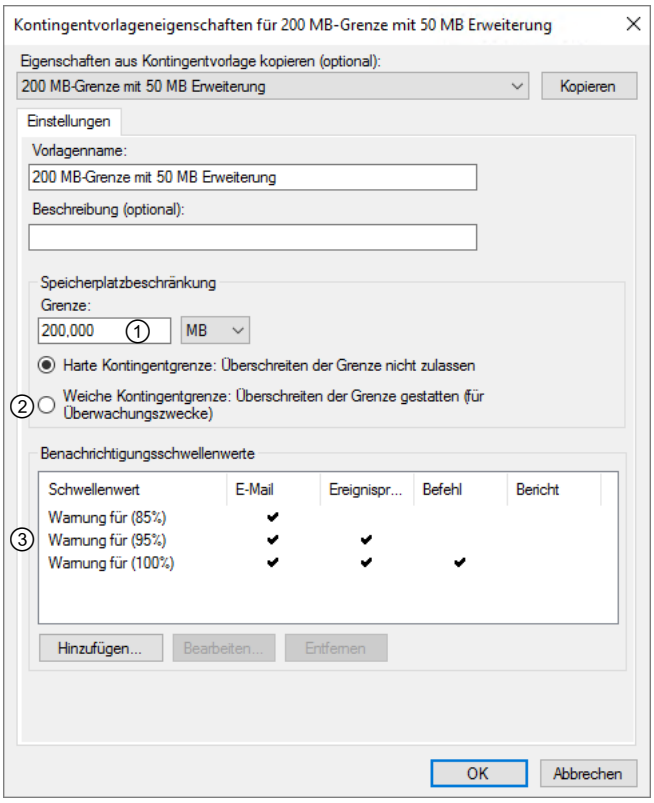
Es sind bereits Kontingentvorlagen vordefiniert, aus denen Sie eigene ableiten können. Am meisten lernen kann man aus der Vorlage *200 MB-Grenze mit 50 MB Erweiterung*.

- Öffnen Sie im Ressourcen-Manager den Knoten *Kontingentvorlagen* und klicken Sie doppelt auf die Vorlage.

① definiert den Grenzwert, auf den sich alle weiteren Konfigurationen beziehen.

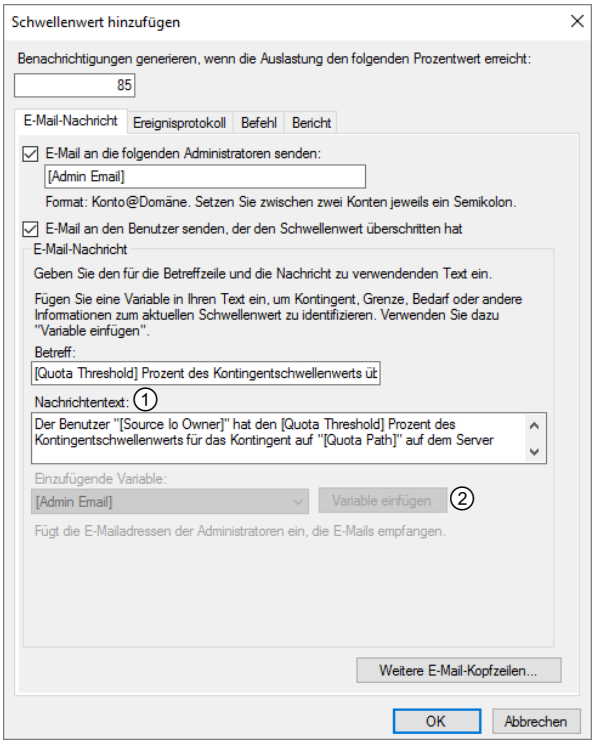
Mit der Kontingentgrenze ② legen Sie fest, ob diese Kontingentvorlage die Speichernutzung begrenzt (*Harte Kontingentgrenze*) oder nur der Überwachung dient (*Weiche Kontingentgrenze*).

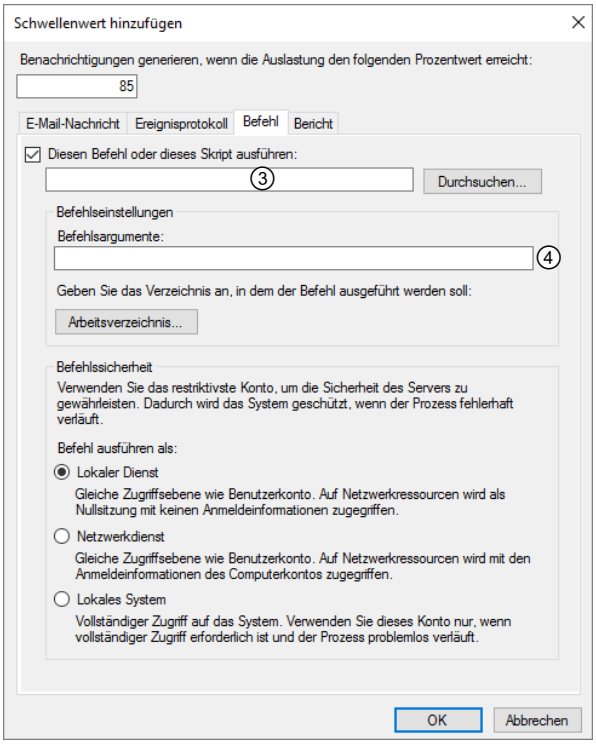
Die Benachrichtigungsschwellenwerte ③ legen fest, was geschieht, wenn ein bestimmter Schwellenwert überschritten wird. Sie können bestehende Schwellen bearbeiten oder entfernen und neue hinzufügen. In dieser Vorlage erhält ein Benutzer bei 85 % Speichernutzung eine vorbereitete E-Mail. Bei 95 % wird eine weitere E-Mail versandt und es wird ein Eintrag ins Ereignisprotokoll des Servers geschrieben. Bei 100 % erhält der Benutzer erneut eine E-Mail, die ihm mitteilt, dass sein Speicher in der Freigabe voll ist, aber einmalig um 50 MB erweitert wurde. Es wird ein weiterer Eintrag ins Ereignisprotokoll geschrieben und ein Befehl ausgeführt, der dem Benutzer weitere 50 MB Speicherplatz zur Verfügung stellt.





Schulversion
© HERDT-Verlag



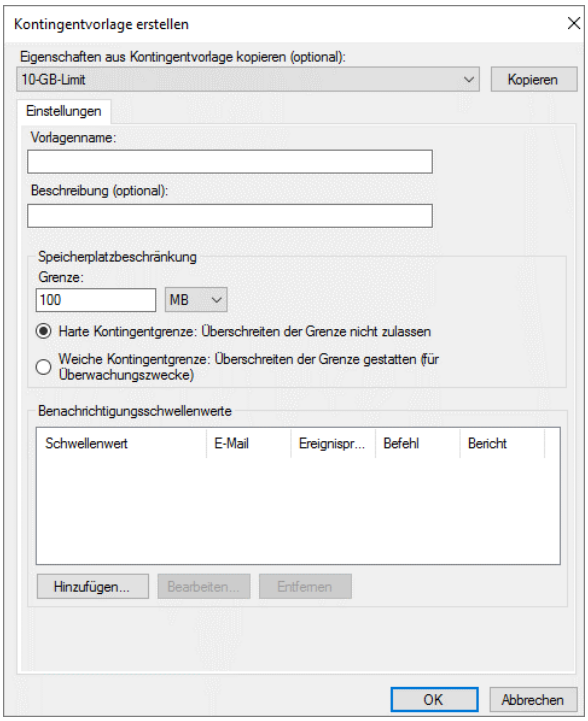

Im Feld *Nachrichtentext* ① können Sie den E-Mail-Text vorbereiten. Über *Variable einfügen* ② können Sie eine Vielzahl an Variablen in den Text einfügen. Die Einträge im Ereignisprotokoll konfigurieren Sie auf dieselbe Art.

Die Kontingent-Erweiterung erfolgt mit dem Befehl `dirquota.exe` ③ und den Befehlsargumenten ④, der die Quotagrenze aus einer anderen Kontingentvorlage kopiert.

## Neue Kontingentvorlage erstellen

- Zum Erstellen einer neuen Vorlage klicken Sie im Ressourcen-Manager in der linken Spalte auf *Kontingentvorlagen* und anschließend im Bereich *Aktionen* auf *Kontingentvorlage erstellen*.

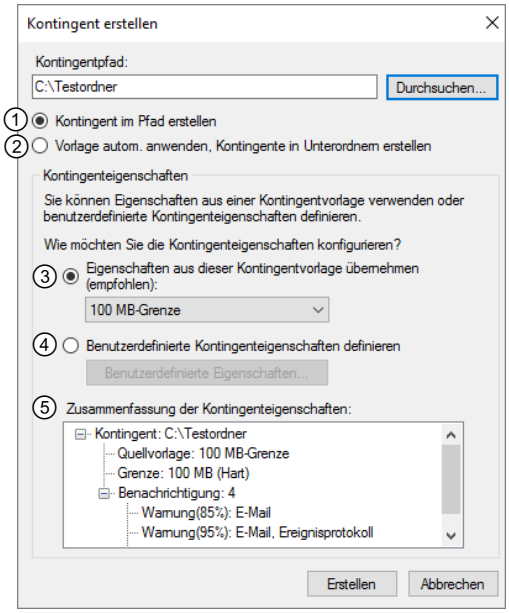
Es erscheint ein Fenster mit den Kontingentvorlagen-eigenschaften, allerdings ohne Einträge. In der obersten Zeile können Sie eine vorhandene Vorlage auswählen und deren Einstellungen kopieren, oder Sie erstellen eine komplett neue Vorlage. Den Namen der neuen Vorlage geben Sie in der zweiten Zeile ein.




*Neue Kontingentvorlage einrichten*

## Kontingent zuweisen

- Markieren Sie im Ressourcen-Manager den Knoten *Kontingente* und klicken Sie im Bereich *Aktionen* auf *Kontingent erstellen*.
- Geben Sie den Kontingentpfad manuell ein oder durchsuchen Sie den Computer.
- Wählen Sie, ob Sie das Kontingent einmalig direkt im angegebenen Pfad erstellen ① oder automatisch für jeden Benutzer in Unterordnern ② erstellen möchten.
- Wählen Sie eine bestehende Kontingentvorlage ③ oder definieren Sie Ihre eigenen Eigenschaften für das Kontingent ④.
- Überprüfen Sie die Zusammenfassung ⑤ und klicken Sie auf *Erstellen.*




Es ist nicht empfehlenswert, eigene Einstellungen ④ für ein Kontingent anzugeben, da sich das Kontingent damit schlecht verwalten lässt. Verwenden Sie stattdessen eine Vorlage.

## Dateiprüfungsverwaltung

Die Dateiprüfungsverwaltung ermöglicht eine einfache Überwachung von Benutzern hinsichtlich der gespeicherten Dateitypen (passive Prüfung). Aktives Prüfen verhindert das Speichern von angegebenen Dateitypen. Zur Durchführung dieser Aufgabe weisen Sie einem Ordner eine Dateiprüfungsvorlage zu.

Die Verwaltung ist sehr ähnlich wie bei den Kontingenten. Das prinzipielle Vorgehen ist folgendes:

- **Dateigruppen** geben an, welche Dateitypen zu ihnen gehören (und welche nicht). Sie können neue Dateigruppen erstellen oder die vorhandenen nutzen/bearbeiten.
- **Dateiprüfungsvorlagen** bestehen aus mindestens einer Dateigruppe und geben an, was geschieht, wenn ein angegebener Dateityp gespeichert wird.
- **Dateiprüfungen** weisen Volumes oder Ordnern Dateiprüfungsvorlagen zu.

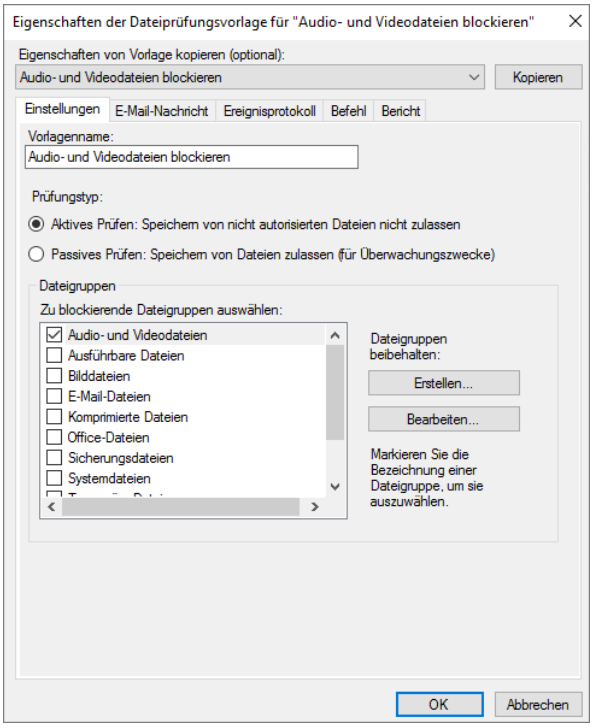
Die Abbildung zeigt die Dateiprüfungsvorlage *Audio- und Videodateien blockieren*.

Unter *Prüfungstyp* legen Sie fest, ob Sie aktiv prüfen, also das Speichern unterbinden, oder passiv prüfen und damit nur die Speichernutzung hinsichtlich der angegebenen Dateigruppen überwachen wollen.

Unter *Zu blockierende Dateigruppen auswählen* können Sie die Dateigruppen auswählen, für die diese Prüfung gilt.

Sie können neue Dateigruppen erstellen sowie die markierte Gruppe bearbeiten. Die weiteren Register entsprechen denen der Kontingentverwaltung.

Auch das Erstellen neuer Dateiprüfungsvorlagen und das Zuweisen von **Dateiprüfungen** entspricht dem Vorgang bei den Kontingentvorlagen.





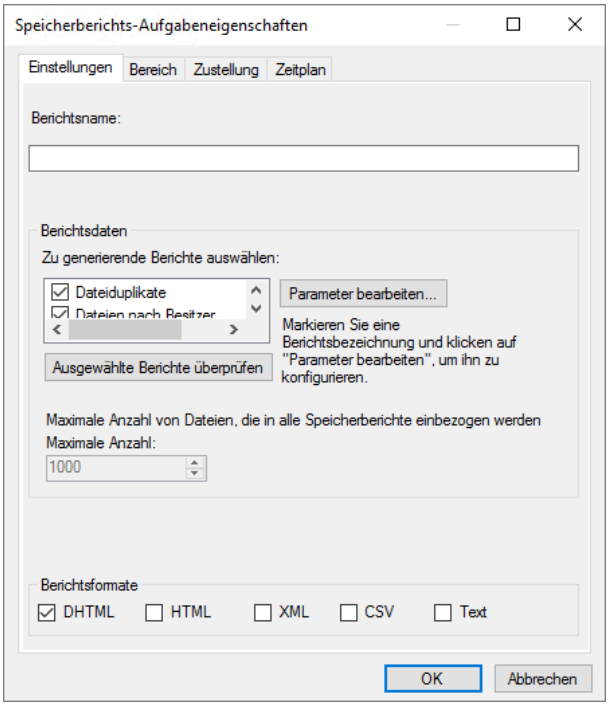
Schulversion
© HERDT-Verlag

## Speicherberichteverwaltung

Mit der Speicherberichteverwaltung können Sie Berichte über Kontingente, Dateiprüfungen und weitere vorkonfigurierte Kategorien erstellen. Besonders nützlich sind dabei die Dateiduplikate und selten verwendeten Dateien.

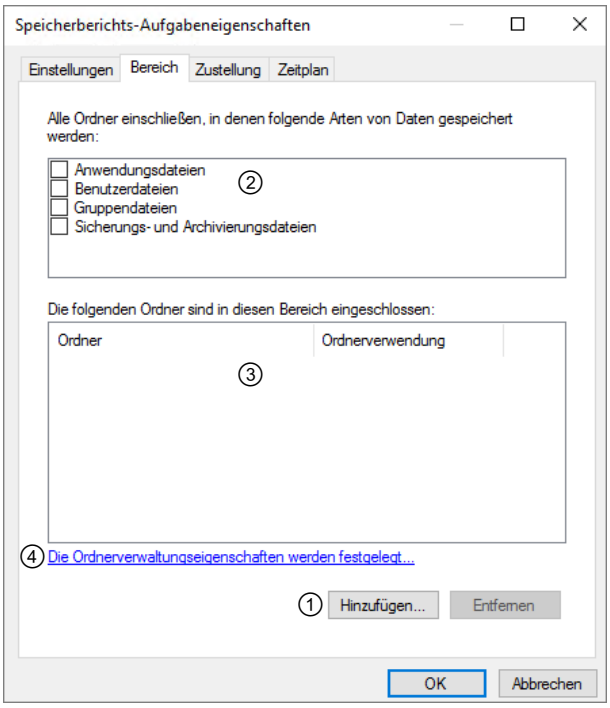
- Klicken Sie im Ressourcen-Manager in der linken Spalte auf *Speicherberichteverwaltung*.
- Klicken Sie im Aktionsbereich auf *Neue Berichtaufgabe planen*.
- Geben Sie auf der Registerkarte *Einstellungen* einen Berichtsnamen ein.
- Wählen Sie die Berichte aus und bearbeiten Sie falls nötig deren Parameter.

  Unter *Ausgewählte Berichte überprüfen* erhalten Sie eine Zusammenfassung.
- Legen Sie die Berichtsformate fest.




- Legen Sie auf der Registerkarte *Bereich* die Ordner fest, die vom Bericht erfasst werden sollen.

  Sie können manuell Ordner hinzufügen ① oder über die Verwaltungseigenschaften der Ordner ② (Anwendungsdaten, Benutzerdaten, Gruppendaten oder Sicherungsdaten) die entsprechenden Ordner automatisch hinzufügen ③. Unter ④ können Sie alle eingerichteten Verwaltungseigenschaften einsehen, verändern und neue Ordner einbeziehen.
- Geben Sie auf der Registerkarte *Zustellung* eine E-Mail-Adresse an und geben Sie auf der Registerkarte *Zeitplan* an, wann der Bericht erstellt werden soll.
- Klicken Sie auf *OK*.



## 18.5 Versionierung und Deduplizierung

### Versionierung für Dateiserver mithilfe von Schattenkopien

Schon beim Einrichten von Dateiservern sollten Sie über Datensicherung und leichte Verwaltbarkeit nachdenken. Ein wichtiger Aspekt ist hier die Dateiversionierung mithilfe des Volumenschattenkopierdienstes (Volume Shadow Copy Service, VSS). Diese Aufgabe übernimmt der Dateiserver-VSS-Agent-Dienst, der normalerweise bei der Installation der Dateidienste mit installiert wird. Die Schattenkopien sorgen dafür, dass die Benutzer der Freigabe dort selbstständig zu Vorgängerversionen zurückkehren können, ohne dass dabei ein Administrator tätig werden müsste. Diese Funktion bietet großen Komfort für Administratoren und Benutzer, deshalb sollten Sie sie unbedingt für Ihre Dateiserver nutzen. Überprüfen Sie das Vorhandensein des Dienstes unter *Serverrollen - Datei- und Speicherdienste - Datei- und iSCSI-Dienste* und installieren Sie ihn gegebenenfalls nach.

### Einrichten der Schattenkopien in der Computerverwaltung

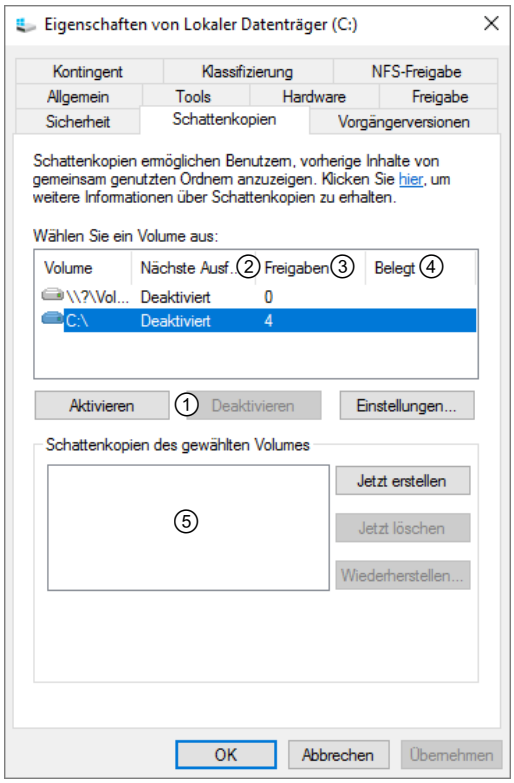
Die Einstellungen für die Schattenkopien von Freigaben finden Sie in der Computerverwaltung oder im Windows-Explorer im Kontextmenü eines Volumes.

- Geben Sie auf dem Dateiserver *B-FS01* im Startmenü „compmgmt.msc“ ein. Sie können auch die Eigenschaften eines Volumes im Windows-Explorer aufrufen.

  Alternativ können Sie die Computerverwaltung auch über das Menü *Tools* im Server-Manager oder das Schnellzugriffsmenü öffnen.
- Erweitern Sie in der Navigationsspalte den Eintrag *Computerverwaltung (lokal) - System*.
- Markieren Sie *Freigegebene Ordner* und klicken Sie auf den Menübefehl *Aktion - Alle Aufgaben - Schattenkopien konfigurieren*.

  Der Dialog *Schattenkopien* wird geöffnet.
- Markieren Sie das betreffende Volume und klicken Sie auf *Aktivieren* ①.

Unter *Einstellungen* können Sie konfigurieren, auf welchem Volume die Schattenkopien gespeichert werden sollen, wie viel Speicherplatz dafür zur Verfügung gestellt wird und in welchen Zeitabständen eine Schattenkopie angefertigt werden soll. In der Volume-Liste wird angezeigt, wann die nächste Schattenkopie erstellt wird ②, wie viele Freigaben sich auf dem Volume befinden ③ und wie viel Speicherplatz von den Schattenkopien auf dem Laufwerk belegt wird ④. Im Bereich ⑤ werden die vorhandenen Schattenkopien aufgelistet. Mit *Jetzt erstellen* können Sie eine Schattenkopie anfertigen.




- Klicken Sie nach Abschluss der Einstellungen auf *OK*.

  Die Schattenkopien sind nun aktiviert und stehen für alle Benutzer der Freigaben auf diesem Volume zur Verfügung.

Beachten Sie, dass die Versionierung mittels VSS auf keinen Fall ein regelmäßiges Backup ersetzen kann!


Schulversion
© HERDT-Verlag

### Datendeduplizierung

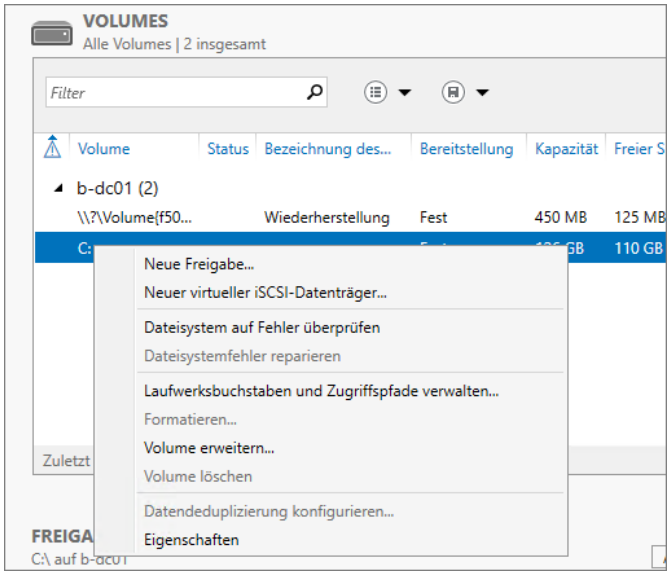
Windows Server 2019 verfügt mit der Datendeduplizierung über ein Werkzeug zur Optimierung der Dateidienste. Hierbei werden mehrfach vorhandene Dateien und Dateibestandteile nur einmal auf dem Dateiserver abgespeichert, indem sie blockweise über Prüfsummen verglichen werden. Die Deduplizierung basiert auf ähnlichen Verfahren wie die Volumenschattenkopien, die für Backups und die Dateiversionierung verwendet werden.

Stellen Sie sicher, dass die Datendeduplizierung als Serverrolle unter *Serverrollen - Datei- und Speicherdienste - Datei- und iSCSI-Dienste* installiert wurde.

- Klicken Sie im *Server-Manager - Datei- und Speicherdienste - VOLUMES* mit der rechten Maustaste auf ein Volume und wählen Sie im Kontextmenü *Datendeduplizierung konfigurieren*.

  Beachten Sie, dass für das Systemvolume *C:* keine Datendeduplizierung verfügbar ist.
- Klicken Sie im Fenster *Deduplizierungs-optionen* auf die Option *Datenduplizierung aktivieren*.
- Nehmen Sie optional weitere Einstellungen zum Zeitplan und zur Ordnerauswahl vor und klicken Sie auf *OK*.

Damit haben Sie die Deduplizierung eingeschaltet.




## 18.6 Weitere Techniken zur Bereitstellung von Dateien

### DFS (Distributed File System)

Bei mehreren Dateiservern wird es für Benutzer immer schwieriger, sich zu merken, welche Freigabe auf welchem Server zu finden ist. Abhilfe schafft das verteilte Dateisystem DFS mit seinen Namensräumen (Namespaces). Im DFS-Namespace erstellen Sie Ordner, die Sie mit beliebigen Freigaben verknüpfen können. Mit DFS können Sie so Ihre gesamte Dateiserver- und Freigabe-Landschaft abstrahieren. Benutzer greifen auf den Namespace zu und werden automatisch zur verknüpften Freigabe weitergeleitet. Ein Benutzer muss sich nur noch seine Freigabe merken, denn aus Benutzersicht besteht kein Unterschied zwischen einer Freigabe und einem Namespace.

DFS bietet weitere Vorteile:

- Wenn eine Freigabe auf einen anderen Server umzieht, müssen Sie das den Benutzern nicht mehr mitteilen. Sie passen einfach die Ordnerverknüpfung im Namespace an.
- Stellen mehrere Server die gleichen Inhalte bereit, bietet DFS gleich mehrere Vorteile:
  - Die DFS-Replikation kann den Abgleich der Inhalte übernehmen.
  - Fällt ein Server aus, wird der Client automatisch an einen anderen vermittelt.
  - Das Active Directory sorgt dafür, dass Clients mit standortinternen Servern arbeiten. Falls die Freigabe nicht im Standort verfügbar ist, wird diejenige Freigabe benutzt, deren Standortverknüpfungen die niedrigsten Kosten aufweisen.

DFS verhindert nicht, dass weiterhin mit den vorhandenen Freigaben gearbeitet wird. Der Einsatz von DFS lohnt sich erst ab dem zweiten Dateiserver, daher wird die Einrichtung von DFS im HERDT-Buch *Windows Server 2019 – Erweiterte Netzwerkadministration* beschrieben.

## Dynamische Zugriffskontrolle mit DAC (Dynamic Access Control)

Seit Server 2012 ist mit DAC ein neuer interessanter Mechanismus hinzugekommen, um große Dateimengen in sehr komplexen Umgebungen verwalten zu können. Dabei werden den Dateien zusätzliche Metadaten angehängt, die anschließend über Regeln und Bedingungen über den Zugriff entscheiden. Die große Neuerung ist dabei, dass diese Metadaten auch dann erhalten bleiben, wenn Dateien an einen anderen Ort verschoben oder kopiert wurden, ähnlich wie bei den Daten für das Digitale-Rechte-Management (DRM).

DAC arbeitet zum Erstellen der DAC-Metadaten mit den automatischen Dateiklassifizierungsdiensten zusammen und konzentriert sich dabei vor allem auf Microsoft-Office-Dateien. DAC erstellt dabei eine ähnliche Hierarchie wie die in diesem Buch beschriebenen lokalen Ressourcen- und Sammelgruppen. So gibt es Attribute wie die Abteilung und besondere Titel (z. B. den Abteilungsleiter), mit deren Hilfe der Zugang über logische Verknüpfungen geregelt wird. Denkbar wäre zum Beispiel, dass die Metadaten einer Word-Datei besagen, dass sie vom Abteilungsleiter der Buchhaltung erstellt wurde. Unabhängig davon wo diese Datei gespeichert ist, sie kann nur von Benutzern geöffnet werden, die die Attribute *Buchhaltung* und *Abteilungsleiter* besitzen. Die Rechte können allerdings auch so gesetzt werden, dass alle Abteilungsleiter aus allen Abteilungen die Datei lesen dürfen.

Die klassischen NTFS- und Freigabeberechtigungen existieren gleichberechtigt neben den DAC-Metadaten. DAC vererbt wie NTFS standardmäßig die Berechtigungen für alle untergeordneten Ordner und Dateien. Für einen Dateizugriff wird entweder das Gespann aus Freigabe- und NTFS-Berechtigungen benötigt oder alternativ der Zugang über DAC ermöglicht. Sobald eine der Berechtigungsarten den Zugang verbietet, kann nicht auf die Datei zugegriffen werden. Mit DAC kann der Anwender in solchen Fällen mit einem Mausklick eine E-Mail an einen Administrator senden und um eine Freischaltung bitten.

Die dynamische Zugriffskontrolle zielt auf die Cloud, in der sich die Daten zu verschiedenen Zeiten an verschiedenen Plätzen und den verschiedensten Geräten befinden können. Die starre Berechtigungsstruktur der Dateifreigaben kann solch eine Flexibilität nicht bieten, andererseits ist so eine Vielseitigkeit und Offenheit in vielen Unternehmen auch gar nicht nötig oder erwünscht.

DAC ist eine sehr junge Technik, die zum jetzigen Zeitpunkt noch nicht vollständig ausgereift scheint. Für eine einfach aufgebaute Firmenumgebung wird DAC definitiv nicht benötigt. Sie wird jedoch im HERDT-Buch *Windows Server 2019 - Erweiterte Netzwerkadministration* ausführlicher behandelt.

## Speicherplätze und Speicherpools

Mit dieser Technik zur Datenträgervirtualisierung können mehrere Datenträger zu einem Pool zusammengeschlossen werden, der virtuelle Datenträger enthält, die nach außen hin wie normale Volumes erscheinen. Dieses Verfahren ermöglicht erheblich mehr Flexibilität und Skalierbarkeit als traditionelle Speicherlösungen und ist im Hinblick auf lokale Clouds sehr interessant, in diesem Buch wird jedoch nicht weiter darauf eingegangen.


Schulversion
© HERDT-Verlag

# 19 Dateidienste planen

**In diesem Kapitel erfahren Sie**

- wie Sie Dateidienste für ein Unternehmensnetz einsetzen
- wie Sie Berechtigungen verwalten können
- wie eine Ordnerstruktur aufgebaut wird

**Voraussetzungen**

- Dateidienste einrichten
- Rechte und Berechtigungen

## 19.1 Gründe für zentrale Datenspeicherung

### Ziele von Dateistrukturen

Bevor Sie mit dem Aufbau einer Dateistruktur für ein Unternehmen beginnen, gilt es die Ziele zu ermitteln, für die das Dateisystem verwendet werden soll. Diese lassen sich unter den folgenden Gesichtspunkten zusammenfassen:

- Gemeinsame Verwendung von Dokumenten
- Zentrale Speicherung, Archivierung und Sicherung
- Hochverfügbarkeit
- Datenaustausch
- Schutz von Informationen
- Minimierung der Kosten

### Gemeinsame Verwendung von Dokumenten

In einem Unternehmen werden viele Mitarbeiter ähnliche oder identische Dokumente verwenden. Beispiele hierfür sind Formatvorlagen, Formulare, Dokumentationen oder Prozessbeschreibungen.

Eines der Ziele einer Dateistruktur muss sein, die mehrfache Speicherung dieser Dateien zu begrenzen, die zentrale Verfügbarkeit zu gewährleisten und den schnellen Zugriff für alle Mitarbeiter sicherzustellen.

Dies lässt sich erreichen, indem bei der Bereitstellung von Dateien konsequent eine logisch aufgebaute Struktur befolgt wird. Je klarer und strukturierter die Dateidienste eingerichtet wurden, desto weniger Raum ergibt sich für Duplikate und Wildwuchs.

Bei mehreren Dateiservern sollten außerdem automatische Replikationsmechanismen wie das DFS zum Einsatz kommen. So können an einem zentralen Speicherort die Dateien verwaltet werden, und die automatische Replikation sorgt dafür, dass an jedem Standort lokal die aktuellen Versionen für die Benutzer zur Verfügung stehen.

### Zentrale Speicherung, Archivierung und Sicherung

Wenn mehrere Benutzer mit Daten arbeiten müssen, die lokal gespeichert werden, sind Verzögerungen unvermeidlich. Es muss geklärt werden, wo welche Daten in welcher Version vorliegen, wie der Zugriff erfolgen kann und wer Berechtigungen erhält. Nur eine zentrale Dateiarchitektur kann diese Prozesse schnell, schlank und sicher gewährleisten.

Ein weiteres Problem ergibt sich, wenn in einem Netzwerk unterschiedliche Versionen von Dateien im Umlauf sind. Dies führt dazu, dass identische Arbeitsschritte mehrfach durchgeführt werden, was zulasten der Produktivität geht. Durch eine zentrale Archivierung werden unterschiedliche Versionen erfasst und verfügbar gemacht, wodurch die Produktivität gesteigert werden kann.

Wenn Daten dezentral im Netzwerk verteilt sind, ergeben sich Probleme bezüglich ihrer Sicherung. Heutige Datenmengen erlauben es nicht, Backupstrategien für Arbeitsplatzrechner praktisch umzusetzen. Daher können Daten nur dann sinnvoll gespeichert werden, wenn dies auf zentralen Servern durchgeführt wird. Auch das Wiederherstellen von Daten kann nur effektiv erfolgen, wenn diese auf zentral verfügbaren Medien vorgehalten werden.

### Hochverfügbarkeit

Die Hochverfügbarkeit von Daten kann erreicht werden, indem Redundanzen bei der Speicherung der Daten zum Einsatz kommen. Hier werden RAID-Systeme (Redundant Array of Independent Disks, redundante Anordnung unabhängiger Festplatten) verwendet, die auf Servern mit hoher Ausfallsicherheit und geringer Ausfallwahrscheinlichkeit installiert werden.

Zusätzlich lassen sich durch Replikation auf mehrere Server die Daten mehrfach verfügbar halten, sodass bei einem Ausfall Benutzer auf ein Replikat zugreifen können. Dafür kann DFS unter Windows Server 2019 eingesetzt werden.

### Datenaustausch

Eine weitere Aufgabe einer Dateistruktur besteht darin, Benutzern effektive Wege für den Datenaustausch zur Verfügung zu stellen. Nur durch gemeinsame, kontrollierte Zugriffe auf bestimmte Speicherorte im Netzwerk ist es möglich, Daten bei Bedarf auszutauschen. Würde eine dezentrale Speicherung erfolgen, so müsste der Zugriff entweder über Wechselmedien erfolgen oder die Daten würden (z. B. per Mail) auch dann übertragen werden, wenn kein sofortiger Zugriff benötigt wird. Flüssige Arbeitsabläufe würden so erschwert.

### Schutz von Informationen

Indem Daten zentral gespeichert werden, ist es möglich, Zugriffe auf diese auch zentral zu steuern. Da die Berechtigungen von professionellem Personal verwaltet werden, kann gewährleistet werden, dass nur die Benutzer und Gruppen Zugriff erhalten, die auch dazu berechtigt sind.

Zusätzlich lassen sich an zentraler Stelle Verschlüsselungsmechanismen einsetzen, die die Daten vor unbefugten Zugriffen schützen. Windows Server 2019 unterstützt hierzu das verschlüsselnde Dateisystem (EFS) für Daten einzelner Benutzer. Für ganze Festplatten kann mit BitLocker der Schutz vor unbefugten Zugriffen auch dann sichergestellt werden, wenn Angreifer physischen Zugriff auf Datenträger erlangen.

Und schließlich lassen sich noch Übertragungen im Netzwerk verschlüsseln, um Daten von bestimmten Quellen zu schützen. So kann etwa die Übertragung vom Dateiserver der Buchhaltungsabteilung mit IPsec verschlüsselt werden, Datenverkehr zwischen anderen Rechnern dagegen unverschlüsselt bleiben, um die Geschwindigkeit von Netzwerkzugriffen zu optimieren.

### Minimierung der Kosten

Indem die mehrfache Speicherung von Daten vermieden wird, werden die Kosten für Festplattensysteme und Sicherungsmedien verringert.

## 19.2 Dateistruktur planen

### Bedarf ermitteln

Sie müssen untersuchen, welche Daten von welchen Mitarbeitern benötigt werden. Hierfür werden genaue Kenntnisse über Arbeitsabläufe benötigt. Nur wenn Sie wissen, wer mit welchen Daten in welcher Reihenfolge arbeiten muss, kann auch ein reibungsloser Datenaustausch sichergestellt werden.


Schulversion
© HERDT-Verlag

### Übungsszenario

In *Firma GmbH* sollen ausgesuchte Dateien aus der Buchhaltung der Verwaltungsabteilung zugänglich gemacht werden. Dazu soll ein Datenaustauschverzeichnis eingerichtet werden, auf das alle Verwaltungsmitarbeiter bis auf die Azubis Lesezugang erhalten sollen. Diesen Datenaustausch darf nur der Abteilungsleiter der Buchhaltung in Berlin einleiten.

### Anforderungen an die Dateistruktur ermitteln

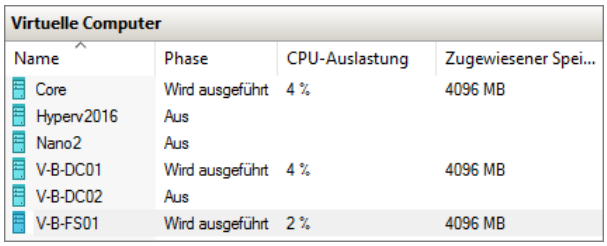
Aus der Analyse der Arbeitsabläufe ergeben sich die folgenden Anforderungen an die Dateistruktur:

- Sie benötigen ein Abteilungslaufwerk für die Buchhaltung in *Berlin*, auf das diese exklusiven Zugriff hat.
- Es muss ein eigenes Datenaustauschverzeichnis geben, über das die ausgewählten Daten der Verwaltungsabteilung zugänglich gemacht werden können.
- Für das Austauschverzeichnis müssen neue lokale Gruppen mit den Zugriffsarten L, AE, VZ und KZ erstellt werden.
- Der Abteilungsleiter der Buchhaltung benötigt für das Austauschverzeichnis die Ändern-Berechtigung (AE), die Sachbearbeiter und der Abteilungsleiter der Verwaltung erhalten Leseberechtigung.

## 19.3 Verzeichnisstruktur anlegen

### Vorbereitung

Sie können die Aufgabe des Dateiservers auf einem Domänencontroller einrichten, in der Praxis sollte jedoch ein dedizierter Server für diese Aufgabe bereitgestellt werden. In der Testumgebung übernimmt der Server *B-FS01* diese Rolle. Erstellen Sie nach der Installation eine zweite Partition, die den restlichen vorhandenen Speicherplatz umfasst. Die erste Partition enthält das Betriebssystem, die zweite ist für die Datenspeicherung reserviert. Konfigurieren Sie die Netzwerkeigenschaften des Servers passend zu Ihrer Umgebung und machen Sie ihn zu einem Mitgliedsserver in der Domäne.



Virtuelle Computer

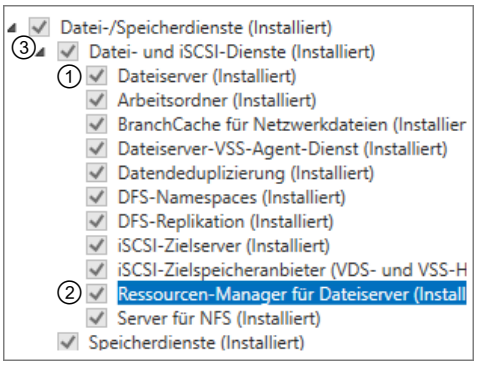
| Name | Phase | CPU-Auslastung | Zugewiesener Spei... |
|---|---|---|---|
| Core | Wird ausgeführt | 4 % | 4096 MB |
| Hyperv2016 | Aus | | |
| Nano2 | Aus | | |
| V-B-DC01 | Wird ausgeführt | 4 % | 4096 MB |
| V-B-DC02 | Aus | | |
| V-B-FS01 | Wird ausgeführt | 2 % | 4096 MB |

*Virtueller Dateiserver V-B-FS01*

### Aufgabe 1

- Fügen Sie auf dem Dateiserver *B-FS01* die Rolle *Dateiserver* mit den Rollendiensten *Dateiserver* ① und *Ressourcen-Manager für Dateiserver* ② hinzu. Erweitern Sie dazu im Fenster *Rollen* die Einträge *Datei- und Speicherdienste* sowie *Datei- und iSCSI-Dienste* ③
- Bestätigen Sie die Installation zusätzlicher Rollen und Features, falls Sie dazu aufgefordert werden.

Die Rolle *Dateiserver* ist standardmäßig aktiviert, dies gilt jedoch nicht für die restlichen Komponenten aus den Datei- und Speicherdiensten.




*Rollendienste für Dateiserver hinzufügen*

## Aufgabe 2

- Erstellen Sie ein Verzeichnis für die Abteilung *Verwaltung* in *Berlin*.
  Verwenden Sie dabei die Namenskonventionen aus Kapitel 1.
- Erstellen Sie die benötigten lokalen Gruppen für die Zugriffe auf das Verzeichnis.
- Geben Sie das Verzeichnis frei und konfigurieren Sie die Freigabe- und NTFS-Berechtigungen.

## Aufgabe 3

- Erstellen Sie ein Datenaustauschverzeichnis für die Abteilung *Buchhaltung* und *Verwaltung*.
- Erstellen Sie die benötigten lokalen Gruppen für die Zugriffe auf das Verzeichnis.
- Geben Sie das Verzeichnis frei und konfigurieren Sie die Freigabe- und NTFS-Berechtigungen so, dass nur der Abteilungsleiter der Buchhaltung Schreibzugriffe auf dieses Verzeichnis durchführen darf.

## Aufgabe 4

Überlegen Sie, wie Sie das Skript zum Erstellen der lokalen Gruppen für Abteilungslaufwerke verbessern könnten.

Für solche Aufgaben ist das Kommandozeilentool *icacls.exe* geeignet. (Der Name bedeutet übrigens 'Improved CACLs', was wiederum 'Change Access Control Lists' heißt.) Der folgende Befehl fügt zum Beispiel dem Ordner *D:\LW_Buchhaltung* (dem Abteilungslaufwerk) die lokale Gruppe *LG-B-LW_Buchhaltung-VZ* für Vollzugriff hinzu:

```
icacls.exe C:Freigaben\LW_Buchhaltung /grant:r LG-B-LW_Buchhaltung-VZ:F /T /C
```

| | |
|---|---|
| `/grant` | Vergibt eine Berechtigung |
| `:r` | Steht für replace (ersetzen) und wird direkt angehängt: `/grant:r` |
| `:F`<br>`:M`<br>`:RX`<br>`:R`<br>`:W` | Wird ohne Leerzeichen an den Namen gehängt. F vergibt den Vollzugriff. Die verschiedenen Berechtigungen sind F = Full (Vollzugriff), M = Modify (Ändern), RX = Read/Execute (Lesen/Ausführen), R = Read (Lesen) und W = Write (Schreiben). |
| `/T` | Vererbt die Berechtigung an alle Unterordner und Dateien |
| `/C` | Unterdrückt Fehlermeldungen |

Der Befehl `icacls` ist sehr mächtig und verfügt über zahlreiche Optionen und Parameter. Einige davon sind nicht einmal in der Hilfe-Funktion aufgelistet. Eine ausführlichere Dokumentation finden Sie im Internet, wenn Sie nach `icacls` suchen.

## Aufgabe 5

- Melden Sie sich auf dem Mitgliedsserver mit unterschiedlichen Benutzern an und überprüfen Sie, ob Ihre Lösung die geforderten Zugriffe erlaubt.


Schulversion
© HERDT-Verlag

# 20 Gruppenrichtlinien

**In diesem Kapitel erfahren Sie**

- wie Sie Gruppenrichtlinien für verschiedene Erfordernisse einsetzen können
- was ein Gruppenrichtlinienobjekt ist
- wie Gruppenrichtlinieneinstellungen verarbeitet werden
- wie Gruppenrichtlinien vererbt werden

**Voraussetzungen**

- Active Directory-Objekte
- Gruppen verwalten

## 20.1 Einsatzbereiche von Gruppenrichtlinien

### Einführung

Bevor Ihnen gezeigt wird, wie Sie Gruppenrichtlinien erstellen und bearbeiten können, ist es wichtig, dass Sie erfahren, um was es sich dabei eigentlich handelt. Schon der Begriff Gruppenrichtlinie ist etwas irreführend, denn es sind keine Richtlinien, die nur für Gruppen gelten, sondern es handelt sich um eine Gruppe von Richtlinien.

### Definition

Gruppenrichtlinien sind Konfigurationsanweisungen. Mit ihrer Hilfe können Sie bestimmte Einstellungen erzwingen. Sie werden – je nach Art – auf einen Standort, die Domäne oder eine Organisationseinheit angewendet und sind teilweise über die Grenzen separater Gesamtstrukturen hinweg wirksam. Sie beinhalten auch die Funktion der Vererbung und die Möglichkeit, die Verwaltung zu delegieren. Gruppenrichtlinien werden im Active Directory gespeichert und auf dem Wege der Replikation domänenweit verfügbar gemacht.

### Vorteile von Gruppenrichtlinien

Allgemein gesprochen verwenden Sie Gruppenrichtlinien, um Desktops von Benutzern und Computern zu konfigurieren. Sie helfen, die Gesamtbetriebskosten eines Netzwerks zu senken, indem die Produktivität von Mitarbeitern auf einem hohen Niveau gehalten wird. Gruppenrichtlinien sind ein mächtiges Instrument zur Konfiguration, Verwaltung und Absicherung des Netzwerks:

- Handlungsmöglichkeiten von Benutzern festlegen
- Aufrechterhaltung von Computerkonfigurationen
- Pflege und Verfügbarkeit der verwendeten Anwendungsprogramme im Unternehmen
- Verwaltungsaufwand der Administratoren senken

### Beispiele für Anforderungen, die mit Gruppenrichtlinien erfüllt werden können

- Die Benutzer der Organisationseinheit *OU-B-Verwaltung* müssen einen Bildschirmschoner mit Kennwortschutz verwenden.
- Die Dokumente im lokalen Ordner *Eigene Dateien* der Benutzer in der OU *OU-B-Verwaltung* sollen im Netzwerk in einem Ordner *<Benutzername>\Eigene Dateien* gespeichert werden.
- In der OU *OU-B-Verwaltung* soll der Benutzername der letzten Benutzeranmeldung nicht im Anmeldedialog angezeigt werden.

- Lokale Kopien von Offline-Dateien sollen beim Abmelden des Benutzers gelöscht werden.
- Das Kennwort für die Benutzeranmeldung in der Domäne soll mindestens sechs Zeichen enthalten.
- Nach 3 ungültigen Anmeldeversuchen soll das Benutzerkonto für 30 Minuten gesperrt werden.

## Einsatzbereiche

| | |
|---|---|
| Registrierungseinträge überschreiben | **Administrative Vorlagen**<br>Mit administrativen Vorlagen steuern Sie Konfigurationen, die auf Werteinträgen der Registry beruhen. Gruppenrichtlinien überschreiben vorhandene Registrierungseinträge. Es gibt diese administrativen Vorlagen für Computer und für Benutzer. |
| Domänensicherheit | **Sicherheitsrichtlinie für Domänen**<br>Solche Einstellungen betreffen verschiedene Aspekte, die im Zusammenhang mit der Anmeldung von Benutzern stehen, z. B. die Länge und die Dauer von Kennwörtern und Kontosperrdauer. |
| Skriptverarbeitung | **Anmeldung/Abmeldung**<br>Skript, das bei der Benutzeranmeldung bzw. -abmeldung ausgeführt wird<br>**Start/Herunterfahren**<br>Skript, das beim Computerstart oder beim Herunterfahren ausgeführt wird |
| Softwareinstallation | Mit Gruppenrichtlinien können Sie die Verteilung und Verwaltung von Software zentral steuern. Die Aufgaben umfassen die Installation, die Aktualisierung (Update) und das Entfernen von Anwendungsprogrammen.<br>Software kann auf Benutzer oder auf Computer verteilt werden. Deshalb gibt es auch hier Gruppenrichtlinien für Benutzer und Gruppenrichtlinien für Computer. |
| Software-einschränkung | Diese Gruppenrichtlinie erlaubt es, die Ausführung von Software zu unterbinden. Sie können so beispielsweise verhindern, dass Benutzer unbekannte oder selbst installierte Software ausführen und damit Computer schädigen. |
| Internet Explorer | Mit diesen Gruppenrichtlinien verwalten Sie die Einstellungen des Internet Explorers. Die Einstellungen beziehen sich z. B. auf die Startseite. |
| Ordnerumleitung | Mit dieser Gruppenrichtlinie können Sie veranlassen, dass persönliche Dokumente des Benutzers nicht im Profilordner, sondern in einem separaten Netzlaufwerk gespeichert werden. Die Ordnerumleitung ist Teil des IntelliMirror-Konzepts und steht im Zusammenhang mit der Verwaltung von Benutzerdaten und Benutzerprofilen. |

## Administrative Vorlagen

Administrative Vorlagen sind softwarebezogene Blöcke von Einstellungen, die das Verhalten von spezifischer Software beeinflussen. Die Einstellungen werden in `.admx`-Dateien mit entsprechenden Registrierungsschlüsseln verknüpft, die Anzeige in der Gruppenrichtlinie erfolgt über die Auswertung der zugehörigen `.adml`-Datei in der passenden Sprachversion. Zusätzlich zu der bei der Installation gewählten Sprache speichert Microsoft auch die englische Version.

So können Sie z. B. das Verhalten des Windows-Explorers in der Datei `WindowsExplorer.admx` konfigurieren. Sie erzwingen beispielsweise das Ausblenden der Laufwerke A: und B:.

```
Datei  Bearbeiten  Format  Ansicht  ?
    <elements>
      <enum id="NoDrivesDropdown" valueName="NoDrives" required="true">
        <item displayName="$(string.ABOnly)">
          <value>
            <decimal value="3" />
          </value>
        </item>
        <item displayName="$(string.COnly)">
```

*Registrierungsschlüssel in `.admx`-Datei mit Wert belegen*


Schulversion
© HERDT-Verlag

Damit nun ein Administrator in der Gruppenrichtlinie auch die richtigen Parameter konfigurieren kann, wird in der passenden `.adml`-Datei eine Interpretationsanweisung für die Zeichenfolge (string) „ABOnly“ geliefert.

Die `.admx`-Dateien werden im Verzeichnis `%systemroot%\PolicyDefinitions` gespeichert, die zugehörigen `.adml`-Dateien im Unterverzeichnis für die jeweilige Sprache, z. B. `%systemroot%\PolicyDefinitions\de-DE`.

```
Datei  Bearbeiten  Format  Ansicht  ?
<?xml version="1.0" encoding="utf-8"?>
<!--  (c) 2006 Microsoft Corporation  -->
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema" xm
  <displayName>Anzeigename hier eingeben</displayName>
  <description>Beschreibung hier eingeben</description>
  <resources>
    <stringTable>
      <string id="ABCDOnly">Nur Laufwerke A, B, C und D beschränken</strin
      <string id="ABConly">Nur Laufwerke A, B und C beschränken</string>
      <string id="ABOnly">Nur Laufwerke A und B beschränken</string>
      <string id="ALLDrives">Alle Laufwerke einschränken</string>
      <string id="ClassicShell">Klassische Shell aktivieren</string>
```

*Deutsche `.adml`-Datei für den Windows-Explorer*

Die `.admx`- und `.adml`-Dateien können mit dem Editor modifiziert werden, um zusätzliche Werte konfigurieren zu können.

## Erweiterung durch neue administrative Vorlagen

Software-Hersteller geben ihren Software-Paketen entsprechende Vorlagen bei. Auch ist zu erwarten, dass Microsoft neue Vorlagendateien erstellt und auf verschiedenen Vertriebswegen verteilt. Mit Gruppenrichtlinien-implementierungen können Sie gegebenenfalls sogar aufgedeckte Sicherheitslücken schnell schließen. Ebenso verteilen und vertreiben Anbieter von Desktop-Betriebssystemen und Netzwerkbetriebssystemen oder Hersteller von Geräten Vorlagendateien mit ihren Produkten. Vorlagen können auch in englischer Sprache verfasst sein.

Vorlagendateien werden zumeist in Verbindung mit einem Utility angeboten. Die Installation solcher Utilities ist nicht erforderlich, wenn Sie dies nicht wünschen. Im Sinne einer zentralisierten, überschaubaren Verwaltung kann es sinnvoll sein, die gewünschten Vorlagendateien in ein vorgesehenes Verzeichnis zu speichern.

Damit die Gruppenrichtlinien auf allen Domänencontrollern ausgewertet werden können, müssen diese auf allen DCs lokal in identischer Version vorliegen.

Ab Windows Server 2008 können Sie die administrativen Vorlagen auf alle Domänencontroller replizieren, indem das Verzeichnis `PolicyDefinitions` unter `Sysvol` im Verzeichnis `Policies` bereitgestellt wird. Diese werden dann anstelle der lokalen Versionen von `PolicyDefinitions` ausgewertet.

## Gruppenrichtlinienergebnisse und -modellierung

Windows Server 2019 bietet mit den Tools *Gruppenrichtlinienergebnisse* und *Gruppenrichtlinienmodellierung* zwei Werkzeuge in der Gruppenrichtlinienverwaltung, die Sie zur Überprüfung und Konzeption der tatsächlich auf ein Objekt angewandten Richtlinien einsetzen können. So lassen sich Probleme und Konflikte mit Richtlinien leichter ausfindig machen bzw. im Vorfeld vermeiden.

## 20.2 Gruppenrichtlinienobjekt

### GPO (Group Policy Object)

Im Gruppenrichtlinienobjekt (Group Policy Object, GPO) werden die einzelnen Gruppenrichtlinien (Gruppenrichtlinieneinstellungen) gespeichert. Der Inhalt des Gruppenrichtlinienobjekts wird sowohl in einer Vorlage als auch in einem Container gespeichert.

### Verknüpfung und Vererbung

Ein Gruppenrichtlinienobjekt ist verknüpft mit dem Speicherort von Objekten, auf die es sich auswirken soll. Diese Speicherorte sind zwar ihrerseits auch Objekte, auf diese hat das GPO aber keine Wirkung. Es kann mit einem Standort, einer Domäne oder einer Organisationseinheit verknüpft sein. Gruppenrichtlinienobjekte werden standardmäßig vererbt.

Je nach Organisationsform des Netzwerks entsteht die Verknüpfung von GPO mit dem Objekt automatisch oder muss explizit erzeugt werden. In jedem Fall kann ein einmal erstelltes GPO auch mit einem weiteren Objekt verknüpft werden.

## 20.3 Verarbeitung der Gruppenrichtlinieneinstellungen

### Reihenfolge bei Verarbeitung von Gruppenrichtlinien

| | |
|---|---|
| Der Computer startet. | |
| **1. Lokale Gruppenrichtlinie** | Auf Computern ab Windows 2000 gibt es ein lokal gespeichertes GPO. Dieses wird abgearbeitet. |
| **2. Startskripts** | Existiert eines oder mehrere Startskripts, wird es/werden sie ausgeführt. Sind mehrere Startskripts vorhanden, werden sie standardmäßig synchron abgearbeitet, d. h., immer erst eins fertig, dann das nächste. |
| **2. Liste der GPOs** | Aus allen GPOs, die diesen Computer betreffen, wird eine Liste erstellt. Die Abarbeitung der GPOs erfolgt standardmäßig synchron in der Reihenfolge:<br>1. GPO für lokalen Computer<br>2. GPO von Standort<br>3. GPO von Domäne<br>4. GPOs von Organisationseinheiten gemäß der vorliegenden Hierarchie |
| Der Anmeldedialog erscheint, der Benutzer meldet sich an. | |
| **3. Benutzerprofil** | Das Benutzerprofil wird geladen. |
| **4. Liste der GPOs** | Aus allen GPOs, die diesen Benutzer betreffen, wird eine Liste erstellt. Die Abarbeitung der GPOs erfolgt standardmäßig synchron in der Reihenfolge:<br>1. GPO für lokalen Computer<br>2. GPO von Standort<br>3. GPO von Domäne<br>4. GPOs von Organisationseinheiten gemäß der vorliegenden Hierarchie |
| **Anmeldeskripts** | Vorhandene Anmeldeskripts werden abgearbeitet. Sind mehrere Anmeldeskripts für den Benutzer gültig, werden sie standardmäßig nacheinander abgearbeitet. |
| Die Benutzeroberfläche erscheint. | |


Schulversion
© HERDT-Verlag

Durch Gruppenrichtlinieneinstellungen können Sie auf die synchrone und asynchrone Verarbeitung von Gruppenrichtlinien und Skripts Einfluss nehmen. Sie haben die Wahl, Skripte parallel oder seriell ausführen zu lassen oder den Desktop bzw. einen Anmeldedialog schon zuzulassen, bevor sämtliche Skripte abgearbeitet wurden. Damit können Sie die Zeit, die das System braucht, um den Anmeldedialog oder den Desktop anzeigt, beeinflussen. Dies kann aber auch verwirrend sein, wenn z. B. Netzlaufwerke erst verbunden werden, nachdem der Benutzer schon auf die grafische Oberfläche zugreift.

### Mehrfachkonfiguration mit Gruppenrichtlinien

Manche Gruppenrichtlinien wirken sich sowohl auf den Computer als auch auf den Benutzer aus. Von der Konfigurationsanweisung *Das Symbol der Netzwerkumgebung nicht anzeigen* ist nicht nur der Computer, sondern auch der Benutzer betroffen.

Bisweilen existieren Gruppenrichtlinien, die auf denselben Sachverhalt abzielen (aber mit entgegengesetzten Wirkungen). Eine gesetzte Konfiguration wird dann durch eine Gruppenrichtlinie, die später ausgeführt wird, überschrieben.

Gruppenrichtlinien und Skripts werden in einer festgelegten Reihenfolge abgearbeitet. Sie müssen die Reihenfolge der Richtlinienverarbeitung kennen, um die gewünschten Konfigurationen auch wirklich zu erzielen.

### Verarbeitungsreihenfolge bei mehreren Gruppenrichtlinien

Haben Sie mehrere GPOs mit einem Standort, einer Domäne oder einer OU verknüpft, werden sie in der Reihenfolge abgearbeitet, wie sie in der Liste erscheinen. Dabei wird zuerst das unterste und zuletzt das oberste GPO abgearbeitet.

### Aktualisierung von Gruppenrichtlinieneinstellungen

Konfigurationen, die durch Gruppenrichtlinien gesetzt werden, werden regelmäßig im Hintergrund aktualisiert. Das Intervall beträgt für Client-Computer ca. 90 Minuten, bei Domänencontrollern etwa 5 Minuten. Eine Ausnahme bei der Aktualisierung bildet unter anderem die Ordnerumleitung. Die Ordnerumleitungsrichtlinie wird nur bei der Benutzeranmeldung umgesetzt und gilt dann, bis der Benutzer sich abmeldet. Die neue Ordnerumleitungsrichtlinie wird erst wirksam, wenn sich der Benutzer erneut anmeldet.

## 20.4 Gruppenrichtlinienberechtigungen

### Berechtigungen bei Einsatz von Gruppenrichtlinien

Damit ein GPO für die Benutzer und die Computer wirksam wird, müssen diese folgende Berechtigungen auf das GPO innehaben:

- Lesen
- Gruppenrichtlinie übernehmen

### Anwendung von Gruppenrichtlinien auf Benutzergruppen

Die kleinste Einheit, die mit einem GPO verknüpft werden kann, ist die OU. Möchten Sie, dass ein GPO nicht für alle Benutzer einer OU, sondern nur für bestimmte Benutzer gültig sein soll, erstellen Sie eine Sicherheitsgruppe. Anschließend können Sie dieser Sicherheitsgruppe die Berechtigungen zum Lesen und Übernehmen des Gruppenrichtlinienobjekts zuweisen.

### Richtlinienbearbeitung in GPOs delegieren

Sie können die Verwaltung von GPOs delegieren. Nur Domänenadministratoren sind zur Delegierung ermächtigt. Die Person oder die Gruppe, die GPOs verwalten soll, benötigt das Schreibrecht auf das GPO.

## 20.5 Vererbung von Gruppenrichtlinien

### Standardmäßige Vererbung

Gruppenrichtlinien werden innerhalb der Domäne standardmäßig vererbt. Eine Gruppenrichtlinie, die Sie mit einer Domäne verknüpft haben, wird an alle Organisationseinheiten der Domäne vererbt.

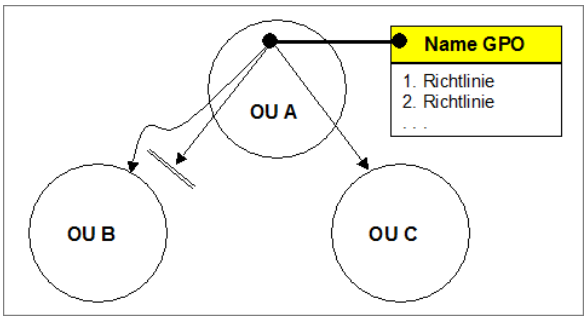
**Reihenfolge der Vererbung**

1. GPOs des Standorts
2. GPOs der Domäne
3. GPOs der OU gemäß der Hierarchie

Eine Sonderstellung bilden die Gruppenrichtlinien, die Sie mit einem Standort verknüpfen. Sie gelten für alle Computer am Standort. Das GPO selbst jedoch wird nur in einer Domäne gespeichert.

Für den Benutzer sind die Richtlinien der OU, zu der er gehört, in jedem Fall wirksam. Sie überschreiben nämlich solche Konfigurationen, die weiter oben in der Hierarchie möglicherweise gesetzt wurden, sofern sie sich auf denselben Sachverhalt beziehen.

Die standardmäßige Vererbung von Richtlinien funktioniert nur, wenn die Einstellungen für die übergeordnete OU und der untergeordneten OU zueinander kompatibel sind. Widersprechen sich die Richtlinien, wird die Richtlinie der übergeordneten OU außer Kraft gesetzt, und es wird nur die Richtlinie der untergeordneten OU wirksam.




*Auswirkung von „Erzwingen“*

### Unternehmensweit geltende Regeln

Um zu verhindern, dass GPOs untergeordneter OUs ein GPO überschreiben oder die Erbschaft dieses GPOs von den Untergeordneten ausgeschlagen wird, verwenden Sie die Option *Erzwingen*. Damit erzwingen Sie die Gültigkeit einer Richtlinie beispielsweise unternehmensweit.

### Vererbung deaktivieren

Sie können auf einer bestimmten Stufe festlegen, dass Richtlinien, die von oben herab vererbt werden könnten, in dieser OU nicht gültig sein sollen.

Sie können allerdings keine GPOs außer Kraft setzen, die mit der Option *Erzwingen* unternehmensweit durchgesetzt werden sollen.


Schulversion
© HERDT-Verlag

# 21 Sicherheitsrichtlinien einsetzen

**In diesem Kapitel erfahren Sie**

- wie Sie die Sicherheitsrichtlinien für Domänencontroller bearbeiten
- wie Sie die Domänenrichtlinien bearbeiten
- wie Sie Richtlinien für Benutzeranmeldungen setzen, um die Sicherheit Ihrer Domäne zu erhöhen
- wie Sie den Benutzerzugriff auf lokale Laufwerke von Arbeitsstationen mit Richtlinien unterbinden

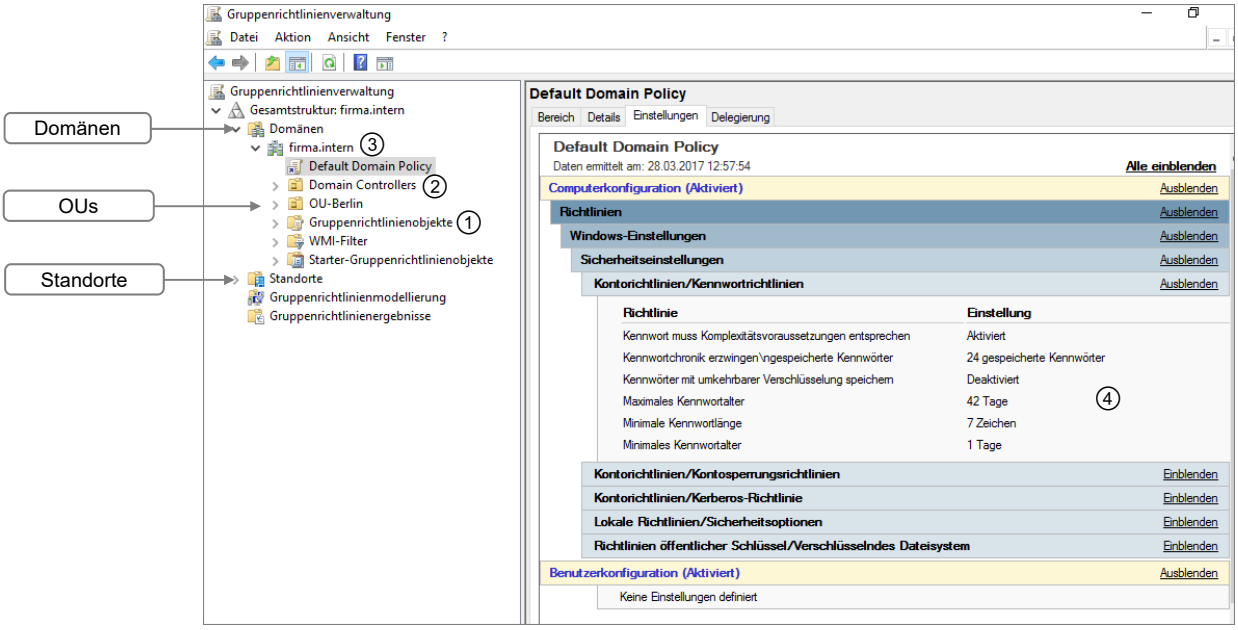
**Voraussetzungen**

- Gruppen verwalten
- Gruppenrichtlinien

## 21.1 Gruppenrichtlinienverwaltung

### Verwaltungswerkzeug

Gruppenrichtlinien verwalten Sie mit der Gruppenrichtlinienverwaltung, die Sie über die Eingabe von `gruppe` im Startbildschirm aufrufen können. Alternativ können Sie dort auch `gpmc.msc` eingeben, denn es handelt sich um die Gruppenrichtlinien-Verwaltungskonsole GPMC (Group Policy Management Console). Das Feature wird auf Domänencontrollern automatisch installiert, auf anderen Rechnern können Sie es hinzufügen.




Die vorhandenen Gruppenrichtlinienobjekte sehen Sie unter ①. In einer neuen Domäne existieren nur zwei GPOs: Die *Default Domain Controllers Policy* ist verknüpft mit der OU *Domain Controllers* ② und die *Default Domain Policy* ist verknüpft mit der Domäne ③. Markieren Sie ein (verknüpftes) GPO, können Sie sich im Register *Einstellungen* ansehen, welche Einstellungen darin gesetzt sind. Über einen Rechtsklick in die Anzeige können Sie diese Ausgabe als Bericht speichern.

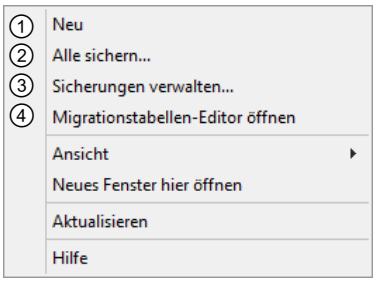
In den anderen Registern nehmen Sie grundsätzliche Einstellungen für das jeweilige Gruppenrichtlinienobjekt vor. In ④ sehen Sie, welche Kennwortrichtlinien standardmäßig in einer neuen Domäne gesetzt sind.

## Einfache Verwaltungsaufgaben

Ihre AD-Standorte sehen Sie erst nach einem Rechtsklick auf den Knoten *Standorte* und der Auswahl *Standorte anzeigen* im Kontextmenü. Dann können Sie angeben, welche Standorte anzuzeigen sind.

Über einen Rechtsklick auf den Knoten *Gruppenrichtlinienobjekte* können Sie die folgenden Aufgaben erledigen:

| | |
|---|---|
| ① | Neue GPOs erstellen: Hier wird immer *Neues Gruppenrichtlinienobjekt* als Name vorgeschlagen. Eindeutige Namen sind nicht notwendig, erleichtern aber die Verwaltung ungemein. |
| ② | Alle GPOs sichern: Den Speicherort müssen Sie angeben. Das ist auch deshalb praktisch, weil Sie diesen Ordner kopieren und beispielsweise in einer Testumgebung wieder importieren können. |
| ③ | Sicherungen wiederherstellen: Nach Angabe des Sicherungsordners werden alle darin enthaltenen GPOs angezeigt. Einzelne Gruppenrichtlinienobjekte können Sie dort auswählen und wiederherstellen. |
| ④ | Migrationstabellen sind keine ganz einfache Verwaltungsaufgabe. Sie können benutzt werden, um beim Import von Gruppenrichtlinienobjekten vorhandene Werte durch andere zu ersetzen. Das ist in der Regel notwendig, wenn GPOs in einer Domäne exportiert und dann in einer anderen importiert werden. Grundsätzlich legen Sie in den Zeilen einer Migrationstabelle jeweils den Quelltyp fest (z. B. Benutzer, Computer, UNC-Pfad) und geben dafür den alten und den neuen Wert an. Beim Import des Gruppenrichtlinienobjekts geben Sie dann die zu verwendende Migrationstabelle an. Genaue Informationen dazu finden Sie beispielsweise unter *http://technet.microsoft.com*. |




*Gruppenrichtlinienobjekte - Kontextmenü*

## Einstellungen für Gruppenrichtlinienverknüpfungen

Sie können eine Reihe von Einstellungen für jede Gruppenrichtlinienverknüpfung vornehmen. Die folgende Tabelle gibt darüber Aufschluss, was die einzelnen Einstellungen bewirken und welche Informationen Sie erhalten.

| Einstellung oder Information | Bedeutung |
|---|---|
| ***Verknüpfungsreihenfolge*** | Die Richtlinien werden in der umgekehrten Reihenfolge (von unten nach oben) abgearbeitet. Die oben stehende Richtlinie überschreibt vorherige Einstellungen durch weiter unten stehende Richtlinien. |
| ***Erzwungen*** | Einstellungen, die in einer erzwungenen Gruppenrichtlinie vorgenommen wurden, können von später verarbeiteten Richtlinien nicht überschrieben werden. |
| ***Verknüpfung aktiviert*** | Nur aktivierte Verknüpfungen haben auch Auswirkungen auf die Objekte. Werden sie deaktiviert, so werden sie zugleich nicht mehr vererbt. |
| ***Objektstatus*** | GPOs können aktiviert sein, oder es können die Bereiche Computerkonfiguration oder Benutzerkonfiguration deaktiviert sein. Dies wird jedoch nicht durch die Verknüpfung bestimmt, sondern muss am Gruppenrichtlinienobjekt eingestellt werden. |
| ***WMI-Filter*** | WMI-Filter können die Anwendung von Richtlinien beeinflussen. Wenn diese mit einer GPO verknüpft sind, werden Sie hier informiert. |
| ***Geändert*** | Wann wurde die GPO zuletzt geändert? |
| ***Domäne*** | In welcher Domäne wurde die GPO erstellt? |


Schulversion
© HERDT-Verlag

## 21.2 Sicherheitsrichtlinien für Domänencontroller bearbeiten

### Aufgabenstellung

Für Tests in der Testumgebung sollen Benutzeranmeldungen an Domänencontrollern ermöglicht werden. Sie hatten dies in vorangegangenen Übungen bereits durch vorübergehendes Hinzufügen der globalen Gruppe *GG-B-Anmeldung_DC* zur Gruppe der Server-Operatoren erreicht. Damit waren allerdings neben der Anmeldung am Domänencontroller weitere eigentlich unerwünschte Rechte verknüpft. Dies können Sie durch eine gezielte Änderung der Sicherheitsrichtlinien für Domänencontroller verhindern. Die Anforderung lautet: eine lokale Anmeldung für die lokale Gruppe *LG-B-DCLogon* zulassen.

### Lokale Gruppe erzeugen

- Sie sind als Administrator angemeldet.
- Öffnen Sie *Active Directory-Benutzer und -Computer*.
- Erweitern Sie den Container *User*.
- Erzeugen Sie eine neue lokale Sicherheitsgruppe mit dem Namen *LG-B-DCLogon*.

### Gruppenmitgliedschaften bearbeiten

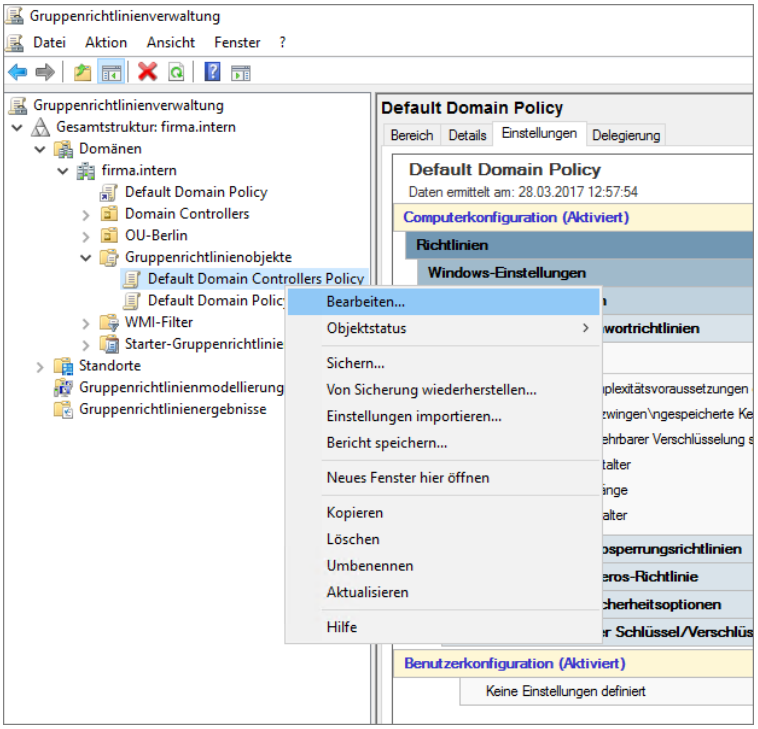
- Machen Sie die globale Gruppe *GG-B-Anmeldung_DC* zum Mitglied in der lokalen Gruppe *LG-B-DCLogon*.
- Entfernen Sie jetzt *GG-B-Anmeldung_DC* aus der lokalen Gruppe *Server-Operatoren*.
- Machen Sie die globale Gruppe *Domänenbenutzer* zum Mitglied in der globalen Gruppe *GG-B-Anmeldung_DC*.

  Können Sie begründen, warum hier eine Konstellation aus zwei Gruppen verwendet wird?
- Veranlassen Sie die Active Directory-Replikation.

### Richtlinie implementieren

- Öffnen Sie die *Gruppenrichtlinien-verwaltung*, indem Sie im Startmenü nach „gpmc.msc“ suchen.
- Erweitern Sie *Gesamtstruktur: firma.intern - Domänen - firma.intern - Gruppenrichtlinien-objekte*.
- Klicken Sie mit der rechten Maus-taste auf *Default Domain Controllers Policy* und wählen Sie *Bearbeiten*.

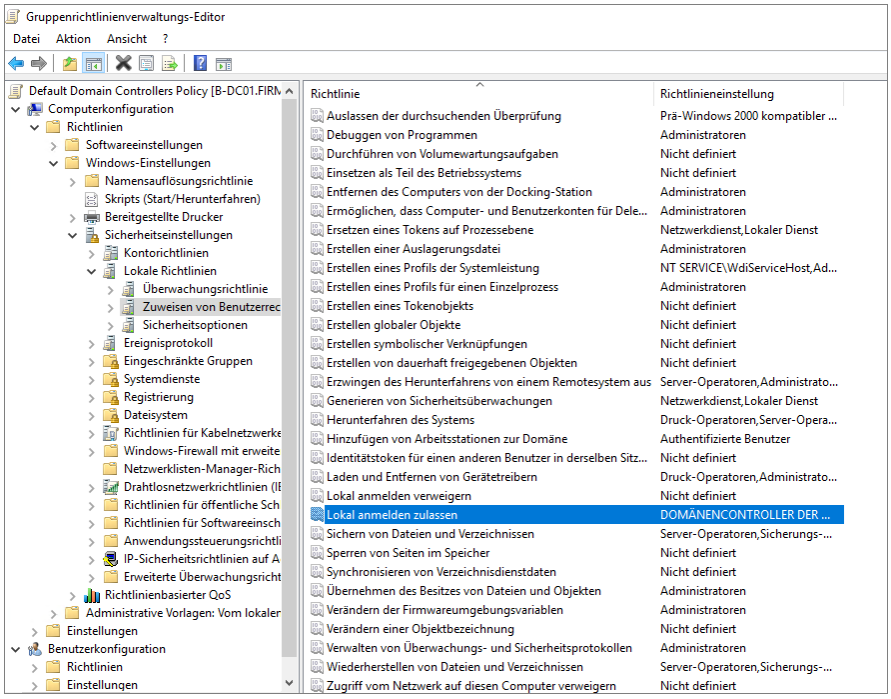
Daraufhin öffnet sich der Gruppenricht-linienverwaltungs-Editor, mit dem Sie die jeweiligen Gruppenrichtlinien verändern und verwalten können.




*Die Gruppenrichtlinienverwaltung GPMC.MSC*

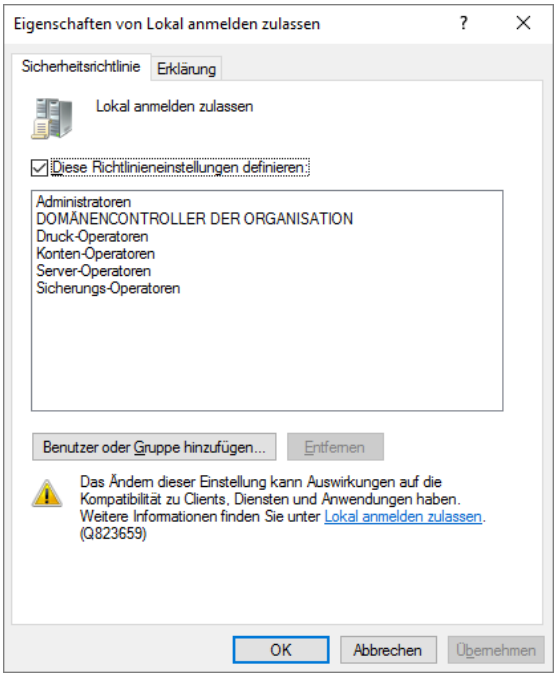
## Richtlinie ändern im Gruppenrichtlininenverwaltungs-Editor

- Erweitern Sie *Computerkonfiguration - Richtlinien - Windows-Einstellungen - Sicherheitseinstellungen - Lokale Richtlinien - Zuweisen von Benutzerrechten*.
- Klicken Sie doppelt auf die Richtlinie *Lokal anmelden zulassen*.




*Auswahl einer Richtlinieneinstellung in Gruppenrichtlinien*

- Klicken Sie im Dialogfenster *Eigenschaften von Lokal anmelden zulassen* auf die Schaltfläche *Benutzer oder Gruppe hinzufügen*.
- Fügen Sie die lokale Gruppe *LG-B-DCLogon* hinzu.
- Übernehmen Sie die Änderung.
- Aktualisieren Sie die Gruppenrichtlinieneinstellung, indem Sie in einer Eingabeaufforderung den Befehl `gpupdate` eingeben.




*Gruppe LG-B-DCLogon hinzufügen*

Dieses Richtlinienobjekt wird beim Heraufstufen eines Servers unter Windows Server 2019 zum Domänencontroller erzeugt. Es erhält den *Namen Default Domain Controllers Policy*, wird mit Standardrichtlinieneinstellungen versehen und mit dem Container *Domain Controllers* verknüpft.

Wenn Sie eine Änderung an den Sicherheitseinstellungen für Domänencontroller durchführen wollen, ist es sinnvoll, diese an der Standardrichtlinie vorzunehmen. Andere Einstellungen sollten Sie jedoch in eigenen Richtlinien verwalten, da sonst die Übersicht verloren gehen kann.

## Richtlinie testen

- Melden Sie sich mit dem Benutzerkonto von *ABaumann* an.

  Ist die Anmeldung erfolgreich?


Schulversion
© HERDT-Verlag

## 21.3 Domänenrichtlinien bearbeiten

### Einleitung

Standardmäßig gelten in einer Domäne unter Windows Server 2019 strenge Kennwortrichtlinien.

Seit Windows Server 2008 können in einer Domäne zusätzliche Kennwortrichtlinien erstellt werden. Diese werden dann allerdings nicht über Gruppenrichtlinien verwaltet. Die Erstellung einer zusätzlichen Kennwort-einstellungsobjektes (Password Settings Object, PSO) bildet den Abschluss dieses Kapitels.

### Aufgabenstellung

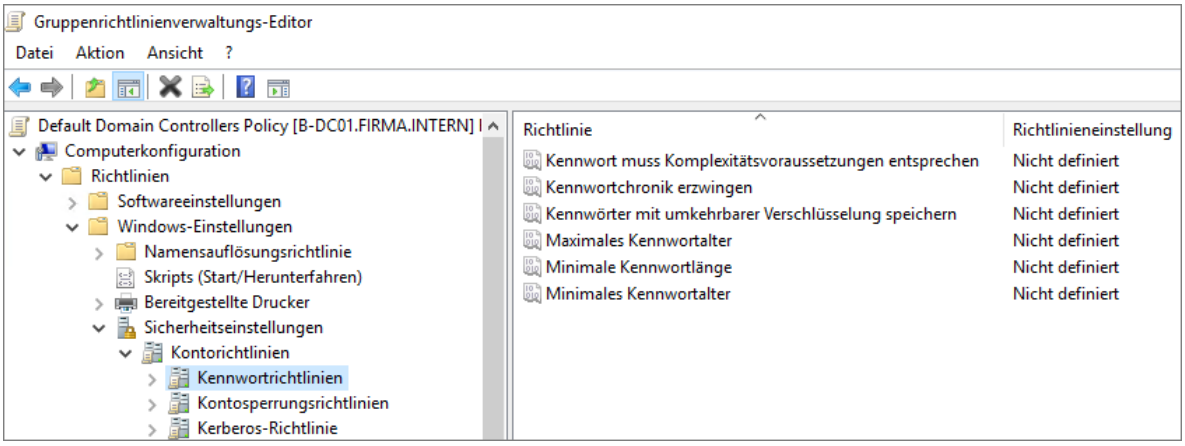
In der Domäne sollen angepasste Sicherheitsrichtlinien durchgesetzt werden:

- Die Kennwörter müssen mindestens 8 Zeichen lang sein.
- Nach 3 ungültigen Anmeldeversuchen soll das betroffene Benutzerkonto gesperrt werden.
- Der Benutzername der vorherigen Anmeldung soll im Anmeldedialog nicht angezeigt werden.
- Benutzer dürfen die lokalen Datenträger ihrer Arbeitsstationen nicht verwenden.
- Benutzer dürfen keine Wechseldatenträger wie z. B. USB-Sticks verwenden.

### Domänenrichtlinien bearbeiten

- Sie sind als Domänenadministrator angemeldet.
- Öffnen Sie die Gruppenrichtlinienverwaltung GPMC.msc.
- Erweitern Sie *Gesamtstruktur: firma.intern - Domänen - firma.intern*.
- Klicken Sie mit der rechten Maustaste auf die Verknüpfung *Default Domain Policy* und wählen Sie *Bearbeiten*.

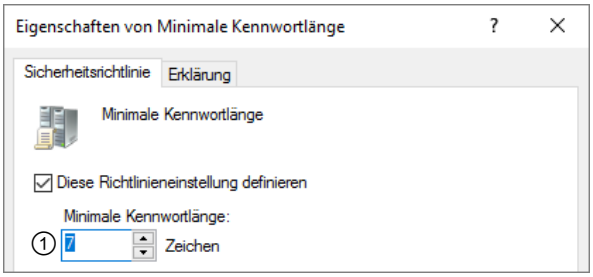
  Es öffnet sich der Gruppenrichtlinienverwaltungs-Editor zur Richtlinie.




*Domänenrichtlinien bearbeiten*

### Kontorichtlinien bearbeiten

- Erweitern Sie unter *Computerkonfiguration* die Struktur *Richtlinien - Windows-Einstellungen - Sicherheitseinstellungen - Kontorichtlinien*.
- Klicken Sie auf *Kennwortrichtlinien*.
- Vergewissern Sie sich, dass die Richtlinie *Kennwort muss Komplexitätsvoraussetzungen entsprechen* aktiviert ist.




*Kennwortlänge definieren*

- Um die Mindestlänge für Kennwörter festzulegen, klicken Sie doppelt auf die Richtlinie *Minimale Kennwortlänge* und geben Sie den gewünschten Wert ein (8) ①.

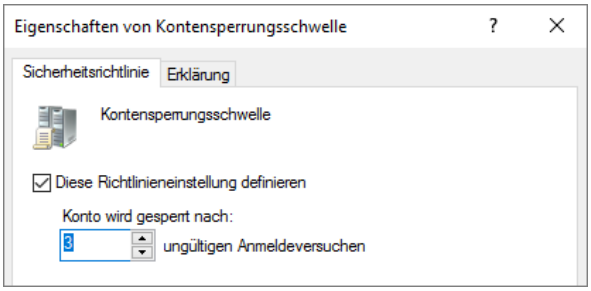
Das maximale Alter von Kennwörtern soll verhindern, dass Kennwörter, die mittels Angriffswerkzeugen entschlüsselt wurden, noch gültig sind.

Mit der Kennwortchronik wird verhindert, dass ein Benutzer nur zwischen wenigen Kennwörtern wechselt.

Das minimale Kennwortalter verhindert, dass Benutzer ihr Kennwort durch mehrfaches sofortiges Ändern auf das Ursprungskennwort zurücksetzen.

## Kontosperrungsrichtlinien bearbeiten

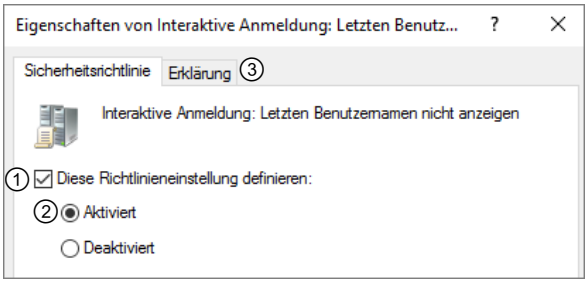
- Klicken Sie auf *Kontosperrungsrichtlinien*.
- Öffnen Sie die Richtlinie *Kontosperrungsschwelle*.
- Definieren Sie die Richtlinie und setzen Sie einen Wert von 3 ungültigen Anmeldeversuchen fest, bevor das Konto gesperrt wird.
- Windows setzt für die übrigen Kontosperrungsrichtlinien neue Zeitintervalle mit Standardwerten fest.




*Kontosperrungsschwelle bearbeiten*

## Richtlinie *Interaktive Anmeldung* bearbeiten

- Um die Richtlinie für den Anmeldedialog zu implementieren, erweitern Sie unter *Computerkonfiguration* die Struktur *Lokale Richtlinien - Sicherheitsoptionen.*
- Öffnen Sie die Richtlinie *Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen*.
- Die Richtlinie ist standardmäßig nicht definiert. Schalten Sie zunächst das Kontrollfeld ① ein.
- Diese Richtlinie ist standardmäßig deaktiviert. Aktivieren Sie die Option ②.




*Anzeige des letzten Benutzers ausblenden*

Um zu ermitteln, ob Sie die Richtlinie aktivieren oder deaktivieren müssen, um die gewünschte Einstellung zu erhalten, müssen Sie immer die Konfigurationsanweisung ③ genau berücksichtigen.

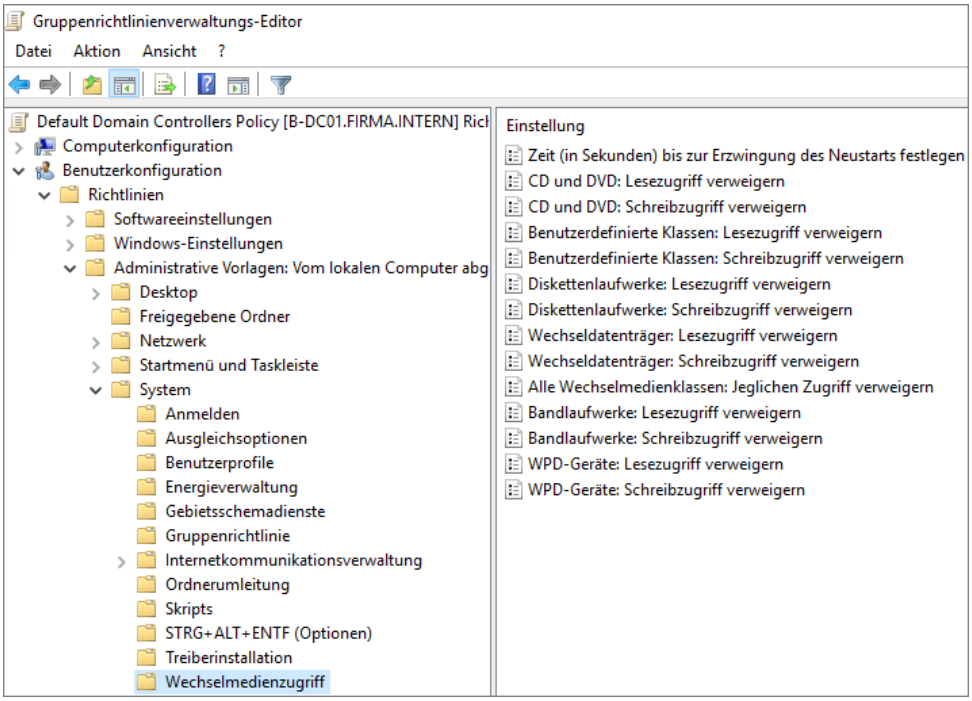
## Zugriff auf Wechseldatenträger und mobile Geräte beschränken

Die folgende Einstellung sollten Sie in der Praxis nicht auf der Domänenrichtlinie vornehmen, sonst wären alle Konten der Domäne davon betroffen. Erstellen Sie stattdessen eine eigene Richtlinie für die Einstellung, die Sie z. B. *GPO-Laufwerkssperrung* nennen könnten.

Heutzutage gibt es zahlreiche verschiedene Wechseldatenträger von Flash-Speicherkarten zu USB-Sticks zu externen Festplatten. Dazu kommen portable Medienplayer, Smartphones und optische Medien. Möglicherweise werden sogar noch Disketten verwendet. Um die Verwendung solcher Wechseldatenträger zu steuern, gibt es eine ganze Reihe von GPOs. Diese sollen z. B. verhindern, dass Benutzer Viren in das Firmennetz einschleppen oder Firmendaten kopieren und aus der Firma entfernen.

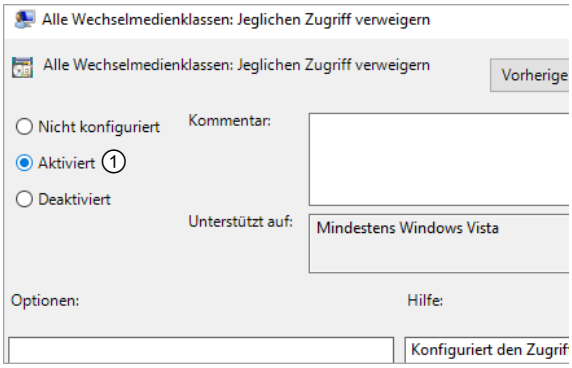
- Erweitern Sie unter *Benutzerkonfiguration* die Struktur *Richtlinien - Administrative Vorlagen - System - Wechselmedienzugriff*.


Schulversion
© HERDT-Verlag




*Zugriff auf Wechselmedien einschränken*

- Klicken Sie doppelt auf die Richtlinie *Alle Wechselmedien: Jeglichen Zugriff verweigern*, um alle Wechselmedien und externen Datenträger zu sperren. Diese Richtlinie hat Vorrang vor allen weiteren Richtlinien zu den einzelnen Geräteklassen.
- Aktivieren Sie im Einstellungsdialog die Richtlinie mit der Option ① und klicken Sie auf *Übernehmen* und dann auf *OK*.




Sie haben nun den Zugriff auf alle Arten von Wechseldatenträgern unterbunden. Wenn Sie nur bestimmte Typen sperren wollen, müssen Sie diese Richtlinie deaktivieren, bevor Sie eine der untergeordneten Richtlinien einsetzen.

## Speichern von Dateien auf lokalen Volumes unterbinden

Sie können den Zugriff auf bestimmte Laufwerksbuchstaben einschränken. Die Laufwerke werden dann zwar noch im Explorer angezeigt, aber es können keine Ordner oder Dateien darauf geöffnet werden. Diese Richtlinie soll z. B. verhindern, dass Benutzer auf der Systempartition Dateien ablegen oder löschen.

- Erweitern Sie unter *Benutzerkonfiguration* die Struktur *Richtlinien - Administrative Vorlagen - Windows-Komponenten - Datei-Explorer*.
- Klicken Sie doppelt auf die Richtlinie *Zugriff auf Laufwerke vom Arbeitsplatz nicht zulassen*.
- Aktivieren Sie die Richtlinie.
- Wählen Sie im Listenfeld die *Alle Laufwerke einschränken*.

## Aufgabe

- Beenden Sie die Bearbeitung von Richtlinien.
- Veranlassen Sie die Aktualisierung der Richtlinie mit `gpupdate` und führen Sie eine Active Directory-Replikation durch.
- Melden Sie sich ab.

## Wirkung der Domänenrichtlinien testen

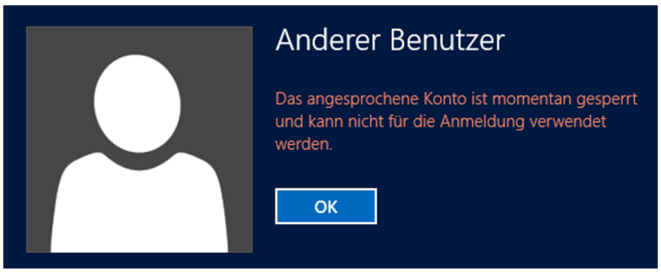
### Anmeldung und Kennwort

- Melden Sie sich mit dem Benutzerkonto von *ABaumann* an.
- Ändern Sie das Kennwort. Betätigen Sie hierzu Strg Alt Entf. Versuchen Sie, als neues Kennwort *xy* zu verwenden.
- Ändern Sie das Kennwort in *geheim&88* und versuchen Sie es erneut.

*Ein Kennwort entspricht nicht den Richtlinien*

### Kontosperrung

- Melden Sie sich ab.
- Verwenden Sie für eine neue Anmeldung mehrfach ein falsches Kennwort für *ABaumann*.




*Konto wurde gesperrt*

### Zugriff auf lokale Laufwerke

- Verknüpfen Sie die Richtlinie *GPO-Laufwerkssperrung* mit einer Test-OU, verschieben Sie einen Benutzer in diese Test-OU und melden Sie sich unter Verwendung des Kontos an.
- Öffnen Sie den Windows-Explorer und klicken Sie doppelt auf das Laufwerk A:.
- Testen Sie, ob Sie auf das DVD-Laufwerk zugreifen können. Binden Sie dazu in der virtuellen Umgebung z. B. das Windows-ISO-Abbild ein.

## Einstellungen für Testumgebung wieder lockern

In der Testumgebung würden die aktuellen Domänenrichtlinien Ihre Handlungsmöglichkeiten für weitere Tests und Übungen beschränken. Deshalb sollen sie wieder außer Kraft gesetzt werden.

Die Domänenrichtlinien lassen sich nicht deaktivieren. Sie sind immer wirksam.

- Melden Sie sich als Administrator an.
- Bearbeiten Sie die Richtlinien der Domäne wie beschrieben, um die unten aufgeführten Einstellungen für die geänderten Richtlinien zu erreichen.
- Veranlassen Sie die Aktualisierung und eine Active Directory-Replizierung.
- Heben Sie in den Eigenschaften des Kontos von *ABaumann* die Sperrung wieder auf.

Beachten Sie, dass mit der Einstellung *nicht definiert* der Registrierungsschlüssel nicht überschrieben wird. Zur Wiederherstellung der Ursprungseinstellungen genügt es nicht, die Richtlinie auf *nicht definiert* zu setzen!

| Kategorie | Richtlinieneinstellung |
|---|---|
| **Komplexitätsvoraussetzungen** | Deaktiviert |
| **Kennwortlänge** | 0 Zeichen |
| **Kontosperrung** | Zahl ungültiger Anmeldeversuche 0 Zeichen. Zeitintervalle für die assoziierten Richtlinien setzt Windows auf Nachfrage zurück. |
| **Anmeldedialog** | Deaktiviert |
| **Zugriffe auf Laufwerke** | Laufwerke nicht einschränken |


Schulversion
© HERDT-Verlag

Beachten Sie, dass diese Einstellungen nicht die maximale Sicherheit bieten, sie sind jedoch im Interesse einer zügigen Bearbeitung von Übungen sinnvoll.

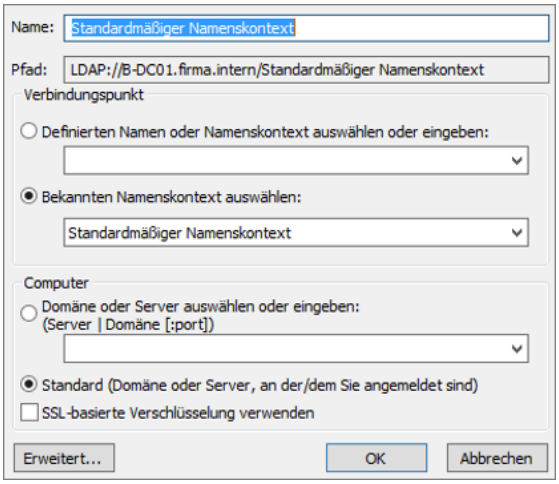
## 21.4 Zusätzliche Kontorichtlinie erstellen

### Password Settings Object (PSO, Kennworteinstellungsobjekt) erstellen

Seit Windows Server 2008 sind mehrere Kontorichtlinien in einer Domäne möglich. Benötigen Sie zusätzliche Kontorichtlinien, können Sie dafür PSOs erstellen und Sicherheitsgruppen zuweisen. Als Werkzeug dafür empfiehlt sich das MMC-Snap-In ADSI-*Editor*. Über das **A**ctive **D**irectory **S**ervice **I**nterfache erhalten Sie Zugriff auf alle Bereiche Ihres AD.

- Öffnen Sie den ADSI-Editor, z. B. durch Eingabe von `adsiedit.msc` in der Eingabeaufforderung oder dem Startmenü.
- Im ADSI-Editor klicken Sie mit der rechten Maustaste auf den Knoten *ADSI-Editor* und wählen im Kontextmenü *Verbindung herstellen*.
- Sollte das erscheinende Fenster anders aussehen als in der Abbildung, stellen Sie die Optionen entsprechend um und tragen Sie den Namen Ihrer Domäne ein, z. B. *firma.intern*.

Damit erhalten Sie Zugriff auf die AD-Objekte, die im angegebenen Kontext enthalten sind.



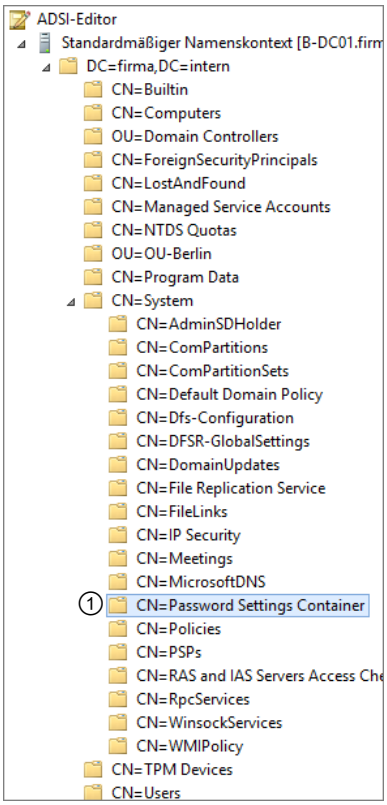

*ADSI-Verbindung erstellen*

- Erweitern Sie *Standardmäßiger Namenskontext - DC=firma, DC=intern - CN=System* und markieren Sie *CN=Password Settings Container* ①.
- Nach einem Rechtsklick auf den Password Settings Container wählen Sie im Kontextmenü *Neu - Objekt*.

Der Assistent zum Erstellen eines neuen PSO wird geöffnet, der Sie durch die Objekterstellung führt.

- Auf der ersten Seite können Sie die Objektklasse auswählen. Klicken Sie auf *Weiter*.
- Vergeben Sie dann einen Namen für das neue PSO, z. B. *PSO-Kennwort*, und klicken Sie auf *Weiter*.
- Im nächsten Fenster legen Sie einen Precedence-Wert für dieses PSO fest, z. B. *20*.

Erstellen Sie mehrere PSOs, müssen in diesem Feld unterschiedliche Zahlen stehen. Ist ein Benutzer Mitglied in mehreren Gruppen, denen unterschiedliche PSOs zugewiesen sind, wird auf den Benutzer das PSO mit dem kleinsten Precedence-Wert angewandt. Dementsprechend sollte ihr härtestes PSO den kleinsten Wert bekommen.




*Password Settings Container*

Auf den folgenden Seiten nehmen Sie dieselben Einstellungen vor wie in der Kontorichtlinie der Default Domain Policy.

- Legen Sie fest, ob das Kennwort mit umkehrbarer Verschlüsselung gespeichert werden soll. In booleschen Feldern geben Sie „true“ oder „false“ ein, hier „false“.
- Legen Sie ebenfalls fest: die Länge der Kennwortchronik, komplexe Kennwörter, die minimale Kennwortlänge, das minimale Kennwortalter – Felder mit der Bezeichnung *Dauer* erfordern die Syntax *TT:HH:MM:SS* (Tage, Stunden, Minuten, Sekunden) –, das maximale Kennwortalter, die Kontosperrungsschwelle, die Zurücksetzungsdauer des Kontosperrungszählers und die Kontosperrungsdauer.

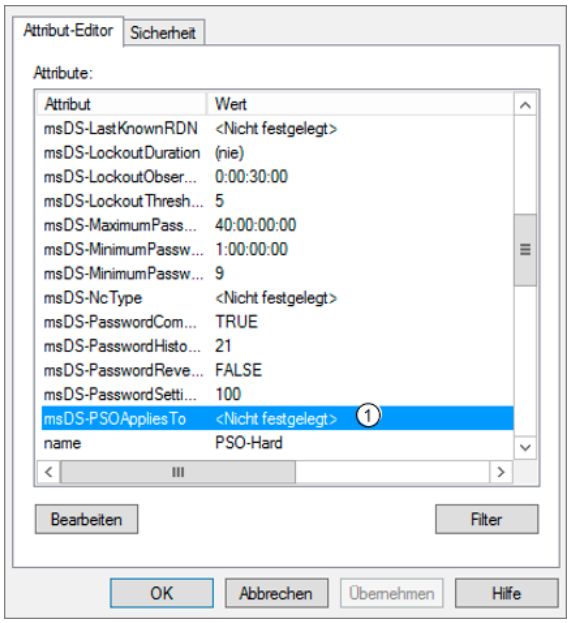
Wenn Sie die Kontosperrdauer auf unendlich (d. h., bis ein Administrator die Sperrung aufhebt) festlegen wollen, müssen Sie `(nie)` einschließlich der Klammer eingeben.

- Auf der letzten Seite können Sie weitere Attribute bearbeiten. Klicken Sie auf *Fertig stellen*.

## Password Settings Object zuweisen

Das Zuweisen von PSOs erfolgt am einfachsten über *Active Direcory-Benutzer und -Computer*.

- Stellen Sie sicher, dass im Menü *Ansicht* die erweiterten Features aktiviert sind.
- Erweitern Sie unterhalb der Domäne den Knoten *System* und klicken Sie auf *Password Settings Container.*
- Klicken Sie mit der rechten Maustaste auf ein PSO, wählen Sie im Kontextmenü *Eigenschaften* und wechseln Sie in das Register *Attribut-Editor*.
- Markieren Sie *msDS-PSOAppliesTo* ① und klicken Sie auf *Bearbeiten*.
- Im folgenden Fenster klicken Sie auf *Windows-Konto hinzufügen*.



*Attribut-Editor für ein PSO*

Fügen Sie hier nur Sicherheitsgruppen hinzu. In diesen Gruppen sollten keine Computerkonten enthalten sein. Für die Mitglieder der Gruppe gelten fortan die Einstellungen des PSO, was sich aber erst beim nächsten Wechsel des Kennworts bemerkbar macht.

Über dasselbe Fenster können Sie die Gruppen auch wieder entfernen.


Schulversion
© HERDT-Verlag

# 22 Gruppenrichtlinien verwalten

**In diesem Kapitel erfahren Sie**

- wie Sie Gruppenrichtlinien planen und erstellen
- wie Sie Gruppenrichtlinien überwachen, testen und verwalten

**Voraussetzungen**

- Konzept der Gruppenrichtlinien
- Sicherheitsrichtlinien

## 22.1 Gruppenrichtlinienimplementierung planen

### Beispielszenario

Das folgende Szenario soll die Problematik der Gruppenrichtlinienplanung erläutern:

Alle Mitarbeiter des Unternehmens müssen einen Bildschirmschoner mit Kennwortschutz verwenden.

In der Vertriebsabteilung soll generell der Zugriff auf lokale Laufwerke beschränkt werden. Die Benutzer sollen ihre Daten stattdessen auf den Netzlaufwerken speichern, die ihnen über Einstellungen aufgrund ihrer Gruppenzugehörigkeiten zugewiesen werden.

*OU-Struktur der Vertriebsabteilung*

Benutzer der Unterabteilung *Werbung* dagegen müssen Plakate gestalten und dazu teilweise sehr große Bilddateien bearbeiten. Da dies bei ausschließlicher Verwendung von Netzlaufwerken zu erheblichen Verzögerungen führen würde, sollen sie auch lokal Daten speichern dürfen.

Eine weitere Abweichung ergibt sich für Vertriebsmitarbeiter, die mobile Geräte einsetzen. Unabhängig von der Unterabteilung oder Gruppenzugehörigkeit müssen diese die lokalen Ressourcen nutzen können, wenn sie an mobilen Geräten angemeldet sind.

### Schritte bei der Planung einer Gruppenrichtlinienimplementierung

#### 1. Schritt

Die Planung einer Gruppenrichtlinienimplementierung beinhaltet das Heraussuchen und die Bewertung von geeigneten Richtlinieneinstellungen, die in ihrer Gesamtheit die gewünschten Ergebnisse erzielen. Oft ist es so, dass ein Ziel, das auf den ersten Blick lapidar erscheint, nur durch das Zusammenwirken mehrerer einzelner Richtlinien effektiv erreicht werden kann.

#### 2. Schritt

Sie müssen dann festlegen, mit welchem Standort oder welcher OU das Gruppenrichtlinienobjekt zu verknüpfen ist und ob das GPO auf untergeordnete Einheiten vererbt werden soll.

#### 3. Schritt

Sie müssen bestimmen, ob die Vererbung von Gruppenrichtlinien in einer OU der Hierarchie auszuschließen ist. Außerdem müssen Sie festlegen, ob die Richtlinieneinstellungen eines GPO mithilfe der Option *Erzwungen* durchgesetzt werden sollen und ob sowohl Computer- als auch Benutzereinstellungen aktiviert sein sollen.

## Ergebnis der Planung

### Bildschirmschoner

Der Einsatz des Bildschirmschoners mit Kennwortschutz muss immer erzwungen werden. Indem die entsprechende Richtlinie auf Domänenebene erstellt und ihre Anwendung erzwungen wird, kann sichergestellt werden, dass diese immer gilt.

### Laufwerke

Die Gruppenrichtlinie mit den Einstellungen zu Laufwerkseinschränkungen und -zuordnungen wird auf die Organisationseinheit *OU-B-Vertrieb* angewendet. Da die Laufwerkszuordnungen auch für Mitarbeiter der Unterabteilung *Werbung* gelten sollen, darf die Vererbung für die *OU-B-Vertrieb-Werbung* nicht deaktiviert werden. Stattdessen muss hier eine zweite Gruppenrichtlinie eingesetzt werden, die die entsprechenden Einschränkungen aktiv aufhebt.

### Problemfall mobile Geräte

Die Analyse zeigt, dass sämtliche Einstellungen, die in den Anforderungen beschrieben wurden, im Bereich Benutzerkonfiguration vorgenommen werden müssen. Die Anforderungen an mobile Geräte richten sich jedoch nach dem Speicherort des Computerobjektes. Es muss also eine Richtlinie angewendet werden, die den Bereich Benutzerkonfiguration in Abhängigkeit vom Speicherort des Computerobjektes erfasst. Dies kann mit dem Loopbackverarbeitungsmodus erfolgen.

## Loopbackverarbeitungsmodus für Benutzergruppenrichtlinie

Der Loopbackverarbeitungsmodus kann die Verarbeitungsreihenfolge von Benutzergruppenrichtlinien verändern.

Entweder ersetzt er die Gruppenrichtlinien des Benutzerobjektes durch jene, die für den Speicherort des Computerobjektes definiert sind (Modus *Ersetzen*), oder er überschreibt die Einstellungen, sodass nur Abweichungen von den normalen Einstellungen des Benutzerobjektes zum Tragen kommen (Modus *Zusammenführen*). Lesen Sie zum besseren Verständnis die folgenden Beispiele:

### Modus *Ersetzen*

In einem Schulungsunternehmen sollen Benutzer während einer Prüfung mit ihrem Benutzernamen angemeldet sein. Dabei dürfen sie nur auf die Prüfungssoftware und den Taschenrechner zugreifen. Außerdem müssen spezielle Anmelde- und Abmeldeskripten verwendet werden und der Rechner darf nicht heruntergefahren werden.

Damit am Prüfungsrechner diese Einstellungen wirksam werden, wird der Loopbackverarbeitungsmodus für Benutzergruppenrichtlinien im Modus Ersetzen aktiviert.

### Modus *Zusammenführen*

Normalerweise dürfen Mitarbeiter der Kundenbetreuung nicht auf die Systemsteuerung zugreifen. Einige Mitarbeiter sollen aber für die Kundenunterstützung weitergebildet werden. Wenn sie sich an einem Übungsrechner anmelden, sollen ihnen hierzu zusätzliche Funktionen bereitstehen.

Für das Beispielszenario bietet sich die Anwendung des Loopbackverarbeitungsmodus für Benutzergruppenrichtlinien im Modus *Zusammenführen* an. Es wird eine weitere Richtlinie definiert, die mit der Organisationseinheit *OU-B-Vertrieb-Mobile_Geräte* verknüpft wird.

## Arbeitsweise

Bevor Sie Gruppenrichtlinien in der Produktivumgebung einsetzen, sollten Sie diese immer in einer Testumgebung prüfen. Ein Fehler in der Richtlinie kann andernfalls das gesamte Netzwerk des Unternehmens gefährden!


Schulversion
© HERDT-Verlag

### Aufgaben

- Planen Sie Gruppenrichtlinien.
- Erstellen sie eine Testumgebung mit vier OUs, Testbenutzern, -gruppen und -computern.
- Erstellen Sie die benötigten Gruppenrichtlinien und verknüpfen Sie diese mit den jeweiligen OUs.
- Nehmen Sie die nötigen Einstellungen in den Gruppenrichtlinien vor.
- Testen Sie die Einstellungen, indem Sie sich mit Testbenutzern auf den unterschiedlichen Testcomputern anmelden.

## 22.2 Test-OU erstellen

### Aufgabenstellung

Um die Wirkung und Funktion der Gruppenrichtlinien zu überprüfen, benötigen Sie eine Hierarchie von Organisationseinheiten. Zwar kann eine komplexe Gruppenrichtlinienstrategie auch durch Filterung von Gruppenrichtlinien erreicht werden, dies bewährt sich aber in der Praxis nicht, da Sie nicht schnell erkennen können, welche Richtlinien für welche Objekte im Active Directory gelten. Sie können die benötigte OU-Struktur erstellen, indem Sie das Snap-In *Gruppenrichtlinienverwaltung* einsetzen. Die Benutzer müssen Sie allerdings mit dem Snap-In *Active Directory-Benutzer und -Computer* erstellen.

### Organisationseinheiten erstellen

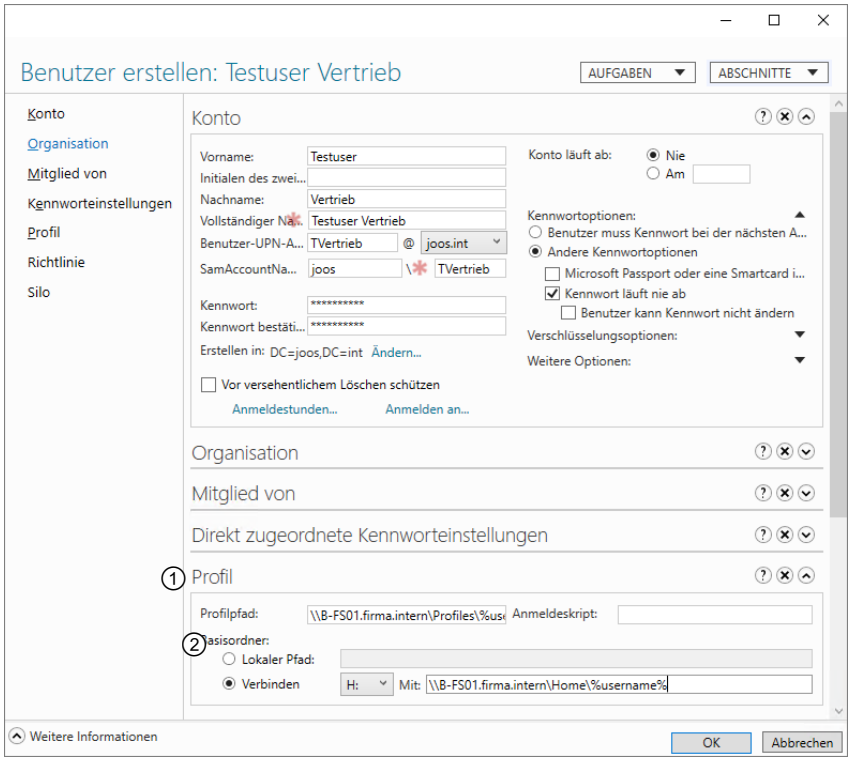
- Erstellen Sie auf einem Dateiserver vier Verzeichnisse namens *Profiles*, *Home*, *Vertrieb* und *Werbung* und geben Sie diese frei.
- Öffnen Sie das Active Directory-Verwaltungscenter und erweitern Sie die Ansicht auf die Domäne *firma.intern*.
- Klicken Sie mit der rechten Maustaste auf die Domäne und wählen Sie den Menüpunkt *Neu - Organisationseinheit*.
- Geben Sie den Namen der Organisationseinheit entsprechend Ihrer Konzeption ein. In der hier beschriebenen virtuellen Umgebung können Sie in der Domäne *firma.intern* neben der *OU-Berlin* eine weitere OU namens *OU-Testumgebung* erstellen, worin Sie dann alle nötigen Test-OUs, Test-Gruppen und Test-Benutzer erstellen. Verwenden Sie sicherheitshalber statt des Standortkürzels B (für Berlin) das Wort „Test“, damit Sie alle beteiligten Objekte jederzeit von den Objekten der Produktivumgebung unterscheiden können.

Die Organisationseinheit *OU-Testumgebung* simuliert im Folgenden die Domäne. Dieser Zusatzschritt ist nötig, da Sie sonst eine domänenweite Richtlinie mit der Domäne verknüpfen müssten.

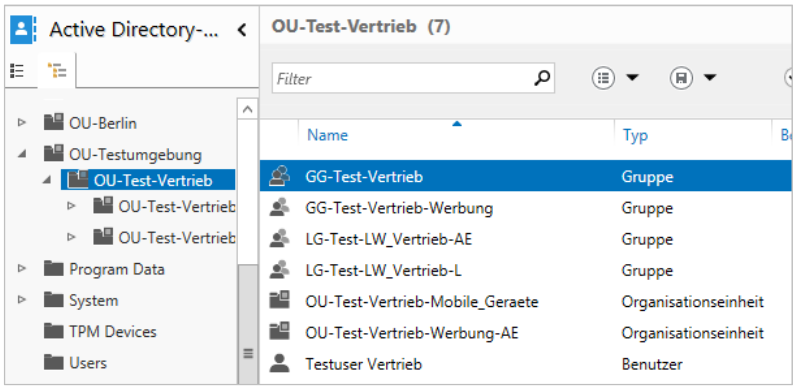
- Bestätigen Sie Ihre Auswahl mit *OK*.
- Verfahren Sie auf der neuen Organisationseinheit identisch, um die untergeordneten Organisationseinheiten zu erstellen.
- Erstellen Sie in diesen nun die benötigten Computer, Gruppen und Benutzer.

Um die korrekte Funktion Ihrer Einstellungen zu überprüfen, müssen Sie sich auch an dem entsprechenden Computer anmelden können. Daher empfiehlt es sich, einen existierenden Computer in die entsprechende OU zu verschieben. In der hier beschriebenen Testumgebung können Sie dafür kurzzeitig den Server *B-FS01* verwenden. Fertigen Sie vor dem Verschieben und Experimentieren einen Snapshot von allen VMs an.

- Konfigurieren Sie für die Benutzerobjekte den Profilpfad ① und den Pfad zum Basisordner ② auf die freigegebenen Ordner im Netzwerk.
- Fügen Sie die Benutzer den jeweiligen globalen Gruppen hinzu.
- Ordnen Sie die globalen Gruppen den jeweiligen lokalen Gruppen für die Freigaben Vertrieb und Werbung zu.
- Konfigurieren Sie die benötigten Freigabe- und NTFS-Berechtigungen auf den zuvor erstellten Freigaben.




*Testbenutzer anlegen*




*Testumgebung vorbereitet*

## 22.3 Gruppenrichtlinien implementieren

### Aufgabenstellung

Zunächst erstellen Sie folgende Gruppenrichtlinienobjekte ohne Verknüpfungen:

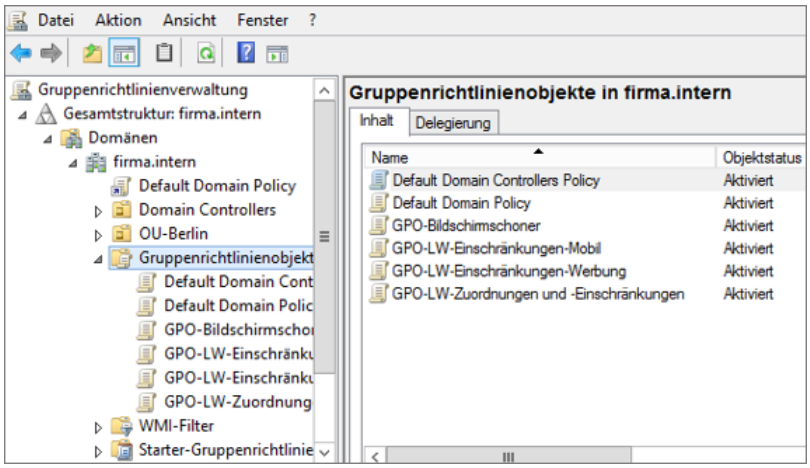
- *GPO-Bildschirmschoner*
- *GPO-LW-Zuordnungen und -Einschränkungen*
- *GPO-LW-Einschränkungen-Werbung*
- *GPO-LW-Einschränkungen-Mobil*

Anschließend nehmen Sie die Einstellungen in den einzelnen GPOs vor. Verknüpfen Sie die Richtlinien mit den Organisationseinheiten.


Schulversion
© HERDT-Verlag

## Aufgabe 1 – Gruppenrichtlinien erstellen

- Öffnen Sie die Gruppenrichtlinienverwaltung und erweitern Sie die Ansicht auf den Ordner *Gruppenrichtlinienobjekte*.
- Klicken Sie mit der rechten Maustaste auf *Gruppenrichtlinienobjekte* und wählen Sie den Menüpunkt *Neu*.
- Geben Sie den Namen der Gruppenrichtlinie entsprechend Ihrer Konzeption ein, in diesem Beispiel *GPO-Bildschirmschoner*.
- Bestätigen Sie Ihre Auswahl mit *OK*.
- Verfahren Sie mit den weiteren GPOs identisch.

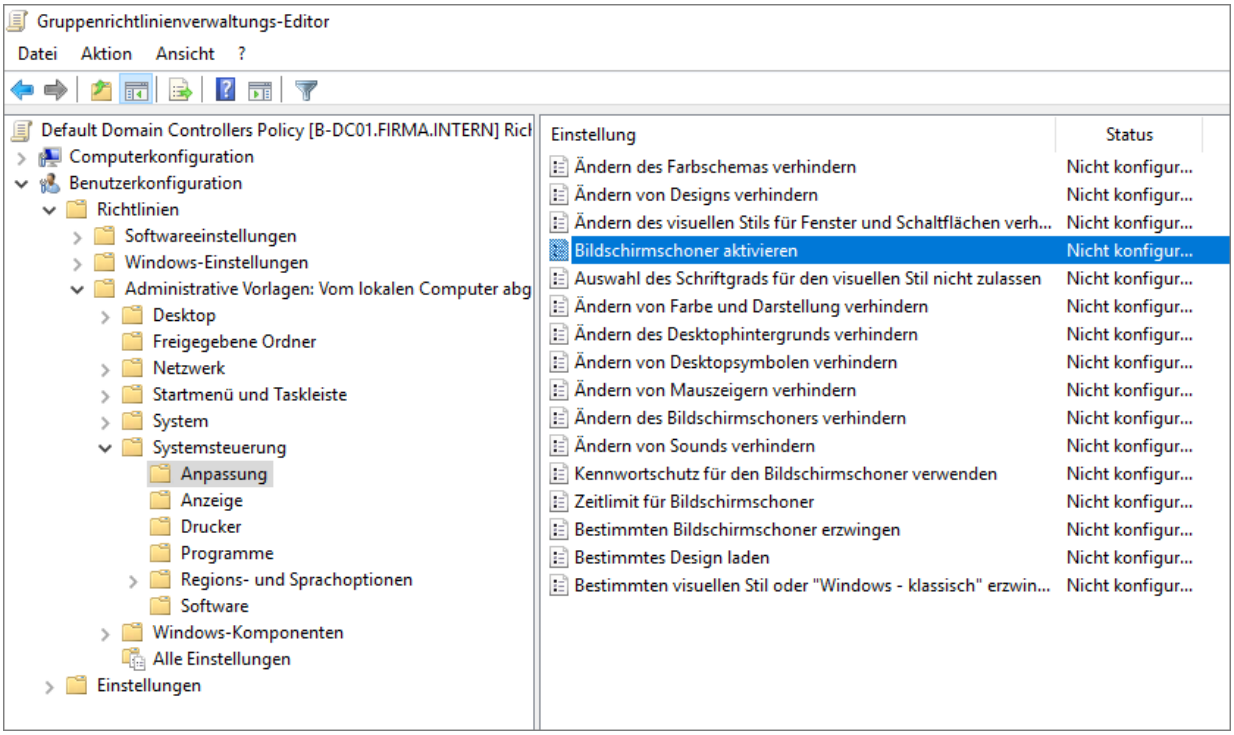



*Gruppenrichtlinien für Testumgebung erstellt*

## Gruppenrichtlinieneinstellungen setzen

Die Gruppenrichtlinieneinstellungen sollen zunächst für *GPO-Bildschirmschoner* vorgenommen werden.

- Klicken Sie mit der rechten Maustaste auf die Gruppenrichtlinie *GPO-Bildschirmschoner* und wählen Sie den Menübefehl *BEARBEITEN*.
- Erweitern Sie unter *Benutzerkonfiguration - Richtlinien- Administrative Vorlagen - Systemsteuerung* den Ordner *Anpassung*.
- Aktivieren Sie die Richtlinie *Bildschirmschoner aktivieren*.
- Aktivieren Sie die Richtlinie *Kennwortschutz für den Bildschirmschoner verwenden*.




*Bildschirmschoner erzwingen*

- Aktivieren Sie die Richtlinie *Bestimmten Bildschirmschoner erzwingen*. Vergeben Sie den Namen `scrnsave.scr`, um den Anmeldebildschirmschoner zu verwenden.

  Dieser muss auf dem Computer lokal unter *%systemroot%/System32* gespeichert sein. Wenn Ihre Clientcomputer nicht unter Windows 8/8.1 oder Windows 10 laufen, müssen Sie entsprechend einen anderen Bildschirmschoner verwenden.
- Beenden Sie die Richtlinienbearbeitung, indem Sie auf das Schließfeld des Fensters klicken.

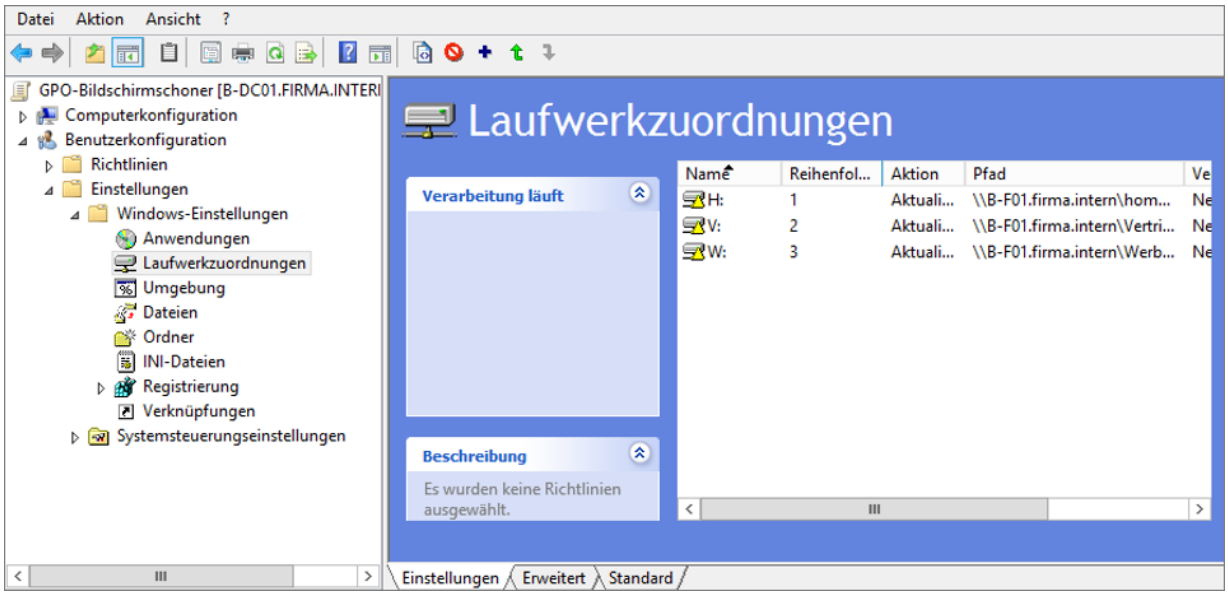
Im Gruppenrichtlinienverwaltungs-Editor haben Sie die Möglichkeit, zwischen den Anzeigen *Erweitert* und *Standard* zu wählen. In der erweiterten Ansicht werden Ihnen zu jeder Gruppenrichtlinieneinstellung erklärende Informationen angezeigt.

## Aufgabe 2 – Gruppenrichtlinieneinstellungen für *GPO-LW-Zuordnungen und -Einschränkungen*

Nun sollen die lokalen Laufwerke für die Benutzer gesperrt werden, damit diese gezwungen sind, ihre Dateien nur auf den bereitgestellten Netzlaufwerken abzulegen.

- Erweitern Sie den Container *Benutzerkonfiguration - Richtlinien - Administrative Vorlagen - Windows-Komponenten - Datei-Explorer*.
- Öffnen Sie die Richtlinien *Diese angegebenen Datenträger im Fenster „Arbeitsplatz“ ausblenden* und *Zugriff auf Laufwerke vom Arbeitsplatz nicht zulassen* und aktivieren Sie die Einstellung jeweils für *Nur Laufwerke A, B, C und D beschränken*.

Im nächsten Schritt geht es darum, dass die eigenen Basisordner aller Benutzer in der Vertriebsabteilung unter *H:* verknüpft werden. Zusätzlich sollen jedem Benutzer die Laufwerke *V:* für *Vertrieb* und *W:* für *Werbung* bereitgestellt werden, falls er Mitglied der jeweiligen Gruppe ist.

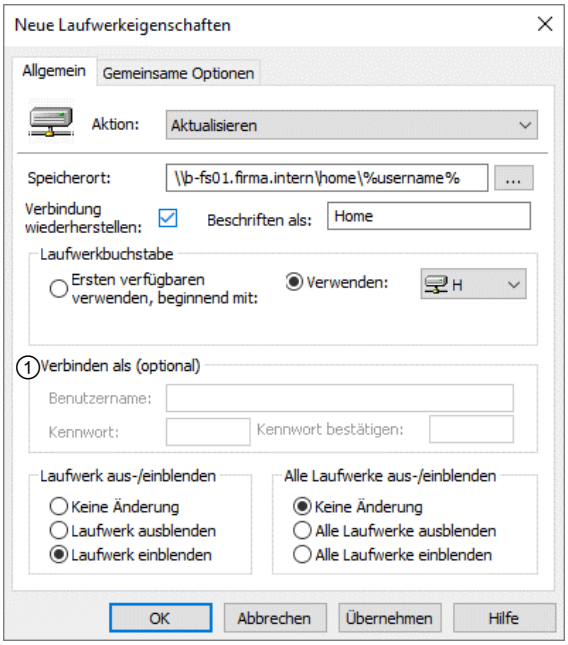



*Laufwerkszuordnungen erstellen*

- Erweitern Sie den Container *Benutzerkonfiguration - Einstellungen - Windows-Einstellungen*. Klicken Sie auf *Laufwerkzuordnungen*.
- Wählen Sie im Kontextmenü *Neu - Zugeordnetes Laufwerk*.


Schulversion
© HERDT-Verlag

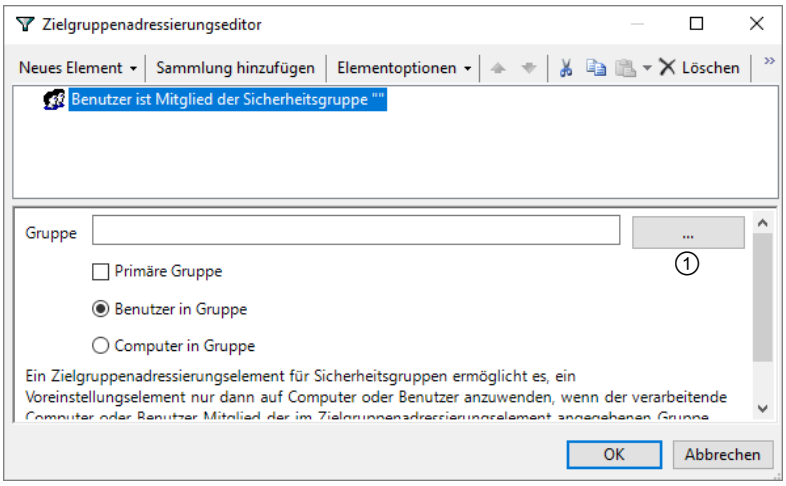
- Wählen Sie im Listenfeld *Aktion* den Eintrag *Aktualisieren*.
- Geben Sie als Speicherort den Netzwerkpfad zu den Basisordnern Ihrer Benutzer oder einen anderen Pfad an.
- Geben Sie eine Beschriftung an, mit der die Verknüpfung aufgeführt werden soll, und wählen Sie bei Bedarf einen Laufwerksbuchstaben.
- Soll die Verbindung in einem anderen Kontext als dem des angemeldeten Benutzers durchgeführt werden, so können Sie dies konfigurieren ①.
- Legen Sie fest, ob das Laufwerk vorrangig eingeblendet oder ausgeblendet werden soll.
- Legen Sie fest, wie mit den anderen Laufwerken zu verfahren ist.
- Bestätigen Sie Ihre Einstellungen mit *OK*.




*Laufwerkszuordnung konfigurieren*

## Gruppenabhängige Laufwerkszuordnung vornehmen

- Verfahren Sie identisch, um eine zweite Laufwerkszuordnung für das freigegebene Laufwerk der Vertriebsabteilung zu erstellen.
- Wählen Sie nun das Register *Gemeinsame Optionen*, aktivieren Sie *Zielgruppenadressierung auf Elementebene* und betätigen Sie die Schaltfläche *Zielgruppenadressierung*.
- Klicken Sie auf *Neues Element* und wählen Sie *Sicherheitsgruppe*.
- Betätigen Sie nun die Schaltfläche ① und wählen Sie mithilfe des Assistenten die Gruppe *GG-Test-Vertrieb* aus.




*Gruppe für die zielgruppenabhängige Laufwerkszuordnung festlegen*

- Bestätigen Sie mit *OK* und schließen Sie die Eigenschaften der Laufwerkszuordnung.
- Verfahren Sie identisch für die Laufwerkszuordnung von *Werbung* für *GG-Test-Werbung.*

## Aufgabe 3

- Konfigurieren Sie die beiden Richtlinien *GPO-LW-Einschränkungen-Werbung* und *GPO-LW-Einschränkungen-Mobil*. Aktivieren Sie hierbei jeweils die Option *Laufwerke nicht einschränken*.

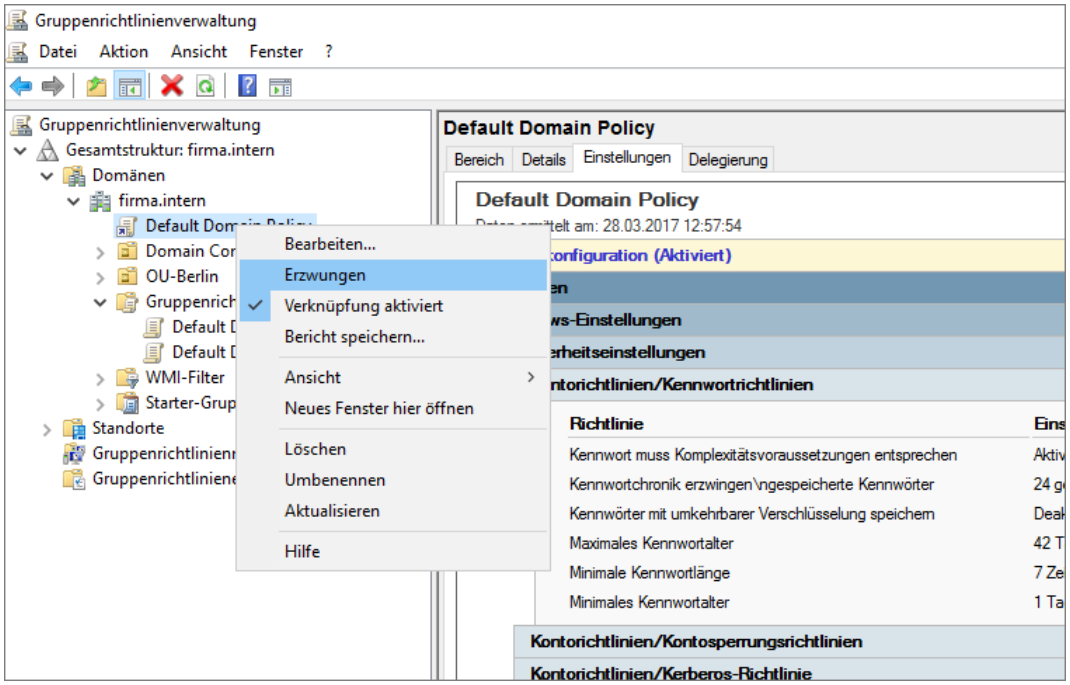
Sie müssen nun zusätzlich den Loopbackverarbeitungsmodus für Benutzergruppenrichtlinien im Modus *Zusammenführen* für die mobilen Geräte definieren.

- Erweitern Sie in der Richtlinie *GPO-LW-Einschränkungen-Mobil* den Bereich *Computerkonfiguration - Richtlinien - Administrative Vorlagen - System - Gruppenrichtlinie* und aktivieren Sie den Loopback-verarbeitungsmodus für Benutzergruppenrichtlinien im Modus *Zusammenführen*.

## Aufgabe 4

Verknüpfen Sie die GPOs entsprechend der Planung.

- Wählen Sie die Organisationseinheiten in der Gruppenrichtlinienverwaltung und aktivieren Sie im Kontextmenü den Befehl *Vorhandenes Gruppenrichtlinienobjekt verknüpfen*.
- Wählen Sie nun die entsprechende Gruppenrichtlinie aus und bestätigen Sie mit *OK*.
- Aktivieren Sie im Kontextmenü von *GPO-Bildschirmschoner* den Befehl *Erzwungen*.




*GPOs verknüpfen und erzwingen*

Daraufhin erscheint an der Gruppenrichtlinienverknüpfung das Symbol eines Vorhängeschlosses.


Schulversion
© HERDT-Verlag

## 22.4 Gruppenrichtlinien testen

### Aufgabenstellung

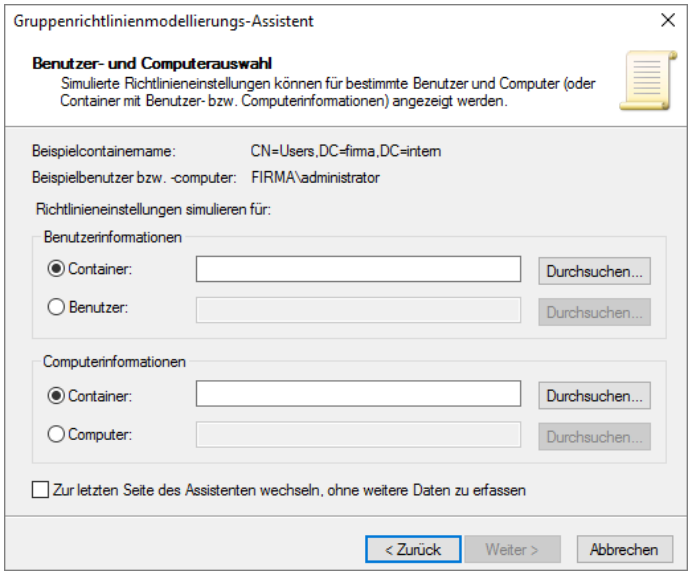
Vor einer Verknüpfung der GPOs soll eine Gruppenrichtlinienmodellierung durchgeführt werden, um die Einstellungen zu überprüfen.

Wenn die Einstellungen erfolgreich waren, soll eine Verknüpfung der GPOs vorgenommen werden.

### Gruppenrichtlinienmodellierung

- Klicken Sie in der Gruppenrichtlinienverwaltung auf *Gruppenrichtlinienmodellierung*, und wählen Sie im Kontextmenü den Befehl *Gruppenrichtlinienmodellierungs-Assistent.*
- Klicken Sie auf *Weiter*, und wählen Sie einen Domänencontroller, der die Richtlinien bereitstellen soll.
- Aktivieren Sie in der Benutzer- und Computerauswahl unter *Benutzerinformationen* das Optionsfeld *Benutzer*, und betätigen Sie die Schaltfläche *Durchsuchen*.
- Wählen Sie nun einen Benutzer, für den die Speicherung in OU-Test-Vertrieb-Mobile_Geräte simuliert werden soll.

  Wählen Sie entweder einen Computer aus der entsprechenden OU oder simulieren Sie dies, indem Sie unter *Container* die entsprechende OU auswählen.
- Aktivieren Sie das Kontrollkästchen *Zur letzten Seite des Assistenten wechseln, ohne weitere Daten zu erfassen*.
- Klicken Sie auf *Weiter,* und stellen Sie den Assistenten fertig.




*Benutzer und Container für die Gruppenrichtlinienmodellierung wählen*

Sie erhalten nun eine Auflistung der Einstellungen, die gelten würden, wenn sich *TVertrieb* an einem beliebigen Rechner aus *OU-Test-Vertrieb-Mobile_Geräte* anmeldet. Diese können Sie jederzeit aktualisieren, indem Sie im Kontextmenü auf *Abfrage erneut ausführen* klicken.

### Ergebnis der Gruppenrichtlinienmodellierung

Das Ergebnis der Gruppenrichtlinienmodellierung von *TVertrieb* umfasst drei Bereiche:

- Die Zusammenfassung zeigt, welche GPOs mit welchen Einstellungen auf welches Objekt angewendet wurden.
- Unter *Einstellungen* werden die Konfigurationen angezeigt, die in der Summe auf dem System gelten, und aus welcher Richtlinie die jeweilige Einstellung stammt.
- Unter *Abfrage* wird aufgezählt, von welchen Systemen die Abfrage unter welchen Einstellungen vorgenommen wurde.

Abschließend können Sie nun die Auswirkungen der Einstellungen mit einer Benutzeranmeldung ausprobieren.

### Benutzeranmeldung und Test mit *TVertrieb*

- Melden Sie sich mit dem Konto von *TVertrieb* am Testcomputer aus *OU-Test-Vertrieb* an.
- Öffnen Sie den Explorer und erweitern Sie *Computer*. Was fehlt?
- Melden Sie sich im Anschluss mit einem Benutzer aus *OU-Test-Vertrieb-Werbung* an demselben Rechner an und vergleichen Sie die Ergebnisse.
- Melden Sie sich schließlich mit dem Konto von *TVertrieb* an einem Testcomputer aus *OU-Test-Vertrieb-Mobile_Geräte* an.

### Gruppenrichtlinienimplementierung beurteilen

Zur Implementierung von Gruppenrichtlinien gehört neben einem ausführlichen Test auch die Beurteilung. Die Beurteilung bezieht sich auf Folgendes:

- ✔ Wirken sich die Richtlinien auf die gewünschten Personen aus?
- ✔ Wurden die definierten Anforderungen mit den Richtlinien effektiv erfüllt?

Aus der Beurteilung ergeben sich gegebenenfalls Anforderungen für weitere Konfigurationsmaßnahmen. Bleibt es zunächst beim Status quo, dokumentieren Sie die Sicherheitslücken.

## 22.5 Gruppenrichtlinienergebnisse

### Auswirkungen von Gruppenrichtlinien überprüfen

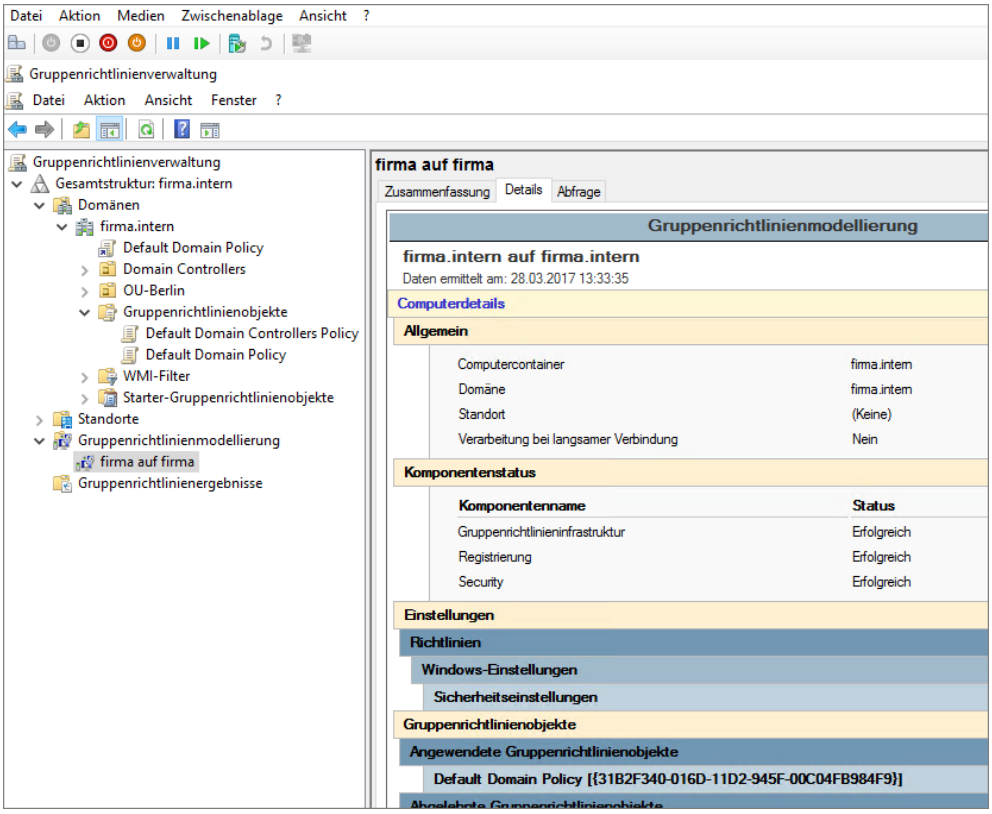
Sie können eine genauere Version der Gruppenrichtlinienüberprüfung anwenden, indem Sie in der Gruppenrichtlinienverwaltung auf die Gruppenrichtlinienergebnisse zugreifen. Auch dabei wird ein Assistent Sie auffordern, einen bestimmten Benutzer und Computer anzugeben; allerdings ist die Voraussetzung dafür, dass dieser Benutzer sich bereits einmal an dem System angemeldet hat.

### Richtlinienergebnissatz anwenden

- Öffnen Sie die Gruppenrichtlinienverwaltung.
- Klicken Sie mit der rechten Maustaste auf das Symbol *Gruppenrichtlinienergebnisse*. Öffnen Sie den Gruppenrichtlinienergebnis-Assistenten.
- Wählen Sie *Dieser Computer* als Ziel der Untersuchung aus. Klicken Sie auf *Weiter*.
- Wählen Sie *Richtlinieneinstellungen anzeigen für* und bestimmen Sie den zu untersuchenden Benutzer. Betätigen Sie die Schaltfläche W*eiter.*

  Eine Übersicht der von Ihnen getroffenen Einstellungen für den Assistenten wird angezeigt.
- Stellen Sie den Assistenten fertig.


Schulversion
© HERDT-Verlag




*Gruppenrichtlinienergebnis anzeigen*

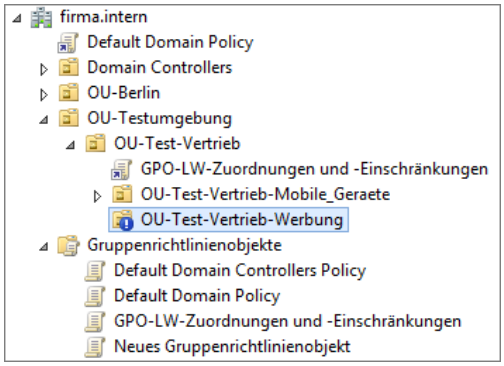
## 22.6 Gruppenrichtlinien bearbeiten

### Aufgabenstellung

Testen Sie, was passiert, wenn Sie die Gruppenrichtlinienvererbung für *OU-Test-Vertrieb-Werbung* deaktivieren.

### Vererbung von Gruppenrichtlinien bearbeiten

Die Gruppenrichtlinien der *OU-Test-Vertrieb* sollen nicht auf die *OU-Test-Vertrieb-Werbung* angewendet werden. Deshalb soll die Richtlinienvererbung deaktiviert werden.




*Vererbung deaktivieren*

- Öffnen Sie die Gruppenrichtlinenverwaltung.
- Klicken Sie mit der rechten Maustaste auf *OU-Test-Vertrieb-Werbung* und wählen Sie den Kontextbefehl *Vererbung deaktivieren*.
- Melden Sie sich mit einem Benutzer aus der OU an einem Rechner an, der nicht in der OU für mobile Geräte gespeichert ist.
- Machen Sie nun eine Pause und kehren Sie frühestens nach 10 Minuten zum Rechner zurück.

Die Deaktivierung der Richtlinienvererbung bewirkt, dass keines der in übergeordneten OUs wirksamen GPOs in der aktuellen OU angewendet wird, es sei denn, es wird explizit durchgesetzt.

# 23 Notfallsicherung

**In diesem Kapitel erfahren Sie**

- mit welchen Methoden Sie Domänencontroller vor einem Ausfall schützen
- wie Sie Domänencontroller nach einem Ausfall wieder in Betrieb nehmen können

**Voraussetzungen**

- Windows Server 2019 installieren
- Active Directory installieren

## 23.1 Strategien und Wiederherstellungsfunktionen

### Fehlertoleranz

Fehlertoleranz bezeichnet ein Konzept, das gewährleistet, dass durch einen Ausfall eines Teils das Ganze nicht nennenswert beeinträchtigt wird.

### Strategien im laufenden Netzwerkbetrieb

Im laufenden Netzwerkbetrieb selbst wirken standardmäßig bereits zahlreiche Mechanismen, die helfen, Fehler zu eliminieren oder kurze Ausfälle ohne Datenverlust zu überwinden. Zu diesen Mechanismen zählen z. B. die Active Directory-Replikation selbst oder redundantes DHCP.

Sie werden jedoch darüber hinaus selbst geeignete Maßnahmen ergreifen, um sicherzustellen, dass Fehler entweder automatisch korrigiert werden oder das System nach einem Ausfall schnell wieder in Betrieb genommen werden kann. Hierzu zählen:

- der Einsatz redundanter Netzteile in Servern,
- der Einsatz fehlertoleranter Datenträger auf Domänencontrollern und Dateiservern,
- regelmäßige Datensicherungen der geschäftlich relevanten Daten,
- regelmäßige Datensicherungen der systemrelevanten Daten.

Um das Active Directory vor Ausfällen zu schützen, empfiehlt sich außerdem der Einsatz von je mindestens zwei Domänencontrollern pro Domäne und Standort.

### Wiederherstellungsfunktionen

- Erweiterte Startoptionen
- Wiederherstellungskonsole
- Systemstatus
- Systemwiederherstellung mit Windows Server-Sicherung


Schulversion
© HERDT-Verlag

## 23.2 Fehlertolerante Datenträger

### RAID

Windows Server 2019 bietet mehrere Strategien, Festplatten optimal hinsichtlich Speicherplatz, Geschwindigkeit und Ausfallsicherheit zu kombinieren. Die einzelnen Technologien bieten unterschiedliche Grade an Datensicherheit und sind nach RAID (Redundant Array of Independent Disks) klassifiziert. Definiert wurden sechs RAID-Stufen, die mit RAID0 bis RAID5 bezeichnet werden. Windows Server 2019 unterstützt auf dynamischen Datenträgern RAID0, RAID1 und RAID5.

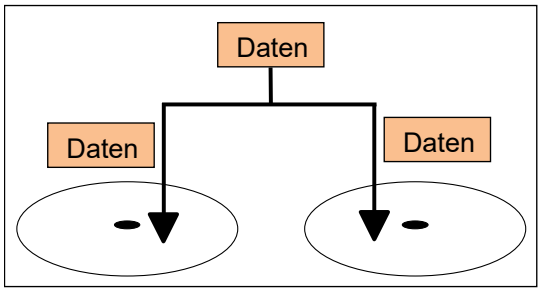
Fehlertoleranz bieten

- gespiegelte Datenträger (RAID1)
- Stripeset mit Parität (RAID5)

### Gespiegelter Datenträger (RAID 1)

Bei der Spiegelung (Disk Mirroring) wird die Information eines Datenträgers völlig identisch auf einem zweiten Datenträger abgespeichert. Beim Ausfall einer Platte gehen keine Informationen verloren.

Diese Technologie erfordert die doppelte Speicherkapazität und verringert die Performance, denn jeder Schreibvorgang muss zweimal ausgeführt werden. Wenn jedoch jede der beiden Platten über einen eigenen Controller angesprochen wird, tritt dieser Nachteil nicht auf.




*Gespiegelter Datenträger*

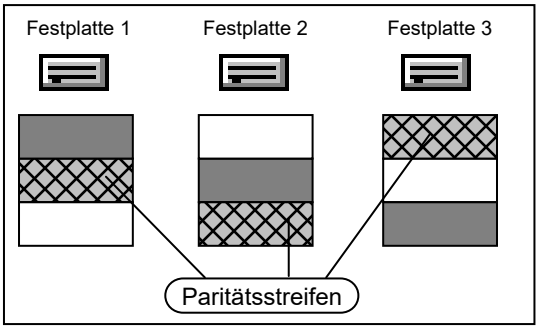
Die Systempartition eines Windows Server 2019 darf nur als RAID1 angelegt werden, andere RAID-Formen werden nicht unterstützt.

### Stripeset mit Parität (RAID 5)

Stripesets mit Parität sind normalen Stripesets sehr ähnlich. Sie enthalten jedoch zusätzlich einen Mechanismus zur Schaffung von Fehlertoleranz.

Jede Festplatte enthält in regelmäßigen Abständen Paritätsstreifen. Hier werden Informationen gespeichert, aus denen beim Ausfall einer beliebigen Platte die verlorenen Daten rekonstruiert werden können. Für ein Stripeset mit Parität werden mindestens drei Festplatten benötigt.

Weder die Systempartition noch die Partition mit der Active Directory-Datenbank dürfen auf einem Stripeset liegen.




*Stripeset mit Parität*

Beachten Sie, dass die von Windows angebotenen RAID-Implementierungen reine Software-Lösungen sind. Sie sind selbst preiswerten hardware-basierten Lösungen mithilfe handelsüblicher RAID-Controller sowohl hinsichtlich der Performance als auch der Verfügbarkeit von Daten im Fehlerfall unterlegen. Ziehen Sie deshalb für Server ein Hardware-RAID grundsätzlich vor.

## 23.3 Erweiterte Startoptionen

### Erweiterte Startoptionen aufrufen

Wenn ein Server nicht mehr startet, versuchen Sie eine Reparatur direkt vor Ort. Hierzu stellt Windows erweiterte Startoptionen zur Verfügung. So besteht die Möglichkeit, den Boot-Vorgang zu untersuchen und die Fehlerquelle zu erkennen (Startprotokollierung) oder Windows in einem Standardmodus (abgesichert) zu starten, der verhindert, dass bestimmte benutzerdefinierte Einstellungen und Treiber verwendet werden, die Probleme verursachen könnten.

- Schalten Sie den Server ein.
- Betätigen Sie nach dem POST des BIOS mehrmals die Tastenkombination ⇧ F8.
  Wenn Sie schnell genug waren, öffnen sich die erweiterten Startoptionen.
- Mit den Cursortasten ↓ bzw. ↑ wählen Sie die gewünschte Startalternative, mit ↵ wird der Start mit der gewählten Option ausgeführt.

Je nach Art des Problems, der mutmaßlichen Ursache und Ihres Lösungsansatzes werden Sie aus den vorhandenen Optionen die geeignete Startoption wählen. Es eignet sich nicht jede Startoption für jede Situation.

| | |
|---|---|
| Abgesicherter Modus | Im abgesicherten Modus werden nur Basistreiber geladen (z. B. PS/2-Maustreiber und VGA-Treiber für den Monitor) sowie die grafische Benutzeroberfläche. Im abgesicherten Modus können Sie beispielsweise fehlerhafte Treiberdateien manuell entfernen oder Konfigurationsfehler beheben. |
| Startprotokollierung aktivieren | Normaler Windows-Start. Dabei wird jedoch eine Protokolldatei (`%WINDIR%\ntbtlog.txt`) erstellt. |
| Letzte als funktionierend bekannte Konfiguration (erweitert) | Wählen Sie diese Startoption, wenn Windows nach einer Änderung an der Systemkonfiguration nicht mehr startet und Sie sich seit der Änderung noch nicht wieder angemeldet haben. Sie können Windows dann veranlassen, zum Starten eine Sicherungskopie der Computerkonfiguration in der Registrierung zu verwenden, die beim letzten erfolgreichen Systemstart aktuell war. |
| Verzeichnisdienst-Wiederherstellung | Diese Option ist nur auf Domänencontrollern verfügbar. Verwenden Sie sie, um Fehler bezüglich des Verzeichnisdienstes zu beheben. |
| Debugmodus | Normaler Windows-Start. Gleichzeitig sendet der Computer Informationen über den Startvorgang über ein serielles Kabel an einen anderen Computer. |

Die Auswahl einer erweiterten Startoption ist jedoch nur möglich, wenn der Server noch von der Systemfestplatte bootet. Ist deren Bootsektor beschädigt oder fehlen Teile der Windows Startumgebung, können Sie das System mit einer Reparaturinstallation von der CD reparieren.

Die Datei `boot.ini` wird unter Windows Server 2019 nicht mehr verwendet. Sie wurde durch Startkonfigurationsdaten (Boot Configuration Data, BCD) ersetzt. In dieser ist festgelegt, wo das Startprogramm Winload.exe gespeichert ist.

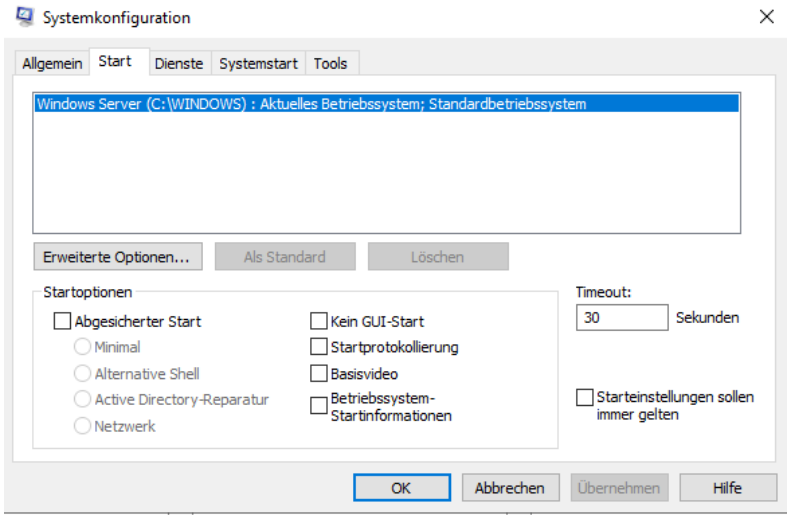
Wenn Sie diese bearbeiten möchten, können Sie sie mit dem Befehlszeilenprogramm bcdedit.exe aufrufen. So können etwa veraltete Einträge einer Multiboot-Konfiguration entfernt werden. Wesentlich einfacher ist aber das Bearbeiten von Starteinstellungen mit dem Tool Systemkonfiguration.


Schulversion
© HERDT-Verlag

### Systemkonfiguration aufrufen

- Öffnen Sie die Systemkonfiguration, indem Sie im Startmenü `msconfig` ↵ eingeben.

- Im Register *Allgemein* können Sie die grundlegenden Startarten festlegen.
- Im Register *Start* können Sie erweiterte Funktionen festlegen und die Startreihenfolge bei einer Multiboot-Konfiguration festlegen.
- Unter *Dienste* ist festgelegt, welche Dienste vom System gestartet werden sollen.
- *Systemstart* zeigt an, welche Anwendungen beim Systemstart aktiviert werden.
- Das Register *Tools* zeigt eine Auflistung von Anwendungen zur Diagnose von Problemen.




*Startoptionen für den Booteintrag festlegen*

## 23.4 Systemstatusdaten

### Systemstatus

Der Systemstatus enthält alle systemspezifischen Daten, die gebraucht werden, um einen Computer nach einem Ausfall wieder in Betrieb zu nehmen. Der Systemstatus ist ein kompletter Satz, der sich aus Dateien unterschiedlicher Herkunft zusammensetzt. Der Systemstatus kann gesichert und wiederhergestellt werden.

Auf einem Mitgliedsserver unter Windows Server 2019 enthält der Systemstatus u. a. folgende Dateien:

- Systemdateien und Startdateien,
- Registrierung,
- COM+ Klassenregistrierungsdatenbank,
- Datenbank für Zertifikatsdienst, sofern der Server als Zertifikatsserver eingesetzt wird,
- die Metabase des Internet Information Servers, sofern dieser installiert ist.

Auf einem Domänencontroller unter Windows Server 2019 enthält der Systemstatus außerdem noch folgende Dateien:

- alle Verzeichnisse für das Active Directory,
- das Verzeichnis `SYSVOL`.

### Systemstatus sichern

Sie können den Systemstatus mit dem Programm Windows Server-Sicherung aus dem Lieferumfang von Windows Server 2019 sichern. Die dabei entstehende Sicherung umfasst mindestens 6 Gigabyte.

## 23.5 Der Active Directory-Papierkorb

### Objekte löschen

Wenn ein Objekt im Active Directory gelöscht wird, muss sichergestellt werden, dass diese Löschung im gesamten Verzeichnis bekannt wird. Dazu wird das Objekt mit einem Tombstone (Grabstein) versehen und so lange repliziert, bis alle Domänencontroller über die Löschung informiert sind.

Die Zeitdauer, für die ein gelöschtes Objekt im System verbleibt, ist im Attribut *TombstoneLifetime* festgelegt und beträgt bei älteren Windows-Server-Betriebssystemen 60 Tage, bei Systemen ab Windows Server 2003 mit SP2 180 Tage.

### Active Directory-Papierkorb

Eine entscheidende Neuerung seit Windows Server 2008 R2 ist der Active Directory-Papierkorb. Mit diesem lassen sich gelöschte Objekte mit all ihren Attributen auch im laufenden Betrieb ohne Probleme wiederherstellen.

Im Gegensatz zu vorherigen Versionen von Windows-Server-Betriebssystemen wird ein gelöschtes Objekt mit seinen Attributen in den versteckten Container *Deleted Objects* verschoben. Bei den Vorgängerversionen ab Windows Server 2003 wurde hier nur der Tombstone (Grabstein) des Objektes hinterlegt. Dieser enthielt zwar einige wenige Attribute (z. B. den RDN oder die SID) des Objektes, war aber für eine erfolgreiche Wiederherstellung eines Benutzers oder einer Gruppe nicht ausreichend.

Mit Windows Server 2019 gibt es die Möglichkeit, Objekte komplett aus dem Papierkorb wiederherzustellen. Dafür sind allerdings einige Vorbereitungen nötig.

### Active Directory-Papierkorb aktivieren

Zuerst müssen der Domänen- und der Gesamtstrukturbetriebsmodus auf Server 2008 R2 oder höher gesetzt werden. Voraussetzung hierfür ist, dass alle Domänencontroller in der Gesamtstruktur unter den entsprechenden Betriebssystemen laufen.

- *Öffnen Sie Active Directory-Domänen und -Vertrauensstellungen*.
- Klicken Sie auf der Domäne im Kontextmenü auf *Domänenfunktionsebene heraufstufen* und wählen Sie z. B. die Funktionsebene *Windows Server 2019*. Verfahren Sie wie gewohnt.
- Klicken Sie auf den ersten Knoten *Active Directory-Domänen und -Vertrauensstellungen* im Kontextmenü auf *Gesamtstrukturfunktionsebene heraufstufen* und wählen Sie die Funktionsebene *Windows Server 2019*. Verfahren Sie wie gewohnt.

### Papierkorb aktivieren

Nun müssen Sie im Active Directory-Verwaltungscenter als Organisationsadministrator für die Gesamtstruktur den Papierkorb aktivieren:

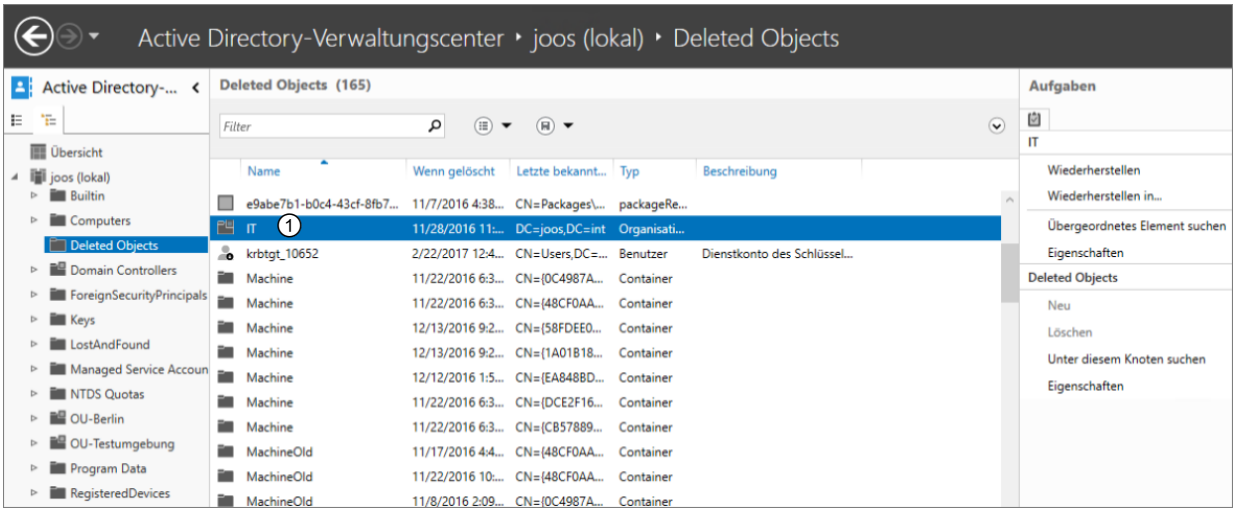
- Öffnen Sie das Active Directory-Verwaltungscenter.
- Markieren Sie die Domäne.
- Wählen *Sie Aufgaben - Papierkorb aktivieren*.
- Bestätigen Sie die Sicherheitsabfrage mit *OK*. Sie werden nun darauf hingewiesen, dass Sie das AD-Verwaltungscenter aktualisieren müssen.
- Warten Sie ab, bis die Replikation aller DCs beendet ist, und bestätigen Sie die Aktualisierung mit *OK*.
- Starten Sie das AD-Verwaltungscenter neu. Der AD-Papierkorb ist nun aktiviert.


Schulversion
© HERDT-Verlag

### Objekte wiederherstellen

Sie können nun gelöschte Objekte aus dem Active Directory-Papierkorb wiederherstellen, indem Sie das Active Directory-Verwaltungscenter verwenden:

- Öffnen Sie das Active Directory-Verwaltungscenter.
- Klicken Sie auf der Domänenebene auf *Deleted Objects*.
- Markieren Sie das wiederherzustellende Objekt ①.
- Verwenden Sie *Wiederherstellen* oder *Wiederherstellen in*, um das Objekt an seinem originalen Speicherort oder einem alternativen Speicherort wiederherzustellen.




*Objekt aus dem Papierkorb wiederherstellen*

## 23.6 Windows-Speicherdiagnose

### Speicher überprüfen

Manchmal entstehen Fehler im System durch fehlerhafte RAM-Bausteine. Diese können von Windows Server 2019 mit dem Arbeitsspeicherdiagnosetool beim Systemstart aufgespürt werden. Allerdings sollten Sie nach Möglichkeit in einem Server ECC-RAM verwenden, das über einen eigenen Korrekturmechanismus verfügt. Wenn Sie jedoch häufiger Speicherfehler feststellen, sollten Sie das Tool verwenden, um den Arbeitsspeicher auf Defekte zu untersuchen. Dies kann erhebliche Zeit in Anspruch nehmen (je nach Geschwindigkeit und Größe des installierten Speichers).

### Speicherdiagnose aufrufen

- Öffnen Sie die Windows-Speicherdiagnose, indem Sie im Startmenü „mdsched“ eingeben.

Sie können nun entweder eine sofortige Überprüfung des Speichers vornehmen oder das System beim nächsten Start einen Test durchführen lassen.

## A


Ablaufdatum, Konto 131
ACE (Access Control Entry) 163
ACL (Access Control List) 141, 158, 160
Active Directory installieren, Vorbereitungen 63
Active Directory, Leistungsmerkmale 14
Active Directory-Benutzer und -Computer 124
Active Directory-Datenbank einsehen 77
Active Directory-Papierkorb 230
Active Directory-Verwaltungscenter 75
Active-Directory-integrierte Zonen 85
AD (Active Directory) 55
AD DS (AD-Domänendienste) 55
Administrative Vorlagen 200
ADML-Datei 201
ADMX-Datei 201
ADSI-Editor 136
AGDLP-Regel 144
Anmelden 131
Anmelden, lokaler Administrator 28
Anmeldestationen, erlaubte 131
Anmeldezeiten, erlaubte 131
APIPA (Automatic Private IP Addressing) 108
Arbeitsgruppe 30
Archivierung, zentrale 195
Aufbau der Testumgebung 4
Aufgabenblock 169
Aufgabenblockansicht 16
Autoritätsursprung, DNS 88
Autoritätsursprung, SOA 100
AXFR 85


## B


Basisordner 131
Benutzerkonto erstellen 132
Benutzerkonto kopieren 133
Benutzerkonto verschieben 134
Benutzerprofil, Einstellungen 138
Benutzerrecht zuweisen 208
Berechtigungen 158
Berechtigungen überprüfen 163
Berechtigungen, Arten 159
Berechtigungen, effektive 160
Berechtigungen, spezielle anzeigen 165
Berechtigungsvererbung überprüfen 163
Bereichsoptionen 115
Bereitstellungsserver 16
Besitz übernehmen 174
Betriebsmaster 59
Bevorzugte DNS-Server, IPv4 92
Bevorzugte DNS-Server, IPv6 94
Bezeichnungen, Aufbau 6
BitLocker-Laufwerks-verschlüsselung 15


## C


CIDR-Notation 106
Cloud 194
Cluster 17, 38
Cmdlets 16, 156
CN (Common Name) 134
CNAME (Canonical Name) 88, 136
Colon hex 106
Commandlets 16
Computer anzeigen 74
Computerkonto erstellen 139
Computername 23, 79
Container, vordefinierte 125


## D


DAC (Dynamic Access Control) 19, 194
DACL 141, 158
Dashboard 29, 36
Dateidienste 183
Dateigruppe 190
Dateiprüfung 190
Dateiprüfungsverwaltung 190
Dateiprüfungsvorlage 190
Dateistruktur planen 196
Dateisystem 21
Dateitypen, Ressourcen-Manager 19
Datenausführungsverhinderung 40
Datenaustausch 196
Datendeduplizierung 193
Datenträgerdeduplizierung 19
Datenträgerkontingente 18
Datenträgervirtualisierung 194
dcpromo 65
DDNS 82
Delegieren, Zonen 86
DEP (Data Execution Prevention) 40
DFS (Distributed File System) 18, 181, 193
DHCP (Dynamic Host Configuration Protocol) 18, 108
DHCP, Benutzerklasse 116
DHCP, Bereich 112
DHCP, Herstellerklasse 116
DHCP, Hot Standby Mode 118
DHCP, maximale Clientvorlaufzeit 118
DHCP, Reservierung 117
DHCP, Serveroptionen 115
DHCP-Failover 118
DHCP-Relay-Agent 109
DN (Distinguished Name) 134, 153
DNS (Domain Name System) 18, 78
DNS, Aliaseinträge 88
DNS, Dateien 87
DNS, Replikationsmethoden 85
DNS, Stammhinweise 98
DNS, Stubzonen 87
DNS, Weiterleitungen 98
DNS-Benachrichtigung 101
DNS-Dienst installieren 95
DNS-Dienst konfigurieren 96
DNS-Domänenname 78
DNS-Eintrag überprüfen 69
DNS-Namensserver 84
DNS-Server 108
DNS-Server, IPv4 92
DNS-Server, IPv6 94
DNS-Stamm 83
Domäne 56
Domänencontroller hinzufügen 71
Domänencontroller hochstufen 66
Domänencontroller installieren 65
Domänencontroller zu Domäne hinzufügen 71
Domänenfunktionsebene 57
Domänennamespace 78
Domänenrichtlinien anpassen 209
Domänenrichtlinien testen 212
Domänenstamm, DNS 83
Doppelpunkt-Hexadezimal-Notation 106
Dotted decimal notation 105
Druckerberechtigungen 178
DSRM (Directory Services Restore Mode) 72
Dynamische Adresszuweisung 109
Dynamische Aktualisierung 114
Dynamische Aktualisierung, DNS 82
Dynamische Zugriffssteuerung, DAC 19


## E


EFS (Encrypted File System) 15
Erstkonfiguration 29
Erweiterte Startoptionen 228, 229
Erzwingen, Gruppenrichtlinien 204


## F


Fehlertolerante Datenträger 227
Fehlertoleranz, Definition 226
Forward-Lookup 80



Schulversion
© HERDT-Verlag

Forward-Lookupzone erstellen 97
FQDN (Fully Qualified Domain Name) 67, 78, 79
Freigabe 181
Freigabe- und Speicherverwaltung 184
Freigabe-Berechtigungen 178
FSMO (Flexible Single Master Operation, Betriebsmaster) 59
Funktionsebene 57

## G

GC (Global Catalog) 60
Gesamtstruktur 56
Gesamtstruktur erstellen 67
Gesamtstrukturfunktionsebene 58
Gespiegelter Datenträger, RAID 1 227
Globale Gruppe erstellen 148
Globale Gruppen in lokale Gruppe aufnehmen 150
Globaler Katalog 60, 67
GlobalNames-Zone 81
gpmc.msc 205
GPO (Group Policy Object) 202
Gruppen mit einer Batchdatei anlegen 152
Gruppen schachteln 143
Gruppen, Gültigkeitsbereich 142
Gruppenmitgliedschaften 131
Gruppenplanung 145
Gruppenplanung mit universalen Gruppen 150
Gruppenrichtlinien beurteilen 224
Gruppenrichtlinien implementieren 218
Gruppenrichtlinien planen 215
Gruppenrichtlinien, Berechtigungen 203
Gruppenrichtlinien, Definition 199
Gruppenrichtlinien, Vererbung 202
Gruppenrichtlinien, Vererbung 204
Gruppenrichtlinien, Vererbung bearbeiten 225
Gruppenrichtlinien, Verknüpfung 202
Gruppenrichtlinien, Vorlagen 201
Gruppenrichtlinieneinstellungen setzen 219
Gruppenrichtlinienergebnisse 201, 224
Gruppenrichtlinien-modellierung 201, 223
Gruppenrichtlinienobjekt 202
Gruppenrichtlinienverknüpfungen 206
Gruppenrichtlinienverwaltungs-Editor 207
Gruppentypen 141
GUID (Globally Unique Identifier) 140

## H

Hardwareanforderungen, Host 24
Hardware-Voraussetzungen 20
Hochverfügbarkeit 196
Hostname 79
Hostnamen 79
Hyper-V 12
Hyper-V, Einrichtung 42
Hyper-V, Hardwarevoraussetzungen 40
Hyper-V, Installation 41
Hyper-V, Live-Migration 38
Hyper-V, Netzwerk einrichten 44
Hyper-V, Prüfpunkt 37
Hyper-V, Prüfpunkt erstellen 53
Hyper-V, Prüfpunkte 43
Hyper-V, Rolle hinzufügen 41
Hyper-V, virtuelle Computer 43
Hyper-V, virtuellen Computer einrichten 47
Hyper-V, virtuellen Computer verwalten 50
Hyper-V-Manager 43

## I

icacls.exe 176
IFM (Install From Media) 71
Informationen, Schutz von 196
Installation 27
Installationsart 24
Installationsmedium 26
Installationsoptionen, Hyper-V 49
Installationsverfahren 21
Interaktive Anmeldung, Richtlinie bearbeiten 210
IP-Konfiguration 30
IP-Protokollauswahl 89
IPv4 konfigurieren 91
IPv4-Adressen 105
IPv6 konfigurieren 93
IPv6-Adressen 106
IPv6-Reverse-Lookupzone 98
ISP 81
IXFR 85

## K

Kacheln 34
Kennwortoptionen 130
Kerberos 14
Komplexes Kennwort 68
Konsistenzprüfung, KCC 122
Konsolenmodus 168
Kontenoperatoren 139
Kontingent 190
Kontingentverwaltung 188
Kontingentvorlagen 188
Kontorichtlinien 213
Kontorichtlinien bearbeiten 209
Kontosperrung 131, 212
Kontosperrungsrichtlinien bearbeiten 210

## L

Laufwerke, Zugriff beschränken 210
LDAP (Lightweight Directory Access Protocol) 55
Leasedauer 113, 114
Lokale Gruppe erstellen 149
Loopbackverarbeitungsmodus 216
LTSC (Long Term Servicing Channel) 11

## M

MAC-Adresse 107, 117
Master-DNS-Server 85
Migration 21
Mitglieder zu globaler Gruppe hinzufügen 148
Mitgliedsserver 21
MMC (Microsoft Management Console) 16, 168
Multiboot 25
Multimaster-Replikationsmodell 58

## N

Namensgebung 6
Namensserver 84
Namensservercaching 81
Netzwerkadresse 107
NLB (Network Load Balancing) 39
nslookup 102
NTDS, Ordner 73
NTDS.dit 55
NTDS-Settings 122
NTFS 19
NTFS-Berechtigungen 172
NTFS-Verrechtung 177

## O

Objektverwaltung 162
Objektverwaltung delegieren 162, 165
Offlineeinstellungen 182
Optisches Laufwerk, Hyper-V 52
Organisationseinheit 60
Organisationseinheit erstellen 128, 217
OU (Organizational Unit) 60

## P


Password Settings Object zuweisen 214
PDC-Emulator 121
PolicyDefinitions 201
Primärer Namensserver 84
Primäres DNS-Suffix 79
Private IP-Adressen 106
Profilpfad 131
PSO (Password Settings Object) 213


## Q


Quota 188


## R


RAID (Redundant Array of Independent Disks) 227
RDN (Relative Distinguished Name) 134
Rechte 158
ReFS (Resilient File System, robustes Dateisystem) 19
Remotedesktopdienste 17
Remoteserver-Verwaltungstools 65, 73
Replikation innerhalb des Standorts 120
Replikation zwischen Standorten 121
Replikationsaufwand 143
Replikationstopologie 123
Ressourcen suchen 179
Ressourcen-Manager 19, 187
Reverse-Lookup 80
Reverse-Lookupzone einrichten, IPv6 98
Reverse-Lookupzone erstellen 97
Richtlinienergebnissatz anwenden 224
RODC (Read-only Domain Controller) 16, 58


## S


SAC (Semi Annual Channel) 11
Schattenkopien 192
Server wiederherstellen 38
Server-Core 11
Server-Manager 36
Serverobjekt 122
Serverrollen 38
Sichere dynamische Aktualisierung 82
Sicherheitsgruppe 141
Sicherheitskonfiguration 31
Sicherheitsrichtlinien für Domänencontroller bearbeiten 207
Sicherheitsrichtlinien, Domäne 209
Sicherung 195
SID (Security Identifier) 140
Snap-In 16
SOA 100
Speicherberichteverwaltung 191
Speicherdiagnose 231
Speicherung, zentrale 195
Spiegelung (Disk Mirroring) 227
SRV-Einträge prüfen 69
SRV-Einträge, Erstellung erzwingen 70
Stammdomäne einrichten 65
Stammhinweise, DNS 98
Stammnamensserver 83
Standardgateway 107
Standort 61
Standort, Domäne 120
Standort, Grundlagen 119
Standort, Namespace 120
Standortverknüpfung 61, 122
Standortverknüpfungsbrücke 122
Stripset mit Parität, RAID 5 227
Struktur 56
Stubzone, DNS 87
Subnetzmaske 106
Subzone, DNS 86
Suchfunktion 35
Symmetric Multiprocessing 17
System wiederherstellen 226
Systemkonfiguration 229
Systemstatus sichern 229
Systemstatus, Definition 229
Sysvol 62, 201
SYSVOL, Ordner 77


## T


TCP/IP 105
Testumgebung, Aufbau 4
Tiles 34
Tombstone 230
TPM-Technik 15
Trusted Platform Module 15
TTL (Time To Live) 81


## U


Überschrift 130
Universale Gruppe 143
Universale Gruppen erstellen 151
UPN (User Principal Name) 133


## V


Verarbeitungsreihenfolge, GPO 203
Verbindungsobjekt 122
Vererbung 164, 173
Vererbung, Berechtigungen 161
Versionierung 192
Versteckte Freigabe 182
Verteilergruppen 141, 142
Vertrauensstellungen 57
Verwaltungsaufgaben zuweisen 16
Verwaltungstool 168
Verzeichnisdienste 13, 55
Verzeichnisdienste deinstallieren 64
Verzeichnisstruktur 56
Virtualisierung 37
Virtualisierungsfunktion 24
Virtuelle Netzwerke 41
Volume Licensing Program 23
Volumenschattenkopierdienst 192


## W


WAN (Wide Area Network) 61
WDS (Windows Deployment Services) 16
Weiterleitungen, DNS 98
Wiederherstellung, Objekt 230
Wiederherstellungsfunktionen 226
Windows PowerShell 16
Windows Script Host 16
Windows Server 2012 R2, Tastenkombinationen 35
Windows Server 2012 R2, Versionen 10
Windows-Bereitstellungsdienste 16
Windows-Domäne 56
WINS-Server 108
WMI (Windows Management Interface) 17


## Z


Zonen, Active-Directory-integrierte 85
Zonen, DNS 83
Zonendatei 83
Zonenreplikation 101
Zonenübertragung bearbeiten 100
Zugriffsbasierte Aufzählung 185




Schulversion

© HERDT-Verlag

# Impressum

Matchcode: W2019N

Autoren: Thomas Joos, Martin Dausch

Produziert im HERDT-Digitaldruck

1. Ausgabe, März 2019

HERDT-Verlag für Bildungsmedien GmbH
Am Kümmerling 21–25
55294 Bodenheim
Internet: www.herdt.com
E-Mail: info@herdt.com

© HERDT-Verlag für Bildungsmedien GmbH, Bodenheim

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder einem anderen Verfahren) ohne schriftliche Genehmigung des Verlags reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Dieses Buch wurde mit großer Sorgfalt erstellt und geprüft. Trotzdem können Fehler nicht vollkommen ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Wenn nicht explizit an anderer Stelle des Werkes aufgeführt, liegen die Copyrights an allen Screenshots beim HERDT-Verlag. Sollte es trotz intensiver Recherche nicht gelungen sein, alle weiteren Rechteinhaber der verwendeten Quellen und Abbildungen zu finden, bitten wir um kurze Nachricht an die Redaktion.

Die in diesem Buch und in den abgebildeten bzw. zum Download angebotenen Dateien genannten Personen und Organisationen, Adress- und Telekommunikationsangaben, Bankverbindungen etc. sind frei erfunden. Eventuelle Übereinstimmungen oder Ähnlichkeiten sind unbeabsichtigt und rein zufällig.

Die Bildungsmedien des HERDT-Verlags enthalten Verweise auf Webseiten Dritter. Diese Webseiten unterliegen der Haftung der jeweiligen Betreiber, wir haben keinerlei Einfluss auf die Gestaltung und die Inhalte dieser Webseiten. Bei der Bucherstellung haben wir die fremden Inhalte daraufhin überprüft, ob etwaige Rechtsverstöße bestehen. Zu diesem Zeitpunkt waren keine Rechtsverstöße ersichtlich. Wir werden bei Kenntnis von Rechtsverstößen jedoch umgehend die entsprechenden Internetadressen aus dem Buch entfernen.

Die in den Bildungsmedien des HERDT-Verlags vorhandenen Internetadressen, Screenshots, Bezeichnungen bzw. Beschreibungen und Funktionen waren zum Zeitpunkt der Erstellung der jeweiligen Produkte aktuell und gültig. Sollten Sie die Webseiten nicht mehr unter den angegebenen Adressen finden, sind diese eventuell inzwischen komplett aus dem Internet genommen worden oder unter einer neuen Adresse zu finden. Sollten im vorliegenden Produkt vorhandene Screenshots, Bezeichnungen bzw. Beschreibungen und Funktionen nicht mehr der beschriebenen Software entsprechen, hat der Hersteller der jeweiligen Software nach Drucklegung Änderungen vorgenommen oder vorhandene Funktionen geändert oder entfernt.