

HTL KREMS

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 2022

Karsten Bratvogel, Thomas Joos

1. Ausgabe, August 2022

ISBN 978-3-98569-107-4

Aufbau und Verwaltung
eines Netzwerks

W2022AVN

1 Informationen zu diesem Buch	4	8 Domänencontroller installieren und neue Domäne erstellen	62
1.1 Voraussetzungen und Ziele	4	8.1 Installation der Verzeichnisdienste vorbereiten	62
1.2 Aufbau und Konventionen	5	8.2 Domänencontroller installieren	63
2 Das Betriebssystem Windows Server 2022	6	8.3 Domänencontroller entfernen	69
2.1 Windows Server 2022	6	9 DNS und Namensauflösung	72
2.2 Dateisysteme	9	9.1 Einführung zu Namensauflösung	72
2.3 Startmenü	10	9.2 Funktionsweise des DNS	73
2.4 Windows Server 2022 mit Tastenkombinationen bedienen	10	9.3 DNS im Active Directory	76
2.5 Server-Manager und Windows Admin Center	11	9.4 DNS-Server konfigurieren	79
3 Netzwerk mit Windows	13	9.5 DNSSEC	84
3.1 Grundlagen des Netzbetriebes	13	10 DHCP – Dynamische IP-Konfiguration	85
3.2 TCP/IP	15	10.1 Dynamic Host Configuration Protocol (DHCP)	85
3.3 Vergabe von IP-Adressen	17	10.2 DHCP-Server installieren	86
3.4 Verzeichnisdienste	19	10.3 DHCP-Server konfigurieren	86
3.5 Verwaltungsfunktionen	20	11 Standorte und Replikation	95
4 Windows Server 2022 installieren	22	11.1 Überblick über Standorte	95
4.1 Vorbereitungen	22	11.2 Replikation	96
4.2 Windows Server 2022 installieren	24	11.3 Standorte verwalten	97
4.3 Basis-Konfiguration	26	11.4 Replikationstopologie erkunden	101
5 Serverfunktionen anpassen	31	12 Active Directory-Konten verwalten	103
5.1 Überblick über die Einstellungsmöglichkeiten	31	12.1 Überblick zu Konten	103
5.2 Anwendungen installieren	32	12.2 Container der Domäne erkunden	104
5.3 Windows-Funktionen verwalten	33	12.3 Organisationseinheiten erstellen und verwalten	105
5.4 Aktuelle Konfiguration einsehen	34	12.4 Listen erstellen	108
5.5 Einstellungen des Betriebssystems ändern	36	12.5 Benutzerkonten erstellen und verwalten	109
5.6 Dienste starten und verwalten	40	12.6 Computerkonten erstellen	112
5.7 Geräte verwalten	42	12.7 Gruppenkonten	112
5.8 Energieverwaltung	45	12.8 Spezielle Konten	115
6 Hardware hinzufügen	47	13 Berechtigungen anpassen	117
6.1 Hardware-Komponenten und Treiber verwenden	47	13.1 Berechtigungen	117
6.2 Hardware automatisch installieren	49	13.2 NTFS-Berechtigungen	118
6.3 Hardware manuell konfigurieren	50	13.3 Freigabeberechtigungen für Ordner	122
6.4 Hardware deaktivieren und deinstallieren	51	13.4 Berechtigungen für Drucker	123
6.5 Treiber- und Hardware-Probleme behandeln	52	14 Dateidienste einrichten	124
6.6 Problembehandlung	53	14.1 Ordnerfreigaben	124
7 Einführung in Active Directory	55	14.2 Dateidienste installieren	125
7.1 Überblick über den Verzeichnisdienst	55	14.3 Freigabe- und Speicherwaltung	127
7.2 Domäne, Struktur und Gesamtstruktur	55	14.4 Ressourcen-Manager für Dateiserver	128
7.3 Funktionsebenen	57	14.5 DFS (Distributed File System)	133
7.4 Domänencontroller, Betriebsmaster und globaler Katalog	58	14.6 Datenträger und Speicherpools	141
7.5 Organisationseinheit – OU	59	15 Drucker verwalten	143
7.6 Standorte im Active Directory	60	15.1 Drucken im Netzwerk	143
7.7 Sysvol	61	15.2 Drucker installieren	145

15.3 Drucker konfigurieren	149	20 Datenträger verwalten	194
15.4 Druckerwarteschlange verwalten	151	20.1 Datenträger	194
15.5 Druckaufträge verwalten	152	20.2 Datenträgerverwaltung	195
15.6 Berechtigungen und Gruppen verwalten	154	20.3 Dateisysteme und Konvertierung	198
16 Gruppenrichtlinien	157	20.4 Datenträger pflegen	199
16.1 Gruppenrichtlinienobjekt (GPO, Group Policy Object)	157	20.5 Schattenkopien einsetzen	200
16.2 Verarbeitung der Gruppenrichtlinienobjekte	159	20.6 Speicherplätze (Storage Spaces)	201
16.3 Gruppenrichtlinieneinstellungen konfigurieren	162	20.7 Speicherpools und virtuelle Datenträger einrichten	203
16.4 Gruppenrichtlinienergebnisse	164	21 Datensicherung	207
16.5 Gruppenrichtlinienimplementierung planen	165	21.1 Sicherungsarten und -strategien	207
16.6 Zusätzliche Kontorichtlinie erstellen	167	21.2 Regelmäßige Datensicherung	208
17 Benutzerprofile verwalten	169	21.3 Sicherung wiederherstellen	212
17.1 Personalisierung der Arbeitsumgebung	169	22 System wiederherstellen	215
17.2 Servergespeicherte Benutzerprofile	171	22.1 Strategien und Wiederherstellungsfunktionen	215
17.3 Servergespeicherte Profile implementieren	173	22.2 Optionen des Systemstarts	215
18 Server überwachen	177	23 Active Directory-Objekte wiederherstellen	219
18.1 Überwachung und Leistungsanalyse	177	23.1 Überblick und Hintergründe	219
18.2 Ereignisanzeige	180	23.2 Active Directory-Objekt autorisierend wiederherstellen	221
18.3 Ereignisabonnements	182	23.3 Alternative Methoden zur Wiederherstellung	224
18.4 Leistungsdaten und der Systemmonitor	184	23.4 Active Directory-Papierkorb	226
19 Die Registrierungsdatenbank	188	Stichwortverzeichnis	228
19.1 Die Windows Server-2022-Registrierung	188		
19.2 In der Registry arbeiten	189		
19.3 Schlüsselsicherheit verwalten	191		
19.4 Regedit, die Kommandozeile und hilfreiche Tools	193		

1 Informationen zu diesem Buch

1.1 Voraussetzungen und Ziele

Zielgruppe

Angesprochen werden (zukünftige) Netzwerkadministratoren, deren Hauptaufgaben im Auf- oder Ausbau und der fortlaufenden Administration eines Active Directory-(Domänen-)Netzwerks unter Windows Server 2022 bestehen. Dabei sind Vorkenntnisse in anderen Windows-Serverbetriebssystemen wie z. B. Windows Server 2012 R2 oder 2019 hilfreich, aber nicht notwendig.

Empfohlene Vorkenntnisse

Erfahrungen in der Konfiguration und Bedienung von Windows-Clients und auf ihnen laufenden Anwendungen sowie eine grobe Vorstellung von der Funktionsweise von Computernetzen.

Lernziele

Das Buch vermittelt Ihnen zunächst einen allgemeinen Überblick über die Aufgaben von Servern und ihre Rolle im Netzwerk. Nach dem Durcharbeiten des Buches sind Sie in der Lage, Windows Server 2022 zu installieren und einzurichten. Sie wissen, wie Sie verschiedene Dienste für die Clients bereitstellen, das Active Directory verwenden und Benutzerkonten verwalten. Neben den alltäglichen Administrationsaufgaben beherrschen Sie auch die Systemwiederherstellung oder die Wiederherstellung gelöschter Active Directory-Konten.

Hinweise zu Soft- und Hardware

Für die meisten Kapitel genügt ein einzelner Windows Server 2022. Wenn Sie jedoch alle Beispiele und Konfigurationen im Buch nachvollziehen wollen, benötigen Sie drei Installationen von Windows Server 2022 und einen Rechner mit Windows 10 oder 11, um die Gruppenrichtlinieneinstellungen zu testen. Die Rechner müssen über ein Netzwerk verbunden sein.

Der gesamte Aufbau lässt sich auf einem einzelnen Rechner mit mindestens 8 GB RAM in einer virtualisierten Umgebung erstellen. Es wird empfohlen, als Host-Betriebssystem Windows Server 2022 und das enthaltene Hyper-V zu verwenden. Auch in Windows 10 / 11 Pro und Enterprise ist Hyper-V enthalten. Sie können aber auch ein anderes Betriebssystem verwenden und die Virtualisierung mit Zusatzsoftware, wie beispielsweise VirtualBox von Oracle (<https://www.virtualbox.org>), realisieren.

Sie benötigen einen Windows Server 2022 Installationsdatenträger (DVD oder USB-Stick), der die Standard- und Datacenter-Edition enthält. Diesen können Sie als Evaluierungsversion von der Microsoftwebseite herunterladen:

(<https://www.microsoft.com/de-de/evalcenter/evaluate-windows-server-2022>)

Dieses Buch bezieht sich auf die Verkaufsversion von Windows Server 2022. Beschrieben werden die funktionsgleichen Editionen Standard und Datacenter, die sich nur im Hinblick auf ihre Lizenzierung unterscheiden. Die günstigere Edition Essentials verfügte bis Windows Server 2016 über eine eigene Bedienoberfläche und einen reduzierten Funktionsumfang. Daher sind die Beschreibungen und Anleitungen aus diesem Buch nur teilweise darauf anwendbar. In Windows Server 2022 bietet die Essentials-Edition die gleiche Oberfläche wie die Standard-Edition.

1.2 Aufbau und Konventionen

Inhaltliche Gliederung

An erster Stelle steht das Kennenlernen des Betriebssystems Windows Server 2022, dann folgen die Installation und Anpassung des Betriebssystems. Nach einer Einführung in Active Directory wird eine Domäne aufgebaut. Anschließend wird diese zum Leben erweckt, indem Benutzer und Gruppen sowie Active Directory-Objekte angelegt und deren Berechtigungen konfiguriert werden. Es folgen die Bereitstellung von Ressourcen im Netzwerk (Speicherplatz, Drucker etc.) sowie das Festlegen von Richtlinien für deren Nutzung. Administrative Alltags-tätigkeiten wie die Fern- oder Festplattenverwaltung, Datensicherung und die Wiederherstellung eines Rechners im Notfall runden das Buch ab.

Typografische Konventionen

Im Text erkennen Sie bestimmte Programmelemente an der Formatierung:

<i>Kursivschrift</i>	kennzeichnet alle vom Programm vorgegebenen Bezeichnungen für Schaltflächen, Dialogfenster, Symbolleisten, Menüs bzw. Menüpunkte sowie Datei- und Verzeichnisnamen und Internetadressen.
Courier	wird für Benutzereingaben verwendet.
Spitze Klammern <>	kennzeichnen Platzhalter.

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 die HERDT-Bücher:
 - ✓ *Windows Server 2022 – Netzwerkadministration*
 - ✓ *Windows Server 2022 – Erweiterte Netzwerkadministration*
 - ✓ *PowerShell – Grundlagen und Verwaltung des Active Directory*
- ✓ Administrationskenntnisse von Clientbetriebssystemen vertiefen. Hierzu bieten wir Ihnen z. B. das Buch *Windows 10 / 11 Systembetreuer: Workstation* an.
- ✓ Netzwerkkenntnisse vertiefen. Dazu bietet Ihnen der HERDT-Verlag folgende Bücher:
 - ✓ *Netzwerke – Grundlagen*
 - ✓ *Netzwerke – Netzwerktechnik*
 - ✓ *Netzwerke – Protokolle und Dienste*
 - ✓ *Netzwerke – Sicherheit*
 - ✓ *Netzwerke – IPv6 Internet Protocol Version 6*

Wir wünschen Ihnen viel Spaß und Erfolg mit diesem Buch.

Ihr Redaktionsteam des HERDT-Verlags

2 Das Betriebssystem Windows Server 2022

2.1 Windows Server 2022

Definition von Betriebssystemen

Betriebssysteme dienen als Mittler zwischen Computerhardware und Softwareprogrammen. Weiter stellen sie eine Schnittstelle für den Anwender zur Verfügung. Diese kann grafisch oder textbasierend sein. Mit steigender Leistungsfähigkeit der Hardware sind auch die Anforderungen an die Betriebssysteme gewachsen. Netzwerkfunktionalitäten für den Einsatz in komplexen Strukturen großer Firmen mit vielen Tausend Benutzern sind für Serverbetriebssysteme eine Selbstverständlichkeit. Diesen Bereich bedient Microsoft durch die Familie der Windows-NT-Systeme, deren jüngster Vertreter Windows Server 2022 ist.

Arbeitsplatz- bzw. Clientbetriebssysteme zielen auf den Einsatz in Privathaushalten und Betrieben. Die jüngsten Vertreter sind Windows 10 und aktuell Windows 11. Beide basieren auf die Weiterentwicklungen des Windows-NT-Betriebssystems. Die erhältlichen Home-Versionen eignen sich nur bedingt für die Zusammenarbeit mit Windows Server 2022.

Bei Windows 10/11 zeigt sich die neue Unternehmensstrategie von Microsoft, Neuerungen durch Updates in bestehenden Systemen schneller auf den Markt zu bringen, als dies bei den Versionswechseln zwischen Vorgängerbetriebssystemen der Fall war. Im Gegensatz zum kostenlosen Upgrade von Windows 10 zu 11 ist der Wechsel von Windows Server 2016/2019 auf Windows Server 2022 kostenpflichtig.

Editionen von Windows Server 2022

Für unterschiedliche Einsatzgebiete werden verschiedene Editionen von Windows Server 2022 angeboten. Sie unterscheiden sich hinsichtlich der unterstützten Hardware sowie der darin enthaltenen Funktionen. Die früheren Server Editionen Enterprise, Webserver und Small Business Server gibt es nicht mehr. Für Firmen mit nicht mehr als 25 Mitarbeitern und 50 Geräten ist die Edition Server Essentials vorgesehen. Die Editionen Standard und Datacenter unterscheiden sich besonders hinsichtlich der lizenzierten virtuellen Sitzungen und einiger Funktionen. Einen Vergleich der Editionen finden Sie hier:

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

Windows Server 2022 ist ausschließlich als 64-Bit-Version erhältlich. Die Mindestanforderungen für alle Editionen sind ein 64-Bit-Prozessor mit mindestens 1,4 GHz, 512 MB RAM (2 GB für die Installation mit grafischer Benutzeroberfläche) und wenigstens 32 GB freier Festplattenplatz. Hinzu kommen noch einige Prozessorfunktionen und eine Netzwerkkarte. Die empfohlenen Hardwarevoraussetzungen richten sich nach den Aufgaben und liegen **erheblich** darüber. Eine ausführliche Liste der Anforderungen ist auf der Webseite der Firma Microsoft verfügbar.

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

Edition	Einsatzgebiet
Windows Server 2022 Essentials	✓ Für Firmenumgebungen bis 25 Benutzer und 50 Geräte ✓ Reduzierter Funktionsumfang, keine Container-Technologie, keine Exchange-Lizenz
Windows Server 2022 Standard	✓ Standardvariante mit reduzierter Funktionalität im Bereich der Hochverfügbarkeit und Storage (keine geschützten VMs, keine Storage Spaces Direct), Lizenzen für zwei Virtualisierungsinstanzen und Hyper-V-Container inbegriffen ✓ Alle Funktionen, maximal 2048 Prozessorkerne auf 64 Sockeln, maximal 48 TB RAM

Edition	Einsatzgebiet
Windows Server 2022 Datacenter	✓ Für den Einsatz in großen Rechenzentren konzipiert; volle Funktionalität, unbegrenzte Anzahl von Serverlizenzen für Virtualisierungsinstanzen ✓ Alle Funktionen, maximal 2048 Prozessorkerne auf 64 Sockeln, maximal 48 TB RAM
Windows Server 2022 Datacenter Azure Edition	✓ Eine spezielle virtuelle Maschinenlizenz ✓ Betrieb auf Azure IaaS oder im Azure Stack HCI Cluster

Editionen und Lizenzen im Vergleich

Microsoft hat mit Windows Server 2022 die Storage-Funktionen automatisiert, die es gestatten, wichtige Daten auf den schnellsten Speichervolumen bereitzustellen, während weniger kritische Daten auf langsameren Geräten mit hoher Speicherkapazität bereitgestellt werden. Auch wurden die Reparaturzeiten von Speichern deutlich reduziert. Weiter gültig bleibt die Aussage, dass nur die Datacenter-Edition **alle** Funktionen bereitstellt. In der Standard-Edition gibt es auch weiterhin keine Storage Spaces Direct und die Speicherreplikate (Storage-Replica) sind auf ein einzelnes Volumen (max. 2 TB) beschränkt. Die bekannten Shield Virtual Machines / Fabrics sind in Server 2022 noch enthalten, werden jedoch nicht weiterentwickelt und wurden als veraltet definiert. Die anderen Funktionen hat Microsoft auch in der Standard-Edition integriert. Diese verfügt zum Beispiel ebenfalls über die Container-Technologie und das Nano-Image als Container.

Allerdings muss beim Einsatz der Hyper-V-Container darauf geachtet werden, dass eine Lizenz der Standard-Edition nur zwei Container erlaubt, da nur 2 VMs erlaubt sind.

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 8 Kerne. Setzen Sie einen Dual-Prozessor mit je acht Kernen ein, müssen Sie also 8 Lizenzen für diese 16 Kerne erwerben. Für jeden Kern mehr müssen Sie ein Core-Pack kaufen, damit alle Kerne lizenziert sind. In Windows Server 2022 Standard dürfen Sie pro Lizenz 2 VMs installieren, Windows Server 2022 Datacenter hat kein Limit. Hier müssen Sie lediglich alle Prozessorkerne des Servers lizenzieren. Lizenzen von Windows Server 2022 sind direkt auf die physische Hardware gebunden.

Standardinstallation mit grafischer Oberfläche

Dies ist die klassische Installationsart mit Windows-Desktop und dem Startmenü im Windows 10-Stil. Durch die grafische Oberfläche sind die Hardwareanforderungen geringfügig höher, dafür lassen sich sämtliche Einstellungen lokal vornehmen. Die Verwaltung erfolgt über den von Windows Server 2012/2012 R2/2016/2019 bekannten Server-Manager und zahlreiche Tools, Assistenten und Konsolen. Die Steuerung über Eingabeaufforderung und PowerShell ist ebenfalls möglich. Das neue Windows Admin Center, die webbasierte Verwaltung von Windows Servern, ist auch in Windows Server 2022 optional. Das Windows Admin Center ist ein getrennter Download und kein fester Bestandteil der Windows Server Edition.

Server-Core

Server-Core ist die von Microsoft bevorzugte Installationsart. Hier werden durch den Verzicht auf die grafische Benutzeroberfläche eine Verringerung des benötigten Speichers und eine erhöhte Sicherheit durch eine geringere Angriffsfläche erreicht.

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. Das Windows Admin Center bietet in diesem Bereich ebenfalls Möglichkeiten zur Verwaltung. Möglich ist auch eine Remoteverbindung. Für die Administration mit den Remoteserver-Verwaltungstools (RSAT) wird Windows 10 / 11 benötigt.

Hyper-V

Eine Sonderinstallationsform ist die Installation von Windows Server 2022 in einer virtuellen Maschine. Microsofts virtuelle Umgebung Hyper-V bietet die Möglichkeit, auf einem physikalischen Server zusätzliche virtuelle Server zu installieren. So können Sie beispielsweise sicherheitsrelevante Server-Dienste (z. B. Domänen-Controller, Zertifikatsdienste) auf separaten Servern betreiben werden. 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 nur in den Editionen Standard und Datacenter nutzbar. Beide Versionen verfügen über einen identischen Funktionsumfang und unterscheiden sich nur in der Anzahl der integrierten Lizenzen für virtuelle Betriebssysteme. Bei der Standard-Edition sind zwei weitere Lizenzen für virtuelle Server enthalten, beim Datacenter ist die Anzahl der virtuellen Instanzen nicht limitiert. Wer Hyper-V nutzen will, kann auch auf den kostenlosen Hyper-V-Server 2019 von Microsoft setzen. Dieser verfügt über einen Funktionsumfang der Datacenter-Edition für Hyper-V und wird als Core-Server installiert. Einen Hyper-V-Server 2022 gibt es nicht mehr.

Neuerungen in Hyper-V

Eine Reihe von Neuerungen, die unter Windows Server 2022 eingeführt wurden, betreffen virtuelle Maschinen und deren Verwaltung. Virtuelle Switches können nun den Datenverkehr bündeln und als Block übertragen, wodurch die CPU des Hostsystems entlastet wird. Nested Virtualization lässt sich nun auch mit AMD Prozessoren realisieren. Hierbei lassen sich bestimmte Technologien auch innerhalb von virtuellen Maschinen einsetzen, was besonders für Container Hosts interessant ist.

Container-Technologie Docker und Unterstützung für Kubernetes

Bei Docker handelt es sich um eine Lösung, die Anwendungen im Betriebssystem über Container virtualisieren kann. Anwendungen lassen sich dadurch leichter bereitstellen, da die Container mit den virtualisierten Anwendungen transportabel sind. Einfach ausgedrückt handelt es sich bei Docker-Containern um virtualisierte Serveranwendungen, die keinen Server und kein eigenes Betriebssystem benötigen. Vorteil dabei ist, dass virtuelle Docker-Container mit ihren Serveranwendungen die Möglichkeit bieten, exakt die Ressourcen zu verwenden, die benötigt werden. Hierfür werden sogenannte Nano-Installationen verwendet. Die Container-Technologie Docker kann mit der Verwaltungslösung Kubernetes (ein Open-Source Projekt) auch in Windows Server 2022 zusammenarbeiten. Dies war bis Windows Server 2016 noch nicht möglich.

Einsatzbereich

Das Einsatzgebiet von Windows Server 2022 sind Netzwerke, die über sogenannte Client-Server-Architekturen verfügen. In einem solchen Netzwerk gibt es generell zwei Typen von Computern: Clients (auch als Workstation oder Arbeitsplatzrechner bezeichnet), an denen gearbeitet wird, und Server, die ihre Dienste zur Verfügung stellen, z. B. zentrale Datenspeicherung, Benutzerverwaltung, Druckdienste oder Internetzugang. Das aktuelle Workstation-Betriebssystem ist Windows 11, allerdings müssen für die volle Unterstützung aller GPO-Einstellungen die administrativen Vorlagen nachinstalliert werden. Alternativ können Sie auch Clients mit älteren Windows-Versionen einsetzen, obwohl dies mit Ausnahme von Windows 10 nicht empfohlen wird. Ältere Systeme werden nicht mehr supportet und je nach Alter fehlen die Möglichkeiten, neuere Funktionen per GPOs zu konfigurieren.

2.2 Dateisysteme

Sicherheitskonzepte von Dateisystemen

Ein Dateisystem regelt die Art, wie Daten auf der Festplatte abgelegt werden. Im Windows-Serverbereich wird seit vielen Jahren ausschließlich NTFS eingesetzt, seit Server 2012/2012 R2 kommt ReFS hinzu. Beide Dateisysteme schützen die Daten vor unbefugtem Zugriff. Um Dateien lesen, verändern oder löschen zu können, müssen die Benutzer über die entsprechenden Berechtigungen verfügen. In Windows Server 2022 empfiehlt Microsoft das Dateisystem ReFs zur Speicherung von **Daten**.

Der Standard NTFS

Das NT File System (NTFS) wurde 1993 von Microsoft eingeführt und ist in seiner heutigen Version 3.1 seit etwa 15 Jahren unverändert im Einsatz. NTFS bietet ein feines System von lokalen Zugriffsberechtigungen und damit eine hohe Datensicherheit bei lokalem Zugriff. Im Gegensatz zum lokalen Zugriff steht der Zugriff auf Freigaben (freigegebene Ordner) über das Netz.

Die Sicherheitskonzepte, die dabei zum Einsatz kommen, sind die folgenden:

Sicherheit bei Netzwerkzugriff	Zugriffssicherheit wird auf Freigabeebene eingestellt. Benutzern wird das Recht erteilt, auf den Inhalt eines Ordners zuzugreifen. Lokal liegt keine Reglementierung vor.
Sicherheit bei lokalem Zugriff bzw. Sicherheit auf Dateiebene	Zugriffssicherheit auf der Ebene des Dateisystems. Vor jedem Zugriff erfolgt eine lokale Sicherheitsüberprüfung. Diese ist immer wirksam, setzt allerdings das Dateisystem NTFS voraus.
Sicherheit über dynamische Zugriffskontrolle (DAC, Direct Access Control) und Active Directory	Über DAC lassen sich Dateien nach Klassen (z. B. Benutzerdaten, Anwendungsdaten) gruppieren und so leichter verwalten. DAC funktioniert zurzeit nur mit NTFS, daher wird es hier aufgeführt.

Das robuste Dateisystem ReFS

Bei Windows Server 2012/2012 R2 ist mit dem **Resilient File System** (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.

Neben der automatischen Korrektur verursacht das Dateisystem keine langen Ausfallzeiten mehr durch Reparaturmaßnahmen. Reparaturen lassen sich im laufenden Betrieb durchführen. Stundenlange Reparaturorgien gehören der Vergangenheit ein. In ReFS lassen sich Metadaten und Prüfsummen von Dateien wesentlich effizienter integrieren als in Vorgängerversionen. Das Dateisystem protokolliert Änderungen in Dateien und kann ursprüngliche Änderungen speichern.

Daher wird ReFS für die Verwendung bei Dateiservern empfohlen. Die Windows Startpartition muss jedoch weiterhin in NTFS formatiert werden, da der Systemstart mit ReFS noch nicht möglich ist.

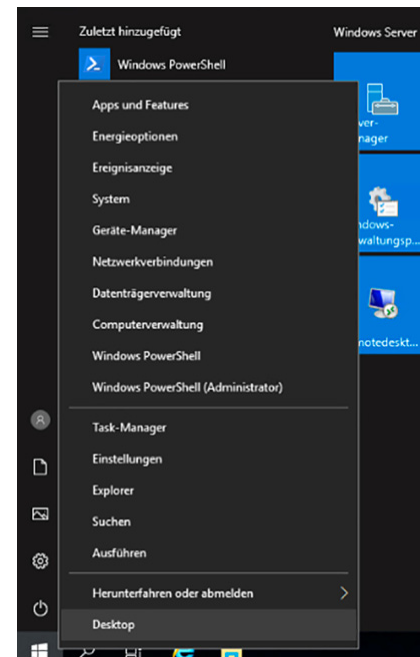
2.3 Startmenü

Das Startmenü von Windows Server 2022 entspricht im Wesentlichen dem mit Windows 10 eingeführten Stil. Der Startbildschirm aus früheren Windows Server-Editionen wurde schon mit Windows Server 2019 wieder abgeschafft und ist daher auch nicht im Server 2022 zu finden.

Bedienung des Startmenüs

Auf dem Desktop gibt es den Start-Button und ein **Schnellzugriffsmenü**, das Sie über einen Rechtsklick in die linke untere Ecke oder über   öffnen können. Von hier aus haben Sie Zugriff auf die wichtigsten Einstellungen von Windows Server 2022.

Die farbigen Rechtecke auf der Windows-Oberfläche werden als **Kacheln** oder **Tiles** bezeichnet. Jede farbige Kachel repräsentiert dabei eine App, während alle Kacheln mit einem Desktop-Icon für eine Desktop-Anwendung stehen. Wechseln Kacheln den angezeigten Inhalt, werden sie auch **Live-Kacheln** oder **Live Tiles** genannt. In Windows Server-Editionen werden die Kacheln allerdings nicht animiert.



Schnellzugriffsmenü

2.4 Windows Server 2022 mit Tastenkombinationen bedienen

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 mehrere Bildschirme
 X	Öffnet das Schnellzugriffsmenü
 K	Öffnet die Seite zum Verbinden von Geräten
Suchen	
 Q	Nach Dateien und Anwendungen suchen
Sonstiges	
 D	Zeigt den Desktop
 Druck	Speichert einen Screenshot im PNG-Format in <i>Bilder</i>
 Pause	Öffnet die Systemeigenschaften
 R	Befehl ausführen
 E	Öffnet ein Explorer-Fenster

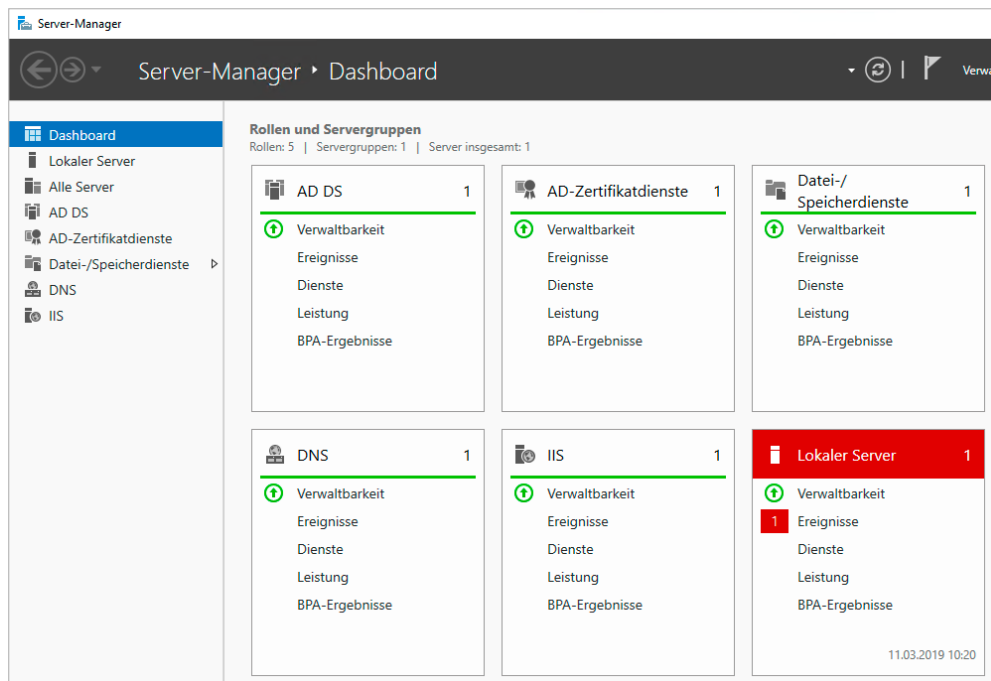
2.5 Server-Manager und Windows Admin Center

Der Server-Manager dient zur Überwachung für einen oder mehrere Server und ist geeignet, um neue Rollen (z. B. DNS-Server, Hyper-V, Domänencontroller) und Features (z. B. Bitlocker, BranchCache) hinzuzufügen und grundlegende Einstellungen vorzunehmen.

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 lediglich während der Einrichtung des Servers erscheinen.

Auch durch das neue Windows Admin Center wird der Server-Manager nicht ersetzt. Das webbasierte Verwaltungswerkzeug muss bei Microsoft gesondert heruntergeladen und installiert werden. Mehr zum Windows Admin Center finden Sie auf der Webseite von Microsoft:

<https://www.microsoft.com/de-de/windows-server/windows-admin-center>



Server-Manager mit dem Dashboard

Zentrale Verwaltungsschnittstelle

Der Server-Manager ist in der Version ab Windows Server 2012/2012 R2 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 Startmenü aufrufen. Über den Server-Manager lassen sich Remoteserver genauso überwachen wie der lokale Server.

Weitere Neuerungen gegenüber der Windows Server 2008-Familie im Überblick

Neuere Windows Server-Editionen bieten zahlreiche kleine und große Veränderungen. Hier sind einige davon aufgelistet:

Oberfläche

- ✓ Neue Windows-Oberfläche
- ✓ Neuer Boot-Manager und neu gestaltete Startoptionen

Funktionalität

- ✓ Vollkommen neu gestalteter Server-Manager
- ✓ Verbessertes Failover-Clustering für erhöhte Verfügbarkeit
- ✓ Neuer Task-Manager, verbesserter Dialog für das Kopieren und Verschieben von Dateien
- ✓ Windows-Explorer mit Menüband (Ribbon)
- ✓ Neue Treiberklassen für USB 3.x und viele andere Geräte
- ✓ Neue PowerShell-Versionen
- ✓ Kleinere Nano Server Images

Datenspeicherung und Virtualisierung

- ✓ Verbesserte Virtualisierung mit zahlreichen Neuerungen, z. B. VMs der zweiten Generation Shared VHDX, geschützte VMs
- ✓ Verbesserte Virtual-Desktop-Infrastruktur (VDI) und Remote Desktop Services (RDS)
- ✓ ReFS, der NTFS-Nachfolger, und iSCSI-Unterstützung
- ✓ Virtuelle Speicherplätze mit Speicherpools und virtuellen Datenträgern
- ✓ Windows Assessment and Deployment Kit (ADK) als Nachfolger von WAIK und OPK
- ✓ Verbesserte Windows-Bereitstellungsdienste (WDS)

Sicherheit

- ✓ Verbesserte BitLocker-Verschlüsselung
- ✓ SmartScreen-Schutz (systemweit)
- ✓ Dynamische Zugriffskontrolle (Dynamic Access Control, DAC), um Zugriffsrechte über Dateiklassen zu regeln
- ✓ Nachinstallierbare administrative Vorlagen für viele Softwareprodukte (ADMX)

3 Netzwerk mit Windows

3.1 Grundlagen des Netzbetriebes

Aufbau von Netzwerken

Zur gemeinsamen Nutzung von (Netzwerk-)Ressourcen (z. B. Druckern oder gemeinsame Dateiablagen) werden Computer in Verbünden eingesetzt. Um diese Ressourcen zentral zugänglich zu machen, bedarf es Netzwerkfunktionalitäten. Die Organisation/Verwaltung der Rechner in Windows-Netzen erfolgt dabei entweder anhand des Arbeitsgruppen- oder des Domänen-Modells.

Grundlagen der Datenkommunikation

Voraussetzung für den Informationsaustausch zwischen Computern sind verschiedene Komponenten. Eine kurze Erklärung wichtiger Komponenten erfolgt jetzt anhand der **Analogie Telefon**. Zum Telefonieren benötigen Sie:

- ✓ Einen Telefonapparat, der Schallwellen in elektrische Signale und wieder zurückverwandelt
Netzwerkadapter sind die Entsprechung bei Computersystemen. So wie es beim Telefon analoge, ISDN- oder VoIP-Anschlüsse gibt, gibt es auch bei Netzwerkkarten verschiedene Übertragungsverfahren. In lokalen Netzen (LAN, Local Area Network) werden fast ausschließlich Ethernet-Adapter eingesetzt.
- ✓ Ein Übertragungsmedium zum Weiterleiten der Signale: Anschluss mit Kabel oder schnurlos über Funk
In kabelgebundenen LANs wird jeder PC mit einem Twisted-Pair-Kabel angeschlossen, das andere Kabelende wird in der Regel mit einem Verteilerknoten (Switch) verbunden. Für die Kommunikation über Funk stehen WLAN Adapter und Access Points zur Verfügung.
- ✓ Eine Telefonnummer zur Adressierung der Teilnehmer
IP-Adressen übernehmen diese Aufgabe in Computer-Netzwerken. Wie beim Telefon gibt es eine Vorwahl (Netz-ID) und eine Telefonnummer (Host-ID). Näheres dazu finden Sie nachfolgend.
- ✓ Vermittlungsstellen/Verteilerknoten, die die Telefonate weiterleiten
Bei Ortsgesprächen (identische Netz-ID) schalten Switches die beiden Kommunikationspartner direkt zusammen. Anders als im Telefonnetz gibt es hier auch sogenannte Broadcasts: Rundrufe an alle. Bei Ferngesprächen (unterschiedliche Netz-IDs) werden immer Router benötigt, um die Datenpakete ins richtige Teilnetz weiterzuleiten.
- ✓ Eine gemeinsame Sprache, ohne die die Gesprächspartner sich nicht verständigen können
Der Protokoll-Stapel TCP/IP (Transmission Control Protocol/Internet Protocol) ist der etablierte Standard.

Übertragungsgeschwindigkeiten

Übertragungsgeschwindigkeiten werden in Bit pro Sekunde angegeben. Die häufigsten Geschwindigkeiten im kabelgebundenen Ethernet-Bereich sind 100 MBit/s (Fast Ethernet), 1 GBit/s (Gigabit Ethernet) und 10 GBit/s.

Funknetze/WLANs (Wireless LAN) arbeiten mit Brutto-Übertragungsraten von 54 MBit/s bis 600 MBit/s. Die tatsächlichen Datenübertragungsraten liegen bei maximal 40 % der Bruttowerte. Bei schlechten Funkverbindungen, vielen verbundenen Teilnehmern und Störungen durch umliegende Funknetze liegen die Nettowerte noch erheblich darunter.

Arbeitsgruppe

Arbeitsgruppen werden auch als Peer-to-Peer-Netzwerke bezeichnet. Hier sind alle Computer gleichberechtigte Partner. Eine zentrale Verwaltung von Benutzern, PCs, Einstellungen usw. ist nicht vorgesehen, sie muss auf jedem Rechner einzeln erfolgen.

Das Arbeitsgruppen-Konzept eignet sich nur für sehr kleine Netzwerke mit maximal 10 Benutzern. Ein Beispiel: Sollen 10 Benutzer mit eigenen Benutzerkonten an 10 verschiedenen PCs arbeiten können, müssen Sie bereits 100 Benutzerkonten verwalten.

Nach der Installation ist jeder Windows-Rechner automatisch Mitglied einer Arbeitsgruppe.

Windows-Domäne

Eine Windows-Domäne ist eine Verwaltungseinheit, über die viele Aufgaben zentralisiert werden. Benutzer- und Gruppenkonten werden nicht mehr lokal auf den Computern gespeichert, sondern zentral in der Domäne angelegt und administriert. Auch Computer verfügen über ein Konto in der Domäne und werden so in das Sicherheitskonzept eingebunden.

Windows-Domänen werden durch sogenannte Domänencontroller (DCs) erstellt bzw. verwaltet. Hierbei handelt es sich um eine Rolle, die nur auf einem Windows-Server ausgeführt werden kann. Da Domänencontroller zentrale Komponenten für den Netzwerkbetrieb sind, sollten Sie nach Möglichkeit mehrere DCs bereitstellen, um gegen einen Ausfall geschützt zu sein. Domänencontroller einer Windows-Domäne gleichen ihre Domänen-Informationen automatisch untereinander ab. Dieser Vorgang wird als Replikation bezeichnet.

Client-Server-Aufgabenverteilungen

Verschiedene Computer übernehmen unterschiedliche Aufgaben in einem Netzwerk. Einige der möglichen Rollen zeigt die folgende Tabelle:

Arbeitsplatzrechner oder Workstation	Computer mit Client-Betriebssystem, z. B. Windows 11, die die Ausführung von Software und den Zugriff auf Netzwerkressourcen erlauben, die von den Servern zur Verfügung gestellt werden. Als Workstation werden im Allgemeinen besonders leistungsfähige Arbeitsplatzrechner bezeichnet, die beispielsweise für CAD oder Videobearbeitung eingesetzt werden und preislich deutlich über einem Arbeitsplatzrechner liegen können.
Domain Controller (Domänencontroller)	Der Domänencontroller hat die Aufgabe, die Zugriffe auf das Netzwerk und seine Komponenten zu regulieren. Auf ihm werden die Benutzerverwaltung und die Sicherheitsstruktur des Domänen-Netzwerkes festgelegt und auf allen Servern sowie Clients der Domäne durchgesetzt.
Fileserver	Der Fileserver stellt Dateien im Netz zur Verfügung. Benutzer können so von jeder Arbeitsstation aus auf ihre Daten zugreifen. In kleinen Umgebungen können hierfür auch Computer mit Windows-Client-Betriebssystemen verwendet werden.
DHCP-Server	Weist allen Clients im Netz automatisch eine IP-Adresse zu
DNS-Server	Löst die Namen von Rechnern und den ihnen zugeordneten Diensten wie mail , www oder ftp in IP-Adressen auf, die vom Computer verarbeitet werden können
Print-Server	Zentralisierte Druckdienste und Verwaltung und Bereitstellung von Netzwerkdruckgeräten
Proxyserver	Der Proxyserver vermittelt stellvertretend für einen Benutzer oder PC die Zugriffe auf das Internet. Seiteninhalte werden häufig zwischengespeichert, die dadurch nicht jedes Mal neu aus dem Internet bezogen werden müssen. Auch sind auf ihm Sicherheitsmechanismen integriert, die den Zugang vom und zum World Wide Web regulieren (Firewall-Funktionen/Inhaltsfilterung/Protokollierung).

Terminalserver	Eine besondere Rolle hat der Terminalserver. Er stellt Clients seine Rechenkapazität zur Verfügung, indem auf ihm Programme laufen, die vom Client (Terminal) aus gesteuert werden können. Ein typisches Einsatzgebiet sind städtische Informationssysteme oder Banken, bei denen dem Mitarbeiter nur der Bildschirm und seine Peripherie (Maus/Tastatur u. a.) für die Bedienung zur Verfügung steht.
Sonstige Aufgaben	Backup-, Datenbank-, Mail-, Web- oder Streaming-Server u. a.

Die verschiedenen Servertypen müssen nicht auf verschiedenen Computern ausgeführt werden. Ein Domänencontroller kann durchaus auch als Datei- und Druckserver dienen, wenn die Leistung des Rechners dies erlaubt.

Die Begriffe Client und Server führen gelegentlich zu Verwirrung. Die Zuordnung der Rechner-Hardware ist meist eindeutig, anders ist es jedoch, wenn es um die Funktion geht. Auch ein Client-Rechner kann z. B. einen Ordner oder Drucker im Netzwerk freigeben und agiert damit als File- oder Print-Server. Gleichzeitig ist er Domänen-Client, der über DCs verwaltet wird. Letztlich stellt jeder Server auf Anfrage den Clients bestimmte Funktionen zur Verfügung. Jede Client-Server-Kommunikation stammt dabei ursprünglich vom Client.

3.2 TCP/IP

TCP/IP bezeichnet ein Protocol-Stack (Protokoll-Stapel), also eine Sammlung 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 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 die noch fehlende Notwendigkeit zur Umstellung.

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 zu einer Folge von Nullen wechselt. 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 binär als eine Folge von 24 Einsen und 8 Nullen 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 (**C**lassless **I**nter-**D**omain **R**outing) 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)
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: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. 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. 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. Möchte 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 unterschiedlich sein (z. B. Glasfaser, Kupferkabel, Funk, Licht)

Standardgateway

Das Standardgateway ist der Default-Router, den ein PC oder Server benutzt, wenn er Datenpakete an Rechner mit einer anderen Netz-ID sendet und über keine Informationen bezüglich der zu benutzenden Wege verfügt. Am häufigsten wird das Standardgateway die Verbindung zum Internet zur Verfügung stellen.

3.3 Vergabe von IP-Adressen

Identifikation im Netzwerk

Generell werden zur Identifikation eines Rechners im Netzwerk drei Informationen benötigt:

- ✓ Die MAC-Adresse (**M**edia **A**ccess **C**ontrol) 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. Ein NetBIOS-Name besteht aus maximal 16 Zeichen, wobei das 16. Zeichen bei Microsoft ein Suffix ist, der den Typ des Gerätes/Dienstes definiert.

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 fordern ihre IP-Konfiguration beim DHCP-Server an. 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 (**A**utomatic **P**rivate **I**P **A**ddressing). 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 (**D**omain **N**ame **S**ystem) 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, da die Notation der Webadressen und der Betrieb auf DNS basiert.

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 Dienstimplementierungen. In modernen Netzwerken ist ein WINS-Server dagegen nicht mehr notwendig.

3.4 Verzeichnisdienste

Aufgabe von Verzeichnisdiensten

Verzeichnisdienste haben die Aufgabe, die Ressourcen eines Netzwerks für alle 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. **Selektiv verfügbar** bedeutet **Verwenden auf bestimmte, definierte Weise**, was auch **gar nicht verwenden** einschließt. Mit **alle** schließlich sind sämtliche Personen gemeint, die auf Netzwerkressourcen zugreifen (beispielsweise über ein LAN oder das Internet).

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 Delegation von Verwaltungsaufgaben oder die Fernverwaltung);
- ✓ der Erweiterbarkeit des Dienstes, um beispielsweise die Fusion zweier Firmen realisieren zu können;
- ✓ der Flexibilität bei der Gestaltung, um beliebige Firmenstrukturen oder Hierarchien abzubilden;
- ✓ der Performance;
- ✓ dem Maß der Verfügbarkeit – auch bei Ausfall eines Teilsystems;
- ✓ Zusammenarbeit mit Verzeichnisdiensten anderer Hersteller;
- ✓ Unterstützung und Integration von internationalen Standards;
- ✓ der Berücksichtigung der Netzwerkinfrastruktur (schnelle/langsame Datenübertragungswege).

Active Directory

Das Active Directory sind die Verzeichnisdienste in Windows-Netzwerken. Beim Active Directory handelt es sich um eine hierarchische und verteilte Datenbank. Sie basiert auf Microsoft-eigenen Datenbank-Funktionen (ESE, Extensible Storage Engine, auch bekannt als JET Blue), die auch in Microsoft Exchange verwendet werden.

Leistungsmerkmale des Active Directory

Anzahl verwaltbarer Objekte	In einer Windows-Domäne können viele Millionen Objekte verwaltet werden.
Sicherheit	Das Authentifizierungsprotokoll Kerberos V5 und die verschiedenen Sicherheitskonzepte der Active Directory-Verzeichnisdienste bieten hervorragende Sicherheit.
Verwaltung	Sowohl die Delegation von Verwaltungsaufgaben als auch die Fernverwaltung werden durch die Active Directory-Verzeichnisdienste unterstützt.
Erweiterbarkeit	Die Erweiterung einer vorhandenen Struktur ist problemlos möglich.
Flexibilität	Hohe Flexibilität und Erweiterbarkeit durch Verschachtelungen Sie haben die Möglichkeit, Hierarchien mit mehr als zwei Stufen zu bilden.
Performance	Hohe Performance, z. B. durch Begrenzung der zu übertragenden Datenmengen
Verfügbarkeit	Hohe Verfügbarkeit wird durch die Bereitstellung von Redundanz der Verzeichnisinformationen erreicht.
Interoperabilität	Windows bietet Unterstützung für die weitverbreiteten Verzeichnisdienste der verschiedenen Hersteller. Active Directory-Funktionen werden über standardisierte Schnittstellen zur Verfügung gestellt.

Unterstützung von Standards	Unterstützung aller internationalen Standards, die momentan für den Netzwerkbetrieb in LAN und WAN etabliert sind
Bezug auf die Netzwerkinfrastruktur	Berücksichtigung von Geschwindigkeiten verschiedener Übertragungswege bei der Häufigkeit der Übertragungen von Verzeichnisinformationen

3.5 Verwaltungsfunktionen

Windows-Deployment-Dienste (Windows Deployment Services, WDS)

Die Windows-Deployment-Dienste ermöglichen eine automatische Bereitstellung von Betriebssystemen zur schnellen Installation von Arbeitsplatzrechnern, Workstations und Servern. Wesentliche Elemente dieses Verfahrens sind die Speicherung eines Abbildes einer Workstation mit der gewünschten Konfiguration (Image) auf einem WDS-Server und die Installation des Betriebssystems über das Netzwerk.

Gruppenrichtlinien – GPOs (Group Policy Objects)

GPOs sind ein mächtiges Verwaltungsinstrument unter Active Directory. Mit ihnen können die Desktops der verschiedenen Benutzer verwaltet werden und Anwendungen von zentraler Stelle aus auf Workstations verteilt werden.

Microsoft Management Console (MMC)

MMC ist eine Verwaltungsplattform, mit der Sie verschiedene Programme zur Verwaltung (Snap-Ins) aufrufen und in einer Oberfläche zusammenfassen können. Sie können die MMC anpassen, indem Sie nur solche Tools aufnehmen, die Sie zur Ausführung der Verwaltungsarbeiten benötigen.

Windows PowerShell

Die PowerShell ergänzt die alte CMD.EXE-Eingabeaufforderung und ist mit ihren vielfältigen Befehlen, Programmiermöglichkeiten und Verknüpfungsoptionen ein mächtiges Werkzeug für den Systemadministrator.

Windows Management Interface (WMI)

Das WMI ist eine Software-Schnittstelle, mit der Verwaltungsprogramme von entfernten Systemen aus aufgerufen werden können. Mit WMI können Sie viele Einstellungen eines Computers abfragen oder konfigurieren.

Terminal Services (Remote Desktop)

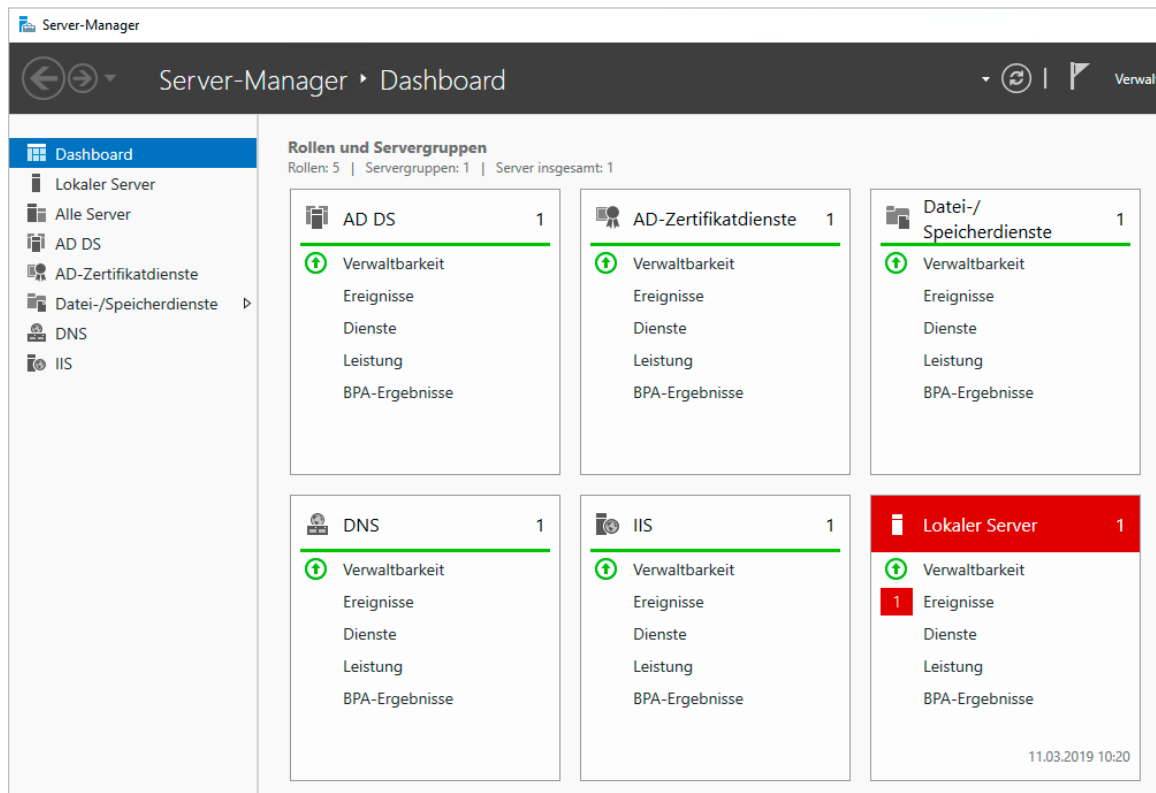
Terminaldienste ermöglichen Benutzern den Fernzugriff auf einen Computer. Die aktuellere Bezeichnung für die Terminal Services ist der Remote Desktop. Sie übertragen nur die Benutzeroberfläche eines Programms auf den Arbeitsplatz des Benutzers. Der Terminalserver übernimmt die gesamte Rechenleistung für die Datenverarbeitung. Die Terminal Services sind in jeder Edition von Windows Server 2022 integriert. Für die Arbeit aus der Ferne können sich Benutzer über VPN mit dem Netzwerk verbinden und Anwendungen auf Remote Desktop Servern starten.

Server-Manager

Mit Windows Server 2012/2012 R2 wurde ein neuer Server-Manager eingeführt. Er stellt die zentrale Verwaltungsplattform aller Server eines Netzwerks unter einer einheitlichen Oberfläche bereit. Der Server-Manager funktioniert in Windows Server 2022 identisch wie in den Vorgängerversionen 2019, 2016 und 2012.

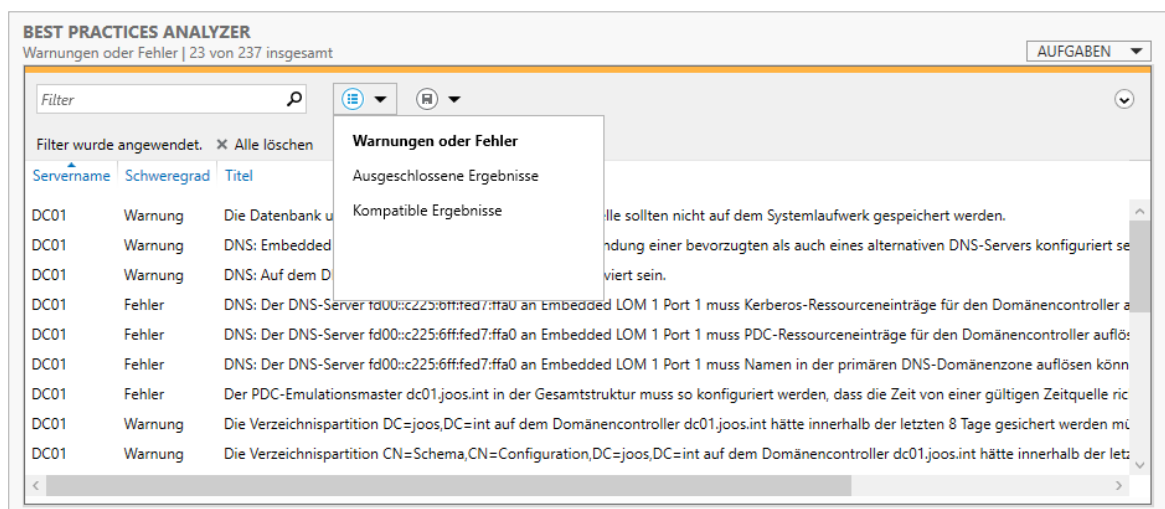
Der Server-Manager präsentiert auf übersichtliche Weise die benötigten Informationen, zeigt relevante Ausschnitte aus der Ereignisanzeige und bietet direkten Zugriff auf zahlreiche Assistenten.

Auf der Titelseite des Server-Managers, dem Dashboard, können Sie neue Rollen und Features hinzufügen und den Status der einzelnen Rollen auf einen Blick erfassen. Anstehende Verwaltungs- und Installationsaufgaben werden mit dem Fähnchen und zusätzlichen Warnsignalen angezeigt.



Jede Serverrolle erhält eine eigene Seite, wie z. B. das AD DS. Einige Rollen werden weiter unterteilt, wie z. B. die Datei- und Speicherdienste.

Bei jeder Rolle werden Ereignismeldungen, der Status der beteiligten Dienste sowie die Auslastung angezeigt. Der **BEST PRACTICES ANALYZER** überprüft die Konfiguration und gibt Hinweise zu potenziellen Problemen und Engpässen.



4 Windows Server 2022 installieren

4.1 Vorbereitungen

Hardware-Voraussetzungen

Die Angaben zur Mindestausstattung basieren auf den Informationen des Software-Herstellers. In der Praxis sind die Anforderungen je nach Investitionsvolumen, Einsatz des Rechners als hochleistungsfähiger Server und Datenaufkommen im Netzwerk deutlich höher.

Wenn Sie einen virtuellen Server in einer Hyper-V mit dem minimalen Speicher von 512 MB zu installieren versuchen, erhalten Sie eine Fehlermeldung.

Hardware	Minimale Ausstattung
Prozessor	1.4 GHz 64-Bit-Prozessor, 64-Bit-Kompatibilität, NX und DEP
Hauptspeicher	Min. 512 MB / 2 GB (GUI)
Festplattenlaufwerk	32 GB freier Speicherplatz
Sonstiges	DVD-ROM, mindestens X VGA-Auflösung (1024 × 768), Maus, Tastatur, Internetzugang

Stellen Sie zumindest für den Installationszeitraum mehr als 800 MB Speicher bereit. Virtuelle Server, deren Speicher unter 800 MB liegt, sollten zwar in der Praxis keine Rolle spielen, können jedoch gerade in Testumgebungen wichtig werden.

Die Mindestausstattung freier Festplattenspeicherplatz von 32 GB gilt nur für Systeme mit weniger als 16 GB Speicher. Bei mehr RAM muss für die Auslagerungsdatei entsprechend mehr Festplattenspeicherplatz zur Verfügung stehen. Zu empfehlen ist mindestens das Doppelte des Hauptspeichers.

Upgrade oder Neuinstallation

Upgrade-Installationen aktualisieren ein vorhandenes Betriebssystem auf eine neuere Version. Sie bieten den Vorteil, dass bereits vorhandene Installationen und Konfigurationen übernommen werden. Vor einem Upgrade müssen Sie überprüfen, ob Windows Server 2022 die vorhandene Soft- und Hardware unterstützt. Erstellen Sie vor einem Upgrade unbedingt ein Backup.

Es folgt eine Übersicht, welche Upgrade-Pfade möglich sind:

- ✓ Upgraden können Sie prinzipiell nur von einem 64-Bit-Betriebssystem.
- ✓ Windows Server 2022 ermöglicht ein direktes Upgrade der vorherigen Windows Server-Edition. Ein Upgrade von älteren Windows-Servern ist nur über mehrere Schritte zur jeweils nächsten Version möglich. Beachten Sie hierbei auch die entstehenden Kosten, die das Upgrade zu Windows 2022 verursachen würde.
- ✓ Durch Eingabe eines neuen Produktschlüssels lässt sich Windows Server 2022 Standard auf Datacenter upgraden.
- ✓ Upgrades sind nur auf dieselbe oder eine höhere Edition möglich, z. B. von einer Standard-Edition auf Standard oder Datacenter, jedoch nicht umgekehrt.
- ✓ Die Sprachversion muss beibehalten werden.



Vor dem Upgrade eines Domänencontrollers müssen Sie sicherstellen, dass das Active Directory-Schema aktualisiert wurde.

Upgrade-Installationen benötigen deutlich mehr freien Speicherplatz auf Ihrem Systemlaufwerk und dauern länger als Neuinstallationen. Auf der anderen Seite bleiben alle Daten und Einstellungen der Domäne erhalten.

Hardware-Komponenten im Rechner

Verwenden Sie bevorzugt Hardware, die für Windows Server 2022 zertifiziert ist. Microsoft stellt für die Recherche eine Hardware-Datenbank zur Verfügung (<http://www.windowsservercatalog.com>). Stellen Sie sicher, dass für verwendete Hardware passende Treiber vorhanden sind.

Installationsart wählen

Windows Server kann auch weiterhin von optischen Medien installiert werden. Einen Testbetrieb ohne gültigen Produktschlüssel gibt es nur für wenige Tage, aber schon bei der Installation sollte der Server aktiviert werden. Eine Neuinstallation ist in wenigen Minuten abgeschlossen.

Die Installation von einer DVD-ROM ist die Standardmethode, von einem USB-Stick geht es noch ein wenig schneller. Microsoft bietet zwei ISO-Abbilder für die Installation der Editionen von Windows Server 2022 zum Download an: eines für die Editionen Standard und Datacenter und ein weiteres für die Windows Server 2022 Essentials. Diese können Sie entweder direkt verwenden, auf DVD brennen oder für die Erstellung eines USB-Installationsmediums nutzen.

180-Tage-Evaluierungsversion

Microsoft bietet den Windows Server 2022 als Evaluierungsversion für 180 Tage zum kostenlosen Download an. Diese können Sie in eine lizenzierte Vollversion umwandeln. Sie können den Testzeitraum nicht verlängern.

Microsoft verwendet die Ausdrücke Evaluierungsversion und Testversion synonym.

Die Evaluierungsversion ist kostenlos als ISO-Image zum Download erhältlich unter <https://www.microsoft.com/de-de/evalcenter>. Sie benötigen ein Microsoft-Konto für die Registrierung.

USB-Stick für Windows Server 2022 erstellen

Liegen Ihnen die Windows Server 2022-Installationsdateien im ISO-Format vor, können Sie die ISO-Datei im Betriebssystem bereitstellen und auf deren Basis einen bootfähigen USB-Stick erstellen. Damit die Image-Datei von Windows Server 2022 (*install.wim*) auf einen USB-Stick mit dem FAT32-Dateisystem passt, müssen Sie diese aufteilen. Ansonsten können Sie die Datei nicht immer kopieren. Das Aufteilen ist aber kein komplizierter Vorgang.

Der Befehl dazu sieht zum Beispiel folgendermaßen aus:

```
Dism /Split-Image /ImageFile:f:\sources\install.wim /SWMFile:c:\temp\install.swm /FileSize:3600
```

Die beiden Dateien können dann anstatt der Datei *install.wim* aus dem Verzeichnis „sources“ auf den USB-Stick kopiert werden. Auf diesem Weg lassen sich auch UEFI-fähige USB-Sticks erstellen. Das Tool *dism.exe* gehört auch zu den Bordmitteln von Windows 10/11, sodass Sie den bootfähigen Datenträger auch auf einer Arbeitsstation erstellen können. Achten Sie darauf, die korrekten Pfade zur originalen *install.wim* und den neuen *install.swm*-Dateien zu verwenden.

Sie können den USB-Stick auch zukünftig für das Speichern von Daten nutzen, zum Beispiel für Treiber. Die Installationsdateien belegen etwa einen Platz von 5,5 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.
- ▶ 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`.
- ▶ Kopieren Sie den kompletten Inhalt der Windows Server 2022-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 2022-Installation.

Mit dem kostenlosen *Windows USB/DVD Download Tool* lassen sich ebenfalls USB-Sticks für die Installation von Windows Server 2022 erstellen. Dieses wird nicht mehr von Microsoft direkt bereitgestellt, ist aber auf anderen Seiten verfügbar. Alternativ können Sie *Rufus* oder *Yumi* für die Erstellung verwenden.

4.2 Windows Server 2022 installieren

Überblick

Die Installation ist sehr einfach, denn es müssen nur wenige Abfragen beantwortet werden. Nach Abschluss der Installation können Sie weitere Einstellungen vornehmen.

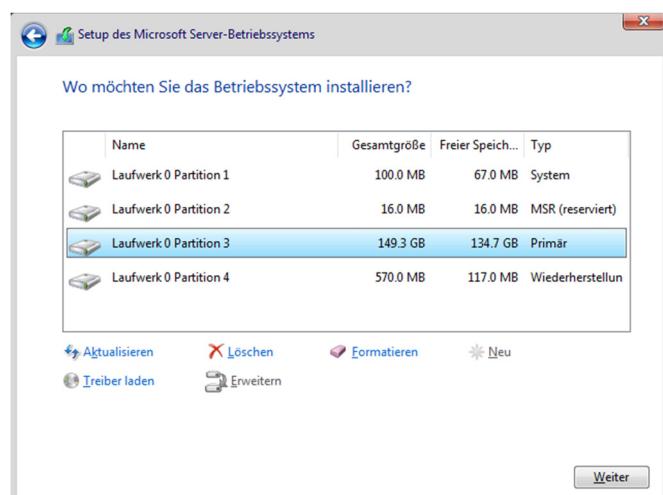
Im Folgenden wird beschrieben, wie Sie eine Neuinstallation von Windows Server 2022 auf einem Rechner ohne vorhandenes Betriebssystem mit einer DVD durchführen.

Windows Server 2022 legt wie seine Vorgänger eine oder mehrere versteckte Partition/en auf der Startfestplatte an. Diese hat beim klassischen Partitionslayout eine Größe von 350–500 MB bzw. etwa 250 MB über 3 Partitionen verteilt im GPT Partitionsstil. In diesem Bereich liegen die Startdateien von Windows Server 2022 und Daten zum Entschlüsseln von BitLocker-Laufwerken. Aktualisieren Sie einen Rechner von Windows Server 2012/2012 R2/2016/2019 zu Windows Server 2022, belässt der Assistent die Startpartition auch auf einer geringeren Größe.

Wer Windows Server 2022 produktiv installieren will, hat grundsätzlich verschiedene Möglichkeiten: Die erste ist eine Aktualisierung des bestehenden Windows Server zu Windows Server 2022. Der Vorteil dabei ist, dass Sie alle Einstellungen und Programme der Windows Server-Voredition zu Windows Server 2022 übernehmen.

Informationen zu den Upgrade-Pfaden finden Sie hier:

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



Partitionierung einer HDD im GPT-Stil

In jedem Fall ist es empfehlenswert, vor der Aktualisierung eine imagebasierte Datensicherung auf einer externen Festplatte durchzuführen. Geht bei der Aktualisierung zu Windows Server 2022 etwas schief, können Sie einfach das Image zurückspielen und so das alte Windows Server-System retten. Dazu verwenden Sie am besten ein Systemabbild.

DVD-Installation von Windows Server 2022

Stellen Sie sicher, dass der Rechner von DVD bootet. Die meisten modernen Computer verfügen über ein Bootmenü, in dem Sie für den nächsten Bootvorgang das Bootlaufwerk wählen können. Dieses Menü erreichen Sie meist mit **[F9]** oder **[F10]**. Eventuell müssen Sie auch die Bootreihenfolge im BIOS-Setup ändern. Auf vielen Rechnern kommen Sie mit **[Entf]** oder **[F12]** beim Rechnerstart ins BIOS.

Im BIOS-Setup ist die Tastatur meistens auf englisches Layout eingestellt. Benötigen Sie eine Bestätigung mit „Yes“, dann denken Sie daran, dass die Tasten Y und Z vertauscht sind.

- ▶ Legen Sie die Installations-DVD in das DVD-ROM-Laufwerk ein und starten Sie den Rechner.

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.

In Windows Server 2012 R2 konnten Core-Server zu herkömmlich installierten Servern umgewandelt werden und umgekehrt. Das ist in Windows Server 2022 nicht mehr möglich. Installieren Administratoren einen Core-Server, muss der Server neu installiert werden, wenn die grafische Oberfläche benötigt wird. Das gilt auch für Server mit grafischer Benutzeroberfläche. Diese lässt sich in Windows Server 2022 nicht mehr deinstallieren.

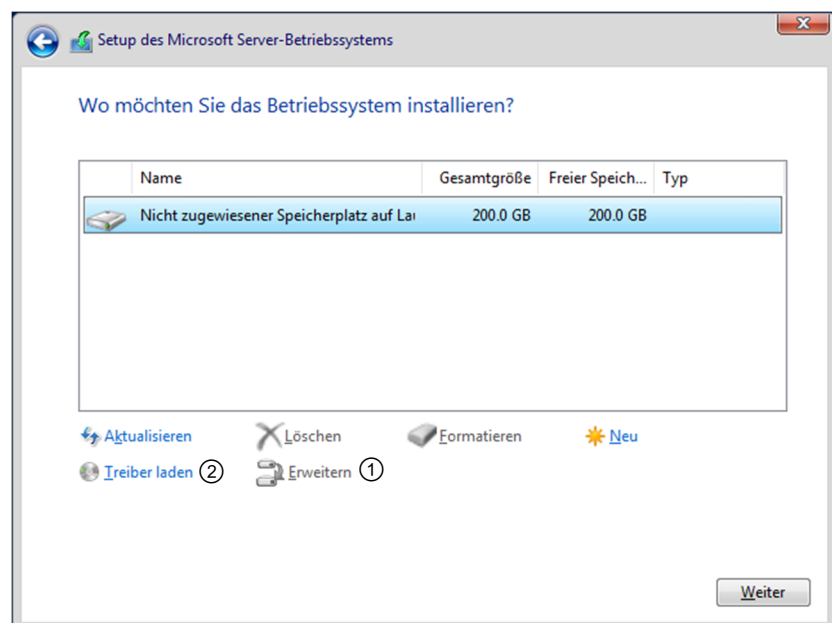
- ▶ Kontrollieren Sie die Spracheinstellungen und klicken Sie dann auf *Weiter*.
- ▶ Klicken Sie auf *Jetzt installieren*.
- ▶ Markieren Sie die Version, die Sie installieren wollen, und klicken Sie dann auf *Weiter*.
- ▶ Akzeptieren Sie die Lizenzbedingungen und klicken Sie auf *Weiter*.
- ▶ Wählen Sie als Installationsart *Benutzerdefiniert: nur Windows installieren* (für fortgeschrittene Benutzer).

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, verwendet Windows den gesamten verfügbaren Speicher der Platte und partitioniert diesen automatisch.

Unterhalb der Partitionsanzeige finden Sie diverse Schaltflächen. Hier können Sie Partitionen erstellen, löschen und formatieren oder bestehende Partitionen erweitern (vergrößern) ①.

Bearbeiten Sie die Festplatte nur so weit, wie es für die Installation erforderlich ist.



Auswahl des Installationsortes

Sollte Windows den Festplattencontroller nicht erkennen, haben Sie unter *Treiber laden* ② die Möglichkeit, den vom Hersteller gelieferten Treiber zu installieren. Erst dann kann der Installationsdialog fortgesetzt werden.

- ▶ Erstellen Sie eine neue Partition im unformatierten Bereich, indem Sie auf *Neu* klicken und dann die Größe mit mindesten 32 GB festlegen.

Je nach Verwendung des Servers kann hier auch ein Vielfaches erforderlich sein, im Normalfall sollten Sie jedoch alle größeren Datenmengen auf einer anderen Partition speichern.

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 ein gültiges Passwort nebst Bestätigung ein und klicken Sie auf *Fertig stellen*.

Standardmäßig muss ein Passwort den Komplexitätsanforderungen genügen, um gültig zu sein. Es muss mindestens drei der folgenden Zeichentypen enthalten:

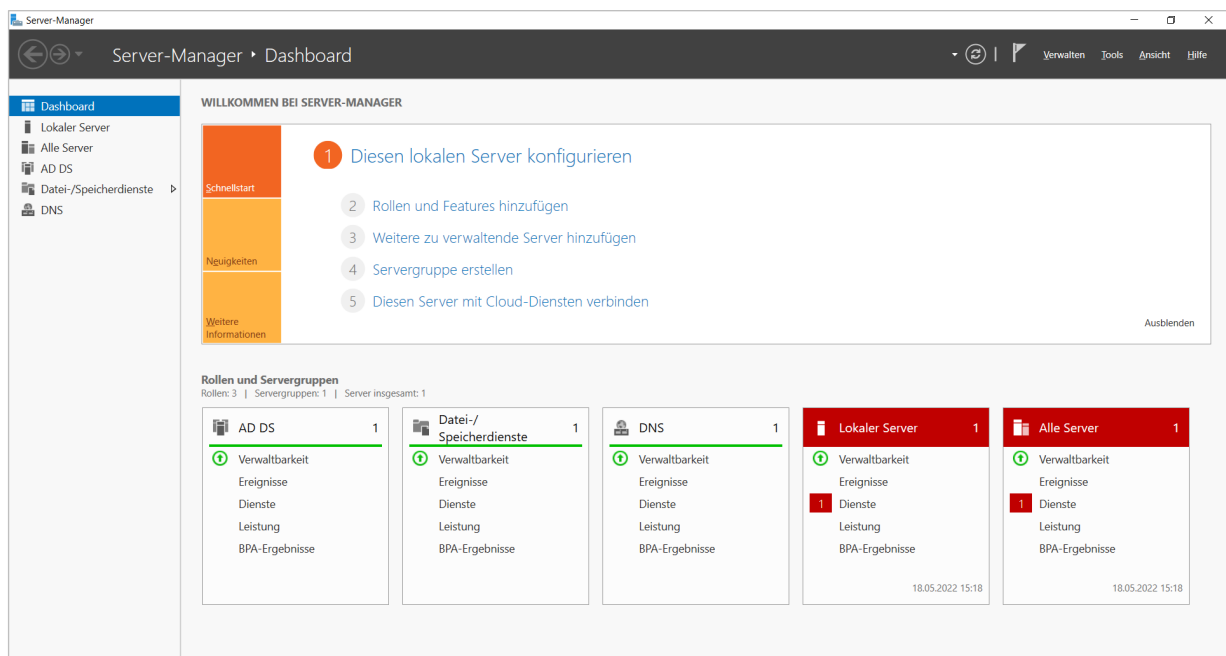
- ✓ Kleinbuchstaben
- ✓ Großbuchstaben
- ✓ Zahlen
- ✓ Sonderzeichen

Die Installation wird nun fortgesetzt. Nach Abschluss der Installation können Sie sich am Rechner anmelden.

4.3 Basis-Konfiguration

Erstkonfiguration im Server-Manager

Nach der Anmeldung öffnet sich der Server-Manager mit dem Dashboard. Das Dashboard soll Ihnen auf den ersten Blick zeigen, wie es um Ihren Server bestellt ist. Grüne Anzeigen bedeuten, dass alles in Ordnung ist, alle roten Bestandteile erfordern jedoch Ihre Aufmerksamkeit.

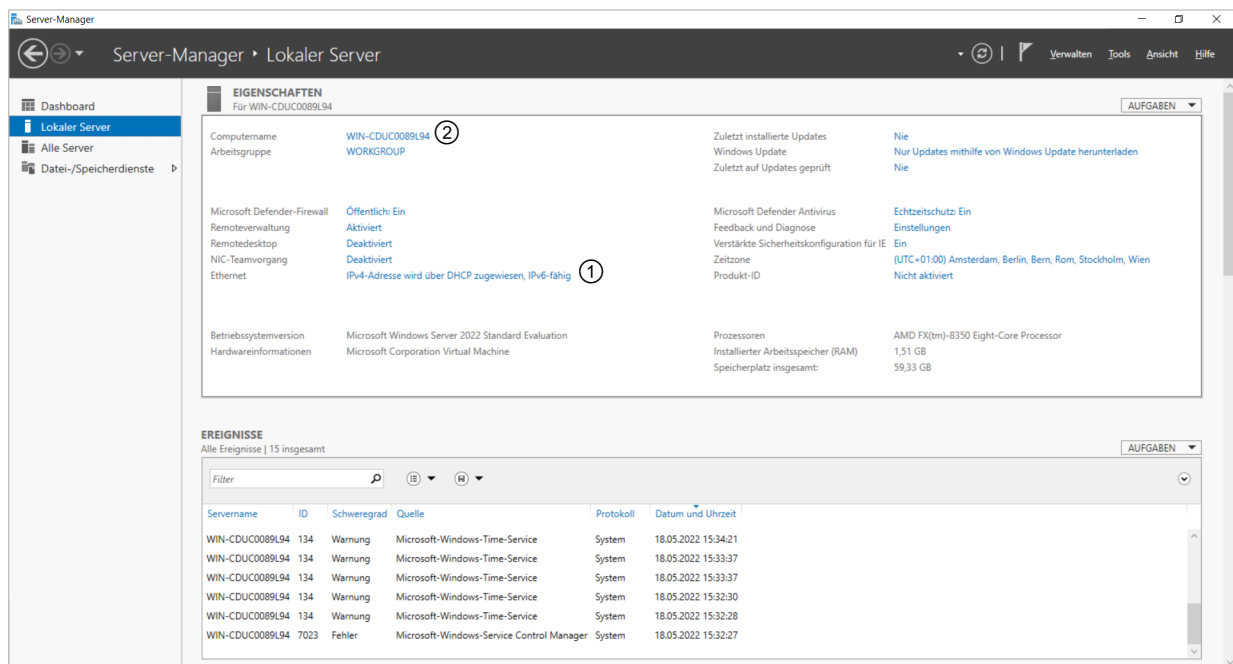


Übersicht Server-Manager

Über das Menü *Ansicht* deaktivieren Sie die Willkommen-Kachel, über *Verwalten/Server-Manager-Eigenschaften* aktivieren Sie das Kontrollkästchen *Server-Manager beim Anmelden nicht automatisch starten*, wenn Sie nicht wollen, dass der Server-Manager automatisch mit Windows startet.

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

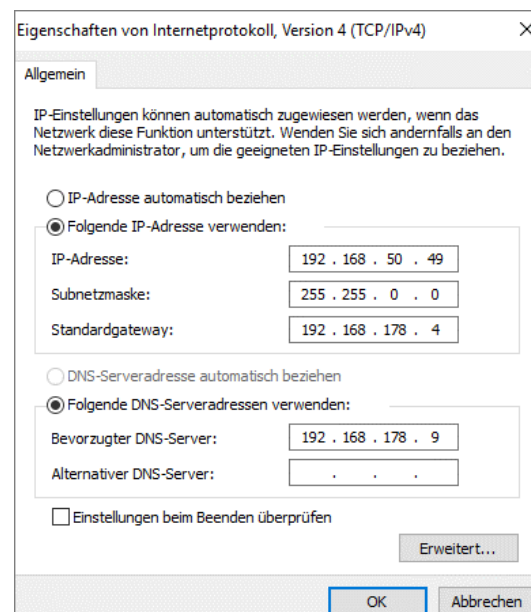
Auf dieser Seite können Sie zahlreiche Einstellungen des lokalen Servers erreichen. Ihre ersten beiden Aufgaben bestehen darin, die Netzwerkeinstellungen ① anzupassen und den Computernamen ② zu ändern.



IP konfigurieren

Da Server meist keine DHCP-Clients sein sollen, müssen Sie ihm jetzt eine IP-Adresse zuweisen.

- Öffnen Sie die Netzwerkverbindungen, indem Sie im Server-Manager auf die Netzwerkverbindung klicken.
 - Öffnen Sie per Rechtsklick die *Eigenschaften* der angezeigten Verbindung.
 - Öffnen Sie dort die Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4).
 - Aktivieren Sie die Option *Folgende IP-Adresse verwenden*.
 - Geben Sie die eindeutige IP-Adresse ein.
 - Kontrollieren Sie die vorgeschlagene Subnetzmaske im Eingabefeld.
 - Geben Sie die IP-Adresse des zuständigen Routers ein.
 - Geben Sie in das Eingabefeld die IP-Adresse eines DNS-Servers ein.
- Falls ein weiterer DNS-Server vorhanden ist, können Sie dessen IP-Adresse in das Eingabefeld eingeben.



Über die Schaltfläche *Erweitert* kommen Sie zu den erweiterten TCP/IP-Einstellungen.

Dazu gehören:

- ✓ einer Netzwerkkarte mehrere IP-Adressen zuweisen,
- ✓ Verwendung von mehr als einem Router,
- ✓ Verwendung von mehr als zwei DNS-Servern,

- ✓ Verwendung von verbindungspezifischen DNS-Namen (bei mehrfach vernetzten Computern),
- ✓ Festlegen, ob und wie dynamische DNS-Aktualisierungen erfolgen.

Sind in Ihrem Netz WINS-Server vorhanden, sollten Sie deren IP-Adresse im Register WINS hinzufügen. Hier können Sie auch angeben, ob und wie die Auflösung von NetBIOS-Namen erfolgt.

Wirkungsweise des primären DNS-Suffixes

Sein primäres DNS-Suffix erhält ein Rechner automatisch, wenn er Mitglied einer Windows-Domäne wird. Zunächst sind standardmäßig immer nur die folgenden Optionen aktiviert:

- ✓ *Primäre und verbindungspezifische DNS-Suffixe anhängen*
- ✓ *Übergeordnete Suffixe des primären DNS-Suffixes anhängen*
- ✓ *Adressen dieser Verbindung in DNS registrieren*

Die einzelnen Optionen spielen bei der Namensauflösung in einer DNS-Infrastruktur eine erhebliche Rolle:

Primäre und verbindungspezifische DNS-Suffixe anhängen – Durch die Aktivierung dieser Option wird festgelegt, dass der Rechner bei der Auflösung von Rechnernamen immer automatisch das konfigurierte primäre DNS-Suffix des eigenen Computernamens anhängt.

Übergeordnete Suffixe des primären DNS-Suffixes anhängen – Diese Option bedeutet, dass die Namen von übergeordneten Domänen bei der Namensauflösung verwendet werden.

DNS-Suffix für diese Verbindung – Zusätzlich haben Sie noch die Möglichkeit, in diesem Bereich ein weiteres beliebiges DNS-Suffix einzutragen.

Adressen dieser Verbindung in DNS registrieren – Auch diese Option ist bereits standardmäßig aktiviert. Ein DNS-Server hat die Möglichkeit, Einträge dynamisch zu registrieren.

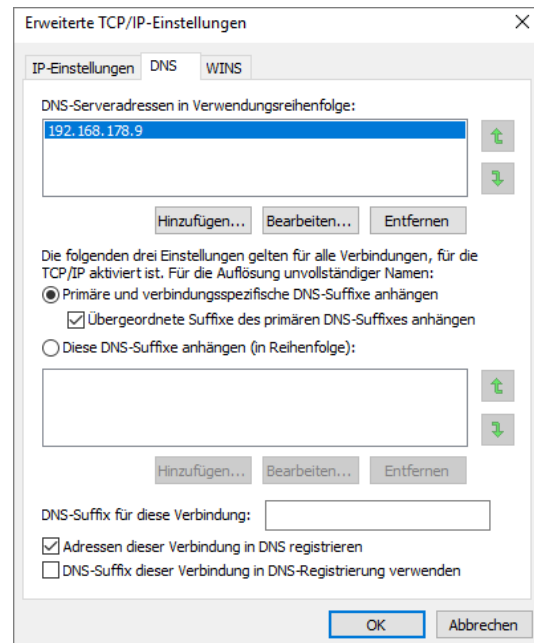
Außer den aktivierten Optionen gibt es noch weitere Möglichkeiten, die Sie in diesem Fenster konfigurieren können:

- ✓ *Diese DNS-Suffixe anhängen* – Wenn Sie diese Option aktivieren, können Sie DNS-Suffixe konfigurieren, nach denen unvollständige Rechnernamen aufgelöst werden.
- ✓ *DNS-Suffix dieser Verbindung in DNS-Registrierung verwenden* – Wenn Sie diese Option aktivieren, wird der Server-Name im DNS mit seinem Computernamen und seinem primären DNS-Suffix registriert.

Beispiel zu DNS-Suffixen

Angenommen, ein Rechner hat die Bezeichnung PC1 und ist Mitglied der Windows Domäne *Verkauf.Herdt.de*. Hierdurch wird dem Client die DNS-Domänenbezeichnung (*Verkauf.Herdt.de*) zu seinem primären DNS-Suffix hinzugefügt.

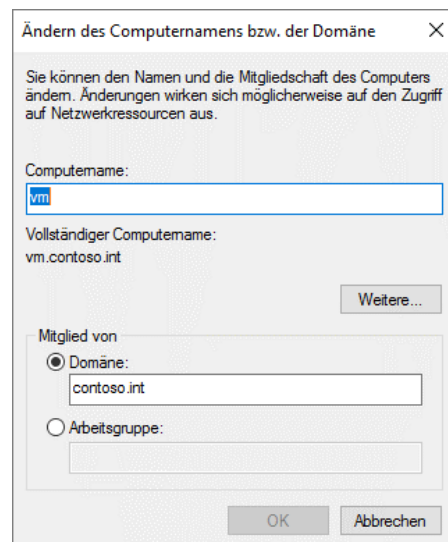
Ein Benutzer gibt jetzt einen einfachen Rechnernamen ein, z. B. `ping PC1` (kein Punkt im Rechnernamen). Die Option *Primäre und verbindungspezifische DNS-Suffixe anhängen* sorgt dafür, dass eine DNS-Abfrage für *PC1.Verkauf.Herdt.de* erfolgt. Kann der DNS-Server diese Abfrage nicht auflösen, dann sorgt die Option *Übergeordnete Suffixe des primären DNS-Suffixes anhängen* dafür, dass eine erneute Abfrage erfolgt, diesmal für *PC1.Herdt.de*, die übergeordnete Domäne. Es wird so lange der linke Bestandteil des Domänennamens (*Verkauf*) gelöscht, bis entweder eine erfolgreiche Namensauflösung erfolgt oder eine Domäne zweiter Ebene erreicht ist (*Herdt.de*).



Computernamen und -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. Sie erreichen das Fenster zum Wechseln der Domäne und des Rechnernamens **auch** durch Eingabe von `sysdm.cpl` im Suchfeld des Startmenüs.

- ▶ Klicken Sie im Server-Manager auf den Namen des Servers.
- ▶ Klicken Sie auf die Schaltfläche *Ändern*.
- ▶ Geben Sie den Computernamen ein.
Er darf maximal 15 Zeichen lang sein und sollte nur aus englischen Buchstaben, Ziffern und dem Bindestrich bestehen. Innerhalb der Domäne bzw. Arbeitsgruppe muss er eindeutig sein.
- ▶ Unter *Weitere* können Sie das primäre DNS-Suffix des Rechners angeben. Wenn Sie den Rechner zum Mitglied einer Domäne machen, wird dort automatisch der Domänenname eingetragen.
- ▶ Soll der Rechner Mitglied einer anderen Arbeitsgruppe werden, passen Sie den Eintrag entsprechend an.
- ▶ Um den Rechner zum Mitglied einer Domäne zu machen, aktivieren Sie diese Option und geben den Namen der Domäne ein.



Veränderungen in diesem Fenster erfordern einen Neustart.

Diese Einstellungen sind bei fast allen Windows-Betriebssystemen identisch. Ausnahme: Windows Client Home-Versionen unterstützen keine Domänen.

Für einen Domänenbeitritt müssen einige Voraussetzungen erfüllt sein:

- ✓ Die IP-Konfiguration muss stimmen. Der Rechner muss mit einem passenden DNS-Server konfiguriert sein und muss 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 in der Domäne zu erstellen.

Anmeldung

Haben Sie eine Neuinstallation durchgeführt und gehört der Computer keiner Domäne an, dann ist der lokale Administrator das einzig gültige Konto. Sie werden direkt nach der Eingabe des Passwortes angemeldet.

Andernfalls melden Sie sich mit einem gültigen Domänenkontonamen und Passwort an.

- ▶ Drücken Sie **Strg** **Alt** **Entf**, um den Anmeldedialog anzuzeigen.
Sie können sich jetzt als *Rechnername\Administrator* lokal anmelden.
- ▶ Für die Anmeldung mit einem Domänenkonto klicken Sie auf *Anderer Benutzer*.
- ▶ Nach einem Klick auf *Anderer Benutzer* können Sie Ihre Anmeldeinformationen eingeben.

Voreingestellt ist die Anmeldung an der Domäne des Computerkontos. Liegt Ihr Benutzerkonto in derselben Domäne, müssen Sie nur den Benutzernamen eingeben, anderenfalls müssen Sie auch die Domäne angeben.

Dies kann auf zwei Arten erfolgen:

- ✓ *Domänen-Name\Benutzername* – hier wird der NetBIOS-Name der Domäne angegeben.
Beispiel: *unsere-firma\administrator*
- ✓ *Benutzername@Domain-FQDN* (Fully Qualified Domain Name) – der sogenannte UPN (**User Principal Name**, Benutzerprinzipalname) besteht aus dem Benutzernamen und dem UPN-Suffix, die durch das Zeichen @ voneinander getrennt werden. Das UPN-Suffix ist der vollständige DNS-Name der Domäne, der auch als **Fully Qualified Domain Name** (FQDN) bezeichnet wird.
Beispiel: *administrator@unsere-firma.intern*

Falls Sie als Benutzername ein Konto angeben, das auch lokal vorhanden ist (z. B. *Administrator*), ändert sich automatisch die Angabe bei *Anmelden an* auf den Rechnernamen. In diesem Fall müssen Sie eine der angegebenen Varianten benutzen.

5 Serverfunktionen anpassen

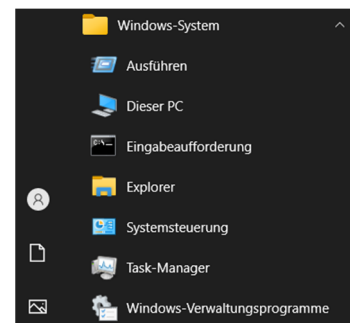
5.1 Überblick über die Einstellungsmöglichkeiten

Windows Server 2022 verfügt über zahlreiche Werkzeuge und Hilfsmittel, um die Einstellungen des Servers vorzunehmen:

- ✓ Die Systemsteuerung: Wie von Windows-Clients her bekannt, können hier zahlreiche Anpassungen rund um das System vorgenommen werden.
- ✓ Die Management-Konsole (MMC): Sie entspricht weitgehend der von Windows-Clients bekannten Konsole, verfügt jedoch über erweiterte Funktionen und Snap-Ins.
- ✓ Der Server-Manager: Hier werden die meisten Werkzeuge zur Überwachung der Serverfunktionen zusammengefasst. Der Server-Manager erlaubt das Hinzufügen neuer Serverrollen und -funktionen und bietet schnellen Zugriff auf Informationen und Werkzeuge.
- ✓ Die PowerShell und die Eingabeaufforderung: Über die PowerShell lassen sich sämtliche Funktionen des Servers und anderer Rechner im Netzwerk steuern. Die PowerShell verfügt mit den sogenannten Cmdlets (Commandlets) über vordefinierte Skripte zu allen Aufgabenbereichen. Sie bietet Hilfe beim Erstellen eigener Cmdlets und ist weitgehend abwärtskompatibel zur weiterhin vorhandenen Eingabeaufforderung.
- ✓ Die Registry: Windows Server 2022 verfügt wie alle Windows-Versionen über einen Registrierungs-Editor, mit dem Sie tiefgreifende Änderungen vornehmen können.

Computer konfigurieren mit der Systemsteuerung

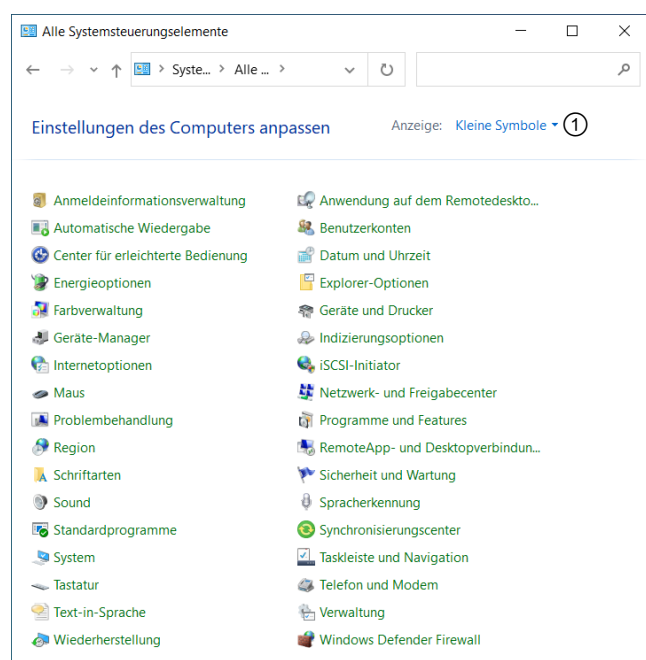
- ▶ Suchen Sie im Suchfeld des Startmenüs nach „Systemsteuerung“ oder öffnen Sie die Systemsteuerung im Startmenü – *Windows-System*.



Über die Systemsteuerung können Sie viele Funktionen zur Konfiguration des Computers aufrufen. Die einzelnen Symbole stehen dabei für die verschiedenen Bereiche, in denen Sie Einstellungen vornehmen können.

Über den Menüpunkt *Anzeige* ① können Sie auswählen, ob Kategorien, kleine oder große Symbole angezeigt werden sollen.

Sie können in eine Symbol-Ansicht umschalten, die die momentanen Kategorien in einzelne Symbole aufricht und mehr an die klassische Ansicht der vorhergehenden Windows-Versionen erinnert.

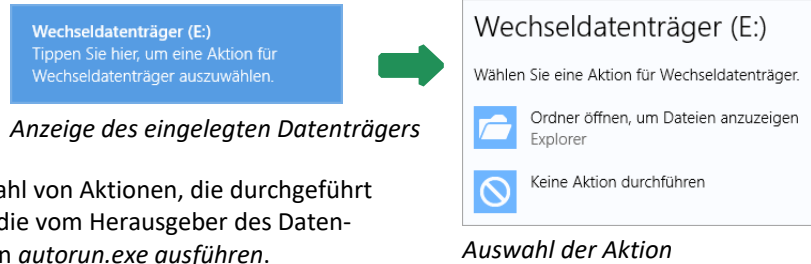


Anzeige der Systemsteuerung mit kleinen Symbolen

5.2 Anwendungen installieren

Software installieren von Wechseldatenträger mit Autoplay-Funktion

Sobald Sie einen Datenträger einlegen oder anschließen, wird er vom System automatisch untersucht und eine Meldung angezeigt.



Anzeige des eingelegten Datenträgers

Auswahl der Aktion

Ein Klick darauf zeigt Ihnen eine Auswahl von Aktionen, die durchgeführt werden können, unter anderem auch die vom Herausgeber des Datenträgers voreingestellte Autoplay-Aktion *autorun.exe ausführen*.

Wenn der Wechseldatenträger bereits einmal eingelegt war, führt das System die beim letzten Mal gewählte Aktion automatisch aus.

Installation von einem beliebigen Ort

Falls Sie nicht über einen Datenträger mit Autostart-Funktion verfügen, gehen Sie wie folgt vor:

- ▶ Starten Sie mit (E) den Explorer und navigieren Sie zu dem Laufwerk und Ordner, worin sich die Installationsdateien befinden.
- ▶ Stellen Sie sicher, dass im Menüband des Explorers die Option *Dateinamenserweiterung* aktiviert ist (Register *Ansicht*, Gruppe *Ein-/ausblenden*, Kontrollfeld *Dateinamenserweiterungen*).
- ▶ Suchen Sie nach ausführbaren Dateien mit Namen wie *Setup* oder *Install* mit der Endung *.exe. Infrage kommen auch *.msi Dateien.

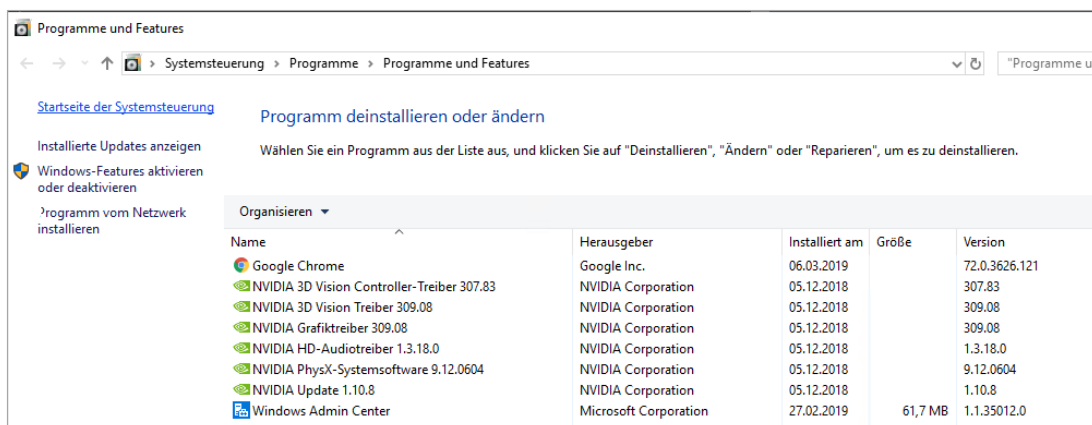
Alternativ können Sie Treiber, die nicht über ein Setup-Programm verfügen, über das Kontextmenü der INF-Dateien installieren.

Anwendungen ändern, entfernen oder reparieren

Installierte Anwendungen bzw. Programme werden unter *Systemsteuerung - Programme und Funktionen* angezeigt. Hier können Sie den Herausgeber, das Installationsdatum sowie Größe und Versionsnummer der Anwendung sehen. Wenn Sie eine Software ausgewählt haben, können Sie sie deinstallieren. Bei mancher Software wird hier auch *Ändern* oder *Reparieren* angeboten. Alternativ starten Sie das Fenster durch Eingabe von „appwiz.cpl“.

- ▶ Klicken Sie im Schnellzugriffsmenü auf *Programme und Features*.
- ▶ Markieren Sie in der Liste das entsprechende Programm.

In der Fußzeile wird oftmals ein Hilfelink angezeigt, über den Sie zur Internetseite des Herstellers gelangen können.



5.3 Windows-Funktionen verwalten

Server-Manager

Wenn Sie im oben abgebildeten Fenster auf *Windows-Features aktivieren oder deaktivieren* klicken, wird der Server-Manager geöffnet und der Assistent zum Hinzufügen von Rollen und Features gestartet. Windows-Funktionen sind entweder als **Serverrolle** oder als **Feature** implementiert. Dabei bezeichnen die Serverrollen die Serverfunktionen wie z. B. DNS, DHCP oder Active Directory-Domänendienste, während die Features zusätzliche Funktionen bereitstellen, wie z. B. BitLocker oder BranchCache.

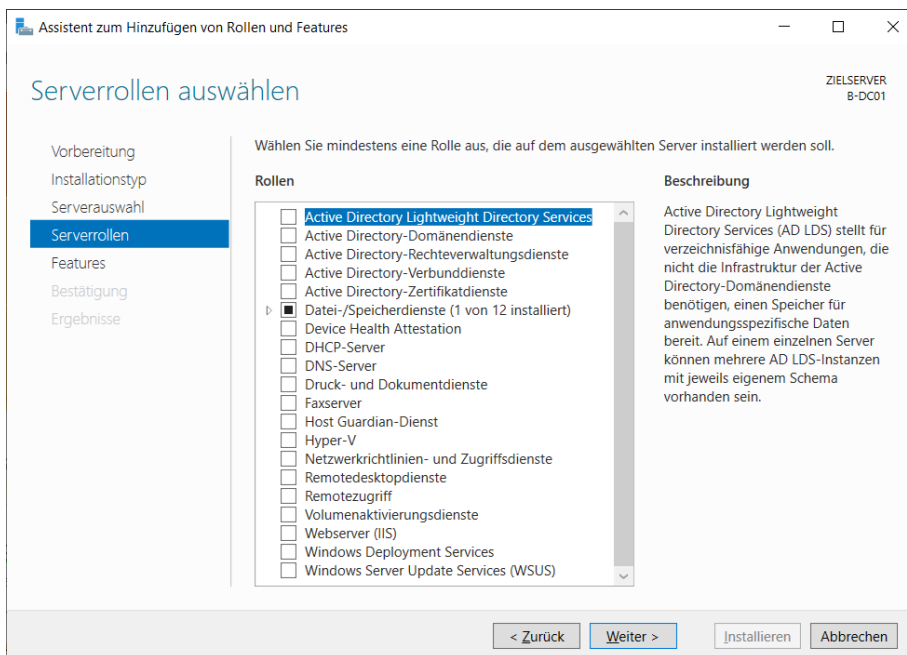
Im Assistenten können Sie auswählen zwischen den Optionen ...

- ✓ *Rollen- oder featurebasierte Installation* (Standard) oder
- ✓ *Szenariobasierte Installation* für den Einsatz von Desktop- oder Sitzungsvirtualisierung. Für diese Option muss der lokale Server der Domäne beigetreten sein.
- ▶ Starten Sie eine rollen- und featurebasierte Installation und wählen Sie im nächsten Schritt aus dem Serverpool einen Server aus.
Alternativ können Sie auch eine virtuelle Festplatte auswählen und diese dann auf einem Server einbinden.

Rollen hinzufügen

Als Nächstes werden im Assistenten die Serverrollen hinzugefügt:

- ▶ Aktivieren Sie das Kontrollfeld neben den zu installierenden Rollen.



Hinzufügen von Serverrollen

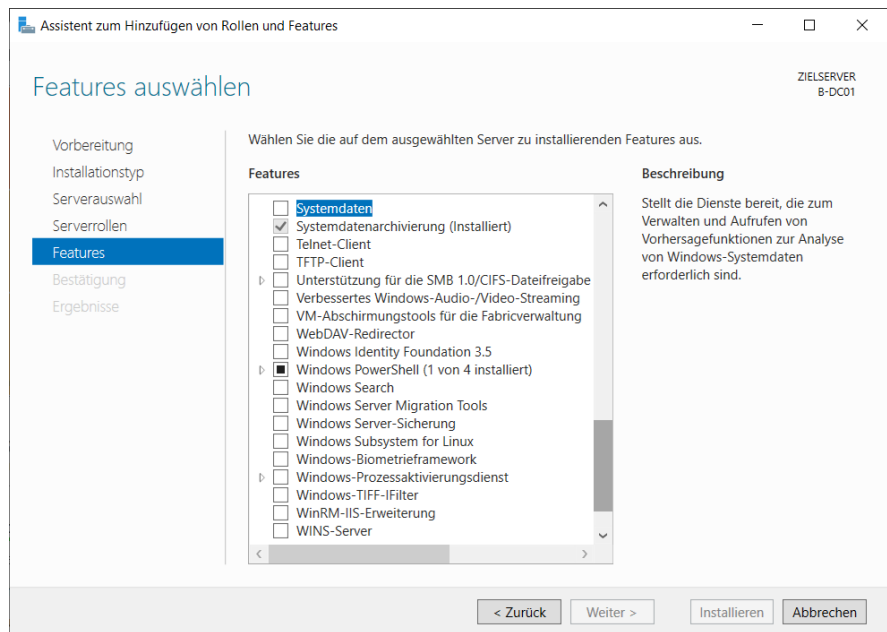
Im rechten Bereich erhalten Sie eine Beschreibung der markierten Rolle.

Der Assistent löst Abhängigkeiten automatisch auf. Setzt eine markierte Rolle eine andere Rolle oder ein nicht installiertes Feature voraus, dann weist Sie der Assistent darauf hin und installiert alle benötigten Komponenten. Auch die notwendigen Firewall-Regeln erstellt der Assistent automatisch.

- ▶ Ein Klick auf *Weiter* führt zum nächsten Schritt des Assistenten.

Features hinzufügen

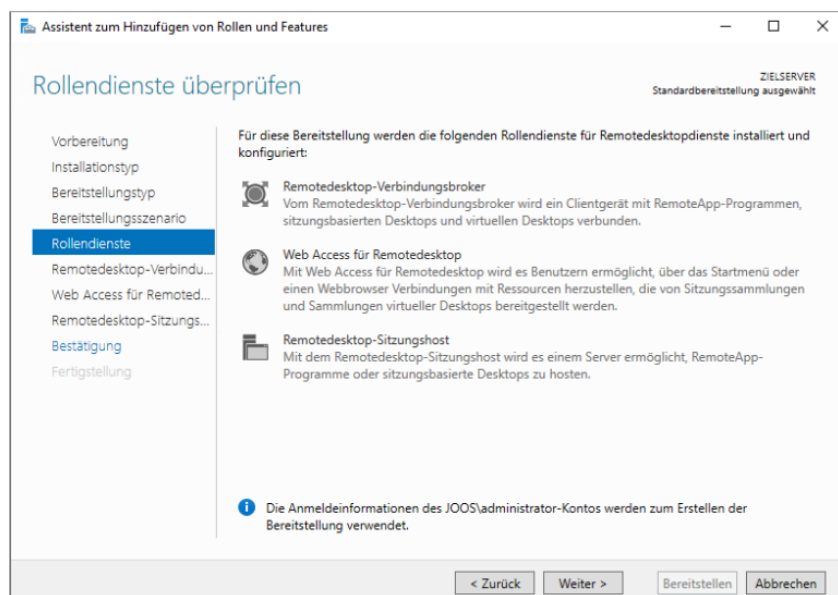
Features sind üblicherweise Zusatzfunktionen, die eine bestehende Server- oder Clientrolle erweitern. Das Vorgehen bei der Installation entspricht dem Hinzufügen von Rollen.



Hinzufügen von Features

Rollendienste für Remotedesktop hinzufügen

Im folgenden Schritt können Sie die verschiedenen Rollendienste hinzufügen, die zur Bereitstellung der Remote-Desktopdienste für die Benutzer im Netzwerk oder über das Internet benötigt werden.



Rollendienste für Remotedesktopdienste hinzufügen

5.4 Aktuelle Konfiguration einsehen

Systeminformationen in der Konsole abrufen

- ▶ Geben Sie im Startmenü `cmd`  ein.
- ▶ Verwenden Sie den Befehl `systeminfo` für eine Systemübersicht.

```

Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Administrator>systeminfo

Hostname: B-DC01
Betriebssystemname: Microsoft Windows Server 2022 Standard Evaluation
Betriebssystemversion: 10.0.20348 Nicht zutreffend Build 20348
Betriebssystemhersteller: Microsoft Corporation
Betriebssystemkonfiguration: Eigenständiger Server
Typ des Betriebssystems: Multiprocessor Free
Registrierter Benutzer: Windows-Benutzer
Registrierte Organisation:
Produkt-ID: 00454-40000-00001-AA469
Ursprüngliches Installationsdatum: 18.05.2022, 15:36:35
Systemstartzeit: 19.05.2022, 09:26:19
Systemhersteller: Microsoft Corporation
Systemmodell: Virtual Machine
Systemtyp: x64-based PC
Prozessor(en): 1 Prozessor(en) installiert.
[01]: AMD64 Family 21 Model 2 Stepping 0 AuthenticAMD ~4013 MHz
Microsoft Corporation Hyper-V UEFI Release v4.0, 01.11.2019
C:\Windows
C:\Windows\system32
\Device\HarddiskVolume1
de;Deutsch (Deutschland)
de;Deutsch (Deutschland)
(UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
1.401 MB
293 MB
2.553 MB
1.394 MB
1.159 MB
C:\pagefile.sys
WORKGROUP
\\B-DC01
3 Hotfix(e) installiert.
[01]: KB5004330
[02]: KB5005039
[03]: KB5005552
1 Netzwerkadapter installiert.

```

Ausführliche Systeminformationen im GUI aufrufen

- Geben Sie im Startmenü `info` oder `msinfo32` ein, um die Systeminformationen aufzurufen. Alternativ können Sie auch im Server-Manager auf *Tools* klicken und aus der Liste *Systeminformationen* auswählen.

Das Verwaltungswerkzeug *Systeminformationen* zeigt detaillierte Informationen zu Ihrem System:

- ✓ Unter *Systemübersicht* finden Sie Informationen über die Version des Betriebssystems, den Prozessor, das BIOS sowie die Größe des Speichers.
- ✓ *Hardwareressourcen* zeigt u. a. Ressourcenkonflikte, verankerte Hardware, E/A (Eingabe-/ Ausgabe-Anschlussadressen) und Informationen zum Arbeitsspeicher.
- ✓ *Komponenten* zeigt u. a. Informationen über Multimedia, Audio, Infrarot-, Speicher- und Eingabegeräte.
- ✓ *Softwareumgebung* liefert u. a. Informationen über Systemtreiber, Aufträge, Dienste und Umgebungsvariablen.

Systeminformationen	
Element	Wert
Betriebssystemname	Microsoft Windows Server 2022 Standard Evaluation
Version	10.0.20348 Build 20348
Zusätzliche Betriebssystembeschreibung	Nicht verfügbar
Betriebssystemhersteller	Microsoft Corporation
Systemname	B-DC01
Systemhersteller	Microsoft Corporation
Systemmodell	Virtual Machine
Systemtyp	x64-basierter PC
System-SKU	None
Prozessor	AMD FX(tm)-8350 Eight-Core Processor, 4013 MHz, 1 Kern(e)
BIOS-Version/-Datum	Microsoft Corporation Hyper-V UEFI Release v4.0, 01.11.2019
SMBIOS-Version	3.1
Version des eingebetteten Controllers	255.255
BIOS-Modus	UEFI
BaseBoard-Hersteller	Microsoft Corporation
BaseBoard-Produkt	Virtual Machine
BaseBoard-Version	Hyper-V UEFI Release v4.0
Plattformrolle	Desktop
Sicherer Startzustand	Ein
PCR7-Konfiguration	Nicht verfügbar
Windows-Verzeichnis	C:\Windows
Systemverzeichnis	C:\Windows\system32
Startgerät	\Device\HarddiskVolume1
Gebietsschema	Deutschland
Hardwareabstraktionsebene	Version = "10.0.20348.143"
Benutzername	Nicht verfügbar
Zeitzone	Mitteleuropäische Sommerzeit
Installierter physischer Speicher	2,00 GB
Gesamter physischer Speicher	1,37 GB
Verfügbare physischer Speicher	406 MB

Bericht erstellen

Sie können alle Systeminformationen in einer Textdatei zusammenfassen.

- ▶ Wählen Sie unter *Datei* den Menüpunkt *Exportieren*.
- ▶ Wählen Sie für die Datei einen Pfad und geben Sie einen Namen ein.

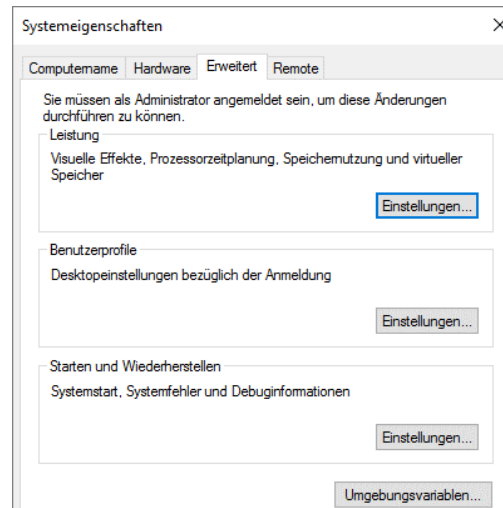
5.5 Einstellungen des Betriebssystems ändern

Erweiterte Systemeigenschaften öffnen

- ▶ Klicken Sie im Schnellzugriffsmenü auf *System*.
- ▶ Klicken Sie auf *Erweiterte Systemeinstellungen*.
- ▶ Wechseln Sie in das Register *Erweitert*.

Das Register enthält drei Bereiche, auf die im Folgenden Bezug genommen wird:

- ✓ Leistung
- ✓ Benutzerprofile
- ✓ Starten und Wiederherstellen
- ✓ Ebenfalls vorhanden ist ein Link zu den Umgebungsvariablen.

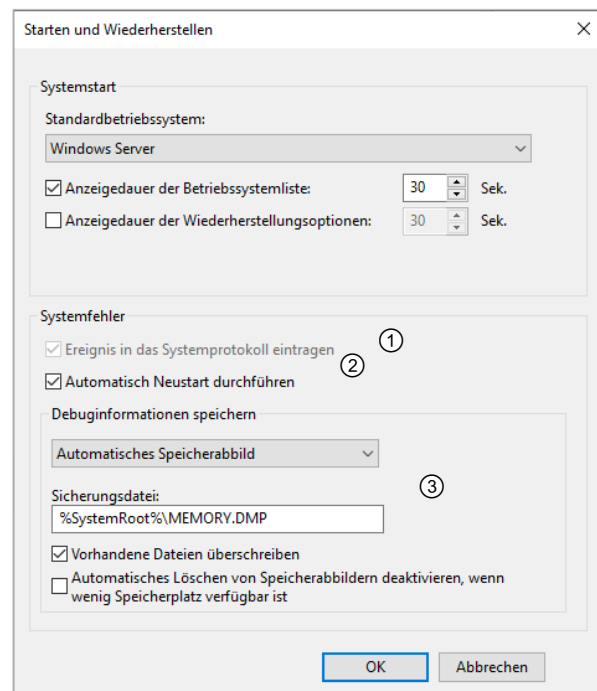


Erweiterte Systemeigenschaften

Bevorzugtes Betriebssystem festlegen

Falls auf dem Server eine Multiboot-Konfiguration erstellt wurde, können Sie festlegen, welches Betriebssystem beim Hochfahren des Systems als Standardsystem in der Auswahlliste des Bootmanagers erscheinen soll. Außerdem können Sie festlegen, nach welcher Wartezeit das Standardsystem automatisch gestartet wird, wenn keine Auswahl im Boot-Menü getroffen wird.

- ▶ Klicken Sie in den erweiterten Systemeinstellungen unter dem Register *Erweitert* im Bereich *Starten und Wiederherstellen* auf *Einstellungen*.
- ✓ Im Listenfeld können Sie das Standardbetriebssystem festlegen.
- ✓ Im Eingabefeld können Sie die Wartezeit bis zur automatischen Auswahl des Standardbetriebssystems bestimmen.
- ✓ Durch Deaktivieren des Kontrollfelds *Anzeigedauer der Betriebssystemliste* können Sie bestimmen, dass beim Hochfahren kein Boot-Menü angezeigt, sondern sofort das Standardbetriebssystem gestartet wird.



Verhalten bei Systemstart und Systemfehler

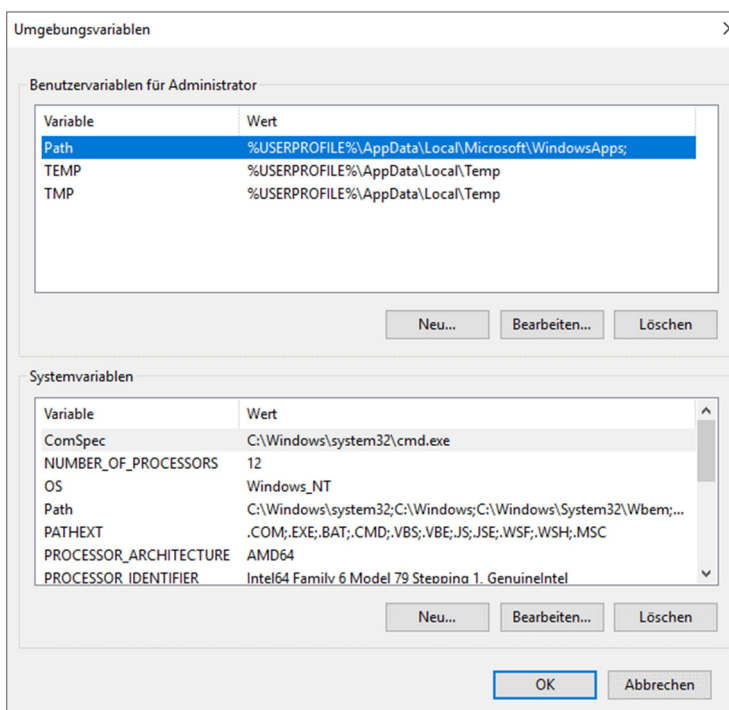
Systemverhalten bei Systemfehlern steuern

Durch die Voreinstellung des Kontrollfelds *Ereignis in das Systemprotokoll eintragen* ① nimmt Windows Server 2022 bei Systemfehlern Eintragungen ins Systemprotokoll vor. Diese Einstellung kann nicht deaktiviert werden.

Über das Kontrollfeld *Automatisch Neustart durchführen* ② können Sie festlegen, dass das System nach einem schweren Systemfehler automatisch neu startet. Im Listenfeld darunter legen Sie den Umfang des Speicherabbildes fest. Der Speicherort kann im Eingabefeld der Sicherungsdatei ③ angepasst werden. Das Speicherabbild legt fest, wie viele Informationen Windows Server 2022 im Moment des Systemfehlers abspeichert. Dabei handelt es sich um eine 1:1-Kopie des Arbeitsspeichers, dessen Größe je nach der ausgewählten Option (klein, nur Kernel, gesamter Speicher, automatisch) stark variiert. Das Anlegen dieses Speicherabbildes kann vonnöten sein, wenn Sie die Hilfe z. B. des Microsoft Software Service in Anspruch nehmen und dieser Schnappschuss zum Zeitpunkt eines Problems zu Debuggingzwecken benötigt wird. Damit ein Speicherabbild angefertigt werden kann, muss eine Auslagerungsdatei auf der Systempartition vorhanden sein.

Umgebungsvariablen des Systems einsehen

- Klicken Sie in den erweiterten Systemeinstellungen unter dem Register *Erweitert* auf *Umgebungsvariablen*.



Umgebungsvariablen

Im unteren Bereich sehen Sie Einstellungen für das System, die Windows Server 2022 während der Installation angelegt hat. Die meisten gelten für alle Benutzer, allerdings können einige durch die Benutzerumgebungsvariablen für das Benutzerkonto überschrieben werden. Änderungen an diesen Einstellungen sind nur in seltenen Fällen notwendig.

- ✓ Mithilfe der Schaltflächen *Neu*, *Bearbeiten* und *Löschen* können Sie neue Umgebungsvariablen anlegen und bestehende ändern bzw. löschen.
- ✓ In der Eingabeaufforderung können Sie sich mit `set` alle Umgebungsvariablen und deren Werte anzeigen lassen.



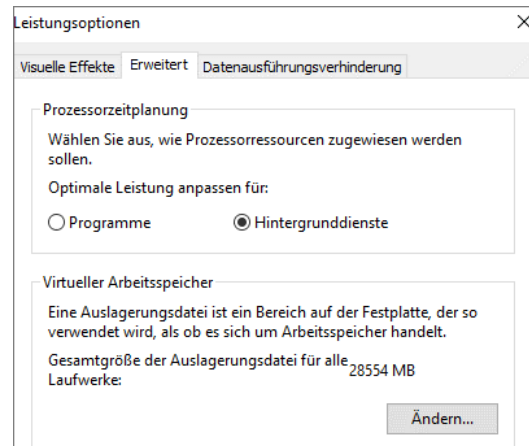
Systemumgebungsvariablen sind für den ordnungsgemäßen Betrieb des Servers unbedingt erforderlich. Löschen Sie deshalb keine der vom Betriebssystem angelegten Variablen.

Sie können sich alle Umgebungsvariablen über das Schnellzugriffsmenü in der *Eingabeaufforderung (Administrator)* mit dem Befehl `set` anzeigen lassen, ebenso ist eine Umleitung der Ausgabe von `set` in eine Datei möglich, beispielsweise `per set > c:\umgebungsvariablen.txt`.

Multitasking und virtuellen Arbeitsspeicher optimieren

Sie können in Windows Server 2022 festlegen, ob Anwendungen oder Hintergrunddienste mehr Prozessorleistung und Arbeitsspeicher erhalten sollen. Als Standard werden bei Servern die Hintergrunddienste bevorzugt.

- ▶ Klicken Sie in der Systemsteuerung auf *System* und öffnen Sie die Systemeigenschaften, indem Sie auf *Erweiterte Systemeinstellungen* klicken.
- ▶ Klicken Sie im Register *Erweitert* im Bereich *Leistung* auf *Einstellungen*.
- ▶ Öffnen Sie in den Leistungsoptionen das Register *Erweitert*.
- ▶ Legen Sie mit den entsprechenden Optionsfeldern fest, wofür die Systemleistung optimiert werden soll.
- ▶ Bestätigen Sie Ihre Eingabe mit *OK*.



Multitasking-Eigenschaften

Größe des virtuellen Arbeitsspeichers ändern

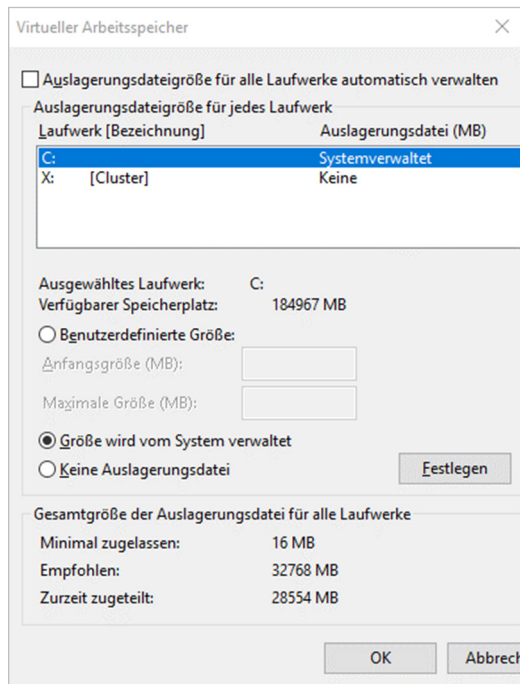
Für das Auslagern von momentan nicht benötigten Speicherseiten und falls der physikalische Arbeitsspeicher (RAM) knapp wird, verwendet Windows Server 2022 Auslagerungsdateien auf Festplatten. Auf jedem Laufwerk kann ein bestimmter Bereich für eine solche Auslagerungsdatei (Dateiname *pagefile.sys*) reserviert werden.

- Sie sollten auf keinen Fall Auslagerungsdateien auf mehreren Partitionen **auf demselben** Laufwerk anlegen, sonst leidet die Geschwindigkeit bei herkömmlichen Magnetfestplatten wegen des sich ständig hin und her bewegenden Schreib-/Lesekopfs enorm. Da beim Auslagern die Leistung dramatisch absinkt, sollten Sie möglichst den Hauptspeicher des Servers so weit aufrüsten, dass im Normalbetrieb so wenig Auslagerung wie möglich stattfinden muss.

Die Größe der Auslagerungsdatei kann durch Windows automatisch verwaltet werden. Sie können deren Größe jedoch auch selbst bestimmen. Wählen Sie als Anfangsgröße die Größe des Arbeitsspeichers und als maximale Größe das Doppelte. Diese Einstellung vermeidet eine Fragmentierung der Festplatte und stellt für besondere Situationen ausreichend Kapazität zur Verfügung. Es gibt keine allgemeingültige Faustregel für die Größe der Auslagerungsdatei. Beobachten Sie daher den Speicherbedarf und passen Sie im Bedarfsfall die Werte an Ihre Bedürfnisse an. Windows verwendet standardmäßig nur das Betriebssystem-Laufwerk für die Auslagerung. Sie sollten die Leistung erhöhen, indem Sie auf mehreren Laufwerken eine Auslagerungsdatei einrichten oder Laufwerke speziell für die Auslagerungsdatei bereitstellen. Wenn Ihr System über eine SSD verfügt, sollten Sie nur auf der schnellen SSD eine Auslagerungsdatei einrichten.

- ▶ Klicken Sie in der Systemsteuerung auf *System* und öffnen Sie die Systemeigenschaften, indem Sie auf *Erweiterte Systemeinstellungen* klicken.
- ▶ Betätigen Sie im Register *Erweitert* der Systemeigenschaften im Bereich *Leistung* die Schaltfläche *Einstellungen*.
- ▶ Klicken Sie im Dialogfenster *Leistungsoptionen* im Register *Erweitert* auf *Ändern*.

Im oberen Bereich des Dialogfensters *Virtueller Arbeitsspeicher* sehen Sie die verfügbaren Laufwerke und die minimale und die maximale Größe der dort reservierten Auslagerungsdatei.



Größe des virtuellen Arbeitsspeichers einstellen

- ▶ Zum Ändern der Werte markieren Sie das entsprechende Laufwerk.
- ▶ Geben Sie die neuen Werte für die Mindest- und für die Maximalgröße ein.
Orientieren Sie sich dabei auch am verfügbaren Speicherplatz auf dem entsprechenden Laufwerk. Sind Sie sich nicht sicher, wählen Sie zunächst den vom Betriebssystem empfohlenen Wert.

Anstatt selbst die Größe des virtuellen Speichers zu bestimmen, können Sie diese auch vom System verwalten lassen. Wählen Sie dazu das Optionsfeld *Größe wird vom System verwaltet*.

Wenn Sie sich mit der Konfiguration der Auslagerungsdateien gar nicht befassen wollen, überlassen Sie Windows die Verwaltung sämtlicher Parameter. Dies ist die Standardeinstellung.

- ▶ Klicken Sie auf die Schaltfläche *Festlegen*, um die Änderungen für dieses Laufwerk zu übernehmen.
- ▶ Um Ihre Änderungen abzuschließen, klicken Sie auf *OK*. Windows muss nach Einstellungen an der Auslagerungsdatei neu gestartet werden.

Datenausführungsverhinderung

Zusammen mit geeigneter Prozessorhardware (im CPU-Umfeld wird dieses Feature als NX-Flag, für No-Execute-Flag, bezeichnet) soll verhindert werden, dass Schadsoftware über typische Sicherheitslücken in Programmen ausgeführt wird. Bei solchen Angriffen wird z. B. beim **Buffer Overflow Exploit** ein Überlaufen von Datenpuffern dazu genutzt, in geschützten Speicherbereichen bösartigen Code auszuführen.

Dabei werden diese sensiblen Speicherbereiche auf eine nicht standardgemäße Weise angesprochen. Dieser Vorgang kann durch DEP bemerkt und verhindert werden.

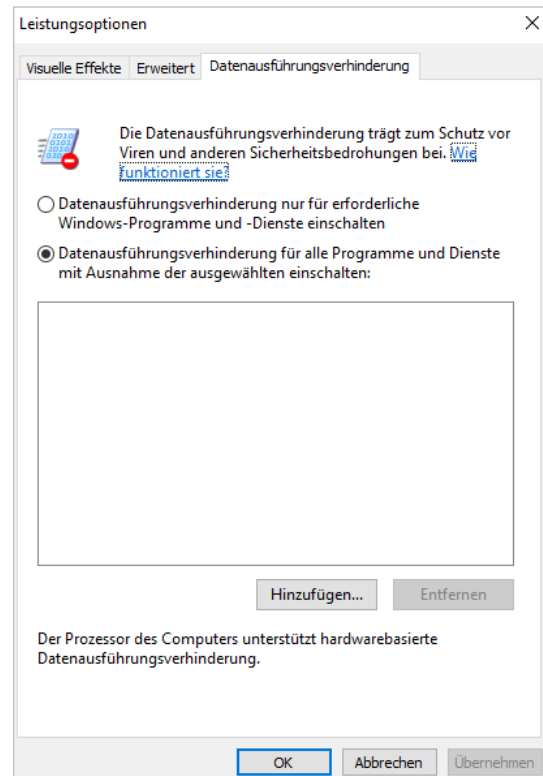
Werden Exploitversuche in der Hardware erkannt, so beendet das Betriebssystem die betroffene Software zwangsweise und der Schad-Code kann nicht ausgeführt werden. Standardmäßig schützt Windows zunächst nur die eigenen Dienste und Programme, Sie können DEP aber auch für alle Programme und Dienste einschalten und dadurch die Sicherheit erheblich erhöhen.

Vor einer dauerhaften Umstellung sollten Sie testen, ob alle von Ihnen genutzten Programme damit kompatibel sind. Einige Software wird wegen unsauberer Programmierung fälschlicherweise wegen eines Exploits vom Betriebssystem beendet. Solche Programme können von DEP ausgenommen werden.

- ▶ Klicken Sie in den erweiterten Systemeinstellungen im Bereich *Leistung* auf *Einstellungen*.
- ▶ Klicken Sie in den Leistungsoptionen auf das Register *Datenausführungsverhinderung*.
- ▶ Wählen Sie die von Ihnen gewünschte Option der DEP-Einstellungen aus.

Software, die bei aktiviertem DEP nicht mehr lauffähig ist, können Sie zu der Liste mit Ausnahmen hinzufügen.

Windows verfügt zusätzlich über eine Software-DEP, die auch auf Computern ohne DEP-Hardwareunterstützung funktioniert. Diese Funktion wird ebenfalls über die Datenausführungsverhinderung eingeschaltet. Die Software-DEP ist kein Ersatz für die Hardware-DEP, sondern nur eine Ergänzung.



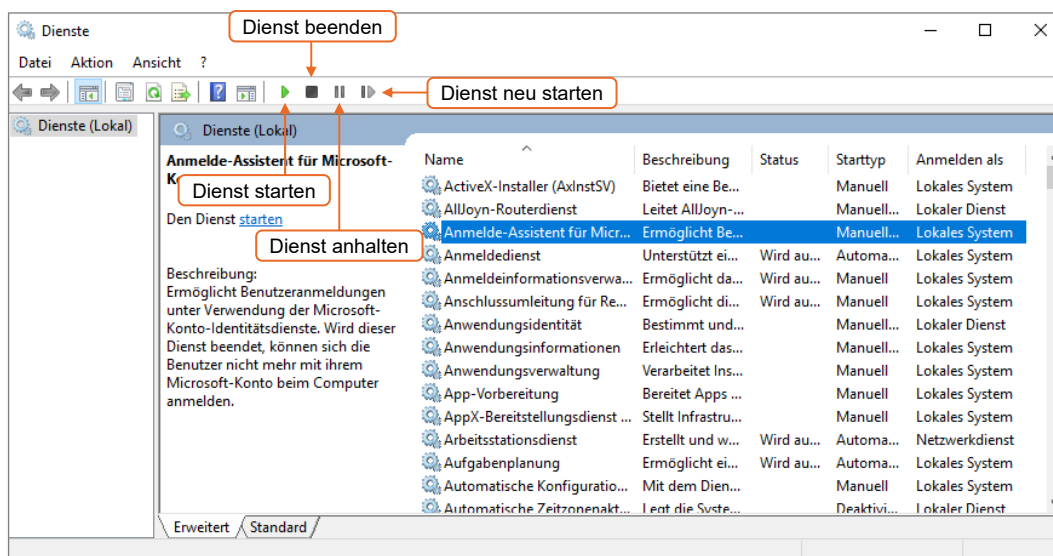
DEP konfigurieren

5.6 Dienste starten und verwalten

Dienstverwaltung öffnen

- ▶ Betätigen Sie  und geben Sie im Startmenü `services.msc`  ein.
oder Öffnen Sie *Dienste* in der Liste *Tools* im Server-Manager.

Dienste sind Komponenten des Betriebssystems, die im Hintergrund arbeiten, wie z. B. das Windows-Ereignisprotokoll oder der Sicherheitskonto-Manager. Nur wenn Sie Mitglied der Gruppe der Administratoren sind, können Sie alle Dienste verwalten.



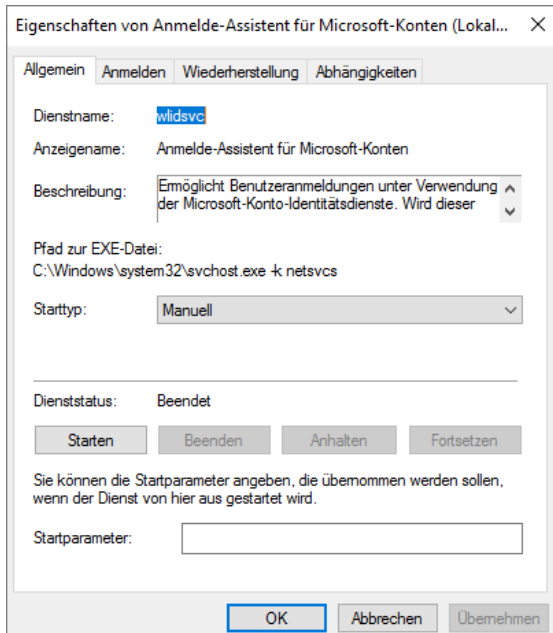
In der Spalte *Beschreibung* erhalten Sie eine kurze Beschreibung des Dienstes. Durch Markieren eines Dienstes und Klicken auf die entsprechenden Symbole können Sie den Dienst starten, beenden, anhalten und neu starten.

Überblick über einige Standarddienste von Windows

Einige wichtige Standarddienste von Windows Server 2022	
Anmelddienst	Unterstützt bei Arbeitsstationen das Weiterleiten der Echtheitsbestätigung bei der Anmeldung in der Domäne, auch bekannt als LSASS-Systemdienst
Aufgabenplanung	Erlaubt die automatische Ausführung von Aufgaben über den Taskplaner
Benutzerprofildienst	Erforderlich für lokale und Domänenanmeldungen
Computerbrowser	Verwaltet die aktuelle Liste der Computer und stellt diese Anwendungen zur Verfügung
DHCP-Client	Empfang dynamischer IP-Adressen und DNS-Aktualisierungen
DNS-Client	Ermöglicht Anfragen an einen DNS-Server zur Namensauflösung
Druckwarteschlange	Verwaltet die anfallenden Druckdateien
Server	Unterstützung für Freigaben und Datenverbindungen zwischen Netzwerkprozessen
Windows-Ereignisprotokoll	Zeichnet Ereignisse, Warnungen und Fehler im System-, Sicherheits- oder Anwendungsprotokoll auf

Dienst verwalten

- ▶ Klicken Sie doppelt auf den gewünschten Dienst.
- ▶ Falls erforderlich geben Sie im Eingabefeld einen Startparameter ein.
- ▶ Klicken Sie auf eine der vier Schaltflächen, um den Dienst zu starten, zu beenden, anzuhalten oder fortzusetzen.



Beachten Sie beim Verwalten von Diensten die Angaben im Register *Abhängigkeiten*. Dort können Sie einsehen, mit welchen anderen Diensten der ausgewählte Dienst verbunden ist. Im oberen Bereich sehen Sie, welche Dienste laufen müssen, damit dieser Dienst gestartet werden kann. Im unteren Bereich sehen Sie, welche Dienste von diesem Dienst abhängen.

Im Register *Wiederherstellung* können Sie festlegen, welches Verhalten Windows Server 2022 zeigen soll, wenn es zu einem Ausfall des Dienstes kommt. Unter Umständen kann es sinnvoll sein, den Dienst oder sogar den Server automatisch neu zu starten.

Starttyp festlegen

Für jeden Dienst können Sie festlegen, ob er manuell oder automatisch gestartet werden oder auch im laufenden Betrieb deaktiviert werden soll.

- ▶ Stellen Sie im Listenfeld den gewünschten Starttyp ein.

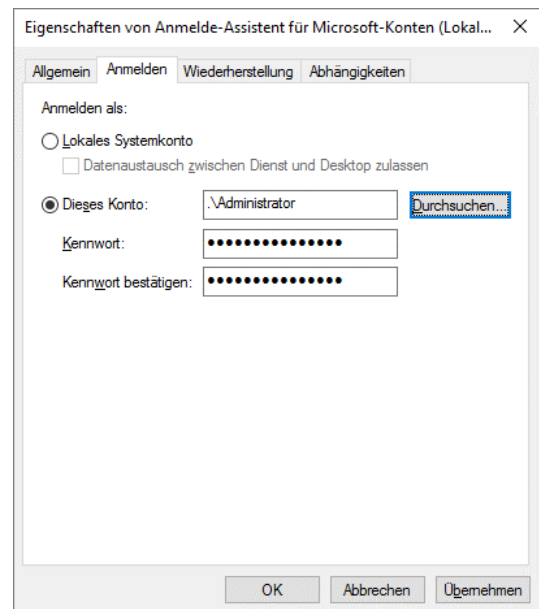
Starttyp	Beschreibung
<i>Automatisch (verzögerter Start)</i>	Dienst startet automatisch nach dem Hochfahren des Systems
<i>Automatisch</i>	Dienst startet automatisch während des Hochfahrens des Systems
<i>Manuell</i>	Dienst muss vom Benutzer oder von einem anderen Dienst gestartet werden
<i>Deaktiviert</i>	Dienst kann weder vom Benutzer noch von einem anderen Dienst gestartet werden

Dienst mit einem Benutzerkonto anmelden

Sie können einige Dienste so konfigurieren, dass diese sich beim Start mit einem bestimmten Benutzerkonto anmelden und mit den Berechtigungen dieses Benutzerkontos Ihre Arbeit verrichten. Im Normalfall sollten Sie zu diesem Zweck vorher ein spezielles Benutzerkonto angelegt haben.

Der SQL-Server verlangt beispielsweise, dass bestimmte seiner Dienste mit einem Dienstkonto gestartet werden.

- ▶ Nach einem Doppelklick auf den entsprechenden Dienst in der Liste wechseln Sie in das Register *Anmelden*.
- ▶ Aktivieren Sie das Optionsfeld *Dieses Konto* und tragen Sie in die Eingabefelder den Benutzernamen und zweimal das Kennwort ein.



Achten Sie darauf, dass beim angegebenen Benutzer das Kennwort niemals abläuft, sonst kann der Dienst irgendwann nicht mehr starten.

5.7 Geräte verwalten

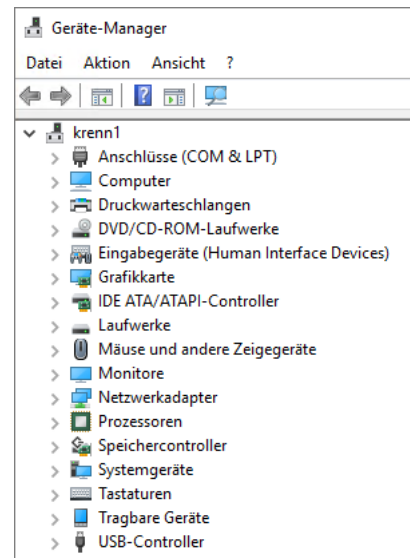
Geräte aktivieren und deaktivieren

Das Aktivieren und Deaktivieren von Geräten ist dann sinnvoll, wenn Sie nicht ständig mit der gleichen Hardware arbeiten. Durch das Deaktivieren eines Geräts halten Sie den entsprechenden Gerätetreiber an und Windows versucht nicht mehr, auf dieses Gerät zuzugreifen. Nur Mitglieder der Gruppe der Administratoren können diese Änderungen vornehmen.

- ▶ Öffnen Sie im Server-Manager unter *Diagnose* den *Geräte-Manager*. *Andere Geräte* zeigt Hardware, die Windows zwar erkannt hat, aber nicht automatisch installieren kann. Hier fehlen meist passende Treiber, es kann sich aber auch um ein Hardwareproblem oder einen Ressourcenkonflikt handeln.
- ▶ Klicken Sie mit rechts auf das Gerät, dessen Status Sie ändern möchten.
Hier können Sie die Treibersoftware aktualisieren, das Gerät aktivieren oder deaktivieren oder die Eigenschaften bearbeiten.

Die Möglichkeiten, den Status eines Geräts zu ändern, sind abhängig von der Hardware und den verwendeten Treibern. Einige Geräte können Sie vielleicht nur entfernen, nicht aber deaktivieren.

Ein deaktiviertes Gerät wird mit einem schwarzen Pfeil versehen, z. B. .

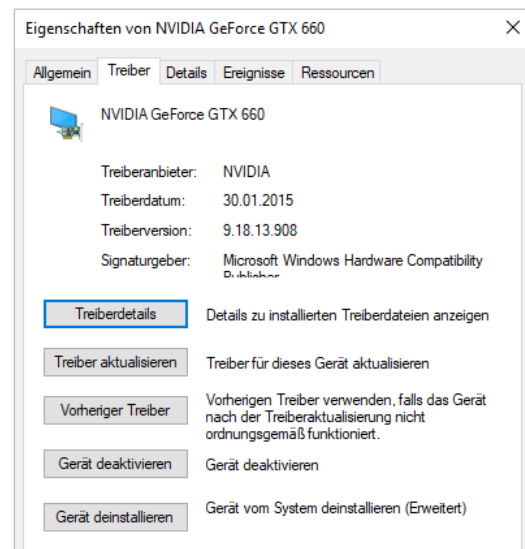


Eigenschaften eines Geräts

In den Eigenschaften eines Geräts erhalten Sie weitere Informationen im Register *Details*. Im Register *Ressourcen* können Sie bei einigen Geräten die Ressourcenzuordnung verändern. Im Register *Treiber* können Sie sich die benutzten Treiberdateien anzeigen lassen.

Sollte ein Gerät nach einer Treiberaktualisierung nicht mehr korrekt funktionieren, dann können Sie auf den vorherigen Treiber zurückschalten.

Je nach ausgewähltem Gerät kann die Anzahl der Register abweichen.



Mehrsprachige Tastaturbelegungen verwalten

Haben Sie ein englischsprachiges Windows-System vorliegen, oder auch eine Installation in einer anderen Sprache, können Sie beliebig weitere Sprachen installieren. Diese stehen bei Microsoft über *.cab-Dateien zur Verfügung. Sie installieren die *.cab-Datei und aktivieren die Sprache in Windows. Zukünftig wird die Oberfläche in der gewünschten Sprache angezeigt.

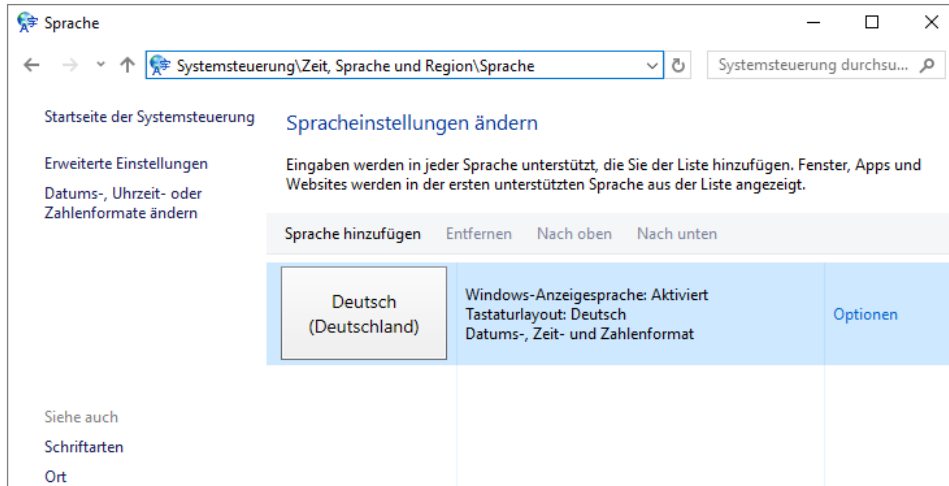
Liegt Ihnen die Sprachdatei vor, suchen Sie im Startmenü nach *lpksetup*. Hier können Sie anschließend die Sprache installieren.

Haben Sie die Sprache installiert, müssen Sie diese aber noch aktivieren. Dazu müssen Sie in der entsprechenden Sprache des Betriebssystems zu *Systemsteuerung\Zeit, Sprache und Region\Sprache* wechseln. Klicken Sie anschließend auf die Sprache, die Sie aktivieren wollen und dann auf *Optionen*. Hier können Sie jetzt die Sprache aktivieren:

- ▶ Rufen Sie in der Systemsteuerung *Zeit, Sprache und Region\Sprache* auf. Falls Sie mehrere Sprachen installiert haben, können Sie auch auf das DEU-Symbol rechts unten in der Taskleiste klicken und *Spracheinstellungen* wählen.

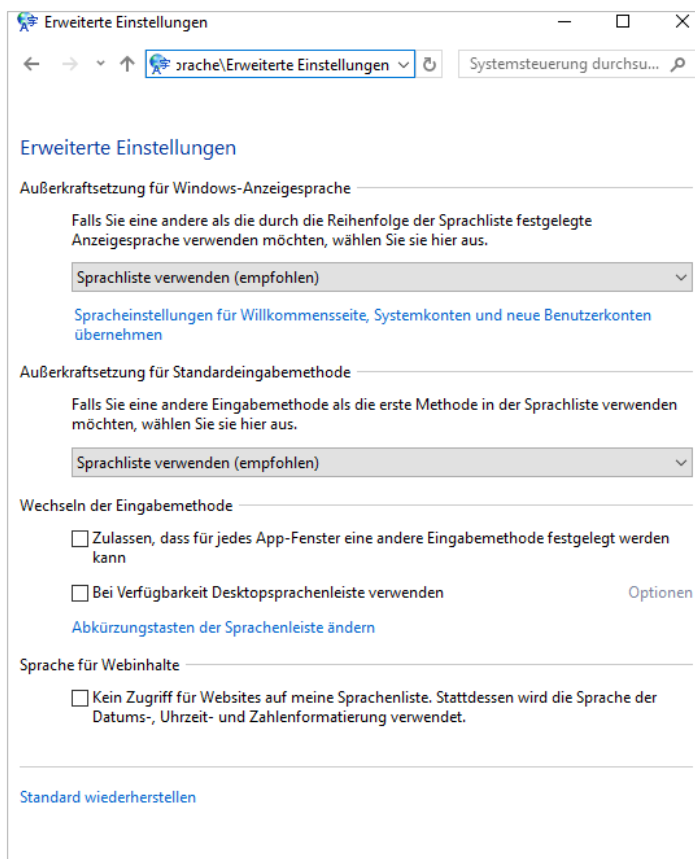
Im Listenfeld sehen Sie die momentan installierten Sprachen.

- ✓ Hier können Sie weitere Sprachen hinzufügen, markierte Sprachen entfernen und die Reihenfolge in der Liste verändern, wobei die oberste Sprache der Standard ist.
- ✓ In den erweiterten Einstellungen können Sie zusätzliche Einstellungen vornehmen.



Erweiterte Spracheinstellungen

Hier können Sie die voreingestellte Standardsprache für Windows und die Eingabesprache außer Kraft setzen. Außerdem können Sie für jedes App-Fenster eine andere Eingabemethode erlauben oder die Abkürzungstasten der Sprachenleiste ändern.



5.8 Energieverwaltung

Advanced Configuration and Power Interface (ACPI)

Die Energieverwaltung von Windows Server 2022 erfolgt mithilfe des Industriestandards ACPI (**A**dvanced **C**onfiguration and **P**ower **I**nterface), das ältere APM (**A**dvanced **P**ower **M**anagement) wird nicht mehr unterstützt.

ACPI ist der Standard für moderne Motherboards. Er besteht aus zwei Teilen, der Konfiguration (Unterstützung von Plug & Play) und der Energieverwaltung. ACPI-Boards können das Betriebssystem zum einen über die aktuelle Gerätekonfiguration und über die möglichen bzw. erlaubten Betriebsarten von ACPI-tauglichen Geräten informieren. Zum anderen kann Windows Server 2022 über ACPI die komplette Steuerung der Energieverwaltung und das Zu- und Abschalten von Geräten übernehmen. ACPI unterstützt z. B. das Herunterfahren von Festplatten oder das Abschalten momentan nicht benötigter USB-Geräte.

Ziel von ACPI ist eine flexible, zustandsorientierte Energieverwaltung, die zum einen erkennt, wenn ein Programm auch ohne Benutzereingaben Rechenleistung benötigt, und die dementsprechend die Prozessorleistung nicht reduziert, gleichzeitig aber Monitor, Grafikkarte und Drucker auf Stand-by-Betrieb setzt. Zum anderen kann der Computer durch das Signal eines Eingabegeräts (Maus, Tastatur, Touchpad) oder eines Netzwerkadapters aus einem Energiesparzustand schnell wieder aktiviert werden.

Wenn Sie überprüfen möchten, ob ein Windows-Computer ACPI verwendet, rufen Sie den Geräte manager auf und klicken Sie in der Geräteliste doppelt auf *Computer*. Bei einem Windows Server 2022 wird dort *ACPI-x64-basierter Computer* angezeigt.

Energiesparende Systemzustände

Server sollen meist rund um die Uhr verfügbar sein, daher wird der Stand-by-Modus normalerweise deaktiviert. In bestimmten Szenarien (z. B. Testumgebungen) können Energiesparfunktionen und Ruhezustand durchaus auch bei Servern sinnvoll sein. Im hybriden Stand-by-Modus von Windows Server 2022 wird der Computer in einen Energiesparmodus versetzt, in dem zunächst alle Inhalte des Arbeitsspeichers auf der Systemfestplatte gesichert werden (dieses Vorgehen entspricht dem Ruhezustand). Anschließend schaltet sich der Computer weitgehend ab, nur der Arbeitsspeicher wird noch mit Energie versorgt, um die Inhalte zu erhalten (entspricht dem herkömmlichen Stand-by-Modus). Durch Betätigen einer Taste wird der Computer wieder aktiviert. Wenn sich die Inhalte noch im Arbeitsspeicher befinden, kann die Arbeit schnell fortgesetzt werden, anderenfalls wird beim Einschalten des Computers der Speicherinhalt aus der Ruhezustands-Datei *hiberfil.sys* von der Festplatte eingelesen und die Arbeit kann am zuvor gesicherten Punkt fortgesetzt werden.

Ruhezustand und Stand-by

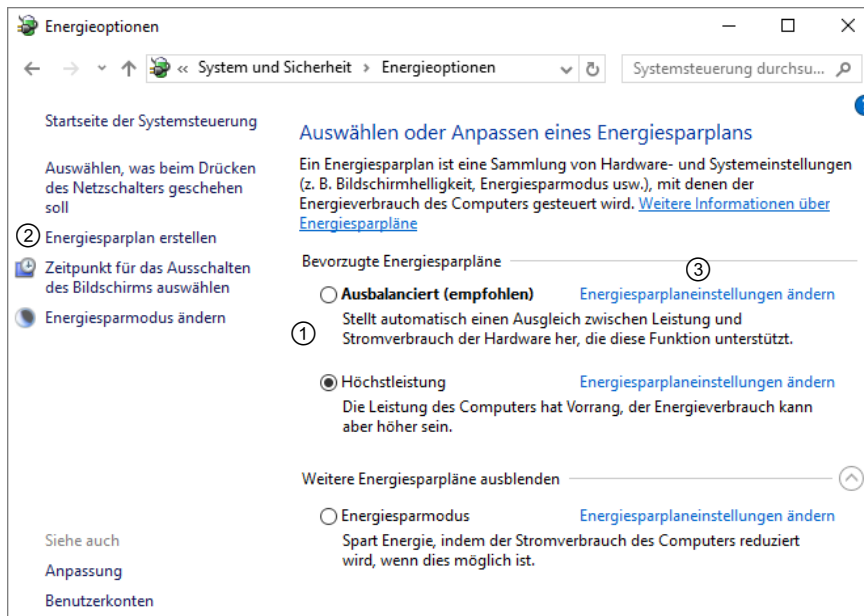
Die aus älteren Windows-Betriebssystemen bekannten Zustände Stand-by (eine Sicherung der Speicherinhalte nur im Arbeitsspeicher) und Ruhezustand (Sicherung der Speicherinhalte nur auf der Festplatte) sind nicht mehr offen verfügbar. Im Verborgenen sind beide Modi noch vorhanden und sie lassen sich auf Wunsch in den erweiterten Einstellungen eines Energiesparplans getrennt voneinander aktivieren.

Mit **[Alt]** **[F4]** vom Desktop aus öffnen Sie den Dialog *Windows herunterfahren*, wo Sie zwischen *Energie sparen*, *Herunterfahren* und *Neustart* wählen können.

Sie können mit Energiesparplänen das Energiesparverhalten des Systems festlegen. Darin wird in zahlreichen Einstellungen bestimmt, wie schnell und unter welchen Bedingungen das System in einen Energiesparzustand wechseln kann. Es liegen mit *Ausbalanciert (empfohlen)*, *Energiesparmodus* und *Höchstleistung* bereits vordefinierte Pläne vor.

Energiesparplan auswählen und anpassen

- ▶ Öffnen Sie die Systemsteuerung und klicken Sie auf *System und Sicherheit*.
- ▶ Klicken Sie auf den Hyperlink *Energieoptionen*. Sie erreichen das Fenster auch über das Starten von „powercfg.cpl“.
- ▶ Führen Sie Ihre Anpassungen durch, indem Sie den entsprechenden Link anklicken ①.



Energieschema auswählen und anpassen

Neuen Energiesparplan erstellen

- ▶ Wenn Ihnen keiner der vorgegebenen Pläne zusagt, erstellen Sie einen neuen Plan ②.
- ▶ Wählen Sie dazu als Basis einen bestehenden Plan aus und stellen Sie ein, nach welcher Zeit sich der Bildschirm ausschalten und der Energiesparmodus aktiviert werden soll.
- ▶ Bestätigen Sie mit *Erstellen*.
Der neue Plan ist jetzt aktiv.
- ▶ Um genauere Einstellungen vorzunehmen, klicken Sie erst auf *Energiesparplaneinstellungen ändern* ③ und anschließend auf *Erweiterte Einstellungen ändern*.
Hier finden Sie unter anderem Einstellungen zum hybriden Stand-by-Modus, zu adaptiver Bildschirmhelligkeit, Kennworteingabe nach Stand-by, Energiesparen verhindern bei Medienwiedergabe und Medienbibliotheks freigaben und Standardaktionen beim Betätigen des Netzschalters.

Falls Sie einen Plan löschen möchten, müssen Sie zuerst auf einen anderen Plan umschalten. Erst dann können Sie ihn in *Energiesparplaneinstellungen ändern* löschen.

6 Hardware hinzufügen

6.1 Hardware-Komponenten und Treiber verwenden

Windows Server 2022 und Plug & Play

Der Schwerpunkt der Hardware-Verwaltung von Windows Server 2022 liegt auf Plug & Play. Plug & Play ermöglicht es, dass Geräte automatisch erkannt, installiert und verwendet werden können. Dazu müssen folgende Voraussetzungen erfüllt sein:

- ✓ Plug-&-Play-fähige Komponente (Standard)
- ✓ Plug-&-Play-BIOS mit ACPI (Advanced Configuration and Power Management) (Standard)
- ✓ Plug-&-Play-Betriebssystem (Standard), z. B. Windows Server 2022. Das System konfiguriert die Komponente so weit wie möglich automatisch, lädt den passenden Treiber und startet das neue Gerät.

ACPI ist Voraussetzung für die Installation von Windows Server 2022 und sorgt dafür, dass Windows die volle Kontrolle über die Hardwareverwaltung und -konfiguration erhält. Früher musste diese Aufgabe vom BIOS übernommen werden.

Treiber für die Hardware-Komponenten

Die Kommunikation von Hardware-Komponenten mit dem Betriebssystem wird über **Treiber** abgewickelt. Treiber sind kleine Programme, die das Betriebssystem benötigt, um Hardware-Komponenten verwenden zu können. Sie sind spezifisch auf die Hardware-Komponente abgestimmt und müssen daher bei Austausch einer Komponente ebenfalls ersetzt werden. Windows Server 2022 kann entweder von Microsoft bereitgestellte Treiber oder die Treiber des Hardware-Herstellers verwenden.

Windows Server 2022 unterstützt das Windows Driver Model (WDM) und das Windows Display Driver Model (WDDM), insbesondere für Audio- und Videogerätetreiber. In WDM- und WDDM-Treibern werden hardware-nahe Funktionen nicht implementiert – das erledigen Kernfunktionen von Windows selbst. Dies bewirkt, dass bei einem Treiberwechsel oder bei einer Aktivierung und Deaktivierung des betroffenen Gerätes das Betriebssystem seltener neu gestartet werden muss. Direkte Hardwarezugriffe durch die Treiber werden von Windows nicht zugelassen, was für ein stabileres Betriebssystem und eine wirksame Durchsetzung von Kopierschutzmaßnahmen für Audio- und Videodaten sorgt (DRM – **D**igital **R**ights **M**anagement).

Windows Server 2022 setzt außerdem eine **digitale Signatur** für Treiber und einen speziellen **Treiberschutz** ein, um Probleme mit falschen oder fehlerhaften Treibern zu vermeiden.

Signierte Treiber

Microsofts Windows Hardware Quality Lab (WHQL) überprüft Treiber auf Funktion und Betriebssicherheit unter Windows Server 2022. Wenn ein Treiber diese Tests besteht, wird er mit einer digitalen Signatur versehen und erhält das Windows-Logo. Auch Hersteller können ihre Treiber selbst signieren. Sie sind dann zwar nicht WHQL-zertifiziert, lassen sich aber in allen Windows-Versionen installieren. Diese zertifizierten oder signierten Treiber sollen eine höhere Stabilität und Sicherheit bieten und weniger Probleme verursachen. Alle Systemdateien und mitgelieferten Treiber von Windows Server 2022 besitzen eine solche digitale Signatur.



Der spezielle Kernelschutz-Modus von Windows Server verbietet grundsätzlich die Installation unsignierter Treiber. Es gibt allerdings die Möglichkeit, den Treiber selbst zu signieren. Auf diese Weise kann das Problem elegant gelöst werden. Alternativ kann das Betriebssystem mit deaktivierter Prüffunktion über die erweiterten Startoptionen ① gestartet werden.



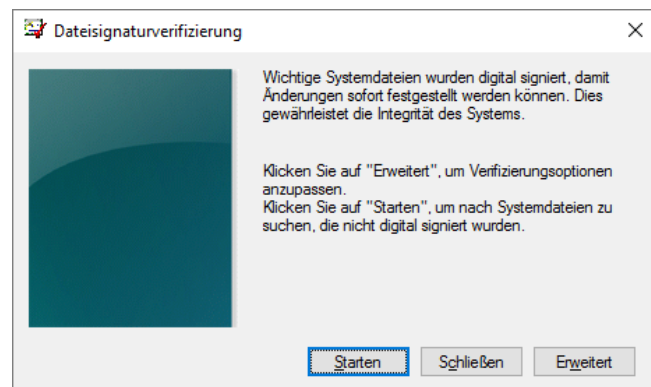
Microsoft bietet zum Signieren von Software das Windows Driver Kit (WDK) für Windows 11 und Windows Server 2022 kostenlos zum Download an. Weitere Informationen finden Sie in der WDK-Dokumentation.

✓ <https://docs.microsoft.com/de-de/windows-hardware/drivers/download-the-wdk>

Treibersignatur überprüfen

Als Administrator können Sie alle Treibersignaturen des Systems mit einem Prüfprogramm testen.

- ▶ Geben Sie im Startmenü `sigverif` ein.
- ▶ Beginnen Sie die Prüfung mit Klick auf die Schaltfläche *Starten*.

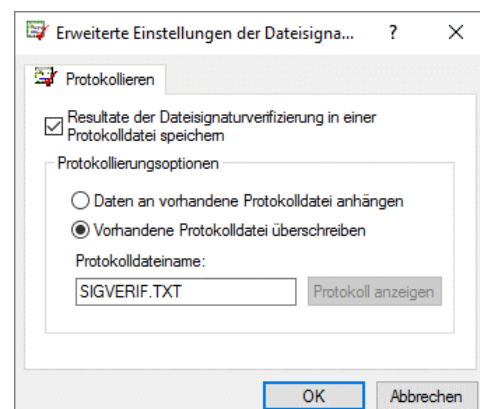


Überprüfung aller Signaturen im System

Protokolldatei einstellen

Vor dem Start der Prüfung können Sie noch Einstellungen zur Protokolldatei vornehmen:

- ▶ Klicken Sie im Dialogfenster *Dateisignaturverifizierung* auf *Erweitert*.
- ▶ Hängen Sie das Protokoll an eine bestehende Protokolldatei an oder wählen Sie den Speicherort und Dateinamen für eine neue Protokolldatei.
Sie können die Speicherung auch ganz ausschalten.
- ▶ Schließen Sie den Dialog mit *OK*.



Einstellungen zur Protokolldatei

6.2 Hardware automatisch installieren

Plug-&-Play-Hardware installieren

Seit einigen Jahren ist alle PC-Hardware Plug-&-Play-fähig. Die Installation neuer Geräte ist daher recht einfach, erfordert meist keine Benutzereingriffe und setzt keine Administratorberechtigungen voraus. Die Erkennung neuer Hardware und deren Installation laufen im Hintergrund ab und sind nur durch ein minimiertes Fenster auf dem Desktop ersichtlich.

Bei zahlreicher Serverhardware ist es möglich, interne Bauteile und Steckkarten während des laufenden Betriebs auszutauschen. Überzeugen Sie sich unbedingt vor dem Austausch davon, dass dies vom Hersteller vorgesehen ist. Im Zweifelsfall sollten Sie den Server herunterfahren.

Externe Geräte installieren

- ✓ Geräte für USB (Universal Serial Bus), IEEE 1394 (FireWire), eSATA, Thunderbolt sowie PCMCIA- und ExpressCards können Sie im laufenden Betrieb anschließen.
- ✓ Ältere Legacy-Geräte für die alten seriellen, parallelen oder PS/2-Schnittstellen, beispielsweise Modems, Drucker oder Tastaturen, dürfen nur bei ausgeschaltetem Computer angeschlossen werden.

Das neue Gerät wird zunächst automatisch identifiziert. Sind passende Klassentreiber verfügbar, werden diese ohne Nachfrage oder Meldung installiert. Hierzu durchsucht Windows Server 2022 seine Treiberdatenbank, die deutlich umfangreicher ist und wesentlich mehr Klassentreiber für Gerätegruppen enthält als bei älteren Windows-Versionen. Anschließend ist das neue Gerät verwendbar. Falls kein geeigneter Treiber für die Hardware-Komponente gefunden wurde, können Sie entweder aus einer Liste von Treibern auswählen, den Pfad zur Treibersoftware eingeben oder über Windows Update danach suchen lassen.

Interne Erweiterungskarten installieren

- ▶ Um eine PCI- oder PCI-Express-Erweiterungskarte in einem Server zu installieren, schalten Sie diesen zunächst aus.
Dies gilt auch für das Einsetzen von Speicherriegeln und den Einbau interner Datenträger.
- ▶ Ziehen Sie den Netzstecker, öffnen Sie das Gehäuse und treffen Sie Maßnahmen gegen statische Aufladung, bevor Sie elektronische Bauteile berühren.
- ▶ Setzen Sie die Karte in einen geeigneten Steckplatz und sichern Sie sie mit Schrauben oder Klemmen gegen Herausrutschen. Schließen Sie das Gehäuse und schalten Sie den Computer wieder ein.

Nach dem Einschalten läuft die Installation ab wie oben beschrieben.



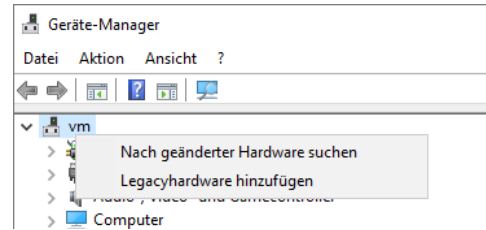
Manche Einbauteile benötigen zusätzliche Stromversorgung. Versichern Sie sich, dass das Netzteil über ausreichende Leistungsreserven verfügt, bevor Sie diese anschließen.

Nicht Plug-&-Play-fähige Hardware automatisch installieren

Falls Sie sehr alte Geräte unter Windows Server 2022 betreiben müssen, die noch kein Plug & Play unterstützen, stehen die Chancen eher schlecht, dafür einen funktionierenden Treiber zu finden. Der Versuch ist davon abhängig, ob es vergleichbare moderne Hardware am Markt gibt und wie hoch die Kosten für die Anschaffung sind. Schnell kommen beim Experimentieren viele Arbeitsstunden zusammen.

Der Hardware-Assistent von Windows Server 2022 kann oftmals auch nicht Plug-&-Play-fähige Geräte erkennen und automatisch installieren. Sie benötigen dafür Administratorberechtigungen.

- ▶ Öffnen Sie den Geräte-Manager mit einem Klick im Schnellzugriffsmenü oder betätigen Sie  und klicken Sie auf *Geräte-Manager*.
- ▶ Klicken Sie mit der rechten Maustaste auf den Namen Ihres Computers und wählen Sie *Legacyhardware hinzufügen*.

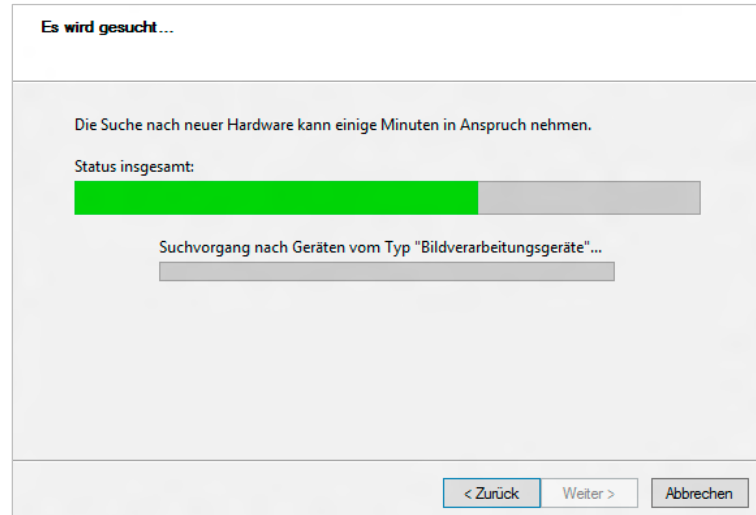


Installation von alten Geräten

Der Hardware-Assistent sucht nun nach neuen Hardware-Komponenten. Falls dabei eine Komponente erkannt wird, kann sie jetzt installiert werden und Sie erhalten eine entsprechende Meldung.

- ▶ Gehen Sie alle Installationsschritte mit dem Assistenten durch.
- ▶ Beenden Sie den Assistenten mit *Fertig stellen*.
Die Komponente ist jetzt installiert und betriebsbereit.

Die automatische Hardware-Erkennung funktioniert bei alten Geräten manchmal nicht. In diesem Fall müssen Sie die Installation manuell mit dem Hardware-Assistenten durchführen.



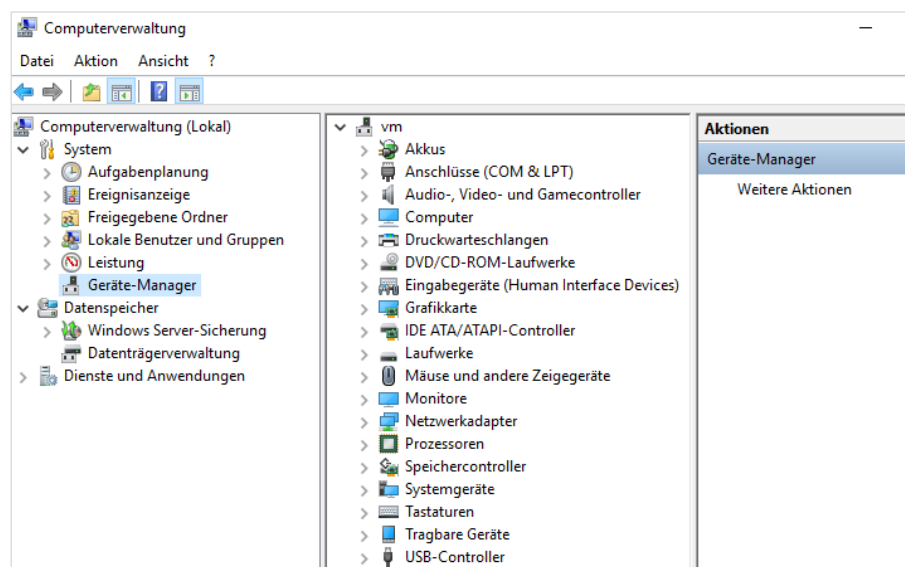
Der Hardware-Assistent sucht neue Komponenten

6.3 Hardware manuell konfigurieren

Hardware-Komponenten mit dem Geräte-Manager konfigurieren

Mit dem Geräte-Manager können Sie installierte Hardware-Komponenten manuell konfigurieren, mögliche Probleme beheben und neue Treiber für die Komponenten installieren. Ein Eingriff ist normalerweise nur erforderlich, wenn bei der Installation Probleme aufgetreten sind. Sie können den Geräte-Manager auch über die Computerverwaltung erreichen:

- ▶ Klicken Sie im Schnellzugriffsmenü auf *Computerverwaltung*.
- ▶ Wählen Sie das Snap-In *Geräte-Manager*.
Der Geräte-Manager zeigt in einer Liste die installierten Geräte an und markiert ein Gerät mit Problemen oder noch fehlenden Treibern mit einem gelben Ausrufungszeichen ⚠.
- ▶ Klicken Sie doppelt auf das Gerät, das konfiguriert werden soll.



Die Liste installierter Hardware im Snap-In „Geräte-Manager“

Je nach Komponententyp bietet das folgende Dialogfenster mehrere Register an, beispielsweise *Allgemein*, *Treiber* und *Ressourcen*.

Im Register *Allgemein* erhalten Sie Informationen über den Betriebszustand der Komponente und können diese aktivieren oder deaktivieren.

Im Register *Treiber* können Sie Detailinformationen zum Gerätetreiber abrufen oder den Treiber aktualisieren.

Im Register *Ressourcen* werden der E/A-Adressbereich (Eingabe/Ausgabe), der Speicherbereich und der IRQ (Interrupt Request, Unterbrechungsanforderung für den Prozessor) konfiguriert.

- ▶ Deaktivieren Sie *Automatisch konfigurieren*.
- ▶ Markieren Sie im Register *Ressourcen* die betreffende Ressource und klicken Sie auf *Einstellung ändern*. Falls dies nicht zugelassen wird, ändern Sie die Einstellung im Listefeld, wo verschiedene Basis-konfigurationen angeboten werden.
- ▶ Geben Sie die erforderlichen Werte für jede Ressource an und klicken Sie auf *OK*.
Falls die gewählte Einstellung zu Konflikten mit anderen Hardware-Komponenten führt, erscheint eine Warnmeldung und Sie müssen andere Werte verwenden.

Bei Plug-&-Play-Komponenten übernimmt Windows die Vergabe der Ressourcen, und die Einstellungsoptionen sind nicht verfügbar. Die Einstellungen für ein manuell zu installierendes Gerät finden Sie in der Dokumentation zu diesem Gerät. Stellen Sie sicher, dass die Einstellungen im Register *Ressourcen* mit diesen Werten übereinstimmen.

6.4 Hardware deaktivieren und deinstallieren

Hardware vorübergehend deaktivieren

- ▶ Starten Sie den Geräte-Manager über das Schnellzugriffsmenü.
- ▶ Öffnen Sie in der Liste die betreffende Gerätekategorie ① und klicken Sie mit der rechten Maustaste auf die gesuchte Komponente.
- ▶ Klicken Sie im Kontextmenü auf *Deaktivieren* und bestätigen Sie die folgende Warnmeldung mit *Ja*.



Die betreffende Komponente wird jetzt abgeschaltet und kann nicht mehr verwendet werden. Sie wird deshalb im Geräte-Manager mit einem Pfeil nach unten ⬇ markiert, der leicht zu übersehen ist.

Hardware deaktivieren oder deinstallieren

- ▶ Klicken Sie im Kontextmenü der Komponente auf *Aktivieren*, um sie wieder zu verwenden.

Hardware dauerhaft deinstallieren

- ▶ Starten Sie den Geräte-Manager und navigieren Sie zu der betreffenden Komponente.
- ▶ Öffnen Sie mit der rechten Maustaste das Kontextmenü und klicken Sie auf *Deinstallieren*, um die Komponente dauerhaft zu entfernen.
- ▶ Bestätigen Sie die angezeigte Warnmeldung mit *OK*. Die Komponente wird jetzt deinstalliert.
- ▶ Schalten Sie den Computer ab und entfernen Sie jetzt die Komponenten aus dem Computer.

Beachten Sie, dass deinstallierte Plug-&-Play-Komponenten beim Neustart des Computers erneut installiert werden, solange sie eingebaut oder angeschlossen sind. Komponenten, die angeschlossen bleiben, aber nicht erneut installiert werden sollen, müssen Sie deshalb deaktivieren.

Nicht im Geräte-Manager angezeigte Hardware entfernen

Einige nicht Plug-&-Play-fähige Treiber sowie Geräte, die bisher installiert waren, jetzt aber nicht mehr angeschlossen sind, werden im Geräte-Manager standardmäßig nicht angezeigt. Sie müssen diese Komponenten erst sichtbar machen, damit sie entfernt werden können.

- ▶ Starten Sie den Geräte-Manager und klicken Sie im Menü *Ansicht* auf *Ausgeblendete Geräte anzeigen*. Anschließend werden alle Komponenten angezeigt und Sie können die Hardware wie üblich entfernen.

Hot-Plugging-fähige Hardware entfernen

Externe Anschlüsse wie FireWire, PC- und ExpressCard, Speicherkartenleser und USB unterstützen Hot Plugging, also das Entfernen von Geräten im laufenden Betrieb. Durch vorzeitiges Entfernen einer Komponente besteht jedoch bei Speichermedien die Möglichkeit, dass Daten verloren gehen, daher sollten Sie alle externen Datenträger auf folgende Art entfernen:

- ▶ Klicken Sie in der Taskleiste auf das Symbol *Hardware sicher entfernen*.
- ▶ Klicken Sie in der angezeigten Liste auf das zu entfernende Gerät, um es anzuhalten. Alle Operationen werden zu Ende geführt und das Gerät wird aus dem System abgemeldet.
- ▶ Warten Sie die Meldung ab, dass das Gerät jetzt entfernt werden kann, bevor Sie es abziehen.

6.5 Treiber- und Hardware-Probleme behandeln

Bedeutung der Hardware-Probleme

Nicht korrekt installierte und konfigurierte sowie fehlerhafte Hardware-Komponenten können schwere Probleme verursachen. Das Betriebssystem kann instabil werden oder lässt sich überhaupt nicht mehr starten. Windows Server 2022 bietet mehrere Verfahren zur Vermeidung und Lösung solcher Probleme:

- ✓ Installation nicht signierter Treiber verhindern
- ✓ Treiberaktualisierung und Treiberzurücksetzung
- ✓ Abgesicherter Modus
- ✓ Systemwiederherstellung

Treiber für ältere Windows-Versionen im Kompatibilitätsmodus installieren

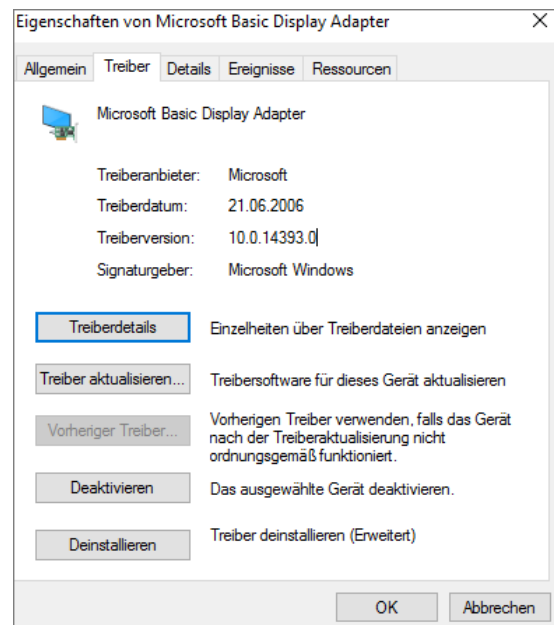
Häufig fehlt es nach Markteinführung einer neuen Windows Server-Edition an passenden Treibern für Hardware und für ältere Geräte werden nur selten angepasste Treiber bereitgestellt. Außerdem stellen viele Hersteller nur Treiber für Clientbetriebssysteme bereit. Da sich am Aufbau der Treiber seit Windows Vista nichts Grundlegendes geändert hat, stehen die Chancen gut, dass ein 64-Bit-Treiber für Windows 7, 8, 8.1, 10 oder Vista auch bei Windows Server 2012/2012 R2/2016/2019 oder 2022 funktioniert.

In einigen Fällen bricht die Treiberinstallation jedoch mit der Fehlermeldung ab, der Treiber sei für diese Betriebssystemversion nicht geeignet. Dieser Fehler tritt auf, wenn während der Installation die Version von Windows mit den Informationen aus der INF-Datei verglichen wird und nicht die Vorgaben erfüllt. Ein möglicher Ansatz zur Behebung ist das manuelle Ändern der INF-Dateien, es geht aber auch, das Treibersetup unter Verwendung der Kompatibilitätseinstellungen zu installieren. Allerdings ist dieses Vorgehen für produktive Serverhardware nicht zu empfehlen.

Treiber aktualisieren oder zurücksetzen

Wenn ein Treiber Probleme verursacht, können Sie versuchen, diesen durch eine neue Version zu ersetzen.

- ▶ Öffnen Sie den Geräte-Manager und navigieren Sie zur Komponente, deren Treiber durch eine neue Version ersetzt werden soll.
- ▶ Klicken Sie mit der rechten Maustaste auf den Eintrag der Komponente und dann auf *Eigenschaften*.
- ▶ Wechseln Sie in das Register *Treiber* und klicken Sie auf *Treiber aktualisieren*.
- ▶ Legen Sie mit dem Hardwareupdate-Assistenten fest, wie nach neuen Treibern gesucht werden soll. Alternativ können Sie auch einen Datenträger mit aktuellen Treibern angeben.
- ▶ Stellen Sie den Assistenten fertig. Windows Server verwendet jetzt den neuen Treiber. Falls dieser Treiber ebenfalls Probleme verursacht, können Sie ihn zurücksetzen und den alten Treiber wieder einsetzen.
- ▶ Klicken Sie auf *Vorheriger Treiber*, um wieder den alten Treiber zu verwenden.



Treiber aktualisieren oder zurücksetzen

Die jeweils aktuellen Treiber und Datenbanken über problematische Treiber erhalten Sie, wenn Sie die Funktion *Windows Update* verwenden. Dabei werden die lokalen Treiberdatenbanken aktualisiert und können anschließend für die Aktualisierung installierter Gerätetreiber verwendet werden.

6.6 Problembehandlung

Problembehandlungsdatenbank

Microsoft sammelt seit Jahren Informationen über instabile Treiber und Wechselwirkungen zwischen verschiedener Software und Windows-Versionen. Diese Daten werden während der Problembehandlung von Windows Server 2022 verwendet, um Hilfestellung und Lösungsvorschläge zu geben.

Häufige Fehler

Nicht korrekt installierte und konfigurierte Hardware-Komponenten sowie fehlerhafte Treiber gehören zu den häufigsten Problemursachen. Fehlerhafte Geräteinstallationen legen im schlimmsten Fall bereits beim ersten Neustart nach der Installation das gesamte Betriebssystem lahm. Sie können aber auch zu Konflikten mit anderen Komponenten und Anwendungen führen, die nicht sofort in Erscheinung treten, aber das System instabil werden lassen. Windows stellt mehrere Möglichkeiten zur Lösung von Problemen bereit, die nach der Installation neuer Hardware auftreten können.

Abgesicherter Modus

- ▶ Starten Sie den Computer neu. Betätigen Sie während des Startvorgangs  **F8**.
Falls Windows beim letzten Startversuch abgestürzt ist, öffnet sich die Windows-Fehlerbehebung auch ohne Tastendruck.
- ▶ Bewegen Sie die Markierung mit den Pfeiltasten zur Option *Abgesicherter Modus* und betätigen Sie .
- ▶ Wenn das System gestartet werden kann, rufen Sie die Systeminformationen auf. Ermitteln Sie durch Anzeigen möglicher Ressourcenkonflikte und Problemgeräte, ob die neue Hardware-Komponente die Problemursache ist.
- ▶ Deinstallieren oder entfernen Sie die Komponente mit dem Geräte-Manager.
Ist die Ursache eine Treiberaktualisierung, dann können Sie die Komponente auch im Geräte-Manager auf den vorherigen Treiber zurücksetzen.
- ▶ Beenden Sie Windows und entfernen Sie die neu hinzugefügte Hardware aus dem Computer.

Beschaffen Sie sich aktuelle Treiber, um das Gerät doch noch erfolgreich zu installieren, und suchen Sie im Internet nach Hinweisen zur Fehlerbehebung.

7 Einführung in Active Directory

7.1 Überblick über den Verzeichnisdienst

Active Directory 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 **Lightweight Directory Access Protocol** (LDAP) genutzt, weshalb gelegentlich auch von einem LDAP-Verzeichnisdienst gesprochen wird.

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 Verzeichniseintrag 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 Konfigurationspartition enthält Informationen über vorhandene Domänen und Vertrauensstellung.
- ✓ Die Domänen-Partition enthält alle Objekte einer bestimmten Domäne.

Der Inhalt der Schema- und der Konfigurationspartition 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 und anschließend durch das Hochstufen des Servers zum Domänencontroller (DC) konfiguriert werden.

7.2 Domäne, Struktur und Gesamtstruktur

Planung der Verzeichnisstruktur

Eine Verzeichnisstruktur sollte den Belangen der Firma, den Verwaltern und den Benutzern gerecht werden. Vor der Implementierung des Verzeichnisdiensts sind Firmenstruktur und Geschäftsbereiche im Hinblick auf logische Zusammenhänge zwischen Geschäftsprozessen, Abhängigkeiten und Hierarchien zu untersuchen. Geografische Gegebenheiten haben in der Regel keinen Einfluss auf die Planung von zu erstellenden Domänen.

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 Domäne einzurichten.

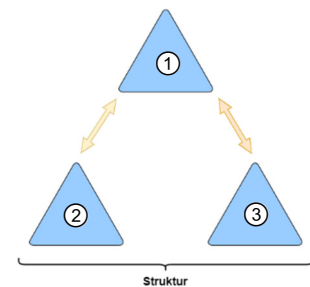
Eine Domäne erstellen Sie durch die entsprechende Installation eines Domänencontrollers. Die Namensgebung für Domänen orientiert sich am DNS-Namespace – dazu später mehr. Ein Domänencontroller (DC) speichert immer sämtliche Objekte seiner Domäne. Er kann niemals DC für mehrere Domänen sein.

Struktur

Eine Struktur entsteht, wenn Sie in Ihrem Active Directory weitere Domänen erstellen und ihnen den Namen einer Subdomäne (zu einer bestehenden Domäne) geben. Eine Struktur wird in der Literatur oft auch als Baum oder **Tree** bezeichnet.

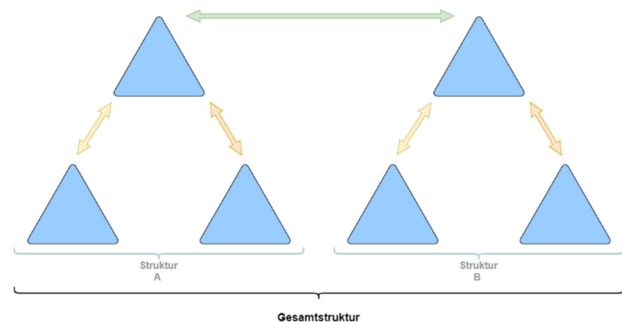
Beispiel

Ihre erste Domäne heißt *firma.intern* ① und Sie erstellen eine zusätzliche Domäne mit dem Namen *forschung.firma.intern* ②. Um die Abbildung umzusetzen, könnten Sie eine dritte Domäne erstellen und ihr den Namen *entwicklung.firma.intern* ③ geben.



Gesamtstruktur

Eine Gesamtstruktur entsteht, wenn Sie im Active Directory eine zusätzliche Domäne erstellen und als Bezeichnung nicht den Namen einer Subdomäne (zu einer vorhandenen Domäne) verwenden, z. B. *zusatzfirma.intern*. Dies setzt auch mindestens einen zusätzlichen DC voraus. Diese Domänen liegen dann neben- und nicht untereinander.



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.

Vertrauensstellungen

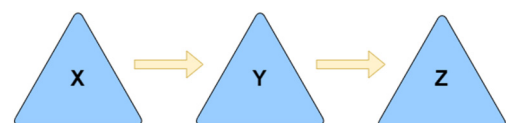
Innerhalb eines Active Directorys werden automatisch Vertrauensstellungen zwischen Domänen angelegt – symbolisiert durch die Pfeile in den beiden Abbildungen oben. Vertrauensstellungen ermöglichen es, dass Benutzer einer Domäne auf Ressourcen einer anderen Domäne zugreifen können.

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.



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.

7.3 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 2016* einen Windows Server 2012R2 zum DC hochzustufen, so wird das fehlschlagen. Mitgliedsserver dagegen sind nicht von der Einschränkung betroffen.



Sind die Voraussetzungen erfüllt, können Sie Funktionsebenen heraufstufen. Ein Herunterstufen ist nur mit Umwegen möglich und nicht empfohlen.

Domänenfunktionsebenen

Es folgt eine Auflistung wichtiger Erweiterungen, die in den einzelnen Funktionsebenen dazukommen:

- ✓ Windows Server 2008 R2 – verbesserte Kerberos-Authentifizierung
- ✓ Windows Server 2012/2012 R2 – Dynamic Access Control
- ✓ Windows Server 2016 – keine zusätzlichen Funktionen

Bei Windows Server 2022 wird als Domänen- und Gesamtstrukturfunktionsebene ebenfalls Windows Server 2016 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.

Gesamtstrukturfunktionsebenen

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

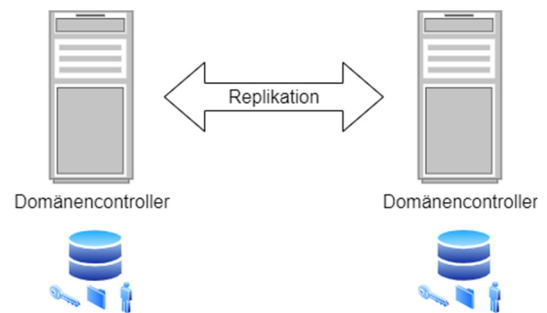
Fügen Sie Ihrem Active Directory neue Domänen hinzu, entspricht deren Domänenfunktionsebene der Gesamtstrukturfunktionsebene. Zum Heraufstufen der Gesamtstrukturfunktionsebenen benötigen Sie das MMC-Snap-In *Active Directory-Domänen und -Vertrauensstellungen*. Klicken Sie mit der rechten Maustaste direkt 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.

7.4 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 von jedem DC erledigt werden. Verändern Sie ein Objekt, so müssen diese Informationen auf die anderen Domänencontroller übertragen werden. Dieser Vorgang wird als **Replikation** bezeichnet. Active Directory verwaltet die Replikationstopologie (welche DCs tauschen ihre Informationen miteinander aus) automatisch. Manuelles Eingreifen ist nur in Spezialfällen notwendig.



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 physikalische Sicherung des Servers (Zugangsschutz, Diebstahlschutz) nicht gegeben ist. Sie können festlegen, welche Benutzerkonten zu einem RODC repliziert werden. Die fehlenden Schreibrechte stellen einen weiteren Schutz gegen Missbrauch dar.

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

- ✓ Gesamtstrukturfunktionsebene mindestens Windows Server 2003
- ✓ Mindestens ein beschreibbarer Domänencontroller mit einem Betriebssystem ab Windows Server 2008 R2 in der Domäne des RODC
- ✓ Ein Domänen-Admin muss den Befehl `adprep /rodcprep` ausgeführt haben.

Betriebsmaster (FSMOs)

Eine Flexible Single Master Operation (FSMO, Betriebsmaster) 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 Rollen sind einmalig in einer Gesamtstruktur, die darauffolgenden 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(Relative Identifier)-Master	Stellt die Eindeutigkeit von Domänen-Objekten sicher (SID-Generierung)
PDC(Primary Domain Controller)-Emulator	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.

Globaler Katalog – GC

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. GC-Server spielen eine wichtige Rolle, ohne die manche AD-Funktionen nicht funktionieren. Sie sollten jeden Domänencontroller auch zu einem globalen Katalog-Server machen.



Ist nicht jeder DC einer Domäne auch GC, dann darf der Infrastruktur-Master dort kein globaler Katalog-Server sein.

7.5 Organisationseinheit – OU

Sinn von Organisationseinheiten

Eine OU (**O**rganizational **U**nit) ist ein Objekt in einer Domäne, das verschiedenen Zwecken dient:

- ✓ Strukturiertes Speichern von Objekten, vergleichbar mit dem Speichern von Dateien in Ordnern
- ✓ Delegation 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.

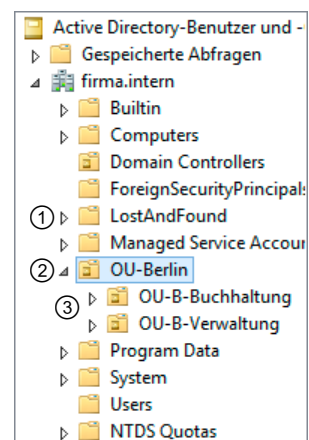
In den Aufbau Ihrer OU-Struktur sollten Sie einige Überlegungen stecken. Entwerfen Sie ein Schema und halten Sie dieses anschließend konsequent ein. Besonders wichtig ist hier die sinnvolle und einheitliche Benennung der einzelnen OUs. Das beginnt mit scheinbar trivialen Dingen, zum Beispiel sollten alle OUs „sprechende“ Namen erhalten, sodass Sie allein durch den Namen Hierarchie, Standort und Funktion erkennen können. 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.

Das Grundmuster vieler größerer Domänen wird in der Abbildung dargestellt:

Zunächst werden geografische Standorte abgebildet ②. Deren Inhalt wird dann weiter untergliedert ③. 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.

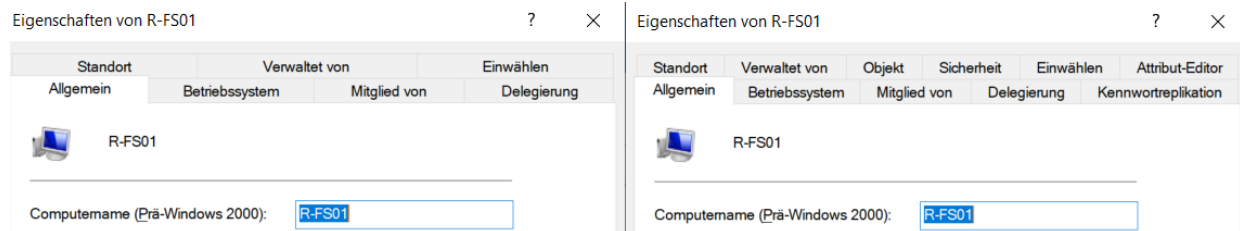
Bei einer zentralen Verwaltung macht es vielleicht eher Sinn, Standort-OUs erst auf der zweiten Ebene zu verwenden und auf der ersten z. B. nach Abteilung oder Funktion zu gliedern.

Sollte bei Ihnen z. B. der Container *LostAndFound* ① nicht angezeigt werden, können Sie im Menü *Ansicht - Erweiterte Features* einschalten.



OU-Struktur

Ohne diese Einstellung werden bei den Objekten bestimmte Eigenschaften nicht angezeigt und es fehlen weitere Optionen zur Bearbeitung.



Gegenüberstellung normale und erweiterte Feature-Ansicht

7.6 Standorte im Active Directory

Was ist ein Active Directory-Standort?

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) WAN-Verbindungen zusammenschließen müssen. Das ist immer mit verschiedenen IP-Netzen und Routing verbunden.

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

- ✓ Sie definieren **Standort-Namen**, 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 Standort-Namen.
- ✓ Sie verschieben Domänencontroller in die entsprechenden Standorte. An jedem Standort sollte ein globaler Katalog vorhanden 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, obwohl der Ortsname oft in der OU-Struktur der Domäne vorkommt. Beim Standort handelt es sich lediglich um eine Ortsbezeichnung für ein oder mehrere IP-Netze.

7.7 Sysvol

Ressourcen für Anmeldungen

Jeder Domänencontroller stellt bei der Anmeldung Gruppenrichtlinien zur Verfügung. Für die Benutzeranmeldung ist zusätzlich ein Anmeldeskript 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*.

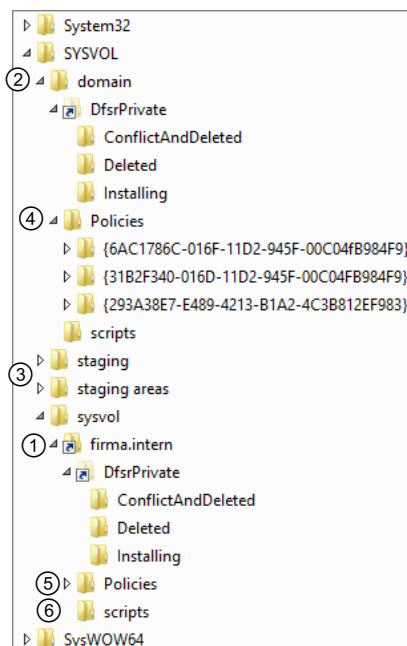
Der Ordner *SYSVOL\sysvol* ist auf jedem DC vorhanden und entspricht der Freigabe *SYSVOL*. Darin befindet sich ein Ordner mit dem Namen Ihrer Domäne ①. Das Pfeilsymbol signalisiert, dass es sich dabei um eine Verbindung handelt. Dieser Link zeigt auf den Ordner *SYSVOL\domain* ②, deshalb sind die angezeigten Inhalte auch identisch.

Die Ordner *SYSVOL\staging* ③ und *SYSVOL\staging areas* ③ werden für die Verwaltung der Replikation benötigt.

In den Ordnern *SYSVOL\domain\Policies* ④ und *SYSVOL\sysvol\<Domänenname>\Policies* ⑤ finden Sie mehrere Ordner, deren Namen mit einer geschweiften Klammer beginnen. Jeder dieser Ordner enthält ein Gruppenrichtlinienobjekt.

Der Ordner *SYSVOL\sysvol\<Domänenname>\scripts* ⑥ 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.

8 Domänencontroller installieren und neue Domäne erstellen

8.1 Installation der Verzeichnisdienste vorbereiten

Voraussetzungen

Bevor Sie anfangen, einen Domänencontroller zu installieren, müssen die folgenden Punkte geklärt sein:

- ✓ Vor der Installation des ersten Windows-Server-2022-Domänencontrollers in einer **vorhandenen** Gesamtstruktur bzw. Domäne muss diese mit ADPrep (s. u.) entsprechend vorbereitet sein.
- ✓ Die Systemzeit und die Einstellung der Zeitzone müssen Ihrer geografischen Position entsprechen.
- ✓ IP-Konfiguration und Netzwerkverbindungen müssen stimmen, falls Sie keine neue Gesamtstruktur erstellen:
 - ✓ Ein DNS-Server der Gesamtstruktur muss angegeben sein; für zusätzliche DCs in einer bestehenden Domäne sollte es ein DNS-Server der Zieldomäne sein.
 - ✓ Zur Erstellung neuer Domänen muss Kontakt mit dem Domain-Name-Master möglich sein.
 - ✓ Statische IP-Konfiguration ist empfehlenswert; kein DHCP.
- ✓ DNS- und NetBIOS-Domännennamen vorhandener und neu zu erstellender Domänen sowie Rechnernamen müssen eindeutig in der Gesamtstruktur sein.
- ✓ Anmeldeinformationen: Zusätzliche Domänen in einer vorhandenen Gesamtstruktur kann nur ein Mitglied der Gruppe Organisations-Admins erstellen. Alle AD-Einstellungen, die mehr als nur eine Domäne betreffen, können nur von Organisations-Admins vorgenommen werden.

Mit dem **Active Directory Preparation Tool** (ADPrep) aktualisieren Sie einerseits das Schema Ihrer Gesamtstruktur und passen andererseits Einstellungen und Objekte in vorhandenen Domänen an. *ADPrep* finden Sie auf der Installations-DVD von Windows Server 2022 im Ordner `\support\adprep`. Kopieren Sie den gesamten Ordner *adprep* auf den Zielrechner.

Schema anpassen

Bevor Sie einzelne Domänen mit *ADPrep* aktualisieren, müssen Sie abwarten, bis eine vollständige Replikation der Gesamtstruktur abgeschlossen ist.

Um das Schema anzupassen, müssen Sie auf dem Schema-Master mit einem Konto angemeldet sein, das Mitglied der folgenden drei Gruppen ist: Organisations-, Schema- und Domänen-Admins der Domäne des Schema-Masters. Der folgende Schritt muss nur ein einziges Mal in einer Gesamtstruktur ausgeführt werden.

- ▶ Starten Sie eine Eingabeaufforderung und geben Sie `adprep /forestprep` ein. Folgen Sie anschließend den Anweisungen des Programms.

Domäne anpassen

Vor der Installation eines Domänencontrollers müssen Sie die vollständige Replikation der Domäne abwarten.

Um Domänencontroller unter Windows Server 2022 in Domänen installieren zu können, müssen dort die folgenden Schritte ausgeführt werden:

- ▶ Melden Sie sich mit einem Domänen-Admin-Konto am Infrastruktur-Master der Domäne an, öffnen Sie eine Eingabeaufforderung und geben Sie `adprep /domainprep /gpprep` ein.
- ▶ Falls Sie schreibgeschützte Domänencontroller (RODC, Read-only DC) einsetzen wollen, geben Sie anschließend den Befehl `adprep /rodcprep` ein.

Installation der Rolle Active Directory-Domänendienste

Vor der Installation eines Domänencontrollers muss zunächst die Rolle *Active Directory-Domänendienste* hinzugefügt werden. Aktivieren Sie jetzt noch nicht die Rolle *DNS-Server*, denn das führt zu einer Fehlermeldung. Die Rolle des DNS-Servers werden Sie zu einem späteren Zeitpunkt hinzufügen.

Sie können die Installation auch in der PowerShell durchführen. Sinnvoll ist das zum Beispiel, wenn Sie auf einem Core-Server Active Directory installieren wollen. In diesem Fall verwenden Sie den folgenden Befehl:

```
Install-WindowsFeature AD-Domain-Services - IncludeManagementTools
```

8.2 Domänencontroller installieren

Installationsschritte

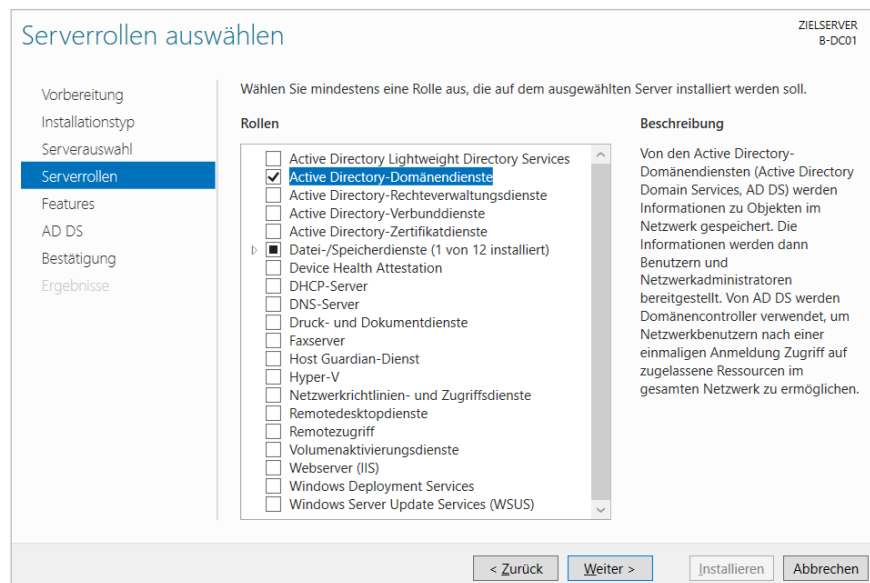
Der Assistent zum Installieren der AD-Domänendienste befindet sich nun im Server-Manager. Das bisher verwendete **dcpromo** ist nur noch aus Kompatibilitätsgründen für den Einsatz in Installationsskripten verfügbar und sollte nicht mehr verwendet werden.

- ▶ Klicken Sie im Server-Manager in der Menüzeile auf *Verwalten*.
- ▶ Klicken Sie auf *Rollen und Features hinzufügen*.
- ▶ Wählen Sie als Installationstyp *Rollenbasierte* oder *Featurebasierte Installation* 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.

- ▶ 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.



Auswahl der Serverrolle AD-Domänendienste

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.

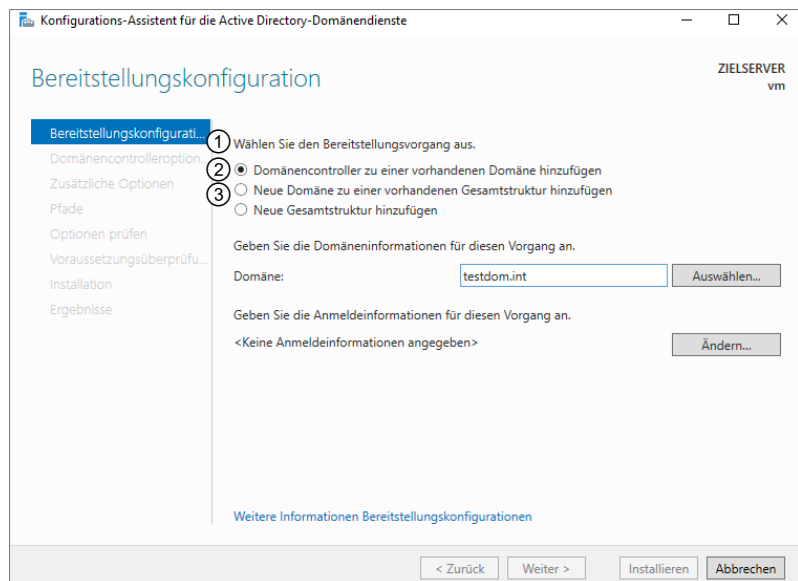
- ▶ Klicken Sie auf den Link, um den Server zum DC heraufzustufen.
- ▶ Falls Sie den Assistenten während der Installation geschlossen haben, klicken Sie im Server-Manager auf das Fähnchen mit den aktuellen Aufgaben. Klicken Sie anschließend auf *Server zu einem Domänencontroller heraufstufen*.

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.
- 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.

Auswahl beim Erstellen des Domänencontrollers

Um einen neuen Domänencontroller in einer vorhandenen Domäne zu installieren, verwenden Sie das Cmdlet `Install-ADDSDomainController`. Damit der Befehl funktioniert, geben Sie den Namen der Domäne ein und konfigurieren das Kennwort für den Verzeichnisdienst-Wiederherstellungsmodus als SecureString:

```
Install-ADDSDomainController -Domainname <DNS-Name der Domäne> -
SafeModeAdministratorPassword (read-host -prompt Kennwort -assecurestring)
```

In diesem Beispiel ist der DNS-Name der Domäne „Joos.int“. Der Befehl installiert auch einen DNS-Server auf dem Domänencontroller. Die Daten werden über Active Directory automatisch repliziert:

```
Install-ADDSDomainController -DomainName joos.int -InstallDNS:$True -
Credential (Get-Credential) -SafeModeAdministratorPassword (read-host -
prompt Kennwort -assecurestring)
```

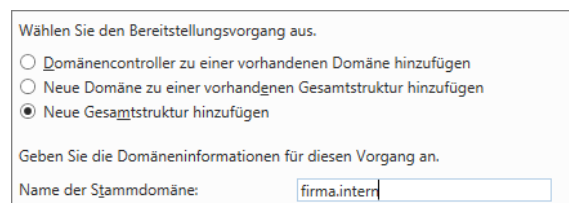
Um die Verbindung mit Active Directory zu verifizieren, sollten auf dem Core-Server folgende Befehle ausgeführt werden. Die Domäne lautet in diesen Beispielen wieder „joos.int“:

```
Nltest/dsgetsite
Nltest/dclist:Joos
Repadmin/showreps
Dcdiag
```

Neue Gesamtstruktur hinzufügen

Diese Option verwenden Sie, wenn es bisher keine Gesamtstruktur und Domänen in Ihrem Unternehmen gibt.

- 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*.



Auf der nächsten Seite können Sie die Domänencontrolleroptionen festlegen:

- ▶ Legen Sie die 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.

Funktionsebenen und Kennwort festlegen, DNS aktivieren

Der erste DC einer Gesamtstruktur muss globaler Katalog-Server sein, alle weiteren sollten es sein. Einen schreibgeschützten Domänencontroller ① 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.

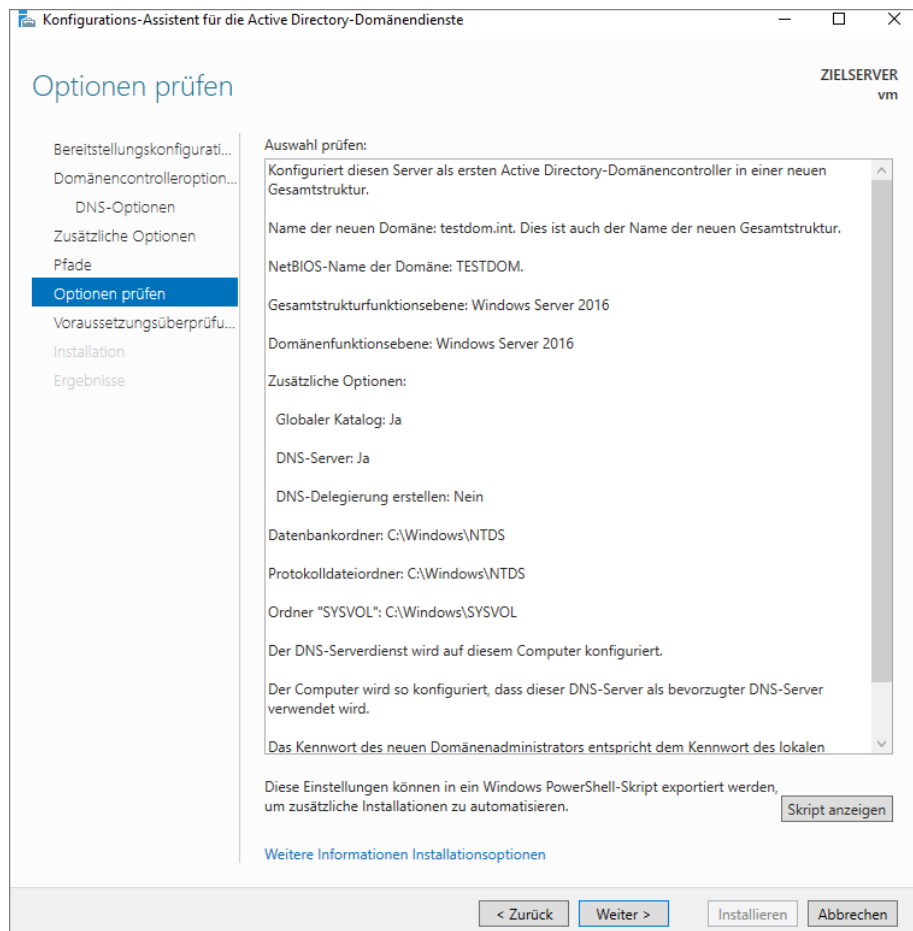
- ▶ Klicken Sie auf *Weiter*.
Sie erhalten auf der Seite *DNS-Optionen* eine Fehlermeldung, die Sie jedoch in diesem Fall ignorieren können. Klicken Sie auf *Weiter*.
- ▶ Überprüfen Sie auf der Seite *Zusätzliche Optionen* den NetBIOS-Domännennamen. Der Assistent schlägt Ihnen den linken Bestandteil 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 dann auf *Weiter*.

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 die hier angegebenen Laufwerke alle Beschleunigungsfunktionen (Schreibcache) ausschaltet, empfiehlt sich in der Praxis die Verwendung eines separaten Datenträgers für AD DS und SYSVOL.

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 wieder verwendet werden.

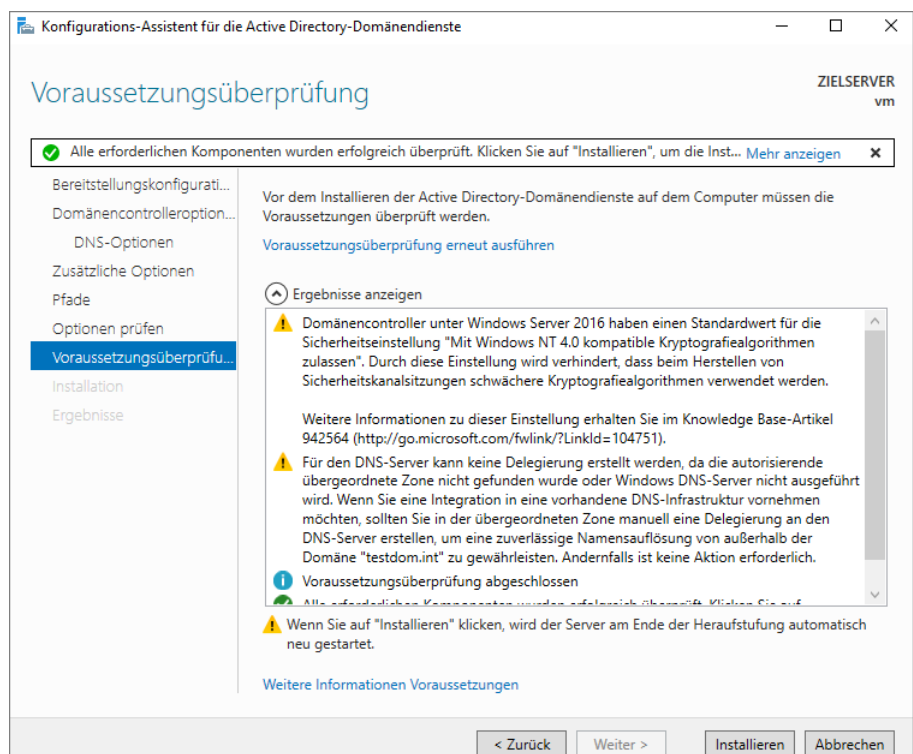
- Überprüfen Sie die Auswahl und klicken Sie auf *Weiter*.



Übersicht aller Optionen

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.

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 den Namen der Domäne und geben Sie gültige Anmeldeinformationen ein. Klicken Sie auf *Weiter*.
- ▶ Aktivieren Sie die Optionen *DNS-Server* und *Globaler Katalog*.
Das Deaktivieren des globalen Katalogs kann in Sonderfällen bei kleinen Filialen in großen Domänen mit schlechter WAN-Anbindung sinnvoll sein. Im Normalfall sollte jeder DC diese beiden Funktionen ausüben.
- ▶ Aktivieren Sie die Option *Schreibgeschützter Domänencontroller (RODC)* für kleine Außenstellen, an denen der Server nicht ausreichend gegen Zugriff gesichert werden kann und wo das Personal keine Änderungen am AD vornehmen soll.
- ▶ Legen Sie den Standort fest. Falls kein passender Standort eingerichtet wurde, verwenden Sie *Default-First-Site-Name*. Klicken Sie auf *Weiter*.

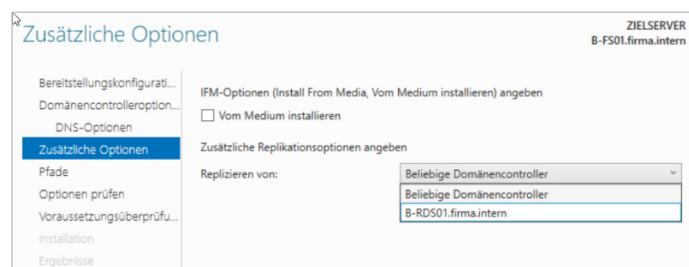
Auf der Seite *DNS-Optionen* können Sie die Option *DNS-Delegierung aktualisieren* einschalten und gültige Anmeldeinformationen für diesen Vorgang eingeben. Dabei wird ein zusätzlicher Nameserver-Eintrag in der DNS-Delegierung der übergeordneten Domäne erstellt.

- ▶ Klicken Sie auf *Weiter*.

Falls Sie einen zusätzlichen DC in einem Strukturstamm 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)** und eignet sich z. B. für die Installation in einer Außenstelle, um den Replikationsverkehr über das WAN zu vermeiden.

- ▶ Aktivieren Sie für IFM die Option *Aus Medienpfad 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*.



Replikationsmedium und Replikationsserver auswählen

Wie Sie solche IFM-Datenträger mit *ntdsutil.exe* erstellen, erfahren Sie später. In großen Domänen kann das Datenaufkommen bei der Erstreplikation recht umfangreich sein. Soll nun in einer netztechnisch schlecht angebundenen Außenstelle ein erster DC installiert werden, so kann das die vorhandene Bandbreite überfordern. Die Daten werden von einem vorhandenen DC exportiert, auf einem passenden Medium gespeichert und z. B. per Kurier zur Außenstelle gebracht.

- ▶ Legen Sie die Speicherorte für die AD-Daten fest. Verwenden Sie dafür möglichst nicht die Systempartition.
- ▶ 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 behoben werden.
- ▶ Klicken Sie auf *Installieren*.
Der Installationsvorgang wird nun ausgeführt und der Server automatisch neu gestartet.

Das Konto *Administrator* dieses Rechners wird automatisch Mitglied der Gruppe *Domänen-Admins*. Als Kennwort wird das bestehende Administratorkennwort verwendet.

Neue Subdomäne erstellen

- ▶ Wählen Sie im Assistenten die Option *Neue Domäne zu einer vorhandenen Gesamtstruktur hinzufügen*.
- ▶ Wählen Sie als Domänentyp *Untergeordnete Domäne*.
- ▶ Geben Sie den Namen bzw. den FQDN der übergeordneten Domäne und den Namen der neuen Domäne ein.
- ▶ Klicken Sie auf *Weiter*.
- ▶ Falls Sie nicht als Organisations-Admin angemeldet sind, klicken Sie auf *Ändern* und geben Sie die benötigten Anmeldeinformationen ein.
- ▶ Klicken Sie auf *Weiter*.
- ▶ Legen Sie die Domänenfunktionsebene fest.

Überprüfung vor der Hochstufung zum DC

Falls Ihre Gesamtstrukturfunktionsebene bereits Windows Server 2016 ist, entfällt dieser Schritt.

- ▶ Klicken Sie auf *Weiter*.
- ▶ Entscheiden Sie, ob der neue DC auch DNS-Server sein und den globalen Katalog enthalten soll. Im Normalfall sollte jeder DC beides sein.
- ▶ Wählen Sie den passenden Standort aus oder wählen Sie *Default-First-Site-Name*.
- ▶ Geben Sie zweimal das DSRM-Kennwort zur Wiederherstellung des Verzeichnisdienstes ein und klicken Sie auf *Weiter*.
- ▶ Klicken Sie auf der Seite *DNS-Optionen* auf *Ändern*, falls Sie abweichende Anmeldeinformationen zur Erstellung der DNS-Delegierung benötigen. Klicken Sie auf *Weiter*.
- ▶ Überprüfen oder ändern Sie auf der Seite *Zusätzliche Optionen* den NetBIOS-Domännennamen und klicken Sie auf *Weiter*.
- ▶ Überprüfen oder ändern Sie auf der Seite *Pfade* die Speicherorte für das AD, Protokolle und SYSVOL. Verwenden Sie dafür möglichst nicht die Systempartition. Klicken Sie auf *Weiter*.
- ▶ Überprüfen Sie alle Einstellungen und klicken Sie auf *Weiter*.
- ▶ Falls die folgende Prüfung erfolgreich verlaufen ist, klicken Sie auf *Installieren*.
Der Installationsvorgang wird nun abgeschlossen und ein Neustart ist erforderlich.

Das Konto *Administrator* dieses Rechners wird automatisch Mitglied der Gruppe *Domänen-Admins*.

Neue Strukturdomäne erstellen

Vor der Installation eines Domänencontrollers für einen neuen Strukturstamm müssen erst Vorbereitungen im DNS getroffen werden. Erklärungen hierzu finden Sie im Kapitel 9.

Die Installation läuft genauso ab wie beim Hinzufügen einer Subdomäne. Unterschiede gibt es nur beim Domänentyp und der notwendigen Vorbereitung des DNS vor Einrichtung des DCs.

- ▶ Wählen Sie im Assistenten die Option *Neue Domäne zu einer vorhandenen Gesamtstruktur hinzufügen*.
- ▶ Wählen Sie als Domänentyp *Strukturdomäne*.
- ▶ Geben Sie den Namen bzw. den FQDN der übergeordneten Domäne und den Namen der neuen Domäne ein.
- ▶ Klicken Sie auf *Weiter*.
- ▶ Falls Sie nicht als Organisations-Admin angemeldet sind, klicken Sie auf *Ändern* und geben Sie die benötigten Anmeldeinformationen ein. Klicken Sie auf *Weiter*.

Ab diesem Punkt verläuft die Installation genau wie beim Einrichten einer Subdomäne.

8.3 Domänencontroller entfernen

Wird ein Domänencontroller aus Active Directory entfernt, sollten Sie einige Vorbereitungen treffen, damit die Anwender durch seinen Ausfall nicht betroffen sind:

- ▶ Stellen Sie sicher, dass der Domänencontroller nicht als bevorzugter oder alternativer DNS-Server von einem anderen Rechner der Domäne verwendet wird (auch nicht als DNS-Weiterleitungsserver).
- ▶ Übertragen Sie alle FSMO-Rollen auf andere Domänencontroller.
- ▶ Entfernen Sie – falls möglich – vor der Herabstufung DNS von diesem Domänencontroller. Haben Sie DNS entfernt, überprüfen Sie auf einem anderen DNS-Server in den Eigenschaften der DNS-Zone, dass der Server auf der Registerkarte *Namenserver* nicht mehr aufgeführt wird. Entfernen Sie aber nicht den Hosteintrag des Servers, da dieser für die Herabstufung noch benötigt wird.
- ▶ Stellen Sie sicher, dass der Domänencontroller nicht an irgendeiner Stelle als Domänencontroller explizit eingetragen ist, zum Beispiel auf einem Linux-Server oder einem Exchange-Server.
- ▶ Entfernen Sie alle Active Directory-abhängigen Dienste wie VPN, Zertifikatstelle oder andere Programme, die nach der Herabstufung nicht mehr funktionieren werden.
- ▶ Wenn es sich bei diesem Server um einen globalen Katalog handelt, konfigurieren Sie einen anderen Server als globalen Katalog und entfernen Sie im Snap-In Active Directory-Standorte und -Dienste unter *Sites/ <Standort des Servers>/<Servername>/Eigenschaften der NTDS-Settings* den Haken bei *Globaler Katalog*.

Deinstallation

Um einen Domänencontroller herunterzustufen, verwenden Sie am besten die PowerShell und das Cmdlet `Uninstall-ADDSDomainController`. Sie müssen noch das lokale Kennwort des Administrators über den Befehl festlegen. Dieses müssen Sie als `SecureString` in der PowerShell definieren. Die Syntax dazu lautet:

```
Uninstall-ADDSDomainController -LocalAdministratorPassword (Read-Host - Prompt "Kennwort" -AsSecureString)
```

Mit `Get-Help Uninstall-ADDSDomainController` erhalten Sie mehr Informationen zu dem Befehl.

Um einen Domänencontroller herabzustufen, können Sie auch den Assistenten zum Entfernen von Rollen und Features verwenden:

- ▶ Klicken Sie im Server-Manager auf *Verwalten - Rollen und Feature entfernen*. Es öffnet sich der Assistent zum Entfernen von Rollen und Features.
- ▶ Wählen Sie in der Serverauswahl den Server aus und klicken auf *Weiter*.

- ▶ Deaktivieren Sie die Serverrolle *Active Directory-Domänendienste* und bestätigen Sie die Entfernung der zugehörigen Features.
Nach einer Prüfung erscheint eine Fehlermeldung, die besagt, dass der Server erst tiefer gestuft werden muss.
- ▶ Klicken Sie auf den Link *Diesen Domänencontroller tiefer stufen*.
Es öffnet sich der Konfigurations-Assistent für die Active Directory-Domänendienste.
- ▶ Überprüfen Sie, ob die Anmeldeinformationen korrekt sind, und ändern Sie sie gegebenenfalls.
- ▶ Aktivieren Sie beim letzten DC einer Domäne die Option *Letzter Domänencontroller in der Domäne*.

Falls es sich um den letzten DC der Domäne handelt, müssen die Domäneninformationen aus dem AD gelöscht werden. Dazu wird die Berechtigung eines Organisations-Admins benötigt.

Bei Problemen beim Entfernen des letzten DCs einer Domäne können Sie die Option *Entfernen dieses Domänencontrollers erzwingen* aktivieren, ansonsten sollten Sie diese Option nur in Notfällen verwenden.

Auf der Seite *Warnungen* werden alle wichtigen Rollen im Active Directory angezeigt, die der DC innerhalb der Domäne innehat.

- ▶ Lesen Sie sich die Auflistung gut durch und überlegen Sie bei jedem Punkt, ob Sie an alle Auswirkungen gedacht haben, die eine Entfernung nach sich zieht.
- ▶ Um den Vorgang fortzusetzen, müssen Sie die Option *Entfernung fortsetzen* aktivieren und auf *Weiter* klicken.

Auf der Seite *Entfernungsoptionen* können Sie auswählen, ob alle DNS-Zonen und alle Anwendungspartitionen des Active Directory entfernt werden sollen. Da ohne Domäne sowieso keine Informationen mehr gerettet werden können, spricht beim letzten DC nichts gegen eine Entfernung.

- ▶ Klicken Sie auf *Partitionen anzeigen*, um in einem neuen Fenster die AD-Anwendungspartitionen anzuschauen.

Wenn Sie den Vorgang fortsetzen, wird das Active Directory gelöscht und die Domäne aufgelöst.

- ▶ Klicken Sie auf *Weiter*.
- ▶ Geben Sie auf der nächsten Seite zweimal ein neues Kennwort für den lokalen Administrator des Computers ein und klicken Sie auf *Weiter*.

Auf der Seite *Optionen prüfen* wird nochmals zusammengefasst, dass dieser Computer der letzte DC der Domäne ist, dass die Domänendienste entfernt werden sollen und dass es die Domäne nicht mehr geben wird. Überlegen Sie noch einmal genau, ob das richtig ist.

- ▶ Klicken Sie auf *Tiefer stufen*, um die Deinstallation des DCs auszuführen.

Nach dem Neustart ist der Rechner Mitglied der Domäne. War es der letzte DC der Domäne, ist der Rechner nun Mitglied einer Arbeitsgruppe.

- ▶ Kontrollieren Sie in jedem Fall die IP-Konfiguration des Rechners, denn der letzte DC einer Domäne behält sein primäres DNS-Suffix.
Das kann Probleme verursachen, wenn er Mitglied einer anderen Domäne werden soll.

Deinstallationsprobleme

Sollte die Deinstallation fehlschlagen, erhalten Sie vom Assistenten Hinweise. Gegebenenfalls sollten Sie auch das Ereignisprotokoll untersuchen. Meistens liegt es an DNS oder an (Netzwerk-)Verbindungsproblemen. Nachdem Sie alle Fehler beseitigt haben, versuchen Sie es erneut. Sollte sich der Domänencontroller nicht deinstallieren lassen, können Sie als letztes Mittel auf der Seite *Anmeldeinformationen* die Option *Entfernen dieses Domänencontrollers erzwingen* aktivieren.



Mit dieser Option entfernen Sie zwar den Domänencontroller vom Server, er wird aber nicht aus dem AD entfernt. Das kann zu verschiedensten Problemen führen. Den ehemaligen DC müssen Sie dann manuell aus dem Active Directory entfernen. Suchen Sie im Internet nach dem Suchbegriff *Metadata Cleanup* oder *Domänencontroller herunterstufen Fehler*. Auf den verschiedensten Seiten erhalten Sie detaillierte Informationen darüber, welche Schritte durchzuführen sind. Während der Prozedur müssen Sie ein Metadata Cleanup durchführen, Korrekturen im DNS machen, das Computerkonto löschen und aus den Active Directory-Standorten und -Dienstern entfernen.

Auch wenn ein herabgestufter Domänencontroller im Anschluss noch als Mitgliedsserver verwendet werden kann, sollten Sie sicherheitshalber das Computerkonto aus der Domäne entfernen und das Betriebssystem neu auf dem Server installieren, um Altlasten zu entsorgen. Auch den Servernamen sollten Sie ändern, wenn aus dem Namen hervorgeht, dass es sich um einen Domänencontroller gehandelt hat.

Hinweis für Testumgebungen

Haben Sie etwas Geduld, wenn Sie die verschiedenen Varianten in Testumgebungen durchführen. Installieren Sie nicht einen DC, um ihn gleich nach dem Neustart wieder zu deinstallieren. Warten Sie mindestens fünf Minuten. Haben Sie AD-Standorte implementiert, warten Sie ab, bis eine vollständige Replikation Ihrer Umgebung stattgefunden hat (mindestens 15 Minuten). Anderenfalls riskieren Sie Probleme und Fehlermeldungen, die nichts mit einer realen Umgebung zu tun haben.

Dieser Hinweis gilt auch für die folgenden Kapitel.

9 DNS und Namensauflösung

9.1 Einführung zu Namensauflösung

Mechanismen zur Namensauflösung

Computer kommunizieren im Netzwerk über IP-Adressen miteinander, für Menschen ist es jedoch einfacher, mit Computer- und Domännennamen zu arbeiten. Namensauflösungsmechanismen ermöglichen es, die Namen in IP-Adressen zu übersetzen und umgekehrt.

Im Internet wird dazu das **Domain Name System (DNS)** genutzt, das sogenannte **FQDNs** (Fully Qualified Domain Names) in IP-Adressen auflöst. Dabei sind die einzelnen Bestandteile durch Punkte getrennt. Der linke Bestandteil eines FQDN ist z. B. die Bezeichnung eines Rechners, der Host-Name. Es folgt die Angabe, zu welcher (Sub-) Domain dieser Host gehört. Ganz rechts befindet sich die 1st-Level-Domain, weitere Unterdomänen stehen jeweils links davor:

<Host-Name>.<3rd-Level-Domain>.<2nd-Level-Domain>.<1st-Level-Domain>

Beispiel: *PC01.Vertrieb.Herdt.de*

Anstelle des Host-Namens kann auch ein Dienst oder eine Ressource angegeben werden (z. B. *www.herdt.de*). In der Antwort wird jedoch immer die IP-Adresse des Rechners stehen, der diesen Dienst bereitstellt.

Tatsächlich steht am rechten Ende eines FQDN noch ein weiterer Namensbestandteil, bestehend aus einem Punkt und einem leeren Namen (acht Nullen). Dieser bezeichnet Root (Wurzel). Dieser braucht jedoch aus Vereinfachungsgründen nicht mit angegeben werden.

Root

Das DNS-System arbeitet nach dem Prinzip: Man muss nicht alles wissen, man muss nur wissen, wen man fragen kann. Die oberste Instanz, die befragt werden kann, ist Root, die Wurzel. Root steht dabei stellvertretend für die sogenannten Root-Nameserver oder Root-Server. Bei diesen handelt es sich um eine Reihe von international betriebenen DNS-Servern, die nur wissen, welche DNS-Server für die jeweiligen 1st-Level-Domains zuständig sind.

Die jeweiligen 1st-Level-Domains (auch Top-Level-Domains genannt, z. B. de, com, org) werden verantwortlich von entsprechenden DNS-Servern verwaltet, die nur ihren Teil des FQDNs auflösen können, aber wissen, welche DNS-Server für die in ihnen enthaltenen 2nd-Level-Domains zuständig sind. Erst diese können den eigentlichen FQDNs, Unterdomänen und anderen enthaltenen Informationen auflösen.

Ob eine 3rd-Level-Domain (und 4th-Level ...) genutzt wird, hängt davon ab, wie der Besitzer einer 2nd-Level-Domain seinen Namensraum strukturiert. Das DNS wurde eingeführt, als die Verwaltung der Rechner in der Domäne über die sogenannten **Hosts**-Dateien der steigenden Zahl von Computern nicht mehr gewachsen war. Für die DNS-Namensauflösung in mittleren und großen Netzwerken werden praktisch immer DNS-Server genutzt. Die Hosts-Datei ist noch vorhanden, wird nun aber nicht mehr für die gesamte Namensauflösung verwendet, sondern nur in Einzelfällen genutzt.

In Windows-Netzen existieren neben dem DNS-Namensraum auch noch sogenannte **NetBIOS**-Namen, die zur Namensauflösung verwendet werden, beispielsweise entstehen die Einträge in der Netzwerkumgebung im Windows-Explorer über die NetBIOS-Namensauflösung. Standardmäßig setzt Windows die NetBIOS-Namensauflösung als sekundären Mechanismus ein, wenn die DNS-Namensabfrage zu keinem Ergebnis führt. Dieser Namensraum ist einfach strukturiert, d. h., eine Unterteilung in verschiedene Bereiche wie die DNS-Sub-Domains ist nicht vorgesehen. Konstruktionsbedingt arbeitet NetBIOS mit Netzwerk-Broadcasts, wo über einen Rundruf an alle nach einem bestimmten Rechner gefragt wird.

Da Broadcasts von Routern nicht weitergeleitet werden, funktioniert das nur innerhalb eines Subnetzes. Damit NetBIOS über mehrere Subnetze hinweg funktioniert, müssen Sie einen **WINS**-Server einsetzen und die Clients, z. B. über DHCP anweisen, diesen zu benutzen. Die Broadcasts werden dann durch gezielte Kommunikation mit dem WINS-Server ersetzt.

Theoretisch können Sie für NetBIOS-Namen auch die Datei *Lmhosts* nutzen.

Rechnernamen

NetBIOS und klassisches DNS unterstützen verschiedene Zeichen und unterschiedlich lange Namen:

- ✓ **DNS** unterstützt die Zeichen a–z, A–Z, 0–9 und den Bindestrich (nicht als erstes Zeichen), Groß- und Kleinschreibung wird ignoriert. Umlaute sind nicht erlaubt. DNS unterstützt zwar seit 2009 auch erweiterte Unicode-Zeichensätze, Sie sollten jedoch weiterhin ausschließlich die oben angegebenen Zeichen verwenden. Ein FQDN kann maximal 253 Zeichen lang sein, die einzelnen Namensbestandteile dürfen 63 Zeichen nicht überschreiten.
- ✓ **NetBIOS** unterstützt fast alle Zeichen, die Sie auch für Dateinamen verwenden können (nicht: \ / : * ? " ; |). NetBIOS-Namen sind maximal 16 Zeichen lang, 15 davon können Sie frei vergeben. Das letzte Zeichen dient intern zur Kennzeichnung, um was es sich handelt, z. B. einen Computer, Benutzer oder eine Domäne.

Verwenden Sie am besten für alle Bezeichnungen in der Domäne (Benutzernamen, Computernamen, Active Directory-Gruppen und Organisationseinheiten etc.) **ausschließlich** den oben angegebenen DNS-Zeichensatz, um Probleme zu vermeiden. Das hat außerdem Vorteile in mehrsprachigen Umgebungen.

9.2 Funktionsweise des DNS

Hierarchische Gliederung

Der globale DNS-Namensraum ist hierarchisch gegliedert und wird als verteilte Datenbank gespeichert.

- ✓ Ganz oben steht die Root-Domain, gekennzeichnet durch einen Punkt. Die Root-Domain enthält nur ein Leerzeichen, daher wird meist auf den Punkt am Ende des FQDN verzichtet.
- ✓ Darunter folgen die 1st-Level-Domains, z. B. *com*, *edu*, *mil* sowie zweibuchstabile Kürzel für Länder, z. B. *de*.
- ✓ Jede 2nd-Level-Domain liegt unter genau einer 1st-Level-Domain; *Herdt.de* ist eine andere Domain als *Herdt.com*. Diese Gliederung setzt sich entsprechend fort.

Jede Domain hat also genau eine übergeordnete Domain und eine beliebige Anzahl an untergeordneten.

Sie können für das interne Netzwerk auch Domännennamen verwenden, die nicht über die Top-Level-Domains und Root aufgelöst werden können (z. B. *meine-firma.intern*). Diese sind über das Internet nicht auflösbar, Sie sparen hierdurch Kosten für die Registrierung und die Pflege bei extern erreichbaren DNS-Servern und die Wahrscheinlichkeit von Angriffen wird verringert.

Zonendateien

Gespeichert wird der Inhalt von Domains in sogenannten Zonendateien, die den kompletten Inhalt ihrer Domain enthalten. Dabei gibt es eine Originaldatei, die sich auf dem Primary Nameserver (Master) befindet, und eine beliebige Anzahl von Kopien, die auf den Secondary Nameservern (Slave) gespeichert werden. Die Begriffe „Zonendatei“ und „Zone“ bedeuten das Gleiche und sind deshalb austauschbar.

Eine Zonendatei könnte auch den Inhalt mehrerer zusammenhängender Domains enthalten, was aber nicht empfehlenswert ist. Da jeder DNS-Server auch mehrere Zonendateien hosten kann, ist es übersichtlicher und verwaltbarer, wenn Sie dem Grundsatz folgen: eine Zone gleich eine Domain.

Jede Zone beinhaltet alle DNS-Server der direkt untergeordneten Domains. Jeder Root-Server kennt alle 1st-Level-DNS-Server, also kennt beispielsweise der DNS-Server für *com* alle 2nd-Level-DNS-Server in der *com*-Domain usw. So entsteht eine hierarchische und verteilte Datenbank. Das Bekanntmachen der untergeordneten DNS-Server wird als (Zonen-) **Delegierung** bezeichnet.

Im klassischen DNS gibt es für jede Domain genau eine primäre Zone (die einzige beschreibbare Datei) und beliebig viele sekundäre Zonen (Kopien). Die Inhalte werden über den sogenannten **Zonentransfer** abgeglichen. Dabei kann ein DNS-Server für Zone A der primäre DNS-Server sein, für Zone B der sekundäre DNS-Server.

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 auf den sekundären Namensserver übertragen.
- ✓ **Inkrementelle Zonenübertragung (IXFR):** Nur die Änderungen an den Zonendaten werden zum sekundären Namensserver übertragen.
- ✓ **Benachrichtigung vom primären Namensserver:** Nach einer Veränderung der Zonendaten benachrichtigt der primäre Namensserver die sekundären über eine Änderung. Die sekundären Namensserver fordern daraufhin eine Zonenübertragung an.
- ✓ **Vom sekundären Namensserver veranlasste Zonenübertragung:** Ein sekundärer Namensserver fragt seinen Master-Server nach Änderungen in der Zonendatei ab, wenn ...
 - ✓ der DNS-Serverdienst auf dem sekundären Namensserver neu gestartet wird;
 - ✓ das Intervall für die Serveraktualisierung abläuft;
 - ✓ er eine Benachrichtigung über Änderungen erhält.

Inhalte einer Zonendatei

Einträge in der Zonendatei heißen Ressourceneinträge (Resource Records). Die Tabelle listet die wichtigsten auf:

Objekt und Kürzel	Erklärung
Autoritätsursprung, SOA	Ressourceneintrag für den primären Nameserver der Zone; legt u. a. die Häufigkeit der Zonentransfers fest
Namensserver, NS	DNS-Server für Zonen werden anhand solcher Einträge vermerkt.
Host, A	Ressourceneintrag für Forward-Lookup-Abfragen nach IPv4-Adressen
Host, AAAA	Ressourceneintrag für Forward-Lookup-Abfragen nach IPv6-Adressen
Zeiger, PTR	Ressourceneintrag für die Namensauflösung im Reverse-Lookup-Verfahren. Die Werte eines Zeigers sind der Hostanteil einer IP-Adresse und der Hostname.
Dienst, SRV	Serviceressourceneinträge speichern Netzwerkressourcen und -dienste. Mit diesen Diensteinträgen werden beispielsweise Domänencontroller lokalisiert.
Alias, CNAME	Ressourceneintrag für einen alternativen Hostnamen
Mail-Exchanger, MX	Ressourceneintrag für einen SMTP-Server, der E-Mails für die Domain annimmt

Dynamisches DNS (DDNS)

Ohne dynamisches DNS müssen die Einträge einer Zonendatei manuell gepflegt werden. Dynamische Aktualisierungen erlauben dagegen eine Automatisierung und verringern den Verwaltungsaufwand. Genau aus diesem Grund wird dynamisches DNS in vielen Bereichen eingesetzt. Der DNS-Client auf einem aktuellen Windows-PC kann seine DNS-Einträge selbstständig erstellen und aktualisieren. Die Einträge werden standardmäßig bei einem Neustart, nach Änderungen an IP-Adresse oder Name sowie alle 24 Stunden aktualisiert. Sie können den Vorgang mit dem Kommando `ipconfig /registerdns` auch manuell durchführen.

Auch der DHCP-Server kann stellvertretend dynamische Aktualisierungen vornehmen, was von Vorteil ist, wenn ein DHCP-Client keine dynamische Aktualisierung unterstützt, z. B. Netzwerkdrucker, Nicht-Windows Betriebssysteme.

DNS-Abfragen

Ein DNS-Client wird auch als **Resolver** bezeichnet. Er kann verschiedene Arten von Abfragen versenden:

- ✓ **Forward Lookup:** Wie lautet die IP-Adresse von FQDN?
- ✓ **Reverse Lookup:** Welchen FQDN hat folgende IP-Adresse?

Lookup-Abfragen sind entweder:

- ✓ **Rekursive Abfragen:** Der Client verlangt eine gültige Antwort vom DNS-Server.
- ✓ **Iterative Abfragen:** Der Resolver verlangt entweder eine gültige Antwort (falls der DNS-Server die Zone selbst vorhält) oder einen Verweis auf einen andern Nameserver, der weiterhilft. Hier spielen die (Zonen-)Delegierungen eine wichtige Rolle.

Wie der Vorgang genau abläuft, zeigt das folgende Beispiel einer DNS-Abfrage nach *www.microsoft.com*:

- ✓ Der Client kontrolliert zunächst, ob er diese Information bereits vorhält. Sie könnte in seiner Hosts-Datei stehen oder sich im lokalen DNS-Cache befinden, weil sie schon vorher abgefragt wurde.
- ✓ Der Client schickt eine rekursive Forward-Lookup-Abfrage an seinen primären DNS-Server.
- ✓ Der DNS-Server kontrolliert, ob er eine Zone für die abgefragte Domain vorhält. Falls ja, schickt er dem Client die Information und kennzeichnet die Antwort als **autorisiert**. Falls nein, überprüft er seinen DNS-Cache und sendet gegebenenfalls die dort enthaltene Antwort. Falls auch der DNS-Cache die Antwort nicht enthält, muss der DNS-Server nun seinerseits nachfragen.
- ✓ Der DNS-Server schickt eine iterative Forward-Lookup-Abfrage an einen der Root-Server. Als Antwort erhält er einen Verweis auf den Nameserver der *com*-Domain (delegierte Zone), der wie alle folgenden Antworten im DNS-Cache gespeichert wird.
- ✓ Der DNS-Server schickt nun eine iterative Abfrage an einen Nameserver der *com*-Domain und erhält als Antwort die IP-Adressen der DNS-Server für *microsoft.com* (delegierte Zone).
- ✓ Der DNS-Server schickt eine iterative Abfrage an einen Nameserver für *microsoft.com* und erhält eine autorisierte Antwort. Da die Antwort nicht aus einer eigenen Zone kommt, wird sie als nicht autorisiert gekennzeichnet und an den Client zurückgegeben.

Der Client akzeptiert jede Antwort seines DNS-Servers, auch wenn diese „nicht vorhanden“ lautet.

Weiterleitungen

Der eben geschilderte Vorgang läuft etwas anders ab, wenn ein DNS-Server mit **Weiterleitungen** konfiguriert ist. Dann übernimmt der DNS-Server die Namensauflösung nicht selbst, sondern schickt eine rekursive Abfrage an seinen konfigurierten Weiterleitungsserver, der nun für die Namensauflösung zuständig ist.

In AD-Domänen werden Weiterleitungen eingesetzt, weil Domänencontroller sehr sensible Daten beinhalten und aus Sicherheitsgründen keinen Kontakt zum Internet haben sollen. DCs übernehmen nur die AD-interne Namensauflösung. Die externe Namensauflösung liefert üblicherweise ein DNS-Server in der DMZ (demilitarisierten Zone, Perimeternetz), der auf den DCs als Weiterleitungsserver eingetragen ist.

Auch dieser DMZ-Rechner arbeitet oft nicht mit einer Namensauflösung über die Root-Zone, sondern ist mit einer Weiterleitung an einen DNS-Server des Internetproviders konfiguriert. Dessen DNS-Cache wird viele Abfragen bereits enthalten, was für schnellere Antworten sorgt und die anderen DNS-Server entlastet.

Neben den allgemeinen Weiterleitungen existieren auch noch **bedingte Weiterleitungen**. Hier werden Weiterleitungsserver für eine bestimmte Domain angegeben.

DNS-Cache

Alle Ergebnisse seiner Abfragen speichert ein DNS-Server in seinem Cache. Dadurch kann er erneute Anfragen nach demselben Inhalt schneller beantworten, der DNS-bezogene Internetverkehr wird reduziert und die Name-server werden entlastet. Wie lange diese gespeicherten Abfragen im Cache verbleiben, legen die abgefragten DNS-Server mit einer TTL (Time to Live) fest. Nach deren Ablauf beantwortet ein DNS-Server Anfragen nicht mehr anhand der Cache-Information, sondern startet eine erneute Namensauflösung.

9.3 DNS im Active Directory

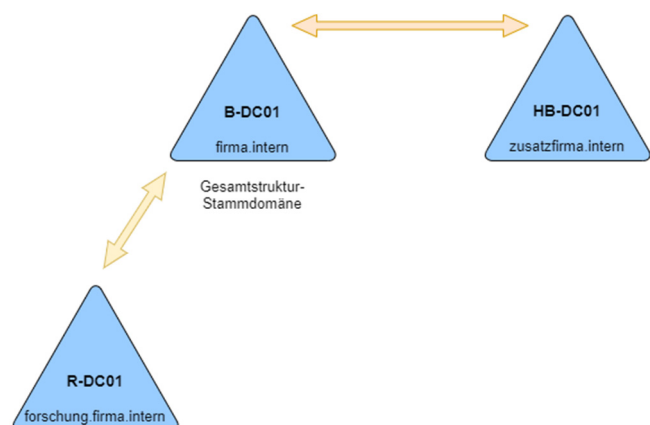
Erster Überblick

Eine Active Directory-Domäne ist immer auch eine DNS-Domain, in der die Domänen-Clients alle zentralen AD-Dienste (z. B. Domänencontroller für die Anmeldung) über DNS-Abfragen finden. Bei der Installation eines Domänencontrollers schlägt der Assistent vor, die DNS-Serverrolle hinzuzufügen, was unbedingt empfehlenswert ist. DNS-Server auf DCs unterstützen einige Features, die andere DNS-Server nicht bieten. Ist jeder DC gleichzeitig auch DNS-Server, dann werden Sie nur in Ausnahmefällen zusätzliche DNS-Server benötigen, weshalb Mitglieds-server hier nicht weiter behandelt werden. Sie können die Rolle DNS-Server dort hinzufügen und mit Ausnahme der Active-Directory-integrierten Zonen alle folgenden Schritte durchführen.

Als Einstieg erscheint es günstig, zunächst DNS in einer etwas komplexeren Gesamtstruktur zu betrachten, so wie es der Installations-Assistent aufbaut. Es gibt in unserem Beispiel drei Standorte: Berlin, Bremen und Regensburg. Alle Computer-Hostnamen bestehen aus einem Standort-Kürzel, ihrer Funktion (DC = Domänencontroller, FS = Fileserver etc.) gefolgt von einer laufenden Nummer. Jeder Server war zu Beginn Mitglied einer Arbeitsgruppe und mit einer statischen IP-Konfiguration versehen; bei *R-DC01* und *HB-DC01* war als primärer DNS-Server *B-DC01* eingetragen. Nach dem Hochstufen zum DC verfügt nun jeder Standort über einen DC innerhalb der Gesamtstruktur.

Die nachfolgenden Betrachtungen gehen von einer Gesamtstruktur aus, bestehend aus drei Domänen mit jeweils einem Domänencontroller:

Active Directory erstellt während der Installation bidirektionale, transitive Vertrauensstellungen zwischen den Domänen, sodass sich prinzipiell jeder Benutzer an jedem Rechner der Gesamtstruktur anmelden und auf jede Ressource zugreifen kann, entsprechende Berechtigungen vorausgesetzt. Dementsprechend muss natürlich auch die domänenübergreifende Namensauflösung funktionieren.



Beispiel

Ein Benutzer der Domäne *forschung.firma.intern* will sich am Rechner *HB-PC01.zusatzfirma.intern* anmelden. Auf *HB-PC01* ist *HB-DC01* als DNS-Server konfiguriert, für die Benutzer-Authentifizierung wird jedoch *R-DC01* benötigt. *HB-DC01.zusatzfirma.intern* muss also die IP-Adresse von *R-DC01.forschung.firma.intern* auflösen können.

DNS-Beziehung zwischen *firma.intern* und *forschung.firma.intern*

Beim Erstellen der Domäne *forschung.firma.intern* hat der Assistent automatisch eine Zonen-Delegierung in der übergeordneten Domäne *firma.intern* erstellt. Dadurch weiß der DNS-Server, wo er nachfragen kann, wenn Informationen über *forschung.firma.intern* bei ihm abgefragt werden.

Bei der Installation zusätzlicher DCs in *forschung* zeigt der Assistent das Fenster *DNS-Delegierung aktualisieren* und schlägt als Antwort *Ja* vor. Wenn Sie die Voreinstellung übernehmen, wird ein zusätzlicher NS-Eintrag in der Delegierung auf *B-DC01* erstellt. Das stellt sicher, dass die Namensauflösung auch beim Ausfall eines DCs in *forschung* funktioniert.

_msdcs.firma.intern ist eine AD-spezifische Domain, die Verweise auf alle DCs der Gesamtstruktur enthält. Sie ist auf allen DCs, die auch DNS-Server sind, vorhanden.

Der Assistent stellt auch sicher, dass die Namensauflösung von *forschung* zur übergeordneten Domäne *firma* funktioniert. Dazu hat er auf *R-DC01* Weiterleitungen an den übergeordneten Domänencontroller *B-DC01* konfiguriert. Das funktioniert zwar, ist aber keine effiziente Lösung. Alle Namensabfragen, die *R-DC01* nicht beantworten kann, schickt er weiter an den angegebenen Nameserver der übergeordneten Domäne *B-DC01*.

Darüber hinaus passen sich diese Einträge nicht automatisch an. Angenommen, in *firma.intern* wird ein zweiter und dritter DC aufgesetzt und anschließend *B-DC01* entfernt, dann verweist diese Weiterleitung ins Leere und die Namensauflösung für *firma.intern* funktioniert nicht mehr. Eine bessere Lösung bieten Stubzones. Näheres dazu folgt weiter unten.

Stammhinweise ist die Windows-Bezeichnung für die oben genannten DNS-Root-Server. Ist diese Option aktiviert, versucht *R-DC01* eine Namensauflösung über die Root-Domain, falls *B-DC01* nicht auf Anfragen reagiert bzw. kein Server angegeben ist. Bei AD-Daten wird das fehlschlagen, da *intern* keine offizielle 1st-Level-Domain ist und AD-Domänen üblicherweise nicht über das Internet erreichbar sind.

DNS-Beziehung zwischen *firma.intern* und *zusatzfirma.intern*

Vor der Installation einer zusätzlichen Struktur müssen Vorbereitungen im DNS der vorhandenen Gesamtstruktur-Stammdomäne vorgenommen werden. In unserem Beispiel musste in der Domäne *firma.intern* eine neue Forward-Lookupzone für *zusatzfirma.intern* erstellt und an einen noch nicht vorhandenen DC/DNS-Server delegiert werden. Microsoft nennt diesen Vorgang **Dummy-Delegierung**.

Zusätzliche Domänencontroller in *zusatzfirma.intern* werden der delegierten Zone auf *B-DC01* nicht automatisch hinzugefügt. Sie sollten dort manuell eingetragen werden, um Fehlertoleranz zu ermöglichen.



Es ist wichtig, dass die Namensauflösung für neue Strukturstämme eingerichtet ist, bevor deren erster DC installiert wird, sonst wird die neue Domäne nicht richtig ins AD integriert.

Die Namensauflösung von *zusatzfirma* nach *firma* ermöglicht der Assistent auf die gleiche Art wie auf *R-DC01* in *forschung*. Auf *HB-DC01* werden Weiterleitungen an *B-DC01* konfiguriert. Es gelten die bereits genannten Bedenken.

Zwischenstand

Im oben genannten Beispiel sitzt ein Mitarbeiter der Regensburger Forschungsabteilung in Bremen am Computer *HB-PC01* aus der Domäne *zusatzfirma.intern*. Damit er sich mit den Benutzerdaten der Regensburger Domäne *forschung.firma.intern* anmelden kann, sind für eine erfolgreiche Namensauflösung mehrere Schritte erforderlich:

- ✓ *HB-PC01.zusatzfirma.intern* sendet eine rekursive Abfrage an den Anmeldeserver für *forschung.firma.intern*, die vom zuständigen DNS-Server *HB-DC01.zusatzfirma.intern* bearbeitet wird.
- ✓ Da *HB-DC01* diese Informationen nicht enthält, schickt er eine rekursive Abfrage an seinen Weiterleitungs-Server *B-DC01.firma.intern*.

- ✓ *B-DC01* enthält zwar nicht die benötigten Informationen, kennt aber aufgrund der Delegation von *forschung.firma.intern* den Nameserver der gesuchten Domäne: *R-DC01*. Dort fragt er nach und liefert die Antwort zurück an *HB-DC01*.
- ✓ *HB-DC01* leitet die Antwort weiter an *HB-PC01* und der Benutzer kann sich anmelden.

Sollten sich die drei Domänen an unterschiedlichen Standorten befinden, erfolgt die Namensauflösung über WAN-Verbindungen, was länger dauert. In so einem Fall kann es günstig sein, wenn sich die benötigten Informationen bereits auf *HB-DC01* befinden. Eine Verbesserung wäre es auch, wenn *B-DC01* als Zwischenschritt entfällt.

Active-Directory-integrierte Zonen

AD-integrierte Zonen gibt es nur auf DNS-Servern, die auf einem Domänencontroller ausgeführt werden. Ihr wesentlicher Vorteil ist, dass jede AD-integrierte Zone eine primäre Zone, und damit beschreibbar ist. Das ist von Vorteil, wenn Sie mit dynamischen Aktualisierungen arbeiten, da die Aktualisierungen auf jedem DNS-Server erfolgen können.

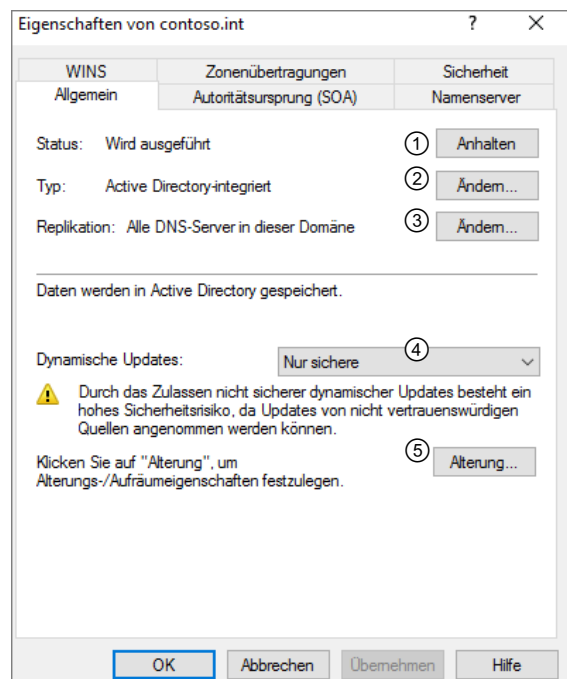
Der Inhalt einer AD-integrierten Zone wird nicht in einer Textdatei gespeichert, sondern in der AD-Datenbank. Auch die Replikation erfolgt nicht über einen Zonentransfer, sondern zusammen mit der AD-Replikation. Sind mehrere DCs vorhanden, erspart das Arbeit, da die Zone inklusive der Konfiguration automatisch auf allen DCs erscheint, die im Replikationsbereich der Zone liegen.

Sie können sekundäre Zonen erstellen, deren Grundlage eine AD-integrierte Zone ist. Die folgende Abbildung zeigt die Eigenschaften einer AD-integrierten Zone.

① ermöglicht es, eine Zone anzuhalten. Anfragen zu angehaltenen Zonen werden nicht beantwortet.

Mit ② ändern Sie den Zonentyp zwischen AD-integriert, nicht AD-integriert. Bei nicht AD-integrierten sekundären Zonen können Sie den Speicherort der primären Zone auf diesen Rechner verlegen. Machen Sie einfach aus der sekundären Zone eine primäre. Das funktioniert nur, wenn Sie entsprechende Rechte in der primären Zone haben. Nach erfolgreicher Umstellung ist die ehemalige primäre Zone eine sekundäre.

③ betrifft nur AD-integrierte Zonen, bei anderen ist diese Zeile ausgegraut. Hier legen Sie fest, wohin die Zonendaten repliziert werden, auf alle DNS-Server dieser Domäne oder auf alle DNS-Server in der Gesamtstruktur. Einstellungen für die Gesamtstruktur können nur Mitglieder der Gruppe Organisations-Admins festlegen.



Bei Standardzonen schalten Sie mit ④ dynamische Aktualisierungen ein oder aus. Bei AD-integrierten Zonen können Sie zusätzlich zwischen nur sicheren und beliebigen dynamischen Updates unterscheiden.

Nur sichere bedeutet, dass nur Clients, die sich erfolgreich authentifiziert haben, ihre Einträge erstellen bzw. ändern dürfen. Diese Sicherheit ist wichtig, um beispielsweise zu verhindern, dass plötzlich Einträge für nicht vorhandene oder feindliche DCs im DNS auftauchen.

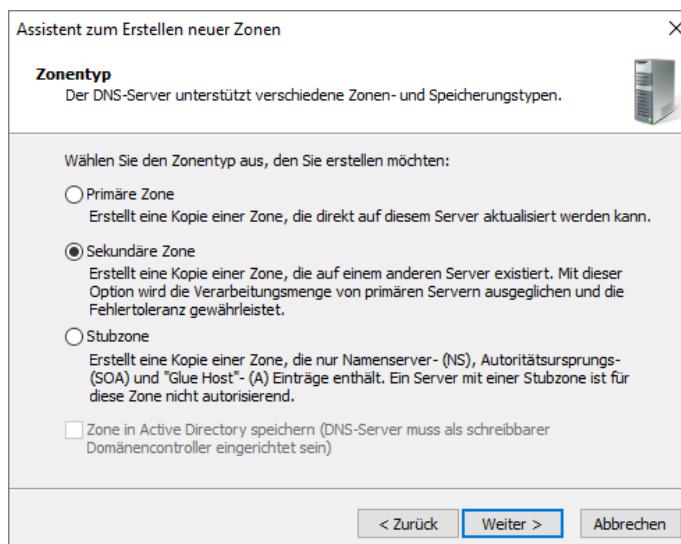
Für diejenige Zone, die Ihre AD-Domäne beinhaltet, sollten Sie unter ⑤ einschalten, dass veraltete Einträge automatisch entfernt werden. Solche Einträge können entstehen, wenn Rechner häufig ihre IP-Adresse ändern. Als Intervalle geben Sie die (größte) Leasedauer an, die Sie für Ihre DHCP-Bereiche konfiguriert haben. Damit wirklich aufgeräumt wird, müssen Sie zusätzlich in den Eigenschaften des DNS-Servers auf dem Register *Erweitert* die Option *Aufräumvorgang bei veralteten Einträgen* aktivieren. Manuell erstellte Einträge sind davon nicht betroffen.

9.4 DNS-Server konfigurieren

Sekundäre Forward-Lookupzone erstellen

Das Beispiel von oben wird fortgeführt. Die Domäne *zusatzfirma.intern* benötigt häufig Zugriff auf Ressourcen aus *forschung.firma.intern*. Deshalb sollen deren DNS-Informationen auf den DCs in *zusatzfirma.intern* gespeichert werden. Dazu sind Schritte in beiden Domänen erforderlich. Zunächst wird die Zone auf *B-DC01* erstellt:

- ▶ Erweitern Sie im Server-Manager unter *Rollen* das DNS-Snap-In und klicken Sie mit rechts auf *Forward-Lookupzonen*. Im Kontextmenü wählen Sie *Neue Zone*.
- ▶ Der Assistent heißt Sie willkommen. Klicken Sie auf *Weiter*.
- ▶ Wählen Sie als Zonentyp *Sekundäre Zone*, sonst erhalten Sie keine Kopie des Inhalts.
- ▶ Geben Sie als Zonenname *forschung.firma.intern* ein. Damit legen Sie sowohl den Namen der DNS-Domain als auch den Namen der Zonendatei fest.
Alle nicht AD-integrierten Zonen werden im Ordner `%windir%\system32\dns` gespeichert. Der Name der Zonendatei lautet *forschung.firma.intern.dns*.



- ▶ Auf der Seite *Master-DNS-Server* legen Sie fest, von wo die Zone repliziert wird. Sie können die IP-Adresse eingeben oder den FQDN *R-DC01.forschung.firma.intern*. Für Fehlerredundanz ist es günstig, hier mehrere Server anzugeben. Der Server mit der besten Netzverbindung sollte oben in der Liste stehen.
Jeder hier angegebene Master-DNS-Server muss Zonenübertragungen an *B-DC01* erlauben.
Zusätzliche Master-DNS-Server können Sie auch später hinzufügen. Klicken Sie in den Eigenschaften der Zone im Register *Allgemein* auf *Bearbeiten*.
- ▶ Auf der letzten Seite des Assistenten kontrollieren Sie Ihre Einstellungen und klicken auf *Fertig stellen*.

Werden weitere Domänencontroller in *zusatzfirma.intern* installiert, müssen diese Schritte auf jedem DC erfolgen. Wahrscheinlich ist es dann auch besser, dort *B-DC01* als Master-DNS-Server auszuwählen. Entscheidungskriterium dafür sind die verfügbare Netzwerkbandbreite und die benötigte Erlaubnis zum Zonentransfer. Auf *B-DC01* kann das ein Domänen-Admin von *zusatzfirma.intern* erledigen.

Auf *R-DC01.forschung.firma.intern* muss *B-DC01* die Erlaubnis zum Zonentransfer erhalten. Die folgenden Einstellungen betreffen nur sekundäre Zonen.

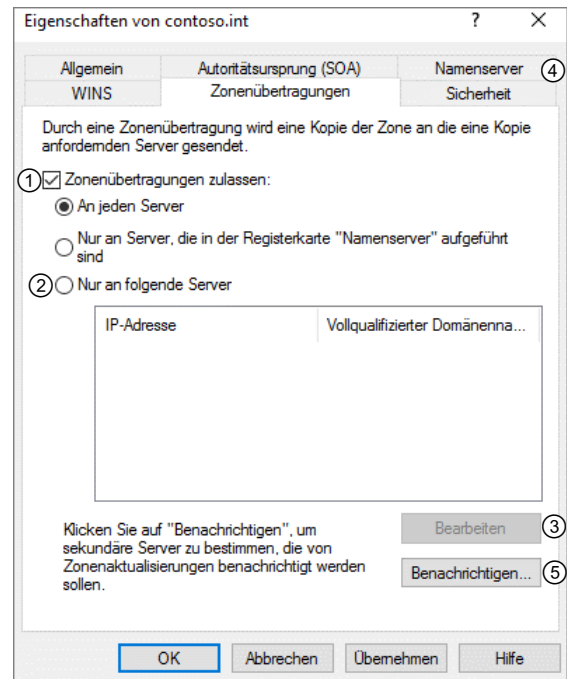
- ▶ Öffnen Sie mit einem Rechtsklick die Eigenschaften der Zone *forschung.firma.intern* und wechseln Sie auf das Register *Zonenübertragungen*.

Mit ① müssen Sie Zonenübertragungen zulassen. Diese sollten nicht an jeden Server möglich sein.

Wenn Sie die Liste manuell festlegen wollen ②, können Sie nach einem Klick auf ③ die Server angeben.

DNS bietet auch die Möglichkeit, einen DNS-Server nach einer Liste der Nameserver für eine Domain zu fragen. Domänencontroller tragen sich in AD-integrierten Zonen selbstständig ein. Für *B-DC01* müsste ein entsprechender NS-Record manuell erstellt werden. Pflegen können Sie die Liste der NS-Einträge auf dem Register ④.

Die Häufigkeit der Zonentransfers wird im Autoritätsursprung (SOA, Start of Authority) festgelegt. Der Standardwert für das Aktualisierungsintervall beträgt 15 Minuten. Über ⑤ können Sie einstellen, dass bei Veränderungen der Zone eine sofortige Benachrichtigung erfolgt. Sie geben dort entweder eine Liste von Servern an oder legen die Nameserver auf dem Register ④ als Benachrichtigungsziel fest.



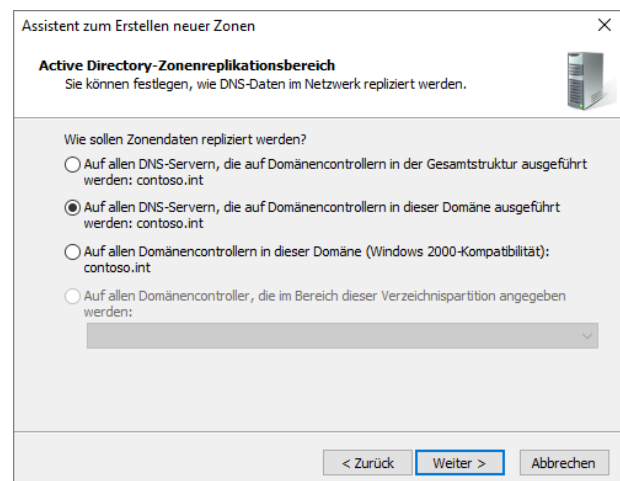
Da es sich bei *forschung.firma.intern* um eine AD-integrierte Zone handelt, können diese Einstellungen auf einem beliebigen DC der Domäne *forschung* erfolgen.

Stubzone erstellen

Eine Stubzone ist weitgehend vergleichbar mit einer sekundären Zone. Nur ist sie stark reduziert, sie speichert ausschließlich Einträge zu Nameservern und eignet sich damit als intelligente Alternative zu den vorhandenen Weiterleitungen. Der wesentliche Unterschied ist die AD-Integrierbarkeit von Stubzones.

Im folgenden Beispiel wird auf *HB-DC01* die Weiterleitung an *B-DC01* durch eine passende Stubzone ersetzt.

- ▶ Klicken Sie mit rechts auf *Forward-Lookupzonen*. Wählen Sie im Kontextmenü *Neue Zone*.
- ▶ Der Assistent heißt Sie willkommen. Klicken Sie auf *Weiter*.
- ▶ Wählen Sie als Zonentyp *Stubzone*. Aktivieren Sie die Option *Zone in Active Directory speichern*, dann erscheint die Stubzone automatisch auf allen DCs in *zusatzfirma.intern*.
- ▶ Im nächsten Schritt legen Sie den Active Directory-Zonenreplikationsbereich fest. Übernehmen Sie die Voreinstellung *Auf allen DNS-Servern, die auf Domänencontrollern in dieser Domäne ausgeführt werden*.
- ▶ Geben Sie den Zonennamen an, der gleichzeitig auch die Domain festlegt: *firma.intern*.
- ▶ Geben Sie auf der nächsten Seite mindestens einen Master-DNS-Server an: *B-DC01.firma.intern*.
- ▶ Kontrollieren Sie auf der letzten Seite die Einstellungen und klicken Sie auf *Fertig stellen*.



Wenn die ersten Einträge in der neuen Zone erschienen sind, können Sie die Weiterleitungen an *B-DC01* in den Servereigenschaften löschen. Durch den Zonentransfer werden neue Nameserver in *firma.intern* automatisch in die Stubzone repliziert.

Primäre Forward-Lookupzone erstellen

Zur weiteren Behandlung des Themas wird davon ausgegangen, dass in der Domäne *forschung.firma.intern* eine zusätzliche DNS-Domain benötigt wird: *entwicklung.firma.intern*. Dies soll keine Active Directory-Domäne sein.

Eine untergeordnete Domäne zu *firma.intern* wird deshalb für das Beispiel gewählt, weil sich damit bisher fehlende Punkte der DNS-Konfiguration besser erklären lassen.

- ▶ Klicken Sie mit rechts auf *Forward-Lookupzonen*. Wählen Sie im Kontextmenü *Neue Zone*.
- ▶ Der Assistent heißt Sie willkommen. Klicken Sie auf *Weiter*.
- ▶ Wählen Sie als Zonentyp *Primäre Zone*. Bei aktivierter Option *Zone in Active Directory speichern* erscheint sie automatisch auf allen DCs in *forschung*. Wenn möglich sollten Sie immer mit AD-integrierten Zonen arbeiten.
Gegen die AD-Integration könnte sprechen, dass diese Zone nur von wenigen Rechnern benötigt wird und die AD-Replikation nicht zusätzlich belasten soll.
- ▶ Übernehmen Sie als Zonenreplikationsbereich *Auf allen DNS-Servern, die auf Domänencontrollern in dieser Domäne ausgeführt werden*.
Dieser Schritt entfällt, wenn Sie keine AD-integrierte Zone erstellen.
- ▶ Geben Sie als Zonenname *entwicklung.firma.intern* ein.
- ▶ Bei einer nicht AD-integrierten Zone legen Sie jetzt den Namen der Zonendatei fest. Der Assistent schlägt *entwicklung.firma.intern.dns* vor. Sollen die DNS-Daten aus einer bereits vorhandenen Datei eingelesen werden, können Sie deren Dateinamen angeben. Der Speicherort ist vorgegeben.
- ▶ Legen Sie im nächsten Fenster fest, ob Sie dynamische Updates zulassen. Bei AD-integrierten Zonen schlägt der Assistent *nur sichere* vor, bei einer klassischen *Dynamische Updates nicht zulassen*.
- ▶ Kontrollieren Sie im letzten Schritt wieder Ihre Einstellungen und klicken Sie auf *Fertig stellen*.

Die Zone ist erstellt und kann mit Einträgen gefüllt werden. In *forschung* wird die Namensauflösung für *entwicklung.firma.intern* funktionieren, da die DCs die Zone vorhalten. *Firma.intern* und *zusatzfirma.intern* wissen allerdings nichts von dieser neuen Zone. Deshalb sind Nacharbeiten notwendig.

Delegierung erstellen

Bei einer Delegierung werden einer Zone die Nameserver der untergeordneten, delegierten Zone hinzugefügt. Die Delegierung für *entwicklung* muss also in der Zone *firma.intern* auf *B-DC01* erfolgen.

- ▶ Klicken Sie mit rechts auf die Zone *firma.intern* und wählen Sie im Kontextmenü *Neue Delegierung*.
- ▶ Der Assistent heißt Sie willkommen. Klicken Sie auf *Weiter*.
- ▶ Geben Sie im nächsten Schritt den Namen der delegierten Domäne ein: *entwicklung*.
Die nicht editierbare Zeile darunter zeigt Ihnen den vollständigen Namen: *entwicklung.firma.intern*.
- ▶ Jetzt müssen Sie Nameserver für die delegierte Zone angeben. Klicken Sie auf *Hinzufügen*.
- ▶ Geben Sie den FQDN von *entwicklung.firma.intern* ein. Die zugehörige IP-Adresse erhalten Sie entweder über *Auflösen* oder Sie geben sie manuell ein.
- ▶ Sie können weitere Nameserver hinzufügen und die vorhandenen bearbeiten oder entfernen.
Aus Fehlerredundanzgründen sollten mehrere Nameserver eingetragen sein.
- ▶ Klicken Sie im letzten Schritt des Assistenten auf *Fertig stellen*.

Die Einträge in der Delegierung passen sich nicht an, wenn zusätzliche Nameserver diese Zone vorhalten oder vorhandene Zonen entfernt werden. Zur späteren Pflege der Einträge bearbeiten Sie die Eigenschaften der Delegierung. Eine Stubzone ist eine dynamische Alternative oder Ergänzung zu dieser Delegierung.

Bedingte Weiterleitung

Wollen Sie festlegen, welche Nameserver für Abfragen einer bestimmten Domain zuständig sind, dann konfigurieren Sie bedingte Weiterleitungen. Deren Einträge werden nicht automatisch aktualisiert (kein Zonentransfer), weshalb auch keinerlei Berechtigungen in der Original-Zone erforderlich sind. Bedingte Weiterleitungen eignen sich deshalb besonders für AD-externe Zonen, die nicht über die Namensauflösung im Internet erreichbar sind.

So können Sie z. B. auf *ftp-server.befreundete.firma* zugreifen, indem Sie eine bedingte Weiterleitung für die Domäne *befreundete.firma* einrichten. Da die Top-Level-Domain *firma* von *root* nicht unterstützt wird, hätten Sie ohne bedingte Weiterleitung keine Möglichkeit für eine serverbasierte Auflösung des FQDN und müssten als Lösung die Hosts-Datei bearbeiten.

- Klicken Sie mit rechts auf *Bedingte Weiterleitungen*.

Mit ① legen Sie den Namen der befreundeten DNS-Domäne fest, z. B. *befreundete.firma*. Unter ② geben Sie die IP-Adresse oder den FQDN eines Namensservers an, der diese Zone speichert, z. B. *dns.befreundete.firma*. Den Servernamen erfragen Sie bitte vom zuständigen Administrator der befreundeten Firma.

Mehrere Einträge bieten Fehlertoleranz. Derjenige Server, zu dem die beste Verbindung besteht, sollte oben in der Liste stehen. Wenn Sie die Weiterleitung im AD speichern ③, müssen Sie sie nicht auf jedem DC konfigurieren.

Reverse-Lookupzone erstellen

Reverse-Lookupzonen benötigen Sie zum Auflösen von IP-Adressen in FQDNs. Sind passende Reverse-Lookupzonen eingerichtet, kann beim Erstellen neuer Host-Einträge automatisch der entsprechende PTR(Pointer)-Eintrag in der Reverse-Lookupzone erstellt werden.

Grundsätzlich wird Reverse Lookup für ein funktionierendes Active Directory nicht benötigt. Allerdings überprüfen manche Anwendungen aus Sicherheitsgründen den Rechnernamen durch eine entsprechende Abfrage. Beispielsweise vergleichen manche Spam-Filter auf SMTP-Servern, ob der im Mail-Header angegebene SMTP-Server tatsächlich zur sendenden IP-Adresse passt.

- Klicken Sie mit rechts auf den Eintrag *Reverse-Lookupzonen*.
- Der Assistent heißt Sie willkommen. Klicken Sie auf *Weiter*.
- Übernehmen Sie als Zonentyp den Vorschlag des Assistenten, eine primäre, AD-integrierte Zone.
- Übernehmen Sie als Zonenreplikationsbereich *auf alle DNS-Server in dieser Domäne*.
- Übernehmen Sie auch den Vorschlag *IPv4 Reverse-Lookupzone*.
- Tragen Sie als Name der Reverse-Lookupzone die Netzwerk-ID Ihres Netzes ein, z. B. 192.168.100 oder 10.10.

Arbeiten Sie mit mehreren IP-Netzen, müssen Sie auch mehrere Reverse-Lookupzonen anlegen. Eventuell lassen sich einige Netze auch zusammenfassen. Beispielsweise könnten hinter dem Eintrag 10.10 die tatsächlich verwendeten Subnetze 10.10.0/24 bis 10.10.255/24 stecken.

- Übernehmen Sie den Vorschlag *Nur sichere dynamische Updates* zulassen.
- Klicken Sie auf der letzten Seite des Assistenten auf *Fertig stellen*.

DNS-Einträge erstellen

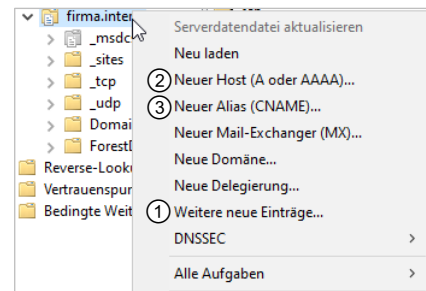
Dank dynamischer Updates wird der größte Teil der DNS-Einträge automatisch erstellt. Dennoch werden Sie gelegentlich Einträge manuell konfigurieren, beispielsweise für Router mit statischer IP-Adresse.

- Klicken Sie mit rechts auf die Zone, in der der Eintrag erstellt werden soll.

Im Kontextmenü werden die wichtigsten Eintragstypen direkt angeboten.

Finden Sie hier nicht den gewünschten Eintragstyp, erhalten Sie unter ① eine Komplettauswahl aller möglichen Einträge.

Es folgen Beispiele für einen neuen Host ② und einen Alias ③.



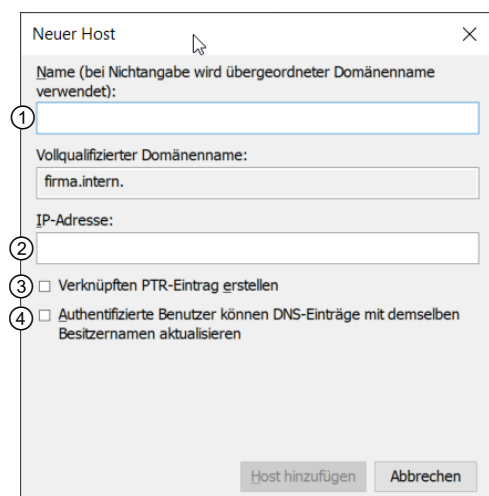
Host erstellen

Als Namen können Sie den Hostnamen des Rechners eingeben ①.

Unter ② legen Sie die IP-Adresse fest.

Mit *Verknüpften PTR-Eintrag erstellen* ③ bestimmen Sie, ob ein entsprechender Eintrag in der Reverse-Lookupzone erstellt wird. Ist keine passende Zone vorhanden, erhalten Sie eine Fehlermeldung.

④ ermöglicht es einem Rechner mit identischem FQDN, diesen Eintrag dynamisch zu aktualisieren. Das kann sinnvoll sein, wenn Sie einen Rechner schon vor dessen Installation oder Umbenennung im DNS eintragen wollen.



Alias erstellen

Ein CNAME (Canonical Name) bietet eine einfache Möglichkeit, einem Rechner mehrere Namen zu geben. Eingesetzt wird das häufig, wenn bestimmte Rechner über ihre Funktion angesprochen werden sollen, z. B. *www*, *ftp* oder *mail*. Natürlich könnten Sie dafür auch zusätzliche A-Einträge erstellen. Diese aktualisieren sich aber nicht automatisch, wenn sich die IP-Adresse des Hosts ändert. Ein Alias verweist auf einen anderen A-Record.

- Tragen Sie den zusätzlichen Namen ein.
- Geben Sie den FQDN ein.
Stattdessen können Sie auch auf *Durchsuchen* klicken und einen Rechner aus einer vorhandenen Zone auswählen.
- Legen Sie fest, ob authentifizierte Benutzer (der Inhaber des FQDN) den Eintrag aktualisieren sollen.
- Betätigen Sie Ihre Konfiguration wie gewohnt.

Probleme in der Namensauflösung beheben

Funktioniert die Namensauflösung nicht, sollten Sie strukturiert vorgehen, um Fehler zu finden. Auch wenn der Fehler auf den ersten Blick nichts mit DNS zu tun hat, lohnt es sich zu überprüfen, ob sich Namen korrekt auflösen lassen. Überprüfen Sie, ob sich der Server sowohl in der Forward- als auch in der Reverse-Lookupzone korrekt eingetragen hat. Öffnen Sie danach eine Eingabeaufforderung und geben Sie den Befehl `nslookup` ein. Die Eingabe des Befehls darf keinerlei Fehlermeldungen verursachen. Es muss der richtige FQDN des DNS-Servers und dessen IP-Adresse angezeigt werden. Sollte das nicht der Fall sein, gehen Sie Schritt für Schritt vor, um den Fehler einzugrenzen:

- ✓ Sollte ein Fehler erscheinen, versuchen Sie es mit dem Befehl `ipconfig /registerdns` in der Eingabeaufforderung.
- ✓ Sollte der Fehler weiterhin auftreten, überprüfen Sie, ob das primäre DNS-Suffix auf dem Server mit dem Zonennamen der DNS-Zone übereinstimmt.
- ✓ Stellen Sie als Nächstes fest, ob die IP-Adresse des Servers stimmt und der Eintrag des bevorzugten DNS-Servers in den IP-Einstellungen korrekt ist.
- ✓ Überprüfen Sie in den Eigenschaften der Zone, ob die dynamische Aktualisierung zugelassen wird und ändern Sie gegebenenfalls die Einstellung, damit die Aktualisierung stattfinden kann. Die Eigenschaften der Zonen erreichen Sie, wenn Sie mit der rechten Maustaste auf die Zone klicken und die Eigenschaften auswählen.

Wenn sich ein Servername mit *nslookup* nicht auflösen lässt, gehen Sie auch hier am besten Schritt für Schritt vor:

- ✓ Ist in den IP-Einstellungen des Servers der richtige DNS-Server als bevorzugt eingetragen?
- ✓ Verwaltet der bevorzugte DNS-Server die Zone, in der Sie eine Namensauflösung durchführen wollen?
- ✓ Wenn der Server diese Zone nicht verwaltet, ist dann auf der Registerkarte *Weiterleitungen* in den Eigenschaften des Servers ein Server eingetragen, der die Zone auflösen kann?
- ✓ Wenn eine Weiterleitung eingetragen ist, kann dann der Server, zu dem weitergeleitet wird, die Zone auflösen?
- ✓ Wenn dieser Server nicht für die Zone verantwortlich ist, leitet er dann wiederum die Anfrage weiter?
- ✓ In Ausnahmefällen kann es vorkommen, dass die Aktualisierung der Reverse-Lookupzone nicht funktioniert hat. In diesem Fall ist der Server zwar in der Forward-Zone hinterlegt, aber nicht in der Reverse-Zone. In diesem Fall können Sie den Eintrag des Servers manuell ergänzen. Dazu müssen Sie lediglich einen neuen Zeiger (engl. Pointer) erstellen. Ein Zeiger oder Pointer ist ein Verweis von einer IP-Adresse zu einem Hostnamen. Kurz nach der Installation kann dieser Befehl durchaus noch Fehler melden.
- ✓ Versuchen Sie die IP-Adresse des Domänencontrollers erneut mit `ipconfig /registerdns` zu registrieren. Nach einigen Sekunden sollte der Name fehlerfrei aufgelöst werden. Sobald Sie *nslookup* aufgerufen haben, können Sie beliebig Servernamen auflösen. Wenn Sie keinen FQDN eingeben, sondern nur den Computernamen, ergänzt der lokale Rechner automatisch den Namen durch das primäre DNS-Suffix des Computers bzw. durch die in den IP-Einstellungen konfigurierten DNS-Suffixe.

9.5 DNSSEC

Erhöhte Sicherheit

Eine zunehmend verbreitete Angriffsmethode im Internet stellt das Fälschen von DNS-Antworten dar. So versuchen z. B. Betrüger, Benutzer auf gefälschte Bank-Webseiten zu locken, um so an ihre PINs und TANs zu gelangen. DNSSEC (Domain Name System Security Extensions) soll nun verhindern, dass jemand falsche Antworten weitergibt, indem mittels Schlüsselsignatur die Echtheit von Antworten gewährleistet wird. Dabei kommen Verfahren zum Einsatz, die aus der Mail-Signatur bekannt sind (asymmetrische digitale Schlüssel).

DNSSEC wurde seit Anfang des Jahrtausends entwickelt. Am 15. Juli 2012 wurden die entsprechenden Schlüssel auf den Root-Servern veröffentlicht. Details zur Einrichtung von DNSSEC können Sie dem HERDT-Buch *Windows Server 2019 / 2022 – Erweiterte Netzwerkadministration* entnehmen.

10 DHCP – Dynamische IP-Konfiguration

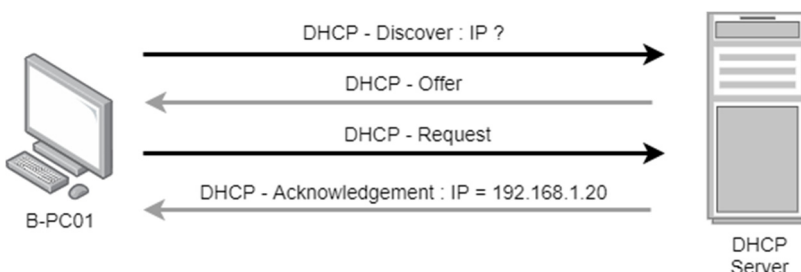
10.1 Dynamic Host Configuration Protocol (DHCP)

Dynamische IP-Konfiguration mit DHCP

Jeder Rechner benötigt für die Kommunikation im Netzwerk eine eindeutige IP-Adresse. Werden IP-Adressen manuell konfiguriert, 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.

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 Datenverkehr wird letztlich über MAC-Broadcasts abgewickelt.



DHCP - Leasevorgang

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** (Anfrage). Auch der Request 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-Agenten erkennt der DHCP-Server auch, welche IP-Adresse der Client benötigt.

DHCP-Relay wird auch als BootP-Relay bezeichnet, denn hier wird dasselbe Verfahren (und die identischen Ports 67 und 68) 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.

10.2 DHCP-Server installieren

Rolle hinzufügen

DHCP können Sie auf jedem Server innerhalb der Domäne installieren, dessen IP-Konfiguration manuell erfolgt ist.

- ▶ Klicken Sie im Server-Manager auf *Verwalten - Rollen und Features 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.

10.3 DHCP-Server konfigurieren

Überblick

Nach der erfolgreichen Installation und Autorisierung des DHCP-Servers werden alle weiteren Einstellungen in der DHCP-Konsole durchgeführt.

- ▶ Geben Sie im Startmenü `dhcp` ein und klicken Sie auf *DHCP*.
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. Auch die Autorisierung des Servers nehmen Sie in diesem Fenster vor.

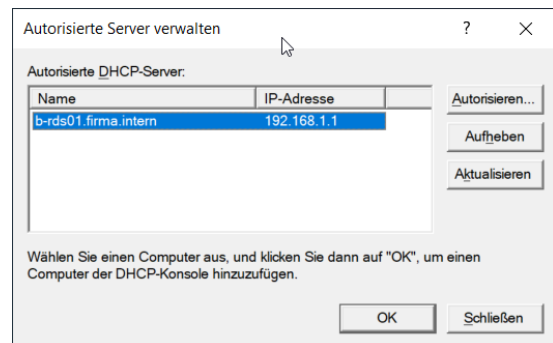
In Ihrem Firmennetzwerk sollten sich stets mehrere DHCP-Server befinden. Diese werden jedoch nicht automatisch angezeigt, sondern müssen manuell in die Konsole aufgenommen werden.

- ▶ 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 *Dieser autorisierte DHCP-Server* und wählen Sie alle Server aus, die hinzugefügt werden sollen.
Falls der Server nicht aufgeführt ist, können Sie den Namen des Servers eingeben oder auf *Durchsuchen* klicken, um die erweiterten Suchmöglichkeiten zu nutzen.

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.

- ▶ 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 *Autorisieren*.
- ▶ 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*.

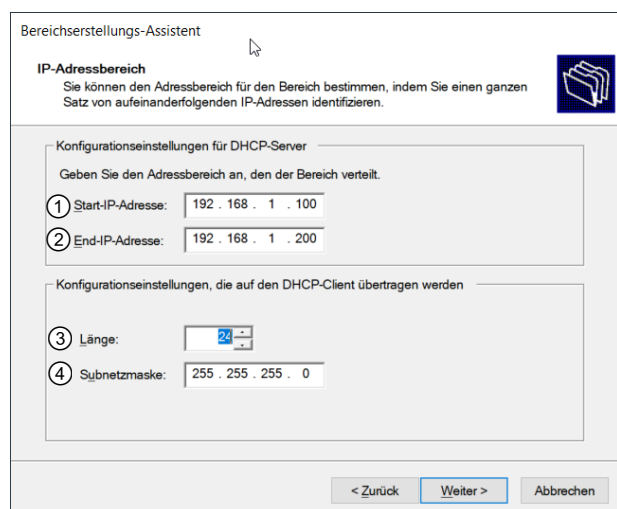


Hinzufügen weiterer DHCP-Server

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.

- ▶ 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 und Beschreibung ein und klicken Sie auf *Weiter*.
- ▶ Geben Sie den IP-Adressbereich an, aus dem Adressen vergeben werden. Dazu legen Sie die kleinste ① und größte IP-Adresse ② fest.
Meistens ist es günstig, hier das komplette IP-Netz anzugeben.
Die Subnetzmaske können Sie entweder durch die Anzahl der gesetzten Bits festlegen ③ oder direkt eingeben ④. Diesen Wert können Sie später nicht mehr verändern!
- ▶ Klicken Sie auf *Weiter*.



IP-Adressbereich und Subnetz festlegen

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.

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.

► 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.

Ausschlüsse und Verzögerungen

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 ist 8 Tage.

Weist ein DHCP-Server einem Client eine IP-Adresse zu, dann ist diese Zuweisung immer auf einen gewissen Zeitraum beschränkt, die sogenannte Leasedauer, die in der Standardeinstellung 8 Tage beträgt. Windows Server 2022 unterscheidet an dieser Stelle nicht zwischen stationären (verkabelten) Computern, die erfahrungsgemäß länger mit dem Netzwerk verbunden sind und mobilen (drahtlosen) Computern, also Notebooks von mobilen Mitarbeitern.

Je länger die Leasedauer, umso länger wird eine IP-Adresse für einen Client reserviert. Abhängig von dieser Zeit durchläuft der DHCP-Client drei Phasen:

Nachdem die Leasedauer zur Hälfte abgelaufen ist, wendet sich der Client an den Server, um die erhaltene IP-Adresse erneut zu bestätigen. Ist der DHCP-Server betriebsbereit, wird die Leasedauer wieder auf ihren ursprünglichen Wert zurückgesetzt, also verlängert. Antwortet der Server nicht, wird der Client in regelmäßigen Abständen einen neuen Versuch unternehmen.

Steht nach Ablauf der Zeit der ursprüngliche DHCP-Server nicht mehr zur Verlängerung zur Verfügung, versucht der DHCP-Client nach 7/8 der Leasedauer, irgendeinen DHCP-Server zu erreichen, der ihm eine neue IP-Adresse zuweisen kann. Auch diesen Versuch wiederholt er in regelmäßigen Abständen.

Nach Ablauf der Leasedauer muss der Client seine IP-Adresse freigeben und versucht nun weiter, einen DHCP-Server zu erreichen, der ihm eine neue IP-Adresse zuweist.

Bei ausreichend verfügbaren IP-Adressen sollte die Leasedauer möglichst hoch gesetzt werden, damit die Clients keine unnötige Netzwerklast erzeugen. Nur wenn die Anzahl der verfügbaren Adressen kleiner als die Gesamtzahl der Computer ist, sollte der Wert so niedrig gewählt werden (unter Umständen sogar im Stundenbereich), dass der DHCP-Server nicht mehr benötigte Adressen schnell wieder aus der Datenbank löschen und anderen Clients zuweisen kann. Nach der Installation des DHCP-Servers kann die Leasedauer noch genauer konfiguriert werden.

► 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.

- Fügen Sie die IP-Adresse von mindestens einem Router (Standardgateway) hinzu.
- Legen Sie das primäre DNS-Suffix 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 gerade erstellten DHCP-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

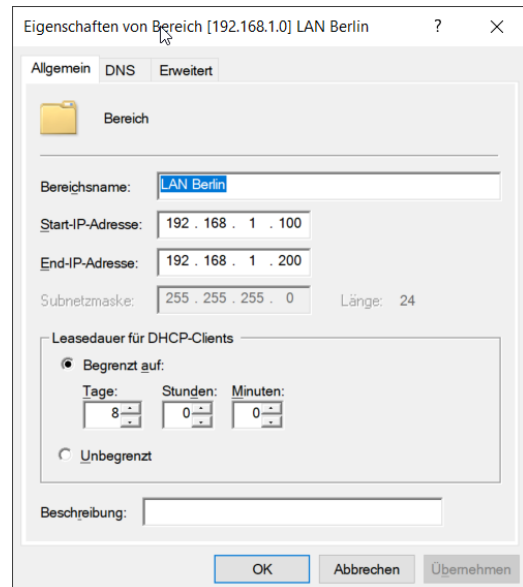
Sie können bestehende Bereiche nachträglich konfigurieren. Hier können Sie zusätzliche Einstellungen vornehmen, die während der Erstellung nicht verfügbar waren.

- ▶ Klicken Sie mit der rechten Maustaste auf den Bereich und wählen Sie *Eigenschaften*.

Der Eigenschaftendialog 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.



Leasedauer einstellen

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.

Die Standard-Leasedauer 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, mit `ipconfig /renew` wird ein neuer Lease angefordert.

Dynamische DNS-Aktualisierungen anpassen

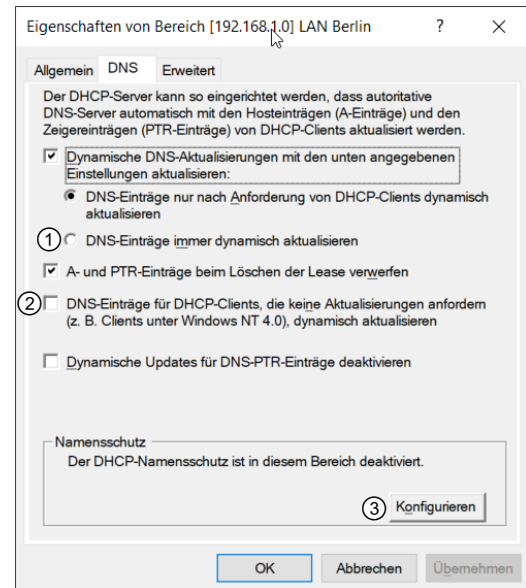
Der DHCP-Server kann beim Vergeben einer Lease entsprechende Einträge im DNS erstellen. Wenn Sie DNS ausschließlich für Rechner ab Windows XP benötigen, sollten Sie die Einstellungen im Register *DNS* nicht verändern.

- Klicken Sie mit der rechten Maustaste auf den DHCP-Bereich und wählen Sie *Eigenschaften*. Wechseln Sie anschließend im Eigenschaftendialog auf das Register *DNS*.

Mit ① legen Sie fest, dass der DHCP-Server DNS-Aktualisierungen übernimmt, unabhängig davon, ob der Client solche anfordert oder nicht. Dem Client wird mitgeteilt, dass der DHCP-Server das übernimmt. Hierbei wird die DHCP-Option 081 verwendet, die in der Optionsliste nicht aufgeführt ist.

Mit ② schalten Sie ein, dass der DHCP-Server auch Clients vor Windows 2000 im DNS registriert, die die Option 081 noch nicht unterstützen.

Unter *Konfigurieren* ③ können Sie den Namensschutz aktivieren. Dadurch wird verhindert, dass bereits vorhandene DNS-Einträge überschrieben werden.



Wenn Sie die DNS-Aktualisierung verändern, müssen Sie dafür sorgen, dass der DHCP-Server bei den Aktualisierungen mit einem Benutzerkonto arbeitet. Dazu öffnen Sie die Eigenschaften von IPv4 und klicken im Register *Erweitert* auf *Anmeldeinformationen*. Ein normales Benutzerkonto in der Domäne des DNS-Servers ist dafür ausreichend, Sie müssen nur darauf achten, dass das Kennwort nicht abläuft.

In der Gruppe *DnsUpdateProxy* in der Domäne befinden sich Computer, die als Proxy für die dynamische Aktualisierung von DNS-Einträgen fungieren können. DHCP-Server werden in diese Gruppen nicht automatisch aufgenommen. Sie sollten die Computerkonten der DHCP-Server in die Gruppe *DnsUpdateProxy* aufnehmen, wenn die DNS-Aktualisierung nicht funktioniert. Alternativ können Sie auf der Registerkarte *Erweitert* in den Eigenschaften für IPv4 oder IPv6 Anmeldedaten hinterlegen, die eine Aktualisierung ermöglichen.

Weitere Bereichseigenschaften

Im Register *Failover* werden die aktuellen Failover-Einstellungen angezeigt, Sie können hier jedoch nicht die Failover-Einrichtung vornehmen. Daher sind die Einstellungen ausgegraut. Im fünften 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.

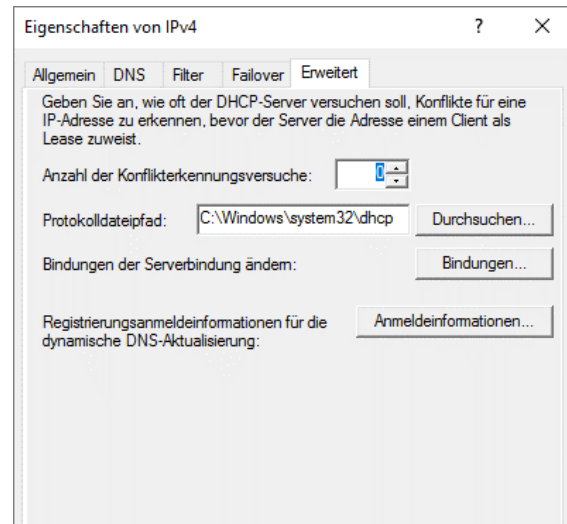
Eigenschaften von IPv4 oder IPv6 anpassen

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*.

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 umkonfigurieren 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.

Konfigurieren Sie in aller Regel die grundlegenden Einstellungen für alle Bereiche als Serveroptionen. Typische Beispiele hierfür sind z. B. die DNS-Server und WINS-Server eines Standorts. Typische Bereichsoptionen sind z. B. das Default-Gateway und dedizierte Router, die für jeden Bereich unterschiedlich sind.

- ▶ Um die **Serveroptionen** zu öffnen, klicken Sie mit der rechten Maustaste auf *IPv4* bzw. *IPv6* und wählen Sie *Optionen konfigurieren*.

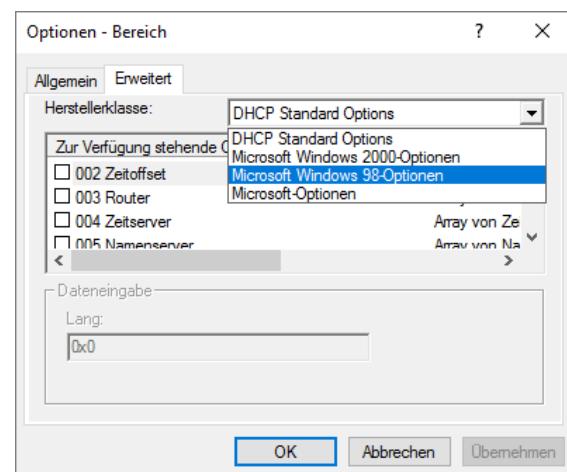
oder

- ▶ Um die **Bereichsoptionen** zu öffnen, klicken Sie im Bereich mit der rechten Maustaste 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 Microsoft Windows-Versionen zu aktivieren.

- ▶ Aktivieren Sie eine Option 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.

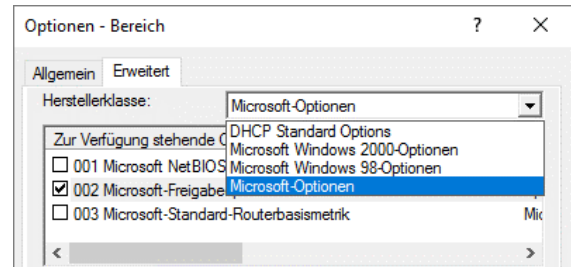
Bei der Eingabe mehrerer IP-Adressen steht die bevorzugte IP-Adresse stets oben. Sie können Einträge hinzufügen oder entfernen.



Wenn Sie WINS-Server (Option 044) angeben, sollten Sie auch den WINS/NBT-Knotentyp (Option 046) konfigurieren. Hier sollten Sie als Wert 0x8 eintragen. Dieser bewirkt, dass vor dem Versuch einer NetBIOS-Namensauflösung mittels Broadcast eine dedizierte Anfrage an einen WINS-Server gesendet wird. Nur wenn diese erfolglos bleibt, wird anschließend das Netzwerk mit einem Broadcast belastet.

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.

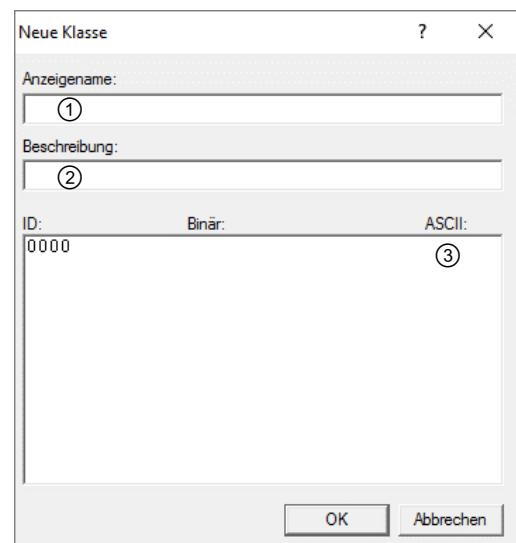


Bei älteren Microsoft Server-Versionen wurden in den Dialogen für die Server- und Bereichsoptionen neben den Herstellerklassen auch die Benutzerklassen angezeigt. Diese können Sie jetzt erreichen, indem Sie im Kontextmenü von IPv4 bzw. IPv6 auf *Benutzerklassen definieren* klicken.

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 Einstellungen 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 ① und eine Beschreibung ② der Benutzerklasse ein.
- ▶ Geben Sie unter *ASCII* ③ dieselbe Bezeichnung ein wie unter ① 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 ③.

Mit `ipconfig /SetClassID` ohne weitere Angabe von Parametern entfernen Sie den Client wieder aus der zugewiesenen Klasse.

Herstellerklassen erstellen

- ▶ Klicken Sie mit rechts auf *IPv4* und wählen Sie im Kontextmenü *Herstellerklassen definieren*.

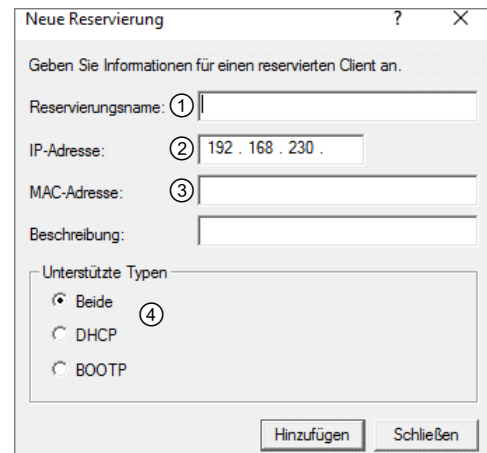
Der weitere Vorgang entspricht dem Hinzufügen von Benutzerklassen.

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 ①; der Name des Netzwerknotens bietet sich dafür an.
- ▶ Ergänzen Sie im Feld ② die IP-Adresse.
- ▶ Geben Sie die MAC-Adresse des Clients ein ③.
- ▶ Aktivieren Sie die entsprechende Option ④.
- ▶ Mit *Hinzufügen* bestätigen Sie die Reservierung.

Anschließend können Sie eine weitere Reservierung eingeben.



Die MAC-Adresse ist auf vielen Netzwerkkomponenten aufgedruckt. Auf einem Windows-Rechner können Sie die MAC-Adressen aller Netzwerkkadpter mit `ipconfig /all` auflisten. Sie werden als „physische Adresse“ angezeigt.

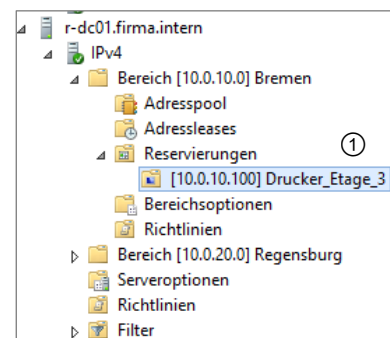
Sie können auch `ping` Netzwerknoten eingeben, um und sich dann die MAC-Adresse mit `arp -a IP-Adresse` anzeigen zu lassen.

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 ① 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.

Für den Fall, dass kein DHCP-Server für das automatische Zuweisen einer IP-Adresse erreicht werden kann, bestimmt Windows eine Adresse in der für Microsoft reservierten IP-Adressierungsklasse, die von 169.254.0.1 bis 169.254.255.254 reicht. Diese Adresse wird verwendet, bis ein DHCP-Server gefunden wird. Dieses Beziehen einer IP-Adresse wird als automatische IP-Adressierung bezeichnet (APIPA).

Bei dieser Methode wird kein DNS, WINS oder Standardgateway zugewiesen, da diese Methode nur für ein kleines Netzwerk mit einem einzigen Netzwerksegment entworfen wurde. Um die APIPA-Funktion zu deaktivieren, müssen Sie in der Registrierung unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters` einen Schlüssel namens `IPAutoconfigurationEnabled` anlegen und ihm den Wert 0 zuweisen. Diese Konfiguration kann derzeit noch nicht über Gruppenrichtlinien verteilt werden. Generell wird empfohlen, die Einstellungen auf den Standardwerten zu belassen.

Um den Ausfall von Arbeitsstationen durch fehlgeschlagene IP-Konfiguration über DHCP zu vermeiden, muss ständig ein DHCP-Server mit freien Adressen verfügbar sein oder eine alternative Konfiguration von Hand auf jedem Rechner für jede Netzwerkkarte eingerichtet werden. Normalerweise werden dafür im Netzwerk mehrere DHCP-Server eingesetzt. Vor einigen Jahren waren die Konfiguration und Koordination der beteiligten DHCP-Server noch aufwendig und schwierig. Nun verfügen die DHCP-Server über leicht zu verwaltende Funktionen für Redundanz und Lastverteilung. DHCP-Failover unterstützt zwei Server mit IPv4-Konfiguration. Die Server können auch Mitglied einer Arbeitsgruppe sein, eine Domänenmitgliedschaft ist nicht unbedingt erforderlich.

Ab Windows 2012/2012 R2 kann mit dem DHCP-Failover die Zusammenarbeit mehrerer DHCP-Server in einem Verbund (Cluster) erheblich vereinfacht werden. 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-Modus** bezeichnet. Failover kann außerdem die Belastung variabel auf beide Server verteilen (Lastenausgleichsmodus oder Load Balance Mode). 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.

- ▶ 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 ①.
- ▶ Stellen Sie im Feld *Maximale Clientvorlaufzeit* (Maximum Client Lead Time, MCLT) ② eine zusätzliche Leasedauer ein, die beim Ausfall eines DHCP-Servers dafür sorgt, dass zwischenzeitlich vergabene Leases nicht erneut vergeben werden können.
Der Standard ist eine Stunde.
- ▶ Wählen Sie bei *Modus* ③ zwischen *Lastenausgleich* und *Hot Standby* aus.
- ▶ Stellen Sie für den Modus *Lastenausgleich* die Lastverteilung ein ④.

oder

- ▶ Stellen Sie für den Modus *Hot Standby* hier ein, wie viel Prozent der im Bereich vorhandenen IP-Adressen für den Standby-Server reserviert werden sollen (nicht abgebildet).

- ▶ Aktivieren Sie bei Bedarf die Option *Intervall für Zustands-Switchover* (Auto State Switchover Interval) ⑤ und stellen Sie ein, wie viel Zeit nach dem letzten Lebenszeichen verstreichen darf, bevor ein DHCP-Server annimmt, dass sein Partner ausgefallen ist ⑥.
- ▶ Aktivieren Sie bei Bedarf die *Nachrichtenauthentifizierung* ⑦ und geben Sie einen geheimen Schlüssel ein, durch den sich die Partnerserver gegenseitig identifizieren können ⑧.
- ▶ 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.

11 Standorte und Replikation

11.1 Überblick über Standorte

Standorte

Standorte dienen dazu, die physischen Gegebenheiten einer Gesamtstruktur abzubilden. Geografisch verteilte Niederlassungen sind in der Regel über (teure und langsame) Mietleitungen verbunden, daher möchte man den Datenverkehr so gering wie möglich halten und bestimmte Verbindungen bevorzugen. Die Standorte im Active Directory ermöglichen es, den standortübergreifenden Datenverkehr zu optimieren. Anschließend greifen die Clients bevorzugt auf lokale Ressourcen am Standort zu, und nur wenn die Ressourcen dort nicht vorhanden sind, wird auf externe Ressourcen zugegriffen. Dabei legen Kosten von Standortverknüpfungen und Zeitreglementierungen fest, welche Verbindung wann genutzt und auf welche Standorte zugegriffen werden soll.

Standorte haben nichts mit Domänen zu tun. An einem Standort können sich alle Ressourcen einer oder mehrerer Domänen befinden oder beliebige Teilmengen davon.

Ein Standort ist eine Ansammlung von Computern, die über schnelle und zuverlässige Datenübertragungswege miteinander verbunden sind (mindestens 512 Kilobit/Sekunde). Langsame Verbindungen, z. B. WAN-Verbindungen, werden genutzt, um die Datenübertragung zwischen Standorten zu ermöglichen. Diese Datenübertragung umfasst dabei neben den Zugriffen der Benutzer auf Netzwerkressourcen den Abgleich der Informationen im Active Directory, der als **Replikation** bezeichnet wird.

Durch das Definieren von Standorten können Sie die Datenübertragungswege gemäß ihrer Geschwindigkeit und Zuverlässigkeit klassifizieren. Dadurch können Sie eine **Replikationstopologie** konfigurieren, die die Datenübertragungswege optimal nutzt.

Das Betriebssystem ordnet Computer automatisch einem Standort zu, indem die IP-Adresse des Computers mit der Liste der bekannten Subnetze und deren Zuordnung zu Standorten verglichen wird.

Zur Einrichtung und Verwaltung von Standorten benötigen Sie die Berechtigungen eines Organisations-Admins, da die Einstellungen domänenübergreifend auf die Gesamtstruktur wirken.

Der erste Standort in einer Gesamtstruktur

Beim Erstellen einer neuen Gesamtstruktur wird gleichzeitig eine physische Struktur erstellt. Sie enthält einen einzigen Standort mit dem Namen *Default-First-Site-Name*. Dieser Standort umfasst am Anfang alle Domänencontroller und alle undefinierten IP-Subnetze.

11.2 Replikation

Grundlegendes zur Replikation

Mit der Ausnahme von schreibeschützten Domänencontrollern (Read-only DC, RODC) können Domänenobjekte auf jedem DC einer Domäne bearbeitet werden. Alle Änderungen werden über die sogenannte Multi-Master-Replikation, bei der die einzelnen DCs gleichberechtigt ihren Inhalt untereinander abgleichen, auch den anderen DCs mitgeteilt. Dabei muss unterschieden werden zwischen standortinterner (Intra-Site) und standortübergreifender Replikation (Inter-Site). Die standortinterne Replikation erfolgt innerhalb weniger Sekunden, während die standort- oder domänenübergreifende Replikation in wesentlich längeren Intervallen erfolgt, dafür aber das Datenaufkommen zwischen den Standorten deutlich reduziert. Domänenübergreifende Replikation ist notwendig, da alle DCs einer Gesamtstruktur über dieselbe Schema- und Konfigurationspartition verfügen müssen und globale Katalogserver eine Teilmenge der Information aller Domänen beinhalten.

Active Directory verfügt unter dem Sammelbegriff **KCC** (Knowledge Consistency Checker) über mehrere Komponenten, die die Replikationstopologie selbstständig einrichten und verwalten. Die wichtigste Komponente ist der **Generator für die standortübergreifende Replikationstopologie** (Inter-Site Topology Generator, **ISTG**), der pro AD-Standort nur einmal existiert, unabhängig von der Anzahl an Domänen und Verzeichnispartitionen.

Der ISTG ist für die standortübergreifende Replikationstopologie und die Verbindungen zwischen den sogenannten Bridgehead-Servern (BHS) zuständig. Der ISTG ermittelt an jedem Standort automatisch einen BHS für jede Verzeichnispartition und jedes Replikationstransportprotokoll. Üblicherweise ist der DC, der die Rolle des ISTG übernimmt, auch ein Bridgehead-Server, diese Aufgabe kann aber auch von einem anderen DC am Standort übernommen werden.

Für die AD-Replikation von Standort zu Standort (Inter-Site) sind ausschließlich die Bridgehead-Server zuständig. Sie dienen dabei als Anlaufstelle oder Brückenkopf. Die BHS sammeln alle Änderungen am Standort und replizieren sie zu den BHS an anderen Standorten. Jeder BHS repliziert eine oder mehrere AD-Verzeichnispartitionen, die in seiner Verzeichnisdatenbank (*NTDS.dit*) enthalten sind und für die er autorisierend ist. So können an einem Standort mehrere BHS vorhanden sein, die jeweils für verschiedene Verzeichnispartitionen zuständig sind.

Da die standortübergreifende AD-Replikation ausschließlich zwischen den BHS konfiguriert wird, werden im Gegensatz zu der standortinternen (Intra-Site) AD-Replikation keine redundanten Verbindungsobjekte erstellt. Es werden lediglich weitere Verbindungsobjekte mit BHS in mehreren AD-Standorten erstellt, wenn es in der Standortverknüpfung (Site-Link) so konfiguriert wurde.

Replikation innerhalb eines Standorts (Intra-Site)

- ✓ Replikation basiert auf Benachrichtigung über Änderungen: Replikationspartner werden nach 15 Sekunden (spätestens nach 5 Minuten) über Änderungen informiert.
- ✓ Erhält ein DC keine Benachrichtigung vom Replikationspartner, fragt er spätestens nach einer Stunde nach.
- ✓ Eine sofortige Replikation findet bei sicherheitsrelevanten Änderungen, z. B. Sperrung eines Benutzerkontos, statt.

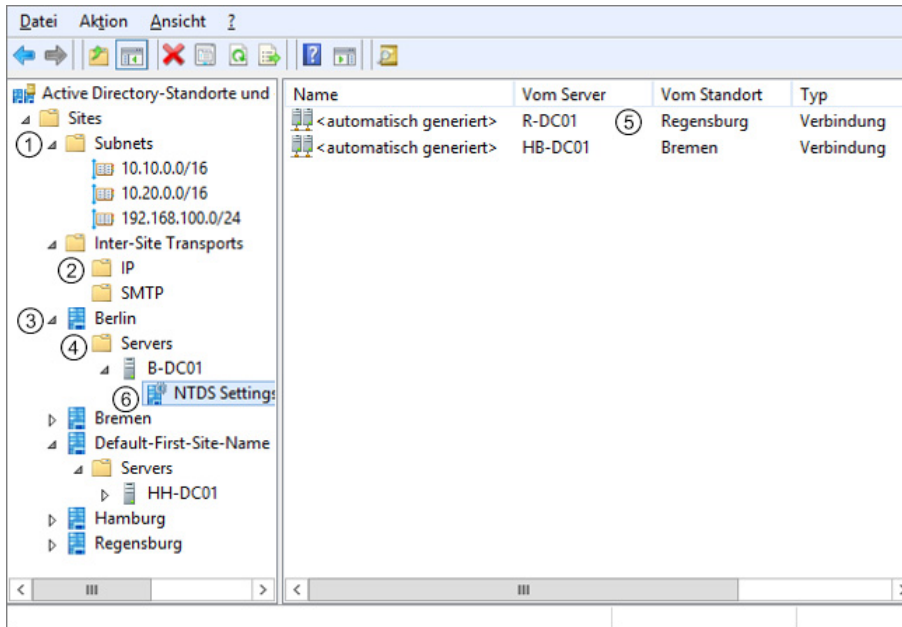
Replikation zwischen Standorten (Inter-Site)

- ✓ Keine Benachrichtigung bei Änderung: Der Zeitplan legt fest, wann und wie häufig repliziert wird.
- ✓ Die Replikation erfolgt komprimiert: (zwar höhere CPU-Last, dafür aber geringerer Bandbreitenbedarf). Der Bridgehead-Server übernimmt die Replikation.
- ✓ Keine sofortige Replikation bei sicherheitsrelevanten Änderungen

11.3 Standorte verwalten

Komponenten der Standortverwaltung

Standorte verwalten Sie mit dem Snap-In *Active Directory-Standorte und -Dienste*. Bei der Konfiguration von Standorten sind mehrere Komponenten beteiligt:



Subnets ① definieren die verwendeten IP-Netze. Hier wurden bereits drei Subnetze erstellt.

Standortverknüpfungen ② werden unter *Inter-Site Transports* im Knoten *IP* konfiguriert. Active Directory legt automatisch den *DEFAULTIPSITELINK* an und fügt alle neuen Standorte dieser Standortverknüpfung hinzu.

Standorte ③ werden unter *Sites* angelegt. Neben dem *Default-First-Site-Name* zeigt die Abbildung die erstellten Standorte *Berlin*, *Bremen*, *Hamburg* und *Regensburg*.

Domänencontroller befinden sich im Knoten *Servers* ④ der einzelnen Standorte. In der Abbildung ist nur der Server *HH-DC01* noch unter *Default-First-Site-Name* zu finden, die anderen Server sind bereits ihren jeweiligen Standorten zugeordnet.

Verbindungsobjekte ⑤ für die AD-Replikation finden sich unter *NTDS Settings* ⑥ bei den einzelnen DCs.

Die Standortverwaltung besteht grundsätzlich aus den folgenden Schritten:

- ✓ Erstellen von Standorten
- ✓ Definieren von IP-Subnetzen und Zuweisen der Subnetze an Standorte
- ✓ Platzieren von Domänencontrollern in Standorten: Das erfolgt automatisch, wenn beim Installieren des DCs Standort und Subnetz schon vorhanden sind und der DC mit einer Standort-IP konfiguriert ist.
- ✓ Erstellen und Konfigurieren von Standortverknüpfungen

Beispiel

Für die weiteren Erklärungen werden Standorte für drei Niederlassungen konfiguriert:

- ✓ **Berlin** stellt die **Firmenzentrale** dar und arbeitet im IP-Netz 10.10/16.
- ✓ In **Regensburg** befindet sich eine Niederlassung, die im Subnetz 10.20/16 arbeitet.

- ✓ In **Bremen** arbeitet die Außenstelle im Subnetz 192.168.100/24.
- ✓ Das Netzwerk ist vollständig geroutet, d. h., jede Niederlassung kann mit jeder anderen kommunizieren.
- ✓ Netzwerkkommunikation zwischen Bremen und Regensburg soll vermieden werden.

Das Beispiel führt zu einer Hub-and-Spokes-Replikationstopologie (Nabe und Speichen). Die Zentrale erhält Informationen von den Außenstellen und verteilt sie an die anderen. Die Außenstellen sprechen nicht direkt miteinander. In vielen Fällen ist dies die beste Lösung.

Neuen Standort einrichten

- ▶ Klicken Sie mit rechts auf *Sites* und wählen Sie im Kontextmenü *Neuer Standort*.
- ▶ Geben Sie den Namen des neuen Standorts ein, z. B. *Bremen*.
Der Standort muss zu einer Standortverknüpfung gehören. Falls die passende Standortverknüpfung noch nicht vorhanden ist, markieren Sie *DEFAULTIPSITELINK* und klicken Sie auf *OK*.

Subnetze einrichten und zuweisen

- ▶ Nach einem Rechtsklick auf *Subnets* wählen Sie im Kontextmenü *Neues Subnetz*.
- ▶ Geben Sie das Adress-Präfix ein, z. B. 192.168.100/24, und markieren Sie den Standort, zu dem dieses Subnetz gehört, in diesem Beispiel ist das *Bremen*.

Falls ein Subnetz schon eingerichtet wurde, können Sie es auch später einem Standort zuweisen:

- ▶ Klicken Sie mit der rechten Maustaste auf den Eintrag 10.20.0.0/16 und wählen Sie *Eigenschaften*.
- ▶ Auf dem Register *Allgemein* erhalten Sie über den Drop-down-Pfeil bei *Standort* Zugriff auf alle definierten Standorte. Hier können Sie *Regensburg* zuweisen.

Standort erstellen und Verknüpfung zuweisen

In Windows Server 2022 können Sie auch Subnetze auf IPv6-Basis erstellen. Nachdem Sie das Subnetz erstellt und die Erstellung mit *OK* bestätigt haben, wird es unterhalb des Konsoleneintrags *Subnets* angezeigt.

Wiederholen Sie diesen Vorgang für jedes Subnetz in Ihrem Unternehmen. Auch IP-Subnetze, in denen keine Domänencontroller installiert sind, in denen sich aber Rechner befinden, die sich bei dem Domänencontroller anmelden, sollten Sie an dieser Stelle anlegen und dem entsprechenden Standort zuweisen.

Wenn Sie den Eintrag *Subnets* in der Konsole anklicken, werden Ihnen auf der rechten Seite alle IP-Subnetze und die ihnen zugewiesenen Standorte angezeigt. Die Zuweisung des Subnetzes zu einem bestimmten Standort kann jederzeit über dessen Eigenschaften geändert werden. Sie können auch nachträglich Standorte erstellen und neue Subnetze vorhandenen Standorten zuweisen.

Standortverknüpfungen erstellen und verwalten

Eine Standortverknüpfung ist ein möglicher Weg für standortübergreifenden AD-Verkehr. Standortverknüpfungen machen nur dann Sinn, wenn alle Standorte in einer Standortverknüpfung vollständig geroutet sind.

- ▶ Klicken Sie mit rechts auf IP und wählen Sie *Neue Standortverknüpfung*.
- ▶ Vergeben Sie einen Anzeigenamen, z. B. *B-HB* ①, und definieren Sie, welche Standorte zu dieser Standortverknüpfung gehören ②.

Über die Schaltflächen *Hinzufügen/Entfernen* ③ können Sie weitere Standorte hinzufügen oder vorhandene entfernen.

Für alle Standorte innerhalb einer Standortverknüpfung legt der KCC die standortübergreifende Replikation automatisch fest. Sie haben dabei keinen Einfluss darauf, welcher Standort seine Aktualisierungen von welchem Standort erhält oder wohin er sie sendet. Sie können den Automatismus manuell beeinflussen, indem Sie nach dem Erstellen der Standortverknüpfungen deren Eigenschaften bearbeiten.

Falls Sie mit zahlreichen Standorten arbeiten und die Replikation zwischen zwei Standorten über verschiedene Standortverknüpfungen hinweg möglich ist, dann legen die Kosten den tatsächlichen Weg der Replikation fest.



Wenn zwischen zwei Standorten unterschiedliche Verbindungen (z. B. über eine Standleitung und eine Wahlverbindung) existieren, sind viele Administratoren versucht, auch unterschiedliche Standortverknüpfungen zu erstellen. Dies ist jedoch ein Fehler, da sich einer Standortverknüpfung keine physikalische Leitung oder Route zuordnen lässt. Erstellen Sie stattdessen nur eine Standortverknüpfung und lösen Sie die Priorisierung des Verkehrs über die Router-Metrik.

Im vorliegenden Beispiel kann eine weitere Standortverknüpfung *Bremen-Regensburg* erstellt und ihr als Kosten 500 zugewiesen werden. Solange die Kosten *Berlin-Bremen* (100) + *Berlin-Regensburg* (100) kleiner sind als bei *Bremen-Regensburg* (500), wird keine direkte Replikation zwischen Bremen und Regensburg stattfinden. Im Beispiel kostet der Weg zwischen Regensburg und Bremen über Berlin nur 200, wird also bevorzugt. Die Verbindung mit den höheren Kosten wird nur verwendet, wenn die günstigere Verbindung unterbrochen ist.

Sie können in den Einstellungen festlegen, wie häufig die standortübergreifende Replikation stattfindet. Der kleinste Wert, den Sie hier eintragen können, beträgt 15 Minuten.

Nach einem Klick auf *Zeitplan ändern* können Sie festlegen, zu welchen Zeiten Replikation stattfindet, z. B. nur zwischen 22:00 h und 06:00 h.

Vergessen Sie nicht, dass der *DefaultIPSiteLink* alle Ihre Standorte enthält und per Default mit dem Kostenfaktor 100 konfiguriert ist. In einem richtig konfigurierten Active Directory sollten keine Verbindungen über den *DefaultIPSiteLink* laufen. Damit Ihre Standortverknüpfungen wirksam werden, setzen Sie die Kosten für den *DefaultIPSiteLink* auf einen extrem hohen Wert, z. B. 99999.

Domänencontroller in Standorte verschieben

Nur durch das Ändern der IP-Konfiguration ändert ein Domänencontroller nicht seinen AD-Standort. Nachdem Sie IP-Subnetz, Standort und Standortverknüpfung erstellt haben, müssen Sie die jeweiligen DCs noch in die passenden Standorte verschieben.

- ▶ Klicken Sie mit rechts auf den entsprechenden DC und wählen Sie *Verschieben*.
- ▶ Markieren Sie den Zielstandort und klicken Sie auf *OK*.

Alternativ können Sie einen Server auch mit der Maus in den Ordner *Servers* eines anderen Standortes ziehen. Achten Sie vor dem Verschieben des Domänencontrollers darauf, dass die IP-Einstellungen des Servers zu den zugewiesenen IP-Subnetzen des neuen Standorts passen.

Die Replikationsverbindungen richtet Windows Server 2022 automatisch ein. Sie sehen diese im Snap-In Active Directory-Standorte und -Dienste über *Sites/<Standort>/<Servers>/<Servername>/NTDS Settings*. Sie können hier auch manuelle Verbindungen einrichten, indem Sie über das Kontextmenü *Neue Verbindung* für die Active Directory-Domänendienste auswählen.

Domänencontroller können Sie auch in der PowerShell an neue Standorte verschieben:

```
Get-ADDomainController <Name des Servers> | Move-ADDirectoryServer -Site  
<Name des Standorts>.
```

Sie können die Replikationsverbindungen auch in der PowerShell anzeigen. Dazu verwenden Sie den Befehl `Get-ADReplicationConnection`.



Achten Sie darauf, dass an jedem Standort mindestens ein globaler Katalogserver (GC) vorhanden ist. Sie können dies überprüfen, indem Sie im Kontextmenü der NTDS-Settings eines Servers auf *Eigenschaften* klicken. Im Register *Allgemein* können Sie die Option *Globaler Katalog* aktivieren.

Standortverknüpfungsbrücken

Bei den Standortverknüpfungsbrücken handelt es sich um eine Art Routing für die Replikationsdaten des AD. Standardmäßig ist eine solche Brücke zwischen allen Standortverknüpfungen vorhanden. Sie sorgt dafür, dass Standorte auch über mehrere Stationen (z. B. die Firmenzentrale) hinweg replizieren können. Die Brücke ermöglicht eine transitive Verbindung zwischen allen Standorten und sorgt so für eine zügigere Verbreitung der Änderungen als eine Replikation von Nachbar zu Nachbar. Erst eine Brücke zwischen allen Standortverknüpfungen ermöglicht den sinnvollen Einsatz von Standorten, Verknüpfungen und Kosten, über die Sie die Replikationswege beeinflussen können. Sie sollten diese Brücke nur in Ausnahmefällen deaktivieren.

Selbst definierte Standortverknüpfungsbrücken sind nur erforderlich, wenn Sie verhindern möchten, dass bestimmte Routen bei der Replikation verwendet werden.

Standardbrücke ausschalten

Falls Sie eigene Brücken zwischen den Standorten einrichten, greifen Sie tief in den Replikationsmechanismus des Active Directory ein. Solche selbst definierten Brücken können verhindern, dass die AD-Replikation tatsächlich die Wege benutzt, die Sie durch die Standortverknüpfungen vorgegeben haben, und eventuell vorhandene Direktverbindungen bleiben ungenutzt. Auch die zugewiesenen Kosten der Verbindungen werden nicht mehr berücksichtigt.

Falls eine besondere Konstellation den Einsatz selbst erstellter Brücken erforderlich macht, können Sie die standardmäßig vorhandene Brücke zwischen allen Standorten folgendermaßen deaktivieren:

- ▶ Klicken Sie mit der rechten Maustaste auf *Sites - Inter-Site Transports - IP* und wählen Sie *Eigenschaften*.
- ▶ Deaktivieren Sie das Kontrollfeld *Brücke zwischen allen Standortverknüpfungen herstellen*, um die Transitivität der Standortverknüpfungen auszuschalten.

Erweiterung des Beispiels

In der Nähe von Bremen wird eine Zweigstelle (Oldenburg) eingerichtet, die netztechnisch von Bremen versorgt wird, wo die meisten Ressourcen liegen. Nach der Definition des verwendeten Subnets für Oldenburg erfolgt die Standortkonfiguration. Hier lassen sich zwei Fälle unterscheiden:

- ✓ Oldenburg mit DC: Definieren Sie *Oldenburg* als eigenen Standort und erstellen Sie eine Standortverknüpfung *HB-OL*.
- ✓ Oldenburg ohne DC: Fügen Sie das definierte Subnetz für Oldenburg dem Standort *Bremen* hinzu.

Fehler in der Konfiguration von Standorten und Standortverknüpfungen können schwerwiegende Folgen haben. Schlimmstenfalls schließen Sie damit Standorte von der Replikation aus. Die folgenden Vorgaben helfen, typische Fehler zu vermeiden.

- ✓ Behalten Sie den Default-First-Site-Name bei und weisen Sie ihm kein Subnetz zu. Alles, was Active Directory nicht anderweitig zuordnen kann, ist dann automatisch Mitglied dieses Standorts.
- ✓ Verändern Sie den DefaultIPSiteLink nicht. Nutzen Sie ihn als Backup, denn jeder Standort wird automatisch Mitglied in dieser Standortverknüpfung.
- ✓ Setzen Sie die Kosten im DefaultIPSiteLink auf einen hohen Wert, z. B. 99999, damit Ihre erstellten Standortverknüpfungen wirksam werden.
- ✓ Jeder Standort ist Mitglied in mindestens einer Standortverknüpfung, zusätzlich zum DefaultIPSiteLink.
- ✓ Jede Standortverknüpfung enthält mindestens zwei Standorte.
- ✓ Alle Standorte in einer Standortverknüpfung sind vollständig geroutet.

11.4 Replikationstopologie erkunden

Verbindungsobjekte

Der KCC (siehe Kapitel 11.2) erstellt automatisch Verbindungsobjekte, die eingehende Replikationsverknüpfungen von anderen DCs symbolisieren.

Für den markierten Domänencontroller (hier *B-DC01*) sehen Sie, von welchem DC in welchem Standort Replikationen erhalten werden.

Active Directory-Replikation erzwingen

Wollen Sie eine sofortige Aktualisierung eines Domänencontrollers erzwingen, dann können Sie die Replikation in *Active Directory-Standorte und -Dienste* manuell auslösen.

- ▶ Markieren Sie die *NTDS Settings* des DCs, den Sie aktualisieren wollen.
- ▶ Klicken Sie mit der rechten Maustaste auf das entsprechende Verbindungsobjekt und wählen Sie den Befehl *Jetzt replizieren*.

Sie können den KCC auch veranlassen, die Replikationstopologie zu überprüfen. Das kann sinnvoll sein, wenn ein DC offline ist und Sie sofortige Aktualisierungen benötigen.

- ▶ Klicken Sie dazu mit der rechten Maustaste auf *NTDS Settings* und wählen Sie im Kontextmenü unter *Alle Aufgaben* den Befehl *Replikationstopologie überprüfen*.

Kommandozeilentool `repadmin.exe`

Mit `repadmin.exe` können Sie viele Aufgaben erledigen und erhalten viele Informationen, die *Active Directory-Standorte und -Dienste* nicht anzeigt. Dazu öffnen Sie eine Eingabeaufforderung (cmd).

`repadmin /showreps <FQDN>` zeigt Informationen zum Replikationsstatus für den angegebenen DC.

`repadmin /showconn <FQDN>` zeigt alle Verbindungsobjekte für den angegebenen DC.

`repadmin /syncall <DC>` synchronisiert den angegebenen DC mit allen seinen Replikationspartnern.

`repadmin /replicate <Ziel-DC> <Quell-DC> <Namenskontext>`

`repadmin /replicate HB-DC01 B-DC01 dc=firma,dc=intern` beispielsweise repliziert den Inhalt der Domänenpartition *firma.intern* vom DC *B-DC01* auf den DC *HB-DC01*.

Weitere Möglichkeiten können Sie sich mit `repadmin /?` anzeigen lassen.

Die häufigsten Fehlerursachen ausschließen

Bevor Sie mit Tools die Replikation genauer untersuchen, sollten Sie zunächst die gravierendsten und häufigsten Fehlerursachen ausschließen:

- ✓ Liegt auf dem Domänencontroller, der sich nicht mehr replizieren kann, ein generelles Problem vor, welches sich mit `Dcdiag` herausfinden lässt? Liegen also die Probleme überhaupt nicht in der Replikation, sondern hat der Domänencontroller eine Funktionsstörung?
- ✓ Wurde auf dem Domänencontroller eine Software installiert, welche die Replikation stören kann, wie Sicherheitssoftware, Virenschanner, Firewall oder sonstiges?
- ✓ Ist auf dem Domänencontroller, mit dem die Replikation nicht mehr stattfinden kann, die Hardware ausgefallen?
- ✓ Liegt unter Umständen nur ein Leitungs-, Router- oder Firewallproblem vor?
- ✓ Lässt sich der entsprechende Domänencontroller noch anpingen und lässt sich der DNS-Name des Servers auflösen?
- ✓ Gibt es generelle Probleme mit der Authentifizierung zwischen den Domänencontrollern, die durch *Zugriff verweigert*-Meldungen gemeldet werden?
- ✓ Sind die Replikationsintervalle zwischen Standorten so kurz eingestellt, dass die vorherige Replikation noch nicht abgeschlossen ist und die nächste bereits beginnt?
- ✓ Wurden Änderungen an der Routingtopologie vorgenommen, die eine Replikation verhindern können?

12 Active Directory-Konten verwalten

12.1 Überblick zu Konten

Verschiedene Arten von Konten

Eine Active Directory-Domäne dient u. a. der zentralen Verwaltung von Konten. Über ihr Konto authentifizieren sich **Benutzer** und **Computer** gegenüber der Domäne. Auch die Zuweisung von Rechten oder die Überwachung von Zugriffen erfolgt über Konten. Zur Vereinfachung dieser Aufgabe werden **Gruppen** gebildet, die Benutzer- und Computerkonten zusammenfassen. **Organisationseinheiten** dienen schließlich der strukturierten Speicherung der Konten. Sie sind vergleichbar mit Ordnern im Dateisystem.

Sicherheitskennung

Systemintern wird jedes Konto durch eine eindeutige Sicherheitskennung (Security Identifier, SID) repräsentiert. Sie besteht aus einem konstanten Domänenbestandteil und einer relativen Kennung (RID). Gelöschte SIDs werden niemals wieder verwendet. Löschen Sie beispielsweise ein Benutzerkonto und erstellen anschließend ein neues, dem Sie identische Eigenschaften zuordnen, wird dieses Objekt mit einer anderen SID gespeichert. Für Active Directory handelt es sich um ein anderes Benutzerobjekt. Das kann z. B. unerwünschte Folgen bei Berechtigungen nach sich ziehen.

Verwaltungstools

Zu Verwaltung der Konten stehen verschiedene Tools zur Verfügung:

- ✓ **Active Directory-Benutzer und -Computer (*dsa.msc*)**: Dieses MMC-Snap-In integriert sich auf Domänencontrollern im Server-Manager unter Rollen.
- ✓ **Active Directory-Verwaltungszentrum (AD Administrative Center, *dsac.exe*)**: Diese Anwendung bietet eine andere Ansicht auf einzelne Konten und ermöglicht schnelleren Zugriff auf viele wichtige Einstellungen.
- ✓ **Kommandozeilentools**: Die sogenannten DS-Befehle ermöglichen die Kontenverwaltung über eine Eingabeaufforderung. Geben Sie für eine Auflistung der anderen DS-Befehle z. B. `dsadd /?` ein. Neben den DS-Befehlen gibt es noch zahlreiche andere Tools. *Csvde.exe* ist z. B. hervorragend geeignet, um Inhalte aus dem AD zu exportieren.
- ✓ **PowerShell**: Mit Windows Server 2022 wird die PowerShell mit Modulen zur Active Directory-Verwaltung ausgeliefert.
- ✓ **Weitere Tools**: mit *LDP.exe* und *AdsiEdit.msc* können Sie sehr tief ins Active Directory eingreifen. Für die Kontenverwaltung sollten Sie auf andere Tools zurückgreifen.

Auf Mitgliedsservern und Clients sind einige dieser Tools standardmäßig nicht vorhanden. Installieren Sie dort die Remoteserver-Verwaltungstools (Remote Server Administration Tools, **RSAT**), damit Sie die Befehle auch von dort aus aufrufen bzw. einer MMC (Microsoft Management Console) hinzufügen können. Beachten Sie, dass für die Remoteverwaltung eines Servers 2022 als Client-Betriebssystem mindestens Windows 10.

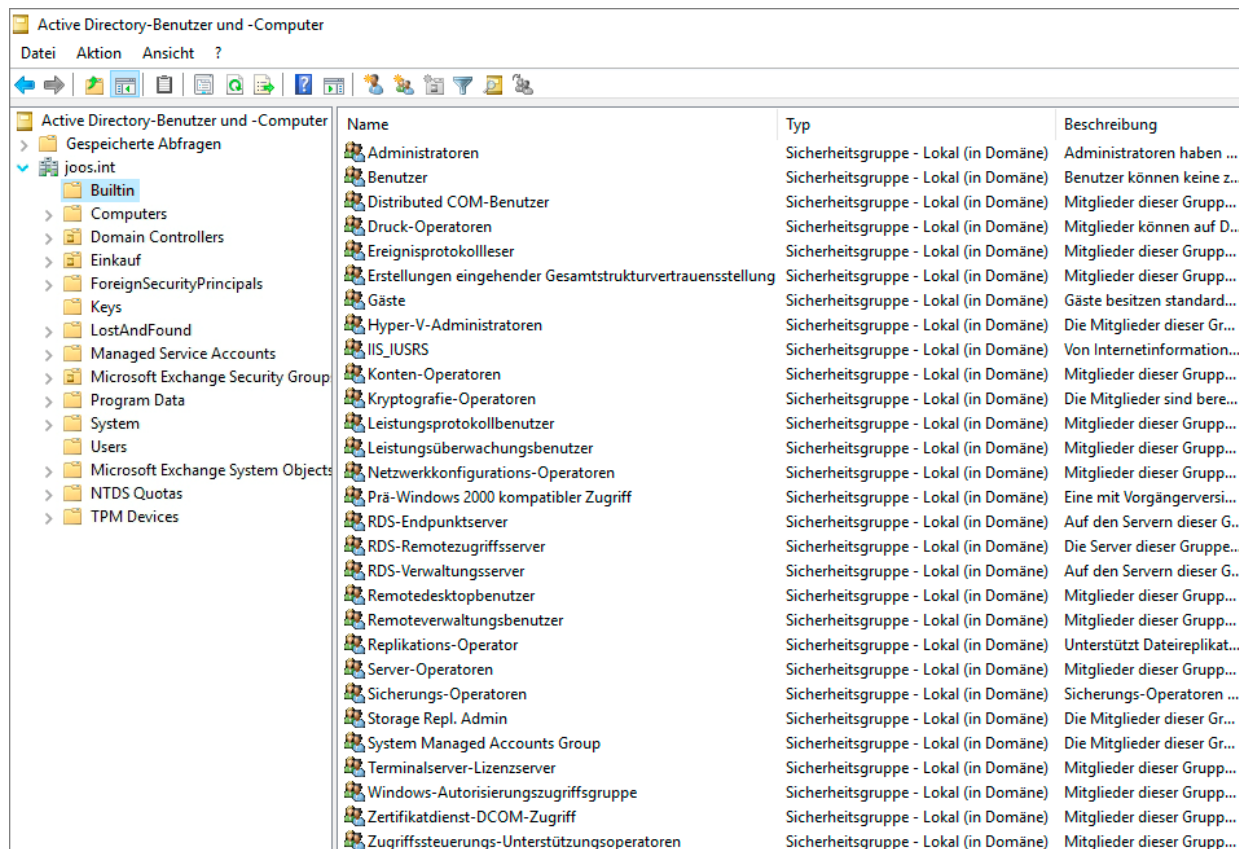
Die folgenden Beschreibungen verwenden das Snap-In *Active Directory-Benutzer und -Computer*. Dieses Tool ist auch für ältere Betriebssysteme verfügbar und arbeitet dort weitestgehend identisch.

12.2 Container der Domäne erkunden

Überblick

Die folgende Abbildung zeigt die Container und OUs einer frisch aufgesetzten Domäne in der erweiterten Ansicht, die Sie unter *Ansicht - Erweiterte Features* aktivieren sollten. Nur so können Sie alle verfügbaren Funktionen nutzen und sämtliche AD-Einträge einsehen.

Bei der Arbeit mit diesem Snap-In ist es sehr wichtig, den Unterschied zwischen einem Container (leeres Ordnersymbol 📁) und einer Organisationseinheit (Ordnersymbol mit Inhalt 📁) zu kennen.



Name	Typ	Beschreibung
Administratoren	Sicherheitsgruppe - Lokal (in Domäne)	Administratoren haben ...
Benutzer	Sicherheitsgruppe - Lokal (in Domäne)	Benutzer können keine z...
Distributed COM-Benutzer	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder dieser Grupp...
Druck-Operatoren	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder können auf D...
Ereignisprotokollleser	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder dieser Grupp...
Erstellungen eingehender Gesamtstrukturvertrauensstellung	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder dieser Grupp...
Gäste	Sicherheitsgruppe - Lokal (in Domäne)	Gäste besitzen standard...
Hyper-V-Administratoren	Sicherheitsgruppe - Lokal (in Domäne)	Die Mitglieder dieser Gr...
IIS_IUSRS	Sicherheitsgruppe - Lokal (in Domäne)	Von Internetinformation...
Konten-Operatoren	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder dieser Grupp...
Kryptografie-Operatoren	Sicherheitsgruppe - Lokal (in Domäne)	Die Mitglieder sind bere...
Leistungsprotokollbenutzer	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder dieser Grupp...
Leistungsüberwachungsbenutzer	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder dieser Grupp...
Netzwerkkonfigurations-Operatoren	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder dieser Grupp...
Prä-Windows 2000 kompatibler Zugriff	Sicherheitsgruppe - Lokal (in Domäne)	Eine mit Vorgängerversi...
RDS-Endpunktserver	Sicherheitsgruppe - Lokal (in Domäne)	Auf den Servern dieser G...
RDS-Remotezugriffsserver	Sicherheitsgruppe - Lokal (in Domäne)	Die Server dieser Gruppe...
RDS-Verwaltungsserver	Sicherheitsgruppe - Lokal (in Domäne)	Auf den Servern dieser G...
Remotedesktopbenutzer	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder dieser Grupp...
Remoteverwaltungsbenutzer	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder dieser Grupp...
Replikations-Operator	Sicherheitsgruppe - Lokal (in Domäne)	Unterstützt Dateireplikat...
Server-Operatoren	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder dieser Grupp...
Sicherungs-Operatoren	Sicherheitsgruppe - Lokal (in Domäne)	Sicherungs-Operatoren ...
Storage Repl. Admin	Sicherheitsgruppe - Lokal (in Domäne)	Die Mitglieder dieser Gr...
System Managed Accounts Group	Sicherheitsgruppe - Lokal (in Domäne)	Die Mitglieder dieser Gr...
Terminalserver-Lizenzserver	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder dieser Grupp...
Windows-Autorisierungszugriffsgruppe	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder dieser Grupp...
Zertifikatdienst-DCOM-Zugriff	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder dieser Grupp...
Zugriffssteuerungs-Unterstützungsoperatoren	Sicherheitsgruppe - Lokal (in Domäne)	Mitglieder dieser Grupp...

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.
- ✓ **Selbst erstellte OUs:** An dieser Stelle erscheinen alle Organisationseinheiten, die innerhalb der Domäne erstellt wurden. Sie bilden die logische Struktur des Active Directory.
- ✓ **ForeignSecurityPrincipals:** Container für SIDs vertrauter Domänen einer anderen Gesamtstruktur.
- ✓ **Keys:** In dieser OU werden Daten gespeichert, die für die Verwendung von gruppierten verwalteten Dienstkonten in Active Directory benutzt werden.

- ✓ **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 Container nur benötigt, wenn unsauber gearbeitet wurde.
- ✓ **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 für Windows 7 und 8 einfacher verwaltet werden.
- ✓ **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 erstellt werden, ohne Angabe der Ziel-OU werden 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:** mit Windows Server 2012 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-Verwaltungszentrum* ist dieser Schritt nicht notwendig.

12.3 Organisationseinheiten erstellen und verwalten

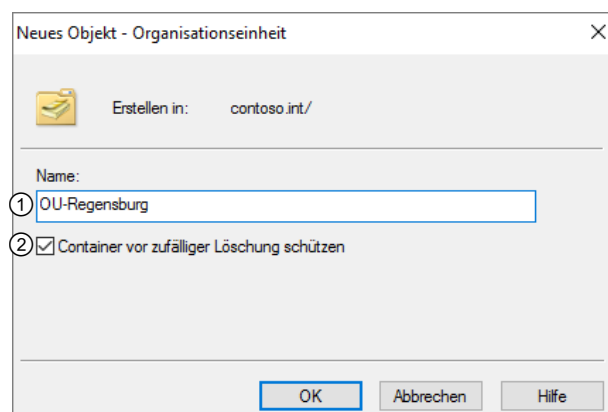
Organisationseinheit erstellen

Sie sollten die Standard-Container der Domäne nicht zum Speichern von Objekten nutzen. Erstellen Sie eine Ihren Bedürfnissen entsprechende OU-Struktur und legen Sie die Konten in der passenden Organisationseinheit ab.

Im vorhergehenden Kapitel wurden die Standorte Berlin, Regensburg und Bremen erstellt. In den meisten Fällen macht es Sinn, diese Standorte auch durch OUs abzubilden.

- ▶ Klicken Sie mit der rechten Maustaste auf den Ort, wo die OU erstellt werden soll (Domäne oder vorhandene OU), und wählen Sie im Kontextmenü den Befehl *Neu - Organisationseinheit*.
- oder
- ▶ Wählen Sie mit der linken Maustaste den Ort, wo die OU erstellt werden soll (Domäne oder vorhandene OU), und klicken Sie in der Menüleiste auf .
 - ▶ Geben Sie den Namen für die Organisationseinheit ① ein.
 - ▶ Deaktivieren Sie bei Bedarf die Option ② und klicken Sie auf *OK*.

Falls die Option *Container vor zufälliger Löschung schützen* ② aktiviert ist, können Sie die OU weder löschen noch verschieben. Während der Planung und Erstellung der AD-Struktur kann dies unerwünscht sein. Um die Option später zu ändern, müssen *Erweiterte Features* der Ansicht eingeschaltet sein, sonst fehlt das Register *Objekt* in den Eigenschaften der OU, auf dem Sie die Option aktivieren oder deaktivieren können.



Objektverwaltung delegieren

Um die Administratoren einer Domäne zu entlasten, können Aufgaben wie z. B. die Kontenverwaltung delegiert werden. Sie können dafür die Gruppe *Konten-Operatoren* im Container *Builtin* nutzen, geben damit aber einem Mitglied sehr weit gehende Rechte. Außer den Administratoren und anderen Operatoren-Gruppen kann ein Konten-Operator alle Konten der Domäne verwalten. Oft ist es wünschenswert, Benutzern die Kontenverwaltung nur für den Inhalt einer OU zu ermöglichen. Dazu delegieren Sie die Verwaltung am besten an eine speziell dafür erstellte Gruppe. Auf diese Weise können Sie einfacher festlegen, an welche Benutzerkonten die Verwaltung delegiert wird.

- ▶ Klicken Sie mit rechts auf die OU (oder Domäne), deren Verwaltung Sie delegieren wollen, und wählen Sie im Kontextmenü *Objektverwaltung zuweisen*.
- ▶ Der Assistent zum Zuweisen der Objektverwaltung heißt Sie willkommen. Klicken Sie auf *Weiter*.
- ▶ Klicken Sie auf *Hinzufügen* und wählen Sie Benutzer oder Gruppen für die Objektverwaltung aus.
- ▶ Klicken Sie auf *Weiter*.

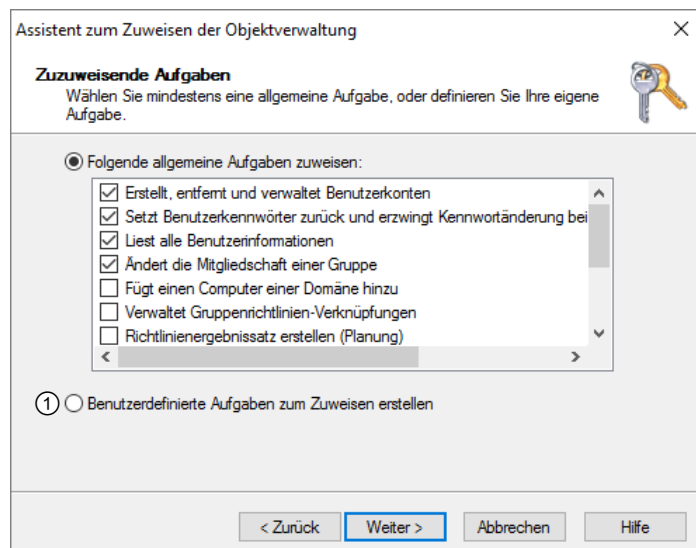
Das Hinzufügen von Benutzern und Gruppen zu **Listen** erfolgt stets auf dieselbe Weise und wird im weiteren Verlauf dieses Buches immer wieder nötig sein. Im Abschnitt 12.4 wird der Vorgang ausführlich beschrieben.

- ▶ Wählen Sie die Aufgaben aus, die Sie delegieren wollen.

In der Abbildung sehen Sie alle Optionen, die benötigt werden, um Benutzer und Gruppen im Delegationsbereich zu verwalten.

- ▶ Aktivieren Sie bei Bedarf die Option ①, um detaillierte Einstellungen vorzunehmen. Die weiteren Schritte des Assistenten hängen von den gewählten Optionen ab.
- ▶ Klicken Sie auf *Weiter*.
- ▶ Überprüfen Sie auf der letzten Seite des Assistenten die Delegierungseinstellungen und klicken Sie auf *Fertig stellen*.

Ein Benutzer, dem die abgebildeten Aufgaben delegiert wurden, kann auch Benutzerkonten aus nicht delegierten OUs zu einer Gruppe dieser OU hinzufügen oder daraus entfernen.

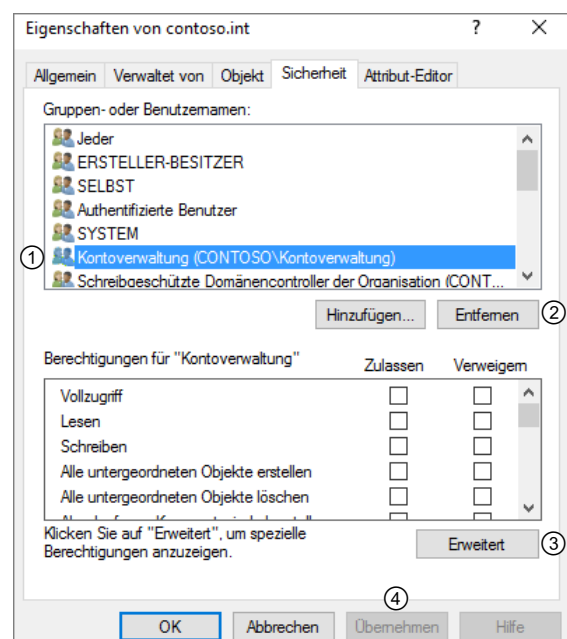


Delegierung entfernen

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-Berlin*.
- ▶ Wechseln Sie auf das Register *Sicherheit* und markieren Sie dort die delegierten Konten ①.
- ▶ Um zu überprüfen, welche Delegierung für diesen Eintrag gilt, klicken Sie auf *Erweitert* ③.

Mit einem Doppelklick auf einen Berechtigungseintrag können Sie sich im folgenden Dialog alle Berechtigungen anzeigen lassen und diese anpassen.



- ▶ Um eine Gruppe zu entfernen, klicken Sie auf *Entfernen* ② und dann auf *Übernehmen* ④.
- ▶ Klicken Sie auf *OK*.

Wenn Sie unsicher sind, welche Einträge Sie entfernen sollten, können Sie die Einstellungen über eine Eingabeaufforderung auf die Standardwerte zurücksetzen. Damit stellen Sie sicher, dass alle wichtigen Einträge wieder vorhanden sind. Anschließend können Sie dann die Delegation neu setzen.

- ▶ Geben Sie in einer Eingabeaufforderung den folgenden Befehl ein:

```
dsacl "ou=OU-Berlin,dc=firma,dc=intern" /ResetDefaultDACL
```

Die Angaben zwischen den Anführungszeichen passen Sie entsprechend an Ihre Domänenstrukturen an. Die Anführungszeichen sind nur zwingend erforderlich, wenn eines der Elemente Leerzeichen enthält. Von der Verwendung von Leerzeichen ist allerdings grundsätzlich abzuraten. Sie sollten sich dennoch angewöhnen, stets Anführungszeichen zu verwenden.

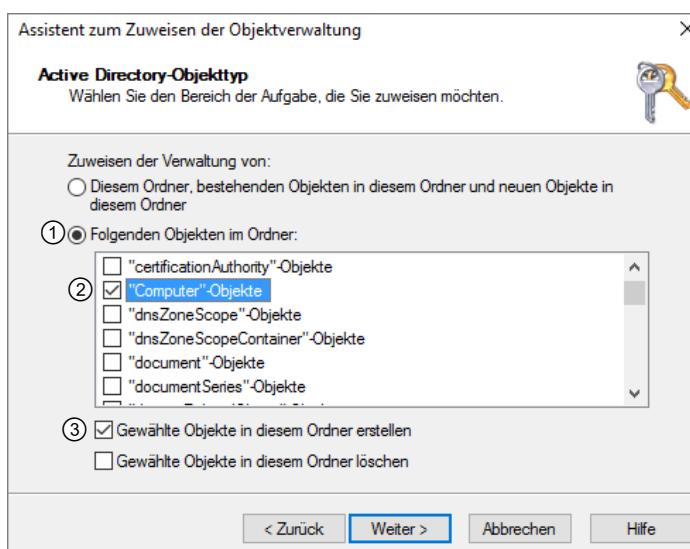
In diesem Beispiel wurde in der Domäne *firma.intern* die Verwaltung von *OU-Berlin* an die lokale Gruppe *LG-B-Kontenverwaltung* delegiert. Die lokale Gruppe enthält wiederum die globale Gruppe *GG-B-Abteilungsleiter*, die alle Abteilungsleiter am Standort Berlin umfasst.

Das Schema beim Aufbau von Berechtigungsstrukturen ist stets dasselbe: Erstellen Sie eine lokale Gruppe mit der Bezeichnung *LG-<Standortkürzel>-<optional: weitere OU>-<Aufgabenbeschreibung>* (z. B. *LG-B-Kontenverwaltung*) und eine globale Gruppe *GG-<Standortkürzel>-<optional: weitere OU>-<Gruppen- oder Funktionsbeschreibung>* (z. B. *GG-B-Abteilungsleiter* oder *GG-B-Verwaltung-Sachbearbeiter*). Fügen Sie anschließend die globale Gruppe (GG) der lokalen Gruppe (LG) hinzu. Auf diese Weise haben Sie die Aufgabe von der Gruppenmitgliedschaft getrennt und können jederzeit erkennen, welche Aufgaben eine Gruppe oder einzelne Benutzer erhalten haben. Die Verwaltung des Active Directory und spätere Änderungen werden dadurch enorm erleichtert. Weitere Informationen finden Sie im Abschnitt 12.7.

Delegation der Erstellung von Computerkonten

Das Erstellen von Computerkonten innerhalb bestimmter OUs ist nicht in den allgemeinen Aufgaben enthalten, Sie können dies jedoch über die benutzerdefinierten Aufgaben einrichten.

- ▶ Klicken Sie mit der rechten Maustaste auf ein Objekt (z. B. eine OU) und wählen Sie *Objektverwaltung zuweisen*.
- ▶ Wählen Sie im Assistenten auf der Seite *Zuzuweisende Aufgabe* die Option *Benutzerdefinierte Aufgaben zum Zuweisen erstellen* und klicken Sie auf *Weiter*.
- ▶ Wählen Sie auf der Seite *Active Directory-Objekttyp* die Option *Folgenden Objekten im Ordner* ①.
- ▶ Aktivieren Sie den Eintrag „*Computer*“-Objekte ②. Aktivieren Sie optional weitere Einträge.
- ▶ Aktivieren Sie für alle aktivierten Einträge die Option *Gewählte Objekte in diesem Ordner erstellen* ③ und klicken Sie auf *Weiter*.

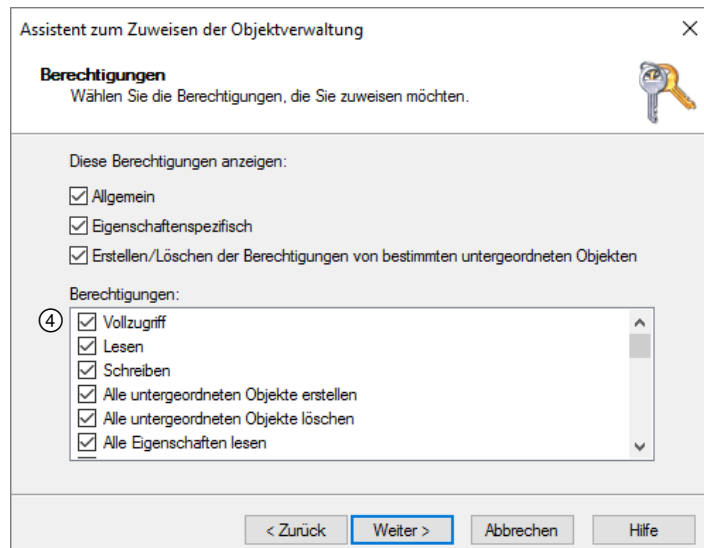


- ▶ Aktivieren Sie im Listenfeld den Eintrag *Vollzugriff* ④, um alle Attribute der Computer-Objekte in dieser OU verwalten zu können.

Daraufhin werden alle Optionsfelder aktiviert. Für die Verwaltung anderer Objekttypen kann es sinnvoll sein, die Berechtigungen feiner einzustellen.

- ▶ Klicken Sie auf *Weiter* und auf der letzten Seite des Assistenten auf *Fertig stellen*.

Nach Abschluss des Vorgangs sind die Mitglieder der ausgewählten Gruppe in der Lage, in dieser OU neue Computer zu erstellen.



12.4 Listen erstellen

Konten angeben, suchen und auswählen

Sie müssen an zahlreichen Stellen Konten zu Listen hinzufügen, z. B. bei der Delegierung von Verwaltungsaufgaben, der Verrechterung von Ressourcen oder der Verwaltung von Gruppenmitgliedschaften. Das Vorgehen ist immer dasselbe:

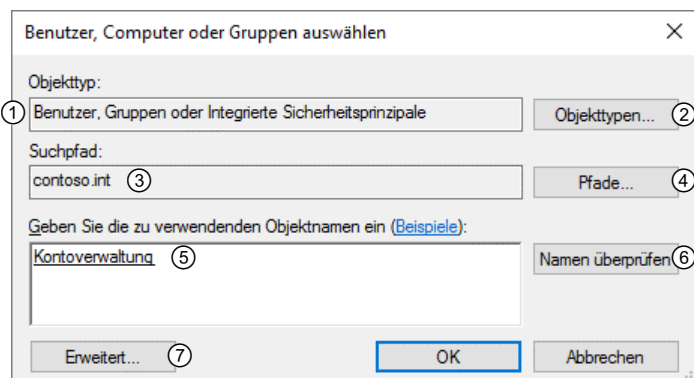
- ▶ Klicken Sie auf die Schaltfläche *Hinzufügen*.

Es öffnet sich der Dialog *Benutzer, Computer oder Gruppen auswählen*.

Die Auflistung ① zeigt an, welche Objekttypen Sie gerade auswählen können. In der Abbildung fehlen z. B. Computerkonten. Nach einem Klick auf *Objekttypen* ② können Sie die Auswahl ändern.

Der Suchpfad ③ gibt an, wo nach den Konten gesucht wird. Unter *Pfade* ④ können Sie eine andere vertraute Domäne, eine OU oder einen einzelnen Computer auswählen.

Im Feld ⑤ können Sie Objektnamen bzw. Teile von Namen direkt eingeben. Mehrere Bezeichnungen werden durch Strichpunkte (Semikolons) voneinander getrennt. Mit *Namen überprüfen* ⑥ können Sie Ihre Eingabe überprüfen und vervollständigen.



Objektsuche

Bei Fehlern erfolgen Hinweise bzw. Nachfragen, was Sie als eingeschränkte Suchfunktion missbrauchen können. Danach werden die Konten mit ihrem UPN (User Principal Name, Benutzername im Format Vorname - Nachname (E-Mail-Format)) dargestellt.

Über *Erweitert* ⑦ kommen Sie zum erweiterten Suchdialog. Der obere Bereich der erweiterten Suche mit Objekttyp und Suchpfad entspricht dem vorherigen Dialog.

Unter ① können Sie wählen, ob der gesuchte Name genau dem Suchbegriff entspricht oder mit dem Suchbegriff beginnt.

- ▶ Geben Sie im Suchfeld ② einen Suchbegriff ein und klicken Sie auf *Jetzt suchen* ③.

Wenn Sie im Suchfeld nichts eingeben und auf *Jetzt suchen* klicken, werden alle gewählten Objekttypen im angegebenen Suchpfad aufgelistet.

Unter *Spalten* ④ können Sie auswählen, welche Daten Sie durchsuchen möchten. Sie können nach zahlreichen Kriterien suchen, wie z. B. nach Telefonnummern, Büros, Initialen, Regionen und Ländern.

Die Auswahl der Objekttypen verändert auch die Anzahl der verfügbaren Spalten. Wenn Sie nach Benutzern suchen, stehen alle Spalten zur Verfügung.

- ▶ Markieren Sie in den Suchergebnissen das gesuchte Konto und klicken Sie auf *OK*.
- ▶ Klicken Sie erneut auf *OK*.

Benutzer, Computer oder Gruppen auswählen

Objekttyp: Benutzer, Gruppen oder Integrierte Sicherheitsprinzipale

Suchpfad: contoso.int

Allgemeine Abfragen

Name: ① ②

Beschreibung:

☐ Deaktivierte Konten

☐ Nicht-ablaufende Kennwörter

Tage seit der letzten Anmeldung:

④ Spalten...

③ Jetzt suchen

Beenden

Suchergebnisse:

Name	E-Mail-Adresse	Beschreibung	Ordner
Administrator		Vordefiniertes K...	contoso.int/Users
Administratoren			contoso.int/Builtin

OK Abbrechen

Erweiterte Objektsuche

Die häufigsten Probleme beim Hinzufügen von Konten werden durch eine falsche Auswahl der Objekttypen oder Spalten verursacht. So müssen Sie z. B. die Spalte *Nachname* hinzufügen, um Personen auch anhand ihres Nachnamens zu finden (standardmäßig wird nur nach vollen Namen gesucht, die stets mit dem Vornamen beginnen). Vergewissern Sie sich ebenfalls, dass Sie in der richtigen Domäne suchen.

12.5 Benutzerkonten erstellen und verwalten

Benutzerkonto erstellen

Vor dem Erstellen von Benutzerkonten sollten Sie eine Namenskonvention zur Benennung der Benutzeranmeldenamen festlegen, denn diese müssen eindeutig sein. Meist werden hierzu der Vor- und der Nachname benutzt, z. B. *LSchmid* für Lisa Schmid. Dieses Abkürzen des Vornamens hat den Vorteil, dass eine zweite Lisa Schmid in der Domäne als *LiSchmid* bezeichnet werden kann. Wenn Sie E-Mail bereitstellen, beziehen Sie die Postfachbezeichnungen in Ihre Planung ein. Ihre Benutzer werden es schätzen, wenn der Benutzeranmeldename der E-Mail-Adresse entspricht.

- ▶ Klicken Sie mit der rechten Maustaste auf die OU, in der das Konto erstellt werden soll, und wählen Sie im Kontextmenü *Neu - Benutzer*.
- ▶ Geben Sie den Vornamen ① und den Nachnamen ② ein.

Der vollständige Name ③ muss innerhalb der OU eindeutig sein. Er wird automatisch aus Vorname, Initialen und Nachname zusammengesetzt.

Sie können die Initialen auch verwenden, um bei doppelt auftretenden Namen für Eindeutigkeit zu sorgen.

Der Benutzeranmeldename ④ muss in der Gesamtstruktur eindeutig sein. Der Prä-Windows-2000-Name ⑤ wird automatisch auf denselben Wert gesetzt wie ④.

Wie Sie zusätzliche UPN-Suffixe ⑥ erstellen können, wird später erklärt.

- ▶ Klicken Sie auf *Weiter*.
- ▶ Geben Sie das Kennwort zweimal ein (① und ②). Standardmäßig müssen Sie komplexe Kennwörter wählen.

Voreingestellt ist, dass der Benutzer sein Kennwort bei der nächsten Anmeldung ändern muss ③. Bei Dienst-Konten muss diese Option deaktiviert werden.

Sie können Benutzer an der Änderung ihres Kennworts hindern ④. Das geht jedoch nicht zusammen mit ③.

Wie oft ein Benutzer sein Kennwort ändern muss, wird in einer Kennwortrichtlinie oder einem Password Settings Object (PSO) festgelegt. Mit *Kennwort läuft nie ab* ⑤ können Sie die Richtlinie überschreiben. Diese Option sollte für Dienste-Konten verwendet werden.

Mit *Konto ist deaktiviert* ⑥ können Sie dafür sorgen, dass das Konto nicht benutzt werden kann. Das ist sinnvoll, wenn Sie Vorlagen-Konten erstellen, die Sie später kopieren.

- ▶ Klicken Sie auf *Weiter* und Sie erhalten eine Zusammenfassung. Dort können Sie das Konto fertigstellen.

Das erstellte Konto ist bereits Mitglied in der Gruppe Domänen-Benutzer und kann sich damit an der Domäne anmelden und auf Rechnern arbeiten.

Benutzereigenschaften bearbeiten

Einige Einstellungen können Sie direkt über einen Rechtsklick auf das Benutzerkonto vornehmen, das Kennwort können Sie nur auf diese Art zurücksetzen. Alle anderen Einstellungen erreichen Sie unter den Eigenschaften oder über einen Doppelklick auf das Objekt. Die erweiterte Ansicht sollte dazu aktiviert sein.

Auf dem Register *Konto* können Sie die Anmeldezeiten ① festlegen, zu denen sich der Benutzer an der Domäne anmelden kann.

Mit *Anmelden an* ② können Sie die Benutzeranmeldung auf vorgegebene Rechner beschränken.

In *Kennwortrichtlinien* können Sie definieren, wie oft ein Benutzer sein Kennwort falsch eingeben darf, bevor das Konto gesperrt wird. Mit ③ können Sie eine bestehende Sperrung wieder aufheben.

Soll ein Konto an einem bestimmten Datum deaktiviert werden, können Sie das unter *Konto läuft ab* ④ einstellen. Das ist z. B. beim Einsatz von Zeitarbeitern oder Praktikanten sinnvoll.

Seine Zugriffsrechte sollte ein Benutzer über die Mitgliedschaft in entsprechenden Gruppen erhalten. Im Register *Mitglied von* ⑤ können Sie die Gruppenmitgliedschaften verwalten.

Im Register *Attribut-Editor* ⑥ können Sie auf alle Eigenschaften eines Objekts zugreifen, z. B. *lastLogon* oder *logonCount*. Manche Eigenschaften können Sie jedoch nur einsehen, da die Bearbeitung dem System vorbehalten ist.

In den Registern *Allgemein*, *Adresse*, *Rufnummern* und *Organisation* können Sie viele Informationen eingeben, nach denen Ihre Benutzer das AD durchsuchen können.

Wenn Sie möglichst viele Informationen ins AD einpflegen wollen, ist die Erstellung eines Benutzerkontos mit einigem Aufwand verbunden. Da viele Informationen bei vielen Benutzerkonten gleich sind, gibt es einige Möglichkeiten, sich die Arbeit zu erleichtern:

- ✓ Markieren Sie mehrere Benutzerkonten. Über einen Rechtsklick können Sie viele Eigenschaften gleichzeitig verändern.
- ✓ Erstellen Sie ein (deaktiviertes) Vorlagen-Konto und füllen Sie es vollständig aus. Über einen Rechtsklick können Sie das Konto kopieren und es werden viele Eigenschaften übernommen. Welche das sind, lässt sich im Schema festlegen.

UPN-Suffixe erstellen

Für AD-Domänen werden oft Namen gewählt, die im öffentlichen DNS nicht erreichbar sind. E-Mails können aber nur an öffentliche DNS-Domains verschickt werden. UPN-Suffixe ermöglichen es, dass sich ein Benutzer scheinbar an einer anderen Domäne anmeldet. Damit wird es möglich, Benutzern die Anmeldung an ihrer E-Mail-Domäne zu ermöglichen.

Ein anderes Einsatzgebiet sind Gesamtstrukturen mit mehreren Domänen, wo sich jeder Benutzer scheinbar an derselben Domäne anmelden soll.

Zur Erstellung von UPN-Suffixen müssen Sie Mitglied der Gruppe Organisations-Admins sein und Sie benötigen das MMC-Snap-In *Active Directory-Domänen und -Vertrauensstellungen* (domain.msc).

- ▶ Klicken Sie mit der rechten Maustaste direkt auf das Snap-In und wählen Sie im Kontextmenü *Eigenschaften*.
- ▶ Geben Sie die gewünschten Suffixe ein.

Diese Suffixe gelten für alle Domänen der Gesamtstruktur. Bei der Erstellung oder Verwaltung von Benutzerkonten stehen sie als zusätzliche Auswahl zur Verfügung. Bedenken Sie, dass das Suffix zum Benutzeranmeldenamen gehört und Benutzeranmeldenamen in einer Gesamtstruktur eindeutig sein müssen.

12.6 Computerkonten erstellen

Computerkonto erstellen

Standardmäßig kann jeder Benutzer zehn Computer zur Domäne hinzufügen. Dabei wird automatisch im Container *Computers* ein Computerkonto erstellt. Soll ein Benutzer mehr als diese zehn Computer zur Domäne hinzufügen, dann benötigt er entweder die Rechte eines Domänen-Admins oder ihm muss die entsprechende Objektverwaltung delegiert worden sein. Eine dritte Möglichkeit besteht darin, ein Computerkonto vorab zu erstellen. Das hat den Vorteil, dass sich das Computerkonto bereits in der richtigen OU befindet und nicht im Container *Computers* landet. Da durch den Speicherort eines Objektes auch die Gruppenrichtlinien bestimmt werden, die auf das Objekt wirken, sollten Sie letzteren Weg bevorzugen. Andernfalls sind Computerkonten bei der Erstellung bis auf die domänenweite Einstellungen unkonfiguriert.

- ▶ Klicken Sie mit der rechten Maustaste auf die gewünschte Organisationseinheit und wählen Sie den Kontextbefehl *Neu - Computer*.
- ▶ Geben Sie einen Namen ① für den Computer ein. Berücksichtigen Sie dabei die Konventionen für DNS-Namen. Windows bildet automatisch den Prä-Windows-2000-Namen (der auch als NetBIOS-Name genutzt wird) ②.
- ▶ Legen Sie über ③ fest, wer diesen Computer zur Domäne hinzufügen kann.
- ▶ Legen Sie fest, ob es sich bei dem Computer um eine NT-Workstation handelt ④.

12.7 Gruppenkonten

Gruppentypen

Es gibt zwei verschiedene Gruppentypen. **Sicherheitsgruppen** steuern den Zugriff auf Ressourcen, indem ihnen Berechtigungen zuweist. **Verteilerguppen** erhalten beim Anlegen eine E-Mail-Adresse und werden mit dieser im Adressbuch angezeigt. Benutzer können Sie wie einzelne Empfänger auswählen.

Gruppenbereiche

Es gibt drei verschiedene Gruppenbereiche: **lokal (in Domäne)**, **global** und **universal**. Die erstgenannte wird auch als domänenlokale oder nur als lokale Gruppe bezeichnet. Verwechseln Sie diese Gruppen nicht mit den rechnerlokalen Gruppen, die es auf allen Nicht-Domänencontrollern gibt. Universale Gruppen werden Sie nur benötigen, wenn Sie mit mehreren Domänen arbeiten.

Die Gruppenbereiche unterscheiden sich durch die folgenden Punkte:

- ✓ Wer kann Mitglied dieser Gruppe sein?
- ✓ Wo kann diese Gruppe verwendet/zugewiesen werden?

Gruppenbereich	Mitgliedschaft	Verwendbarkeit
Lokal (in Domäne)	Benutzer- und Computerkonten beliebiger Domänen, globale und universelle Gruppen beliebiger Domänen, lokale Gruppen derselben Domäne	nur in derselben Domäne
Global	Benutzer- und Computerkonten derselben Domänen, globale Gruppen derselben Domäne	in beliebigen Domänen
Universal	Benutzer- und Computerkonten beliebiger Domänen, globale und universelle Gruppen beliebiger Domänen	in beliebigen Domänen

Hinweise zum Gruppenbereich *Universal*

- ✓ Universale Gruppen vergrößern den globalen Katalog, weil Mitgliedschaften im Katalog gespeichert werden und entsprechend domänenübergreifend repliziert werden müssen.
- ✓ Das Ändern von Mitgliedschaften in universalen Gruppen verursacht Netzwerkverkehr, weil mit der Änderung der globale Katalog repliziert wird.
- ✓ Das Zugriffstoken (enthält alle Daten über den Benutzer und seine Berechtigungen) ist bei universalen Gruppen größer als bei globalen oder lokalen Gruppen.
- ✓ Sie können Domänencontroller für einen Standort anweisen, die Mitgliedschaft in universalen Gruppen zwischenspeichern, 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.

Machen Sie ausschließlich globale (oder universale) Gruppen zu Mitgliedern einer universalen Gruppe, nicht einzelne Benutzer oder Computer.

Beispiel für den Einsatz universaler Gruppen

Sie arbeiten mit mehreren Domänen und in jeder Domäne gibt es Buchhalter. Alle Buchhalter benötigen Zugriff auf die Buchhaltungs-Server. Hier ist die Verwendung einer universalen Gruppe sinnvoll:

- ✓ Erstellen Sie in jeder Domäne eine globale Gruppe (z. B. GG-Buchhalter) und fügen Sie die Benutzerkonten aller Buchhalter zur globalen Gruppe hinzu. Auf diese Art verwaltet jede Domäne ihre eigenen Buchhalter.
- ✓ Erstellen Sie eine universale Gruppe (z. B. UG-Buchhalter), die alle globalen Buchhalter-Gruppen beinhaltet.
- ✓ Zur Verrechnung der Buchhaltungs-Server benutzen Sie dann die universale Gruppe entsprechend den unten folgenden Angaben.

Gruppenkonto erstellen

- ▶ Klicken Sie mit der rechten Maustaste auf die OU, in der Sie die Gruppe erstellen wollen, und wählen Sie im Kontextmenü den Befehl *Neu - Gruppe*.
- ▶ Geben Sie den Gruppennamen ein.
Windows erzeugt automatisch den Prä-Windows-2000-Namen.
- ▶ Legen Sie den *Gruppenbereich* und den *Gruppentyp* fest.
Zur Verrechnung können Sie nur Sicherheitsgruppen verwenden.

Sie sollten bei der Benennung von Gruppen ebenso strukturiert vorgehen wie bei den OUs. Bezeichnen Sie globale Gruppen stets durch ein vorangestelltes *GG*, lokale Gruppen durch *LG* und universale Gruppen durch *UG*. Verwenden Sie außerdem für LGs und GGs ein Standortkürzel sowie die OU und eine verständliche Bezeichnung für die Funktion der Gruppe. Gruppennamen wie z. B. *GG-B-Buchhaltung* sind selbsterklärend, es lohnt sich also, auf unverständliche Abkürzungen zu verzichten. Dieser Aufbau führt dazu, dass Sie die Art und den Zweck der Gruppe erkennen können, außerdem werden die verschiedenen Gruppentypen in den Verwaltungstools zusammenhängend untereinander angezeigt.

Gruppenkonten verwalten

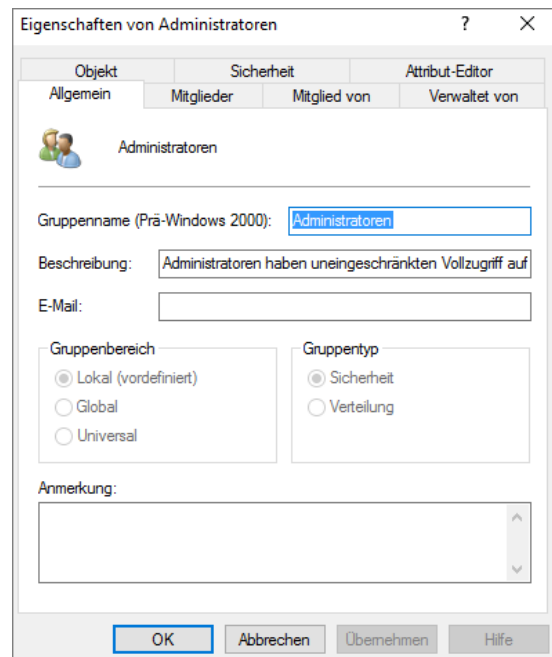
- Klicken Sie doppelt auf die Gruppe, die Sie verwalten wollen.

Im Register *Allgemein* können Sie sowohl den Gruppenbereich als auch den Gruppentyp verändern. Globale Gruppen können Sie nur über den Zwischenschritt *Universal* in lokale Gruppen konvertieren. Das funktioniert jedoch nur, wenn die Voraussetzungen bezüglich der Gruppenmitgliedschaften erfüllt sind.

Neu erstellte Gruppen haben zunächst keine Mitglieder. Auf der Registerkarte *Mitglieder* können Sie Mitglieder hinzufügen. Sie können auch Benutzerkonten über deren Eigenschaften zu einem Gruppenmitglied machen.

Neu erstellte Gruppen sind noch nicht Mitglied einer anderen Gruppe. Auf der Registerkarte *Mitglied von* können Sie sie einer oder mehreren Gruppen hinzufügen. Setzen Sie Gruppenverschachtelung nur mit Bedacht ein, sonst verlieren Sie schnell den Überblick, wer denn nun wirklich Mitglied einer Gruppe ist.

Im Register *Verwaltet von* können Sie die Verwaltung der Mitglieder dieser Gruppe delegieren.



Verrechnung mit Gruppen

Wenn Sie den folgenden Regeln zur Verrechnung folgen, benötigen Sie eventuell mehr Gruppenkonten als bei anderen Verrechnungsvarianten. Allerdings steigt die Übersichtlichkeit, und die Alltagsadministration beim Zuweisen von Berechtigungen geht deutlich schneller.

- ✓ Weisen Sie Berechtigungen ausschließlich domänenlokalen Gruppen zu.
Für jede Ressource (z. B. Laufwerk = LW) sollten Sie eine lokale Gruppe mit Rechten für das Lesen (L), Schreiben (S), den Vollzugriff (VZ) und ohne Zugriffsberechtigung (kein Zugriff, KZ) erstellen.
Für die bequeme Erstellung der Gruppen sind selbst erstellte DSAdd-Skripte bestens geeignet.
- ✓ Fassen Sie Benutzer mit den gleichen Anforderungen in globalen Gruppen zusammen.
Jeder Benutzer kann Mitglied in vielen Gruppen sein.
- ✓ Weisen Sie den Benutzern Rechte zu, indem Sie globale Gruppen zu domänenlokalen hinzufügen.

Für das obige **Beispiel** der Buchhalter könnte das folgendermaßen aussehen:

- ✓ In der Domäne der Buchhaltungs-Server werden vier domänenlokale Gruppen erstellt, z. B. *LG-B-LW_Buchhaltung-L*, *LG-B-LW_Buchhaltung-S*, *LG-B-LW_Buchhaltung-VZ* und *LG-B-LW_Buchhaltung-KZ*.
- ✓ Auf den Buchhaltungs-Servern werden den domänenlokalen Gruppen die entsprechenden Berechtigungen zugewiesen.

- ✓ Ab jetzt müssen Sie die Buchhaltungs-Server nicht mehr anfassen, wenn es um die Zuweisung von Zugriffsrechten geht. Machen Sie einfach die passenden globalen (oder universalen) Gruppen zu Mitgliedern in den entsprechenden domänenlokalen Gruppen.
- ✓ Als weiterer Vorteil bleiben die Berechtigungslisten auf den Buchhaltungs-Servern sehr übersichtlich.

Die Gruppenmitgliedschaften werden einem Benutzer bei der Anmeldung an der Domäne zugewiesen. Verändern Sie die Gruppenmitgliedschaften eines angemeldeten Benutzers, ändert sich nichts an dessen Berechtigungen. Der Benutzer muss sich zuerst ab- und dann wieder anmelden. Darüber hinaus müssen diese Veränderungen auf den Anmelde-DC des Benutzers repliziert worden sein. Wurde die Gruppenmitgliedschaft in einem anderen Standort verändert als dem, an dem sich der Benutzer anmeldet, kann das einige Zeit dauern. Um den Vorgang zu beschleunigen, können Sie die standortübergreifende Replikation von Hand anstoßen.

12.8 Spezielle Konten

Konten, die Sie kennen sollten

Es existieren einige Konten, die Sie nicht verwalten, wohl aber benutzen können.

- ✓ **Jeder:** Jedes Konto, das sich in einer beliebigen vertrauten Domäne erfolgreich authentifiziert hat. Dieses Konto wird gerne zur Verrechnung benutzt. Meistens sind aber eigentlich die Domänen-Benutzer damit gemeint. Entsteht eine Vertrauensstellung, haben Sie damit auch der vertrauten Domäne Berechtigungen erteilt.
- ✓ **Ersteller-Besitzer:** der Besitzer eines Objekts
- ✓ **Interaktiv:** das Benutzerkonto, das lokal am Rechner angemeldet ist
- ✓ **Netzwerk:** jedes Konto, das über das Netzwerk auf den Rechner zugreift
- ✓ **System:** repräsentiert das Betriebssystem. Dieses Konto verfügt über die größten Rechte auf einem Rechner. Verändern Sie seine Einstellungen nur, wenn Sie genau wissen, was Sie tun.

Weitere wichtige Gruppen:

- ✓ **Domänen-Benutzer:** Die primäre Gruppe von jedem Benutzerkonto. Jedes Benutzerkonto, das Sie erstellen, ist automatisch Mitglied dieser globalen Gruppe.
- ✓ **Benutzer:** Diese Gruppe gibt es als domänenlokale Gruppe und auch auf jedem Windows-Rechner. In der rechnerlokalen Gruppe werden die Domänen-Benutzer automatisch Mitglied, sobald der Rechner der Domäne hinzugefügt wird. Dadurch wird jedes Benutzerkonto der Domäne ein Benutzer eines Mitgliedsrechners.
- ✓ **Domänen-Admins:** Enthalten die Administratoren, welche die lokale Domäne verwalten und umfassende Rechte in dieser Domäne besitzen. Ein Administrator ist jeweils nur für eine Domäne zuständig. Wenn Sie mehrere Domänen in einer Gesamtstruktur anlegen, gibt es mehrere Benutzerkonten *Administrator*, die jeweils zu einer Domäne gehören und nur in dieser einen Domäne volle administrative Berechtigungen besitzen. Domänen-Admins haben in einer Domäne umfassendere Rechte als Organisations-Admins.
- ✓ **Administratoren:** Die Mitgliedschaft in dieser Gruppe gibt einem Konto die administrativen Rechte auf einem Rechner. Administratoren gibt es auch als domänenlokale Gruppe. Mitglieder dieser Gruppe sind die Domänen-Admins und die Gruppe Organisations-Admins. Dadurch kann jeder Organisations-Admin jeden Domänencontroller der Gesamtstruktur administrieren.
- ✓ **Organisations-Admins:** Sind eine spezielle Gruppe von Administratoren, die Berechtigungen für alle Domänen in Active Directory besitzen. Sie haben auf Ebene der Gesamtstruktur die meisten Rechte, in einzelnen Domänen haben jedoch die Domänen-Admins mehr Rechte. Organisations-Admins gibt es nur in der Rootdomäne.
- ✓ **Schema-Admins:** Sind eine der kritischsten Gruppen überhaupt. Mitglieder dieser Gruppe dürfen Veränderungen am Schema von Active Directory vornehmen. Produkte, die das Schema von Active Directory erweitern, wie zum Beispiel Exchange, können nur installiert werden, wenn der installierende Administrator in dieser Gruppe Mitglied ist.

Das Konto *Administrator* in der ersten installierten Domäne einer Gesamtstruktur ist das wichtigste und kritischste Konto im gesamten System. Es erlaubt den administrativen Zugriff auf alle wichtigen Systemfunktionen und ist Mitglied aller Administratorengruppen.

Einige der Gruppen sind nur in der ersten innerhalb der Gesamtstruktur eingerichteten Domäne definiert. Andere Gruppen erstellt Windows Server 2022 erst nach der Installation bestimmter Dienste wie DNS und DHCP:

- ✓ **DHCP-Administratoren:** Dürfen DHCP-Server in der Domäne verwalten. Die Gruppe wird nach der Installation des ersten DHCP-Servers auf einem Domänencontroller der Domäne erstellt.
- ✓ **DHCP-Benutzer:** Enthält Benutzerkonten, die lesend auf die Informationen des DHCP-Diensts zugreifen, aber keine Änderungen vornehmen dürfen. Diese Gruppe ist nur für Administratoren und Operatoren, nicht für normale Benutzer oder Computer relevant. Computer, die DHCP-Adressen anfordern, müssen darin nicht aufgenommen werden.
- ✓ **DnsAdmins:** Diese Gruppe enthält die Administratoren für DNS-Server. Dieser Gruppe sind keine Benutzer zugeordnet. Sie kann verwendet werden, um die Administration von DNS-Servern zu delegieren. Das ist vor allem dann von Bedeutung, wenn die DNS-Infrastruktur eines Unternehmens von Administratoren verwaltet wird, die nicht für die Active Directory-Umgebung zuständig sind. Diese Gruppe wird erst angelegt, wenn ein DNS-Server auf einem Domänencontroller erstellt wurde, der seine Informationen in Active Directory verwaltet.
- ✓ **DnsUpdateProxy:** In dieser Gruppe befinden sich Computer, die als Proxy für die dynamische Aktualisierung von DNS-Einträgen fungieren können. Diese Gruppe steht nur zur Verfügung, wenn ein Domänencontroller angelegt wird. In diese Gruppe können Sie zum Beispiel DHCP-Server aufnehmen, die dynamische DNS-Einträge für die Clients auf den DNS-Servern erstellen sollen.
- ✓ **Richtlinien-Ersteller-Besitzer:** Diese Gruppe umfasst die Anwender, die Gruppenrichtlinien für die Domäne erstellen dürfen. Das können Administratoren sein, die sich nur um diese Aufgabe in der Gesamtstruktur kümmern.
- ✓ **WINS Users:** Diese Gruppe wird angelegt, wenn es einen WINS-Server auf einem der Domänencontroller gibt. In ihr befinden sich die Benutzer, die nur Leserechte auf die WINS-Datenbank haben.

Die Gruppen *DnsUpdateProxy*, *Organisations-Admins*, *Schema-Admins* und *DnsAdmins* werden in der ersten Domäne, die in einer Gesamtstruktur eingerichtet wird, definiert. Dies ist gleichzeitig die oberste Domäne der ersten Struktur der Gesamtstruktur. Einer Gruppe können Benutzer und Benutzergruppen aus unterschiedlichen Domänen der Struktur hinzugefügt werden.

13 Berechtigungen anpassen

13.1 Berechtigungen

Zugriffssteuerung

Zugriffsberechtigungen werden mithilfe von Zugriffskontrolllisten (Access Control List, ACL) gesteuert. Es gibt zwei Arten von ACLs:

- ✓ Die Discretionary Access Control List (DACL) enthält die Berechtigungen für jedes einzelne Objekt. Dabei werden für jedes Konto einzelne Access Control Entries (ACEs) abgespeichert, die den Zugriff regeln.
- ✓ Die Security Access Control List (SACL) speichert, wer hinsichtlich welcher Zugriffe überwacht wird. Überwachungseinträge werden dann im Sicherheitsprotokoll der Ereignisanzeige gespeichert. Verwalten können Sie beide ACLs unter den Eigenschaften eines Objekts im Register *Sicherheit*.

Welche Berechtigungen Sie vergeben können, hängt vom Objekt ab. Für ein Benutzerkonto sind das andere Berechtigungen als etwa bei einer Datei, einem Registry-Eintrag oder einem Drucker. Die Delegierung der Objektverwaltung im vorangehenden Kapitel änderte z. B. die Berechtigungen einer OU.

Während der Anmeldung generiert Windows für den Benutzer ein Zugriffstoken, das die Sicherheits-ID (Security ID, SID) des Benutzerkontos enthält sowie die SIDs der Gruppen, in denen der Benutzer Mitglied ist. Beim Zugriff auf eine Datei vergleicht Windows die Einträge des Token mit der ACL und ermittelt daraus die Berechtigung. Dazu addiert das System die Berechtigungen für jeden übereinstimmenden Eintrag. Ein Benutzer bekommt die Berechtigungen, die seinem Konto zugewiesen sind sowie alle Berechtigungen, die den Gruppen zugewiesen sind, in denen er Mitglied ist.

Geben Sie einem Benutzerkonto die Berechtigung *Lesen* und wird einer Gruppe, in der dieser Benutzer Mitglied ist, zusätzlich die Berechtigung *Schreiben* zugewiesen, ergeben sich die effektiven Berechtigungen *Lesen* und *Schreiben*. Um die Berechtigungen zu setzen, wählen Sie in den Eigenschaften des Ordners oder der Datei die Registerkarte *Sicherheit*.

Folgende Grundsätze gelten für alle DACLs, unabhängig von den möglichen Berechtigungen:

- ✓ **Besitzer:** Jedes Objekt hat einen Besitzer, in der Regel ist das der Ersteller des Objekts. Der Besitzer kann immer die Berechtigungen seines Objekts verändern. Seit Windows Server 2003 kann Besitz übertragen werden.
- ✓ **Positive Zuweisung:** Wer nicht in der DACL erfasst ist, hat keinerlei Berechtigungen.
- ✓ **Standardberechtigungen:** Für jedes Objekt sind Standardberechtigungen definiert, die für den größten Teil der administrativen Aufgaben geeignet sind. Meistens setzen sie sich aus einer Reihe einzelner Berechtigungen zusammen. Es existiert immer der Eintrag *Vollzugriff*, der alle Berechtigungen umfasst.
- ✓ **Zulassen und verweigern:** Für eingetragene Konten können Sie Berechtigungen zulassen oder verweigern. Ist ein Konto mehrfach erfasst (z. B. durch Mitgliedschaft in verschiedenen Gruppen), addieren sich die *Zulassen*-Berechtigungen auf.
- ✓ **Verweigern überschreibt Zulassen**, d. h., verweigte Berechtigungen können nicht mehr zurückgewonnen werden. Ein Beispiel: In einer DACL tragen Sie die Gruppe *Jeder* ein und weisen ihr als Berechtigung *Vollzugriff verweigern* zu. Nun hat niemand mehr Zugriff auf das Objekt, unabhängig davon, welche Einträge sonst noch vorhanden sind. Nur der Besitzer kann das wieder ändern.
- ✓ **Vererbung:** Neu angelegte Objekte erben ihre Berechtigungen vom übergeordneten Objekt. Eine neue Datei verfügt über dieselben Berechtigungen wie der Ordner, in dem sie erstellt wurde, ein neuer Registry-Eintrag erbt seine Berechtigungen vom Schlüssel, in dem er erstellt wurde, ein Konto von der OU usw.
- ✓ **Überwachung:** Für jede Berechtigung können Sie überwachen, wer versucht, diese Berechtigung zu nutzen, d. h., Sie können auf Erfolg bzw. Fehler überwachen. Die Überwachung konfigurieren Sie immer bei den erweiterten Berechtigungen (siehe unten).

Berechtigungen der Gruppe *Benutzer* im Standardfall

- ✓ **Standardberechtigungen:** *Lesen, Ausführen und Ordnerinhalt anzeigen und Lesen*.
Damit erhält ein Benutzer lesenden Zugriff auf alle Dateien in diesem Ordner nebst Unterordnern.
- ✓ **Spezielle Berechtigungen:** *Dateien erstellen / Daten schreiben und Ordner erstellen / Daten anhängen*.
Damit kann ein Benutzer neue Ordner und Dateien erstellen, deren Besitzer er dann ist.
- ✓ Dem Konto *ERSTELLER-BESITZER* sind alle NTFS-Berechtigungen zugewiesen.
Da hier die Standardvererbung deaktiviert ist, handelt es sich nicht um Standardberechtigungen. Jeder Benutzer kann seine Dateien bearbeiten und löschen, die Ordner nur, wenn kein anderer Benutzer darin Objekte erstellt hat.

Wenn der *Ersteller-Besitzer* aus der DACL gelöscht wird, hat er keine Berechtigungen mehr, kann also seine Dateien nicht mehr bearbeiten.

13.2 NTFS-Berechtigungen

Einführung

Der Umgang mit Berechtigungen und die Verreckung von Ordnern und Dateien sind komplexe Aufgaben.

Die eben genannten Grundsätze werden nun an einem Beispiel erläutert und weiter ausgeführt. Der Ordner *Buchhaltung* wurde vom Benutzer *Administrator* auf einem leeren NTFS-Volume erstellt. Der Ordner erbt seine Berechtigungen vom übergeordneten Objekt, dem Volume. Zusätzlich ist es möglich, einzelnen Benutzern oder Gruppen Berechtigungen zu verweigern, wobei die Verweigerung immer Vorrang hat. Auch wenn ein Benutzer Mitglied in einer Gruppe ist, die Berechtigungen auf einen Ordner hat, verweigert Windows den Zugriff, wenn der Benutzer über eine Gruppe oder sein Benutzerkonto in der Verweigerungsliste eingetragen ist.

Beispiel

Auf eine Datei sollen alle Mitarbeiter der Buchhaltung (mit der Mitgliedschaft in der gleich benannten Gruppe) Zugriff erhalten. Eine Ausnahme machen dabei allerdings die Auszubildenden, die ebenfalls Mitglied der Gruppe *Buchhaltung* sind.

Wenn der Gruppe *Buchhaltung* der Zugriff auf diese Datei erlaubt ist, erhalten auch die Auszubildenden Zugriff, da sie Mitglied der Gruppe sind. Sie können der Gruppe *Auszubildende* den Zugriff verweigern. So erhalten die Auszubildenden zwar den Zugriff durch die Mitgliedschaft in der Gruppe *Buchhaltung*, der ihnen aber durch die Mitgliedschaft in der Gruppe *Auszubildende* verweigert wird.

Unterschied zwischen Rechten und Berechtigungen

Neben den **Berechtigungen** gibt es auch noch **Rechte**, die auch als Privilegien bezeichnet werden. Berechtigungen hängen immer an einem konkreten Objekt und werden über dessen DACL verwaltet. Rechte hängen an einem System und gelten für alle Objekte des Systems. Ein Beispiel: Es gibt die NTFS-Berechtigung *Besitz übernehmen*, die jeder Benutzer erhalten kann. Administratoren ist das System-Recht *Übernehmen des Besitzes von Dateien und Objekten* zugewiesen. Damit können sie den Besitz jedes Objekts übernehmen und als Besitzer können sie dann die Berechtigungen ändern.

NTFS-Berechtigungen konfigurieren

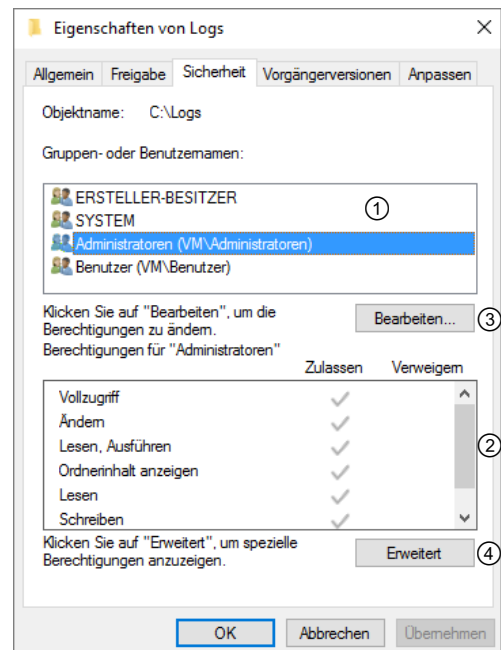
- Klicken Sie mit der rechten Maustaste auf einen Ordner und wählen Sie *Eigenschaften*.
- Wechseln Sie in das Register *Sicherheit*.

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.

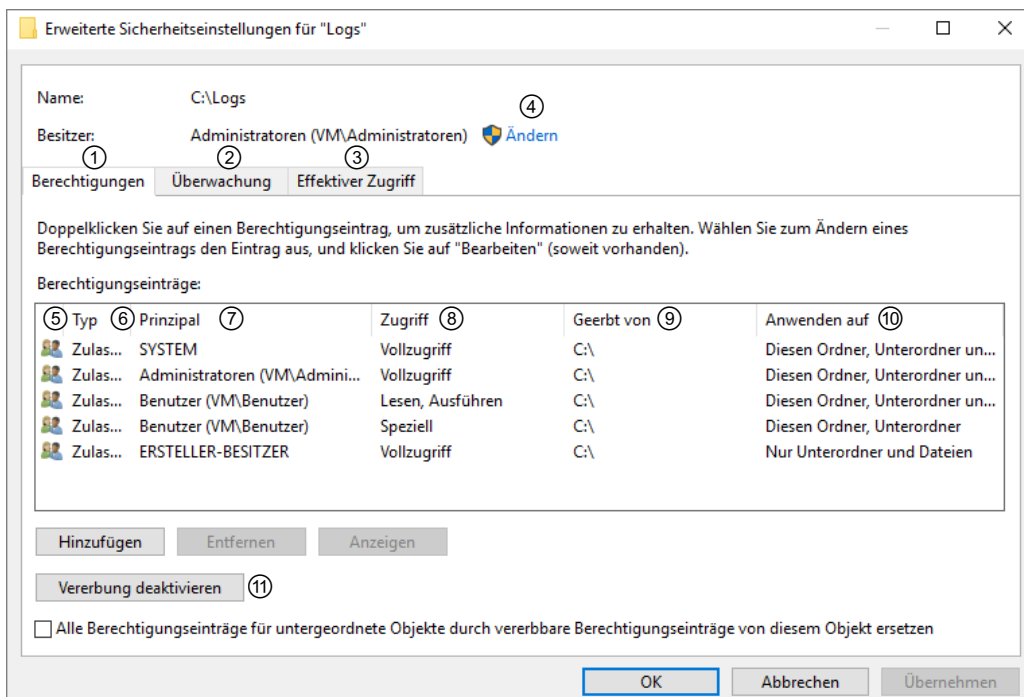


Nach einem Klick auf *Bearbeiten* ③ können Sie sowohl Konten hinzufügen als auch zusätzliche Berechtigungen vergeben. Geerbte Einträge können Sie dort nicht verändern.

Mit *Erweitert* ④ kommen Sie zu den erweiterten Sicherheitseinstellungen, wo Sie spezielle Berechtigungen einsehen und vergeben können.

Erweiterte Sicherheitseinstellungen

Die erweiterten Sicherheitseinstellungen verfügen über drei Registerkarten: *Berechtigungen* ①, *Überwachung* ② und *Effektiver Zugriff* ③. Im oberen Bereich des Fensters werden der Datei- oder Ordnername und der Besitzer angezeigt. Über den Link *Ändern* ④ können Sie den Besitz übertragen.



So sind die Berechtigungseinträge in den erweiterten Sicherheitseinstellungen aufgebaut:

- ✓ Das Symbol ⑤ zeigt, ob es sich um eine Gruppe oder ein Einzelkonto handelt.
- ✓ Der *Typ* ⑥ kann *Zulassen* oder *Verweigern* sein.
- ✓ Der *Prinzipal* ⑦ ist der Name des Benutzers oder der Gruppe.
- ✓ Unter *Zugriff* ⑧ wird die Art der Berechtigung angezeigt (Vollzugriff, Lesen, Ausführen, Schreiben etc.).
- ✓ Unter *Geerbt von* ⑨ wird angezeigt, von wo die Zugriffsrechte vererbt wurden.
- ✓ *Anwenden auf* ⑩ zeigt, für welche Dateien, Ordner und Unterordner die Berechtigung gilt.

Der Eintrag *Speziell* unter *Zugriff* ⑧ 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* ⑪ 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.

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.

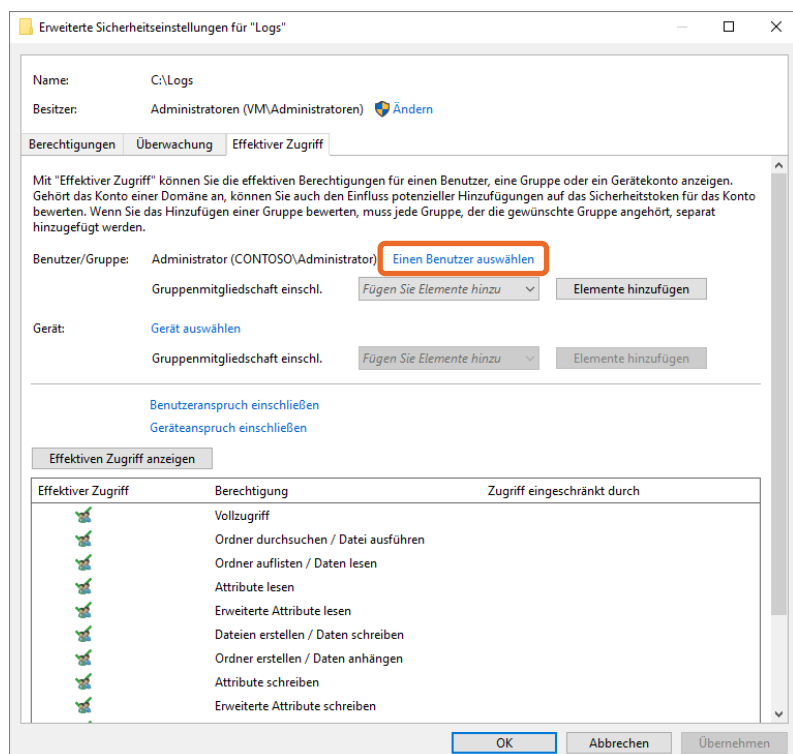
Effektiven Zugriff einsehen

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.

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 Berechtigungen erteilen, die zur Anpassung 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*.
- ▶ Geben Sie den Namen des neuen Besitzers ein oder suchen Sie unter *Erweitert* nach Benutzerobjekten. Bestätigen Sie Ihre Auswahl mit *Übernehmen* und *OK*.

Tipps und Hinweise zur NTFS-Verrechterung

- ✓ 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: Sie benötigen in der Regel nur vier Einträge in der Berechtigungsliste:

- ✓ Administratoren mit Vollzugriff; nicht unbedingt nötig, erleichtert aber oft die Arbeit;
- ✓ System mit Vollzugriff; nicht unbedingt nötig;
- ✓ eine domänenlokale Ressourcen-Gruppe mit Lese-Berechtigungen: lesen, ausführen und Ordnerinhalt anzeigen und lesen; eventuell nicht nötig;
- ✓ eine domänenlokale Ressourcen-Gruppe mit Ändern-Berechtigungen.



Verrechten Sie möglichst nur auf der ersten Ordnersebene, sodass alle untergeordneten Objekte über dieselben Berechtigungen verfügen, sonst kämpfen Sie mit dem geschilderten Verschieben-Problem.

Manchmal ist es notwendig, das Löschen von Ordner zu verhindern. Über komplizierte Berechtigungen kommen Sie in der Regel ans Ziel, das geht aber auch einfacher. Erstellen Sie in dem Ordner eine Datei und weisen Sie ihr folgende Berechtigungen zu: Gruppe *Jeder* - *Vollzugriff verweigern*.

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 bedenkenlos löschen.

Warum Benutzer keinen 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. Das willkürliche Ändern von Berechtigungen kann als dummer Streich betrachtet werden oder auch als Mobbing.

13.3 Freigabeberechtigungen 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 Freigabeberechtigungen erklärt. Die Freigaben können Sie u. a. in der Computerverwaltung und im Server-Manager unter *Datei-/Speicherdienste - Freigaben* einsehen.

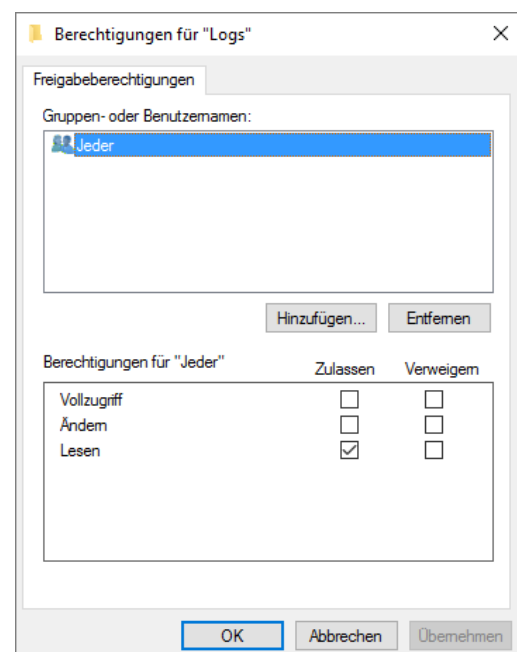
- ▶ Geben Sie im Startmenü `compmgmt.msc` ein und wählen Sie *Computerverwaltung*.
- ▶ Klicken Sie in der linken Spalte auf *System - Freigegebene Ordner - Freigaben*.
- ▶ Klicken Sie mit der rechten Maustaste auf eine Freigabe und wählen Sie *Eigenschaften*.

Freigabeberechtigungen 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 Freigabeberechtigungen und regeln Sie die Zugriffe mit NTFS-Berechtigungen. Es gibt nur drei Berechtigungen. 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 Freigabeberechtigungen 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.

Berechtigungen für den Zugriff über das Netzwerk nehmen Sie über die Registerkarte *Freigabe* in den Eigenschaften des Ordners, Schaltfläche *Erweiterte Freigabe* vor. Mit Berechtigungen legen Sie fest, wer über das Netzwerk auf den PC zugreifen darf. Den jeweiligen Benutzer müssen Sie vorher auf dem PC mit dieser Freigabe anlegen, falls Sie die Freigabe in einer Arbeitsgruppe einrichten.

Die Festlegung auf NTFS-Ebene, also für das Dateisystem, erfolgt über die Eigenschaften eines Ordners auf der Registerkarte *Sicherheit*. Nach jeweils einem Klick auf die Schaltflächen *Bearbeiten* und *Hinzufügen* können Sie neue Benutzer, denen Sie Berechtigungen gewähren wollen, hinzufügen.



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 2022 beim Erstellen einer Freigabe nur die Leseberechtigung zu. Über das Netzwerk kann niemand den Inhalt der Freigabe verändern. Weisen Sie einem Benutzerkonto die Berechtigung *Lesen* für einen Ordner zu und bekommt zusätzlich eine Gruppe, in der dieser Benutzer Mitglied ist, die Berechtigung *Schreiben* zugewiesen, ergeben sich die effektiven Berechtigungen *Lesen* und *Schreiben*. Windows arbeitet mit den engsten Sicherheitseinschränkungen. Hat ein Benutzer das Recht „Vollzugriff“ auf eine Freigabe und befindet sich in der Freigabe ein Verzeichnis, für das der Benutzer nur lesenden Zugriff hat, dann gilt der lesende Zugriff, nicht der Vollzugriff der Freigabe.

Hat er im Dateisystem Vollzugriff und wurde auf die Freigabe nur das Leserecht vergeben, darf er auf den Ordner über das Netzwerk nur lesend zugreifen. Er kann allerdings lokal auf dem Computer oder über andere überlappende Freigaben, die diese Einschränkung nicht haben, mit mehr Rechten zugreifen. Die Berechtigungen bilden daher immer eine Schnittmenge zwischen Freigabeberechtigungen und Berechtigungen auf dem Dateisystem (NTFS oder ReFS).

13.4 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 2022 standardmäßig beim Installieren eines neuen Druckers einrichtet. Hier werden nur die Berechtigungen erklärt. Näheres zur Druckerverwaltung erfahren Sie im Kapitel *Drucker verwalten*.

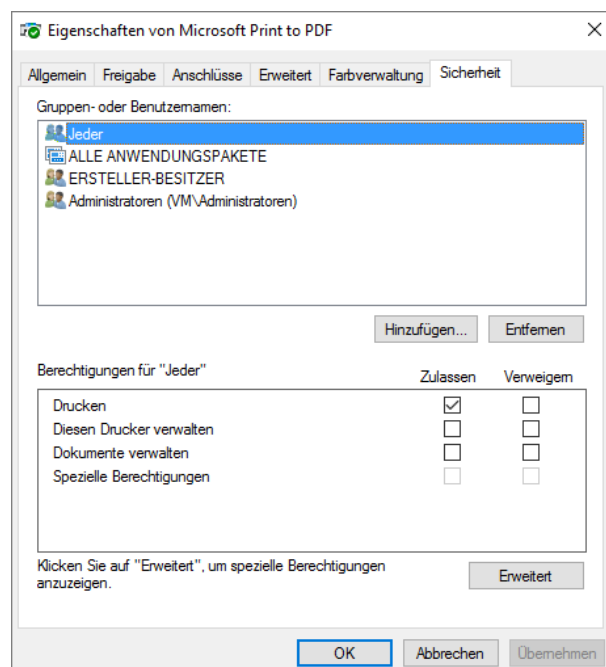
- ▶ Öffnen Sie die Systemsteuerung und klicken Sie auf *Hardware*.
Wählen Sie *Geräte und Drucker*.
- ▶ Klicken Sie mit der rechten Maustaste auf einen Drucker und wählen Sie *Druckereigenschaften*.
- ▶ Klicken Sie auf die Registerkarte *Sicherheit*.

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.

14 Dateidienste einrichten

14.1 Ordnerfreigaben

Überblick

Eine zentrale Dateiablage mit der Möglichkeit, von beliebigen Rechnern aus auf den Datenbestand zuzugreifen, ist eine Grundfunktion 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 Freigaben in einem Stamm zusammenfassen und hilft so, den Überblick zu behalten.

Im Folgenden werden zunächst Freigaben mit dem 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.

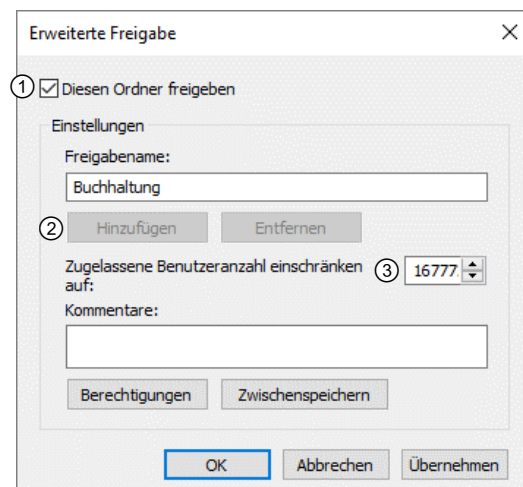
Seit Windows Server 2012 hat sich in der Dateiserver-Verwaltung vieles verändert. Einige Aufgaben können mit dem Server-Manager erledigt werden, andere nur mit dem Ressourcen-Manager für Dateiserver oder der DFS-Verwaltung. Und schließlich gibt es auch Tätigkeiten, die nur in der Computerverwaltung oder in der Active Directory-Verwaltung ausgeführt werden können.

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 Freigabennamen ein Dollarzeichen \$ anhängen, machen Sie daraus eine versteckte Freigabe, die standardmäßig im Windows-Explorer nicht angezeigt wird. Freigabennamen müssen auf einem Rechner eindeutig sein.



Sie können Ordner unter mehreren verschiedenen Freigabennamen freigeben ② und den Freigaben so unterschiedliche Freigabeberechtigungen zuweisen.

Berechtigungen wurden im vorhergehenden 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 und in Arbeitsgruppen ist, je nach Betriebssystem, zwischen 10–20 als Maximum vorgegeben.

Im Windows-Explorer können Sie nicht alle Optionen für Freigaben einstellen.

Offlineeinstellungen – Zwischenspeichern

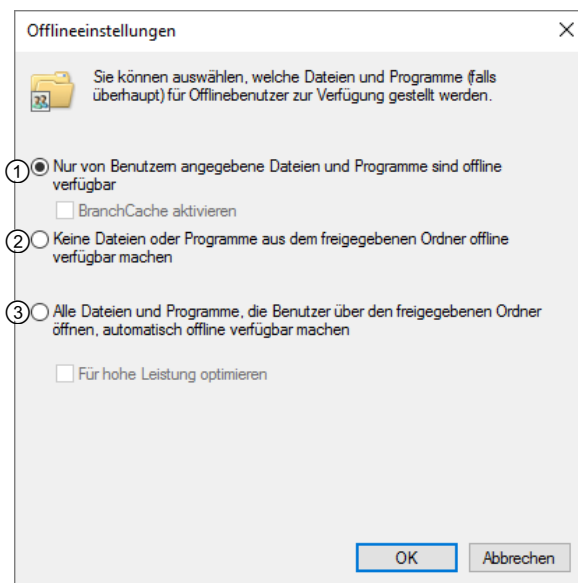
Offlineeinstellungen zielen in erster Linie auf Laptop-Benutzer, die außerhalb des Firmennetzwerks Zugriff auf den Freigabeninhalt benötigen. Bei entsprechender Client-Konfiguration kann ein Benutzer überall fast so arbeiten, als wäre sein Rechner am Firmennetz angeschlossen.

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.



Objekte, die offline verfügbar gemacht werden, sind während der Bearbeitung nicht gesperrt. Dies kann dazu führen, dass unterschiedliche Versionen entstehen. Wenn mobile Benutzer wieder mit dem Netzwerk verbunden sind, wird bei der Synchronisierung die jeweils neueste Version die anderen überschreiben. Da dies dazu führen kann, dass Arbeit verloren geht, sollten Sie möglichst nur Ordner offline zur Verfügung stellen, die im alleinigen Besitz von Benutzern sind. Für von Gruppen genutzte Ordner sollten die Benutzer selektiv eine Version speichern, um sich so der Versionierung bewusst zu sein.

14.2 Dateidienste installieren

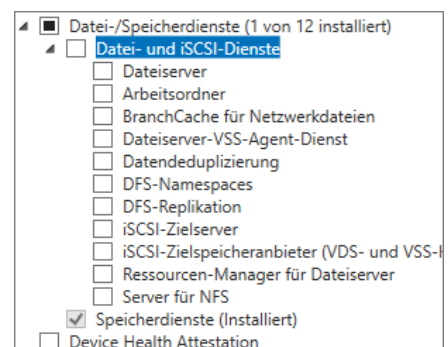
Soll ein Rechner als Fileserver dienen, empfiehlt es sich, die Rolle *Dateidienste* zu installieren. Dadurch stehen zusätzliche Möglichkeiten für die Verwaltung der Freigaben zur Verfügung.

Sobald Sie auf dem Rechner eine Freigabe erstellt haben, wird die Serverrolle *Dateidienste* automatisch im Server-Manager installiert, aber keines der zusätzlichen Features aktiviert.

- ▶ 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:

- ✓ Ziel des *BranchCache* ist es, den Netzwerkverkehr zwischen Standorten, die über WAN miteinander verbunden sind, zu reduzieren. Zu diesem Zweck werden aus der Zentrale heruntergeladene Daten in der Außenstelle auf einem Windows Server- oder Clientcomputer zwischengespeichert. Benötigt ein weiterer Client die gleiche Datei, lädt er diese aus dem Cache und vermeidet hierdurch einen erneuten Zugriff über das WAN.



Dateidienste-Rollen

- ✓ Sobald Sie mehr als ein paar Ordnerfreigaben benötigen, bietet DFS interessante Möglichkeiten. Sie sollten daher *DFS-Namespaces* und *DFS-Replikation* sowie alle erforderlichen Features installieren.
- ✓ *iSCSI-Zielserver* und *Zielspeicheranbieter* benötigen Sie nur, wenn dieser Server iSCSI-Speicher zur Verfügung stellen soll.
- ✓ Der *Ressourcenmanager für Dateiserver* sollte in jedem Fall installiert werden.
- ✓ *Server für NFS* benötigen Sie, wenn Sie Speicherplatz 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.

Ausführliche Informationen zum Branchcache finden Sie hier:

- ✓ <https://docs.microsoft.com/de-de/windows-server/networking/branchcache/branchcache>

Freigaben im Server-Manager

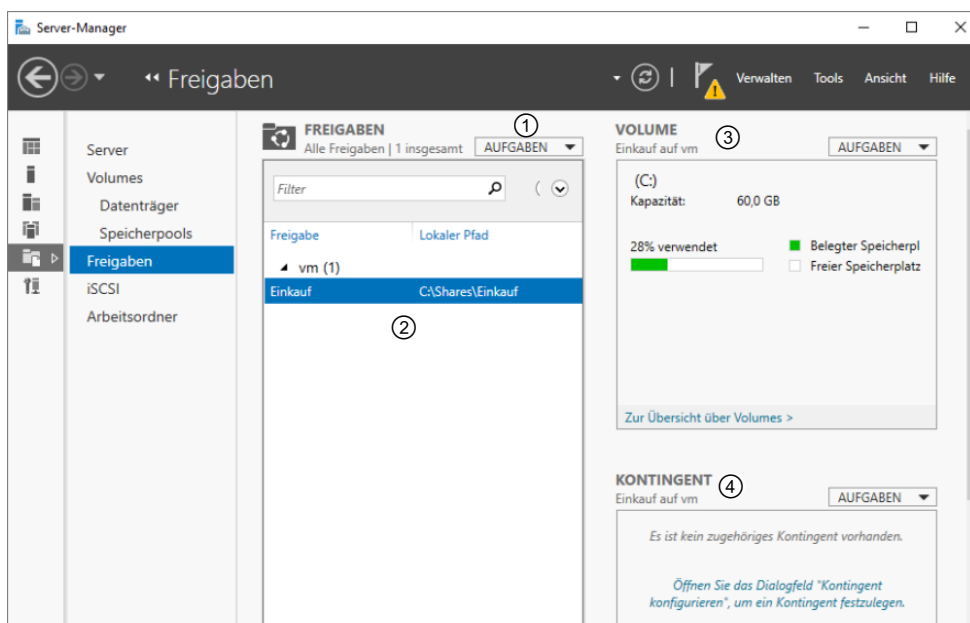
Auf der Seite *Freigaben* können Sie folgende Aufgaben ausführen:

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** ③ erhalten 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** ④ sehen Sie einen Überblick über die Kontingenteinstellungen, die Sie über *AUFGABEN* auch verändern können.

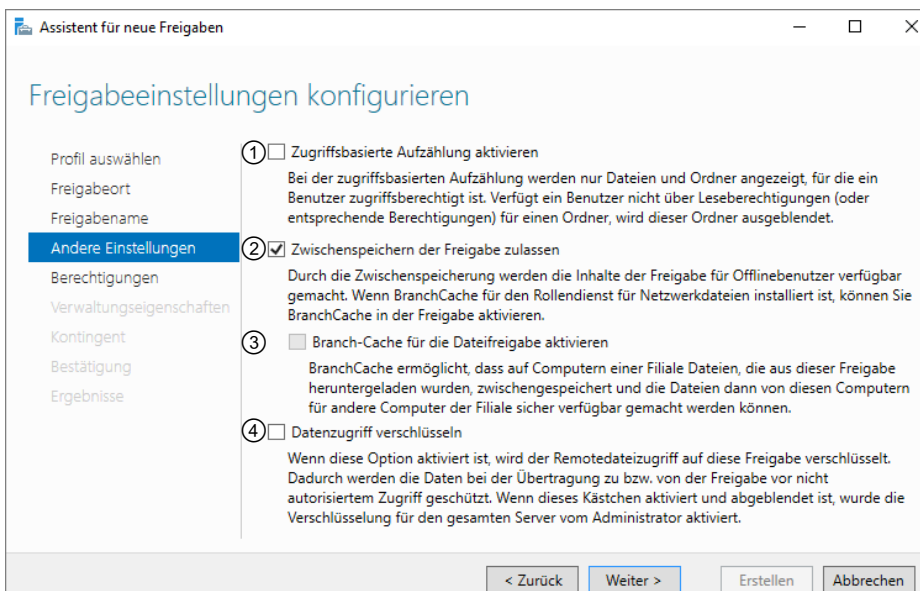
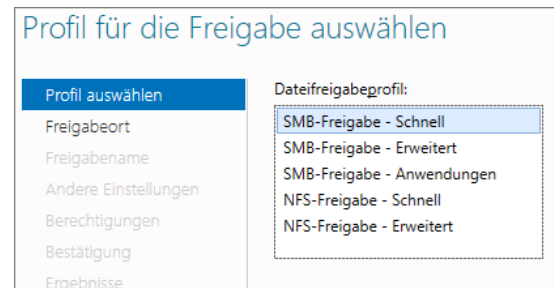


14.3 Freigabe- und Speicherverwaltung

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 - AUFGABEN** auf **Neue Freigabe**.
- ▶ Wählen Sie das Profil der SMB- oder NFS-Freigabe aus und klicken Sie auf **Weiter**.
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 Freigabennamen und optional eine Beschreibung. Ändern Sie wenn nötig den lokalen Pfad und Remotepfad zur Freigabe und klicken Sie auf **Weiter**.
- ▶ 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.
 - ✓ **BranchCache** ③ ist, wie beschrieben, eine Datei-Zwischenspeicherung zur Entlastung von WAN Verbindungen zwischen Standorten.
 - ✓ **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-, Sicherungs- und 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**.

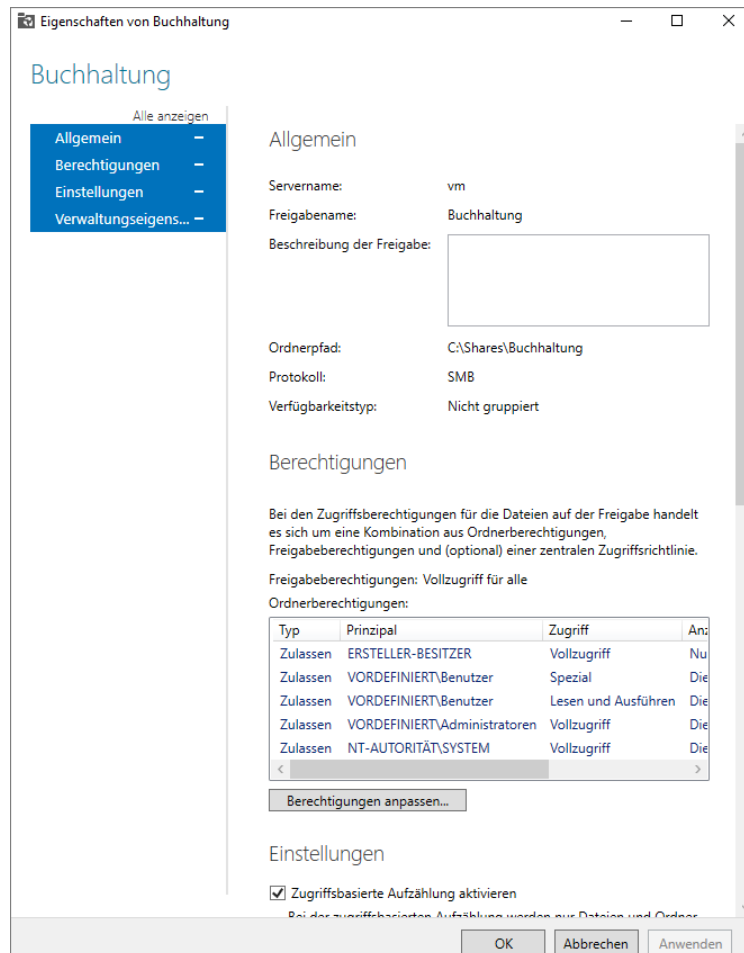
- ▶ Weisen Sie auf Wunsch eine bestehende Kontingentrichtlinie zu und klicken Sie auf *Weiter*. (Kontingentrichtlinien werden im folgenden Unterkapitel erklärt.)
 - ▶ Überprüfen Sie die Einstellungen und klicken Sie auf *Erstellen*.
- Auf der letzten Seite wird angezeigt, ob alle Konfigurationsschritte 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:

- ✓ allgemeine Daten zur Freigabe,
- ✓ Zugriffsberechtigungen (Resultat aus Freigabeberechtigung, NTFS-Berechtigungen und Zugriffsrichtlinien),
- ✓ zugriffsbasierte Aufzählung,
- ✓ Zwischenspeichern (offline),
- ✓ BranchCache,
- ✓ Übertragungsverschlüsselung,
- ✓ Verwaltungseigenschaften.



Freigabe-Eigenschaften im Server-Manager

14.4 Ressourcen-Manager für Dateiserver

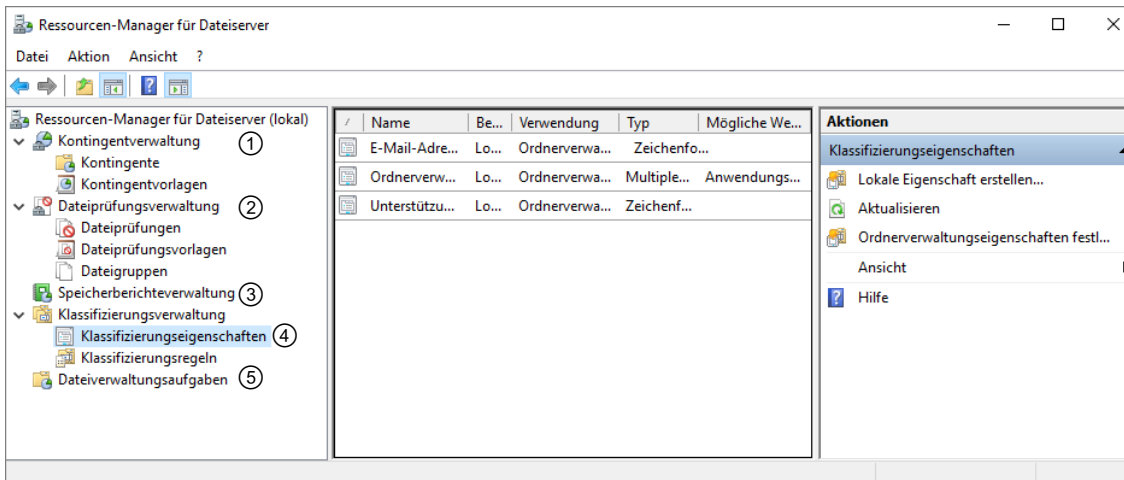
Überblick

Auf Dateiservern sammeln sich schnell große Mengen an Dateien an, wenn die Speicherung nicht geregelt wird. Von kopierten Datenträgerinhalten bis hin zu Video-, Foto- und Musiksammlungen ist hier vieles zu finden. Außerdem speichern Mitarbeiter gerne den letzten Jahresbericht in ihrem persönlichen Ordner und viele erhalten per Massen-E-Mails die gleichen 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 und begrenzen. Die Dateiprüfungsverwaltung ermöglicht Dateitypen für die Verwendung auszuschließen. Berichte helfen zu erkennen, womit der Speicherplatz belegt ist.

Ressourcen-Manager für Dateiserver

Sie können den Ressourcen-Manager für Dateiserver über das Menü *Tools* des Server-Managers starten.



Im Ressourcen-Manager können Sie folgende Aufgaben ausführen:

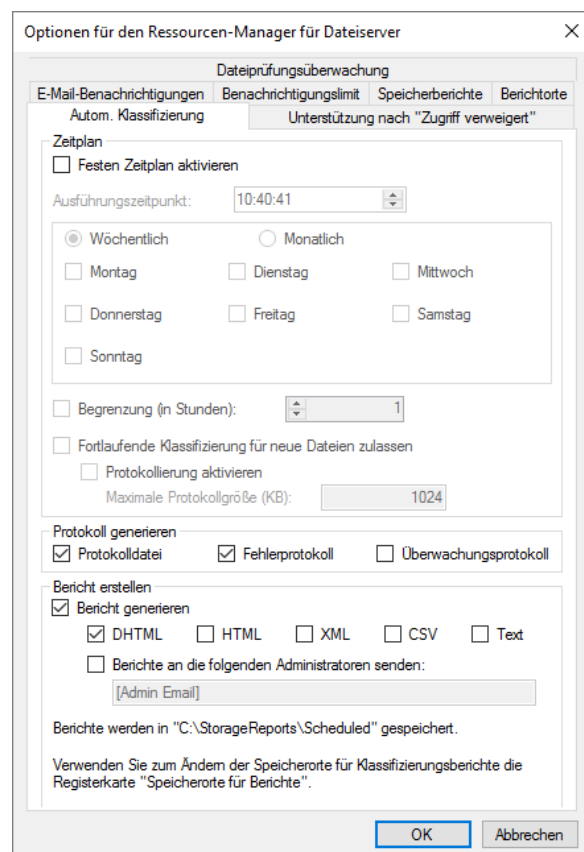
- ① Kontingente verwalten;
- ② nach Dateitypen und -gruppen filtern, um ihnen bestimmte Handlungen zuzuordnen (z. B. Speicherungsverbot);
- ③ Speicherberichte nach eigenen Kriterien erstellen und anzeigen lassen;
Berichte werden in `C:\StorageReports\Interactive` gespeichert;
- ④ Klassifizierungsregeln 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 obersten 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,
- ✓ 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.

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.

Kontingentvorlageneigenschaften für 100 MB-Grenze

Eigenschaften aus Kontingentvorlage kopieren (optional):
 100 MB-Grenze Kopieren

Einstellungen

Vorlagenname:
 100 MB-Grenze

Beschreibung (optional):

Speicherplatzbeschränkung

Grenze:
 100.000 ① MB

② ☒ Harte Kontingentgrenze: Überschreiten der Grenze nicht zulassen
☐ Weiche Kontingentgrenze: Überschreiten der Grenze gestatten (für Überwachungszwecke)

③ Benachrichtigungsschwellenwerte

Schwellenwert	E-Mail	Ereignispr...	Befehl	Bericht
Warnung für (85%)	✓			
Warnung für (95%)	✓	✓		
Warnung für (100%)	✓	✓		

Hinzufügen... Bearbeiten... Entfernen

OK Abbrechen

① definiert den Grenzwert, auf den sich alle weiteren Konfigurationen beziehen.

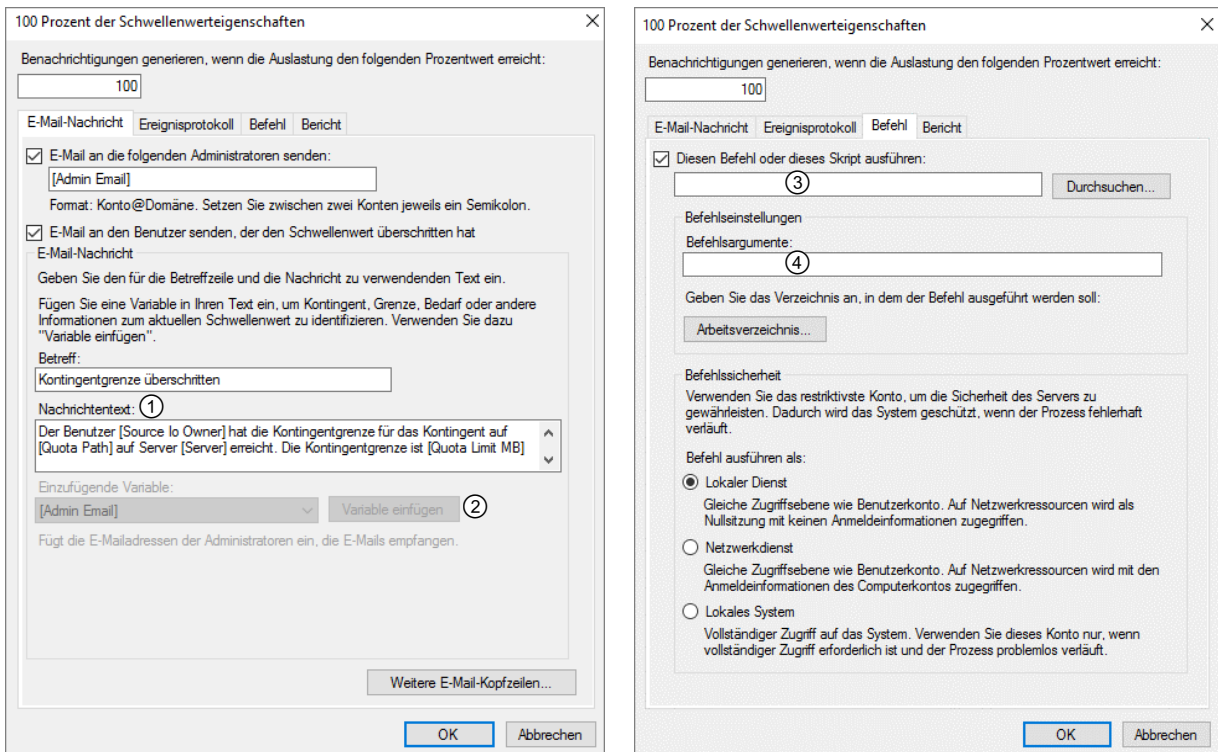
Mit der Kontingentgrenze ② legen Sie fest, ob diese Kontingentvorlage die Speichernutzung begrenzt (*Harte Kontingentgrenze*) oder nur der Überwachung dient (*Weiche Kontingentgrenze*).

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.



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 Kontingenterweiterung erfolgt mit dem Befehl `dirquota.exe` ③ und den Befehlsargumenten ④, der die Quotagrenze aus einer anderen Kontingentvorlage kopiert.

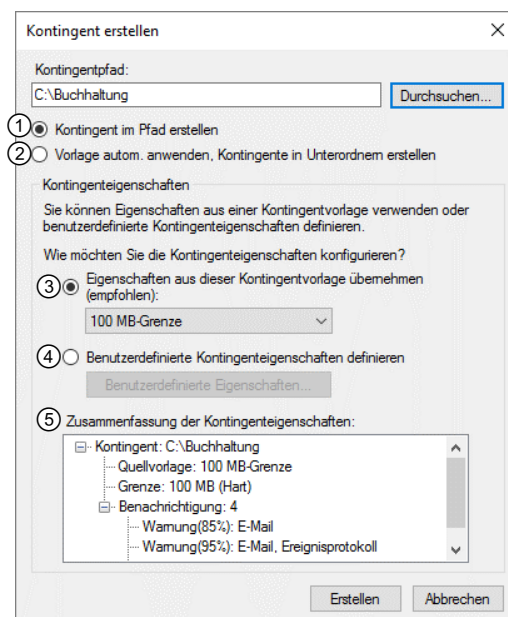
Neue Kontingentvorlage erstellen

- 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 das auf der vorigen Seite abgebildete Fenster mit den Kontingentvorlageeigenschaften, allerdings ohne Einträge. In der obersten Zeile können Sie dann eine vorhandene Vorlage auswählen und deren Einstellungen *Kopieren*. Den Namen der neuen Vorlage geben Sie in der zweiten Zeile ein.

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.

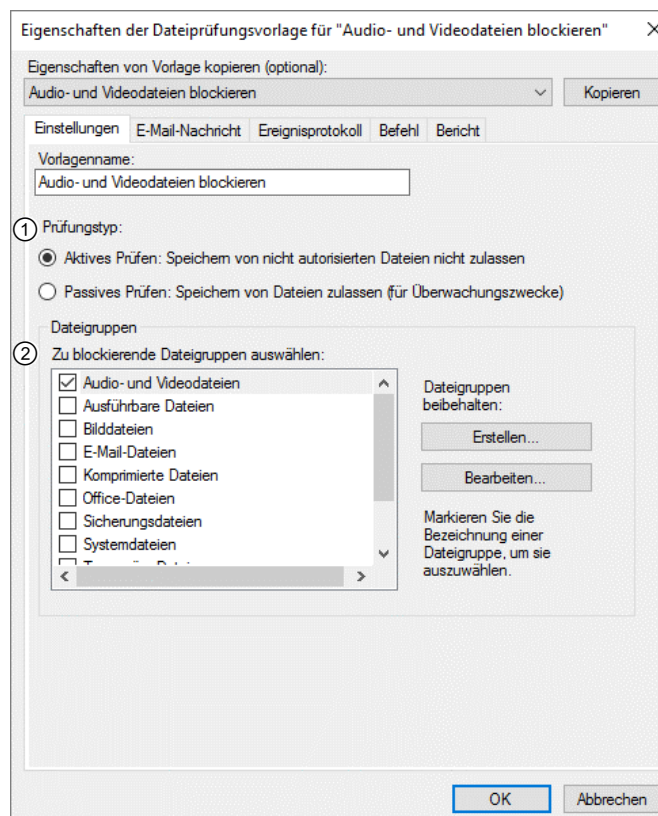
Die Abbildung zeigt die Dateiprüfungsvorlage *Audio- und Videodateien blockieren*.

Unter *Prüfungstyp* ① 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* ② 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** entsprechen dem Vorgang bei den Kontingentvorlagen.



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 Berichtsaufgabe 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*.

14.5 DFS (Distributed File System)

Überblick

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.

Der Einsatz von DFS lohnt sich ab dem zweiten Dateiserver. DFS verhindert nicht, dass weiterhin mit den vorhandenen Freigaben gearbeitet wird.

DFS installieren

Falls DFS noch nicht installiert wurde, können Sie dies im Assistenten zum Hinzufügen von Rollen und Features nachholen.

- ▶ Erweitern Sie auf der Seite *Serverrollen auswählen* den Eintrag *Datei- und iSCSI-Dienste* und aktivieren Sie die Einträge *DFS-Namespaces* und *DFS-Replikation*.
- ▶ Führen Sie die Installation mit einem Klick auf *Installieren* durch.

DFS-Verwaltung

Die Administration des DFS findet ausschließlich über die Konsole *DFS-Verwaltung* statt.

- ▶ Geben Sie im Startbildschirm *dfs* ein und wählen Sie *DFS-Verwaltung*. Alternativ können Sie die DFS-Verwaltung auch über das Menü *Tools* im Server-Manager öffnen.

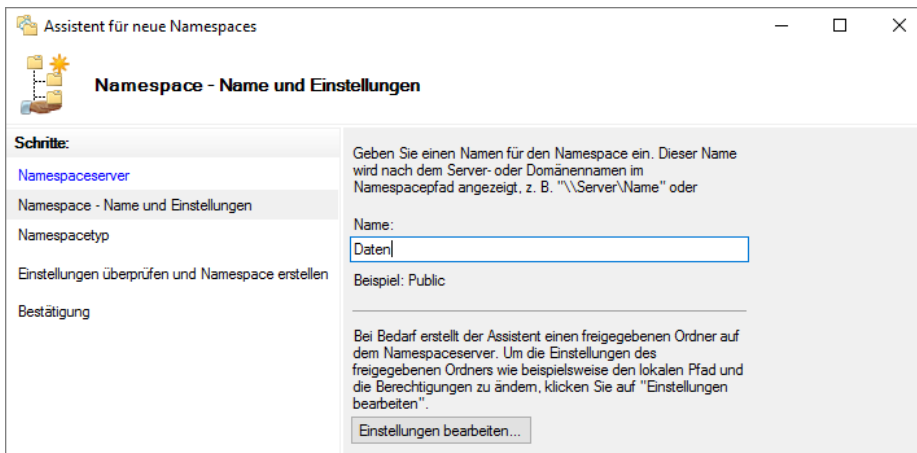
Namespace erstellen

Im DFS können Sie beliebig viele Namespaces einrichten. Besonders benutzerfreundlich ist es für die Benutzer, wenn Sie mehrere Namespaces erstellen, z. B. *Verwaltung*, *Buchhaltung*, *Produktion* etc. Jeder Benutzer hat dann seine Freigabe, in der er alle Ordner findet, die er benötigt. So erstellen Sie einen neuen Namespace:

- ▶ Erweitern Sie in der linken Spalte den Eintrag *DFS-Verwaltung* und klicken Sie mit der rechten Maustaste auf *Namespaces*. Wählen Sie im Kontextmenü *Neuer Namespace*.
- ▶ Geben Sie im Assistenten den Namen eines Servers ein, der den Namespace hosten soll. Über einen Klick auf *Durchsuchen* können Sie einen Server auswählen.
- ▶ Klicken Sie auf *Weiter*.

Für die Fehlerredundanz können Sie später zusätzliche Server hinzufügen.

- ▶ Geben Sie einen Namen für den Namespace an. Der Name des Namespace entspricht der „Freigabe“, auf die Ihre Benutzer später zugreifen.
- ▶ Klicken Sie auf *Einstellungen bearbeiten* und wählen Sie die Ordnerberechtigungen aus. Klicken Sie anschließend auf *OK* und dann auf *Weiter*.



Über *Einstellungen bearbeiten* legen Sie die Freigabeberechtigungen fest. Bedenken Sie, dass Ihre Einstellung die maximale Berechtigung darstellt, die Benutzer beim Zugriff über den DFS-Stamm erhalten. Daher sollten Sie an dieser Stelle in der Regel großzügige Berechtigungen vergeben, die dann weiter eingeschränkt werden können. Eine geeignete Einstellung ist z. B. *Vollzugriff für Administratoren, Lese/Schreibberechtigung für andere Benutzer*. Wenn Sie hier restriktive Einstellungen vornehmen, können Benutzer keine weiter reichenden Berechtigungen mehr erhalten.

- ▶ Legen Sie den Typ des Namespace fest und klicken Sie auf *Weiter*.

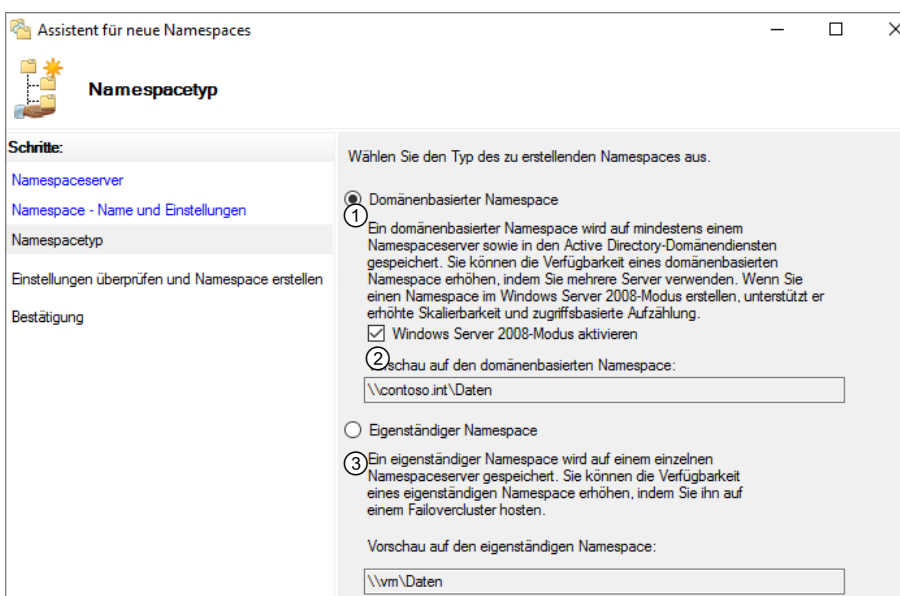
Sie können einen domänenbasierten ① oder eigenständigen Namespace ③ erstellen.

Für den *Windows Server 2008-Modus* ② müssen folgende Voraussetzungen erfüllt sein:

- ✓ Gesamtstrukturfunktionsebene ab Windows Server 2003
- ✓ Domänenfunktionsebene ab Windows Server 2008
- ✓ Alle Namespaceserver laufen mindestens unter Windows Server 2008.

Wann immer möglich sollten Sie diese Option aktivieren, denn sonst funktioniert die zugriffsbasierte Aufzählung nicht über DFS.

Einen eigenständigen Namespace ③ sollten Sie in einer Domäne nur in Ausnahmefällen installieren.



- ▶ Überprüfen Sie die Zusammenfassung und klicken Sie auf *Erstellen*. Der Namespace wird erstellt.
- ▶ Die letzte Seite zeigt die Ergebnisse und eventuelle Fehler. Klicken Sie auf *Schließen*.

Namespaceserver hinzufügen

- ▶ Markieren Sie den Namespace und klicken Sie im Bereich *Aktionen* auf *Namespaceserver hinzufügen*.
- ▶ Fügen Sie einen Namespaceserver hinzu und klicken Sie auf *OK*.

Damit werden die Einstellungen für diesen Namespace auf weiteren Servern zur Verfügung gestellt. Arbeiten Sie mit mehreren Standorten, ist es sinnvoll, den Namespace auch in jedem Standort vorzuhalten. Sonst muss der Zugriff auf den Namespace über eine eventuell langsame und teure WAN-Strecke erfolgen.

Eigenschaften eines Namespace bearbeiten

Sie können die Eigenschaften eines Namespace bearbeiten.

- ▶ Klicken Sie mit der rechten Maustaste auf einen Namespace und wählen Sie *Eigenschaften*.

Der Eigenschaftendialog besteht aus drei Registerkarten. Auf der Registerkarte *Allgemein* werden Name, Typ und Beschreibung angezeigt.

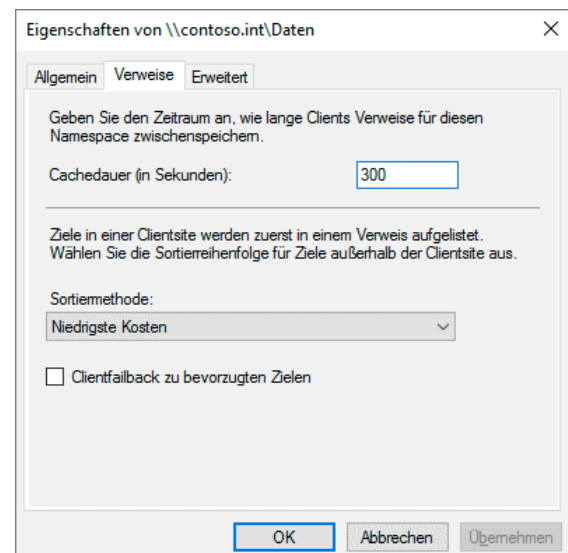
- ▶ Wechseln Sie auf die Registerkarte *Verweise*.

Beim Zugriff auf einen Namespace erhält der Client eine Liste des Inhalts. Wie lange diese Liste zwischengespeichert wird, legen Sie mit der *Cachedauer* fest.

Im Namespace können als Ordnerziele Server aus verschiedenen Standorten angegeben sein. Im Feld *Sortiermethode* legen Sie fest, ob und wie auf standortexterne Server zugegriffen wird.

Sollte eine Ressource mehrfach vorhanden sein und der bevorzugte Server des Clients fällt aus, so wird er einen anderen Server wählen. Mit der Option *Clientfailback zu bevorzugten Zielen* sorgen Sie dafür, dass der Client dorthin zurückwechselt, sobald der Server wieder online ist.

Im Register *Erweitert* können Sie die zugriffsbasierte Aufzählung einschalten, die standardmäßig nicht aktiviert ist.



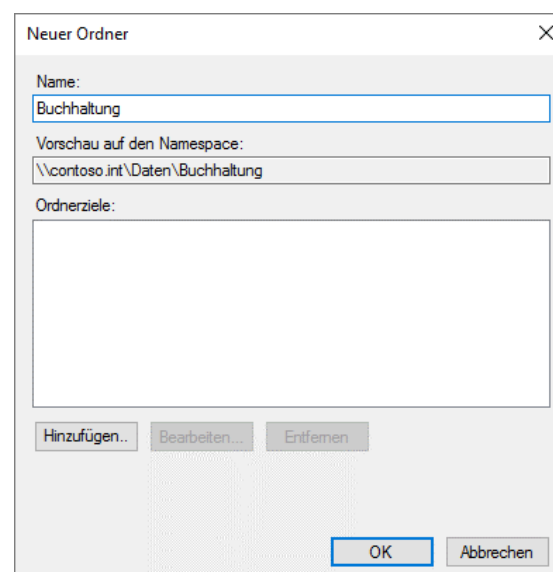
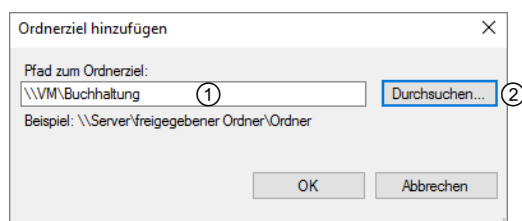
Eigenschaften von Namespace

Freigaben zum Namespace hinzufügen

Bis jetzt haben Sie mit dem Namespace nichts anderes als eine „intelligente Freigabe“ erstellt. Zum Einhängen von Freigaben in den Namespace gehen Sie folgendermaßen vor:

- ▶ Markieren Sie den Namespace und klicken Sie im Bereich *Aktionen* auf *Neuer Ordner*.
- ▶ Geben Sie den Namen des Ordners ein.

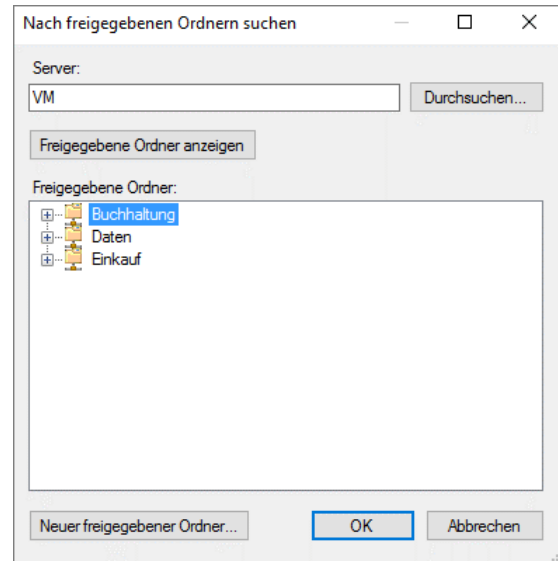
Über *Hinzufügen* können Sie den Ordner mit einem Ordnerziel verknüpfen. Dazu geben Sie entweder den UNC-Pfad ein ① oder Sie klicken auf *Durchsuchen* ②.



Dort geben Sie den Server an und klicken auf *Freigegebene Ordner anzeigen*. Nun können Sie aus den Freigaben wählen oder neue Freigaben erstellen.

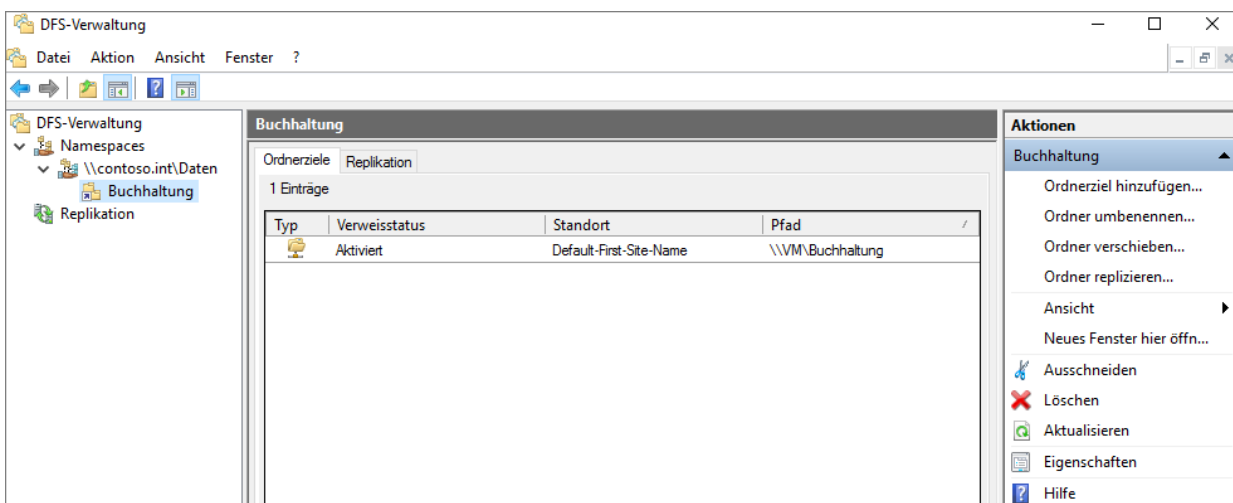
Beim Zugriff auf ein Ordnerziel greifen die Berechtigungen, die dort konfiguriert sind, falls sie nicht bereits durch die Berechtigungen des Namespace eingeschränkt sind. Fügen Sie ein zweites Ordnerziel hinzu, werden Sie gefragt, ob Sie eine Replikationsgruppe erstellen wollen. Mehrere Ordnerziele sind nur sinnvoll, wenn deren Inhalt identisch ist bzw. identisch werden soll.

Wenn Sie hier kein Ordnerziel angeben, können Sie in dem erstellten Ordner einen neuen Ordner anlegen und dort Ordnerziele definieren. So können Sie im Namespace zunächst eine Struktur erstellen, z. B. *Buchhaltung*, *Einkauf*, *Produktion*, und die Ordnerziele erst auf der nächsten Ebene definieren. Mehrere Namespaces sind dafür meist die bessere Lösung.



Zwischenstand

Nachdem Sie einige Namespaces erstellt und mit Ordnern ausgestattet haben, könnte Ihre DFS-Verwaltung ähnlich aussehen wie in der folgenden Abbildung.



Namespace erkunden

Für drei Abteilungen wurden Namespaces erstellt und in jedem Namespace wurden Ordner mit passenden Ordnerzielen definiert. Alle Abteilungen haben einen vergleichbaren Aufbau der Ordner- bzw. Freigabestruktur. Die Anleitungen verweisen jeweils auf dieselbe Freigabe.

Die Ordner *DFSRoots* und *DfsrPrivate*

Auf jedem Namespaceserver legt Windows automatisch den Ordner *DFSRoots* an. In diesem Ordner werden Unterordner für erstellte Namespaces und Ordner angelegt, die dieser Server hostet.



Verändern Sie nichts im Ordner *DFSRoots*! Fügen Sie niemals Dateien oder Ordner hinzu!

Wenn eine Freigabe (ein freigegebener Ordner) Mitglied in einer DFS-Replikationsgruppe ist, entsteht im Freigabeordner automatisch der Unterordner *DfsrPrivate* mit weiteren Unterordnern, die zur Verwaltung der Replikation benötigt werden.

Auch der Ordner *DfsrPrivate* darf nicht manuell verändert werden!

Replikation für DFS-Ordner einrichten

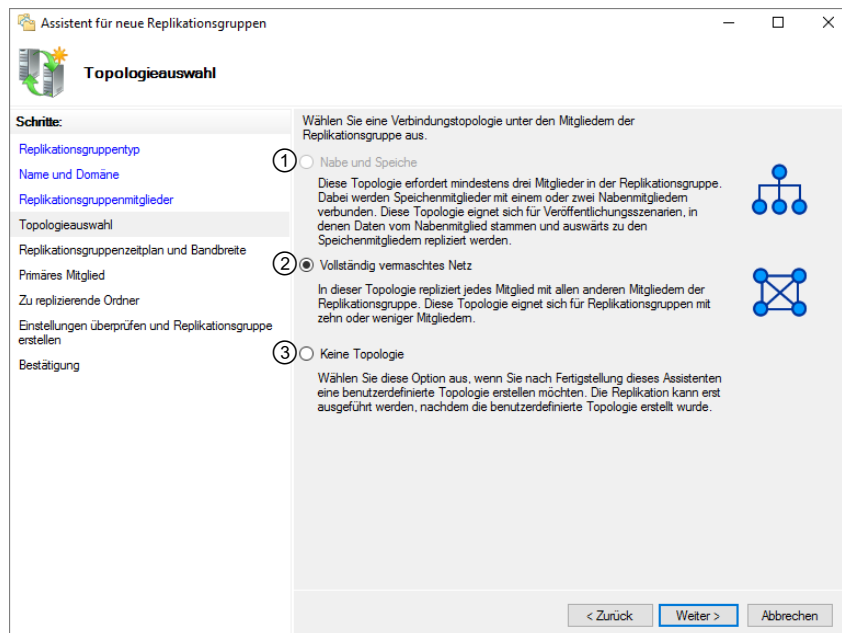
Die Replikation für DFS-Ordner richten Sie über einen Assistenten ein. Im folgenden Beispiel wurden im Name-space *Buchhaltung* dem Ordner *Betriebsanleitungen* zwei weitere Ordnerziele auf anderen Servern hinzugefügt.

- ▶ Markieren Sie alle Ordnerziele und klicken Sie im Bereich *Aktionen* auf *Ordner replizieren*.
Der Assistent für die Ordnerreplikation erscheint.
- ▶ Bei Bedarf verändern Sie den vorgeschlagenen Namen für den replizierten Ordner und die Replikationsgruppe. Klicken Sie auf *Weiter*.
- ▶ Prüfen Sie auf der zweiten Seite die Berechtigungen und klicken Sie auf *Weiter*.
Falls hier angezeigt wird, dass Ziele nicht hinzugefügt werden können, deutet dies auf Probleme mit DNS oder im Active Directory hin.
- ▶ Legen Sie nun das primäre Mitglied fest und klicken Sie auf *Weiter*.
Bei der ersten Replikation legt das primäre Mitglied den Inhalt des Ordners fest.

Bei *Nabe und Speiche* ① wird ein Server zur Nabe gemacht, mit der alle anderen Server (die Speichen) ihren Inhalt abgleichen. Replikationen zwischen den Speichen finden nicht statt. Diese Topologie erfordert mindestens drei Mitglieder.

Ein vollständig vermaschtes Netz ② bedeutet, dass sämtliche Server untereinander ihren Inhalt abgleichen. Diese Variante ist nur für kleinere Topologien bis 10 Mitglieder geeignet.

Mit *Keine Topologie* ③ müssen Sie nach der Erstellung der Ordnerreplikation die Topologie vollständig selbst erstellen. Dies ist nur in Ausnahmefällen sinnvoll.



- ▶ Wählen Sie die Topologie für die Ordnerreplikation aus und klicken Sie auf *Weiter*.

Replikationstopologie *Nabe und Speiche* einrichten

Diese Replikationstopologie erfordert mindesten drei Mitglieder und ermöglicht eine zentralisierte Verteilung der Daten. Sinnvoll ist das beispielsweise dann, wenn Sie mit mehreren Standorten arbeiten, die alle nur direkt mit der Zentrale kommunizieren können, aber nicht untereinander. Die Idee dahinter ist folgende:

- ✓ Sie definieren wenige Nabenmitglieder (eins bis drei), die ihre Inhalte untereinander replizieren.
- ✓ Sie definieren beliebig viele Speichenmitglieder, die ihren Inhalt zu einem oder zwei Nabenmitgliedern replizieren.
- ✓ Die Naben verteilen die Inhalte auf die Speichen.
- ▶ Legen Sie das Nabenmitglied fest, mit dem alle Server ihren Ordnerinhalt replizieren. Klicken Sie auf *Weiter*.

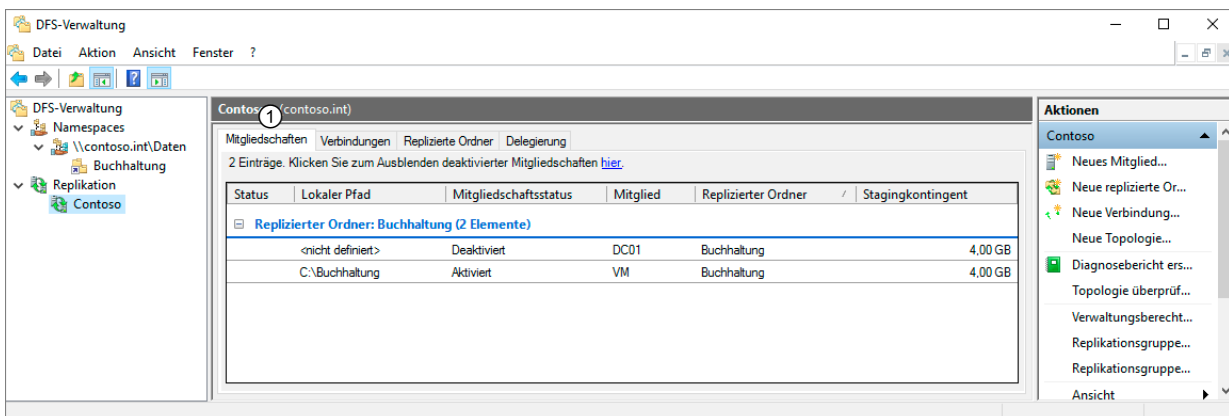
- ▶ Überprüfen Sie die Einstellungen für die Speichenmitglieder. Legen Sie bei Bedarf für jedes Speichenmitglied die Nabe und die optionale Nabe fest und klicken Sie auf *Weiter*.
- ▶ Legen Sie fest, welche Bandbreite die Replikation nutzen darf oder zu welchen Zeiten die Replikation stattfinden soll. Klicken Sie auf *Weiter*.
- ▶ Überprüfen Sie die Einstellungen in der Zusammenfassung und klicken Sie auf *Erstellen*.
- ▶ Die letzte Seite zeigt die Ergebnisse und eventuelle Fehler. Klicken Sie auf *Schließen*.

Damit haben Sie eine Replikationsgruppe erstellt, die im Knoten *Replikation* angezeigt wird und weiter konfiguriert werden kann.

- Beachten Sie, dass es im DFS keine sichere Versions- bzw. Konfliktverwaltung gibt. Wird zwischen zwei Replikationen eine Datei auf zwei unterschiedlichen Servern verändert, wird bei der nächsten Replikation die ältere Datei durch die neuere ersetzt. Die ältere Datei wird in den versteckten Ordner `\DfsPrivate\ConflictedAndDeleted` verschoben, auf den nur Administratoren Zugriff haben. Dieses Verzeichnis existiert in jeder Freigabe, die in eine DFS-Replikation eingebunden ist. Für Ordner, auf die viele Benutzer Schreibzugriff haben, ist die DFS-Replikation daher nur bedingt geeignet.

Replikationsgruppen verwalten

Replikationsgruppen verwalten Sie ebenfalls in der DFS-Verwaltung. Klicken Sie auf eine Replikationsgruppe, sehen Sie deren Einstellungen.

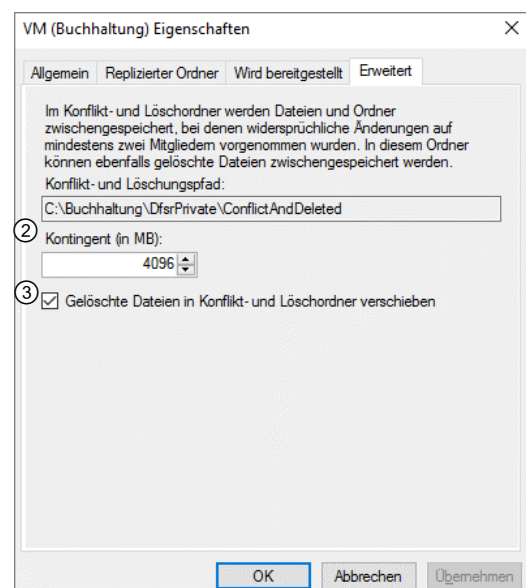


Die Registerkarte *Mitgliedschaften*

Im Register *Mitgliedschaften* ① sehen Sie in der DFS-Verwaltung genau, welcher lokale Ordner auf welchem Server zur Replikationsgruppe gehört. Über einen Rechtsklick können Sie die Eigenschaften eines Ordners bearbeiten.

Mit *Kontingent* ② legen Sie die Größe des Konflikt- und Löschornders fest, in den Dateien bei Replikationskonflikten verschoben werden. Sie können das Verschieben auch vollständig deaktivieren ③.

Auf der Registerkarte *Wird bereitgestellt* können Sie den Speicherort und die Größe des Staging-Ordners verändern. Voreingestellt ist der Ordner `\DfsPrivate\Staging` in der jeweiligen Freigabe mit einer Größe von 4096 MB. In diesem Ordner werden alle ausgehenden Replikationen zwischengespeichert. Er sollte groß genug sein, dass alle Veränderungen zwischen zwei Replikationen darin Platz finden.

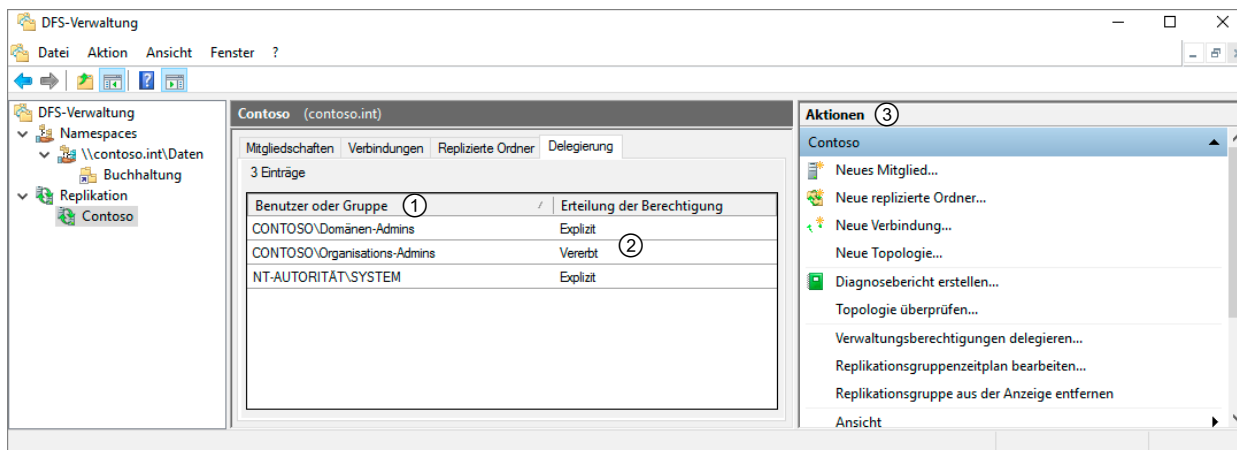


Die Registerkarte *Replizierte Ordner*

Im Register *Replizierte Ordner* sehen Sie den Namen des replizierten DFS-Ordners und seinen Namespacepfad und Veröffentlichungsstatus. Über einen Rechtsklick erreichen Sie die Eigenschaften des replizierten Ordners, wo Sie Filter definieren und damit Dateien oder Unterordner von der Replikation ausschließen können. Generell bietet es sich an, alle Einstellungen zu überprüfen, ob diese den Anforderungen entsprechen. Allerdings reichen die Standard-Einstellungen in den meisten Fällen aus.

Die Registerkarte *Delegierung*

Im Register *Delegierung* können Sie sehen, welche Gruppen oder Benutzer ① zur Verwaltung eines Namespaces berechtigt sind und ob diese Berechtigung vererbt oder explizit erteilt wurde ②. Im Bereich *Aktionen* ③ können Sie z. B. neue Verwaltungsberechtigungen delegieren und bestehende Delegierungen löschen.



Neue Replikationsgruppe erstellen

In der DFS-Verwaltung können Sie neue Replikationsgruppen erstellen.

- Klicken Sie in der linken Spalte mit der rechten Maustaste auf *Replikation* und wählen Sie *Neue Replikationsgruppe erstellen*. Alternativ geht das auch im Bereich *Aktionen*.

Der Assistent für neue Replikationsgruppen entspricht weitgehend dem Assistenten für die Ordnerreplikation, der oben beschrieben wurde. Der wesentliche Unterschied besteht darin, dass Sie jetzt die beteiligten Server angeben müssen und festlegen, welcher Quell-Ordner in welchen Ziel-Ordner repliziert wird. Bei diesen Ordnern muss es sich nicht um Freigaben handeln.

Wollen Sie z. B. einen zentralen Backup-Server realisieren, wählen Sie auf der ersten Seite des Assistenten *Replikationsgruppe für Datensammlung*. Auf den folgenden Seiten müssen Sie die Replikationsgruppe benennen, den Quell-Server und die zu replizierenden Ordner angeben, den Ziel-Server festlegen und angeben, in welche Ziel-Ordner dort repliziert wird, und die Bandbreite bzw. den Zeitplan festlegen. Der erstellten Replikationsgruppe können Sie im Anschluss weitere Mitglieder hinzufügen.

Alle Mitglieder einer Replikationsgruppe müssen Mitglied derselben Domäne sein.

Mit DFS-Stamm verbinden

- Öffnen Sie den Windows-Explorer.
- Verknüpfen Sie ein Netzlaufwerk mit der Freigabe \\<Domänenname>\<Namespace>, z. B. \\unserefirma.intern\buchhaltung.

Sie sehen anschließend die freigegebenen Ordner, die Sie im Namespace angelegt haben. Dabei ist für den Benutzer nicht erkennbar, auf welchen Server er damit zugreifen würde.

Benötigen Sie nur kurzen Zugriff, können Sie diese Angabe auch im Adressfeld eingeben.

Netzlaufwerksverknüpfungen können Sie auch über die Kommandozeile erstellen:

```
net use <Laufwerksbuchstabe> <UNC-Pfad>\<Ordner>
```

z. B. `net use Y: \\Firma.Intern\Buchhaltung`

Der Befehl `net use` kennt weitere Schalter, die Sie mit `net use /?` anzeigen können. Schauen Sie bei dieser Gelegenheit nach, was der Befehl `net` sonst noch alles kann. Der Befehl kann sich für Ihre selbst erstellten Batchdateien als sehr nützlich erweisen.



Beachten Sie, dass bei der Angabe von Freigabenamen zwischen Groß- und Kleinbuchstaben unterschieden wird. Dies gilt sowohl für den Explorer als auch für den Kommandozeilenbefehl. Wenn Sie also keine Freigabenamen wie *bUchhAltUnG* (*\\fRmA.iNtErn*) wünschen, achten Sie sorgfältig auf die Schreibweise.

14.6 Datenträger und Speicherpools

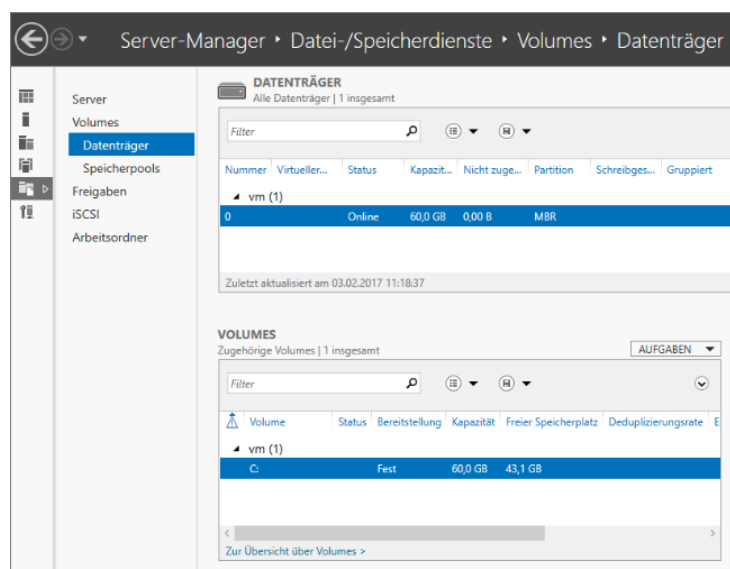
Überblick

Mit Windows Server 2012 wurden als eine wichtige Neuerung die Speicherpools eingeführt. In Windows Server 2022 können Sie diese im Cluster sogar auf verschiedene Clusterknoten ausdehnen. Bei einem Speicherpool handelt es sich um einen Verbund von Speichermedien, die vom System wie ein klassischer Datenträger (Festplatte oder RAID) angesprochen werden. Dabei können unterschiedliche Datenträger im Mix eingesetzt werden, der logische und der physische Speicherort werden dabei komplett voneinander getrennt. Sie könnten z. B. neben eingebauten Festplatten und SSDs auch USB-Medien, iSCSI-Laufwerke und NAS in einem Speicherpool zusammenfassen.

Datenträger

Unter Datenträgern versteht Microsoft in diesem Zusammenhang die folgenden Speichermedien:

- ✓ **Klassische Festplatten.** Diese stellen aufgrund der Kosten-Nutzen-Relation den Großteil der Datenträger in heutigen Serversystemen dar. Über welchen Anschluss die Festplatten dabei mit dem System verbunden sind, spielt eine untergeordnete Rolle. Infrage kommen interne Bus-Systeme wie SAS oder SATA ebenso wie externe Anschlüsse wie eSATA, USB oder iSCSI.
- ✓ **Solid State Discs (SSD).** Die SSD speichert Daten nicht mehr als magnetische Information auf einer rotierenden Scheibe (wie die Festplatte), sondern in Chips, ähnlich einem USB-Stick. Dies hat die Vorteile, dass die Informationen deutlich schneller abgerufen werden können und der klassischen Fragmentierung eine geringere Rolle zukommt. Dem gegenüber stehen der deutlich höhere Preis und die bisher geringen Erfahrungen zur langfristigen Zuverlässigkeit.



- ✓ **USB-Stick.** Auch USB-Sticks werden unterstützt, was gerade hinsichtlich der Lese-Schreib-Performanz auf älteren Servern eine interessante Option darstellt, da mit nachrüstbaren USB 3.0-Controllern so eine schnelle Schnittstelle geschaffen werden kann, um Zugriffe auf häufig benötigte Daten zu optimieren.

Speicherpool

Ein **Speicherpool** ist ein Verbund von einem oder mehr Datenträgern, die zu einem gemeinsamen Speicherplatz zusammengefasst werden. Die Datenträger können dabei unterschiedliche Größe und Geschwindigkeit aufweisen, das System wird eine Optimierung zur Ausnutzung vornehmen. So können Sie z. B. festlegen, dass häufig verwendete Daten automatisch auf SSDs abgelegt werden.

Windows Server 2022 bietet weiterhin die Speicherpools. Einfach ausgedrückt fassen Sie mehrere, physische Datenträger zusammen und konfigurieren diese als einen gemeinsamen, virtuellen Datenträger. In Windows Server 2022 hat Microsoft die Funktionen erweitert und verbessert, zum Beispiel die Unterstützung für SSD-/NVMe-Festplatten sowie der Möglichkeit, in einem Cluster alle lokalen Festplatten der Clusterknoten zu einem Storage Space Direct zusammenzufassen.

Speicherpools werden über den Server-Manager verwaltet. Hier legen Sie zunächst einen Speicherpool an und weisen diesem anschließend verschiedene Speicherplätze zu. Dabei handelt es sich um die Volumes, auf denen Sie wiederum Freigaben erstellen. Ein Pool kann mehrere Speicherplätze, auch virtuelle Festplatten genannt, umfassen. Speicherplätze bestehen in Windows Server 2022 also aus virtuellen Festplatten, die Speicherpools zugewiesen sind. Die Speicherpools nutzen wiederum die zugrundeliegenden, physischen Festplatten.

Im ersten Schritt werden physische Datenträger zu einem Speicherpool zusammengefasst, auf dem dann ein virtueller Datenträger (ähnlich einer Partition) erstellt wird.

Je nach verwendeten physischen Datenträgern werden dabei auch verschiedene an RAID (**R**edundant **A**rray of **I**ndependent **D**isks) angelegte Betriebsarten unterstützt. Wenn Sie nur SSDs verwenden, werden keine RAID-Level unterstützt. Verwenden Sie dagegen klassische Festplatten oder eine Mischung aus diesen und SSDs, so können Sie die folgenden RAID-Level einsetzen:

- ✓ **Simple:** Hierbei handelt es sich um einen einfachen Datenträger, der im Prinzip einem übergreifenden Volume entspricht. Redundanz bietet dieser nicht.
- ✓ **Mirror:** Der Spiegelsatz entspricht einem RAID-1. Sämtliche Daten werden auf zwei Speicher gleichzeitig geschrieben.
- ✓ **Parity:** Dies entspricht einem RAID-5, bei dem mindestens drei physische Datenträger verwendet werden müssen. Neben den verteilten Informationen werden die Paritätsinformationen auf einen zusätzlichen Datenträger geschrieben. So kann bei Ausfall von einem Datenträger (Parity mit mindestens drei Datenträgern) oder zwei Datenträgern (mindestens sieben physische Datenträger) trotzdem noch auf die Daten zugegriffen werden, ohne gleich die doppelte Menge an Speicherplatz zu verwenden, wie beim Mirror.

Laut Microsoft ist der Einsatz von Speicherpools und virtuellen Datenträgern der Verwendung von Hardware-RAIDs vorzuziehen. In kleineren Firmen kann die Einbindung von zusätzlichen Speichermedien über USB oder iSCSI eine interessante Option darstellen, wenn der fest verbaute Speicherplatz zur Neige geht und keine weiteren Schnittstellen existieren.

Ausführliche Informationen zum Einrichten und der Verwaltung von Speicherpools finden Sie in Kapitel 20.6.

15 Drucker verwalten

15.1 Drucken im Netzwerk

Bezeichnungen und Begriffe

Microsoft verwendet seit Jahren die gleiche Bezeichnungsweise rund um das Drucken. Als Systembetreuer sollten Sie diese Windows-Terminologie kennen und durchgehend verwenden, auch wenn viele Benutzer dies nicht tun.

Druckgeräte

Druckgeräte sind physikalische **Geräte**, die den eigentlichen Druckvorgang ausführen.

Netzwerkfähige Druckgeräte sind eigenständige Druckgeräte, die über eine Netzwerkschnittstelle verfügen. Sie können im Netzwerk direkt angesprochen werden und übernehmen oft die Funktion eines Druckservers mit eigener Druckerwarteschlange. **Lokal angeschlossene Druckgeräte** sind am weitesten verbreitet. Sie werden häufig über USB mit dem Computer verbunden.

Drucker

Drucker sind das, was Sie während der Druckerinstallation erstellen und einrichten und was daraufhin in *Geräte und Drucker* zu sehen ist. Drucker sind **Softwareschnittstellen** zwischen dem Dokument und dem Druckgerät.

Der Drucker umfasst alle notwendigen Treiber für ein bestimmtes **Druckgerät** und stellt eine eigene Druckerwarteschlange zur Verfügung.

Lokale Drucker sind Drucker, deren Treiber lokal installiert wurden und die eine lokale Druckerwarteschlange zur Verfügung stellen. Wo das dazugehörige Druckgerät steht, ist dabei unerheblich.

Der Spooler-Dienst

Spooling ist die englische Bezeichnung für das Zwischenspeichern von Druckaufträgen in einer Spool-Datei und die Verteilung der Aufträge an die lokal installierten Drucker. Bei Windows heißt dieser Dienst **Druckwarteschlange** oder **Spooler**. Der Spooler wertet dabei die Priorität der Drucker aus und gibt den Druckern mit höherer Priorität beim Zugang zum Druckgerät den Vorzug. Dadurch können auch später hinzugefügte wichtige Druckaufträge früher ausgedruckt werden als bereits in der Warteschlange vorhandene Aufträge mit geringerer Priorität. Wenn der Spooler ausfällt oder hängt, kann nicht mehr gedruckt werden.

Die Druckerwarteschlange (Queue)

Unter Windows werden Druckaufträge standardmäßig in eine Druckerwarteschlange gestellt, aus der sie vom Drucker an das Druckgerät weitergeleitet werden. Alle auf einem Computer installierten Drucker verfügen über eine eigene Warteschlange, die vom Spooler-Dienst aus dem zentralen Spoolordner gespeist wird. Diese Zwischenspeicherung sorgt dafür, dass Druckaufträge auch dann an einen Drucker gerichtet werden können, wenn das Druckgerät gerade beschäftigt oder ausgeschaltet ist.

Druckdienste im Netzwerk

Als **Netzwerkdrucker** werden Drucker bezeichnet, auf deren Druckerwarteschlange über das Netzwerk zugegriffen werden kann. Die Warteschlange befindet sich dabei nicht auf dem Computer, von dem der Druckauftrag stammt, sondern auf dem Remotecomputer oder im Druckgerät selbst. Es ist unwichtig, auf welche Weise die dazugehörigen Druckgeräte an den Computer angeschlossen sind und an welchem Ort sie sich befinden.

Druckserver sind Computer, deren Aufgabe die Bereitstellung von Druckern im Netzwerk ist. Sie sorgen durch ihre zentrale Verwaltung der Druckerwarteschlangen für eine effizientere Nutzung der Druckgeräte. Bei hohem Druckaufkommen wird dabei erhebliche Prozessor-, Festplatten- und Speicherkapazität belegt. Der Druckserver muss stets eingeschaltet sein, um die Druckdienste zur Verfügung zu stellen. Bei Windows-Serverbetriebssystemen ist der Druckserver ein Rollendienst der Serverrolle *Druck- und Dokumentdienste*.

LPR-Drucker (Line-Printer-Remote) werden vom System als lokale Drucker behandelt, die Ausgabe wird jedoch auf einen zentralen Druckserver umgeleitet. Sie finden sich vor allem in großen Rechenzentren mit UNIX-Servern, auf denen das Server-Gegenstück, der Line Printer Daemon (LPD), läuft.

Druckerpools müssten eigentlich Druckgerätepools heißen, denn es handelt sich hier tatsächlich um eine Ansammlung funktionsgleicher **Druckgeräte**, die über einen einzigen Drucker angesteuert werden.

Zusammenfassung aller Begriffe:

Drucker	Softwareschnittstelle, besteht aus Treibern und Druckerwarteschlange
Druckgerät	Hardware
Netzwerkfähiges Gerät	Druckgerät mit Netzwerkschnittstelle
Lokal angeschlossenes Gerät	Druckgerät wird über USB (und teilweise auch noch parallel) direkt am Computer angeschlossen
Lokaler Drucker	Drucker mit lokaler Druckerwarteschlange
Spooler (Druckerwarteschlange)	Windows-Dienst zur Verwaltung aller Druckerwarteschlangen
Druckerwarteschlange	Liste der Druckaufträge eines Druckers
Netzwerkdrucker	Druckerwarteschlange wird über das Netzwerk freigegeben
Druckserver	Computer, der Druckdienste im Netzwerk bereitstellt
LPR-Drucker	UNIX-Druckerserver zur Ausgabe von Druckaufträgen über das Netzwerk
Druckerpool	Baugleiche Druckgeräte, die über einen Drucker angesprochen werden

Geräte und Drucker

Im Ordner *Geräte und Drucker* finden Sie Informationen zur Konfiguration und zum Status der verfügbaren Drucker. Jedes Druckersymbol stellt eine Druckerwarteschlange dar und offenbart bestimmte Eigenschaften des Druckers.

- Zeigen Sie alle installierten Drucker an, indem Sie in der Systemsteuerung auf *Geräte und Drucker* klicken.

Häkchen im grünen Kreis	Für den aktuellen Benutzer wurde dieser Drucker als Standarddrucker definiert.
Icon mit Benutzerpiktogrammen neben dem Drucker	Der Drucker ist im Netzwerk freigegeben und andere Benutzer können darauf drucken.
Netzwerkabel unter dem Drucker <Druckername> an <Computername>	Dieser Drucker wurde auf einem anderen Rechner freigegeben und von diesem Rechner wurde eine Verbindung zu ihm aufgebaut. Die Bezeichnung zeigt ebenfalls, dass der Drucker an einem anderen Computer freigegeben wurde.

15.2 Drucker installieren

Lokal angeschlossenes Druckgerät automatisch erkennen und installieren

Alle Druckgeräte der letzten Jahre beherrschen Plug & Play, daher werden sie sofort beim Anschließen erkannt und installiert, wenn ein Treiber vorhanden ist. Sie können diesen Vorgang aber auch manuell ausführen:

- ▶ Klicken Sie in *Geräte und Drucker* auf *Geräte und Drucker hinzufügen*.
Windows sucht daraufhin nach Geräten mit Plug & Play. Wenn ein passender Treiber vorhanden ist, wird er installiert.
- ▶ Sollte Windows Server 2022 die Treiber nicht finden, legen Sie die Treiber-CD ein (falls vorhanden) oder suchen Sie auf Ihrem Computer oder im Internet nach dem passenden Treiber.
Falls es für Windows Server 2022 keine Treiber gibt, suchen Sie nach einem 64-Bit-Treiber (x64) für Windows 11, 10 oder 8.1, dann erst nach Treibern für Windows 7 oder Vista usw.
- ▶ Wählen Sie im Assistenten z. B. den Namen des Druckers und Freigabeeinstellungen. Drucken Sie auf Wunsch eine Testseite.
- ▶ Stellen Sie den Assistenten fertig.

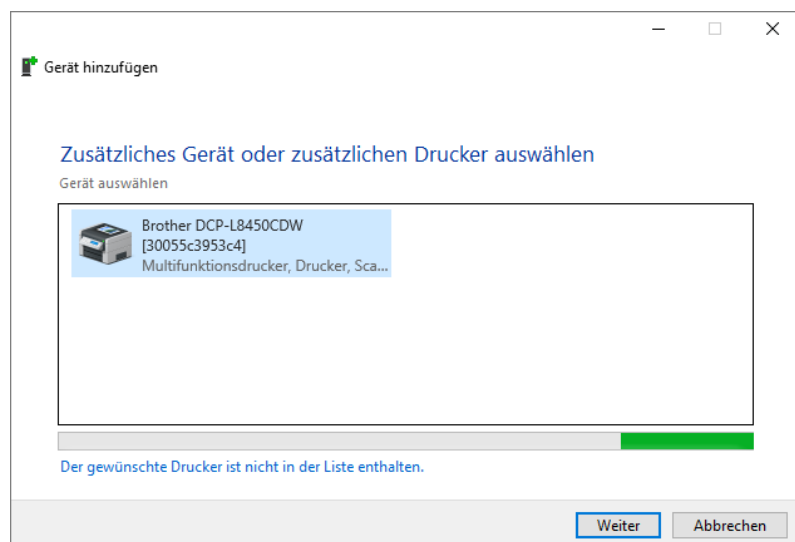
Der Drucker ist nun fertig eingerichtet und kann benutzt werden. Sie finden das Symbol für den installierten Drucker im Druckerordner. Wenn es sich um den ersten Drucker auf diesem Rechner handelt, wird er automatisch als Standarddrucker festgelegt.

Die Windows-Installation benötigt den Pfad zur INF-Datei. Das bedeutet, dass Sie so gut wie alle Treiber aus dem Internet erst entpacken müssen, da es sich oft um selbstentpackende Setup-Programme handelt. Bei solchen ausführbaren Dateien ist es einfacher, sie direkt auszuführen und den Windows-Assistenten nicht zu verwenden.

Lokalen Drucker ohne Plug & Play installieren

Wenn das Druckgerät nicht automatisch erkannt wurde, beherrscht es kein Plug & Play und muss von Hand eingerichtet werden:

- ▶ Klicken Sie in *Geräte und Drucker* auf *Drucker hinzufügen*.
Der Assistent sucht nun lokal und im Netzwerk nach verfügbaren Druckern.
- ▶ Wählen Sie den Drucker aus und klicken Sie auf *Weiter*.
Daraufhin öffnet sich der Dialog zur Auswahl des Druckertreibers.
- ▶ Falls der Drucker nicht angezeigt wird, klicken Sie auf *Der gesuchte Drucker ist nicht aufgeführt*.
Es öffnet sich der Dialog, mit dem Sie im Netzwerk nach Druckern suchen können: *Der gewünschte Drucker ist nicht in der Liste enthalten*.

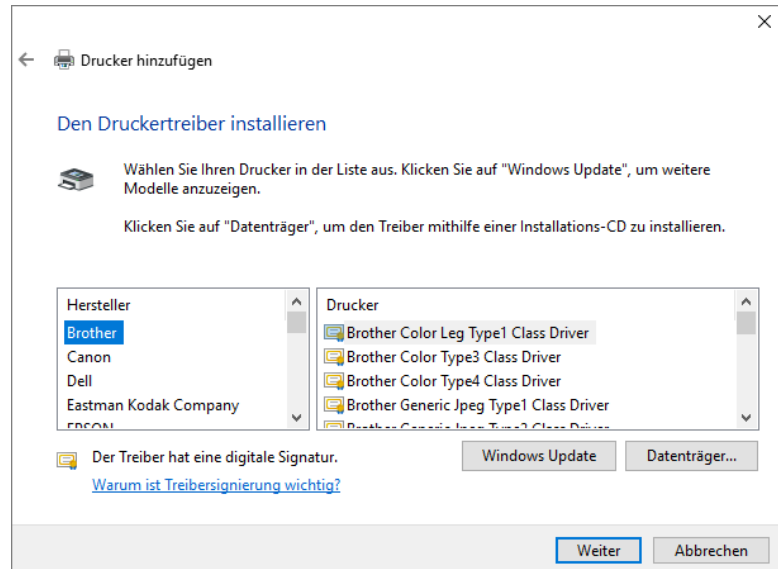


Druckersuche

Druckertreiber auswählen und Einrichtung abschließen

Die hier beschriebenen Schritte gelten für die Einrichtung von Druckgeräten, die nicht automatisch erkannt wurden. Hier können Sie manuell den Treiber auswählen und die Druckereinrichtung abschließen.

- ▶ Klicken Sie auf *Windows Update*, um die Treiberdatenbank zu aktualisieren.
- ▶ Wählen Sie den Hersteller und Druckertyp aus.
- ▶ Falls der Treiber nicht aufgeführt ist, klicken Sie auf *Datenträger*, um auf Ihrem Computer die INF-Datei des Treibers zu öffnen.
- ▶ Klicken Sie auf *Weiter*.
- ▶ Wählen Sie einen Namen für den Drucker und klicken Sie auf *Weiter*.
- ▶ Wählen Sie, ob der Drucker freigegeben werden soll, und geben Sie, wenn ja, einen Freigabenamen ein.
- ▶ Machen Sie optional über ein Optionsfeld den Drucker zum Standarddrucker für den angemeldeten Benutzer.
- ▶ Schließen Sie den Assistenten ab, indem Sie die Schaltfläche *Fertig stellen* betätigen.

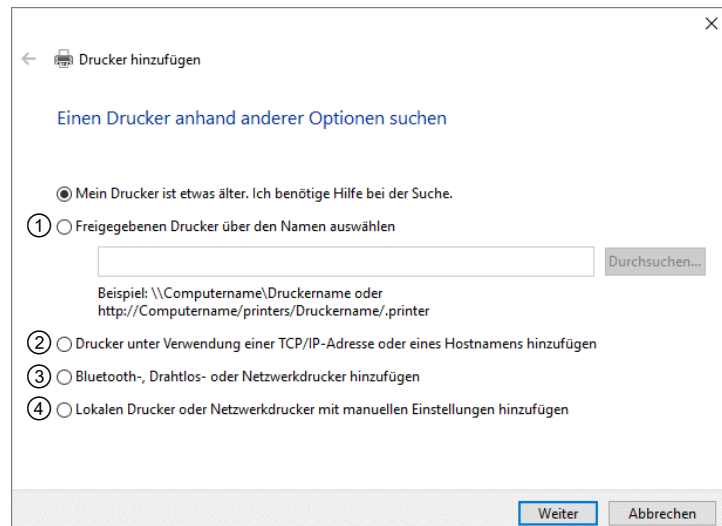


Druckerhersteller und Druckertyp auswählen

Einen Drucker anhand anderer Optionen suchen

Hier können Sie Drucker einrichten, die nicht automatisch gefunden werden konnten.

- ▶ Wählen Sie aus, welche Art von Drucker oder Druckgerät Sie einrichten wollen: einen im Netzwerk freigegebenen Drucker ①, einen Netzwerkdrucker bzw. ein netzwerkfähiges Druckgerät mit eigener IP-Adresse ②, ein Plug-&-Play-fähiges Gerät ③ oder einen Drucker, bei dem Sie sämtliche Einstellungen per Hand vornehmen ④.
- ▶ Wählen Sie eine Option und klicken Sie auf *Weiter*.

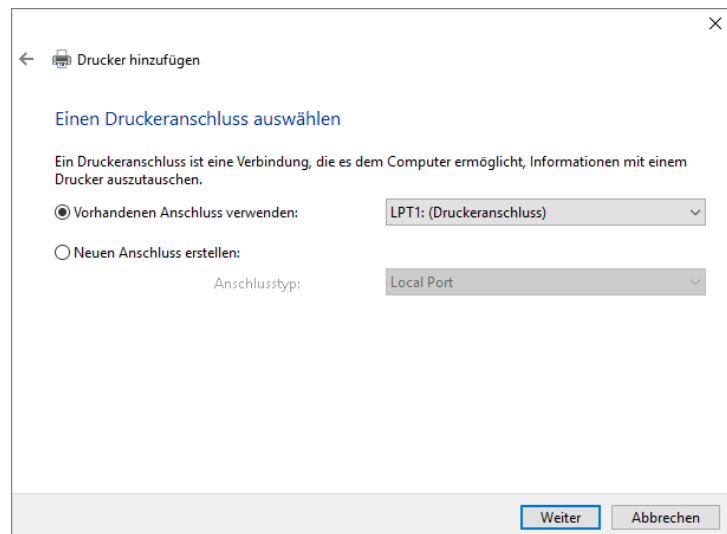


Art des Druckers auswählen

Druckeranschluss einstellen

Für den neuen Drucker müssen Sie einen bestehenden Druckeranschluss festlegen oder einen neuen Anschluss erstellen.

- ▶ Bei einem lokal angeschlossenen Druckgerät geben Sie den Port an, an dem der Drucker angeschlossen wird.
- ▶ Bei einem netzwerkfähigen Druckgerät aktivieren Sie im Listenfeld *Typ* die Einstellung *Standard TCP/IP Port*.
Im folgenden Dialog können Sie die Netzwerkeigenschaften des Druckers, die IP-Adresse und das verwendete Protokoll festlegen.
- ▶ Klicken Sie nach Auswahl des Druckeranschlusses auf *Weiter*.
Es öffnet sich der Dialog zur Treiber-
auswahl.

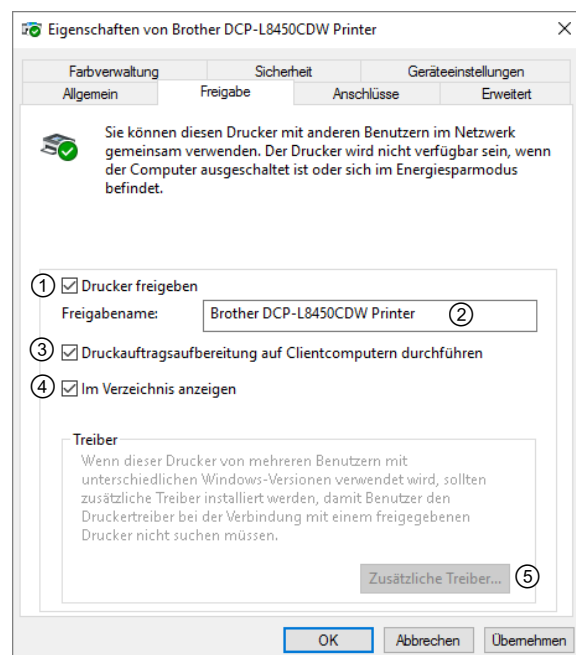


Druckeranschluss auswählen

Drucker freigeben

- ▶ Klicken Sie in der Systemsteuerung auf *Geräte und Drucker*.
- ▶ Klicken Sie im Kontextmenü des freizugebenden Druckers auf *Druckereigenschaften*.
- ▶ Wechseln Sie in das Register *Freigabe*.
- ▶ Aktivieren Sie das Optionsfeld *Drucker freigeben* ① und geben Sie einen Freigabennamen ein ②.
- ▶ Aktivieren Sie die Option *Im Verzeichnis anzeigen* ④, damit Sie den Drucker über das AD verwalten können und Benutzer anhand des Standorts und der Druckfunktion danach suchen können.
Über die Option *Zusätzliche Treiber* ⑤ können Sie Treiber für andere Windows-Versionen bereitstellen.
- ▶ Bestätigen Sie Ihre Eingaben mit *OK*.

Wenn Sie die Option ③ aktiviert lassen, wird der Druckserver entlastet. Um die Freigabe wieder zu beenden, deaktivieren Sie das Optionsfeld *Drucker freigeben*.



LPR-Drucker einrichten

Um einen LPR-Drucker (UNIX-Netzwerkdrucker) einrichten zu können, muss das Feature **LPR-Portmonitor** installiert werden.

- ▶ Starten Sie im Server-Manager den Assistenten zum Hinzufügen von Rollen und Features und fügen Sie auf der Seite *Features auswählen* den **LPR-Portmonitor** hinzu.
- ▶ Beginnen Sie die Installation genauso wie für ein lokal angeschlossenes Druckgerät ohne Plug-&-Play-Erkennung.
- ▶ Wählen Sie im Dialogfenster *Einen Druckeranschluss auswählen* das Optionsfeld *Neuen Anschluss erstellen* und markieren Sie im Listenfeld *Anschlusstyp* den Eintrag **LPR Port**.

- ▶ Geben Sie den DNS-Namen oder die IP-Adresse des Rechners ein, auf dem der Line Printer Daemon (LPD) läuft, und geben Sie den Namen des Druckers oder der Druckerwarteschlange ein.
- ▶ Folgen Sie den Anweisungen des Assistenten und schließen Sie die Installation ab.

Nach diesen Maßnahmen steht der Drucker im Netzwerk zur Verfügung. Damit sich dieser auf Clientcomputern verbinden lässt, ist der einfachste Weg die Zeichenfolge `\\<Server-Name des Drucker-Hosts>\<Name der Drucker-freigabe>`. Den Drucker sehen Sie auch im Explorer, wenn Sie auf Netzwerk klicken. Ist der Drucker nicht sofort ersichtlich, klicken Sie auf den Namen des Computers, der den Drucker zur Verfügung stellt.

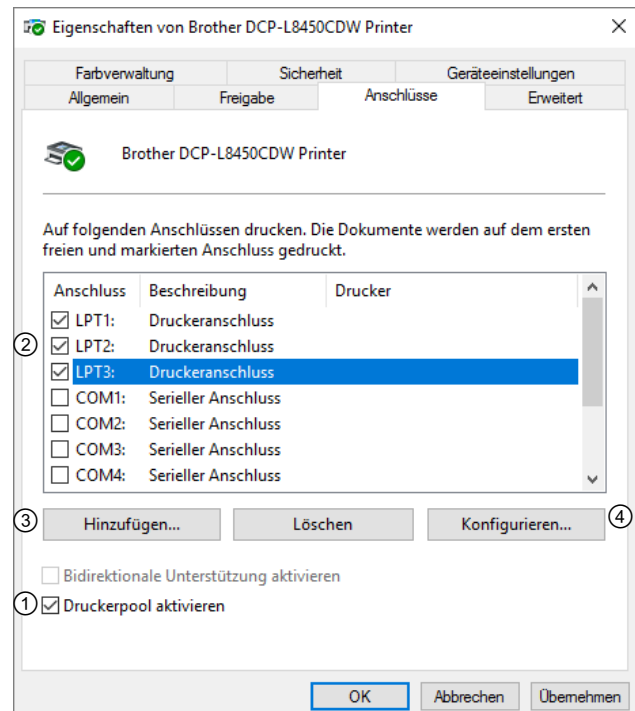
Druckerpool einrichten

Wenn Sie mehrere identische Druckgeräte lokal an einen Druckserver anschließen, können Sie diese über einen einzigen Drucker ansprechen, indem Sie den **Druckerpool** aktivieren. Wenn nun mehrere Aufträge an diesen Drucker geschickt werden, vergibt der Druckserver den ersten Auftrag an das erste freie Druckgerät, den nächsten Auftrag an das nächste freie Gerät und so weiter.

- ▶ Öffnen Sie *Geräte und Drucker*.
- ▶ Installieren Sie den Drucker.
- ▶ Klicken Sie nach Abschluss der Installation im Kontextmenü dieses Druckers auf *Druckereigenschaften*.
- ▶ Wechseln Sie in das Register *Anschlüsse* und aktivieren Sie das Kontrollfeld *Druckerpool aktivieren* ①.

Nun können Sie in der Spalte *Anschluss* alle Ports auswählen, an denen die baugleichen Druckgeräte angeschlossen sind ②. Sie können weitere Anschlüsse hinzufügen ③ oder vorhandene Anschlüsse konfigurieren ④.

- ▶ Bestätigen Sie Ihre Eingabe mit *Übernehmen* und *OK*.



Oft ist es möglich, nicht nur baugleiche, sondern auch ähnliche Geräte eines Herstellers in einem Pool zu vereinen, wenn Sie den Treiber bzw. Funktionsumfang des kleinsten Gerätes verwenden.

Sie können Einstellungen von Druckern in der PowerShell anpassen. Dazu verwenden Sie das CMDlet `Set-PrinterConfiguration`. Ein Beispiel wäre das Anpassen der Papiergröße von Druckaufträgen. Im Gegensatz zur grafischen Oberfläche können Sie z. B. für alle Drucker auf einem Druckserver die Papiergröße auf einmal festlegen: `Get-Printer | Set-PrintConfiguration -PaperSize A4`.

Zusätzlich zu `Set-PrinterConfiguration` gibt es aber auch die Möglichkeit, Informationen anzuzeigen. Dazu verwenden Sie das CMDlet `Get-PrinterConfiguration`.

Auch dieses können Sie mit `Get-Printer` verknüpfen, um sich zum Beispiel die Papiergröße der Drucker auf dem Server anzuzeigen: `Get-Printer | Get-PrintConfiguration | ft PrinterName, PaperSize`.

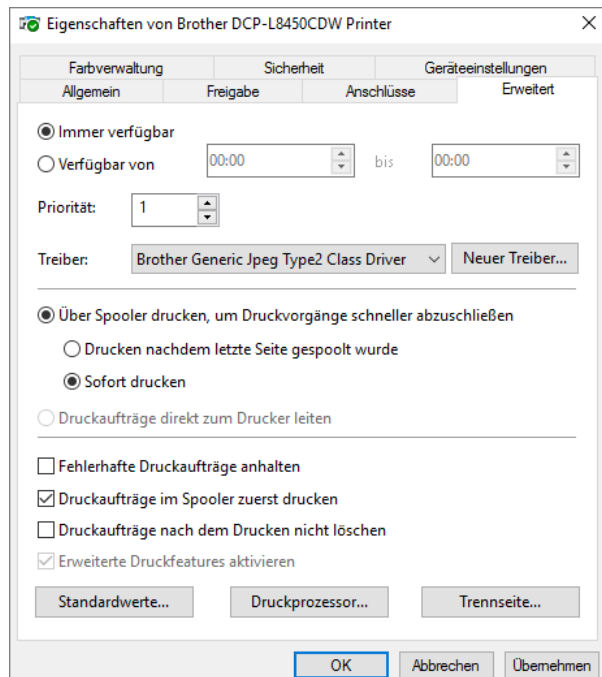
15.3 Drucker konfigurieren

Druckertreiber für den lokalen Drucker aktualisieren

- ▶ Öffnen Sie im Kontextmenü des Druckers den Menüpunkt *Druckereigenschaften*.
- ▶ Wechseln Sie in das Register *Erweitert*.

Der aktuell verwendete Druckertreiber wird im Listenfeld *Treiber* angezeigt. Er kann folgendermaßen aktualisiert werden:

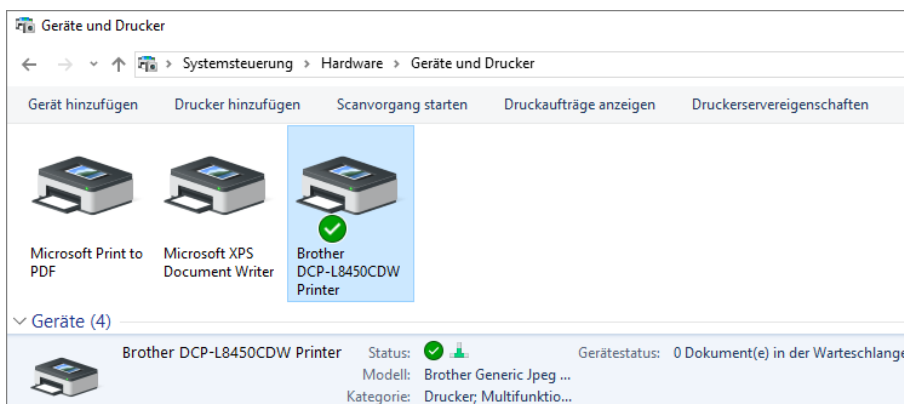
- ▶ Klicken Sie auf *Neuer Treiber*.
Der Assistent für die Druckertreiberinstallation wird geöffnet.
- ▶ Klicken Sie in einem der folgenden Dialogfenster auf *Datenträger* und wählen Sie den Speicherort der INF-Datei des neuen Druckertreibers aus.
- ▶ Folgen Sie den Anweisungen des Assistenten.



Lokalen Druckertreiber aktualisieren

Druckertreiber für den Druckserver aktualisieren

- ▶ Öffnen Sie den Geräte- und Druckerordner und klicken Sie zuerst auf einen installierten Drucker und dann auf *Druckerservereigenschaften*.



Druckerservereigenschaften bearbeiten

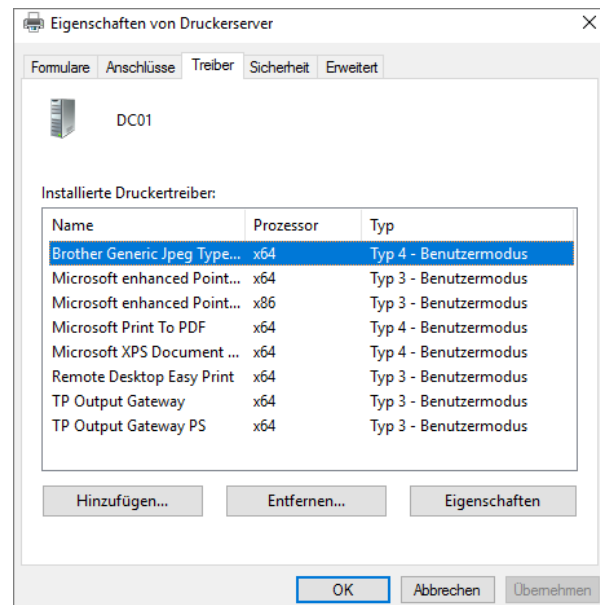
- ▶ Wählen Sie das Register *Treiber*.

Druckertreiber für andere Betriebssysteme hinzufügen

Es ist unter Windows Server 2022 möglich, für freigegebene Drucker die Treiber für andere Windows-Versionen und Plattformen zentral verfügbar zu machen und so den Clients im Bedarfsfall die Installation der Treiber vom Druckerserver aus zu ermöglichen. Es können Treiber für alle modernen Windows-Versionen in 32 Bit oder 64 Bit hinterlegt werden.

- ▶ Betätigen Sie die Schaltfläche *Hinzufügen*.
Windows Server 2022 startet den Assistenten für die Druckertreiberinstallation.
- ▶ Aktivieren Sie die Kontrollfelder der Prozessorplattformen x86 und x64, für die Sie Treiber zur Verfügung stellen wollen.
- ▶ Wählen Sie den passenden Treiber aus wie bei einer normalen Treiberinstallation.
- ▶ Wiederholen Sie den Vorgang, falls Sie beide Plattformen angewählt haben.
- ▶ Schließen Sie die Installation der Druckertreiber mit einem Klick auf *Fertig stellen* ab.

Windows wird Sie gegebenenfalls nach Datenträgern fragen, auf denen sich die Druckertreiber befinden. Geben Sie hier den Pfad zur INF-Datei an. Gegebenenfalls müssen Sie dazu das Treiberpaket entpacken. Auf einem x64-System können Sie die Windows-Treiber für x86 von einem 32-Bit-Windows-Installationsmedium entnehmen und umgekehrt.



Auf dem Druckserver installierte Treiber

- ! Die Druckerbezeichnung muss in den INF-Dateien für x86 und x64 **identisch** sein, sonst erkennt Windows nicht, dass es sich um denselben Drucker handelt. Ändern Sie gegebenenfalls die Bezeichnung.

Standarddrucker festlegen

- ▶ Klicken Sie in *Geräte und Drucker* mit der rechten Maustaste auf einen Drucker und wählen Sie im Kontextmenü den Menüpunkt *Als Standarddrucker festlegen*.

Standarddruckeinstellungen für alle Benutzer definieren

Für alle Benutzer kann eine Standarddruckkonfiguration festgelegt werden.

- ▶ Öffnen Sie *Geräte und Drucker* und wählen Sie im Kontextmenü des Druckers, den Sie bearbeiten möchten, den Menüpunkt *Druckeinstellungen*.
- ▶ Klicken Sie im Register *Erweitert* auf *Standardwerte*.
Im folgenden Dialog können Sie die Einstellungen für die Orientierung des Ausdrucks, die Seitenreihenfolge und die Anzahl der Seiten pro Blatt festlegen.

Sie können weiterhin den Einzugsschacht des Druckgeräts oder die Papierart bestimmen.

Standortunabhängiges Drucken

Standortunabhängiges Drucken ermöglicht durch die Standorterkennung über die Netzwerk-ID, dass Druckaufträge automatisch an einen nahegelegenen Drucker gesendet werden.

Wenn die Funktion aktiv ist, erscheint im Geräte- und Druckerordner ein zusätzlicher Menüpunkt *Standarddrucker verwalten*. Sie können mithilfe dieses Menüs entscheiden, welcher Drucker für Ihr Notebook der Standarddrucker sein soll, abhängig davon, in welchem Netzwerk Sie sich gerade aufhalten.

15.4 Druckerwarteschlange verwalten

Druckerwarteschlange konfigurieren

Alle eingehenden Druckaufträge werden als Datei im Spoolordner abgelegt. Alle Druckaufträge aus allen Druckerwarteschlangen werden dabei in einer einzigen Druckwarteschlange (dem Spooler) zusammengefasst und in einer Datei gespeichert. Sobald diese Spooldatei erstellt ist, kann die Anwendung, die den Ausdruck angefordert hat, wieder benutzt werden. Die Ausgabe des Druckauftrags an den Drucker erfolgt im Hintergrund, während der Benutzer schon wieder mit der Anwendung arbeitet. Der Spooler-Dienst ordnet sie den jeweiligen Druckerwarteschlangen zu und sortiert die Aufträge nach ihrer Priorität.

Druckaufträge können auch dann in die Warteschlange gestellt werden, wenn das Druckgerät nicht angeschlossen, nicht eingeschaltet oder deaktiviert (offline) ist. Wenn Sie den Drucker in den Eigenschaften der Druckerwarteschlange auf offline geschaltet haben, werden die Druckaufträge gespeichert und ausgeführt, sobald Sie ihn wieder als online festgelegt haben.

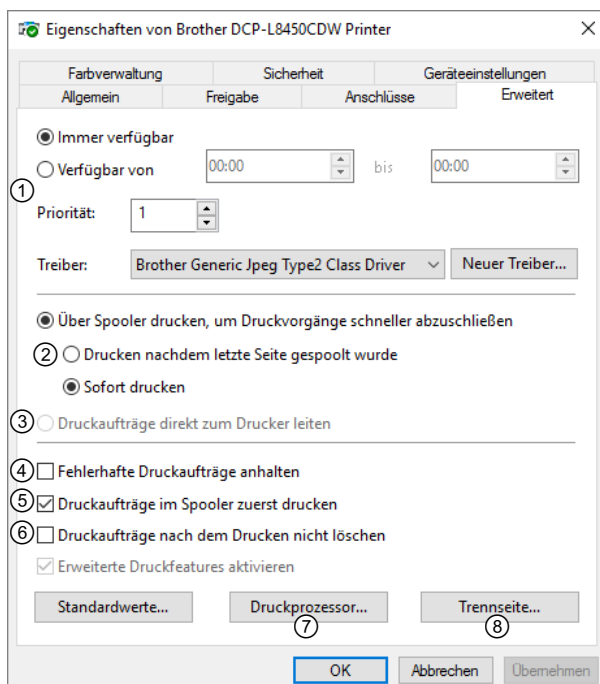
Druckerwarteschlange beeinflussen

Die Standardeinstellungen von Windows Server 2022 für die Druckerwarteschlangen sind für die meisten Anforderungen geeignet und müssen nicht geändert werden, Sie können jedoch für jeden installierten Drucker detaillierte Einstellungen vornehmen:

- ▶ Klicken Sie im Kontextmenü des Druckers, den Sie bearbeiten möchten, auf *Druckereigenschaften*.
- ▶ Wechseln Sie in das Register *Erweitert*.

Hier können Sie z. B. folgende Einstellungen vornehmen:

- ✓ Verfügbarkeit und Priorität des Druckers ①;
- ✓ Drucken sofort starten oder erst, nachdem die letzte Seite gespoolt wurde (kann das Spooling beschleunigen) ②;
- ✓ Druckaufträge direkt an den Drucker leiten (schaltet die Druckerwarteschlange ab und umgeht den Spooler) ③;
- ✓ fehlerhafte Druckaufträge anhalten ④;
- ✓ Druckaufträge im Spooler zuerst drucken ⑤;
- ✓ Druckaufträge nach dem Drucken nicht löschen ⑥;
- ✓ Druckprozessor ändern ⑦;
- ✓ Trennseite zwischen Druckaufträgen einfügen und einstellen ⑧.



Einstellungen der Druckerwarteschlange

Spoolordner verschieben

Wenn ein Druckserver regelmäßig große Datenmengen zu verarbeiten hat, kann es sinnvoll sein, den Spoolordner auf ein anderes Laufwerk mit viel freiem Speicherplatz oder schnelleren Datenträgern (z. B. SSDs) zu verschieben. Diese Einstellung betrifft alle installierten Drucker.

- ▶ Klicken Sie im Geräte- und Druckerordner auf *Druckerservereigenschaften*.
- ▶ Klicken Sie im Register *Erweitert* auf *Erweiterte Einstellungen ändern*.
- ▶ Geben Sie im Eingabefeld einen anderen Pfad für den Spoolordner ein.

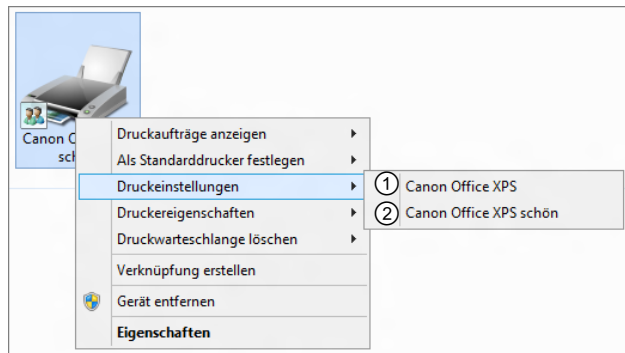
Mehrere Drucker für ein Druckgerät nutzen

Es kann sinnvoll sein, mehrere Drucker (Druckerwarteschlangen) für ein physikalisches Druckgerät einzurichten. Auf einer Workstation könnten den verschiedenen Druckern z. B. unterschiedliche Druckformate zugewiesen werden. Auf einem Druckserver könnte durch unterschiedliche Prioritäten und Druckberechtigungen für die einzelnen Drucker gesteuert werden, wer zuerst auf dem Druckgerät drucken darf. So können eilige Briefe über den Drucker mit hoher Priorität sofort ausgedruckt werden, während die Broschüre mit 200 Seiten auf dem Drucker mit niedriger Priorität wartet, bis keine anderen Druckaufträge mehr vorliegen.

Weitere mögliche Einsatzszenarien sind z. B.:

- ✓ **Tagesdrucker** für den laufenden Betrieb und **Nachtdrucker**, z. B. für den Druck von Broschüren;
- ✓ **unterschiedliche Druckprioritäten** für verschiedene Benutzer und/oder Drucker;
- ✓ **PCL- und Postscript-Druck**. In diesem Fall müssen Sie in den einzelnen Warteschlangen jeweils den Druckermodus mit einer Trennseite festlegen. Dafür liefert Windows passende Trennseiten.
- ✓ Farb- und Schwarz-Weiß-Drucker;
- ✓ unterschiedliche Standard-Papierformate oder -Einzugsschächte.

Beispiel: Durch das manuelle Hinzufügen von zwei Druckern mit demselben Treiber haben Sie nun zwei Drucker: einmal für Schnelldruck in Schwarz-Weiß ① mit Priorität 10 und einmal für Farbdruk ② mit Priorität 1. Beide Drucker greifen auf das gleiche Druckgerät zu. Das Druckgerät ist wegen Wartungsarbeiten momentan noch ausgeschaltet. In beiden Druckerwarteschlangen befindet sich jeweils mindestens ein Dokument.



Zwei Druckerwarteschlangen

Wenn das Druckgerät wieder verfügbar ist, wird wegen der höheren Priorität zuerst der Druckauftrag in Schwarz-Weiß ausgeführt.

15.5 Druckaufträge verwalten

Status von Druckaufträgen einsehen

- Klicken Sie im Geräte- und Druckerordner doppelt auf den entsprechenden Drucker.
- oder Klicken Sie doppelt auf das Druckersymbol neben der Uhrzeitanzeige in der Taskleiste.

Das Druckersymbol in der Taskleiste wird nur bei ausstehenden Druckaufträgen angezeigt. Bei mehreren Druckerwarteschlangen wird für jede aktuell verwendete Druckerwarteschlange ein eigenes Fenster geöffnet.

In der Spalte *Status* wird angezeigt, ob das Dokument gerade gedruckt wird, ob der Ausdruck des Dokuments angehalten wurde oder ob es gerade in die Warteschlange geladen wird.

Brother DCP-LB450CDW Printer

Drucker Dokument Ansicht

Dokumentname	Status	Besitzer	Seiten	Größe	Gesendet	Anschluss
 Unbenannt - Editor	An Drucker...	administra...	1/1	45,8 KB	10:20:26 06.02.2017	

1 Dokument(e) in der Warteschlange

Die geöffnete Druckerwarteschlange

Sie sehen außerdem, wer den Druckauftrag abgeschickt hat, wieviele Seiten der Auftrag umfasst, wieviel Speicherplatz der Auftrag im Spoolerordner belegt und wann der Auftrag abgeschickt wurde. Angaben über den Druckeranschluss erhalten Sie nur, wenn das Druckgerät direkt mit dem Server verbunden ist. Handelt es sich um einen netzwerkfähigen Drucker, bleibt diese Spalte leer.

Über einen rechten Mausklick auf ein Dokument können Sie den Druckauftrag anhalten bzw. den angehaltenen Druckauftrag fortsetzen. Das Neustarten eines Druckauftrags ist nur sinnvoll, wenn gedruckte Aufträge nicht gelöscht werden. *Abbrechen* bedeutet, dass der Druckauftrag gelöscht wird.

Um alle Druckaufträge auf einmal zu löschen, klicken Sie im Menü *Drucker* auf *Alle Druckaufträge abbrechen*.

Druckerwarteschlange eines Druckers anhalten/fortsetzen

- ▶ Öffnen Sie die Druckerwarteschlange.
- ▶ Im Menü *Drucker* wählen Sie *Drucker anhalten*.

Durch erneuten Aufruf des Menüpunktes *Drucker anhalten* werden weitere Druckaufträge an den Drucker gesendet.

Bedenken Sie, dass nach dem Anhalten der Druckerwarteschlange der Drucker nicht sofort aufhört zu drucken. Die Daten im Arbeitsspeicher des Druckgeräts werden weiterhin ausgedruckt. Je nach eingesetztem Drucker und Art der Druckaufträge können das ziemlich viele Seiten sein.

Alle Druckerwarteschlangen anhalten/fortsetzen

Sind viele Drucker installiert, ist es recht mühselig, diese alle einzeln anzuhalten und wieder zu starten. In diesem Fall ist es einfacher, den Spooler-Dienst zu beenden.

- ▶ Im Server-Manager erweitern Sie den Knoten *Konfiguration\ Dienste* und beenden/starten dort den Dienst *Druckerwarteschlange*. Alternativ können Sie ihn auch anhalten/fortsetzen.

oder Geben Sie in einer Eingabeaufforderung ein:

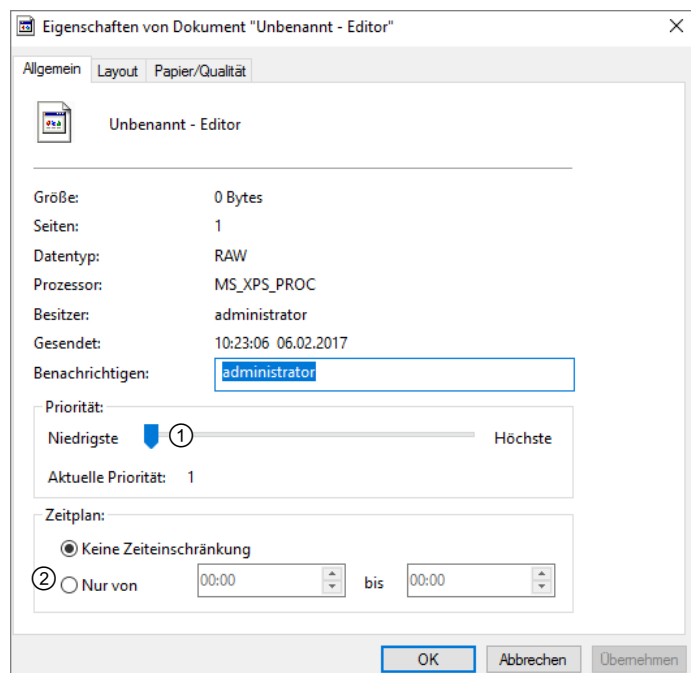
```
net stop spooler  gefolgt von net start spooler 
```

Alternativ können Sie auch mit `net pause spooler` und `net continue spooler` arbeiten.

Priorität und Zeitplan von Druckaufträgen verändern

Wenn es im Drucker nicht anders konfiguriert wurde, erhalten standardmäßig alle Druckaufträge innerhalb einer Druckerwarteschlange die geringste Priorität (1) und werden in Eingangsreihenfolge bearbeitet.

- ▶ Öffnen Sie die Druckerwarteschlange.
- ▶ Wählen Sie im Kontextmenü eines Dokuments den Menüpunkt *Eigenschaften*.
- ▶ Wechseln Sie in das Register *Allgemein*.
- ▶ Sie können die Priorität des Druckauftrags mit dem Schieberegler ① verändern. Aufträge mit höherer Priorität werden zuerst ausgedruckt.
- ▶ Um den Zeitplan des Druckauftrags zu ändern, aktivieren Sie das Optionsfeld ② und geben Sie einen Zeitraum ein, in dem der Druckauftrag ausgeführt werden soll.



Priorität und Zeitplan eines Druckauftrags ändern

15.6 Berechtigungen und Gruppen verwalten

Standardberechtigungen für das Drucken und Verwaltung von Druckern/Dokumenten

Sie können im Zusammenhang mit dem Drucken bestimmten Gruppen Berechtigungen erteilen und verweigern. Dazu gehören insbesondere die Berechtigungen zum Drucken, zur Verwaltung des Druckers und zur Verwaltung einzelner Dokumente in der Druckerwarteschlange.

Die Standardeinstellungen sind wie folgt:

Gruppe	Drucken	Drucker verwalten	Dokumente verwalten
Administratoren	X	X	X
ERSTELLER-BESITZER			X
Jeder	X		

Durch diese Einstellungen kann ein Benutzer, der einen Druckauftrag in die Druckerwarteschlange gestellt hat und somit Mitglied der Gruppe ERSTELLER-BESITZER geworden ist, seinen eigenen Druckauftrag verwalten. Administratoren können auch Druckaufträge anderer Personen verwalten.

- Wechseln Sie in den Druckereigenschaften des Druckers, für den Sie die Berechtigungen anpassen möchten, in das Register *Sicherheit*.

Hier können Sie durch Markieren der einzelnen Benutzergruppen deren Berechtigungen einsehen ①.

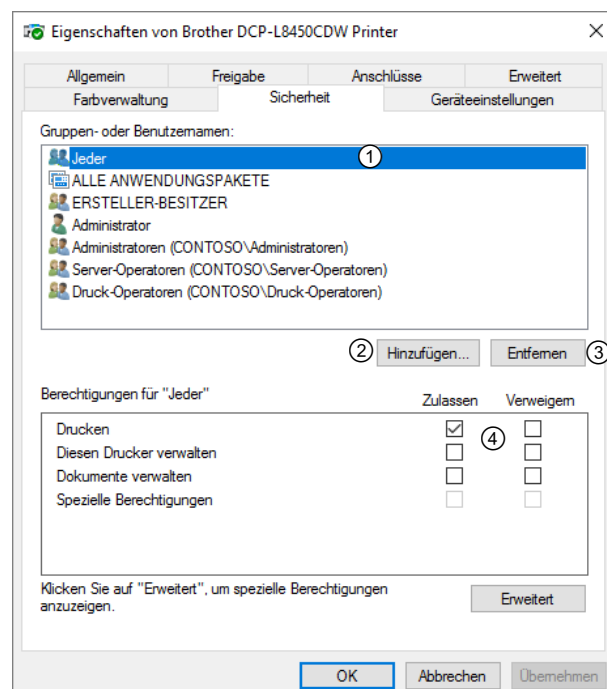
Gruppen hinzufügen

- Klicken Sie auf *Hinzufügen* ② oder *Entfernen* ③, um neue Benutzer oder Gruppen hinzuzufügen oder zu entfernen.
- Passen Sie die Berechtigungen an, indem Sie die Kontrollfelder ④ für *Zulassen* bzw. für *Verweigern* aktivieren.
- Bestätigen Sie Ihre Eingaben mit *OK*.

Sie können Gruppen oder Personen die Berechtigung zum Drucken nehmen, indem Sie sie aus der Liste entfernen oder indem Sie ihnen die Berechtigung verweigern. Durch das Verweigern der Berechtigung werden die betroffenen Personen explizit vom Zugriff auf den Drucker ausgeschlossen, unabhängig davon, in welcher Gruppe sie sich befinden.

Hier gibt es drei Berechtigungen, die standardmäßig zugeordnet werden können:

- ✓ **Drucken** – Erlaubt die Ausgabe von Dokumenten auf dem Drucker. In den meisten Fällen ist hier die Gruppe „Jeder“ eingetragen, das heißt jeder Anwender darf den Drucker nutzen. Hier sollte die Gruppe entfernt werden. Anschließend kann zum Beispiel eine neu erstellte Gruppe hinzugefügt werden, die das Recht erhält, den Drucker zu nutzen. Andere Benutzergruppen außer Administratoren sollten nicht das Recht haben, den Drucker zu nutzen.
- ✓ **Diesen Drucker verwalten** – Ermöglicht die Veränderung von Druckereinstellungen, wie bei den auf den vorangegangenen Seiten beschriebenen Festlegungen.



Berechtigungen für Druckerbenutzer

- ✓ **Dokumente verwalten** – Erlaubt die Verwaltung von Warteschlangen und damit beispielsweise das Löschen von Dokumenten aus solchen Warteschlangen. Dieses Recht sollten entweder Administratoren erhalten, oder speziell geschulte Anwender, die Dokumente aus den Druckwarteschlangen löschen sollen.

Überblick: Gleiche Aufgaben – andere Wege

Die Druck- und Dokumentdienste können Sie im Server-Manager als Rolle hinzufügen. Verwaltet ein Server viele freigegebene Drucker, wird deren Verwaltung deutlich einfacher und integrierter. Die Konfigurationsschritte der einzelnen Drucker erfolgen auf die oben dargestellte Art, nur der Zugang zu den einzelnen Einstellungen ist einfacher.

Der wesentliche Unterschied ist, dass Sie mit den Druck- und Dokumentdiensten keine Drucker verwalten können, die nicht für das Netzwerk freigegeben sind.

Druck- und Dokumentdienste installieren

- ▶ Klicken Sie im Dashboard des Server-Managers auf *Rollen und Features hinzufügen*.
- ▶ Wählen Sie *Rollenbasierte Installation* und anschließend den Server aus.
- ▶ Aktivieren Sie die Serverrolle *Druck- und Dokumentdienste* und bestätigen Sie die dazugehörigen Features.
- ▶ Aktivieren Sie auf der Seite *Features* bei Bedarf *LPR-Portmonitor*.
- ▶ Aktivieren Sie auf der Seite *Rollendienste* auf Wunsch den LPD-Dienst und weitere Rollendienste.
- ▶ Klicken Sie auf *Installieren*, um den Vorgang abzuschließen.

Wählen Sie die Rollendienste aus, die für "Druck- und Dokumentdienste" installiert werden müssen.

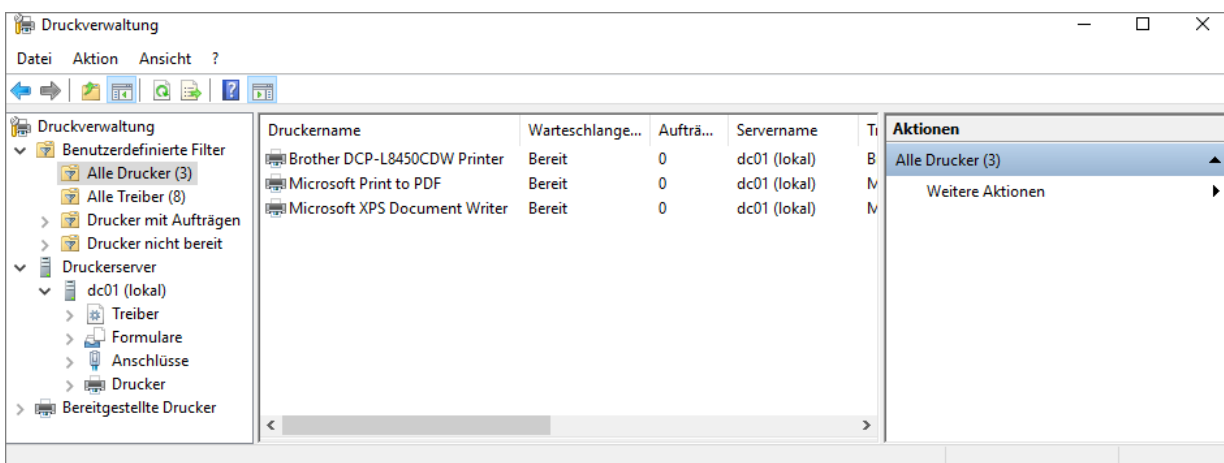
Rollendienste	Beschreibung
☒ Druckerserver	
☐ Internetdrucken	
☐ LPD-Dienst	Der LPD-Dienst (Line Printer Daemon) ermöglicht Benutzern an UNIX-basierten Computern oder anderen Computern mit dem LPR-Dienst (Line Printer Remote) das Drucken auf den freigegebenen Druckern des Servers.
☐ Server für verteilte Scanvorgänge	

Ausschnitt der Seite „Rollendienste hinzufügen“ im Assistenten

Nach der Installation finden Sie im Server-Manager eine neue Seite namens *Druckdienste*, auf der Sie wie üblich die beteiligten Rollen und Dienste sowie die Auslastung und Statusmeldungen sehen können. Die eigentliche Verwaltung der Drucker findet in der Druckverwaltung statt, die Sie im Server-Manager über das Menü *Tools* aufrufen können.

Druckverwaltung verwenden

Mit der Druckverwaltung können Sie alle im Netzwerk freigegebenen Drucker ansehen und verwalten.



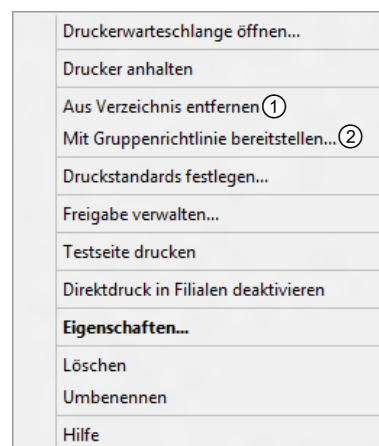
Unter *Druckverwaltung - Druckserver - <Servername> - Drucker* sehen Sie alle vorhandenen Drucker und verschiedene Statusinformationen.

Mit einem Doppelklick auf einen Drucker öffnen Sie dessen Eigenschaften. Über das Kontextmenü können Sie die Druckerwarteschlange öffnen und zahlreiche andere Einstellungen vornehmen.

Über *In Verzeichnis auflisten* können Sie den Drucker im Active Directory veröffentlichen. Ist der Drucker bereits veröffentlicht, steht dort *Aus Verzeichnis entfernen* ①.

Eine Aufgabe, die Sie nur mit dem Snap-In *Druck- und Dokumentdienste* erledigen können, finden Sie unter *Mit Gruppenrichtlinie bereitstellen* ②. Sie geben dort die zu verwendenden Gruppenrichtlinienobjekte an und legen fest, ob der Drucker Computern oder Benutzern zugewiesen wird.

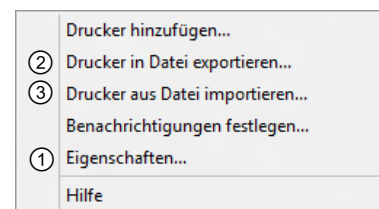
Näheres zu Gruppenrichtlinien erfahren Sie in Kapitel 16.



Kontextmenü eines Druckers auf einem Druckserver

Eigenschaften des Druckservers

Nach einem Rechtsklick auf den Servernamen erhalten Sie das abgebildete Kontextmenü. Über *Eigenschaften* ① gelangen Sie in die Druckservereigenschaften und können die Einstellungen vornehmen, die oben erläutert wurden.



Kontextmenü eines Druckservers

Druckserver migrieren

Muss der Druckserver auf andere Hardware verlegt werden, gehen Sie folgendermaßen vor:

- ▶ Klicken Sie im Kontextmenü des Eintrags *<Servername>* auf *Drucker in Datei exportieren* ②. Der Assistent für die Druckermigration wird gestartet.
- ▶ Legen Sie Pfad und Bezeichnung für die Datei fest und schließen Sie den Vorgang ab.
- ▶ Kopieren Sie diese Datei auf den neuen Server.
- ▶ Installieren Sie auf dem neuen Server die Rollen *Druck- und Dokumentdienste*.
- ▶ Wählen Sie im Kontextmenü des neuen Druckservers *Drucker aus Datei importieren* ③ und geben Sie den Pfad zur exportierten Datei an.

Damit können Sie sämtliche Einstellungen und benutzten Treiber des alten Druckservers auf den neuen übertragen. Das Zuweisen der neuen Drucker auf den Clients übernimmt der Assistent nicht. Dies können Sie über die Gruppenrichtlinien erledigen.

16 Gruppenrichtlinien

16.1 Gruppenrichtlinienobjekt (GPO, Group Policy Object)

Überblick

Ein Gruppenrichtlinienobjekt enthält eine Vielzahl an Einstellungsmöglichkeiten für Computer und Benutzer. In einem neuen GPO ist zunächst keine dieser Einstellungen konfiguriert und Sie aktivieren diejenigen, die Sie zuweisen wollen. Das GPO verknüpfen Sie dann mit einer Organisationseinheit (der Domäne oder einem Standort), und allen Computern bzw. Benutzern unterhalb des Verknüpfungspunktes werden die Gruppenrichtlinieneinstellungen des GPO zugewiesen (Vererbung).

Sie können dasselbe GPO gleichzeitig an verschiedenen Stellen zuweisen. Standorte, Domänen und OUs (Verknüpfungspunkte) können Sie mit mehreren GPOs verknüpfen. Verteilt werden GPOs über Domänencontroller, die auch deren Replikation übernehmen. Über verschiedene Einstellungsmöglichkeiten kann dieses Standardverhalten modifiziert werden.

Gruppenrichtlinien sind ein mächtiges Verwaltungswerkzeug im Active Directory, mit dem Sie den allergrößten Teil der Computer- und Benutzerkonfiguration vornehmen sollten. Einstellungen, die Sie über Gruppenrichtlinien verteilen, kann ein Benutzer in der Regel nicht verändern.

Durch das Verschieben eines Computer- oder Benutzerkontos in eine andere Organisationseinheit werden gegebenenfalls andere Gruppenrichtlinienobjekte angewendet. Beenden Sie die Verknüpfung eines GPOs, kommen die darin enthaltenen Einstellungen nicht weiter zur Anwendung, dabei gibt es allerdings Ausnahmen.

Viele Informationen zu diesem Thema finden Sie unter www.gruppenrichtlinien.de.

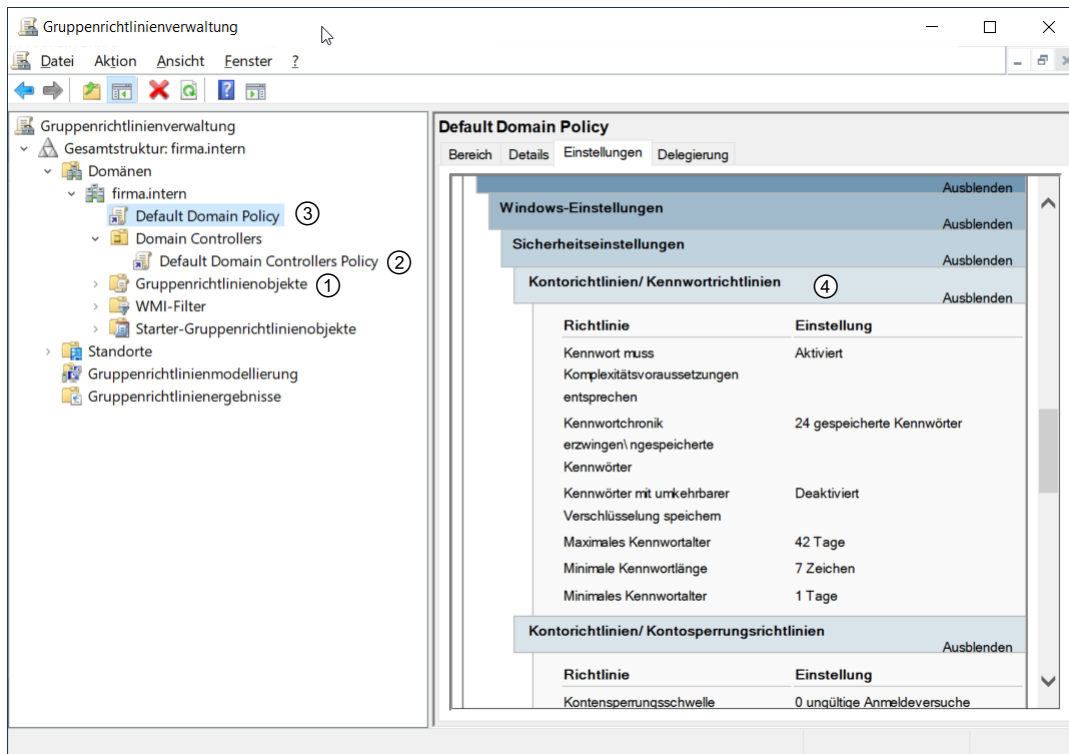
Verwaltungswerkzeug

Gruppenrichtlinien verwalten Sie mit der *Gruppenrichtlinienverwaltung*. Auf Domänencontrollern wird dieses Feature automatisch installiert, auf anderen Rechnern, z. B. Windows 10/11 können Sie es hinzufügen, indem Sie die entsprechenden Remoteserver-Verwaltungstools (RSAT, Remote Server Administration Tools) installieren. Dabei handelt es sich um ein Feature on Demand, welches direkt bei bestehender Internetverbindung installiert wird.

Links (vgl. Abb. der folgenden Seite) sehen Sie die möglichen Verknüpfungspunkte (Domäne, OUs, Standorte). Damit Standorte angezeigt werden, müssen Sie diese jedoch zuerst der Anzeige 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.

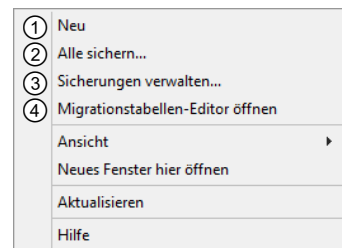


Einfache Verwaltungsaufgaben

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. Sie müssen eindeutige Namen verwenden.
- ② Alle GPOs sichern. Die Speicherung erfolgt im eingestellten Speicherpfad. Die Sicherung ist praktisch, weil sich der Ordner kopieren und beispielsweise in einer Testumgebung wieder importieren lässt.
- ③ Sicherungen verwalten. Nach Angabe des Sicherungsordners werden alle darin enthaltenen GPOs angezeigt. Einzelne Gruppenrichtlinienobjekte können dort ausgewählt und wiederhergestellt werden. Alternativ können Sie die Einstellungen anzeigen.
- 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>. Einen Artikel in englischer Sprache finden Sie hier:



Gruppenrichtlinienobjekte - Kontextmenü

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754682\(v=ws.11\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754682(v=ws.11)?redirectedfrom=MSDN)

Einstellung in einer Gruppenrichtlinie können verschiedene Zustände annehmen. Diese können Sie in den einzelnen Richtlinienobjekten konfigurieren. Viele Einstellungen entsprechen dem folgenden Prinzip:

- ✓ **Aktiviert:** Bei dieser Einstellung wird die Konfiguration auf das Zielobjekt angewendet und weitergegeben.
- ✓ **Deaktiviert:** Bei dieser Einstellung wird die Konfiguration der Gruppenrichtlinie auf dem Server auf den Standard zurückgesetzt.

- ✓ **Nicht konfiguriert:** Bei dieser Einstellung wird die lokale Einstellung des Clients beibehalten und durch die Gruppenrichtlinie nicht geändert.

Im Bereich *Hilfe* oder auf der Registerkarte *Erklärung* finden Sie eine ausführliche Erklärung zu der Einstellung und deren Auswirkungen. Bevor Sie eine Einstellung aktivieren, sollten Sie sich möglichst immer die Erklärung genau durchlesen. Bietet eine Richtlinie weitere Einstellungen, können Sie diese entsprechend über Menüs, Dropdownfelder oder durch die Eingabe von Werten konfigurieren.

16.2 Verarbeitung der Gruppenrichtlinienobjekte

Reihenfolge bei der Verarbeitung von GPOs

Auf jedem Windows-Rechner existiert ein lokales Gruppenrichtlinienobjekt. In Arbeitsgruppen ist dies das einzige GPO, das angewendet wird.

Beim Starten des Computers wird die Computerkonfiguration der zugewiesenen GPOs in einer vorgegebenen Reihenfolge abgearbeitet:

- ✓ **Lokales GPO**
- ✓ Alle GPOs, die mit dem **Standort** des Computers verknüpft sind.
Standorte sind neutral bezüglich Domänen, deshalb können nur Organisations-Admins GPOs mit Standorten verknüpfen.
- ✓ Alle GPOs, die mit der Computer-**Domäne** verknüpft sind
- ✓ Es folgen die GPOs, die mit der (übergeordneten) **Organisationseinheit** des Computers verknüpft sind.
Dann folgen **untergeordnete OUs**, bis die OU des Computerkontos erreicht ist.

Bei der Anmeldung des Benutzers wird dann die Benutzerkonfiguration in der angegebenen Reihenfolge zugewiesen. Dabei wird allerdings dem Pfad zum Benutzerkonto gefolgt. Befindet sich das Benutzerkonto in einer anderen Domäne oder Organisationseinheit als das Computerkonto, werden dabei möglicherweise andere GPOs benutzt.

Vor der Anwendung der Benutzer-GPOs wird das Benutzerprofil geladen. Wurde dem Benutzerkonto ein Anmeldeskript zugewiesen, so wird dies **nach** der Verarbeitung der Gruppenrichtlinien abgearbeitet.

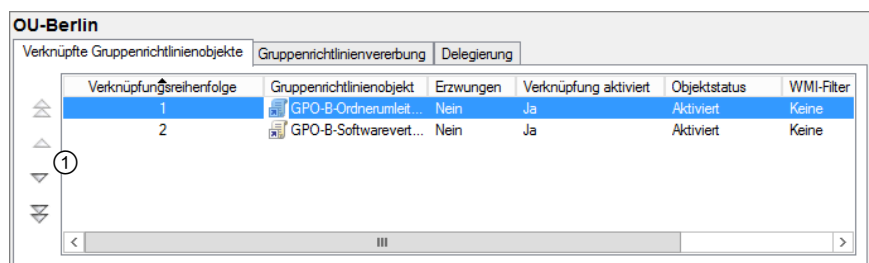
Die GPOs werden standardmäßig in Intervallen von ca. 90 Minuten erneut verarbeitet und zugewiesen. Dieses Intervall lässt sich durch eine Gruppenrichtlinieneinstellung verändern.

Sind einem Verknüpfungspunkt mehrere GPOs zugewiesen, können Sie dort deren Verknüpfungsreihenfolge festlegen.

- ▶ Klicken Sie auf den Verknüpfungspunkt.

Über die Pfeile ① können Sie das markierte GPO an eine andere Stelle verschieben.

Wurden in mehreren GPOs Einstellungen zu einer bestimmten Richtlinie vorgenommen, so werden diese überschrieben. Das GPO oben in der Liste wird als letztes abgearbeitet, hat also die höchste Priorität an dieser Stelle.



Verknüpfungsreihenfolge festlegen

Konfigurationskonflikte

Sind in verschiedenen GPOs dieselben Einstellungen mit unterschiedlichen Werten konfiguriert, überschreiben die später angewendeten Einstellungen die vorhergehenden. Das Motto dabei ist: „Je näher am Objekt, desto gültiger die Einstellungen“.

Manche Einstellungen können Sie sowohl in der Computerkonfiguration als auch in der Benutzerkonfiguration vornehmen. Widersprechen sich diese Einstellungen, dann gelten die Computereinstellungen.

Standardverhalten beeinflussen

Das bisher geschilderte Verhalten bei der Zuweisung von Gruppenrichtlinienobjekten lässt sich auf verschiedene Arten beeinflussen:

- ✓ **Vererbung deaktivieren** (nicht empfohlen):
Über einen Rechtsklick auf eine Domäne oder Organisationseinheit können Sie die Vererbung deaktivieren. GPOs von übergeordneten Verknüpfungspunkten werden dann nicht mehr verarbeitet.
- ✓ **Erzwingen** (nicht empfohlen):
Über einen Rechtsklick auf ein verknüpftes Gruppenrichtlinienobjekt können Sie dessen Verarbeitung erzwingen. Die Einstellungen in diesem GPO werden dann auf jeden Fall angewendet und können nicht durch später verknüpfte GPOs überschrieben werden.
Diese Einstellung überschreibt *Vererbung deaktivieren*, d. h., dieses GPO wird dort trotzdem verarbeitet.
- ✓ **Sicherheitsfilterung** (empfohlen):
GPOs sind mit Berechtigungen versehen. Verfügt ein Benutzer- oder Computerkonto nicht über die Berechtigungen *Lesen* und *Gruppenrichtlinie übernehmen*, werden die entsprechenden Einstellungen nicht angewendet.
- ✓ **WMI-Filter** (bei Bedarf):
Über WMI können Sie eine Vielzahl an Informationen über einen Computer abfragen (z. B. Betriebssystem-Version, freier Festplattenspeicher, installierte Softwarepakete). Weisen Sie einem GPO einen WMI-Filter zu, wird es nur angewendet, wenn alle Abfragen im WMI-Filter zutreffen.
- ✓ **Loopback-Verarbeitungsmodus** (bei Bedarf):
Mit dieser Gruppenrichtlinieneinstellung können Sie festlegen, ob die Benutzerkonfiguration (ausschließlich oder zusätzlich) über die Computer-GPOs erfolgt. Notwendig kann das sein, wenn Sie für einzelne Computer (z. B. Terminalserver oder öffentlich zugängliche Rechner) spezielle Benutzerkonfigurationen benötigen.

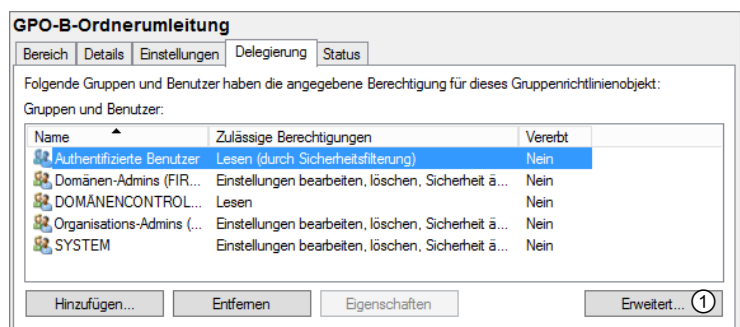
Sicherheitsfilterung einstellen

Auf welche Benutzer- und Computerkonten die Einstellungen eines GPO angewendet werden, legen Sie über dessen Berechtigungen fest. Dies ist eine der ganz wenigen Stellen, wo das Verweigern von Berechtigungen sinnvoll ist.

Erstellen Sie eine (domänenlokale) Gruppe und machen Sie diejenigen Computer- bzw. Benutzerkonten zum Mitglied, auf die das Gruppenrichtlinienobjekt nicht angewendet werden soll.

- ▶ Markieren Sie das entsprechende GPO und wechseln Sie auf das Register *Delegierung*.

Über die Systemgruppe *Authentifizierte Benutzer* wird das GPO für alle Konten zugewiesen. Nach einem Klick auf ① können Sie die Berechtigungen bearbeiten. Fügen Sie die erstellte Gruppe hinzu und verweigern Sie ihr die beiden Berechtigungen *Lesen* und *Gruppenrichtlinie übernehmen*.



Berechtigungen auf GPO

- ! Bedenken Sie beim Bearbeiten von Berechtigungen für ein GPO, dass dieses an verschiedenen Stellen verknüpft sein kann. Veränderungen an den Berechtigungen wirken sich auf alle Verknüpfungspunkte aus. Deshalb ist es vorteilhafter, mit Verweigerungen zu arbeiten, statt die Gruppe *Authentifizierte Benutzer* zu entfernen.

WMI-Filter erstellen

WMI-Filter sind einarbeitungsintensiv, ermöglichen dafür aber sehr detaillierte Abfragen. Grundsätzlich definieren Sie dabei in einer SQL-ähnlichen Syntax eine oder mehrere Abfragen, die als Ergebnis entweder „Wahr“ oder „Falsch“ liefern. Diesen Filter verknüpfen Sie dann mit einem GPO. Die GPO-Einstellungen werden nur angewendet, wenn der WMI-Filter „Wahr“ zurückliefert.

- ▶ Klicken Sie mit der rechten Maustaste auf den Knoten *WMI-Filter* und wählen Sie im Kontextmenü *Neu*.
- ▶ Vergeben Sie im folgenden Fenster einen Namen für den Filter und klicken Sie auf *Hinzufügen*.
- ▶ Definieren Sie die Abfrage und klicken Sie auf *OK*.

Sind Sie zum vorhergehenden Fenster zurückgekehrt, wo der Filter eingetragen wurde, können Sie über die entsprechenden Schaltflächen weitere Filter hinzufügen, vorhandene bearbeiten oder entfernen und den Filter speichern.

Der abgebildete Filter liefert nur dann „Wahr“ zurück, wenn auf einem Rechner das Betriebssystem Windows 10/11 mit dem Produkttyp *Client* (Domänencontroller = 2, Memberserver = 3) installiert ist.

```
select * from Win32_OperatingSystem where Version like "10.%" and ProductType="1"
```

Weitere Informationen in englischer Sprache finden Sie hier: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-wmi-filters-for-the-gpo>

WMI-Filter zuweisen

- ▶ Markieren Sie das GPO, dem Sie den Filter zuweisen wollen, und wechseln Sie in das Register *Bereich*.

Über ① erhalten Sie Zugriff auf alle definierten WMI-Filter und können den passenden auswählen.

- ▶ Bestätigen Sie die Abfrage, ob Sie den WMI-Filter ändern wollen, mit *Ja*.

Informationen im Register *Bereich*

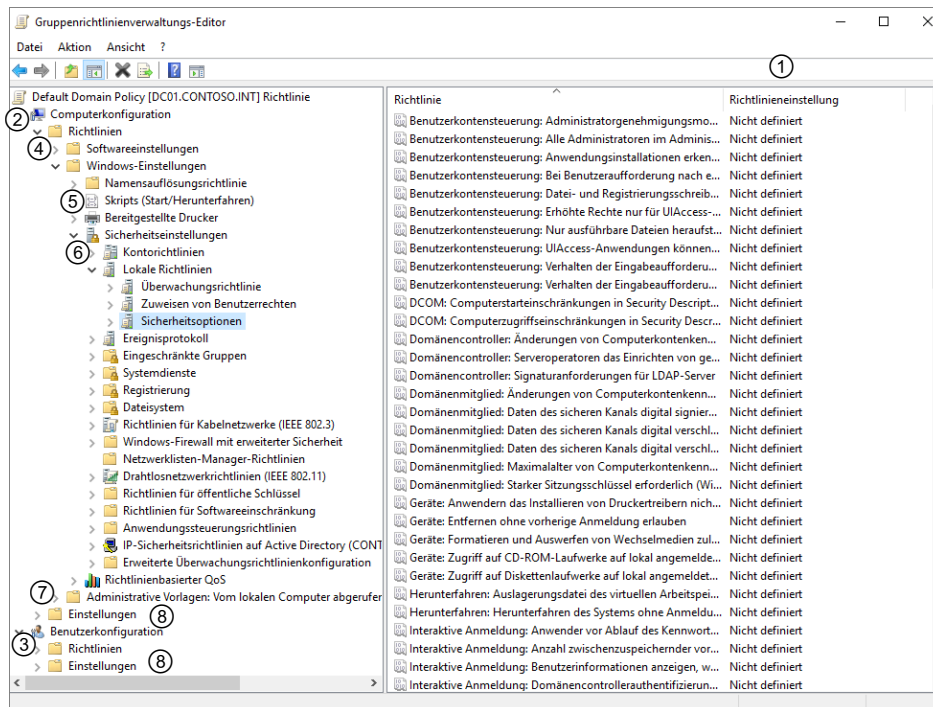
In ② sehen Sie, wo dieses GPO in ③ verknüpft ist (Standard ist die eigene Domäne). Arbeiten Sie mit mehreren Domänen, müssen Sie hier andere Einstellungen vornehmen, um alle Verknüpfungspunkte zu sehen. Auch Verknüpfungen mit Standorten werden nur angezeigt, wenn Sie das entsprechende Verzeichnis auswählen.

WMI-Filter zuweisen

- ! Verlassen Sie sich nicht auf die Einträge in ④. Sicherheitsfilterungen, die mit der Berechtigung *Verweigern* konfiguriert sind, werden hier nicht angezeigt.

16.3 Gruppenrichtlinieneinstellungen konfigurieren

Überblick



Jedes Gruppenrichtlinienobjekt ist (anfänglich) identisch aufgebaut, es sind keinerlei Einstellungen vorhanden ①. Werden solche Einstellungen an keiner Stelle konfiguriert, setzt Windows dafür interne Standardwerte.

Computerkonten konfigurieren Sie über die Einstellungen unter ②, Benutzerkonten über ③. Viele Einstellungsmöglichkeiten finden Sie an beiden Stellen.

Über ④ können Sie Software an Rechner verteilen. Analog finden Sie Software unter *Benutzerkonfiguration*.

Mit ⑤ können Sie Skripte angeben, die beim Start/Herunterfahren eines Rechners bzw. beim Anmelden/Abmelden eines Benutzers ausgeführt werden.

Unter ⑥ können Sie viele Sicherheitseinstellungen konfigurieren. Unter dem Eintrag *Registrierung* können Sie beispielsweise direkt die Sicherheitseinstellungen von Registry-Schlüsseln setzen oder verändern.

Die Einstellungen unter ⑦ erstellen oder verändern Einträge in den Registry-Einstellungen des Computers oder Benutzers. Zunehmend mehr Softwarehersteller veröffentlichen administrative Vorlagen für die zentrale Konfiguration ihrer Produkte. Solche Vorlagen können Sie in ein GPO einbinden.

Die Einstellungen ⑧ wurden mit Windows Vista eingeführt. Konfigurationen, die Sie dort vornehmen, funktionieren anders. Sie sind eher als Vorschläge zu verstehen, denn Benutzer können diese Einstellungen teilweise verändern. Sie werden auch nicht entfernt, wenn das GPO nicht mehr auf ein Konto wirkt. Die Konfiguration von Gruppenrichtlinien ist ein derart umfassendes Thema, dass auf viele Punkte hier nicht weiter eingegangen werden kann. Im Anschluss wird die Konfiguration an einigen Beispielen dargestellt, weitere folgen im Kapitel 17.

Kontorichtlinie bearbeiten

Der vorgesehene Ort für die Kontorichtlinie ist die Default Domain Policy. Wenn Sie die folgenden Einstellungen in einem GPO konfigurieren, das nicht mit der Domäne verknüpft ist, gelten die Einstellungen nur für Benutzerkonten, die lokal auf den betroffenen Rechnern erstellt werden, nicht für Domänen-Konten.

- Klicken Sie mit der rechten Maustaste auf die Default Domain Policy und wählen Sie im Kontextmenü *Bearbeiten*.

- Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor den Knoten *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Kontorichtlinien*.

Zu den Kontorichtlinien gehören die Kennwortrichtlinien und die Kontosperrungsrichtlinien.

- Öffnen Sie den Knoten *Kennwortrichtlinien*.

Durch einen Doppelklick auf einen Eintrag können Sie dessen Einstellung verändern.

Richtlinie	Richtlinieneinstellung
① Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Kennwortchronik erzwingen	24 gespeicherte Kennwörter
② Kennwörter mit umkehrbarer Verschlüsselung speichern	Deaktiviert
Maximales Kennwortalter	42 Tage
Minimale Kennwortlänge	7 Zeichen
Minimales Kennwortalter	1 Tage

Richtlinie ① bedeutet, dass ein Kennwort mindestens ein Zeichen aus drei der folgenden vier Gruppen enthalten muss: a–z, A–Z, 0–9, Sonderzeichen und dass es maximal drei zusammenhängende Zeichen aus dem Benutzeranmeldennamen enthalten darf.

Die Kennwortchronik gibt an, wie viele unterschiedliche Kennwörter ein Benutzer verwenden muss, bevor er ein vorheriges wieder verwenden kann. Ohne diese Einstellung muss ein Benutzer nur den Dialog *Kennwort ändern* abarbeiten, kann dabei aber *Altes Kennwort* und *Neues Kennwort* identisch setzen.

Die Richtlinie ② sollte unbedingt deaktiviert bleiben.

Das maximale Kennwortalter gibt an, wie oft ein Benutzer sein Kennwort ändern muss. Standardmäßig wird er 14 Tage vor dem Ablauf darauf hingewiesen. Das können Sie über eine Gruppenrichtlinieneinstellung verändern.

Das minimale Kennwortalter gibt an, wie viele Tage zwischen zwei Kennwortänderungen liegen müssen.

- Öffnen Sie den Knoten *Kontosperrungsrichtlinien*.

In diesem Fenster legen Sie fest, was passiert, wenn ein Benutzer sein Kennwort öfters falsch eingibt.

Richtlinie	Richtlinieneinstellung
Kontosperrungsschwelle	0 ungültigen Anmeldeversuchen
Kontosperrdauer	Nicht definiert
Zurücksetzungsdauer des Kontosperrungszählers	Nicht definiert

Wenn Sie einen Wert für die Kontosperrungsschwelle eingeben, schlägt Windows für die anderen beiden Einträge automatisch je 30 Minuten vor. Mit der Kontosperrungsschwelle legen Sie fest, wie oft ein Benutzer sein Kennwort falsch eingeben darf, bis sein Konto gesperrt wird. Werte zwischen 3 und 6 sind hier günstig. Wer es bis dahin nicht geschafft hat, der rät.

Die Kontosperrungsdauer gibt an, nach welcher Zeit die Sperrung des Kontos wieder aufgehoben wird. Innerhalb dieser Zeitspanne kann das manuell erfolgen, durch einen Benutzer mit ausreichenden Berechtigungen zur Kontoverwaltung. Der letzte Eintrag gibt an, nach welchem Zeitraum der interne Zähler für falsch eingegebene Kennwörter wieder auf null gesetzt wird.

Eine Kennwortsschwelle sorgt für einen relativ guten Schutz gegen Passwort-Attacken auch bei kürzeren Kennwörtern (kleiner 10), kann Ihnen aber zusätzliche Arbeit durch das Entsperren von Benutzerkonten bereiten. „Witzbolde“ können das auch benutzen, um eine Anmeldung anderer Benutzer zu verhindern. Mit einer passenden Überwachung/Protokollierung finden Sie das aber heraus.



Vorsicht mit der Überwachung! Üblicherweise wird davon ausgegangen, dass Protokollierung als solche unproblematisch ist. Die Auswertung der Protokolle ist eine andere Sache. Erkundigen Sie sich im Zweifelsfall bei einem Juristen.

Seit Windows Server 2008 können in einer Domäne zusätzliche Kontorichtlinien erstellt werden. Diese werden dann allerdings nicht über Gruppenrichtlinien verwaltet. Die Erstellung einer zusätzlichen Kontorichtlinie bildet den Abschluss dieses Kapitels.

Anmeldung überwachen – Überwachungsrichtlinie

Die Überwachung von Anmeldungen aktivieren Sie im Knoten *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Überwachungsrichtlinie*. Dort finden Sie zwei relevante Einträge für Anmeldungen:

- ✓ **Anmeldeereignisse überwachen:** Anmeldeereignisse finden immer auf demjenigen Rechner statt, auf den zugegriffen wird. Sie werden auch dort protokolliert.
- ✓ **Anmeldeversuche überwachen:** Anmeldeversuche protokolliert derjenige Rechner, der den Benutzer authentifiziert. In einer Domäne ist das ein Domänencontroller. In vielen Fällen ist es günstiger, nur diese Richtlinie zu aktivieren.
- ✓ **Objektzugriffsversuche überwachen:** Solange diese Richtlinie nicht aktiviert ist, funktioniert die Überwachung nicht, die Sie bei den Berechtigungen (z. B. NTFS) einstellen.

16.4 Gruppenrichtlinienergebnisse

Arbeiten Sie mit vielen Gruppenrichtlinien, dann ist es oft nicht ganz einfach herauszufinden, welche Richtlinieneinstellung aus welcher GPO stammt. Dabei hilft der Knoten *Gruppenrichtlinienergebnisse* in der Gruppenrichtlinienverwaltung. Nach einem Durchlauf des Assistenten sehen Sie für angegebene Computer (und Benutzer), welche Richtlinieneinstellungen dort mit welchen Werten gesetzt sind und welche GPO diese Einstellungen vorgenommen hat.

Benutzerrichtlinien können Sie nur anzeigen lassen, wenn der Benutzer bereits am Computer angemeldet war.

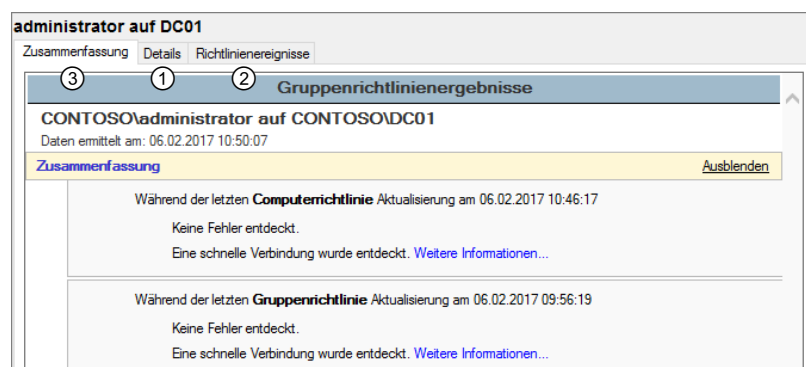
- ▶ Klicken Sie mit der rechten Maustaste auf *Gruppenrichtlinienergebnisse* und wählen Sie im Kontextmenü *Gruppenrichtlinienergebnis-Assistent*.
- ▶ Der Assistent heißt Sie willkommen. Klicken Sie auf *Weiter*.
- ▶ Geben Sie auf der nächsten Seite den Computer an und legen Sie fest, ob Sie die Computerrichtlinien im Ergebnis ausblenden wollen. In diesem Fall erhalten Sie nur die Benutzerrichtlinieneinstellungen.

Die folgende Seite listet auf, für welche Benutzerkonten Sie die Benutzereinstellungen ausgeben können. Dort können Sie einen Benutzer auswählen oder die Ausgabe von Benutzerrichtlinieneinstellungen deaktivieren.

- ▶ Sie erhalten eine Zusammenfassung der Auswahl. Klicken Sie auf *Weiter*.
- ▶ Auf der letzten Seite können Sie den Assistenten fertigstellen.

Das Register *Details* ① zeigt, welche Richtlinieneinstellungen mit welchem Wert gesetzt sind und von welchem GPO diese Einstellung kommt.

Im Register ② erhalten Sie die richtlinienspezifischen Einträge des Ereignisprotokolls vom angegebenen Rechner. Bei Problemen mit der Richtlinienverarbeitung finden Sie dort entsprechende Einträge.



Gruppenrichtlinienergebnis anzeigen

Den Inhalt der Register *Zusammenfassung* ③ und *Details* ① können Sie über einen Rechtsklick als Bericht speichern.



Wenn Sie beim Versuch, Gruppenrichtlinienergebnisse für einen Remoterechner zu ermitteln, eine Fehlermeldung erhalten wie z. B. *Der RPC-Server ist nicht verfügbar*, dann bedenken Sie, dass die Firewall auf diesem Rechner solche Zugriffe unterbinden kann. Die integrierte Firewall können Sie über Gruppenrichtlinieneinstellungen entsprechend konfigurieren. Dieser Hinweis gilt für alle Remotezugriffsversuche.

16.5 Gruppenrichtlinienimplementierung planen

Ein Beispiel

Anhand eines einfachen Beispiels sollen die möglichen Schritte erläutert werden, die zur Implementierung von Gruppenrichtlinien gehören.

Anforderungen festlegen

Folgende Konfigurationen und Handlungsbeschränkungen für Benutzer sollen realisiert werden:

Alle Benutzer, die mit der Bearbeitung von Aufträgen befasst sind,

1. dürfen das Windows-Betriebssystem ihrer Arbeitsstationen nicht updaten,
2. dürfen die Software an ihren Arbeitsstationen nicht konfigurieren,
3. sollen Netzlaufwerke nicht verbinden oder trennen können,
4. sollen nicht über das Symbol *Netzwerk* auf Ressourcen des Netzwerks zugreifen können.

Außerdem soll gelten:

5. Benutzer, die Rechnungen ausstellen, dürfen ihre Arbeitsstationen nicht herunterfahren.

Anforderungen überprüfen

Die Anforderungen legen zwei Gruppenrichtlinienobjekte nahe: eines für die Benutzer der Auftragsbearbeitung und eines für die Benutzer, die Rechnungen ausstellen. Es gilt zu prüfen, ob sich diese beiden Gruppen personell überschneiden. Ist das der Fall, lassen sich die Anforderungen eventuell noch über Computerrichtlinien umsetzen. Überschneiden sich die Gruppen und arbeiten beide Gruppen abwechselnd an den gleichen Rechnern, müssen die Anforderungen angepasst oder die Sicherheitsfilterung verwendet werden, damit die Anwender nur die passende Richtlinie übernehmen.

Richtlinieneinstellungen ermitteln

Jetzt folgt das Heraussuchen von geeignet erscheinenden Richtlinieneinstellungen. Oft erscheint eine gewünschte Einstellung auf den ersten Blick simpel, lässt sich dann aber nur durch das Zusammenwirken mehrerer einzelner Richtlinien erreichen.

Möglicherweise stellen Sie an dieser Stelle auch fest, dass bestimmte gewünschte Effekte nur über die Computerkonfiguration umzusetzen sind. Widerspricht das Ihren Anforderungen, müssen diese modifiziert werden. Anderenfalls erstellen Sie jetzt die GPOs (siehe Abschnitt *Gruppenrichtlinienimplementierung: Erstellen – Testen – Auswerten*).

Testen der GPOs – Testumgebung

Zu diesem Zeitpunkt sollten Sie unbedingt verhindern, dass die Einstellungen der GPOs auf Produktiv-Konten angewendet werden. Das erfolgt am besten mit Test-Konten und einem Test-PC, die in Test-OUs beheimatet sind.

Die Test-OU sollten Sie in der OU der betroffenen Computerkonten erstellen, da sonst Auswirkungen von (fehlenden) geerbten Gruppenrichtlinien die Ergebnisse verfälschen können. Für das Beispiel benötigen Sie eventuell zwei unterschiedliche Test-OUs. Sie können das Computerkonto des Test-PCs zwischen den OUs verschieben, sollten dann aber durch einen anschließenden Neustart sicherstellen, dass die passenden Gruppenrichtlinien verwendet werden.

Für die Test-Benutzer kopieren Sie einfach je ein repräsentatives Benutzerkonto. Auch hier erstellen Sie in der Organisationseinheit des Benutzerkontos eine untergeordnete Test-OU und verschieben das Benutzerkonto dorthin.

Dann verknüpfen Sie die erstellten Gruppenrichtlinienobjekte mit den entsprechenden Test-OUs.

Jetzt melden Sie sich mit dem Konto des Test-Benutzers an und testen Ihre Einstellungen.

Im Zweifelsfall wiederholen Sie die vorangehenden Punkte so lange, bis Sie ein zufriedenstellendes Ergebnis erhalten.

Verknüpfung der GPOs festlegen

Im Idealfall überschneiden sich die Benutzer der beiden Gruppen nicht, sie arbeiten an unterschiedlichen PCs und die betroffenen Konten sind in getrennten OUs untergebracht. Sind in den GPOs alle Einstellungen über die Benutzerkonfiguration umgesetzt, spielen die Computerkonten keine Rolle (und umgekehrt).

In diesem Fall verknüpfen Sie die Gruppenrichtlinienobjekte einfach mit der jeweiligen Organisationseinheit. Erhält ein Benutzer dann einen neuen Aufgabenbereich (Wechsel zwischen Rechnungsstellung und Auftragsbearbeitung), verschieben Sie sein Benutzerkonto einfach in die andere OU.

Sind diese Voraussetzungen nicht gegeben, sollten Sie, wie schon erwähnt, mit Sicherheitsfilterungen arbeiten. Falls noch nicht geschehen, erstellen Sie zwei (globale) Gruppen (z. B. *GG-Auftragsbearbeitung* und *GG-Rechnungsstellung*), fügen ihnen die entsprechenden Konten hinzu und bearbeiten die Berechtigungen der Gruppenrichtlinienobjekte so, dass sie nur noch auf die entsprechenden Gruppen angewendet werden. Dazu müssen Sie in jedem Fall die Gruppe *Authentifizierte Benutzer* entfernen.

Die GPOs müssen Sie auf jeden Fall an einer Stelle verknüpfen, die alle betroffenen Konten erfasst. Die Domäne ist kein idealer Ort dafür. Bedenken Sie, dass Sie GPOs mehrfach an verschiedenen Stellen verknüpfen können.

Wechselt jetzt ein Benutzer seinen Aufgabenbereich, müssen Sie ihn aus der einen Gruppe entfernen und zur anderen hinzufügen. Eleganter ist die vorhergehende Methode.

Gruppenrichtlinienimplementierung: Erstellen – Testen – Auswerten

Erstellen

Im Beispiel entscheiden Sie sich für die abgebildeten Einstellungen im Knoten *Benutzerkonfiguration* \ *Richtlinien* \ *Administrative Vorlagen*.

Daraus folgen zwei Punkte:

- ✓ Sie benötigen keine Test-OU für Computerkonten. Das Konto des Test-PCs legen Sie an dieselbe Stelle wie die Computerkonten, die die Mitarbeiter benutzen.
- ✓ Sollte in den weiteren Tests keine Computerkonfiguration dazukommen, deaktivieren Sie in den GPOs den computerspezifischen Teil, z. B. über einen Rechtsklick auf das GPO und *Objektstatus - Computerkonfigurationseinstellungen deaktiviert* im Kontextmenü. Die Abarbeitung von Gruppenrichtlinien geht dann schneller.

Erstellen Sie jetzt die beiden GPOs und verknüpfen Sie sie mit den Test-OUs der Benutzerkonten.

Benutzerkonfiguration (Aktiviert)	
Richtlinien	
Administrative Vorlagen	
Richtliniendefinitionen (ADMX-Dateien) wurden beim lokalen Computer abgerufen.	
Startmenü und Taskleiste	
Richtlinie	Einstellung
Befehle "Herunterfahren", "Neu starten", "Energie sparen" und "Ruhezustand" entfernen und Zugriff darauf verweigern	Aktiviert
Ein-/Aus-Schalter im Startmenü ändern	Aktiviert
Wählen Sie eine der folgenden Aktionen	
Richtlinie	Einstellung
Links und Zugriff auf Windows Update entfernen	Aktiviert
Menüeintrag "Ausführen" aus dem Menü "Start" entfernen	Aktiviert
Menüeintrag "Netzwerkverbindungen" aus dem Menü "Start" entfernen	Aktiviert
Programme im Menü "Einstellungen" entfernen	Aktiviert
Symbol "Netzwerk" aus dem Menü "Start" entfernen	Aktiviert
Systemsteuerung/Software	
Richtlinie	Einstellung
Option "Programme von Microsoft hinzufügen" ausblenden	Aktiviert
Windows-Komponenten/Windows-Explorer	
Richtlinie	Einstellung
Optionen "Netzlaufwerk verbinden" und "Netzlaufwerk trennen" entfernen	Aktiviert
Symbol "Gesamtes Netzwerk" nicht in "Netzwerkumgebung" anzeigen	Aktiviert

Richtlinieneinstellungen für das Beispiel

Testen und Auswerten

Wenn Sie verschiedene Clientbetriebssysteme einsetzen (z. B. Windows 10 und Windows 11), sollten Sie Tests mit allen Versionen durchführen.

Tests mit Windows 10 zeigen u. a.:

Das Menü *Ausführen* ist immer noch vorhanden, nimmt allerdings nicht mehr alle Befehle an.

- ✓ Öffnet ein Benutzer die *cmd.exe* über einen Doppelklick im Explorer, stehen ihm nach wie vor alle Kommandozeilenbefehle zur Verfügung.
- Mit `net use` kann er nach wie vor Netzlaufwerke verbinden oder trennen.
- Um das zu verhindern, könnten Sie z. B. Richtlinien für Softwareeinschränkung konfigurieren.

Bei Tests werden Sie häufig mit verschiedenen Einstellungen experimentieren. Wollen Sie sich nicht nach jeder Veränderung im GPO ab- und wieder anmelden, hilft der Befehl `gpupdate /force` in einer Eingabeaufforderung. Damit werden die Gruppenrichtlinieneinstellungen erneut vom Domänencontroller abgerufen und angewendet. Bedenken Sie eventuelle Replikationsverzögerungen zwischen den Domänencontrollern.

16.6 Zusätzliche Kontorichtlinie erstellen

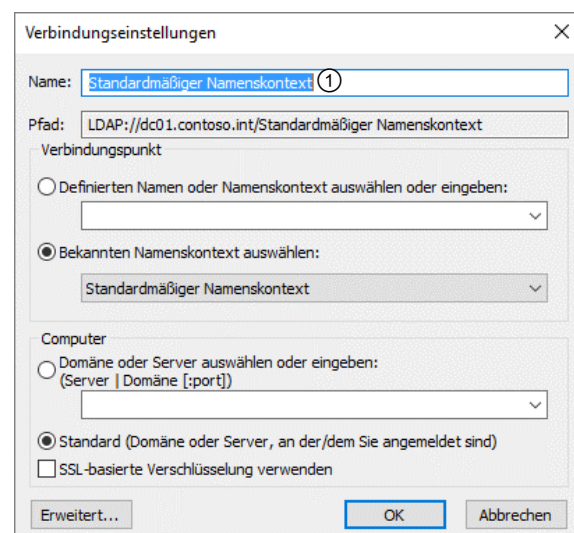
Password Settings Object (PSO, Kennworteinstellungsobjekt) erstellen

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 **Active Directory Service Interface** erhalten Sie Zugriff auf alle Bereiche Ihres AD.

- ▶ Öffnen Sie den ADSI-Editor, z. B. durch Eingabe von `adsiedit.msc` in der Eingabeaufforderung.
- ▶ Klicken Sie im ADSI-Editor mit der rechten Maustaste auf den Eintrag *ADSI-Editor* und wählen Sie im Kontextmenü *Verbindung herstellen*.
- ▶ Sollte das erscheinende Fenster anders aussehen als in der Abbildung, stellen Sie die Optionen entsprechend um und tragen in ① den Namen Ihrer Domäne ein, z. B. *firma.intern*.

Damit erhalten Sie Zugriff auf die AD-Objekte, die im angegebenen Kontext enthalten sind.

- ▶ Erweitern Sie die einzelnen Knoten, bis der Password Settings Container sichtbar wird.
- ▶ Nach einem Rechtsklick auf den Password Settings Container wählen Sie im Kontextmenü *Neu - Objekt*.
- ▶ Klicken Sie im ersten Fenster auf *Weiter*.
- ▶ Vergeben Sie einen Namen für das neue PSO.
- ▶ Legen Sie im nächsten Fenster einen Precedence-Wert für dieses PSO fest.



ADSI-Verbindung erstellen

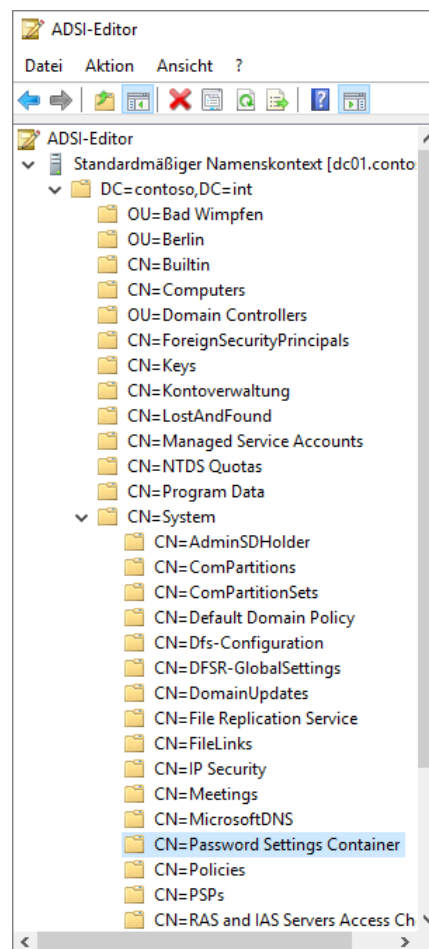
Erstellen Sie mehrere PSOs, müssen in diesem Feld unterschiedliche Zahlen stehen. Ist ein Benutzer Mitglied in mehreren Gruppen, denen unterschiedliche PSOs zugewiesen sind, wird auf den Benutzer das PSO mit dem kleinsten Precedence-Wert angewandt. Dementsprechend sollte Ihr härtestes PSO den kleinsten Wert bekommen.

In den folgenden Fenstern 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*.

Es folgen:

- ✓ die Länge der Kennwortchronik, komplexe Kennwörter, minimale Kennwortlänge;
- ✓ das minimale Kennwortalter; Felder mit der Bezeichnung *Dauer* erfordern die Syntax TT:HH:MM:SS (Tage, Stunden, Minuten, Sekunden);
- ✓ maximales Kennwortalter, Kontosperrungsschwelle, Zurücksetzungsdauer des Kontosperrungszählers und die Kontosperrungsdauer.
- ▶ Im letzten Fenster könnten Sie weitere Attribute bearbeiten. Klicken Sie auf *Fertig stellen*.



Password Settings Container

Password Settings Object zuweisen

Das Zuweisen von PSOs erfolgt am einfachsten über *Active Directory-Benutzer und -Computer*.

- ▶ Stellen Sie sicher, dass im Menü *Ansicht - Erweiterte Features* aktiviert ist.
- ▶ 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 den Eintrag *msDS-PSOAppliesTo* und klicken Sie auf *Bearbeiten*.
- ▶ Klicken Sie im folgenden Fenster auf *Windows-Konto hinzufügen* und fügen Sie die gewünschten Konten hinzu.

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. Im selben Fenster können Sie die Gruppen auch wieder entfernen.

17 Benutzerprofile verwalten

17.1 Personalisierung der Arbeitsumgebung

Überblick

Verwenden mehrere Anwender den gleichen Rechner, erhält jeder Benutzer bei der Anmeldung seine persönliche Arbeitsumgebung. Dazu gehören neben seinen persönlichen Dateien auch zahlreiche Einstellungen, z. B. Rechts-/Linkshänder-Maus, Desktopverknüpfungen und Hintergrundbild. Alle diese Einstellungen befinden sich in Benutzerprofilen, die auf dem Rechner in speziellen Ordnern gespeichert werden.

Arbeitet ein Benutzer abwechselnd an verschiedenen Rechnern, muss er alle benötigten Einstellungen auf jedem Rechner (einmalig) erneut vornehmen. Zugriff auf seine persönlichen Dateien erhält er nur rechnerspezifisch, d. h., speichert er Dateien in den vorgeschlagenen Standardordnern, erhält er nur auf dem jeweiligen Rechner Zugriff darauf.

Servergespeicherte Profile ermöglichen es, dass die Einstellungen dem Benutzer folgen. Deshalb werden sie auch wandernde Profile (Roaming Profiles) genannt.

Benutzerprofil bei der ersten Anmeldung

Meldet sich der Benutzer erstmalig an einem Rechner an, existiert dort für ihn noch kein Profilordner. Für dessen Erstellung werden folgende Schritte durchlaufen:

- ✓ Wurde dem Benutzer ein **servergespeichertes Benutzerprofil** zugewiesen, wird geprüft, ob am angegebenen Speicherort das Profil vorhanden ist. Falls ja, wird es von dort kopiert. Existiert dort kein Benutzerprofil, wird zunächst der Profilordner angelegt und es folgen die gleichen Schritte wie bei einem Benutzer ohne servergespeichertes Profil.
- ✓ Existiert in der Freigabe *Netlogon* des Domänencontrollers ein Ordner *Default User*, wird dieses Profil kopiert. Ansonsten erhält der Benutzer eine Kopie des lokalen Ordners *Default User*.

Ordner für Benutzerprofile

Auf dem lokalen Rechner entspricht der Ordnername für das Benutzerprofil dem Benutzeranmeldenamen. In welchem Ordner das Benutzerprofil dort gespeichert wird, hängt ab vom verwendeten Betriebssystem. Seit Windows Vista sind die Benutzerprofile standardmäßig im Ordner **Benutzer** bzw. **Users** auf der Systempartition zu finden.

Dass dieser Ordner im Dateisystem eigentlich **Users** ① heißt, zeigt die Abbildung.

Sie sehen auch einen Symlink ② sowie eine Verbindung (Junction) ③, die alle Zugriffe auf den Ordner *Default User* nach *C:\Users\Default* umgeleitet. Über solche Verknüpfungen wird die Kompatibilität mit Anwendungen sichergestellt, die Dateien in bestimmten Ordnern erwarten.

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. Alle Rechte vorbehalten.
C:\Users\Administrator>cd..

C:\Users>dir /a
Volume in Laufwerk C: hat keine Bezeichnung.
Volumennummer: B474-2B09

Verzeichnis von C:\Users ①
14.10.2016 10:58 <DIR>      .
14.10.2016 10:58 <DIR>      ..
06.02.2017 09:56 <DIR>      Administrator
16.07.2016 14:34 ②<SYMLINKD> All Users [C:\ProgramData]
14.10.2016 10:58 <DIR>      Default
16.07.2016 14:34 ③<JUNCTION> Default User [C:\Users\Default]
16.07.2016 14:21      174 desktop.ini
12.09.2016 12:56 <DIR>      Public
                1 Datei(en),          174 Bytes
                7 Verzeichnis(se), 48.568.291.328 Bytes frei

C:\Users>mklink /?
Erstellt eine symbolische Verknüpfung.

MKLINK [[/D] | [/H] | [/J]] Verknüpfung Ziel ④

/D      Erstellt eine symbolische Verknüpfung für ein Verzeichnis.
        Standardmäßig wird eine symbolische Verknüpfung für
        eine Datei erstellt.
/H      Erstellt eine feste Verknüpfung anstelle einer
        symbolischen Verknüpfung.
/J      Erstellt eine Verzeichnisverbindung.
Verknüpfung Gibt den Namen für die symbolischen Verknüpfung an.
Ziel        Gibt den Pfad (relativ oder absolut) an, auf den die
        neue Verknüpfung verweist.
```

④ zeigt das Kommando MKLINK, mit dem Sie solche Verknüpfungen selbst erstellen können.

Über den Link *Erweiterte Benutzerprofileigenschaften konfigurieren* im Fenster *Benutzerkonten* der Systemsteuerung (Kategorieansicht) (*Systemsteuerung - Benutzerkonten - Benutzerkonten*) können Sie sich alle Benutzerprofile auf einem PC unter Windows 8/8.1/10/11 anzeigen lassen und diese verwalten. Sie sehen an dieser Stelle auch die Größe des jeweiligen Profils.

Im Ordner auf der Festplatte des Profils befinden sich mehrere Unterordner. Die persönlichen Daten jedes Benutzers liegen in seinem eigenen Ordner, auf den nur er selbst sowie die Administratoren Zugriff haben.

Aufbau eines Benutzerprofils

Zur Abwärtskompatibilität hat Microsoft zusätzlich einige Verknüpfungen eingefügt, die in den vorangegangenen Windows-Versionen noch verwendet wurden oder die direkt auf einen anderen Ordner verweisen.

Folgende Ordner spielen dabei eine wesentliche Rolle. Beachten Sie jedoch, dass einige Ordner standardmäßig im Explorer ausgeblendet sind. Sie müssen zunächst die versteckten Dateien aktivieren:

- ✓ *Desktop*: Symbole und Einstellungen des Benutzerdesktops
- ✓ *Eigene Dokumente*: Standardmäßiger Speicherort aller persönlicher Dateien eines Benutzers
- ✓ *Downloads*: Speicherort aller Downloads
- ✓ *Favoriten*: Favoriten des Internet Explorers
- ✓ *Eigene Musik*: Ablageort von Musikdateien
- ✓ *Eigene Videos*: Ablageort für gespeicherte Filmdateien
- ✓ *Eigene Bilder*: Ablageort für Bilddateien und Grafiken
- ✓ *Suchvorgänge*: Ablageort für abgespeicherte Suchen
- ✓ *AppData*: Ablageort für benutzerspezifische Daten und Systemdateien von Applikationen. Diesen Ordner sehen Sie nur, wenn Sie in den Explorer-Optionen die versteckten Dateien anzeigen lassen.
- ✓ *Gespeicherte Spiele*: Zentraler Ablageort für Spielstände von kompatiblen Windows-Spielen
- ✓ *Links*: Hierbei handelt es sich um die Favoriten im Windows-Explorer

Neben den Ordnern findet sich im Profilpfad die Datei *NTUSER.DAT*. Diese enthält die Einstellungen der Registry, die sich dort unter HKEY_CURRENT_USER (HKLM) befinden. Die gesamten benutzerspezifischen Einstellungen sind hier enthalten. Sie müssen dazu die versteckten und geschützten Systemdateien einblenden lassen. Sie finden diese Möglichkeit auf der Registerkarte *Ansicht* im Explorer nach einem Klick auf *Optionen/Ordner* und *Suchoptionen ändern*.

Zur Vereinheitlichung von anwendungsspezifischen Daten hat Microsoft den Ordner *AppData* im Benutzerprofil eingeführt. Dieser Ordner enthält die drei Unterordner:

- ✓ *Local*
- ✓ *LocalLow*
- ✓ *Roaming*

In den beiden Ordnern *Local* und *LocalLow* speichert Windows Daten von Anwendungen, die nicht mit dem Benutzer bei der Verwendung von verschiedenen Arbeitsstationen mitwandern.

Der Ordner *Roaming* enthält die Daten, die benutzerspezifisch sind und für servergespeicherte Profile verwendet werden können. Diese Daten können mit dem Benutzer auf verschiedene Arbeitsstationen mitwandern.

Unter den Windows-Versionen vor Windows Vista und Windows 7 hat der Ordner *All Users* die Inhalte zur Verfügung gestellt, die für alle Anwender auf dem PC gegolten haben. So war es möglich, durch Bearbeitung eines einzelnen Ordners die Einstellungen aller Benutzer anzupassen. Beispiel für den Einsatz von *All Users* war das Startmenü oder der Inhalt des Desktops, der sich immer aus dem eigenen Benutzerprofil und dem Inhalt des Ordners *All Users* zusammensetzte.

Hatten Sie eine Verknüpfung in den Ordner `\All Users\Startmenü` kopiert, wurden diese bei allen Benutzern des PCs im Startmenü angezeigt. In Windows 8/8.1/10/11 ist der Ordner `C:\Users\All Users` nur noch als Verknüpfung vorhanden, die auf den Ordner `C:\ProgramData` verweist. Hier wird wiederum auf das Profil *Öffentlich* unter `C:\Users` verlinkt.

Wie bei den Vorgängerversionen legt Windows 8/8.1/10/11 automatisch ein neues Profil an, wenn sich Benutzer das erste Mal am PC anmelden.

17.2 Servergespeicherte Benutzerprofile

Einführung

Grundsätzlich lassen sich zwei verschiedenen Arten von servergespeicherten Benutzerprofilen unterscheiden:

- ✓ Veränderbare Benutzerprofile:

Bei der Anmeldung wird das Benutzerprofil vom Server geladen und bei der Abmeldung auf den Server zurück gespeichert. Dabei wird nicht jedes Mal der komplette Inhalt des Profilordners hin und her kopiert, sondern nur diejenigen Dateien, die sich zwischenzeitlich verändert haben. Bestimmte Ordner sind von der Speicherung auf dem Server ausgeschlossen.

- ✓ Verbindliche Profile (obligatorisch, mandatory):

Bei der Anmeldung wird das Benutzerprofil vom Server geladen bzw. wird die bereits lokal vorhandene Kopie mit der Server-Version aktualisiert. Während der Arbeit kann der Benutzer alle Funktionen nutzen wie bei den anderen Profilen auch. Bei der Abmeldung erfolgt keinerlei Rückspeicherung auf den Server. Meldet sich der Benutzer erneut an, erhält er dieselben Einstellungen (z. B. Hintergrundbild) wie zuvor. Dateien, die der Benutzer in der vorhergehenden Sitzung erstellt hat, werden dabei nicht gelöscht.

Diese Version kann (sinnvoll) auch mehreren Benutzern gleichzeitig zugewiesen werden. Obligatorische Profile lassen sich nur über servergespeicherte Profile umsetzen.

Ein servergespeichertes Profil wird verbindlich, wenn Sie auf dem Profil-Server die Datei *NTUSER.DAT* umbenennen in *NTUSER.MAN*.

Die meisten Programme schlagen je nach Dateityp den Ordner *Eigene Dokumente*, *Eigene Bilder*, *Eigene Musik* oder *Eigene Videos* als Standardspeicherort vor. Viele Anwender speichern Dateien auch gern auf dem Desktop. Alle diese Orte liegen im Benutzerprofil. Sind dort viele Dateien gespeichert, dauert die Anmeldung sehr lange. Über Ordnerumleitungen können bestimmte Ordner aus dem Profil ausgelagert und an anderen Orten gespeichert werden. Damit geht die Anmeldung dann schneller und erzeugt weniger Datenverkehr.

Servergespeicherte Profile zuweisen

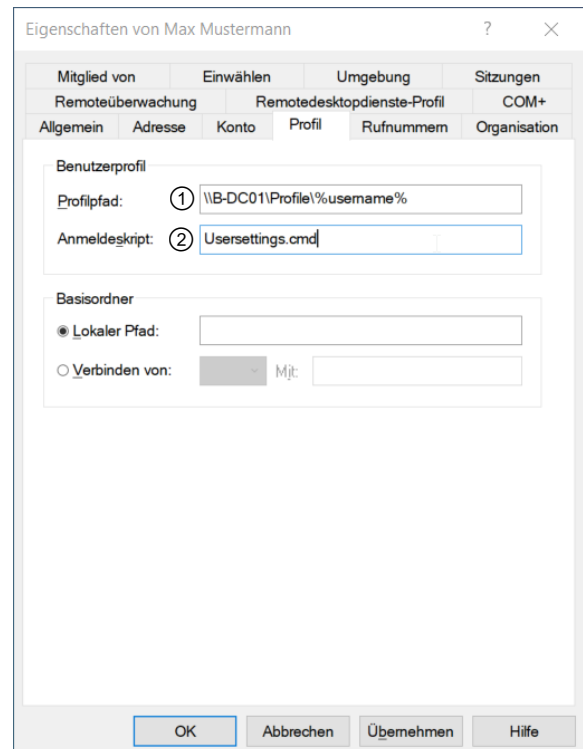
So weisen Sie einem oder mehreren Benutzerkonten ein servergespeichertes Profil zu:

- ▶ Markieren Sie die betreffenden Benutzerkonten und klicken Sie im Kontextmenü auf *Eigenschaften*.
- ▶ Wechseln Sie in das Register *Profil*.

Hier können Sie den Profilpfad ① und ein Anmeldeskript ② eintragen. Die zu verwendende Syntax ist:

```
\\<Servername>\<Freigabename>\<Ordnername>
```

Der Ordner wird automatisch erstellt und mit Rechten konfiguriert. Dabei wird *%Username%* automatisch durch den Anmeldenamen des Benutzers ersetzt.



Beachten Sie, dass nur der Benutzer Zugriff auf seinen Profilordner erhält. Sie können über Gruppenrichtlinien dafür sorgen, dass auch Admins Vollzugriff erhalten. *%Username%* ist eine von zahlreichen Umgebungsvariablen. Sie können in einer Eingabeaufforderung mit dem Befehl `set` alle Variablen anzeigen lassen.

Anmeldeskript

Ein Anmeldeskript ② ist eine ausführbare Datei, die mit den Rechten des jeweiligen Benutzers bei der Benutzeranmeldung ausgeführt wird. Sie wird eingesetzt, um dem Benutzer beispielsweise Netzlaufwerke oder Drucker zuzuordnen. Anmeldeskripts lassen sich mit Gruppenrichtlinien am einfachsten umsetzen bzw. verwalten.

Anmeldeskripts müssen in der Freigabe *Netlogon* auf den Domänencontrollern liegen. Sie geben hier nur den Namen des Skripts ein.

Sie können Benutzern in Active Directory Anmeldeskripts zuweisen, die auf den Computern ausgeführt werden, sobald sich der Benutzer anmeldet. Über Gruppenrichtlinien lassen sich sogar Skripte starten, die beim Starten, Herunterfahren, bei der Abmeldung und zusätzlich noch bei der Anmeldung ablaufen. Es gibt daher fünf Arten von Skripten, die Administratoren Anwendern oder Computern zuweisen können. Es ist auch möglich, mehrere Typen von Skripten zu mischen. Windows-Computer führen alle aus.

Um automatisch Befehle beim Anmelden von Benutzern oder beim Starten des PCs ausführen zu lassen, gibt es folgende Möglichkeiten:

- ✓ Das klassische Anmeldeskript, das in den Eigenschaften des Profils eingetragen ist. Die Ausführung sieht der Anwender teilweise in einem Fenster der Eingabeaufforderung.
- ✓ Anmeldeskript in den Gruppenrichtlinien für Benutzer
- ✓ Abmeldeskript in den Gruppenrichtlinien für Benutzer
- ✓ Skript in den Gruppenrichtlinien beim Hochfahren eines Computers, unabhängig vom Benutzer
- ✓ Skript in den Gruppenrichtlinien beim Herunterfahren eines Computers, unabhängig vom Benutzer

Das klassische Anmeldeskript, das Programme und Befehle ausführt, hinterlegen Sie auf der Registerkarte *Profil* in den Eigenschaften der Benutzer. An dieser Stelle haben Sie auch die Möglichkeit, das lokale Benutzerprofil des Anwenders auf eine Freigabe zu speichern. Damit die Skripte beim Anmelden von Benutzern auch starten, müssen Sie die Dateien und die Programme, welche die Skripte starten sollen, in der NETLOGON-Freigabe auf den Domänencontrollern speichern.

Wenn Sie ein Skript in die NETLOGON-Freigabe eines Domänencontrollers kopieren, wird es durch den Datei-replikationsdienst (File Replication Service, FRS) automatisch auf die anderen Domänencontroller repliziert. Überprüfen Sie den Vorgang oder kopieren Sie das Skript manuell. Der lokale Speicherort der NETLOGON-Freigabe ist der Ordner `\Windows\SYSVOL\sysvol\<Domänennamen>\scripts`.

Mit klassischen Anmeldeskripten ist es nicht möglich, den Programmcode auszuführen, während der Computer startet. Dies ist nur über Gruppenrichtlinien innerhalb einer Active Directory-Domäne möglich. Diese Skripte wirken beim Anmelden und Abmelden eines Benutzers sowie beim Starten und Herunterfahren eines Computers.

Ein weiterer Vorteil ist, dass sich solche Skripts auch auf einzelne Organisationseinheiten oder sogar ganze Domänen anwenden lassen. Die Skripts werden in den Gruppenrichtlinien an folgender Stelle hinterlegt:

- ✓ Skriptausführung für Computer während des Starts und beim Herunterfahren:
Computerkonfiguration/Richtlinien/Windows-Einstellungen/Skripts (Start/Herunterfahren) gesteuert.
- ✓ Skripte für Anwender beim An- oder Abmelden werden über *Benutzerkonfiguration/Richtlinien/Windows-Einstellungen/Skripts (Anmelden/Abmelden)* gesteuert.

Außer speziellen Skripts lassen sich in den Gruppenrichtlinien auch diverse Einstellungen hinterlegen, die den Ablauf der Skripts steuern. Die Einstellungen sind in den Gruppenrichtlinien zu finden. Die entsprechenden Erläuterungen und Hilfen finden Administratoren direkt in der Hilfe der jeweiligen Einstellung. Folgende Richtlinieneinstellungen spielen dabei eine Rolle:

- ✓ *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Skripts*
- ✓ *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Anmeldung*
- ✓ *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Gruppenrichtlinien*
- ✓ *Benutzerkonfiguration/Richtlinien/Administrative Vorlagen/Skripts*
- ✓ *Benutzerkonfiguration/Richtlinien/Administrative Vorlagen/Anmeldung*

Basisordner

Basisordner geben Ihnen die Möglichkeit, einem Benutzer bei der Anmeldung eine persönliche Netzlaufwerksverknüpfung mitzugeben. Daraufhin wird die Variable `%Homedrive%` angepasst.

Zur Zuweisung eines Basisordners legen Sie einen freien Laufwerksbuchstaben auf dem Client fest und geben die Freigabe wie oben an. Auch hier entsteht der Ordner von selbst und wird automatisch mit passenden Berechtigungen versehen.

Arbeiten Sie mit einer Ordnerumleitung, können Sie hier den Pfad zum umgeleiteten Ordner *Eigene Dateien* eingeben.

17.3 Servergespeicherte Profile implementieren

Überblick

Zur Umsetzung von servergespeicherten Profilen gehören die folgenden Schritte:

- ✓ Die Freigabe auf dem Profilserver vorbereiten
- ✓ Falls Basisordner verwendet werden, die Freigabe für die Basisordner vorbereiten

- ✓ Für eine Ordnerumleitung:
 - ✓ Die Ordnerumleitungs-Freigabe vorbereiten (das kann der Basisordner sein)
 - ✓ Die Gruppenrichtlinien erstellen und verknüpfen
- ✓ Die Benutzereinstellungen anpassen (Registerkarte *Profil*)
- ✓ Für obligatorische Profile: im servergespeicherten Profil die Datei *NTUSER.DAT* umbenennen in *NTUSER.MAN*

Servergespeicherte Profile sind beispielsweise für Benutzer sinnvoll, die an unterschiedlichen Rechnern arbeiten.

Die Ordnerumleitung entfernt Ordner aus dem Benutzerprofil und speichert sie auf einem angegebenen Server, was eine zentralisierte Datensicherung ermöglicht. Bedenken Sie, dass umgeleitete Ordner nicht mehr auf dem Client vorhanden sind. Für Laptop-Benutzer, die auch außerhalb des Firmennetzes arbeiten, müssen Sie dann dafür sorgen, dass diese Dateien auch offline verfügbar sind, und eine Synchronisierung einrichten.

Server-Freigaben vorbereiten

Erstellen Sie die Freigabe für die Ordnerumleitungen am besten nicht auf dem Profilserver. Kann der Client bei der Anmeldung das Profil nicht laden, wird der Benutzer mit einem temporären Profil angemeldet und erhält keinen Zugriff auf diese Dateien. Das passiert nicht, wenn sie auf einem anderen Server liegen.

Für alle Freigaben, die Sie erstellen, gelten grundlegend dieselben Schritte:

- ▶ Erstellen Sie auf dem jeweiligen Server die entsprechenden Ordner (z. B. *Profiles* und *Home*). Als *Profiles\$* und *Home\$* erscheinen die Freigaben nicht in der Netzwerkumgebung.
- ▶ Deaktivieren Sie für die Profile-Freigabe das Zwischenspeichern.
Für die Ordnerumleitungs-Freigabe sollten Sie das automatische Zwischenspeichern aktivieren, zumindest dann, wenn Daten von Laptop-Benutzern dort gespeichert werden.
Benutzer müssen über **Vollzugriff** auf ihr Profil und Basisverzeichnis verfügen.
- ▶ Konfigurieren Sie die NTFS-Berechtigungen für die erstellten Ordner wie in der folgenden Tabelle:

Benutzer/Gruppe	NTFS-Berechtigungen	Übernehmen für ...
Administratoren	Vollzugriff	diesen Ordner, Unterordner und Dateien
System	Vollzugriff	diesen Ordner, Unterordner und Dateien
Ersteller-Besitzer	Vollzugriff	nur Unterordner und Dateien
<Benutzer>	Ordner auflisten / Daten lesen, Attribute lesen, Ordner erstellen / Daten anhängen	nur diesen Ordner

<Benutzer> ersetzen Sie durch eine passende Gruppe, die diejenigen Benutzerkonten enthält, die ihre Dateien hier ablegen sollen.



Die Benutzerprofile von Windows-XP-Clients und älter sind nicht mit den modernen Benutzerprofilen ab Windows Vista kompatibel. Solche älteren Profile werden im Profilordner als <Benutzeranmeldename>.**v1** gespeichert, die neuen Profile enden, je nach Windows-Version, mit **.v2** - **.v6**. Ohne Ordnerumleitungen kann ein Benutzer seine Einstellungen nicht mitnehmen, wenn er zwischen Rechnern mit unterschiedlichen Windows Versionen wechselt. Die Dateien in den Ordnern *Eigene Dateien* bzw. *Dokumente* sind nur unter dem jeweiligen Betriebssystem zugreifbar.

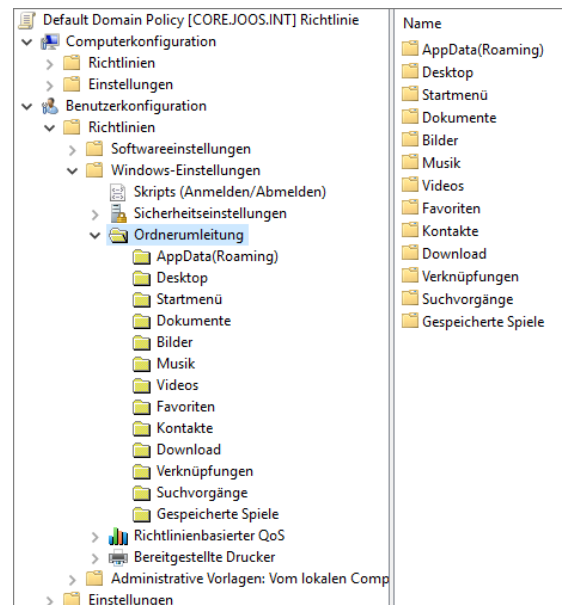
Microsoft erweitert ständig die Funktionen von Windows. Das gilt auch für Windows 10/11. Im Benutzerprofil kann festgelegt werden, für welche Betriebssystem-Version das Profil geeignet ist. Derzeit gibt es sechs Versionen (keine Angabe der Version, bis hin zu v6 für Rechner ab Windows 10 Version 1607). Die Version wird als Erweiterung für das Verzeichnis verwendet, in dem das servergespeicherte Profil gespeichert wird, zum Beispiel `\\server\freigabe\profil.v6`.

Ordnerumleitung konfigurieren

Ordnerumleitungen konfigurieren Sie über Gruppenrichtlinien. Erstellen Sie ein eigenes Gruppenrichtlinienobjekt. Die notwendigen Einstellungen finden Sie unter *Benutzerkonfiguration - Richtlinien - Windows-Einstellungen - Ordnerumleitung*.

Diejenigen Ordner, die die größten Datenmengen enthalten, sollten Sie auf jeden Fall umleiten. Für Windows XP sind das die Ordner *AppData*, *Desktop* und *Dokumente*. Ab Vista sollten Sie zusätzlich die Ordner *Bilder*, *Musik*, *Videos*, *Download* und *Gespeicherte Spiele* aufnehmen. Unter XP waren das Unterordner von *Dokumente*, soweit vorhanden.

Sie können bei der folgenden Konfiguration einen Standardpfad für alle betroffenen Benutzer angeben oder unterschiedliche Pfade für verschiedene Gruppen. Sie können auch mehrere GPOs erstellen. Was für Sie am günstigsten ist, hängt vor allem von der Struktur Ihrer Organisationseinheiten und der Anzahl der Benutzer ab.



Das folgende Beispiel bezieht sich auf die Umleitung des Ordners *Dokumente*.

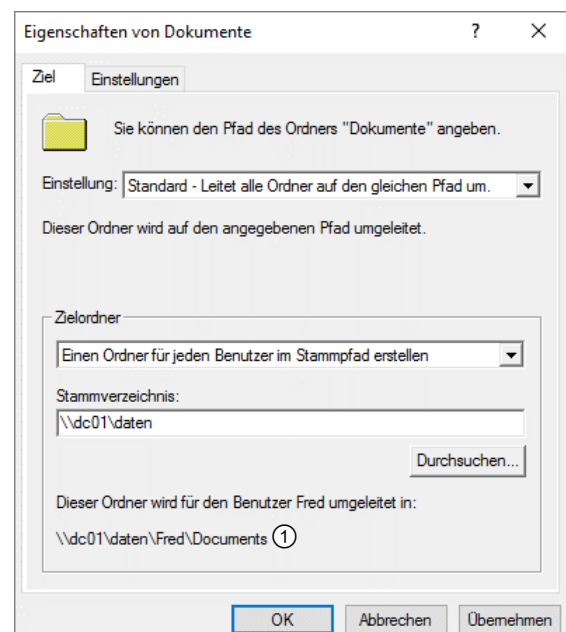
- ▶ Klicken Sie mit der rechten Maustaste auf den Ordner *Dokumente* und wählen Sie im Kontextmenü *Eigenschaften*.
- ▶ Schalten Sie die Ordnerumleitung unter *Einstellung* ein. Sie haben die Wahl zwischen den Optionen *Standard* und *Erweitert*.

Unter *Zielordner* bestimmen Sie das Ziel der Ordnerumleitung. Hier können Sie u. a. einen umgeleiteten Ordner z. B. wieder zurück an seinen Originalplatz kopieren.

Als *Stammverzeichnis* geben Sie den UNC-Pfad der Ordnerumleitungs-Freigabe an. Je nachdem, was Sie als Zielordner gewählt haben, können hier auch genauere Angaben (Unterordner) erforderlich sein. Sie können auch den Pfad zu einem konfigurierten Basisordner angeben.

Unter ① sehen Sie ein Beispiel für die spätere Umleitung.

- ▶ Wechseln Sie auf das Register *Einstellungen*.



Im Register *Einstellungen* können Sie bestimmen, wie die Ordnerumleitung abläuft.

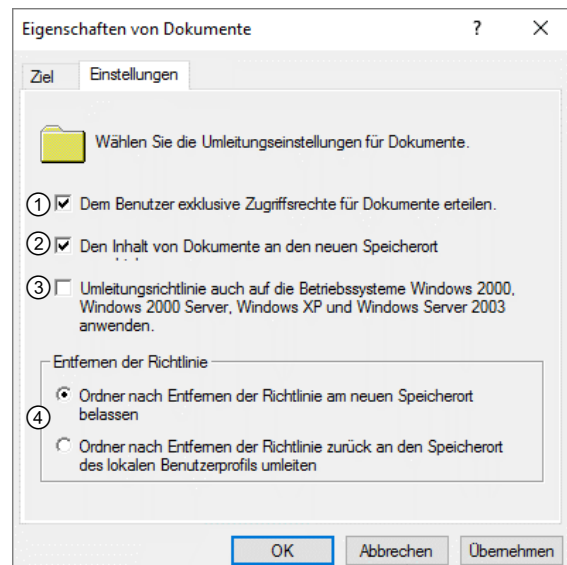
Dem Benutzer exklusive Zugriffsrechte für Dokumente erteilen ① ist für die Administration unpraktisch. Benötigt ein Admin Zugriff auf den Ordner, muss er zuerst den Besitz übernehmen, die Berechtigungen ändern, seine Arbeiten erledigen und dann den Besitz wieder zuweisen.

Unterlaufen dabei Fehler, kann der Benutzer nicht mehr auf die Daten in diesem Ordner zugreifen. Sie sollten den Haken entfernen.

Den Inhalt von Dokumente an den neuen Ort verschieben ② löscht die Dateien vom Rechner, nachdem sie erfolgreich verschoben wurden. Ohne diese Option verbleiben Kopien auf dem Rechner.

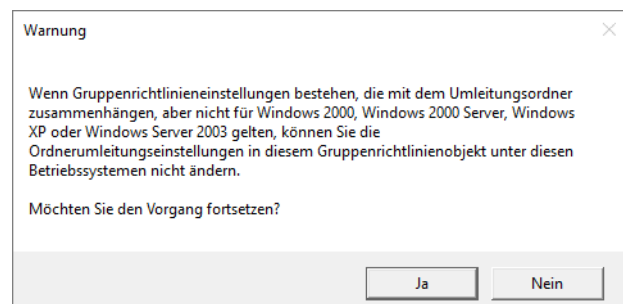
Ohne Aktivierung der Umleitungsrichtlinie ③ funktioniert die Ordnerumleitung erst ab Windows Vista.

Mit ④ legen Sie fest, ob nach Entfernen der Richtlinie der Ordner am neuen Ort belassen oder zurück an den Ort des lokalen Benutzerprofils verschoben wird.



Standardeinstellungen

- ▶ Klicken Sie zum Übernehmen der Einstellungen auf **Übernehmen**.
Sie erhalten eine Warnmeldung zu den Besonderheiten der älteren Windows-Versionen.
- ▶ Klicken Sie auf **Ja**.
- ▶ Klicken Sie auf **OK**.



Weitere Gruppenrichtlinieneinstellungen für servergespeicherte Profile

Alle folgenden Richtlinien müssen auf die Clientcomputer angewendet werden. Sie finden sie unter *Computerkonfiguration - Richtlinien - Administrative Vorlagen*. Ab hier folgen relative Angaben.

- ✓ **Netzwerk - Offlinedateien - Alle Offlinedateien vor der Abmeldung synchronisieren** und **Netzwerk - Offlinedateien - Untergeordnete Ordner immer offline verfügbar machen**
Arbeiten Sie mit Ordnerumleitungen, müssen Laptop-Benutzer auch unterwegs Zugriff auf die umgeleiteten Ordner erhalten. Neben den genannten Richtlinien müssen möglicherweise noch weitere aktiviert werden.
- ✓ **System - Anmelden - Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten**
Diese Einstellung sollten Sie in der Default Domain Policy aktivieren. Ohne diese Richtlinie kann es u. a. vorkommen, dass zugewiesene Skripts nicht (richtig) abgearbeitet werden oder Netzlaufwerke, die bei der Anmeldung zugewiesen werden, nicht funktionieren. Auch die Verarbeitung von Gruppenrichtlinien kann negativ beeinflusst werden.
- ✓ **System - Benutzerprofile - Zeitlimit für langsame Netzwerkverbindungen für Benutzerprofile steuern**
Hier geht es wieder um mobile Laptop-Benutzer, für die der Profilserver nicht erreichbar ist. Die Anmeldung erfolgt schneller, wenn Sie hier passende Werte eintragen.
- ✓ **System - Benutzerprofile - Sicherheitsgruppe "Administratoren" zu servergespeicherten Profilen hinzufügen**
Ohne diese Einstellung erhalten die Benutzer exklusiven Zugriff auf ihr Profil, daher muss ein Administrator für jeden Zugriff auf den Profilordner zuerst den Besitz übernehmen, die Berechtigungen ändern, seine Arbeiten erledigen und den Besitz wieder zuweisen. Unterlaufen ihm dabei Fehler, verliert der Benutzer den Zugriff auf sein servergespeichertes Profil und wird mit einem temporären Profil angemeldet, was zusätzliche Arbeit verursacht.

18 Server überwachen

18.1 Überwachung und Leistungsanalyse

Windows Server 2022 verfügt über zahlreiche Mechanismen zur Überwachung der System- und Netzwerkressourcen. Viele der Werkzeuge überschneiden sich in ihren Funktionen, insbesondere bei der Ressourcenüberwachung. Einige spezielle Tätigkeiten lassen sich nur mit einem bestimmten Werkzeug durchführen, es lohnt sich also, alle Überwachungsmöglichkeiten zu kennen und zu nutzen.

Analyse der Leistung von Computern und der Netzwerklast

Server-Manager	Der Server-Manager ist mit dem Dashboard und den nach Serverrollen getrennten Ereignismeldungen, Leistungsdiagrammen, Auflistungen der beteiligten Dienste, Rollen und Features gut zur einfachen Überwachung und Administration geeignet.
Ereignisanzeige	Die Ereignisanzeige zeigt diverse Vorgänge des Systems, die in unterschiedlichen Protokollen festgehalten werden: ✓ Anwendungsprotokoll ✓ Installation ✓ Sicherheitsprotokoll ✓ Systemprotokoll
Task-Manager	Der Task-Manager zeigt aktuell laufende Prozesse auf einem System auf und bietet einen Überblick über die Auslastung von Prozessoren und Speicher.
Ressourcenmonitor	Der Ressourcenmonitor bietet einen tieferen Einblick in die Aktivität von Netzwerk, Datenträgern, CPU sowie Speicherauslastung als der Task-Manager.
Leistungsüberwachung	Mit der Leistungsüberwachung lassen sich detaillierte Informationen über das System erfassen, in Statistiken zusammenstellen, speichern und auswerten.
Windows Admin Center	Mit dieser Lösung, die erst installiert werden muss, können Sie auch mit einem Webbrowser Windows-Server überwachen.

Überwachung und Protokollierung

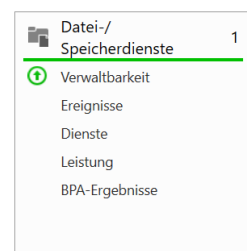
Windows protokolliert automatisch diverse Ereignisse, z. B. das Starten und Beenden von Diensten oder Systemfehler. Darauf können Sie keinen Einfluss nehmen. Wie Sie Sicherheitsüberwachungen bei Objektzugriffen konfigurieren, wurde im Kapitel zu den Berechtigungen erklärt.

Bei Problemen im System können Sie die Ursache in der Regel über die entsprechenden Protokolle herausfinden oder eingrenzen. Der Server-Manager zeigt auf dem Dashboard kritische Ereignisse getrennt nach Serverrollen an und erleichtert so das Auffinden und Beseitigen von Fehlern.

Anzeige von Ereignissen im Server-Manager und auf dem Dashboard

Windows Server 2022 verfügt über einen komplett umgestalteten Server-Manager. Im Gegensatz zu den Vorgängerversionen dient der Manager nun hauptsächlich als Schaltzentrale zum Aufrechterhalten des Betriebs und nicht mehr als ein Universalwerkzeug, in dem man (fast) alles einstellen und einrichten kann.

Der Server-Manager kommt erst zur vollen Geltung, wenn der Server und die Domäne fertig eingerichtet sind, denn nun sieht der Administrator auf den ersten Blick, wenn irgendwo ein Problem aufgetaucht ist. Außerdem werden Fehler- und Warnmeldungen nach Serverrollen sortiert angezeigt, der Status der beteiligten Dienste überwacht und die Ressourcenauslastung grafisch dargestellt.



Durch diese übersichtliche Präsentation werden die von den älteren Server-Versionen bekannten Werkzeuge zwar nicht überflüssig gemacht, verlieren aber für den Administrationsalltag deutlich an Bedeutung.

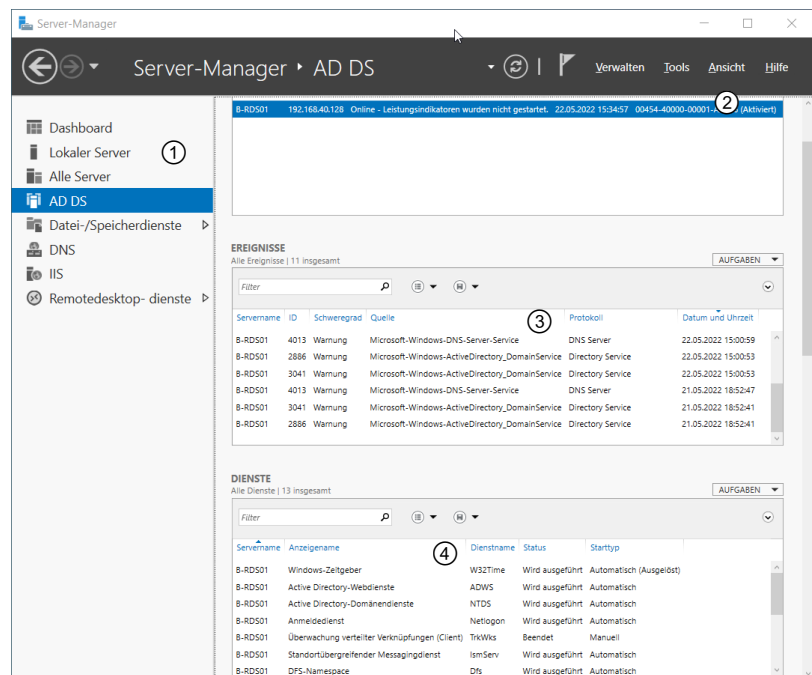
Auf der ersten Seite des Server-Managers, dem Dashboard, erhalten Sie einen schnellen Überblick über den Zustand Ihrer Serverinfrastruktur. Für jede installierte Serverrolle werden in einem Kasten die Bezeichnung sowie die Kategorien *Verwaltbarkeit*, *Ereignisse*, *Dienste*, *Leistung* und *BPA-Ergebnisse* angezeigt. Wenn Sie auf eine Kategorie klicken, können Sie in der Detailansicht einstellen, welche Art von Ereignissen oder Meldungen Sie angezeigt bekommen wollen. In der Standardeinstellung werden nur schwerwiegende Probleme und Fehler angezeigt.



Dashboard-Ausschnitt

In der linken Spalte des Server-Managers ① können Sie schnell zwischen den verschiedenen Serverrollen, verschiedenen Servern und dem Dashboard wechseln. Auf der rechten Seite wird Ihnen ein Überblick über eine Serverrolle gegeben. Über die Schaltflächen *AUFGABEN* können Sie weitere Funktionen abrufen.

Die Seiten für die Serverrollen sind stets gleich aufgebaut: Zuerst sehen Sie, auf welchem Server Sie sich gerade befinden ②. Dann werden die letzten *Ereignisse* ③ und der Status der beteiligten Dienste ④ angezeigt. Als Nächstes können Sie mit dem Best Practices Analyzer verschiedene Prüfungen durchführen, um Verbesserungsvorschläge und Hinweise auf Probleme zu erhalten.



Ausschnitt Server-Manager mit einer Übersichtsseite pro Serverrolle

In der Sparte *LEISTUNG* erhalten Sie einen Überblick über CPU-Auslastung und Speicherbedarf. Als letzter Block werden alle beteiligten Rollen und Features angezeigt. Hier können Sie Rollen und Features hinzufügen und entfernen.

Arbeiten mit Protokollen

Ereignisprotokolle sammeln Einträge von verschiedenen Quellen. Hier wird zum Beispiel festgehalten, wenn ein Dienst regelmäßig mit einem Fehler beendet wird. In so einem Fall können Sie sich mithilfe der Ereignis-ID auf die Suche nach einer Lösung für das Problem machen. Voraussetzung dafür ist die regelmäßige Kontrolle der Protokolle.

Grundlagen von Ereignisprotokollen

In der Ereignisanzeige können Sie alle Protokolle einsehen. Sie können die Ereignisanzeige für den lokalen Rechner oder für entfernte Rechner einrichten, wenn Sie die Berechtigung dazu haben. In Abonnements können Sie Sammlungen von Ereignissen verschiedener Rechner zusammenfassen. Im Folgenden wird die Ereignisanzeige des lokalen Rechners beschrieben. Die Ereignisanzeige gliedert sich in vier Abschnitte:

<i>Benutzerdefinierte Ansichten</i>	Hier können bestimmte Arten von Ereignissen gefiltert zusammengefasst werden. In den Standardeinstellungen werden hier administrative Ereignisse gezeigt, die alle kritischen Fehler- und Warnungseignisse aller für die Administration wichtigen Protokolle umfassen.
<i>Windows-Protokolle</i>	Hier finden Sie die wichtigsten Informationen zum aktuellen Zustand des Betriebssystems.
<i>Anwendungs- und Dienstprotokolle</i>	Je nach aktivierten Funktionen und installierten Anwendungen können sich hier spezifische Protokolle finden.
<i>Abonnements</i>	Ein Abonnement definiert eine Sammlung von Ereignissen, die auf verschiedenen Computern im Netzwerk stattfinden. Angezeigt werden diese unter <i>Windows-Protokolle - Weitergeleitete Ereignisse</i> .

Windows-Protokolle

<i>Anwendung</i>	In diese Sektion schreiben Anwendungen wie das Sicherungsprogramm, der Druckmanager und der Windows-Anmeldeprozess ihre Ereignismeldungen.
<i>Sicherheit</i>	Im Sicherheitsprotokoll finden Sie Informationen zu sicherheitssensiblen Aktivitäten. Teilweise werden diese automatisch überwacht, teilweise können Sie die Überwachung von Objekten festlegen. Beispiele dafür sind die Protokollierung des Systemstarts, die Überwachung des Zugriffs auf Dateien, die Überwachung von Benutzeraktionen oder Anmeldevorgängen.
<i>Installation</i>	Jede Installation einer Software wird im Installationsprotokoll vermerkt. Zusätzlich finden sich hier solche Informationen wie beispielsweise ein ausstehender Neustart, der für das Fertigstellen einer Installation benötigt wird.
<i>System</i>	Hier werden systeminterne Ereignisse eingetragen. Dabei werden nicht nur Fehler, sondern auch erfolgreiche Ereignisse protokolliert (z. B. der Start eines Dienstes).
<i>Weitergeleitete Ereignisse</i>	Wenn Sie Abonnements eingerichtet haben, finden sich hier die Ereignisse.

Ereignisebenen

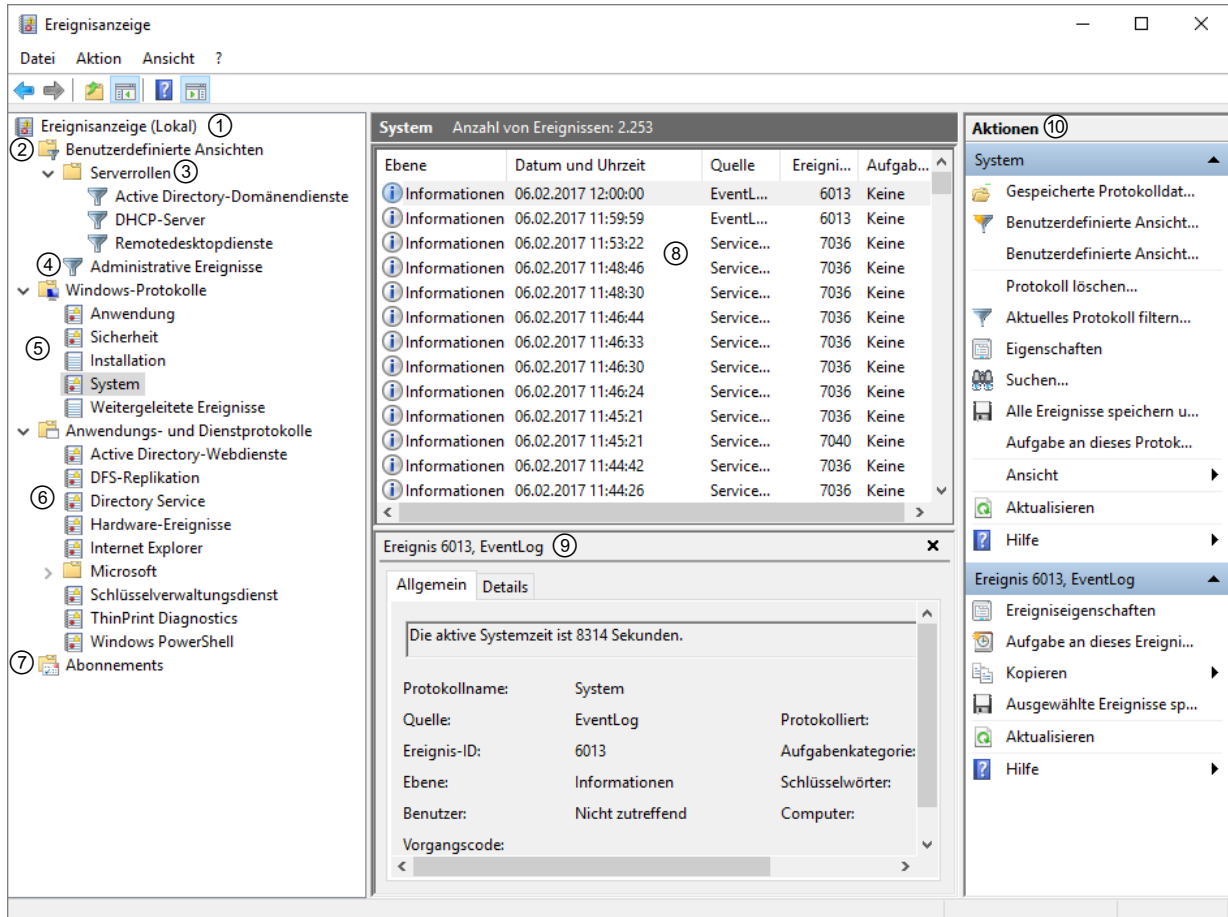
Ereignisebenen (früher Ereignistypen) beschreiben, wie ein Ereignis einzustufen ist. Insbesondere für benutzerdefinierte Ansichten können Sie bestimmte Ebenen filtern.

<i>Kritisch</i>	Kritische Ereignisse werden protokolliert, wenn eine Anwendung, ein Dienst oder eine Komponente einen Fehler aufweist, der einen Neustart oder Weiterbetrieb unmöglich macht. Ein Beispiel wäre das Überlaufen der Systempartition.
<i>Fehler</i>	Diese Meldung erscheint, wenn ein schwerwiegender Fehler aufgetreten ist, etwa ein Dienst nicht gestartet werden konnte.
<i>Warnung</i>	Hier wird vor nicht kritischen Ereignissen gewarnt, die später zu Fehlern führen könnten. Ein Beispiel wäre, dass kein Domänencontroller gefunden werden konnte.
<i>Information</i>	Auf dieser Ereignisebene wird festgehalten, wenn eine Aktion erfolgreich durchgeführt wurde, beispielsweise ein Treiber geladen wurde.
<i>Überwachung erfolgreich</i>	So ein Eintrag wird ins Sicherheitsprotokoll eingetragen, wenn eine Legitimierung durchgeführt wurde, z. B. bei erfolgreicher Anmeldung mit korrektem Kennwort.
<i>Überwachung gescheitert</i>	Ein Eintrag dieser Art bedeutet, dass ein Benutzer versucht hat, etwas zu tun, wozu er nicht legitimiert war, etwa sich mit einem falschen Kennwort anzumelden.

18.2 Ereignisanzeige

Protokoll in der Ereignisanzeige einsehen

- Öffnen Sie die Ereignisanzeige über *Server-Manager - Tools - Ereignisanzeige*, oder durch Eingabe von `eventvwr.msc` im Startmenü.



- ① zeigt, mit welchem Rechner Sie verbunden sind (hier ist es der lokale Rechner). Wenn Sie diesen Eintrag markieren, erhalten Sie im mittleren Bereich eine Zusammenfassung wichtiger Ereignisse.
- ② Benutzerdefinierte Ansichten umfassen alle Serverrollen und administrativen Ereignisse. Bei den Serverrollen ③ werden die Meldungen genau wie im Server-Manager nach Rollen getrennt angezeigt.
- ④ *Administrative Ereignisse* fasst alle Fehler und Warnungen zusammen.
- ⑤ zeigt die einzelnen Windows-Protokolle. Wurden auf dem Rechner Abonnements eingerichtet, enthält der Eintrag *Weitergeleitete Ereignisse* die abonnierten Ereignisse von anderen Rechnern.
- ⑥ *Anwendungs- und Dienstprotokolle* fasst Ereigniseinträge entsprechend zusammen.
- ⑦ Hier befinden sich die auf dem Rechner eingerichteten Abonnements.

Im mittleren Bereich der Ereignisanzeige ⑧ sehen Sie alle Ereignismeldungen in der aktiven Kategorie (hier ist es *Anwendung*). Die Einträge lassen sich nach zahlreichen Kriterien sortieren. Darunter sehen Sie eine Beschreibung des Ereignisses ⑨ mit weiteren Details.

Im rechten Bereich der Ereignisanzeige ⑩ werden je nach aktiver Kategorie verschiedene Aktionen angeboten.

Ereignisdetails anzeigen

- Wählen Sie in der Baumstruktur eine Struktur und klicken Sie doppelt auf den Protokolleintrag.

Der obere Bereich liefert Ihnen Informationen über einen Fehler oder über einen Vorgang, der erfolgreich ausgeführt werden konnte.

Genauere Informationen über das Ereignis können Sie über den Hyperlink *Onlinehilfe* beziehen, der Sie zur Microsoft Knowledge Base weiterleitet.

Wenn Sie zusätzliche Sicherheitsereignisse protokollieren möchten, müssen Sie dies zuerst mit Überwachungsrichtlinien aktivieren.

Protokoll konfigurieren

- Klicken Sie mit der rechten Maustaste auf das Protokoll, das Sie anpassen möchten, und wählen Sie *Eigenschaften* aus.
- Legen Sie im Register *Allgemein* im Bereich *Protokollgröße* ① fest, was die maximale Protokollgröße sein soll und nach welchen Kriterien das Protokoll überschrieben bzw. gelöscht werden soll.

Im Register *Abonnements* können Sie einstellen, ob und von welchen anderen Computern ebenfalls Ereignismeldungen gesammelt werden sollen, sodass sie Ihnen ebenfalls zur Ansicht lokal zur Verfügung stehen.

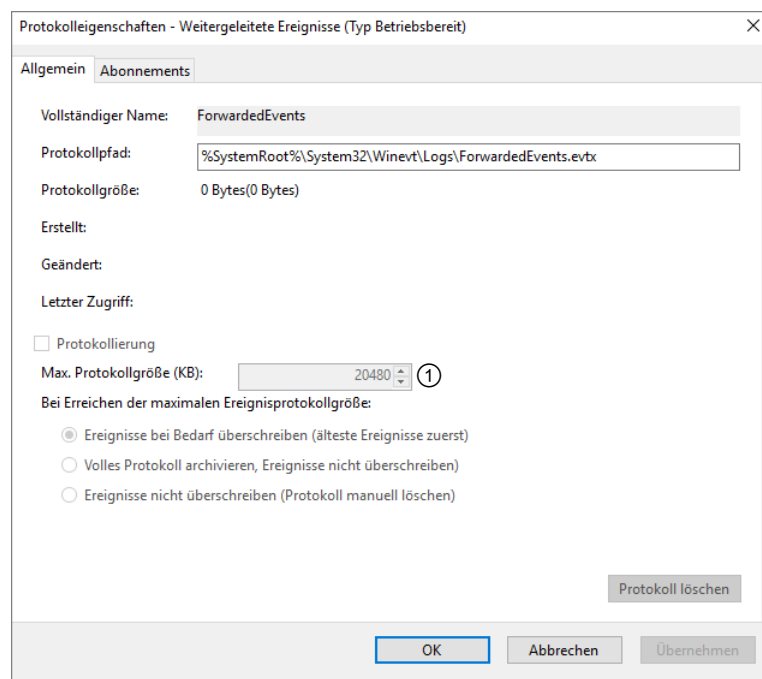
Protokoll manuell löschen

Alle Protokolle (auch solche, für die Sie einen automatischen Löschvorgang definiert haben) können Sie manuell löschen. Dabei werden alle Protokolleinträge des betreffenden Protokolls gelöscht.

- Rufen Sie das Kontextmenü des Protokolls auf, das Sie löschen möchten, und aktivieren Sie den Kontextmenüpunkt *Protokoll löschen*.



Ereignisdetails



Eigenschaften eines Protokolls

18.3 Ereignisabonnements

Überblick

Obwohl der neu gestaltete Server-Manager die Ereignismeldungen mehrerer Computer anzeigen kann, verfügt auch Windows Server 2022 über die aus älteren Server-Versionen bekannten Ereignisabonnements. Hiermit können Sie bestimmte Ereigniseinträge verschiedener Computer auf einem Rechner sammeln und in eigenen Protokollen abspeichern. Das erleichtert die spätere Auswertung von Ereigniseinträgen ungemein, da Sie sich nicht mehr mit verschiedenen Computern verbinden müssen und nur diejenigen Ereignisse abonnieren, die Ihnen relevant erscheinen.

Grundsätzlich lassen sich zwei Arten von Abonnements unterscheiden:

- ✓ Sammlungsinitiiert: Der Sammlungscomputer ruft die Ereignisse von den angegebenen Quellcomputern ab.
- ✓ Quellcomputerinitiiert: Die Quellcomputer schicken die konfigurierten Ereignisse zum Sammlungscomputer.

Abonnements verwalten Sie am einfachsten im Server-Manager im Knoten *Diagnose - Ereignisanzeige - Abonnements*.

Computer vorbereiten

Für den Einsatz von Abonnements müssen alle beteiligten Computer vorbereitet werden. Das erledigen Sie am einfachsten in einer Eingabeaufforderung.

- ▶ Geben Sie auf dem **Sammlungscomputer** `winrm qc` und anschließend `wecutil qc` ein. Beantworten Sie die Nachfragen mit `j` (Ja) bzw. `y` (Yes).
- ▶ Geben Sie auf dem **Quellcomputer** `winrm qc` ein. Beantworten Sie die Nachfragen mit `y` (Yes).

Erstellen Sie sammlungsinitiierte Abonnements, benötigt der Sammlungscomputer (bzw. das dort konfigurierte Abo-Konto) die Berechtigung, die Ereignisprotokolle der Quellcomputer zu lesen. Dabei lassen sich zwei Fälle unterscheiden:

- ✓ Keine Einträge im Sicherheitsprotokoll sammeln: Dann bietet sich die (rechnerlokale) Gruppe *Ereignisprotokollleser* an. Mitglieder dieser Gruppe erhalten keinen Zugriff auf das Sicherheitsprotokoll.
- ✓ Alle Einträge sammeln: Hier ist der Einsatz der (rechnerlokalen) Gruppe *Administratoren* am einfachsten.



In vielen Beschreibungen zu Ereignisabonnements erhalten Sie den Hinweis, dass Sie das Computerkonto des Sammlungs-Servers zum Mitglied der lokalen Administratoren auf den Quellcomputern machen sollten. Das ist ein gefährlicher Tipp, denn damit kann jeder Benutzer, der auf dem Sammlungs-Server angemeldet ist, als Administrator auf den Quellcomputer zugreifen. Führen Sie das Abonnement besser unter einem speziellen Benutzerkonto aus, das Mitglied der lokalen Administratoren ist. Am einfachsten erreichen Sie das mit einem Benutzerkonto, das Mitglied in der Gruppe *Domänen-Admins* ist.

Die rechnerlokalen Gruppen auf den Quellcomputern finden Sie im Server-Manager im Knoten *Konfiguration - Lokale Benutzer und Gruppen - Gruppen*.

Sammlungsinitiiertes Ereignisabonnement erstellen

Sammlungsinitiierte Abonnements erstellen Sie in der Ereignisanzeige des Sammlungscomputers.

- ▶ Klicken Sie im Kontextmenü des Knotens *Abonnements* auf *Abonnement erstellen*.
- ▶ Vergeben Sie einen Namen ① und optional eine Beschreibung für das Abo.
- ▶ Legen Sie unter *Zielprotokoll* ② fest, in welchem Protokoll das Abo gespeichert wird.
Wenn Sie Abonnements über die Eigenschaften eines Ereignisprotokolls erstellen, ist der Eintrag hier fest vorgegeben.

Im Bereich *Abonnementtyp und Quellcomputer* ③ legen Sie fest, ob dieses Abonnement sammlungs- oder quellcomputerinitiiert ist. Über die Schaltfläche *Computer auswählen* ④ wählen Sie den Sammlungscomputer aus. Dort können Sie auch einen Konnektivitätstest durchführen.

Unter *Erweitert* ⑤ können Sie weitere Einstellungen vornehmen, die noch beschrieben werden.

- ▶ Nach einem Klick auf *Ereignisse auswählen* ⑥ definieren Sie, welche Ereignisse dieses Abo sammelt. Es öffnet sich das Fenster *Abfragefilter*.

Bei *Protokolliert* ① legen Sie einen Zeitraum fest. In neu definierten Abfragen interessieren Sie Ereignisseinträge, die mehrere Wochen alt sind, eventuell nicht.

Unter *Ereignisebene* ② legen Sie fest, welche Art/ Ebene von Ereignisseinträgen Sie sammeln wollen. Informationen und auch Warnungen sind in Abos eher uninteressant.

Legen Sie fest, ob Sie Ereignisse protokoll- oder quellspezifisch abonnieren ③. Über den Drop-down-Pfeil ④ beim jeweiligen Eintrag schränken Sie Ihre Auswahl weiter ein.

Im Bereich darunter können Sie weitere Filterkriterien festlegen, z. B. nur bestimmte Ereignis-IDs ⑤ oder Schlüsselwörter ⑥, die dann abhängig von der vorher getroffenen Auswahl sind.

Denselben Abfragefilter erhalten Sie, wenn Sie Filter für Ereignisprotokolle erstellen.

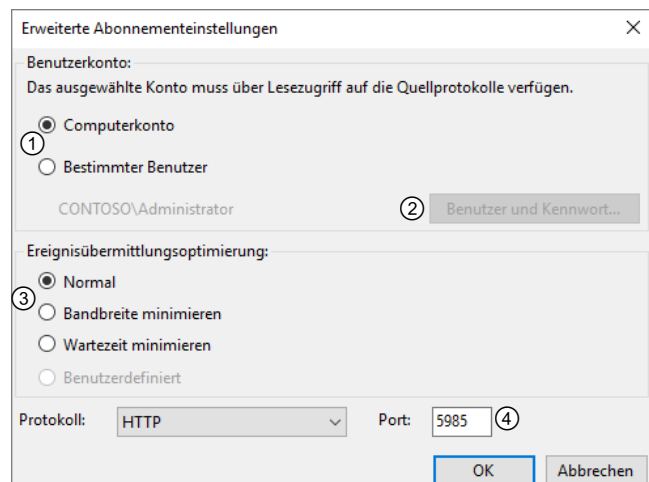
Erweiterte Abonnementseinstellungen

In den Abonnementeigenschaften können Sie über die Schaltfläche *Erweitert* weitere Einstellungen vornehmen.

Über ① legen Sie fest, wer die Ereigniseinträge auf den Quellcomputern liest. Wenn Sie hier ein Benutzerkonto angeben ②, achten Sie darauf, dass dessen Kennwort nicht abläuft.

In den Übermittlungsoptionen ③ legen Sie fest, wie schnell neue Ereignisse auf dem Sammlungs-Server erscheinen.

Wenn Sie Veränderungen am Protokoll oder Port vornehmen ④, müssen Sie das den Quellcomputern mitteilen. Verwenden Sie dazu den Befehl `winrm` mit den entsprechenden Schaltern.



Mit diesen Einstellungen ist das Abonnement fertig definiert. Durch einen Doppelklick darauf können Sie seine Einstellungen verändern.

Quellcomputerinitiiertes Ereignisabonnement erstellen

Quellcomputerinitiierte Abos erstellen Sie grundsätzlich auf dieselbe Art wie sammlungsinitiierte Abos. Dabei gibt es zwei wesentliche Unterschiede:

- ✓ In den Abonnementeigenschaften müssen Sie keine Computer festlegen.
- ✓ Sie müssen den Quellcomputern über Gruppenrichtlinien mitteilen, wer der Sammlungscomputer ist.

Die notwendigen Einstellungen finden Sie im Gruppenrichtlinienobjekt unter *Computerkonfiguration - Richtlinien - Administrative Vorlagen - Windows-Komponenten - Ereignisweiterleitung*.

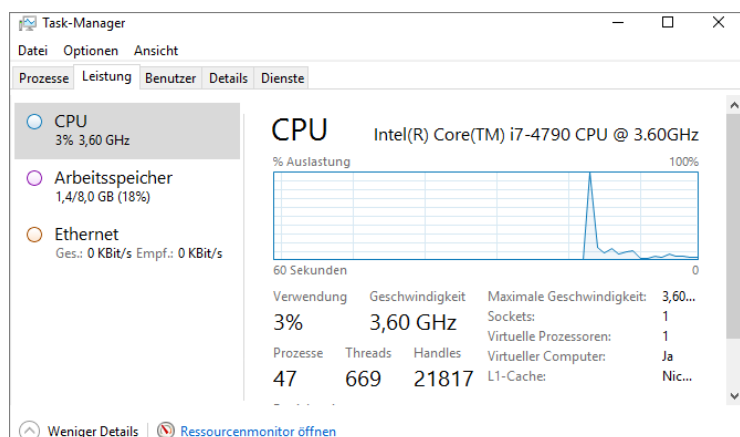
18.4 Leistungsdaten und der Systemmonitor

Auswertungen

Die Analyse laufender Systeme, insbesondere das Aufspüren von Engpässen und Schwachstellen, ist ein wichtiges Aufgabenfeld der Systemadministration.

Einen schnellen Überblick über aktuelle Werte des lokalen Rechners erhalten Sie mit dem **Task-Manager**, den Sie über einen Rechtsklick in die Taskleiste oder `Strg` `↑` `Esc` aufrufen.

Der Task-Manager ist neu gestaltet und gibt einen schnellen Überblick über die Systemauslastung und laufende Prozesse und Dienste.



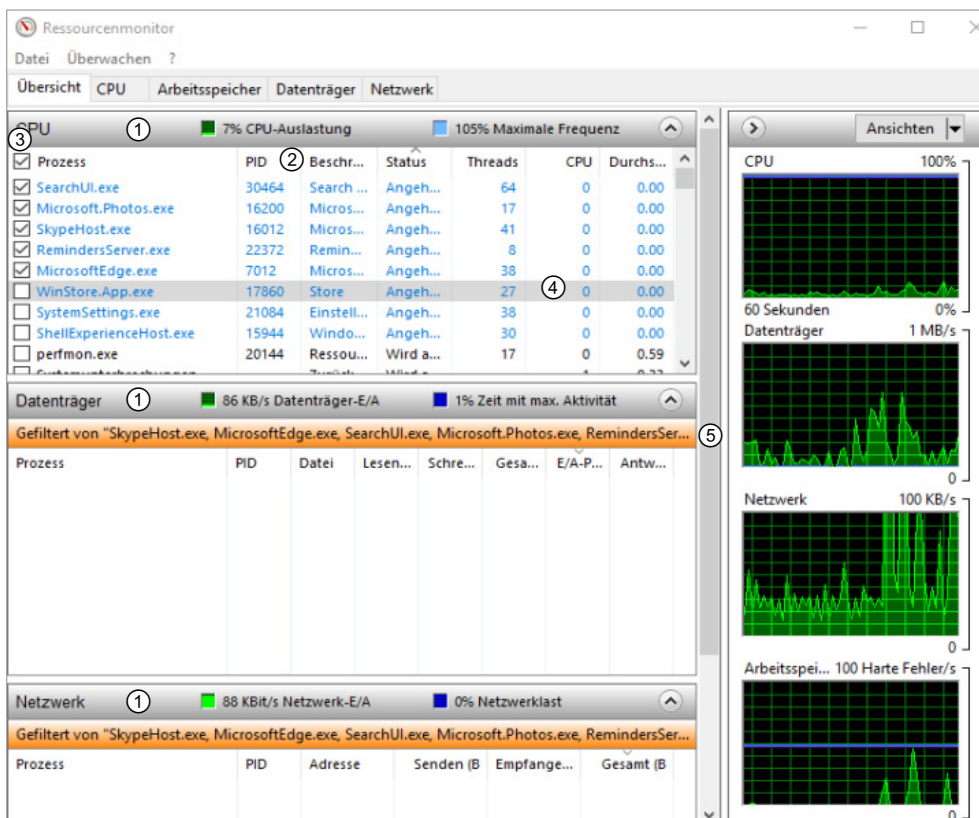
Die Registerkarte „Leistung“ im Task-Manager

Eine grafische Übersicht der Auslastung von CPU, RAM und Netzwerk finden Sie auf der Registerkarte *Leistung*. Von dort können Sie über eine Schaltfläche den **Ressourcenmonitor** starten.

Neu hinzugekommen ist die Möglichkeit, den Dateipfad von laufenden Anwendungen und Prozessen zu öffnen. Außerdem können Sie nun den Status aller Dienste anzeigen und verändern. Der neue Task-Manager ist auf jeden Fall einen genaueren Blick wert.

Ressourcenmonitor

Der Ressourcenmonitor (*resmon.exe*) bietet mehr Informationen als der Task-Manager. Der Ressourcenmonitor stellt für den lokalen Computer Echtzeit-Informationen zur Auslastung von Hardwareressourcen (CPU, Arbeitsspeicher, Datenträger und Netzwerk) und Softwareressourcen (Dateihandles und Module) zur Verfügung. Leider lassen sich die damit erfassten Daten nicht speichern.



Die Registerkarte „Übersicht“ im Ressourcenmonitor

- ✓ Jedes Registerblatt enthält mehrere Tabellen ①, die zusätzliche Informationen geben.
- ✓ Mit einem Klick auf einen Spaltenkopf ② sortieren Sie die Tabelle nach dem entsprechenden Kriterium. Nach einem Rechtsklick können Sie weitere Spalten ein- oder vorhandene ausblenden.
- ✓ Über die Kontrollkästchen ③ können Sie Filter definieren, die die Anzeige der anderen Tabellen und Register beeinflussen. Die Werte der markierten Prozesse werden in den Listen ④ und Diagrammen ⑤ orange hervorgehoben. Mit dem obersten Kontrollkästchen einer Liste (vor *Abbild*) deaktivieren Sie alle Filter.
- ✓ Nach einem Rechtsklick können Sie z. B. Prozesse beenden und anhalten oder online nach Informationen zum Prozess suchen.
- ✓ Im Menü *Datei* können Sie Ihre Einstellungen speichern bzw. laden.

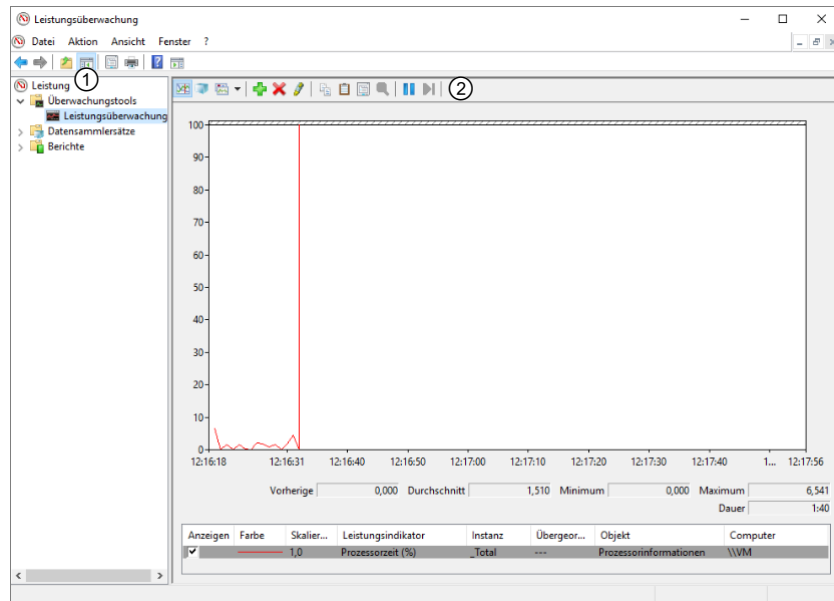
Leistungsüberwachung

Die Leistungsüberwachung dient zum Anzeigen und Aufzeichnen der Systemauslastung. Mit ihr können Sie Messwerte einzelner Systemkomponenten (etwa Prozessorauslastung) in Echtzeit darstellen oder zur späteren Auswertung protokollieren. Darüber hinaus können Sie Warnungen generieren, falls bestimmte Messwerte einen konfigurierbaren Bereich über- bzw. unterschreiten.

- Geben Sie im Startbildschirm **Leistung** ein und klicken Sie auf **Leistungsüberwachung**.
oder Klicken Sie im Server-Manager im Menü **Tools** auf **Leistungsüberwachung**.

Die Leistungsüberwachung lässt sich auch mehrmals öffnen. Dadurch können Sie beispielsweise die Werte von zwei Servern nebeneinander darstellen. Um den Computer auszuwählen, klicken Sie mit der rechten Maustaste auf den Eintrag **Leistung** ① und wählen Sie **Verbindung mit einem anderen Computer herstellen**.

Die Bedienung erfolgt über eine Reihe von Symbolen ②. Eine Beschreibung des Symbols erscheint, wenn Sie mit dem Mauszeiger auf das Symbol zeigen.



Die Leistungsüberwachung von Windows Server 2022

Messdaten definieren

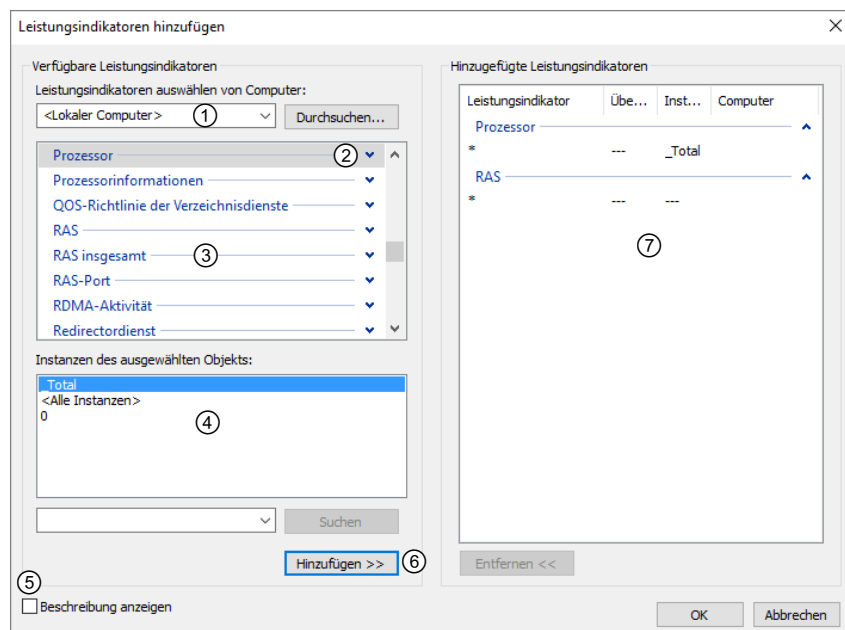
- Klicken Sie auf das Symbol .

Bei ① legen Sie fest, ob Sie Leistungsdaten des lokalen oder eines anderen Rechners erfassen wollen.

Mit dem Pfeilsymbol können Sie einzelne Leistungsobjekte ② aufklappen und erhalten dann Zugriff auf die Leistungsindikatoren ③ des Objekts.

Ihre Markierung kann mehrere Instanzen ④ umfassen (z. B. Multiprozessorsystem). Bei mehreren Instanzen erfasst der Eintrag **_Total** alle Instanzen gleichzeitig.

Unter ⑤ können Sie sich eine Beschreibung anzeigen lassen.



Mit **Hinzufügen** ⑥ nehmen Sie die Markierung in die Überwachung ⑦ auf und können eine weitere Auswahl treffen.

Anzeige des Diagramms verändern

Das Diagramm wird entweder als Kurve (Grafik), als Balkendiagramm oder als Bericht angezeigt.

- Klicken Sie auf *Eigenschaften* (.

Im Register *Grafik* können Sie die Art der Anzeige ändern. Dort können Sie auch die vertikale Skalierung festlegen. Manche Leistungsindikatoren sollten nicht gleichzeitig dargestellt werden. Es macht z. B. keinen Sinn, gleichzeitig einen Prozentwert und den Netzwerkdurchsatz in Bytes/s darzustellen.

Auf den restlichen Registern können Sie die farbliche Gestaltung der Darstellung in weiten Bereichen festlegen.

Datensammlersatz erzeugen

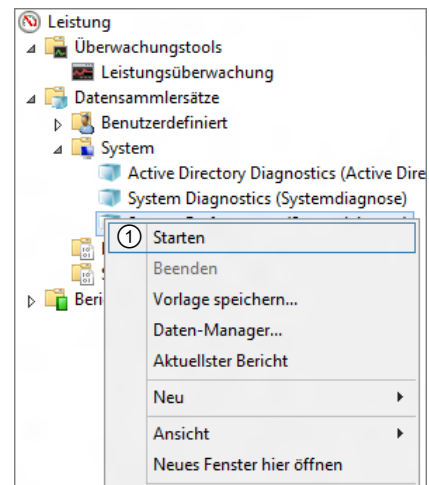
Datensammlersätze (auch Sammlungssätze genannt) sind Bausteine für die Leistungsüberwachung und -berichterstellung. Einige werden bereits mitgeliefert.

- Wählen Sie den Container *Datensammlersätze* und öffnen Sie im Untercontainer *System* das Kontextmenü des Datensammlersatzes, den Sie erzeugen wollen (z. B. *System Performance*).
- Wählen Sie aus dem Kontextmenü den Befehl *Starten* ①.

Sie können wahlweise auch eigene (benutzerdefinierte) Datensammlersätze erzeugen, was aber nicht ganz einfach ist. Benutzen Sie dabei das Kontextmenü im Container *Benutzerdefiniert*.

Dabei legen Sie den Datensammlersatz mithilfe von Indikatoren ähnlich an, wie Sie im Systemmonitor die Leistungsindikatoren definiert haben.

Zusätzlich können Sie einen Zeitplan oder Stopp-Kriterien für die Datensammlung und weitere Eigenschaften definieren.



Die Sammlung beenden	► Klicken Sie im rechten Kontextmenü auf den Punkt <i>Beenden</i> .
Die Protokolldatei laden	► Klicken Sie im Systemmonitor auf das Symbol  und öffnen Sie die entsprechende Protokolldatei.

19 Die Registrierungsdatenbank

19.1 Die Windows Server-2022-Registrierung

Aufbau und Funktion der Registrierung

Informationen zur Konfiguration von System und Software speichert Windows in einer zentralen Datenbank namens Registrierung (Registry). Einträge in der Registrierungsdatenbank steuern das Betriebssystem und Anwendungen sowie den Betrieb von Hardware-Komponenten und Gerätetreibern.

Einträge in der Registrierungsdatenbank

Einträge in der Registrierungsdatenbank werden beispielsweise geändert und ergänzt, wenn ...

- ✓ neue Programme oder Hardware-Komponenten installiert werden,
- ✓ Einstellungen verändert werden,
- ✓ Hardware-Komponenten anders konfiguriert werden.



Die Registrierungsdatenbank kann auch manuell bearbeitet werden, manuelle Eingriffe in die Registrierungsdatenbank sollten jedoch nur mit größter Vorsicht erfolgen. Eine falsche Bearbeitung der Registry kann die Funktionalität von Windows stark beeinträchtigen.

Eine vorteilhafte Methode zur Änderung der Systemkonfiguration ist das Erstellen von Gruppen- oder Systemrichtlinien. Ermitteln Sie deshalb vor einem manuellen Eingriff in die Registrierung immer, ob Sie die gewünschte Einstellung mittels Richtlinien vornehmen können.

Funktion der Unterstrukturen

Die Registrierungsdatenbank besteht aus fünf Hauptschlüsseln mit folgenden Informationen:

Schlüssel	Abgelegte Informationen
HKEY_CLASSES_ROOT	Hier werden Daten zur Konfiguration der Anwendungsprogramme gespeichert, u. a. die Verknüpfung zwischen Dateierdung und zugehörigem Programm.
HKEY_CURRENT_USER	Diese Unterstruktur enthält die Konfiguration des angemeldeten Benutzers. Der Zweig wird als Kopie der entsprechenden Einstellungen aus HKEY_USERS übernommen.
HKEY_LOCAL_MACHINE	Hier liegen die wesentlichen Informationen zur Konfiguration des lokalen Computers. Die Einträge werden bei der Installation neuer Komponenten aktualisiert und sind benutzerunabhängig.
HKEY_USERS	Diese Unterstruktur enthält Einträge zu allen Benutzern, die am Rechner angemeldet waren.
HKEY_CURRENT_CONFIG	Diese Unterstruktur erstellt Windows beim Computerstart. Sie enthält einen Ausschnitt der Einstellungen aus HKEY_LOCAL_MACHINE.

Die Einträge in der Registrierungsdatenbank sind entweder ein Schlüssel oder ein Wert. Die Schlüssel übernehmen die Funktion von Ordnern und sehen im Registrierungs-Editor so aus: . Werte können so  oder so  aussehen.

Wertetypen

Die eigentlichen Konfigurationseinstellungen werden durch eingetragene Werte festgelegt. Dafür verwendet die Windows-Registrierung sechs verschiedene Datentypen:

Datentyp	Eigenschaft
REG_SZ	Wert besteht aus einer Zeichenkette
REG_BINARY	Einzelner binärer Wert
REG_DWORD	Ein „Double Word“, bestehend aus 32 Bit
REG_QWORD	Ein „Quad Word“, bestehend aus 64 Bit
REG_MULTI_SZ	Wert besteht aus mehreren Zeichenketten
REG_EXPAND_SZ	Wert besteht aus einer erweiterbaren Zeichenkette

Schlüssel
Zeichenfolge
Binärwert
DWORD-Wert (32-Bit)
QWORD-Wert (64-Bit)
Wert der mehrteiligen Zeichenfolge
Wert der erweiterbaren Zeichenfolge

Neuen Registry-Eintrag erstellen

Speicherort der Registry

Gespeichert werden die Daten der Registry im Ordner `\Windows\system32\config`. Einzige Ausnahme ist die Unterstruktur `HKEY_CURRENT_USER`, die in der Datei `ntuser.dat` im Benutzerprofil abgelegt ist.

19.2 In der Registry arbeiten

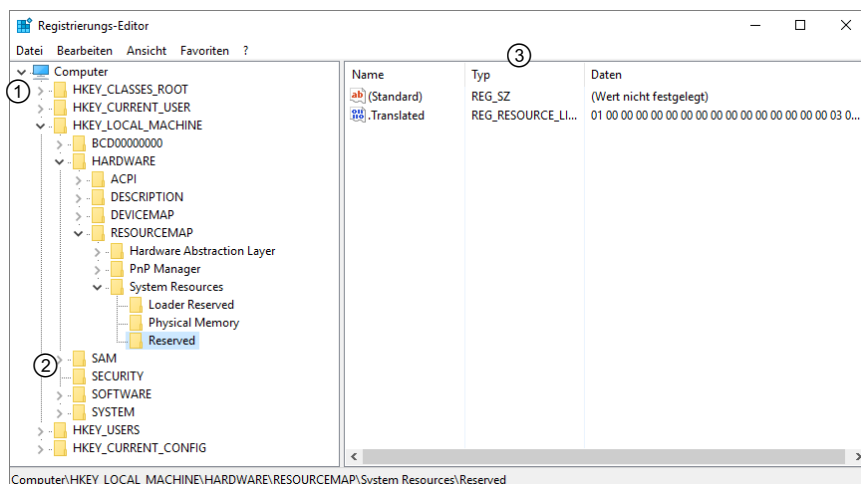
Der Registrierungs-Editor

Die Registry wird mit dem Registrierungs-Editor `regedit.exe` bearbeitet.

- Geben Sie zum Öffnen des Registrierungs-Editors im Startbildschirm `regedit`  ein oder rufen Sie ihn aus der Kommandozeile heraus auf.

Sie sehen die Hauptschlüssel ①, die weitere Schlüssel enthalten, die z. T. mehrfach verschachtelt sind. Die einzelnen Werte und Daten des markierten Schlüssels ② werden auf der rechten Seite angezeigt ③.

Die Navigation im Registrierungs-Editor erfolgt genauso wie im Windows-Explorer. Auch die restliche Bedienung ist vergleichbar. Beispielsweise finden Sie im Menü *Datei* den Kontextmenüpunkt *Drucken* und können dann angeben, ob Sie alles oder nur die ausgewählte Teilstruktur drucken wollen.



Registrierung eines Remotecomputers bearbeiten

Sie können auch die Registrierungsdatenbank eines anderen Computers im Netzwerk bearbeiten. Dafür benötigen Sie entsprechende Berechtigungen auf dem anderen Rechner, und keine Firewall darf die Zugriffe unterbinden.

- ▶ Klicken Sie auf den Menüpunkt *Datei - Mit Netzwerkregistrierung verbinden*.
- ▶ Legen Sie den Computernamen fest und klicken Sie anschließend auf *OK*.
Dabei entsteht eine neue Struktur mit dem Namen des Computers, die den Zugriff ermöglicht.
- ▶ Über *Datei - Von Netzwerkregistrierung trennen* beenden Sie die Verbindung wieder.

Registrierung durchsuchen

Im Registrierungs-Editor können Sie nach Schlüsseln, einzelnen Werten sowie deren Einträgen suchen. Die Suche erfolgt vom markierten Eintrag aus nach unten.

- ▶ Markieren Sie den Startpunkt der Suche.
- ▶ Betätigen Sie **Strg** **F** oder rufen Sie den Menüpunkt *Bearbeiten - Suchen* auf.
- ▶ Geben Sie die gewünschte Zeichenfolge ein.
Im Bereich *Suchoptionen* können Sie die Suche weiter spezifizieren.
- ▶ Mit **F3** setzen Sie die Suche fort und springen zur nächsten Fundstelle.

Werte ändern

- ▶ Öffnen Sie den betreffenden Schlüssel und klicken Sie doppelt auf den Wert, den Sie ändern möchten.

Je nach Datentyp des ausgewählten Wertes wird ein entsprechender Editor geöffnet. Bei DWORD-Werten können Sie zwischen Hexadezimaldarstellung und Dezimaldarstellung wählen. Bei mehrteiligen und einfachen Zeichenfolgen können Sie die Werte als Text eingeben, Binärwerte werden im Hex-Editor bearbeitet.

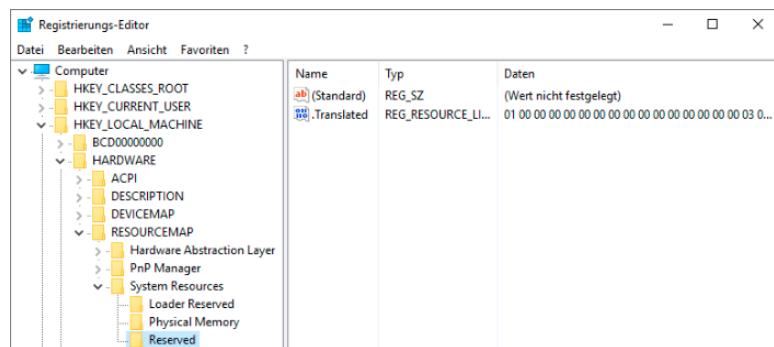
- ▶ Verändern Sie den Wert wie erforderlich und bestätigen Sie mit *OK*.

Schlüssel sichern

Vor dem Bearbeiten oder Erstellen von Einträgen sollten Sie den entsprechenden Schlüssel sichern. Mit der erstellten Datei können Sie die ursprünglichen Daten schnell zurücksetzen. Haben Sie Einträge erstellt, dient die Datei als Referenz für das, was hinzugekommen ist.

- ▶ Markieren Sie den entsprechenden Schlüssel und rufen Sie den Menüpunkt *Datei - Exportieren* auf.
- ▶ Legen Sie im Dialogfenster *Registrierungsdatei exportieren* Speicherort und Dateinamen fest.

Die Abbildung zeigt einen Export der benutzerspezifischen Einstellungen des Windows-Explorers. Mit einem Doppelklick auf eine solche REG-Datei lassen sich deren Einstellungen in die Registry importieren.



Exportierter Schlüssel



Seien Sie sehr vorsichtig, wenn Sie verschiedene Rechner auf diese Art bearbeiten. Beispielsweise sind die Speicherorte für manche Einstellungen nicht unter allen Windows-Versionen identisch.

Schlüssel wiederherstellen

Wenn Sie einen Schlüssel verändert haben und das System sich anschließend nicht erwartungsgemäß verhält, können Sie die ursprüngliche Konfiguration wiederherstellen.

- ▶ Öffnen Sie im Explorer den Ordner, in dem sich die Registrierungsdatei mit dem benötigten Schlüssel befindet.
- ▶ Klicken Sie doppelt auf die Datei und bestätigen Sie die angezeigte Warnung mit *Ja*.

Der Registrierungs-Editor überschreibt jetzt die aktuellen Daten in der Registrierung mit den Informationen aus der gespeicherten Datei und gibt danach eine entsprechende Meldung aus.

Struktur laden

Der Registrierungs-Editor bietet die Möglichkeit, Registrierungseinträge aus einer gespeicherten Registry-Datei zu laden. Sinnvoll einsetzen lässt sich das, um die Registry-Einstellungen eines nicht angemeldeten Benutzers einzusehen, zu speichern oder zu bearbeiten. Das funktioniert nur, wenn entweder die Struktur *HKEY_LOCAL_MACHINE* oder *HKEY_USERS* markiert ist.

- ▶ Markieren Sie den Eintrag *HKEY_USERS* und wählen Sie im Menü *Datei - Struktur laden*.
- ▶ Öffnen Sie im Fenster *Struktur laden* den Ordner des gewünschten Benutzerprofils, markieren Sie die Datei *ntuser.dat* und klicken Sie auf *Öffnen*.

Es erscheint ein Fenster, in dem Sie den Schlüsselnamen angeben müssen. Dafür bietet sich der Name des Benutzers an.

Sie haben eine neue Struktur unter *HKEY_USERS* erstellt, in der Sie Zugriff auf die Registrierungseinstellungen des Benutzers haben, so als wäre er gerade angemeldet und würde seinen Schlüssel *HKEY_CURRENT_USER* bearbeiten.

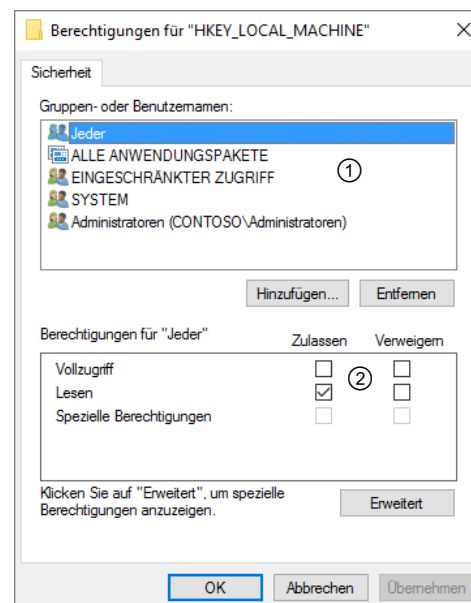
Wenn Sie die eben erstellte Struktur markieren, können Sie diese mit *Datei - Struktur entfernen* wieder entladen.

19.3 Schlüsselsicherheit verwalten

Zugriffsberechtigungen für Schlüssel verwalten

Registrierungsschlüssel lassen sich vor unbefugtem Zugriff sichern und das System lässt sich vor Fehlern durch manuelle Beschädigung der Registrierung schützen. Auf der anderen Seite sollten Sie genau wissen, was Sie tun, denn für den reibungslosen Betrieb von Windows muss das System und auch der Benutzer ständig auf viele Bereiche der Registry zugreifen können. Sie sollten daher nur ausgewählte Bereiche vor dem Zugriff schützen und nur in Sonderfällen die Leseberechtigung entziehen.

- ▶ Klicken Sie im Registrierungs-Editor mit der rechten Maustaste auf den Schlüssel, für den Sie Zugriffsberechtigungen erteilen möchten.
- ▶ Rufen Sie im Kontextmenü den Menüpunkt *Berechtigungen* auf.
- ▶ Markieren Sie im Listefeld *Gruppen- oder Benutzernamen* ① die Gruppe oder Benutzer, deren Berechtigungen Sie ändern wollen.
- ▶ Klicken Sie auf *Hinzufügen*, um neue Benutzer oder Gruppen in die Liste aufzunehmen.
- ▶ Konfigurieren Sie mithilfe der Kontrollfelder *Zulassen* und *Verweigern* ② die Berechtigungen.



Zugriffsberechtigungen verwalten

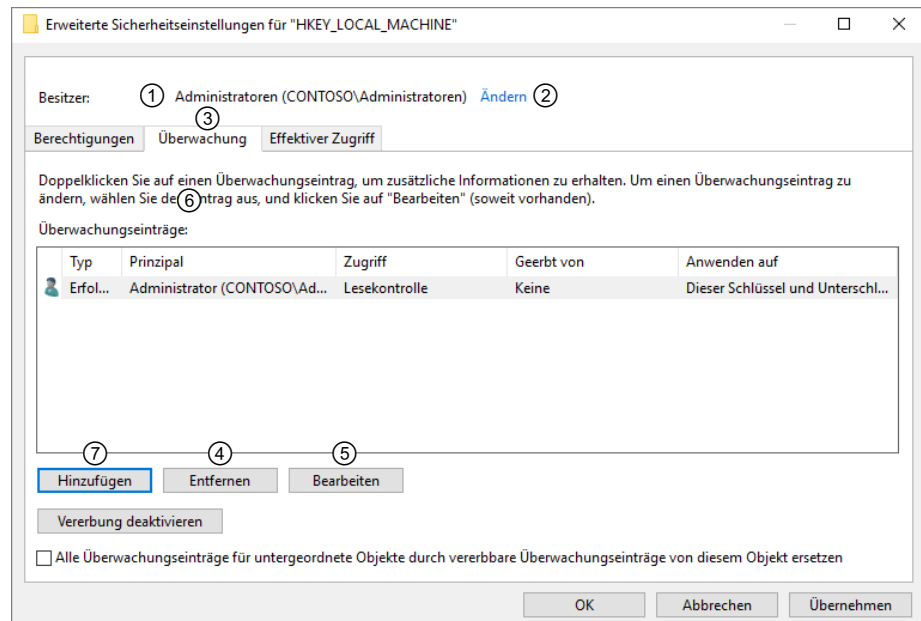
Wenn Sie spezielle Berechtigungen vergeben wollen, klicken Sie auf die Schaltfläche *Erweitert* und verfahren Sie wie bei der Vergabe spezieller NTFS-Berechtigungen.

- Klicken Sie auf *OK*.

Besitz an einem Schlüssel übernehmen

Falls ein Registrierungsschlüssel nicht im Besitz der Gruppe *Administratoren* ist, können Sie ihn als Administrator möglicherweise nicht verwalten. Sie müssen dann den Besitz an diesem Schlüssel übernehmen, beispielsweise um ihn zu löschen. Seien Sie hier besonders vorsichtig, denn diese Bereiche der Registry werden aus gutem Grund auf diese Weise geschützt.

- Klicken Sie im Kontextmenü des Schlüssels, den Sie in Besitz nehmen wollen, auf *Berechtigungen* und im nächsten Dialog auf *Erweitert*.
Der aktuelle Besitzer ① des Schlüssels wird Ihnen angezeigt.
- Klicken Sie auf *Ändern* ② und wählen Sie im Folgedialog die Gruppe der Administratoren. Bestätigen Sie mit *OK*.
- Klicken Sie auf *Übernehmen* und *OK*.

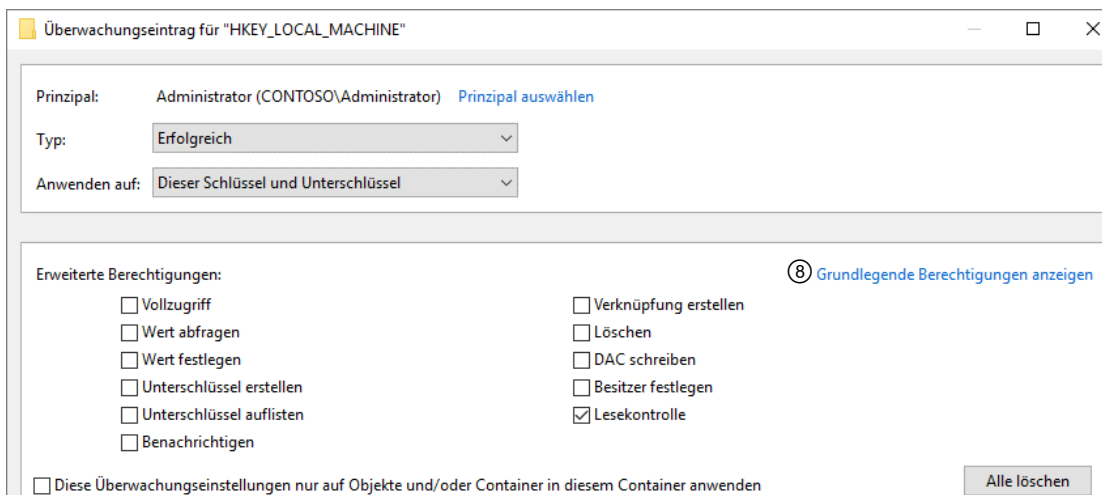


Besitz an einem Schlüssel übernehmen und Überwachung einrichten

Schlüsselzugriffe überwachen

Der Zugriff auf die Registrierung und einzelne Schlüssel kann überwacht werden, um den Urheber von Änderungen ausfindig zu machen.

- Klicken Sie in den erweiterten Sicherheitseinstellungen des Schlüssels, für den Sie den Zugriff überwachen möchten, auf die Registerkarte *Überwachung* ③. Entfernen ④ oder bearbeiten ⑤ Sie vorhandene Überwachungseinträge ⑥.
- Klicken Sie auf *Hinzufügen* ⑦.
Das Dialogfenster *Überwachungseintrag für* wird geöffnet.
- Legen Sie unter *Prinzipal auswählen* fest, für welche Benutzer die Überwachung gilt.
- Legen Sie im Listenfeld *Typ* fest, welche Aktion überwacht werden soll. Wählen Sie zwischen *Alles*, *Erfolgreich* und *Fehlgeschlagen* aus.
- Wählen Sie unter *Anwenden auf*, ob die Überwachung für Schlüssel, Unterschlüssel oder beides gelten soll.
- Klicken Sie auf den Link ⑧ (Abbildung Folgeseite), um zwischen grundlegenden und erweiterten Berechtigungen umzuschalten.
- Achten Sie darauf, dass das Kontrollfeld *Lesekontrolle* aktiviert ist.
- Übernehmen Sie die Einstellungen mit *OK*, *Übernehmen* und *OK* und schließen Sie den Registrierungs-Editor.



Überwachungseintrag bearbeiten

Beachten Sie, dass zusätzlich eine Gruppenrichtlinie definiert werden muss, die eine Überwachung von Objektzugriffen zulässt, bevor die Überwachung in Kraft treten kann. Gruppenrichtlinien werden mit dem entsprechenden Snap-In der MMC erstellt.

19.4 Regedit, die Kommandozeile und hilfreiche Tools

Kommandozeile

Regedit beherrscht einige Schalter, die Sie vielleicht gewinnbringend einsetzen können:

- ✓ `regedit /m` öffnet eine (weitere) Instanz des Registrierungs-Editors. Damit können Sie beispielsweise mehrere Schlüssel nebeneinander darstellen und vergleichen.
- ✓ `regedit /s <Datei>` importiert eine (exportierte) REG-Datei ohne Rückfrage.

Hinweise und Tipps



Wie alle manuellen Eingriffe sind auch die folgenden Hinweise mit Vorsicht zu betrachten und sollten ohne vorhergehende Tests nicht in Produktivumgebungen eingesetzt werden.

Die meisten Programme speichern ihre Konfiguration in der Registry unter `HKEY_CURRENT_USER\Software`. Wollen Sie nun bestimmte Einstellungen für Benutzer vorgeben, heißt das, dass Sie bestimmte Registry-Einträge setzen müssen. Der bevorzugte Weg dafür wären administrative Vorlagen des Herstellers, die Sie über Gruppenrichtlinien verteilen. Da solche Vorlagen aber nicht immer erhältlich sind, können Sie die entsprechenden Schlüssel einfach von einem korrekt konfigurierten Benutzer exportieren und den Benutzern bei der Anmeldung einspielen. Das erfolgt dann über ein Anmeldeskript, das Sie am besten über eine Gruppenrichtlinie zuweisen.

Manche Software läuft nur, wenn man als Mitglied der Gruppe *Administratoren* oder Hauptbenutzer angemeldet ist. Das liegt fast immer daran, dass die Anwendung Dateien im Programmordner und/oder Einträge unter `HKEY_LOCAL_MACHINE\Software` verändern will. Benutzer haben hier nur Leseberechtigungen. Um herauszufinden, welche Zugriffe scheitern, können Sie den Process Monitor benutzen. Dabei handelt es sich um ein Tool, das Sie von der Sysinternals-Seite unter <https://docs.microsoft.com/de-de/sysinternals/> herunterladen können. Dort befinden sich noch viele weitere Tools, die die Arbeit eines Administrators erheblich erleichtern können. Dieser Prozessmonitor protokolliert alle Datei- und Registry-Zugriffe in einem Livesystem. Über entsprechende Filter und Sortioptionen (interessant sind nur fehlgeschlagene Zugriffe) finden Sie die Problemstellen recht schnell heraus – zumindest beim zweiten Mal. Dann können Sie die Berechtigungen für die betroffenen Dateien und/oder Registry-Schlüssel entsprechend anpassen, was sich auch über Gruppenrichtlinien erledigen lässt.

20 Datenträger verwalten

20.1 Datenträger

Datenträger und Speichermedien

Datenträger sind alle Speichermedien, auf denen Daten dauerhaft abgelegt werden können, z. B. magnetische Festplatten, optische Medien sowie Flash-Speicher wie Solid-State-Disks oder USB-Sticks. Im Gegensatz dazu stehen flüchtige Speichermedien, auf denen gespeicherte Daten mit Abschalten der Betriebsspannung verloren gehen, wie der Hauptspeicher (RAM, Random Access Memory), Grafikkartenspeicher oder Cache-Speicher auf Prozessoren. Auf Datenträgern können Volumes eingerichtet werden; diese können mit einem Dateisystem formatiert werden und sind dann über Laufwerksbuchstaben oder -pfade ansprechbar.

Ein Volume kann in der Ordnerstruktur bereitgestellt (gemountet) werden. Das bedeutet, dass ihm kein Laufwerksbuchstabe zugeordnet wird, sondern dass es in einem beliebigen **leeren** Ordner innerhalb eines anderen NTFS-formatierten Volumes eingehängt werden kann. Dieser Ordner wird dann als Bereitstellungspunkt bezeichnet. Der Benutzer bemerkt das Mounten allenfalls an einem geänderten Ordnersymbol, ansonsten ist der Vorgang transparent.

Basisdatenträger und Basisvolumes

Die klassisch eingerichtete Standardfestplatte ist unter Windows ein Basisdatenträger. Jeder Basisdatenträger kann bis zu vier primäre Partitionen enthalten. Da die Bootinformationen im sogenannten Master Boot Record (MBR) liegen, wird dieser Datenträgertyp unter Windows auch als MBR-Datenträger bezeichnet. Sind mehr als vier Partitionen auf einem Basisdatenträger erwünscht, kann eine primäre Partition durch eine erweiterte Partition ersetzt werden, die wiederum in beliebig viele logische Laufwerke unterteilt werden kann. Folglich können maximal drei primäre Partitionen und eine erweiterte Partition eingerichtet werden. Bei GPT-Datenträgern besteht diese Begrenzung nicht.

Partitionen und logische Laufwerke werden auch Basisvolumes genannt. Um ein Basisvolume verwenden zu können, muss es formatiert und mit einem Laufwerksbuchstaben oder -pfad versehen werden.

Dynamische Datenträger und dynamische Volumes

Dynamische Datenträger erweitern die Möglichkeiten, den Speicherplatz von Datenträgern einzuteilen und zur Verfügung zu stellen. Basisdatenträger können in dynamische Datenträger konvertiert werden. Alle Basisvolumes auf diesem Datenträger werden dann zu dynamischen Volumes. Eine Rückkonvertierung ist nur unter Verlust aller Daten möglich. Von dynamischen Datenträgern kann nicht gebootet werden, außerdem ist die Versorgung mit Datenträger-Tools von Drittanbietern wegen des proprietären Microsoft-Formats eingeschränkt.

Dynamische Datenträger können Teil einer einzigen Festplatte sein, sie können aber auch mehrere Festplatten umfassen. Dabei können verschiedene Festplatten einfach nur logisch zusammengefasst werden (übergreifender Datenträger, Spanned Volume) oder das Volume kann als Stripeset konfiguriert werden, was einem Software-RAID (**R**edundant **A**rray of **I**ndependent **D**isks) entspricht. Durch die neuen Speicherpools und virtuellen Datenträger verlieren die herkömmlichen Volumetypen wie Stripeset und RAID 5 stark an Bedeutung, sind aber noch verfügbar. Windows kann weder von einem Software-RAID noch von den neuartigen virtuellen Datenträgern booten, daher kommt für das Systemlaufwerk zur Geschwindigkeitssteigerung nur eine SSD oder ein Hardware-RAID mit eigenem Controller infrage.

In früheren Windows-Versionen war der große Vorteil der dynamischen Volumes, dass sie verkleinert und vergrößert werden konnten, während Basisvolumes mit Bordmitteln nicht verändert werden konnten. Seit Windows Server 2012 ist dies möglich. Dynamische Volumes unterstützen vielfältige Möglichkeiten bei der Partitionierung und Verwaltung. Daher haben sie auch heute noch ihre Berechtigung. Mit Basisvolumes lassen sich z. B. keine Volumes in NTFS-Ordern bereitstellen oder über mehrere Laufwerke verteilen.

GPT-Datenträger

GPT-Datenträger (GUID-Partitionstabellen-Datenträger) sind die neuere Form der Festplattenadressierung und unterstützen Datenträger und Partitionen, die größer als 2 Terabyte sind, außerdem können mehr als vier Basispartitionen angelegt werden, daher sind keine erweiterten Partitionen erforderlich. GPT verdrängt zunehmend den alten MBR-Festplattentyp.

Partitionen und logische Laufwerke

Jede MBR-Basisfestplatte kann in bis zu vier Partitionen unterteilt werden. Bei Partitionen wird zwischen primären und erweiterten Partitionen unterschieden. Wenn mehr als vier Partitionen benötigt werden, muss eine der Partitionen als erweiterte Partition eingerichtet und dann in logische Laufwerke unterteilt werden. Es darf nur eine erweiterte Partition pro Festplatte geben. Außerdem kann nur von einer primären, aktiven Partition gebootet werden und im System kann nur eine der primären Partitionen aktiv sein.

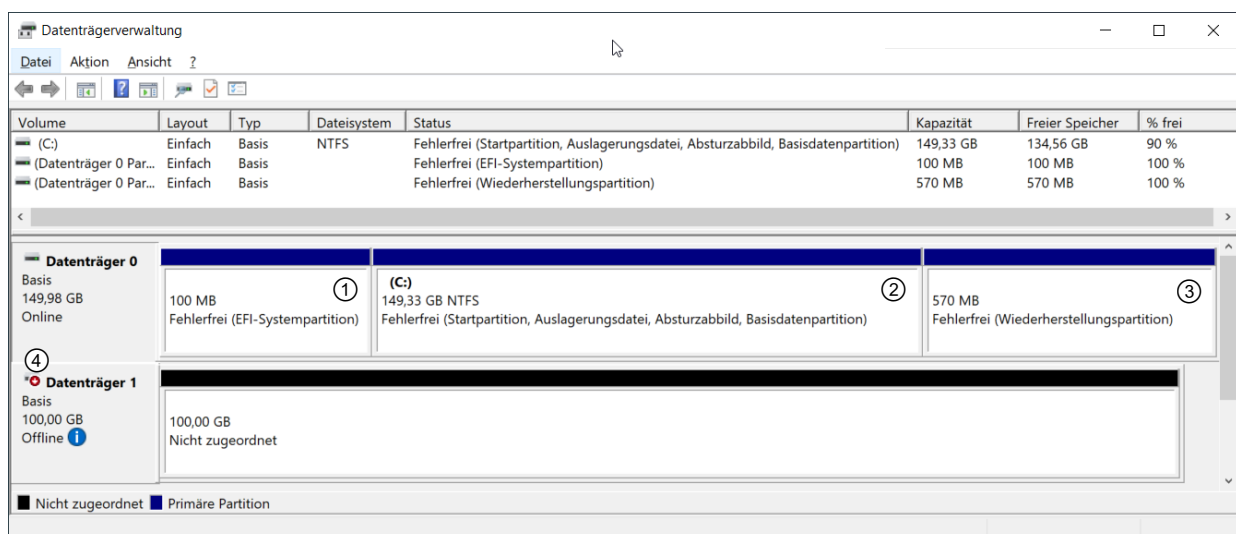
20.2 Datenträgerverwaltung

Überblick

Wie in den älteren Windows-Server-Versionen ist die Datenträgerverwaltung für die Einrichtung und Partitionierung der Laufwerke zuständig. Die Datenträgerverwaltung wird jedoch langfristig durch die Verwaltungsfunktionen und Assistenten der Datei- und Speicherdienste im Server-Manager ersetzt werden, die vollkommen unabhängig von der Datenträgerverwaltung arbeitet. Nur dort können die neuen Möglichkeiten zur Bereitstellung von Speicherplätzen mit Speicherpools und virtuellen Datenträgern genutzt werden.

Die Datenträgerverwaltung erreichen Sie als Snap-In der Computerverwaltung oder über den Befehl `diskmgmt.msc`. Klicken Sie dann auf *Festplattenpartitionen erstellen und formatieren*.

Die nachfolgende Abbildung zeigt die Laufwerkskonfiguration eines Server 2022.



Im oberen Bereich erhalten Sie u. a. Informationen über einzelne Volumes, zum Layout, dem Typ des Datenträgers und dem (freien) Speicherplatz. Die Spalte *Status* gibt an, ob Fehler auf dem Volume vorliegen und ob es besondere Aufgaben (Startpartition, Systempartition etc.) übernimmt.

Der untere Bereich zeigt Informationen zu den einzelnen Datenträgern (Festplatten), z. B. welche Volumes mit welcher Größe sich darauf befinden und ob nicht zugewiesene Speicherbereiche und offline geschaltete Datenträger vorhanden sind. Die Farbcodierung erleichtert den Überblick. Datenträger werden von null aufwärts gezählt. Datenträger 1 ist also die zweite Festplatte im Rechner.

Windows Server 2022 wurde in diesem Beispiel mit den Standardeinstellungen im GPT-Layout installiert.

Am Anfang der Festplatte erstellt der Assistent eine EFI-Partition von 100 MB. Dieser Partition wird kein Laufwerksbuchstabe zugewiesen ①. Der nachfolgende Teil des Speicherplatzes von Datenträger 0 wird überwiegend der Systempartition C: zugewiesen ②. Hieran schließt eine 570 MB große Wiederherstellungspartition ③ an, die ebenfalls keinen Laufwerksbuchstaben erhält.

Der kleine rote Pfeil  ④ auf Datenträger 1 zeigt an, dass der Datenträger offline ist.

Datenträgerinformationen	
Datenträger	Datenträger 0
Typ:	Basis
Partitionsstil	GUID-Partitionstabelle (GPT)
Kapazität	153584 MB
Verfügbarer	3 MB
Status:	Online
Reservierter Speicher:	100 MB

Volumes	
Volume	Kapazität
	570 MB
(C:)	152911 MB

Vor dem Entfernen von Festplatten sollten Sie diese mit einem Rechtsklick offline schalten. Bei dynamischen Datenträgern ist dieser Schritt besonders wichtig, da sich Informationen zum Datenträger auch auf den anderen Festplatten befinden können. Das Offlineschalten löscht diese Einträge.

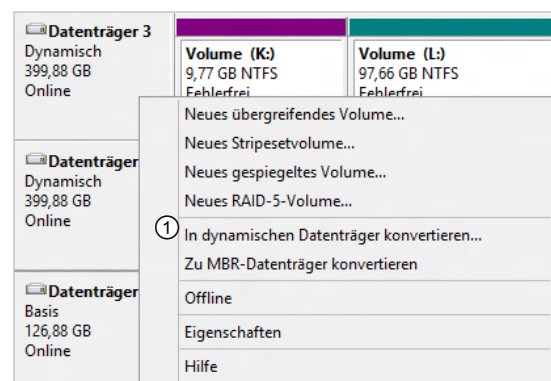
In einer Eingabeaufforderung sind Sie mit *diskpart.exe* und *format.exe* deutlich flexibler als in der Datenträgerverwaltung. Sie können allerdings auch leichter einen schwerwiegenden Fehler begehen.

Basisdatenträger in dynamischen Datenträger umwandeln

- ▶ Klicken Sie mit der rechten Maustaste auf einen Basisdatenträger und wählen Sie den Kontextbefehl für die Konvertierung ①.
- ▶ Bestätigen Sie die Auswahlliste mit *OK*.

Die Festplatte wird konvertiert. Bei einer Konvertierung von Basis zu dynamisch werden vorhandene Partitionen und logische Laufwerke automatisch in Volumes überführt.

Es ist nicht möglich, einen dynamischen Datenträger ohne Datenverlust in einen Basisdatenträger umzuwandeln.



Neues Volume erstellen

- ▶ Klicken Sie mit der rechten Maustaste auf einen freien Bereich der Festplatte und wählen Sie im Kontextmenü den Volumetyp aus.
- ▶ Der Assistent heißt Sie willkommen, klicken Sie auf *Weiter*.
- ▶ Legen Sie die Größe des Volumes fest. Der Assistent schlägt den gesamten zusammenhängenden freien Speicherbereich vor.
- ▶ Weisen Sie im nächsten Fenster einen Laufwerksbuchstaben zu. Sie können auch keinen zuweisen oder das Volume in einem leeren NTFS-Ordner bereitstellen.
- ▶ Legen Sie im nächsten Schritt die Formatierungsoptionen fest und klicken Sie auf *Weiter*.

Das Standard-Dateisystem unter Windows ist trotz der Einführung von ReFS auch weiterhin NTFS ①. Sie können ReFS für Datenlaufwerke verwenden, allerdings unterstützen nicht alle Windows-Editionen dieses Dateisystem. Die Verwendung von ReFS auf Systempartitionen wird nicht unterstützt.

FAT32 oder exFAT sind nur in Spezialfällen sinnvoll, und andere Clustergrößen ② werden nur selten benötigt.

- ▶ Wählen Sie eine aussagekräftige Bezeichnung, die nicht zu lang sein sollte und keine Umlaute und Sonderzeichen enthält ③.

The screenshot shows the 'Assistent zum Erstellen neuer einfacher Volumes' dialog box, specifically the 'Partition formatieren' step. The text says: 'Sie müssen die Partition erst formatieren, um Daten auf der Partition zu speichern.' Below this, it asks: 'Geben Sie an, ob und mit welchen Einstellungen dieses Volume formatiert werden soll.' There are two radio buttons: 'Dieses Volume nicht formatieren' (unselected) and 'Dieses Volume mit folgenden Einstellungen formatieren:' (selected). Under the selected option, there are three settings: 'Zu verwendendes Dateisystem:' set to 'NTFS' with a circled 1, 'Größe der Zuordnungseinheit:' set to 'Standard' with a circled 2, and 'Volumebezeichnung:' set to 'Volume' with a circled 3. At the bottom, there are two checkboxes: 'Schnellformatierung durchführen' (checked with a circled 4) and 'Komprimierung für Dateien und Ordner aktivieren' (unchecked with a circled 5). At the very bottom are three buttons: '< Zurück', 'Weiter >', and 'Abbrechen'.

Mit ④ wird das Volume beim Formatieren nicht auf fehlerhafte Sektoren überprüft und verkürzt die Zeit für die Formatierung enorm. Mit ⑤ aktivieren Sie die Komprimierung für alle Dateien und Ordner auf dem Volume. Im Windows-Explorer geht das auch für einzelne Ordner oder Dateien.

- ▶ Überprüfen Sie auf der letzten Seite die Zusammenfassung und klicken Sie auf *Fertig stellen*. Das Volume wird eingerichtet und formatiert.

Das Aktivieren der Komprimierung und die Schnellformatierung sind nicht uneingeschränkt zu empfehlen. Die Komprimierung kann den Festplattendurchsatz verlangsamen, sie erzeugt in jedem Fall zusätzliche CPU-Last. Es ist empfehlenswerter, eine zusätzliche oder größere Festplatte einzubauen, als den Prozessor zu belasten.

Mit der Option *Schnellformatierung* wird auf eine vorherige Überprüfung des Datenträgers verzichtet. Verwenden Sie diese Option vorsichtshalber nur, wenn Sie sicher sind, dass es keine fehlerhaften Sektoren gibt, z. B. weil Sie vor Kurzem eine Überprüfung mit `chkdsk .exe` durchgeführt haben.

Bestehendes Volume in Verzeichnisbaum einbinden

Volumes lassen sich nicht nur über Laufwerksbuchstaben ansprechen. Sie können auch nachträglich in einem Ordner bereitgestellt werden.

- ▶ Klicken Sie mit der rechten Maustaste auf das Volume und wählen Sie im Kontextmenü den Punkt *Laufwerksbuchstaben und -pfade ändern*.
- ▶ Klicken Sie auf *Hinzufügen*.
- ▶ Klicken Sie anschließend auf *Durchsuchen* und geben Sie einen leeren Ordner als Ziel an.
- ▶ Verlassen Sie das Menü mit *OK*.

Ein zugewiesener Laufwerksbuchstabe wird dadurch nicht entfernt. Dies können Sie über einen erneuten Aufruf des Dialogfensters *Laufwerksbuchstaben und -pfade ändern* erreichen.

The screenshot shows the 'Assistent zum Erstellen neuer einfacher Volumes' dialog box, specifically the 'Laufwerksbuchstaben oder -pfad zuordnen' step. The text says: 'Sie können dieser Partition einen Laufwerksbuchstaben oder -pfad zuordnen, um auf die Partition schneller zugreifen zu können.' There are three radio buttons: 'Folgenden Laufwerksbuchstaben zuweisen:' (unselected, with a dropdown showing 'E'), 'In folgendem leeren NTFS-Ordner bereitstellen:' (selected), and 'Keinen Laufwerksbuchstaben oder -pfad zuweisen' (unselected). Below the selected option is a text input field and a 'Durchsuchen...' button.

Volume in Ordner bereitstellen

Beachten Sie, dass es nicht möglich ist, über *Ändern* in einem Schritt den bisherigen Laufwerksbuchstaben zu entfernen und das Volume im Verzeichnisbaum bereitzustellen. Diese Aufgabe erfordert zwei Schritte.

20.3 Dateisysteme und Konvertierung

Das robuste Dateisystem ReFS

Das ReFS (Resilient File System) ist eine Neuentwicklung von Microsoft, die langfristig das bekannte NTFS ersetzen soll. Zum jetzigen Zeitpunkt wird NTFS weiterhin benötigt, da Windows nicht von ReFS booten kann. Das robuste Dateisystem ReFS soll die Verwaltung von Speicherplatz ermöglichen, der über die gesamte Netzwerkinfrastruktur des Unternehmens verteilt sein kann. Besonderes Augenmerk lag bei der Entwicklung auf der Datenintegrität und Ausfallsicherheit. In Verbindung mit den neu eingeführten Speicherpools und virtuellen Datenträgern ergibt sich mit ReFS ein universelles Datenspeichermodell mit folgenden Eigenschaften:

- ✓ hohe Zuverlässigkeit und Schutz vor Datenverlusten durch Metadaten Speicherung und Integritätsströme,
- ✓ hohe Skalierbarkeit und Flexibilität durch Thin Provisioning und erweiterte Maximalgrößen,
- ✓ Beibehaltung vieler NTFS-Funktionen, Weglassen veralteter Funktionen,
- ✓ hohe Verfügbarkeit durch Beseitigung von Fehlern ohne Offlinezeiten, beschleunigtes Chkdsk,
- ✓ vorbeugende Fehlererkennung durch Integritätsprüfungen und automatische Bereinigung.

ReFS soll auf lange Sicht NTFS vollständig ersetzen. Da Windows Server 2022 nicht von einer ReFS-Partition booten kann, kann zum jetzigen Zeitpunkt noch nicht auf NTFS verzichtet werden.

Eine Umwandlung von NTFS zu ReFS und umgekehrt ist nicht vorgesehen. Es ist jedoch problemlos möglich, in beiden Richtungen Dateien unter Beibehaltung der meisten Attribute zu kopieren. Ausgenommen sind die Verschlüsselung mittels dem verschlüsselnden Dateisystem EFS (Encrypted File System), das von ReFS nicht unterstützt wird, und die NTFS-Komprimierung.

Von FAT zu NTFS oder ReFS umwandeln

Sie können bestehende lokale FAT32-Partitionen ohne Datenverlust in NTFS umwandeln. Eine Rückwandlung von NTFS nach FAT32 ist mit Windows-Bordmitteln nicht möglich.

- Geben Sie in der Eingabeaufforderung den folgenden Befehl ein:

```
convert <Laufwerksbuchstabe> /fs:NTFS /v
```

Mit der Option /v (verbose, ausführlich) erhalten Sie ausführliche Informationen über den Konvertierungsprozess.

Sie können auch in der Befehlszeile oder der PowerShell die Formatierung durchführen und ReFS verwenden. Dazu nutzen Sie in der PowerShell den Befehl

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

oder

```
Format-Volume -DriveLetter <Buchstabe> -FileSystem ReFS -Full
```

Eine Schnellformatierung führen Sie in der Befehlszeile mit

```
Format /fs:ReFS /q <Buchstabe>:
```

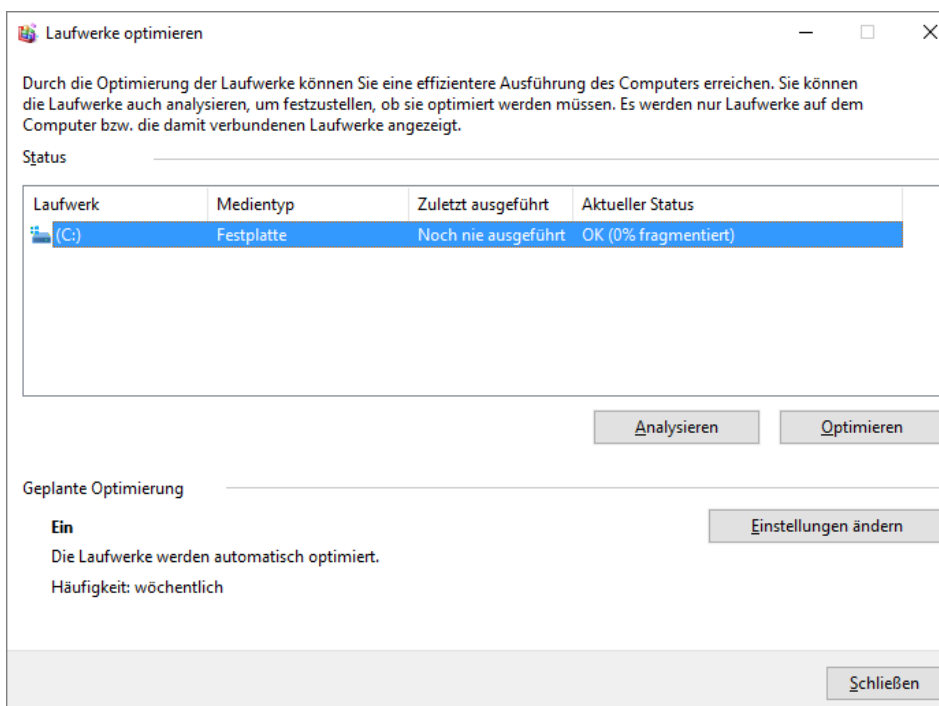
durch. Sie können für Software-RAIDs in Windows Server 2022 auch das ReFS-Dateisystem verwenden. Die Erstellung und Verwaltung ist identisch mit der Verwendung von NTFS.

20.4 Datenträger pflegen

Datenträger optimieren

Bei der Datenträgeroptimierung werden die einzelnen Volumes untersucht und falls erforderlich defragmentiert. Dieser Vorgang findet standardmäßig wöchentlich statt, Sie können ihn aber auch manuell starten und einstellen.

- ▶ Geben Sie im Startmenü `dfrgui` ein und wählen Sie *Laufwerke defragmentieren*. Alternativ können Sie im Explorer oder in der Datenträgerverwaltung im Kontextmenü eines Volumes auf *Eigenschaften* und dann auf der Registerkarte *Tools* auf *Optimieren* klicken.
- ▶ Wählen Sie ein Laufwerk und klicken Sie auf *Analysieren* oder *Optimieren*. Sie können auch mehrere Laufwerke anwählen.



Laufwerksoptimierung

Unter *Einstellungen ändern* können Sie bestimmen, welche Laufwerke in der geplanten Optimierung enthalten sein sollen und wie oft diese durchgeführt wird.

Es ist hier nicht möglich, mehrere Zeitpläne für verschiedene Laufwerke zu erstellen.

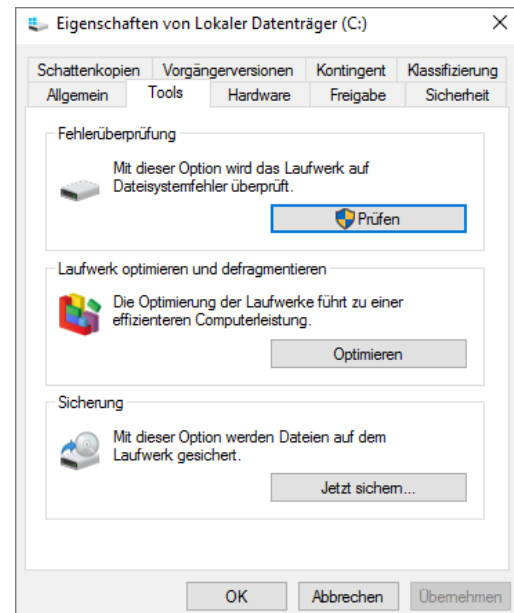
Die Defragmentierung ist nur bei herkömmlichen Magnetfestplatten sinnvoll. Windows deaktiviert daher automatisch die Defragmentierung von SSDs, da hier eine Defragmentierung nur schädliche Auswirkungen hätte. Es wird außerdem erkannt, ob es sich bei dem Datenträger um ein virtuelles Laufwerk handelt.

Zur effizienten Durchführung der Defragmentierung werden vom System mindestens 15 % freier Speicherplatz auf dem Volume benötigt. Wenn diese nicht verfügbar sind, sollten Sie vorher Daten auf andere Festplatten auslagern. Um die Systempartition, von der kaum Programme entfernt werden können, jederzeit defragmentieren zu können, sollte sie ausreichend groß dimensioniert sein.

Datenträger auf Fehler überprüfen

Eine manuelle Prüfung ist normalerweise nicht nötig, denn Windows führt diese Prüfung im Bedarfsfall automatisch durch. Manuelle Prüfungen sollten Sie wenn möglich durchführen, wenn keine Benutzer auf Daten des zu prüfenden Volumes zugreifen. Wollen Sie die Überprüfung sofort durchführen, müssen Sie dafür sorgen, dass alle Dateien geschlossen sind, oder die Prüfung beim nächsten Neustart durchführen lassen.

- ▶ Klicken Sie im Explorer oder in der Datenträgerverwaltung im Kontextmenü eines Volumes auf *Eigenschaften* und wählen Sie auf der Registerkarte *Tools* die Schaltfläche *Prüfen*.
- ▶ Klicken Sie auf *Laufwerk scannen*.
- ▶ Klicken Sie nach Durchführung der Prüfung auf *Schließen*. Unter *Details anzeigen* können Sie das Ereignisprotokoll für die Prüfung einsehen.



Das Register „Tools“ eines Volumes

Falls momentan Schreib-/Lesevorgänge auf dem betreffenden Volume durchgeführt werden, erhalten Sie eine Meldung, dass nicht sofort überprüft werden kann. Nun können Sie festlegen, ob die Überprüfung beim nächsten Hochfahren des Computers vorgenommen werden soll.

Datenträgerkontingente verwenden

Das NTFS-Dateisystem bietet die Möglichkeit, mit Kontingenten zu arbeiten, allerdings ist dieser Mechanismus heute nicht mehr zeitgemäß. Die Kontingentverwaltung lässt sich viel effektiver über den Ressourcen-Manager für Dateiserver umsetzen.

20.5 Schattenkopien einsetzen

Momentaufnahmen des Datenbestandes

Schattenkopien ermöglichen den Rückgriff auf ältere Versionen einer Datei, beispielsweise wenn eine Datei überschrieben und geändert wurde. Über einen Rechtsklick auf die betroffene Datei lässt sich im Kontextmenü die Vorgängerversion wiederherstellen. Es öffnet sich ein Fenster, in dem ältere Versionen angezeigt werden. Abhängig vom zugewiesenen Speicherplatz für die Schattenkopien werden bis zu 64 Vorgängerversionen gespeichert. Bei gelöschten Dateien klicken Sie auf den Ordner, in dem die Datei gespeichert war.

Schattenkopien können sich für die Dateiwiederherstellung auf Dateiservern als sehr nützlich erweisen, selbst wenn sie für die Benutzer nicht zur Verfügung stehen. Schattenkopien sind kein Ersatz für Backups, jedoch lassen sich einzelne Dateien schnell wiederherstellen, falls das Tages-Backup noch nicht durchgeführt wurde.

Unter Windows XP wurde der Volumeschattenkopiedienst eingeführt und ist seit Windows Vista in einer wesentlich leistungsfähigeren Version Bestandteil aller Server- und Client-Betriebssysteme von Microsoft.

Damit die Schattenkopien verfügbar sind, muss die Serverrolle *Datei- und Speicherdienste - Datei- und iSCSI-Dienste - Dateiserver-VSS-Agent-Dienst* aktiv sein.

Schattenkopien aktivieren

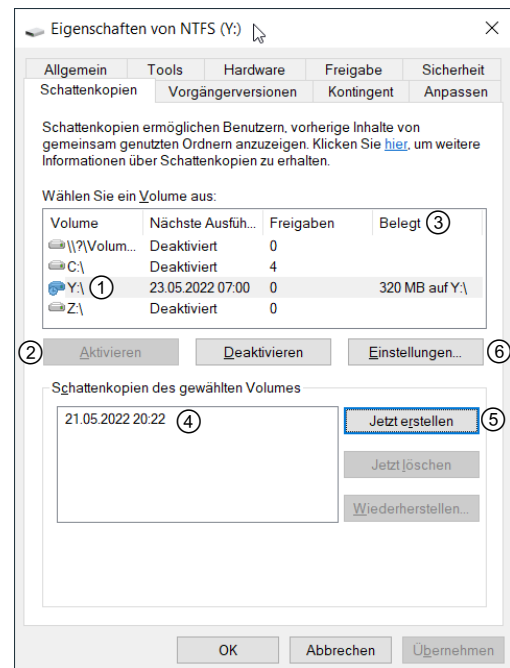
- ▶ Öffnen Sie die Eigenschaften eines Laufwerks und wechseln Sie in das Register *Schattenkopien*.
- ▶ Markieren Sie im Listefeld ① das betreffende Volume und klicken Sie auf *Aktivieren* ②.

Wenn Sie die Schattenkopien für ein Volume aktivieren, erstellt der Dienst *Volumeschattenkopie* ein erstes Abbild des Datenbestandes und legt es im versteckten Ordner *System Volume Information* auf dem betreffenden Laufwerk ab.

Die Spalte *Belegt* ③ zeigt, wie viel Speicherplatz die Schattenkopien momentan belegen. In der Liste ④ sehen Sie, wie viele Schattenkopien vorhanden sind und wann diese erstellt wurden.

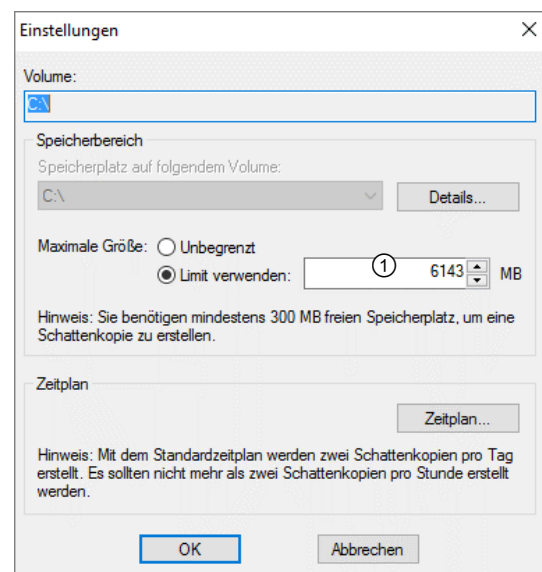
Mit *Jetzt erstellen* ⑤ erzeugen Sie eine Schattenkopie.

Mit der Schaltfläche *Einstellungen* ⑥ können Sie die Eigenschaften der Schattenkopien konfigurieren.



Speicherplatz und Zeitplan konfigurieren

- ▶ Klicken Sie auf *Einstellungen* (siehe ⑥ der oberen Abbildung).
- ▶ Klicken Sie auf *Speicherplatz auf folgendem Volume*, um das Volume zu ändern.
- ▶ Klicken Sie auf *Details...*, um weitere Informationen abzurufen.
- ▶ Stellen Sie auf Wunsch das Speicherplatzlimit für die Schattenkopien ein ①.
- ▶ Klicken Sie auf *Zeitplan*, um die Zeiten und Intervalle zu ändern.
Voreingestellt ist eine Schattenkopie an jedem Werktag morgens um 07:00 Uhr.
- ▶ Klicken Sie auf *OK*, um die Einstellungen zu übernehmen.



20.6 Speicherplätze (Storage Spaces)

Der Bedarf an Speicherplatz pro Benutzer steigt kontinuierlich und es ist eine ständige Herausforderung, den nötigen Speicherplatz bereitzustellen, zu erweitern und zu verwalten. Neben leistungsfähigen und teuren Speicherlösungen kommen in vielen Betrieben auch Kombinationen von Dateiservern und Network Attached Storage (NAS) zum Einsatz. Für diese Umgebungen haben Systeme ab Windows Server 2012 mit **Speicherplätzen**, **Speicherpools** und **virtuellen Datenträgern** interessante neue Wege zur Bereitstellung von Speicherplatz zu bieten. Hierbei können beliebig viele Datenträger zusammengefasst und auf unterschiedlichste Weise mit dem Server verbunden werden. Dadurch ist es zunehmend unwichtiger zu wissen, auf welchem physischen Datenträger eine Datei tatsächlich gespeichert ist. Viel wichtiger ist, dass die Informationen stets auf einfache Weise zugänglich sind und eine ausreichende Daten- und Ausfallsicherung gewährleistet ist.

Neue Funktionen seit Windows Server 2012 sind:

- ✓ **Datendeduplizierung:** spart Speicherplatz, da identische Daten nur einmal gespeichert werden;
- ✓ **iSCSI-Zielserver:** stellt über den iSCSI-Standard (Internet SCSI) Speicherplatz für andere Server und Anwendungen im Netzwerk bereit;
- ✓ **Speicherplätze und Speicherpools:** Speichervirtualisierung, bei der physische Datenträger zu Speicherpools zusammengefasst werden, in denen wiederum Speicherplätze (virtuelle Datenträger) erstellt werden;
- ✓ **einheitliche Remoteverwaltung der Datei- und Speicherdienste im Server-Manager:** ermöglicht es Ihnen, mehrere Dateiserver, einschließlich ihrer Rollendienste und ihres Speichers, von einem Remotestandort aus über ein einziges Fenster zu verwalten;
- ✓ **Windows PowerShell-Cmdlets für Datei- und Speicherdienste:** stellt Windows PowerShell-Cmdlets bereit, mit denen die meisten Verwaltungsaufgaben für Datei- und Speicherserver ausgeführt werden können;
- ✓ **SSD-Erkennung und -Unterstützung** für schnellere Speicherzugriffe.

Speicherpools

Hierbei handelt es sich um eine Sammlung mehrerer physischer Datenträger, die zu einem einzigen Speicherbereich zusammengefasst werden. Bei den Datenträgern kann es sich um eingebaute oder externe Festplatten, Solid-State-Disks (SSD), USB-Sticks und andere Flash-Speicher handeln. Möglich (wenn auch nicht sinnvoll) ist sogar die Verwendung von virtuellen Festplatten. Optische Laufwerke sind nicht geeignet (auch nicht mit wiederbeschreibbaren Medien). Die Größe eines Speicherpools und die Anzahl von Datenträgern ist praktisch unbegrenzt.

Virtuelle Datenträger

Jeder Speicherpool kann einen oder mehrere virtuelle Datenträger enthalten. Diese logischen Datenträger können mit einem Laufwerksbuchstaben versehen werden und wie üblich vom System angesprochen werden. Aus Sicht von Windows unterscheidet sich so ein virtueller Datenträger nicht von einer gewöhnlichen Festplattenpartition. Virtuelle Datenträger werden hauptsächlich verwendet, um mit der Vergabe von Laufwerksbuchstaben und Bezeichnungen sowohl für Anwendungen als auch für den Benutzer den gewohnten Rahmen zu schaffen. Als Dateisystem ist ReFS wegen seiner Sicherungsmechanismen empfehlenswert, Sie können aber auch NTFS verwenden.

Die virtuellen Datenträger wurden bei den Preview-Versionen von Windows Server 2012 und Windows 8 noch als Storage Spaces bezeichnet, während Microsoft diese Bezeichnung bei der Verkaufsversion von Windows Server 2012 als einen Oberbegriff für das Speichersubsystem (die Kombination aus Speicherpool und enthaltenen virtuellen Datenträgern) verwendet. Die Bezeichnung „virtuelle Datenträger“ kann ebenfalls leicht zu Verwechslungen mit den virtuellen Festplattendateien im VHD- bzw. VHDX-Format führen. Vollends verwirrend wird es, weil die virtuellen Datenträger bei Windows 8 als Speicherplätze bezeichnet werden.

Schlanke Speicherzuweisung mit Thin Provisioning

Bei der Erstellung virtueller Datenträger kann ähnlich wie bei dynamischen virtuellen Festplatten (VHD oder VHDX) mehr Speicherplatz zugeteilt werden, als physisch im Speicherpool verfügbar ist. Sobald der physische Speicherplatz zur Neige geht, wird vom Speicherplatz eine Warnmeldung ausgegeben. Daraufhin kann der Speicherplatz aufgestockt werden, indem weitere Festplatten angeschlossen werden. Dieses Konzept nennt man **Thin Provisioning** oder schlanke Speicherzuweisung. Alle virtuellen Datenträger in einem Speicherpool teilen den physisch vorhandenen Speicherplatz unter sich auf.

Wenn also auf einem virtuellen Datenträger durch das Löschen von Dateien Platz freigemacht wurde, steht dieser Platz anschließend auch den anderen virtuellen Datenträgern zur Verfügung.

Planung des Speicherplatzes

- Es gibt eine Reihe von Überlegungen, die Sie vor der Einrichtung des Speicherplatzes berücksichtigen sollten:
 - ✓ Vor der Einrichtung eines Speicherpools sollten Sie alle dafür vorgesehenen Datenträger mit dem System verbinden bzw. einbauen. Bevorzugen Sie für Speicherpools interne Laufwerke.
 - ✓ Alle Daten auf einem Datenträger gehen verloren, sobald er einem Speicherpool hinzugefügt wird.
 - ✓ Alle Daten eines Datenträgers, der aus einem Speicherpool entfernt wurde, sind unlesbar.
 - ✓ Vermeiden Sie den Zusammenschluss von Datenträgern mit völlig unterschiedlichen Leistungsdaten in einem Speicherpool, z. B. keine 1-Terabyte-Festplatte zusammen mit einem 1-GB-USB-Stick.
 - ✓ Alle Datenträger des Speicherpools müssen ständig angeschlossen und eingeschaltet sein. Externe Datenträger dürfen also nicht entfernt werden, solange der Speicherpool existiert.

Datensicherheit

Die Datensicherheit kann mithilfe von Spiegelungsverfahren (mehrfache Speicherung auf verschiedenen Datenträgern) oder Paritätsinformationen, die eine Rekonstruktion der Daten auch nach Ausfall eines Datenträgers ermöglichen, erhöht werden. Die dabei eingesetzten Verfahren erfüllen in etwa dieselbe Funktion wie die RAID-Level 1 und 5, sind aber nicht gleichzusetzen.

Bei der Spiegelung (**Mirror**) werden die Daten auf mindestens zwei Datenträgern gespeichert, sodass selbst bei Ausfall eines Datenträgers die Daten noch vorhanden sind. Bei der 3-Wege-Spiegelung dürfen sogar 2 Datenträger ausfallen, ohne dass dabei Daten verloren gehen. Bei Verwendung von Parität (**Parity**) werden Paritätsinformationen für die Dateien des einen Datenträgers auf den anderen Datenträgern gespeichert und umgekehrt. Aus diesen Paritätsinformationen können die Daten bei Ausfall des Datenträgers rekonstruiert werden. Parity benötigt weniger Speicherplatz als eine Spiegelung, die Schreibvorgänge belasten den Prozessor jedoch spürbar und sind erheblich langsamer. Am schnellsten ist die Raid-0-ähnliche einfache Variante (**Simple**) ohne Ausfallsicherheit, Sie sollten diesen Typ jedoch wegen der großen Ausfallwahrscheinlichkeit nicht verwenden.

Verwenden Sie Spiegelung für alle Laufwerke mit gemischten Dateien, die sich häufig ändern, und Parity für Laufwerke mit großen Dateien wie z. B. ISO-Abbildern von optischen Medien, die sich selten ändern und wenig Schreibzugriffe erfordern.

- Bevor Sie den Speicherplätzen von Windows Server 2022 Ihre wichtigen Daten anvertrauen, sollten Sie eine Kopie Ihres Datenbestands anfertigen. Bei der Verwendung neuer Speichertechnologien sollten Sie stets kritisch und vorsichtig vorgehen.

20.7 Speicherpools und virtuelle Datenträger einrichten

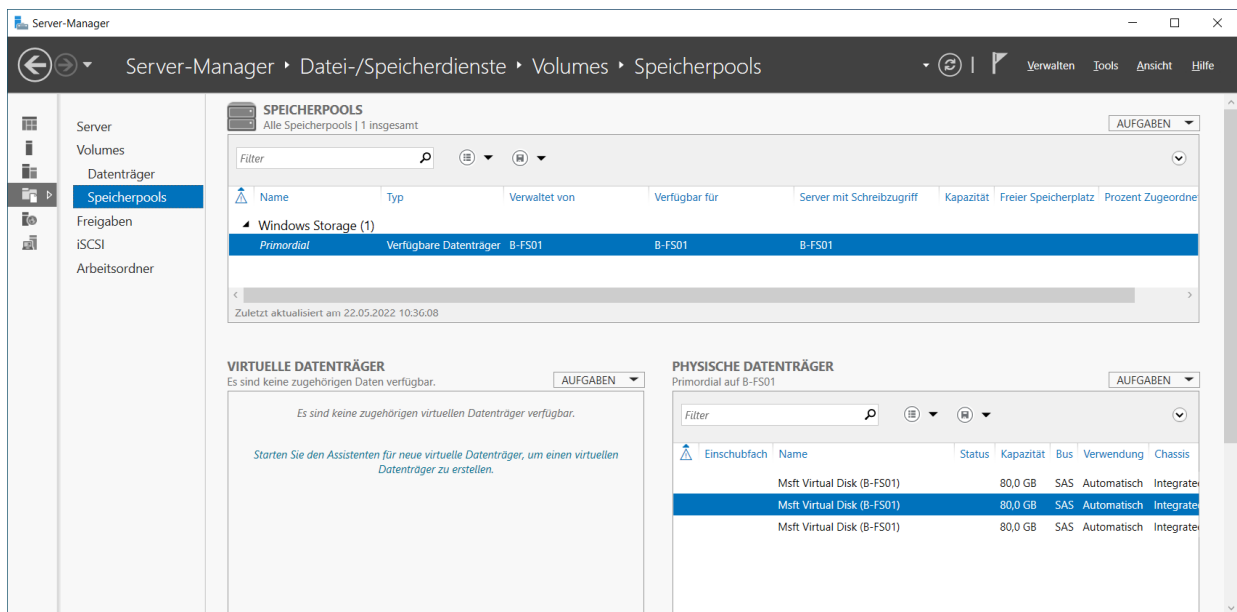
Speicherpool erstellen

Die Verwaltung der Speicherpools und Speicherplätze findet nicht in der Datenträgerverwaltung statt, sondern über *Server-Manager - Datei- und Speicherdienste - Speicherpools*. Diese Rolle ist standardmäßig installiert.

Es ist möglich, einen Speicherpool mit einem einzigen Datenträger zu erstellen. Wenn schon ein Speicherpool existiert, können Sie entweder Datenträger hinzufügen oder einen weiteren Speicherpool erstellen. Mehrere Pools sorgen für vollständige physische Trennung der Daten, was im Hinblick auf Datensicherheit vorteilhaft sein kann.

- ▶ Klicken Sie im Server-Manager auf *Datei- und Speicherdienste*.

- Klicken Sie auf *Volumes - Speicherpools*.

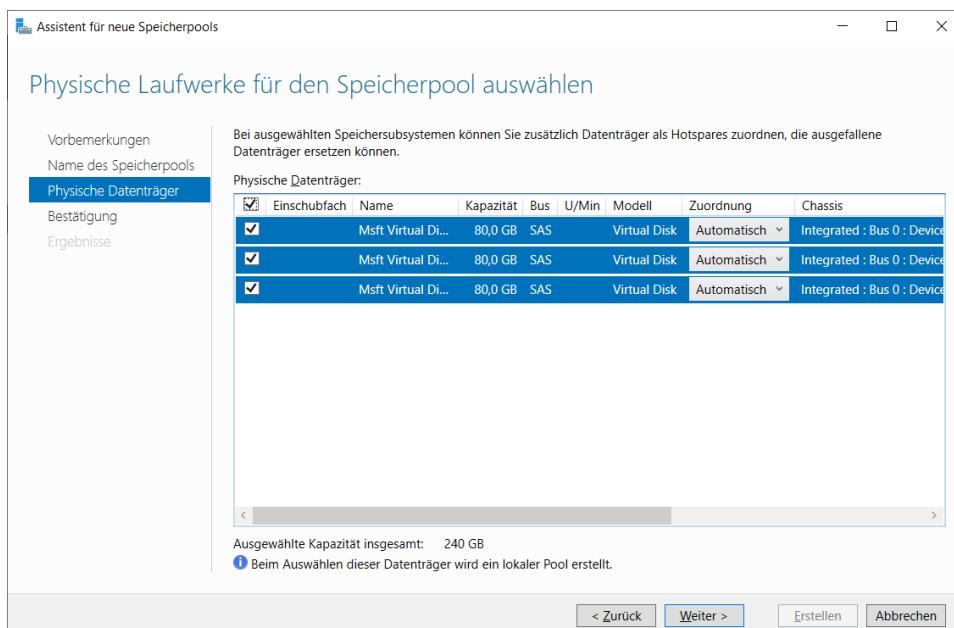


Speicherpools in Server-Manager

Auf der Seite *Speicherpools* werden im oberen Bereich die existierenden Speicherpools angezeigt. Links darunter sehen Sie unter *Virtuelle Datenträger* alle fertig eingerichteten logischen Laufwerke. Rechts sehen Sie alle im aktuellen Pool enthaltenen physischen Datenträger.

Alle unpartitionierten Datenträger werden unter als *Primordial* (ursprünglicher Pool) angezeigt.

- Um einen neuen Speicherpool zu erstellen, klicken Sie unter *Speicherpools* auf *Aufgaben* und dort auf *Neuer Speicherpool*.
Der Assistent für neue Speicherpools wird geöffnet.
- Lesen Sie die Vorbemerkungen und klicken Sie auf *Weiter*.
- Vergeben Sie einen Namen und optional eine Beschreibung für den Speicherpool.
Wählen Sie aus den verfügbaren Datenträgern aus, welche in den neuen Pool aufgenommen werden sollen. Standardmäßig ist dies der ursprüngliche Pool (*Primordial*).



- ▶ Klicken Sie auf *Weiter*.
- ▶ Bestätigen Sie die Auswahl durch Klick auf die Schaltfläche *Erstellen*.

Nachdem der Speicherpool erstellt ist, können Sie logische Laufwerke für die Datenspeicherung anlegen.

- ▶ Wählen Sie im Bereich *Virtuelle Datenträger* unter *Aufgaben - Neuer virtueller Datenträger*.
- ▶ Bestimmen Sie, in welchem Speicherpool das Laufwerk erstellt wird und bestätigen Sie die Auswahl mit *OK*.
- ▶ Folgen Sie dem Assistenten.
- ▶ Legen Sie einen Namen für das neue Laufwerk fest und klicken Sie auf *Weiter*.
- ▶ Lassen Sie die Gehäuseinformationen deaktiviert.
- ▶ Konfigurieren Sie die Speicheranordnung.

Auf der Seite Speicheranordnung können Sie zwischen drei verschiedenen Layout-Varianten wählen:

- ✓ *Simple*: entspricht RAID 0, keine Speicherplatzverluste, jedoch sehr unsicher und daher wenig empfehlenswert;
- ✓ *Mirror*: entspricht etwa RAID 1, Speicherplatz wird durch Spiegelung halbiert, Failover-Cluster möglich;
- ✓ *Parity*: ähnlich RAID 5. Es werden drei oder mehr Festplatten benötigt, um den Ausfall von maximal einer Platte auszugleichen. Die Verwendung im Failover-Cluster ist nicht möglich. Die Geschwindigkeit ist vor allem bei Schreibzugriffen erheblich langsamer als bei den anderen Modi.

Bei *Simple* können Sie über den gesamten Speicherplatz verfügen, während sich der nutzbare Speicherplatz bei Spiegelung (*Mirror*) halbiert und bei *Parity* auf etwa zwei Drittel reduziert.

Layout:	Beschreibung:
Simple	Data and parity information are striped across physical disks, increasing reliability, but somewhat reducing capacity. This storage layout requires at least three disks to protect you from a single disk failure, and cannot be used in a failover cluster.
Mirror	
Parity	

- ▶ Wählen Sie einen Bereitstellungstyp.

Mit *Dünn* ist die schlanke Speicherzuweisung (Thin Provisioning) gemeint, bei der nur der tatsächlich benötigte Speicherplatz verwendet wird. *Fest* bedeutet feste Speicherzuweisung (Thick Provisioning), wobei die Größe des virtuellen Datenträgers fest ist und sämtlicher Speicherplatz schon bei der Erstellung belegt wird.

- ▶ Bestimmen Sie die Größe des Laufwerkes.
- ▶ Bestätigen Sie die Auswahl durch Klick auf die Schaltfläche *Erstellen*.

Assistent zur Erstellung eines Volumes

Nach der Fertigstellung startet automatisch ein Assistent für die Erstellung eines Volumes, damit das Laufwerk eingebunden wird.

- ▶ Folgen Sie dem Assistenten mit Klicken auf die Schaltfläche *Weiter*.
- ▶ Im vierten Schritt legen Sie einen Laufwerksbuchstaben an oder können den Speicher in einem Ordner des Dateisystems bereitstellen.
- ▶ Legen Sie auf der Folgeseite den Typ des Dateisystems und den Namen fest.
- ▶ Entscheiden Sie, ob die Datenduplizierung verwendet werden soll.

Deduplizierung aktivieren

Für Volumes können Sie die Datendeduplizierung aktivieren ① und das Dateialter angeben, ab dem dupliziert werden soll ②. Außerdem können Sie Dateierweiterungen von der Deduplizierung ausschließen ③ und den Zeitplan festlegen ④.

☒ **Datendeduplizierung auf diesem Volume aktivieren:** ①

Alter (in Tagen), ab dem Dateien dedupliziert werden sollen: 30 ②

Geben Sie die Dateierweiterungen ein, die Sie von der Datendeduplizierung ausschließen möchten. Trennen Sie die Erweiterungen durch ein Komma. Beispiel: "doc,txt,png"

Auszuschließende Dateierweiterungen: ③

Zeitplan für die Deduplizierung festlegen... ④

Standardmäßig ist bei der Deduplizierung die Hintergrundoptimierung aktiviert, die Sie jedoch deaktivieren können ⑤.

Sie haben die Möglichkeit, eine Durchsatzoptimierung ⑥ einzuschalten, die zu bestimmten Zeitpunkten mit normaler Priorität durchgeführt wird. Da dieser Vorgang sehr ressourcenintensiv ist, bietet sich dafür die Nacht oder das Wochenende an.

Sie können auf Wunsch einen zweiten Zeitplan erstellen ⑦.

- Übernehmen Sie die Änderungen auf dieser Seite, indem Sie auf **OK** klicken.

Setzen Sie den anschließend Assistenten fort.

- Bestätigen Sie die Zusammenfassung durch Klick auf die Schaltfläche **Erstellen**.
- Schließen Sie den Erstellungsdialog.

B-FS01 - Deduplizierungszeitplan

B-FS01.firma.intern

⑤ ☒ **Hintergrundoptimierung aktivieren**
Die Datendeduplizierung wird regelmäßig mit niedriger Priorität ausgeführt und bei Auslastung des Systems angehalten, um die Leistung möglichst nicht zu beeinträchtigen.

⑥ ☐ **Durchsatzoptimierung aktivieren**
Während der angegebenen Zeiten wird die Datendeduplizierung mit normaler Priorität ausgeführt und verbraucht die erforderlichen Ressourcen, um die Leistung zu maximieren.
Wochentage: ☒ Montag ☒ Dienstag ☒ Mittwoch ☒ Donnerstag ☒ Freitag ☒ Samstag ☒ Sonntag
Startzeit: 01:45
Dauer (in Stunden): 6

⑦ ☐ **Zweiten Zeitplan für die Durchsatzoptimierung erstellen**
Während der angegebenen Zeiten wird die Datendeduplizierung mit normaler Priorität ausgeführt und verbraucht die erforderlichen Ressourcen, um die Leistung zu maximieren.
Wochentage: ☒ Montag ☒ Dienstag ☒ Mittwoch ☒ Donnerstag ☒ Freitag ☒ Samstag ☒ Sonntag
Startzeit: 09:00
Dauer (in Stunden): 8

OK Abbrechen Anwenden

Sie können jederzeit weitere Laufwerke zu einem Pool hinzufügen, es ist jedoch nicht vorgesehen, dass Sie Laufwerke aus dem Pool wieder entfernen.



Obwohl es möglich wäre, sollten Sie auf keinen Fall auf einem Speicherplatz übergreifende oder gespiegelte Volumes, Stripesetvolumes oder RAID-5-Volumes anlegen und auf virtuelle Festplattendateien (VHD/VHDX) verzichten. Im besten Fall leidet nur die Geschwindigkeit, im schlimmsten Fall drohen vorzeitige Plattendefekte und Datenverlust.

iSCSI-Blockspeicher hinzufügen

Internet Small Computer System Interface (iSCSI) ermöglicht das Ansprechen von Blockspeichern mittels TCP über das Ethernet. iSCSI kann in einem 10-Gbit-Netzwerk eine kostengünstige und ähnlich leistungsfähige Alternative zu Fibre Channel darstellen. Seit Windows Server 2012 können Sie iSCSI über den Server-Manager und seine Assistenten oder über zahlreiche PowerShell-Commandlets verwalten.

Der iSCSI-Zielsever stellt im Netzwerk den Speicherplatz zur Verfügung. Bei der Einrichtung geben Sie ein Volume an, auf dem eine virtuelle Festplattendatei im VHD-Format angelegt wird. (Die von Hyper-V angelegten VHDs können verwendet werden, das neue Format VHDX wird noch nicht unterstützt.) Anschließend weisen Sie der iSCSI-Ressource (auch als iSCSI LUN bezeichnet) einen Namen zu und legen fest, von welchen Servern aus auf diese Ressource zugegriffen werden darf. Diese iSCSI-Initiatoren müssen sich mit einer IQN identifizieren. Zwischen Windows Servern 2022 ist eine neue vereinfachte Methode der Identifizierung möglich.

21 Datensicherung

21.1 Sicherungsarten und -strategien

Überblick

Eine regelmäßige Datensicherung schützt vor Datenverlusten, die z. B. durch Festplatten- oder Benutzerfehler verursacht werden. Dafür ist bei Windows Server 2022 das Feature *Windows Server-Sicherung* zuständig, dass sich auch mit *WBAdmin.exe* über die Eingabeaufforderung steuern lässt.

Sicherungsmedien

Als Sicherungsziele können Sie speziell dafür vorgesehene Festplatten, Volumes oder Netzwerkfreigaben angeben. Die Sicherung auf DVD/RW-Medien wird nur bei der sogenannten einmaligen (d. h. manuell durchgeführten) Sicherung unterstützt. Auf diesem Sicherungsziel werden die Daten in komprimierter Form abgelegt. Der Systemstatus oder einzelne Dateien lassen sich von Wechselmedien nicht wiederherstellen.

Sicherungsarten

Die Windows Server-Sicherung arbeitet blockbasiert. Dabei werden nicht einzelne Dateien, sondern Datenblöcke gesichert. Da nur die veränderten Blöcke einer Datei gesichert werden, spart diese Methode bei mehreren Sicherungen viel Speicherplatz auf dem Sicherungsmedium. Aus Sicht des Benutzers handelt es sich stets um eine Vollsicherung, allerdings werden nur dann alle Daten neu geschrieben, wenn ein neues Backupmedium verwendet wird.

Es ist empfehlenswert, für die Sicherung eine eigene Partition bzw. einen separaten Datenträger zu verwenden. Dieser wird daraufhin neu formatiert (alle Daten gehen dabei verloren) und ist im Explorer nicht mehr sichtbar.



Es ist auch möglich, eine Netzwerkfreigabe als Backupziel zu verwenden, hier kann allerdings nur jeweils die aktuelle Backupversion gespeichert werden.

Die Datensicherung sichert die Daten blockbasiert von den Datenträgern, nicht pro Datei. Standardmäßig führt das Tool immer vollständige Sicherungen durch. Über den Menübefehl *Aktion/Leistungseinstellungen konfigurieren* können Sie aber auch inkrementelle Sicherungen aktivieren. Eine inkrementelle Sicherung sichert alle Daten, die sich seit der letzten Sicherung geändert haben. Unveränderte Daten werden nicht gesichert, da sich diese in einer vorherigen Sicherung befinden. Bei dieser Sicherungsart bauen die Datensicherungen aufeinander auf.

Zu einem gewissen Zeitpunkt benötigen Sie eine Vollsicherung, zum Beispiel freitags. Am Montag werden alle Daten gesichert, die sich seit Freitag verändert haben. Am Dienstag werden alle Daten gesichert, die sich seit Montag verändert haben.

Sicherungen und die Volumeschattenkopie

Die Serversicherung verwendet den Mechanismus der Volumeschattenkopien und erlaubt so auch die Sicherung geöffneter Dateien.

21.2 Regelmäßige Datensicherung

Windows Server-Sicherung installieren

Die Windows Server-Sicherung gehört nicht zum Standardinstallationsumfang. Sie müssen dieses Feature erst installieren. Je nachdem, welche Rollen Sie bereits installiert haben, kann es auch automatisch mit installiert worden sein.

- ▶ Klicken Sie im Dashboard des Server-Managers auf *Rollen und Features hinzufügen*.
- ▶ Wählen Sie den Server aus und klicken Sie auf *Weiter*, bis Sie auf die Seite *Features* gelangen. Aktivieren Sie dort das Feature *Windows Server-Sicherung*.
- ▶ Klicken Sie auf *Weiter und Installieren*, um das Feature einzurichten.

Das Kommandozeilentool *wbadmin.exe* wird mit der Serversicherung installiert. Die Windows Server-Sicherung überwacht automatisch den Speicherplatz auf den Datenträgern, auf denen die Sicherungen abgelegt werden. Steht nicht mehr genügend Plattenplatz zur Verfügung, werden Sie entsprechend darüber informiert und die Sicherung wird nicht durchgeführt. Außerdem wird der Datenträger nicht mehr im Explorer des Servers angezeigt und steht ausschließlich nur für die Datensicherung zur Verfügung.

Microsoft Azure Backup

Microsoft schlägt Ihnen an mehreren Stellen des Sicherungsassistenten vor, Microsoft Azure Backup zu verwenden, um online in der Microsoft Cloud Ihre Daten zu sichern. Dies mag zwar für manche Unternehmen durchaus eine Option darstellen, da dadurch eine sichere Verfügbarkeit von Serverdaten auch bei größeren Unfällen (z. B. Brandereignis) gewährleistet werden kann, stellt aber durch die entstehenden Kosten einen Sonderfall dar. Des Weiteren sind bei einer Lösung mit Microsoft Azure Backup datenschutzrechtliche Überlegungen nötig. Im vorliegenden Buch wird daher Microsoft Azure Backup nicht weiter erörtert. Die Anbindung an Microsoft Azure Backup nehmen Sie mit dem Windows Admin Center vor.

Windows Server-Sicherung starten

Sicherungen des lokalen Servers können Sie im Server-Manager konfigurieren. Wollen Sie Sicherungen auf anderen Rechner konfigurieren, benötigen Sie dafür die Verwaltungskonsolle *wbadmin.msc*.

Nicht-Administratoren können Sicherungen nur ausführen, wenn sie Mitglied der Gruppe *Sicherungs-Operatoren* auf dem jeweiligen Rechner sind.

- ▶ Geben Sie im Startmenü *sicherung* ein und klicken Sie auf *Windows Server-Sicherung*. Alternativ können Sie auch *wbadmin* im Startmenü eingeben.

Mit dem Befehl *Get-Command - Module WindowsServerBackup* lassen Sie sich in Windows Server 2022 die Cmdlets der PowerShell anzeigen. Mit den drei folgenden Befehlen lassen Sie sich eine ausführliche Hilfe und Beispiele der Cmdlets in der PowerShell anzeigen:

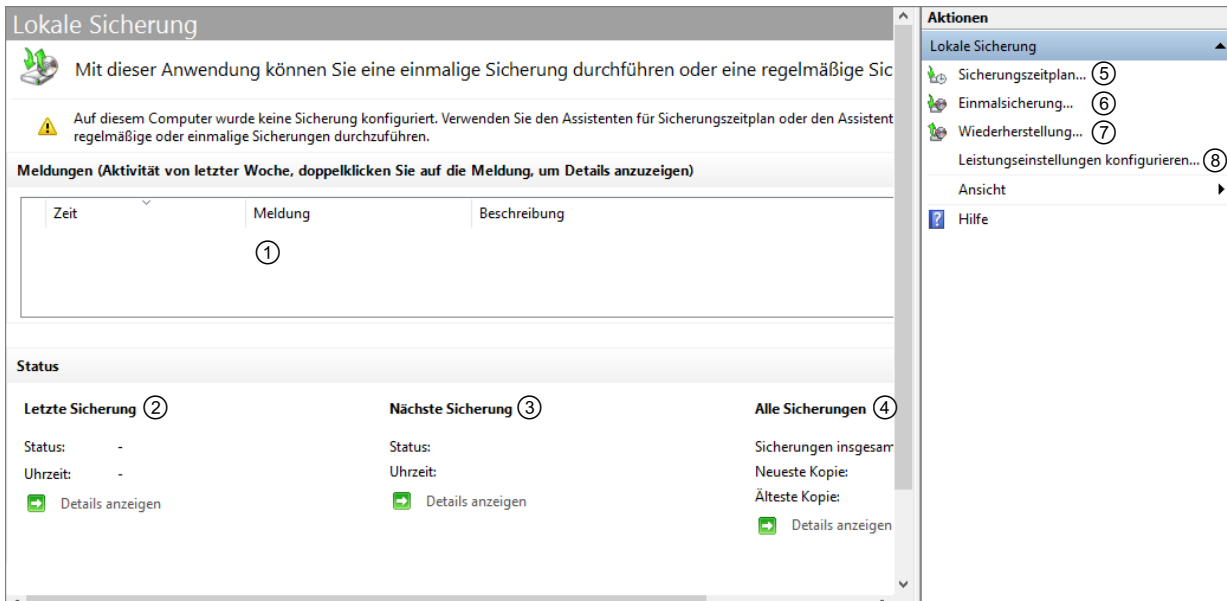
- ✓ `Get-Help <Cmdlet_Name> -Detailed`
- ✓ `Get-Help <Cmdlet_Name> -Examples`
- ✓ `Get-Help <Cmdlet_Name> -Full`

Um eine neue Sicherung über die PowerShell zu erstellen, müssen Sie zunächst einen Sicherungssatz anlegen, also eine Richtlinie, die steuert, welche Daten der Server sichern soll.

Überblick

Im Bereich *Meldungen* ① sehen Sie die Meldungen der Sicherungsvorgänge der letzten Woche. Unter *Status* sehen Sie die letzte Sicherung ②, die nächste geplante Sicherung ③ oder alle vorhandenen Sicherungen ④. Mit Klick auf *Details anzeigen* können Sie zusätzliche Informationen einblenden.

Im Bereich *Aktionen* können Sie einen Sicherungszeitplan ⑤ erstellen, eine Einmalsicherung durchführen ⑥, die Wiederherstellung einleiten ⑦ und Leistungseinstellungen konfigurieren ⑧. Eine Verbindung mit einem anderen Server herstellen können Sie nur in der Konsole, nicht im Server-Manager. Damit lassen sich Sicherungen für mehrere Maschinen durchführen oder planen. Die Sicherung erfolgt auf dem jeweiligen Server, Sie können sie nur remote konfigurieren.



Sicherungszeitplan erstellen

Nach der Installation sollten Sie die regelmäßige Sicherung Ihres Datenbestandes konfigurieren. Für tägliche (mehrmalige) Sicherungen eignet sich ein Sicherungszeitplan.

- ▶ Klicken Sie auf *Sicherungszeitplan*.
- ▶ Auf der ersten Seite erhalten Sie einen Überblick, klicken Sie auf *Weiter*.
- ▶ Wählen Sie bei der Sicherungsart zwischen *Vollständiger Server (empfohlen)* oder *Benutzerdefiniert* und klicken Sie auf *Weiter*.

Die weiteren Schritte unterscheiden sich, anhängig von Ihrer Auswahl. In diesem Beispiel wurde *Benutzerdefiniert* gewählt. Bei einer vollständigen Sicherung entfallen einige Schritte.

Im Fenster *Elemente für Sicherung auswählen* geben Sie an, was gesichert werden soll. Über *Erweiterte Einstellungen* erreichen Sie ein Fenster, in dem Sie einzelne Laufwerke, Ordner oder Dateien von der Sicherung ausschließen können.

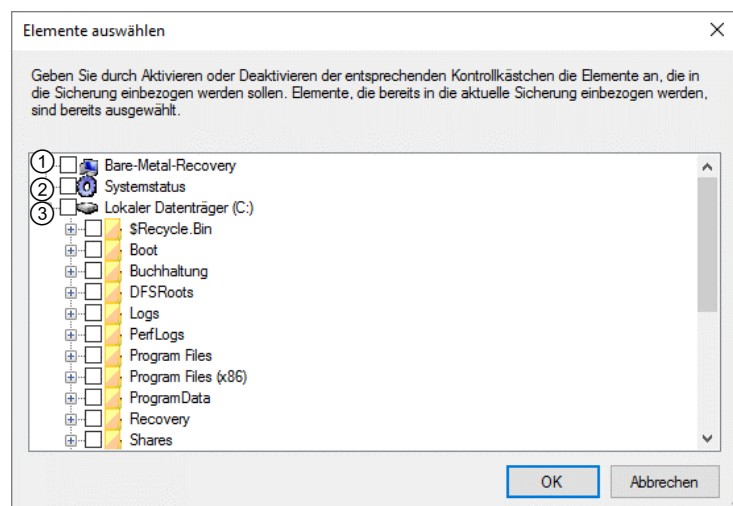
- ▶ Klicken Sie auf *Elemente hinzufügen* und wählen Sie im Auswahldialog aus, welche Partitionen und Ordner oder Dateien Sie sichern wollen.
- ▶ Klicken Sie auf *OK*.

Es gibt mehrere Auswahlmöglichkeiten für das Backup:

Bare-Metal-Recovery ①

Ein Bare-Metal-Recovery sichert das gesamte System, die Partition *System-reserviert*, den Systemstatus und die Systempartitionen, nicht jedoch weitere Partitionen. Mithilfe dieser Sicherung und einer Windows-Server-2022-DVD können Sie das gesamte Betriebssystem schnell wiederherstellen.

Eine solche Sicherung sollte eigentlich von jedem Server vorhanden sein und immer aktualisiert werden, wenn Sie die Hardware des Rechners ändern oder lokale Konfigurationen vornehmen. Als Sicherungsziel dafür bietet sich ein Netzlaufwerk an, in dem alle Server zentral gesichert werden.



Systemstatus ②

Der Systemstatus umfasst alle zentralen Einstellungen eines Servers. Auf einem Mitgliedsserver unter Windows Server 2022 enthält er u. a. folgende Dateien:

- ✓ Systemstart-Dateien,
- ✓ Registrierung,
- ✓ COM+Klassenregistrierungsdatenbank,
- ✓ auf Zertifikats-Servern die Datenbank für den Zertifikatsdienst,

auf Domänencontrollern zusätzlich:

- ✓ Active Directory (*NTDS.dit*),
- ✓ das Verzeichnis *Sysvol*.

Auf Domänencontrollern sollte zumindest der Systemstatus regelmäßig gesichert werden, da Sie damit eine Sicherung des Active Directory erreichen. Die benötigen Sie z. B. für die Wiederherstellung gelöschter Konten oder Gruppenrichtlinien. Weitere Informationen dazu erhalten Sie im Kapitel 23.



Für die Wiederherstellung des Systemstatus oder des vollständigen Systems müssen Sie dieselbe Version von Windows Server-Sicherung verwenden, mit der die Sicherung erstellt wurde.

Unter <http://blog.dikmenoglu.de> finden Sie viele interessante Informationen rund ums Active Directory, u. a. den Artikel: „Einen Server mit Rücksichern des System State zum DC stufen“.

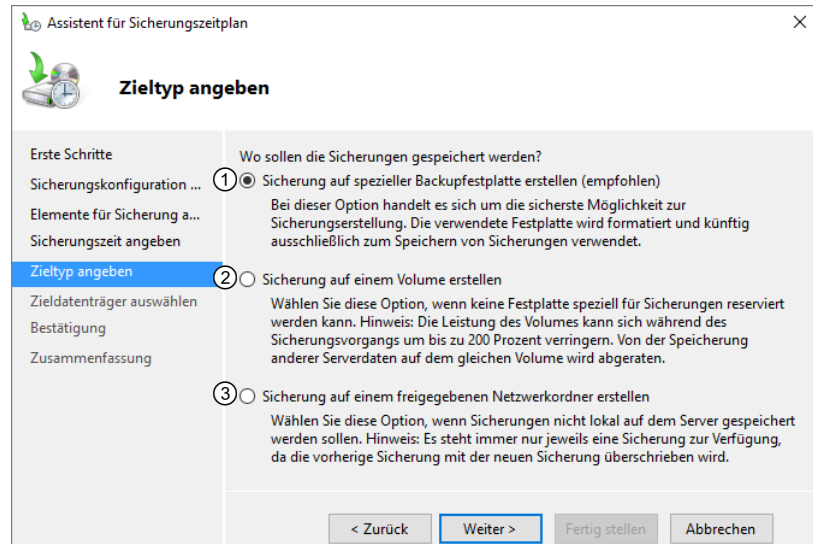
Lokaler Datenträger ③

Hierbei handelt es sich um die lokale System-Platte inklusive der Startpartition für das Betriebssystem. Sie ist für den Start von Windows und damit für ein Bare-Metal-Recovery erforderlich.

- ▶ Klicken Sie auf *Weiter*.
- ▶ Wählen Sie im Fenster *Sicherungszeit angeben* zwischen *Einmal pro Tag* und *Mehrmals am Tag*. Legen Sie für Ihre Auswahl die Sicherungszeit(en) fest und klicken Sie auf *Weiter*.
- ▶ Legen Sie fest, wohin die Datensicherung erfolgen soll.

Empfohlen wird die Sicherung auf eine separate Festplatte ①. Diese Festplatte wird im Anschluss formatiert (Sie erhalten später nochmals einen Hinweis darauf) und in Zukunft nicht mehr im Windows-Explorer angezeigt. Alle Daten darauf gehen verloren.

Mit *Sicherung auf einem Volume erstellen* ② können Sie auf ein vorhandenes Volume sichern und werden dann im nächsten Schritt aufgefordert, das Volume auszuwählen.



Über ③ legen Sie eine Netzwerkfreigabe als Sicherungsziel fest. Bedenken Sie, dass Sie immer nur die jeweils letzte Datensicherung wiederherstellen können. Benötigt ein Benutzer eine Datei, die er vor zwei Tagen gelöscht hat, ist diese nicht mehr vorhanden, daher ist diese Einstellung für einen Sicherungszeitplan nicht empfehlenswert.

- ▶ Haben Sie sich im vorhergehenden Schritt für eine spezielle Backupfestplatte entschieden, erscheint jetzt ein Fenster, in dem Sie den Zieldatenträger auswählen. Nach einem Klick auf *Alle verfügbaren Datenträger anzeigen* öffnet sich ein Fenster, in dem Sie aus den angeschlossenen Festplatten auswählen können.

Erscheinen angeschlossene Festplatten nicht in diesem Fenster, dann haben Sie eventuell vergessen, diese zuvor in der Datenträgerverwaltung zu initialisieren, indem Sie mit der rechten Maustaste auf die Bezeichnung des Datenträgers klicken und erst *Online* wählen und dann *Initialisieren*.

- ▶ Prüfen Sie auf der letzten Seite die Zusammenfassung Ihrer Einstellungen und klicken Sie auf *Fertig stellen*.

Wählen Sie als Sicherungsziel ein lokales Volume, erstellt die Windows Server-Sicherung dort den Ordner *WindowsImageBackup* und darin einen Unterordner mit dem Namen des Rechners.

Durch einen erneuten Aufruf von *Sicherungszeitplan* können Sie die getätigten Einstellungen verändern, z. B. zusätzliche Festplatten als Sicherungsziel angeben oder den Sicherungszeitplan entfernen.

Es ist im Assistenten nicht möglich, mehrere verschiedene Sicherungszeitpläne mit unterschiedlichen Ordnern oder Ziellaufwerken zu erstellen. Sie können dies jedoch über *wbadmin.exe* in der Eingabeaufforderung oder in der PowerShell erreichen.

Der Einsatz von Backupfestplatten mit einem Zeitplan macht die Sicherung bequem und einfach. Ältere Datensicherungen werden automatisch gelöscht, wenn auf den Sicherungsplatten der Speicherplatz zur Neige geht. Mehrere Backuplaufwerke, abwechselnd benutzt, schützen gegen den Ausfall einer Sicherungsplatte; zumindest können Sie dann auf die vorletzte Datensicherung zugreifen. Externe USB-Festplatten ermöglichen auch die sichere Aufbewahrung eines Backups in einem anderen Gebäude oder in einem feuerfesten Sicherheitsschrank.

Reichen Ihnen die dargestellten Möglichkeiten nicht aus, können Sie eigene Skripten erstellen (*wbadmin.exe* oder PowerShell) und diese über die Aufgabenplanung regelmäßig ausführen lassen. Ein Beispiel für ein einfaches Sicherungsskript erhalten Sie im Kapitel 23.

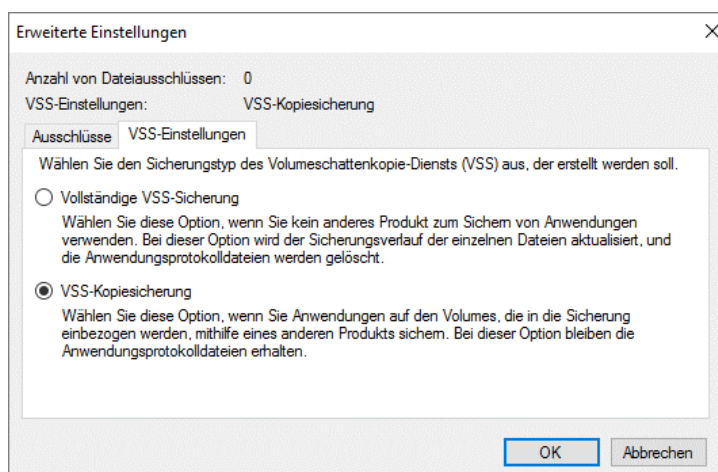
Einmalige Sicherung durchführen

- ▶ Klicken Sie auf den Link *Einmalsicherung*.
- ▶ Wählen Sie, ob Sie die Einmalsicherung mit den gleichen Optionen wie die geplante Sicherung durchführen oder die Einstellungen verändern möchten, und klicken Sie auf *Weiter*.
Beachten Sie, dass bei der Übernahme der Optionen auch das Ziellaufwerk unveränderlich übernommen wird.
- ▶ Klicken Sie auf *Sicherung*, um die Sicherung zu starten.
- ▶ Haben Sie keinen Zeitplan eingerichtet oder wünschen Sie eine abweichende Konfiguration oder ein anderes Ziellaufwerk, wählen Sie *Unterschiedliche Option* und wählen Sie wie oben beschrieben die Partitionen und Ordner aus. Klicken Sie dann auf *Weiter*.

Bei vorhandenem Sicherungszeitplan erfolgt standardmäßig eine Kopiesicherung, um den regulären Zyklus nicht durcheinanderzubringen. Wollen Sie lieber eine Normal-sicherung durchführen, stellen Sie das über einen Klick auf *Erweiterte Einstellungen* im Register *VSS-Einstellungen* um.

- ▶ Wählen Sie das Ziellaufwerk.
Bei der Einmalsicherung können Sie auch optische Medien wie CD-R oder DVD-RW verwenden.

Von DVDs können Sie nur komplette Volumes wiederherstellen. Die Auswahl einzelner Ordner oder Dateien ist nicht möglich.



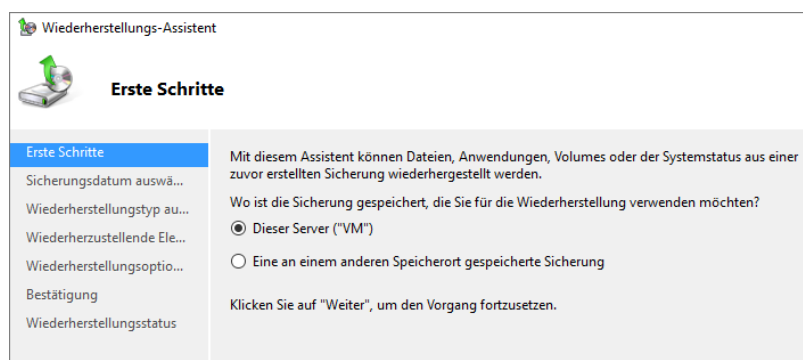
- ▶ Prüfen Sie auf der letzten Seite die Optionen und klicken Sie auf *Sicherung*, um das Backup zu starten.

21.3 Sicherung wiederherstellen

Wiederherzustellende Daten auswählen

- ▶ Klicken Sie auf den Link *Wiederherstellung*.
- ▶ Geben Sie an, wo die wiederherzustellenden Dateien gespeichert sind: auf diesem Server oder an einem anderen Speicherort.

Andere Speicherorte können lokale Datenträger oder Netzwerkfreigaben auf anderen Servern sein. Befinden sich die Sicherungen mehrerer Server an diesem Speicherort (Netzwerk-freigabe, *\\WindowsImageBackup*), müssen Sie den wiederherzustellenden Server angeben. Auf diese Art können Sie auch Datensicherungen wiederherstellen, die auf anderen Servern erstellt wurden.



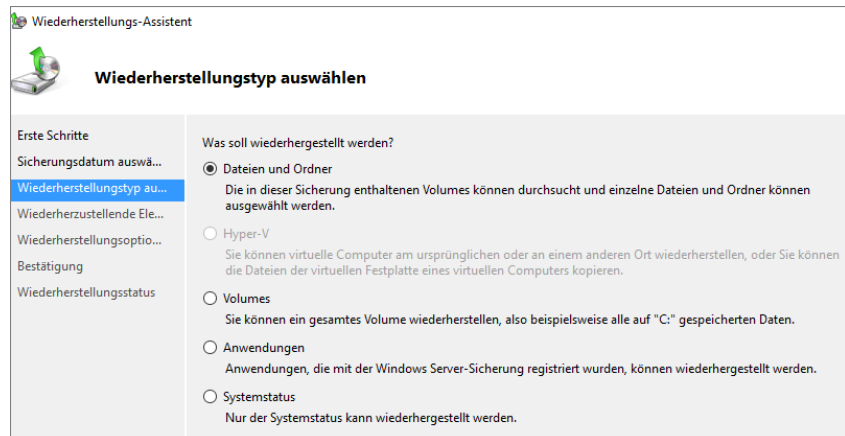
- ▶ Wählen Sie Ihren lokalen Server aus.
- ▶ Wählen Sie Datum und Uhrzeit der Sicherung aus, von der Sie Daten wiederherstellen möchten.

Falls das Backupmedium mit dem gewählten Sicherungszeitpunkt offline ist, werden Sie darauf hingewiesen. Schließen Sie das Medium ans System an, bevor Sie Daten wiederherstellen.

Wiederherstellungstyp auswählen

Im nächsten Fenster können Sie entscheiden, ob Sie einzelne Dateien und Ordner, Hyper-V-Maschinen, ganze Volumes, registrierte Anwendungen oder den Systemstatus wiederherstellen möchten.

Beachten Sie, dass ein Bare-Metal-Recovery nur über das Booten von der Windows-DVD und die Systemwiederherstellung möglich ist.



Ordner und Dateien wiederherstellen

- ▶ Um Ordner oder einzelne Dateien wiederherzustellen, wählen Sie die entsprechende Option. Markieren Sie im nächsten Fenster dann diejenigen Elemente, die Sie wiederherstellen wollen.
- ▶ Legen Sie die Wiederherstellungsoptionen fest.

Die Daten können je nach Art des Backups an den ursprünglichen oder einen alternativen Speicherort zurückgesichert werden. Sie legen fest, wie verfahren wird, wenn am Zielort gleichnamige Dateien vorhanden sind: Kopien erstellen, die vorhandenen Dateien überschreiben oder diese Dateien nicht wiederherstellen. Hier legen Sie auch fest, ob die ursprünglichen ACLs (NTFS-Berechtigungen und Überwachung) wiederhergestellt werden.

Der Assistent zeigt Ihnen eine Zusammenfassung und nach einem Klick auf *Wiederherstellung* werden die Daten zurückgesichert. Zum Abschluss erhalten Sie eine Zusammenfassung über die zurückgesicherten Daten.

Volumes wiederherstellen

Das Wiederherstellen von gesamten Volumes ist äquivalent zur Wiederherstellung eines Festplattenimages mithilfe bekannter Software von Drittanbietern (z. B. Acronis). Ein komplettes Volume wiederherzustellen ist bei einem Festplattenausfall die schnellste Möglichkeit, sämtliche Daten wieder nutzbar zu machen.

Beachten Sie, dass Sie Sicherungen der Systempartition und der versteckten Bootpartition nur wiederherstellen können, indem Sie von DVD booten und die Systemwiederherstellung einsetzen.

- ▶ Wählen Sie im Assistenten die Option, Volumes wiederherzustellen.
- ▶ Aktivieren Sie die Volumes, die Sie wiederherstellen möchten, und geben Sie an, auf welches Volume die Wiederherstellung erfolgen soll.
Sie erhalten einen Hinweis, dass das Wiederherstellen eines Volumes sämtliche Daten auf dem Zielvolume überschreibt.
- ▶ Überprüfen Sie die Optionen und klicken Sie auf *Wiederherstellen*, um den Vorgang zu starten.

Anwendungen wiederherstellen

Sie können festlegen, dass nur eine bestimmte Anwendung wiederhergestellt werden soll. Hier stehen folgende Anwendungen zur Auswahl:

- ✓ AD (Active Directory)
- ✓ FRS (File Replication Service, Dateireplikationsdienst)
- ✓ Registry (Registrierungsdatenbank)

- ▶ Wählen Sie die Anwendung, die Sie wiederherstellen wollen, und klicken Sie auf *Weiter*.
- ▶ Wählen Sie einen Speicherort für die Dateien.
Eine Wiederherstellung am ursprünglichen Ort ist aus Windows heraus nicht möglich. Verwenden Sie hierfür die Systemwiederherstellung von DVD.
- ▶ Klicken Sie auf *Wiederherstellen*.

Systemstatus wiederherstellen

Sie können den Systemstatus wiederherstellen, der das Active Directory und weitere Systemeinstellungen umfasst. Dabei wird ein Neustart erforderlich.

Sie können festlegen, ob die Dateien am ursprünglichen Speicherort oder einem anderen Ort wiederhergestellt werden sollen.

Ein Wiederherstellen am ursprünglichen Speicherort ist nur möglich, wenn der Computer im Verzeichnisdienst-Wiederherstellungsmodus (DSRM) gestartet wurde.

Optional können Sie die autorisierende Wiederherstellung des AD aktivieren, wenn Sie das AD in den Zustand aus dem Backup zurückversetzen wollen. Überlegen Sie sich genau, ob dies in Ihrer Situation das Richtige ist. Das Zurückversetzen des Active Directories in einen früheren Zustand kann schwerwiegende Folgen haben.

- ▶ Wählen Sie einen Speicherort und klicken Sie auf *Wiederherstellen*.

Haben Sie auf dem Server eine vollständige Datensicherung erstellt, können Sie damit den kompletten Server wiederherstellen, falls dieser zum Beispiel nicht mehr starten kann. Dazu muss der Datenträger, auf dem sich die Sicherung befindet, mit dem Server verbunden sein. Der Server muss mit der Windows Server 2022-DVD gebootet werden.

Bricht der Startvorgang von Windows Server 2022 einige Male ab, startet der Server auch ohne Installations-Dateien automatisch den Wiederherstellungsmodus. Auch hier lässt sich die Wiederherstellung des Servers durchführen.

- ▶ Klicken Sie auf der Startseite des Installations-Assistenten auf *Weiter*.
- ▶ Wählen Sie anschließend *Computerreparaturoptionen*.
In den Systemwiederherstellungsoptionen wählen Sie *Option zur Wiederherstellung einer Systemabbildsicherung* aus.
- ▶ Dazu klicken Sie auf *Problembehandlung* und *Systemimage-Wiederherstellung*.

22 System wiederherstellen

22.1 Strategien und Wiederherstellungsfunktionen

Fallen in einem Netzwerk wichtige Dienste oder ganze Server aus, sollte dies den laufenden Betrieb möglichst wenig, besser noch gar nicht beeinträchtigen. Fehlertoleranz bezeichnet ein Konzept, das gewährleistet, dass sich die Störung eines Systems nicht auf das Ganze auswirkt.

Im laufenden Netzwerkbetrieb helfen bereits zahlreiche Mechanismen, kurze Ausfälle zu überbrücken. Dazu zählen z. B. die Active Directory-Replikation, die Konsistenzprüfung, DFS mit Domänenstamm oder die langen Standard-Leasedauern im DHCP-Server.

Darüber hinaus müssen Sie selbst mit geeigneten Maßnahmen sicherstellen, dass Fehler entweder automatisch korrigiert werden oder Systeme nach einem Ausfall schnell wieder in Betrieb genommen werden können. Dazu zählen der Einsatz fehlertoleranter Datenträger und regelmäßige Datensicherungen. Gegen den Ausfall des Active Directory schützt der Einsatz mehrerer Domänencontroller je Domäne.

Kann ein Windows Server 2022 nicht mehr korrekt starten, erfolgt in den meisten Fällen ein automatischer Reparaturversuch des Systems, der häufig zum Erfolg führt. Sollte dies nicht der Fall sein, werden beim nächsten Startversuch die erweiterten Startoptionen angezeigt.

Der Einsatz entsprechender Serverhardware mit redundanten Netzteilen, Lüftern und Festplatten, Speicherbausteinen mit eingebautem Korrekturmechanismus (ECC-RAM) und unterbrechungsfreien Stromversorgungen (USVs) soll den fehlerfreien Betrieb des Netzwerks sicherstellen. In Extremfällen werden sogar komplette Rechenzentren redundant ausgelegt und an unterschiedlichen geografischen Standorten betrieben. Damit lassen sich sogar Großereignisse wie Erdbeben oder Flugzeugabstürze abfangen. Für die meisten Netzwerke sind solche Lösungen jedoch wegen der immensen Kosten nicht praktikabel.

22.2 Optionen des Systemstarts

Nutzen der erweiterten Startoptionen

Falls Windows Server 2022 nicht ordnungsgemäß startet, wird automatisch versucht, das System zu reparieren. In vielen Fällen ist dies auch ohne Eingreifen des Benutzers erfolgreich. Im Prinzip sind neben mehreren neuen Funktionen auch alle von Windows Server 2008 R2 bekannten Mechanismen und Startoptionen vorhanden.

Auf vielen Systemen funktioniert das Unterbrechen des Systemstarts mit  **F8** nicht zuverlässig. Auf diesen Systemen können Sie von einem Installationsmedium booten. Aus Windows heraus können Sie mit  **R** den Ausführen-Dialog öffnen und folgenden Befehl eingeben:

```
shutdown.exe /r /o /f /t 00 
```

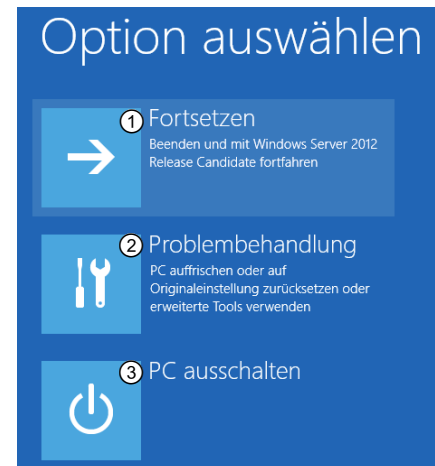
Daraufhin wird ein sofortiger Neustart ausgelöst und Windows bootet in die erweiterten Startoptionen.

Mithilfe bestimmter Startoptionen können Sie wählen, auf welche Weise der Startvorgang fortgesetzt werden soll. So besteht die Möglichkeit, den Boot-Vorgang zu untersuchen und die Fehlerquelle zu erkennen (Startprotokollierung) oder Windows Server 2022 in einem Standardmodus (abgesichert) zu starten, der verhindert, dass bestimmte benutzerdefinierte Einstellungen und Treiber verwendet werden, die Probleme verursachen könnten.

Optionen

Auf dem Optionsbildschirm können Sie ...

- ✓ Windows normal starten ①,
- ✓ die **Problembehandlung** starten ② oder
- ✓ den PC ausschalten ③.

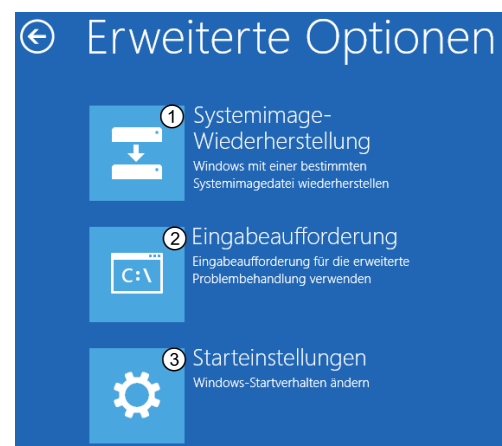


Problembehandlung

Durch einen Klick auf *Problembehandlung* gelangen Sie in den Bildschirm *Erweiterte Optionen*. Hier können Sie ...

- ✓ die Systemimage-Wiederherstellung starten ①,
- ✓ eine Eingabeaufforderung öffnen ② oder
- ✓ die Windows-Starteinstellungen aufrufen ③.

Bei ③ wird ein Neustart ausgelöst und Sie gelangen zu den von älteren Windows-Server-Versionen bekannten erweiterten Startoptionen.



Systemimage-Wiederherstellung

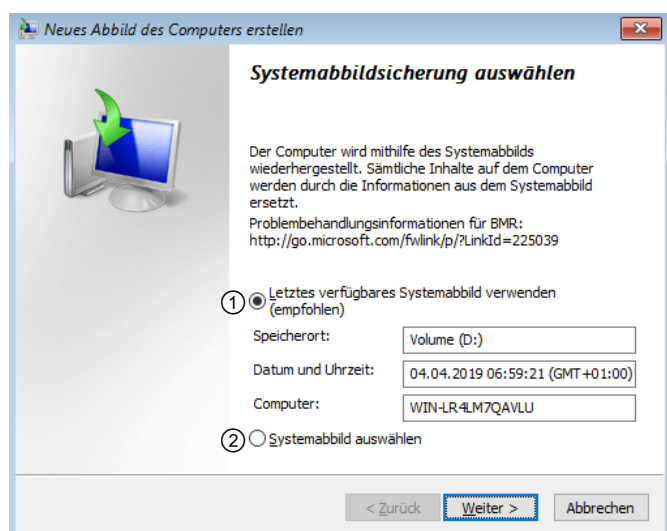
In der Systemimagesicherung bzw. Systemabbildsicherung können Sie ein bestehendes Systemabbild einspielen oder ein neues Systemabbild anfertigen. Ein Systemabbild umfasst den gesamten Zustand des Systems. Wenn Sie ein Abbild angefertigt haben, können Sie dieses jederzeit wieder zurückspielen. Hierdurch wird das System auf den Stand zurückgesetzt, in dem es sich zum Sicherungszeitpunkt befand.



Alle später vorgenommenen Änderungen am System (beispielsweise das Installieren von Programmen) bzw. an Ihren Dokumenten etc. werden dabei überschrieben. Es sei denn, Sie verwenden für Ihre persönlichen Daten und Einstellungen eine eigene Partition oder einen eigenen Datenträger.

Bei Windows Server 2022 können Sie die Systemimage-Wiederherstellung über die erweiterten Einstellungen des Bootmenüs starten. Dazu können Sie auch eine Windows-DVD verwenden.

- ▶ Starten Sie Windows vom Installationsmedium, klicken Sie im Dialog *Windows Setup* auf *Weiter* und dann auf *Computerreparaturoptionen*.
- ▶ Klicken Sie auf *Problembehandlung - Erweiterte Optionen - Systemwiederherstellung*.
- ▶ Wählen Sie ein Benutzerkonto aus und melden Sie sich an.
- ▶ Klicken Sie auf *Weiter* und wählen Sie entweder das letzte verfügbare Systemabbild ① oder ein anderes Abbild ② aus und klicken Sie auf *Weiter*.



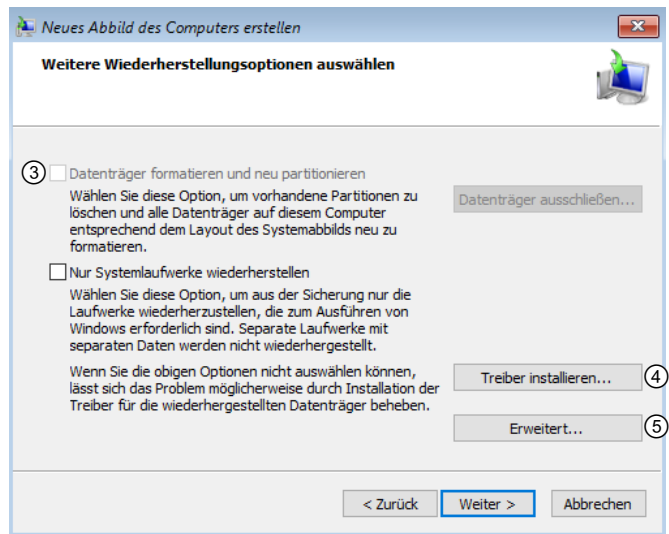
Bei Auswahl ② wählen Sie auf der nächsten Seite das Image und auf der darauffolgenden Seite den Zeitpunkt aus.

- ▶ Klicken Sie auf *Weiter*.
- ▶ Aktivieren Sie falls erwünscht die Neupartitionierung und Formatierung der gewählten Zielpartition ③.

Sie können außerdem zusätzliche Treiber installieren (z. B. bei abweichenden Harddiskcontrollern) ④ und unter *Erweitert* ⑤ den automatischen Neustart und die Datenträgerüberprüfung ein- und ausschalten.

- ▶ Klicken Sie auf *Weiter*.
- ▶ Klicken Sie auf *Fertig stellen*.

Das System wird nun in den ausgewählten Zustand zurückversetzt.



Erweiterte Startoptionen

Nachdem Sie in den Starteinstellungen einen Neustart ausgelöst haben, sehen Sie die erweiterten Startoptionen. Sie können die erweiterten Startoptionen auch aufrufen, indem Sie beim Start des Computers häufig die Taste (F8) betätigen. Sie müssen dabei allerdings sehr schnell sein, sonst kommt der Tastendruck zu spät.

Mit den Pfeiltasten und treffen Sie eine Auswahl, mit starten Sie die Auswahl. Hier können Sie zahlreiche Optionen für den nächsten Systemstart setzen.

<i>Computer reparieren</i>	Nach einer lokalen Anmeldung erhalten Sie Zugriff auf die Systemwiederherstellungsoptionen.
<i>Abgesicherter Modus</i>	Im abgesicherten Modus werden nur Basistreiber und -dienste geladen. Wenn Sie die Variante <i>mit Eingabeaufforderung</i> gewählt haben, steht Ihnen keine grafische Oberfläche, sondern nur die Eingabeaufforderung zur Verfügung. Sie können mit dem abgesicherten Modus beispielsweise fehlerhafte Treiberdateien manuell entfernen oder Konfigurationsfehler beheben.
<i>Startprotokollierung aktivieren</i>	Normaler Windows-Start, bei dem die Protokolldatei <i>Ntblog.txt</i> erstellt wird. Über diese Datei finden Sie heraus, an welcher Stelle der normale Start abbricht (nach einem Neustart in den abgesicherten Modus).
<i>Video mit niedriger Auflösung aktivieren</i>	Wenn Probleme mit dem Grafiktreiber einen Systemstart verhindern, können Sie hier Server 2022 im Standard-VGA-Modus starten. Dann sollten Sie die Tastaturnavigation beherrschen, da einige Fenster zu groß für den Desktop sind.
<i>Letzte als funktionierend bekannte Konfiguration (erweitert)</i>	Startet Windows nach einer Änderung an der Systemkonfiguration nicht mehr und hat sich niemand seit der Änderung (erfolgreich) angemeldet, veranlassen Sie Windows damit zum Starten einer Sicherungskopie der Computerkonfiguration. Bei Veränderungen an Treibern funktioniert das in der Regel gut.
<i>Reparaturmodus für Verzeichnisdienste</i>	Mit der Verzeichnisdienstwiederherstellung können Sie auf Domänencontrollern Fehler im Verzeichnisdienst beheben.
<i>Debugmodus</i>	Aktiviert den Windows-Kerneldebugger, wodurch erweiterte Informationen, z. B. in Absturzabbildern, erzeugt werden

Die erweiterten Startoptionen erreichen Sie nur, wenn der Server noch von der Systemfestplatte bootet. Ist deren Bootsektor beschädigt oder fehlen Teile der Windows-Startumgebung, können Sie das System von der Installations-DVD starten. Sie erhalten dann Zugriff auf dieselben Systemwiederherstellungsoptionen wie bei der Auswahl *Computer reparieren*.

Wenn Sie in den erweiterten Startoptionen  betätigen, gelangen Sie in eine Betriebssystemauswahl. Falls mehrere Einträge im Bootmenü vorhanden sind, können Sie hier auswählen, welchen Sie starten wollen.

In diesem Bildschirm können Sie mit  zur Windows-Speicherdiagnose springen.

Abgesicherten Modus verwenden

Der abgesicherte Modus ist auch bei Windows Server 2022 noch vorhanden. Im abgesicherten Modus lädt Windows nur für den Start unbedingt notwendige Komponenten und Treiber. Sie können einen vor Auftreten des Startproblems installierten Gerätetreiber manuell deinstallieren und danach versuchen, Windows wieder normal zu starten. Sie haben die Auswahl zwischen dem abgesicherten Modus mit oder ohne Netzwerk und einer Eingabeaufforderung.

Eingabeaufforderung in den Systemwiederherstellungsoptionen

Sowohl beim Booten von DVD als auch beim Starten von Festplatte können Sie in den erweiterten Startoptionen mit  **F10** eine Eingabeaufforderung mit Administratorrechten öffnen. Diese kann bei der Behebung von Startproblemen gute Dienste leisten.

Denken Sie daran, dass bestimmte Befehle nur verfügbar sind, wenn Sie den korrekten Pfad eingeben (`bcdedit .exe` beispielsweise zum Bearbeiten der Windows-Bootoptionen befindet sich im Windows-Installations-Unterordner *System32*). Starten Sie die Eingabeaufforderung nach einem DVD-Boot, müssen Sie das Laufwerk und den Ordner wechseln. Möglicherweise müssen Sie auch den Pfad des Systemlaufwerks anpassen. Mit dem Befehl `set` können Sie die benötigten Umgebungsvariablen für Pfade auch temporär zuweisen (siehe dazu auch `set /help`).

Alle Ihnen zur Verfügung stehenden Befehle der Eingabeaufforderung können Sie sich mit `help` anzeigen lassen.

23 Active Directory-Objekte wiederherstellen

23.1 Überblick und Hintergründe

Überblick

Der Einsatz mehrerer Domänencontroller schützt vor Kompletterverlust der Active Directory-Daten und schafft Redundanzen für die Bearbeitung von Anfragen. Er schützt nicht gegen das Löschen von Objekten, da eine solche Veränderung auf alle DCs repliziert wird. Zur Wiederherstellung gelöschter Konten müssen Sie deshalb andere Methoden verwenden.

Löschen Sie Objekte nur, falls ein Grund dafür vorliegt. Benutzerkonten sollten Sie z. B. zuerst deaktivieren und erst nach einem vordefinierten Zeitraum löschen, wenn sie mit Sicherheit nie mehr benötigt werden.

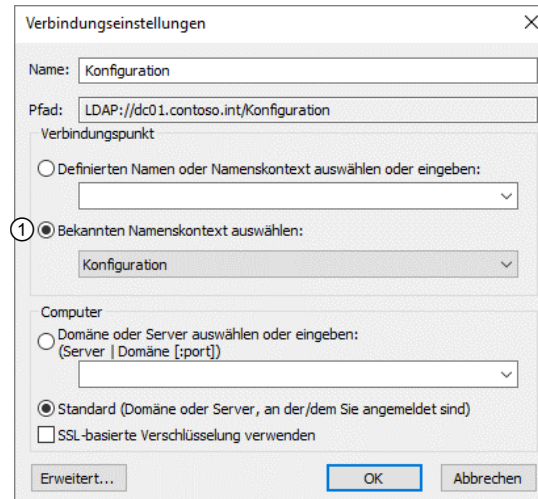
Tombstones einfügen

Ein gelöscht Objekt verschwindet nicht sofort aus dem Active Directory, es wird zunächst „getombstoned“, es wird sozusagen begraben und erhält einen Grabstein. Dabei verliert es fast alle seine Eigenschaften. Während der Tombstone Lifetime verbleiben die Tombstones im Active Directory und werden erst nach deren Ablauf vollständig entfernt. Eine Wiederherstellung gelöschter Objekte ist nur während dieser Zeit möglich. Älter darf auch das benutzte Backup nicht sein, sonst entstehen Geisterobjekte.

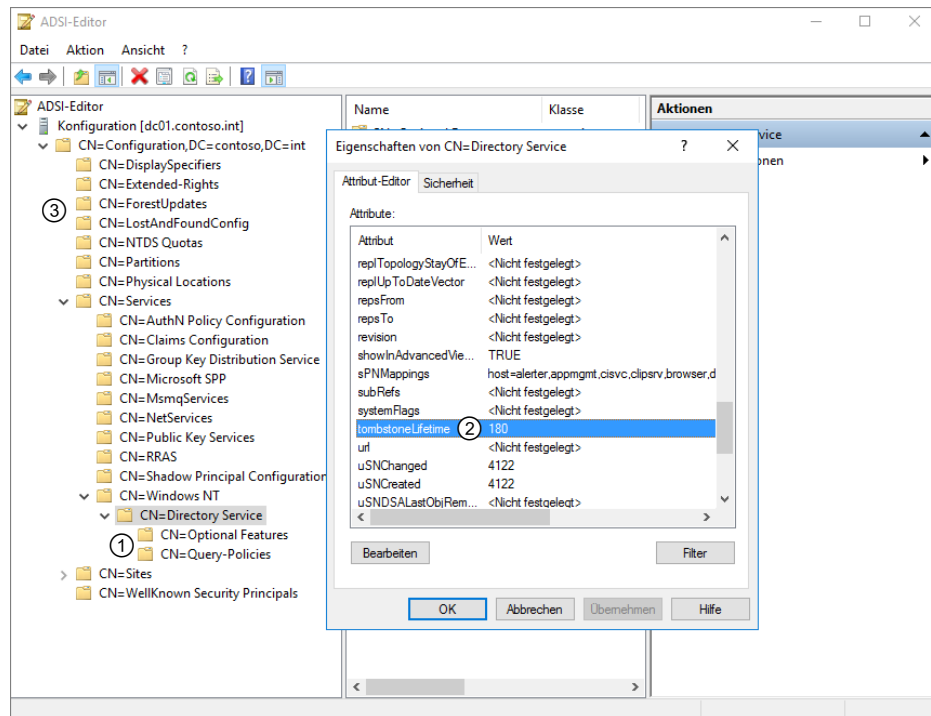
Tombstone Lifetime verändern

Die Tombstone Lifetime können Sie im ADSI-Editor einstellen. Beachten Sie, dass Sie sich dazu mit der Konfigurationspartition des AD verbinden müssen. Bei früheren Server-Versionen gelangten Sie automatisch in die Konfiguration, wenn Sie im ADSI-Editor den standardmäßigen Namenskontext wählten.

- ▶ Klicken Sie im ADSI-Editor mit der rechten Maustaste in der Konsolenstruktur auf *ADSI-Editor*. Wählen Sie *Verbindung herstellen*.
- ▶ Aktivieren Sie in den Verbindungseinstellungen die Option *Bekannten Namenskontext auswählen* ① und wählen Sie im Listenfeld den Eintrag *Konfiguration* aus.
- ▶ Klicken Sie auf *OK*.



Welchen Zeitraum die Tombstone Lifetime in Ihrem AD umfasst, hängt davon ab, mit welchem Betriebssystem das AD erstellt wurde. Sie liegt seit einigen Server-Versionen standardmäßig bei 180 Tagen. Die Abbildung zeigt, an welcher Stelle Sie den Knoten *Directory Service* ① finden. In dessen Eigenschaften befindet sich die Variable *tombstone-Lifetime* ②. Mit einem Klick auf *Bearbeiten* können Sie den Wert verändern.



Beachten Sie dabei, dass die Tombstone Lifetime in der Konfigurationspartition ③ des AD liegt. Alle Änderungen wirken sich auf die Gesamtstruktur aus und können nur von Organisations-Admins vorgenommen werden.

Weshalb Images keine Sicherung ersetzen können

Da das Active Directory mit einem Multimaster-Modell arbeitet, müssen Mechanismen zur Synchronisation der Datenbank verwendet werden. Bei jeder Änderung an einem Objekt speichert ein Domänencontroller eine USN (Update Sequence Number) zu den Veränderungen. Diese USN ist spezifisch für einen Domänencontroller, nicht für ein Objekt.

Angenommen, auf DC 1 wird ein Objekt verändert, dann erfolgt die AD-Replikation in etwa folgendermaßen:

- ✓ DC 1 informiert DC 2, dass Änderungen vorhanden sind.
- ✓ DC 2 teilt DC 1 mit, welche USN er bei der letzten Replikation von ihm erhalten hat.
- ✓ DC 1 schickt alle Veränderungen mit höherer USN an DC 2.

Diese Vorgehensweise bedingt, dass Images keine Sicherung des AD ersetzen können. Näheres hierzu erfahren Sie im Artikel „Warum Images nicht als Datensicherung taugen“ unter:

<https://www.faq-o-matic.net/2006/08/04/warum-images-nicht-als-datensicherung-taugen/>

Sollte Ihr Active Directory aus einer einzigen Domäne mit nur einem Domänencontroller bestehen, spricht nichts gegen eine Image-Sicherung.

Ausfall eines einzelnen Domänencontrollers

Fällt einer von mehreren Domänencontrollern aus, verbleibt das Active Directory-Verzeichnis sowohl strukturell intakt als auch inhaltlich aktuell. Nach einer normalen Wiederherstellung erhält der Domänencontroller die aktuellen Verzeichnisdaten automatisch im Zuge einer normalen Replikation. Wird der Domänencontroller nicht wiederhergestellt, müssen dessen Einträge aus dem Active Directory entfernt werden. Das Stichwort dafür ist *Metadata Cleanup*.

Floating Single Master Operation Server (FSMO)

Es gibt Aufgaben, die nur von einzelnen Domänencontrollern ausgeführt werden dürfen, da eine Inkonsistenz der Daten hier zu gravierende Folgen hätte. Diese werden als Floating Single Master Operation (FSMO, in etwa: schwebende oder übertragbare Einzelmasterhandlung) bezeichnet.

In der Gesamtstruktur sind das die Rollen des Schema-Masters (verantwortlich für die Definition von Objekten und ihren Eigenschaften) und der Domänennamensbetriebsmaster (verantwortlich für die Eindeutigkeit von Domänennamen und -SIDs sowie für die Pflege von Vertrauensstellungen).

In jeder Domäne einer Gesamtstruktur gibt es die folgenden drei FSMO-Rollen einmalig:

- ✓ **PDC-Emulator:** verantwortlich für Kennwortänderungen und Kontosperrungen;
- ✓ **RID-Master:** erstellt und verteilt die Relative Identifier (vergleichbar einer Ausweisnummer von Objekten);
- ✓ **Infrastrukturmaster:** verantwortlich für Objekte, die ihre Domänenzugehörigkeit verändert haben.

Wenn ein FSMO ausfällt und definitiv nicht wiederhergestellt werden kann, muss seine Rolle auf einem anderen Domänencontroller aktiviert werden. Dazu benötigen Sie das Kommandozeilentool `ntdsutil -roles`.

Wiederherstellung gelöschter Objekte

Das Wiederherstellen eines gelöschten Objekts erfolgt durch seine autorisierende Wiederherstellung. Dazu müssen Sie den LDAP-Pfad des wiederherzustellenden Objektes kennen. Die übrigen Verzeichnisdaten werden von dieser Maßnahme nicht betroffen.

Stellen Sie beispielsweise eine Organisationseinheit autorisierend wieder her, setzen Sie dabei die Kennwörter aller enthaltenen Benutzer- und Computerkonten auf den Stand der Datensicherung zurück. Das kann Anmeldeprobleme der betroffenen Konten nach sich ziehen.

Einfacher wird es, wenn Sie den Active Directory-Papierkorb einsetzen und kostenlose Zusatz-Tools verwenden.

23.2 Active Directory-Objekt autorisierend wiederherstellen

Überblick

Die klassische Wiederherstellung von AD-Objekten umfasst folgende Einzelschritte, die in der angegebenen Reihenfolge auszuführen sind:

- ✓ Booten in den Modus *Verzeichnisdienstwiederherstellung*
- ✓ Systemstatus zurücksichern, nicht neu starten
- ✓ Gelöschte Objekte autorisierend wiederherstellen
- ✓ Normaler Reboot

Nach der Darstellung dieser Schritte erhalten Sie einige Hinweise zu alternativen Methoden.

Booten in den Modus *Verzeichnisdienstwiederherstellung*

Anhalten können Sie die Active Directory-Dienste auf allen Domänencontrollern seit Windows Server 2000 durch einen Reboot in die erweiterten Startoptionen ( **F8**) und die Auswahl *Verzeichnisdienstwiederherstellung*. Bei einem anschließenden normalen Neustart werden die Verzeichnisdienste wieder gestartet.

Nach einem Boot in den Modus *Verzeichnisdienstwiederherstellung* müssen Sie sich als lokaler Administrator anmelden. Dafür benötigen Sie das entsprechende Kennwort, das bei der Installation des DCs angegeben wurde.

Sollte es unbekannt sein, setzen Sie es **vor** dem Reboot zurück, in einer Eingabeaufforderung über das Kommando:
`ntdsutil "set dsrm password" "reset password on server null"`

Sie geben dann das neue Kennwort ein, wiederholen es und verlassen `ntdsutil` durch die zweimalige Eingabe von `quit`.

Sie können die drei Kommandos auch einzeln eingeben. Nach `ntdsutil` sind Sie im `ntdsutil`-Prompt und können sich jeweils mit `help` anzeigen lassen, welche Kommandos an dieser Stelle zur Verfügung stehen.

Seit Windows Server 2008 geht das Beenden und Starten der Active Directory-Dienste auch ohne Neustarts über eine Eingabeaufforderung: `net stop ntds` beendet die Verzeichnisdienste, `net start ntds` startet sie erneut. Das Anhalten müssen Sie mit `j` bestätigen.

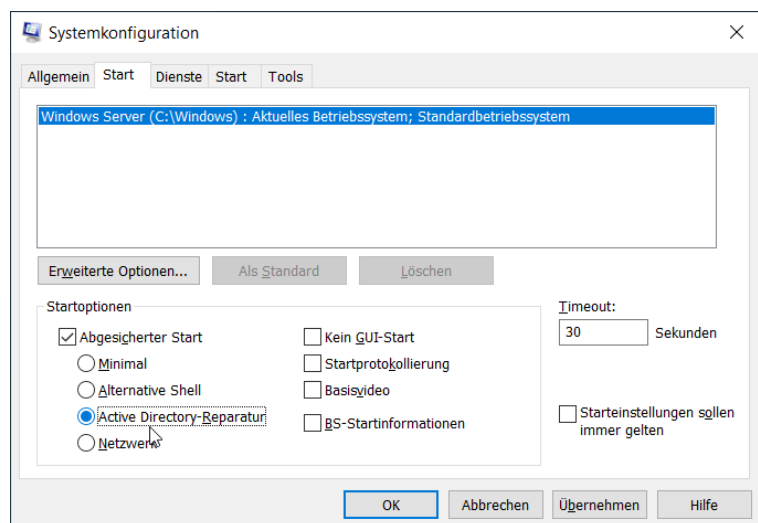
- Auf diese Art können Sie den Systemstatus (System State) nicht zurückspielen. Booten Sie dazu mit  **F8** in die erweiterten Startoptionen und starten Sie die Verzeichnisdienstwiederherstellung. Ein angehaltener Verzeichnisdienst dient anderen Aufgaben, z. B. einer Defragmentierung der Datei `ntds.dit`.

Systemstatus wiederherstellen

Den Systemstatus können Sie entweder über die Kommandozeile oder die Windows Server-Sicherung wiederherstellen. Eine autorisierende Wiederherstellung können Sie nur nach einem Reboot in den Modus *Verzeichnisdienstwiederherstellung* durchführen.

Bei Windows Server 2022 ist das Zeitfenster für die Eingabe von  **F8** (abhängig von der verwendeten Hardware) so kurz, dass es nur nach mehrmaligem Versuch gelingt, die erweiterten Startoptionen aufzurufen. Verwenden Sie stattdessen die Systemkonfiguration (`msconfig`), um den nächsten Start für die Active Directory-Reparatur festzulegen.

Nach der Wiederherstellung des Systemstatus kehrt Windows automatisch in den normalen Startmodus zurück.



Startoptionen in der Systemkonfiguration

Systemstatus mit der Windows Server-Sicherung wiederherstellen

Mit der Windows Server-Sicherung können Sie den Inhalt des `Sysvol`-Ordners nur über eine vollständige Wiederherstellung des Active Directory zurücksichern.

- ▶ Starten Sie in der Windows Server-Sicherung eine Wiederherstellung und wählen Sie die passende Sicherung mit dem Systemstatus.
- ▶ Markieren Sie auf der Seite *Wiederherstellungstyp auswählen* die Option *Systemstatus*.

- Wenn Sie die Option *Autorisierende Wiederherstellung von Active Directory-Dateien ausführen* aktivieren, stellen Sie zwar den Inhalt des `Sysvol`-Ordners wieder her, Sie setzen aber Ihre gesamte Domäne auf den Stand der Datensicherung zurück.

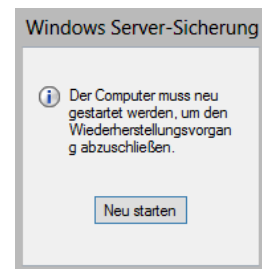
Wollen Sie das nicht und müssen Sie trotzdem den Inhalt von *Sysvol* wiederherstellen, müssen Sie mit der Kommandozeile arbeiten.

- ▶ Sie erhalten einen Hinweis bezüglich replizierter Inhalte, den Sie mit *OK* bestätigen.
- ▶ Starten Sie auf der letzten Seite das Wiederherstellen.
Aktivieren Sie **nicht** das Kontrollfeld bei *Server automatisch neu starten, um die Wiederherstellung abzuschließen*.

Sie erhalten einen letzten Hinweis, dass der Vorgang nicht mehr angehalten oder abgebrochen werden kann, den Sie mit *Ja* bestätigen. **Brechen Sie den Vorgang nach dem Start auf keinen Fall ab.** Das Betriebssystem kann sonst nicht mehr booten.

Nach dem Abschluss der Wiederherstellung werden Sie aufgefordert, den Rechner neu zu starten. Führen Sie diesen Schritt **jetzt noch nicht** durch! Vor dem Neustart muss die autorisierende Wiederherstellung der gelöschten Objekte erfolgen.

Ein Neustart ist nur sinnvoll, wenn Sie die autorisierende Wiederherstellung des gesamten AD aktiviert haben. Dann entfällt auch der Schritt *Gelöschte Objekte autorisierend wiederherstellen*.



Systemstatus über die Eingabeaufforderung wiederherstellen

Informieren Sie sich vor der Wiederherstellung über die verschiedenen Schalter von *wbadmin*. Beispielsweise können Sie mit `-authsysvol` auch den Inhalt von *Sysvol* wiederherstellen. Standardmäßig ist dieser Schalter nicht gesetzt.

- ▶ Öffnen Sie als Administrator eine Eingabeaufforderung (*cmd.exe*).
Informationen über vorhandene Sicherungen erhalten Sie mit `wbadmin get versions`.

Die Versions-ID benötigen Sie für die Wiederherstellung. Haben Sie bei der Sicherung alternative Sicherungsziele angegeben, können Sie die dort enthaltenen Sicherungen anzeigen lassen, wenn Sie Folgendes an den Befehl anhängen:

`-backuptarget : <Laufwerk> und <Laufwerk>` dabei durch das alternative Sicherungsziel ersetzen.

- ▶ Starten Sie die Wiederherstellung mit folgendem Kommando:
`wbadmin start systemstaterecovery -version:<Versions-ID>`.
Die Versions-ID entspricht der Datumsangabe.
- ▶ Beantworten Sie die folgenden zwei Nachfragen mit *J* für Ja.
Dann beginnt die Wiederherstellung des Systemstatus.
Nach dem Abschluss der Wiederherstellung werden Sie aufgefordert, den Rechner neu zu starten.
Führen Sie diesen Schritt **jetzt noch nicht** durch! Vor dem Neustart muss die autorisierende Wiederherstellung der gelöschten Objekte erfolgen.

Gelöschte Objekte autorisierend wiederherstellen

Wenn Sie diesen Schritt weglassen, haben Sie nur den System State zurückgesichert. Damit können Sie beispielsweise eine lokal korrupte Datenbank (*ntds.dit*) wiederherstellen. Bei der nächsten AD-Replikation aktualisiert sich dann der Inhalt.

In den folgenden Schritten benötigen Sie eine genaue Ortsangabe der wiederherzustellenden Objekte. Diese lässt sich u. a. mit dem Kommandozeilentool *csvde* erstellen.

Öffnen Sie eine Admin-Eingabeaufforderung.

- ▶ Geben Sie ein:
`ntdsutil "activate instance ntds" "authoritative restore"`
- ▶ Einzelne Konten stellen Sie wieder her mit
`restore object <DN>`.
Zur Wiederherstellung ganzer Organisationseinheiten nutzen Sie `restore subtree <DN>`.

Für <DN> geben Sie den Distinguished Name des Objekts ein.

Wenn Sie an dieser Stelle über einen csvde-Export des AD verfügen, können Sie diese Textdatei (mit Notepad) öffnen, darin nach dem Konto suchen, die Fundstelle in die Zwischenablage kopieren und bei `ntdsutil` wieder einfügen.

- ▶ Vor der Wiederherstellung jedes Objekts erfolgt eine Rückfrage, ob Sie sicher sind, die Sie mit Ja bestätigen.

Nach der Wiederherstellung jedes Objekts erhalten Sie eine Zusammenfassung.

Sind alle Objekte wiederhergestellt, beenden Sie `ntdsutil` durch die zweimalige Eingabe von `quit` und können den Rechner neu starten.

Nach dem Neustart sind die autorisierend wiederhergestellten Objekte wieder vorhanden, im selben Zustand wie bei der Sicherung.

Einen einfachen csvde-Export erstellen Sie in einer Eingabeaufforderung mit dem Kommando
`csvde -f <Datei>`.

23.3 Alternative Methoden zur Wiederherstellung

Aufwand reduzieren

Die oben dargestellte Methode ist gut geeignet, wenn Sie eine Organisationseinheit mit viel Inhalt gelöscht haben. Für die Wiederherstellung von einigen wenigen gelöschten Konten ist der Aufwand aber sehr hoch. Das Neuerstellen hat diverse Nachteile, die alle damit zusammenhängen, dass die neuen Konten mit neuen SIDs erstellt werden. Beispielsweise funktionieren dann die Benutzerprofile und Basisverzeichnisse nicht mehr und weiteres Nacharbeiten ist notwendig.

Im Folgenden erhalten Sie einige Hinweise zu alternativen Methoden, die den Einsatz kostenloser Tools erfordern.

Alle Methoden können Sie ohne Reboot und ohne Wiederherstellung des Systemstatus durchführen und alle Methoden funktionieren auch mit dem Active Directory-Papierkorb. Ohne AD-Papierkorb kann keine der Methoden das Kennwort eines gelöschten Kontos wiederherstellen.

Tombstones wiederbeleben

Tombstones können Sie mit dem Kommandozeilentool **adrestore** sehr schnell und einfach reanimieren. Zwei einfache Beispiele sollen das zeigen. Die Eingabe von:

- ✓ `adrestore hub` zeigt alle Tombstones, deren Common Name „hub“ enthält.
Damit finden Sie gelöschte Objekte und die benötigten Angaben zur Wiederherstellung.
- ✓ `adrestore -r "franz huber"` stellt den Tombstone mit dem Common Name Franz Huber wieder her.

Ohne Active Directory-Papierkorb stellen Sie damit allerdings nur das Konto wieder her und alle seine Eigenschaften sind verloren. Immerhin funktionieren damit alte Konfigurationen wie beispielsweise Benutzerprofile, sie müssen nur neu zugewiesen werden.

Herunterladen können Sie **adrestore** auf den Internetseiten von Microsoft: <https://docs.microsoft.com/de-de/>.

ADRecycleBin erfüllt im Wesentlichen dieselben Aufgaben wie **adrestore**, nur mit grafischer Oberfläche.

Active Directory-Snapshots

Seit Windows Server 2008 ist es möglich, Snapshots vom aktuellen Stand des Active Directory zu speichern. Solche Snapshots lassen sich dann mounten und Sie erhalten damit Zugriff auf einen historischen Stand des AD. Über spezielle Tools lassen sich dadurch Tombstones wiederherstellen und mit den Informationen aus dem Schnappschuss befüllen.

- ▶ Öffnen Sie eine Eingabeaufforderung.
- ▶ Über das Kommando `ntdsutil snapshot "activate instance ntds"` erreichen Sie die richtige Stelle.
- ▶ Mit `create` erstellen Sie einen neuen Schnappschuss.

```
Administrator: Eingabeaufforderung - ntdsutil
C:\Users\Administrator>ntdsutil
ntdsutil: snapshot
Snapshot: activate instance ntds
Aktive Instanz wurde auf "ntds" festgelegt.
Snapshot: create
Snapshot wird erstellt...
Der Snapshotsatz {bc160ca0-38dc-4676-9bbc-3f0d0fb2909d} wurde erfolgreich generiert.
Snapshot: list all
1: 2017/02/06:15:25 {bc160ca0-38dc-4676-9bbc-3f0d0fb2909d}
2: C: {192e98f4-ad68-4949-84d8-3757c49df3f1}
Snapshot: mount 2
Der Snapshot {192e98f4-ad68-4949-84d8-3757c49df3f1} wird als C:\$SNAP_201702061_2_VOLUME$ bereitgestellt.
Snapshot: -
```

AD-Snapshot mit ntdsutil

- ▶ Vorhandene Schnappschüsse können Sie an dieser Stelle mit `list all` anzeigen.
- ▶ Mit `mount <Nummer>` ① machen Sie einen Schnappschuss zugreifbar ②.

Jetzt können Sie beispielsweise im Explorer lesend auf die enthaltenen Dateien zugreifen.

- ▶ Mit `unmount <Nr. >` können Sie den Schnappschuss wieder aushängen.
Dazu müssen Sie an der richtigen Stelle in `ntdsutil` sein.

Benötigen Sie auch Zugriff auf den Inhalt der Active Directory-Datenbank, um beispielsweise ältere Zustände zu betrachten, können Sie den gemounteten Schnappschuss für einige AD-Tools zugänglich machen.

`dsamain -dbpath "<Snapshot-Pfad>\Windows\NTDS\ntds.dit" -ldapport <Port>`
ermöglicht den Zugriff auf den historischen Stand des AD.

- ▶ Geben Sie für `<Snapshot-Pfad>` den Inhalt von ② ein und ersetzen Sie `<Port>` mit einem freien Port, z. B. 15000. Diese Eingabeaufforderung muss jetzt so stehen bleiben. Wenn Sie sie schließen, ist der Zugriff auf Port `<Port>` nicht mehr möglich.

Den Schnappschuss können Sie beispielsweise mit `LDP.exe` oder `ADSI-Edit.msc` über den angegebenen Port betrachten. Damit erhalten Sie zumindest Informationen über die (ehemaligen) Eigenschaften der Objekte.

Beispielskript für eine automatische AD-Sicherung

Mit der Windows Server-Sicherung können Sie nur einen Sicherungszeitplan erstellen. Wollen Sie ihn nur zur Sicherung anderer Daten nutzen, können Sie den Systemstatus über ein Skript sichern. Das hat dann auch den Vorteil, dass bei der Ausführung dieses Skripts aufgerufen oder ein AD-Snapshot erstellt werden kann. Das Skript können Sie dann über die Aufgabenplanung in konfigurierbaren Intervallen automatisch ausführen lassen.

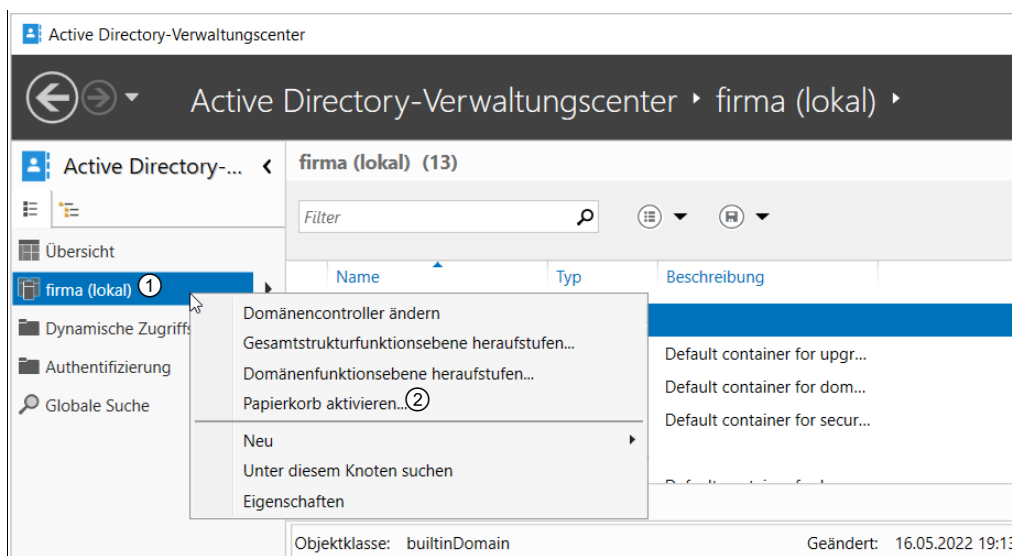
23.4 Active Directory-Papierkorb

Verbesserung seit Windows Server 2012

Mit Windows Server 2008 R2 wurde der Active Directory-Papierkorb eingeführt. Dieser bewirkt, dass beim Löschen eines Objektes nicht nur die SID mit einem Tombstone versehen wird, sondern auch die Eigenschaften erhalten bleiben. So kann durch Entfernen des Tombstones das Objekt mit seinen Eigenschaften wiederhergestellt werden. Mit Server 2012 wurde der Active Directory-Papierkorb zusätzlich um eine grafische Benutzeroberfläche erweitert.

Der Active Directory-Papierkorb steht erst ab der Gesamtstrukturfunktionsebene Windows Server 2008 R2 zur Verfügung und muss einmalig für die Gesamtstruktur aktiviert werden.

Active Directory-Papierkorb aktivieren



Active Directory-Verwaltungscenter

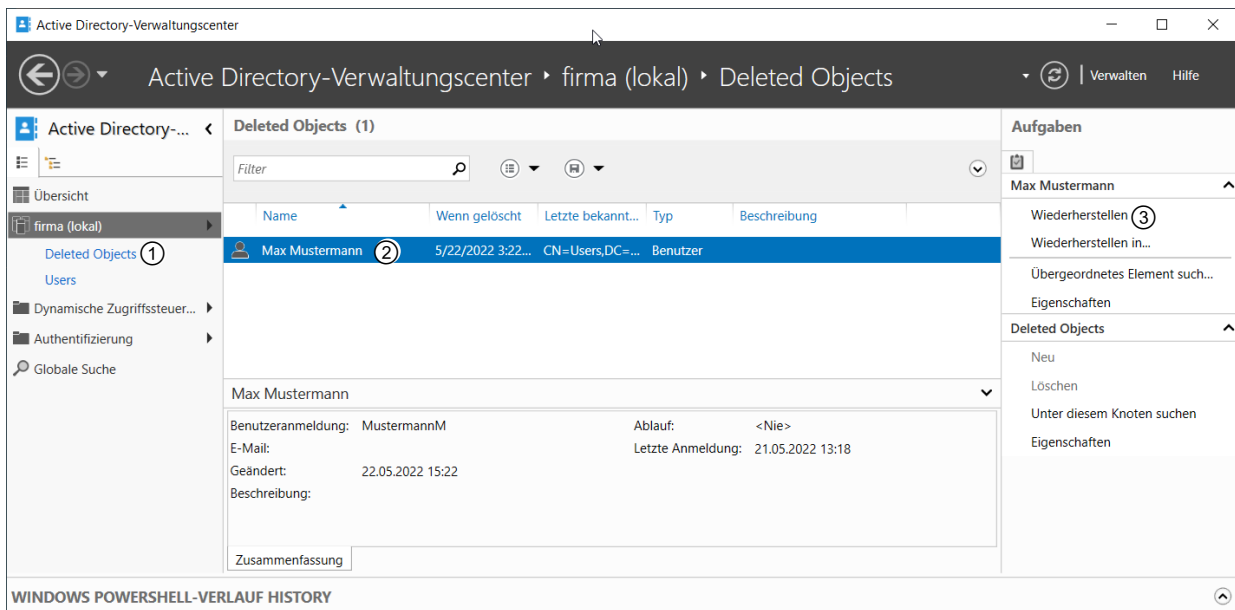
- ▶ Öffnen Sie als Administrator das Active Directory-Verwaltungscenter. Sie starten das Center zum Beispiel durch Eingabe von *dsac* im Startmenü.
- ▶ Navigieren Sie auf den Knoten der Domäne ①, für die Sie den AD-Papierkorb aktivieren möchten, und klicken Sie unter *Aufgaben* auf *Papierkorb aktivieren* ②.
Sie erhalten nun eine Warnmeldung, dass dieser Schritt nicht rückgängig gemacht werden kann.
- ▶ Bestätigen Sie die Rückfrage mit *OK*.
Sie erhalten nun eine weitere Warnmeldung, die besagt, dass das AD-Verwaltungscenter aktualisiert werden muss und dass die Aktivierung des Papierkorbs an alle Domänencontroller der Gesamtstruktur repliziert werden muss.
- ▶ Bestätigen Sie diese mit *OK*.

Wie lange ein Objekt im AD-Papierkorb verbleibt, wird vom Attribut *msDS-DeletedObjectLifetime* bestimmt. Standardmäßig beträgt dieser Wert null, d. h., die Tombstone Lifetime bestimmt die Dauer.



Bei der Aktivierung des AD-Papierkorbs löschen Sie alle vorhandenen Tombstones.

Gelöschte Objekte wiederherstellen



Wenn Sie nun ein gelöschtes Objekt wiederherstellen möchten, navigieren Sie auf den Knoten *Deleted Objects* ①, wählen Sie das entsprechende Objekt aus ② und betätigen Sie unter *Aufgaben* den Eintrag *Wiederherstellen* ③.

A

Abgesicherten Modus verwenden	218
Abgesicherter Modus	54
Abonnements	182
ACE (Access Control Entries)	117
ACL (Access Control List)	117
ACPI (Advanced Configuration and Power Management)	45, 47
Active Directory	19
Active Directory-Domänendienste	63
Active Directory-Papierkorb	226
Active Directory-Standort	60
ADRecycleBin	225
adrestore	224
Alias	83
Anmeldeskript	172
Anmeldung überwachen	164
Anwendungen installieren/entfernen/reparieren	32
APIPA (Automatic Private IP Addressing)	18
Arbeitsgruppe	14
Auslagerungsdatei konfigurieren	38
AXFR (Asynchronous Full Transfer Zone)	74

B

Basisdatenträger	194
Basisdatenträger umwandeln	196
Basisordner	173
Basisvolumes	194
Benutzereigenschaften	110
Benutzerkonto erstellen	109
Benutzerprofil	169
Berechtigungen	117
Bereichsoptionen	91
Bereitstellungspunkt	194
Besitz übernehmen	121
Besitz übernehmen, Registrierungsschlüssel	192
Besitzer	117
Betriebsmaster	58
BHS (Bridgehead-Server)	96
Buffer Overflow	39

C

CIDR-Notation	16
Cmdlets	31
CNAME (Canonical Name)	83
Colon hex	16
Computerkonto erstellen	112
Container	104

D

DACL (Discretionary Access Control List)	117
Dashboard	11, 26, 177
Dateidienste	125
Dateigruppe	132
Dateiprüfung	132
Dateiprüfungsverwaltung	132
Dateiprüfungsvorlage	132
Datenausführungsverhinderung	39
Datenkommunikation	13
Datensicherung	207
Datenträger	141, 194
Datenträger auf Fehler überprüfen	200
Datenträger optimieren	199
Datenträger pflegen	199
Datenträger, dynamischer	194
Datenträgerkontingente	200
Datenträgerverwaltung	195
dcpromo	63
Deduplizierung aktivieren	206
Default-First-Site-Name	95
DefaultIPSiteLink	98
Delegierung	106
DFS (Distributed File System)	124, 133
DFS-Namespace	134
DFS-Replikation	138
DFS-Replikationsgruppen	139
DFS-Stamm, Verbinden mit	140
DHCP (Dynamic Host Configuration Protocol)	18, 85
DHCP, Benutzerklasse	92
DHCP, Bereich	87
DHCP, Herstellerklasse	92
DHCP, Hot-Standby-Modus	94
DHCP, Lastenausgleichsmodus	94
DHCP, maximale Clientvorlaufzeit	94
DHCP, Reservierung	93
DHCP, Serveroptionen	91
DHCP-Failover	93
DHCP-Relay-Agent	85
Dienst verwalten	41
Dienst, Starttyp	42
Dienstverwaltung öffnen	40
Digitale Signatur für Treiber	47
DN (Distinguished Name)	224
DNS (Domain Name System)	72
DNS, Active-Directory-integrierte Zonen	78
DNS, Alterung	78
DNS, Aufräumvorgang	78
DNS, bedingte Weiterleitung	82
DNS, Delegierung	74, 77, 81
DNS, Dummy-Delegierung	77
DNS, dynamische Updates	78
DNS, dynamisches, DDNS	75

DNS, Forward Lookup	75
DNS, Funktionsweise	73
DNS, iterative Abfrage	75
DNS, rekursive Abfrage	75
DNS, Replikation	74
DNS, Reverse Lookup	75
DNS, Stammhinweise	77
DNS, Weiterleitungen	75, 77
DNS, Zonentyp	78
DNS-Cache	76
DNS-Server	18
Domäne	55
Domänencontroller entfernen	69
Domänencontroller hinzufügen	67
Domänencontroller installieren	63
Domänenfunktionsebene	57, 68
Domänenlokale Gruppe	112
Doppelpunkt-Hexadezimal-Notation	16
Dotted decimal notation	15
Druck- und Dokumentdienste	155
Druckaufträge, Status einsehen	152
Drucken, Berechtigungen verwalten	154
Drucker	143
Drucker freigeben	147
Drucker, Bezeichnungen	143
Drucker, LPR-Drucker einrichten	147
Drucker, Standarddrucker festlegen	150
Druckerberechtigungen	123
Druckerpool	144
Druckerpool einrichten	148
Druckertreiber aktualisieren	149
Druckerwarteschlange	143
Druckerwarteschlange konfigurieren	151
Druckgeräte	143
Druckserver	144
DSRM (Directory Services Restore Mode)	68
Dynamische Adresszuweisung	85
Dynamische Aktualisierung	90

E

Einmalsicherung	212
Energiesparpläne	45
Energieverwaltung	45
Ereignisanzeige	178
Ereignisdetails anzeigen	181
Ereignis-ID	181
Ereignisprotokoll	178
ERSTELLER-BESITZER, Konto	118
Erstkonfiguration, Server-Manager	26
Erweiterungskarten installieren, Plug & Play	49

F		HKEY_LOCAL_MACHINE	188	N	
Features hinzufügen	34	HKEY_USERS	188	Netzwerkadresse	17
Fehlertoleranz, Definition	215	Hosts-Datei	72	Netzwerkdrucker	143
Festplatte konvertieren	196	Hybrider Stand-by-Modus	45	Neuerungen im Überblick	12
Filter	181	Hyper-V	8	No-Execute-Flag	39
Flexible Single Master Operation (FSMO, Betriebsmaster)	58	I		NTDS (NT Directory Service)	65
Forward-Lookupzone	79, 81	IFM (Install From Media)	67	NTDS Settings	97
FQDN (Fully Qualified Domain Name)	9, 30, 64, 72	Installation	24	NTDS.dit	55, 96
Freigabe	124	Installationsart	23	NTFS (NT File System)	9
Freigabe- und Speicherverwaltung	127	IPv4-Adressen	15	NTFS, Überwachung	164
Freigabeberechtigungen	122	IPv6-Adressen	16	NTFS-Berechtigungen	118
FSMO (Floating Single Master Operation Server)	58, 221	iSCSI (Internet Small Computer System Interface)	206	NTFS-Verreichtung	121
Funktionsebenen	57	ISTG (Inter-Site Topology Generator)	96	NX-Flag	39
G		IXFR (Incremental Zone Transfer)	74	O	
GC (Global Catalog)	59	K		Objektverwaltung delegieren	106
Geräte aktivieren/deaktivieren	42	Kacheln	10	Objektzugriffsversuche	
Geräte installieren	49	KCC (Knowledge Consistency Checker)	96	überwachen	164
Geräte und Drucker	144	Kennwortrichtlinien	163	Obligatorisches Profil	171
Geräte-Manager	50	Kernelschutz	47	Offlineeinstellungen	125
Geräte-Manager, ausgeblendete Geräte anzeigen	52	Komplexes Kennwort	65	Ordnerumleitung	175
Gesamtstruktur	56	Kontingent	131	Organisations-Admin	68, 69
Gesamtstruktur erstellen	64	Kontingentverwaltung	130	Organisationseinheit	59
Gesamtstrukturfunktionsebenen	57	Kontingentvorlagen	130	OU (Organizational Unit)	59, 105
Globaler Katalog	59, 65	Kontorichtlinien	162, 167	P	
GPO (Group Policy Object)	157	Kontosperrungsrichtlinien	163	Parität (Parity)	203
GPT-Datenträger	195	L		Partitionen	195
Gruppenbereich	112	LDAP (Lightweight Directory Access Protocol)	55	Plug & Play	47
Gruppenkonto erstellen	113	Leasedauer	88, 89	PowerShell	20, 31
Gruppenkonto verwalten	114	Leistungsüberwachung	186	Private IP-Adressen	16
Gruppenrichtlinien	20	Line Printer Daemon	144	Problembehandlung	216
Gruppenrichtlinien, Implementierung planen	165	Logische Laufwerke	195	Problembehandlung, Hardware	53
Gruppenrichtlinien, Verarbeitung	159	Lokale Drucker	143	Protokoll löschen	181
Gruppenrichtlinienergebnisse	164	Lokale Gruppe	112	Protokollgröße	181
Gruppenrichtlinienobjekt	157	LPR (Line Printer Remote)	144	Protokollierung	177
Gruppentyp	112	LPR-Drucker	144	PSO (Password Settings Object)	167
GUID-Partitionstabellen	195	LPR-Portmonitor	147	PSO zuweisen	168
H		M		Q	
Hardware deaktivieren	51	MAC-Adresse	17, 93	Queue	143
Hardware deinstallieren	51	Master-DNS-Server	79	Quota	130
Hardware entfernen, Hot-Plugging	52	MBR (Master Boot Record)	194	R	
Hardware hinzufügen	47	MBR-Datenträger	194	RAID-Level	142
Hardware, Probleme behandeln	52	Mirroring	203	RAID-System	194
Hardware-Voraussetzungen	22	MMC (Microsoft Management Console)	20	ReFS (Resilient File System, robustes Dateisystem)	9
HKEY, Unterstrukturen der Registrierung	188	Mounten	194	REG_, Wertetypen der Registrierung	189
HKEY_CLASSES_ROOT	188	Multimaster-Replikationsmodell	58	regedit.exe	189
HKEY_CURRENT_CONFIG	188	Multitasking optimieren	38	Registrierung	188
HKEY_CURRENT_USER	188			Registrierungsdatenbank	188
				Registrierungs-Editor	189

Registry	188	Spiegelung	203	Upgrade, Neuinstallation	22
Remote Desktop	20	Spooler	143	UPN (User Principal Name)	30
Remoteserver-Verwaltungstools	103	Spoolordner	143	UPN-Suffix	111
repadmin	102	Spoolordner verschieben	151	USB-Stick	142
Replikation	95, 96, 101	SSD (Solid State Discs)	141	USN (Update Sequence Number)	220
Replikation, Standort	96	Standardberechtigungen	117		
Replikationstopologie	101	Standardbetriebssystem	36	V	
Ressourcen zuweisen	51	Standardgateway	17		
Ressourcen-Manager	128	Standort	95	Verbindliches Profil	171
Ressourcenmonitor	185	Standortunabhängiges Drucken	150	Verbindungsobjekt	10
Reverse Lookupzone	82	Standortverknüpfung	60, 99	Vererbung	117, 120
Roaming Profiles	169	Standortverknüpfungsbrücke	100	Verrechnung mit Gruppen	114
RODC (Read-only Domain Controller)	58	Startoptionen, erweiterte	215	Versteckte Freigabe	124
Rollen hinzufügen	33	Storage Pools	201	Vertrauensstellungen	56
Rollendienste für Remotedesktop		Storage Spaces	201	Verzeichnisdienste	19, 55
hinzufügen	34	Struktur	56	Verzeichnisstruktur	55
RSAT (Remote Server Administration Tools)	103	Strukturdomäne erstellen	69	Virtuellen Arbeitsspeicher konfigurieren/optimieren	38
		Stubzone	80	Volume	194
		Subdomäne erstellen	68	Volume erstellen	196
		Subnetzmaske	15	Volume, dynamisches	194
S		System wiederherstellen	215	Volumeschattenkopie	200, 207
		Systemeigenschaften	36		
SACL (Security Access Control List)	117	Systemimage-Wiederherstellung	216	W	
Sammlungssatz	187	Systeminformationen	35		
Schattenkopie	200	Systemstart, Optionen	215	WDK (Windows Driver Kit)	48
Schattenkopie aktivieren	201	Systemsteuerung	31	WDS (Windows Deployment Services)	20
Schlüssel sichern, Registrierung	190	Systemverhalten	37	Wiederherstellung, Anwendungen	214
Schlüssel wiederherstellen, Registrierung	191	Systemwiederherstellungs-optionen,		Wiederherstellung, Ordner und Dateien	213
Schlüsselsicherheit verwalten, Registrierung	191	Eingabeaufforderung	218	Wiederherstellung, Systemstatus	214
Schlüsselzugriffe überwachen, Registrierung	192	Sysvol	61	Wiederherstellung, Volumes	213
Server-Core	8	T		Windows Azure Backup	208
Servergespeicherte Benutzerprofile	171	Tastaturbelegung, mehrsprachige	43	Windows Server 2022, Editionen	6
Server-Manager	11, 20, 33	TCP/IP	15	Windows Server 2022, Tastenkombinationen	10
Server-Manager, Erstkonfiguration	26	Terminaldienste	20	Windows-Domäne	14, 55
Server-Sicherung installieren	208	Testversion	23	WINS-Server	18
Server-Sicherung starten	208	Thin Provisioning	202	WMI (Windows Management Interface)	20
Sicherheitsereignisse	181	Tiles	10		
Sicherheitsgruppe	112	Time to Live	76	Z	
Sicherheitskennung	103	Tombstone	219		
Sicherung wiederherstellen	212	Tombstone Lifetime	220	Zonendatei	73
Sicherung, einmalige	212	Treiber	47	Zonendatei, Einträge	74
Sicherung, System-reservierte	210	Treiber aktualisieren/zurücksetzen	53	Zonendatei, Ressourceneinträge (Resource Records)	74
Sicherung, Systemstatus	210	Treibersignatur überprüfen	48	Zonentransfer	79
Sicherungsarten	207	TTL	76	Zugriffsbasierte Aufzählung	127, 135
Sicherungsmedien	207	U		Zugriffssteuerung	117
Sicherungszeitplan erstellen	209				
SID (Security Identifier)	103	Übertragungsgeschwindigkeiten	13		
Speicherberichtverwaltung	133	Überwachung	177		
Speichermedien	194	Überwachungsrichtlinien	164, 181		
Speicherort der Registry	189	Umgebungsvariablen	37		
Speicherpools	141	Universelle Gruppe	113		

Impressum

Matchcode: W2022AVN

Autoren: Karsten Bratvogel, Thomas Joos

Produziert im HERDT-Digitaldruck

1. Ausgabe, August 2022

HERDT-Verlag für Bildungsmedien GmbH
Am Kuemmerling 19
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.

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

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.