

LERNEN EINFACH GEMACHT



Windows Server

für
dummies®



Windows Server
installieren und konfigurieren

Das Netzwerk verwalten,
überwachen und sichern

Wichtige Serverrollen kennen:
Active Directory, DNS, DHCP,
Dateiserver, Hyper-V

Thomas Bär
Frank-Michael Schlede

Windows Server für Dummies

Schummelseite

WAS BEI DER ARBEIT MIT DEM SERVER HELFEN KANN

Die folgenden Tipps werden Ihr Leben und Ihre Arbeit mit dem Server leichter machen:

- ✓ **Anmelden am Server:** Grundsätzlich muss zur Anmeldung am Windows-Server die Tastenkombination **Strg** + **Alt** + **Entf** genutzt werden, um dann Nutzernamen und Passwort einzugeben.
- ✓ **Anmelden an einer Domäne:** Zur Anmeldung an einen Domänencontroller ist der Nutzernamen immer in der Form <DOMÄNENNAME\KONTONAME> einzugeben.
- ✓ **Wer braucht den Media Player?** Standardmäßig ist auch bei Windows Server der Media Player installiert. Durch Aufruf des folgenden Befehls an der Kommandozeile mit Administratorberechtigung ist das Problem erledigt und der Media Player deinstalliert:

```
dism /online /Disable-Feature  
/FeatureName:WindowsMediaPlayer /norestart
```

- ✓ **Schneller Zugriff auf die Systemeigenschaften:** Sie wollen den Zugriff via Remotedesktop auf Ihren Server ermöglichen? Der folgende Aufruf an der Kommandozeile macht den schnellen Zugriff auf die »altbewährten« Systemeigenschaften möglich, wo Sie diese Einstellung vornehmen können:

```
sysdm.cpl
```

- ✓ **Informationen zu Sitzungen mit den Remotedesktop-Diensten:** Welche Nutzer mit einem Windows-Server via Remotedesktop verbunden sind, zeigt Ihnen der Aufruf des folgenden Befehls:

```
qwinsta /server:<Servername>
```

- ✓ Wird <Servername> weggelassen, zeigt der Befehl die Verbindungen zum aktuellen Server an. Auch interessant: Mit dem Parameter /vm zeigt das Programm Informationen zu Sitzungen innerhalb von virtuellen Computern an.
- ✓ **»cmd« an der aktuellen Stelle:** Gerade Administratoren brauchen häufig die Kommandozeile, die auch durch den Aufruf des Befehls `cmd` gestartet werden kann. Wer die Eingabeaufforderung direkt an der Stelle im Dateibaum starten will, an der er sich befindet, gibt einfach den Befehl `cmd` in die Adressleiste des Explorers ein. Dann öffnet sich das Fenster der Eingabeaufforderung mit dem

aktuellen Pfad als Startpunkt.

- ✓ **SSH-Server unter Windows Server 2019:** Wer in seinem Netzwerk nicht nur Windows-, sondern auch Linux-Server einsetzt, wird zum Verbindungsaufbau auch auf die Secure Shell (SSH) zurückgreifen wollen. Die entsprechende Server-Software kann mithilfe der PowerShell installiert werden:

```
Get-WindowsCapability -Online | ? name -like  
*OpenSSH.Server* | Add-WindowsCapability -Online
```

- ✓ Der Aufruf prüft zunächst den korrekten Namen des Pakets, um es dann auch gleich zu installieren. Mit dem nachfolgenden Aufruf wird anschließend der Dienst auf Ihrem Server gestartet:

```
Start-Service sshd
```



Thomas Bär und Frank-Michael Schlede

Windows Server **für** **dummies®**

Fachkorrektur von Nina Eichinger

WILEY
WILEY-VCH GmbH

Windows Server für Dummies

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

© 2022 Wiley-VCH GmbH, Boschstraße 12, 69469 Weinheim, Germany

Wiley, the Wiley logo, Für Dummies, the Dummies Man logo, and related trademarks and trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries. Used by permission.

Wiley, die Bezeichnung »Für Dummies«, das Dummies-Mann-Logo und darauf bezogene Gestaltungen sind Marken oder eingetragene Marken von John Wiley & Sons, Inc., USA, Deutschland und in anderen Ländern.

Das vorliegende Werk wurde sorgfältig erarbeitet. Dennoch übernehmen Autoren und Verlag für die Richtigkeit von Angaben, Hinweisen und Ratschlägen sowie eventuelle Druckfehler keine Haftung.

Print ISBN: 978-3-527-71552-7

ePub ISBN: 978-3-527-81906-5

Coverfoto: © basiczto – stock.adobe.com

Korrektur: Claudia Lötschert, Neuss

Über die Autoren

Thomas Bär, der seit Ende der neunziger Jahre in der IT tätig ist, bringt weitreichende Erfahrungen bei der Einführung und Umsetzung von IT-Prozessen im Gesundheitswesen mit. Dieses in der Praxis gewonnene Wissen hat er seit Anfang 2000 in zahlreichen Publikationen als Fachjournalist in einer großen Zahl von Artikeln umgesetzt. Er lebt und arbeitet in Günzburg.

Frank-Michael Schlede arbeitet seit den achtziger Jahren in der IT und ist seit 1990 als Trainer und Fachjournalist tätig. Nach unterschiedlichen Tätigkeiten als Redakteur und Chefredakteur in verschiedenen Verlagen arbeitet er seit Ende 2009 als freier IT-Journalist für verschiedene Online- und Print-Publikationen sowie als Trainer für LinkedIn Learning. Er lebt und arbeitet in Pfaffenhofen an der Ilm.

Inhaltsverzeichnis

[Cover](#)

[Titelblatt](#)

[Impressum](#)

[Über die Autoren](#)

[Einführung](#)

[Über dieses Buch](#)

[Was Sie nicht lesen müssen](#)

[Törichte Annahmen über den Leser](#)

[Wie dieses Buch aufgebaut ist](#)

[Symbole, die in diesem Buch verwendet werden](#)

[Wie es weitergeht](#)

[Teil I: Windows-Server-Grundlagen](#)

[Kapitel 1: Windows-Server-Grundlagen](#)

[Das kleine 1x1 der Server](#)

[Hardware-Anforderungen](#)

[Hardware Compatibility List – HCL](#)

[Darf es ein bisschen mehr sein? Sizing des Servers](#)

[Kapitel 2: Wer zählt die Versionen und Editionen?](#)

[Server-Geschichte: Windows NT Server bis 2019](#)

[Windows Server 2019: Neuerungen und Vorteile](#)

[Editionen, Versionen und Service-Kanäle](#)

[Andere Welten \(1\): Windows-Subsystem für Linux](#)

[Andere Welten \(2\): Container, Docker, Kubernetes](#)

[Windows Server 2022 – die kommende Generation](#)

[Kapitel 3: Cloud und lokal](#)

[Installation: Cloud oder lokal?](#)

[Windows Server in der Azure Cloud](#)

[Alternative Cloud-Anbieter und deren Anbindungen](#)

Kapitel 4: Fenster oder Konsole?

[Windows-Oberfläche versus Kommandozeile](#)

[Was die Eingabeaufforderung so kann](#)

[Kommandozeile: Arbeiten direkt »am Prompt«](#)

Kapitel 5: PowerShell und der Server

[Wichtige PowerShell-Grundlagen](#)

[Begriffe und Besonderheiten der PowerShell](#)

[Erste Schritte zum eigenen Skript](#)

[PowerShell in der Server-Verwaltung einsetzen](#)

Teil II: Einrichtung und wichtige Rollen

Kapitel 6: Installation von Windows Server

[Die Frage nach dem Boot-Medium](#)

[Schritt für Schritt: die Installation](#)

[Alternative: Core-Server installieren](#)

Kapitel 7: Active Directory

[Was ist überhaupt ein Active Directory?](#)

[Grundbegriffe rund um das Active Directory](#)

[Installation einer Active-Directory-Domäne](#)

[Erste Benutzer und Computer](#)

[Administrative Konten](#)

[Weiteren Domänencontroller in einer Domäne installieren](#)

[Replikation](#)

[Betriebsmasterrollen](#)

[Entfernung eines Domänencontrollers](#)

[Active-Directory-Verwaltung über den Client](#)

[Active-Directory-Papierkorb](#)

[Active-Directory-Verwaltungscenter](#)

[Gruppen, Benutzer, Container und OUs](#)

Kapitel 8: DNS und DHCP

[Grundlagen der Namensauflösung](#)

[Basiseinrichtung des DNS-Server-Diensts](#)

[DNS-Konfiguration](#)

[Microsoft-DNS-Server-Historie](#)

[Allgemeine DNS-Sicherheit](#)

[DNS absichern mit DNSSEC und DANE](#)

[Konfiguration von DNSSEC](#)

[Grundlagen von DHCP](#)

[APIPA](#)

[Installieren eines DHCP-Servers](#)

[IPAM](#)

Kapitel 9: Speicherdienste – Datei-Server

[Platten und Storage](#)

[RAID, iSCSI-Zielserver und iSCSI-Initiator](#)

[iSCSI-Zielspeicheranbieter](#)

[Server für NFS](#)

[Freigaben, Datei-Server, Ressourcenmanager](#)

[Datenduplizierung](#)

[DFS-Namespaces](#)

[DFS-Replikation](#)

[Grundlagen zu BranchCache für Datei-Server](#)

[Grundlagen zu Arbeitsordnern](#)

Kapitel 10: Erweiterte Ressourcenfreigaben

[Versteckte und administrative Freigaben](#)

[Dateifreigaben organisieren](#)

[Dynamic Access Control](#)

[Prüfung des effektiven Zugriffs](#)

Kapitel 11: Hyper-V

[Virtualisierung: Begriffe und Bestandteile](#)

[Vorteile beim Einsatz von Hyper-V](#)

[Einrichtung der Hyper-V-Rolle](#)

[Hyper-V konfigurieren](#)

[Manager für virtuelle Switches](#)

Kapitel 12: Virtuelle Computer einsetzen

[Anlegen einer virtuellen Maschine](#)

[Konfiguration der virtuellen Maschine](#)

Kapitel 13: Windows und Linux als Gastssystem

[Virtuelle Computer mit der PowerShell im Griff](#)

[Ein genauerer Blick auf die Prüfpunkte](#)

[Ubuntu-Linux als Gastssystem](#)

Kapitel 14: Druckdienste

[Begrifflichkeiten](#)

[Installation von Druck- und Dokumentendiensten](#)

[Druckerserver in der Druckerverwaltung hinzufügen](#)

[Arbeiten mit Druckfiltern](#)

[Drucker in der Druckerverwaltung hinzufügen](#)

[Drucker bereitstellen](#)

[Drucker im- und exportieren](#)

[Druckaufträge im Spooler ansehen](#)

[Line Printer Daemon und Line Printer Remote](#)

[Druckertreiberisolation](#)

[Internetdrucken](#)

Teil III: Windows-Server im Einsatz

Kapitel 15: Domänen-Beitritt

[Vorbedingungen für den Domänen-Beitritt](#)

[Einbinden in die Domäne](#)

[Offline einer Domäne beitreten](#)

Kapitel 16: Gruppenrichtlinien

[Gruppenrichtlinienobjekt verknüpfen](#)

[Gruppenrichtlinienobjekt löschen](#)

[Gruppenrichtlinien und Gruppen](#)

[WMI-Filter](#)

[WMI Query Language](#)

[Zielgruppenadressierung](#)

[Administrative Vorlagen](#)

[Central Store](#)

[Handlungsempfehlung für Gruppenrichtlinien](#)

[Praktische Empfehlungen](#)

[Troubleshooting für Gruppenrichtlinien](#)

Kapitel 17: Überwachung des Server-Betriebs

[Der Server-Manager](#)

[Verwalten des lokalen Servers](#)

[Lokalen Server konfigurieren](#)

[Überblick über das Tools-Menü](#)

Kapitel 18: Das Windows Admin Center

[Was ist das Windows Admin Center \(WAC\)?](#)

[Installation](#)

[Konfiguration und erster Einsatz](#)

Kapitel 19: Windows-Server-Updates

[Einstellungen und Features für die Updates](#)

[Update-Richtlinien verändern](#)

[Update-Einstellungen mittels sconfig ändern](#)

Kapitel 20: Backup

[Grundlagen der Sicherung und Wiederherstellung](#)

[Windows-Server-Sicherung](#)

[Einrichten von Backup-Jobs](#)

[Recovery-Medium nutzen](#)

[Einzelne Dateien wiederherstellen](#)

[Worum handelt es sich beim Azure-Backup-Dienst?](#)

Kapitel 21: Ausfälle und deren Vermeidung

[Vermeidung von Ausfällen](#)

[Monitoring](#)

Kapitel 22: Fernzugriffe

[Konsolenzugriffe](#)

[Microsoft Management Console \(MMC\)](#)

[Remote Desktop \(RDP\)](#)

[Dritthersteller-Tools](#)

Kapitel 23: Troubleshooting

[Erst die Ereignisanzeige – dann der Rest!](#)

[Eigene Dokumentationen](#)

[Server-Manager als Hilfestellung](#)

[IPv6 unterdrücken](#)

[Wo finde ich Unterstützung?](#)

Teil IV: Der Top-Ten-Teil

Kapitel 24: Die 10 besten Server-Tools

[Veeam Backup & Replication Community Edition](#)

[AD Replication Status Tool](#)

[Specops Password Auditor für Active Directory](#)

[Winscp](#)

[Microsoft Security Compliance Toolkit 1.0 \(SCT\)](#)

[WiseDateman Password Control](#)

[WireShark](#)

[RSAT](#)

[SysMon](#)

[SysInternals Suite \(komplett\)](#)

Stichwortverzeichnis

End User License Agreement

Tabellenverzeichnis

Kapitel 5

[Tabelle 5.1: Ausgewählte Alias-Bezeichnungen in der PowerShell](#)

[Tabelle 5.2: Vergleichsoperatoren der PowerShell](#)

Kapitel 7

[Tabelle 7.1: AGULP-Tabelle](#)

Kapitel 8

[Tabelle 8.1: Windows-DNS-Server-Features](#)

Kapitel 16

Illustrationsverzeichnis

Kapitel 1

[Abbildung 1.1: Die Oberfläche von Windows Server 2019: Sie ist auf den ersten Bli...](#)

[Abbildung 1.2: Erfüllt der Prozessor alle Voraussetzungen für den Einsatz mit Win...](#)

[Abbildung 1.3: Bietet Übersicht über Server-Hard- und Software und zeigt die Badg...](#)

Kapitel 2

[Abbildung 2.1: Windows Server in einer seiner ersten Ausprägungen hatte viel Ähnl...](#)

[Abbildung 2.2: Dieser Windows Server 2019 zeigt sowohl durch die Oberfläche als a...](#)

[Abbildung 2.3: Direkte Verbindung zur offenen Linux-Welt: Mithilfe des WSL werden...](#)

[Abbildung 2.4: Bis auf die aktualisierte Versionsnummer sind auf den ersten Blick...](#)

Kapitel 3

[Abbildung 3.1: Über ein Portal stehen die verschiedenen Möglichkeiten von Azure d...](#)

[Abbildung 3.2: Das Anlegen und Erstellen eines virtuellen Windows Servers 2019 au...](#)

[Abbildung 3.3: Ein virtueller Windows-2019-Server ist auf der Azure Cloud eingeri...](#)

[Abbildung 3.4: Das DHP Dashboard mit dem Ressourcenzugriff](#)

[Abbildung 3.5: Zugriff aus dem DHP Datacenter per VNC auf den neuen Server](#)

[Abbildung 3.6: Die Firewall-Steuerung von KAMP DHP arbeitet auch mit dynamischen ...](#)

[Abbildung 3.7: Anlage eines VPN-Zugangs ins KAMP DHP Datacenter](#)

Kapitel 4

[Abbildung 4.1: Die empfohlene »minimale« Installation von Windows Server 2019 geh...](#)

[Abbildung 4.2: Standardmäßig ist die PowerShell als Kommandozeile voreingestellt....](#)

[Abbildung 4.3: Das Fenster der Eingabeaufforderung lässt bei den aktuellen Versio...](#)

[Abbildung 4.4: Zwei Wege, die Festplatten und Laufwerksbuchstaben des Windows-Serv...](#)

Kapitel 5

[Abbildung 5.1: Die PowerShell ist in der Version 5 standardmäßig auf allen Versio...](#)

[Abbildung 5.2: Die PowerShell ISE \(Integrated Scripting Environment\) ist ein mäch...](#)

[Abbildung 5.3: Ein Aufruf des Cmdlets »get-command« bringt die standardmäßig auf ...](#)

[Abbildung 5.4: Mithilfe des sehr flexiblen Pipeline-Mechanismus ist es leicht mög...](#)

[Abbildung 5.5: Attribute und Methoden erlauben den Zugriff auf die jeweiligen Eig...](#)

[Abbildung 5.6: Die Arbeit mit Variablen in der PowerShell ist einfach. Dabei über...](#)

[Abbildung 5.7: Die Arrays stellen Ihnen eine Datenstruktur bereit, die es ermögli...](#)

[Abbildung 5.8: Mithilfe der Vergleichsoperatoren können Sie logische Abfragen und...](#)

[Abbildung 5.9: Mithilfe der unterschiedliche cmdlets zum Mustervergleich können S...](#)

[Abbildung 5.10: Ein einfaches Beispiel für eine »if«-Verzweigung in einem PowerSh...](#)

[Abbildung 5.11: Eine einfache »For«-Schleife, die deren grundsätzliche Funktionsw...](#)

[Abbildung 5.12: Die Variante »Foreach« der »For«-Schleife eignet sich besonders g...](#)

[Abbildung 5.13: Die »While«-Schleife ist eine klassische »abweisende« Schleife: W...](#)

[Abbildung 5.14: Die Ausführungsrichtlinien sollen verhindern, dass Nutzer gefährl...](#)

[Abbildung 5.15: Welche Prozesse sind aktiv und brauchen wie viel Zeit von der CPU...](#)

[Abbildung 5.16: Hilfe steht immer parat in der PowerShell. Ist diese nicht auf de...](#)

[Abbildung 5.17: Zwei verschiedene beispielhafte Ausgabemöglichkeiten für Prozesse...](#)

[Abbildung 5.18: Mit dem Cmdlet »Get-Printer« bringen Sie alle Drucker und Drucker...](#)

[Abbildung 5.19: Schnelles Umbenennen eines Druckernamens mithilfe des Cmdlets »Re...](#)

[Abbildung 5.20: Die PowerShell bieten Ihnen viele Module und Cmdlets, mit deren H...](#)

[Abbildung 5.21: Diese Auflistung zeigt, welche Cmdlets für die Arbeit mit Netzwer...](#)

[Abbildung 5.22: Standardmäßig unterstützt Windows Server 2019 zunächst keine Adap...](#)

[Abbildung 5.23: Nach der Installation des WLAN-Features muss nur noch der entspre...](#)

[Abbildung 5.24: Mithilfe des Cmdlets »Get-NetIPAddress« können Sie viele Informat...](#)

[Abbildung 5.25: Direkt die Verbindung zu einem System im Netzwerk überprüfen? Das...](#)

[Abbildung 5.26: Mithilfe von »Test-NetConnection« können Sie nicht nur die Verbin...](#)

Kapitel 6

[Abbildung 6.1: Die freie Software »Rufus« hilft dabei, einen bootfähigen USB-Stic...](#)

[Abbildung 6.2: Der erste Bildschirm bei der Installation von Windows Server 2019 ...](#)

[Abbildung 6.3: Eine wichtige Auswahl bei der Installation: Welche Edition von Win...](#)

[Abbildung 6.4: Die Auswahl der Installationsart: Bei einer neuen Installation von...](#)

[Abbildung 6.5: Wo möchten Sie Windows installieren? In diesem Menü können Sie die...](#)

[Abbildung 6.6: Der wichtigste Schritt nach dem ersten Neustart: das Festlegen ein...](#)

[Abbildung 6.7: Geschafft: Der Windows-Server ist installiert. Zum Entsperren des ...](#)

[Abbildung 6.8: Die sehr »spartanische« Oberfläche bei der Installation als Core-S...](#)

[Abbildung 6.9: In einer Core-Server-Installation stehen einige Programme an der K...](#)

Abbildung 6.10: Der Editor kann auch auf dem Core-Server eingesetzt werden und so...

Kapitel 7

Abbildung 7.1: Der Installationsassistent unterstützt den Administrator bei der E...

Abbildung 7.2: Die Installation des Domänendienstes ist abgeschlossen.

Abbildung 7.3: Alles klar – die Installation des DC kann beginnen.

Abbildung 7.4: Die Anlage eines Benutzerkontos auf dem Server

Abbildung 7.5: Für Änderungen sind nun Administrationsrechte erforderlich.

Abbildung 7.6: Aufruf der Computerverwaltung vom Server aus

Abbildung 7.7: Alle lokalen Konten sind deaktiviert.

Abbildung 7.8: Standard-Gruppenzuordnung eines Administratorkontos

Abbildung 7.9: Das vordefinierte Administrator-Konto wurde deaktiviert.

Abbildung 7.10: Hinzufügen von Servern in den Server-Manager

Abbildung 7.11: Gruppenzuordnung auf einem RODC

Abbildung 7.12: Auswahl des Replikationspartners für den neuen DC

Abbildung 7.13: Namentlich nicht ganz passend – Fileserver2 ist nun auch ein DC.

Abbildung 7.14: Namensauflösung zur Domäne mit zwei DCs

Abbildung 7.15: Beide Server in der Demo-Umgebung sind demselben Standort zugewie...

Abbildung 7.16: Pro Replikationsverbindung kann der Administrator einen Zeitplan ...

Abbildung 7.17: Mit dem »netdom«-Kommando ermittelt der Administrator die aktuell...

Abbildung 7.18: Das Entfernen eines nicht mehr aktiven DC ist über einen Assisten...

Abbildung 7.19: Die Aktivierung des AD-Papierkorbs im AD-Verwaltungscenter ist nu...

Abbildung 7.20: Neben der Wiederherstellung gelöschter Objekte können Sie im Verw...

Abbildung 7.21: Vordefinierte Sicherheitsgruppen im Container »Builtin«

Abbildung 7.22: Bei Anlage einer Gruppe legt der Administrator im Gruppenbereich ...

Abbildung 7.23: Benutzer können Mitglieder verschiedener Gruppen sein.

Abbildung 7.24: Die Mehrheit der Dienste unter Windows arbeitet mit dem

[Konto »SY...](#)

[Abbildung 7.25: Ausgabe der Gruppenzugehörigkeiten](#)

Kapitel 8

[Abbildung 8.1: Durch Manipulation der »hosts«-Datei erzeugt die Namensauflösung s...](#)

[Abbildung 8.2: Die Installation des DNS-Diensts wird durch den Assistenten unters...](#)

[Abbildung 8.3: Ein DNS-Server ist typischerweise für eine oder mehrere Zonen zust...](#)

[Abbildung 8.4: Ob Fantasiename oder echter Name – die Namensauflösung funktionier...](#)

[Abbildung 8.5: Die Debugprotokollierung hilft bei der Fehlersuche.](#)

[Abbildung 8.6: Die Wiederherstellung der Stammhinweise ist durch die Kopierfunkt...](#)

[Abbildung 8.7: Sofern A-Eintrag und PTR-Eintrag vorliegen, löst »nslookup« in bei...](#)

[Abbildung 8.8: Computer erlauben als Client die Abfrage vieler DNS-Server.](#)

[Abbildung 8.9: Die Überprüfung des Master-DNS-Servers ist für die erfolgreiche An...](#)

[Abbildung 8.10: DNS-Server ohne AD-integrierte DNS-Zonen speichern die Dateien im...](#)

[Abbildung 8.11: Administratoren verwenden dieses Dialogfenster zur Festlegung der...](#)

[Abbildung 8.12: Die Erstellung der Schlüsselsignatur sieht komplizierter aus, als...](#)

[Abbildung 8.13: DNSSEC erweitert die Zone um eine Vielzahl von Einträgen.](#)

[Abbildung 8.14: Prüfung der DNSSEC-Einstellungen im Vergleich](#)

[Abbildung 8.15: Ohne Autorisierung funktioniert ein DHCP-Server im AD nicht ordnu...](#)

[Abbildung 8.16: Die IP-Bereichsangabe im DHCP-Dialog ist dankenswert einfach.](#)

[Abbildung 8.17: Denkbar einfach und schnell zu bearbeiten: die Eingabe der notwen...](#)

[Abbildung 8.18: Zur Bearbeitung von Reservierungslisten eignet sich ein Tabellenk...](#)

[Abbildung 8.19: Der Massenimport für IP-Reservierungen ist mit der PowerShell seh...](#)

[Abbildung 8.20: Über Server- und Bereichsoptionen steuern Administratoren grundle...](#)

[Abbildung 8.21: Konfiguration einer Failover-Beziehung als »Hot Standby«](#)

[Abbildung 8.22: Welche Rolle der Server im DHCP-Failover einnimmt, gibt das Eigen...](#)

[Abbildung 8.23: Welche Rolle der Server im DHCP-Failover einnimmt, gibt das Eigen...](#)

[Abbildung 8.24: Die Einrichtung von IPAM startet im Server-Manager.](#)

[Abbildung 8.25: IPAM-Konfiguration: selber machen – oder machen lassen?](#)

[Abbildung 8.26: Die Einrichtung von IPAM erfordert die Anlage einiger Gruppenrich...](#)

[Abbildung 8.27: Erfolgreich – die Gruppenrichtlinienobjekte wurden erzeugt.](#)

[Abbildung 8.28: IP-Adressverwaltung mit IPAM](#)

Kapitel 9

[Abbildung 9.1: Die Installation der Server-Rolle geschieht, wie gewohnt, über den...](#)

[Abbildung 9.2: Im Server-Manager ist für den Administrator ersichtlich, welche iS...](#)

[Abbildung 9.3: Wie gewöhnliche Festplatten muss der Administrator den iSCSI-Daten...](#)

[Abbildung 9.4: Schattenkopien und Vorgängerversionen funktionieren auch ohne die ...](#)

[Abbildung 9.5: Automatische Erstellung von Schattenkopien unter Windows über die ...](#)

[Abbildung 9.6: Die Installation über den Server-Manager fügt die Verwaltungstools...](#)

[Abbildung 9.7: Dank eines Assistenten ist die Einrichtung einer NFS-Freigabe mit ...](#)

[Abbildung 9.8: In der obigen Einstellung hätte jeder Computer Vollzugriff auf die...](#)

[Abbildung 9.9: Die NFS-Freigabe-Verwaltung direkt im Windows Explorer](#)

[Abbildung 9.10: Die Freigabe von Ordnern und Volumes funktioniert unabhängig von ...](#)

[Abbildung 9.11: Der Datei-Server-Dialog erlaubt den Zugriff auf einen Teilbereich...](#)

[Abbildung 9.12: Je nach Einstellung protokolliert der Server in seiner Ereignisan...](#)

[Abbildung 9.13: Die Speicherberichterverwaltung erlaubt die unkomplizierte Erstell...](#)

[Abbildung 9.14: Die Konfiguration der Datendeduplizierung nimmt der Administrator...](#)

[Abbildung 9.15: DFS-Namespaces erlauben eine Freigabebereitstellung, ohne aus den...](#)

[Abbildung 9.16: Der Windows-Replikationsdienst DFS-R eignet sich für eher statisc...](#)

Kapitel 10

[Abbildung 10.1: PCs in der Netzwerkumgebung von Windows](#)

[Abbildung 10.2: Auflistung aller Freigaben auf dem PC](#)

[Abbildung 10.3: Laufwerkzuordnung per Gruppenrichtlinie](#)

[Abbildung 10.4: ERSTELLER-BESITZER wurde entfernt.](#)

[Abbildung 10.5: Obwohl kein Zugriff erlaubt, wird der Ordner dennoch angezeigt](#)

[Abbildung 10.6: Aktivierung von ABE im Server-Manager](#)

[Abbildung 10.8: Eingabe eines Attributwerts in den erweiterten Features](#)

[Abbildung 10.9: Die Verwendung von DCA erfordert die Aktivierung auf den DCs.](#)

[Abbildung 10.7: Möglichkeit zur Einrichtung der dynamischen Zugriffssteuerung \(DA...](#)

[Abbildung 10.10: Festlegung der Berechtigung](#)

[Abbildung 10.11: Zuordnung einer CAP über eine Gruppenrichtlinie](#)

[Abbildung 10.12: Der Eintrag der Ressource Property im Ressourcen-Manager](#)

[Abbildung 10.13: Zuordnung einer Ressource Property](#)

[Abbildung 10.14: Zuweisung einer Richtlinie zu einer Datei](#)

[Abbildung 10.15: Anzeige des effektiven Zugriffs basierend auf Ansprüchen \(Claims...](#)

Kapitel 11

[Abbildung 11.1: Der Assistent im Server-Manager führt Schritt für Schritt durch d...](#)

[Abbildung 11.2: Die Features für den Hyper-V: Durch sie kommen die Verwaltungswer...](#)

[Abbildung 11.3: Ein wichtiger Schritt bei der Einrichtung von Hyper-V ist das Anl...](#)

[Abbildung 11.4: Die Konsole des Hyper-Managers: Sie erlaubt unter anderem das Ers...](#)

[Abbildung 11.5: Etwas verborgen finden sich im Einstellungsmenü von Hyper-V auch ...](#)

[Abbildung 11.6: Der Manager für virtuelle Switches: Ohne einen solchen virtuellen...](#)

[Abbildung 11.7: Das Anlegen eines ersten externen virtuellen Switches ist mit dem...](#)

[Abbildung 11.8: Nachdem der Switch angelegt wurde, existiert ein virtueller Netzw...](#)

[Abbildung 11.9: Das Modul Hyper-V der PowerShell stellt auch eine Reihe von Befeh...](#)

[Abbildung 11.10: Das Anlegen und Zuweisen eines neuen virtuellen Switches ist mit...](#)

Kapitel 12

[Abbildung 12.1: Der Eintrag »Virtueller Computer« führt zum Assistenten für das A...](#)

[Abbildung 12.2: Die Wahl der Generation einer virtuellen Maschine ist davon abhän...](#)

[Abbildung 12.3: Unter »Netzwerk konfigurieren« legen Sie fest, ob und mit welchem...](#)

[Abbildung 12.4: Hier können Sie die virtuelle Festplatte anlegen und konfiguriere...](#)

[Abbildung 12.5: Die abschließende Zusammenfassung zeigt alle Einstellung, die Sie...](#)

[Abbildung 12.6: Die noch »leere« virtuelle Maschine kann nun über die Einstellung...](#)

[Abbildung 12.7: Konfiguration und Verwaltung wie bei einem »echten« PC: Diese Ein...](#)

[Abbildung 12.8: Im Eintrag »Firmware« können Sie die Startreihenfolge der virtuel...](#)

[Abbildung 12.9: Die Einstellungen für den Arbeitsspeicher der virtuellen Maschine...](#)

[Abbildung 12.10: In den Einstellungen für den SCSI-Controller können Sie weitere ...](#)

[Abbildung 12.11: Prüfpunkte sind ein sehr nützliches Feature, durch das virtuelle...](#)

Kapitel 13

Abbildung 13.1: Um die Installation des Betriebssystems in der VM zu starten, müs...

Abbildung 13.2: Ohne virtuelles DVD-Laufwerk geht es nicht. Nur so kann das Gasts...

Abbildung 13.3: Kein Unterschied zu einer »normalen« Installation, sobald der vir...

Abbildung 13.4: Der virtuelle Computer ist aktiv und bietet bei der Anmeldung mit...

Abbildung 13.5: Der Netzwerkadapter im Gastsystem: ein Ausschnitt aus dem Vollbil...

Abbildung 13.6: Das Menü an der oberen Leiste der Konsole bietet einige Einstell...

Abbildung 13.7: Das PowerShell-Modul für Hyper-V stellt eine große Auswahl an Cmd...

Abbildung 13.8: Informationen zu den aktiven und nicht aktiven virtuellen Maschin...

Abbildung 13.9: Prüfpunkte können im Hyper-V-Manager direkt aus dem Kontextmenü d...

Abbildung 13.10: Der neue Prüfpunkt wurde in einer aktiven virtuellen Maschine er...

Abbildung 13.11: Das Cmdlet »Checkpoint-VM« hilft dabei, einen neuen Prüfpunkt fü...

Abbildung 13.12: Das Zurücksetzen eines virtuellen Computers durch die Anwendunge...

Abbildung 13.13: Auch mithilfe der PowerShell kann ein virtueller Computer auf ei...

Abbildung 13.14: Ein sicherer Start für einen virtuellen Computer mit Ubuntu-Linu...

Abbildung 13.15: Die Installation einer aktuellen Linux-Version (hier Ubuntu 20.0...

Abbildung 13.16: Nach der Installation: Ubuntu Linux in einer virtuellen Maschine...

Abbildung 13.17: Mithilfe dieser Konfiguration im Linux-Gast kann dieser im Vollb...

Kapitel 14

Abbildung 14.1: Mit der Zeit sammeln sich Unmengen an Druckertreibern.

Abbildung 14.2: Bei der Rollenbeschreibung wurde der Text nicht übersetzt.

Abbildung 14.3: Die Dienste LPD und IPP werden die meisten

Administratoren nicht ...

Abbildung 14.4: Bei Bedarf kann sich der Administrator die Gesamtzahl der Element...

Abbildung 14.5: Die Druckerverwaltung erlaubt die Anlage eigener Filter, die der ...

Abbildung 14.6: Wenn es schnell gehen soll: Ohne Druckertreiberidentifikation geh...

Abbildung 14.7: Druckertreiber lädt der Administrator über das »Windows Update« b...

Abbildung 14.8: Das Kommandozeilentool »PrintBrm.exe« ist beim Umzug oder zur Sic...

Abbildung 14.9: Altmodisch, unsicher – aber praktisch: der LPR-Druck

Abbildung 14.10: Den Betriebsmodus der Treiberisolation legt der Administrator pr...

Abbildung 14.11: Um Internetdruck auf dem Server zu nutzen, ist die gleichzeitige...

Abbildung 14.12: Die Verwaltungsseite für Druckaufträge

Abbildung 14.13: Der Client für den Internetdruck auf einem Windows-10-PC

Kapitel 15

Abbildung 15.1: Vor dem Beitritt zur Domäne: Der Server besitzt bereits einen ein...

Abbildung 15.2: Ein Aufruf des Ping-Kommandos zeigt, ob der Domänencontroller vom...

Abbildung 15.3: Damit der Server in die Domäne aufgenommen werden kann, müssen Än...

Abbildung 15.4: In den Eigenschaften des IPv4-Protokolls konfigurieren Sie Ihr Sy...

Abbildung 15.5: Es ist nicht unbedingt notwendig, aber praktisch, wenn bereits im...

Abbildung 15.6: Der Server wird Mitglied der Domäne, deren Namen an dieser Stelle...

Abbildung 15.7: Die eigentliche Anmeldung an der Domäne erfolgt mit dem Konto ein...

Abbildung 15.8: Die Anmeldung an einer Domäne muss immer den Namen der Domäne ent...

Abbildung 15.9: Ein Offline-Beitritt zu einer AD-Domäne gliedert sich in zwei Sch...

Abbildung 15.10: Der zweite Schritt: Auf dem Server wird die Datei mit den

[Daten ...](#)

Kapitel 16

[Abbildung 16.1: Gruppenrichtlinienobjekte sind OUs in der Gruppenrichtlinienverwa...](#)

[Abbildung 16.2: Anlage einer Verknüpfung für eine Gruppenrichtlinie](#)

[Abbildung 16.3: Die Abarbeitungsreihenfolge verläuft von unten nach oben.](#)

[Abbildung 16.4: Inhalt und Ablageort des Gruppenrichtlinienobjekts](#)

[Abbildung 16.5: Beim Löschen eines Gruppenrichtlinienobjekts entfernt Windows aut...](#)

[Abbildung 16.6: Mit der Sicherheitsfilterung wirken Gruppenrichtlinien direkt auf...](#)

[Abbildung 16.7: Das WMI Filter Validation Utility ersetzt die fehlende Testfunkt...](#)

[Abbildung 16.8: Zielgruppenadressierung mit zwei Eigenschaften in einer ODER-Verk...](#)

[Abbildung 16.9: Administrative Vorlagen erlauben eine einfache Einstellungssteuer...](#)

[Abbildung 16.10: Das Dialogfenster für administrative Vorlagen](#)

[Abbildung 16.11: Mithilfe der expliziten Zuweisung von Anmelderechten wird die An...](#)

[Abbildung 16.12: Nur bestimmte Personen dürfen sich an diesem Computer anmelden.](#)

[Abbildung 16.13: Ein Desktophintergrund, der per Gruppenrichtlinie festgelegt wur...](#)

[Abbildung 16.14: Windows bietet viele Möglichkeiten, die Sicherheit zu erhöhen: b...](#)

[Abbildung 16.15: Hier ist die Zuordnung des Browsers über die Dateinamenerweiteru...](#)

[Abbildung 16.16: Programme im Griff: Wordpad kann nun nicht mehr gestartet werden...](#)

[Abbildung 16.17: Eine Auswertung von Gruppenrichtlinien per »gpreresult«](#)

Kapitel 17

[Abbildung 17.1: Beim ersten Start meldet sich der Server-Manager mit einem Dashbo...](#)

[Abbildung 17.2: Fast alle Einstellungen und Konfigurationsmöglichkeiten sind dire...](#)

[Abbildung 17.3: Bei den Eigenschaften des Server-Managers ist es möglich,](#)

[das Akt...](#)

[Abbildung 17.4: Die Seite »Lokaler Server« des Server-Managers bietet viele Infor...](#)

[Abbildung 17.5: Nach der Auswahl von »Lokaler Server herunterfahren« können Sie d...](#)

[Abbildung 17.6: Bei den Eigenschaften des lokalen Servers sind die Einträge als H...](#)

[Abbildung 17.7: Mehrere Wege führen zu den Server-Tools: Sie sind aus dem Server-...](#)

[Abbildung 17.8: Viele Tools – wie hier die Computerverwaltung – werden in einer M...](#)

[Abbildung 17.9: Die drei Windows-Protokolle »Anwendung«, »Sicherheit« und »System...](#)

Kapitel 18

[Abbildung 18.1: Wer das Windows Admin Center einsetzen will, kann sich auf Micros...](#)

[Abbildung 18.2: Bei der Installation des WAC entscheiden Sie auch, ob Sie Microso...](#)

[Abbildung 18.3: Für die Installation auf einem Stand-alone-Server ist der Einsatz...](#)

[Abbildung 18.4: Es erleichtert die Verwaltung entfernter Systeme mit dem WAC, wen...](#)

[Abbildung 18.5: Der letzte Schritt: Port für den Dienst angeben und Zertifikat zu...](#)

[Abbildung 18.6: Wie starte ich das Windows Admin Center? Der Setup-Assistent gibt...](#)

[Abbildung 18.7: Der erste Start: Noch ist nur der Windows-Server, auf dem das WAC...](#)

[Abbildung 18.8: Auswahl und Hinzufügen einer Ressource zum WAC auf einem Windows ...](#)

[Abbildung 18.9: Das Hinzufügen eines Servers zum Windows Admin Center](#)

[Abbildung 18.10: Der neue Server wurde hinzugefügt und erscheint in der Übersicht...](#)

[Abbildung 18.11: Mehrere Systeme mit den gleichen Anmeldedaten einzubinden, gelin...](#)

[Abbildung 18.12: Nach Auswahl der Einstellungen werden dem Nutzer zunächst die Ko...](#)

[Abbildung 18.13: Wie kann das WAC auf das Internet zugreifen? Manchmal](#)

kann es du...

Abbildung 18.14: Das Windows Admin Center kann mit vielen Erweiterungen ergänzt w...

Abbildung 18.15: WAC zeigt die verfügbaren Erweiterungen mitsamt deren Details an...

Abbildung 18.16: Die Übersichtsseite eines Servers zeigt im Windows Admin Center ...

Abbildung 18.17: Das Menü »Einstellungen« ermöglicht es Ihnen, einige wichtige Be...

Abbildung 18.18: Die »Rollenbasierte Zugriffssteuerung« ermöglicht es Nutzern, be...

Abbildung 18.19: Nachdem die »Rollenbasierte Zugriffssteuerung« aktiviert wurde, ...

Abbildung 18.20: WAC erlaubt es dem Nutzer, jedes Tool aus der Liste in einem eig...

Kapitel 19

Abbildung 19.1: Gibt es Updates für meinen Server? Die Windows-Einstellungen und ...

Abbildung 19.2: Windows Server zeigt Ihnen an, welche Richtlinien für die Updates...

Abbildung 19.3: Auf der Seite »Update und Sicherheit« finden Sie unter »Windows U...

Abbildung 19.4: Sie können das Herunterladen der Updates auf dieser Seite für sie...

Abbildung 19.5: Mithilfe der »Erweiterten Optionen« ist es möglich, die Installat...

Abbildung 19.6: Die Übermittlungsoptimierung kann Downloads von Updates beschleun...

Abbildung 19.7: Kein automatischer Neustart für den Server: Der Zeitraum für dies...

Abbildung 19.8: Wenn Updates wieder entfernt werden müssen, kommt auf dem Server ...

Abbildung 19.9: Über den Aufruf von »gpedit.msc« kann auf Windows Server der Edit...

Abbildung 19.10: Mit dem Eintrag »Automatische Updates konfigurieren« können Sie ...

Abbildung 19.11: Auch das Kommandozeilen-Programm »sconfig« bietet recht komforta...

[Abbildung 19.12: Mithilfe von »sconfig« können Sie die Update-Einstellungen sehr ...](#)

Kapitel 20

[Abbildung 20.1: Die »Windows Server-Sicherung« ist komplett assistentengestützt u...](#)

[Abbildung 20.2: VSS-Optionen für die Sicherung von einzelnen Elementen](#)

[Abbildung 20.3: Zunächst gilt es, den Speicherort für das Backup auszuwählen, dan...](#)

[Abbildung 20.4: Die »Windows Server-Sicherung« bietet die Optionen zur vollständi...](#)

Kapitel 21

[Abbildung 21.1: Die schnelle Installation von Updates ist die wichtigste Maßnahme...](#)

[Abbildung 21.2: Wird die entsprechende Option aktiviert, erhält der Server auch U...](#)

[Abbildung 21.3: Mit »mdsched« können Sie den Betriebszustand des Arbeitsspeichers...](#)

[Abbildung 21.4: Die Windows-Bordmittel bieten eine laufende Überwachung, um Serve...](#)

[Abbildung 21.5: Nagios XI und NCPA helfen dem Windows-Administrator beim Monitori...](#)

[Abbildung 21.6: O&O Syspectr eignet sich besonders für verteilte Umgebungen.](#)

Kapitel 22

[Abbildung 22.1: Zugriff auf die Konsole über PS-Execute](#)

[Abbildung 22.2: Zugriff über Windows-PowerShell-Remoting](#)

[Abbildung 22.3: Verbindung mit einem anderen Computer in der MMC herstellen](#)

[Abbildung 22.4: Aktivierte Remotedesktop-Verbindung auf einem Windows Server 2022...](#)

[Abbildung 22.5: Das kostenlose Ultra-VNC bietet ebenfalls die Funktion zur Versch...](#)

[Abbildung 22.6: Bekannte Fernzugriffslösung aus Deutschland: Teamviewer](#)

[Abbildung 22.7: Kostenfreie Fernwartungs-Software von O&O Software – Syspectr](#)

Kapitel 23

Abbildung 23.1: Erste Anlaufstelle bei Fehlverhalten: das Eventlog

Abbildung 23.2: Die Zeichen stehen auf Rot – der Server-Manager erinnert den Admi...

Abbildung 23.3: Ergebnis einer BPA-Prüfung des DHCP-Service

Abbildung 23.4: Microsoft hilft bei der Suche nach dem einen passenden Partner.

Einführung

Server – das sind doch diese Maschinen, die irgendwo im Rechenzentrum (oder gar »in der Wolke«) stehen und auf denen alles abläuft: Unsere Mail liegt auf irgendeinem Server bei einem Provider, Daten werden auf einem Cloud-Laufwerk gespeichert, das sich in der Regel auf irgendeinem Server befindet, und im Büro ermahnt die IT die Mitarbeiter streng, alle Daten nur auf dem Server in der Domäne abzuspeichern.

Und obwohl uns allen Server alltäglich begegnen, muss doch kein Nutzer tiefer in das Thema einsteigen. Warum also ein Buch – zudem ein Dummies-Buch –, das sich mit diesem Thema der IT-Profis und -Nerds beschäftigt?

So ernteten wir dann zunächst auch milden Spott und Kopfschütteln von unseren vielen Bekannten und Freunden aus dem IT-Umfeld. Allgemeiner Tenor war: »Dummies und Server, das passt nicht«. Ein Blick auf die vielen Bücher auf dem Markt, die sich der Thematik »Windows Server« widmen, zeigt dann auch vor allem Werke, die einen Seitenumfang von 1.000 Seiten und mehr haben.

Über dieses Buch

Wer dieses Buch lesen sollte? Nach unserer Meinung: alle! Alle, die sich mit Windows-Servern auseinandersetzen möchten, entweder aus rein privatem Interesse oder weil es beruflich ansteht. In dem vorliegenden Buch sind die Themen aufeinander abgestimmt und in eine logisch aufbauende Reihenfolge gebracht. Somit haben auch Laien die Möglichkeit, sich rasch in das Server-Thema einzufinden.

Windows für den Dauerbetrieb, ein Windows-Computer, der Dienste für andere Benutzer und Computer zur Verfügung stellt – das ist ein Windows-Server. Wenn Sie so etwas bewerkstelligen möchten, dann sind Sie hier goldrichtig.

Als IT-Journalisten sind wir es gewohnt, auf den Punkt zu schreiben und ohne Umschweife ein Thema zu betrachten. Diese Erfahrung aus vielen

Hundert Zeitschriftenbeiträgen haben wir mit in das Buch genommen. Wir haben uns dabei ohne permanente Querverweise auf die wesentlichen Funktionsbereiche konzentriert. Alles, was Sie hier lesen, ist 1:1 so getestet und umgesetzt worden – es funktioniert!

Keine Sorge! Die wichtigsten Grundlagen für den Server-Betrieb haben durchaus Bestand. Eine Domäne, DNS und DHCP – das sind Funktionalitäten, die bereits in den frühen 2000er-Jahren mit Windows-Servern bewerkstelligt wurden. Auch wenn der IT-Branche stets unterstellt wird, dass sich faktisch alles rasch verändert, so ist dies bei den Betriebsgrundlagen glücklicherweise nicht der Fall. Mit jeder neuen Version wurde es jedoch für den Administrator immer einfacher. Diese Einfachheit darf jedoch nicht darüber hinwegtäuschen, dass Sie als IT-Verantwortlicher für Server genau verstehen müssen, was »unter der Haube« geschieht.



Wenn Sie im Internet nach Hilfestellungen bei Problemen suchen, achten Sie bitte unbedingt auf den Zeitstempel der Information. Nicht selten finden sich ältere Posts noch immer sehr weit oben in den Suchergebnissen und beschreiben Lösungswege, die nicht mehr aktuell sind.

Was Sie nicht lesen müssen

Dieses Buch ist als Einführung in das Thema Windows Server gedacht und kann an einem Stück von vorne bis hinten durchgearbeitet werden. Natürlich können Sie jederzeit Kapitel überspringen, in denen Themen behandelt werden, die nicht interessant für Sie sind. Wir empfehlen jedoch das Durcharbeiten von Kapitel zu Kapitel.

Törichte Annahmen über den Leser

Da Sie sich die Einleitung bis hierhin durchgelesen haben, gehen wir davon aus, dass Sie ein wahrlich ernstes Interesse an Windows-Servern haben. Als der Verlag auf uns zukam, haben wir uns einige Gedanken

gemacht, wer das Buch wohl lesen wird. Dabei haben wir die folgenden möglichen Lesergruppen identifiziert:

- ✓ **IT-Professional.** Sie haben schon viel Erfahrung im IT-Bereich und möchten Ihr Wissen um den Bereich Windows Server erweitern. Bisher haben Sie die Leistungen der Server genutzt, nun möchten Sie sie auch selbst bereitstellen können und sich mit diesem Bereich weiterbilden.
- ✓ **Computer-Enthusiast.** Sie sind so was wie ein »Nerd«: Sie kennen sich bei IT-Themen bestens aus und möchten irgendwann einmal Workloads mit Windows-Servern bereitstellen. Erfahren Sie, welche Grundlagen für Exchange, SQL-Server und SharePoint erforderlich sind.
- ✓ **Umsteiger.** Sie sind Linux-Administrator und möchten die Microsoft-Besonderheiten in einer strukturierten, kompakten Art und Weise kennenlernen.
- ✓ **Angehende Fachinformatiker.** Sie stehen in der Ausbildung und möchten das Grundlagenwissen über Windows-Server noch einmal von jemand anderem beschrieben erhalten.

Wie dieses Buch aufgebaut ist

Wir haben dieses Buch in drei Teile aufgeteilt. Während der erste Teil einige Grundlagen, Hintergründe und Entwicklungen rund um den Windows-Server beschreibt, sind die Teile II und III auf die Praxis ausgerichtet.

Teil I – Die Grundlagen des Windows-Servers

Was unterscheidet eigentlich einen Server von einem normalen Windows-Rechner, wie ihn die meisten Nutzer auf oder unter ihrem Schreibtisch stehen haben? Um den Windows-Server von einem »normalen« Rechner (ganz gleich ob unter Windows oder einem anderen Betriebssystem) abzugrenzen, befassen wir uns in diesem ersten Teil nicht nur mit der Entwicklung des Windows-Servers von den NT-Frühzeiten über Windows 2000 bis hin zur aktuellen Version 2022, sondern zeigen Ihnen auch, was

ein Server-System generell ausmacht: Welche Art von Hardware definiert einen Server? Welche unterschiedlichen Server-Editionen bietet Ihnen Microsoft? Zudem zeigen wir in diesem Teil auch, wie Sie mit dem Server grundsätzlich arbeiten können – nämlich sowohl mit der bekannten Windows-Oberfläche als auch direkt in der Kommandozeile. Dabei erfahren Sie auch, wie Sie die PowerShell einsetzen können, um Ihren Server zu verwalten.

Teil II – Einrichtung und wichtige Rollen

Nachdem Sie in [Teil I](#) etwas über die Server-Grundlagen und das kleine 1x1 solcher Systeme gelesen haben, wenden wir uns in [Teil II](#) der Technik des Windows-Servers zu. Wir schildern, wie das Server-Betriebssystem auf die Hardware kommt, und beschreiben die Unterschiede zwischen dem »Server mit Windows-Oberfläche« und einem Core-Server. Dann geht es ausführlich um ein Thema, das den Server in Theorie und Praxis an sich definiert: der Verzeichnisdienst Active Directory, seine Installation und seine Funktionen, aber auch um andere wichtige Rollen und Features, die Sie höchstwahrscheinlich für Ihren Windows-Server benötigen und deshalb auch einrichten müssen. Neben Diensten wie DNS und DHCP geht es in diesem Teil um die oft geschmähten, aber wichtigen Druckerdienste und nicht zuletzt um die Rolle, die Windows Server mit Hyper-V bei der Virtualisierung spielt.

Teil III – Das richtige Leben: Windows Server im Einsatz

Alles, was Sie in [Teil I](#) und [Teil II](#) gelesen und dann vielleicht auch selbst ausprobiert haben, kann Ihnen im »echten Server-Leben« helfen oder ist in einigen Fällen auch Voraussetzung dafür, dass Sie Ihren Windows-Server dann auch einsetzen können. Im dritten Teil unseres Buchs befassen wir uns mit einigen Themen, die im täglichen Server-Einsatz auf Sie zukommen: Sie lernen, wie Sie Ihren Server in eine bestehende Domäne und damit in ein bestehendes AD-Netzwerk aufnehmen können. Ein weiteres extrem wichtiges Thema beim täglichen Einsatz eines Windows-Servers sind zweifelsohne die Gruppenrichtlinien, die wir Ihnen ausführlich vorstellen und erläutern. Für den alltäglichen Betrieb

unerlässlich sind dann noch die Themen, die sich mit der Überwachung des Server-Betriebs befassen. In diesem Zusammenhang stellen wir Ihnen auch das neue Admin Center vor und zeigen, wie Sie damit arbeiten können. Zu den Themen, die bei Anwendern und Administratoren eher einen unteren Platz auf der Beliebtheitsskala einnehmen, gehören die Updates und Backups ebenso wie die Vermeidung von Ausfällen und das allgemeine Troubleshooting – sie runden den dritten Teil im Hinblick auf den Server-Einsatz sinnvoll ab.

Teil IV – Der Top-Ten-Teil

Kein Dummies-Buch ohne Top-Ten-Teil: Wir nennen Ihnen zehn Software-Werkzeuge aus der Praxis, die Ihnen die Arbeit mit einem Windows-Server sehr erleichtern können.

Symbole, die in diesem Buch verwendet werden

Damit Sie dieses Buch einfacher lesen und leichter benutzen können, machen Sie Symbole auf bestimmte Informationen aufmerksam.



Die Hand mit dem Faden kennzeichnet Informationen, an die Sie sich erinnern sollten, zum Beispiel einen besonderen Befehl, den Sie bei der Arbeit mit dem Windows Server immer wieder verwenden können.



Es war ein andauerndes Diskussionsthema zwischen uns, den Autoren, und dem Lektorat, an welcher Stelle es denn einfach »zu technisch« wird. Allerdings haben wir uns zumeist mit der Begründung durchgesetzt, dass ein Server nun mal ein hochtechnisches Thema ist. Es ist uns aber auch klar, dass nicht jeder wie wir in einer »Tekie-Blase« leben und arbeiten kann. Darum haben wir nach Möglichkeit versucht, technische Informationen, die wir als besonders interessant oder wichtig erachten, mit dem

Techniker-Symbol zu kennzeichnen. Sicher werden Sie diese Informationen nicht immer brauchen – aber wenn es technische Fragen gibt, sind Sie hier richtig.



Wenn Sie beim Ausprobieren vorsichtig sein müssen, damit Sie keine wichtigen Dateien löschen oder Ihre Umgebung ansonsten irgendwie beschädigen, haben wir die entsprechenden Informationen mit dem Warndreieck versehen. Gerade, wenn Sie mit einem Server arbeiten, sollten Sie sich an diese Ratschläge unbedingt halten. Glauben Sie uns, dass Sie sich dadurch viele Stunden oder gar Tage der Fehlersuche und Frustration sparen können.



Mit der Glühbirne kennzeichnen wir einen besonderen Tipp, der Ihnen Vorteile bringt, wenn Sie ihn befolgen.

Wie es weitergeht

Dieses Buch vermittelt die Grundlagen zu Windows-Servern und den essenziellen Diensten, die eine lokale Domäne braucht. Welche Literatur für Sie im Anschluss wichtig ist, hängt davon ab, was Sie bewerkstelligen möchten. Dem Zeitgeist entsprechend würden wir Ihnen *Microsoft Azure für Dummies* ans Herz legen, da zukünftige IT-Entwicklungen auf Cloud-Techniken aufsetzen.

Geht es für Sie beruflich mit Windows-Servern weiter, so ist möglicherweise der Erwerb eines entsprechenden Zertifikats von Microsoft für Administratoren eine interessante Option. Das Zertifikatsprogramm von Microsoft ist aktuell in einem starken Wandel, sodass wir an dieser Stelle keine direkte Empfehlung für einzelne Kurse geben möchten. Es ist aber auf jedem Fall ein sinnvoller Schritt, sich das erworbene Wissen zertifizieren zu lassen.

Aber nun wünschen wir Ihnen erst mal viel Spaß und Eifer mit unserem Buch!

Teil I

Windows-Server-Grundlagen



IN DIESEM TEIL ...

- ✓ Das kleine 1x1 der Server
- ✓ Windows-Server-Editionen
- ✓ Unterschiede: Cloud oder lokal?
- ✓ Wie man mit dem Server arbeiten kann: GUI, Konsole und PowerShell

Kapitel 1

Windows-Server-Grundlagen

IN DIESEM KAPITEL

Das kleine 1x1 der Server

Hardware für Windows Server

Hardware Compatibility List – HCL)

Darf es ein bisschen mehr sein? Sizing des Servers

Ganz gleich, in welchem Umfeld Sie arbeiten oder wie oft Sie privat Computer einsetzen: Microsofts Betriebssystem *Windows* ist Ihnen sicher bekannt, und wahrscheinlich haben Sie auch schon damit gearbeitet.

Ebenso werden Sie, gerade im beruflichen Umfeld, schon auf die eine oder andere Art mit einem Server – häufig eben auch mit einem Windows-Server – in Berührung gekommen sein, auf dem Sie dann über das Netzwerk Ihre Dokumente und Arbeiten ablegen. Hatten Sie dabei bereits die Gelegenheit, einen Blick auf die Oberfläche des aktuellen Windows Server 2019 zu werfen, so werden Sie zunächst einmal feststellen, dass diese sich scheinbar kaum von der Oberfläche der aktuellen Version Windows 10 auf Ihrem Desktop unterscheidet. Die [Abbildung 1.1](#) zeigt das auch sehr deutlich. In diesem Kapitel erfahren Sie, wo die wesentlichen Unterschiede zwischen diesen zwei Ausprägungen des Betriebssystems liegen, was Windows Server ausmacht und auch, wie ein solcher Server in der Regel ausgerüstet sein sollte.

Das kleine 1x1 der Server

Der Begriff eines Servers wird in der IT zumeist durch zwei Definitionen charakterisiert beziehungsweise auch so verwendet: Wer den Blick mehr

auf die Hardware richtet, wird einen Server in der Regel als eine physische Maschine beschreiben, die in einem Netzwerk eingebunden ist. Auf dieser Maschine sind dann neben dem Betriebssystem eine oder mehrere Software-basierende Server-Lösungen wie beispielsweise Mail- oder Anwendungs-Server aktiv. Solche Hardware-Server werden dann häufig auch als Hostsysteme bezeichnet.

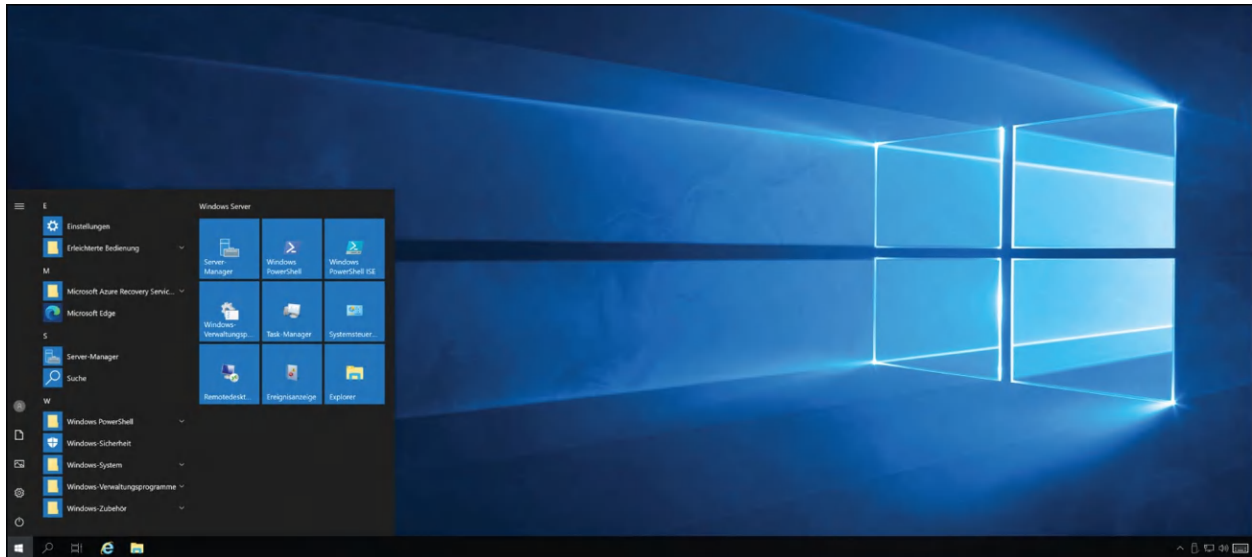


Abbildung 1.1: Die Oberfläche von Windows Server 2019: Sie ist auf den ersten Blick nur schwer von der von Windows 10 zu unterscheiden.

Bei den Software-basierten Servern handelt es sich um Programme, die anderen Rechnern – den sogenannten Clients – bestimmte Dienste über das Netzwerk zur Verfügung stellen. Die Verbindung funktioniert dabei nach dem Client-Server-Prinzip. Server-Programme müssen aber nicht zwangsläufig auf einer Server-Hardware oder einem speziellen Server-Betriebssystem installiert sein und betrieben werden. Grundsätzlich kann jeder Rechner als Server agieren, wobei dabei natürlich nicht die gleiche Leistungsfähigkeit bereitsteht, die ein Server-Betriebssystem oder eine entsprechende Server-Hardware bieten kann.

So lassen sich auch ganz verschiedene Software-basierte Server-Typen auf einer physischen Maschine unter einem Betriebssystem betreiben. Im professionellen Einsatz ist es jedoch häufig so, dass jeder Server auf einem eigenständigen Rechner untergebracht oder sogar auf mehrere Rechner verteilt wird. Die IT-Fachleute sprechen dann von einem

dedizierten Server. Auf diese Weise lässt es sich dann vermeiden, dass sich Hardware- und Software-Auslastung eines Diensts auf die Performance anderer Dienste auswirkt, was gerade dann der Fall sein kann, wenn viele Client-Systeme den entsprechenden Dienst einsetzen. Wenn wir hier in diesem Buch von Windows-Server reden, dann meinen wir damit Microsofts Server-Betriebssystem.



Grundsätzlich geht es beim Client-Server-Modell (auch Client-Server-Konzept, -Architektur, -System oder -Prinzip genannt) darum, Aufgaben und Dienstleistungen innerhalb eines Netzwerks zu verteilen. Dabei werden die entsprechenden Aufgaben von Programmen bearbeitet, die in Clients und Server unterteilt werden. Das Client-System kann einen oder auch mehrere Dienste vom Server anfordern (zum Beispiel die aktuell benötigten Betriebsmittel). Bei den Clients kann es sich beispielsweise um Arbeitsrechner unter Windows oder Linux, um sogenannte Thin Clients oder mobile Endsysteme handeln. Der dafür zuständige Server kann sich auf demselben oder einem anderen Rechner im Netzwerk befinden. Er antwortet auf die Anforderung und stellt das Programm, eine Funktion oder die Betriebsmittel zur Verfügung. In der Regel ist ein solcher Server dazu in der Lage, gleichzeitig mehrere Clients zu bedienen.

Hardware-Anforderungen

Obwohl es – wie zuvor bereits ausgeführt – im Prinzip möglich ist, einen »normalen« PC, auf dem beispielsweise ein Windows 10 installiert ist, als Server-System zu betreiben, das beispielsweise anderen Rechnern im Netzwerk Dateidienste zur Verfügung stellt, ist dieses Vorgehen in der Praxis weder ratsam noch effizient. Aufgrund der höheren Anforderungen, die an einen Server und das Server-Betriebssystem gestellt werden, ergeben sich auch entsprechende Anforderungen an die Server-Hardware: Der Standard-PC vom Elektronik-Discounter ist in der Regel nicht dafür geeignet.

Microsoft stellt sowohl für die Desktop- als auch für die Server-Betriebssysteme Listen mit den Anforderungen bereit, die eine Hardware für den Einsatz mit dem jeweiligen System erfüllen muss. Wer also beispielsweise Windows Server in der Version 2019 aufsetzen will, kann in der offiziellen Onlinedokumentation von Microsoft unter der Adresse <https://docs.microsoft.com/de-de/windows-server/get-started-19/sys-reqs-19> die entsprechenden Daten finden. Aus gutem Grund weisen die Microsoft-Experten an dieser Stelle aber darauf hin, dass es schwierig ist, allgemeingültige Angaben für die Systemanforderungen eines Server-Betriebssystems zu geben.

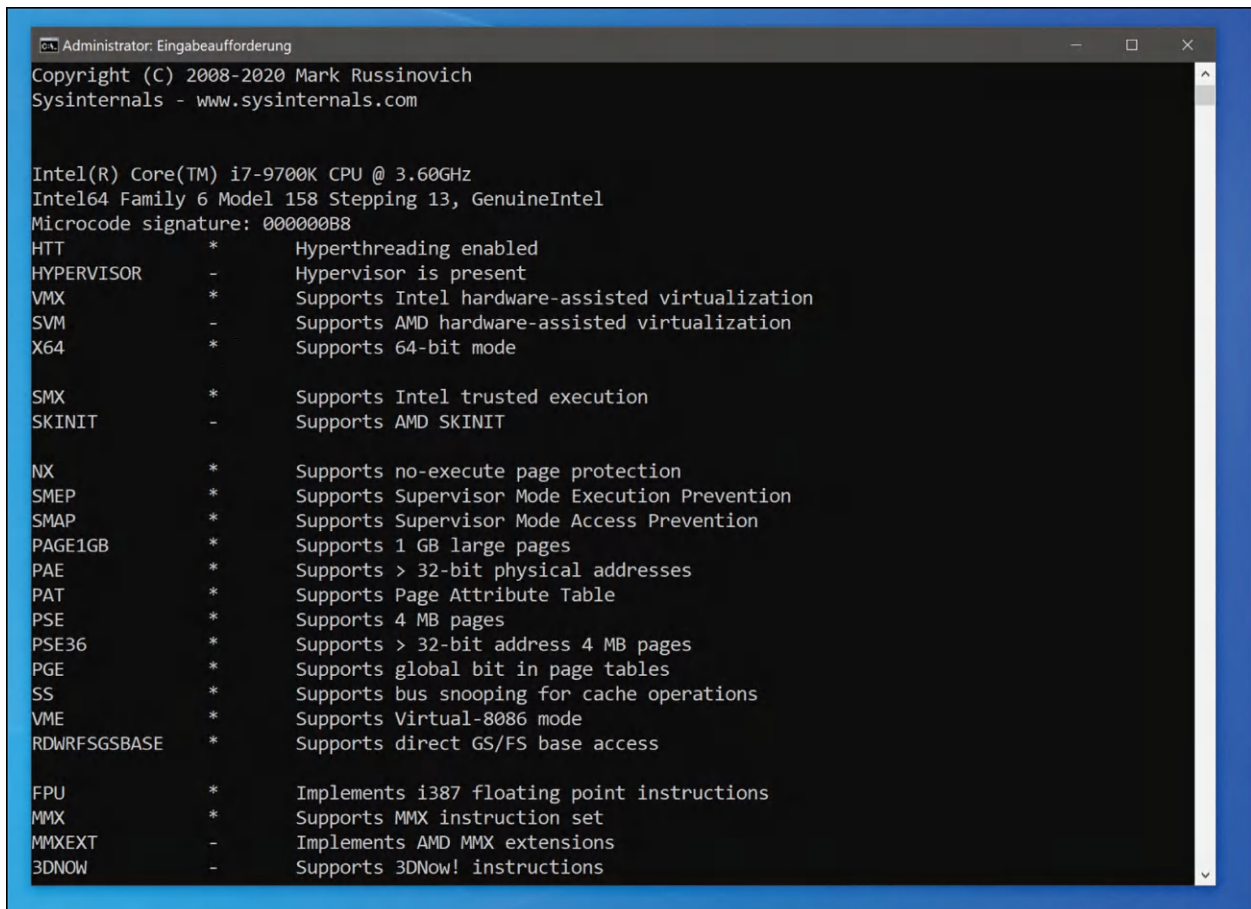


Dass es viele Möglichkeiten gibt, ein Server-Betriebssystem bereitzustellen, ist es grundsätzlich unrealistisch, allgemein gültige Systemanforderungen anzugeben. Wer einen Servereinsatz plant, sollte für jede Server-Rolle, die er in seinem Netz bereitstellen möchte, die Dokumentation zurate ziehen. Dort findet er dann auch Informationen über die Ressourcenanforderungen, die für bestimmte Server-Rollen wichtig sind. Letztendlich sollte jeder, der einen Server professionell einsetzen will, Testbereitstellungen durchführen, um die entsprechenden Systemanforderungen für benötigte Bereitstellungsszenarien zu ermitteln.

Trotzdem kann es sinnvoll sein, einen kurzen Blick auf die Voraussetzungen zu werfen, die Microsoft als minimal für den Einsatz des Server-Betriebssystems nennt. Als CPU muss bei den aktuellen Versionen des Windows-Servers unbedingt ein 64-Bit-Prozessor zum Einsatz kommen. Von der bei früheren Versionen bis hin zu Windows Server 2008 noch erhältlichen Unterstützung für 32-Bit-Hardware hat Microsoft endgültig Abschied genommen. Als Taktfrequenz für den eingesetzten Prozessor nennt der Hersteller einen Minimalwert von 1,4 GHz. Weiterhin wichtig: Neben der allgemeinen Kompatibilität zum x64-Anweisungsset muss die eingesetzte CPU unter anderem auch bestimmte Sicherheitstechniken wie NX (No execute) oder DEP (Data Execution Prevention) direkt in Hardware unterstützen.

Sind Sie sich nicht sicher, ob eine von Ihnen als Server geplante Hardware

die entsprechenden Voraussetzungen erfüllt, so können Sie entweder in den Datenblättern des Herstellers suchen oder die Freeware CoreInfo verwenden, die von Microsoft unter der Adresse <https://docs.microsoft.com/de-de/sysinternals/downloads/coreinfo> zum Herunterladen angeboten wird. Dieses in der [Abbildung 1.2](#) zu sehende Kommandozeilenprogramm zeigt Ihnen alle Informationen zu der im jeweiligen System verbauten CPU an. Diese Anzeige umfasst zumeist deutlich mehr als zwei Bildschirmseiten an Informationen, aber das Programm bietet Ihnen die Möglichkeit, sich mittels Parameter an der Kommandozeile nur ausgesuchte Details anzeigen zu lassen.

The image shows a screenshot of a Windows command prompt window titled "Administrator: Eingabeaufforderung". The window displays the output of the Sysinternals CoreInfo tool. At the top, it shows the copyright information: "Copyright (C) 2008-2020 Mark Russinovich" and "Sysinternals - www.sysinternals.com". Below this, it lists the CPU information: "Intel(R) Core(TM) i7-9700K CPU @ 3.60GHz", "Intel64 Family 6 Model 158 Stepping 13, GenuineIntel", and "Microcode signature: 000000B8". The main part of the output is a list of CPU features and their status, organized into columns. Features marked with an asterisk (*) indicate that the feature is supported, while those marked with a hyphen (-) are not. The features listed include HTT (Hyperthreading enabled), HYPERVISOR (Hypervisor is present), VMX (Supports Intel hardware-assisted virtualization), SVM (Supports AMD hardware-assisted virtualization), X64 (Supports 64-bit mode), SMX (Supports Intel trusted execution), SKINIT (Supports AMD SKINIT), NX (Supports no-execute page protection), SMEP (Supports Supervisor Mode Execution Prevention), SMAP (Supports Supervisor Mode Access Prevention), PAGE1GB (Supports 1 GB large pages), PAE (Supports > 32-bit physical addresses), PAT (Supports Page Attribute Table), PSE (Supports 4 MB pages), PSE36 (Supports > 32-bit address 4 MB pages), PGE (Supports global bit in page tables), SS (Supports bus snooping for cache operations), VME (Supports Virtual-8086 mode), RDWRFSGSBASE (Supports direct GS/FS base access), FPU (Implements i387 floating point instructions), MMX (Supports MMX instruction set), MMXEXT (Implements AMD MMX extensions), and 3DNOW (Supports 3DNow! instructions).

```
Administrator: Eingabeaufforderung
Copyright (C) 2008-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

Intel(R) Core(TM) i7-9700K CPU @ 3.60GHz
Intel64 Family 6 Model 158 Stepping 13, GenuineIntel
Microcode signature: 000000B8
HTT          *      Hyperthreading enabled
HYPERVISOR   -      Hypervisor is present
VMX          *      Supports Intel hardware-assisted virtualization
SVM          -      Supports AMD hardware-assisted virtualization
X64          *      Supports 64-bit mode

SMX          *      Supports Intel trusted execution
SKINIT       -      Supports AMD SKINIT

NX           *      Supports no-execute page protection
SMEP         *      Supports Supervisor Mode Execution Prevention
SMAP         *      Supports Supervisor Mode Access Prevention
PAGE1GB      *      Supports 1 GB large pages
PAE          *      Supports > 32-bit physical addresses
PAT          *      Supports Page Attribute Table
PSE          *      Supports 4 MB pages
PSE36        *      Supports > 32-bit address 4 MB pages
PGE          *      Supports global bit in page tables
SS           *      Supports bus snooping for cache operations
VME          *      Supports Virtual-8086 mode
RDWRFSGSBASE *      Supports direct GS/FS base access

FPU          *      Implements i387 floating point instructions
MMX          *      Supports MMX instruction set
MMXEXT       -      Implements AMD MMX extensions
3DNOW        -      Supports 3DNow! instructions
```

Abbildung 1.2: Erfüllt der Prozessor alle Voraussetzungen für den Einsatz mit Windows Server? Das Freeware-Programm CoreInfo gibt Auskunft.

Zu den weiteren wichtigen Faktoren für den Server-Einsatz gehören Art und Umfang des Hauptspeichers (RAM). Wenn Sie den Windows-Server

in seiner »minimalistischsten« Ausprägung – also in der sogenannten Core-Version ohne Windows-Desktop – installieren wollen, so können Sie diesen durchaus mit 512 MByte RAM betreiben. Wollen Sie allerdings eine Windows-Oberfläche auf Ihrem Server einsetzen, so müssen es dann mindestens 2 GByte RAM sein, die sich in Ihrem System wiederfinden. Für einen Server-Rechner sollten dabei grundsätzlich RAM-Module mit ECC-Technik (Fehlerkorrektur-Technik) zum Einsatz kommen, bei denen Fehler bei der Speicherung und Übertragung von Daten erkannt und durch Redundanzen korrigiert werden können.

Wenn Sie jemals auch nur einen Windows-10-Rechner selbst aufgesetzt haben, werden Sie wahrscheinlich schon wissen, dass Sie mit den hier genannten Minimalwerten für den Hauptspeicher Ihres Servers kaum glücklich werden können. Können Sie einen Windows-Server im Testbetrieb noch durchaus mit 16 oder vielleicht sogar 8 GByte RAM betreiben, so sollten Sie im produktiven Einsatz doch mindestens 32 oder besser 64 GByte RAM in einem solchen Gerät einsetzen. Gerade wenn Sie daran denken, den Server auch als Host für spätere Virtualisierungsprojekte zu nutzen, sollten Sie keinesfalls mit Hauptspeicher geizen.

Gleiches gilt für den Speicherplatz, den Ihr Server auf der Festplatte benötigt. Microsoft gibt hier als absolutes Minimum eine Größe von 32 GByte für die Systempartition an – was dann gerade für einen Windows-Server in der Core-Version (also ohne grafische Benutzeroberfläche) und der Rolle als Webserver ausreicht. Bereits wenn Sie erwägen, Ihren Server über das Netzwerk zu installieren, benötigen Sie mehr Speicherplatz für die Systempartition. Beim Einsatz von mehr als 16 GByte Hauptspeicher wird ebenfalls mehr Speicherplatz für Auslagerungen, Ruhezustand und Sicherungsdateien in der Systempartition benötigt. Weiterhin sollten Sie beachten, dass Sie für den Einsatz unter Windows Server 2019 in Ihrem System einen Speicheradapter benötigen, der mit der PCI-Express-Architekturspezifikation konform ist. Speichergeräte, die nur das PATA-Protokoll (Parallel Advanced Technology Attachment) unterstützen, können Sie unter Windows Server 2019 nicht einsetzen – das gilt generell für alle Start-, Auslagerungs- oder Datenlaufwerke des Systems und natürlich auch für weitere (ältere) Protokolle zur Datenübermittlung wie

ATA/IDE und EIDE.

Neben der Selbstverständlichkeit mindestens eines Ethernet-Adapters, der im Gigabit-Bereich arbeitet und sinnvollerweise auch PXE (Pre-boot Execution Environment) unterstützt, brauchen Sie ein DVD-Laufwerk, falls Sie Ihr Server-System von einem solchen Medium installieren wollen. Grafikkarte und Monitor sollten in der Lage sein, eine Mindestauflösung von 1024 x 768 (Super-VGA) zu unterstützen.



Für die Installation von Windows Server 2019 auf Ihrer Hardware ist es nicht unbedingt notwendig, dass sich auf dem Motherboard des Rechners ein sogenannter TPM-Chip (Trusted Platform Module) befindet. Wollen Sie bei dem Server aber Features wie die Bitlocker-Verschlüsselung auch für das Betriebssystem nutzen, wird dieser Chip benötigt. Wenn das der Fall ist, muss bei solchen Hardware-basierten TPMs die Version 2.0 der TPM-Spezifikation implementiert sein. Dieses muss zudem über ein EK-Zertifikat (Endorsement Key) verfügen, das entweder vorab vom Hardware-Hersteller für das TPM bereitgestellt wird oder beim ersten Start vom Gerät abgerufen werden kann. Weitere Informationen dazu finden Sie in der Microsoft-Dokumentation zum TPM-Schlüsselnachweis: <https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/manage/component-updates/tpm-key-attestation>.

Hardware Compatibility List – HCL

Wenn Sie unsere Auflistung der grundsätzlich benötigten Hardware aufmerksam durchgelesen haben, fragen Sie sich nun vielleicht, wie Sie die richtige Hardware für Ihr Windows-Server-Betriebssystem finden und dann sicher sein können, dass die gewählten Komponenten auch reibungslos mit dem Betriebssystem zusammenarbeiten können. Microsoft hat zu diesem Zweck das sogenannte »Windows Hardware Compatibility Program« ins Leben gerufen, das dabei helfen soll, Systeme zu entwickeln beziehungsweise die Systeme und Komponenten zu finden, die problemlos und sicher mit der gewünschten Betriebssystemversion

zusammenarbeiten. Der im Web bereitstehende »Windows Server Catalog«, der in [Abbildung 1.3](#) zu sehen ist, hilft ebenfalls bei diesen Fragen.

IT-Profis werfen daher zunächst einen Blick auf die HCL (Hardware Compatibility List), bevor sie sich für ein bestimmtes System entscheiden. Neben der mehr auf die Bedürfnisse der Hardware-Entwickler ausgerichteten Dokumentation zum Hardware-Kompatibilitätsprogramm unter <https://docs.microsoft.com/de-de/windows-hardware/design/compatibility/> bietet sich für den Entscheidungsprozess vor allen Dingen der sogenannte »Windows Server Catalog« unter <https://www.windowsservercatalog.com/> an, um die richtige Hard- und Software für Ihren Windows-Server zu finden. Dort werden zudem die Badges vorgestellt, die Hardware-Hersteller wie Dell und Hewlett-Packard beispielsweise auf ihren Server-Systemen anbringen, um zu verdeutlichen, dass diese Rechner den Vorgaben der HCL entsprechen.



Abbildung 1.3: Bietet Übersicht über Server-Hard- und Software und zeigt die Badges: der Windows Server Catalog

Darf es ein bisschen mehr sein? Sizing des Servers

Nachdem Sie nun wissen, welche minimale Ausrüstung Sie benötigen, um einen Windows-Server zu betreiben, und vielleicht auch schon mal einen Blick auf das Angebot der verschiedenen Hardware-Anbieter geworfen haben, steht nun noch die Frage im Raum, wie viel Server es denn sein darf.

Eine recht einfache Antwort darauf finden Sie, wenn Sie ganz ähnlich der Aussage vorgehen, die Sie von einem geschäftstüchtigen Verkäufer beispielsweise zur Unterstützung der Entscheidung beim Kauf eines neuen Autos bekommen: »Nehmen Sie einfach ein bisschen mehr, wer weiß, wann Sie es dann vielleicht brauchen ...«.

Nun geht es beim Server-Sizing – also bei der Entscheidung, wie »groß und mächtig« die Hardware für Ihren Windows-Server ausfallen soll – nicht nur um das vorhandene Budget, sondern auch um die Anforderungen, die Sie beziehungsweise Ihr Unternehmen und die Nutzer an den Server stellen. Dabei gibt es eine ganze Reihe von Aspekten, zu denen unter anderem Dinge wie Ausfallsicherheit, Verfügbarkeit der Hardware und Erweiterbarkeit zählen. Aber die Leistungsfähigkeit – gern auch als Performance bezeichnet – ist und bleibt ein zentrales Entscheidungskriterium bei der Serverwahl. So geht es dann eben beim Server-Sizing in den meisten Fällen darum, den Server mit der besten Performance für den Einsatz der gewünschten Anwendungen im eigenen Unternehmen zu finden.

Soll ein Windows-Server beispielsweise als reiner Datenbank-Server zum Einsatz kommen, so ist es in der Regel relativ einfach, die Entscheidungen zu fällen: Hier machen die Anbieter solcher Lösungen – ebenso wie die Anbieter anderer professioneller Anwendungen wie CRM- oder ERP-Systeme – ziemlich genaue Angaben darüber, wie viel zusätzlichen Hauptspeicher der Server beispielsweise benötigen wird, wenn die Anwendung noch einmal 50 Nutzer mehr bedienen soll. Bei einer allgemeineren Betrachtung sollten Sie sich in Bezug auf die Ausrüstung und das Sizing Ihres Windows-Servers unter anderem die folgenden Fragen stellen:

- ✓ Wie schnell werden Anfragen beantwortet und Operationen durchgeführt?
- ✓ Wie viele dieser Anfragen und Operationen kann Ihr Server gleichzeitig bearbeiten?
- ✓ Wie viel Zeit benötigt der Server, um gespeicherte Informationen zu lesen oder zu schreiben?

Sie werden schnell feststellen, dass Sie beispielsweise mit einem Blick auf Typ und Leistungsfähigkeit der CPU (Zahl der Prozessorkerne/Taktfrequenz), Cache-Ausstattung, Größe des verfügbaren Hauptspeichers und auch der Art der verwendeten Massenspeicher (zum Beispiel traditionelle Festplatten oder SSDs) und einigen Tests schnell

dazu in der Lage sein werden, diese Fragen für Ihren Server und Ihre Einsatzzwecke zu beantworten.

Kapitel 2

Wer zählt die Versionen und Editionen?

IN DIESEM KAPITEL

Server-Geschichte: Windows NT Server bis 2019

Windows Server 2019: Neuerungen und Vorteile

Editionen, Versionen und Service-Kanäle

Andere Welten (1): Windows-Subsystem für Linux

Andere Welten (2): Container, Docker, Kubernetes

Windows Server 2022 – die kommende Generation

Im ersten Kapitel haben wir uns allgemein mit der Definition und den Fähigkeiten eines Server-Betriebssystems befasst. Nun wollen wir uns mehr Windows Server und seinen verschiedenen Ausprägungen, Versionen und Editionen zuwenden.

Server-Geschichte: Windows NT Server bis 2019

Dazu werfen wir zunächst einen kurzen Blick auf die Entwicklung des Server-Betriebssystems aus Redmond: Microsoft hat Anfang der 1980er-Jahre begonnen, neben dem damals weitverbreiteten *MS-DOS* mit *Windows NT* (für »New Technology«) eine weitere Betriebssystemlinie zu entwickeln und zu etablieren, die besonders den Ansprüchen großer Unternehmen und professioneller Anwender gerecht werden sollte. Dabei ging es vor allen Dingen um die Bereiche Geschwindigkeit, Sicherheit

und Zuverlässigkeit. Solche Features konnten bis zu diesem Zeitpunkt nur von den RISC-basierten (Reduced Instruction Set Computer) Rechnern geliefert werden, die unter den verschiedensten Unix-Derivaten arbeiteten. Mit einem Server-System, das auf die x86-Architektur der Intel-Prozessoren aufsetzte und dort Merkmale wie symmetrisches Multiprocessing zur Verfügung stellte, konnte Microsoft eine weitaus preisgünstigere Server-Architektur anbieten.



RISC: Reduced Instruction Set Computer (Computer mit reduziertem Befehlssatz). Hier geht es darum, wie der Befehlssatz eines Prozessors aufgebaut wird, also um die Architektur der CPU. Bei den RISC-CPUs wurde auf komplexe Befehle verzichtet, sodass die Ausführung der Assembler-Programme in einem Prozessortakt ablaufen konnte. Diese Prozessoren haben heute allerdings kaum noch Bedeutung, da beispielsweise auch die CISC-Prozessoren (Complex Instruction Set Computer) von Intel seit Anfang der 90er-Jahre solche Techniken bieten.

Multiprocessing: Beim Multiprocessing können Programme von mehreren Prozessoren verarbeitet werden. Dieser Begriff bezeichnet häufig auch die gleichzeitige Bearbeitung eines Programms durch mehrere Computer.

Microsoft pflegt leider eine lange Tradition, wenn es darum geht, Software und ganz besonders Betriebssysteme mit Bezeichnungen und Nummerierungen zu versehen, die sich im Lauf der Zeit immer mal wieder ändern. Darum folgt hier auch nur ein sehr komprimierter Überblick über die einzelnen Versionen und ihr Erscheinungsdatum:

Windows NT 3.1 bis 4.0: Diese ersten Versionen von Microsofts Server-Betriebssystem kamen von 1993 bis 1996 auf den Markt. Während die Versionen 3.1, 3.5 und 3.51 zum NT-Release 3 gehörten ([Abbildung 2.1](#) zeigt Windows NT Server Version 3.1), trug einzig der *NT Server 4.0* die Release-Nummer 4. Von diesem Betriebssystem bot Microsoft erstmals auch eine sogenannte Enterprise-Version für größere Unternehmen und eine Multiuser-fähige Version unter der Bezeichnung *Windows NT 4.0 Terminal Server* an.

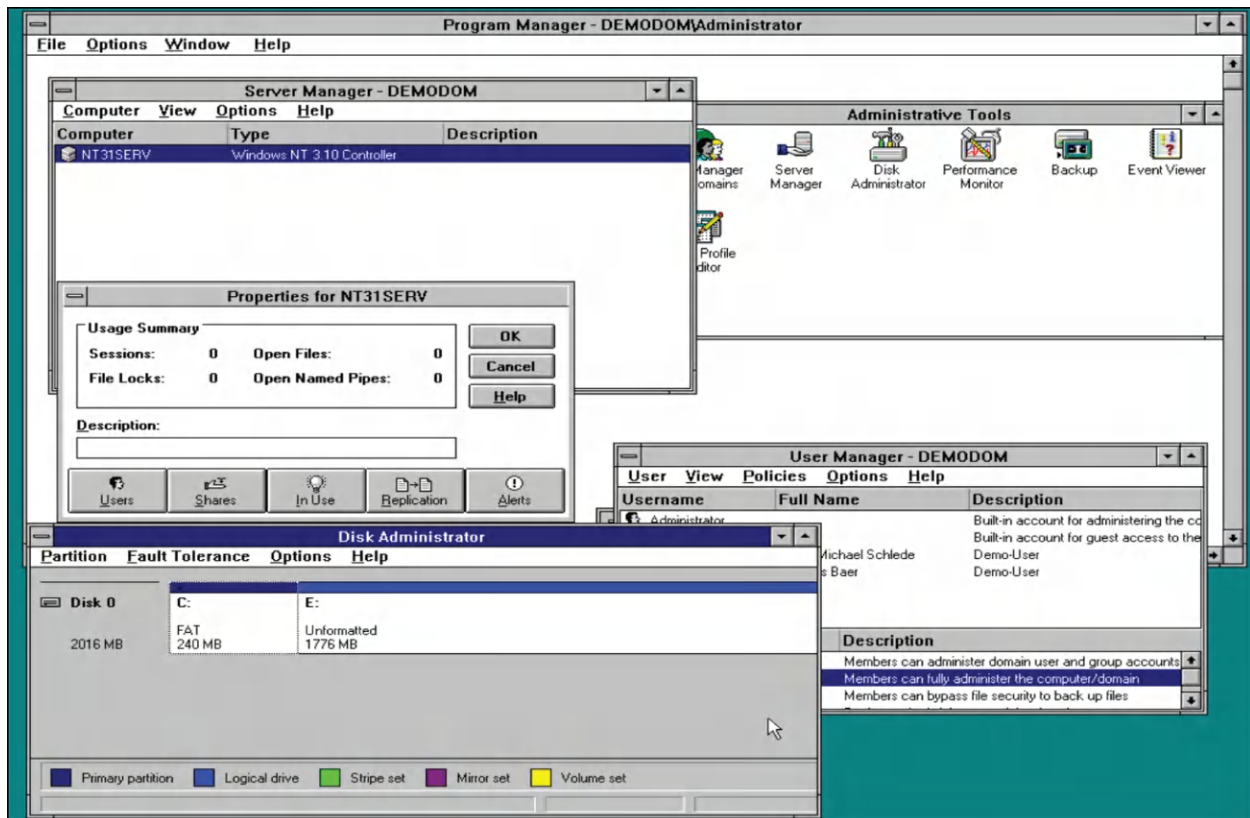


Abbildung 2.1: Windows Server in einer seiner ersten Ausprägungen hatte viel Ähnlichkeit mit dem damaligen Windows auf dem Desktop.

Windows 2000 bis Windows Server 2003 R2: Diese Versionen, die in den Jahren 2000 bis 2005 auf den Markt kamen, gehören zu den NT-Betriebssystemen, die intern eine Release-Nummer 5 tragen. Mit dem *Windows Server 2003* (NT 5.2) gab es dann erstmals auch eine spezielle Version für den Einsatz als Speicherplattform. Diese Variante – der *Windows Storage Server* – wurde als Bundle-Produkt von Hardware-Anbietern vertrieben. Ab *Windows Server 2003* stand das Betriebssystem auch in der 64-Bit-Variante zur Verfügung. Auch eine Version unter der Bezeichnung *Windows Home Server* kam mit dem Release *Windows Server 2003 R2* auf den Markt.

Windows Server 2008 bis Windows Server 2012 R2: Diese Versionen erschienen von 2008 bis 2013 und gehören zu der Reihe der NT 6-Releases. Die Version *Windows Server 2008 R2* war die erste, die nur noch in der 64-Bit-Ausprägung zur Verfügung stand.

Windows Server 2016 bis Windows Server 2019: Die Server der aktuellen

NT 10-Line wurden von Microsoft von 2016 bis 2018 veröffentlicht. Sie bieten den Nutzern in der GUI-Version die gleiche Oberfläche wie Windows 10 an.

Windows Server 2019: Neuerungen und Vorteile

Der Windows Server 2019 kam im Oktober 2018 heraus. Grundsätzlich handelt es bei dieser aktuellen Version der NT-10-Linie (basierend auf Windows 1809) um eine Weiterentwicklung auf Basis der Version Windows Server 2016. Sie wurde von Microsoft mit einer ganzen Reihe von Neuerungen und der Unterstützung moderner Technik beispielsweise im Bereich des Einsatzes von Container-Techniken ausgestattet. Zu den Neuerungen zählen unter anderem:

- ✓ Integrierte Unterstützung der Kubernetes-Technologie
- ✓ Windows Subsystem für Linux
- ✓ Erweiterung bei der Sicherheit mittels Windows Defender Advanced Threat Protection (ATP)
- ✓ Sicherheitsfeatures für abgeschirmte virtuelle Maschinen
- ✓ System Insights: Ein Predictive-Analytics-Werkzeug, das es erlaubt, lokale Daten eines Windows-Servers wie beispielsweise Ereignisse und Leistungsindikatoren zu analysieren. Die Software wird durch ein Machine-Learning-Modell unterstützt. So kann sie Ihnen bessere Einblicke in die Funktionsweise Ihres Servers präsentieren.
- ✓ Umfangreiche Erweiterungen und Ergänzung im Storage-Bereich

Vielleicht vergleichen Sie ja gerade einen frisch installierten Windows-2019-Server mit den hier beschriebenen Informationen und stellen fest, dass es da doch noch viel mehr gibt. Wie schon zuvor kurz angesprochen, sind die Entwickler äußerst schnell damit, Änderungen und neue Features »hinterherzuschieben«. So kam es durchaus sein, dass die Version, die Sie installiert haben, im Bereich EINSTELLUNGEN | SYSTEM | INFO als

Version nicht wie in [Abbildung 2.2](#) gezeigt 1809, sondern 1903, 1909, 2004 oder 20H2 anzeigt. Im nächsten Abschnitt klären wir, was es mit diesen unterschiedlichen Bezeichnungen und Versionen auf sich hat.

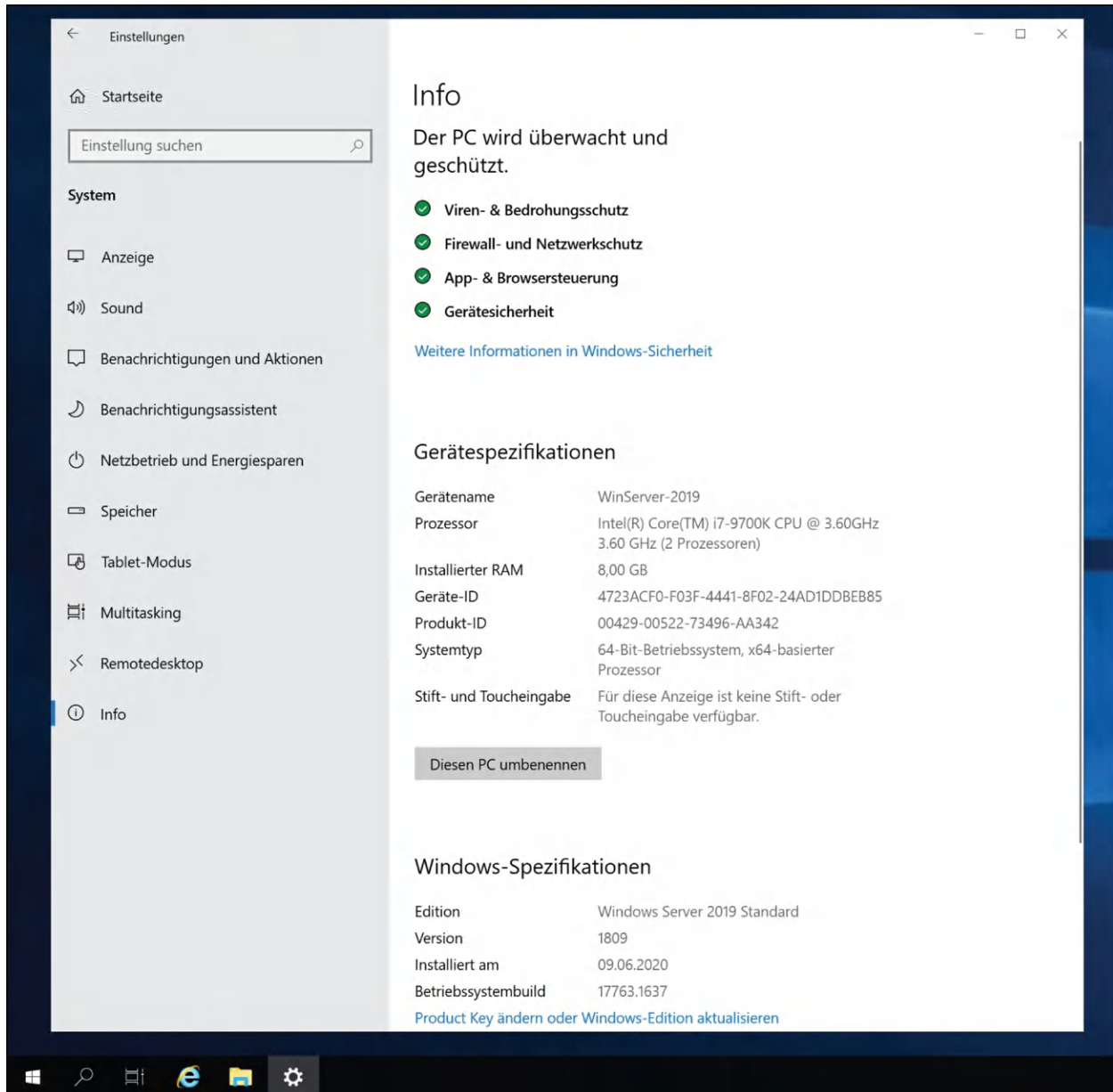


Abbildung 2.2: Dieser Windows Server 2019 zeigt sowohl durch die Oberfläche als auch bei den Systeminfos, dass er auf der Windows-Version 1809 basiert.

Editionen, Versionen und Service-Kanäle

Microsoft stellt das Server-Betriebssystem grundsätzlich in zwei sogenannten primären Release-Kanälen bereit: der Long-Term Servicing Channel (LTSC) und der halbjährliche Kanal.



Long-Term Servicing Channel (LTSC): In diesem Kanal wird alle zwei bis drei Jahre eine Windows-(Haupt-)Version zur Verfügung gestellt. Systeme in diesem Kanal erhalten sowohl sicherheitsrelevante als auch nicht sicherheitsrelevante Updates, jedoch keine neuen Funktionen oder Features.

Halbjährlicher Kanal (Semi-Annual Channel – SAC): Microsoft stellte bis zur Version 2019 für die Server-Produkte in diesem Kanal zweimal jährlich neue Versionen (im Frühjahr und Herbst) zur Verfügung, wobei existierende Systeme weiterhin Support erhalten sollen. Mit dem kommenden Server 2022 wird es diesen Kanal nicht mehr geben. Neue und künftige Server-Versionen stehen dann nur noch als LTSC-Release bereit.

Weitere Infos dazu finden Sie in der Microsoft-Dokumentation:
<https://docs.microsoft.com/de-de/windows-server/get-started/windows-server-release-info>

Für professionelle Anwender in den Unternehmen, die Wert auf Stabilität und Zuverlässigkeit für ihre Anwendungen legen, ist es sinnvoll, Windows Server in LTSC-Ausprägung zu betreiben. Ein weiterer Vorteil: Sie erhalten diese Systeme mit fünf Jahren grundlegenden und fünf Jahren erweiterten Support. Beim halbjährlichen Kanal stehen standardmäßig hingegen nur 18 Monate Support zur Verfügung.

Wenn Sie sich für einen Windows-Server entschieden haben, müssen Sie sich als Nächstes für eine der sogenannten Editionen der Software entscheiden. Grundsätzlich stehen drei Editionen für den Server bereit:

- ✓ *Windows Server Essentials:* Ein Release für kleine Unternehmen mit nur grundlegenden Anforderungen an einen Server und nicht mehr als 25 Benutzern. Besitzt eingeschränkte Funktionalität gegenüber der Standardversion, unterstützt keine Container-Technik und wird ohne Exchange-Lizenz geliefert.

- ✓ *Windows Server Standard*: Standardvariante, die alle Server-Rollen beinhaltet, aber Einschränkungen im Storage-Bereich und bei der Hochverfügbarkeit aufweist ([Abbildung 2.2](#)). Kann mit bis zu zwei Virtualisierungsinstanzen betrieben werden und unterstützt Container-Technik.
- ✓ *Windows Server Datacenter*: Besonders für den Einsatz in den Rechenzentren großer Unternehmen oder Provider konzipiert. Alle Funktionalitäten und unbegrenzte Lizenzen für virtuelle Maschinen und Container.

Wer über Server-Systeme und Lizenzen spricht, muss zudem auch über die sogenannten CALs (Client-Zugriffslizenzen) reden. Diese Client-Zugriffslizenzen werden pro Benutzer oder Gerät mit Zugriff auf einen Server benötigt. Nur die Essential-Edition erlaubt den Betrieb von bis zu 25 Clients ohne CALs.

Andere Welten (1): Windows-Subsystem für Linux

Microsoft und seine Betriebssysteme wurden sehr lange Zeit als die erklärten Feinde der Open-Source-Szene und ihrer Linux-Betriebssysteme betrachtet. Doch in den letzten Jahren hat Microsoft den Anschluss an diese Communitys gesucht: Software-Projekte werden als Open Source entwickelt und über die Entwicklerplattform Git bereitgestellt.

Seit dem Anniversary Update (Build1607) für Windows 10 und der Version 1709 von Windows Server ist das Windows Subsystem for Linux (WSL) ein Teil dieser Bestrebungen. [Abbildung 2.3](#) zeigt das WSL auf einem Windows Server direkt nach der Installation. Microsoft hat dieses Feature immer weiter ausgebaut und ist auch aktuell bestrebt, die Möglichkeiten dieser Anbindung an die Unix-/Linux-Welt weiterzuentwickeln. Während für die Windows-10-Systeme allerdings mit der WSL2 bereits eine deutlich erweiterte Version des Linux-Subsystems zur Verfügung steht, die unter anderem *Docker-Images* für Linux verwalten kann und einen vollständigen Linux-Kernel bereitstellt, ist dies

für die Server-Systeme noch nicht der Fall. In Windows Server 2019 wird WSL2 aktuell nicht unterstützt, wer diese Subsystem-Version auf dem Server einsetzen will, kann das nur mit einer Vorabversion des kommenden Server-Releases 2022 tun.

```

System information as of Mon Jan 18 14:41:16 STD 2021

System load: 0.52      Processes:           7
Usage of /home: unknown  Users logged in:      0
Memory usage: 20%      IPv4 address for eth0: 192.168.0.115
Swap usage: 0%

0 updates can be installed immediately.
0 of these updates are security updates.

This message is shown once a day. To disable it please create the
/home/micha/.hushlogin file.
micha@WinServer-2019:~$ screenfetch

      ./+o+-
    yyyyy- -yyyyyy+
  ://+////////-yyyyyyo
.++ .:/++++++/-+.sss/`
.::+o: /+++++++/:-:-/-
o:+o+:+.`..``.-/oo+++++/
.:o:+o/.      `+sssoo+/
.++/+:+oo+o:`      /sssooo.
/+++//+:`oo+o      /:-::-:
\+/+o+++`o+o      ++//.
.++.o+++oo+:`      /dddhhh.
+.o+oo:.      `oddhhhh+
\+.++o+o`-`-`-`-:ohdhhhhh+
`o+++ `ohhhhhhhhhyo++os:
.o:`.syhhhhhhh/.oo++o`
/osyyyyyyo++ooo+++/
      +ooooo\+:
      `oo++.

micha@WinServer-2019:~$

micha@WinServer-2019
OS: Ubuntu 20.04 focal(on the Windows Subsystem for Linux)
Kernel: x86_64 Linux 4.4.0-17763-Microsoft
Uptime: 0m
Packages: 626
Shell: bash 5.0.17
Disk: 57G / 240G (24%)
CPU: Intel Core i7-9700K @ 4x 3.6GHz
RAM: 1765MiB / 8190MiB

```

Abbildung 2.3: Direkte Verbindung zur offenen Linux-Welt: Mithilfe des WSL werden Linux-Programme auch auf Windows Server ausgeführt.



Das Windows Subsystem für Linux (WSL) stellt Entwicklern eine GNU-/Linux-Umgebung bereit, die sie direkt unter Windows ausführen können. Dazu gehören dann die meisten Befehlszeilen-Tools (wie etwa vim, emacs, tmux) sowie verschiedene Hilfsprogramme und Anwendungen. Grundsätzlich kommt hierbei

eine Kompatibilitätsschicht zum Ausführen von Linux-Executables im ELF-Format in Windows zum Einsatz. Nutzer können sich dazu das Image der ihnen favorisierten Linux-Version aus dem Microsoft Store herunterladen. Da auf einem Windows-Server-System in der Regel kein Zugriff auf den Store bestehen wird, können diese Images auch direkt heruntergeladen werden.

Microsoft stellt unter <https://docs.microsoft.com/de-de/windows/wsl/install-on-server> eine genaue Beschreibung bereit, wie Anwender das WSL auf einem Windows-Server installieren und in den Betrieb nehmen können.

Andere Welten (2): Container, Docker, Kubernetes

Die Hinwendung von Microsoft zur Open-Source-Welt ist mit der Unterstützung von Linux aber noch nicht beendet. Wer sich in der letzten Zeit etwas in der Welt der IT umgehört hat, wird gerade, wenn es um die Server-Systeme geht, an Themen wie Container, Docker und Kubernetes nicht vorbeikommen. Da wir uns in diesem Buch auf den »Windows-Server an sich«, seine Konfigurationen und die grundlegenden Einsatzszenarien konzentrieren, können wir diese Themen nur streifen. Wer sich in den letzten Jahren mit der professionellen IT und ihren Methoden befasst hat, kommt am Thema Container zweifelsohne nicht vorbei. Sowohl für Entwickler als auch für Administratoren – beide Anwendergruppen, die vielfach schnell wechselnde Systemumgebungen benötigen – besitzt diese Technologie große Vorteile. Mithilfe der Container-Images können Anwendungen und ganze Anwendungsumgebungen schnell ausgerollt und eingesetzt werden. Grundsätzlich führte Microsoft die Container auf dem Windows-Server mit der Version 2016 ein. Windows Server 2019 unterstützt unterschiedliche Container-Arten:

- ✓ *Windows-Container:* Die »Windows Container On Windows (WCOW) stellen das traditionelle Container-Modell auf dem

Windows-Server da. Sie verwenden den gleichen Betriebssystemkern wie das darunterliegende Hostsystem. Mit dieser Technik ist die Nutzung vorhandener Windows-Technologien wie .NET, ASP.NET und PowerShell möglich.

- ✓ *Linux-Container:* »Linux Container On Windows (LCOW)« können ebenfalls auf einem Windows Server 2019 zum Einsatz kommen. Viele Lösungen, die in den unterschiedlichen Container-Repositories angeboten werden, setzen auf Linux-Container auf. Dazu muss auf dem Windows-Server eine Version von Docker-Enterprise eingesetzt werden. Mit dem Server 2019 werden nun auch Linux-Container mit Hyper-V-Isolation unterstützt. Jeder Container erhält so eine eigene schlanke Linux-VM, die mithilfe des Docker-Diensts auf dem Windows-Host verwaltet wird.
- ✓ *Hyper-V-Container:* Diese Art der Container ermöglichen es einem Administrator, eine Instanz eines Windows-Servers vollständig zu isolieren, um auf diese Weise zum Beispiel besonders sensitive Anwendungen zu schützen. Die Isolierung geschieht dabei sowohl gegenüber anderen Containern als auch dem Host-Server selbst. Dazu muss die Hyper-V-Rolle auf dem Server installiert sein.

Mit Windows Server 2019 hat Microsoft nicht nur einige neue Funktionen für Verwaltung und Einsatz von Container-Techniken wie Docker eingeführt. Mit dieser Version unterstützt der Windows-Server nun auch die Integration der Orchestrierungslösung Kubernetes. Kubernetes ist ein Framework, das aus mehreren Software-Komponenten besteht, die auf virtuellen oder physischen Servern installiert werden. Microsoft stellt unter <https://docs.microsoft.com/de-de/virtualization/windowscontainers/kubernetes/getting-started-kubernetes-windows> eine umfangreiche Dokumentation zum Thema Kubernetes unter Windows bereit. Wenn Sie tiefer in den Einsatz von Containern und Docker auf Ihrem Windows Server eintauchen wollen, so finden Sie unter <https://docs.microsoft.com/de-de/virtualization/windowscontainers/> ebenfalls eine ausführliche Dokumentation samt Anleitungen zum Einstieg in diese Themen.

Windows Server 2022 – die kommende Generation

Und wie geht es weiter mit Windows Server? Im sogenannten Insider-Programm stellt Microsoft sowohl bei den Server- als auch bei den Client-Betriebssystemen interessierten IT-Fachleuten und -Spezialisten immer wieder Vorabversionen der Betriebssysteme zur Verfügung. Durch die Rückmeldungen dieser Personengruppe können die Entwicklungsabteilungen in Redmond dann häufig leichter Fehler aufspüren oder ohne ihre Entscheidungen überprüfen. Allerdings kommt es dabei regelmäßig vor, dass in diesen Versionen implementierte Features und neue Möglichkeiten aus mannigfaltigen Gründen dann doch nicht ihren Weg in die endgültige, freigegebene Version des Betriebssystems finden.

Im März 2021 hat Microsoft auf der hauseigenen Veranstaltung Ignite die Version 2022 des Servers angekündigt. Für die »Windows-Insider« stand kurz danach eine erste Vorabversion zum Testen bereit, die im Verlauf der ersten Jahreshälfte durch mehrere Updates den Status Version 21H2 erreichte ([Abbildung 2.4](#)). Trotzdem müssen Nutzer, die diese Vorabversion installieren, echte Unterschiede noch suchen. Grundsätzlich verhält sich die Vorabversion von Windows Server 2022 wie die Vorgänger 2019 und 2016. Auch wenn bis jetzt bei jeder neuen Version mindestens ein neuer Betriebsmodus für den Verzeichnisdienst Active Directory hinzukam, ist dies bei Windows Server 2022 im Sommer 2021 noch nicht der Fall. Bekannt ist allerdings, dass Microsoft mit diesem kommenden Server-Release ein weiteres Mal den Support verändert: Ab Windows Server 2022 soll es dann nur noch LTSC-Versionen (Long-Term Servicing Channel) für die Server geben. Dabei verspricht das Unternehmen, alle zwei bis drei Jahre eine neue Hauptversion von Windows Server zu veröffentlichen. Die Anwender erhalten dann fünf Jahre Mainstreamsupport und fünf weitere Jahre erweiterten Support. Eine Tabelle zu den Versionen und ihren Laufzeiten stellt Microsoft hier <https://docs.microsoft.com/de-de/windows-server/get-started/windows-server-release-info> bereit. Grundsätzlich sind

LTSC-Versionen gerade für den Einsatz eines Servers eine gute Wahl: Sie bieten eine lange Option für die Wartung. Die Systeme erhalten weiterhin sowohl die sicherheitsrelevanten als auch die nicht sicherheitsrelevanten Updates, aber keine neuen Features und Funktionen.

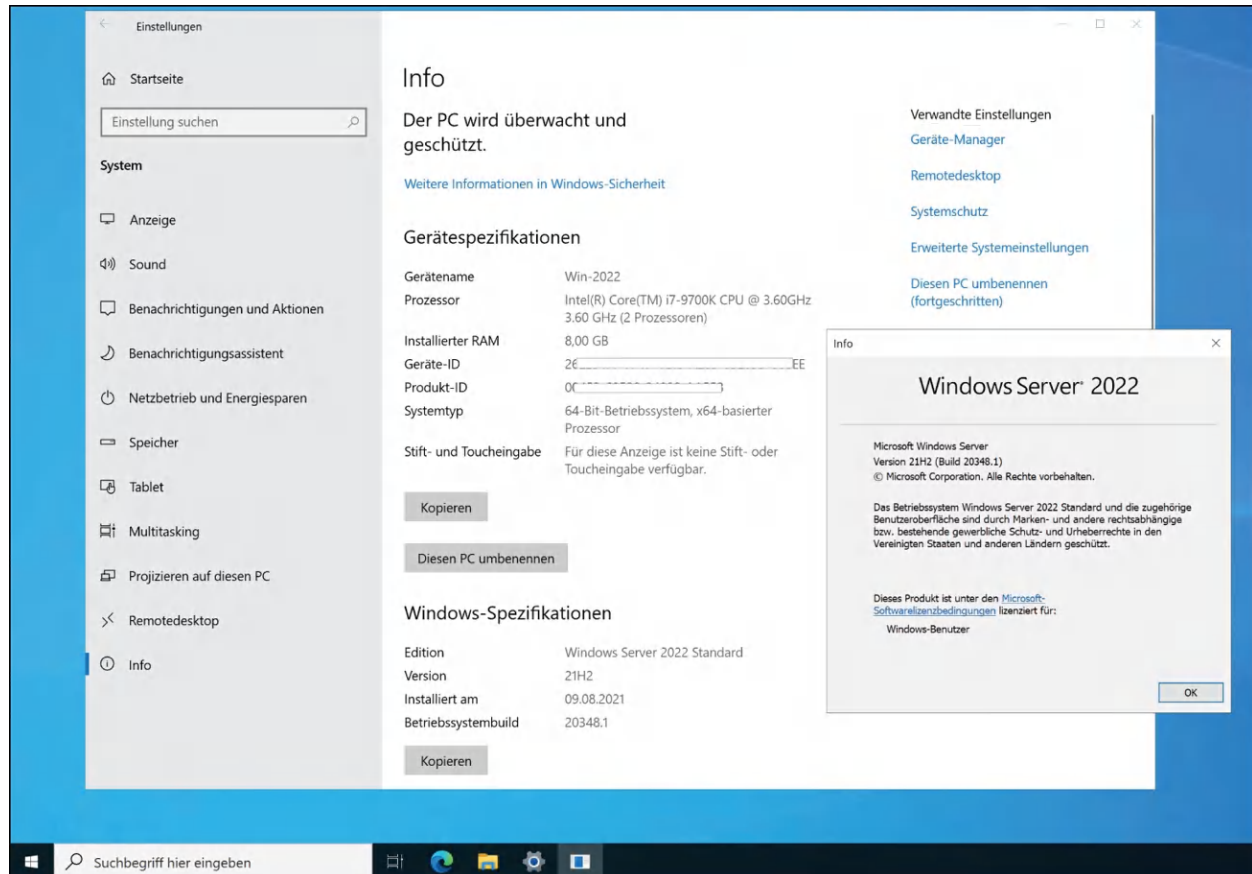


Abbildung 2.4: Bis auf die aktualisierte Versionsnummer sind auf den ersten Blick bei der Vorabversion Windows Servers 2022 nur sehr geringe Unterschiede zur Version 2019 erkennbar.

Geht es um neue Funktionen und Features, so sind die laut Microsoft bei Windows Server 2022 vor allen Dingen in den folgenden Bereichen zu finden:

- ✓ Sicherheit,
- ✓ Hybridintegration und -verwaltung und
- ✓ Cloud-Integration.

Viele der Verbesserungen im Bereich der Sicherheit fasst Microsoft unter

der Bezeichnung »Secure Core Server« (Server mit gesicherten Kernen) zusammen. Dabei werden Schutzfunktionen, wie sie teilweise auch schon bei den Windows-10-Versionen zum Einsatz kommen, nun auch Teil der Server-Version. Das geschieht unter anderem durch entsprechende Hardware wie ein Trusted Platform Module (TPM) und System Guard. Zudem sind auf Windows Server 2022 unter dem Stichwort »Secured Connectivity« die Netzwerkprotokolle HTTPS und TLS 1.3 standardmäßig aktiviert. Dadurch werden die Client-Systeme, die eine Verbindung zum Server aufbauen, deutlich besser geschützt.

Ganz wichtig ist laut Microsoft bei Windows Server 2022 die noch engere Verknüpfung mit Microsoft Azure, die auch ihren Niederschlag in den neuen und kommenden Versionen des Windows Admin Centers finden wird. Diese Software wird ab der Version 2103.2 die Anbindung von Azure-Funktionen wie Azure Arc oder Storage Migration Service an Windows Server 2022 ermöglichen. Dabei soll Azure Arc es ermöglichen, Funktionen und Technologien aus Microsoft Azure direkt in lokalen Rechenzentren zur Verfügung zu stellen. Das wird bei Microsoft unter »Hybride Verwaltung« verstanden und verknüpft den Windows-Server noch enger mit der Cloud.

Wer aber bereits einmal ein Insider-Release einer Windows-Version getestet hat, wird wissen, dass derartige Vorabversionen für den produktiven Einsatz absolut nicht geeignet sind. Unser erster Eindruck zeigt aber, dass sich die grundlegenden Verwaltungsfunktionen und -features höchstens in kleinen Details ändern werden. Ein wirklich endgültiges Datum für eine allgemeine Verfügbarkeit von Windows Server 2022 hat Microsoft auch Mitte 2021 noch nicht verkündet – es heißt nur, dass das Betriebssystem bis Ende des Jahres auf den Markt kommen soll.

Kapitel 3

Cloud und lokal

IN DIESEM KAPITEL

Unterschiede zwischen Cloud-Installation und lokalen Windows-Einrichtungen

Windows Server in der Azure Cloud

Alternative Cloud-Anbieter und deren Anbindungen

Auch wenn Sie bisher noch keinen Windows-Server installiert haben, werden Sie doch gewisse Vorstellungen davon haben, wie so ein Betriebssystem auf Ihre Hardware gelangt: Eine Installation »vor Ort« (auch als »on-premise« bezeichnet) wird in der Regel ein Medium erfordern, von dem die Software installiert wird. Das kann eine DVD, eine Festplatte, ein USB-Medium oder auch einfach eine sogenannte Image-Datei sein. Wer sich allerdings ein bisschen umhört, wird auch im Zusammenhang mit der Installation eines Betriebssystems immer wieder das Stichwort Cloud hören.

Installation: Cloud oder lokal?

Kommt die Rede auf eine Cloud-Installation, so ist damit allerdings nicht immer klar umrissen, was genau damit gemeint ist: So können Sie beispielsweise ein Windows-10-System installieren, indem Sie eine kleine Datei von Microsoft herunterladen, die dann die zur Installation benötigten Daten aus der Cloud nachlädt und das Betriebssystem auf Ihrer lokal vorhandenen Hardware installiert. Das bedeutet, Sie haben eine »Cloud-Installation« ausgeführt, bei der Sie keine physikalischen Medien mehr benötigen. Beim Betrieb Ihres lokalen Server-Systems bleibt aber alles, wie Sie es wahrscheinlich schon gewohnt sind.

Ganz anders hingegen, wenn Sie ein Betriebssystem direkt in der Cloud betreiben. Das ist eine Variante, die gerade von Anwendern bei Server-Systemen gern verwendet wird: Sie erlaubt es Ihnen, schnell und ohne dass dazu aufwendige Hardware vor Ort nötig wäre, einen neuen Server einzurichten und zu betreiben. Der Server wird dabei im Rechenzentrum des Cloud-Anbieters auf der notwendigen und technisch erforderlichen Hardware in Form einer virtuellen Maschine betrieben, und Sie als Nutzer greifen über das Netzwerk darauf zu. Das bedeutet natürlich auch, dass Sie eine entsprechend stabile, schnelle und zuverlässige Internet-Anbindung benötigen. Auf Basis eines solchen Servers können Sie dann auch weitere Server-Dienste einrichten und über das Internet direkt mit Ihrem Netzwerk verbinden. Sie mieten sich also einen Server und zahlen in der Regel auch nach verbrauchter Zeit oder verbrauchten Ressourcen.

Windows Server in der Azure Cloud

Neben den bekannten Internet-Providern bietet auch Microsoft unter den Namen Azure eigene Cloud-Dienste an. Diese Cloud-Techniken stellen Ihnen Dienste wie Datenbanken oder Webseiten zur Verfügung, was generell als »Platform as a Service« (PaaS) bezeichnet wird. Aber die Azure Cloud unterstützt auch virtuelle Server und virtuelle Netzwerke. Hinzu kommen noch Speicherdienste, sodass in der Cloud komplette IT-Infrastrukturen aufgebaut werden können (IaaS – Infrastructure as a Service).

Wenn Sie einfach nur mal einen solchen virtuellen Windows-Server ausprobieren wollen, so können Sie das über das Azure-Portal, das Sie unter <https://portal.azure.com> finden ([Abbildung 3.1](#)). Zum Anmelden benötigen Sie ein Microsoft-Konto. Sie können sich aber auch – und das ist der Weg, den wir vorschlagen würden – über die Adresse <https://azure.microsoft.com/de-de/free/> ein kostenloses Azure-Konto anlegen. Das ermöglicht es Ihnen, bestimmte Dienste bis zu 12 Monate ohne weitere Kosten auszutesten, und Sie bekommen für 30 Tage ein Guthaben, das Sie für die Azure-Dienste einsetzen können. Allerdings brauchen Sie auch hier ein Microsoft-Konto, das Sie jedoch im Rahmen der Anmeldung erstellen können.

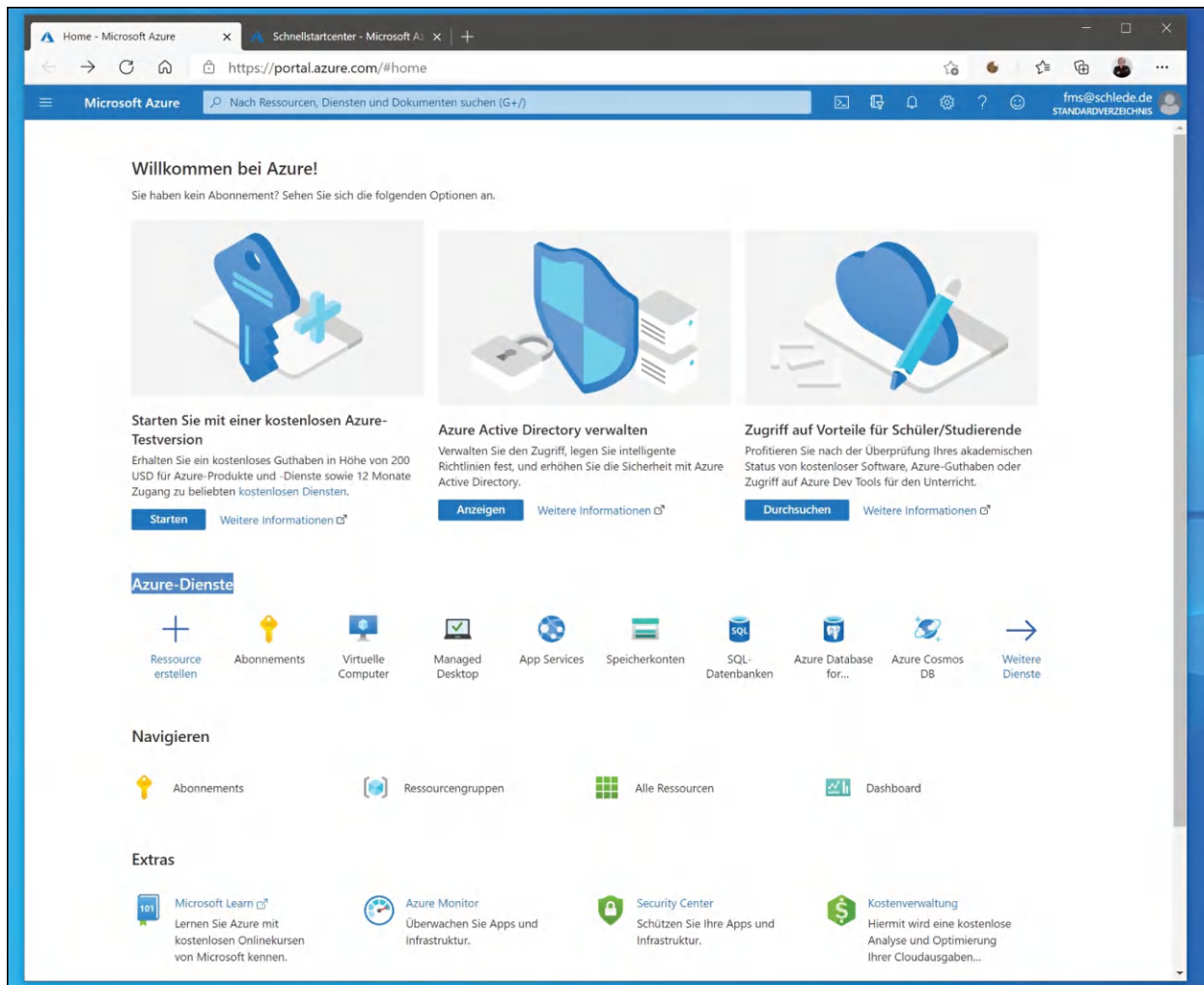


Abbildung 3.1: Über ein Portal stehen die verschiedenen Möglichkeiten von Azure direkt bereit – darunter auch der Einsatz eines Windows-Servers.

Danach können Sie über das Azure-Portal einen Windows-Server in der Azure Cloud anlegen:

1. Wählen Sie nach der Anmeldung am Portal unter **AZURE-DIENSTE** die Option **VIRTUELLE COMPUTER** aus.
2. Über das **HINZUFÜGEN** (repräsentiert durch ein Pluszeichen) können Sie dann entscheiden, ob Sie eine komplett neue virtuelle Maschine anlegen oder mit einer vordefinierten Konfiguration starten möchten.
3. Wählen Sie die neue VM, so gelangen Sie auf ein Formular, in das Sie dann die Daten zu Ihrem Projekt eintragen müssen. Ein Beispiel sehen Sie in der [Abbildung 3.2](#). Dort können Sie dann beispielsweise auch

Windows Server 2019 auswählen.

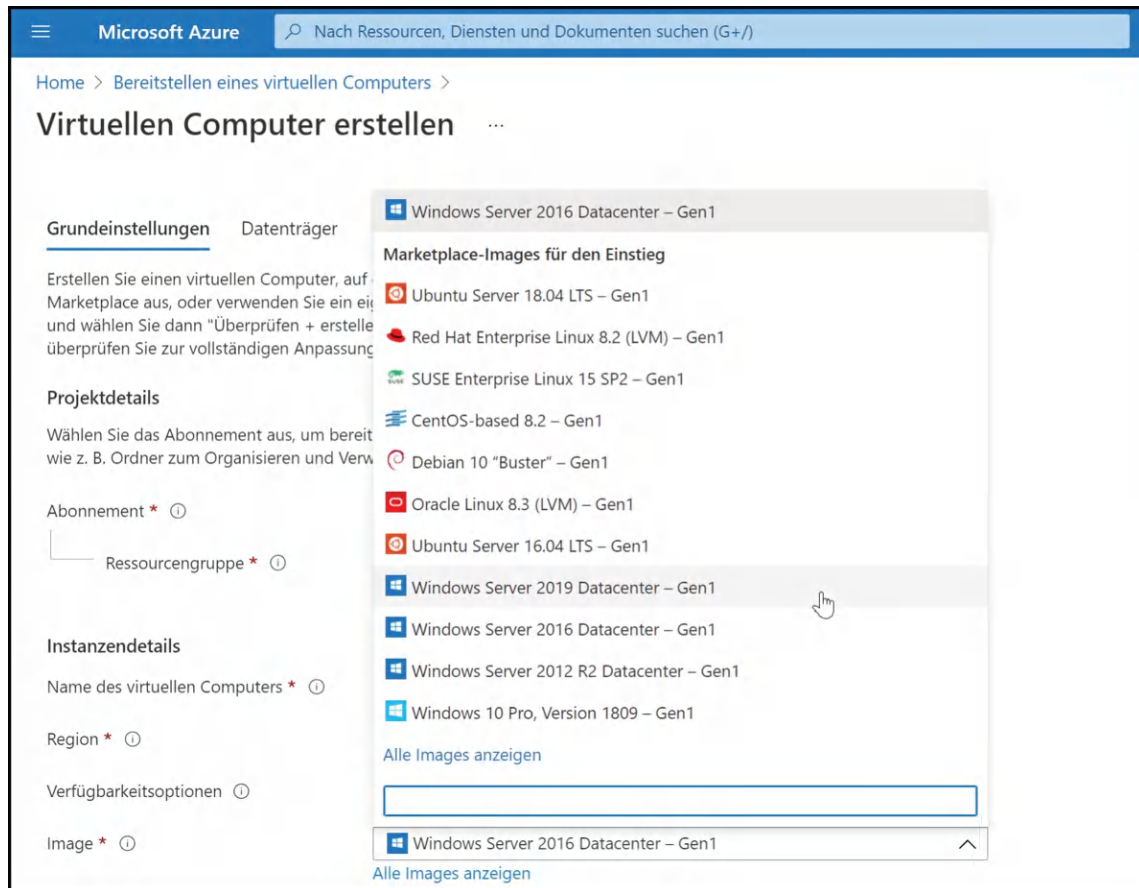


Abbildung 3.2: Das Anlegen und Erstellen eines virtuellen Windows Servers 2019 auf der Azure Cloud geht schnell vonstatten.

4. Haben Sie alle Angaben vorgenommen und dabei auch den voreingestellten RDP-Port übernommen, können Sie direkt auf den virtuellen Computer zugreifen, nachdem das System ihn für Sie erstellt hat.

Sie können bei den Betriebssystemen sowohl verschiedene Ausprägungen von Windows als auch unterschiedlichste Linux-Varianten auswählen. Sie bekommen im Formular auch gleich die Kosten für die von Ihnen ausgewählte Variante angezeigt. Die hängen dabei von der ausgewählten Hardware-Ausstattung ab, die Sie gewählt haben – also beispielsweise Arbeitsspeicher sowie Anzahl und Leistung der virtuellen CPUs. Ist Ihr virtueller Rechner eingerichtet (Azure prüft zuvor noch, ob alle Einstellungen in Ordnung sind), dann können Sie direkt von Ihrem

Arbeitsrechner aus mittels eines RDP-Clients (Remote Desktop Protocol) eine Verbindung zu der im Formular angegebenen IP-Adresse aufbauen. Sie finden die dafür notwendige Software standardmäßig auf allen Windows-Rechnern unter der Bezeichnung REMOTEDESKTOPVERBINDUNG. Haben Sie dort die öffentliche IP-Adresse Ihres virtuellen Servers eingegeben, können Sie sich mit dem Nutzernamen und Ihrem Passwort, das Sie bei der Einrichtung festgelegt haben, an dem System anmelden. Möglicherweise wird Ihnen dann eine Zertifikatwarnung angezeigt, die Sie mit JA oder WEITER bestätigen. Dann steht die Verbindung, und Sie können in einem Fenster wie in [Abbildung 3.3](#) gezeigt, mit dem virtuellen Server wie gewohnt arbeiten.

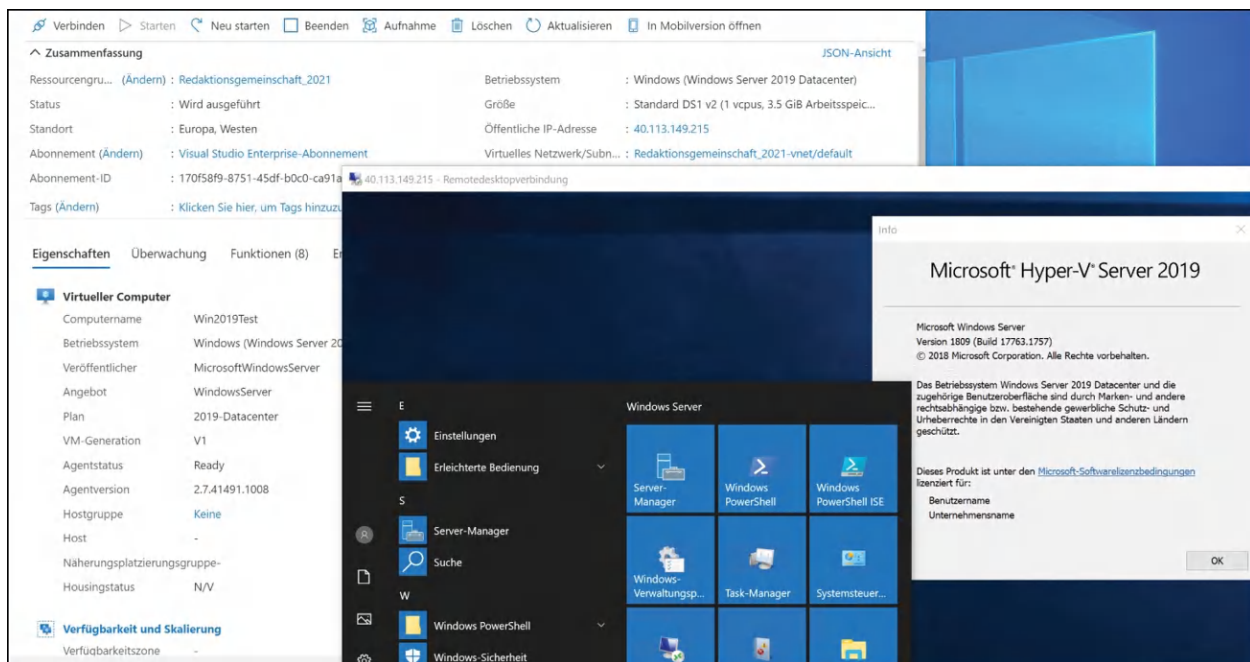


Abbildung 3.3: Ein virtueller Windows-2019-Server ist auf der Azure Cloud eingerichtet. Sie können über eine Remotedesktop-Verbindung darauf zugreifen und mit dem System arbeiten.

Insgesamt ist ein neuer Server auf der Azure Cloud schnell und einfach eingerichtet. Auch wenn die Installation dieses Betriebssystems auf lokaler Hardware ebenfalls recht flott von der Hand läuft, so besitzt dieser Ansatz auf jeden Fall den großen Vorteil, dass keine dedizierte Hardware vor Ort vorhanden sein muss. Zudem können Sie den Server beliebig »aufrüsten« wenn Sie mehr Leistung benötigen, oder ihn einfach auch wieder löschen, wenn eine Einsatz- oder Testphase vorbei ist.

Alternative Cloud-Anbieter und deren Anbindungen

Geht es um Cloud-Technik, so ist sich Microsoft verständlicherweise »selbst immer am nächsten«: Das Unternehmen aus Redmond unternimmt wirklich alles, um Ihnen als Administrator den Umstieg in die Cloud ganz leicht zu gestalten – natürlich mit Azure: der Microsoft Cloud.

Die Flaggschiffe im Portfolio von Microsoft sind nicht mehr Microsoft Office oder Microsoft Windows. Seit Ende der 2010er-Jahre verdient die Firma mehr Geld mit dem Cloud-Business. Insbesondere das Komplettpaket Office 365 und die Speicherdienste, so Brancheninformationen, stützen diesen wirtschaftlichen Erfolg.

In den vielen Seiten des Kleingedruckten der Lizenzbedingungen stellt das Unternehmen sicher, dass anderen Anbietern die freiheitliche Bereitstellung von Windows-Servern in Cloud-ähnlichen Rechenzentren eher verwehrt, denn erleichtert wird.

Aus diesem Grunde sind eher kostengünstige Anbieter stets darauf erpicht, dass der sich virtuell einmietende Kunde doch bitte selbst um seine Windows-Serverlizenzen bemühen möge. Diese Haltung stellt sicher, dass im Zweifelsfall der Kunde den Lizenzverstoß bewusst begangen hat und nicht der Plattformanbieter.

Wer schon Erfahrungen im Bereich der Lizenzierung im Umfeld der Virtualisierung sammeln konnte, wird um die Variante Datacenter-Edition wissen. Solang es sich um »den einen Kunden« handelt, ist das auch kein Problem. Sollten Sie jedoch die virtualisierten Ressourcen verschiedenen »Mandanten« zur Verfügung stellen, ist Microsoft der Meinung, dass ein Lizenzverstoß vorliegt.

Allerdings gibt es Szenarien, bei denen Sie als Administrator einzelne Windows-Server in einem virtualisierten, angemieteten Rechenzentrumsbereich betreiben möchten. In anderen Szenarien möchten Sie möglicherweise die komplette Domäne in diesem RZ aufbauen und den Client-Computern über »Direct Access« die Anbindung ermöglichen.

Bei einem anderen Anbindungsweg soll ein Server in einem Cloud-Rechenzentrum per VPN an die heimische Umgebung angebunden werden.

KAMP DHP

Die im deutschsprachigen Raum etablierten Hoster und Provider wie SpaceNet, 1&1 IONOS oder Strato haben Angebote für Server in der Cloud im Programm. Exemplarisch möchten wir an dieser Stelle auf das Business-Cloud-Angebot des ebenfalls etablierten Anbieters KAMP eingehen.

Der Dynamic Hardware Pool (DHP) des in Oberhausen ansässigen Netzwerkdienstleisters KAMP ist eine in Deutschland betriebene Cloud-Plattform für Unternehmen. Im DHP sind alle gebuchten Ressourcen wie

- ✓ Virtuelle CPUs,
- ✓ RAM,
- ✓ Storage und
- ✓ Netzwerk-Traffic

für den Administrator über eine Webseite aufrufbar. Dieses »virtuelle Datacenter« kann, je nach Bedarf, gemäß den eigenen Anforderungen hin erweitert werden. Die Flexibilität und bedarfsgerechte Abrechenbarkeit sind dabei typische Wesensmerkmale des Cloud-Computings.



Mit KAMP DHP profitieren Unternehmen von einer der wenigen IT-Lösungen, die beginnend mit der Bereitstellung im eigenen ISO 27001, ISO 9001 und ECB-S-zertifizierten deutschen Rechenzentrum über die Programmierung der Virtualisierungs-Software bis hin zur gesamten DHP-Produktentwicklung »aus einer Hand« stammt. Sensible Daten erhalten durch den konsequenten Verzicht auf Third-Party-Software keinen Zugriff »durch eine Hintertür«, die Sicherheitskette bleibt durchgehend im Verantwortungsbereich von KAMP und damit im deutschen Rechtsraum. KAMP DHP wird konform zur ISO 27018 betrieben, die die Verarbeitung von

personenbezogenen Daten in der Cloud regelt.

Die Erweiterungspakete sind einzeln buchbar, und was uns bei dem Angebot dieser Firma besonders gut gefällt, ist deren Credo: »Qualität statt langer Vertragsbindungen«.

Technisch beruht DHP auf der eigenen Virtualisierungsplattform Virtualcore, einer Weiterentwicklung der unter Unix und Linux weit verbreiteten KVM-Technik. Neben Microsoft Windows gibt es in dem App-Manager eine Reihe vorinstallierter Betriebssystem-Templates zur Auswahl:

- ✓ Ubuntu
- ✓ CentOS
- ✓ Debian



Was Hyper-V für Microsoft und ESXi für VMware ist, das ist KVM bei Linux und Unix.

Vorinstallation heißt in diesem Fall, dass Sie als Administrator nicht mit dem »Einlegen« von virtuellen Datenträgern beginnen müssen, sondern innerhalb kürzester Zeit eine neue VM auf Basis der Vorlage entsteht.

Bei den Linux-basierten Systemen geht der Komfort sogar noch deutlich weiter. Dank der Turnkey-Linux-Pakete können Sie über 100 fertig konfigurierte Applikationen wie zum Beispiel Server mit Joomla, WordPress oder TYPO3, Customer Relationship Management-Systeme (CRM) wie vTiger oder SugarCRM oder Fileserver wie ownCloud direkt »out of the box« bereitstellen.

Erstellen wir exemplarisch einen neuen Windows-Server in DHP:

1. Anmeldung per Browser an der DHP-Login-Seite
<https://dhp.kamp.de/>.
2. Die Standardanmeldung erfolgt per Benutzername und Passwort. Zur Erhöhung der Sicherheit ist im Zusammenspiel mit einem Authenticator eine Zwei-Faktor-Authentifizierung (2FA) möglich.

3. Im Browser erscheint das sogenannte DHP Dashboard mit einer Übersicht der genutzten und verfügbaren Ressourcen und dem Zugriff auf verschiedene Befehle – siehe [Abbildung 3.4](#).

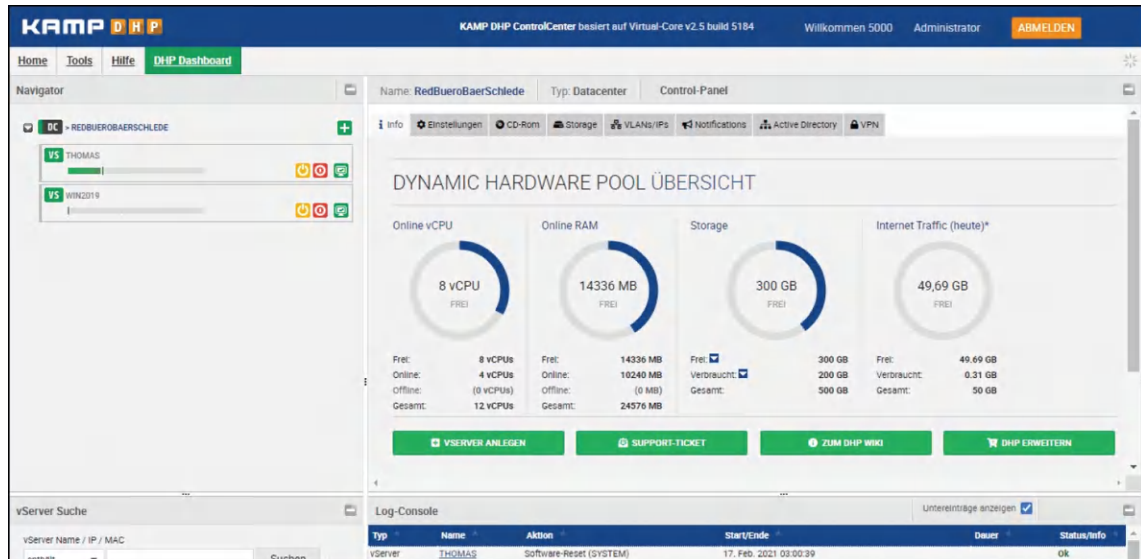


Abbildung 3.4: Das DHP Dashboard mit dem Ressourcenzugriff

4. Zum Erstellen eines neuen Servers klickt der Administrator auf das Plus-Symbol.
5. Es erscheint eine Auswahl von verschiedenen Betriebssystemen, unter anderem Windows Server 2016 und 2019 – wir entscheiden uns für den jeweils jüngsten Windows-Kandidaten.
6. Es erscheint das Dialogfenster zur Festlegung der Hardware-Ressourcen zum Template. In unserem Test passt das Template direkt zum Monat des Aufsetzens – sprich alle bis zu diesem Zeitpunkt ausgebrachten Patches und Services Packs sind enthalten. Nun gilt es, einige wenige Einstellungen vorzunehmen:
- NAME der Maschine, hierbei handelt es sich um den Namen für die Anzeige innerhalb des virtuellen Datacenters. Der Hostname wird, wie bei einem lokalen Server, im Anschluss angepasst.
 - Anzahl VIRTUELLER CPUS – der Assistent schlägt zwei vCPUs vor. Je nach gebuchter Anzahl von virtuellen Hauptprozessoren können bis zu 16 vCPUs zum Einsatz

kommen.

- Zugewiesener RAM – zwischen 512 MByte und 64 GByte.
- HD-GRÖSSE– der Grundwert beträgt stets 50 GByte, da das Template auf dieser Größe vorkonfiguriert ist. Sofern Sie an dieser Stelle einen größeren Wert angeben, gilt es im Nachgang, auf dem laufenden Windows-System den verbleibenden Speicherplatz einer Partition zuzuordnen oder eine neue anzulegen.
- Der Benutzername Administrator ist derzeit fest vorgegeben, Sie legen nur noch das Passwort fest.
- Die Netzwerkeinstellungen bieten in unserem Paket lediglich die Auswahl VLAN-DHP-PUBLIC[FW] und IPV4 AUS DEM GLOBALEN POOL VERWENDEN.
- Klicken Sie auf SPEICHERN, und die Maschine wird erstellt. Nach weniger als einer Minute können Sie sich über das grüne Monitor-Symbol über »RemoteScreen v2« (einer VNC-Variante) auf die Konsole aufschalten – siehe [Abbildung 3.5](#).

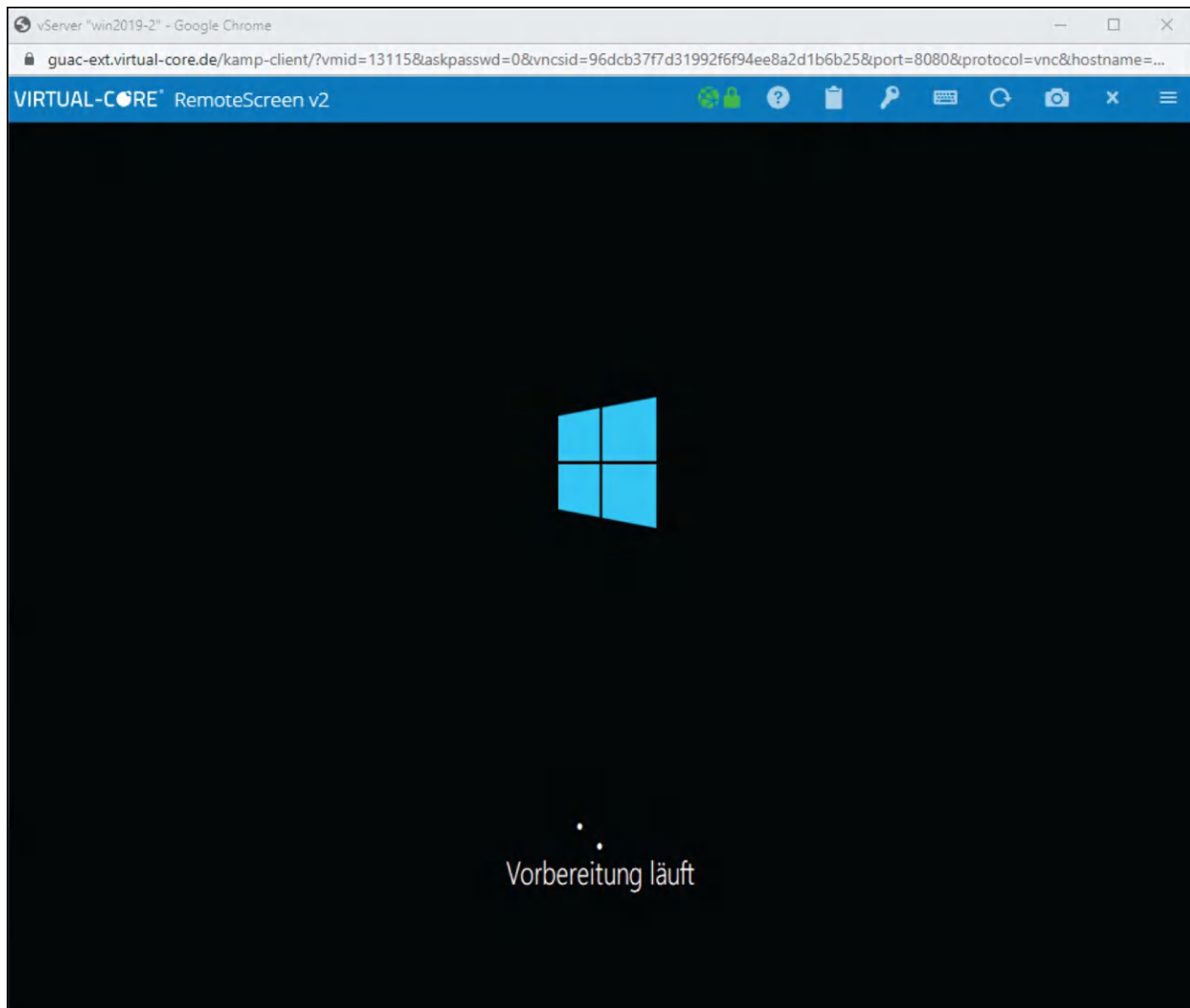


Abbildung 3.5: Zugriff aus dem DHP Datacenter per VNC auf den neuen Server

Zu diesem Zeitpunkt ist der neue Server ausschließlich über das DHP Dashboard zu erreichen, da die Firewall-Einstellungen einen Zugriff aus dem öffentlichen Netzwerk verhindern.

Zwischen den virtuellen Maschinen eines Kunden in einem virtuellen Datacenter wird der Netzwerkverkehr jedoch von dieser Firewall nicht unterbunden. In diesem Fall gelten ausschließlich die Regularien der Windows-Firewall.

Die IPv4-Adresse erhält der Server, wie beim Einrichtungsvorgang benannt, aus einem Pool der Firma KAMP. Eigene IP-Adressen für den Datenaustausch zwischen den VMs können Sie als Administrator zusätzlich vergeben. Systembedingt arbeitet DHP in den kleineren

Editionen nur mit einem virtuellen NIC. Erweiterte Netzwerkstrukturen, wie beispielsweise VLANs, erfordern ein »Enterprise«-Paket.

Über die Firewall-Einstellungen ([Abbildung 3.6](#)) können Sie sehr genau festlegen, welche Protokolle durchgängig sein sollen und von welcher Quelle aus. Verfügen Sie beispielsweise über eine feste IP-Adresse, können Sie sehr einfach den RDP-Zugriff auf diese Quelladresse beschränken. Dank der Unterstützung von DynDNS ist aber auch die Verwendung von dynamischen Adressen für den Zugriff realisierbar.

The screenshot shows a web-based interface for editing a firewall rule. The title is 'FIREWALLREGEL BEARBEITEN'. The form contains the following fields and values:

Field	Value
Aktiv	☐
Scope	Server
Quell-IP / DynHost	*
Netzwerkarte	alle externen
Protokoll	TCP
Port	3389
Verbindung	erlauben
Beschreibung	RDP

At the bottom of the form are two buttons: 'Abbrechen' (Cancel) and 'Firewallregel speichern' (Save Firewall Rule).

Abbildung 3.6: Die Firewall-Steuerung von KAMP DHP arbeitet auch mit dynamischen Hostadressen.

Zum Zeitpunkt der Manuskripterstellung befand sich das DHP Active Directory noch im Beta-Stadium. Um eine Domäne im DHP aufzubauen, gibt es einige wenige Voraussetzungen:

- ✓ Quemu-Gast-Komponente ist aktiv (Standardeinstellungen).
- ✓ Der Hostname und der Name in der DHP-Verwaltung sind identisch.
- ✓ Auf dem Server ist die Rolle des Domänen-Controllers bereits installiert, und der Server ist zum DC hochgestuft worden.

Anschließend können Sie in der Gesamtübersicht von DHP die gewünschte Maschine als Domänen-Controller markieren. Auch ohne diese Einstellung ist es möglich, eine Domäne in DHP zu betreiben. Die gesonderte Zuweisung des Merkmals sorgt beispielsweise dafür, dass neue vServer bereits beim Anlegen durch den Administrator einer Organisationseinheit einer Domäne zugewiesen werden. Das vereinfacht eine Gruppenlinien-basierte Zuweisung von Einstellungen deutlich.

VPN-Zugriff in die Cloud

In einem Zusammenspiel von lokalen Ressourcen und einem ausgelagerten Teil von Servern in einem virtuellen Datacenter wie im Fall von KAMP DHP stellt sich natürlich die Frage, wie ein Austausch stattfindet. Site-to-Site-Konfiguration über vorbereitete Appliances gibt es hier nicht, wohl aber die Möglichkeit, sich per VPN auf Betriebssystemebene zu verbinden. Für die weit verbreitete FRITZ!box von AVM können Sie den entfernten Server mit dem kostenfreien VPN-Client von ShrewSoft ausstatten. KAMP selbst bietet mit dem ebenfalls kostenfreien WireGuard-VPN eine Variante an, bei der Sie sich direkt in das DHP-Public-VLAN einwählen und zu allen virtuellen Servern Verbindung aufbauen können.

Die Installation eines VPN-Zugangs ins Rechenzentrum ([Abbildung 3.7](#)) ist in wenigen Augenblicken erledigt – kein Vergleich zu den »Installationsorgien« anderer Anbieter.

VPN-ZUGANG ANLEGEN

Beschreibung:	BÄR
Öffentlicher Schlüssel:	wird automatisch erzeugt...
IPv4-Adresse:	wird automatisch vergeben...
IPv6-Adresse:	wird automatisch vergeben...
Zusätzliche Routen:	in CIDR Notation, durch Kommata getrennt Tragen Sie hier Routen ein, die sich im Netz des VPN-Zugangs befinden und auf die Sie von Ihren vServern aus zugreifen möchten.
Redirect Default GW:	☒ Das Umleiten des Default Gateways wird für alle Road Warrior Setups empfohlen. Wenn Sie ein Site2Site VPN aufbauen, sollten Sie den Default Gateway des VPN-Zugangs nicht umleiten. Sie müssen dann allerdings beim Anlegen jedes neuen vServers die Config des VPN-Zugangs anpassen oder dedizierte IP Netze in Ihr DHP Paket buchen.
Verbinde über IPv6:	☐ Dies betrifft die Verbindung zum Wireguard VPN, nicht den Traffic innerhalb des VPNs. Sie können beispielsweise über IPv6 verbinden und trotzdem per IPv4 und IPv6 auf die vServer in Ihrem Datacenter über den VPN-Zugang zugreifen.

Abbildung 3.7: Anlage eines VPN-Zugangs ins KAMP DHP Datacenter



Die Redaktionsgemeinschaft des Autorenduos arbeitet seit vielen Jahren für Software-Tests mit der KAMP-DHP-Basis zusammen. Große Teile dieses Buchs wurden auf einer VM im Rechenzentrum von KAMP per Remotedesktop-Verbindung verfasst.

Praktischerweise gibt es ein kostenfreies Minipaket zum Testen – das Ganze ohne zeitliche Limitierung und ohne Kaufverpflichtung, jedoch ohne die Option, Windows als Betriebssystem zu wählen.

Kapitel 4

Fenster oder Konsole?

IN DIESEM KAPITEL

Warum ein Server auch eine Kommandozeile braucht

»Normale« Windows-Oberfläche versus Kommandozeile

Was die Eingabeaufforderung so kann

Beispiele für die Arbeit »direkt am Prompt«

Wenn Sie schon etwas länger Microsofts Betriebssysteme verwenden, dann können Sie sich vielleicht noch an die Zeiten von MS-DOS erinnern. Dieses Betriebssystem, das auch noch als Fundament der ersten Windows-Versionen diente, kannte im Prinzip noch keine Fenster, wie wir sie heute gewohnt sind. Alle Befehle und Anweisungen mussten direkt an der Kommandozeile eingegeben werden, auf der ein blinkender Cursor auf die Eingabe wartete.

Wer schon mit Linux-Systemen gleich welcher Version oder Ausprägung gearbeitet hat, kennt ebenfalls die Eingabe direkt auf der Kommandozeile in der jeweiligen Betriebssystem-Shell. Echte Linux-Puristen schwören nach wie vor darauf, dass nur der sein System wirklich versteht, der diese Art der Kommunikation mit dem Betriebssystem beherrscht.

Microsoft hat in den letzten Jahren auch die Windows-Server wieder mehr in Richtung Kommandozeile ausgerichtet: Immer mehr Komponenten im Windows-Server können mit der PowerShell verwaltet und gesteuert werden. Das zeigt sich nicht zuletzt daran, dass Microsoft bei der Installation von Windows Server 2019 als Standardauswahl die »Minimalversion« der grafischen Oberfläche empfiehlt ([Abbildung 4.1](#)).

Windows-Oberfläche versus Kommandozeile

Grundsätzlich bietet Ihnen jede aktuelle Windows-Version zwei Shells zum Arbeiten an der Kommandozeile an: die Eingabeaufforderung (von Microsoft manchmal auch generell als »Befehls-Shell« bezeichnet) und die PowerShell. Shell-Programme ermöglichen eine direkte Kommunikation zwischen Ihnen und dem Betriebssystem oder den Anwendungen. Zudem stellen beide Shells auch eine Umgebung zum Automatisieren des Server-Betriebs dar. Während Sie im Fenster der PowerShell sowohl Windows-Befehle als auch PowerShell-Cmdlets ausführen können, stehen Ihnen in der Eingabeaufforderung nur die Windows-Befehle zur Verfügung. PowerShell-Cmdlets können Sie dort nicht ausführen.

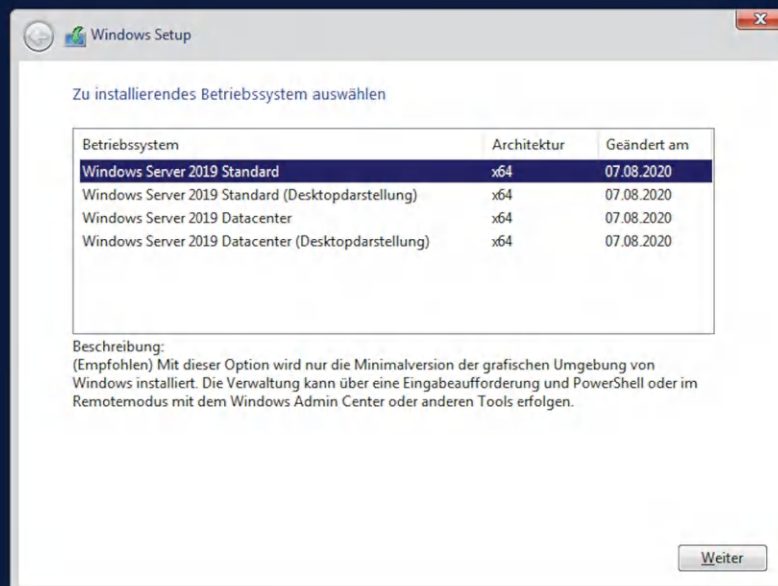


Abbildung 4.1: Die empfohlene »minimale« Installation von Windows Server 2019 geht schon von der Verwaltung mittels Eingabeaufforderung aus.

Microsoft setzt standardmäßig auf den Einsatz der PowerShell auch als Kommandozeile. Wenn Sie also einen Rechtsklick auf START oder über  +  das auch als »Power-Menü« bezeichnete Menü aufrufen, finden Sie dort zunächst nur die Einträge zum Aufruf der PowerShell. Erst wenn Sie in die Windows-Einstellungen wechseln und dort im Abschnitt PERSONALISIERUNG den Bereich TASKLEISTE aufrufen, finden Sie dort wie in [Abbildung 4.2](#) zu sehen einen Schiebeschalter, den Sie auf die Position »Aus« setzen. Dann erscheinen im »Power-Menü« wieder die beiden Aufrufe für die Eingabeaufforderung, wie ebenfalls in der [Abbildung 4.2](#) zu sehen. Sie können dann ein Fenster für die Eingabeaufforderung mit den normalen Nutzerrechten oder den erweiterten Rechten eines Administrators aufrufen, was bei vielen systemnahen Aufrufen und Kommandos notwendig ist. Wollen Sie die Eingabeaufforderung starten, so können Sie auch den Befehl `cmd` im Suchfenster auf dem Desktop eingeben, und das Konsolenfenster erscheint auf dem Desktop Ihres Servers.

Bleibt die häufig diskutierte Frage: Brauchen Sie die Kommandozeile? Ganz sicher brauchen Sie diese Eingabeform, wenn Sie Ihren Server in der Minimal- oder auch Core-Version betreiben. Wobei in diesen Fällen viele Anwender die PowerShell bevorzugen. Trotzdem bietet Ihnen auch die Kommandozeile der »traditionellen Art« viele Möglichkeiten und Funktionen.

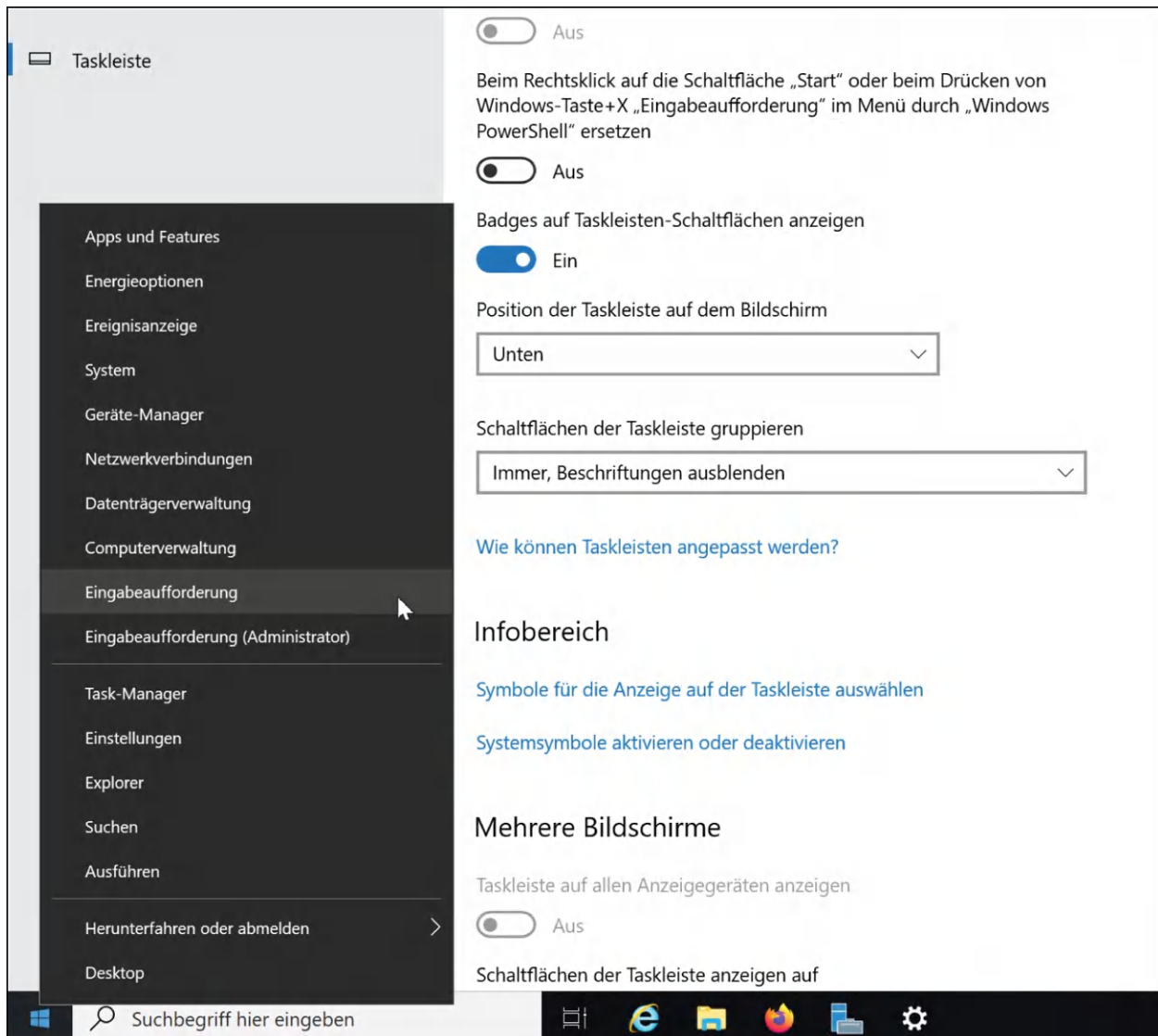


Abbildung 4.2: Standardmäßig ist die PowerShell als Kommandozeile voreingestellt. Ändern Sie das in den Windows-Einstellungen, so finden Sie beim Rechtsklick auf »Start« dort wieder die Eingabeaufforderung.

Was die Eingabeaufforderung so kann

Die Kommandozeile und damit auch das sogenannte Konsolenfenster haben keinen guten Ruf bei den Windows-Anwendern. Wenn Sie mit einem Windows-Server arbeiten wollen oder müssen, dann sollten Sie sich aber auf jedem Fall etwas genauer mit diesem Teil des Betriebssystems befassen. Selbst die Entwickler in Redmond haben diese Software lange

sehr stiefmütterlich behandelt. Seit den Updates für die Windows-Systeme, die 2019 herauskamen, wurde aber auch an dieser Stelle mit jedem Windows-Feature-Update nachgebessert. Das mag nicht zuletzt daran liegen, dass die gleiche Konsole ja auch für den Einsatz mit der PowerShell verwendet wird (nur dass sie dann standardmäßig mit einem blauen Hintergrund startet).

Konnten Sie das Konsolenfenster in früheren Windows-Versionen nicht beliebig skalieren, wie Sie es eigentlich von jedem Fenster unter Windows gewohnt sind, so ist das nun mit den aktuellen Versionen problemlos möglich. Wenn Sie einen Rechtsklick auf die obere Leiste des Fensters der Konsole ausführen, bekommen Sie ein Pull-down-Menü präsentiert, in dem Sie unter anderem auch die Schriftgröße und -farbe in dem Fenster einstellen können. Wählen Sie in diesem Pull-down-Menü den Eintrag EIGENSCHAFTEN und in diesem Fenster dann die Registerkarte OPTIONEN aus, so bekommen Sie eine ganze Reihe von Einstellmöglichkeiten für dieses Fenster präsentiert ([Abbildung 4.3](#)).

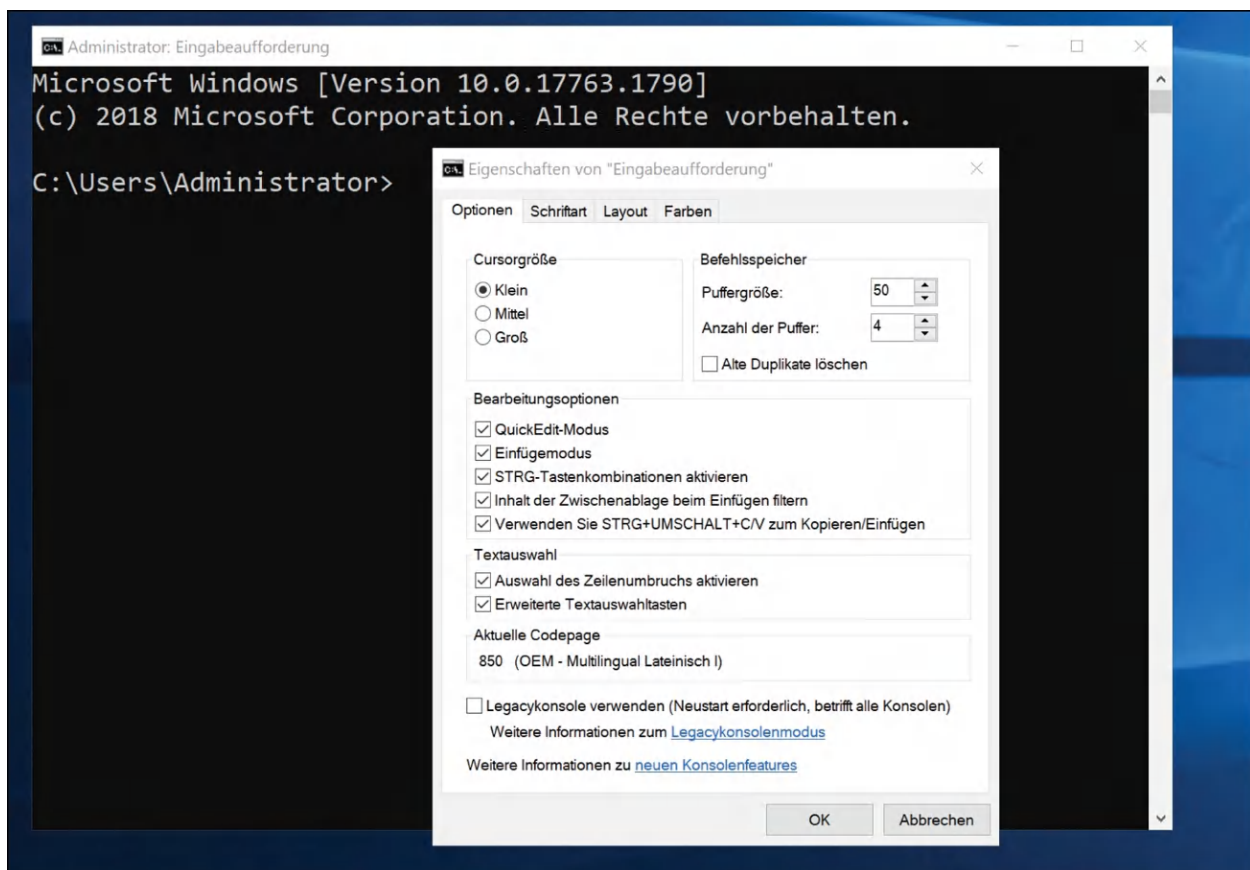


Abbildung 4.3: Das Fenster der Eingabeaufforderung lässt bei den aktuellen Versionen von Windows Server umfangreiche Einstellungen zu.

In diesem Menü finden Sie dann auch die Neuerungen und Verbesserungen, die die Entwickler der Eingabeaufforderung und damit auch PowerShell-Konsole spendiert haben:

- ✓ Die  -Tastenkombinationen können nun aktiviert werden.
- ✓ Sie können den Inhalt der Zwischenablage beim Einfügen filtern.
- ✓ Ein bis dato schmerzlich vermisste Eigenschaft: Nun ist es auch möglich,  +  +  oder  zum Kopieren oder Einfügen im Konsolenfenster zu verwenden.
- ✓ Sie können die Auswahl des Zeilenumbruchs aktivieren und
- ✓ bekommen zudem die Möglichkeit, erweiterte Textauswahltasten zu verwenden.

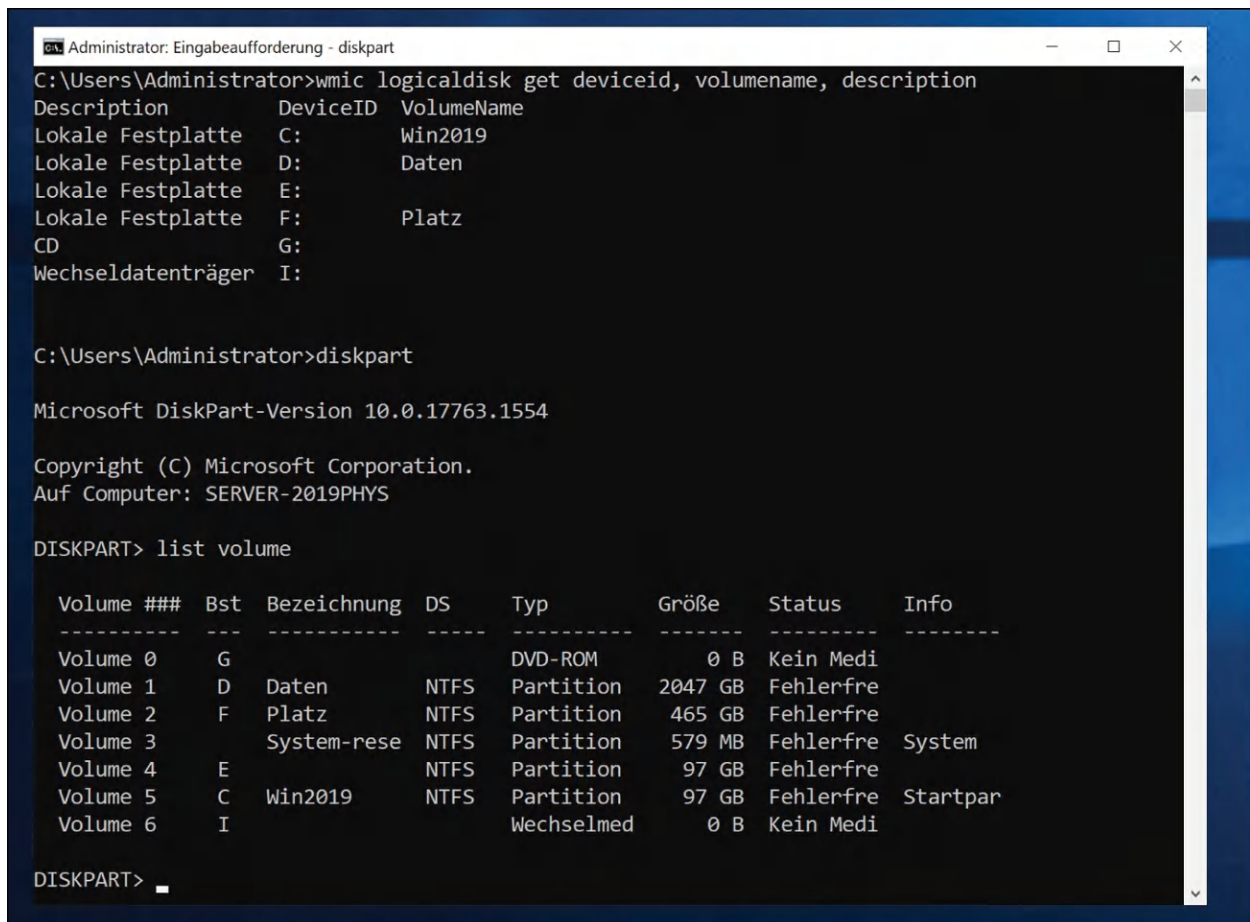
In der [Abbildung 4.3](#) sehen Sie, dass wir alle diese Möglichkeiten ausgewählt haben, da sie die Arbeit mit der Eingabeaufforderung doch sehr erleichtern. Stellen Sie allerdings fest, dass keine dieser Möglichkeiten im Konsolenfenster auf Ihrem Server funktioniert, so sollten Sie ebenfalls in dieses Menü schauen. Dort steht nämlich auch die Möglichkeit bereit, eine sogenannte »Legacyconsole« zu starten. Nach einem Neustart der Eingabeaufforderung verhält sie sich dann wieder so, wie Sie es vielleicht von den »alten« Windows-Versionen gewohnt. Diese Einstellung gilt dann für alle Konsolen, also ebenfalls für das Fenster, das Sie beim Aufruf der PowerShell präsentiert bekommen.

Kommandozeile: Arbeiten direkt »am Prompt«

Wer es gewohnt ist, mit der grafischen Windows-Oberfläche zu arbeiten, wird sich vielleicht zunächst einmal etwas schwertun, beispielsweise so triviale Aufgabe wie das Auflisten der vorhandenen Laufwerke und Festplatten auszuführen. Dürfte den meisten Nutzerinnen und Nutzern das

Anzeigen der Dateien und Ordner mittels des `dir`-Befehls (für »directory« – Verzeichnis) noch geläufig sein, scheint es mit der Anzeige der Laufwerksbuchstaben zunächst etwas schwieriger zu sein. Doch hier kann einer der vielen Befehle helfen, die Ihnen auf der Kommandozeile direkt zur Verfügung stehen.

Wollen Sie von der Kommandozeile aus sehen, welche Festplattenlaufwerke sich in Ihrem Server befinden und welche Laufwerksbuchstaben ihnen jeweils zugeordnet sind, so bieten sich dazu zwei Möglichkeiten an, deren Aufruf Sie in der [Abbildung 4.4](#) sehen können.



```
Administrator: Eingabeaufforderung - diskpart
C:\Users\Administrator>wmic logicaldisk get deviceid, volumename, description
Description      DeviceID VolumeName
Lokale Festplatte C:      Win2019
Lokale Festplatte D:      Daten
Lokale Festplatte E:
Lokale Festplatte F:      Platz
CD               G:
Wechseldatenträger I:
```

```
C:\Users\Administrator>diskpart

Microsoft DiskPart-Version 10.0.17763.1554

Copyright (C) Microsoft Corporation.
Auf Computer: SERVER-2019PHYS

DISKPART> list volume

  Volume ###  Bst  Bezeichnung  DS      Typ          Größe   Status   Info
  -
Volume 0      G      DVD-ROM      0 B      DVD-ROM      0 B      Kein Medi
Volume 1      D      Daten        NTFS     Partition    2047 GB  Fehlerfre
Volume 2      F      Platz        NTFS     Partition    465 GB   Fehlerfre
Volume 3      System-rese NTFS     Partition    579 MB   Fehlerfre System
Volume 4      E      NTFS         NTFS     Partition    97 GB    Fehlerfre
Volume 5      C      Win2019      NTFS     Partition    97 GB    Fehlerfre Startpar
Volume 6      I      Wechseldatenträger Wechseldatenträger 0 B      Kein Medi
```

```
DISKPART> _
```

Abbildung 4.4: Zwei Wege, die Festplatten und Laufwerksbuchstaben des Windows-Servers direkt an der Kommandozeile anzuzeigen.

Zunächst einmal können Sie auf WMI, die Windows Management Instrumentation, zurückgreifen. Einige Erläuterungen dazu finden Sie am Ende des Kapitels. Der folgende Aufruf bringt die gewünschten

Informationen auf den Bildschirm:

```
wmic logicaldisk get deviceid, volumename, description
```

Eine weitere Methode besteht darin, das Kommandozeilenprogramm `diskpart` einzusetzen. Dieses Programm dient zwar vornehmlich dazu, Festplatten zu verwalten und aufzuteilen, lässt sich aber auch gut zur Anzeige der Informationen über die Massenspeicher nutzen. Das Programm arbeitet interaktiv, Sie kommen nach dem Aufruf einen Prompt angezeigt, an dem Sie den gewünschten Befehl eingeben können:

```
diskpart  
list volume
```

In der [Abbildung 4.4](#) sehen Sie auch diesen Aufruf. Durch Eingabe von `exit`

verlassen Sie dann das `diskpart`-Programm wieder. Wollen Sie wissen, was das Programm sonst noch so kann, geben Sie ein Fragezeichen `?` oder `HELP` am `diskpart`-Prompt ein. Sie bekommen dann alle Befehle mit einer kurzen Beschreibung angezeigt.

Unter der Adresse <https://docs.microsoft.com/de-de/windows-server/administration/windows-commands/windows-commands> stellt Microsoft alle sogenannten Win32-Konsolen-Befehle in einer Referenz zur Verfügung. Hier werden Sie für (fast) alle Gelegenheiten den richtigen Befehl und Aufruf für das Arbeiten mit der Kommandozeile finden können.



Wie viel Speicher steckt im lokalen oder entfernten Computer, wie ist die Festplatte angeschlossen, und wie bekommen Sie diese Informationen? Hier kann WMI, die Windows Management Instrumentation, helfen. Das ist die Microsoft-Implementierung und Erweiterung des Common Information Models (CIM), einer Kernfunktionalität des standardisierten Web Based Enterprise Managements (WBEM) für die Windows-Plattform. WMI ermöglicht den schreibenden und lesenden Zugriff auf nahezu alle Einstellungen von Windows-Systemen. Sie kann sowohl mithilfe der

Kommandozeile als auch mittels der PowerShell eingesetzt werden.
Einen detaillierten Grundlagenartikel zum Thema, den dieses
Autorenteam für die Publikation IP-Insider verfasst hat, finden Sie
unter der Adresse: <https://bit.ly/2PKjqM0>

Kapitel 5

PowerShell und der Server

IN DIESEM KAPITEL

Was ist die PowerShell und warum sollte sie auf dem Server zum Einsatz kommen?

Grundlagen der PowerShell

Begriffe und Besonderheiten der PowerShell

Erste Schritte zum eigenen Skript

PowerShell in der Server-Verwaltung einsetzen

Vielleicht haben Sie ja schon einige Erfahrungen mit dem Windows-Betriebssystem gesammelt und kennen damit Ihren »Weg durch die Fenster«. Dann fragen Sie sich vielleicht nun, warum Sie von dieser komfortablen Art der Bedienung mit Maus und Windows auf die im Prinzip recht archaische Arbeit an der Kommandozeile wechseln sollten. Auch viele gestandene Windows-Profis nähern sich noch heute mit großem Misstrauen dieser Art des Arbeitens auf den Server-Systemen, während Unix-/Linux-erfahrene Anwender den Einsatz von Skriptsprachen unterschiedlichster Art zumeist regelmäßig einsetzen. Wer allerdings seinen Windows-Server schnell, effizient und teilweise auch automatisiert verwalten und betreuen will, kommt um die Skriptsprache PowerShell nicht herum. Dieses Kapitel bietet Ihnen deshalb einen groben Überblick über die PowerShell und ihre Fähigkeiten.



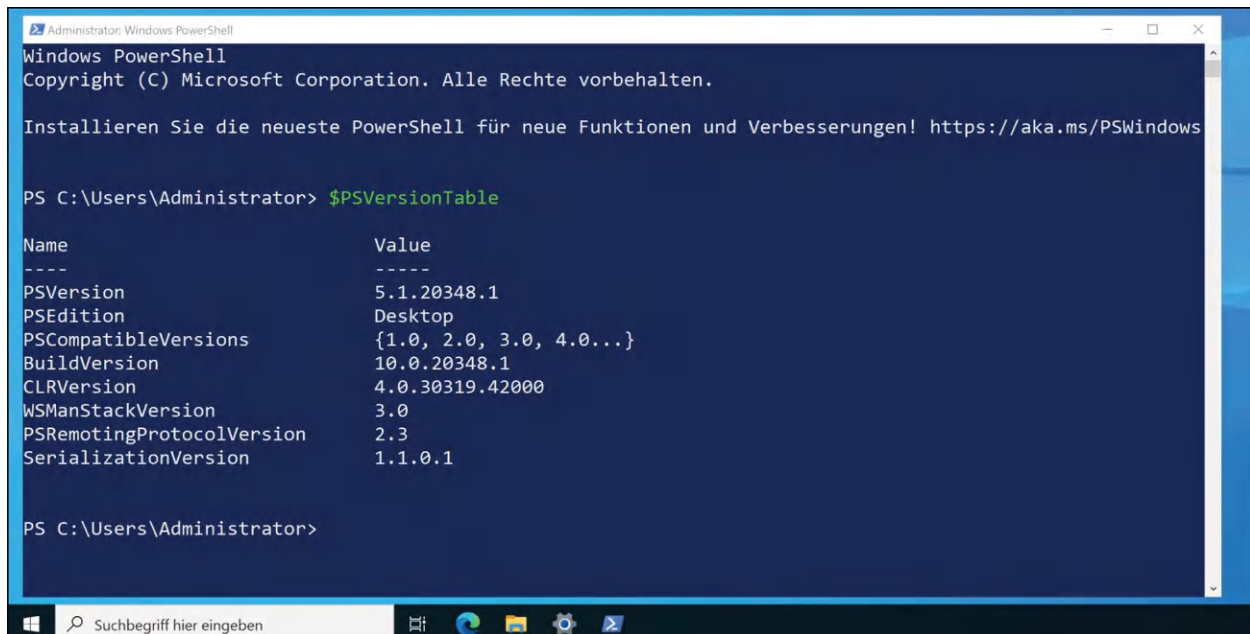
Skriptsprachen sind Programmiersprachen genau wie beispielsweise C, C++ oder Pascal und Fortran. Das wesentliche Unterscheidungsmerkmal zu diesen »normalen« Programmiersprachen besteht darin, dass der Code von

Skriptsprachen nicht durch einen Compiler in Binärcode übersetzt wird, der dann direkt auf der CPU in Form von Maschinenbefehlen abgearbeitet wird, sondern dass diese Programme durch einen sogenannten Interpreter zur Laufzeit abgearbeitet werden. Dadurch sind Skriptsprachen besonders gut dazu geeignet, schnell kleine Programme zu entwickeln, die beispielsweise zum Testen von Konfigurationen und Installationen eingesetzt werden können.

Während viele traditionelle Skriptsprachen sich auch dadurch auszeichnen, dass sie nur wenige Sprachelemente und Konstrukte aufweisen, die zur Bewältigung komplexer Aufgaben benötigt werden, kann die PowerShell beispielsweise mit dem konsequenten Einsatz der Objektorientierung auch dafür und zur Automatisierung von Verwaltungsaufgaben auf dem Windows-Server eingesetzt werden.

Wichtige PowerShell-Grundlagen

Wie finde ich die PowerShell auf meinem Windows-Server? Öffnen Sie ganz einfach das STARTMENÜ und wählen Sie die Kachel mit der Beschriftung POWERSHELL aus. Darauf öffnet sich ein Fenster mit der standardmäßig auf allen Versionen des Windows-Servers installierten PowerShell 5.1 ([Abbildung 5.1](#)).



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

Installieren Sie die neueste PowerShell für neue Funktionen und Verbesserungen! https://aka.ms/PSWindows

PS C:\Users\Administrator> $PSVersionTable

Name                           Value
----                           -
PSVersion                      5.1.20348.1
PSEdition                      Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.20348.1
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1

PS C:\Users\Administrator>
```

Abbildung 5.1: Die PowerShell ist in der Version 5 standardmäßig auf allen Versionen des Windows-Servers zu finden.

In diesem Fenster steht Ihnen dann eine Kommandozeile zur Verfügung, an der Sie PowerShell-Befehle eingeben können. Diese werden dann direkt ausgeführt; Sie arbeiten interaktiv mit der Shell.



Standardmäßig werden Sie auf einem Windows Server 2019 die PowerShell in der Version 5.1 installiert vorfinden. Das trifft auch auf die Vorabversionen von Windows Server 2022 zu. Allerdings entwickelt Microsoft die PowerShell stetig weiter, sodass in der Zwischenzeit eine Open-Source-Variante in der Version 7.1 existiert. Ein großer Unterschied zur »alten« Standardversion besteht darin, dass diese Shell und die Skriptsprache auch auf anderen Plattformen wie Linux oder macOS eingesetzt werden kann. Wir beschränken uns hier bis auf wenige Ausnahmen auf die Standardvariante der PowerShell, wie Sie diese auf dem Windows-Server finden können. Wollen Sie aber auch in die Version 7 hineinschnuppern, so können Sie diese ab der Version Windows Server 2008 R2 problemlos parallel zur vorhandenen PowerShell auf dem Server installieren und nutzen. Sie finden die jeweils neueste Version auf GitHub unter der folgenden Adresse:

<https://github.com/PowerShell/PowerShell/releases>.

Wollen Sie eigene Skripte für Ihren Windows-Server entwickeln, die Sie später wiederverwenden oder auch weitergeben können, so ist das Arbeiten mit der *Windows PowerShell ISE* (Integrated Scripting Environment) deutlich einfacher. Sie erhalten mit der ISE eine Entwicklungsumgebung ([Abbildung 5.2](#)), wie Sie sie vielleicht schon von anderen Programmiersprachen her kennen. Sie können dieses Programm ebenfalls direkt aus dem Startmenü des Windows-Servers heraus aufrufen.

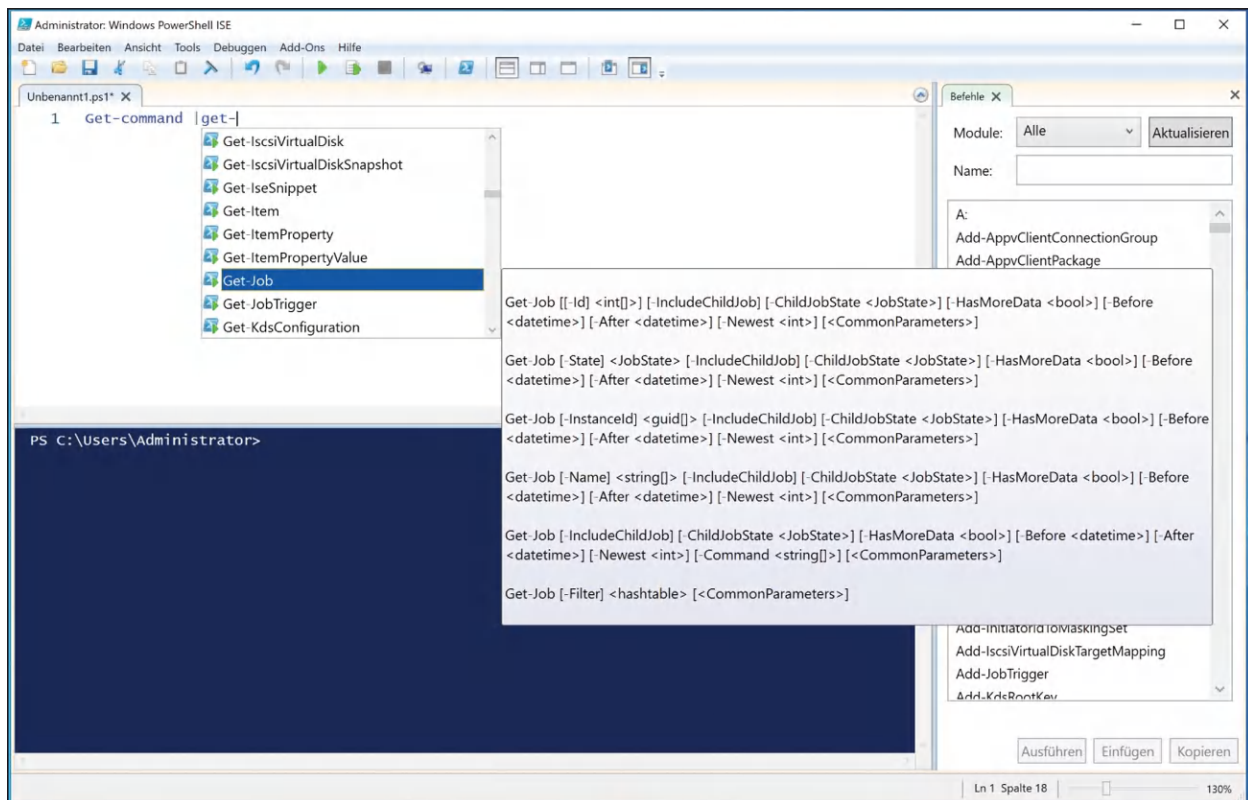


Abbildung 5.2: Die PowerShell ISE (Integrated Scripting Environment) ist ein mächtiges Werkzeug, das Sie beim Erstellen von Skripten unterstützt.



Gerade wenn Sie noch wenig oder keine Erfahrung mit der PowerShell haben, sollten Sie die ISE einsetzen. Obwohl auch in der Konsole eingegebene Befehle automatisch farbig dargestellt werden, geht die Unterstützung in der ISE doch viel weiter: Wenn Sie mit dem Eintippen von Befehlen und Anweisungen beginnen, versucht das Programm automatisch, die Eingabe zu ergänzen, sodass Sie im

Idealfall genau die Anweisung oder den Befehl (mit möglichen Parametern) angezeigt bekommen, den Sie für Ihr Skript benötigen.

Begriffe und Besonderheiten der PowerShell

Damit Sie die ersten Schritte mit der PowerShell auf Ihrem Windows-Server unternehmen können, möchten wir Ihnen zunächst einige Begrifflichkeiten und Besonderheiten der PowerShell vorstellen:

- ✓ *Objekte*: Die PowerShell arbeitet im Gegensatz zu den meisten konventionellen Skriptsprachen objektorientiert. Während Sie sich beispielsweise bei den Linux-Shells bei der Arbeit mit Systemkommandos immer wieder damit befassen müssen, deren Ausgaben als Texte zu ver- und bearbeiten, behandelt die PowerShell zum Beispiel die Windows-Dienste und -Prozesse mit ihren Ausgaben als Objekte. Das erleichtert deren Verarbeitung deutlich. Auch dadurch wird die PowerShell zum idealen Werkzeug für die systemnahe Arbeit auf einem Server.
- ✓ *Cmdlet*: Ein einzelner Befehl in der PowerShell heißt Commandlet (kurz Cmdlet). Ein solches Commandlet besteht typischerweise aus drei Teilen: einem Verb, einem Substantiv und einer (optionalen) Liste für Parameter. Dabei werden Verb und Substantiv mit einem Bindestrich verbunden. Die optionalen Parameter werden durch Leerzeichen davon abgetrennt. Ein solches Kommando besitzt dann also die grundsätzliche Form:

Verb-Substantiv [-Liste der Parameter]

Ein beispielhaftes Cmdlet, das alle PowerShell-Kommandos auf dem Server anzeigt, sieht dann so aus:

`get-command`

Das ist, wie Sie in der [Abbildung 5.3](#) sehen können, eine ziemlich lange Liste, die auch nicht auf eine Bildschirmseite passt. Die PowerShell arbeitet dabei nicht Case-sensitiv: Das bedeutet, dass sie

bei den Cmdlets nicht zwischen Groß- und Kleinschreibung unterscheidet.

CommandType	Name	Version	Source
Alias	Add-AppPackage	2.0.1.0	Appx
Alias	Add-AppPackageVolume	2.0.1.0	Appx
Alias	Add-AppProvisionedPackage	3.0	Dism
Alias	Add-ProvisionedAppPackage	3.0	Dism
Alias	Add-ProvisionedAppxPackage	3.0	Dism
Alias	Add-WindowsFeature	2.0.0.0	ServerManager
Alias	Apply-WindowsUnattend	3.0	Dism
Alias	Disable-PhysicalDiskIndication	2.0.0.0	Storage
Alias	Disable-StorageDiagnosticLog	2.0.0.0	Storage
Alias	Dismount-AppPackageVolume	2.0.1.0	Appx
Alias	Enable-PhysicalDiskIndication	2.0.0.0	Storage
Alias	Enable-StorageDiagnosticLog	2.0.0.0	Storage
Alias	Expand-IscsiVirtualDisk	2.0.0.0	IscsiTarget
Alias	Flush-Volume	2.0.0.0	Storage
Alias	Get-AppPackage	2.0.1.0	Appx
Alias	Get-AppPackageDefaultVolume	2.0.1.0	Appx
Alias	Get-AppPackageLastError	2.0.1.0	Appx
Alias	Get-AppPackageLog	2.0.1.0	Appx
Alias	Get-AppPackageManifest	2.0.1.0	Appx
Alias	Get-AppPackageVolume	2.0.1.0	Appx
Alias	Get-AppProvisionedPackage	3.0	Dism
Alias	Get-DiskSNV	2.0.0.0	Storage
Alias	Get-PhysicalDiskSNV	2.0.0.0	Storage
Alias	Get-ProvisionedAppPackage	3.0	Dism
Alias	Get-ProvisionedAppxPackage	3.0	Dism
Alias	Get-StorageEnclosureSNV	2.0.0.0	Storage
Alias	Get-WBVsBackupOptions	1.0.0.0	WindowsServerBackup
Alias	Initialize-Volume	2.0.0.0	Storage
Alias	Mount-AppPackageVolume	2.0.1.0	Appx
Alias	Move-AppPackage	2.0.1.0	Appx

Abbildung 5.3: Ein Aufruf des Cmdlets »get-command« bringt die standardmäßig auf dem Windows-Server vorhandenen Befehle auf den Bildschirm. Allerdings ist die Liste sehr lang.

- ✓ **Provider:** Die PowerShell-Provider stellen Ihnen in Skripten den Zugriff auch auf Daten und Komponenten des Betriebssystems bereit, auf die Sie ansonsten von der Befehlszeile aus nicht problemlos zugreifen können. Dabei werden die Daten in einheitlicher Form als Laufwerk dargestellt, sodass Nutzerinnen und Nutzer darauf mit den üblichen Kommandos navigieren und zugreifen können. Die PowerShell stellt unter anderem Provider für die Festplattenzugriffe und das Arbeiten mit der Windows Registry bereit.
- ✓ **Aliase:** Ein Alias ist ein alternativer Name für ein Cmdlet oder einen

Befehl in der PowerShell. Das auf Windows Server 2019 aktuelle Release der PowerShell umfasst mehr als 150 solcher Alias-Bezeichnungen. Wir haben in [Tabelle 5.1](#) einige dieser Kurznamen aufgeführt, die nicht zuletzt auch dazu dienen, Umsteigern von Unix-/Linux-Shells oder von der Eingabeaufforderung (`cmd.exe`) unter Windows den Einstieg zu erleichtern.

Alias	<i>Vollständiges Kommando</i>
cat	Get-Content
cd	Set-Location
cls	Clear-Host
cp	Copy-Item
dir	Get-ChildItem
pwd	Get-Location
ni	New-Item
write	Write-Output
where	Where-Object

[Tabelle 5.1](#): Ausgewählte Alias-Bezeichnungen in der PowerShell

- ✓ **Pipelines:** Die Pipelines sind ein wichtiges Element, das auch in anderen Shell-Implementierung beispielsweise unter Linux in der `bash` (Bourne-again shell) zum Einsatz kommt. Mithilfe dieses Mechanismus ist es Ihnen möglich, die Ausgabe des einen Cmdlets direkt an ein anderes Cmdlet zur Weiterverarbeitung zu übergeben. Dazu kommt der sogenannte Pipeline-Operator `»|«` zum Einsatz. Im Gegensatz zu den traditionellen Implementierungen der Pipeline, bei denen nur Zeichenketten weitergegeben werden können, ermöglicht die PowerShell die Weitergabe von Objekten mitsamt ihren Eigenschaften und Methoden, was die Flexibilität dieses Mechanismus noch einmal deutlich erhöht. Eine typische Befehlskette dieser Art sieht dann folgendermaßen aus:

```
get-service | get-member
```

Das Cmdlet `get-service` listet allein aufgerufen, also ohne weitere

Parameter, alle Dienste auf dem Windows-Server auf. Wird die Ausgabe hier ohne weitere Filter an das Cmdlet `get-member` weitergegeben, so listet dieses alle Methoden und Eigenschaften von `get-service` auf. Pipelines kommen gerade bei systemnahen Skripten oft auch in mehreren Stufen zum Einsatz, wobei es häufig darum geht, die Ausgaben zu filtern und zu formatieren. Die [Abbildung 5.4](#) zeigt diesen Aufruf und seine Ausgabe auf Windows Server 2019.

```

Windows PowerShell
PS C:\Users\micha> get-service | get-member

TypeName: System.ServiceProcess.ServiceController

Name      MemberType Definition
-----
Name      AliasProperty Name = ServiceName
RequiredServices AliasProperty RequiredServices = ServicesDependedOn
Disposed  Event        System.EventHandler Disposed(System.Object, System.EventArgs)
Close     Method       void Close()
Continue  Method       void Continue()
CreateObjRef Method       System.Runtime.Remoting.ObjRef CreateObjRef(type requestedType)
Dispose   Method       void Dispose(), void IDisposable.Dispose()
Equals    Method       bool Equals(System.Object obj)
ExecuteCommand Method       void ExecuteCommand(int command)
GetHashCode Method       int GetHashCode()
GetLifetimeService Method       System.Object GetLifetimeService()
GetType   Method       type GetType()
InitializeLifetimeService Method       System.Object InitializeLifetimeService()
Pause     Method       void Pause()
Refresh   Method       void Refresh()
Start     Method       void Start(), void Start(string[] args)
Stop      Method       void Stop()
WaitForStatus Method       void WaitForStatus(System.ServiceProcess.ServiceControllerStatus desiredStatus), void...
CanPauseAndContinue Property     bool CanPauseAndContinue {get;}
CanShutdown Property     bool CanShutdown {get;}
CanStop   Property     bool CanStop {get;}
Container Property     System.ComponentModel.IContainer Container {get;}
DependentServices Property     System.ServiceProcess.ServiceController[] DependentServices {get;}
DisplayName Property     string DisplayName {get;set;}
MachineName Property     string MachineName {get;set;}
ServiceHandle Property     System.Runtime.InteropServices.SafeHandle ServiceHandle {get;}
ServiceName Property     string ServiceName {get;set;}
ServicesDependedOn Property     System.ServiceProcess.ServiceController[] ServicesDependedOn {get;}
ServiceType Property     System.ServiceProcess.ServiceType ServiceType {get;}
Site      Property     System.ComponentModel.ISite Site {get;set;}
StartType Property     System.ServiceProcess.ServiceStartMode StartType {get;}
Status    Property     System.ServiceProcess.ServiceControllerStatus Status {get;}
ToString  ScriptMethod System.Object ToString();
  
```

Abbildung 5.4: Mithilfe des sehr flexiblen Pipeline-Mechanismus ist es leicht möglich, die Ausgabe eines Kommandos an ein anderes weiterzuleiten.

- ✓ **Module:** Obwohl die PowerShell schon standardmäßig mit sehr vielen Skripten und Möglichkeiten auf dem Windows-Server vorhanden ist, werden Sie immer wieder, gerade wenn Sie beginnen, mit Ihrem Server mehr Aufgabe zu erledigen, auf Bereiche stoßen, für die zunächst einmal keine Cmdlets zur Verfügung stehen. Ein Beispiel dafür ist die Arbeit mit dem Verzeichnisdienst Active Directory, für die in der Standardinstallation keine Unterstützung bereitsteht. Bei den Modulen handelt es sich um eine Sammlung von Funktionen, Befehlen

und Skriptdateien, die thematisch zusammengefasst und zumeist in einem einzigen Verzeichnis zu finden sind.

Module sind vor allem für Server wichtig, wenn diese mit unterschiedlichen Rollen und Features eingesetzt werden. Sie können dann die benötigten Module importieren und deren Befehlssatz verwenden. Mit dem Aufruf von

```
Get-Module -ListAvailable
```

werden die zur Verfügung stehenden Module aufgelistet. Lassen Sie dabei `-ListAvailable` weg, so werden nur die in der aktuellen Sitzung geladenen Module angezeigt.

Erste Schritte zum eigenen Skript

PowerShell-Skripte können Ihnen dabei helfen, monotone alltägliche Aufgabe, die bei der Verwaltung und Betreuung eines Windows-Servers anfallen, zu automatisieren und häufig auch zu vereinfachen. Sie finden im Web sehr viele Sammlungen solcher Skripte und Beispiellösungen für viele Einsetzmöglichkeiten rund um den Server. Doch gibt es eben immer wieder Aufgaben, die es gilt, individuell zu lösen – ein eigenes Skript muss her. Damit Sie selbst PowerShell-Skripte entwickeln können, zeigen wir Ihnen in diesem Abschnitt die wichtigsten Daten- und Kontrollstrukturen, die Sie dafür verwenden können. Diese Beschreibung ist weder vollständig, noch kann sie einen kompletten Programmierkursus bieten, sondern sie stellt einen Einstieg in die Entwicklung eigener Skripte dar.

Einige Informationen zu Objekten

Keine Angst – wir werden Ihnen hier keine langen theoretischen Erläuterungen zur Objektorientierung unterbreiten. Wir möchten Ihnen nur ein weiteres Mal vor Augen führen, dass Sie in der PowerShell – ganz gleich, ob Sie »nur« Einzeiler an der Kommandozeile verfassen oder umfangreiche Skripte entwickeln – immer mit Objekten umgehen. Weshalb wir im folgenden Abschnitt einige gängige Objekt und Beispiele für das Arbeiten mit ihnen vorstellen.

- ✓ *Attribute und Methoden:* Immer dann, wenn es um Objekte geht, werden Sie auch die Begriffe Attribute (oder auch Eigenschaften) und Methoden hören. Attribute sind die Eigenschaften eines Objekts. Sie sagen also, wie ein Objekt ist, ob beispielsweise grün oder blau, groß oder klein beziehungsweise einfach nur eine Zeichenkette oder eine Zahl. Methoden sind hingegen Funktionen, die Ihnen sagen, was Sie mit diesem Objekt tun können. Das Cmdlet `Get-Member` zeigt Ihnen die Attribute und Methoden eines Objekts an. Der folgende Aufruf listet die Attribute von `Get-Date` auf, ein Cmdlet, das Systemuhrzeit und -datum in einem entsprechenden Objekt bereitstellt:

```
Get-Date | Get-Member -Membertyp Property
```

Ohne `-Membertyp` würde der Aufruf auch alle Methoden mit auflisten, die Sie auf dieses Objekt anwenden können. Das folgende Beispiel zeigt den Aufruf der Methode `.dayofweek`, mit deren Hilfe der Wochentag eines Datums abgefragt werden kann. Methoden werden immer mit einem Punkt vor dem Methodennamen aufgerufen:

```
(Get-Date -Year 1961 -Month 04 -day 04).dayofweek
```

Sie können diese Ausgabe auch in der folgenden Form aufrufen, die etwas deutlicher zeigt, dass hier auf ein bestimmtes Objekt zugegriffen wird:

```
Get-Date -Year 1961 -Month 04 -Day 04 | Select-Object dayofweek
```

Die Ausgaben dieser Aufrufe können Sie in der [Abbildung 5.5](#) sehen. Diese Beispiele haben wir der PowerShell-Dokumentation von Microsoft entnommen.

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-Date | Get-Member -MemberType Property

TypeName: System.DateTime

Name      MemberType Definition
-----
Date      Property  datetime Date {get;}
Day       Property  int Day {get;}
DayOfWeek Property  System.DayOfWeek DayOfWeek {get;}
DayOfYear Property  int DayOfYear {get;}
Hour      Property  int Hour {get;}
Kind      Property  System.DateTimeKind Kind {get;}
Millisecond Property int Millisecond {get;}
Minute    Property  int Minute {get;}
Month     Property  int Month {get;}
Second    Property  int Second {get;}
Ticks     Property  long Ticks {get;}
TimeOfDay Property  timespan TimeOfDay {get;}
Year      Property  int Year {get;}

PS C:\Users\Administrator> (Get-Date -Year 1961 -Month 04 -day 04).dayofweek
Tuesday
PS C:\Users\Administrator> Get-Date -Year 1961 -Month 04 -Day 04 | Select-Object dayofweek

DayOfWeek
-----
Tuesday
```

Abbildung 5.5: Attribute und Methoden erlauben den Zugriff auf die jeweiligen Eigenschaften und Funktionen eines Objekts.

- ✓ **Variablen:** Wie jede andere Programmiersprache benötigt auch die PowerShell Variablen als Container für Daten aller Art. Das reicht von Zahlen über Zeichenketten bis hin zu Kommandos. Auch bei den Variablenamen unterscheidet die PowerShell nicht zwischen Groß- und Kleinschreibung. Diese Namen können dabei auch Sonderzeichen enthalten. Microsoft rät allerdings davon ab, diese zu nutzen, und gibt die Empfehlung, sich bei Variablenamen auf alphanumerische Zeichen und den Unterstrich »_« zu beschränken. Sie werden feststellen, dass in den meisten Skripten die Variablenamen mit einem Großbuchstaben beginnen. Das müssen Sie nicht tun, wir haben allerdings festgestellt, dass diese Vorgehensweise zur Lesbarkeit eines Skripts beiträgt. Eine explizite Deklaration, wie sie in einigen Skript- und Programmiersprachen notwendig ist, müssen Sie in der PowerShell nicht vornehmen: Sie können Variablen zu jeder Zeit innerhalb eines Skripts anlegen. Das geschieht mithilfe des Dollar-Zeichens »\$«. Ein korrekter Dateiname kann dann so aussehen:

\$Var_1

Rufen Sie eine Variable auf diese Weise auf, so wird die PowerShell Ihnen ihren aktuellen Inhalt auf dem Bildschirm anzeigen. Mit folgenden Zuweisungen legen Sie Werte in der Variablen ab:

```
$Var_1 = 42  
$Var_1 = "Test"
```

Dabei wird der Typ der Variablen durch den zugewiesenen Wert bestimmt – im zweiten Fall wird der vorherige numerische Wert durch eine Zeichenkette überschrieben. Die [Abbildung 5.6](#) zeigt Ihnen, wie das dann auf der Kommandozeile der PowerShell aussieht.

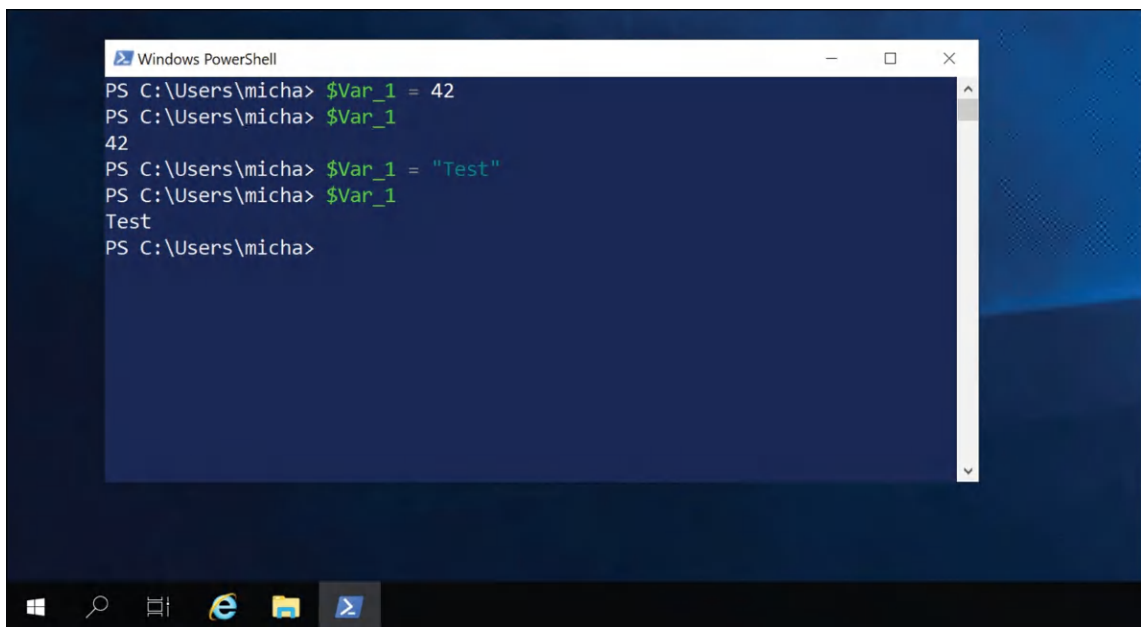
A screenshot of a Windows PowerShell window. The title bar reads 'Windows PowerShell'. The command prompt shows the following sequence of commands and outputs:
PS C:\Users\micha> \$Var_1 = 42
PS C:\Users\micha> \$Var_1
42
PS C:\Users\micha> \$Var_1 = "Test"
PS C:\Users\micha> \$Var_1
Test
PS C:\Users\micha>
The window has a dark blue background. The taskbar at the bottom shows the Start button, search, task view, and several application icons including Edge, File Explorer, and PowerShell.

Abbildung 5.6: Die Arbeit mit Variablen in der PowerShell ist einfach. Dabei überschreibt eine neue Zuweisung Typ und Wert des vorherigen Inhalts.

- ✓ **Array:** Eine weitere Datenstruktur, die in fast jeder Programmiersprache anzutreffen ist, wird als Array bezeichnet. Dabei handelt es sich um einen Datentyp, der es Ihnen ermöglicht, zusammengehörige Werte in einer Variablen zu versammeln. Diese können Sie dann über einen Index ansprechen. Eine einfache Zuweisung läuft dabei folgendermaßen ab:

```
$Buchstaben = "A", "B", "C", "X", "Z"
```

Wobei wir hier als Datentyp einzelne Zeichen verwenden, die wir jeweils in Hochkommas einschließen. Durch den einfachen Aufruf

von `$Buchstaben` bekommen Sie dann den Inhalt des Arrays angezeigt, wie Sie in [Abbildung 5.7](#) sehen können. Da das Objekt Array die Methode `.count` kennt, können Sie mit ihrer Hilfe beispielsweise nun die Anzahl der Elemente im Array anzeigen lassen:

```
$Buchstaben.count
```

Ein Array arbeitet mit einem Index, mit dessen Hilfe Sie direkt auf einzelne Elemente zugreifen können. Dabei zeigt Ihnen der Aufruf von

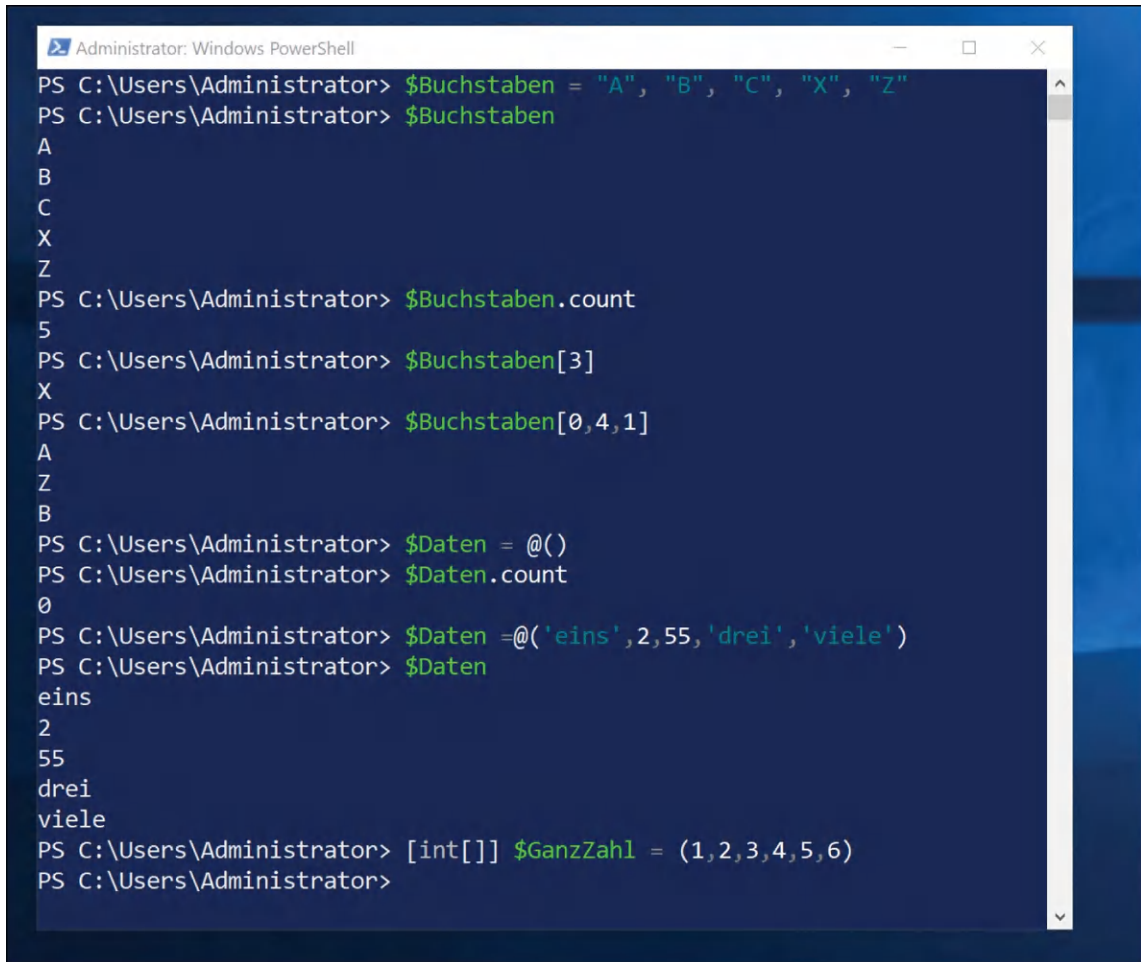
```
$Buchstaben[3]
```

das vierte Element »X« des Arrays an, da die interne Zählung wie bei vielen Programmiersprachen mit dem Element »0« beginnt. Deshalb zeigt der Aufruf

```
$Buchstaben[0, 4, 1]
```

dann auch die Elemente »A«, »Z« und »B« an. Wollen Sie ein leeres Array zum späteren Befüllen anlegen, so müssen Sie dazu die folgende Schreibweise wählen:

```
$Daten = @()
```

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window has a dark blue background with white text. The command prompt shows several commands and their outputs. First, an array of letters is created and displayed. Then, the count of elements is shown. Next, an element at a specific index is retrieved. Then, a range of elements is retrieved. After that, an empty array is created and its count is shown. Finally, an array of mixed data types is created and displayed. The last command shows the declaration of an integer array, but its output is not shown.

```
PS C:\Users\Administrator> $Buchstaben = "A", "B", "C", "X", "Z"
PS C:\Users\Administrator> $Buchstaben
A
B
C
X
Z
PS C:\Users\Administrator> $Buchstaben.count
5
PS C:\Users\Administrator> $Buchstaben[3]
X
PS C:\Users\Administrator> $Buchstaben[0,4,1]
A
Z
B
PS C:\Users\Administrator> $Daten = @()
PS C:\Users\Administrator> $Daten.count
0
PS C:\Users\Administrator> $Daten = @('eins',2,55,'drei','viele')
PS C:\Users\Administrator> $Daten
eins
2
55
drei
viele
PS C:\Users\Administrator> [int[]] $GanzZahl = (1,2,3,4,5,6)
PS C:\Users\Administrator>
```

Abbildung 5.7: Die Arrays stellen Ihnen eine Datenstruktur bereit, die es ermöglicht, zusammengehörige Werte in einer Variablen zu versammeln.

Wie Sie in den Beispielen in der [Abbildung 5.7](#) sehen können, ist es auch möglich, einem solchen Array »gemischte« Datentypen, also Zeichenketten und Zahlen zuzuweisen. Möchten Sie ein Array anlegen, dass nur einen bestimmten Datentyp, wie beispielsweise Ganzzahlen (Integers) aufnehmen kann, so müssen Sie hier eine Deklaration für Ihr Array vornehmen:

```
[int[]] $GanzZahl = (1,2,3,4,5,6)
```

Versuchen Sie dann, diesem Array beispielsweise eine Zeichenkette zuzuweisen, wird die PowerShell mit einer Fehlermeldung reagieren.

Wichtig für viele Zwecke: Vergleichsoperatoren

Operatoren und logische Ausdrücke werden Sie ebenfalls in fast jeder

Programmiersprache finden. So ist beispielsweise die Steuerung eines Programmablaufs innerhalb eines Skripts in vielen Fällen nicht ohne Vergleichsoperatoren zu realisieren. Allerdings kommen bei der PowerShell hier nicht die in vielen anderen Skript- und Programmiersprachen für Vergleiche genutzten Zeichen wie »>«, »<« oder »=« zum Einsatz, sondern es werden Abkürzungen der jeweiligen englischen Begriffe verwendet, die von einem Bindestrich angeführt werden. [Tabelle 5.2](#) gibt Ihnen einen Überblick darüber.

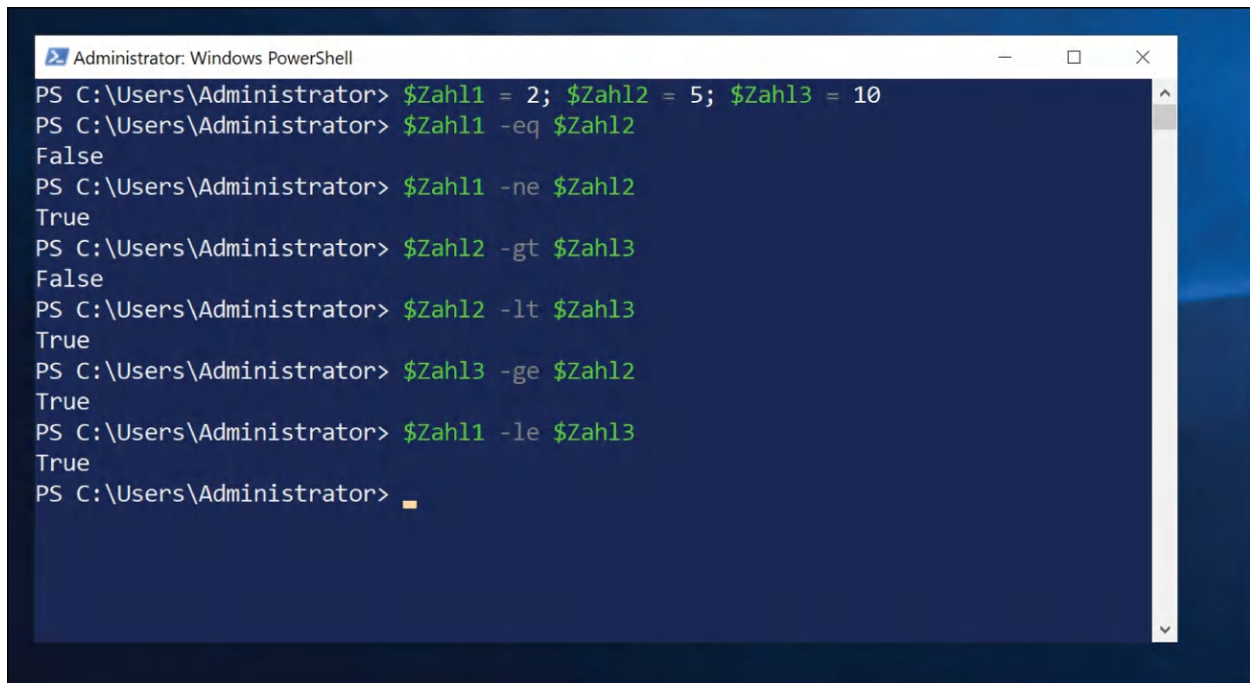
PowerShell-Operator	steht für
-gt	größer als (greater than)
-ge	größer als oder gleich (greater than or equal)
-lt	kleiner als (less than)
-le	kleiner als oder gleich (less than or equal)
-eq	ist gleich (equal)
-ne	ist nicht gleich (not equal)

Tabelle 5.2: Vergleichsoperatoren der PowerShell

Hat man sich erst einmal an die zunächst etwas ungewöhnliche Schreibweise gewöhnt, gehen Vergleiche in der PowerShell schnell von der Hand.

```
$Zahl1 = 2; $Zahl2 = 5; Zahl3 = 10
$Zahl1 -eq $Zahl2
False
```

Dieses Beispiel zeigt Ihnen nicht nur, dass Sie mehrere Variablen in einer Zeile zuweisen können, wenn Sie diese Zuweisungen durch ein Semikolon »;« trennen, sondern auch, wie Sie einen Vergleichsoperator grundsätzlich einsetzen können. In der [Abbildung 5.8](#) finden Sie dieses Beispiel mit weiteren Operatoren weiter ausgeführt. Die PowerShell gibt als Ergebnis eines solchen Vergleichs dann entweder `False` oder `True` aus, je nachdem ob der Vergleich zutreffend ist oder nicht. Diesen Rückgabewert können Sie dann entsprechend weiterverwenden, zum Beispiel bei Programmverzweigungen.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> $Zahl1 = 2; $Zahl2 = 5; $Zahl3 = 10
PS C:\Users\Administrator> $Zahl1 -eq $Zahl2
False
PS C:\Users\Administrator> $Zahl1 -ne $Zahl2
True
PS C:\Users\Administrator> $Zahl2 -gt $Zahl3
False
PS C:\Users\Administrator> $Zahl2 -lt $Zahl3
True
PS C:\Users\Administrator> $Zahl3 -ge $Zahl2
True
PS C:\Users\Administrator> $Zahl1 -le $Zahl3
True
PS C:\Users\Administrator>
```

Abbildung 5.8: Mithilfe der Vergleichsoperatoren können Sie logische Abfragen und Überprüfungen durchführen.

Natürlich stehen Ihnen auch Operatoren zur Verfügung, mit deren Hilfe sie Muster vergleichen können (das sogenannte »Pattern Matching«). Diese kommen dann zum Einsatz, wenn Sie Zeichenketten vergleichen wollen oder müssen. Beachten Sie dabei bitte, dass Sie Zeichenketten in der Regel mit einfachen »'« oder doppelten Anführungszeichen »"« einschließen müssen, damit die PowerShell sie auch als solche behandelt. Als Beispiele dafür haben wir die Operatoren `-like` und `-match` gewählt. Bei dieser Art der Vergleiche wird sehr häufig mit Wildcards gearbeitet. Dabei steht das Zeichen »*« für beliebig viele oder auch kein Zeichen, während das Fragezeichen »?« in der Vergleichszeichenkette dann für genau ein Zeichen steht.

```
$Teststring = "Windows"
$Teststring -like "W*"
True
```

Mithilfe von `-notlike` wird die Aussage dann bei fehlender Übereinstimmung als wahr gewertet:

```
$Teststring -notlike "Linux"
True
```


Während Sie bei der Verwendung von `-like` und dem Einsatz von Wildcards die Position der gesuchten Zeichen kennen sollten, können Sie mit `-match` feststellen, ob die eine Zeichenkette einfach nur ein Teil unabhängig von der Position im untersuchten String ist:

```
$Teststring -match "ind"  
True
```

Auch hier steht Ihnen mit `-nomatch` wieder die Möglichkeit zur Verfügung, die logische Abfrage umzukehren. Alle diese Operatoren unterscheiden standardmäßig, wie es in der PowerShell üblich ist, nicht zwischen Groß- und Kleinschreibung. Wünschen Sie eine Überprüfung, die »Case-sensitiv« arbeitet und diese Unterscheidung beachtet, so stehen Ihnen die entsprechenden cmdlets mit einem »c« im ansonsten unveränderten Namen zur Verfügung:

```
$Teststring -clike "windows"  
False
```

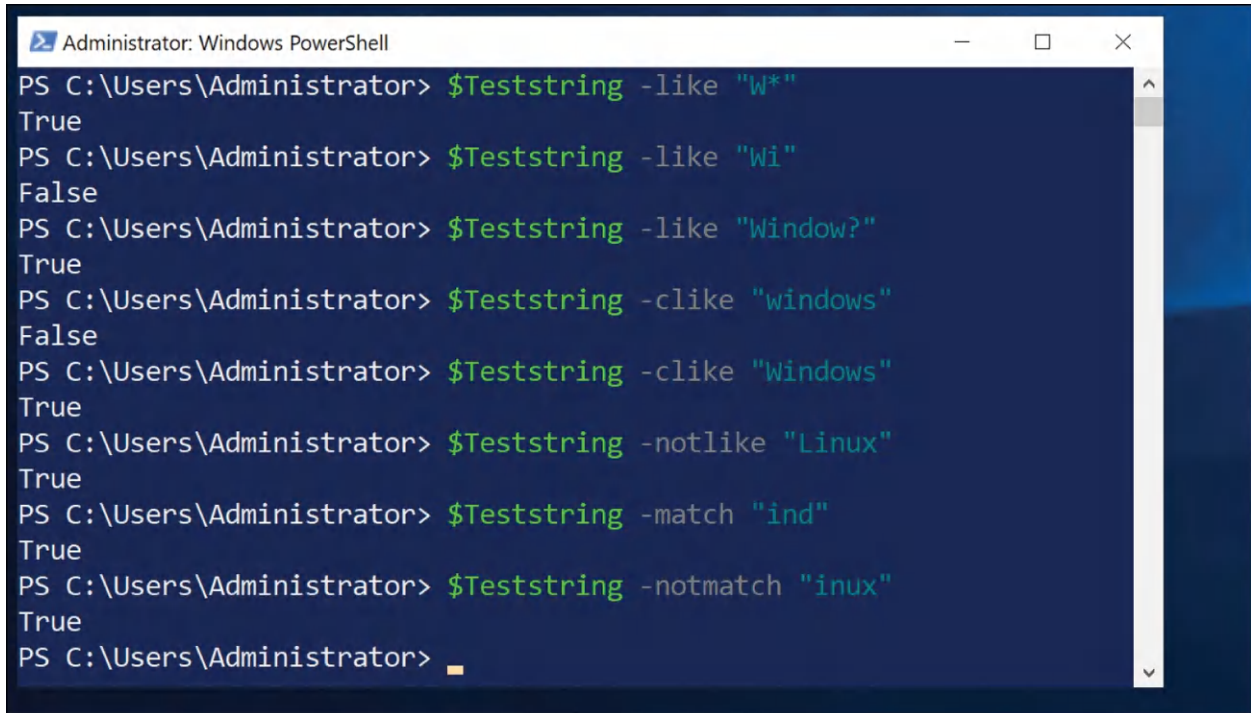
Die [Abbildung 5.9](#) zeigt Ihnen diese unterschiedlichen Aufrufe in der Übersicht.

Eine umfassende Auflistung aller Operatoren, die Sie in der PowerShell auch in der neuen Version 7.1 einsetzen können, stellt Ihnen Microsoft unter https://docs.microsoft.com/de-de/powershell/module/microsoft.powershell.core/about/about_operators zusammen mit entsprechenden Beispielen bereit.



Wenn Sie sich weiter mit dem Thema Mustererkennung und Vergleich von Zeichenketten befassen, werden Sie es irgendwann nicht mehr vermeiden können, sich mit den »regulären Ausdrücken« (kurz auch als »Regex« bezeichnet) zu befassen. Dabei handelt es sich um Zeichenketten auf Basis syntaktischer Regeln, die es Ihnen ermöglichen, Zeichenfolgen zu beschreiben. Wenn Sie schon mit Linux-/Unix-Systemen und deren Shell-Skripten gearbeitet haben, werden Sie diese Art von zunächst sehr kryptisch scheinenden Angaben schon kennen:

```
$Eingabe -match "^\\d{3}\\w{4,8}$"
```



```
PS C:\Users\Administrator> $Teststring -like "W*"
True
PS C:\Users\Administrator> $Teststring -like "Wi"
False
PS C:\Users\Administrator> $Teststring -like "Window?"
True
PS C:\Users\Administrator> $Teststring -clike "windows"
False
PS C:\Users\Administrator> $Teststring -clike "Windows"
True
PS C:\Users\Administrator> $Teststring -notlike "Linux"
True
PS C:\Users\Administrator> $Teststring -match "ind"
True
PS C:\Users\Administrator> $Teststring -notmatch "inux"
True
PS C:\Users\Administrator>
```

Abbildung 5.9: Mithilfe der unterschiedliche cmdlets zum Mustervergleich können Sie die Inhalte von Zeichenketten logisch abprüfen.

Dieser Aufruf stellte zum Beispiel sicher, dass in die Variable `$Eingabe` nur Daten, die aus drei Ziffern gefolgt von mindestens vier, aber nicht mehr als acht Buchstaben bestehen, hineingelangen. Eine Einführung in die Arbeit mit den regulären Ausdrücken, wie sie in der PowerShell unterstützt werden, würde den Rahmen dieses Buchs zweifelsohne sprengen. Sie finden aber auf im Web sehr viele Anleitungen und Beispiele, die erläutern, wie Sie mit deren Hilfe Vergleiche durchführen oder auch Werte und Zeichen ersetzen können. Unter der URL <https://bit.ly/2P19qJV> finden Sie auch einen umfassenden Artikel als Einführung in dieses Thema, den wir als Autorenteam für die Computerwoche verfasst haben.

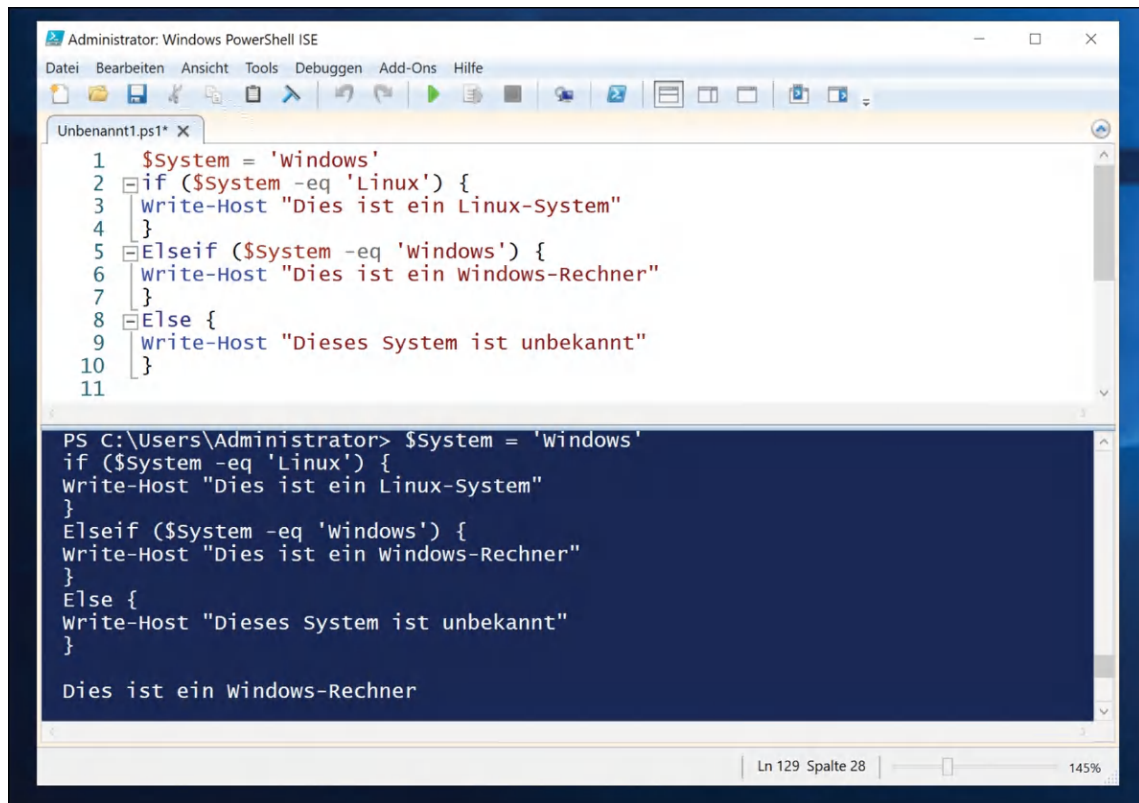
Verzweigungen und Schleifen

Ganz gleich, mit welcher Programmier- oder Skriptsprache Sie sich auseinandersetzen: Sie benötigen Kontrollstrukturen wie Schleifen, die es Ihnen erlauben, den Ablauf Ihres Programms in die richtigen Bahnen zu

lenken. Da macht die PowerShell keine Ausnahmen:

- ✓ *Die if-Anweisung:* In vielen Skripten werden Sie auf Situationen stoßen, in denen eine Entscheidung darüber zu treffen ist, welche Programmschritte im Ablauf als Nächstes ausgeführt werden sollen. Das wird als bedingte Entscheidung bezeichnet und kann mithilfe der `if`-Anweisung umgesetzt werden. Die Bedingung für die Anweisung wird dabei in Klammern gesetzt, während die auszuführenden Programmschritte in geschweifte Klammern eingeschlossen werden. Das folgende Listing, dessen Ablauf und Ausgabe Sie in der [Abbildung 5.10](#) sehen, zeigt den grundsätzlichen Einsatz der `if`-Anweisung:

```
$System = 'Windows'
If ($System -eq 'Linux') {
Write-Host "Diese ist ein Linux-System"
}
Elseif ($System -eq 'Windows') {
Write-Host "Dies ist ein Windows-Rechner"
}
Else {
Write-Host "Dieses System ist unbekannt"
```



```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

Unbenannt1.ps1* X
1 $System = 'windows'
2 if ($System -eq 'Linux') {
3     Write-Host "Dies ist ein Linux-System"
4 }
5 elseif ($System -eq 'windows') {
6     Write-Host "Dies ist ein windows-Rechner"
7 }
8 else {
9     Write-Host "Dieses System ist unbekannt"
10 }
11

PS C:\Users\Administrator> $System = 'windows'
if ($System -eq 'Linux') {
Write-Host "Dies ist ein Linux-System"
}
elseif ($System -eq 'windows') {
Write-Host "Dies ist ein windows-Rechner"
}
else {
Write-Host "Dieses System ist unbekannt"
}

Dies ist ein windows-Rechner

Ln 129 Spalte 28 145%
```

Abbildung 5.10: Ein einfaches Beispiel für eine »if«-Verzweigung in einem PowerShell-Skript

Wir haben für dieses Beispiel die PowerShell ISE gewählt, wie Sie ebenfalls in der [Abbildung 5.10](#) sehen können. Dabei zeigt Ihnen das Beispiel unter anderem auch, wie Programmblöcke mithilfe der geschweiften Klammern eingesetzt werden. Weiterhin haben wir in diesem Beispiel das Cmdlet `Write-Host` eingesetzt, das es uns erlaubt, Meldungen auf dem Bildschirm auszugeben. In der Klammer hinter der `if`-Anweisung vergleicht die PowerShell zunächst den Inhalt der Variablen `$System` mit der Zeichenkette `'Linux'`. Fällt der Vergleich (wie in diesem Fall) negativ aus, so geht der Programmablauf bei der nächsten Anweisung – hier ein `elseif` – weiter. Trifft der Vergleich zu, so wird der Programmblock innerhalb der geschweiften Klammern dahinter ausgeführt. Würde dieser Vergleich auch negativ ausfallen, so würde die PowerShell schließlich die Anweisung im Programmblock hinter `else` ausführen. Eine `if`-Anweisung kann beliebig viele `elseif`-Anweisung samt Programmblöcken, aber nur eine `else`-Anweisung haben. Sie können aber auch komplett auf eine `Else`- oder `Elseif`-

Anweisung verzichten.



Achten Sie dabei immer auf die korrekte Umsetzung der Logik: Trifft eine Abfrage hinter der `if`-Anweisung niemals zu, so werden die Anweisungen im Programmblock dahinter auch nie ausgeführt werden.

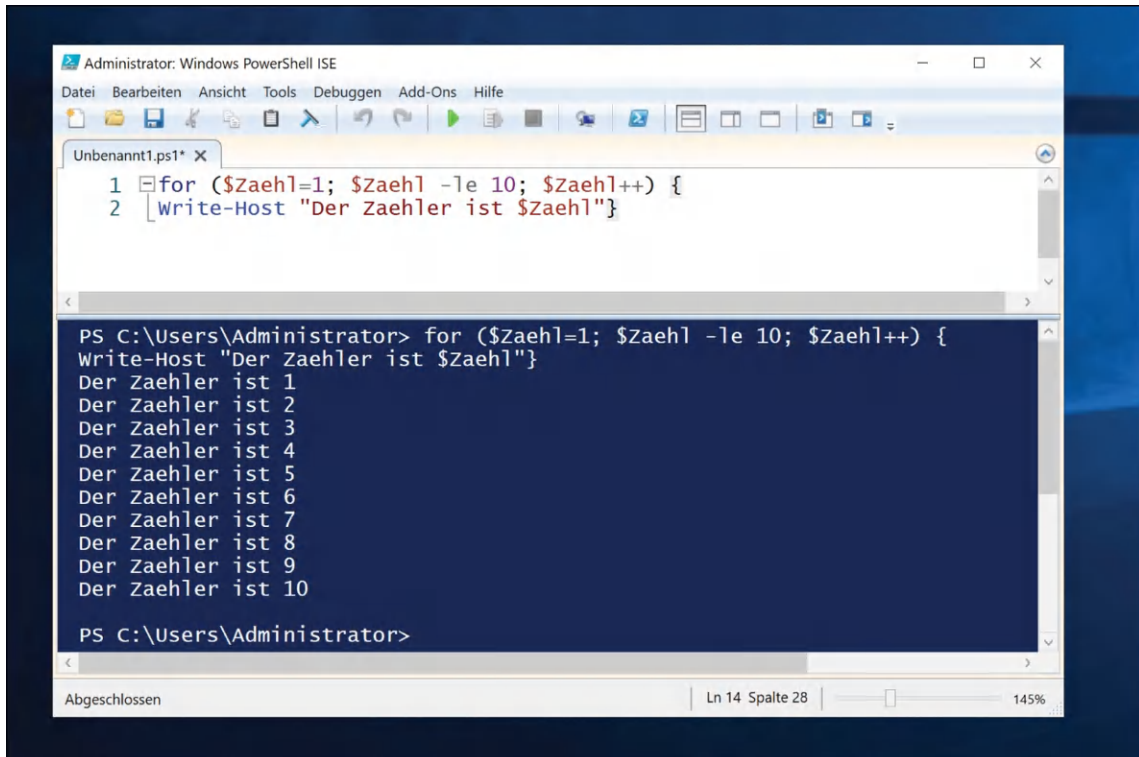
- ✓ *Die For- und Foreach-Anweisung:* Eine For-Schleife ist in fast jeder Programmiersprache zu finden. Sie führt grundsätzlich einen bestimmten Befehl oder auch eine ganze Folge von Befehlen und Programmschritten aus, bis ein bestimmter Wert erreicht ist oder eine bestimmte Situation eintritt. Die Schleife überprüft nach jedem Durchlauf, ob die Abbruch- beziehungsweise Ende-Bedingung erreicht ist, und benötigt einen Start- sowie einen Endwert, um zu funktionieren. Der grundsätzliche Aufruf einer For-Schleife besitzt dabei die folgende Form

`For (Startwert; Laufbedingung; Laufvariable)`

Ein Beispiel dafür:

```
For ($Zaehl = 1; $Zaehl -le 10; $Zaehl++) {  
  Write-Host "Der Zaehler ist $Zaehl" }
```

In diesem einfachen Aufruf wird zunächst die Variable `$Zaehl` mit dem Wert »1« initialisiert. Die Schleife soll so lange laufen, wie der Wert in dieser Variablen kleiner oder gleich »10« ist. Mithilfe des Inkrement-Operator »++« zählen wir den Wert der Laufvariablen hoch. Dabei steht `$Zaehl++` für `$Zaehl = $Zaehl +1`. Der Wert wird also jedes Mal um »1« erhöht. Aufruf und Ablauf dieser Schleife sind in der [Abbildung 5.11](#) zu sehen.

The image shows a screenshot of the Windows PowerShell ISE (Integrated Scripting Environment) running as Administrator. The title bar reads "Administrator: Windows PowerShell ISE". The menu bar includes "Datei", "Bearbeiten", "Ansicht", "Tools", "Debuggen", "Add-Ons", and "Hilfe". The toolbar contains various icons for file operations and execution. The script editor shows a file named "Unbenannt1.ps1" with two lines of PowerShell code:

```
1 for ($Zaehl=1; $Zaehl -le 10; $Zaehl++) {  
2   Write-Host "Der Zaehler ist $Zaehl"}  
3
```

The console window below shows the execution of this script. The prompt is "PS C:\Users\Administrator>". The output consists of ten lines, each displaying "Der Zaehler ist" followed by a number from 1 to 10. The prompt returns to "PS C:\Users\Administrator>". The status bar at the bottom indicates "Abgeschlossen" (Completed), "Ln 14 Spalte 28", and a zoom level of "145%".

Abbildung 5.11: Eine einfache »For«-Schleife, die deren grundsätzliche Funktionsweise sehr schön demonstriert.

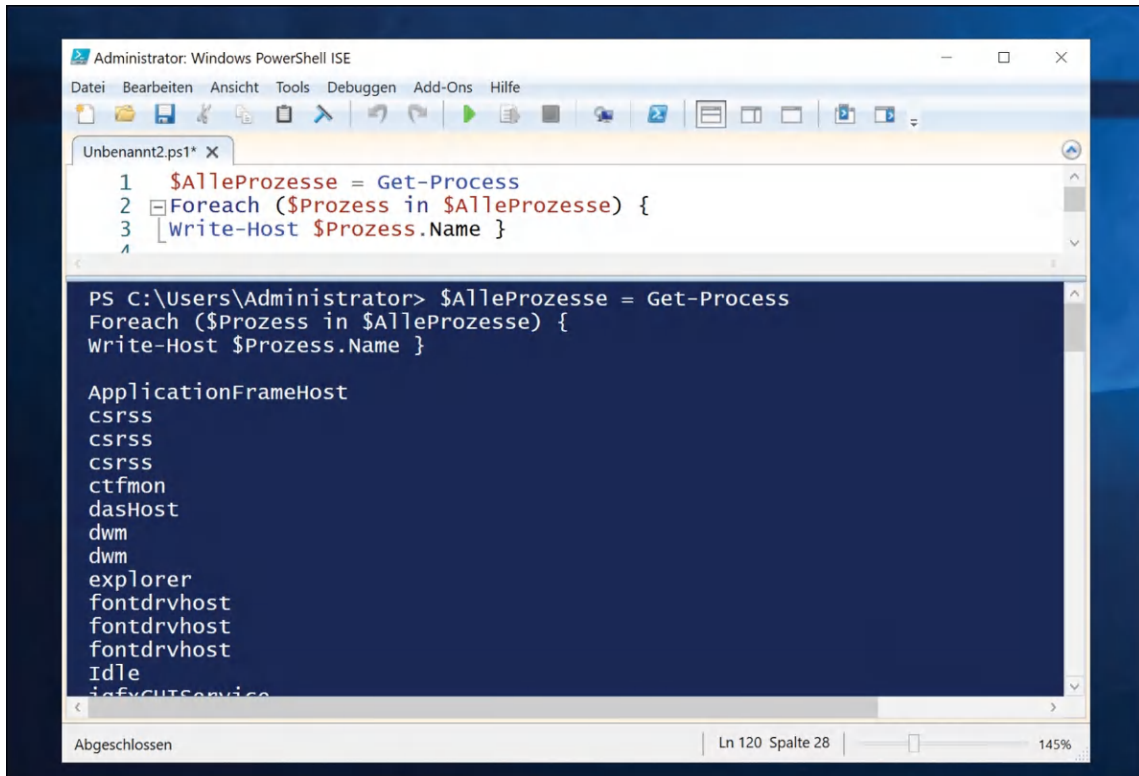
Mit der `foreach`-Schleife steht Ihnen eine weitere Ausprägung dieses Steuerungselements zur Verfügung, das sich besonders gut dafür eignet, um beispielsweise alle Objekte in einem Array abzuarbeiten und beispielsweise jeweils ein spezielles Attribut abzuarbeiten:

```
$AlleProzesse = Get-Process
```

Alle auf dem Server aktiven Prozesse (beziehungsweise die sie repräsentierenden Objekte) werden im Array `$AlleProzesse` abgespeichert.

```
Foreach ($Prozess in $AlleProzesse) {  
  Write-Host $Prozess.Name }  
}
```

Die Schleife übergibt in jedem Durchlauf jeweils ein Objekt an die Variable `$Prozess`, von der dann mittels `write-Host` jeweils das Attribut `Name` angezeigt wird. Sie sehen diesen Aufruf in der [Abbildung 5.12](#). Probieren Sie diese Art der Schleifen aus, um ein Gefühl dafür zu bekommen, wie diese arbeiten.



```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

Unbenannt2.ps1* X
1 $AlleProzesse = Get-Process
2 Foreach ($Prozess in $AlleProzesse) {
3   Write-Host $Prozess.Name }

PS C:\Users\Administrator> $AlleProzesse = Get-Process
Foreach ($Prozess in $AlleProzesse) {
Write-Host $Prozess.Name }

ApplicationFrameHost
csrss
csrss
csrss
ctfmon
dasHost
dwm
dwm
explorer
fontdrvhost
fontdrvhost
fontdrvhost
Idle
igfxCUIService
```

Abbildung 5.12: Die Variante »Foreach« der »For«-Schleife eignet sich besonders gut dafür, Objekte und deren Eigenschaften aus einem Array abzuarbeiten.



Ein beliebter Fehler bei der Verwendung von Schleifen jeder Art ist die Verwechslung einer Zuweisung mit einem Vergleich. Deshalb hier die Erinnerung: Das Zeichen »=«, das im gewöhnlichen Sprachgebrauch auch als »ist gleich« bezeichnet wird, stellt in der PowerShell eine reine Zuweisung dar.

```
$Zaehl = 1
```

weist der Variablen \$Zaehl den Wert »1« zu. Vergleiche jeder Art von Werten oder Bedingungen müssen mit den Vergleichsoperatoren wie -le durchgeführt werden.

```
$Zaehl -le 10
```

vergleicht, ob der Wert in \$Zaehl kleiner oder gleich »10« ist. Wenn also einmal eine Schleife in Ihrem PowerShell-Skript nicht so wie gedacht funktioniert, überprüfen Sie zunächst einmal, ob die Operatoren und Zuweisung richtig sind.

- ✓ Die *While-Anweisung*: Bei der **while**-Schleife handelt es sich um eine sogenannte »abweisende« Schleife. Das bedeutet: Wird die Schleifenbedingung vor dem ersten Durchlauf nicht erfüllt, so werden die Befehle im Schleifenkörper auch nicht ausgeführt. Bei der **while**-Schleife benötigen Sie in den Klammern hinter dem Schlüsselwort auch nur eine Bedingung:

```
$Wert = 9
while ($Wert -gt 0) {
Write-Host "Der Wert ist $Wert"
$Wert--}
```

Dieses sehr einfache Beispiel, das Sie auch in [Abbildung 5.13](#) sehen, zeigt die wichtigsten Punkte beim Einsatz der **while**-Schleife: Sie müssen sicherstellen, dass die Laufvariable einen Startwert hat, der es erlaubt, den Schleifenkörper auszuführen. Zudem müssen Sie dafür sorgen, dass Sie in der Schleife diesen Wert so verändern, dass die Schleife irgendwann auch abbricht. Ansonsten laufen Sie Gefahr, dass Ihr Skript in eine Endlosschleife läuft. Das haben wir hier durch Einsatz des Dekrement-Operators » --« verhindert, der für `$Wert = $Wert -1` steht und dadurch heruntergezählt wird, bis er »0« erreicht und der Schleifenkörper nicht mehr ausgeführt wird.

In der PowerShell stehen Ihnen noch weitere Schleifentypen und Konstrukte zur Verfügung, die Ihnen dabei helfen, den Programmablauf in Ihren Skripten zu kontrollieren und zu steuern. In der Onlinedokumentation von Microsoft zur PowerShell finden Sie unter dem Eintrag »Flusssteuerung« <https://docs.microsoft.com/de-de/powershell/scripting/learn/ps101/06-flow-control?view=powershell-7.1> alle Möglichkeiten zusammen mit entsprechenden Beispielskripten aufgelistet.

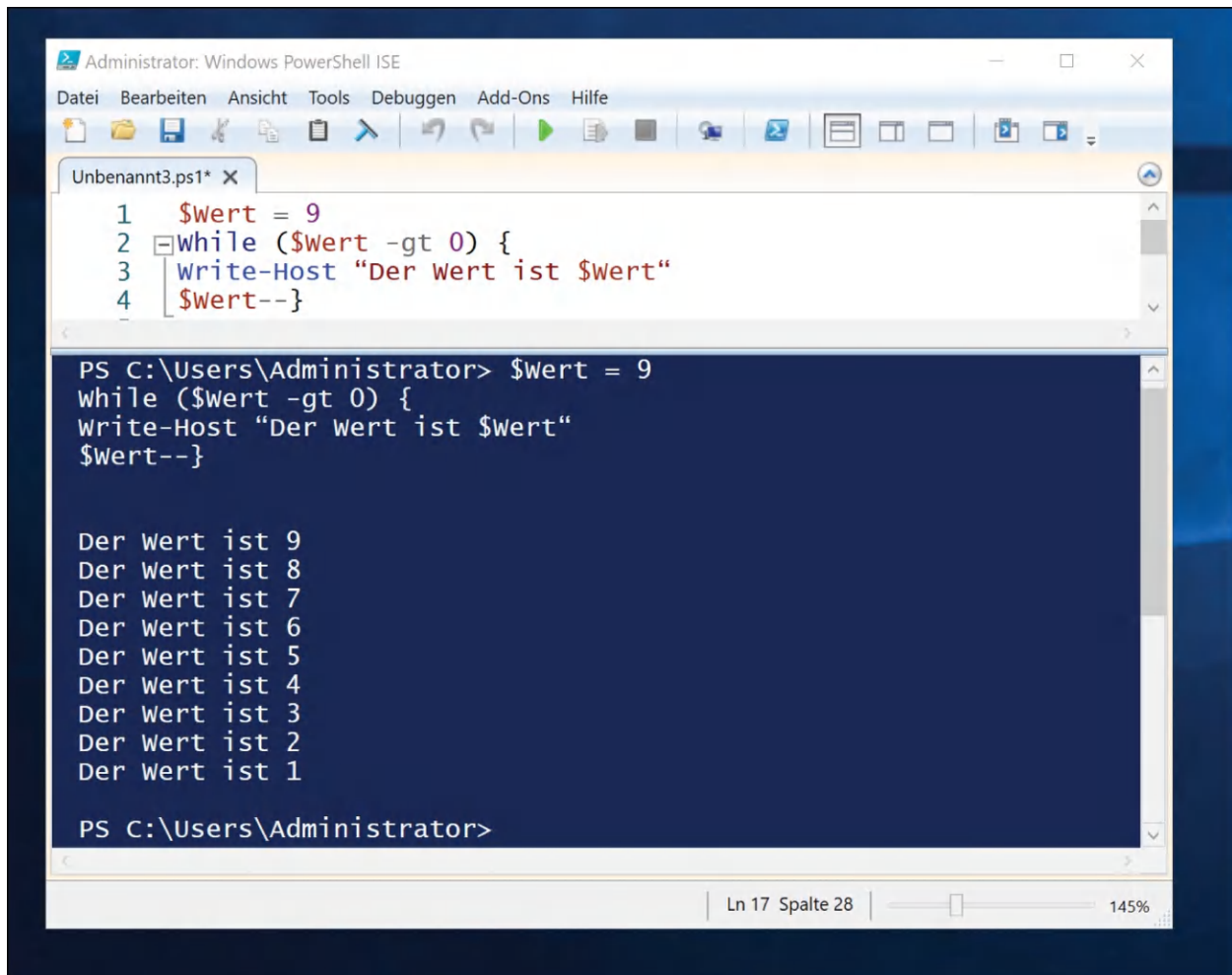


Abbildung 5.13: Die »While«-Schleife ist eine klassische »abweisende« Schleife: Wird die Startbedingung nicht erfüllt, so wird sie auch nicht ausgeführt.

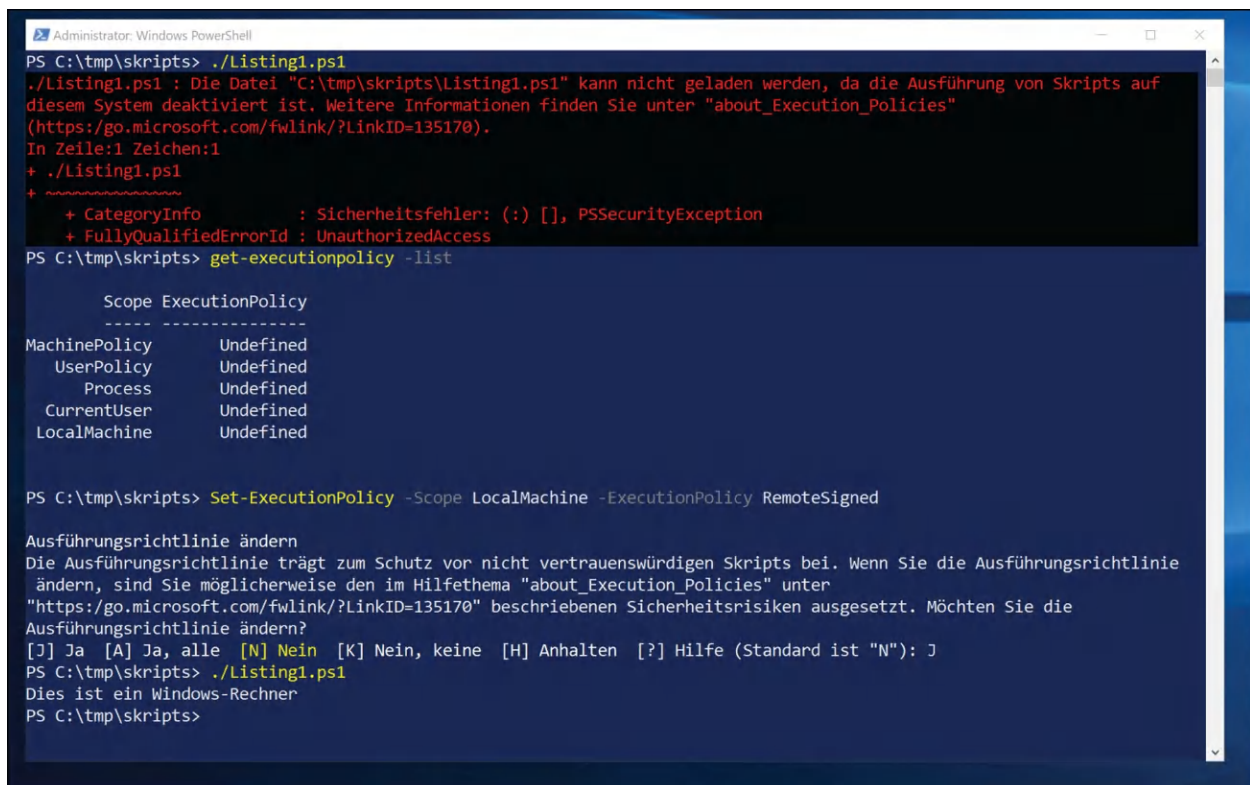
Wie Sie ein Skript »zum Laufen« bringen ...

Wenn Sie die ersten Skripte mithilfe der ISE erstellt haben, dann können Sie diese als Dateien mit der Endung ».ps1« abspeichern. Diese können Sie mit der PowerShell aufrufen beziehungsweise (wenn die Dateierweiterung auf dem System korrekt verknüpft ist) auch mit einem Doppelklick starten. Allerdings kann es durchaus passieren, dass Sie dafür zunächst einmal noch die Hürde der Ausführungsrichtlinie (Execution Policy) überwinden müssen.

Was sind Ausführungsrichtlinien? Diese Einstellungen sollen Nutzer davor schützen, versehentlich oder unwissentlich nicht sichere oder gefährliche Skripte auf dem System auszuführen. Wenn Sie beispielsweise Ihre PowerShell-Skripte auf einem Windows-Server in der Version 2012

oder früher oder auch unter Windows 10 ausführen möchten, so werden Sie in der Regel eine Anzeige auf den Bildschirm bekommen, wie Sie diese im oberen Teil der [Abbildung 5.14](#) sehen können.

Wenn Sie uns allerdings bis zu diesem Punkt auf einer Version 2019 des Windows-Servers gefolgt sind, so werden Sie dieses Problem in der Regel nicht haben. Diese Systeme sind nämlich bereits standardmäßig so konfiguriert, dass Sie Ihre Skripte auf jeden Fall lokal ausführen können. Grundsätzlich verhindern die Ausführungsrichtlinien lediglich das Ausführen bestimmter Skripte, nicht aber von bloßen Cmdlets.



```
Administrator: Windows PowerShell
PS C:\tmp\skripts> ./Listing1.ps1
./Listing1.ps1 : Die Datei "C:\tmp\skripts\Listing1.ps1" kann nicht geladen werden, da die Ausführung von Skripten auf diesem System deaktiviert ist. Weitere Informationen finden Sie unter "about_Execution_Policies" (https://go.microsoft.com/fwlink/?LinkID=135170).
In Zeile:1 Zeichen:1
+ ./Listing1.ps1
+ ~~~~~
+ CategoryInfo          : Sicherheitsfehler: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess

PS C:\tmp\skripts> get-executionpolicy -list

Scope ExecutionPolicy
-----
MachinePolicy Undefined
UserPolicy Undefined
Process Undefined
CurrentUser Undefined
LocalMachine Undefined

PS C:\tmp\skripts> Set-ExecutionPolicy -Scope LocalMachine -ExecutionPolicy RemoteSigned

Ausführungsrichtlinie ändern
Die Ausführungsrichtlinie trägt zum Schutz vor nicht vertrauenswürdigen Skripten bei. Wenn Sie die Ausführungsrichtlinie ändern, sind Sie möglicherweise den im Hilfethema "about_Execution_Policies" unter "https://go.microsoft.com/fwlink/?LinkID=135170" beschriebenen Sicherheitsrisiken ausgesetzt. Möchten Sie die Ausführungsrichtlinie ändern?
[Y] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "N"): J
PS C:\tmp\skripts> ./Listing1.ps1
Dies ist ein Windows-Rechner
PS C:\tmp\skripts>
```

Abbildung 5.14: Die Ausführungsrichtlinien sollen verhindern, dass Nutzer gefährliche Skripte ausführen. Auf älteren Versionen des Windows-Servers müssen sie zunächst umkonfiguriert werden.

Mithilfe des Cmdlets `Get-ExecutionPolicy` und der Option `-list` bekommen Sie alle Ausführungsrichtlinien angezeigt, die für die verschiedenen Bereiche Ihres Servers konfiguriert sind. Sind diese alle – wie in unserem Beispiel in [Abbildung 5.14](#) – auf »Undefined« gesetzt, so wird die PowerShell keine Skripte ausführen. Mithilfe des Aufrufs

```
Set-Executionpolicy -Scope LocalMachine -ExecutionPolicy RemoteSigned
```

setzen Sie die Richtlinie auf dem Server auf die Einstellung, die standardmäßig auf dem Windows Server 2019 zu finden ist. Allerdings können Sie dieses Cmdlet nur mit Administratorrechten ausführen. Die Ausführungsrichtlinie wird in den meisten Fällen als RemoteSigned festgelegt, was eine Abwägung zwischen Sicherheit und Bequemlichkeit darstellt. RemoteSigned stellt sicher, dass lokale Skripte immer ausgeführt werden können, während Skripte aus anderen Quellen nur dann ausgeführt werden, wenn sie signiert sind.

Insgesamt stehen sechs Einstellmöglichkeiten für eine Ausführungsrichtlinie zur Verfügung. Die mit den meisten Einschränkung ist Restricted. Sie war bis zur Version 2012 die Standardeinstellung, die das Ausführen von Skripten auch für Administratoren komplett unterbindet. Bei der Einstellung Allsigned werden nur signierte Skripte ausgeführt, was auch für lokale Skripte gilt. Kommt die Einstellung RemoteSigned zum Einsatz, so können lokale Skripte ausgeführt werden, während aus dem Internet heruntergeladene wiederum signiert werden müssen. Bei der Verwendung von Unrestricted können alle Skripte ausgeführt werden, allerdings muss bei jedem Ausführen eines unsignierten Skripts aus dem Internet dieses via Prompt explizit bestätigt werden. Wählen Sie Bypass, so wird die Ausführung durch keinerlei Meldung, Warnung oder Einschränkung behindert. Die Einstellung Undefined entfernt schließlich jede zugewiesene Richtlinie. Wie bei Restricted ist dann keine Ausführung von Skripten mehr möglich. Sollten Sie gezwungen sein, diese Einstellung auf Ihrem Server zu verändern, so sollten Sie in der Regel RemoteSigned wählen.

PowerShell in der Server-Verwaltung einsetzen

Sie werden nicht zuletzt anhand der Lektüre unseres Dummies-Buchs sehr schnell zu der Erkenntnis gelangen, dass die Verwaltung und Betreuung

eines Servers ganz allgemein und damit natürlich auch die eines Windows-Servers ein Thema ist, das sich eigentlich nicht zwischen zwei Buchdeckel pressen lässt. Das gilt noch einmal verstärkt, wenn es sich um die Verwaltung und Betreuung eines solchen Systems unter Einsatz der PowerShell handelt: Hier treffen die vielfältigen und oftmals komplexen Aufgaben im Umfeld eines Servers auf die immense Flexibilität der PowerShell, die dann zudem noch mithilfe einer großen Zahl von Modulen erweitert werden kann.



Wir möchten Ihnen hier im letzten Abschnitt unseres PowerShell-Kapitels einen generellen Überblick über einige sehr grundlegende Einsatzmöglichkeiten der PowerShell bei der Administration Ihres Windows-Servers geben. Auf den Webseiten von Microsoft finden Sie beispielsweise im sogenannten »Scripting Blog« unter der Adresse <https://devblogs.microsoft.com/scripting/> immer wieder neue Beispiele und Anregungen in englischer Sprache für den Einsatz der PowerShell im systemnahen Umfeld. Eine weitere sehr gute Quelle für Skripte und Lösungen mithilfe der PowerShell ist die »PowerShell Gallery«, die Sie unter der Adresse <https://www.powershellgallery.com/> finden können.

Wir haben uns für diesen Abschnitt auf einige der grundlegenden täglichen Aufgaben konzentriert, die sicher auch auf Ihrem Windows-Server anfallen werden, und stellen einige Ansätze und Codebeispiele dafür vor.

Prozesse finden und überwachen

Was läuft auf meinem Server oder welcher Prozess ist es, der mir gerade so viel Probleme bereitet? Ihr Windows-Server führt eine interne Tabelle mit allen aktiven (und teilweise auch »ruhenden«) Prozessen, die Ihnen genau darüber Auskunft geben kann. Mithilfe der PowerShell und einigen Kommandos können Sie sich diese Informationen entsprechend aufbereiten. Das geht natürlich auch mit dem Task-Manager, der Ihnen auf dem Server wie in jeder anderen Windows-Version zur Verfügung steht. Aber mit der PowerShell haben Sie hier weitaus mehr Möglichkeiten.

Das Cmdlet, das Ihnen alle Prozesse auf Ihrem Server auflistet, heißt `Get-process`. Das bringt Ihnen aber zunächst nur eine in der Regel recht lange Liste auf den Bildschirm. Wollen Sie nur bestimmte Prozesse anzeigen, beispielsweise alle, deren Name mit dem Buchstaben »M« beginnt, so können Sie dazu ein sogenanntes »Wildcard«-Zeichen verwenden:

```
Get-process M*
```

Das Zeichen »*« steht dabei für eine beliebige Anzahl von beliebigen Zeichen (das umfasst auch kein Zeichen), die dem führenden »M« folgen dürfen. Beachten Sie bitte, dass die PowerShell auch an dieser Stelle nicht zwischen Groß- und Kleinschreibung unterscheidet. Wenn Ihnen diese Art der Anzeige dann zu unübersichtlich sein sollte, können Sie sie auch mithilfe des Pipeline-Operators zum Sortieren an ein weiteres Cmdlet, in diesem Fall `Sort-object`, weiterleiten:

```
Get-process M* | sort-object cpu -descending
```

Dabei wird dem Cmdlet `Sort-object` durch `cpu` das Kriterium zur Sortierung (in diesem Fall die CPU-Zeit) mitgegeben und durch `-descending` angewiesen, dass diese Sortierung in absteigender Reihenfolge geschehen soll. Das Ergebnis dieses und des vorherigen Beispiels können Sie in der [Abbildung 5.15](#) sehen.

```
Auswählen Windows PowerShell
PS C:\Users\micha> Get-process M*

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
228 13 3036 10648 0,73 4316 0 msdtc
398 28 16940 83392 0,02 392 1 msedge
150 9 1760 6840 0,11 808 1 msedge
1278 51 30772 104360 0,19 1680 1 msedge
490 26 11108 32632 0,05 3852 1 msedge
241 14 5960 17068 0,06 4192 1 msedge
227 14 11260 23604 1,27 5584 1 msedge
354 30 53664 113244 0,06 6484 1 msedge
422 16 8296 18296 0,02 4188 0 msixexec
800 75 200152 153268 0,02 3272 0 MsMpEng

PS C:\Users\micha> Get-process M* | sort-object cpu -descending

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
394 31 68040 122864 2,20 6484 1 msedge
1243 50 32320 106656 1,67 1680 1 msedge
385 27 14752 78628 1,25 392 1 msedge
439 19 10864 32700 0,36 3852 1 msedge
227 14 11108 23352 0,08 5404 1 msedge
241 14 6632 17140 0,06 4192 1 msedge
152 9 1812 7020 0,02 808 1 msedge
668 75 196256 150972 0,02 3272 0 MsMpEng
228 13 3036 10648 0,73 4316 0 msdtc
```

Abbildung 5.15: Welche Prozesse sind aktiv und brauchen wie viel Zeit von der CPU? Mithilfe der PowerShell ist das eine einfache Abfrage.

Schon dieses kleine und noch sehr einfache Beispiel zeigt, welche Möglichkeiten sich durch die Verbindung der verschiedenen Cmdlets ergeben. Wenn Sie wissen möchten, was hinter den unterschiedlichen Bezeichnungen wie »NPM(K)« oder »PM(K)« bei einer solchen Anzeige steckt, sollten Sie auf die sehr gute und umfangreiche Hilfefunktion der PowerShell zurückgreifen. Sie steht ihnen jederzeit zur Verfügung, indem Sie einfach `Get-help` gefolgt von dem gesuchten Cmdlet aufrufen:

`Get-help get-process`

Rufen Sie die Hilfe auf diese Art auf einem Rechner das erste Mal auf, so kann es sein, dass Windows feststellt, dass sich noch nicht für alle PowerShell-Module die aktuellen Hilfedateien auf Ihrem Rechner befinden. Das System fragt Sie dann, ob ein entsprechender Download

durchgeführt werden soll. Dieser startet sofort, wenn Sie die Frage mit »Ja« beantworten, und kann je nach Stand der Hilfedateien auf Ihrem Rechner etwas Zeit in Anspruch nehmen ([Abbildung 5.16](#)). Geben Sie dann nach dem Download den Hilfebefehl mit der Option `-full` ein, so bekommen Sie sehr ausführliche Informationen in englischer Sprache zum angefragten Cmdlet.

```
Administrator: Windows PowerShell
```

```
Hilfe für Modul NetConnection wird aktualisiert  
Es wird nach dem Hilfeinhalt gesucht...  
[ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo]
```

svchost	3460	0,03125	Hostprozess für Windows-Dienste
svchost	3468	0,09375	Hostprozess für Windows-Dienste
svchost	3476	0	Hostprozess für Windows-Dienste
svchost	3484	0,03125	Hostprozess für Windows-Dienste
svchost	3504	0	Hostprozess für Windows-Dienste
svchost	3672	0,0625	Hostprozess für Windows-Dienste
svchost	4052	0	Hostprozess für Windows-Dienste
svchost	4372	0	Hostprozess für Windows-Dienste
svchost	4428	0,03125	Hostprozess für Windows-Dienste
svchost	4452	0,015625	Hostprozess für Windows-Dienste
svchost	4464	0,140625	Hostprozess für Windows-Dienste
svchost	4708	0,03125	Hostprozess für Windows-Dienste
svchost	5088	0,0625	Hostprozess für Windows-Dienste
svchost	5348	0,5	Hostprozess für Windows-Dienste
svchost	5404	0,109375	Hostprozess für Windows-Dienste
svchost	5440	0,21875	Hostprozess für Windows-Dienste
svchost	5624	0,09375	Hostprozess für Windows-Dienste
svchost	5792	1,734375	Hostprozess für Windows-Dienste
svchost	5956	0,0625	Hostprozess für Windows-Dienste
svchost	6548	0,09375	Hostprozess für Windows-Dienste
System	4	16,84375	
taskhostw	5504	0,078125	Hostprozess für Windows-Aufgaben
vmcompute	4440	0,0625	Hyper-V-Hostserverdienst
vmms	3568	0,203125	Verwaltungsdienst für virtuelle Computer
wininit	744	0	
winlogon	932	0,171875	Windows-Anmeldeanwendung
winlogon	6768	0,078125	Windows-Anmeldeanwendung
WUDFHost	1696	0,03125	Windows Driver Foundation - Benutzermodus-Treiberframework-Hostprozess

```
PS C:\Users\Administrator> get-help get-process
```

Möchten Sie Update-Help ausführen?

Das Update-Help-Cmdlet lädt die neuesten Hilfedateien für Windows PowerShell-Module herunter und installiert sie auf dem Computer. Weitere Informationen zum Update-Help-Cmdlet finden Sie unter "<https://go.microsoft.com/fwlink/?LinkId=210614>".

[J] Ja [N] Nein [H] Anhalten [?] Hilfe (Standard ist "J"): J

Abbildung 5.16: Hilfe steht immer parat in der PowerShell. Ist diese nicht auf dem aktuellen Stand, kann ein Update wie hier direkt nachgeladen werden.

```
Get-help get-process -full
```

Bei all diesen Ausgaben ist es gerade dann, wenn Sie einen Überblick über das Geschehen auf Ihrem Server bekommen wollen, sehr wichtig, dass die Ausgabe auf dem Bildschirm übersichtlich gelingt. Dazu bietet die PowerShell unterschiedliche Möglichkeiten an. So können Sie beispielsweise das Cmdlet `Format-Table` (oder sein Alias `ft`) verwenden,

um die Ausgabe in einer nach Ihren Vorstellungen geordneten Tabelle aufzulisten:

```
Get-Process | Format-Table Name, Fileversion, Productversion,  
Company
```

Dabei liest Format-Table dann die entsprechenden Eigenschaften aus und stellt sie in Form einer Liste dar. Etwas schöner und vielseitiger ist dabei der Einsatz des Cmdlets Out-GridView, das Ihnen die Ergebnisse in einem separaten Fenster darstellt, in dem Sie die Ausgabe zudem noch interaktiv durch Angabe zusätzlicher Kriterien verändern können. Allerdings müssen Sie in diesem Fall das Cmdlet Select-Object in der Pipeline »dazwischenschalten«, um die Eigenschaften herauszulesen. Das beherrscht Out-GridView nicht, kann aber vorformatierte Werte von Select-Object aus der Pipeline übernehmen:

```
Get-Process | Select-Object Name, Fileversion, Productversion,  
Company | Out-GridView
```

In der [Abbildung 5.17](#) können Sie sehen, dass beide Ausgaben die gleichen Daten anzeigen. Im Fenster OUT-GRIDVIEW sehen Sie auch den Eintrag KRITERIEN HINZUFÜGEN, der es Ihnen erlaubt, die Ausgabe interaktiv zu verändern, indem Sie sich beispielsweise nur die Prozesse mit einem bestimmten Namen anzeigen lassen.

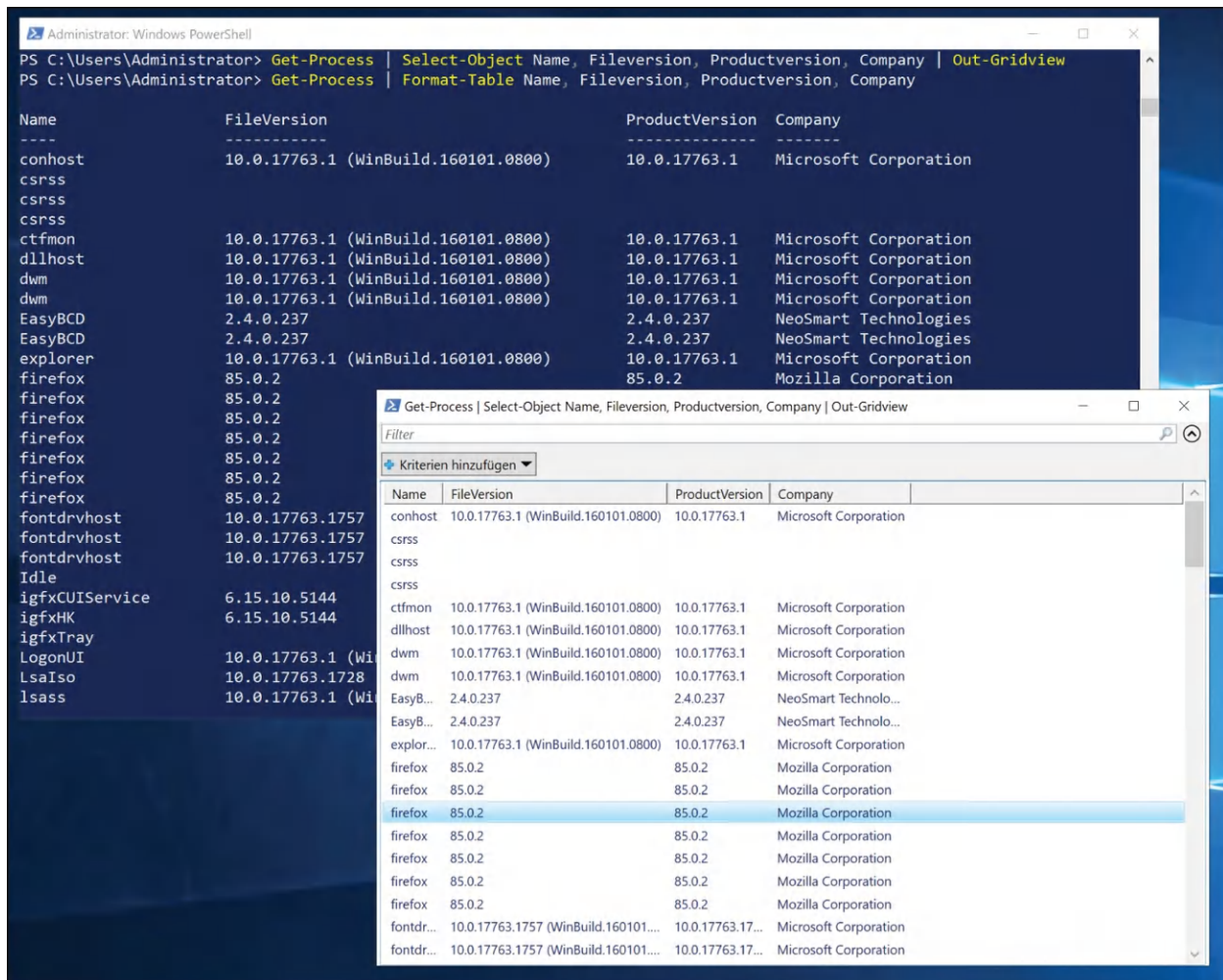


Abbildung 5.17: Zwei verschiedene beispielhafte Ausgabemöglichkeiten für Prozesse. Das Cmdlet »Out-GridView« ist hierbei am flexibelsten.

Drucker im Griff behalten

Auch wenn immer vom »papierlosem Büro« geredet wird – die Drucker sind wichtige Endgeräte und werden es mit großer Sicherheit noch eine ganze Weile bleiben. Arbeiten Sie ausschließlich mit nur diesem einem Server und vielleicht sogar nur einem Drucker, so können Sie diesen bei Windows Server 2019 auf die gleiche Art und Weise in den Windows-Einstellungen verwalten, wie Sie es vielleicht schon von Windows 10 her kennen. Wozu dann die PowerShell einsetzen? Neben der Möglichkeit, mithilfe von PowerShell-Befehlen und Skripten sehr schnell auch sogenannte Bulk-Jobs auszuführen – also Arbeiten, bei denen beispielsweise eine ganze Reihe von Druckern konfiguriert werden soll –, müssen Sie auch auf die Druckerverwaltung via PowerShell

zurückgreifen, wenn Sie beispielsweise mit der Core-Version des Windows-Servers arbeiten und Ihnen keine Windows-Oberfläche zur Verfügung steht. Wir zeigen Ihnen in diesem Abschnitt die grundlegenden Kommandos für die Druckerverwaltung mit der PowerShell.

Wollen Sie alle auf Ihrem Server installierten Drucker anzeigen, so gelingt das durch den einfachen Aufruf des Cmdlets `Get-Printer`, wie er in der [Abbildung 5.18](#) zu sehen ist. Dieses Kommando bringt dann alle Drucker und Druckerverbindungen Ihres Servers auf den Bildschirm.

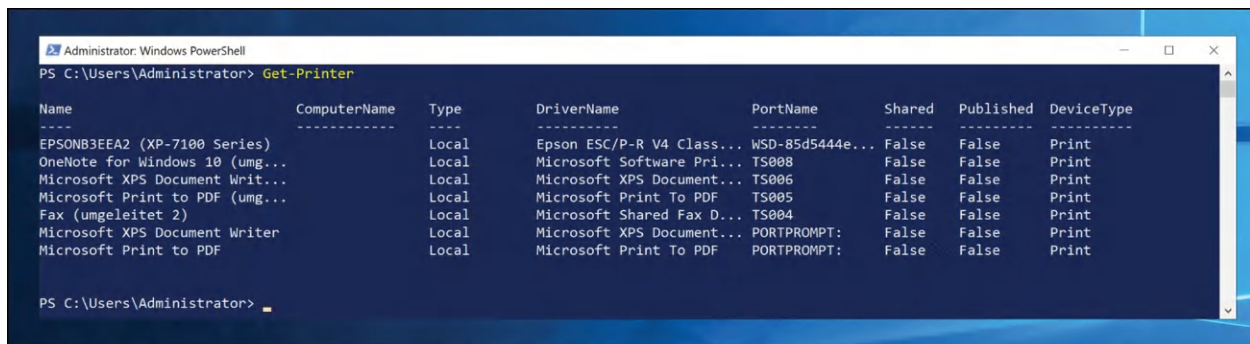


Abbildung 5.18: Mit dem Cmdlet »Get-Printer« bringen Sie alle Drucker und Druckerverbindungen Ihres Windows-Servers auf den Bildschirm.

Dabei sehen Sie dann gleich auch, dass der Windows-Server hier standardmäßig schon einige »virtuelle Drucker« installiert hat, mit deren Hilfe Sie beispielsweise direkt PDF- oder auch XPS-Dateien aus Ihren Dokumenten erstellen können. Wollen Sie mehr über einen speziellen Drucker und dessen Daten erfahren, können Sie den folgenden Aufruf starten:

```
Get-Printer | Format-List Name, Drivername, Printerstatus
```

Hier kommt wieder das Cmdlet `Format-List` zum Einsatz, um beispielsweise die Ausgabe des Druckernamens, des Druckertreibers und seines Status auszugeben. Sie können sich mit `Get-Printer` auch eine Liste der Drucker anzeigen lassen, die auf einem anderen Rechner im Netzwerk installiert sind. Das setzt natürlich voraus, dass Sie die entsprechenden Zugriffsrechte auf dieses andere System besitzen.

```
Get-Printer -Computername Server2
```

Anstelle des Namens können Sie an dieser Stelle dann auch die IP-

Adresse des anderen Systems angeben.

In der Zusammenarbeit von dem Cmdlet `Get-Printjob` mit `Get-Printer` können Sie sich selbstverständlich auch die Aufträge anzeigen lassen, die gerade auf einem Drucker aktiv sind:

```
Get-Printer "Druckername" | Get-Printjob | fl
```

Geben Sie keinen expliziten Druckernamen an, so gibt der Aufruf alle aktiven Jobs auf allen installierten Druckern aus. Spätestens dann ist die Weiterleitung an das Cmdlet `Format-List` (hier als Alias `fl`) sehr sinnvoll. Wenn Sie Druckaufträge löschen wollen, können Sie das unter Verwendung von `Remove-PrintJob` erledigen und dabei unter anderem auch genau einen Drucker ansteuern:

```
Remove-PrintJob -PrinterName "Epson1" -ID 1
```

Oder Sie löschen nur die Druckaufträge eines bestimmten Nutzers:

```
Get-Printer | Get-PrintJob | where UserName -Like  
<Benutzername> | Remove-PrintJob
```

Mit dem `Like`-Operator vergleichen Sie dabei auf den richtigen Nutzernamen.

Das letzte Beispiel für einen Einsatz der PowerShell in der Druckerverwaltung sehen Sie in der [Abbildung 5.19](#). Oftmals bekommen die Drucker bei der automatischen Installation sehr umständliche, lange Namen, die eine Ansprache deutlich erschweren. In unserem Beispiel war das ein Epson-Drucker. Wir haben uns dann zunächst die komplette Bezeichnung des Druckers in einer Variablen (hier `$Drucker`) abgespeichert, wobei den Namen hier mit der Wildcard `»*«` übergeben haben. Dann haben wir deren Inhalt mit `-InputObject` an das Cmdlet `Rename-Printer` übergeben, das dann einen neuen Namen an den Drucker (hier `»TintenDruck«`) vergibt. `Get-Printer` zeigt das Ergebnis.

```
$Drucker = Get-Printer -name "Epson*"
Rename-Printer -InputObject $Drucker -NewName "TintenDruck"
```

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-Printer

Name                           ComputerName  Type      DriverName          PortName        Shared  Published  DeviceType
----
EPSONB3EEA2 (XP-7100 Series)    Local         Local     Epson ESC/P-R V4 Class... WSD-85d5444e... False   False      Print
OneNote for Windows 10 (umg...   Local         Local     Microsoft Software Pri... TS008           False   False      Print
Microsoft XPS Document Writ...   Local         Local     Microsoft XPS Document... TS006           False   False      Print
Microsoft Print to PDF (umg...   Local         Local     Microsoft Print To PDF   TS005           False   False      Print
Fax (umgeleitet 2)              Local         Local     Microsoft Shared Fax D... TS004           False   False      Print
Microsoft XPS Document Writer   Local         Local     Microsoft XPS Document... PORTPROMPT:     False   False      Print
Microsoft Print to PDF          Local         Local     Microsoft Print To PDF   PORTPROMPT:     False   False      Print

PS C:\Users\Administrator> $Drucker = Get-Printer -name "Epson*"
PS C:\Users\Administrator> Rename-Printer -InputObject $Drucker -NewName "TintenDruck"
PS C:\Users\Administrator> Get-Printer

Name                           ComputerName  Type      DriverName          PortName        Shared  Published  DeviceType
----
TintenDruck                    Local         Local     Epson ESC/P-R V4 Class... WSD-85d5444e... False   False      Print
OneNote for Windows 10 (umg...   Local         Local     Microsoft Software Pri... TS008           False   False      Print
Microsoft XPS Document Writ...   Local         Local     Microsoft XPS Document... TS006           False   False      Print
Microsoft Print to PDF (umg...   Local         Local     Microsoft Print To PDF   TS005           False   False      Print
Fax (umgeleitet 2)              Local         Local     Microsoft Shared Fax D... TS004           False   False      Print
Microsoft XPS Document Writer   Local         Local     Microsoft XPS Document... PORTPROMPT:     False   False      Print
Microsoft Print to PDF          Local         Local     Microsoft Print To PDF   PORTPROMPT:     False   False      Print

PS C:\Users\Administrator>

```

Abbildung 5.19: Schnelles Umbenennen eines Druckernamens mithilfe des Cmdlets »Rename-Printer«

Schauen Sie sich mithilfe des Cmdlets `Get-Help` die weiteren Befehle für das Print-Management wie unter anderem `Add-Printer`, `Remove-Printer` oder `Restart-Printjob` (zum Neustart eines Druckauftrags) an und probieren Sie diese aus.

Das Netzwerk und dessen Geräte

Ohne Netzwerk geht es heute in der Regel nicht mehr. Also werden Sie Ihren Windows-Server sicher auch in einem Netzwerk betreiben. Bei der Verwaltung des Servers ist es wichtig, dass Sie die entsprechenden Komponenten, die eine reibungslose Netzwerkverbindung garantieren, überwachen und managen können. Die PowerShell bietet Ihnen hier eine ganze Reihe von Möglichkeiten und natürlich auch die entsprechenden Cmdlets dazu.

Für den Einstieg ist es sinnvoll, dass Sie sich zunächst einmal einen Überblick über die aktuell vorhandenen Module und deren Cmdlets verschaffen – auch um festzustellen, welche in Hinblick auf die Arbeit mit dem Netzwerk interessant sind. Der folgende Aufruf bringt alle auf dem jeweiligen System zur Verfügung stehenden Module auf den Bildschirm. Das Cmdlet `Get-Module` zeigt Ihnen bei einem einfachen Aufruf ohne weitere Parameter alle auf Ihrem Server geladenen Module an. Wollen Sie

wissen, welche zusätzlich verfügbaren Module Sie importieren können, dann geben Sie den folgenden Aufruf ein, der Ihnen eine lange Liste auf den Bildschirm bringen wird:

```
Get-Module -ListAvailable
```

Der folgende Aufruf von `Get-Module` mit `-All` zeigt zudem alle exportierten Dateien für alle verfügbaren Module an. Da dieser Aufruf die Liste noch umfangreicher macht, haben wir die Ausgabe des Aufrufs mittels einer Pipeline an das Cmdlet `where-Object` (in diesem Fall haben wir dessen Alias `where` verwendet) geleitet. Damit dieses Cmdlet mit jedem Objekt, das es aus der Pipeline übergeben bekommt, auch arbeiten kann, kommt innerhalb der geschweiften Klammern die spezielle Variable `$_` zum Einsatz, in der dann dieses Objekt zu finden ist. Mittels `.Name` greifen wir dann auf die Eigenschaft `Name` des jeweiligen Objekts zu und vergleichen diesen Namen anschließend mithilfe des Operators `-like` mit der Zeichenkette `"Net*"`. Schließlich haben wir die Ausgabe dieses Kommandos dann mit einer weiteren Pipeline an `Out-GridView` weitergeleitet, um die gefundenen Daten in einem Fenster darzustellen.

```
Get-Module -ListAvailable -All | where {$_.Name -like "Net*" } | Out-GridView
```

Wenn Ihnen dieser Aufruf zunächst etwas verwirrend vorkommt, dann probieren Sie ihn einfach einmal aus. Verändern Sie dabei auch mal verschiedene Daten und Einstellungen. Diese Art der Aufrufe und Verarbeitung ist typisch für die PowerShell, und durch entsprechendes Ausprobieren werden Sie schnell ein Gefühl für die daraus entstehenden Möglichkeiten bekommen. Das Ergebnis dieses Aufrufs ist immer noch ziemlich umfangreich (was nicht zuletzt dem Einsatz von `-All` geschuldet ist), wie Sie in der [Abbildung 5.20](#) sehen können. Es zeigt Ihnen eindrucksvoll, wie viele Kommandos rund um das Thema Netzwerke – wozu unter anderem auch die Einstellungen der Windows Defender Firewall gehören – Sie von der PowerShell zur Verfügung gestellt bekommen.

In dieser langen Auflistung finden Sie dann auch einige Module wie `NetAdapter`, `NetSecurity` oder `NetTCPIP`, die Ihnen den entsprechenden

Zugriff auf die Netzwerkressourcen zur Verfügung stellen. Dabei ist es sicher interessant zu wissen, welche Cmdlets diese Module im Einzelnen beinhalten. Auch dabei kann natürlich die PowerShell helfen. So listet beispielsweise:

Get-Command -Modul NetAdapter

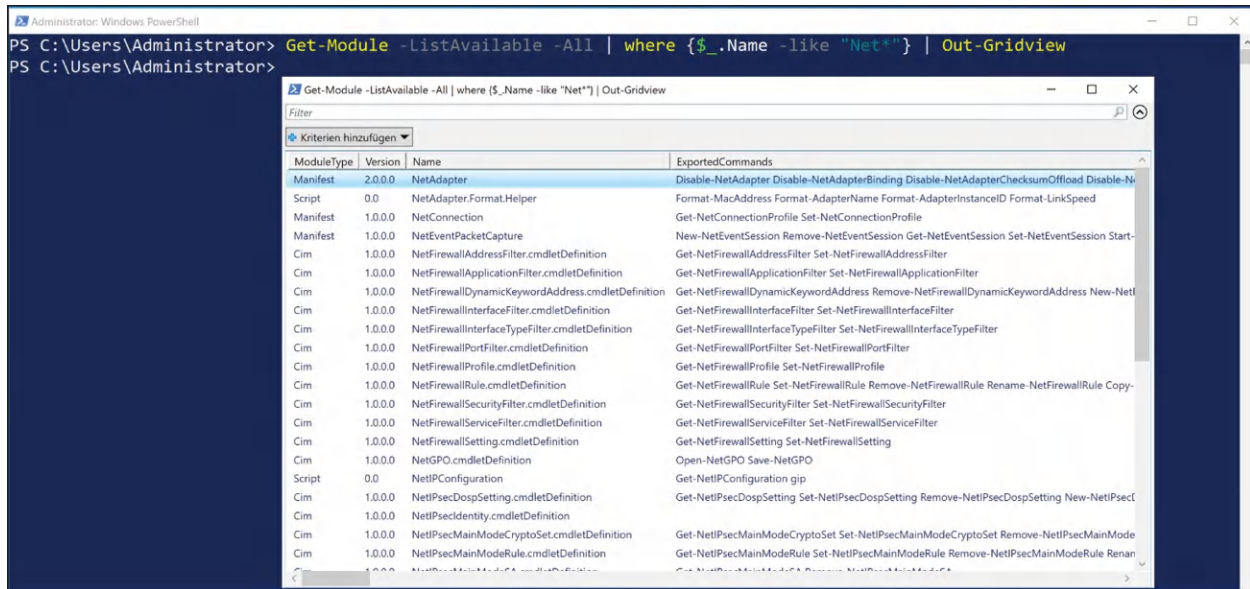


Abbildung 5.20: Die PowerShell bieten Ihnen viele Module und Cmdlets, mit deren Hilfe Sie das Netzwerk und dessen Geräte verwalten können.

die Cmdlets auf, die Ihnen im Modul NetAdapter zur Verfügung stehen. Das sind dann die Kommandos, die sich direkt auf die Netzwerkkarte(n) in Ihrem Server beziehen. Diese Liste ist zwar schon kürzer als die vorherige Auflistung, aber beinhaltet immer noch mehr als genug Kommandos, wie die [Abbildung 5.21](#) zeigt.

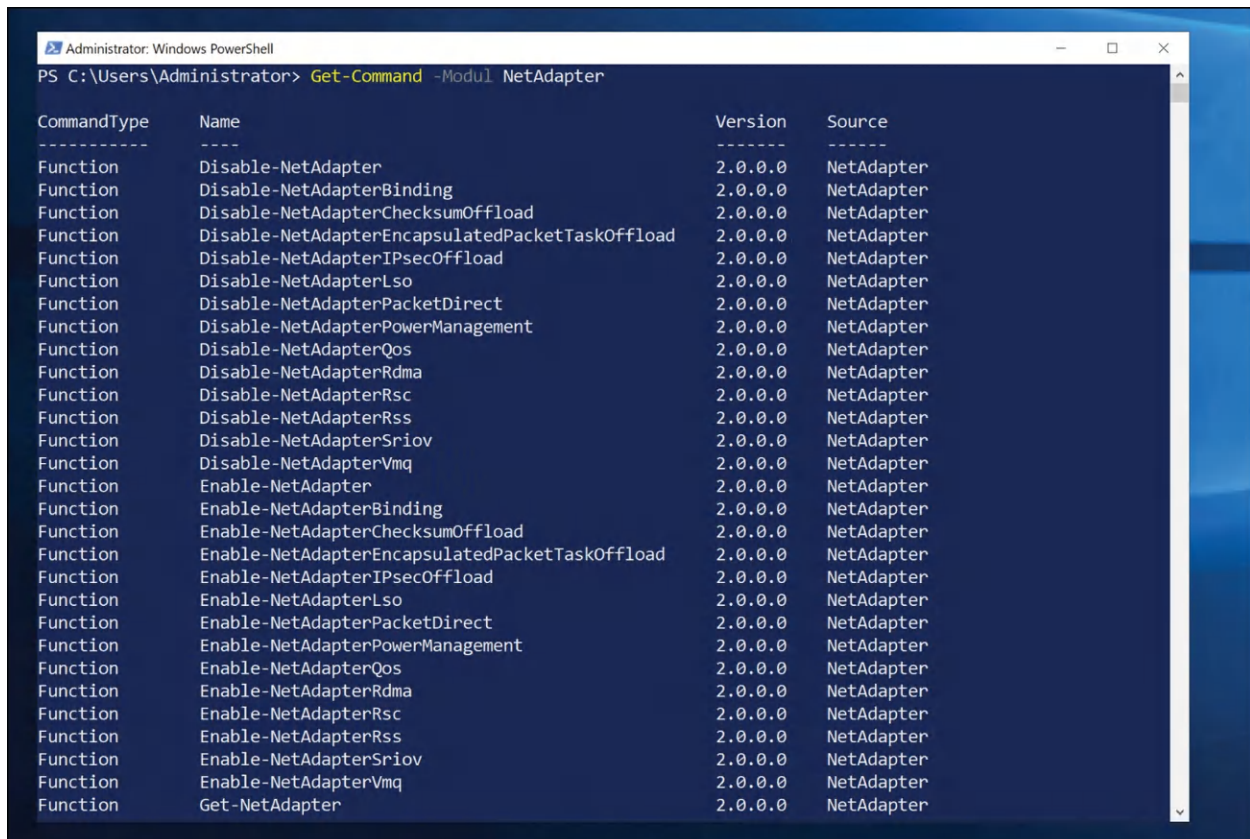


Abbildung 5.21: Diese Auflistung zeigt, welche Cmdlets für die Arbeit mit Netzwerkkarten die PowerShell zur Verfügung stellt.

Arbeiten mit den Netzwerkkarten im Server

Der einfachste Aufruf, der sich zunächst einmal anbietet, ist die Anzeige der im Server vorhandenen und aktiven Netzwerkkarten:

Get-Netadapter

Dabei werden Sie möglicherweise feststellen, dass bei diesem Aufruf keine WLAN-Karte angezeigt wird, obwohl sich in Ihrem System vielleicht sogar eine solche Karte befindet. Eine Überprüfung mittels:

Get-Netadapter -Name "WLAN"

bestätigt dies durch eine Fehlermeldung ([Abbildung 5.22](#)).


```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-Netadapter

Name                           InterfaceDescription         IfIndex Status           MacAddress             LinkSpeed
----                           -
Ethernet0                      Intel(R) 82574L Gigabit Network Conn... 13 Up              00-0C-29-28-94-9B      1 Gbps

PS C:\Windows\system32> Get-Netadapter -Name "WLAN"
Get-Netadapter : Es wurden keine MSFT_NetAdapter-Objekte gefunden, bei denen die Name-Eigenschaft gleich "WLAN" ist. Überprüfen Sie den Wert der Eigenschaft, und versuchen Sie es erneut.
In Zeile:1 Zeichen:1
+ Get-Netadapter -Name "WLAN"
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (WLAN:String) [Get-NetAdapter], CimJobException
+ FullyQualifiedErrorId : CmdletizationQuery_NotFound_Name,Get-NetAdapter

PS C:\Windows\system32> Get-WindowsOptionalFeature -Online | where FeatureName -match Wireless

FeatureName : WirelessNetworking
State       : Disabled

PS C:\Windows\system32> Enable-WindowsOptionalFeature -Online -FeatureName WirelessNetworking
Möchten Sie den Computer jetzt neu starten, um den Vorgang abzuschließen?
[Y] Yes [N] No [?] Hilfe (Standard ist "Y"): Y
```

Abbildung 5.22: Standardmäßig unterstützt Windows Server 2019 zunächst keine Adapter für das drahtlose Netzwerk: Das lässt sich aber durch die Installation dieses Features leicht ändern.

Grundsätzlich geht man bei Microsoft wohl davon aus, dass ein Windows-Server standardmäßig eher nicht über eine drahtlose Verbindung ins Netz gelangt. Was aber, wenn Sie Ihren Windows-Server mit einer drahtlosen Verbindung betreiben wollen? Als sogenanntes Feature stellt der Windows-Server auch die Möglichkeit bereit, mit WLAN-Verbindungen zu arbeiten. Mit dem folgenden Aufruf

```
Get-WindowsOptionalFeature -Online
```

können Sie alle optionalen Features Ihres aktuelle laufenden Windows-Systems auflisten. Achtung: Sie können dieses Kommando und auch nachfolgend beschriebene nur mit erhöhten Rechten, also in einer PowerShell-Sitzung mit Administratorrechten, ausführen. Da wir in diesem Beispiel nur an dem optionalen Feature wireless interessierte sind, nutzen wir wieder das Cmdlet where-Object in Form des Alias where, um das gesuchte Feature und seinen Status anzuzeigen:

```
Get-WindowsOptionalFeature -Online | where FeatureName -match Wireless
```

Wenn Sie dann auf Ihrem Server eine Meldung wie die in der [Abbildung 5.22](#) zu sehen bekommen, die Ihnen sagt, dass dieses Feature »disabled«

ist, müssen Sie es zunächst einmal installieren:

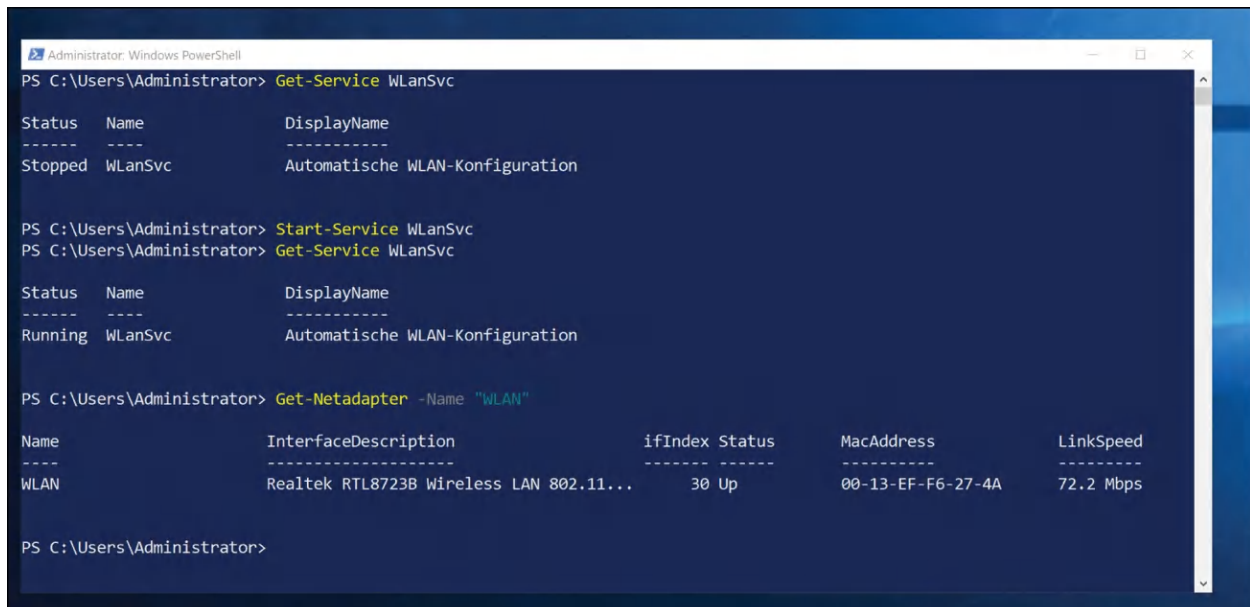
```
Enable-WindowsOptionalFeature -Online -FeatureName  
WirelessNetworking
```

Danach ist dann – wie in [Abbildung 5.22](#) ebenfalls zu sehen – ein Neustart des Betriebssystems notwendig.

Nach dem Neustart des Betriebssystems sollten Sie zunächst überprüfen, ob der Systemdienst für das WLAN auf dem Server bereits läuft.

```
Get-Service WlanSvc
```

In der Regel wird er – wie in der [Abbildung 5.23](#) zu sehen – zunächst gestoppt sein.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-Service WlanSvc

Status Name      DisplayName
-----
Stopped WlanSvc    Automatische WLAN-Konfiguration

PS C:\Users\Administrator> Start-Service WlanSvc
PS C:\Users\Administrator> Get-Service WlanSvc

Status Name      DisplayName
-----
Running WlanSvc    Automatische WLAN-Konfiguration

PS C:\Users\Administrator> Get-Netadapter -Name "WLAN"

Name InterfaceDescription      ifIndex Status MacAddress LinkSpeed
----
WLAN Realtek RTL8723B Wireless LAN 802.11... 30 Up 00-13-EF-F6-27-4A 72.2 Mbps

PS C:\Users\Administrator>
```

Abbildung 5.23: Nach der Installation des WLAN-Features muss nur noch der entsprechende Systemdienst gestartet werden.

Ändern Sie das mittels des Befehls:

```
Start-Service WlanSvc
```

Danach besitzt dieser Systemdienst den Status Running, und Sie können nun bei der Abfrage mittels

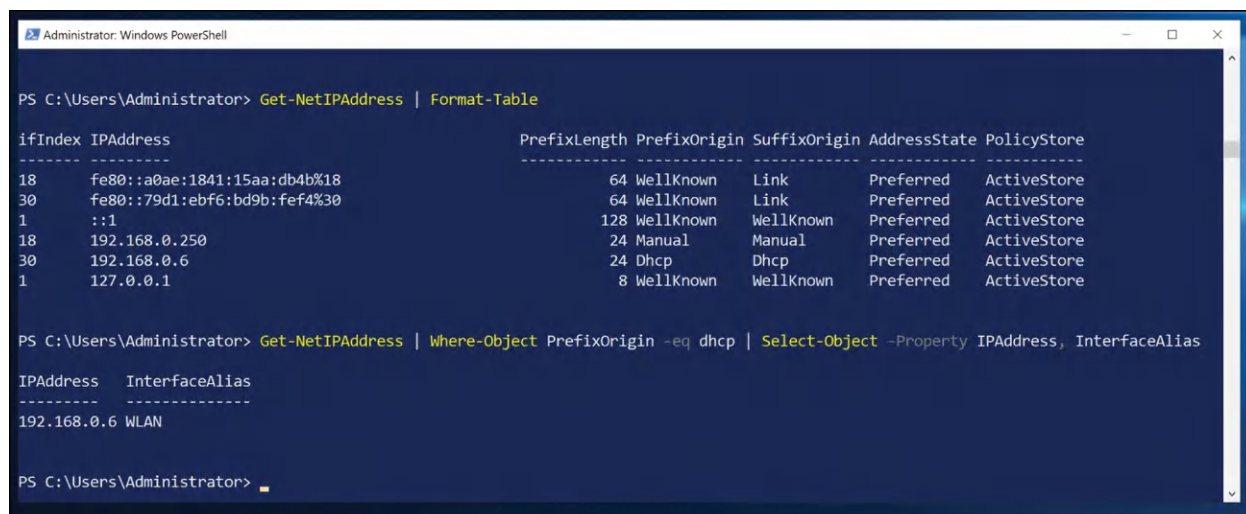
```
Get-NetAdapter -Name "WLAN"
```

nicht nur die WLAN-Karte, sondern unter anderem auch deren

Beschreibung und Übertragungsrate sehen ([Abbildung 5.23](#)).

Die Flexibilität der PowerShell und der Einsatz einer Pipe ermöglichen aber noch weitaus genauere Abfragen. So zeigt der Aufruf mittels des Cmdlets `Get-NetIPAddress` in [Abbildung 5.24](#) die IP-Adressen der in diesem Server vorhandenen Netzwerkverbindungen. Dabei haben wir die Ausgabe an `Format-Table` weitergeleitet, damit sie etwas übersichtlicher dargestellt wird:

`Get-NetIPAddress | Format-Table`



```
PS C:\Users\Administrator> Get-NetIPAddress | Format-Table
```

ifIndex	IPAddress	PrefixLength	PrefixOrigin	SuffixOrigin	AddressState	PolicyStore
18	fe80::a0ae:1841:15aa:db4b%18	64	WellKnown	Link	Preferred	ActiveStore
30	fe80::79d1:ebf6:bd9b:fef4%30	64	WellKnown	Link	Preferred	ActiveStore
1	::1	128	WellKnown	WellKnown	Preferred	ActiveStore
18	192.168.0.250	24	Manual	Manual	Preferred	ActiveStore
30	192.168.0.6	24	Dhcp	Dhcp	Preferred	ActiveStore
1	127.0.0.1	8	WellKnown	WellKnown	Preferred	ActiveStore

```
PS C:\Users\Administrator> Get-NetIPAddress | Where-Object PrefixOrigin -eq dhcp | Select-Object -Property IPAddress, InterfaceAlias
```

IPAddress	InterfaceAlias
192.168.0.6	WLAN

```
PS C:\Users\Administrator>
```

Abbildung 5.24: Mithilfe des Cmdlets »Get-NetIPAddress« können Sie viele Informationen über die installierten Netzwerkkarten anzeigen.

Der zweite Aufruf des Cmdlets `Get-NetIPAddress` in [Abbildung 5.24](#) wurde geschrieben, um die Netzwerkschnittstellen zu finden, die ihre Adressen via DHCP bezogen haben. Dabei werden zunächst mittels `where-object` und eines Vergleichs auf DHCP die Adressen herausgefiltert, die diesen Eintrag besitzen. Mittels `select-object` werden von diesen Objekten dann mit den Eigenschaften (Properties) IP-Adresse und Name der jeweilige Netzwerkschnittstelle auf den Bildschirm gebracht. In unserem Fall war das nur die eine Adresse für die WLAN-Schnittstelle:

```
Get-NetIPAddress | Where-Object PrefixOrigin -eq dhcp |  
Select-Object -Property IPAddress, InterFaceAlias
```

Benötigen Sie Informationen darüber, welche Hardware bei den

Netzwerkadaptern zum Einsatz kommt, kann der folgende Aufruf hilfreich sein:

```
Get-NetAdapterHardwareInfo
```

Da dieses Cmdlet auch den Hardware-Slot in Ihrem PC ausgibt, in dem sich die Netzwerkkarte befindet, ist dieses Kommando immer wieder sehr nützlich, wenn es um die Fehlersuche und deren Beseitigung geht. Sie brauchen mehr Informationen zur IP- und DNS-Adresse für eine bestimmte Netzwerkschnittstelle? Dieser Aufruf bringt sie Ihnen (mit vielen Informationen) auf den Bildschirm:

```
Get-Netadapter -Name "Ethernet" | Get-NetIPAddress
```

Aber auch das Umbenennen einer Netzwerkschnittstelle ist mithilfe der PowerShell leicht möglich:

```
Rename-NetAdapter - Name "Ethernet" -NewName "LANintern"
```

Variationen bekannter Netzwerkkommandos

Wenn Sie schon mit anderen Systemen wie beispielsweise Linux gearbeitet oder auch nur einen Standard-Windows-Computer in das Netzwerk gebracht haben, dann kennen Sie vielleicht auch schon eine Reihe von Testkommandos wie »Ping« mit deren Hilfe Sie die Verbindung zu anderen Computern im Netz testen können. Auch für diese Zwecke bietet Ihnen die PowerShell entsprechende Cmdlets an.

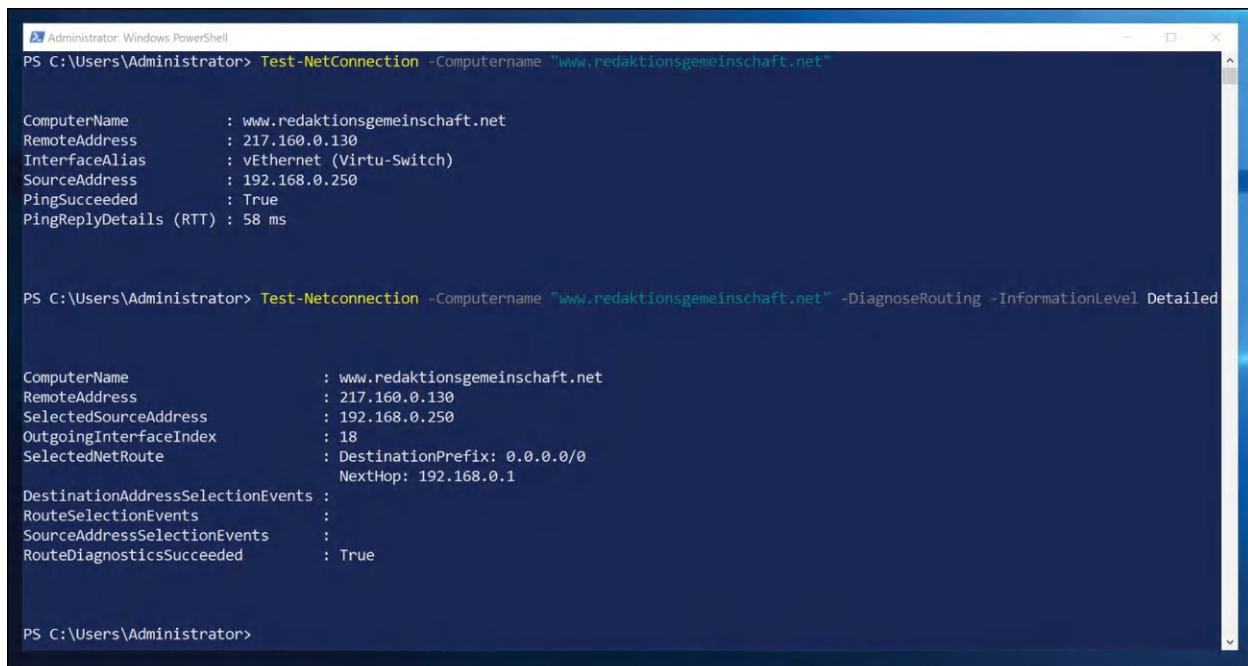
So sieht die PowerShell-Variante dieses Befehls zum Testen einer Verbindung aus:

```
Test-Netconnection -Computername  
"www.redaktionsgemeinschaft.net"
```

Statt wie in diesem Beispiel die Webadresse können Sie bei - Computername natürlich auch direkt eine IP-Adresse des Ziel-Computers angeben. Nun mag es zunächst wenig sinnvoll erscheinen, den einfachen Ping-Befehl durch dieses Cmdlet zu ersetzen. Aber dieser PowerShell-Aufruf lässt sich nicht nur deutlich besser in Skripte einbinden (wo dann beispielsweise die Ausgabe weiterverarbeitet werden kann), sondern bietet auch weitere interessante Optionen:

```
Test-Netconnection -Computername  
"www.redaktionsgemeinschaft.net" -DiagnoseRouting -  
Informationlevel Detailed
```

Wie Sie in [Abbildung 5.25](#) sehen können, wird auf diese Weise zugleich eine ausführliche Diagnose über die Verbindung zum Remote-System ausgeführt und angezeigt.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Test-NetConnection -Computername "www.redaktionsgemeinschaft.net"

ComputerName      : www.redaktionsgemeinschaft.net
RemoteAddress     : 217.160.0.130
InterfaceAlias    : vEthernet (Virtu-Switch)
SourceAddress     : 192.168.0.250
PingSucceeded     : True
PingReplyDetails (RTT) : 58 ms

PS C:\Users\Administrator> Test-Netconnection -Computername "www.redaktionsgemeinschaft.net" -DiagnoseRouting -InformationLevel Detailed

ComputerName      : www.redaktionsgemeinschaft.net
RemoteAddress     : 217.160.0.130
SelectedSourceAddress : 192.168.0.250
OutgoingInterfaceIndex : 18
SelectedNetRoute   : DestinationPrefix: 0.0.0.0/0
                   : NextHop: 192.168.0.1
DestinationAddressSelectionEvents :
RouteSelectionEvents :
SourceAddressSelectionEvents :
RouteDiagnosticsSucceeded : True

PS C:\Users\Administrator>
```

Abbildung 5.25: Direkt die Verbindung zu einem System im Netzwerk überprüfen? Das geht mit dem Cmdlet »Test-NetConnection«.

Wer sich jetzt eher an den Befehl »Tracert« erinnert fühlt, soll natürlich auch dafür ein PowerShell-Pendant präsentiert bekommen:

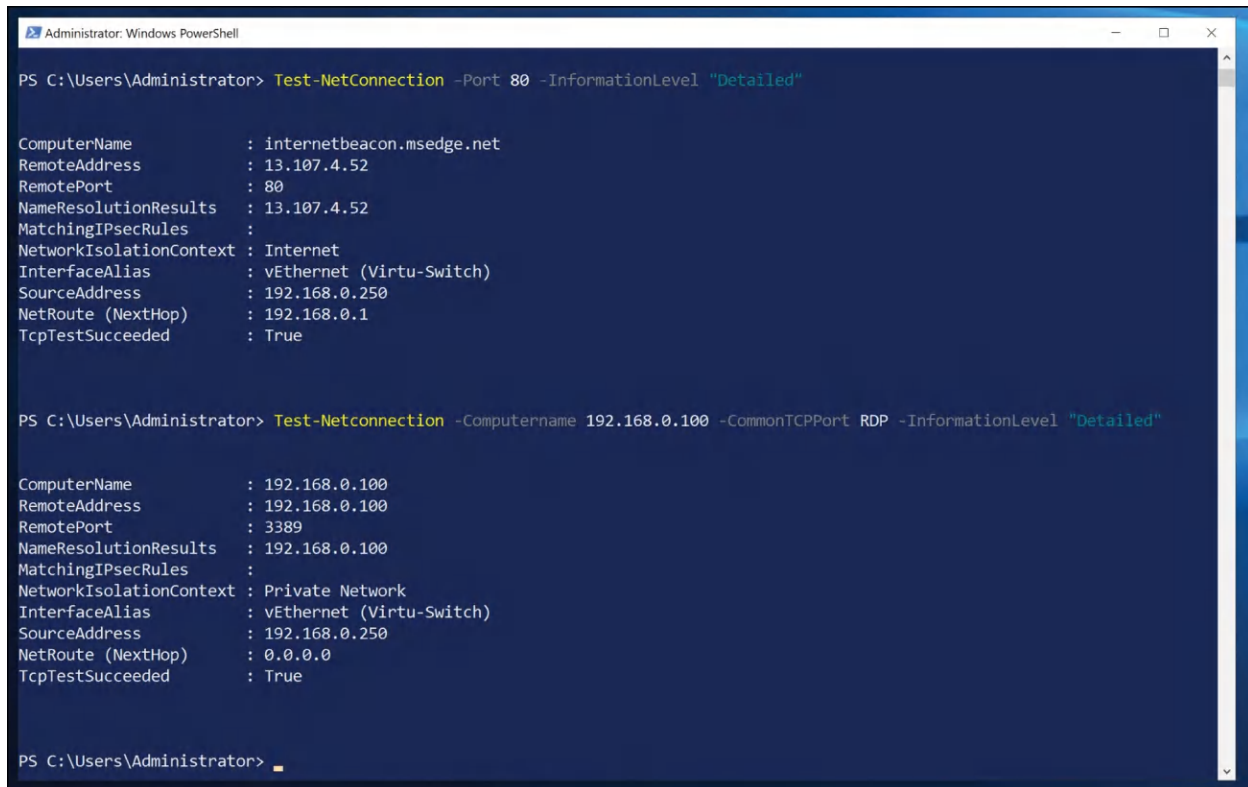
```
Test-Netconnection -Computername  
"www.redaktionsgemeinschaft.net" -TraceRoute
```

Aber das Cmdlet Test-Netconnection kann noch mehr. So kann es Ihnen beispielsweise auch bei der Suche nach offenen Ports oder einem bestimmten Port helfen:

```
Test-NetConnection -Port 80 -InformationLevel "Detailed"
```

Wenn Sie dabei wie in unserem Beispiel hier und im oberen Beispiel in [Abbildung 5.26](#) keinen Remote-Computer als Ziel angeben, verwendet das Cmdlet automatisch einen Default-Microsoft-Server mit der Adresse

»internetbeacon.msedge.net«.



```
Administrator: Windows PowerShell

PS C:\Users\Administrator> Test-NetConnection -Port 80 -InformationLevel "Detailed"

ComputerName           : internetbeacon.msedge.net
RemoteAddress          : 13.107.4.52
RemotePort             : 80
NameResolutionResults  : 13.107.4.52
MatchingIPsecRules     :
NetworkIsolationContext : Internet
InterfaceAlias         : vEthernet (Virtu-Switch)
SourceAddress          : 192.168.0.250
NetRoute (NextHop)     : 192.168.0.1
TcpTestSucceeded       : True

PS C:\Users\Administrator> Test-NetConnection -Computername 192.168.0.100 -CommonTCPPort RDP -InformationLevel "Detailed"

ComputerName           : 192.168.0.100
RemoteAddress          : 192.168.0.100
RemotePort             : 3389
NameResolutionResults  : 192.168.0.100
MatchingIPsecRules     :
NetworkIsolationContext : Private Network
InterfaceAlias         : vEthernet (Virtu-Switch)
SourceAddress          : 192.168.0.250
NetRoute (NextHop)     : 0.0.0.0
TcpTestSucceeded       : True

PS C:\Users\Administrator> _
```

Abbildung 5.26: Mithilfe von »Test-NetConnection« können Sie nicht nur die Verbindung ins Netzwerk, sondern auch die zu offenen Standard-Ports untersuchen.

Geht es hingegen darum, zu testen, ob die Verbindung auf einem Standard-Port des Zielsystems offen ist, so stellt die Option -CommonTCPPort die verschiedensten Möglichkeiten wie RDP, SMB oder HTTP zur Auswahl bereit:

```
Test-Netconnection -Computername 192.168.0.100 -CommonTCPPort RDP -InformationLevel "Detailed"
```


Teil II

Einrichtung und wichtige Rollen



IN DIESEM TEIL ...

- ✓ Installation, Installationsmedien und der Core-Server
- ✓ Active Directory
- ✓ DNS und DHCP
- ✓ Speicherdienste und Dateiserver
- ✓ Erweiterte Ressourcenfreigaben
- ✓ Hyper-V und virtuelle Computer
- ✓ Druckdienste

Kapitel 6

Installation von Windows Server

IN DIESEM KAPITEL

Überlegungen vor der ersten Installation

Welches Installationsmedium soll es sein?

Schritt für Schritt: die Installation

Alternative: Core-Server installieren

Wenn Sie eine der vielen Anleitungen zur Installation eines Windows-Servers im Internet lesen, so werden Sie darin häufig die Frage finden, ob Sie eine Neuinstallation oder ein Update einer bestehenden Installation vornehmen wollen. Wird beispielsweise bereits Windows Server 2012 R2 ausgeführt, so können Sie auch ein Upgrade auf Windows Server 2016 oder Windows Server 2019 durchführen. Aber nicht für alle ältere Betriebssysteme stellt Microsoft einen Upgrade-Pfad zu einem neueren Betriebssystem zur Verfügung. Bevor Sie ein Betriebssystem-Update starten, sollten Sie, wie bei allen Updates, alle Daten dieses Systems auf einem externen Medium sichern.

In der Regel werden Sie aber eine Neuinstallation auf einem freien System (wird auch als Bare-Metal-Installation bezeichnet) vornehmen wollen. Sie können aber natürlich einen Windows Server parallel zu einer bereits bestehende Windows-10-Installation in einer anderen Partition installieren. Allerdings sollten Sie dann auch genügend freien Speicherplatz auf der oder den Festplatten haben.

Die Frage nach dem Boot-Medium

Bis vor wenigen Jahren war es noch keine Frage: Wer ein neues

Betriebssystem installieren wollte, bekam vom Hersteller ein Installationsmedium (oder in den Zeiten der Disketten auch durchaus mehrere Medien) geliefert, von dem aus er seinen Computer zur Installation neu startete. Aktuell werden sich die meisten Nutzer eine ISO-Datei mit dem Betriebssystem herunterladen und diese dann von einem Medium aus starten. ISO-Dateien sind einfach nur Abbilder von DVD-Images und können dementsprechend auch auf eine DVD gebrannt werden, wenn Sie dann ein solches Medium vorziehen. Wollen Sie das Betriebssystem nur in einer virtuellen Maschine beispielsweise unter Virtual Box oder VMware Player installieren, so können Sie das ISO-Image auch direkt mithilfe der Virtualisierungs-Software laden.

Besonders interessant dürfte aber für die meisten Anwender die Installation mithilfe eines USB-Sticks sein, da in der Regel jede moderne PC-Hardware einen Start von einem solchen Medium unterstützt. Allerdings reicht es dazu nicht aus, einfach den Inhalt einer ISO-Datei auf einen Stick zu kopieren. Sie benötigen einen bootfähigen USB-Stick, damit Ihr PC die Installation beginnen kann. Im Internet finden Sie diverse Programme, die diese Aufgabe erfüllen. Wir empfehlen in diesem Fall die freie Software »Rufus«, die Sie beispielsweise unter der Adresse <https://rufus.ie/> herunterladen und direkt ohne Installation auf einem Windows-Rechner starten können ([Abbildung 6.1](#)). Da die ISO-Abbilder der Windows-Server in der Regel etwas größer als 5 GByte sind, sollten Sie auf jedem Fall einen USB-Stick bereithalten, der diese Größe problemlos aufnehmen kann. Wir haben die besten Erfahrungen mit 8 GByte großen Medien gemacht.

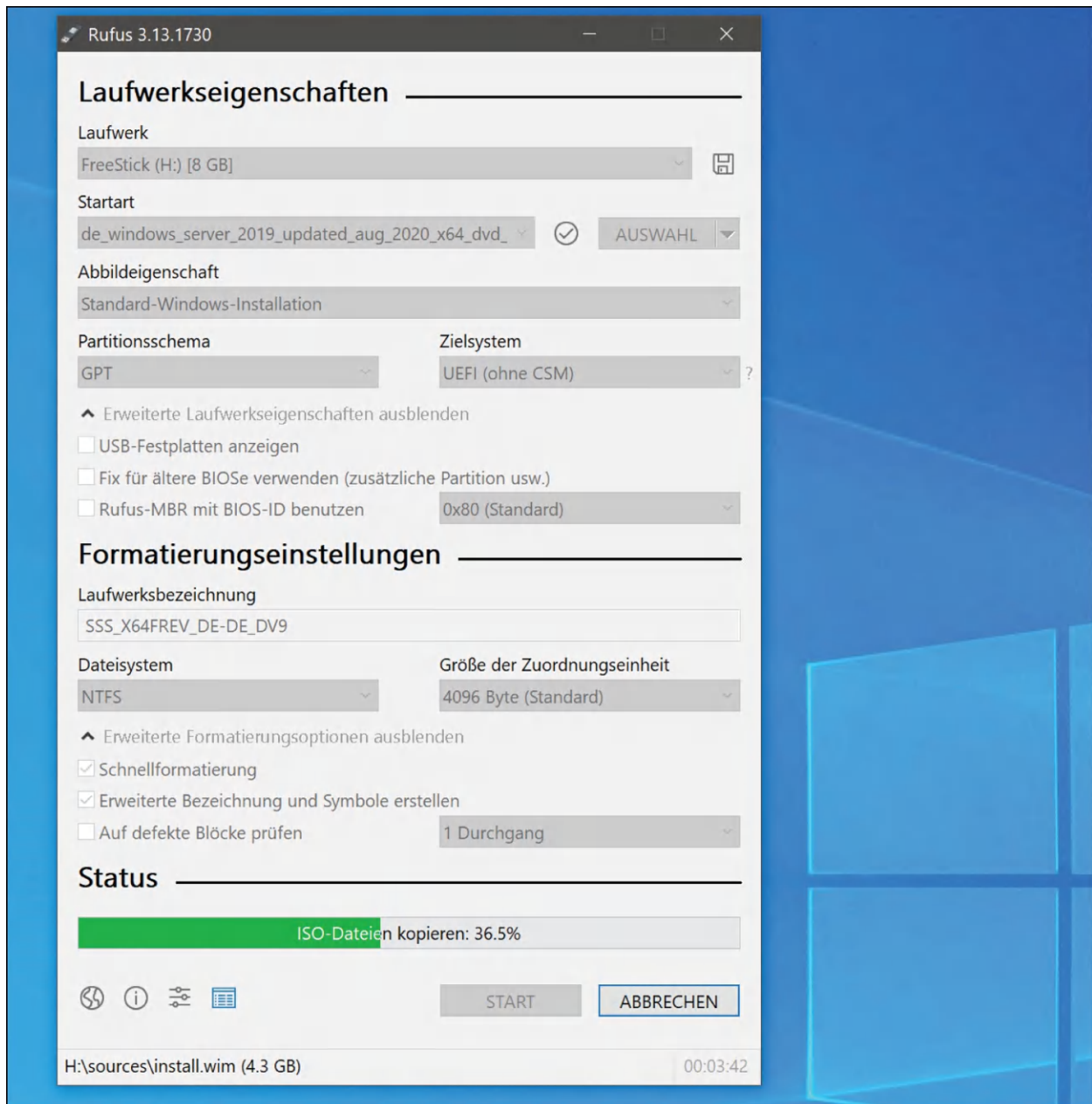


Abbildung 6.1: Die freie Software »Rufus« hilft dabei, einen bootfähigen USB-Stick für die Server-Installation zu erstellen.

Ein großer Vorteil der Software besteht darin, dass sie beispielsweise bei der Verwendung einer ISO-Datei mit dem Windows Server 2019 automatisch die richtigen Standardwerte für das Zielsystem (siehe [Abbildung 6.1](#)) einstellt. Nachdem der USB-Stick eingerichtet ist, können Sie ihn mit einem USB-Port Ihres Rechners verbinden und diesen starten. Die meisten gängigen UEFI-Varianten auf neueren PCs unterstützen ein Boot-Menü, über das Sie Ihr System direkt vom USB-Stick starten

können. Ein solches Menü lässt sich zumeist über den Druck auf die Taste **F12**, **F10** oder **Esc** öffnen. Welche Taste es ist, hängt vom Hersteller des Mainboards Ihres PC ab.

Schritt für Schritt: die Installation

Nachdem Sie Ihr System mit dem USB-Stick hochgefahren haben, startet die Installation von Windows Server 2019 und präsentiert Ihnen zunächst den ersten Auswahlbildschirm ([Abbildung 6.2](#)) auf dem Sie neben der Sprache der Installation auch das Format für Uhrzeit und Währung sowie die Tastaturbelegung beziehungsweise Eingabemethode wählen können.

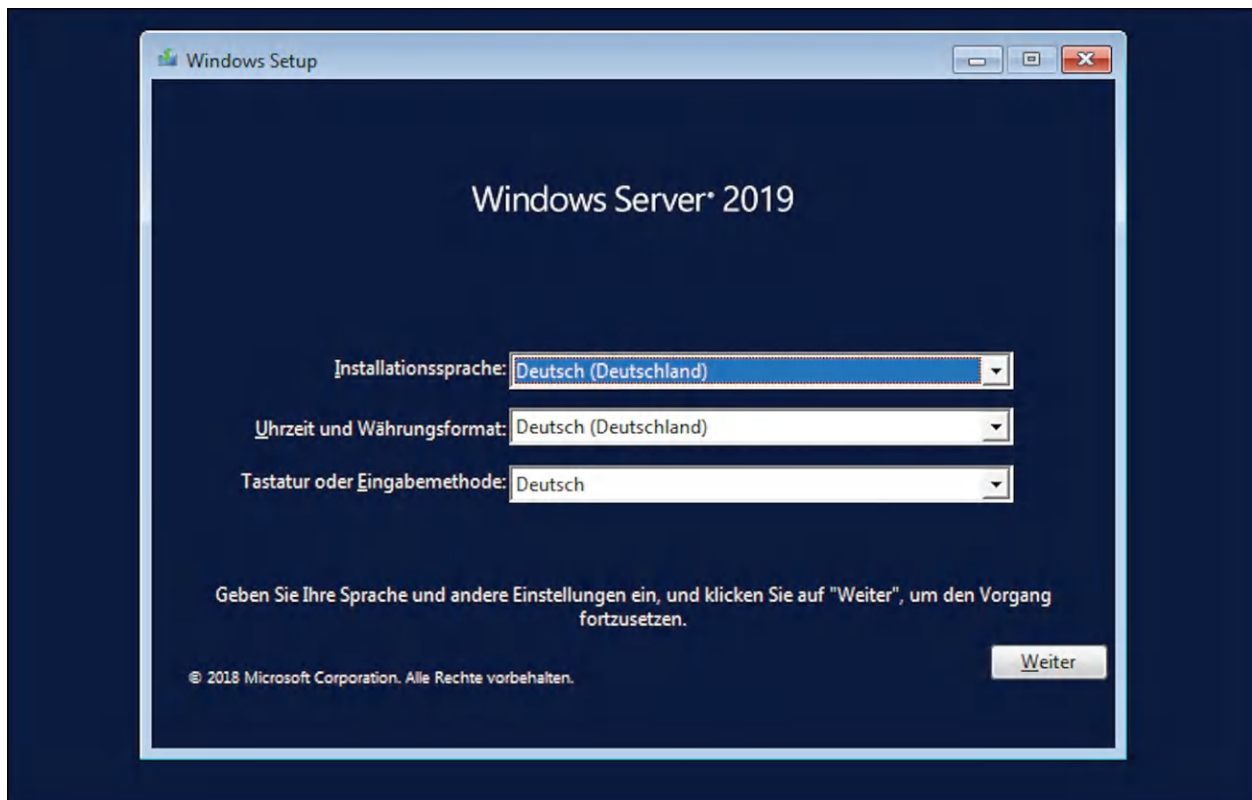


Abbildung 6.2: Der erste Bildschirm bei der Installation von Windows Server 2019 zeigt in der Regel die richtige Vorauswahl für das System an.

Hier werden Sie zumeist nichts ändern müssen, da Windows Ihnen in der Regel schon die richtigen Werte vorgibt.

1. Nach einem Mausklick auf WEITER müssen Sie dann auf dem nächsten Bildschirm JETZT INSTALLIEREN auswählen.

2. Danach wählen Sie die gewünschte Windows-Server-Edition aus, die Sie auf Ihrem System installieren wollen. Wie Sie in [Abbildung 6.3](#) sehen, können Sie hier entscheiden, ob Sie einen Server mit grafischer Benutzeroberfläche (wie Sie diese beispielsweise von Windows 10 kennen) oder einen sogenannten Core-Server, der nur über die Kommandozeile zu verwalten ist, installieren wollen. Achtung: Der Core-Server ist hier als Standard vorgewählt, Sie müssen in diesem Menü also die DESKTOPDARSTELLUNG auswählen, wenn Sie die Windows-Oberfläche nutzen wollen.

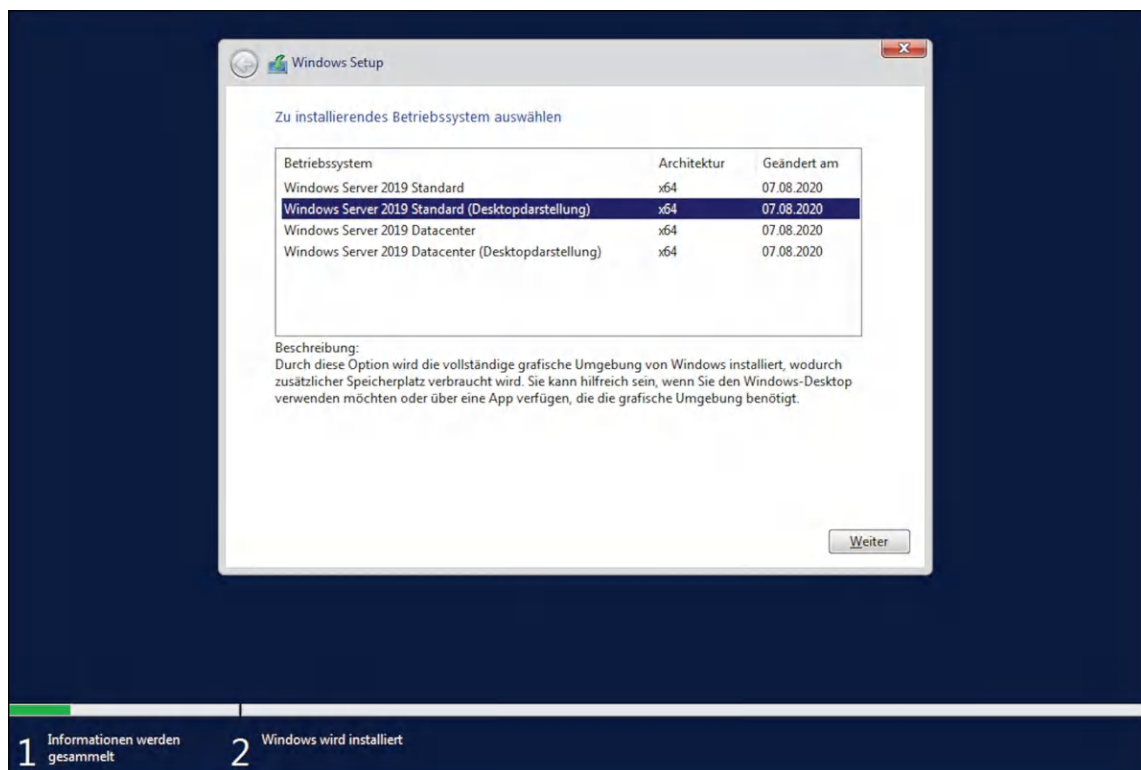


Abbildung 6.3: Eine wichtige Auswahl bei der Installation: Welche Edition von Windows Server wollen Sie auf Ihrem System einsetzen?



Bei der Wahl zwischen DESKTOPDARSTELLUNG und Core-Server sollten Sie genau überlegen, wofür Sie sich entscheiden. Haben Sie beispielsweise die DESKTOPDARSTELLUNG gewählt (also einen Server mit Windows-Oberfläche) so können Sie dieses System später nicht einfach wieder in einen Core-Server umwandeln. Dazu müssen Sie dann Windows Server 2019 neu

installieren. Die grafische Oberfläche (GUI) lässt sich hingegen später nachinstallieren.

3. Auf dem folgenden Bildschirm müssen Sie dann das Kästchen für ICH AKZEPTIERE DIE LIZENZBEDINGUNGEN anklicken, damit es weitergeht.
4. Danach werden Sie aufgefordert, die Art der Installation zu wählen ([Abbildung 6.4](#)). Handelt es sich um einen »Ersteinsatz« des Betriebssystems, so sollten Sie unbedingt die zweite Option BENUTZERDEFINIERT: NUR WINDOWS INSTALLIEREN auswählen. Auch wenn es dieser Bildschirm anders suggeriert: Gerade die Auswahl des Updates einer vorherigen Windows-Version erfordert die größere Erfahrung vom Nutzer, weil schnell wichtige Daten überschrieben werden oder gelöscht werden können. Die sogenannte benutzerdefinierte Installation erfordert nur einen ausreichend großen freien Bereich auf der Festplatte, den Sie – falls er noch nicht vorhanden ist – dann im nächsten Schritt auch noch anlegen können.

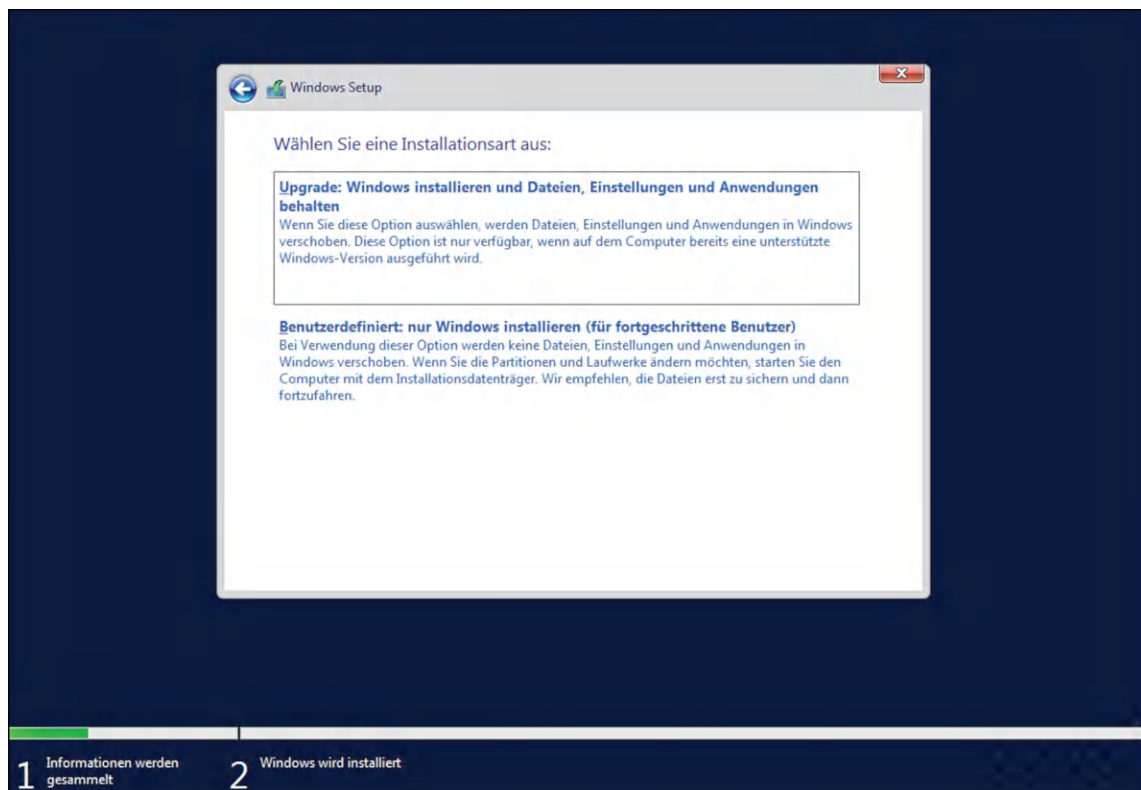


Abbildung 6.4: Die Auswahl der Installationsart: Bei einer neuen Installation von Windows Server ist die zweite Option zumeist die richtige Wahl.

5. Der folgende Bildschirm zeigt Ihnen die Aufteilung der Festplatte(n) in Ihrem System. Sie können in diesem Menü, das Sie in der [Abbildung 6.5](#) sehen, bei entsprechend freiem Platz auf dem Datenträger auch eine weitere neue Partition anlegen sowie einen bestehenden Bereich formatieren oder auch löschen. Sie sollten beim Festplattenplatz auf keinem Fall zu sparsam sein: 100 GByte oder auch mehr helfen Ihnen, auf der »sicheren Seite« zu sein, wenn Sie Ihren Server erst einmal im Einsatz haben.
6. Haben Sie die Einteilung der Festplatte nach Ihren Vorstellungen und Bedürfnissen vorgenommen, wählen Sie WEITER. Der eigentliche Installationsvorgang startet, und Windows beginnt damit, die benötigten Dateien, Features und Updates auf der Festplatte zu installieren.
7. Anschließend führt das Betriebssystem einen Neustart aus. Direkt danach erfolgt ein sehr wichtiger Schritt: Sie werden aufgefordert, das Administrator-Passwort für Ihren Server festzulegen ([Abbildung 6.6](#)).

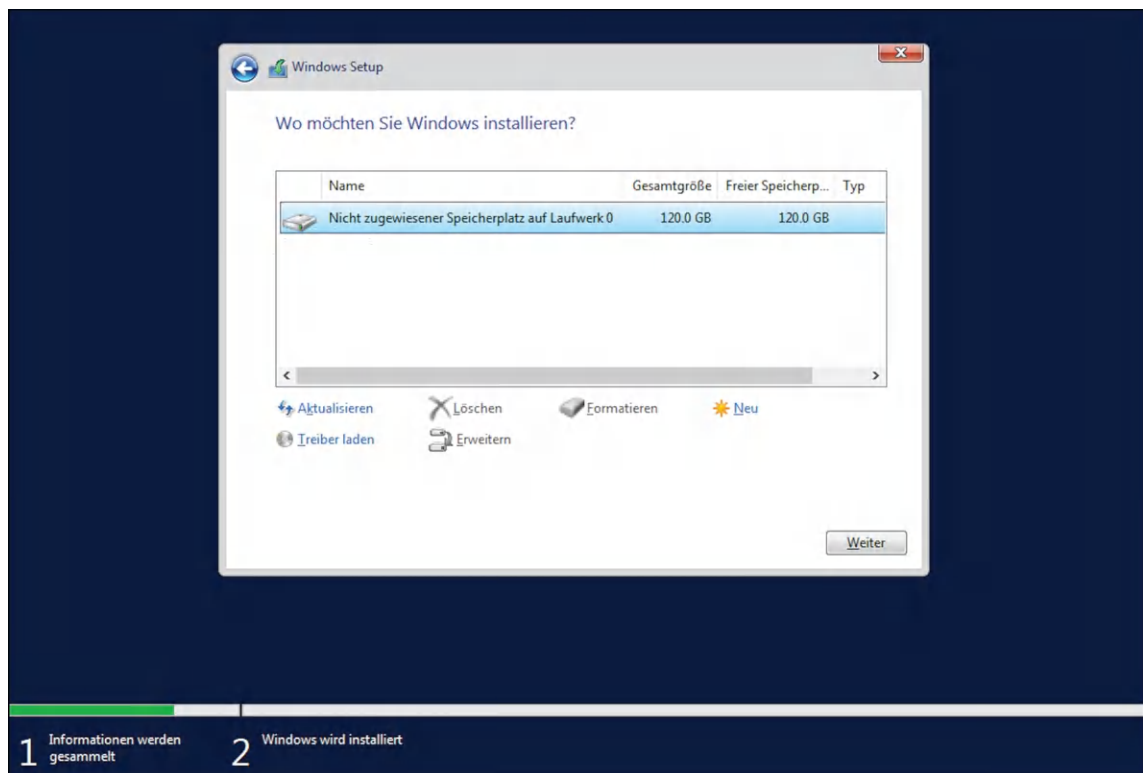


Abbildung 6.5: Wo möchten Sie Windows installieren? In diesem Menü können Sie die Einteilung auf der Festplatte nach Ihren Vorstellungen ändern.

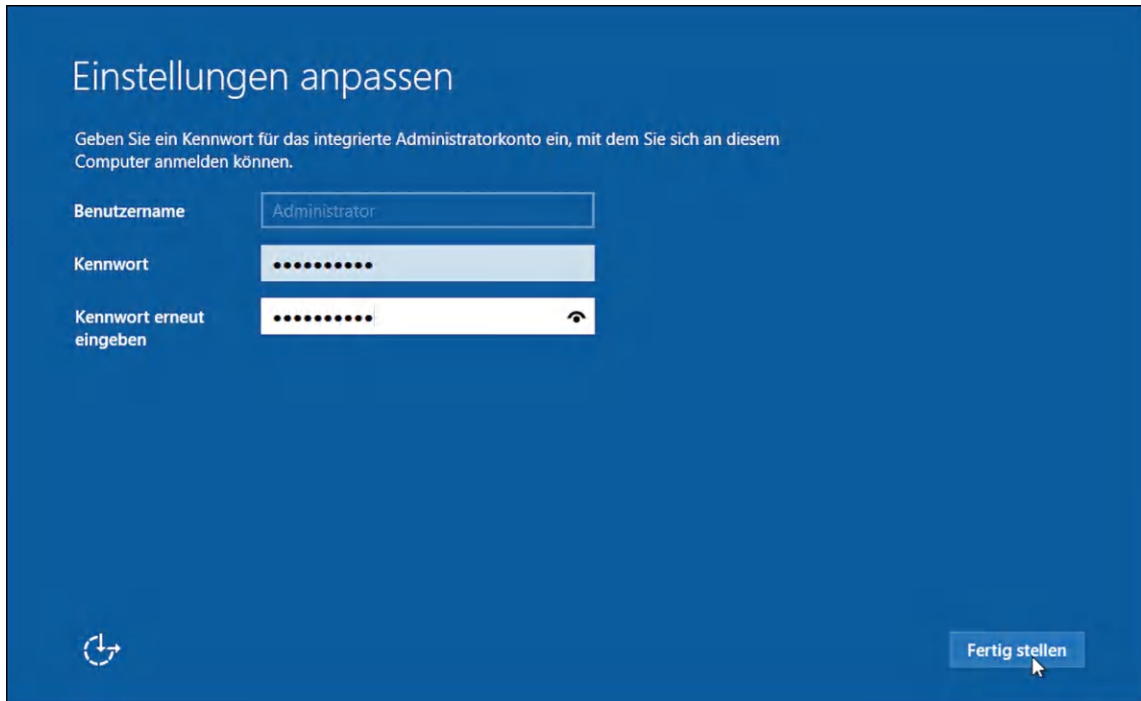


Abbildung 6.6: Der wichtigste Schritt nach dem ersten Neustart: das Festlegen eines Administrator-Passworts



Auch an dieser Stelle noch einmal der wichtige Hinweis: Selbst für einen Testserver sollten Sie keinesfalls ein zu triviales Passwort auswählen.

8. Danach erscheint der Anmeldebildschirm des Windows-Servers, an dem Sie sich nun mithilfe des zuvor eingegebenen Administrator-Passworts anmelden können.
9. Auch wenn der Anmeldebildschirm dem eines Windows-10-Systems sehr ähnlich ist, sollten Sie an dieser Stelle doch eine Besonderheit beachten: Sie müssen hier zunächst mit der Tastenkombination **Strg** + **Alt** + **Entf** den Bildschirm entsperren, bevor Sie sich mit Kontonamen und Passwort anmelden können. Diesen Hinweis finden Sie auch auf der Anmeldeseite des Systems ([Abbildung 6.7](#)).



Abbildung 6.7: Geschafft: Der Windows-Server ist installiert. Zum Entsperren des Anmeldebildschirms müssen Sie **Strg** + **Alt** + **Entf** verwenden.

Alternative: Core-Server installieren

Wenn Sie ohne die bekannte Windows-Oberfläche mit Ihrem Server arbeiten wollen, dann können Sie während der Installation bei der Auswahl der Editionen ([Abbildung 6.3](#)) die Standardeinstellung wählen. Danach läuft die Installation des Windows-Servers auf die gleiche Art und Weise ab, wie wir sie hier zuvor geschildert haben. Den ersten Unterschied werden Sie dann an der Stelle bemerken, an der Sie das System nach dem Neustart auffordert, das Passwort für das Administrator-Konto einzugeben. Im Gegensatz zu der Oberfläche, die Sie in der [Abbildung 6.6](#) sehen, bekommen Sie nun nur noch die sehr eingeschränkte Oberfläche der Kommandozeile präsentiert ([Abbildung 6.8](#)), um dieses Passwort einzugeben.

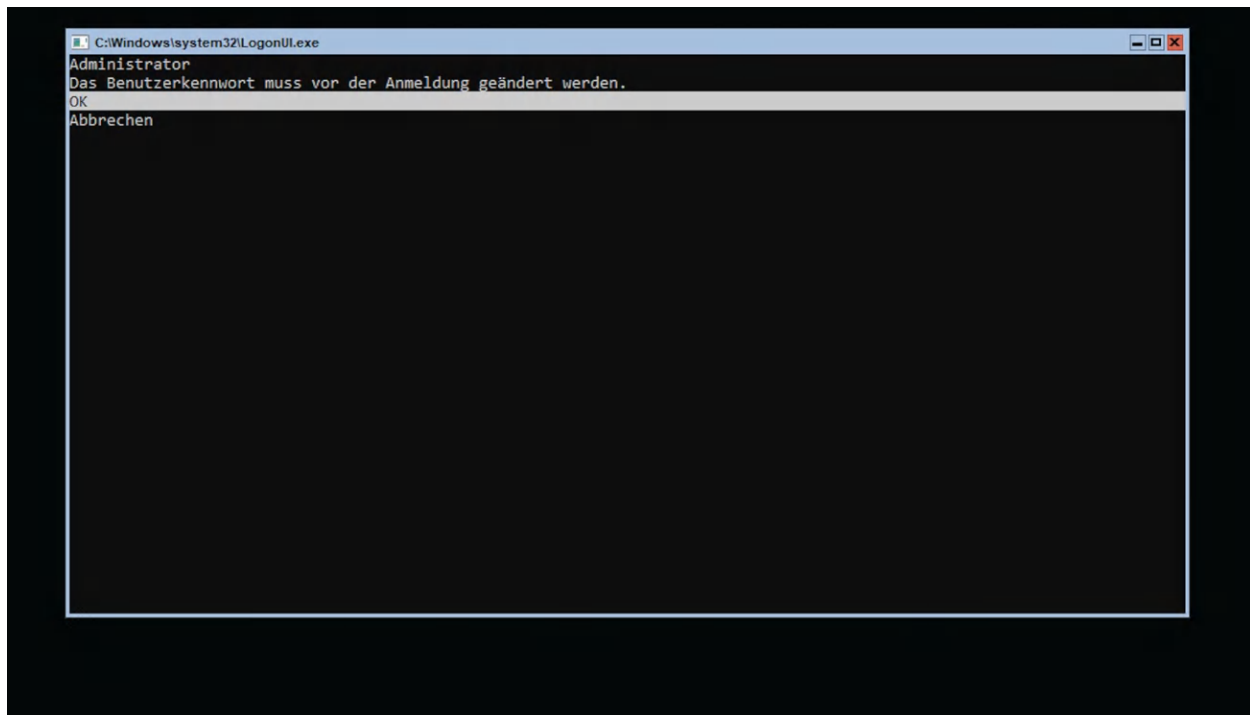


Abbildung 6.8: Die sehr »spartanische« Oberfläche bei der Installation als Core-Server fordert auf diese Weise die Eingabe des Administrator-Passworts

Auch der nachfolgende Anmeldebildschirm bietet Ihnen dann nur noch den Hinweis auf die Entsperrung mittels + + in einem Konsolenfenster. Nach der Anmeldung müssen Sie dann auf entsprechende Kommandozeilenprogramme oder die PowerShell zurückgreifen, um Ihren Server weiter einzurichten und zu bedienen.

Wollen Sie an dieser Stelle einige grundlegende Einstellungen wie Netzwerkeinstellungen, Computernamen, Domänen-Mitgliedschaft setzen und Windows aktualisieren und aktivieren, so können Sie dazu beispielsweise das Kommandozeilen-Programm Serverkonfiguration verwenden. Dieses Werkzeug können Sie mit dem Befehl `sconfig` starten und sich dann in seiner Oberfläche durch die verschiedenen Menüpunkte bewegen ([Abbildung 6.9](#)).

Einige wenige Programme der »normalen« Windows-Oberfläche lassen sich auch auf dem Core-Server starten. Dazu gehört beispielsweise der Editor (NOTEPAD.EXE). So nutzen einige Administratoren dann dieses Programm, um mithilfe seines ÖFFNEN-Dialogs leichter im Dateisystem zu navigieren, was in der Kommandozeile etwas mehr Schwierigkeiten

bereiten kann ([Abbildung 6.10](#)).

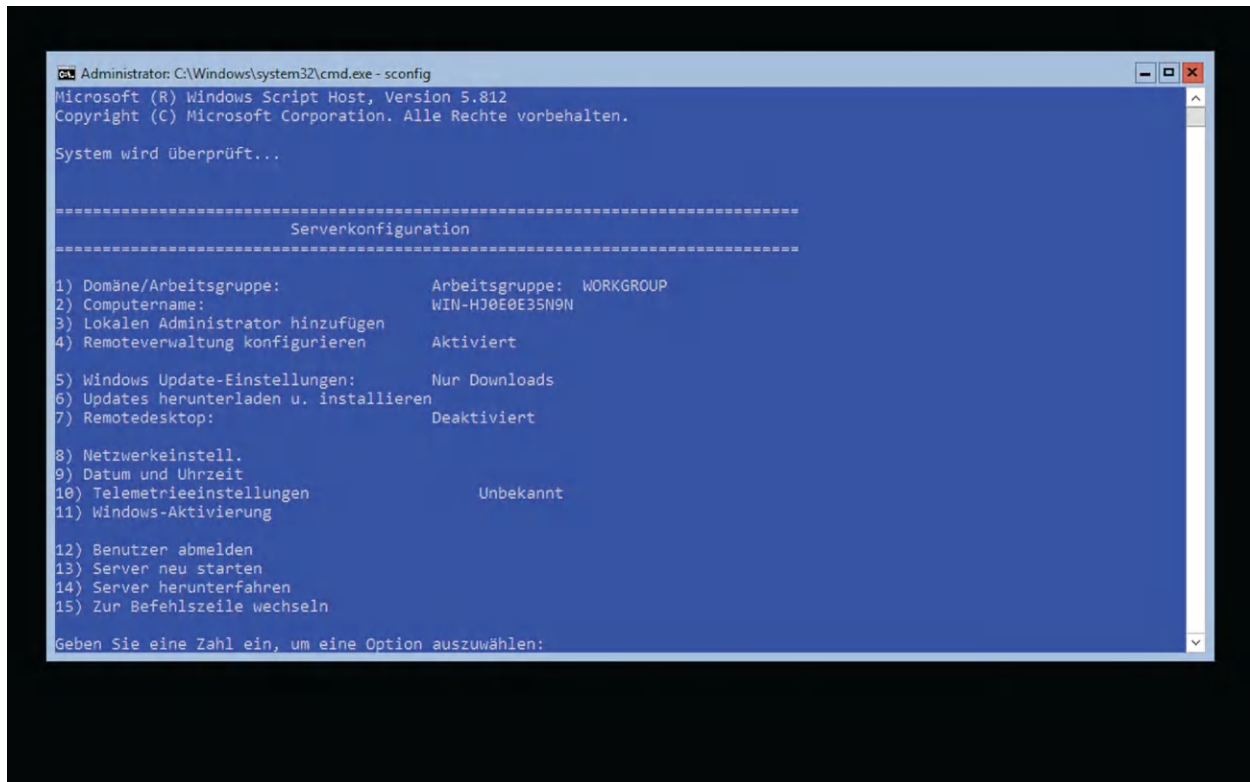


Abbildung 6.9: In einer Core-Server-Installation stehen einige Programme an der Kommandozeile bereit, die eine weitere Einrichtung erleichtern. Zum Beispiel das hier gezeigte Werkzeug »Serverkonfiguration« (sconfig).

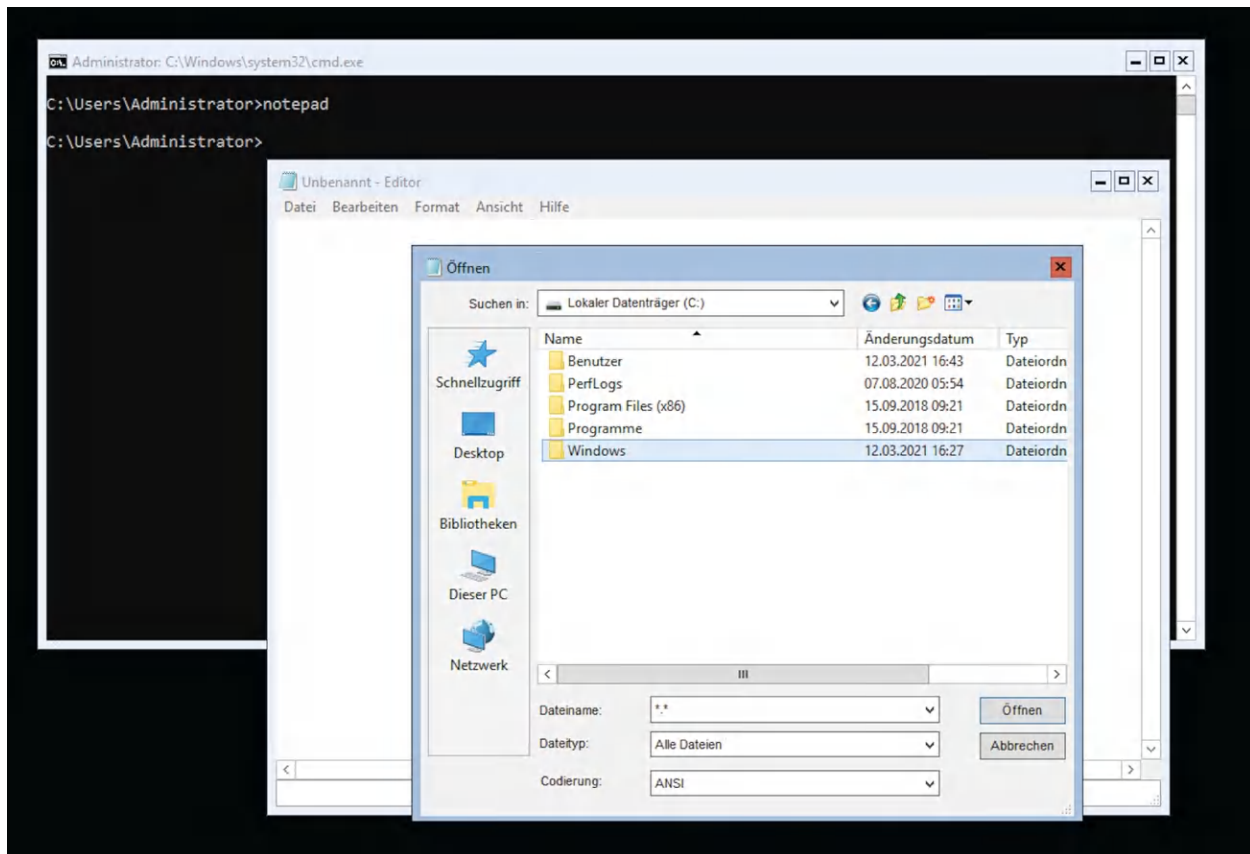


Abbildung 6.10: Der Editor kann auch auf dem Core-Server eingesetzt werden und so bei der Navigation im Dateisystem helfen.

Kapitel 7

Active Directory

IN DIESEM KAPITEL

- Grundbegriffe rund um das AD
- Installation eines Domänencontrollers
- Erste Benutzer und Computer
- Administrative Konten
- Hinzufügen eines weiteren DC oder RODC
- Replikation
- Remote-Verwaltung
- Active-Directory-Papierkorb
- Gruppen und Rechte

Normalerweise füllt das Thema Active Directory ein eigenes Buch – so umfangreich sind die technischen und organisatorischen Möglichkeiten des wahrscheinlich erfolgreichsten Verzeichnisdiensts auf unserem Planeten.

Wir beschränken uns an dieser Stelle auf die zwingend erforderlichen Grundlagen zum Thema AD, befassen uns mit der Installation und dem Aufbau der notwendigen Technik, um den Verzeichnisdienst in einer KMU-Umgebung (kleine und mittlere Unternehmen) einzurichten.

Auch wenn es sich heutzutage jeder Administrator überlegen sollte, ob es noch erforderlich ist, Server-Strukturen lokal vorzuhalten, sollte auch bei Einsatz von Azure und Office365 ein gewisses Grundwissen über das Active Directory vorliegen, weswegen wir zumindest unter »Laborbedingungen« eine eigene Installation eines AD durchführen wollen.



Active-Directory-artige Umgebungen sind nicht auf die Produkte von Microsoft beschränkt. Die Firma Univention bietet mit dem Univention Corporate Server, kurz UCS, eine Open-Source-Implementation des Microsoft-Active-Directory-Verzeichnisdiensts auf Basis einer komplett vorkonfigurierten Samba-Software auf Debian-Linux-Basis. Neben dem Verzeichnisdienst als grundlegende Verwaltungsstruktur bietet der UCS weitere Server-Dienste wie einen CIFS/SMB-kompatiblen Datei- und Druck-Service. Die Grundvariante des UCS ist somit in der Lage, einen Microsoft-Domänencontroller gänzlich zu ersetzen. Im »Core«-Paket ist der UCS komplett kostenfrei.

Es geht dabei um nicht mehr, aber auch nicht weniger, als den Ersatz eines Windows-Servers für kleinere Installationen mit Benutzerverwaltung, PC-Organisation, Gruppenverwaltung und Freigaben für Drucker und Verzeichnisse.

Was ist überhaupt ein Active Directory?

Ein Active Directory ist ein erweiterbarer und skalierbarer Verzeichnisdienst, mit dem Sie als Administrator Netzwerkressourcen effizient verwalten können. Gut – und was ist dann ein Verzeichnisdienst? Ein Verzeichnisdienst (englisch: »Directory Service«) stellt in einem Netzwerk eine zentrale Sammlung von Daten zur Verfügung. Diese Daten sind in einer hierarchischen Datenbank gespeichert – Clients können, je nach Berechtigung, diese Informationen durchsuchen, modifizieren und löschen. Das Active Directory speichert unter anderem die Informationen zu:

- ✓ Benutzern
- ✓ Gruppen
- ✓ Computern

- ✓ Netzwerkdiensten
- ✓ Server
- ✓ Freigaben
- ✓ Peripheriegeräten
- ✓ Speicherplatz
- ✓ Zugriffsberechtigungen
- ✓ Anwendungen

In unstrukturierten Umgebungen ohne einen zentralen Verzeichnisdienst, beispielsweise wenn drei Computer in einer Arbeitsgruppe organisiert sind, trägt jeder der Computer die auf ihm eingerichteten Informationen zu Freigaben und Berechtigung selbst. Ist dieser Computer ausgeschaltet oder defekt, ist kein Zugriff auf diese Informationen möglich. Nicht nur die Daten stehen nicht mehr zur Verfügung, auch die Information, dass es überhaupt Daten unter einer Freigabe mit Berechtigungen gab, sind weg. Überspitzt dargestellt: Wird das Telefon ausgeschaltet, verschwinden die ganze Telefonnummer und das im Telefon gespeicherte Adressbuch.

In einer Verzeichnisdienststruktur gibt es zentrale Anlaufstellen, die diese Daten bereithalten. Das Verzeichnis speichert alle Geräte und Ressourcen eines Netzwerks und alle damit verbundenen Attribute.

Ziel dieser strukturellen Darstellung ist es, die Organisation als digitales Abbild nachzubilden. Einzelne Unternehmens- und Organisationsbereiche sind über sogenannte Domänen voneinander abgegrenzt. Die Struktur einer Domäne kann hierarchisch sein. Eine Domäne ist ein organisatorisch abgetrennter Netzbereich, in dem gleiche Sicherheitseinstellungen und -richtlinien gelten.

Grundbegriffe rund um das Active Directory

Es geht leider nicht anders – ein paar Begriffe müssen bereits bekannt sein, sonst wird das nichts mit der fehlerfreien Installation eines AD.

- ✓ Domäne – Organisatorisch abgetrennter Netzwerkbereich, in dem die gleichen Sicherheitseinstellungen und Richtlinien gelten; wird durch das Schema und die Konfiguration beschrieben.
- ✓ LDAP (Lightweight Directory Access Protocol) – Das Active Directory von Microsoft basiert auf LDAP. Dieses Protokoll definiert die Syntax, über die Informationen aus dem Verzeichnis abzufragen sind.
- ✓ Kerberos – Das im AD-Umfeld zum Einsatz kommende Authentifizierungsprotokoll; sorgt dafür, dass ein Benutzer, nach erfolgter Anmeldung, nicht ständig wieder sein Passwort eingeben muss.
- ✓ CIFS (Common Internet File System) – Das Protokoll zur Speicherung von Dateien im Netzwerk; auch als »Server Message Block« (SMB) bekannt.
- ✓ DNS (Domain Name System) – Das Protokoll, über das die Namensauflösung arbeitet.
- ✓ Schema – Beschreibt die formale Struktur des Verzeichnisdiensts.
- ✓ Konfiguration – Die Struktur des Active Directory befindet sich in der Konfiguration.
- ✓ Domänencontroller – Server mit der Rolle zur Verwaltung der Domäne. Größere Installationen verfügen über mehrere Domänencontroller (DC).
- ✓ RODC (Read Only Domain Controller) – Ein vollwertiger Domänencontroller, der Anfragen von Clients verarbeitet, aber selbst keine schreibenden Zugriffe in die Datenbank vornimmt.
- ✓ Replikation – Das Active Directory arbeitet im Multimasterbetrieb. Jeder vollwertige DC ist in der Lage, Änderungen vorzunehmen, die an die anderen DCs und RODCs zu übermitteln sind. Dieser Vorgang heißt Replikation.

Installation einer Active-Directory-

Domäne

Die Einrichtung einer Domäne mit einem DC ist an sich kein Hexenwerk. Wir gehen an dieser Stelle davon aus, dass es sich um den ersten DC in der Umgebung handelt – oder dass wir uns in einer »Laborumgebung« befinden. Sollte es in demselben Netzwerk bereits ein Active Directory geben, auf das die Computer bereits Zugriff haben, und sollten Sie als Administrator noch niemals zuvor ein eigenes AD aufgesetzt haben, ist das der ideale Zeitpunkt, um mit dem Administrator der bereits vorhandenen Umgebung Kontakt aufzunehmen – ansonsten wird es der Kollege vermutlich in Kürze von selbst tun – und das wollen Sie nicht!

Erforderliche Vorbereitung:

- ✓ Installiertes Windows-Server-Betriebssystem auf einer »vertrauenswürdigen Maschine«
 - Hardware oder virtuelle Maschine ist irrelevant
 - Idealerweise ein frisch installiertes Windows
 - Möglichst keine Applikation oder »Altlasten« auf dem System
 - Sicherer Betrieb hinter einer Firewall
 - Frei von Schadprogrammen
 - Für den Dauerbetrieb ausgelegte Hardware
- ✓ Alle aktuellen Windows-Updates
- ✓ Kein erforderlicher ausstehender Neustart
- ✓ Feste IPv4-Adresse
- ✓ Feste IPv6-Adresse, sofern möglich
- ✓ Servernamen bereits festgelegt
- ✓ Kenntnis der aktuellen DNS-Struktur
- ✓ Netzwerkkonfiguration ist als »privates Netzwerk« eingestuft
- ✓ Komplexes, lokales Administrationskennwort
- ✓ Festgelegter Domänenname



Zur Installation einer neuen Domäne müssen Sie diese benennen – logisch! Die Beantwortung der Frage, wie die Domäne heißen soll, ist nicht ganz so trivial, wie es zunächst scheint.

In älteren Empfehlungen hieß es stets, die AD-Domäne sollte für den vollqualifizierte Domänennamen (FQDN) um ein inoffizielles Suffix wie `.site` oder `.local` erweitert werden, da dies keine Top-Level-Domänennamen (TLD) seien und es somit nicht zu unerwünschten Namensauflösung kommen würde.

Aber – wie können wir uns sicher sein, dass sie das nicht irgendwann einmal werden? Angenommen die Organisation oder Firma heißt »Redaktionsgemeinschaft Bär-Schlede«, dann könnten Sie `redaktionsgemeinschaft-baer-schlede.de` als Website im Internet reservieren. Etwas lang zu schreiben, daher doch eher `baer-schlede.de`. Typischerweise richten Sie eine Webseite bei einem Dienstleister Ihrer Wahl im Internet ein und reservieren dort die Domäne. Ein guter Name für die Active-Directory-Domäne (Stammdomäne) wäre nun

`ad.baer-schlede.de`

Um nun aber sicherzustellen, dass sich Anwender bei der Anmeldung nicht im Schema `ad\user`, sondern `baer-schlede\user` anmelden, ist es erforderlich, bei der Installation des ersten Domänencontrollers den NetBIOS-Namen anstelle `ad` auf `baer-schlede` umzustellen!

Das »Gleichschalten« von DNS- und Domänennamen hat für die Organisation Vorteile:

- ✓ Ein einziger Domänenname auf der obersten Ebene
- ✓ Trennung zwischen interner und externer Nutzung ist einfach möglich
- ✓ Weltweit eindeutige Servernamen
- ✓ Zertifikate sind stets passend
- ✓ Anmeldung über die öffentliche E-Mail-Adresse möglich, aber

auch *Domänenname\Benutzernamen*

Die Installation geschieht über den SERVER-MANAGER und erfordert lokale Administrationsrechte:

1. Melden Sie sich als lokaler Administrator an und starten Sie den Server-Manager, alternativ starten Sie den SERVER-MANAGER als Administrator, hierzu ist ein Rechtsklick auf den SERVER-MANAGER erforderlich.
2. Klicken Sie oben rechts im SERVER-MANAGER auf HINZUFÜGEN VON ROLLEN/FEATURES.
3. Wählen Sie den lokalen Server aus.
4. Wählen Sie unter Serverrollen ACTIVE DIRECTORY DOMÄNENDIENSTE aus und klicken Sie auf WEITER.
5. Bestätigen Sie das Hinzufügen der zusätzlich erforderlichen Features inklusive der Verwaltungstools (siehe [Abbildung 7.1](#)).

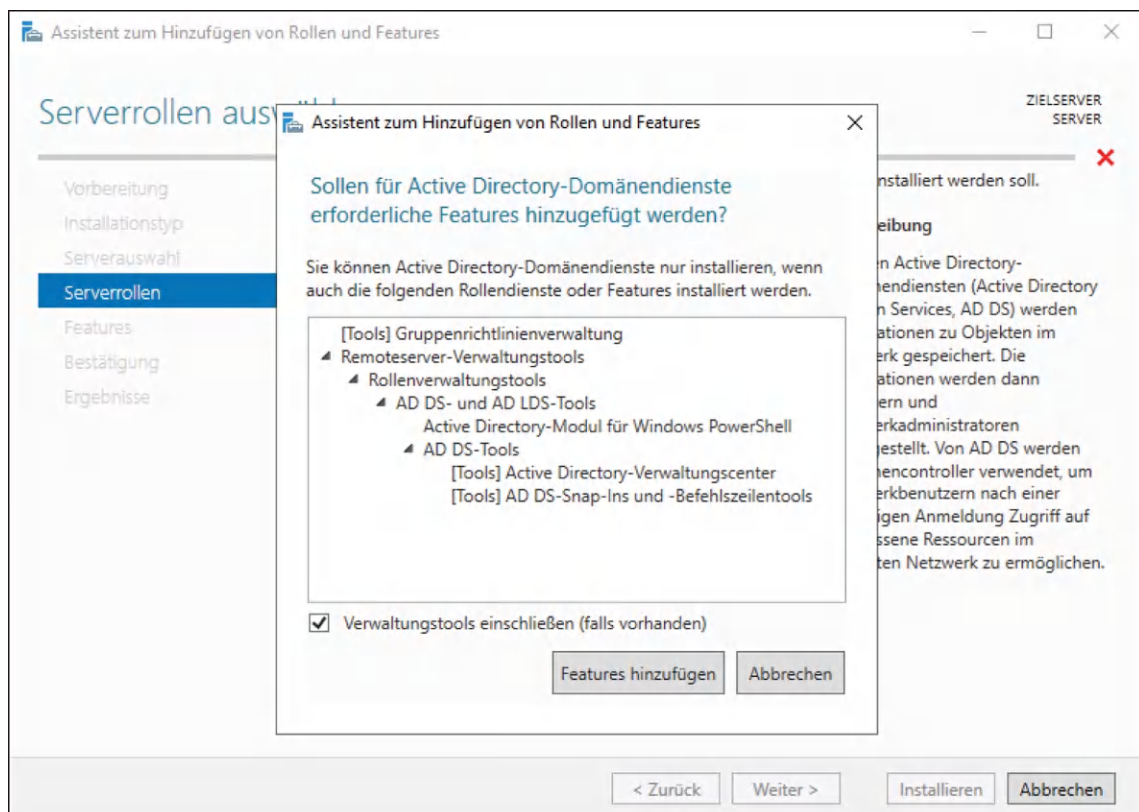


Abbildung 7.1: Der Installationsassistent unterstützt den Administrator bei der

Einrichtung der Domäne.

6. Wir gehen in unserem Beispiel davon aus, dass Sie außer einem Internet-Router oder -Gateway keinen Windows-DNS-Server in Ihrem Netzwerk betreiben. Wählen Sie daher den DNS-SERVER als weitere Serverrolle aus und klicken Sie auf WEITER.



Kein Windows-basierter DNS-Server = kein funktionierendes Active Directory!

7. Bedingt durch die im Vorfeld gewählte Option der Installation der Verwaltungstools ist unter FEATURES bereits die GRUPPENRICHTLINIENVERWALTUNG ausgewählt. Klicken Sie, ohne Änderung, auf WEITER.
8. Es erscheint ein Infodialog zu den Themen zweiter DC, der DNS-Verpflichtung und den Vorteilen der Nutzung von Azure. Bestätigen Sie den Dialog mit WEITER.
9. Es erscheint ein weiterer Infodialog, bestätigen Sie auch diesen mit WEITER.
10. Es folgen eine abschließende Zusammenfassung und die Frage, ob der Assistent den Server bei Bedarf automatisch neustarten darf. Sie können diesen Dialog mit JA bestätigen und den Assistentendialog über SCHLIEßEN verlassen.
11. Nach einigen Minuten erscheint im Server-Manager-Dashboard die Erfolgsmeldung (siehe [Abbildung 7.2](#)), dass die Installation abgeschlossen ist und nun die Konfiguration des AD ansteht.

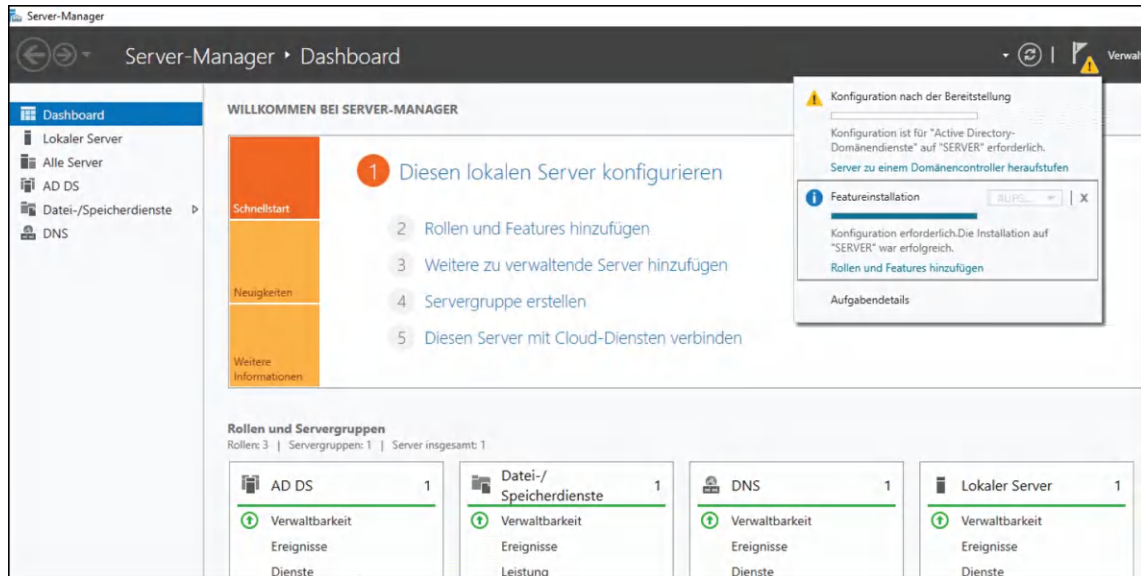


Abbildung 7.2: Die Installation des Domänendienstes ist abgeschlossen.

12. Klicken Sie auf den Link **SERVER ZU EINEM DOMÄNENCONTROLLER HERAUFSTUFEN**, um den Konfigurationsassistenten für die Active-Directory-Domänendienste zu starten.
13. Die erste Frage betrifft den Bereitstellungsvorgang. Besteht bereits eine Domäne und dieser Server soll als zusätzlicher DC zum Einsatz kommen, wählen Sie die erste Option.
Soll eine neue Domäne in einer bereits bestehenden Gesamtstruktur entstehen, wählen Sie die zweite Option. Beachten Sie hierzu den umfangreichen Microsoft-Docs-Beitrag unter <https://bit.ly/35uXtXi>.
Für eine neue Gesamtstruktur mit einer neuen Stammdomäne wählen Sie die dritte Option und geben den Namen der Domäne ein. In dem hier beschriebenen Demoszenario `ad.baer-schlede.de`.
14. Der zweite Assistentendialog betrifft die Domänencontrolleroptionen. Wir folgen unserer Demonstration und wählen in den Auswahlfeldern zu den Funktionsebenen **WINDOWS SERVER 2016**.



Es gibt für Windows Server 2019 keine eigenständigen Funktionsebenen für die Gesamtstruktur und die Domänenfunktion.

15. Unter den Domänencontrollerfunktionen sollten

- DNS-Server
- Globaler Katalog

ausgewählt sein. Geben Sie das Verzeichnisdienst-Wiederherstellungspasswort zweimal ein. Ein Ausdruck des Passworts eignet sich gut zur Ablage in einem versiegelten Briefumschlag im Panzerschrank.

16. Aller Wahrscheinlichkeit nach erhalten Sie einen Hinweis, dass die Delegierung für DNS-Server nicht eingetragen werden kann, da wir das Häkchen im Vorfeld nicht entfernt hatten. In unserem Demo-Fall ist der Hinweis belanglos.

17. In der zusätzlichen Option können Sie nun den NetBIOS-Domänennamen eingeben. Wie bereits im Abschnitt *Installation einer Active-Directory-Domäne* zur Namensfindung erläutert, legen wir diesen für unsere Demo-Umgebung mit dem DNS-Namen »ad.baer-schlede.de« auf baer-schlede fest.

18. Sie können die Standardpfade für die AD-Datenbank, die Protokolldateien und den SYSVOL-Ordner anpassen oder im Standard belassen. Sofern die C-Platte über ausreichend Speicherplatz verfügt, lassen Sie die Einträge einfach unverändert, insbesondere in einer Demo-Umgebung.

19. Es folgt die abschließende Zusammenfassung mit der Möglichkeit, sich die Konfiguration als PowerShell-Skript anzeigen beziehungsweise exportieren zu lassen. Mithilfe dieses Kommandos könnten Sie alle von Ihnen gewählten Optionen über die PowerShell auf einem anderen Server wiederholt zur Anwendung bringen.

20. Es folgt eine Zusammenfassung mit der Voraussetzungsprüfung (siehe [Abbildung 7.3](#)). Wenn diese bestanden wurde, können Sie mit der tatsächlichen Installation des Active Directorys beginnen.

Nun wird es einige Minuten dauern – es folgt ein Neustart.

21. Es erscheint der Anmeldedialog. Eine Anmeldung als lokaler Administrator ist nicht mehr möglich. Sie müssen sich mit einem

Domänen-Admin-Account anmelden.

22. Sie werden als Administrator der Domäne vom SERVER-MANAGER-Dialog begrüßt.

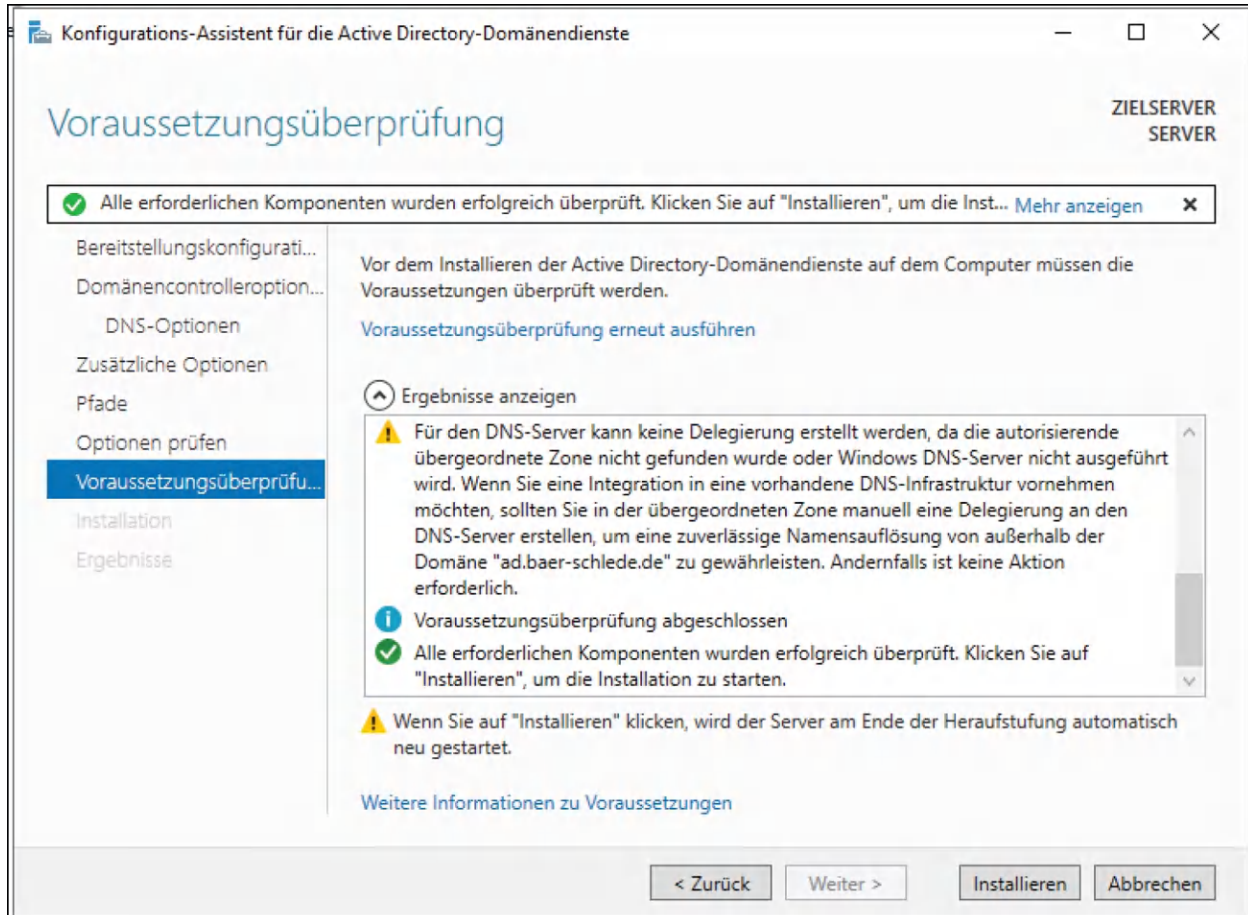


Abbildung 7.3: Alles klar – die Installation des DC kann beginnen.

Erste Benutzer und Computer

Bevor wir tiefer in die verschiedenen Dialoge und Funktionen einsteigen, wollen wir unserer Domäne die ersten »Bewohner« geben. Hierfür brauchen wir ein Windows-Client-System – dabei dürfte es sich um einen Windows-10-Computer mit einer Business-Variante des Betriebssystems handeln. Home-Editionen sind vom Domänenbeitritt ausgeschlossen – eine künstliche Limitierung des Herstellers.

Dieser Computer muss im selben TCP/IP-Bereich liegen und den Domänencontroller über das Netzwerk erreichen. Im Zweifelsfall geben

Sie ihm eine feste IP-Adresse und als DNS-Server die IP-Adresse des Domänencontrollers.

Einfache Benutzeranlage:

1. Öffnen Sie auf dem DC den SERVER-MANAGER.
2. Wählen Sie oben rechts TOOLS und anschließend das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
3. Wählen Sie den Ordner USERS in der Baumstruktur unter dem DNS-Domännennamen. Es erscheint eine Auflistung der bereits vorhandenen Gruppen.
4. Klicken Sie mit der rechten Maustaste in die rechte Fensterhälfte und wählen Sie im Kontextmenü NEU und anschließend BENUTZER.
5. Legen Sie einen Benutzer an (siehe [Abbildung 7.4](#)) und klicken Sie auf WEITER.

Neues Objekt - Benutzer

Erstellen in: ad.baer-schlede.de/Users

Vorname: Karl-Heinz Initialen:

Nachname: Glücklich

Vollständiger Name: Karl-Heinz Glücklich

Benutzeranmeldename: gluecklich @ad.baer-schlede.de

Benutzeranmeldename (Prä-Windows 2000): BAER-SCHLEDE\ gluecklich

< Zurück Weiter > Abbrechen

Abbildung 7.4: Die Anlage eines Benutzerkontos auf dem Server

6. Es erscheint der Dialog zur Festlegung des Kennworts. Geben Sie ein sicheres Passwort ein. Da es sich in der Regel um ein Initial-Kennwort handelt, belassen Sie es bei der voreingestellten Option **BENUTZER MUSS KENNWORT BEI DER NÄCHSTEN ANMELDUNG ÄNDERN**.

Sofern es sich wirklich nur um eine Demo-Umgebung handelt, können Sie auch eine Kombination wählen, die in der Praxis niemals zum Einsatz kommen sollte:

- **BENUTZER KANN KENNWORT NICHT ÄNDERN**
- **KENNWORT LÄUFT NIE AB**

7. Bestätigen Sie die Eingabe – und Sie haben Ihr erstes Benutzerkonto angelegt. In der Standardeinstellung von Windows handelt es sich bei

diesem Konto um einen DOMÄNENBENUTZER und nicht um ein Administratorkonto.

Im nächsten Schritt gilt es, einen Windows-Computer der Domäne beitreten zu lassen:

1. Wechseln Sie nun auf den Windows-Client-Computer.
2. Öffnen Sie die SYSTEMSTEUERUNG. Drücken Sie hierzu die  auf der Tastatur und geben Sie das Wort »Systemsteuerung« ein, wählen Sie das Programm aus dem Suchdialog aus.
3. Öffnen Sie die Einstellungen zu SYSTEM.
4. Klicken Sie auf EINSTELLUNGEN ÄNDERN im Abschnitt EINSTELLUNGEN FÜR COMPUTERNAMEN, DOMÄNE UND ARBEITSGRUPPE.
5. Klicken Sie auf die Schaltfläche ÄNDERN in der Registerkarte COMPUTERNAME.
6. Wählen Sie die Option MITGLIED VON DOMÄNE und geben Sie den Namen Ihrer Domäne ein, in unserem Beispiel `ad.baer-schlede.de`, und bestätigen Sie den Dialog.
7. Melden Sie sich mit dem Benutzerkonto an, das Sie im vorherigen Schritt angelegt haben.
8. Der Client-PC startet nun neu und tritt der Domäne bei.



Microsoft Windows gewährt jedem Benutzer in der Standardeinstellung die Möglichkeit, bis zu 10 Arbeitsstationen einer Domäne hinzuzufügen. Die Rede ist von normalen Benutzern – nicht Domänenadministratoren!

Sollten Sie das in der Produktivumgebung einmal ändern wollen, sind folgende Schritte erforderlich:

1. Starten Sie über Ausführen `Adsiedit.msc` mit Domänenadministrationsrechten, idealerweise auf einem

Domänencontroller.

2. Erweitern Sie den Knoten »DC=*Domänenname*«.
3. Öffnen Sie das Kontextmenü durch einen Rechtsklick und wählen Sie den Befehl EIGENSCHAFTEN.
4. Wählen Sie BEIDE und anschließend in der Auswahl MS-DS-MACHINEACCOUNTQUOTA.
5. Passen Sie den Wert gemäß Ihren Vorstellungen an.
6. Klicken Sie auf OK, um den Vorgang abzuschließen.

Zusammenfassend ist es gelungen, innerhalb weniger Minuten einen Domänencontroller einzurichten, ein Benutzerkonto anzulegen und einem Client-PC den Beitritt zu ermöglichen. Bei der Anmeldung an den Computer müssen Sie lediglich die Domäne auswählen – in der Standardeinstellung wird Windows dies künftig von allein vorblenden. Klicken Sie unten links auf ANDERER BENUTZER, melden Sie sich mit dem Benutzerkonto an. Unterhalb des Eingabefelds für das Passwort entdecken Sie den Domännennamen.

Auf den ersten Blick mag sich auf dem Windows-Client-PC nicht sehr viel verändert haben. Versuchen Sie jedoch einmal, den Computer umzubenennen, die IP-Adresse zu ändern oder ein Programm zu installieren. Was passiert?

Die meisten Änderungen am System, beispielsweise die Installation von Software (siehe [Abbildung 7.5](#)), erfordern nun die Eingabe eines entsprechend berechtigten Administrationskontos. Bereits zu diesem Zeitpunkt haben Sie als Administrator bereits eine ganze Menge in Bezug auf die Betriebssicherheit erledigt.

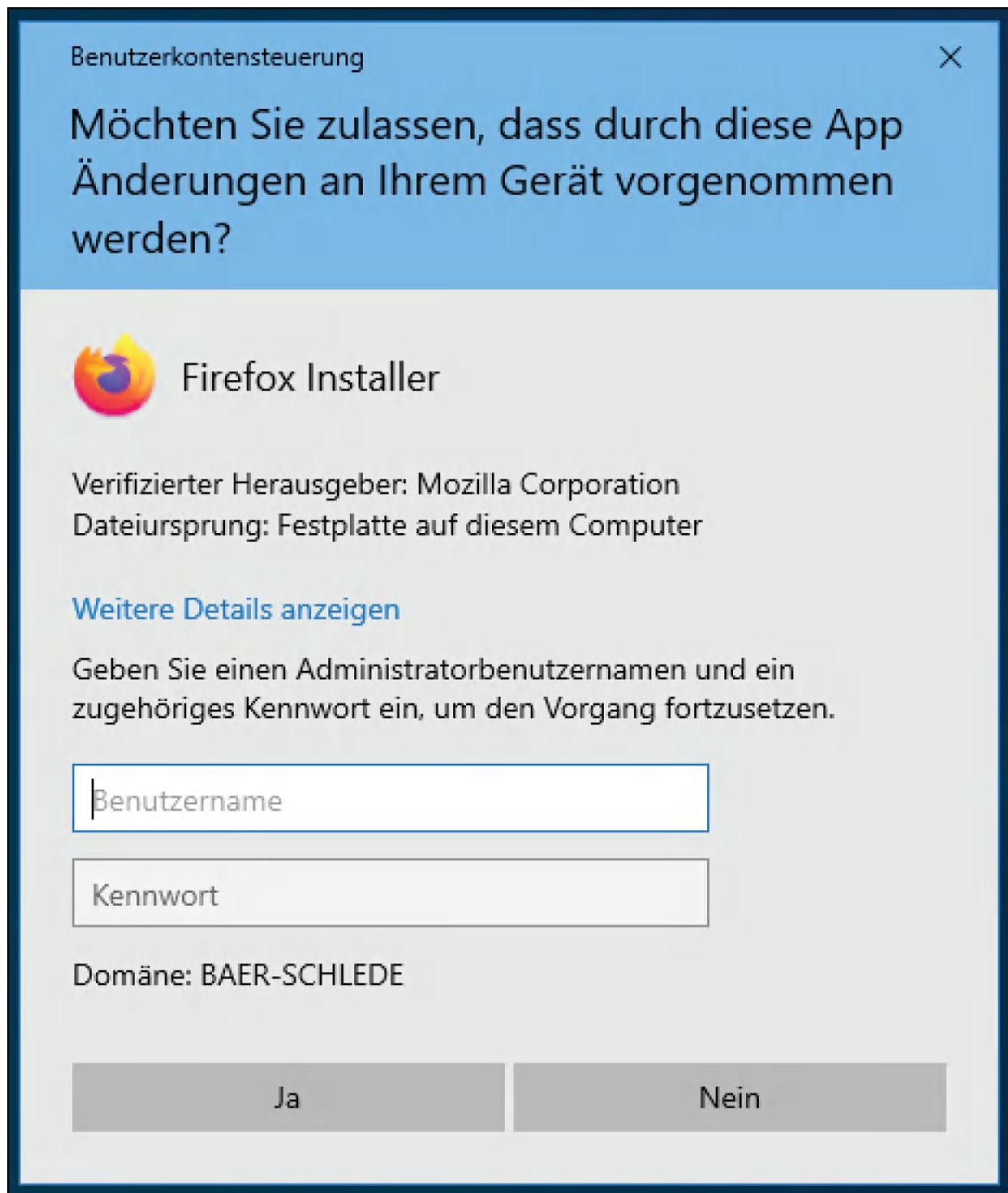


Abbildung 7.5: Für Änderungen sind nun Administrationsrechte erforderlich.

Würde ein nicht privilegierter Benutzer seine Kontodaten eingeben, verweigert Windows die Installation oder Änderung mit dem Hinweis »Der angeforderte Vorgang erfordert erhöhte Rechte«.

Wechseln wir an dieser Stelle zurück auf den Domänencontroller:

1. Wechseln Sie in der Baumstruktur des Dialogfensters ACTIVE DIRECTORY-BENUTZER UND -COMPUTER auf den Eintrag COMPUTERS.
2. Sie sehen nun einen Eintrag für den Windows-Client-Computer, der zuvor unter Verwendung der einfachen Benutzerrechte der Domäne beitrat.
3. Klicken Sie mit der rechten Maustaste auf den Computernamen und wählen Sie im Kontextmenü den Befehl EIGENSCHAFTEN aus.
4. Windows zeigt nun die wichtigsten Informationen zu dem PC an, beispielsweise die Betriebssystemversion oder die Mitgliedschaft zu Gruppen. Schließen Sie das Fenster der EIGENSCHAFTEN.
5. Klicken Sie mit der rechten Maustaste auf den Computernamen und wählen Sie im Kontextmenü den Befehl VERWALTEN aus (siehe [Abbildung 7.6](#)).

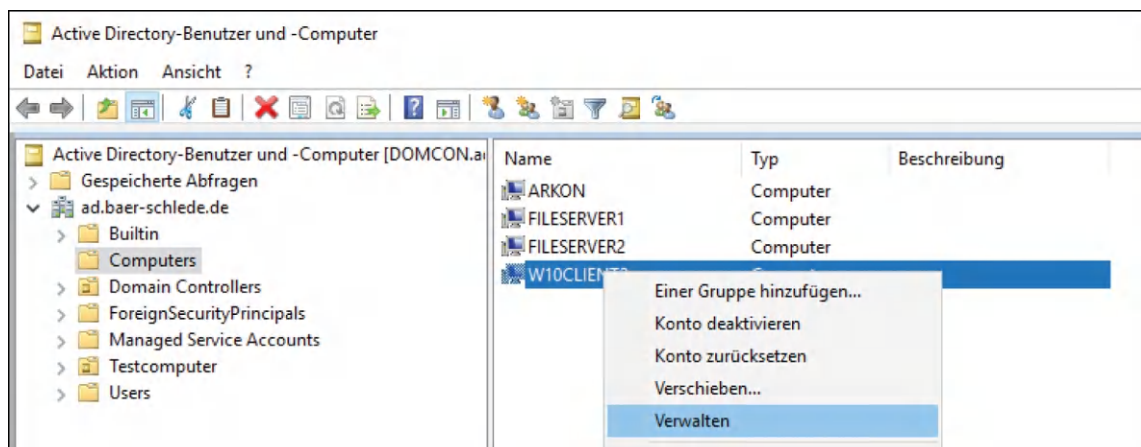


Abbildung 7.6: Aufruf der Computerverwaltung vom Server aus

Es dauert einen kurzen Augenblick, und dann erscheint der Dialog der Computerverwaltung des entfernten Rechners direkt auf dem Server.

Die Domäne bestimmt nun das Verhalten des Client-Computers und die Domäne legt fest, welche Rechte der angemeldete Benutzer auf dem System hat. Da der PC jedoch schon über ein lokales Konto verfügte, besteht nach wie vor die Möglichkeit, dass sich ein Anwender mit einem

früheren lokalen Konto anmeldet und Anpassung vornimmt, die nicht im Sinne des Administrators sind.

Das betrifft nun weniger die Einstellungen als die Software-Ausstattung. Viele Eigenschaften des Computers bestimmt die Domäne über Gruppenrichtlinien, zu denen wir in einem eigenen Kapitel kommen werden.

Deaktivieren Sie den lokalen Benutzer auf dem Client-Computer vom Server aus:

1. Wählen Sie im Computerverwaltungsdialog den Eintrag LOKALE BENUTZER UND GRUPPEN.
2. Suchen Sie das Benutzerkonto, das vor dem Domänenbeitritt bereits verfügbar war. Klicken Sie mit der rechten Maustaste auf den Namen und wählen Sie im Kontextmenü den Befehl EIGENSCHAFTEN.
3. Wählen Sie die Option KONTO IST DEAKTIVIERT ([Abbildung 7.7](#)).

Nun ist sichergestellt, dass sich nur noch Benutzer der Domäne an dem Computer anmelden können.

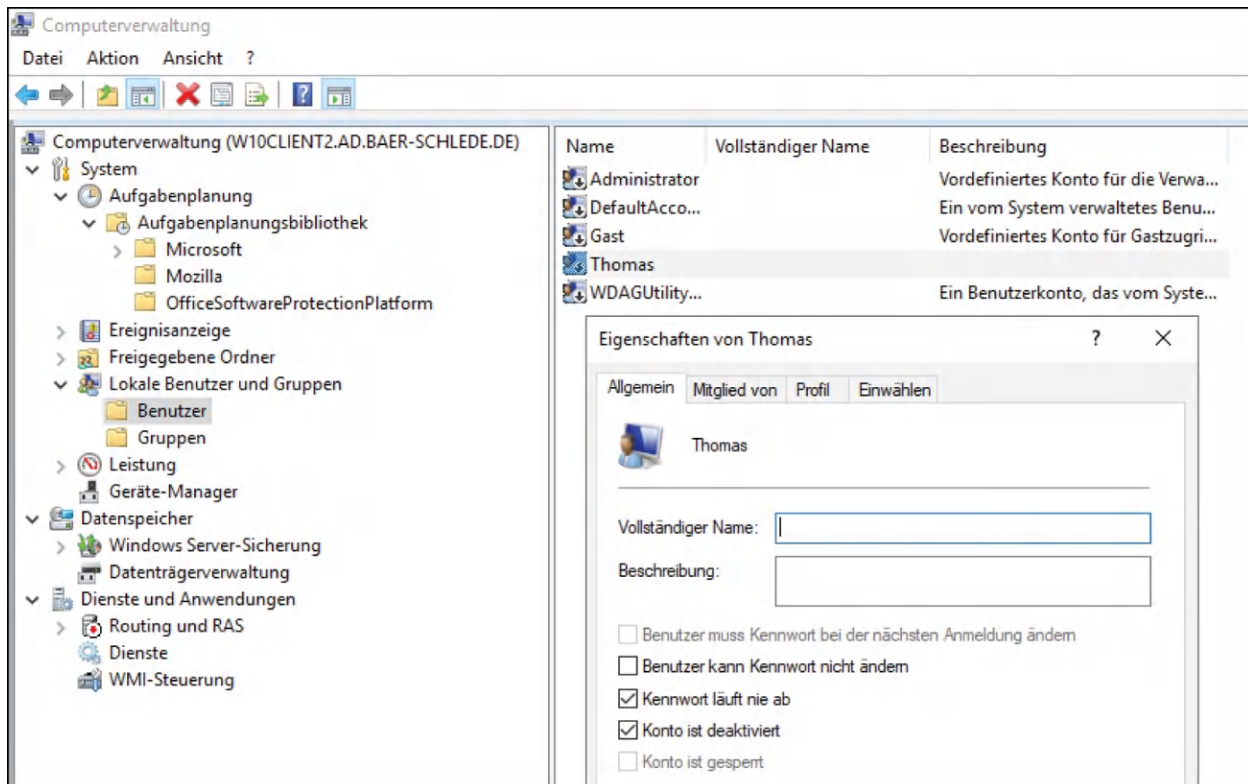


Abbildung 7.7: Alle lokalen Konten sind deaktiviert.



Benutzer, die sich schon einmal an einem PC oder Laptop angemeldet haben, können dies auch dann durchführen, wenn kein Domänencontroller zur Verfügung steht. Das ist insbesondere bei mobilen Computern hilfreich.

Anwender, die noch niemals mit dem PC gearbeitet haben, können sich nur anmelden, sofern die Domäne erreichbar ist.

Leider gibt es keine direkte Funktion des Windows-Servers, die verhindern würde, dass sich Benutzer an jedem Computer in der Domäne anmelden können. Eine solche Lösung ist jedoch leicht als Gruppenrichtlinie zu realisieren – dazu mehr in dem gesonderten Kapitel.

Administrative Konten

Aus großer Kraft folgt große Verantwortung – das hörte der schüchterne Schüler Peter Parker, besser bekannt als Spiderman, im Film von seinem

Onkel Ben Parker als Ermahnung, diese Kräfte verantwortungsbewusst einzusetzen. Auch ohne ein Marvel-Fan zu sein, kann dieser Satz gut auf einen Administrator umgemünzt werden:



Aus großer Macht folgt große Verantwortung.

Administratoren eines Servers und der Domäne, also Sie, tragen die Verantwortung für die Funktionalität des Systems. Aus eben diesem Grund verwenden verantwortungsbewusste Administratoren diesen Account nur zu administrativen Zwecken. Das klassische »Administrator«-Konto der Domäne ist Mitglied bestimmter Gruppen (siehe [Abbildung 7.8](#)).

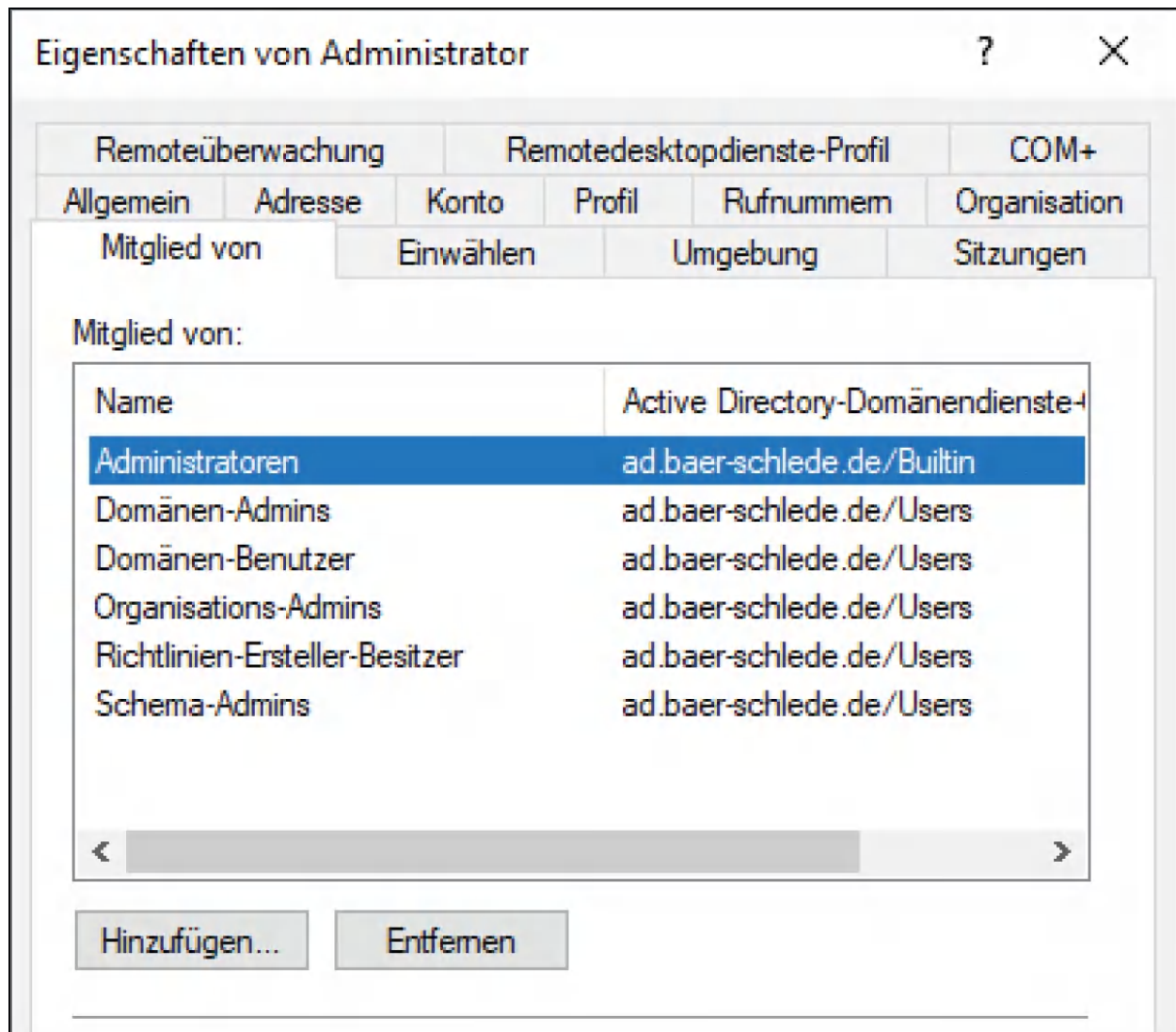


Abbildung 7.8: Standard-Gruppenzuordnung eines Administratorkontos

Wir gehen davon aus, dass Sie sich für Ihre regulären Aufgaben als Benutzer bereits ein normales »Domänen-Benutzer«-Konto angelegt haben und im Tagesgeschäft nur mit diesem Konto arbeiten.



Administratoren arbeiten nur dann mit Administrationsrechten, wenn diese zwingend erforderlich sind. Insbesondere sollten Sie sicherstellen, dass Sie keine E-Mail-Korrespondenz mit Admin-Rechten bearbeiten oder im Internet surfen. Es droht stets die Gefahr, dass Sie bei diesen Aufgaben Schad-Software ausgesetzt werden. Ein aktiviertes Makrovirus, das Dateien verschlüsselt, kann nur die Daten verschlüsseln, auf die der Benutzer Schreibzugriff hat, in dessen Account das Virus aktiv ist. Als Administrator wären das möglicherweise »alle Daten« mit entsprechend fatalen Auswirkungen.

Was verbirgt sich hinter den anderen Gruppen?

- ✓ ADMINISTRATOREN – Administratoren haben uneingeschränkten Vollzugriff auf den Computer beziehungsweise die Domäne.
- ✓ DOMÄNEN-ADMINS – Administratoren der Domäne, Mitglied von:
 - Abgelehnte RODC-Kennwortreplikationsgruppe (Kennwörter von Mitgliedern dieser Gruppe können nicht auf schreibgeschützte Domänencontroller repliziert werden.)
 - Administratoren
- ✓ ORGANISATIONS-ADMINS – Angegebene Administratoren der Organisation, Mitglied von:
 - Abgelehnte RODC-Kennwortreplikationsgruppe (Kennwörter von Mitgliedern dieser Gruppe können nicht auf schreibgeschützte Domänencontroller repliziert werden.)
 - Administratoren
- ✓ RICHTLINIEN-ERSTELLER-BESITZER – Mitglieder dieser Gruppe können Gruppenrichtlinien für die Domäne ändern. Mitglied von:

- Abgelehnte RODC-Kennwortreplikationsgruppe (Kennwörter von Mitgliedern dieser Gruppe können nicht auf schreibgeschützte Domänencontroller repliziert werden.)
- ✓ SCHEMA-ADMINS – Designierte Administratoren des Schemas, Mitglied von:
Abgelehnte RODC-Kennwortreplikationsgruppe (Kennwörter von Mitgliedern dieser Gruppe können nicht auf schreibgeschützte Domänencontroller repliziert werden.)



Mitglieder der Gruppe SCHEMA-ADMINS dürfen Änderungen am Schema, also der zugrunde liegenden Definition von Attributen und Objekten, vornehmen. Dies ist ein sehr seltener Vorgang. Es ist ausreichend, dass Sie die Gruppe nur dann mit einem administrativen Benutzer füllen, sofern Änderungen erforderlich sind. Ansonsten: Stellen Sie sicher, dass die Gruppe leer ist.

Es ist stets eine gute Idee, sich von dem Standardkonto des Administrators zu befreien und individuelle Administrationskonten verwenden. Das hat gute Gründe:

- ✓ Personalisierte Administrationskonten sind nachvollziehbar. Im Zweifelsfall ist über Protokollierungsmechanismen ermittelbar, wer welche Änderungen vorgenommen hat.
- ✓ Eine nachträgliche Anpassung von Berechtigungen ist im personalisierten Administrationsumfeld viel einfacher möglich, beispielsweise wenn zusätzliche Applikationen wie Exchange oder SharePoint zum Einsatz kommen. Nicht jeder in der IT, der grundsätzlich dem administrativen Stab zugeordnet wird, braucht Zugriff auf »alles«.
- ✓ Grundsätzlich verkleinert sich das potenzielle Angriffsrisiko. Wenn der Anmeldename für einen administrativen Account bekannt ist – und das ist bei »Administrator« oder »root« der Fall –, gilt es nur noch, das Kennwort ausfindig zu machen.

Sollte, aus welchem Grund auch immer, weiterhin ein nicht-personalisiertes Administrationskonto erforderlich sein, könnte das dazugehörige Passwort versiegelt in einem Panzerschrank abgelegt werden. Eine weitere Variante ist die Aufteilung des Passworts in mehrere Teile, wobei vertrauenswürdige Mitarbeiter jeweils nur einen Teil des Passworts kennen.

In unserer Demonstrationsumgebung wird nun neben dem einfachen Benutzerkonto für thomas ein thomas-adm-Konto angelegt und mit entsprechenden Rechten versorgt. Anschließend wird das Administratorkonto deaktiviert:

1. Melden Sie sich auf dem Domänencontroller unter Verwendung des ADMINISTRATOR-Kontos an.
2. Aufruf des Verwaltungsprogramms ACTIVE DIRECTORY-BENUTZER UND -COMPUTER, Wechsel in der Baumstruktur in USERS
3. Auswahl des ADMINISTRATOR-Kontos mit der rechten Maustaste, Auswahl des Befehls KOPIEREN aus dem Kontextmenü
4. Ausfüllen des Dialogs mit den Feldern VORNAME, NACHNAME, optionale Erweiterung des Felds VOLLSTÄNDIGER NAME um den Zusatz (Adm). Vergabe des Benutzeranmeldenamens thomas-adm. Bestätigung durch WEITER
5. Vergabe des Passworts, Bestätigung durch WEITER und abschließender Klick auf FERTIG STELLEN
6. Abmeldung als ADMINISTRATOR
7. Anmeldung als thomas-adm
8. Aufruf des Verwaltungsprogramms ACTIVE DIRECTORY-BENUTZER UND -COMPUTER, Wechsel in der Baumstruktur in USERS
9. Auswahl des ADMINISTRATOR-Kontos mit der rechten Maustaste, Auswahl des Befehls DEAKTIVIEREN aus dem Kontextmenü. In der grafischen Darstellung im Dialogfenster wird das Icon mit einem

kaum wahrnehmbaren Pfeil nach unten als »deaktiviert« markiert (siehe [Abbildung 7.9](#)).

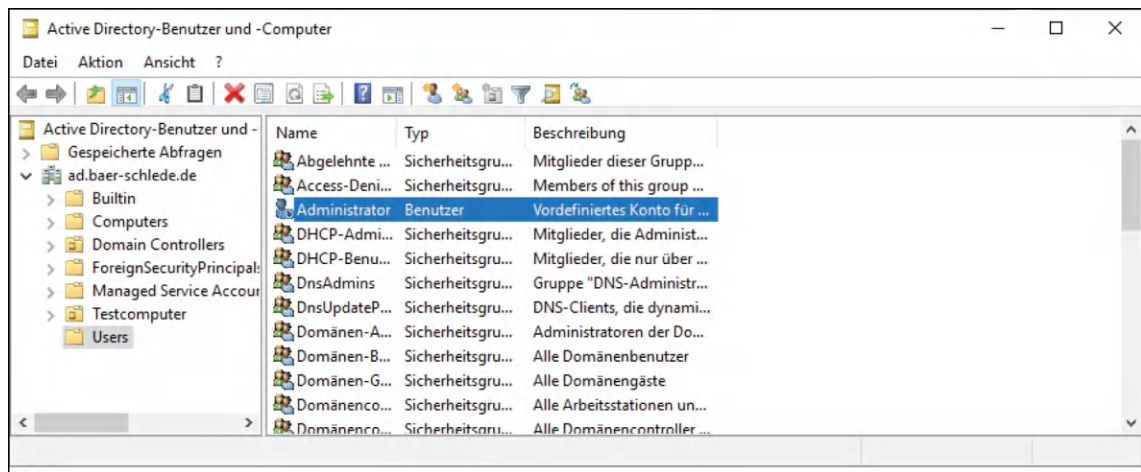


Abbildung 7.9: Das vordefinierte Administrator-Konto wurde deaktiviert.

Weiteren Domänencontroller in einer Domäne installieren

Eine Domäne mit nur einem einzigen Domänencontroller ist für den Administrator schwierig zu verwalten. Sobald »der Server« heruntergefahren ist, sind die Verwaltungsfunktionen nicht mehr aktiv, und die Namensauflösung ist außer Kraft gesetzt. Selbst in eher kleinen Umgebungen empfiehlt sich daher der Einsatz eines zweiten DC.

Wie der Administrator die Struktur seiner Landschaft betreibt, bleibt dabei ihm selbst überlassen – da gibt es kein allgemeingültiges »falsch oder richtig«. Im kleinen Umfeld kann beispielsweise dem »leistungsstarken Boliden«, der auch als Datei- und Druckserver fungiert, problemlos eine DC-Rolle aufgelastet werden. Ihm zur Seite kann ein eher leistungsarmes System stehen, das ausschließlich die Funktionsrolle als weiterer DC trägt.



Der Grundsatz ist ganz einfach: Zwei DCs sind besser als ein DC!

Für jede per WAN angebundene Außenstelle sollten Sie zudem das Vorhalten eines RODC in Erwägung ziehen.

Die Installation eines weiteren Domänencontrollers entspricht funktionell der Einrichtung des ersten DC. Sinnvollerweise ist der Server bereits im Vorfeld der Domäne als »Mitgliedserver« beigetreten. Das Prozedere hierfür entspricht dem Vorgang der Aufnahme eines Client-PC in die Domäne.

Sie können entweder den SERVER-MANAGER auf dem zweiten Server lokal starten oder den SERVER-MANAGER auf dem vorhandenen DC verwenden, wählen Sie hierzu:

1. Starten Sie den SERVER-MANAGER auf dem Domänencontroller.
2. Oben rechts auf VERWALTEN klicken und den Befehl SERVER HINZUFÜGEN auswählen.
3. Im Suchdialog »Active Directory« unter NAME (CN) den Hostnamen eingeben und die Schaltfläche SUCHE STARTEN anklicken, siehe [Abbildung 7.10](#).

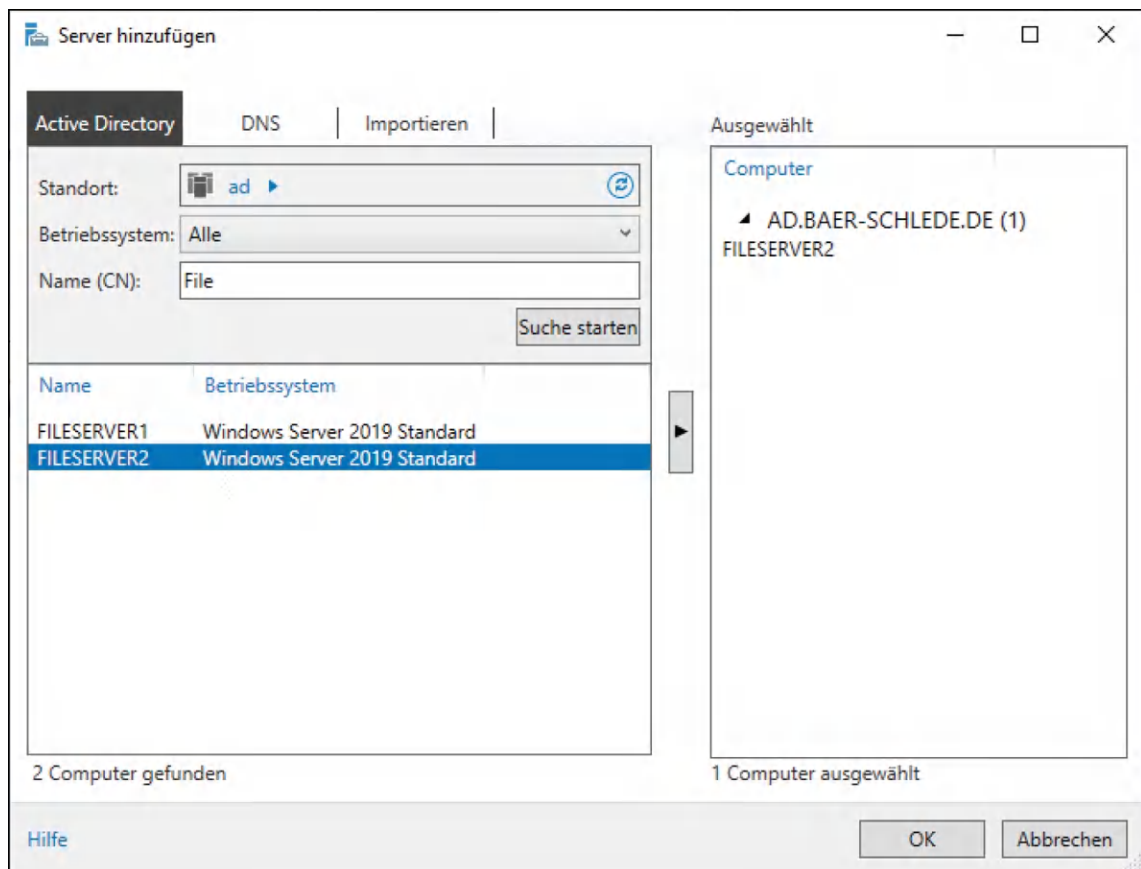


Abbildung 7.10: Hinzufügen von Servern in den Server-Manager

4. Fügen Sie den gewünschten Server hinzu. Anschließend können Sie die SERVER-MANAGER auch zur Verwaltung dieses Servers aus der Konsole des Domänencontrollers heraus nutzen.

Nun können wir aus dem Server-Manager des Domänencontrollers heraus den Mitgliedsserver verwalten und zu einem weiteren Domänencontroller »machen«.

1. Klicken Sie oben rechts im SERVER-MANAGER auf HINZUFÜGEN VON ROLLEN/FEATURES.
2. Wählen Sie den gewünschten Server aus.
3. Wählen Sie unter Serverrollen ACTIVE DIRECTORY DOMÄNENDIENSTE aus und klicken Sie auf WEITER.
4. Wählen Sie die Option DOMÄNENCONTROLLER ZU EINER VORHANDENEN DOMÄNE HINZUFÜGEN aus.
 - Es besteht auch die Möglichkeit, einen SCHREIBGESCHÜTZTEN DOMÄNENCONTROLLER (RODC) zu installieren.



Schreibgeschützte DCs sind in erster Linie für den Einsatz in WAN-angebundenen Außenstellen gedacht. Sie beschleunigen das Log-on der lokalen Benutzer und können Repliken (Kopien) der DNS-Datenbank sowie des Global Catalog vorhalten.

RODC unterliegen wiederum aber auch einigen Limitierungen. Standardmäßig speichert ein RODC keine Passwörter. Diese Einstellung hat den Nachteil, dass sich Benutzer in der Außenstelle nicht anmelden können, wenn die Netzverbindung in die Zentrale unterbrochen ist. Der RODC benötigt in der Standardkonfiguration stets den Kontakt zu einem regulären DC, weil er Benutzer selbst nicht authentifizieren kann. Über die Zuordnung zur Gruppe »Zulässige RODC-Kennwortreplikationsgruppe« kann der Administrator für ein Zwischenspeichern einiger oder aller Passwörter sorgen (siehe [Abbildung 7.11](#)).

Microsoft führte Read-only Domain Controller erstmals in Windows Server 2008 ein. Seitdem hat sich an dem Konzept praktisch nichts verändert. Einzig bei den Management-Tools sind seit der Version Server 2012 PowerShell-Cmdlets hinzugekommen, mit denen sich RODC-Konten vorab im AD eintragen (Staging) und Domänencontroller installieren lassen.

5. Der Domänenname und die zu verwendenden Anmeldeinformationen sind einzugeben. Das Kennwort für den Wiederherstellungsmodus ist, wie bei allen Domänencontrollern, zwingend erforderlich – es muss sich nicht um dasselbe Passwort handeln, das beim ersten DC zum Einsatz kam.
6. Anschließend folgt die Eingabe des DC, von dem aus die Replikation stattfinden soll (siehe [Abbildung 7.12](#)). Geben Sie hier nichts ein, wählt der Installationsassistent einen beliebigen DC aus.

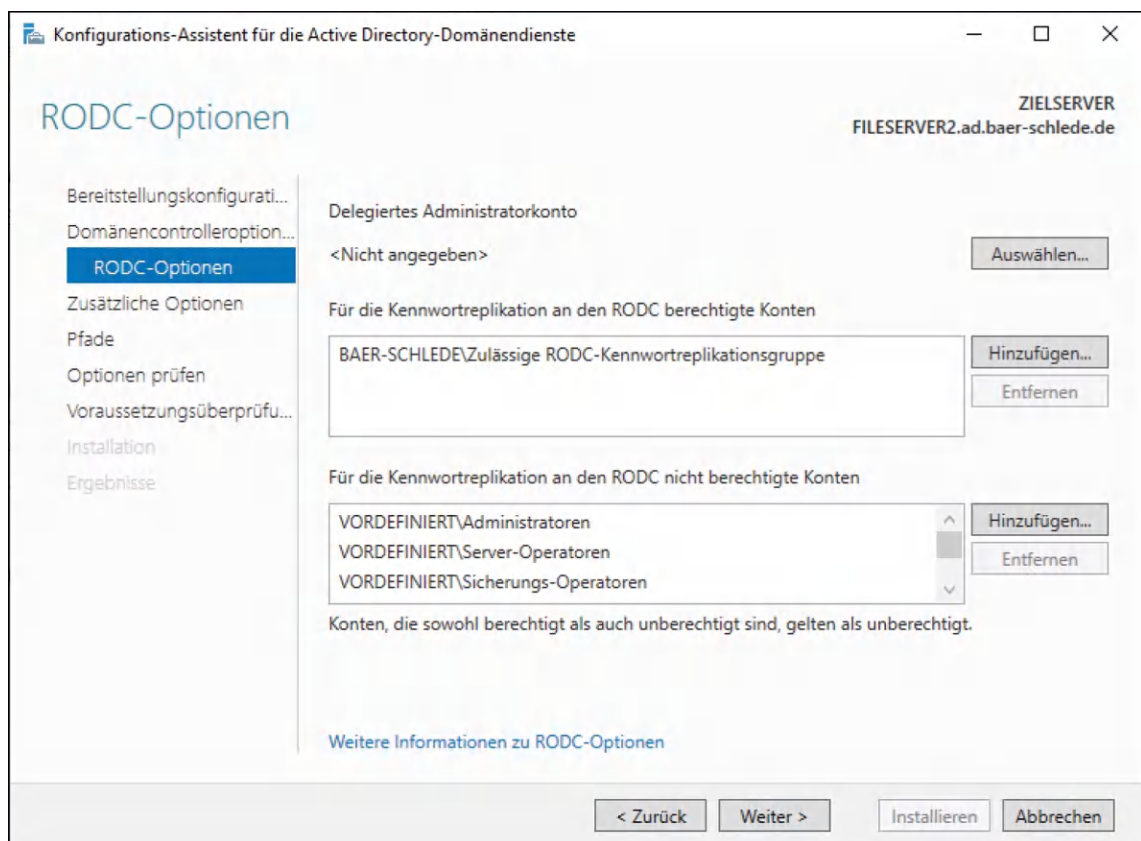


Abbildung 7.11: Gruppenzuordnung auf einem RODC

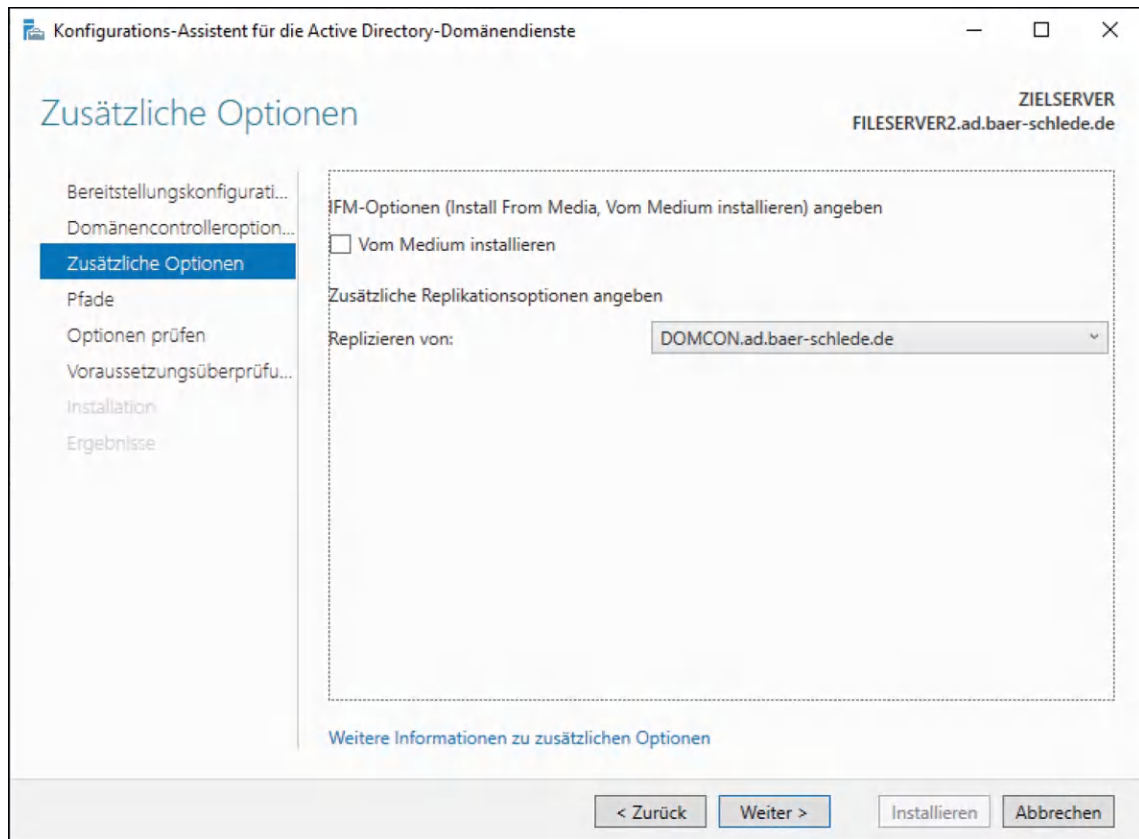


Abbildung 7.12: Auswahl des Replikationspartners für den neuen DC



Alternativ besteht die Möglichkeit der Einrichtung über das Einlesen eines sogenannten IFM-Datenträgers (aus einem Backup heraus), anschließend muss dann nur noch das verbleibende Delta über die Replikation bereitgestellt werden. Das ist jedoch nur erforderlich, sofern das AD sehr viele Objekte enthält und die Netzwerkanbindung an dem Standort von schlechter Qualität ist.

7. Die anderen Punkte ähneln dem bereits beschriebenen Szenario bei der Installation des ersten DC.
8. Nach einem Neustart überprüfen Sie das Vorhandensein eines weiteren Domänencontrollers im Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND -COMPUTER. In der Baumstruktur der Domäne befindet sich im Ordner DOMAIN CONTROLLERS nun ein weiterer Eintrag. In [Abbildung 7.13](#) ist zu sehen, dass der Computer mit dem Namen »Fileserver2« nun ein Domänencontroller

ist.

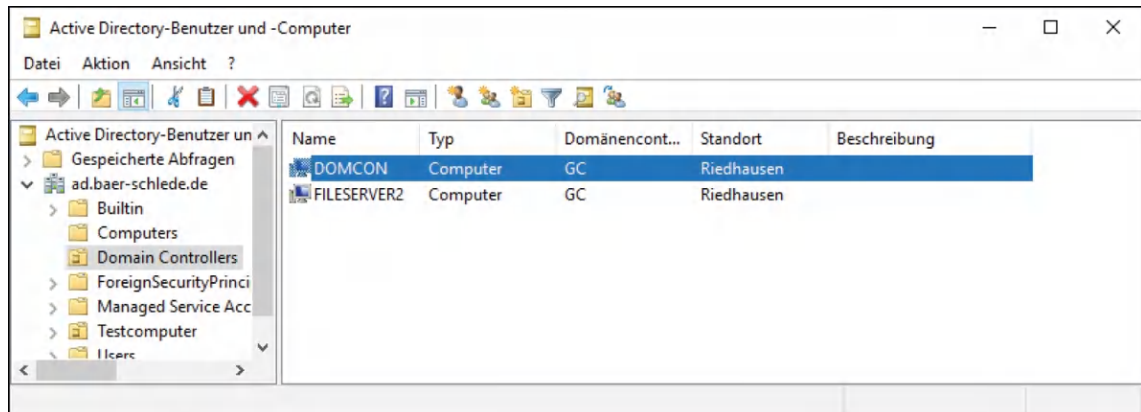


Abbildung 7.13: Namentlich nicht ganz passend – Fileserver2 ist nun auch ein DC.

Mit der Bereitstellung eines zweiten Domänencontrollers geschieht eine nicht uninteressante Veränderung. Wenn Sie bisher versucht haben, die Domäne per ICMP-Echo-Request zu erreichen

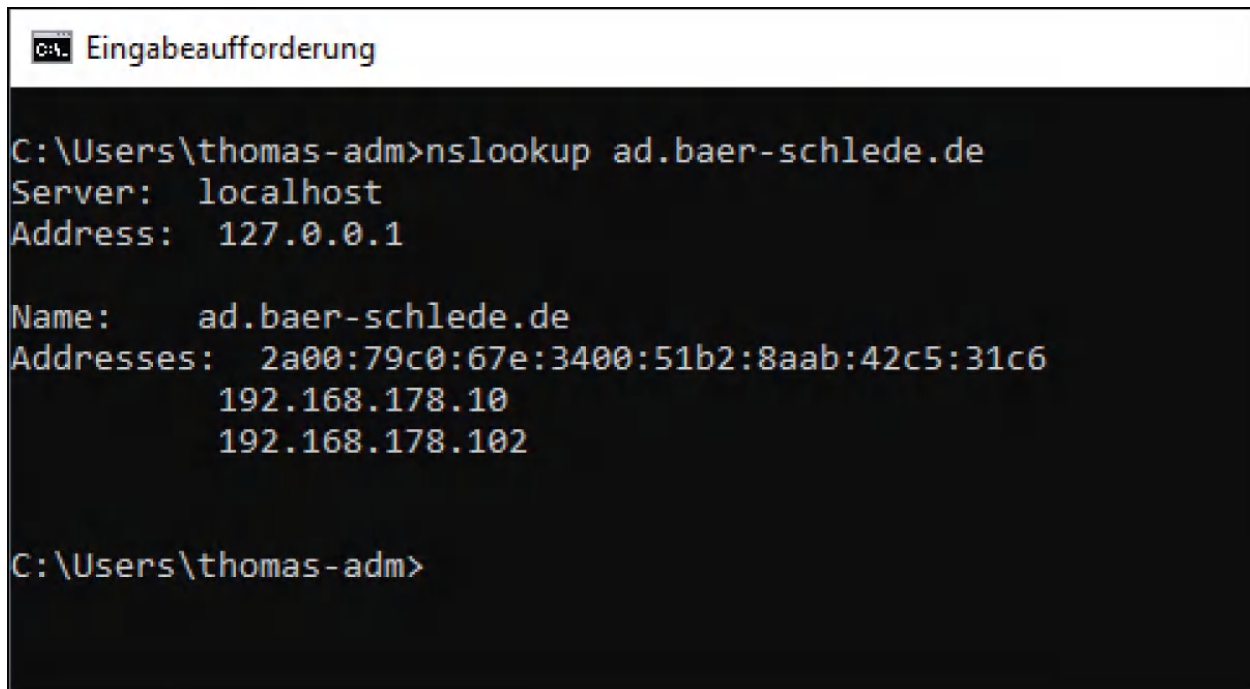
`ping Domänenname`

hat stets nur der eine Domänencontroller geantwortet. Nun, da zwei DCs in der Demo-Umgebung vorhanden sind, gilt es, einen Blick auf die Namensauflösung zu werfen, zu sehen in [Abbildung 7.14](#).

Die Domäne ist nun unter mehreren IP-Adressen erreichbar. Wenn Sie von einem Client-Computer aus einen Ping auf den Domänennamen absetzen, reagiert einer der Domänencontroller. Schalten Sie diesen aus und warten kurz, wird auf dasselbe Ping-Kommando der andere DC reagieren.



In der praktischen Anwendung können Sie sich auch über das Remotedesktop-Protokoll (RDP) direkt auf den Domänennamen verbinden. Sie müssen sich den genauen Namen eines DC nicht unbedingt merken.



```
C:\Users\thomas-adm>nslookup ad.baer-schlede.de
Server:      localhost
Address:     127.0.0.1

Name:       ad.baer-schlede.de
Addresses:  2a00:79c0:67e:3400:51b2:8aab:42c5:31c6
            192.168.178.10
            192.168.178.102

C:\Users\thomas-adm>
```

Abbildung 7.14: Namensauflösung zur Domäne mit zwei DCs

Dass die Daten und Einstellungen auf den Domänencontrollern stets passend sind, dafür sorgt die im folgenden Abschnitt beschriebene Technik.

Replikation

Nachdem unsere Demo-Umgebung nun über einen zweiten Domänencontroller verfügt, ist es an der Zeit, uns noch einmal näher mit einem Begriff auseinanderzusetzen, der im vorherigen Abschnitt schon einmal fiel: Replikation. Schon sehr früh hatten wir zudem die Begrifflichkeit »Multimaster« verwendet.

Konzeptionell ist das Active Directory als Verzeichnisdienst so konzipiert, dass es mehrere zentrale Verwaltungsserver geben kann. Der Vorgang des erforderlichen Informationsabgleichs nennt sich Replikation.

Domänendaten werden auf alle Domänencontrollern innerhalb einer bestimmten Domäne repliziert. Schema- und Konfigurationsdaten werden in alle Domänen der Domänenstruktur oder -gesamtstruktur repliziert. Alle Objekte und eine Teilmenge der Objekteigenschaften der

Domänenstruktur replizieren die Systeme in den sogenannten globalen Katalog.



In unserer kleinen Demo-Umgebung mit gerade einmal zwei Domänencontrollern sind diese Infos kaum relevant. Sollten Sie jedoch weitere Domänen anbinden, sollte es Ihnen bewusst sein, dass Objektdaten auch außerhalb der Domänengrenzen repliziert werden können.

In der Praxis sorgt die Replikation dafür, dass die Domänencontroller hinsichtlich ihrer benötigten Informationen auf demselben Stand sind und die Domäne auch dann ordnungsgemäß arbeitet, sofern ein DC nicht erreichbar ist.

Sie können sich die Details zu den Replikationseinstellungen auch in der kleinen Umgebung einmal näher anschauen:

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-STANDORTE UND DIENSTE.
4. Öffnen Sie die Baumstruktur so, dass Sie unter SITES ein blaues Hochhaussymbol für Ihren Standort sehen. Sofern Sie keinen Namen definiert haben, heißt der Eintrag DEFAULT-FIRST-SITE-NAME. In der [Abbildung 7.15](#) sind beide Server dem Standort »Riedhausen« zugewiesen.

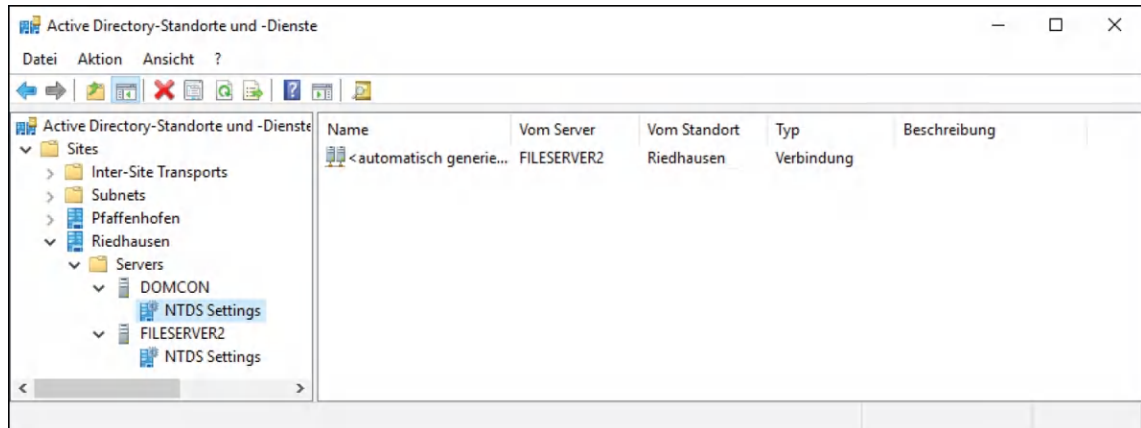


Abbildung 7.15: Beide Server in der Demo-Umgebung sind demselben Standort zugewiesen.

5. Öffnen Sie die Struktur so, dass Sie die NTDS SETTINGS zu einem Server im Dialogfenster sehen. In der [Abbildung 7.15](#) ist zu sehen, dass der Server »DOMCON« eine Replikation vom Server »FILESERVER2« unterhält.
6. Klicken Sie nun mit der rechten Maustaste auf den Eintrag <AUTOMATISCH GENERIERT> und wählen Sie den Befehl EIGENSCHAFTEN aus dem Kontextmenü.
7. Über die Schaltfläche ZEITPLAN ÄNDERN können Sie festlegen, wie oft diese Verbindung über das Netzwerk repliziert wird. Die Auswahlmöglichkeiten sind in [Abbildung 7.16](#) zu sehen.

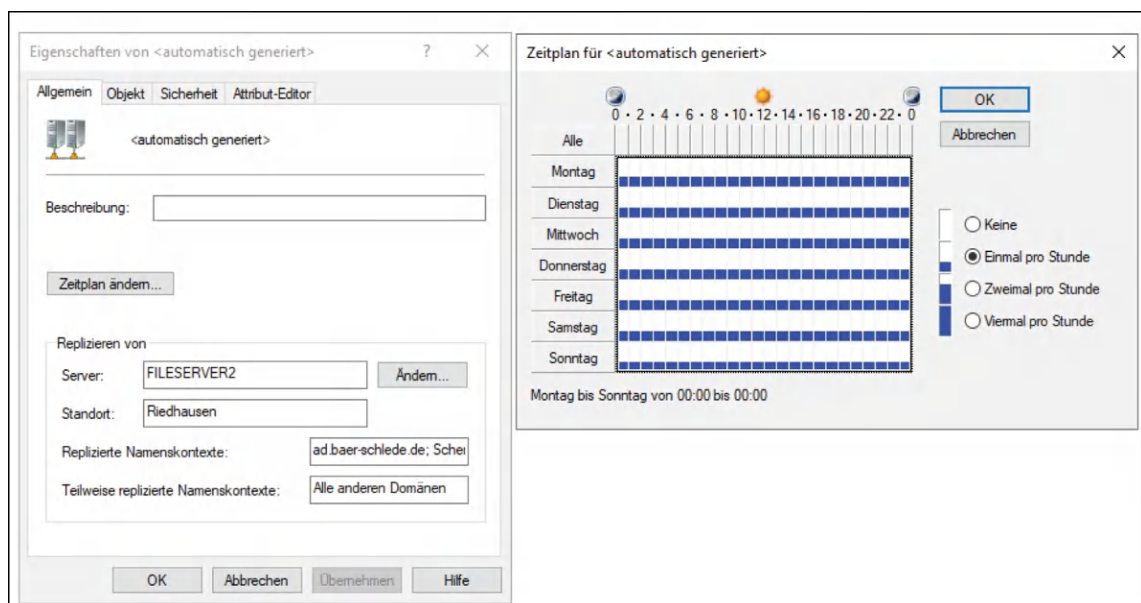


Abbildung 7.16: Pro Replikationsverbindung kann der Administrator einen Zeitplan für den Abgleich definieren.

Je nach Domänengröße, Anzahl der Standorte und Netzwerkanbindung kann es für Sie als Administrator erforderlich sein, die Replikationseinstellungen anzupassen. In der klassischen Umgebung mit zwei DCs in einem Netzwerk an einem Standort müssen Sie an dieser Stelle keine Anpassungen vornehmen.



Die Replikation rund um die Domäne ist ein äußerst spannendes Themengebiet. Wenn Sie sich tiefer mit dieser Materie auseinandersetzen möchten, sei auf einen Blog-Eintrag von Philipp Föckeler aus dem Jahr 2010 hingewiesen (inhaltlich immer noch korrekt): <https://www.faq-o-matic.net/2010/08/31/active-directory-replikation-im-detail/>.

Betriebsmasterrollen

Der Replikationsmechanismus sorgt zwar dafür, dass die DCs über dieselben Informationen verfügen, aber dennoch sind die Domänencontroller mitnichten identisch. Natürlich – ein RODC – als »Nur-Lese-Domänencontroller« unterscheidet sich von einem vollwertigen, schreibbefähigten DC, aber auch das ist nicht gemeint. Die Active-Directory-Domäne verwendet verschiedenen Betriebsmasterrollen, die in einem Multimasterbetrieb nur umständlich zu betreiben sind. In der Summe geht es um fünf verschiedene Rollen:

- ✓ Schemamaster – Der Schemamaster steuert die Aktualisierung und Änderungen des Verzeichnisschemas. Um das Verzeichnisschema anpassen zu können, müssen Sie auf den Schemamaster zugreifen können. Insgesamt darf in einer Domäne nur ein Schemamaster vorhanden sein. Änderungen am Schema sind sehr selten.
- ✓ Domänennamenmaster – Steuert das Hinzufügen oder Entfernen von Domänen zu beziehungsweise aus der Gesamtstruktur. Es gibt nur einen Domänennamenmaster in einer Domäne.

- ✓ RID-Master – Diese Benutzerrolle ist dafür zuständig, relative IDs zu erzeugen und zu vergeben. Immer wenn Sie als Administrator ein Benutzer-, Computer- oder Gruppenobjekt erzeugen, wird es mit einer ID versehen. Diese ID ist eine eindeutige Sicherheitskennung und ist auch der Grund dafür, dass Sie ein Objekt auch umbenennen können, ohne dass die logischen Verknüpfungen verloren gehen würden. Die ID besteht aus einem Sicherheitskennungspräfix, der zur Domäne gehört.
- ✓ PDC-Emulationsmaster – In gemischten Installationen, die auch Windows-Server mit älteren Betriebssystemversionen enthalten, fungiert ein PDC-Emulator als Windows-NT-PDC (Primary Domain Controller). In diesem Betriebsmodus ist der Server mit dieser Betriebsmasterrolle für die Authentifizierung von Anmeldungen, die Verarbeitung von Kennwortänderungen und die Replikation von Aktualisierungen auf die Reservedomänencontroller verantwortlich. Eine Aufgabe, die dem PDC-Emulationsmaster noch heute zufällt, ist die des Standardzeitserver mit der Aufgabenstellung der Zeitsynchronisation in der Domäne.
- ✓ Infrastrukturmaster – Der Server mit dieser Betriebsmasterrolle ist für Aktualisierung von Objektreferenzen zuständig. Durch einen regelmäßigen Abgleich mit dem »globalen Katalog« prüft der Infrastrukturmaster die aktuellen Daten und repliziert Änderungen.

Sie können über die Eingabeaufforderung sehr leicht ermitteln, welcher DC im Moment welche Betriebsmasterrollen innehat:

```
dsquery server -hasfsmo schema
dsquery server -hasfsmo name
dsquery server -hasfsmo rid
dsquery server -hasfsmo pdc
dsquery server -hasfsmo infr
```

Alternativ gibt es einen Befehl, um alle Rollen zeitgleich zur Anzeige zu bringen, wie in [Abbildung 7.17](#) zu sehen:



```
C:\Users\thomas-adm>netdom query fsmo
Schemamaster                DOMCON.ad.baer-schlede.de
Domänennamen-Master         DOMCON.ad.baer-schlede.de
PDC                         DOMCON.ad.baer-schlede.de
RID-Pool-Manager            DOMCON.ad.baer-schlede.de
Infrastrukturmaster         DOMCON.ad.baer-schlede.de
Der Befehl wurde ausgeführt.

C:\Users\thomas-adm>
```

Abbildung 7.17: Mit dem »netdom«-Kommando ermittelt der Administrator die aktuelle Zuordnung der Betriebsmasterrollen.

```
netdom query fsmo
```

Für gewöhnlich erfolgt die Zuweisung der Betriebsmasterrollen automatisch, und Sie müssen sich als Administrator nicht weiter darum kümmern. Bei der Installation des ersten DC erhält dieser erwartungsgemäß alle Rollen.

Enthält eine Domäne zwei oder mehr Domänencontroller, sollten Sie für die Betriebsmasterrollen zwei DCs konfigurieren. In diesem Fall wird ein Domänencontroller zum »Betriebsmaster« und der andere zum »Reservebetriebsmaster«. Die Reserve kommt zum Einsatz, wenn der Hauptbetriebsmaster ausfällt. Aus gutem Grund sollten diese beiden Server direkte Replikationspartner sein und über eine leistungsstarke Netzwerkanbindung verfügen.



In großen Domänen verteilen Administratoren die Betriebsmasterrollen auf möglichst viele DCs. Zwei Rollen, die nicht aufgeteilt gehören, sind Schemamaster und Domänennamenmaster. Weisen Sie diese beiden Betriebsmasterrollen stets einem Server zu.

Sie können die Betriebsmasterrollen bei Bedarf wie folgt verändern:

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND DOMÄNEN.
4. Selektieren Sie mit der rechten Maustaste in der Baumstruktur den Namen der gewünschten Domäne.
5. Klicken Sie im Kontextmenü auf ALLE AUFGABEN | BETRIEBSMASSTER...
6. In dem Dialogfenster haben Sie die Möglichkeit, die Betriebsmasterrollen in den Registerkarten RID, PDC und INFRASTRUKTUR anzupassen.

Entfernung eines Domänencontrollers

Manchmal besteht die Notwendigkeit, einen bereits in Betrieb befindlichen DC von seinen Diensten zu entbinden, sei es, um den Server komplett außer Betrieb zu nehmen oder um lediglich die DC-Rolle von dem Server zu entfernen. Glücklicherweise ist es recht einfach möglich, die Rolle wieder zu entfernen:

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl VERWALTEN.
3. Wählen Sie den Befehl ROLLEN UND FEATURES ENTFERNEN.
4. Bestätigen Sie die Vorbemerkungen mit WEITER.
5. Wählen Sie den gewünschten Server aus, sollte der zu entfernende DC nicht mehr erreichbar sein, lesen Sie bitte den nächsten Abschnitt in diesem Buch. Bestätigen Sie die Serverauswahl mit WEITER.
6. Entfernen Sie die betreffende Rolle ACTIVE DIRECTORY-DOMÄNENDIENSTE.
7. Bestätigen Sie den folgenden Dialog »Diesen Domänencontroller

tiefer stufen«.

8. Es erscheint ein weiterer Warnhinweis, den Sie mit WEITER bestätigen müssen.
9. Da nun wieder ein lokales Administrationskonto aktiv sein wird, gilt es, das Kennwort für den lokalen Administrator festzulegen und die Eingabe mit WEITER zu bestätigen.
10. Der Server ist – nach einem Neustart – wieder ein normaler Mitgliedserver in der Domäne.



Das Tieferstufen eines DC hat eine Vielzahl von automatisierten Aktivitäten zur Folge:

- ✓ Dienste NETLOGON und KDC (Key Distribution Center) anhalten
- ✓ Dienst KDC entfernen
- ✓ Bereinigung der Registry
- ✓ Löschen spezifischer Ordner für DCs
- ✓ Bereinigung der DNS-Einträge des DC für LDAP, Kerberos und im globalen Katalog
- ✓ Computerobjekt wird um DC-spezifische Merkmale befreit
- ✓ Computerobjekt wird wieder unter COMPUTERS einsortiert
- ✓ DC wird aus der AD-Datenbank gelöscht
- ✓ Replikation dieser Anpassung an alle verbliebenen DCs

Manchmal steht Ihnen als Administrator aber der zu entfernende DC nicht mehr physisch zur Verfügung – weil es ihn nicht mehr gibt oder weil er aus technischen Gründen nicht mehr einsatzfähig ist. Der »nicht mehr existierende DC« ist in der Praxis ein »gern gesehenes Phänomen«, wenn Sie etwas reparieren dürfen, was jemand anderes »verbockt« hat.

In diesem Fall bleibt nur noch die »harte Entfernung« aus der Domäne.

Sofern der zu entfernende DC keine FSMO-Betriebsrollen mehr trägt und jünger als ein Windows Server 2012 R2 ist, können Sie den Server über einen Assistenten entfernen:

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND DOMÄNEN.
4. Selektieren Sie mit der rechten Maustaste den zu entfernenden Domänencontroller und wählen Sie den Befehl LÖSCHEN.
5. Bestätigen Sie Bestätigungsdialog mit JA.
6. Es erscheint folgender Dialog zum Vorgang DOMÄNENCONTROLLER LÖSCHEN, siehe [Abbildung 7.18](#).



Abbildung 7.18: Das Entfernen eines nicht mehr aktiven DC ist über einen Assistenten möglich.

7. Bestätigen Sie die untere Option, um den DC dauerhaft aus der Domäne zu entfernen.
8. Der Server wird als DC ausgetragen.

Möglicherweise wurde zwar der DC gelöscht, aber nicht mithilfe des Assistenten ordnungsgemäß entfernt. Nun sind leider einige manuelle Arbeitsschritte erforderlich:

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm AD-STANDORTE UND -DIENSTE.
4. Entfernen Sie den DC aus dem Ordner SERVERS am passenden Standort. Wählen Sie hierzu den Befehl LÖSCHEN aus dem Kontextmenü.
5. Schließen Sie den Dialog AD-STANDORTE UND -DIENSTE.
6. Wechseln Sie in das Verwaltungsprogramm DNS.
7. Löschen Sie alle Einträge des DC in allen Zonen.
8. War der DC gleichzeitig ein DNS-Server, öffnen Sie die Eigenschaften und entfernen Sie den DC in der Registerkarte NAMENSSERVER.

Sofern auf dem zu entfernenden und nicht mehr erreichbaren DC noch FSMO-Rollen »aktiv« sind, müssen Sie mithilfe eines Kommandozeilenprogramms mit Namen Ntdsutil einen sogenannten METADATACLEANUP durchführen. Achten Sie darauf, dass das Tool eine administrativ gestartete Konsole verlangt.



Sie finden die erforderlichen Informationen zur manuellen Bereinigung mit dem Tool unter <https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/deploy/ad-ds-metadata-cleanup>.



Niemals – aber wirklich niemals – dürfen Sie versuchen, einen einmal als defekt deklarierten DC wieder ins Netzwerk einzubinden. Sollte ein Hardware-Schaden behoben und der Server zwischenzeitlich als DC entfernt worden sein, bleibt nur die Neuinstallation und ein anschließender Domain-Join als neuer Mitgliedserver. Anschließend kann die Maschine wieder zu einem DC heraufgestuft werden.

Active-Directory-Verwaltung über den Client

Sollten Sie schon etwas länger im »Windows-Server-Dunstkreis« aktiv sein, werden Sie bestimmt von RSAT gehört haben. Hierbei handelt es sich um die »Remote Server Administration Tools« von Microsoft. RSAT bietet Administratoren die Möglichkeit, von ihrem Windows-Client-Computer aus direkt ihre Server und die Domäne verwalten zu können, ohne sich immer per RDP-Sitzung auf den Server aufschalten zu müssen.

In den jüngeren Windows-10-Versionen, beschränkt auf die Editionen »Pro« und »Enterprise«, ist es nicht mehr notwendig, die RSAT herunterzuladen und zu installieren. Die Tools müssen lediglich aktiviert werden:

1. Rufen Sie die Einstellungs-App in Windows 10 auf.
2. Navigieren Sie zu APPS.
3. Klicken Sie rechts auf OPTIONALE FEATURES.
4. Klicken Sie auf FEATURE HINZUFÜGEN.
5. Wählen Sie RSAT: TOOLS FÜR ACTIVE DIRECTORY DOMAIN SERVICES UND LIGHTWEIGHT DIRECTORY SERVICES aus.
6. Klicken Sie auf INSTALLIEREN.

Danach sind die Verwaltungstools für Active Directory in Windows 10 verfügbar. Sie finden die Verwaltungsprogramme im Startmenü.

Active-Directory-Papierkorb

Versehentlich gelöschte Objekte stellen grundsätzlich ein Ärgernis dar, da macht das Active Directory keine Ausnahme. Aber anders als ein »versemmeltes« Word-Dokument hat das Löschen einer Berechtigungsgruppe mitunter fatale Auswirkungen.

Mit jeder Windows-Serverversion hat Microsoft daran gearbeitet, das

»Schreckgespenst« immer weiter zu bändigen, sodass in den jüngeren Versionen sogar eine grafische Oberfläche für die Wiederherstellung versehentlich gelöschter Objekte besteht. Die Zeiten, in denen über NTDSUTIL in der Eingabeaufforderung gearbeitet werden muss, sind glücklicherweise vorbei.

- ✓ In der Standardeinstellung ist der Active-Directory-Papierkorb deaktiviert.
- ✓ Die Aktivierung erfordert eine Gesamtstruktur »Funktionsebene Windows Server 2008 R2« oder höher.
- ✓ Das Aktivieren des Active-Directory-Papierkorbs kann nicht mehr rückgängig gemacht werden.
- ✓ Zum Verwalten des Papierkorb-Features über eine Benutzeroberfläche ist das ACTIVE DIRECTORY-VERWALTUNGSCENTER ab Windows Server 2012 vorgesehen.

So aktivieren Sie die Funktion:

1. Stellen Sie sicher, dass alle FSMO-Replikationspartner in Betrieb sind.
2. Starten Sie den SERVER-MANAGER.
3. Wählen Sie oben rechts im Menü den Befehl TOOLS.
4. Wählen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-VERWALTUNGSCENTER.
5. Über das Kontextmenü der Gesamtstruktur wählen Sie PAPIERKORB AKTIVIEREN, siehe [Abbildung 7.19](#). Ist er bereits aktiviert, ist die Funktion ausgegraut.

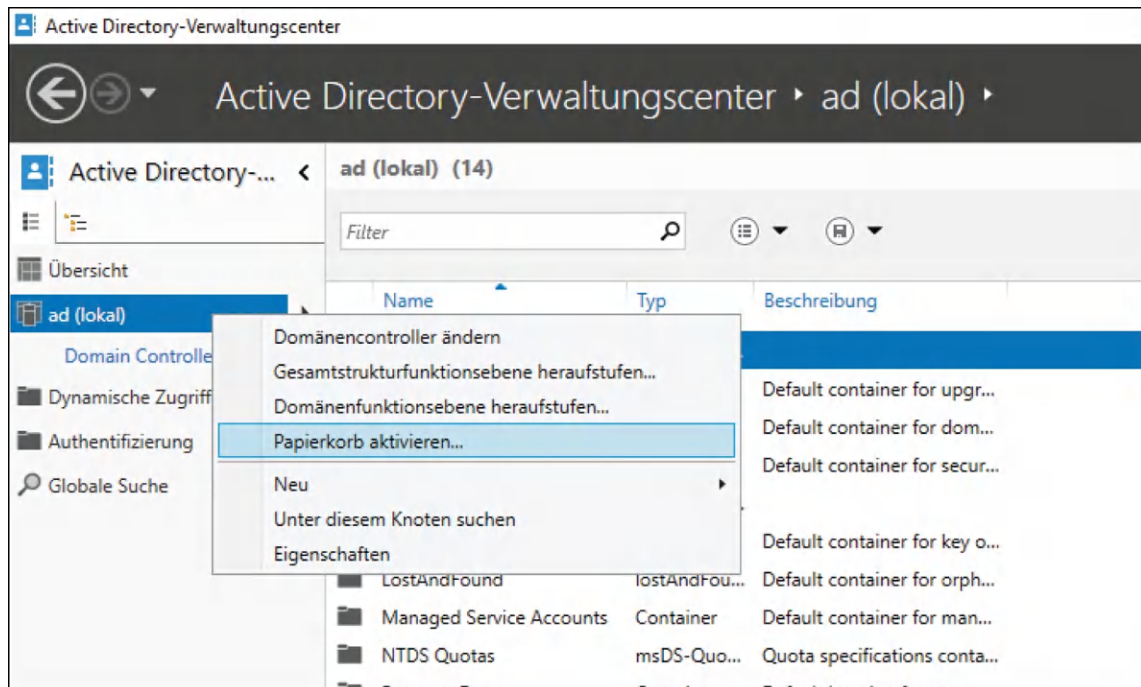


Abbildung 7.19: Die Aktivierung des AD-Papierkorbs im AD-Verwaltungscenter ist nur möglich, sofern alle beteiligten DCs zum Zeitpunkt der Aktivierung erreichbar sind.

6. Sofern nicht alle DC-Replikationspartner aktiv sind, erscheint eine Fehlermeldung, die das Aktivieren verhindert.



Sinnvollerweise sollten Sie sich mit der Funktion der Wiederherstellung im Vorfeld mit Testdaten vertraut machen. Löschen Sie einen Benutzer, den Sie Gruppen zugeordnet haben, oder eine »verschachtelte Gruppe« und stellen Sie diese im AD Verwaltungscenter wieder her.

Active-Directory-Verwaltungscenter

Das AD-Verwaltungscenter ist eine praktische Hilfe, um das Arbeiten mit AD-Konten und -Strukturen zu vereinfachen. Anstatt sich die verschiedenen Funktionen in unterschiedlichen Dialogfenstern »zusammenzuklicken«, gibt es in dem noch recht jungen Verwaltungscenter eine interessante Zusammenstellung der gebräuchlichen Funktionen.

- ✓ Suche nach Benutzerkonten
- ✓ Änderung von Passwörtern
- ✓ Zuordnung zu Gruppen
- ✓ Wiederherstellung von gelöschten Objekten mithilfe des AD-Papierkorbs

Die Wiedererstellung einzelner Objekte ist einfach durchzuführen:

1. Klicken Sie im Navigationsbereich des ACTIVE DIRECTORY-VERWALTUNGSCENTERS auf den Domänennamen.
2. Doppelklicken Sie in der Verwaltungsliste auf DELETED OBJECTS.
3. Klicken Sie mit der rechten Maustaste auf WIEDERHERSTELLEN oder klicken Sie auf WIEDERHERSTELLEN im Bereich AUFGABEN.
4. Das Objekt wird an seinem ursprünglichen Ort wiederhergestellt. Alternativ gibt es den Befehl WIEDERHERSTELLEN IN, um das Objekt an einem anderen Ort wiederherzustellen, siehe [Abbildung 7.20](#).

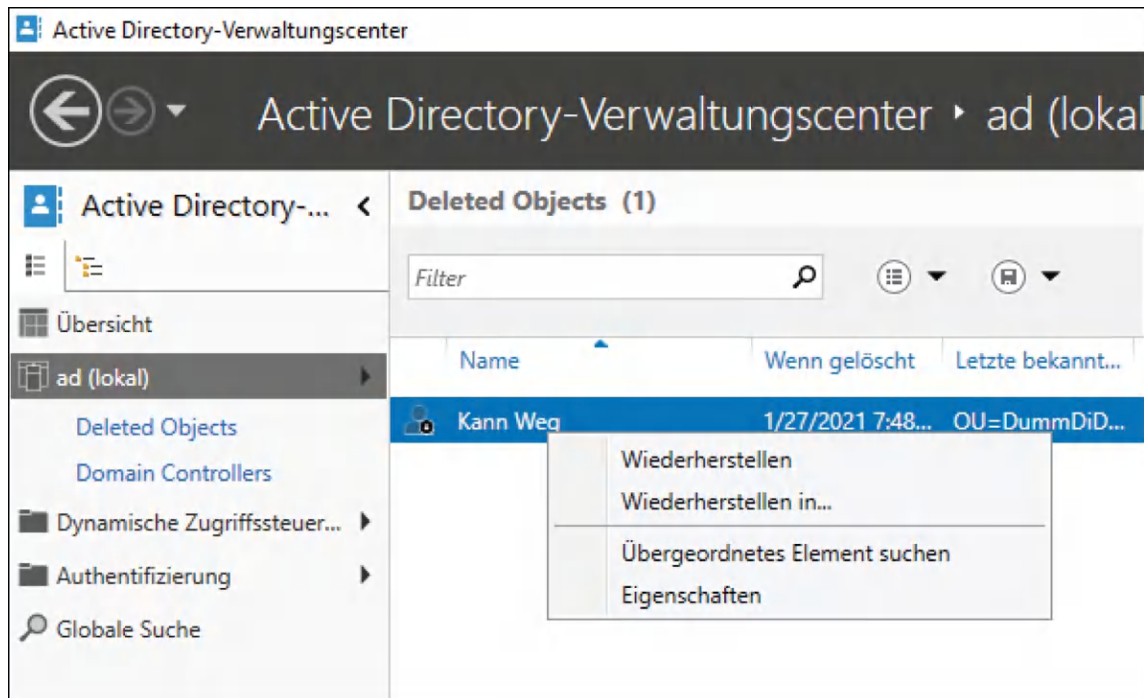


Abbildung 7.20: Neben der Wiederherstellung gelöschter Objekte können Sie im

Verwaltungscenter Benutzer suchen, Passwörter ändern oder Gruppenzuordnungen vornehmen.

Die Wiederherstellung mehrerer Objekte auf derselben Ebene geschieht funktionell wie die Einzelobjektwiederherstellung. Verwenden Sie die -Taste, um eine Mehrfachauswahl durchzuführen.

Das in der [Abbildung 7.20](#) zu sehende Kommando ÜBERGEORDNETES ELEMENT SUCHEN ist leider nicht zur »gefälligen Zierde« vorhanden, sondern offenbart schon jetzt einen funktionellen Mangel:



Sie müssen den Wiederherstellungsprozess unbedingt verstehen, um mehrere über- und untergeordnete Objekte wiederherzustellen, da das Active-Directory-Verwaltungscenter verschachtelte Strukturen gelöschter Objekte nicht in einer einzelnen Aktion wiederherstellen kann.

Diese Einschränkung bedingt die folgende Vorgehensweise:

1. Stellen Sie das oberste Objekt in der gelöschten Struktur wieder her.
2. Stellen Sie die direkt untergeordneten Objekte dieses übergeordneten Objekts wieder her.
3. Stellen Sie die direkt untergeordneten Objekte dieser übergeordneten Objekte wieder her.
4. Wiederholen Sie den Vorgang so lange, bis Sie alle Objekte wiederhergestellt haben.

Sie können untergeordnete Objekte nur wiederherstellen, wenn Sie deren übergeordnetes Objekt wiederhergestellt haben. Andernfalls wird der folgende Fehler ausgegeben: »Der Vorgang konnte nicht ausgeführt werden, da das übergeordnete Objekt instanziiert oder gelöscht wurde«.



Weitere Informationen und Tipps zur Wiederherstellung von Objekten im AD finden Sie in einem äußerst umfangreichen Microsoft-Doc zum Thema »Advanced AD DS Management«

(Technisches Level 200), zu finden unter <https://bit.ly/3opbxZ5>.

Gruppen, Benutzer, Container und OUs

Kommen wir nun zu einer primären Aufgabe in einer Domäne: der Anlage und Verwaltung von Benutzer- und Computerobjekten. Hierbei handelt es sich um elementare Bestandteile der Domäne – konzeptionell schon viele Jahre alt und schon zu Windows-NT-Zeiten enthalten.

Beim ersten Blick in das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND -COMPUTER gibt die Ansicht einige Strukturen preis:

- ✓ Builtin
- ✓ Computers
- ✓ Domain Controllers
- ✓ ForeignSecurityPrincipals
- ✓ Managed Service Accounts
- ✓ Users

Dem aufmerksamen Betrachter wird nicht entgangen sein, dass alle Icons identisch sind, mit Ausnahme des Ordners für DOMAIN CONTROLLERS. Bei den hier sichtbaren Objekten handelt es sich um Container auf der obersten Ebene der Domänenpartition. Einzig die DOMAIN CONTROLLERS sind eine OU (Organization Unit – im deutschsprachigen Raum Organisationseinheiten genannt). Das Plural-s bei den »Domain Controllers« ist stets vorhanden, auch wenn Sie in Ihrer Umgebung nur einen Domänencontroller betreiben.

Container und OUs sind keine Gruppen, sondern Strukturelemente. Der Unterschied zwischen einem Container und einer OU besteht darin, dass Sie auf einer OU spezifische Einstellungen in Form von Gruppenrichtlinien zuweisen können. Container sind hierzu nicht geeignet.

Klicken Sie auf den Container BUILTIN, sehen Sie eine Auflistung von vordefinierten Benutzergruppen, siehe [Abbildung 7.21](#).

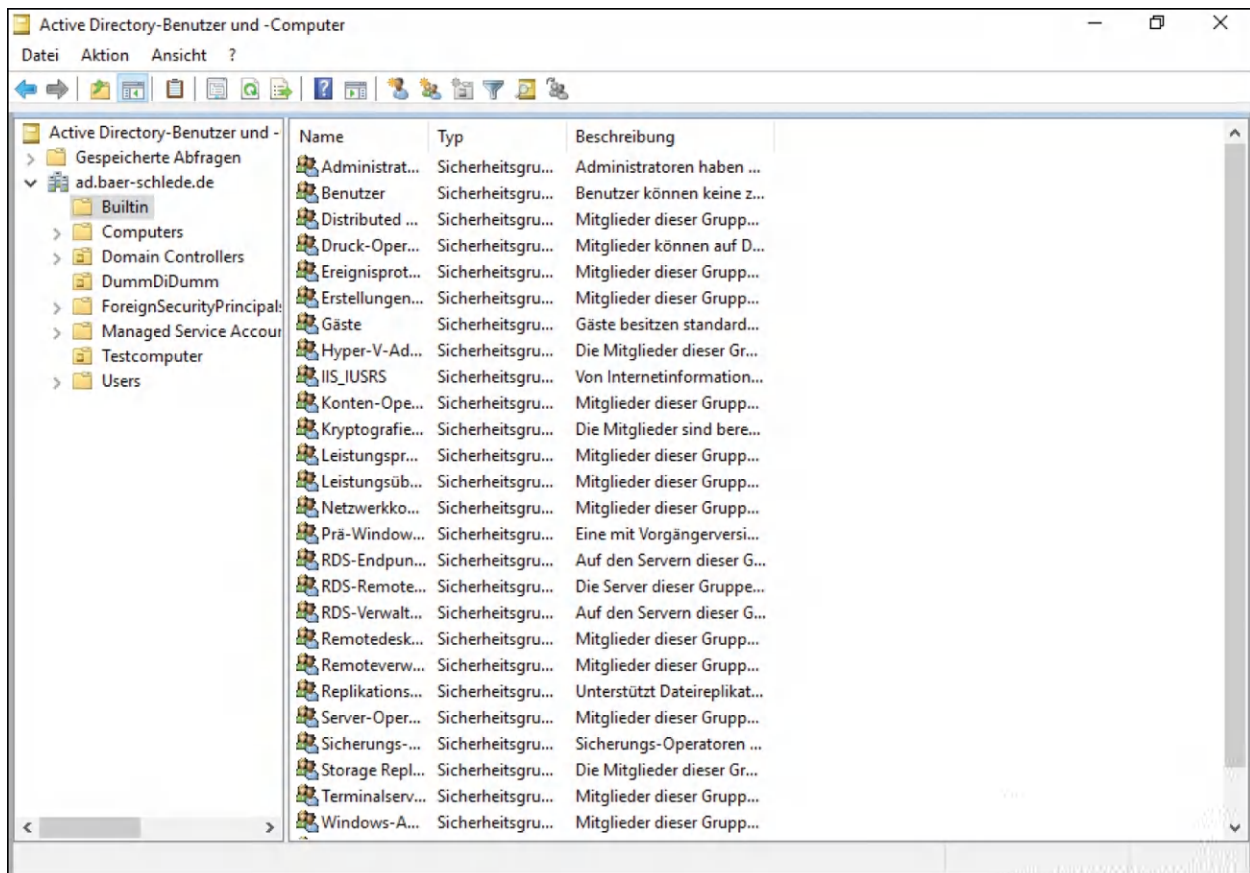


Abbildung 7.21: Vordefinierte Sicherheitsgruppen im Container »Builtin«

Es handelt sich bei den hier aufgelisteten Gruppen um sogenannte Sicherheitsgruppen. Zwei bekannte Gruppen sind gleich obenauf zu sehen:

- ✓ Administratoren
- ✓ Benutzer

Richten Sie nun einmal Ihr Augenmerk auf den Container USERS und schauen Sie sich diese Auflistung genauer an. Auch dort werden Sie zwei wichtige Gruppen, aber auch Benutzer entdecken:

- ✓ Administrator
- ✓ Gast

- ✓ Domänen-Admins
- ✓ Domänen-Benutzer

Eine Gruppe ist eine Zusammenfassung von Benutzern, Gruppen oder weiteren Gruppen. Benutzer und Computer können Mitglieder mehrerer Gruppen gleichzeitig sein. Benutzer und Gruppen können aber nur Mitglied einer OU- oder Containerstruktur sein.

Bei Gruppen im Active Directory wird zwischen zwei Typen unterschieden:

- ✓ Sicherheitsgruppen
- ✓ Verteilergruppen

Letztere sind in unserem Buch nicht von Bedeutung, da sie zur reinen E-Mail-Verteilung zum Einsatz kommen.

Erstellung von Gruppen

Es gibt insgesamt drei Arten von Sicherheitsgruppen:

- ✓ Lokal (in Domäne)
- ✓ Global
- ✓ Universell

Um die verschiedenen Arten von Sicherheitsgruppen erkennen zu können, empfiehlt es sich, eine Gruppe anzulegen:

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
4. Klicken Sie mit der rechten Maustaste auf den Ordner USERS (hierbei handelt es sich um ein Beispiel).
5. Wählen Sie im Kontextmenü NEU | GRUPPE. Es erscheint das Dialogfenster NEUES OBJEKT – GRUPPE, zu sehen in [Abbildung](#)

7.22.

- LOKAL (IN DOMÄNE) – Diese lokalen Sicherheitsgruppen kommen in erster Linie zur Vergabe von Berechtigungen zum Einsatz. Sie erlauben die Aufnahme von Mitgliedern auch aus anderen Domänen. Die lokale Sicherheitsgruppe kann nur für die Berechtigung von Ressourcen innerhalb der eigenen Domäne genutzt werden. Sie können in eine lokale Sicherheitsgruppe weitere lokale Sicherheitsgruppen hinzufügen. Sie sind nur in der eigenen Domäne sichtbar.
- GLOBAL – In Globale Sicherheitsgruppen sind Benutzer- und Computerobjekte der Domäne enthalten. Wenn eine globale Sicherheitsgruppe Zugriff auf Ressourcen einer anderen Domäne benötigt, muss sie zur lokalen Sicherheitsgruppe der anderen Domäne hinzugefügt werden. Sie können nur Mitglieder der eigenen Domäne der Gruppe hinzufügen. Diese Gruppen können jedoch auch zum Zugriff auf Ressourcen in einer anderen Domäne berechtigt werden. Globale Sicherheitsgruppen können als Mitglied in lokalen Sicherheitsgruppen beliebiger Domänen, universelle Sicherheitsgruppen und globale Sicherheitsgruppen der eigenen Domäne aufgenommen werden.

The screenshot shows a Windows dialog box titled "Neues Objekt - Gruppe". At the top, it says "Erstellen in: ad.baer-schlede.de/Users". Below this, there are two text boxes for the group name, both containing "PG-APP-ERP_SYSTEM". Underneath, there are two sections: "Gruppenbereich" (Group Scope) and "Gruppentyp" (Group Type). In the "Gruppenbereich" section, the "Global" radio button is selected. In the "Gruppentyp" section, the "Sicherheit" (Security) radio button is selected. At the bottom right, there are "OK" and "Abbrechen" (Cancel) buttons.

Abbildung 7.22: Bei Anlage einer Gruppe legt der Administrator im Gruppenbereich die Art der Gruppe fest.

- **UNIVERSAL** – Universelle Sicherheitsgruppen dienen der Berechtigung zum Zugriff auf Ressourcen in mehreren Domänen. Alle Gruppen für den Microsoft-Exchange-Betrieb sind beispielsweise universelle Gruppen. Die Gruppenmitgliedschaftsliste wird im globalen Katalog gespeichert.

In der Praxis spricht nichts dagegen, innerhalb des einzigen Netzwerks in einer Domäne stets universelle Gruppen zu verwenden. Im Sinne der besseren Übersicht empfiehlt es sich jedoch für den Administrator, sich an eine rollen- und rechtebasierte Konzeption zu halten.

Dazu passt die hübsche Abkürzung »AGULP«. Konten (»A«ccounts) werden »G«lobalen Gruppen zugewiesen, diese (falls erforderlich) »U«niversalen Gruppen. Die globalen Gruppen sind wiederum in

(Domänen-)»L«okalen Gruppen enthalten, die Domänen-lokalen Gruppen werden in den Rechten (»P«ermissions) verwendet. In [Tabelle 7.1](#) ist das resultierende Schema ersichtlich:



In kleinen Umgebungen mit nur einem Netzwerkbereich ist es vollkommen ausreichend, in der Domäne stets universelle Gruppen zu verwenden.

Gruppenbereich	Kann in Domänen-lokalen Gruppen enthalten sein	Kann in globalen Gruppen enthalten sein	Kann in universellen Gruppen enthalten sein
Lokale Domänengruppe	Selbe Domäne	Nein	Nein
Globale Gruppe	Ja	Selbe Domäne	Ja
Universelle Gruppe	Ja	Nein	Ja

Tabelle 7.1: AGULP-Tabelle

Benutzer Gruppen zuweisen

Gruppen sind zur Aufnahme von Computern, Benutzern und weiteren Gruppen geeignet. Legen wir exemplarisch eine kleine Konstellation an und betrachten wir die Auswirkungen:

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
4. Klicken Sie mit der rechten Maustaste auf den Ordner USERS.
5. Wählen Sie im Kontextmenü NEU | GRUPPE. Erstellen Sie eine Gruppe »Sekretariat« mit dem Gruppennamen »PG-Sekretariat«. Als Gruppenbereich wählen Sie UNIVERSAL und den Typ SICHERHEIT.



Wir haben uns angewöhnt, den Einsatzzweck einer Gruppe bereits

über die Bezeichnung zum Ausdruck zu bringen. Der Vorsatz »PG-« steht hier für »Permission Group«, also Berechtigungsgruppe. Hierbei handelt es sich nur um ein Beispiel – das kann jeder Administrator halten, wie er will. Wichtig ist lediglich: Gönnen Sie sich ein stringentes System!

6. Klicken Sie erneut mit der rechten Maustaste auf den Ordner USERS.
7. Wählen Sie im Kontextmenü NEU | GRUPPE. Erstellen Sie eine Gruppe »Chefsekretariat« mit dem Gruppennamen »PG-Chefsekretariat«. Als Gruppenbereich wählen Sie UNIVERSAL und den Typ SICHERHEIT.
8. Klicken Sie erneut mit der rechten Maustaste auf den Ordner USERS.
9. Wählen Sie im Kontextmenü NEU | BENUTZER. Erstellen Sie ein Benutzerkonto für »Hildegard Mayer« als Chefsekretärin. Benutzername, Kennwort und die Merkmale für die Kennwortänderung sind für dieses Beispiel unerheblich.
10. Klicken Sie erneut mit der rechten Maustaste auf den Ordner USERS.
11. Wählen Sie im Kontextmenü NEU | BENUTZER. Erstellen Sie ein Benutzerkonto für »Julia Schmidt« als Sekretärin.
12. Öffnen Sie das Benutzerkonto von » Julia Schmidt « durch einen Doppelklick, wählen Sie die Registerkarte MITGLIED VON und wählen Sie die Schaltfläche HINZUFÜGEN..., um das Konto der Gruppe »PG-Sekretariat« zuzuordnen, zu sehen in [Abbildung 7.23](#).

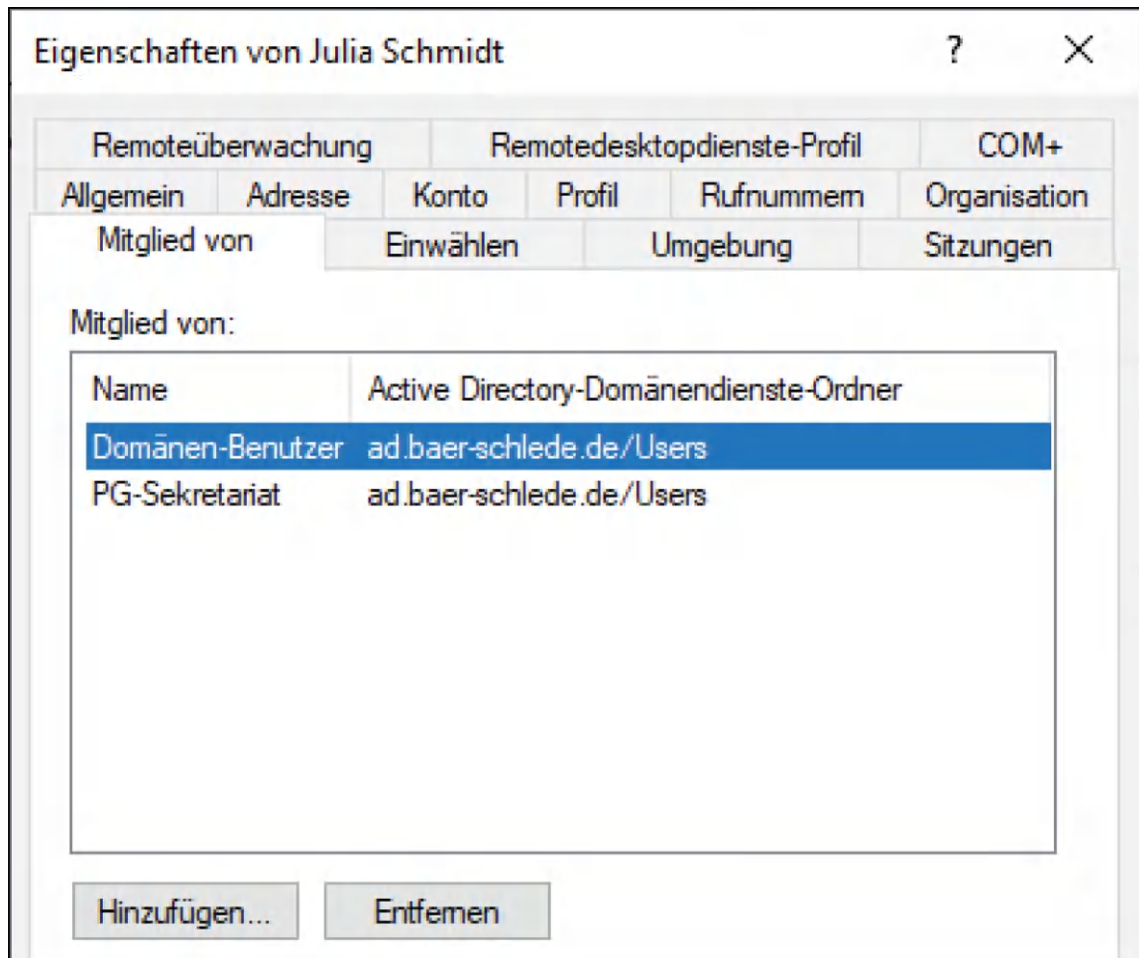


Abbildung 7.23: Benutzer können Mitglieder verschiedener Gruppen sein.

Geben Sie hierzu den Objektnamen ein und wählen Sie die Schaltfläche NAMEN ÜBERPRÜFEN, um einen Schreibfehler auszuschließen – wurde der Name korrekt geschrieben, wird er unterstrichen dargestellt. Über ERWEITERT... können Sie einen detaillierten Suchdialog aktivieren.

13. Öffnen Sie nun die Gruppe »PG-Chefsekretariat« über einen Doppelklick und wählen Sie die Registerkarte MITGLIEDER. Wählen Sie nun die Schaltfläche HINZUFÜGEN... und suchen Sie das Benutzerkonto von »Hildegard Mayer«, um es zuzuordnen. Wählen Sie nun in dem Dialogfenster die Registerkarte MITGLIED VON, klicken Sie auf die HINZUFÜGEN... und suchen Sie die Berechtigungsgruppe »PG-Sekretariat«.
- Schließen Sie das Hinzufügen des Benutzerkontos von Frau Mayer

und die Gruppenmitgliedschaftszuordnung in die Berechtigungsgruppe »PG-Sekretariat« durch einen Klick auf OK ab.

14. Öffnen Sie noch einmal die Gruppe »PG-Sekretariat« und öffnen Sie die Registerkarte MITGLIEDER, um die Zuordnung aus dieser Perspektive anzuschauen.

In unserem Beispiel ist Frau Mayer als Chefsekretärin über ihre Gruppenmitgliedschaft der Berechtigungsgruppe PG-Chefsekretariat automatisch zum Mitglied der Gruppe PG-Sekretariat geworden. In der praktischen Konsequenz bedeutet dies, dass Chefsekretärinnen und Chefsekretäre auch Zugriff auf freigegebene Objekte der Gruppe »PG-Sekretariat« besitzen.

Mitglieder der Sicherheitsgruppe »PG-Sekretariat« wiederum haben nicht automatisch Zugriff auf freigegebene Objekte, für die die Gruppe »PG-Chefsekretariat« erforderlich ist.



Bei der Zuweisung von Zugriffsrechten sollten Sie stets Sicherheitsgruppen verwenden und keine Benutzer direkt zuordnen. Das mögen Sie beim jetzigen Vorgang vielleicht als Mehraufwand empfinden. Mittel- bis langfristig wird es Ihnen garantiert viel Zeit sparen.

Praktisch an dem Konzept der Gruppenzugehörigkeit ist die Flexibilität bei etwaigen Veränderungen. Stellen wir uns vor, dass Frau Mayer beschließt, den Posten als Chefsekretärin aufzugeben, um wieder im regulären Sekretariat zu arbeiten.

An ihrer statt wird eine neue Kollegin eingestellt – »Sieglinde Nägele« wird als neues Benutzerkonto angelegt und dem Chefsekretariat zugewiesen, anschließend wird Frau Mayer aus der entsprechenden Sicherheitsgruppe entfernt und der Gruppe »PG-Sekretariat« zugeordnet. Sofern keine »personalisierte Zuweisung« von Rechten auf Benutzerkonten erfolgte, sind derlei Umstellung mit wenigen Mausklicks erledigt:

1. Starten Sie den SERVER-MANAGER.

2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
4. Klicken Sie mit der rechten Maustaste auf den Ordner USERS.
5. Wählen Sie im Kontextmenü NEU | BENUTZER. Erstellen Sie ein Benutzerkonto für »Sieglinde Nägele« als Chefsekretärin. Benutzername, Kennwort und die Merkmale für die Kennwortänderung sind für dieses Beispiel unerheblich.
6. Öffnen Sie nun die Gruppe »PG-Chefsekretariat« über einen Doppelklick und wählen Sie die Registerkarte MITGLIEDER. Wählen Sie nun die Schaltfläche HINZUFÜGEN... und suchen Sie das Benutzerkonto von »Sieglinde Nägele«, um es zuzuordnen.
7. Anschließend markieren Sie das Konto von »Hildegard Mayer« und wählen die Schaltfläche ENTFERNEN.
8. Öffnen Sie nun die Gruppe »PG-Sekretariat« über einen Doppelklick und wählen Sie die Registerkarte MITGLIEDER. Wählen Sie nun die Schaltfläche HINZUFÜGEN... und suchen Sie das Benutzerkonto von »Hildegard Mayer«, um es zuzuordnen.



Zwar zeigt der Windows Server stets Benutzernamen und Gruppen, um den menschlichen Anwendern die Bearbeitung und die Wiedererkennung zu vereinfachen. Technisch arbeitet Windows im Hintergrund jedoch stets mit einer eindeutigen Kennung – der sogenannten »Sicherheitskennung« (SID).

Die SIDs der Konten bestehen aus dem Sicherheitskennungspräfix der Domäne und einer eindeutigen RID (Relative ID), die vom RID-Master zugewiesen wurde. Der Einrichtung der SID ist es zu verdanken, dass Sie Benutzerkonten auch komplett umbenennen können, ohne dass es dabei zu Problemen kommt. Beim Löschen und der Neuanlage eines gleichlautenden Kontos erzeugt Windows eine unterschiedliche SID.

Benutzerkontentypen

Im Zusammenspiel mit Windows-Servern wird zwischen zwei unterschiedlichen Benutzerkontentypen unterschieden:

- ✓ Domänenbenutzerkonten – Mit dem AD definierte Benutzerkonten werden als Domänenbenutzerkonten bezeichnet. Anwender melden sich mit diesem Benutzerkonten an und können im Anschluss auf alle Ressourcen in der Domäne unter dieser »Identität« zugreifen. Administratoren erstellen und bearbeiten diese Konten mit dem Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
- ✓ Lokale Benutzerkonten – Auf lokalen Computern (Server oder Clients) definierte Benutzerkonten werden als lokale Benutzerkonten bezeichnet. Lokale Benutzerkonten können nur auf den lokalen Computer zugreifen und müssen sich vor dem Zugriff auf Ressourcen, die über das Netzwerk bereitgestellt werden, authentifizieren. Sie erstellen lokale Benutzer über das Dienstprogramm LOKALE BENUTZER UND GRUPPEN.



In einer Domäne besitzen nur Arbeitsstationen (Clients) und Mitgliedsserver lokale Benutzer- und Gruppenkonten. Auf dem ersten Domänencontroller einer Domäne werden diese Konten aus der Datenbank des lokalen Sicherheitsmanagers (Security Account Manager, SAM) in das Active Directory verschoben und somit zu Domänenkonten. DCs besitzen keine lokalen Konten.

In der Praxis ist es durchaus üblich, mit lokalen Berechtigungen auf Mitgliedsservern zu arbeiten. Insbesondere in größeren oder auf Sicherheit ausgerichteten Umgebungen gibt es Konstellationen, bei denen IT-Personal zwar über lokale Administrationsrechte verfügt, im Domänenkontext jedoch nur über reguläre Benutzerrechte.

Standardbenutzerkonten und Gruppen

Die verschiedenen administrativen Konten haben wir bereits betrachtet, es gibt aber noch einige vordefinierte Konten, über die Sie Kenntnis haben

sollten. Bei der Installation von Windows Server stehen automatisch einige Standardbenutzer und -gruppen zur Verfügung. Diese dienen als Basis für den Ausbau des Netzwerks. Hierbei handelt es sich um drei Standardkontoarten:

- ✓ INTEGRIERT – Mit Betriebssystem, Anwendungen und Diensten installierte Benutzer- und Gruppenkonten.
- ✓ VORDEFINIERT – Mit dem Betriebssystem installierte Benutzer- und Gruppenkonten.
- ✓ SONDERGRUPPEN – Spezielle Gruppen, die bei Zugriff auf Netzwerkressourcen implizit erstellt werden.



Sie können die vom Betriebssystem erstellten Standardbenutzer und -gruppen, beispielsweise die Gruppe »Administratoren«, zwar ändern, jedoch nicht löschen. Die Neuanlage der Gruppen würde eine neues SID generieren und nicht mehr zur erforderlichen SID passen.

Bei den integrierten Benutzerkonten, die Windows für besondere Zwecke verwendet, unterscheiden wir:

- ✓ SYSTEM – Bei diesem lokalen Computerkonto handelt es sich um eine Art Pseudokonto. Unter diesem Benutzer laufen die Systemprozesse und Tasks auf Systemebene. Das SYSTEM-Konto ist Mitglied der Administratorengruppe auf dem Server und hat somit alle Benutzerrechte auf der Maschine. Sofern Dienste oder Applikationen unter SYSTEM laufen, haben sie folglich uneingeschränkten Vollzugriff auf den Server.

Werfen Sie einmal einen Blick auf die Dienste Ihres Servers und Sie werden ebenso wie hier in [Abbildung 7.24](#) sehen, dass sich die Mehrzahl der Dienste auf der Maschine als »lokales System« anmelden – dahinter verbirgt sich das SYSTEM-Konto.

Es gibt zudem Dienste, die das »lokale Systemkonto« verwenden und darüber hinaus über das gesetzte Optionshäkchen Datenaustausch zwischen Dienst und Desktop zulassen und mit dem Desktop

interagieren dürfen.

- ✓ LOKALER DIENST – Der lokale Dienst ist ebenfalls eine Art Pseudokonto. Jedoch anders als das SYSTEM-Konto können Sie als Administrator das Recht nicht per Option im Dialog auswählen, sondern müssten es bei den Diensten direkt unter dem Eintrag DIESES KONTO eingeben.

Anders als das SYSTEM-Konto ist das Pseudokonto LOKALER DIENST nicht Mitglied der Administratorengruppe, sondern ein Mitglied der Gruppe »Benutzer«. Wie der Name schon erahnen lässt, kann dieser Pseudobenutzer nur auf lokale Ressourcen des eigenen Systems zugreifen und nicht auf Netzwerkressourcen.

- ✓ NETZWERKDIENST – Bei diesem Pseudokonto handelt es sich um die netzwerkfähige Variante von LOKALER DIENST. Der NETZWERKDIENST ist ebenfalls Mitglied der Gruppe »Benutzer«. Die Möglichkeiten dieses Kontos sind also geringer als bei SYSTEM, aber höher als bei LOKALER DIENST.
- ✓ GAST – Während die bisher genannten Konten Pseudokonten darstellen, mit denen sich de facto niemand tatsächlich anmeldet, ist das Konto GAST ein reguläres Benutzerkonto. Per Definition ist das GAST-Konto für einmalige oder gelegentliche Zugriffe vorgesehen. Passend zu diesem Konto gibt es auch eine Standardgruppe mit dem Namen »Gäste« auf lokaler Ebene und eine Standardgruppe »Domänen-Gäste«.

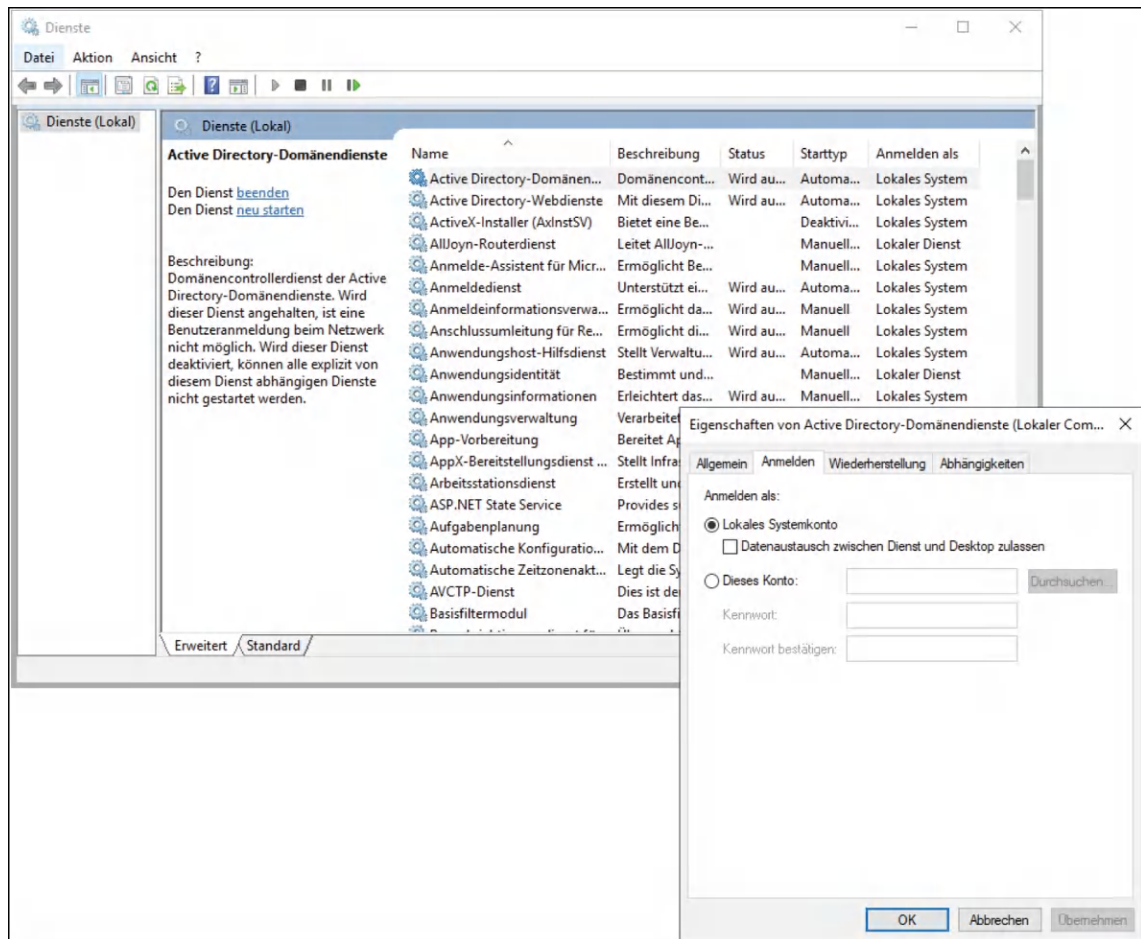


Abbildung 7.24: Die Mehrheit der Dienste unter Windows arbeitet mit dem Konto »SYSTEM«.

In der Standardauslieferung von Windows und Windows Server ist das GAST-Konto deaktiviert. Zwar sind die Rechte des GAST-Kontos limitiert, es ist aber auch Mitglied der Gruppe JEDER und kann somit möglicherweise auf mehr Daten zugreifen, als dem Administrator recht ist.



Sie sollten das Konto GAST nicht aktivieren. Wenn Sie es dennoch tun müssen, stellen Sie sicher, dass Sie es vor der ersten Verwendung stärker einschränken, das Kennwort regelmäßig ändern und das Konto idealerweise umbenennen.

Rechte und Privilegien

Typischerweise ordnen Sie als Administrator einem Benutzerkonto eine

oder mehrere Gruppen zu, um folgende Fähigkeiten zuzuweisen:

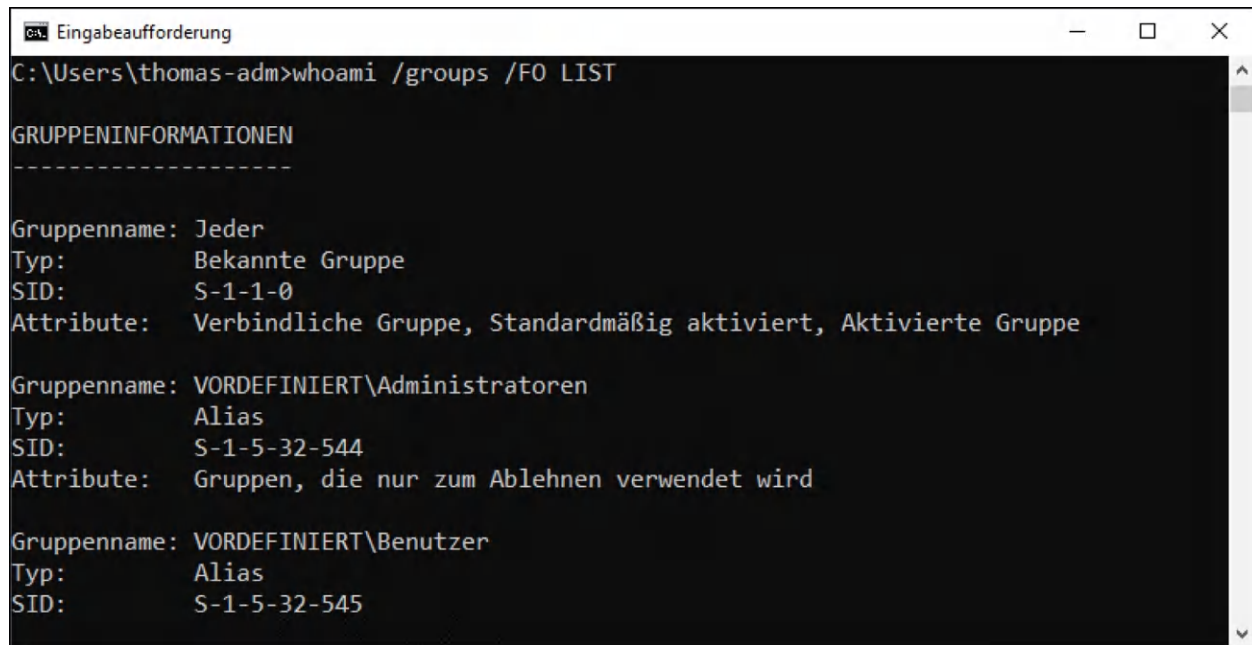
- ✓ **Anmelderechte** – Sie können beispielsweise festlegen, ob sich eine Gruppe an einem Server oder Computer lokal oder per Remotedesktop-Zugriff anmelden darf.
- ✓ **Vordefinierte Fähigkeiten** – Mitglieder der Gruppe »Administratoren« oder »Benutzer« erhalten automatisch eine Reihe von Rechten und Fähigkeiten. Beispielsweise kann ein Administrator andere Benutzerkonten anpassen, Mitglieder der normalen Gruppe »Benutzer« sind zwar in der Lage, ihr eigenes Kennwort zu ändern (sofern berechtigt), sie können aber keine anderen Benutzerkonten ändern.
- ✓ **Zugriffsberechtigung** – Typischerweise steuern Administratoren die Zugriffe wie Lesen, Ändern oder Löschen über Gruppenzugehörigkeiten. Die Vergabe von Zugriffsberechtigungen ist eine der wichtigsten Fähigkeiten von Gruppen.
- ✓ **Privilegien** – Hierbei handelt es sich um detaillierte Benutzerrechte, die an Gruppen gebunden sind, mit deren Hilfe Sie als Administrator sehr präzise die Rechte steuern können. Möglicherweise haben Sie eine solch detaillierte Auflistung bereits vermisst – unter Windows geschieht diese Steuerung über Gruppenrichtlinien. Es ist zwar generell möglich, Gruppenrichtlinien auch auf einzelne Benutzer einwirken zu lassen, in der Praxis kommt jedoch die Zuweisung einer Gruppenrichtlinie auf eine Gruppe zum Einsatz.



Weitere Details zur Verwendung von Gruppenrichtlinien finden Sie in [Kapitel 17](#), während sich das [Kapitel 10](#) im Detail mit der Freigabe von Ressourcen im Zusammenspiel mit Gruppen auseinandersetzt.

Um sich möglichst zügig die eigene Gruppenzugehörigkeit anzeigen zu lassen, siehe [Abbildung 7.25](#), empfiehlt sich das Kommandozeilenprogramm `whoami` mit einem Befehlsschalter:

```
whoami /groups /FO LIST
```



```
C:\Users\thomas-adm>whoami /groups /FO LIST

GRUPPENINFORMATIONEN
-----

Gruppenname: Jeder
Typ:         Bekannte Gruppe
SID:         S-1-1-0
Attribute:   Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe

Gruppenname: VORDEFINIERT\Administratoren
Typ:         Alias
SID:         S-1-5-32-544
Attribute:   Gruppen, die nur zum Ablehnen verwendet wird

Gruppenname: VORDEFINIERT\Benutzer
Typ:         Alias
SID:         S-1-5-32-545
```

Abbildung 7.25: Ausgabe der Gruppenzugehörigkeiten

Kapitel 8

DNS und DHCP

IN DIESEM KAPITEL

- Grundlagen der Namensauflösung
- Installation und Konfiguration von DNS
- DNS-Funktionen der verschiedenen Windows-Server
- Grundlagen von DNSSEC
- Grundlagen von DHCP
- Dynamische Adressierung
- Installation von IPAM

Aller Wahrscheinlichkeit nach haben Sie es schon einmal gehört: Ohne DNS-Namensauflösung geht beim Active Directory gar nichts. Und sollen wir Ihnen was sagen? Das stimmt! Ohne die funktionelle Grundlage, der Namensauflösung, ist eine Verwaltung von Windows-Domänen schlichtweg nicht möglich.

Und, weil das Thema wirklich so wichtig ist, haben wir uns dazu entschieden, dass wir zu einigen DNS-Themen etwas detaillierter ans Werk gehen als vielleicht an anderen Stellen in diesem Buch. Auch dem gestandenen Administrator und IT-System-Berater kann es nicht schaden, sich noch einmal intensiver mit den Grundlagen auseinanderzusetzen.

Grundlagen der Namensauflösung

DNS (Domain Name Service) ist wohl der wichtigste Dienst vieler IP-basierter Netzwerke und kaum wegzudenken. Letztendlich fungiert DNS wie ein Telefonbuch, in dem statt Telefonnummern IP-Adressen mit

Namen, wie beispielsweise tecchannel.de verknüpft sind. Einer der Server, der die Website der Suchmaschine Google zum Zeitpunkt der Manuskripterstellung hostet, ist über die IP-Adressen 216.58.205.227 in der IPv4-Notation und 2a00:1450:4001:819::2003 in der IPv6-Schreibweise zu erreichen. Da sich – spätestens mit IPv6 – kaum ein Anwender freiwillig diese Zahlenkolonnen merken will, gibt es DNS.



Mitunter ist der »Einfallsreichtum« bei der Namensvergabe durch primär technisch geprägte Administratoren so weitreichend, dass eine IPv4-Adresse für Benutzer möglicherweise doch leichter zu merken ist. Das verbreitete Codieren aller erdenklichen Merkmale, wie Betriebssystem, Standort, Aufgabe oder Seriennummer von Computern, führen dazu, dass das DNS ad absurdum geführt wird.

Ursprünglich geht der Name Service auf das Jahr 1983 zurück. Paul Mockapetris definierte in den Request for Comments (RFC) 882 und 883 seinen ersten Entwurf für eine Namensauflösung. Beide RFC-Grundlagen sind mittlerweile durch die RFC 1034 und 1035 abgelöst und durch die IETC (Internet Engineering Task Force) um weitere Standards ergänzt worden.



Ohne DNS-Namensauflösung würde das Internet in der uns bekannten Form gar nicht funktionieren. Verschiedene Internet-Dienstleister und Provider betreiben öffentliche DNS-Server.

Einfach zu merkende Adressen sind beispielsweise 8.8.8.8 und 8.8.4.4 beziehungsweise 2001:4860:4860::8888 und 2001:4860:4860::8844 von Google oder 1.1.1.1 und 1.0.0.1 beziehungsweise 2606:4700:4700::1111 und 2606:4700:4700::1001 von Cloudflare.

Die ursprüngliche Aufgabe bestand darin, die lokale hosts-Datei, die für die Namensauflösung zuständig ist, abzulösen und ein verteiltes System zur Namensauflösung bereitzustellen. Die Kernmerkmale des DNS sind aus der Frühzeit erhalten geblieben:

- ✓ dezentrale Verwaltung
- ✓ hierarchische Strukturierung des Namensraums in Form eines Baums
- ✓ Eindeutigkeit der Namen und einzelner Server
- ✓ unabhängige Erweiterbarkeit



Die hosts-Datei gibt es noch immer! Sie befindet sich bei Windows-Computern unter `C:\Windows\System32\drivers\etc`. Sie wird standardmäßig als erste Quelle abgefragt, wenn es darum geht, zu einem Host-Namen die IP-Adresse zu analysieren.

Ein kleines Beispiel soll die Funktionalität der hosts-Datei aufzeigen:

1. Starten Sie die Eingabeaufforderung und geben Sie ein

```
ping allwissendemuellhalde
```

Aller Wahrscheinlichkeit nach kann Ping die allwissendemuellhalde nicht finden.

2. Wiederholen Sie den Vorgang mit

```
ping wikipedia.de
```

So weit, so gut. Ihr Computer kann also für existierende Adressen über DNS die IP-Adressen ermitteln. Das hat noch wenig mit der hosts-Datei zu tun, dazu kommen wir jetzt:

3. Kopieren Sie die IP-Adresse von Wikipedia in die Zwischenablage.
4. Öffnen Sie nun den Editor mit Administrationsrechten.
5. Wählen Sie DATEI ÖFFNEN:
`C:\Windows\System32\drivers\etc\hosts`.
6. Kopieren Sie die IP-Adresse an die unterste Stelle.
7. Geben Sie hinter der IP-Adresse ein Leerzeichen ein und den Hostnamen: allwissendemuellhalde.
8. Speichern Sie die Datei.

Wenn Sie nun in Ihren Browser `http://allwissendemuellhalde` eingeben und den Zertifikatsfehler beim Seitenaufruf ignorieren, erreichen Sie die Webseite unter diesem Namen. Wenn Sie den Vorgang noch einmal wiederholen und den Eintrag statt für die `allwissendemuellhalde` für www.telekom.de anlegen, wird die Tragweite der `hosts`-Datei deutlich (siehe [Abbildung 8.1](#)).



Abbildung 8.1: Durch Manipulation der »hosts«-Datei erzeugt die Namensauflösung seltsame Ergebnisse.

Noch bevor Microsoft Windows einen DNS-Server befragt, greift das Betriebssystem zunächst auf die lokale `hosts`-Datei zu und prüft, ob es einen Eintrag gibt, der für einen Hostnamen auf eine IP-Adresse verweist. Dieses Verhalten geht auf die frühesten Computer zurück.



Wenn Sie im Rahmen des Troubleshootings einmal an einen Computer gelangen, dessen Namensauflösungsverhalten mehr als seltsam ist – beispielsweise, weil eine ganze Domäne noch immer auf einer uralten IP-Adresse zu finden ist oder ein bereits demontierter Server noch immer auf seinen Namen reagiert –, dann werfen Sie einen Blick in die `hosts`-Datei.

Basiseinrichtung des DNS-Server-Diensts

Ein grundinstallierter Windows-Server ist, sofern er von einem DHCP-Server-Dienst mit einer IP-Lease versorgt wurde, schon in der Lage, über das Netzwerk DNS-Anfragen abzugeben. Hier unterscheidet sich der Server nicht von einem einfachen Windows-Client-Computer.

Sofern Sie in Ihrem Netzwerk über ein Active Directory verfügen, haben Sie aller Wahrscheinlichkeit nach auch einen aktiven DNS-Server im Einsatz. Sollten Sie wiederum auf einem nicht weiter konfigurierten Server einen AD-Domänendienst installieren wollen, wird der Einrichtungsassistent des Server-Managers Sie als Administrator direkt zur Einrichtung eines DNS-Diensts motivieren.

Aufgrund der engen Verzahnung des Active Directory mit dem DNS ist die gleichzeitige Installation überaus sinnvoll und wird in der Installationsbeschreibung explizit empfohlen.



Vor ein paar Jahren grassierte ein Gerücht durch die Internetforen, dass der Installationsassistent von Windows bei der Einrichtung des Active Directory den DNS nicht ordnungsgemäß konfigurieren würde. Dieses Gerücht bestand früher schon zu Unrecht – und daran hat sich bis heute nichts geändert.

Losgelöst von dieser Empfehlung soll nun ein DNS-Server auf einem Windows-Server unabhängig von einer Domänenanbindung zur Installation kommen. Verwenden Sie hierzu einfach den Assistenten zum Hinzufügen von Rollen und Features im Server-Manager (siehe [Abbildung 8.2](#)).

1. Wählen Sie unter im Abschnitt SERVERROLLEN den DNS-SERVER aus.

Verfügt Ihr Server lediglich über eine dynamische IP-Adresse, erscheint ein Warnhinweis, dass eine statische IP-Adresse erforderlich

ist.

2. Bestätigen Sie im weiteren Verlauf die folgenden Dialoge mit WEITER, OK und SCHLIESSEN.

Nach einigen Minuten steht unter Tools oder im Startmenü unter Windows-Verwaltungsprogramme der DNS-Manager zur Verfügung.

3. Klicken Sie auf den Servernamen in der Baumstruktur unter dem Eintrag DNS, und im Inhaltsbereich des Fensters erscheinen die Einträge:
 - Forward-Lookupzonen
 - Reverse-Lookupzonen

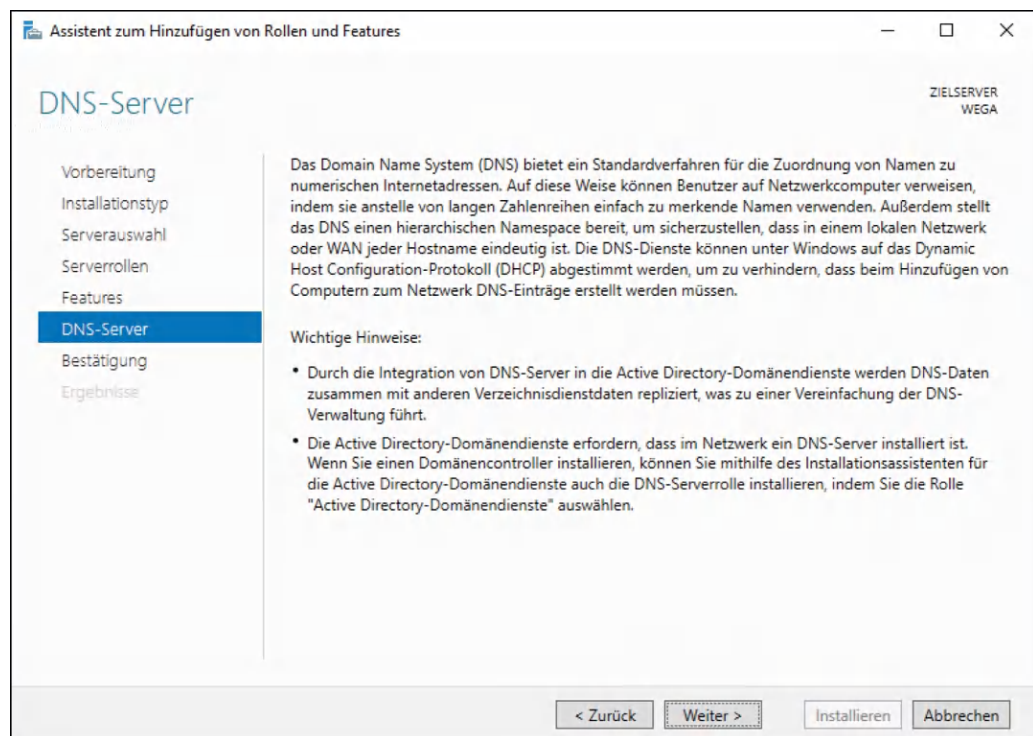


Abbildung 8.2: Die Installation des DNS-Diensts wird durch den Assistenten unterstützt. Der DNS-Server funktioniert auch ohne AD-Anbindung.

- Vertrauenspunkte
- Bedingte Weiterleitung
- Stammhinweise
- Weiterleitungen

Zum jetzigen Zeitpunkt ist zwar der DNS-Server-Dienst installiert, aber er ist noch nicht aktiv. Mit den nächsten Schritten sorgen wir für eine Inbetriebnahme dahin gehend, dass der Server DNS-Anfragen von beliebigen Client-Computern beantwortet.

4. Rechtsklick auf den Server-Namen im DNS-Manager in der Baumstruktur.
5. DNS-SERVER KONFIGURIEREN auswählen.
6. Mittige Auswahl FORWARD-LOOKUPZONE ERSTELLEN
7. Bestätigen Sie DIESER SERVER VERWALTET DIE ZONE.
8. Verwenden Sie einen Fantasienamen für die Zone, beispielsweise (siehe [Abbildung 8.3](#)) mooofs.moep.

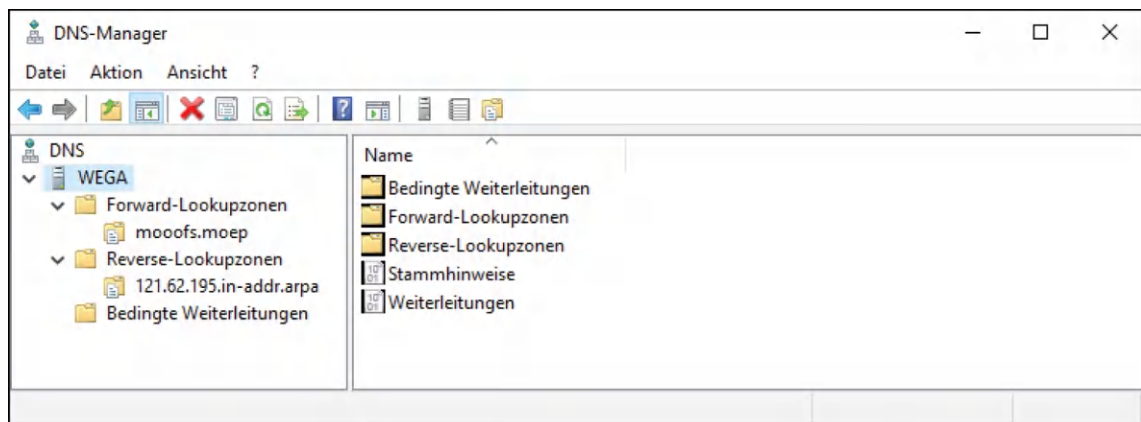


Abbildung 8.3: Ein DNS-Server ist typischerweise für eine oder mehrere Zonen zuständig und löst die Namen für den Bereich auf.

9. Bestätigen Sie die Anlage der neuen Datei mit WEITER.
10. Wählen Sie DYNAMISCHE UPDATES NICHT ZULASSEN.
Wenn Sie über einen vorgelagerten DNS-Dienst verfügen, zum Beispiel auf Ihrem Internet-Router, können Sie diesen als Weiterleitungsziel angeben, oder Sie nutzen nur die Stammserver (des Internets).
11. Schließen Sie den Vorgang ab.

Virtuell oder Hardware?

Diese Frage quält die IT-Experten seit Anbeginn der x86-/x64-Virtualisierung in den Rechenzentren. Natürlich können Sie alle Ihre DNS-Server auch rein virtuell betreiben. Sofern Sie sich Cloud-Systeme bei Microsoft oder Amazon zulegen werden, die Ihnen keine Hardware-Maschine zur Verfügung stellen, um Ihren DC oder DNS darauf zu installieren, geht es gar nicht anders. Sie müssen lediglich sicherstellen, dass Ihr DNS-Server selbst beim Ausfall vieler anderer Systeme noch zur Verfügung steht. Sie sollten also die Abhängigkeit gering halten – insbesondere was das Storage- und Netzwerksystem angeht.

Grundsätzlich haben Sie nun einen DNS-Dienst aktiv. Noch werden Sie keine Veränderung bemerken, da noch kein DNS-Client seine Anfrage an diesen Server richtet. Der Einfachheit halber passen wir den DNS-Eintrag des Servers selbst an, indem wir die Adapteroption ändern.

1. Drücken Sie die linke Windowstaste und geben Sie über die Tastatur Ethernet ein, wählen Sie ETHERNET-EINSTELLUNGEN.
2. Wählen Sie ADAPTEROPTIONEN ÄNDERN.
3. Wählen Sie Ihre aktive Netzwerkkarte per Doppelklick aus.
4. Klicken Sie auf EIGENSCHAFTEN.
5. Wählen Sie INTERNETPROTOKOLL, VERSION 4 (TCP/IPv4).
6. Klicken Sie auf EIGENSCHAFTEN.
7. Wählen Sie im unteren Bereich FOLGENDE DNS-SERVERADRESSEN VERWENDEN: und tragen Sie unter BEVORZUGTER DNS-SERVER 127.0.0.1 ein.
Sie brauchen keinen alternativen DNS-Server-Eintrag.
8. Bestätigen Sie die Anpassung mit OK.

Nun ist Ihr Server so eingestellt, dass er Anfragen zur Namensauflösung an sich selbst, also den eigenen DNS-Server richtet. Unbekannte Namen, das sind zum gegenwärtigen Zeitpunkt alle, leitet der Server entweder an den vorgelagerten DNS-Server weiter oder fragt diese über die DNS-Stammlinie ab.



DNS-Stammlinie verweisen auf die Root-Server. Zum

Zeitpunkt der Manuskripterstellung gibt es weltweit 13 dieser Root-Server, wobei 10 in den USA positioniert sind.

Öffnen Sie nun einmal die Eingabeaufforderung und geben Sie

```
nslookup google.de
```

ein. Es erscheint die Ausgabe einer nicht autorisierenden Antwort mit der IP-Adresse der Suchmaschine. Im oberen Bereich ist unter Server localhost und als Adresse 127.0.0.1 zu sehen. Ihr eigener Server hat die Antwort gegeben.

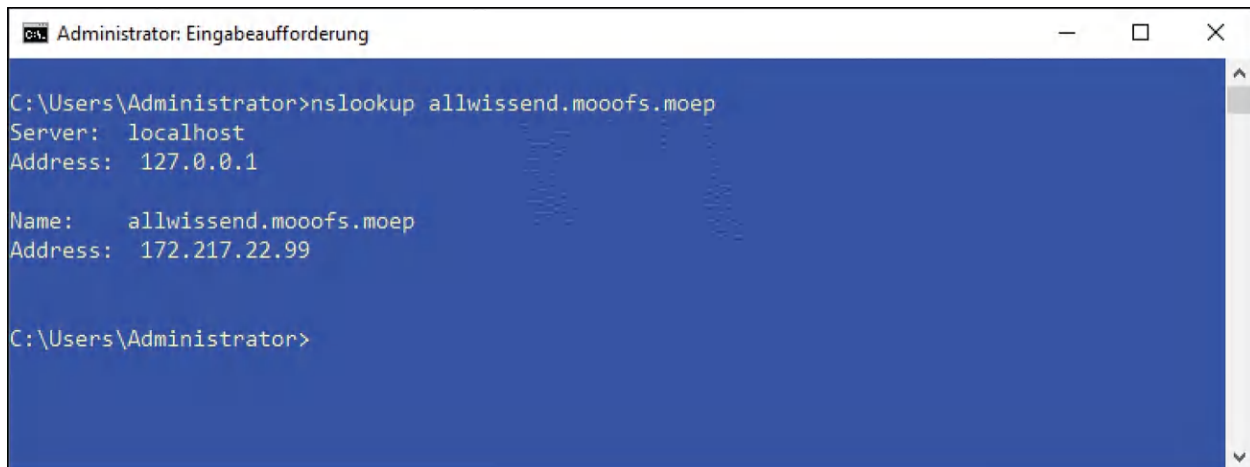
Sofern Sie einen weiteren Client-Computer in Ihrem Netzwerk haben, können Sie nun auch auf diesem Computer als DNS-Server die IP-Adresse Ihres Windows-Servers eintragen. Nur natürlich nicht mit der localhost-Adresse 127.0.0.1, sondern der »echten IP-Adresse« des DNS-Servers.

Alles, was dieser Server nun auflöst, hat er von anderer Stelle erfahren – er selbst ist zwar Träger der Fantasie-Zone »moofs.moep«, für die gibt es aber zum gegenwärtigen Zeitpunkt keinen einzigen Hosteintrag.

Das Anlegen eines Eintrags ist schnell erledigt:

1. Öffnen Sie den DNS-Manager.
2. Klicken Sie auf FORWARD-LOOKUPZONE.
3. Klicken Sie mit einem Rechtsklick auf die gewünschte Zone.
4. Wählen Sie NEUER HOST (A ODER AAAA).
5. Geben Sie allwissend ein, verwenden Sie als IP-Adresse die zuvor ermittelte IP-Adresse von Google (zum Beispiel 172.217.22.99).

Lösen Sie nun den Namen auf – und er verweist auf die IP-Adresse von Google (siehe [Abbildung 8.4](#)).



```
C:\Users\Administrator>nslookup allwissend.moofs.moep
Server: localhost
Address: 127.0.0.1

Name:    allwissend.moofs.moep
Address: 172.217.22.99

C:\Users\Administrator>
```

Abbildung 8.4: Ob Fantasiename oder echter Name – die Namensauflösung funktioniert.

Wenn Sie den kompletten Vorgang in diesem Kapitel verfolgt haben, sollten Sie bereits über eine angepasste `hosts`-Datei auf Ihrem Server verfügen. Wir hatten darin den Hostnamen telekom.de auf die IP-Adresse von Wikipedia festgelegt.

Ein Ping auf dem Server wird auf die IP-Adresse aus der `hosts`-Datei gelenkt, der Befehl `nslookup` wiederum verweist auf die Weiterleitung oder die Stammhinweise und somit auf die tatsächliche IP-Adresse der Firma.

Abschließend sei noch auf die weiteren Funktionen aus dem Fenster DNS-MANAGER kurz hingewiesen:

- ✓ Reverse-Lookupzonen sind das Spiegelbild der Namensauflösung und liefern zu einer IP-Adresse den passenden Domänen- beziehungsweise Hostnamen, der sich über einen sogenannten Pointer-Eintrag (PTR) ergibt. In vielen Umgebungen wird bei der Anlage eines DNS-Eintrags, dem sogenannten A-Eintrag in IPv4-Umgebungen, automatisch eine Verknüpfung mit einem PTR-Eintrag vorgenommen. Das Optionshäkchen ist in der Standardeinstellung von Windows stets gesetzt.
- ✓ Bedingte Weiterleitungen steuern für bestimmte Namen bei Übereinstimmung die Weiterleitung an einen zusätzlich konfigurierten DNS-Server.
- ✓ Weiterleitungen legen fest, welche DNS-Server abzufragen sind,

sobald der eigene DNS-Server die Abfrage nicht auflösen kann, typischerweise handelt es sich um die IP-Adresse des Internet-Gateways.

- ✓ Stammhinweise verweisen auf sogenannte Root-Server, die für die eigenen Zonen Namensauflösungen durchführen, sofern die DNS-Server aus der Weiterleitung kein Ergebnis lieferten.

DNS-Konfiguration

Der Administrator findet in den Registerkarten des Eigenschaftenfensters des DNS-Servers einige äußerst hilfreiche Einstellungen und Funktionen, die wir uns an dieser Stelle einmal genauer anschauen wollen. Wie bereits erwähnt: Dem Thema Namensauflösung widmen wir in unserem Buch unsere besondere Aufmerksamkeit.

- ✓ Ein Rechtsklick auf DNS in der Baumstruktur des DNS-Managers bietet dem Administrator die Möglichkeit, sich von dieser Stelle aus mit einem weiteren DNS-Server zu verbinden.
- ✓ Ein Rechtsklick auf den Server-Namen in der Baumstruktur des DNS-Managers erlaubt die Anlage einer neuen Zone, die Konfiguration des DNS-Servers, die Festlegung der Alterungseinstellungen für alle Zonen, das Löschen des Cache, den direkten Aufruf von nslookup und den Aufruf der Eigenschaften.
- ✓ Ein Rechtsklick auf den Zonennamen unter FORWARD-LOOKUPZONEN erlaubt die Eingabe neuer Host-, Alias-, MX-Domänen- oder Delegationseinträge, ferner die Konfiguration von DNSSEC und den Aufruf der Eigenschaften.

Der Eigenschaftendialog für den DNS-Server bietet sieben einzelne Registerkarten:

- ✓ **SCHNITTSTELLEN** – Hier legt der Administrator fest, auf welchen IP-Adressen der DNS-Server überhaupt reagiert. In Umgebungen, in denen IPv6 nicht zum Einsatz kommt (noch die breite Masse), könnte der Systemverantwortliche aus Gründen der Übersichtlichkeit bei

Bedarf IPv6-Adressen für das »Abhören« der DNS-Anfragen ausklammern. Wir raten jedoch davon ab, die »lokalen fe80:«-IPv6-Adressen auszuschließen. Wichtiger ist es, externe IPv4-Adressen von DNS-Anfragen fernzuhalten.

- ✓ **WEITERLEITUNGEN** – Die allgemeine Weiterleitung an dieser Stelle ist so etwas wie ein Standardgateway für DNS-Anfragen. Hier kommen üblicherweise die IP-Adressen von vorgelagerten DNS-Servern zum Einsatz (DNS-Server des Internetproviders zum Beispiel). Sofern keine Weiterleitung verfügbar ist, nutzt der DNS-Server die Stammhinweise der Internet-Root-Server, sofern das entsprechende Optionshäkchen gesetzt ist. Besondere Beachtung gilt dem unteren Hinweis in dem Fenster: Existieren bedingte Weiterleitungen für bestimmte Domänen, so haben diese Vorrang vor der Nutzung der Weiterleitung auf der hier festgelegten Server-Ebene.
- ✓ **ERWEITERT** – Hier findet der Systemverantwortliche einige Spezialoptionen, die für gewöhnlich unverändert bleiben sollten. Dazu passend haben die Entwickler dem Fenster eine ZURÜCKSETZEN-Schaltfläche spendiert, um Fehleinstellungen rückgängig zu machen. Zwei Optionen sind möglicherweise im Praxisumfeld sinnvoll: Die erste Option betrifft die Aktivierung des automatischen Aufräumens von veralteten Einträgen mit einem beliebigen Wert. Bei statischen DNS-Servern kann sich der Administrator dies sparen, da es keine automatischen Veränderungen gibt, die einer regelmäßigen Bereinigung bedürfen.

Die zweite, spannendere Option ermöglicht das Deaktivieren von Round-Robin-(Rundlauf-)Verfahren. Weist ein Administrator einem DNS-Hostnamen mehrere IP-Adressen zu, wechselt der DNS-Server bei jeder Anfrage automatisch und periodisch die zurückgegebene IP-Adresse. Somit besteht grundsätzlich die Möglichkeit, die tatsächlich angesprochenen Server auszutauschen, was zu einer zufälligen Lastenverteilung und einer erhöhten Ausfallsicherheit führt. Über das Optionsfeld in dieser Registerkarte kann der Administrator die wechselnde Rückmeldung der IP-Adresse auf dem DNS-Server unterbinden.



Wer sich für das Round-Robin-Verfahren und den Vergleich mit einem Network Load Balancer unter Windows interessiert, dem sei die Webseite von Frank Carius (MVP und Dipl.-Ing. (BA) für technische Information) ans Herz gelegt, zu erreichen unter <https://www.msxfaq.de/cluster/dnsroundrobin.htm>.

- ✓ STAMMHINWEISE – Zeigt die IP-Adresse(n) der Internet-Root-Server an und erlaubt deren Bearbeitung.
- ✓ DEBUGPROTOKOLLIERUNG – Normalerweise legt ein DNS-Server in der Ereignisanzeige lediglich dann Einträge an, wenn eine neue Zone angelegt wurde oder Hostnamen eingefügt oder gelöscht werden. Praktischerweise dokumentiert das Eventlog den exakten Zeitstempel und hält fest, welcher der administrativen Benutzer für die Anpassung verantwortlich ist. Die Einträge in der Ereignisanzeige eignen sich für die laufende Dokumentation der DNS-Anpassungen, ohne jedoch alle Details, wie Eigenschaftenänderungen, mitzuschreiben.

Für die Fehlersuche – beispielsweise, wenn eine Zonenübertragung nicht funktioniert oder Client-Computer keine Namensauflösung durchführen können – ist die Debugprotokollierung ein perfektes Hilfsmittel. Die Anzahl von Optionen dürften so ziemlich jedes Einsatzfeld abdecken (siehe [Abbildung 8.5](#)), und im Bedarfsfall kann der Administrator die Pakete auch für bestimmte IP-Adressen filtern. Die DNS-Protokolldatei arbeitet über 16 Felder, die in der Textdatei selbst noch einmal erläutert sind. Praktischerweise gibt es einen definierbaren Maximalwert für die Protokolldatei, somit besteht grundsätzlich die Möglichkeit, das aktuelle Geschehen rund um den DNS-Server festzuhalten.

- ✓ EREIGNISPROTOKOLLIERUNG – Legt über vier Optionen die Protokollierungstiefe in der Ereignisanzeige unter Windows-Protokolle, Anwendungs- und Dienstprotokolle, Microsoft, Windows, DNS-Server und hier das Protokoll »Überwachung« fest. Neben der Dokumentation aller Ereignisse stehen zur Auswahl KEINE

EREIGNISSE, NUR FEHLER und FEHLER UND WARNUNGEN. Nicht alle Konfigurationsänderungen erzeugen einen Eintrag in der Ereignisanzeige. Die Aktivierung der Debugprotokollierung oder die Änderung der dortigen Pfadangabe finden sich beispielsweise nicht im Eventlog wieder ([Abbildung 8.5](#)).



Eine Liste aller DNS-Server-Ereignis-IDs finden Sie in einem älteren Microsoft-Docs-Beitrag unter [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn800669\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn800669(v=ws.11)).

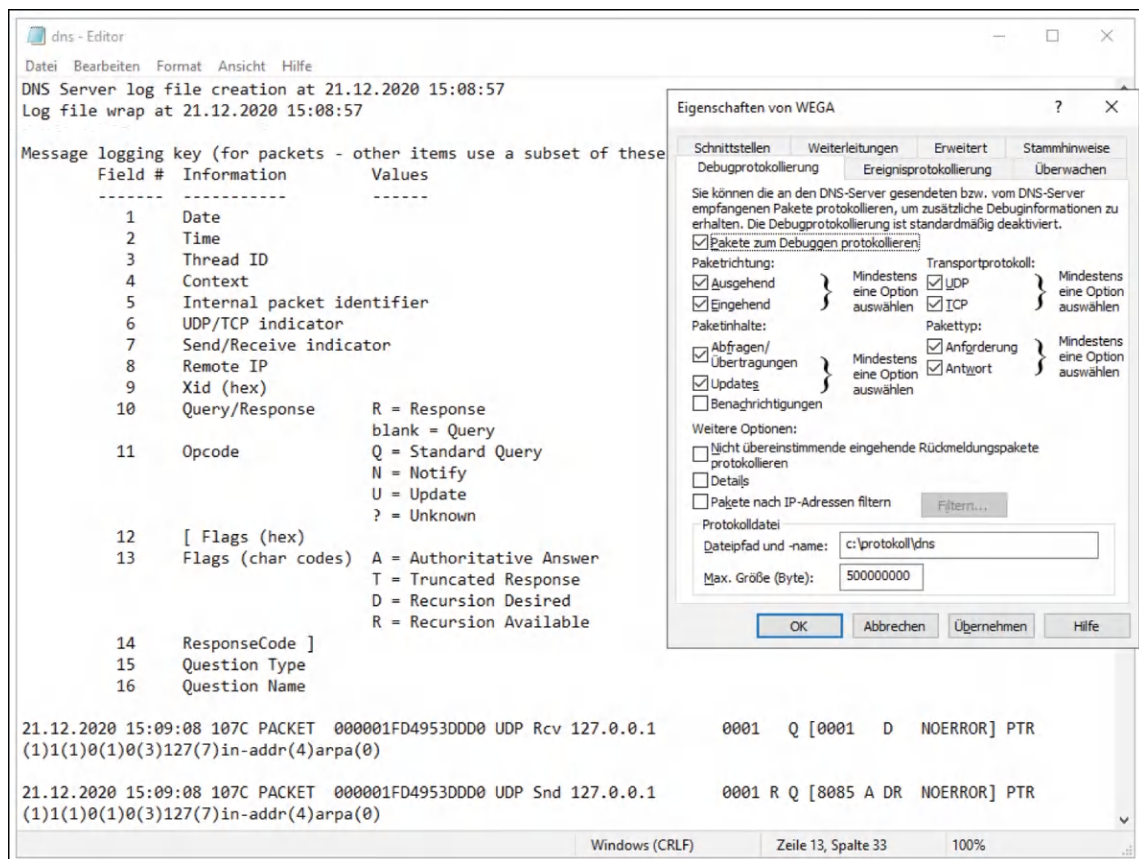


Abbildung 8.5: Die Debugprotokollierung hilft bei der Fehlersuche.

- ✓ **ÜBERWACHEN** – Windows-Server verfügen über integrierte Funktionen zur Überwachung von DNS-Servern. Zur Auswahl stehen die einfache Abfrage auf diesem DNS-Server sowie die rekursive Abfrage auf andere DNS-Server. Der Administrator kann durch einen

Mausklick auf JETZT TESTEN sofort eine Prüfung durchführen oder einen automatischen Test in einem beliebigen Sekunden- oder Stundenintervall anstoßen. Das Dialogfenster haben die Entwickler von Microsoft etwas eigenwillig umgesetzt: Intervallgesteuerte Tests schreibt die Software nur in die oberste Zeile der kleinen Tabelle. Alle Testergebnisse unterhalb der ersten Zeile sind stets manuelle Prüfungen.

DNS-Stamminweise wiederherstellen

Selten, aber doch – meist infolge von Unachtsamkeit – kommt es vor, dass die Stamminweise auf einem DNS-Server verloren gehen. Öffnet der Administrator die Registerkarte STAMMHINWEISE im Eigenschaftendialog zum Server im DNS-Manager und herrscht dort gähnende Leere, ist das kein Grund, in Panik zu geraten.

Während auf den früheren Versionen von Windows Server nun fleißige Tipparbeit angesagt war, ist dieser Fehler jetzt mit einem einzelnen Mausklick zu reparieren. Wählen Sie hierzu die Schaltfläche unten rechts mit der Beschriftung VOM SERVER KOPIEREN und geben Sie als IP-Adresse den öffentlichen Google-DNS-Server 8.8.8.8 ein und bestätigen Sie die Eingabe. Nach einer weiteren Bestätigung durch die Schaltfläche ÜBERNEHMEN sind die erforderlichen Einträge wieder vorhanden.

Dass einige Root-Server mit der IP-Adresse »Unbekannt« aufgelistet sind, stellt kein funktionelles Problem dar – zu sehen in [Abbildung 8.6](#).

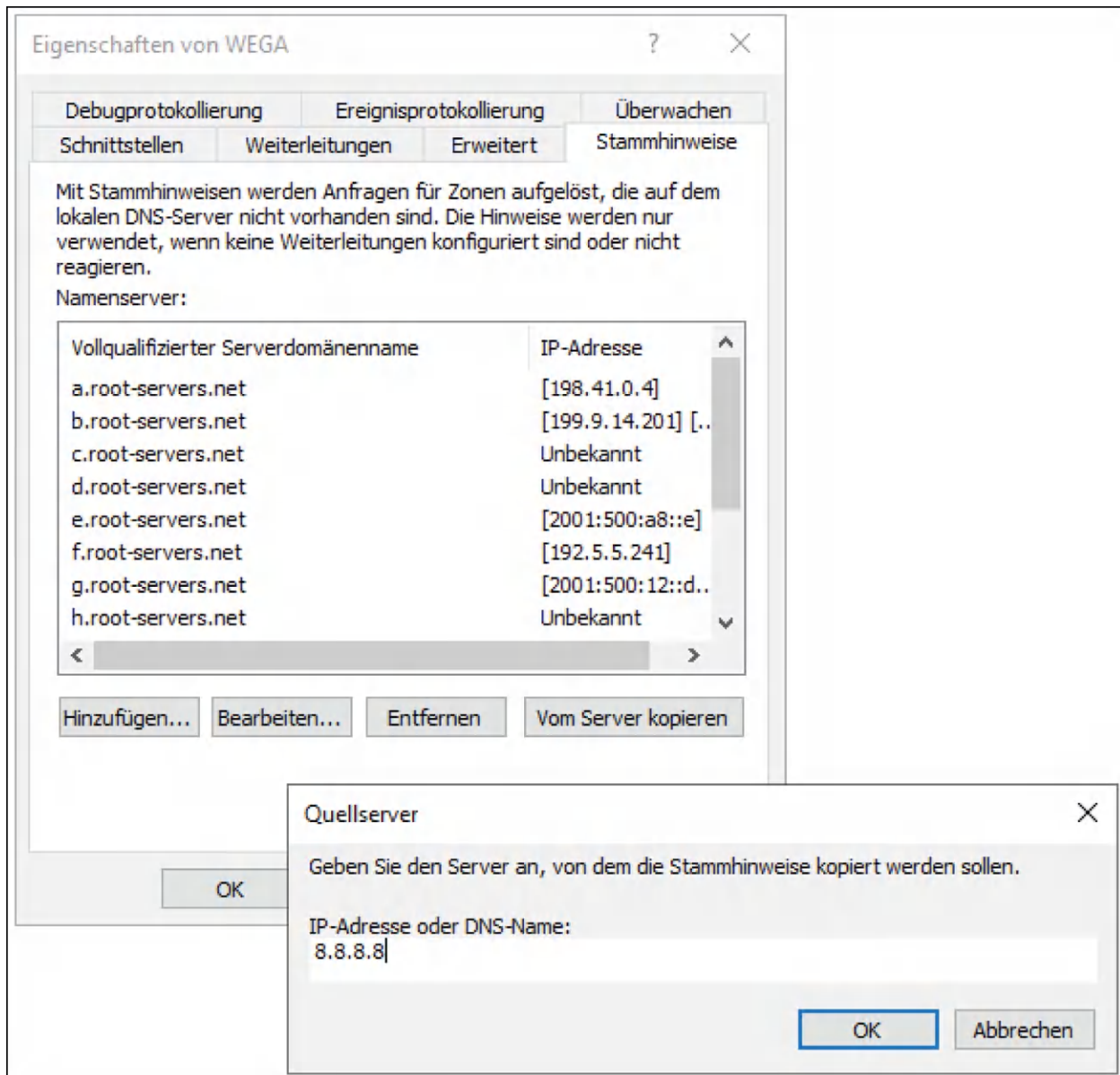


Abbildung 8.6: Die Wiederherstellung der Stammhinweise ist durch die Kopierfunktion einfach.

Verwalten von DNS-Einträgen

Das Erstellen und Bearbeiten von DNS-Einträgen ist Tagesgeschäft für Administratoren. Durch dynamische Updates im Zusammenspiel mit DHCP brauchen sich Windows-Administratoren um die typischen Server- und Client-Hostnamen-Bewegungen jedoch kaum zu kümmern.

Im Folgenden finden Sie eine Übersicht der am häufigsten benötigten Eintragstypen:

- ✓ A (IPv4-Adresse) – Zuordnung einer IPv4-Adresse zu einem Hostnamen. Verfügt ein Computer über mehrere Netzwerkkarten oder mehrere IPv4-Adressen, empfiehlt es sich, mehrere Einträge anzulegen. Ausnahmen sind Einträge in typischen Storage-Netzen, bei denen direkt die IPv4-Adresse angesprochen wird, statt eine Namensauflösung zu verwenden.
- ✓ AAAA (IPv6-Adresse) – wie IPv4-Adresse, jedoch in neuer Notation.
- ✓ CNAME (Canonical Name) – legt einen Alias für einen Hostnamen fest. Wird intensiv im Zusammenhang mit Webservern genutzt, um über eine IP-Adresse viele verschiedene Webseiten direkt anzusteuern. Zudem hilfreich, wenn technisch geprägte Hostnamen das Merken erschweren.
- ✓ MX (Mail Exchanger) – Legt einen Mailserver in der Domäne fest, der für die Weiterleitung von E-Mail-Nachrichten an die entsprechenden Mailserver in der Domäne zuständig ist.

Die A- und AAAA-Einträge ordnen einer IP-Adresse einen Hostnamen zu, der PTR-Eintrag erstellt zu Reverse-Lookup-Zwecken einen Zeiger auf den Host. Dieser Eintrag wird in der Reverse-Lookupzone angelegt, um zu einer IP-Adresse auch einen Host- beziehungsweise Domänennamen auflösen zu können.

Anlage einer Reverse-Lookupzone

Eine Forward-Zone haben wir zum Einstieg in das Kapitel bereits angelegt. Nun soll die Reverse-Lookupzone für den IPv4-Bereich 195.62.121.0 angelegt werden:

1. Öffnen Sie den DNS-Manager.
2. Klicken Sie mit der rechten Maustaste auf REVERSE-LOOKUPZONEN.
3. Wählen Sie im Kontextmenü NEUE ZONE... aus.
4. Klicken Sie auf WEITER.
5. Wählen Sie PRIMÄRE ZONE und anschließend klicken Sie auf WEITER.

6. Bestätigen Sie IPV4-REVERSE-LOOKUPZONE und klicken Sie auf WEITER.
7. Geben Sie unter Netzwerk-ID 195.62.121 ein und klicken Sie auf WEITER.
8. Bestätigen Sie die Anlage einer neuen DNS-Namensdatei mit WEITER.
9. Bestätigen Sie die Auswahl DYNAMISCHE UPDATES NICHT ZULASSEN, eine Einstellung bei der nur die vom Administrator angelegten PTR-Einträge zur Anwendung kommen. Klicken Sie auf WEITER.
10. Wählen Sie FERTIG STELLEN.

Anlage eines Hosteintrags

Wenn Sie also einen NEUEN HOST eintragen und das Häkchen für VERKNÜPFTEN PTR-EINTRAG ERSTELLEN setzen, legt der DNS-Server beide Einträge an – sofern diese Reverse-Lookupzone besteht. Wie eine solche Zone anzulegen ist, finden Sie auf der folgenden Seite.

Die Anlage eines Hosteintrags ist schnell erledigt:

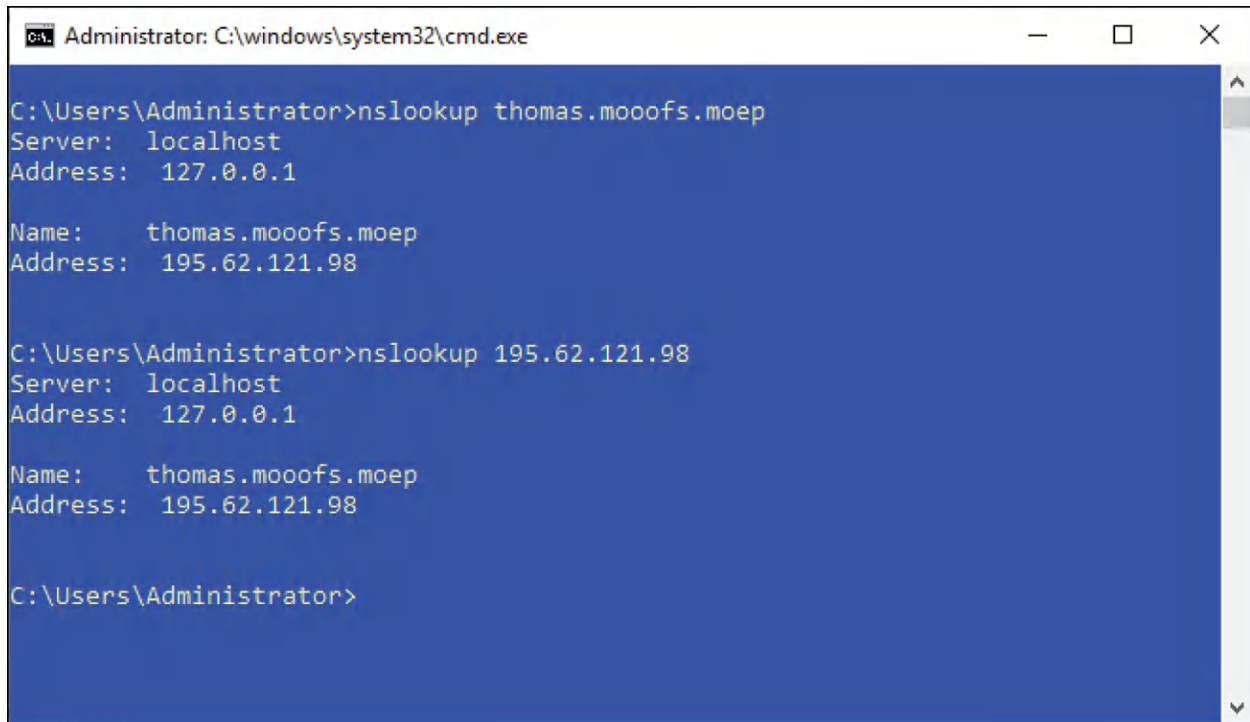
1. Öffnen Sie den DNS-Manager.
2. Wählen Sie die gewünschte Domäne unter FORWARD-LOOKUPZONEN.
3. Wählen Sie, nach einem Rechtsklick, im Kontextmenü NEUER HOST (A ODER AAAA)
4. Wählen Sie den gewünschten Namen.
5. Geben Sie die IP-Adresse ein.
6. Aktivieren Sie die Option VERKNÜPFTEN PTR-EINTRAG ERSTELLEN, sofern eine rückwärtige Auflösung von IP-Adresse zum Hostnamen möglich sein soll.



Die Option »Authentifizierte Benutzer können DNS-Einträge mit

demselben Namen aktualisieren« ist nur verfügbar, wenn der DNS-Server in einer Domäne mit Domänencontroller betrieben wird.

Sofern beide Einträge vorhanden sind, wird nslookup in beide »Richtungen« hin auflösen können, wie in [Abbildung 8.7](#) zu sehen.

A screenshot of a Windows command prompt window titled "Administrator: C:\windows\system32\cmd.exe". The window has a blue background. The text inside shows two nslookup commands and their results. The first command is "nslookup thomas.moofsf.moep", which returns "Server: localhost", "Address: 127.0.0.1", "Name: thomas.moofsf.moep", and "Address: 195.62.121.98". The second command is "nslookup 195.62.121.98", which returns "Server: localhost", "Address: 127.0.0.1", "Name: thomas.moofsf.moep", and "Address: 195.62.121.98". The prompt "C:\Users\Administrator>" is visible at the bottom.

```
Administrator: C:\windows\system32\cmd.exe

C:\Users\Administrator>nslookup thomas.moofsf.moep
Server: localhost
Address: 127.0.0.1

Name: thomas.moofsf.moep
Address: 195.62.121.98

C:\Users\Administrator>nslookup 195.62.121.98
Server: localhost
Address: 127.0.0.1

Name: thomas.moofsf.moep
Address: 195.62.121.98

C:\Users\Administrator>
```

Abbildung 8.7: Sofern A-Eintrag und PTR-Eintrag vorliegen, löst »nslookup« in beide Richtungen auf.

Wurde ursprünglich keine Reverse-Lookupzone definiert oder unterblieb die Verknüpfung mit einem PTR-Eintrag, kann der Administrator dies nachholen:

1. Öffnen Sie den DNS-Manager.
2. Wählen Sie die gewünschte Reverse-Lookupzone.
3. Wählen Sie, nach einem Rechtsklick, im Kontextmenü NEUER ZEIGER (PTR)...
4. Wählen Sie den gewünschten Hostnamen im Auswahldialog aus oder geben Sie den Hostnamen von Hand ein.

Wenn Sie manuell tätig werden, müssen Sie die IP-Adresse ebenfalls von Hand eingeben.



Die Option »Authentifizierte Benutzer können alle DNS-Einträge mit demselben Namen aktualisieren. Diese Einstellung gilt nur für DNS-Einträge für einen neuen Namen.« ist nur verfügbar, wenn der DNS-Server in einer Domäne mit Domänencontroller betrieben wird.

Funktionell unterscheidet sich die Anlage von MX-Einträgen oder CNAME-Einträgen nicht von der Eingabe von Host- oder PTR-Einträgen. Im Gegensatz zu den bisherigen Dialogfenstern hat der MX-Eintrag jedoch eine zusätzliche Parameterangabe für die Mailserverpriorität. Hierbei handelt es sich um einen Wert zwischen 0 und 65.535, mit dem die Priorität des Servers in der Domäne angegeben wird.



Der Mailserverprioritätswert wird, wie in der IT beinahe überall üblich, falsch herum eingegeben. Der Server mit dem geringsten Wert hat üblicherweise die höchste Priorität. Weisen Sie stets Prioritätswerte zu, die genügend Spielraum für künftige Anpassungen und Erweiterungen bieten – indem beispielsweise immer in Zehnerschritten gearbeitet wird.

Primärer und sekundärer DNS-Server

Die Namensauflösung per DNS ist für das Funktionieren moderner Windows-Netzwerke unerlässlich. Sofern der Administrator mehr als einen Server in seiner Umgebung zu verwalten hat, empfiehlt es sich, über ein »Doppelgespann« von DNS-Servern nachzudenken. Glücklicherweise muss sich der IT-Profi nicht gleich mit solch hochtrabenden Techniken wie einem Cluster auseinandersetzen, um sicherzustellen, dass die Namensauflösung auch dann funktioniert, wenn einer der Server mal nicht erreichbar ist.

Sicherlich ist Ihnen im IP-Dialogfeld schon aufgefallen, das Computersysteme, und das gilt nicht nur für Windows, üblicherweise die Angabe von zwei DNS-Servern erwarten. Sofern Sie sich etwas tiefer in das Dialogfenster vorwagen, wird klar, dass Sie viele DNS-Server angeben können. Die Nutzung verschiedener DNS-Server ist somit von Haus aus vorgesehen. Reagiert ein DNS-Server nicht auf die Anfrage,

verwendet der DNS-Client auf dem Computer den nächsten Server-Eintrag, um einen Namen oder PTR-Eintrag aufzulösen.



Die mehrfache Angabe von DNS-Servern auf dem Client-Computer klingt ein wenig nach primärem und sekundärem DNS-Server, wie Sie es aus den Netzwerkeinstellungen am PC kennen (siehe [Abbildung 8.8](#)). Das hat aber mit dem Betrieb eines Sekundär-DNS-Servers durch den Administrator nichts zu tun.

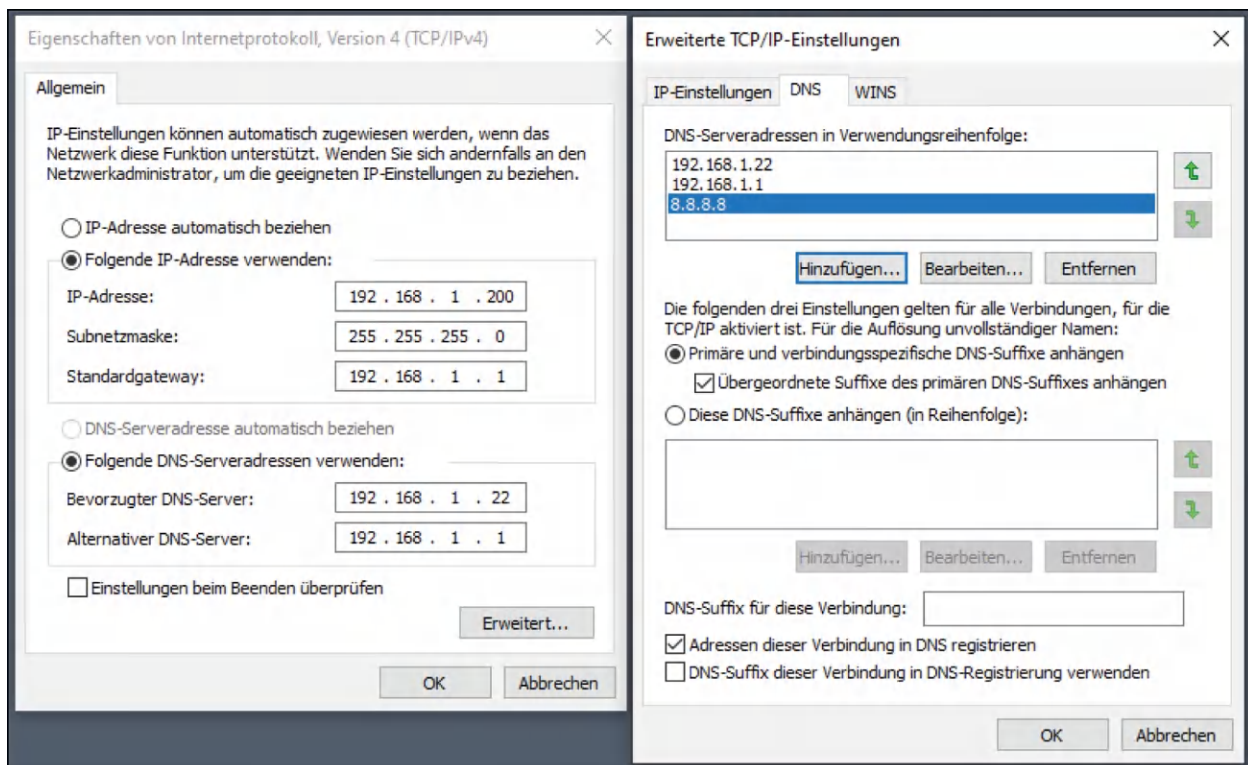


Abbildung 8.8: Computer erlauben als Client die Abfrage vieler DNS-Server.

Was sind also primäre und sekundäre DNS-Server? Bei der Einrichtung entscheidet der Administrator, ob der DNS-Server die einzurichtende Zone als eine der Zonentypen betreiben will:

- ✓ Primäre Zone – Erstellt eine Kopie einer Zone, die direkt auf diesem Server aktualisiert werden kann. Der primäre DNS-Server ist der Host der steuernden Zonendatei, die alle autoritativen Informationen für eine Domain enthält, darunter auch wichtige Informationen wie die IP-Adresse der Domain und wer für die Verwaltung der Domain

verantwortlich ist. Änderungen auf dem primären DNS überträgt dieser an die Sekundärzonenserver.

- ✓ Sekundäre Zone – Erstellt eine Kopie einer Zone, die auf einem anderen Server existiert. Mit dieser Option wird die Anzahl der Anfragen auf einen primären Server reduziert und gleichzeitig die Fehlertoleranz gewährleistet. Sekundäre Server tragen schreibgeschützte Kopien der Zonendatei, und sie beziehen ihre Informationen von einem primären Server. Die dazu erforderliche Kommunikation heißt Zonentransfer.



Jede Zone kann nur einen primären DNS-Server, jedoch eine beliebige Anzahl von sekundären DNS-Servern haben.

Spielen wir den Gedanken in einem Active Directory noch einmal durch: Sie haben beispielsweise einen Domänencontroller, der gleichzeitig der primäre DNS-Server ist. Wenn Sie nun einen zweiten DNS-Server installieren, können Sie, wenn der DC ausfällt, weiterhin Namen auflösen – das ist gut –, aber Sie haben keinen Domänencontroller mehr – das ist schlecht.

Bei Verwendung der vollständigen Active-Directory-Integration entfällt eigentlich die Notwendigkeit zur Bereitstellung von sekundären Servern. In diesem Anwendungsfall ist eher die Konfiguration mehrerer Domänencontroller zur Verwaltung der DNS-Dienste angezeigt, da sich das AD um die Replikation der DNS-Informationen auf den Servern selbst kümmert.

In kleinen und mittleren Umgebungen wird typischerweise der DNS-Eintrag des Internet-Diensteanbieters als zweiter Eintrag genutzt. In größeren Umgebungen könnte die Aufteilung auf sekundäre DNS-Server aus Sicherheitsgründen sinnvoll sein. Die Konfiguration ist nicht kompliziert:

1. Installieren Sie zunächst den DNS-Server auf dem Windows-Server.
2. Starten Sie den DNS-Manager.

3. Klicken Sie auf NEUE ZONE.
4. Wählen Sie SEKUNDÄRE ZONE.
5. Wählen Sie FORWARD-LOOKUPZONE.
6. Geben Sie den vollständigen DNS-Namen für die Zone ein, und klicken Sie auf WEITER.
7. Klicken Sie in die Liste »Masterserver«, geben Sie den Hostnamen oder die IP-Adresse des DNS-Servers ein. Der Assistent wird die Eingabe überprüfen, wie in [Abbildung 8.9](#) zu sehen.

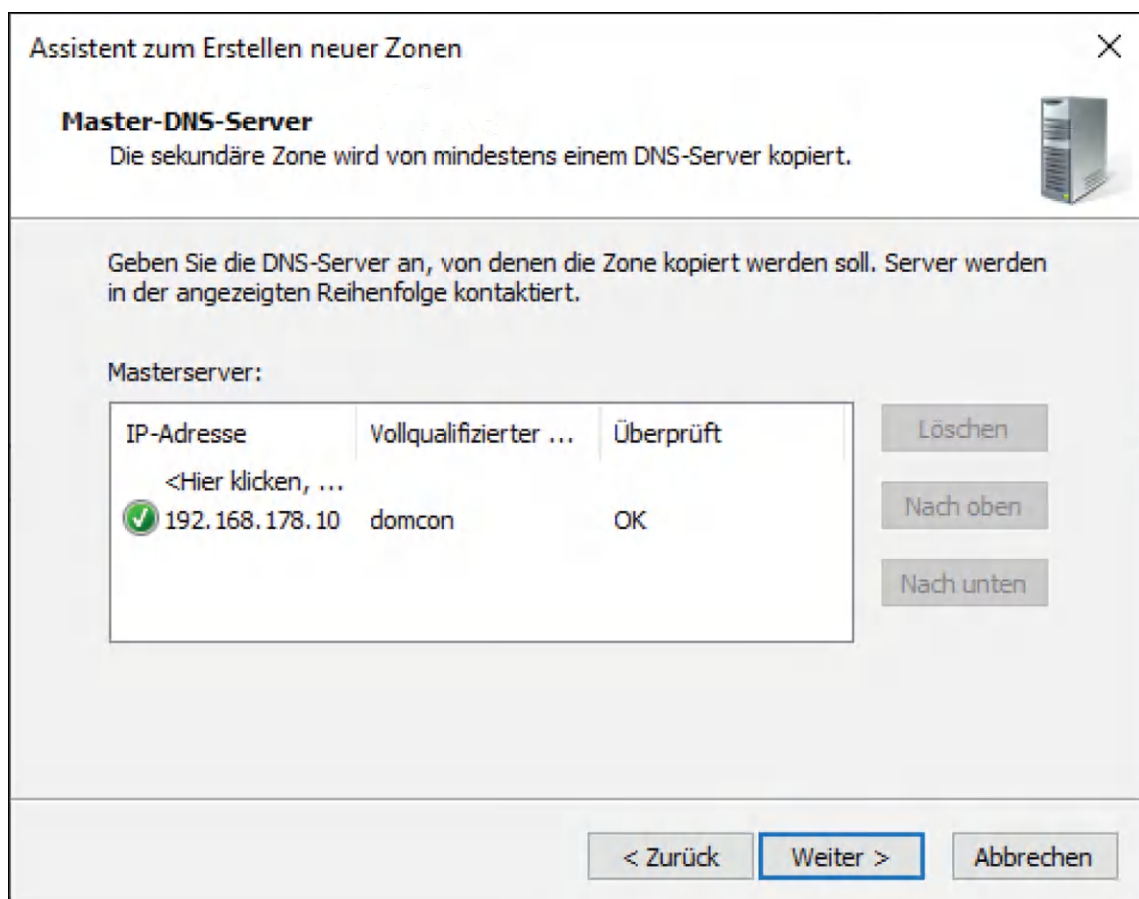


Abbildung 8.9: Die Überprüfung des Master-DNS-Servers ist für die erfolgreiche Anlage eines Sekundärservers entscheidend.

8. Klicken Sie auf WEITER und FERTIGSTELLEN. Je nach Konfiguration des primären DNS-Servers erhalten Sie nun eine Fehlermeldung, dass keine Übertragung vom Masterserver durchgeführt werden kann.

9. Wechseln Sie auf den primären DNS-Server oder binden Sie sich diesen als weiteren Server in den DNS-Manager-Dialog ein.
10. Markieren Sie die gewünschte Forward-Lookupzone und wählen Sie, nach einem Rechtsklick, im Kontextmenü den Befehl EIGENSCHAFTEN aus.
11. Wechseln Sie in die Registerkarte ZONENÜBERTRAGUNG. Aktivieren Sie die Zonenübertragung über das entsprechende Optionshäkchen und lassen Sie die Zonenübertragung an jeden Server zu oder tragen Sie den neuen Server als Nameserver ein.
Sofern es sich um ein »AD-integrierten DNS« handelt, ist der Wechsel auf den Zonentyp »Primär« ohne »Zone in Active Directory speichern« auf dem Masterserver erforderlich.

Nun können Sie den sekundären DNS-Server als Nameserver im Netzwerk bekannt geben und nutzen. Sofern Sie den zusätzlichen DNS-Server den Client-Computern über DHCP oder manuelle Einträge bekannt machen, wird dieser entsprechend bei Namensauflösungsanfragen berücksichtigt.



DNS-Anfragen sollten in der Regel nicht länger als 25 Millisekunden dauern, da ansonsten die Verarbeitungsgeschwindigkeit vieler Aktionen für den Anwender gefühlt »ewig dauern«. Auch für die kleinste Außenstelle lohnt es sich deshalb auf jeden Fall, ein System mit einem lokalen DNS-Server zu installieren und zu betreiben, und wenn es im Zweifelsfall dann auch nur ein Caching-Server auf dem lokalen Router ist.

Nur um es noch einmal in Erinnerung zu rufen: In einer Active-Directory-Struktur empfiehlt sich üblicherweise die Einrichtung mehrerer Domänencontroller. Sofern es um Sicherheitsbedenken geht – beispielsweise, da der physische Server in einer Umgebung zum Einsatz kommt, die nicht zu 100 % gegenüber Fremdzugriffen geschützt ist, ist ein RODC (Read-Only Domain Controller) eine interessante Alternative.

Wenn ein Computer ein RODC wird, repliziert er eine vollständige Kopie

aller sogenannten Anwendungsverzeichnispartitionen, die DNS benutzt. Das sind unter anderem die Domänenpartition, Forest-DNSZones und DomainDNSZones. So ist sichergestellt, dass der DNS-Server, der auf dem RODC läuft, vollständige schreibgeschützte Kopien aller DNS-Zonen zur Verfügung hat. Aus der Sicht des Administrators ist ein RODC ein vollständiger DC-/DNS-Server, ohne direkte Veränderungsmöglichkeit. Änderungen sind nur auf einem Standarddomänencontroller möglich.

Ein Windows-DNS-Server, der Zonen nicht im Active Directory speichert, legt diese unter %systemroot%\system32\dns\{Zonenname} als Textdatei ab (der Name der Datei ist im Eigenschaftendialog der Zone auf der Registerkarte DNS editierbar, sofern die Replikation nicht über das AD stattfindet). Der Aufbau der Datei ist in [Abbildung 8.10](#) zu sehen.

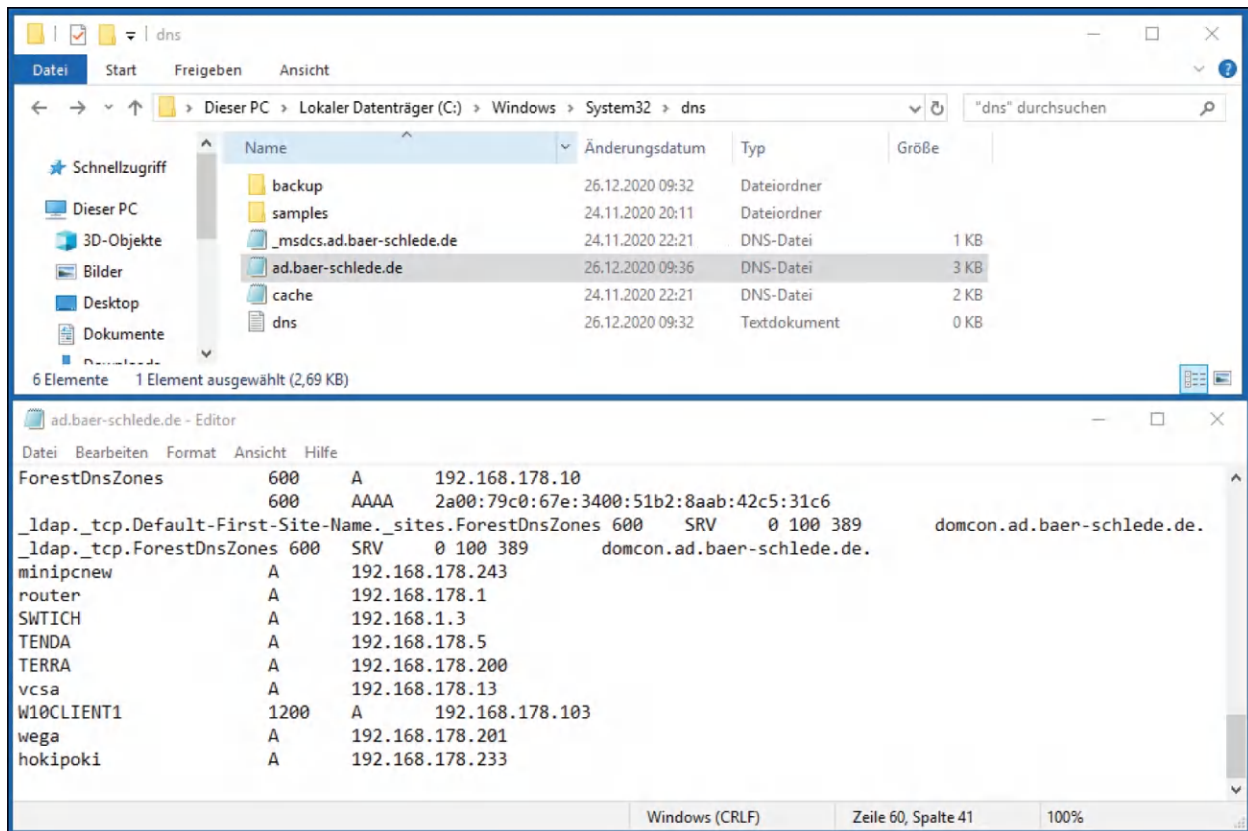


Abbildung 8.10: DNS-Server ohne AD-integrierte DNS-Zonen speichern die Dateien im Dateisystem im Windows-Verzeichnis.

Diese Textdatei enthält alle Informationen, wie die gültige Seriennummer des DNS-Eintrags oder die Angaben zu den Zeitintervallen. Sofern der

DNS-Server im Typ Active-Directory-integriert arbeitet, ist diese Datei inaktiv.

Zoneneigenschaften

Jede DNS-Zone verfügt über Eigenschaften, die der Administrator bei Bedarf anpassen kann. Mit diesen Eigenschaften werden die allgemeinen Zonenparameter unter Verwendung der sogenannten SOA-Datensätze (Start of Authority) gesetzt und Sicherheits-, Übertragungs- und Alterungseinstellungen vorgenommen.

1. Öffnen Sie den DNS-Manager.
2. Wählen Sie die gewünschte Zone unter FORWARD-LOOKUPZONEN aus.
3. Öffnen Sie das Kontextmenü durch einen Rechtsklick und wählen Sie EIGENSCHAFTEN.

In der Registerkarte ALLGEMEIN legt der Administrator die Grundeinstellungen für diese Zone fest und kann bei Bedarf die Namensauflösung der Zone anhalten oder wieder aktivieren, ohne dass die Auflösung für andere Zonen davon betroffen ist. In der Zonenkonfiguration legen Sie fest, ob es sich um eine primäre oder sekundäre Zone handelt und ob die Zone im Active Directory zu speichern ist.

Die Zonenreplikation erlaubt vier Einstellungen und setzt voraus, dass die Zone AD-integriert ist:

- ✓ alle DNS-Server, die auf DCs in der Gesamtstruktur des AD betrieben werden
- ✓ alle DNS-Server, die auf DCs in der Domäne betrieben werden
- ✓ alle DCs, die in dieser Domäne betrieben werden
- ✓ alle DCs im Bereich dieser Verzeichnispartment (sofern vorhanden)

Die Anpassungsmöglichkeiten bei den »Dynamischen Updates« sind abhängig vom Zonentyp. Ohne AD-Integration gibt es die Optionen:

- ✓ Keine dynamischen Updates
- ✓ Nicht sichere und sichere dynamische Updates

Die Option

- ✓ Nur sichere Updates

steht nur zur Verfügung, sofern der Zonentyp »Active-Directory-integriert« ist. Bei den dynamischen Updates handelt es sich um die Fähigkeit von DNS-Clients, die Registrierung und Verwaltung der eigenen Adress- und Zeigereinträge vorzunehmen. Diese Form der Aktualisierung eignet sich für Computer, die dynamisch über DHCP konfiguriert sind. Dynamische Aktualisierungen erleichtern das zügige gegenseitige Auffinden der Computer im Netzwerk.



Verwenden Sie ausschließlich »Nur sichere« dynamische Updates in Active Directory-Umgebungen. Bei sicheren Aktualisierungen können Administratoren über Zugriffssteuerungslisten festlegen, welche Computer oder Benutzer Änderungen durchführen dürfen.

Das Zusammenspiel von dynamischen DNS-Updates und DHCP ist ein überaus interessanter Prozess, der die »Anatomie« der beiden Dienste beschreibt. Aus Platzgründen verweisen wir hier auf einen älteren, aber noch immer gültigen, Support-Eintrag bei Microsoft:

<https://support.microsoft.com/de-de/help/816592/how-to-configure-dns-dynamic-updates-in-windows-server-2003>.

Einstellungen zur »Alterung« von DNS-Einträgen sind nur dann erforderlich, wenn Sie im Vorfeld dynamische Updates zuließen. In der Standardeinstellung würde der DNS-Server alle Einträge bis in alle Ewigkeit aufbewahren und weiter auch die veralteten Namen auflösen. Sofern Client-Computer sich im Netzwerk quasi selbst eintragen, kommt es irgendwann vor, dass ein alter Computer selbst dann noch als Eintrag vorhanden ist, wenn er längst entsorgt wurde.



Seien Sie bei der Aktivierung des automatischen Löschens alter

DNS-Einträge sehr umsichtig. Eine Fehlkonfiguration kann dazu führen, dass die Auflösung nicht mehr ordnungsgemäß funktioniert und Sie mehr Probleme erzeugt haben, als Alteinträge machen würden. Sofern es keinen besonderen Grund gibt: Lassen Sie es einfach aus!

Sie können veraltete Ressourcen-Einträge über zwei Intervalle (Stunden/Tage) steuern:

- ✓ Intervall für Nichtaktualisierung – Die Zeit zwischen der letzten Aktualisierung des Zeitstempels eines Eintrags und dem Zeitpunkt, zu dem der Zeitstempel wieder aktiviert werden kann.
- ✓ Aktualisierungsintervall – Die Zeit zwischen dem frühesten Zeitpunkt, zu dem der Zeitstempel eines Eintrags aktualisiert werden kann, und dem Zeitpunkt, zu dem der Eintrag aufgeräumt werden kann. Das Aktualisierungsintervall muss länger sein als der maximale Zeitraum der Eintragsaktualisierung.

Die Summe der beiden Intervalle ist letztendlich maßgeblich für den Aufräumvorgang.



Wer das Aufräumen der DNS-Namen trotz unserer warnenden Worte aktivieren möchte (oder muss), dem sei ein dazu passender Blog-Eintrag von Wolfgang Sommergut dringend ans Herz gelegt: <https://www.windowspro.de/wolfgang-sommergut/alte-dns-eintraege-automatisch-loeschen-unter-windows-server>.

Die Registerkarte AUTORITÄTENURSPRUNG (SOA) ist möglicherweise eines der Dialogfenster, dessen Name am wenigsten auf den Inhalt schließen lässt. Sie sehen das Fenster in [Abbildung 8.11](#). Es geht hier um die generelle Definition der Gültigkeit von DNS-Einträgen.

Eigenschaften von ad.baer-schlede.de ? X

WINS	Zonenübertragungen	Sicherheit
Allgemein	Autoritätsursprung (SOA)	Namensserver

Seriennummer:

Primärer Server:

Verantwortliche Person:

Aktualisierungsintervall: ▼

Wiederholungsintervall: ▼

Läuft ab nach: ▼

Minimale Gültigkeitsdauer (Standard): ▼

TTL für diesen Eintrag: (TTTTT:HH.MM.SS)

Abbildung 8.11: Administratoren verwenden dieses Dialogfenster zur Festlegung der allgemeinen Zoneneigenschaften.

- ✓ SERIENNUMMER – Version der DNS-Datenbankdatei, wird

automatisch bei jeder Änderung aktualisiert. Eine manuelle Erhöhung der Nummer ist über die Schaltfläche INKREMENT möglich. Sekundäre Server verwenden diese Nummer, um Änderungen an den DNS-Einträgen der Zone zu ermitteln.

- ✓ PRIMÄRER SERVER – FQDN des Nameservers, gefolgt von einem Punkt. Mit der Schaltfläche DURCHSUCHEN... können Administratoren den primären Server für die Zone festlegen.
- ✓ VERANTWORTLICHE PERSON – E-Mail-Adresse der zuständigen Person. Sofern der Eintrag nicht definiert wurde, wird »Hostmaster@{Domänenname}« angezeigt.
- ✓ AKTUALISIERUNGSINTERVALL – Zeitraum, innerhalb dessen sekundäre Server eine Überprüfung der Zonenaktualisierung vornehmen. Standardwert: 15 Minuten.
- ✓ WIEDERHOLUNGSINTERVALL – Schlägt die Aktualisierung fehl, gilt dieses Intervall für den nächsten Versuch. Standardwert: 10 Minuten.
- ✓ LÄUFT AB NACH – Der Gültigkeitszeitraum für Zonendaten auf dem sekundären Server. Kann der sekundäre Server während dieser Zeit keine Daten von einem primären Server herunterladen, laufen die Daten im Zwischenspeicher (Cache) ab, und der sekundäre Server stellt die Beantwortung von DNS-Anfragen ein. Standardwert: 1 Tag.
- ✓ MINIMALE GÜLTIGKEITSDAUER (STANDARD) – Minimale Gültigkeitsdauer (TTL – Time To Live) für zwischengespeicherte Einträge auf dem sekundären Server. Bei Erreichen dieses Werts läuft der zugehörige Eintrag auf dem sekundären Server ab und wird gelöscht. Die nächste Anforderung für diesen Eintrag muss der sekundäre Server an den primären Server richten. Standardwert: 1 Stunde.
- ✓ TTL FÜR DIESEN EINTRAG – Wie lange soll die Definition für den Autoritätenursprung (SOA) gelten. Sinnvollerweise entspricht dieser Wert dem Wert für die minimale Gültigkeitsdauer (Standard). Standardwert: 1 Stunde.



Wählen Sie für die beiden TTL-Einträge einen relativ hohen Wert (24 Stunden), um den erforderlichen Netzwerkverkehr zu verringern.

Batch-Export von DNS-Einträgen

In diesem Abschnitt geht es darum, dass wir die Einträge aus einem DNS-Server zu Dokumentationszwecken in eine Datei ausleiten wollen. Sofern der DNS nicht im AD integriert wäre, könnte die DNS-Datei aus %systemroot%\system32\dns\{Zonename} als Quelle für dieses Unterfangen dienen. Unglücklicherweise existiert diese auf AD-integrierten DNS-Servern nicht oder ist in einem älteren Stand.

Mithilfe des Kommandozeilenbefehls dnscmd ist diese Aufgabenstellung mit einem Einzeiler zu bewerkstelligen:

```
dnscmd {IP-DNS-Server} /ZoneExport {Zonename} {Zielfile.txt}
```

Der Befehl erstellt die Datei und legt diese im Verzeichnis %windir%\system32\dns unter dem gewünschten Namen ab. Von dort aus kann der Administrator diese in sein Dokumentationsverzeichnis überführen.

Der Befehl dnscmd erlaubt außerdem die Bearbeitung von DNS-Einträgen im Batch-Modus, somit wird

```
dnscmd domcon /Recordadd ad.baer-schlede.de moep A  
192.168.178.233
```

dazu führen, dass auf einem DNS-Server mit dem Namen domcon in der Domäne ad.baer-schlede.de ein neuer Hosteintrag A für den Namen moep angelegt wird, der auf die Adresse 192.168.178.233 verweist. Entsprechend wird

```
dnscmd domcon /RecordDelete ad.baer-schlede.de moep A /f
```

den Eintrag wieder entfernen.



Wer jetzt noch mit dnscmd arbeitet, sollte seine Jobs auf die entsprechenden PowerShell-Kommandos umstellen. Microsoft weist

bereits daraufhin, dass der Befehl in einer künftigen Version möglicherweise entfernt wird.

Wer sich gleich an die Arbeit mit der PowerShell gewöhnen möchte, verwendet in der PowerShell folgenden Befehl:

```
Export-DnsServerZone -Name "{Zonename}" -FileName "{Datei}.txt"
```

Das Kommando für den Eintrag einer IPv4-Adresse aus dem obigen Beispiel lautet in der PowerShell:

```
Add-DnsServerResourceRecordA -Name "moep" -ZoneName "ad.baer-schlede.de" -IPv4Address "192.168.178.233"
```

Und das Löschen erledigt:

```
Remove-DnsServerResourceRecord -ZoneName "ad.baer-schlede.de" -RRType "A" -Name "moep" -Force
```



Eine Liste der möglichen PowerShell-cmdlets und deren Beschreibung findet der interessierte Leser in den Microsoft Docs unter: <https://docs.microsoft.com/en-us/powershell/module/dnsserver/?view=win10-ps>.

Microsoft-DNS-Server-Historie

Microsoft als Hersteller von Windows setzte in den frühen Tagen der Computer zunächst, wie viele andere Hersteller, auf eigene Entwicklungen und positionierte einen äußerst einfachen, sehr wirkungsvollen Namensdienst: WINS (Windows Name Service). In verteilten Umgebungen ist dieser nur leider kaum nutzbar.

Während DNS Verwaltbarkeit und Steuerbarkeit anbietet, verzichtet WINS auf derlei Möglichkeiten und ist schlicht und einfach da und arbeitet. Spätestens mit der Vorstellung von Windows 2000 Server änderte das Unternehmen aus Redmond seine Strategie grundlegend.



Vergessen Sie einfach WINS – Sie werden ihn nicht mehr brauchen.

Für diejenigen Leser, die jetzt gleich tiefer bohren wollen: Suchen Sie nach LLMNR und dem SRV-Ressourceneintrag »GlobalNames« im Internet.

Die Domänen- und Verzeichnisverwaltung »Active Directory« basiert zwingend auf DNS. Der DNS-Dienst unter Windows Server ist wiederum eng in DHCP (Dynamic Host Configuration Protocol) integriert, sodass Windows-basierte DHCP-Clients und Windows-basierte DHCP-Server automatisch Hostnamen und IP-Adressen auf dem DNS-Server für die entsprechende Domäne registrieren.

Normalerweise ist DNS unter Windows Server direkt in die Active-Directory-Domänendienste integriert. In dieser Umgebung spiegeln DNS-Namespaces die Active-Directory-Gesamtstrukturen und -Domänen in einer Organisation. Netzwerkhosts und -dienste konfigurieren Administratoren mit DNS-Namen, sodass sie im Netzwerk von anderen Client-PCs und Rechnern über die DNS-Server gesucht werden können.

Damit kein falscher Eindruck entsteht: Windows-Server können auch vollkommen losgelöst von einem Active Directory als DNS-Server fungieren, aber das kann auch jeder Standard-Internet-Router. Der DNS-Serverdienst unter Windows Server unterstützt die in den RFCs für DNS festgelegten Standards und hält diese umfassend ein. Daher ist der Microsoft DNS vollständig mit jedem anderen RFC-kompatiblen DNS-Server kompatibel. In allen Client- und Serverversionen des Betriebssystems Windows ist eine DNS-Clientauflösung als Dienst fest integriert. Mit jeder neuen Windows-Version hat Microsoft einige Funktionen verbessert oder zusätzliche Features aufgenommen (siehe [Tabelle 8.1](#)).

Version	Verbesserte oder zusätzliche Funktion(en)
Windows Server 2003 Enterprise	Unterstützung für IPv6
Windows Server 2008	Mit dem Windows Server 2008 führte Microsoft die Read-Only Domain Controllers (RODCs) ein, somit waren Administratoren erstmalig in der Lage, schreibgeschützte, primäre DNS-Zonen über RODCs bereitzustellen. Das Performance-Verhalten wurde dahingehend verbessert, dass das Laden der Zonen beim Betriebssystemneustart bereits im Hintergrund begann.

Einführung von Blockierungslisten für Anfragen, um zum Beispiel prinzipiell anfällige DNS-basierte Protokolle zu blockieren; wie die Protokolle WPAD (Web Proxy Auto-Discovery Protocol) oder das ISATAP (Intra-site Automatic Tunnel Addressing Protocol), die das dynamische Update zum Registrieren eines Hostcomputers verwenden.

Windows Server 2008R2	Die größte Änderung mit Windows Server 2008 R2 und dem dazugehörigen Windows-7-Client-Betriebssystem ist jedoch die Unterstützung für DNSSEC (DNS Security Extensions). DNSSEC basiert auf diversen RFCs, die DNS dahin gehend erweitern, dass die Herkunftsautorität und Datenintegrität gewährleistet und ein authentifiziertes Dementieren der Existenz möglich ist
Windows Server 2012	Mit der Einführung von Windows Server 2012 hat Microsoft einen Installationsassistenten vorgestellt, der die Implementierung von DNSSEC vereinfacht. Zu den kleinen Veränderungen in Windows Server 2012 gehören eine bessere Schlüsselverwaltung und Onlinesignierung bei den DNS-Sicherheitserweiterungen (DNSSEC) sowie neu unterstützte DNSSEC-Standards (NSEC3 und RSA/SHA-2) mit besserer Integration in Active Directory.
Server 2012 R2	Einige neue PowerShell-Commandlets für DNS.
Windows Server 2016	Unterstützung für DANE (DNS based Authentication of Named Entities). Das Netzwerkprotokoll dient dazu, den Datenverkehr abzusichern, und stellt sicher, dass Zertifikate von TLS-Verbindungswegen nicht unbemerkt austauschbar sind. Das Konzept hinter DANE, definiert in RFC 6394 und 6698, ist an sich recht einfach: Anstelle einer CA-Instanz das Vertrauen zu schenken, prüfen Systeme gemäß DANE den sogenannten TLSA-Record bei einer DNS-Anfrage. Nur wenn dieser Eintrag zur Identität und dem Zertifikat passt, gilt die Verbindung als sicher. Zwei weitere Verfahren unterstützt der neueste DNS-Server von Microsoft: »Unknown Record« gemäß RFC 3597 und IPv6 root hints. Bei Letzterem handelt es sich um Einträge, die die IANA veröffentlicht und Windows nunmehr korrekt interpretiert und nachlädt. RFC 3597 wiederum erlaubt die Einbindung noch nicht unterstützter Record-Einträge in den DNS-Server-Zones im Name-Cache.
Windows Server 2019	Keine Änderung.

Tabelle 8.1: Windows-DNS-Server-Features

Allgemeine DNS-Sicherheit

Bevor Sie sich zur Einführung von weiterführenden Techniken wie DNSSEC unter Windows entscheiden, gilt es im Vorfeld, einige grundlegende Sicherheitskonzepte von Windows zu aktivieren. DNS ist unter Windows sehr schnell eingerichtet, und obwohl Microsoft im Allgemeinen darauf achtet, gleich zu Anfang eine sichere Konfiguration zu wählen, gibt es noch Spielraum nach oben.

In den Eigenschaften der DNS-Zone, dort in der Registerkarte

ALLGEMEIN, findet der Administrator die Optionen zu den dynamischen Updates. Wird hier der Wert »nur sichere« ausgewählt, sind nur in der Domäne authentifizierte Computer berechtigt, dynamische DNS-Updates vorzunehmen. In kleineren oder auf Sicherheit optimierten Umgebungen empfiehlt es sich, das System der dynamischen Updates komplett abzuschalten und nur auf manuelle Einträge zu setzen.

Bei der Replikation der DNS-Zonen sollte der sicherheitsbewusste Administrator festlegen, dass die DNS-Daten im Active Directory integriert zu replizieren sind. Ein regelmäßiger Blick in die Registerkarte NAMESERVER offenbart, ob veraltete Servereinträge vorhanden sind, die es zu entfernen gilt. Insgesamt empfiehlt es sich, den »Best Practices Analyzer« für Server-Manager auf Windows-Servern von Zeit zu Zeit zu verwenden, da dieser auch sicherheitsrelevante Einstellungen und Parameter prüft.



Wie wichtig die Sicherheitsaspekte bei DNS sind, zeigen die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) in ihrem IT-Grundschutzkatalog in Abschnitt 5.18.

DNS absichern mit DNSSEC und DANE

Experten warnen bereits seit vielen Jahren, dass das DNS-System nicht ausreichend gesichert ist. Die Namensauflösung wird beinahe von allen Applikationen, Betriebssystemen und IT-Strukturen genutzt. Hacker und andere Kriminelle haben daher recht leichtes Spiel, da sie sich üblicherweise darauf verlassen können, dass die DNS-Verbindungen auf den meisten Unternehmens-Firewalls ungefiltert bleiben. Lokale DNS-Server lösen netzinterne Namen auf und fungieren normalerweise als DNS-Lookup-Server. Aufgrund der großen Netzwerkdatenmenge beim DNS machen sich viele Administratoren zudem kaum die Mühe, sich innerhalb des Datenstroms einmal genauer anzuschauen, was über die

Ports 53 und 853 so alles fließt.

- ✓ DNS-Cache-Poisoning – Hierbei wird der Cache mit den Zoneninformationen von DNS-Servern manipuliert. Infolge dieser Veränderung überträgt der manipulierte Server die Zone an andere DNS-Server und sorgt dafür, dass sich falsche Zoneninformationen verbreiten. Client-Computer erhalten auf ihre DNS-Anfrage somit nicht mehr die richtigen IP-Adressen, landen möglicherweise auf falschen Webseiten oder die Mail-Kommunikation wird umgeleitet.
- ✓ DNS-Spoofing – Hierbei wird nicht die komplette Zone manipuliert, sondern nur einige wenige Einträge. Das Ergebnis ist dasselbe: Die resultierende IP-Adresse einer DNS-Anfrage ist falsch. Auch kann es durch DNS-QueryID-Spoofing gelingen, die nächste Anfragenummer einer DNS-Anfrage zu »erraten« und dem anfragenden Rechner mittels dieser Nummer eine gefälschte Antwort zukommen zu lassen.
- ✓ DNS-Tunneling – Beim sogenannten »DNS-Tunneling« umgehen Hacker die klassischen Verteidigungsmechanismen, indem sie den üblicherweise offenen DNS-Port zum Austausch von Daten verwenden. Dateien, in kleine Stückchen von ein paar Bytes zerlegt und verschlüsselt, gelangen über DNS-Anfragen und deren Antworten durch die Schutzfunktionen.

Für die hier beschriebenen Sicherheitsprobleme rund um DNS gibt es Lösungen – und die heißen DNSSEC und DANE. Der Support für DNSSEC wurde bereits mit dem Server 2008 eingeführt, und eine dynamische Ordnung der DNS-Forwarder bot bereits der Windows Server 2012R2. DANE folgte mit dem Windows Server 2016.

DNSSEC (Domain Name System Security Extensions) stellen eine ganze Reihe von Internetstandards dar, die DNS zur Gewährleistung der Authentizität und Integrität der Daten erweitern. DNSSEC stellt sicher, dass ein Ersteller auch wirklich dazu autorisiert ist, eine DNS-Zonendaten weiterzureichen. Dadurch wird DNSSEC zu einem wirksamen Mittel gegen das »Cache-Poisoning«. Die Übertragung der Ressource Records wird über digitale Signaturen gesichert. Jedoch findet eine Authentifizierung von Servern oder Clients selbst nach wie vor nicht statt.

DNSSEC sichert lediglich die Nameserver-Abfragen, was in Verbindung mit verschlüsselnden Übertragungsprotokollen wie TLS durchaus sinnvoll ist. Eine bereits bekannte Schwachstelle in diesem Konstrukt ist jedoch ein »korruptes Routing«. DNSSEC ermittelt zwar korrekterweise eine Ziel-IP-Adresse, die jedoch aufgrund des »verbogenen Routings« an einen falschen Rechner gelangen könnte. Kann sich dieser Computer durch ein kompromittiertes oder versehentlich ausgestelltes Zertifikat ausweisen, fällt dies nicht weiter auf. Um das Zusammenspiel von DNSSEC und TLS weiter zu sichern, gibt es DANE.

Das Netzwerkprotokoll DANE (DNS based Authentication of Named Entities) dient dazu, den Datenverkehr abzusichern, und stellt sicher, dass Zertifikate von TLS-Verbindungswegen nicht unbemerkt austauschbar sind. Das Konzept hinter DANE, definiert durch die IETF in RFC 6394 und 6698, ist an sich recht einfach: Statt einer CA-Instanz zu vertrauen, prüfen Systeme gemäß DANE den sogenannten TLSA-Record bei einer DNS-Anfrage. Nur wenn der Eintrag zur Identität und dem Zertifikat passt, gilt die Verbindung als sicher.

Konfiguration von DNSSEC

Um das Schutzsystem für DNS unter Microsoft Windows Server einzurichten, sind nur wenige Anpassungen in der Konfiguration erforderlich, die zumeist mit der Bestätigung der vorgegebenen Standardeinstellungen erledigt werden können. Die Inbetriebnahme ist zweigeteilt:

- ✓ Anpassung einiger Parameter auf allen beteiligten DNS-Servern
- ✓ Erstellung einer Gruppenrichtlinie für Windows-Client-Systeme

Wir starten die Aktivierung auf einem Windows-DNS-Server. Exemplarisch soll DNSSEC nun für eine neue Zone mit Namen »testzone« eingerichtet werden:

1. Starten Sie den Server-Manager.
2. Prüfen Sie, ob die Kachel »DNS« keinen Fehlerstatus aufweist. Der

Server-Manager erzeugt automatisch eine »rote Kachel«, sofern etwas nicht stimmt.

3. Starten Sie den DNS-Manager oben rechts über Tools.
4. Klicken Sie auf die Forward-Lookupzonen mit der rechten Maustaste und wählen Sie den Befehl NEUE ZONE.
5. Wählen Sie mithilfe des Assistenten eine PRIMÄRE ZONE an, OHNE DYNAMISCHE UPDATES und mit Integration ins Active Directory.
6. Wählen Sie im Kontextmenü nach einem Rechtsklick auf die gewünschte Zone im Menü DNSSEC den Befehl ZONE SIGNIEREN aus.

Daraufhin startet ein kleiner Assistent, der den Administrator durch die Konfiguration mit einigen Hilfstexten begleitet. Keine Angst vor den vielen Fachbegriffen! Auch wenn Sie sich nicht mit dem Thema Verschlüsselung auskennen, können Sie DNSSEC auf Basis der Standardeinstellungen aktivieren.

Es folgt eine mehrseitige Ausgabe der Sicherheitseinstellungen, die in diesem Rahmen vorgenommen wird. Sie können wie schon erwähnt auch die unterste Option – und damit die Standardeinstellungen – auswählen. Bei Bedarf können Sie die Parameter später noch anpassen.

- Zonensignaturparameter anpassen
- Schlüsselmaster: {Domänencontroller}
- [Schlüsselsignaturschlüssel (Key Signing Key, KSK): 1]
- Algorithmus: RSA/SHA-256
- Schlüssellänge: 2048 Bits
- Schlüsselspeicheranbieter: Microsoft Software Key Storage Provider
- DNSKEY-Signaturgültigkeit: 168 Stunden
- Replikation: Aktiviert

- Rolloverstatus: Aktiviert
- Rolloverfrequenz: 755 Tage
- Anfängliches Rolloveroffset: 0 Tage {...}

Auszugsweise sieht die Ausgabe in etwa so aus wie in [Abbildung 8.12](#).

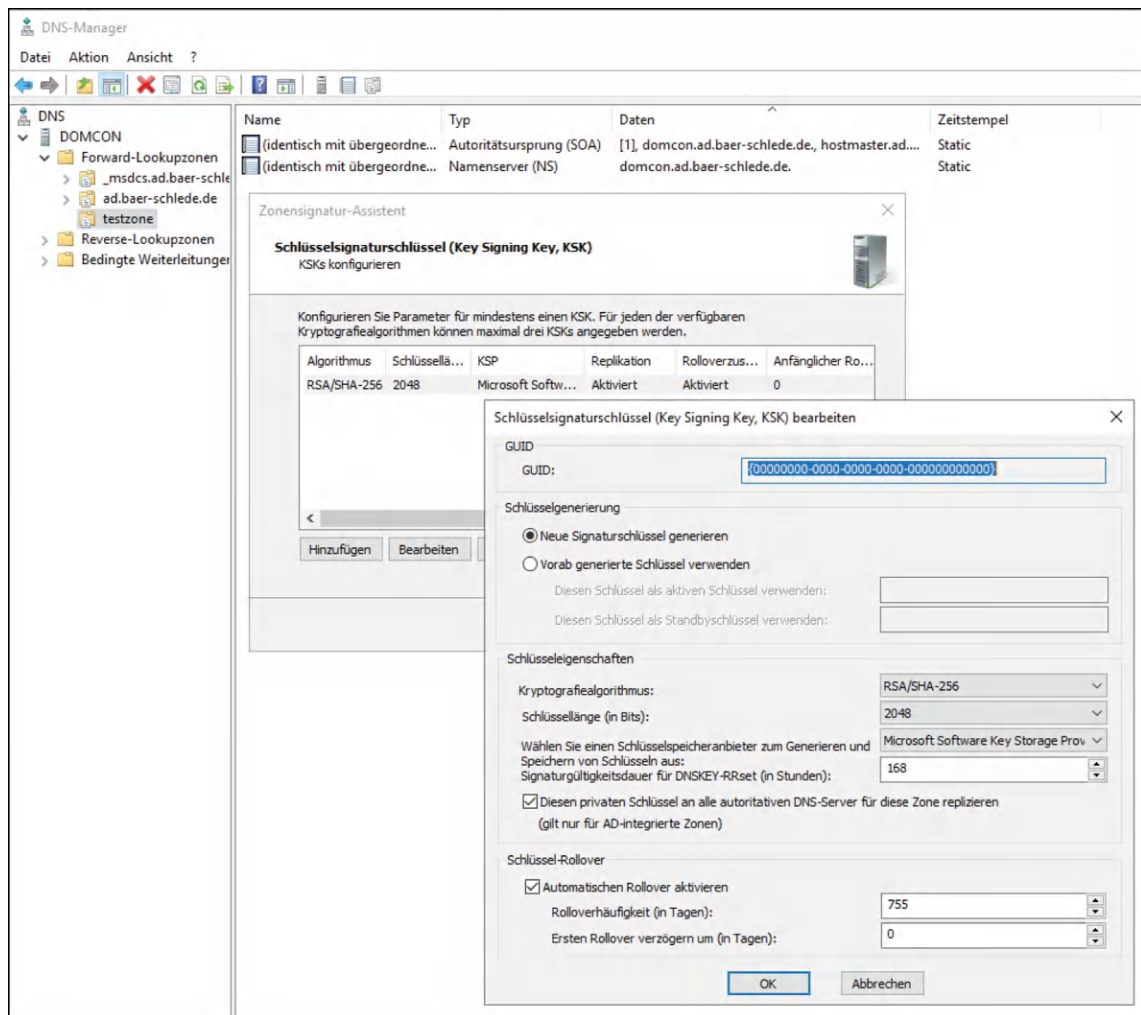
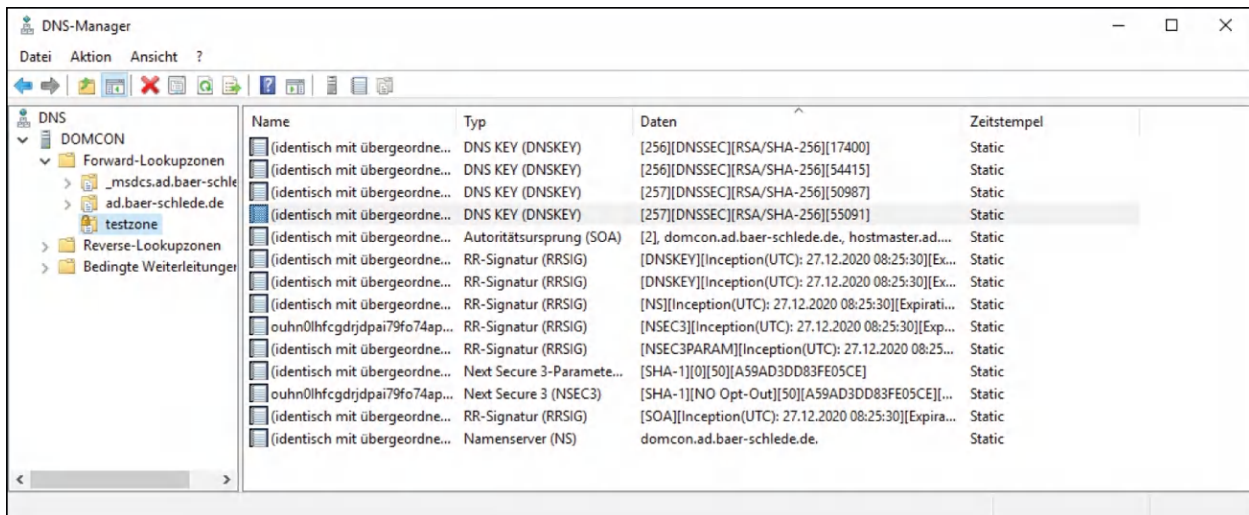


Abbildung 8.12: Die Erstellung der Schlüsselsignatur sieht komplizierter aus, als sie letztendlich ist.

- Bestätigen Sie die Einträge im Abschnitt Zonensignaturschlüssel, (ZSK) ebenfalls mit den vorgegebenen Standardwerten.
- Belassen Sie Next Secure (NSEC), sofern gefragt, bei den Standardwerten NSEC3 mit Iterationen 50 und dem zufälligen Salt-Wert von 8.

9. Wählen Sie die automatische Aktualisierung der Vertrauensanker beim Schlüssel-Rollover nach RFC 5011.
10. Bestätigen Sie Signierungs- und Abfrageparameter für SHA1 und SHA-256 mit den vorgeblendeten Werten.
 - TTL des DS-Eintrags in Sekunden 3600
 - TTL des DNSKEY-Eintrags in Sekunden 3600
 - Abrufzeitraum der sicheren Delegation 12 Stunden
 - Signaturbeginn in Stunden – 1
11. Es folgt die Zusammenfassung, die es mit WEITER zu bestätigen gilt.
12. Klicken Sie auf FERTIG STELLEN, um die Signierung der Zone durchzuführen.

Zunächst erkennt der Administrator überhaupt keinen Unterschied, was an der ausbleibenden Fensteraktualisierung von Windows liegt. Nach einem Klick auf AKTUALISIERUNG wird die Zone mit einem kleinen (kaum erkennbaren) Schlosssymbol dargestellt, siehe [Abbildung 8.13](#), und in der Zonenübersicht finden sich einige vom Assistenten angelegte Einträge.



Name	Typ	Daten	Zeitstempel
(identisch mit übergeordne...	DNS KEY (DNSKEY)	[256][DNSSEC][RSA/SHA-256][17400]	Static
(identisch mit übergeordne...	DNS KEY (DNSKEY)	[256][DNSSEC][RSA/SHA-256][54415]	Static
(identisch mit übergeordne...	DNS KEY (DNSKEY)	[257][DNSSEC][RSA/SHA-256][50987]	Static
(identisch mit übergeordne...	DNS KEY (DNSKEY)	[257][DNSSEC][RSA/SHA-256][55091]	Static
(identisch mit übergeordne...	Autoritätsursprung (SOA)	[2], domcon.ad.baer-schlede.de., hostmaster.ad....	Static
(identisch mit übergeordne...	RR-Signatur (RRSIG)	[DNSKEY][Inception(UTC): 27.12.2020 08:25:30][Ex...	Static
(identisch mit übergeordne...	RR-Signatur (RRSIG)	[DNSKEY][Inception(UTC): 27.12.2020 08:25:30][Ex...	Static
(identisch mit übergeordne...	RR-Signatur (RRSIG)	[NS][Inception(UTC): 27.12.2020 08:25:30][Expirati...	Static
(identisch mit übergeordne...	RR-Signatur (RRSIG)	[NSEC3][Inception(UTC): 27.12.2020 08:25:30][Exp...	Static
(identisch mit übergeordne...	RR-Signatur (RRSIG)	[NSEC3PARAM][Inception(UTC): 27.12.2020 08:25...	Static
(identisch mit übergeordne...	Next Secure 3-Paramete...	[SHA-1][0][50][A59AD3DD83FE05CE]	Static
(identisch mit übergeordne...	Next Secure 3 (NSEC3)	[SHA-1][NO Opt-Out][50][A59AD3DD83FE05CE][...	Static
(identisch mit übergeordne...	RR-Signatur (RRSIG)	[SOA][Inception(UTC): 27.12.2020 08:25:30][Expira...	Static
(identisch mit übergeordne...	Namensserver (NS)	domcon.ad.baer-schlede.de.	Static

Abbildung 8.13: DNSSEC erweitert die Zone um eine Vielzahl von Einträgen.

1. Legen Sie, zum Test, einen neuen Host-A-Eintrag an.
2. Wechseln Sie auf einen Client-Computer.

3. Geben Sie in der Eingabeaufforderung `nslookup {name}.{testzone}` ein. Das Ergebnis sollte sich nicht von einem x-beliebigen anderen Namensauflösungseintrag unterscheiden.

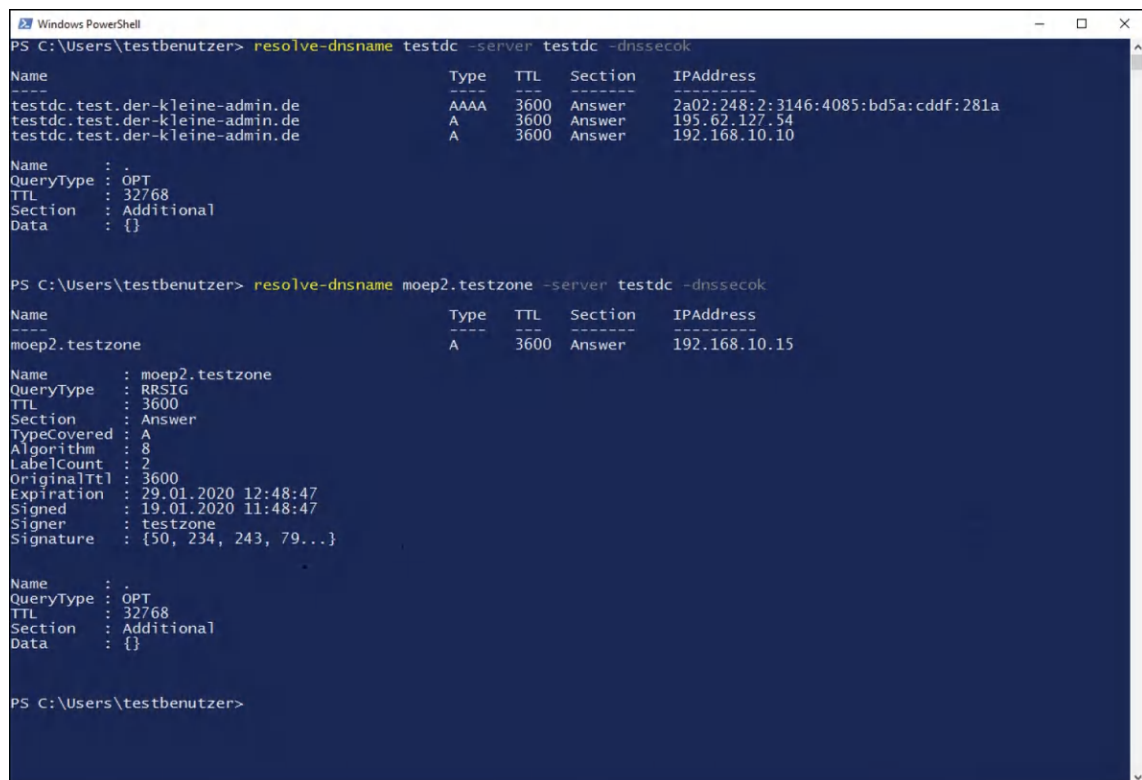
Nach dieser Anpassung ist also zunächst einmal alles unverändert – die Zone wird nach Anfragen von DNS-Clients durch den DNS-Server ganz normal beantwortet, da die Verwendung von DNSSEC zur Auflösung auf der DNS-Client-Seite noch zu aktivieren ist.

Hierzu wechselt der Administrator in die Gruppenrichtlinienverwaltung und legt ein neues Gruppenrichtlinienobjekt an:

1. Wechseln Sie in die »Gruppenrichtlinienverwaltung«.
2. Die DNSSEC-spezifischen Parameter entdecken Sie unter **COMPUTERKONFIGURATION | RICHTLINIEN | WINDOWS-EINSTELLUNGEN** im Unterpunkt **NAMENSAUFLÖSUNGSRICHTLINIE**.
3. Im Dialogfenster **NAMENSAUFLÖSUNGSRICHTLINIE** wird im Kasten **REGEL ERSTELLEN** hinter der Standardauswahl **SUFFIX** die gewünschte Zone eingetragen.
4. Wählen Sie in der Registerkarte **DNSSEC** die Option **DNSSEC IN DIESER REGEL AKTIVIEREN** aus.
5. Haken Sie in der Registerkarte **DNSSEC** nun die Option **SICHERSTELLUNG DURCH DNS-CLIENTS ERFORDERLICH, DASS NAMENS- UND ADRESSDATEN VOM DNS-SERVER ÜBERPRÜFT WURDEN** an.
6. Wählen Sie am unteren Fensterrand unterhalb des Richtlinienkastens die Schaltfläche **ERSTELLEN**.
 - Anschließend ist der Eintrag in der **RICHTLINIENTABELLE FÜR DIE NAMENSAUFLÖSUNG** (unterer Fensterbereich) sichtbar.
 - Nach der Verknüpfung der GPO (Gruppenrichtlinienobjekt) mit der ausgewählten OU (Organisationseinheit) der Computer ist die DNSSEC-gestützte Namensauflösung für die Zone auf den

DNS-Clients aktiv.

7. Um sicherzustellen, dass das Verfahren auch Anwendung findet, öffnen Sie auf einem DNS-Client die PowerShell.
8. Geben Sie `resolve-dnsname {Hostnamen in Zone} -server {DNS-Servername} -dnssecok` ein und vergleichen Sie die Ausgabe mit einem Eintrag ohne aktive DNSSEC-Einstellung, wie in [Abbildung 8.14](#) zu sehen.



```
PS C:\Users\testbenutzer> resolve-dnsname testdc -server testdc -dnssecok

Name                                     Type      TTL      Section  IPAddress
----
testdc.test-der-kleine-admin.de         AAAA      3600     Answer   2a02:248:2:3146:4085:bd5a:cddf:281a
testdc.test-der-kleine-admin.de         A         3600     Answer   195.62.127.54
testdc.test-der-kleine-admin.de         A         3600     Answer   192.168.10.10

Name      : .
QueryType : OPT
TTL       : 32768
Section   : Additional
Data      : {}

PS C:\Users\testbenutzer> resolve-dnsname moep2.testzone -server testdc -dnssecok

Name                                     Type      TTL      Section  IPAddress
----
moep2.testzone                          A         3600     Answer   192.168.10.15

Name      : moep2.testzone
QueryType : RRSIG
TTL       : 3600
Section   : Answer
TypeCovered : A
Algorithm : 8
LabelCount : 2
OriginalTtl : 3600
Expiration : 29.01.2020 12:48:47
Signed     : 19.01.2020 11:48:47
Signer     : testzone
Signature   : {50, 234, 243, 79...}

Name      : .
QueryType : OPT
TTL       : 32768
Section   : Additional
Data      : {}

PS C:\Users\testbenutzer>
```

Abbildung 8.14: Prüfung der DNSSEC-Einstellungen im Vergleich

Grundlagen von DHCP

Es gibt wahrscheinlich niemanden, der noch nicht in den Genuss der Dienstleistung des Dynamic Host Configuration Protocol (DHCP) gekommen ist. Die wichtigste Aufgabe des bereits 1993 definierten Protokolls besteht darin, einem Netzwerkinterface bei Kontakt mit dem Netzwerk eine Adresse zuzuweisen. Als zweitwichtigste Aufgabe teilt DHCP dem Client weitere entscheidende Informationen mit, beispielsweise welcher Server für ihn für die Namensauflösung zuständig

ist.

Im Zusammenhang mit DHCP fallen stets zwei Begriffe, die bekannt sein müssen:

- ✓ Lease – Der Client erhält eine IP-Adresse vom DHCP-Server nur für eine gewisse Dauer, sie ist quasi »ausgeliehen«. Wie lange die Ausleihe gültig ist, ist über die Lease-Time geregelt. Ein aktiver Client ist rechtzeitig vor Ende der Lease-Time bemüht, eine Verlängerung zu erwirken, um dieselbe IP-Adresse zu behalten.
- ✓ Scope – Der administrative Bereich einer Gruppe von IP-Adressen, für die sich ein oder mehrere Server verantwortlich zeigen. Im Scope definiert der Administrator die zu vergebenden IP-Adressen, Gateway-Einstellungen oder DNS-Server.

Im SOHO-Umfeld (SOHO = Small Office/Home Office) übernimmt die Aufgabe des DHCP-Servers traditionell das Kombinationsgerät aus Router und DSL-/Kabel-Modem – zumeist eine FritzBox oder ein Gerät aus der Speedport-Serie. Im Zusammenspiel mit dem Microsoft Active Directory gilt, dass der DHCP-Dienst typischerweise AD-integriert arbeitet, ähnlich dem DNS-Dienst unter Windows.

Werfen wir zunächst einen Blick auf die Anatomie einer DHCP-Lease-Vergabe:

- ✓ Bedingungen: Aus Sicht des DHCP-Clients muss sich der DHCP-Server im selben Netzwerksegment befinden, da DHCP auf Broadcasts (Rundrufe) basiert und Router diese Anfragen ausfiltern (Broadcast-Domäne). Befindet sich der DHCP-Server in einem anderen Netzwerksegment, so muss ein sogenannter DHCP-Relay-Agent installiert werden, der die DHCP-Anfragen an den eigentlichen Server weitergibt.
- ✓ Verlängerung: Neben der IP-Adresse erhielt der Client in der DHCPACK-Nachricht weitere Informationen:
 - Lease Time (Gültigkeitsdauer)
 - Renewal Time (T1), im Standard 50 % der Lease Time

- Rebinding Time (T2), im Standard 87,5 % der Lease Time

Nach Ablauf von T1 versucht der Client, seine Lease Time zu verlängern, und sendet einen DHCPREQUEST per Unicast an den Server, der die ursprüngliche IP-Konfiguration bereitstellte.

Üblicherweise antwortet dieser mit einem DHCPACK unter Nennung derselben IP- und Rahmeninformationen, jedoch mit einer neuen Gültigkeitsdauer.

Erhält der Client keine Antwort, beginnt dieser bei Überschreitung von T2 DHCPREQUEST-Nachrichten per Broadcast zu versenden, um eine gültige IP-Konfiguration von einem anderen DHCP-Server zu erhalten.

- ✓ Gültigkeitsdauerüberschreitung: Hat der Client über die Gültigkeitsdauer hinaus keine Verlängerung erwirkt, beispielsweise da der Computer ausgeschaltet war, muss er die Konfiguration von der entsprechenden Netzwerkkarte »lösen« und das initiale Adresszuweisungsverfahren beginnen.
- ✓ Erstmalige Adresszuweisung:
 1. Ein Client besitzt noch keine IP-Adresse und möchte diese von einem DHCP-Server zugewiesen bekommen. Der Client schickt auf dem Interface eine sogenannte DHCPDISCOVER-Nachricht als Netzwerk-Broadcast – Absender 0.0.0.0, Zieladresse 255.255.255.255, Ziel-Port UDP 67, Quell-Port UDP 68. In dieser Nachricht übermittelt der Client seine (eigentlich) eindeutige MAC-Adresse.
 2. Alle erreichbaren DHCP-Server antworten mit einer DHCPOFFER und übermitteln. In Abhängigkeit davon, ob der Client bei seiner DHCPDISCOVER-Anfrage ein sogenanntes Broadcast-Bit gesetzt hat, senden die DHCPSEVER ihre DHCPOFFER als Broadcast an die Adresse 255.255.255.255, Ziel-Port UDP 68, Quell-Port UDP 67 oder als Unicast an die vorgeschlagene IP-Adresse unter Nennung der MAC-Adresse des Clients.
 3. Der Client entscheidet sich für eines der Angebote und sendet

einen DHCPREQUEST an den gewählten Server. Diese Anfrage geschieht wiederum als Broadcast mit Absender 0.0.0.0, Zieladresse 255.255.255.255, Ziel-Port UDP 67, Quell-Port UDP 68. Alle weiteren Server werten diese Nachricht als Absage für ihr Angebot.

4. Der gewählte Server bestätigt die Anfrage mit einer DHCPACK-Nachricht und übermittelt neben der IP-Adresse einige weitere Informationen.
5. Der Client prüft die tatsächliche Verfügbarkeit der übermittelten IP-Adresse durch einen ARP-Request. Antwortet ein anderer Host im Netzwerk auf diese »Rückfrage«, weist der Client die vorgeschlagene IP-Adresse gegenüber dem Server mit einem DHCPDECLINE zurück.

APIPA

Wer schon sehr lange mit Microsoft Windows arbeitet, kennt möglicherweise noch das Verhalten, dass ein PC überhaupt keine IP-Adresse zugewiesen bekam. Seit vielen Versionen verfügt das Betriebssystem jedoch über eine Variante der Internet Protocol Automatic Configuration (IPAC) – unter Windows als Automatic Private IP Addressing (APIPA) umgesetzt.

Dieses Protokoll nutzt einen von der Internet Assigned Numbers Authority (IANA) vergebenen IP-Bereich zur automatischen Generierung von privaten IP-Adressen. Diese automatische Selbstzuweisung einer IP-Adresse soll sicherstellen, dass ein Computer mit anderen angeschlossenen Geräten über das IP-Protokoll kommunizieren kann, auch ohne dass ein DHCP-Server zur Verfügung steht.

Die IPv4-Autokonfiguration funktioniert folgendermaßen:

- ✓ Der Computer wählt eine IPv4-Adresse aus dem hierfür vorgesehenen Subnetz der Klasse B aus (169.254.0.0/16).
- ✓ Vor der Verwendung der IPv4-Adresse führt der Client selbstständig einen ARP-Test durch, um sicherzustellen, dass diese Adresse nicht

bereits von einem anderen Gerät in »Netzwerkreichweite« genutzt wird.

- ✓ Wird die IPv4-Adresse hingegen bereits verwendet, wiederholt der Computer den ersten Schritt und testet bis zu zehn Adressen, bevor eine Fehlermeldung ausgegeben wird.
- ✓ Sofern nutzbar, konfiguriert sich der Client die Netzwerkkarte unter Verwendung der gewählten IPv4-Adresse. Anschließend versucht der Client weiterhin, eine Verbindung zum DHCP-Server herzustellen, indem er alle fünf Minuten einen Broadcast ins Netzwerk ausgibt.



Unter IPv6 ist ein APIPA-Prozedere nicht erforderlich. Hier nutzen Computer die sogenannten Link-Local-Adressen, die nur innerhalb abgeschlossener Netzwerksegmente gültig sind. Ein Netzwerksegment ist ein lokales Netz, gebildet mit Switches oder Hubs, bis zum ersten Router. Reserviert ist hierfür der Bereich »fe80::/10«.



Wir werden uns im Rahmen dieses Buchs nur auf IPv4-DHCP konzentrieren. In der Praxis kommen IPv6-Szenarien im KMU-Umfeld (noch) nicht zum Einsatz. Sie sollten dennoch nicht auf die Idee kommen, Ihrem DC- oder Exchange-Server die IPv6-Kommunikation gänzlich zu unterbinden, da Sie ziemlich sicher auf Anomalien stoßen werden. Mithilfe von Firewalls gilt es, das Server-Netzwerk gegenüber unerwünschter IPv6-Kommunikation aus dem »Client/Access-Netzwerk« abzuschotten. Weitere Informationen zur Konfiguration von IPv6 unter Windows für fortgeschrittene Benutzer finden Sie in den Microsoft Docs unter:

<https://docs.microsoft.com/de-de/troubleshoot/windows-server/networking/configure-ipv6-in-windows>.

Installieren eines DHCP-Servers

Die Installation des DHCP-Servers geschieht am einfachsten über den

Server-Manager und die dortige Auswahl des Assistenten ROLLE HINZUFÜGEN.

Ein DHCP-Server sollte über statische IPv4- und IPv6-Adressen verfügen – in jedem Subnetz, für die sie zuständig sind.

1. Wählen Sie im Server-Manager im oberen Menü unter VERWALTEN den Befehl ROLLEN UND FEATURES HINZUFÜGEN.
2. Wählen Sie auf der Seite SERVER-ROLLEN den Eintrag DHCP-SERVER aus und klicken Sie zweimal auf WEITER und anschließend auf FERTIG.

Der Installationsassistent installiert und startet den Dienst.

3. Schließen Sie den Feature-Installationsdialog mit SCHLIESSEN.
4. Klicken Sie im oberen Menü auf das gelbe Ausrufezeichen neben dem Fahnsymbol und wählen Sie unter BENACHRICHTIGUNG den Link DHCP-KONFIGURATION ABSCHLIESSEN.

Nach der Installation erscheint der DHCP-Konfigurations-Assistent.

5. Klicken Sie auf WEITER.
6. Geben Sie die Anmeldeinformation zum Authentifizieren dieses DHCP-Servers in den Active-Directory-Domänendienst an.

Typischerweise handelt es sich hierbei um den Administrator-Account der Domäne.

7. Bestätigen Sie Ihre Auswahl mit COMMIT AUSFÜHREN.

Der Server ist nun im Active Directory autorisiert. Eine Automatisierung ist für den AD-Betrieb zwingend erforderlich, daher auch die erforderliche Eingabe eines administrativen Kontos, siehe [Abbildung 8.15](#).

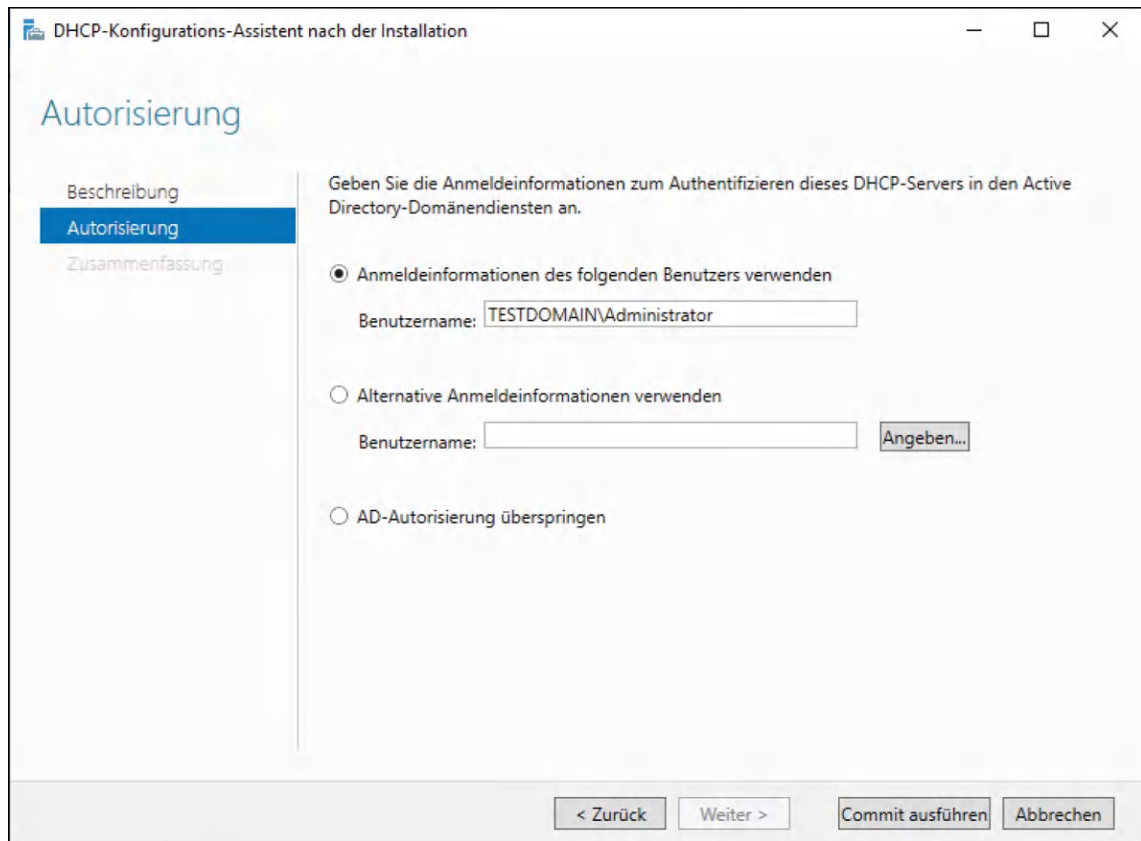


Abbildung 8.15: Ohne Autorisierung funktioniert ein DHCP-Server im AD nicht ordnungsgemäß.



Wurde die Autorisierung des DHCP-Servers nicht vorgenommen, muss sich der Administrator nicht wundern, wenn der aktivierte Bereich nicht als aktiv angezeigt wird und der Server folglich auch keine IP-Adressen verteilt. Die Autorisierung ist für DHCP-Server in einem Active Directory verpflichtend.

Im Gegensatz zu einem Router mit DHCP-Funktion bietet der Windows-Server einen autorisierten DHCP Dienst.

- ✓ Die Autorisierung ist an sich eine reine Sicherheitsmaßnahme, damit in einem Active Directory nur dafür vorgesehene Server IP-Adressen verteilen. Die Autorisierung findet normalerweise im Zuge der Installation statt oder nachträglich über einen Rechtsklick im DHCP-Dialog SERVER HINZUFÜGEN... oder AUTORISIERTE SERVER VERWALTEN.

- ✓ Die Autorisierung können Sie durch einen Rechtsklick auf den Servernamen im Dialog »DHCP« mit AUTORISIERUNG AUFHEBEN wieder beenden.

Die Einrichtung eines neuen DHCP-Bereichs führen Sie über einen Assistenten durch:

1. Wählen Sie im DHCP-Dialog den gewünschten Server aus.
2. Wählen Sie das gewünschte IP-Protokoll (v4 oder v6) aus und öffnen Sie durch einen Rechtsklick das Kontextmenü.
3. Geben Sie den Namen und eine Beschreibung ein.
4. Im nächsten Schritt gilt es, den IP-Bereich einzugeben. Bei der Berechnung der Subnetzmaske ist der Assistent behilflich, siehe [Abbildung 8.16](#).
5. Im folgenden Dialog haben Sie die Möglichkeit, Adressen auszuschließen und eine Subnetzverzögerung in Millisekunden anzugeben – hierzu später noch etwas mehr.
6. Geben Sie im nächsten Fenster des Bereichserstellungs-Assistenten die Lease-Dauer ein.
Der Standardwert von Microsoft beträgt acht Tage. In einer sich wenig ändernden Umgebung ein guter Wert.
7. Bestätigen Sie, sofern für Ihre Umgebung passend, mit WEITER.



- Bedenken Sie, dass eine Lease-Dauer von acht Tagen gleichzeitig bedeutet, dass Änderungen in der Konfiguration, beispielsweise eine angepasste DHCP-Option, erst nach acht Tagen sicher auch vom »letzten Client« verarbeitet wurden. Deshalb ist eine kürzere Lease-Dauer in einer konfigurationsintensiveren Phase möglicherweise sinnvoller.
8. Nun haben Sie die Möglichkeit, DHCP-Optionen festzulegen. Dies können Sie zwar auch zu jedem späteren Zeitpunkt machen. Es empfiehlt sich jedoch, das Standard-Gateway und den DNS-Server bereits zum jetzigen Zeitpunkt einzutragen. Bestätigen Sie die Option

JA, DIESE OPTIONEN JETZT KONFIGURIEREN mit WEITER.

9. Geben Sie die IP-Adresse des gewünschten Standard-Gateways ein.
10. Geben Sie den Domännennamen und den DNS-Server ein.

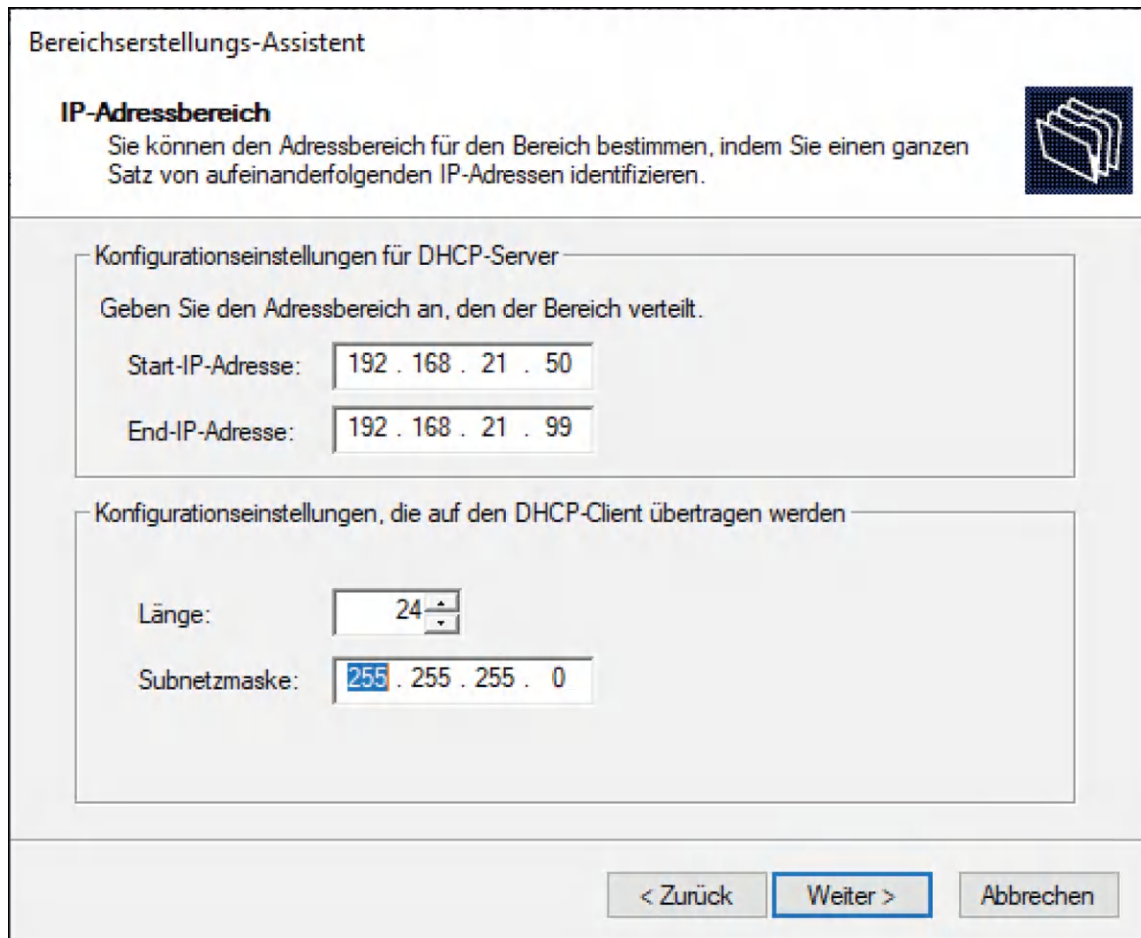


Abbildung 8.16: Die IP-Bereichsangabe im DHCP-Dialog ist dankenswert einfach.

11. Sie können die Eingabe von WINS überspringen.
12. Sie können den DHCP-Bereich nun gleich aktiv schalten oder zu einem späteren Zeitpunkt aktivieren.

DHCP-Reservierungen

Reservierungen nutzen Administratoren von DHCP-Servern, um sicherzustellen, dass Endgeräte stets dieselbe IP-Adresse bekommen.

Um es gleich vorwegzunehmen: Ob ein Administrator mit fest vergebenen IP-Adressen arbeiten will, alles dynamisch vergibt oder mit DHCP-

Reservierungen arbeitet, das bleibt ihm selbst überlassen. Es gibt hierzu keine »falsche Vorgehensweise«. Ein Fehler wäre es jedoch, sich keine Gedanken dazu zu machen.

Feste IP-Adresse funktionieren auch dann, wenn das komplette DNS-/DHCP-System nicht arbeitet. Aus diesem Grunde sind feste IP-Adresse prädestiniert für die wichtigsten Netzwerk- und Serverinfrastruktursysteme – Komponenten, die sich ohnehin nicht dynamisch anpassen ließen.

Mit DHCP-Reservierungen sorgt ein DHCP-Server dafür, dass ein Client immer wieder dieselbe IP-Adresse erhält. Innerhalb der eigenen Infrastruktur kommt dies der festen IP-Adresse schon sehr nahe, jedoch erweitert um den Vorteil, dass das Gerät in einer fremden Umgebung per DHCP eine andere Adresse bekommen würde und eine Veränderung der IP-Adresse in der eigenen Umgebung lediglich eine Anpassung der Reservierung erfordert und kein »Aufschalten« auf das Gerät durch den Administrator. Für die meisten Server-Systeme, aber auch feste Geräte wie Drucker, ist eine DHCP-Reservierung praktisch.



Niemand hindert Sie daran, auf dem Gerät selbst noch eine feste IP-Adressen manuell einzutragen – zusätzlich zur DHCP-Reservierung. Somit stehen alle Geräte gemeinsam in der DHCP-Liste.

Die dynamische Zuweisung von IP-Adressen über den DHCP-Server stellt für die Client-Computer den Normalzustand dar. Nur so sind Administratoren in der Lage, flexibel Bereiche anzupassen. Die Anlage einer Reservierung ist denkbar einfach, siehe [Abbildung 8.17](#).

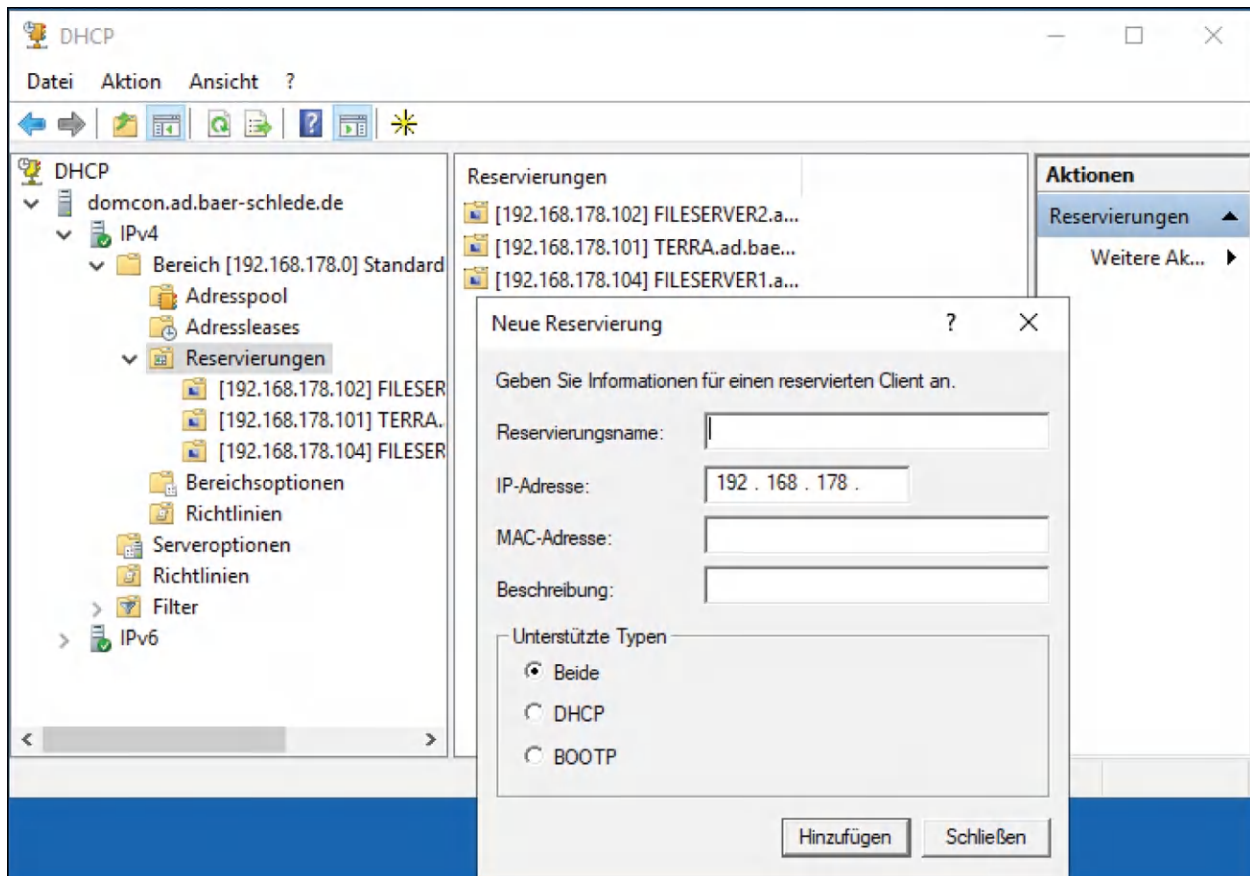


Abbildung 8.17: Denkbare einfach und schnell zu bearbeiten: die Eingabe der notwendigen Felder für eine neue Reservierung

1. Öffnen Sie den DHCP-Dialog im Server-Manager unter TOOLS oder im Startmenü unter WINDOWS-VERWALTUNGSPROGRAMME.
2. Wählen Sie im Kontextmenü, nach einem Rechtsklick auf RESERVIERUNGEN, den Befehl NEUE RESERVIERUNG.
3. Füllen Sie die erforderlichen Felder aus und klicken Sie auf HINZUFÜGEN.



Die Eingabe von MAC-Adressen ist gemeinhin eher Qual als Freude. Sie können aus einer dynamisch zugewiesenen IP-Adresse mit einem Mausklick eine Reservierung anlegen – ganz ohne manuelle Eingaben.

Wechseln Sie im DHCP-Dialog auf ADRESSLEASES, wählen Sie den gewünschten Eintrag und klicken Sie im Kontextmenü auf ZUR

RESERVIERUNG HINZUFÜGEN.

Sie können Reservierungen löschen, ohne dass der DHCP-Client sofort die IP-Adresse verliert, sofern dieser im Betrieb ist.

Wenn es nur darum geht, ein oder zwei Reservierungen anzulegen, ist die grafische Oberfläche von Windows ein passendes Hilfsmittel. Gilt es jedoch, eine größere Anzahl von Adressen zur Reservierung einzutragen – Stichwort: Masse! –, ist die PowerShell hilfreich:

Erzeugen Sie zunächst die gewünschten Einträge in einer CSV-Datei, wählen Sie folgende Spaltenbezeichnungen:

- ✓ ScopeID
- ✓ Name
- ✓ ClientID
- ✓ Option66

Sofern Sie die Liste mit einem Tabellenkalkulationsprogramm wie Microsoft Excel pflegen, speichern Sie die Liste im CSV-Format (siehe [Abbildung 8.18](#)). Üblicherweise verwendet das Programm als Trennzeichen das Semikolon.

	A	B	C	D
1	ScopeID	Name	ClientID	IPAddress
2	192.168.200.	PRINTER1	D8-AA-BB-CC-DD-01	192.168.200.11
3	192.168.200.	PRINTER2	D8-AA-BB-CC-DD-02	192.168.200.12
4	192.168.200.	PRINTER3	D8-AA-BB-CC-DD-03	192.168.200.13
5	192.168.200.	PRINTER4	D8-AA-BB-CC-DD-04	192.168.200.14
6	192.168.200.	PRINTER5	D8-AA-BB-CC-DD-05	192.168.200.15
7	192.168.200.	PRINTER6	D8-AA-BB-CC-DD-06	192.168.200.16
8	192.168.200.	PRINTER7	D8-AA-BB-CC-DD-07	192.168.200.17
9	192.168.200.	PRINTER8	D8-AA-BB-CC-DD-08	192.168.200.18
10	192.168.200.	PRINTER9	D8-AA-BB-CC-DD-09	192.168.200.19

Abbildung 8.18: Zur Bearbeitung von Reservierungslisten eignet sich ein Tabellenkalkulationsprogramm.

Verwenden Sie für den »Bulk-Import« in der PowerShell ein Kommando im Stil, wie es in [Abbildung 8.19](#) zu sehen ist:

```
Import-csv -path ".\druckerliste.csv" -delimiter ";" | Add-DhcpServerv4Reservation
```

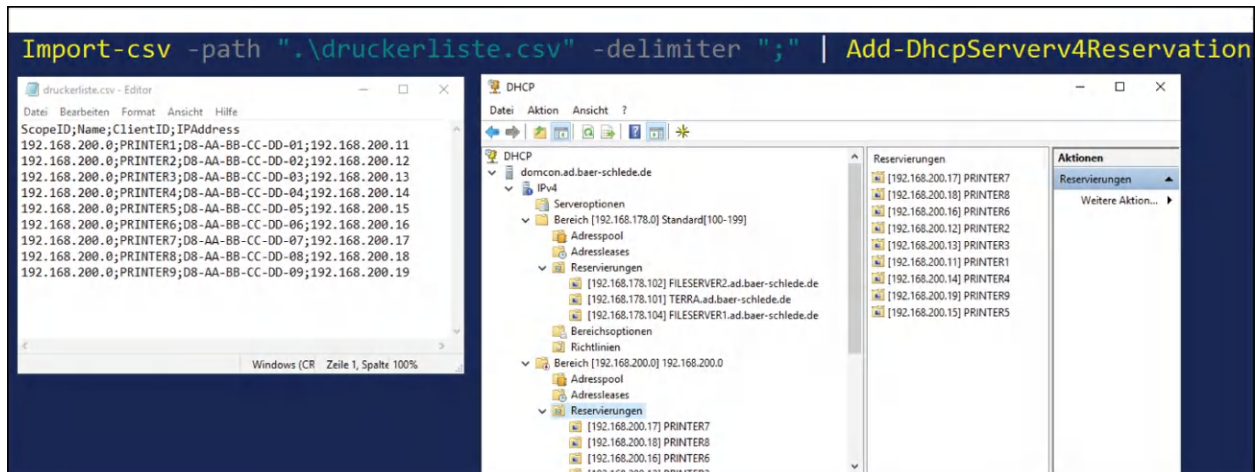


Abbildung 8.19: Der Massenimport für IP-Reservierungen ist mit der PowerShell sehr leicht zu bewerkstelligen.

Die Eintragung einer einzelnen Reservierung über die PowerShell ist ebenfalls möglich:

```
Add-DhcpServerv4Reservation -ScopeId 192.168.200.0  
-IPAddress 192.168.200.20 -ClientId "D8-AA-BB-CC-DD-10" -Name  
"PRINTER10"
```



Weitere Informationen zur Steuerung von DHCP-Servern mit der PowerShell finden Sie in den Microsoft Docs unter:
<https://docs.microsoft.com/en-us/powershell/module/dhcpserver/?view=win10-ps>.

DHCP-Optionen

Schon bei der Einrichtung des ersten IP-Bereichs mit dem Installationsassistenten gab es die Möglichkeit, Bereichsoptionen zu definieren – typischerweise die Einträge für Gateway und DNS.

Grundsätzlich wird zwischen zwei verschiedenen Optionsarten unterschieden:

- ✓ Serveroptionen – Dienen als Standardeinstellungen für alle Bereiche.
- ✓ Bereichsoptionen – Optionen für einen bestimmten Bereich (Scope). Bereichsoptionen überschreiben Serveroptionen.

Ein typisches Beispiel für eine Bereichsoption ist das Standard-Gateway, und ein klassisches Beispiel für eine Serveroption wären Zeitserver-Einträge. Zeitserver-Einträge sind in Microsoft Active Directory an sich zwar nicht erforderlich, aber für Geräte, die sich außerhalb des AD befinden, möglicherweise hilfreich.

Spätestens wenn sich Administratoren mit der Bereitstellung von Installations-Images auseinandersetzen (Stichwort PXE – Pre Execution Environment), werden zwei DHCP-Optionen besonders wichtig, die in [Abbildung 8.20](#) im Dialogfenster zu sehen sind:

- ✓ Option 066 – Hostname des Startservers
- ✓ Option 067 – Name der Startdatei

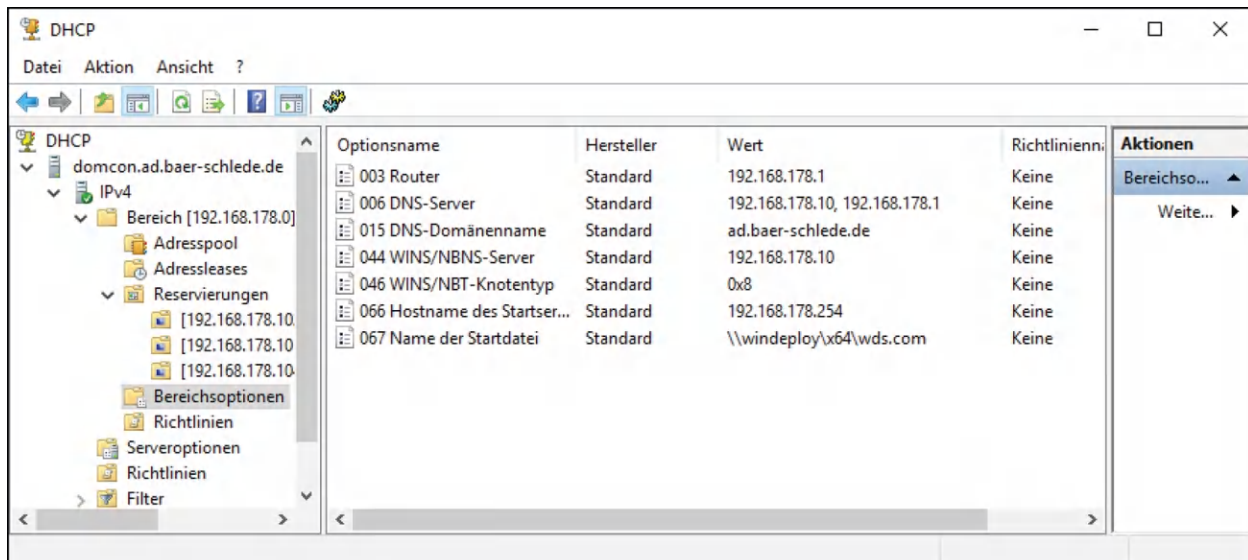


Abbildung 8.20: Über Server- und Bereichsoptionen steuern Administratoren grundlegende Einstellungen in der Netzwerkumgebung.

Eine weitere Option, die möglicherweise von Interesse sein könnte, ist der

Eintrag unter 252 mit dem Titel WPAD. Hinter WPAD verbirgt sich das »Web Proxy Autodiscovery Protocol«. Über einen Rechtsklick auf BEREICHSOPTIONEN können Sie diese ergänzen. Es handelt sich hierbei um eine schon ältere Entwicklung, die auf das Jahr 1996 zurückgeht. Die Idee dahinter ist, Client-Computern bereits bei der DHCP-Anfrage den zuständigen Proxy-Server mitzugeben.

In modernen, reinen AD-Umgebungen mag die Funktion WPAD nicht mehr interessant sein. Wer aber vor der Herausforderung steht, in verschiedenen Umgebungen unterschiedliche Proxy-Konfigurationen vorhalten zu müssen, und dies nicht per Gruppenrichtlinien umsetzen kann, sollte sich WPAD zumindest im Zusammenspiel von DNS und DHCP anschauen.



Weitere Informationen zum Thema Einrichtung von WPAD für DHCP und DNS finden Sie in einem spannenden Blog-Eintrag von Mark Heitbrink unter:
<https://www.gruppenrichtlinien.de/artikel/proxykonfiguration-wpad-als-alternative>.

DHCP-Failover

Im Zuge der Installation gab es die Möglichkeit, eine »Subnetzverzögerung in Millisekunden« anzulegen. Klären wir nun, was es mit diesem Wert auf sich hat. Normalerweise würde ein DHCP-Server auf eine Anfrage sofort reagieren. Bis in die 2010er-Jahre war das Setzen einer bewussten Verzögerung der übliche Weg, um mehrere DHCP-Server für denselben Bereich aktiv zu betreiben.



Das gleichzeitige Betreiben von DHCP-Servern mit einem geteilten Bereich für die Ausfallsicherheit durch eine Subnetzverzögerung wird auch »Split Scope« genannt.

Der DHCP-Server, bei dem eine Verzögerung die Reaktion verlangsamt, antwortet erst dann auf eine DHCP-Anfrage, wenn der eigentlich vorgesehene, primäre DHCP-Server aufgrund einer Störung zu langsam oder gar nicht antwortet.

Diese Variante der »Ausfallsicherheit« beim DHCP benötigen Administratoren seit dem Windows Server 2012 nicht mehr – hierfür steht nun die Failover-Option im DHCP-Server zur Verfügung.

Die Einrichtung des DHCP-Failover geschieht nicht über eine zusätzliche Rollen- oder Feature-Installation, sondern direkt aus dem Dialogfenster in der DHCP-Verwaltung:

1. Wählen Sie im DHCP-Dialog ein Protokoll oder einen Bereich.
2. Klicken Sie rechts, um das Kontextmenü zu öffnen.
3. Wählen Sie den Befehl FAILOVER KONFIGURIEREN...
4. Der Einrichtungsassistent startet und erwartet die Angabe des gewünschten Bereichs.
5. Wählen Sie im nächsten Dialog, zu sehen in [Abbildung 8.21](#), den Partnerserver aus. Sofern der gewünschte Server nicht in der Liste der autorisierten DHCP-Server erscheint, stellen Sie sicher, dass dieser autorisiert ist. Klicken Sie auf WEITER.

Zur Auswahl stehen zwei verschiedene Betriebsmodi:

- Lastenausgleich – Verteilung der Anfragen auf beide Maschinen nach einem prozentuellen Verteilungsschlüssel.
- Hot Standby – Variante mit einem aktiven und einem passiven Partner. Ein prozentueller Bereich des Adress-Pools wird für den inaktiven Partner vorreserviert.

INTERVALL FÜR ZUSTANDS-SWITCHOVER – Festlegung eines Zeitraums, nach dessen Verstreichen ein DHCP-Server in den Zustand »Partner Down« versetzt wird. Danach vergibt er IP-Adressen, ohne dass er versucht, den anderen Server zu kontaktieren. Diese Option ist standardmäßig nicht aktiviert, sodass man den Server manuell in diesen Status versetzen müsste.

Nach der Einrichtung des DHCP-Failover überträgt der aktive Server die Bereiche, Leases, Optionen und Reservierungen auf seinen Partner.

Welche Rolle ein DHCP-Server in einem Failover-Verbund einnimmt und wie es um den Status steht, identifiziert der Administrator über den

Eigenschaftendialog FAILOVER im Kontextmenü ([Abbildung 8.22](#)).



Das Löschen eines DHCP-Failover ist im Bereich mit dem Befehl FAILOVERKONFIGURATION AUFHEBEN von beiden Seiten aus möglich.

Der aktive DHCP verbleibt auf dem Server, auf dem die Aufhebung durchgeführt wurde.

Failover konfigurieren

Neue Failoverbeziehung erstellen



Erstellen Sie eine neue Failoverbeziehung mit dem Partner
"fileserver1.ad.baer-schlede.de".

Name der Beziehung:

Maximale Clientvorlaufzeit: Stunde Minuten

Modus:

Hot Standby-Konfiguration

Rolle des Partnerservers:

Für Standbyserver reservierte Adressen: %

☐ Intervall für Zustands-Switchover: Minuten

☒ Nachrichtenauthentifizierung aktivieren

Gemeinsamer geheimer Schlüssel:

< Zurück

Weiter >

Abbrechen

Abbildung 8.21: Konfiguration einer Failover-Beziehung als »Hot Standby«

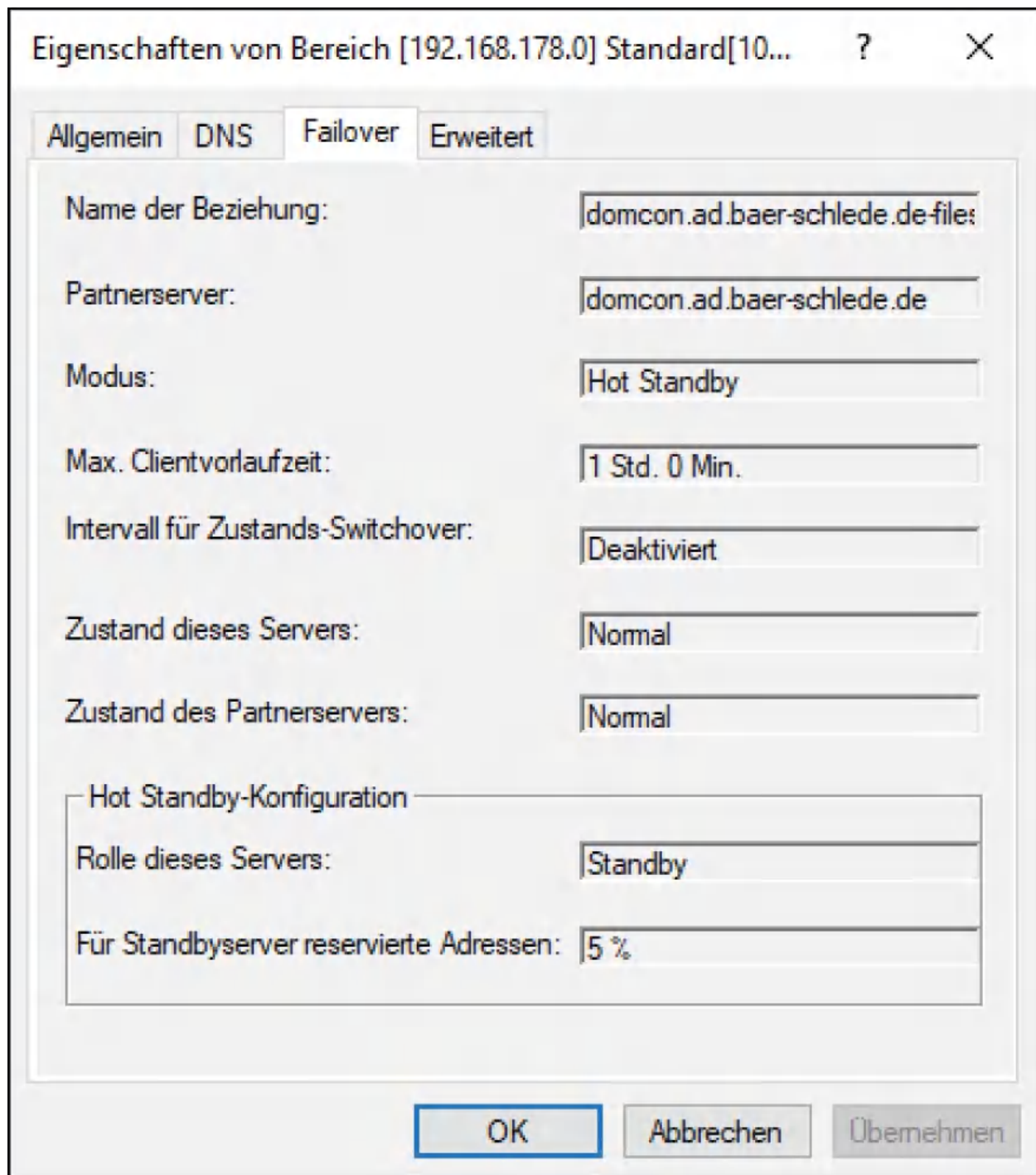


Abbildung 8.22: Welche Rolle der Server im DHCP-Failover einnimmt, gibt das Eigenschaftenfenster preis.

IPAM

Mit dem Server 2012 wurde den Windows-Administratoren ein neues

Feature zur Verfügung gestellt: der IP-Adressverwaltungsserver – kurz IPAM. Der Server dient der zentralen Verwaltung des IP-Adressraums und der damit verbundenen Dienste DNS und DHCP. Gleichzeitig bietet das Feature die automatische Erkennung eben dieser Server in der AD-Gesamtstruktur. Praktischerweise ermöglicht dies dem Administrator die Verwaltung der statischen und dynamischen IPv4- und IPv6-Adressen und soll dabei helfen, Trendentwicklungen in den Bereichen zu identifizieren.



In kleineren Umgebungen werden Sie IPAM nicht benötigen!

- ✓ IPAM unterstützt den Administrator bei der zentralen Verwaltung von DNS und DHCP.
- ✓ Die Daten speichert IPAM entweder in der internen Windows-Datenbank, oder Sie können die Informationen optional auf einem SQL-Server ablegen.
- ✓ Beim IPAM-Server muss es sich um einen Mitgliedserver handeln.
- ✓ Der IPAM-Server darf keine Domänencontroller-Dienste führen.
- ✓ IPAM ermöglicht eine klare Rechtedelegation.

Die Installation des »IP-Adressverwaltungsserver IPAM«-Features geschieht auf einem Mitgliedsserver wie gewohnt über den Server-Manager und endet mit der Zusammenfassung der zu installierenden Funktionen, zu sehen in [Abbildung 8.23](#).

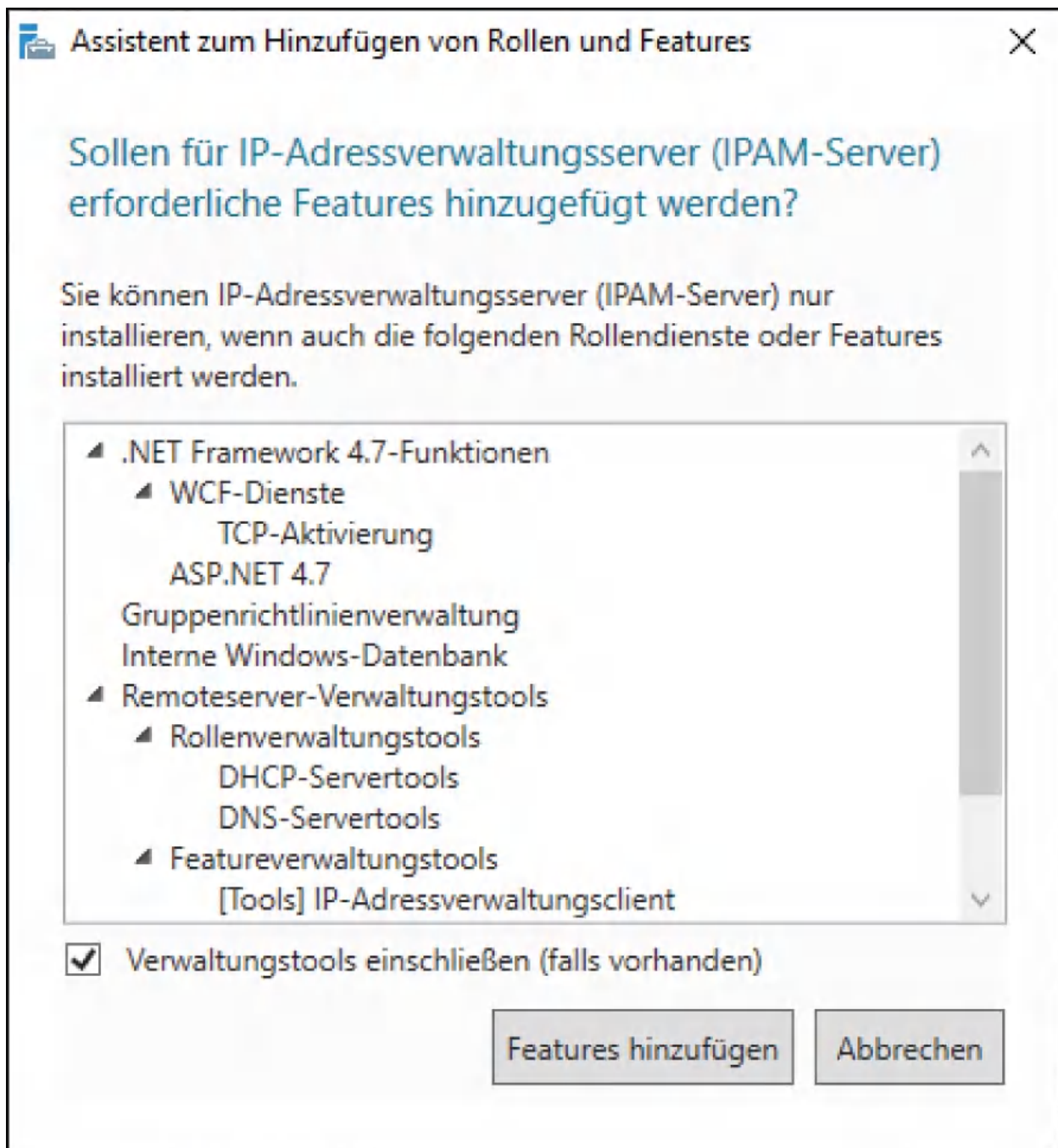


Abbildung 8.23: Welche Rolle der Server im DHCP-Failover einnimmt, gibt das Eigenschaftsfenster preis.

Ein Assistent unterstützt Sie bei der Einrichtung, direkt aus dem Server-Manager heraus (siehe [Abbildung 8.24](#)).

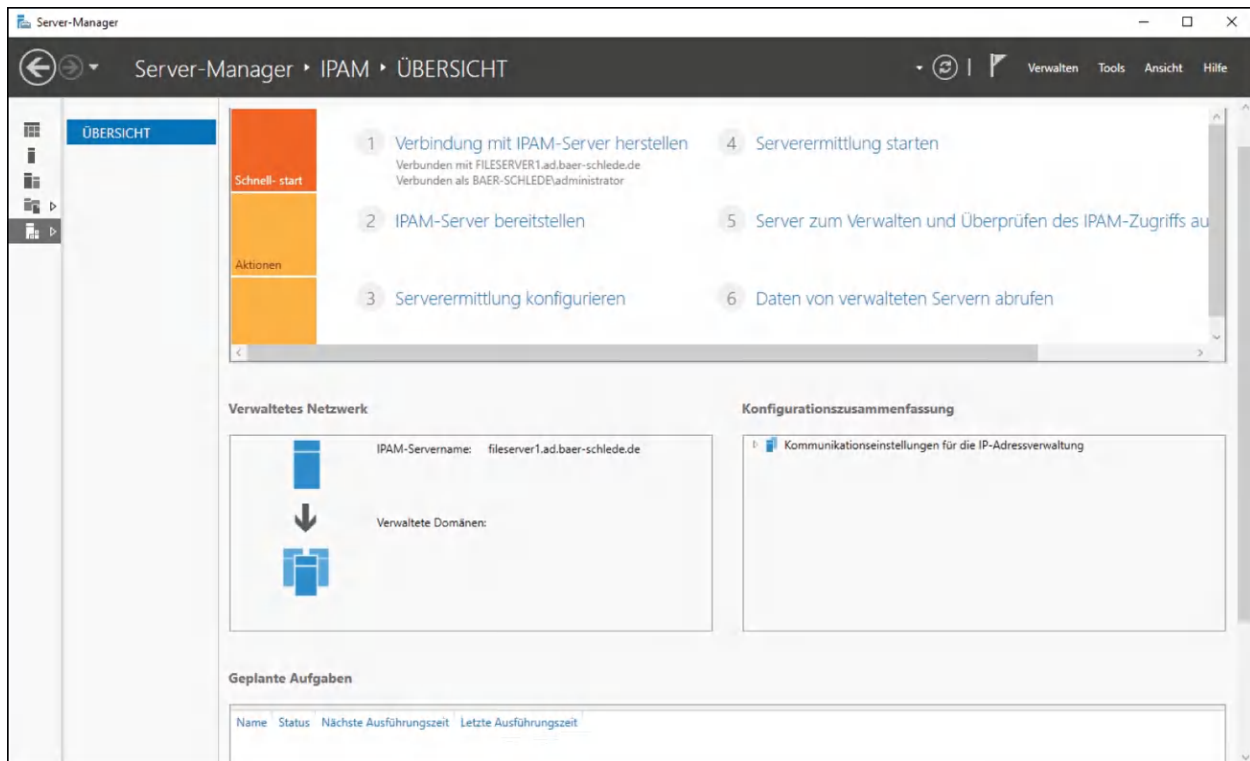


Abbildung 8.24: Die Einrichtung von IPAM startet im Server-Manager.

Während der Installation, SCHRITT 2 im Assistenten, haben Sie die Aufgabe festzulegen, ob eine manuelle oder gruppenrichtlinienbasierte Methode durchgeführt werden soll.

Bei der manuellen Methode müssen Sie die erforderlichen Netzwerkfreigaben, die Sicherheitsgruppen und eventuelle Firewall-Regeln für jeden der verwaltenden Server manuell konfigurieren. Bei der anderen Variante erzeugt der Einrichtungsassistent die entsprechenden Gruppenrichtlinien automatisch (siehe [Abbildung 8.25](#)), verknüpft diese mit der Domäne und passt die Sicherheitsfilterung an.



Sofern Sie sich für die gruppenrichtlinienbasierte Methode bei der Installation von IPAM entscheiden (was wir nur zur gut verstehen können), erkennen Sie die angelegten Gruppenrichtlinienobjekte (GPOs) an dem in diesem Zuge festgelegten Präfix. Sinnvollerweise sollten Sie dieses passend auswählen, beispielsweise IPAM.

Im nächsten Schritt (3) prüfen Sie die Serverermittlung, die einige

Augenblicke dauern kann, und fügen die gewünschte Domäne hinzu. Es folgt der Aufgabenschritt (4): die Server-Ermittlung. Auch diese Ermittlung kann wieder einige Minuten an Zeit in Anspruch nehmen. In unseren Praxistests hat sich gezeigt, dass ein Neustart der Server stets hilfreich war.

Nach einigen Minuten sollten Sie in der Lage sein, den SCHRITT 5 im IPAM-Server-Manager auszuwählen. Mit einer gewissen Wahrscheinlichkeit wird der hinzugefügte Server, zumeist der DC, im Zugriffstatus »Blockiert« ausgewiesen.

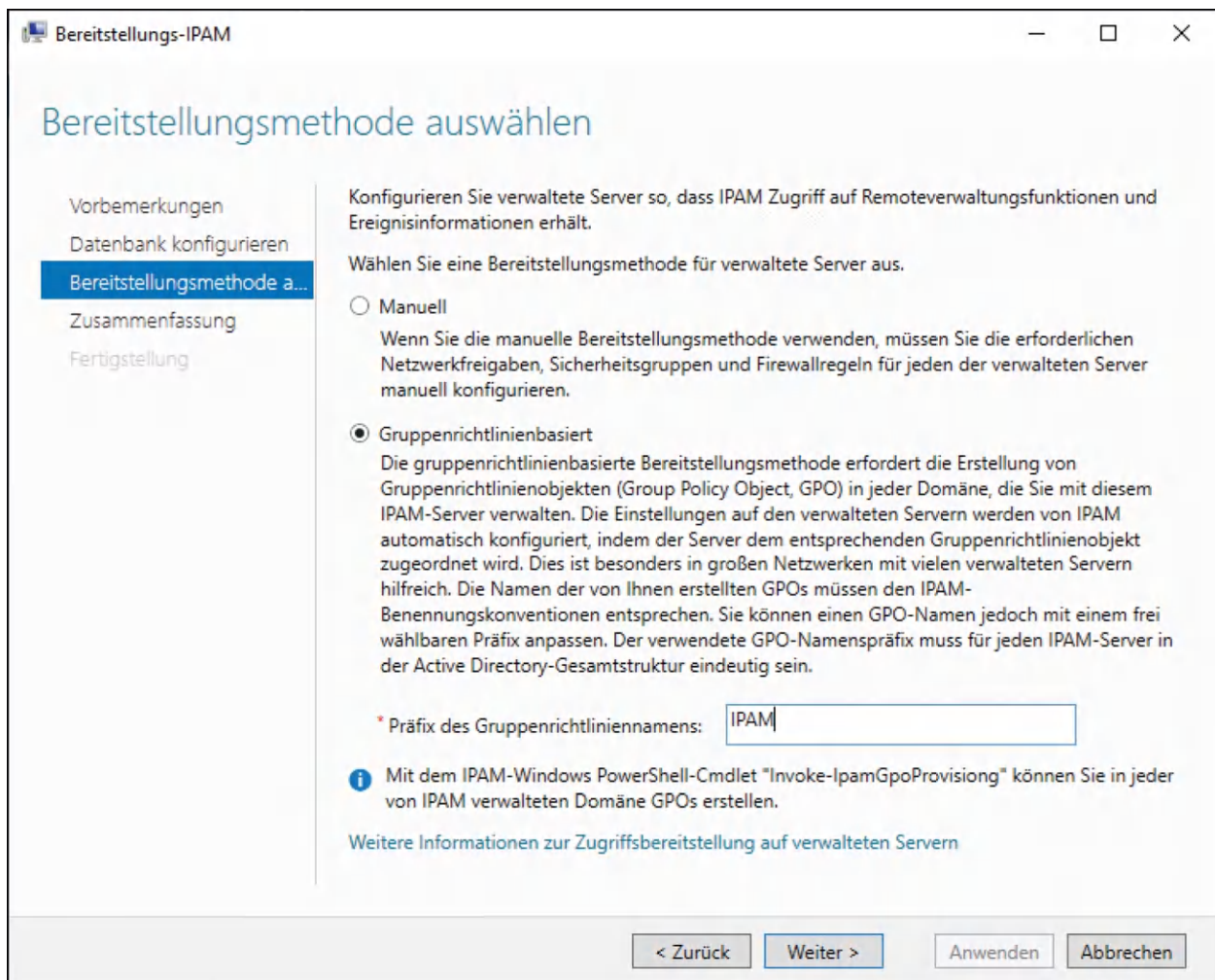


Abbildung 8.25: IPAM-Konfiguration: selber machen – oder machen lassen?

Starten Sie auf dem IPAM-Server die PowerShell und geben Sie folgendes Kommando ein:


```
Invoke-IPAMGpoProvisioning -Domain {DOMÄNE} -GpoPrefixName  
{hier IPAM} -IpamServerFqdn {FQDN IPAM-SERVER} -  
DelegatedGpoUser {Administrator@DOMAIN}
```

Im weiteren Verlauf werden Sie viermal aufgefordert, den jeweiligen Einrichtungspunkt mit J zu bestätigen – siehe [Abbildung 8.26](#).

Beachten Sie dabei unbedingt die Hinweise des Assistenten!

Wechseln Sie auf einen Domänencontroller, starten Sie die Eingabeaufforderung und aktualisieren Sie die Gruppenrichtlinien:

```
gpupdate /force
```

Prüfen Sie, ob die Gruppenrichtlinienobjekte angelegt wurden – siehe [Abbildung 8.27](#).

```
PS C:\Users\administrator.BAER-SCHLEDE>>> Invoke-IPAMGpoProvisioning -Domain ad.baer-schlede.de -GpoPrefixName IPAM -Ip  
amServerFqdn FILESERVER1.ad.baer-schlede.de -DelegatedGpoUser administrator@ad.baer-schlede.de  
  
Bestätigen  
Mit dem Cmdlet "Invoke-IPAMGpoProvisioning" werden drei Gruppenrichtlinienobjekte in der durch den Parameter "Domain"  
angegebenen Domäne erstellt und verknüpft, die zum Bereitstellen von IPAM-Zugriffseinstellungen auf den durch IPAM  
verwalteten Servern dienen. Mit dem Cmdlet wird außerdem die domänenweite DNS-Zugriffssteuerungsliste geändert, um den  
Lesezugriff für IPAM zu ermöglichen. Der Wert für "GpoPrefixName" muss mit dem im Assistenten für die  
IPAM-Bereitstellung angegebenen Wert bei der Auswahl der Option für die gruppenrichtlinienbasierte Bereitstellung  
übereinstimmen. Möchten Sie diese Aktion ausführen?  
[J] Ja [N] Nein [H] Anhalten [?] Hilfe (Standard ist "J"): j  
  
Die Gruppenrichtlinie erfordert, dass jedes Computerkonto über die Berechtigung zum Lesen von GPO-Daten von einem  
Domänencontroller verfügt, damit die Einstellungen der Benutzergruppenrichtlinie erfolgreich angewendet werden können.  
Das Entfernen der Gruppe "Authentifizierte Benutzer" kann die Verarbeitung von Benutzergruppenrichtlinien verhindern.  
Weitere Informationen finden Sie unter https://support.microsoft.com/kb/3163622.  
Möchten Sie den Vorgang fortsetzen?  
[J] Ja [N] Nein [H] Anhalten [?] Hilfe (Standard ist "J"): j  
WARNUNG: Die Gruppenrichtlinie erfordert, dass jedes Computerkonto über die Berechtigung zum Lesen von GPO-Daten von  
einem Domänencontroller verfügt, damit die Einstellungen der Benutzergruppenrichtlinie erfolgreich angewendet werden  
können. Fügen Sie die Domänencomputer oder die Sicherheitsgruppe "Authentifizierte Benutzer" mindestens mit  
Leseberechtigungen hinzu. Weitere Informationen finden Sie unter https://support.microsoft.com/kb/3163622.  
  
Die Gruppenrichtlinie erfordert, dass jedes Computerkonto über die Berechtigung zum Lesen von GPO-Daten von einem  
Domänencontroller verfügt, damit die Einstellungen der Benutzergruppenrichtlinie erfolgreich angewendet werden können.  
Das Entfernen der Gruppe "Authentifizierte Benutzer" kann die Verarbeitung von Benutzergruppenrichtlinien verhindern.  
Weitere Informationen finden Sie unter https://support.microsoft.com/kb/3163622.  
Möchten Sie den Vorgang fortsetzen?  
[J] Ja [N] Nein [H] Anhalten [?] Hilfe (Standard ist "J"): j  
WARNUNG: Die Gruppenrichtlinie erfordert, dass jedes Computerkonto über die Berechtigung zum Lesen von GPO-Daten von  
einem Domänencontroller verfügt, damit die Einstellungen der Benutzergruppenrichtlinie erfolgreich angewendet werden  
können. Fügen Sie die Domänencomputer oder die Sicherheitsgruppe "Authentifizierte Benutzer" mindestens mit  
Leseberechtigungen hinzu. Weitere Informationen finden Sie unter https://support.microsoft.com/kb/3163622.  
  
Die Gruppenrichtlinie erfordert, dass jedes Computerkonto über die Berechtigung zum Lesen von GPO-Daten von einem  
Domänencontroller verfügt, damit die Einstellungen der Benutzergruppenrichtlinie erfolgreich angewendet werden können.  
Das Entfernen der Gruppe "Authentifizierte Benutzer" kann die Verarbeitung von Benutzergruppenrichtlinien verhindern.  
Weitere Informationen finden Sie unter https://support.microsoft.com/kb/3163622.  
Möchten Sie den Vorgang fortsetzen?  
[J] Ja [N] Nein [H] Anhalten [?] Hilfe (Standard ist "J"): j  
WARNUNG: Die Gruppenrichtlinie erfordert, dass jedes Computerkonto über die Berechtigung zum Lesen von GPO-Daten von  
einem Domänencontroller verfügt, damit die Einstellungen der Benutzergruppenrichtlinie erfolgreich angewendet werden  
können. Fügen Sie die Domänencomputer oder die Sicherheitsgruppe "Authentifizierte Benutzer" mindestens mit  
Leseberechtigungen hinzu. Weitere Informationen finden Sie unter https://support.microsoft.com/kb/3163622.  
PS C:\Users\administrator.BAER-SCHLEDE>>> .
```

Abbildung 8.26: Die Einrichtung von IPAM erfordert die Anlage einiger Gruppenrichtlinien über ein PowerShell-Kommando.

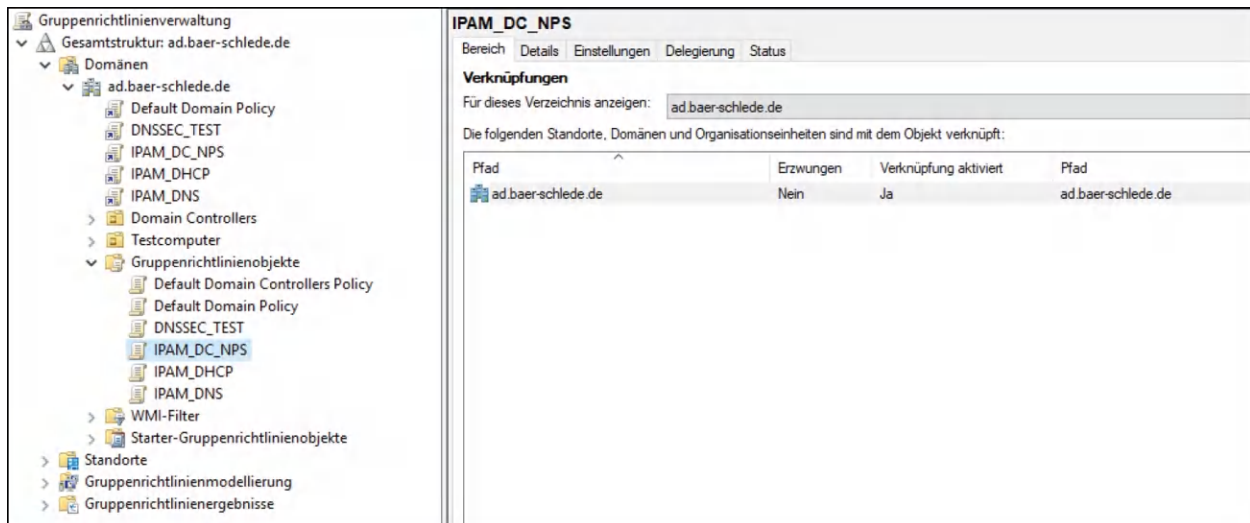


Abbildung 8.27: Erfolgreich – die Gruppenrichtlinienobjekte wurden erzeugt.

Anschließend können Sie mit IPAM IP-, DHCP- und DNS-Bereiche im Server-Manager verwalten und dokumentieren ([Abbildung 8.28](#)). Anstelle vom System getrennter Listen im Excel-Format haben Sie so die Möglichkeit, »live« mit den Daten zu arbeiten:

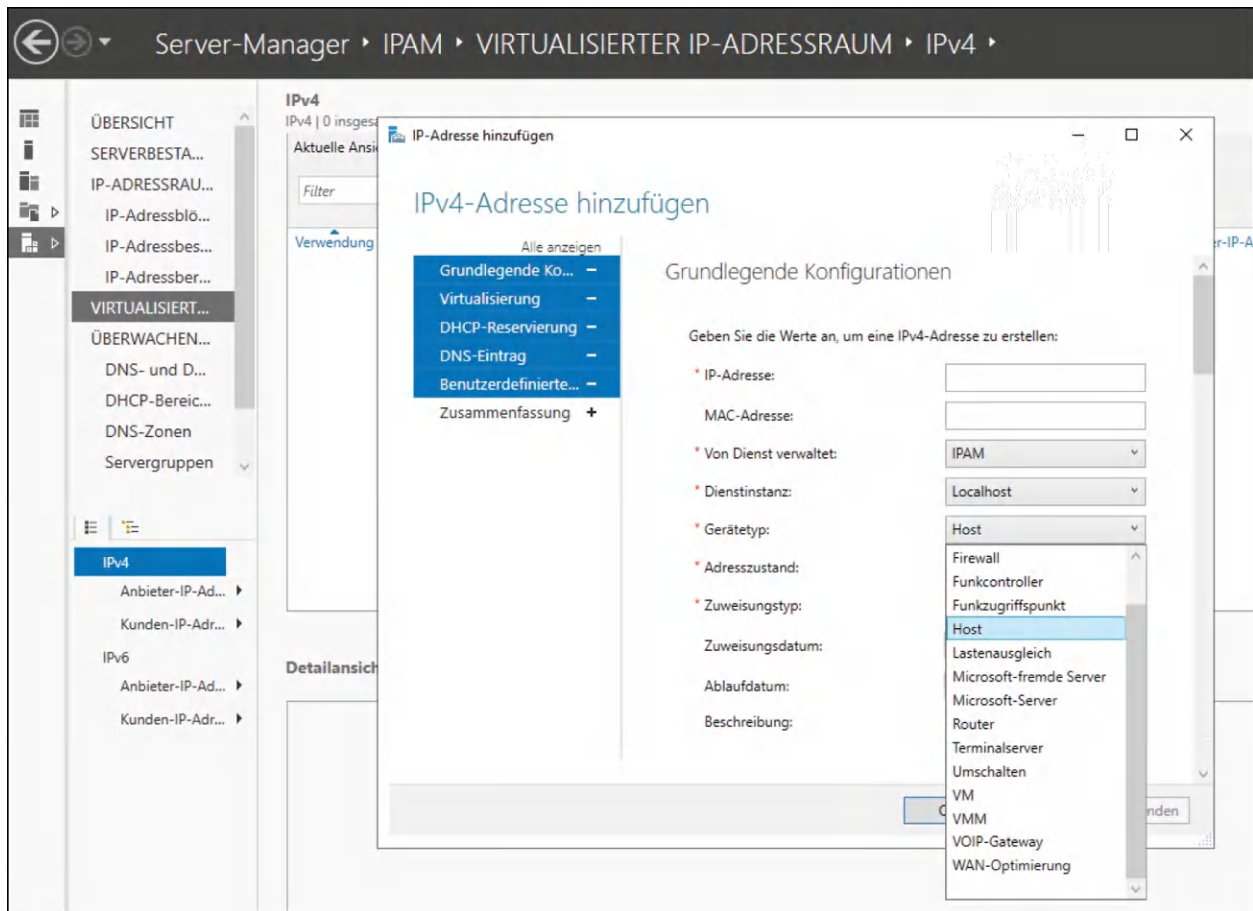


Abbildung 8.28: IP-Adressverwaltung mit IPAM

Kapitel 9

Speicherdienste – Datei-Server

IN DIESEM KAPITEL

Grundlagen zu Speicherdiensten

iSCSI

Datei- und Speicherdienste

Eine der wichtigsten Aufgaben eines Servers besteht darin, Dateien und Daten zur Verfügung zu stellen. Diese Bereitstellung erfolgt unter Windows auf viele verschiedene Arten, die in der Summe Speicherdienste genannt werden.

Glücklicherweise gibt es bei Windows Server den SERVER-MANAGER, der dem Administrator einen guten Überblick darüber gibt, welche der vom Hersteller mitgegebenen Basisfunktionen auf der Maschine aktiv sind und welche nicht. Dank der Fähigkeit, sich mit dem Server-Manager auch auf andere Windows-Server »aufzuschalten«, ist ein zügiger Blick auf dessen Konfiguration oder die gemeinsame Verwaltung sehr einfach möglich. Der SERVER-MANAGER ist also die erste Anlaufstelle – auch wenn es um die Fähigkeiten als »Speicher« geht.

In der Rubrik DATEI/SPEICHERDIENSTE hat der Server in Summe zwölf Rollen zu bieten, mit denen aus dem einfachen Windows-Server ein mehr oder weniger komplexes Storage-System wird. Server-Systeme sind, da macht Windows keine Ausnahme, wie Baukästen konzipiert, die sich, ganz nach Wunsch des Administrators, zusammenstellen lassen. Der Flexibilität sind kaum Grenzen gesetzt. Von einer eher statischen Ausnahme dann doch einmal abgesehen. Der unterste Eintrag lautet SPEICHERDIENSTE, in der Auswahlliste bereits markiert und mit dem Hinweis »Installiert« in Klammern. Das Beste an dieser Rolle: »Die Speicherdienste bieten Speicherverwaltungsfunktionen. Diese werden

immer installiert und können nicht entfernt werden.« Spannend! Warum es dann überhaupt einen Eintrag in der Liste gibt – das bleibt ein Geheimnis der Entwickler in Redmond.

Bei den anderen elf Kandidaten auf der Liste geht es da deutlich spannender zur Sache. Die Freude als Administrator ist berechtigt, denn der Windows-Server hat viel mehr zu bieten, als es zunächst den Eindruck macht. Insbesondere in kleineren Umgebungen ist der Griff zur Zusatz-Software eines Drittanbieters häufig gar nicht erforderlich – das hat Ihr Server selbst drauf. Ohne sich nun über das Beratungsgeschäft der IT-Consultants negativ äußern zu wollen, aber mitunter empfehlen diese ihren Kunden Software-Produkte, die weit mehr leisten, als es der Kunde überhaupt braucht. Das hat möglicherweise ja etwas damit zu tun, dass beim Verkauf die Marge doch nicht ganz so gering ist, wie es gern behauptet wird.

Platten und Storage

Bevor wir nun auf die Server-Rollen für einen Windows-Datei-Server eingehen werden, noch etwas Grundsätzliches zu Festplatten, Festplattenanbindung und den Leistungsanforderungen. Die Bezeichnung Festplatte hat schon etwas Patina angesetzt, denn rotierende Datenträger mit »festen Platten« kommen immer seltener zum Einsatz. Heutige SSDs (Solid State Disks) speichern die Informationen auf Flash-Halbleiterbausteinen, ganz ohne Mechanik. Technisch gesehen sind SSDs eigentlich schon seit mehreren Dekaden bekannt, doch erst Mitte der 2010er-Jahre eine Standardausrüstung bei Client-Computern, später auch bei Server-Systemen. SSDs sind viel schneller als mechanische Platten, verbrauchen weniger Strom und sind geräuschlos. Allesamt gute Merkmale für einen Client-Computer oder Server-Systeme, die nicht in Server-Räumen oder Rechenzentren zum Einsatz kommen.

Typischerweise verfügen Server über mehrere Festplatten, die der Controller als gemeinsamer Festplattenverbund (RAID) anspricht. Windows, als Betriebssystem, sieht diesen Verbund als ein »logical Volume«. Eine Gruppe von mechanischen Festplatten kann dabei äußerst überzeugende Leistungsdaten liefern, zumal IT-Ingenieure bei den RAID-

Adaptern seit vielen Jahren Optimierungsarbeit leisten und dank Pufferspeicher ebenfalls sehr schnelle Reaktionszeiten erzielen. Aber machen wir uns nichts vor: In ein paar Jahren gibt es sie wahrscheinlich nicht mehr, die lärmenden, rotierenden Festplatten.



Zur langfristigen Datenspeicherung ohne Einsatz sind mechanische Festplatten besser geeignet. Je nach technischer Umsetzung der NAND-Flash-Speicher in den SSDs kann es sein, dass die Speicherdauer, ohne Betriebszeit, für die Daten nur wenige Monate beträgt, wie beispielsweise beim »Triple-Level Cell«-(TLC-)Speicher. Solange der Server in Betrieb ist und ständig damit beschäftigt ist, Daten zu lesen und zu speichern, droht von der Seite jedoch keine Gefahr.

Mithilfe verschiedener Techniken wird die systembedingte, begrenzte Lebensdauer der Speicherzellen der SSDs verlängert. Wir wollen hier nicht näher darauf eingehen – bei Interesse forschen Sie im Internet nach »Dynamic Wear Levelling« oder »Static Wear Levelling«.



In sehr kleinen Umgebungen ist der Einsatz von SATA-SSDs in Servern gerade noch vertretbar. In produktiv genutzte Server gehören SAS-Platten oder -SSDs, diese sind für den Dauerbetrieb ausgelegt.

RAID, iSCSI-Zielsever und iSCSI-Initiator

Hinsichtlich des Speicherausbaus unterscheiden sich Server drastisch voneinander. Es gibt Geräte mit mehreren »Festplatteneinschüben« und Systeme mit nur einem Flash-Speicher, auf dem nur das Betriebssystem Platz findet. Ein typischer Anwendungs-Server in großen Rechenzentren hat lediglich zwei Platten, die in einem RAID1-Verbund organisiert sind.



Im RAID 1 speichert der Controller stets dieselben Informationen

auf beide Festplatten. Fällt eine Festplatte aus, kann der Administrator diese durch eine identische oder von der Kapazität her größeren Platte ersetzen. Der RAID-Controller erkennt, dass es sich um eine »neue Platte ohne Verbundkennung handelt«, und legt den identischen Speicherinhalt der verbliebenen Festplatte wieder an. Sofern ein solcher Wechsel im laufenden Betrieb funktioniert, nennt sich das Hot Plugging. Wartet eine weitere, leere Festplatte nur darauf, dass eine andere Platte ausfällt, so bezeichnen IT-Profis diese wartende Platte als Hot Spare.

Eine andere, weit verbreitete Variante des Festplattenverbunds ist RAID 5. Hierbei handelt es sich um die Verteilung eines Volumes auf mindestens drei Festplatten, wobei eine Platte im laufenden Betrieb ausfallen kann, ohne dass ein Volume »Daten verliert« oder »offline« gesetzt werden müsste.

Die Einstellung RAID 0 verknüpft mindestens zwei Festplatten zu einem gemeinsamen Volume, mit dem Ziel, die Betriebsgeschwindigkeit zu erhöhen. Fällt eine Platte aus, ist der komplette Verbund betroffen. Eine besonders beliebte Variante ist die Kombination der Betriebsformen 0 und 1 zu RAID 10 – schnell und sicher.

Üblicherweise wird der RAID-Verbund direkt über den Controller definiert – sprich auf einer Ebene unterhalb des Betriebssystems. Windows ist, wie die meisten modernen Betriebssysteme, in der Lage, ebenfalls RAID-Verbünde zu betreiben. Diese Variante ist insbesondere im Zusammenspiel mit der Virtualisierung Hyper-V spannend. In kleineren Umgebungen ist der Einsatz von Hardware-RAID meist die richtige Entscheidung.

Server in Rechenzentren mit kleinen lokalen Festplatten arbeiten typischerweise mit externen Speichersystemen. Die Anbindung geschieht entweder per »Fibre Channel« oder per »iSCSI«. Letzteres ist der nunmehr gebräuchlichere Standard, da hierfür lediglich »normale Netzwerkkomponenten« erforderlich sind. Im einfachsten Fall verbindet ein Ethernet-Kabel zwei Ethernet-Netzwerkkarten zwischen zwei Servern, und die Steuer- und Datenpakete fließen zwischen diesen Systemen hin

und her.

Die beiden beteiligten Maschinen übertragen die Datenpakete für die Festplattenzugriffe dabei nicht mehr über ein SATA- oder SAS-Kabel, sondern mittels SCSI-Befehlssatzes über die Netzwerkschnittstellen. In großen Umgebungen legen Administratoren für diesen Einsatzzweck gesonderte Netzwerkbereiche an, oft mit eigenen Switches, um einen vom eigentlichen LAN-Datenverkehr abgetrennten Bereich zu bilden. In diesen Storage-Netzwerken fehlen viele Dienste, die normalerweise ein Netzwerk ausmachen, beispielsweise DHCP, DNS oder ein Standard-Gateway. Im Zuge der fortschreitenden Virtualisierung sind auch Storage-Systeme und -Netzwerke nunmehr ein »Software-definiertes Netzwerk«.

Nun sind wir beim iSCSI-ZIELSERVER, einer der Rollen des Windows-Servers angekommen. Betrachten wir beispielhaft die Erstellung einer iSCSI-Festplatte auf einem Windows-Server und die Einbindung auf einem Windows-Client. Auf der Client-Seite heißt die benötigte Software »iSCSI Initiator« – diese ist kostenfrei, arbeitet als Dienst und wird von Microsoft bereitgestellt.

Die Installation des iSCSI-Zielservers geschieht über den Server-Manager:

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts ROLLEN/FEATURES HINZUFÜGEN.
3. Wählen Sie SPEICHERDIENSTE.
4. Wählen Sie iSCSI-ZIELSERVER (siehe [Abbildung 9.1](#)).

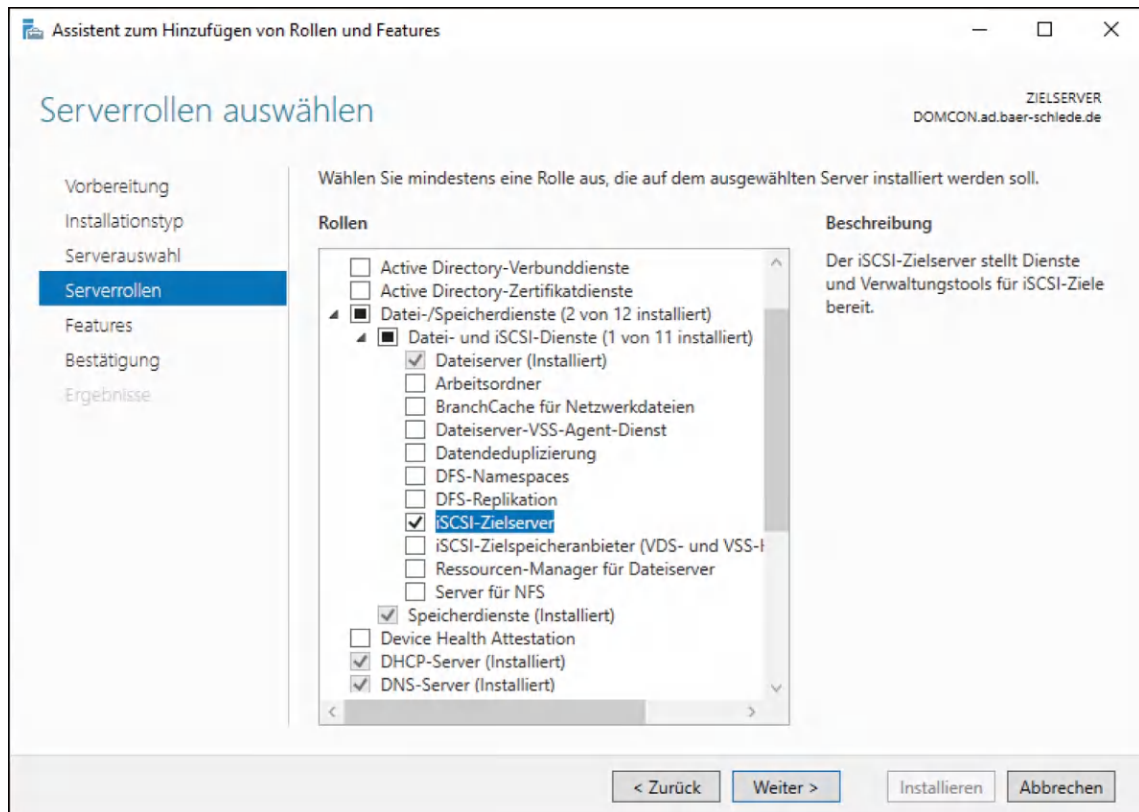


Abbildung 9.1: Die Installation der Server-Rolle geschieht, wie gewohnt, über den Server-Manager.

5. Bestätigen Sie die folgenden Dialoge mit WEITER.

Über den Initiator »spricht« der Computer iSCSI-basierte Speicher über das TCP/IP-Netzwerk an. Das anvisierte Ziel in dieser Kommunikation wird typischerweise als »Target« bezeichnet. Ein Target ist zumeist eine Festplatte oder ein Festplattenverbund, aber auch Bandlaufwerke oder Bandroboter können Administratoren per iSCSI als Target ansprechen. Das IP-Netzwerk, die dritte erforderliche Komponente, befindet sich zwischen Target und Initiator und ist für den Transport der Daten zuständig. Definiert wurde iSCSI in den RFCs 3720 und 7143. Die RFCs beschreiben das Verpacken der Daten in TCP/IP-Pakete und weitere Einzelheiten. Für die Kommunikation sind die TCP-Ports 860 und 3260 erforderlich. Auf aktuellen Windows-Betriebssystemen stellt der Konfigurationsprozess zumeist sicher, dass entsprechend freizügige Regeln in der Windows-Defender-Firewall eingerichtet sind.

Die Einrichtung geschieht über den Assistenten zum Hinzufügen von

Rollen und Features im Server-Manager, und es gilt, die Rolle iSCSI-ZIELSERVER auszuwählen. Die Einrichtung dauert lediglich ein paar Augenblicke und erfordert keinen Neustart des Servers. Auch die Konfiguration von iSCSI-Targets geschieht direkt aus dem Server-Manager heraus. Sofern ordnungsgemäß installiert, entdeckt der Administrator sie auf der linken Seite im Menü. Dank des Konfigurationsassistenten ist die Einrichtung denkbar einfach und erfordert nur wenige Eingaben.



Kommt es bei der Auswahl des Zugriffs-Servers zur Fehlermeldung »Die IQN für *Rechnername* kann nicht bestimmt werden«, wechseln Sie auf den Zielcomputer und öffnen dort den iSCSI-Initiator. Im Register KONFIGURATION finden Sie den generierten IQN-Namen im Stil: [iqn.1991-05.com](http://qn.1991-05.com).microsoft:Client-Name als FQDN.



Das Namensformat IQN ist im RFC 3270 (<https://tools.ietf.org/html/rfc3270>) definiert. Wesentliche Bestandteile sind das Literal »IQN« (iSCSI Qualified Name), das Datum der Inbesitznahme durch den Domänenbesitzer im Format JJJJ-JJ, der reservierte Domänenname, gefolgt von einem Doppelpunkt und typischerweise dem Client-Namen.

Unter Windows ist

- ✓ ein bereitgestelltes iSCSI-Target stets ein virtueller iSCSI-Datenträger.
- ✓ die Bereitstellung »echter« angeschlossener Laufwerke, zum Beispiel einem Bandlaufwerk, über iSCSI nicht möglich.
- ✓ eine umfassende Verschlüsselung ist nur erforderlich, wenn das Storage-Netzwerk komplex ist und sich verschiedene Arbeitsbereiche, Abteilungen oder Mandanten das Netzwerk teilen.

Nach der Anlage des iSCSI-Targets starten Sie auf dem Zielcomputer – hierbei kann es sich auch um ein Windows-Client-Betriebssystem handeln – den iSCSI-Initiator und geben im Abschnitt ZIELE den Servernamen

des Targets ein. Nach einem Klick auf SCHNELL VERBINDEN... erscheint eine Erfolgsmeldung, die mit FERTIG zu bestätigen ist. Auf der Server-Seite ist ersichtlich, welcher iSCSI-Initiator sich mit welchem Target verbunden hat – siehe [Abbildung 9.2](#).

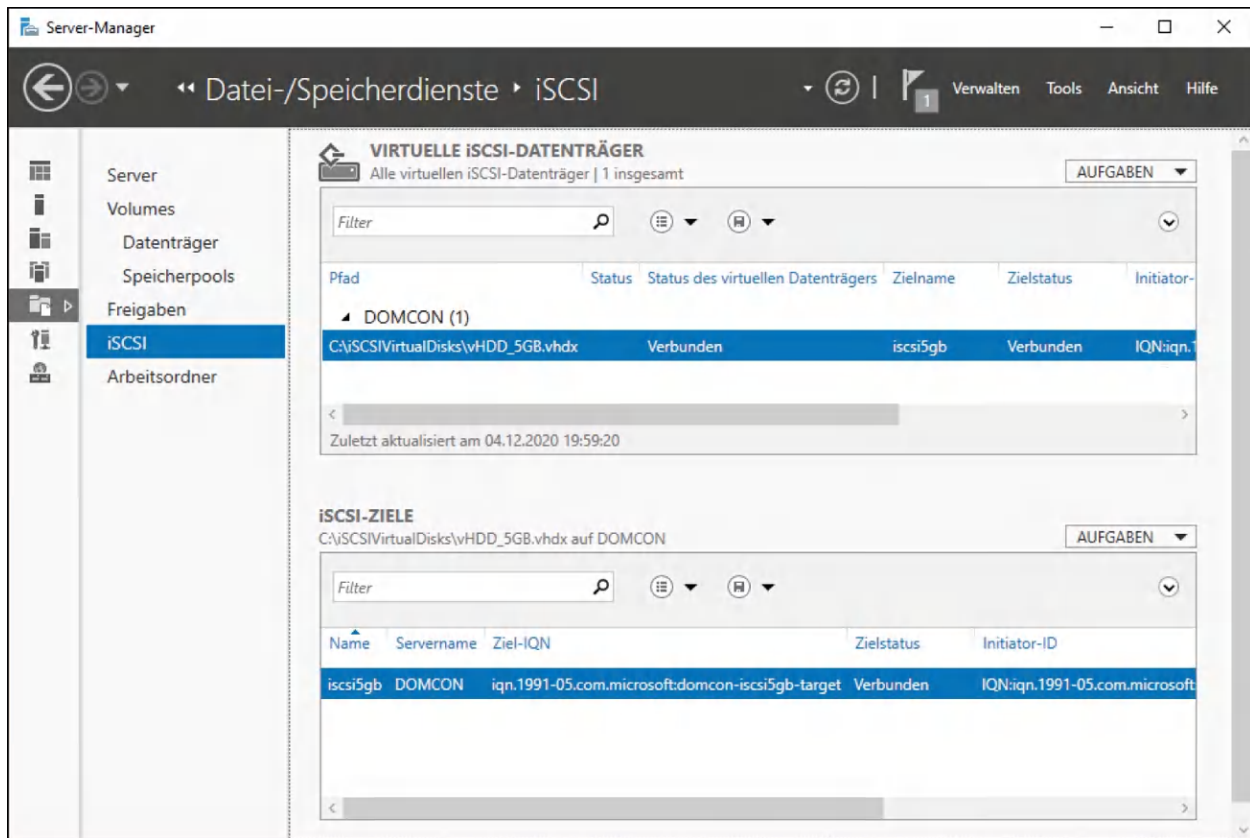


Abbildung 9.2: Im Server-Manager ist für den Administrator ersichtlich, welche iSCSI-Initiator-Computer welche Targets nutzen.

Wer nun erwartet, es würde automatisch ein Dialog auftauchen, in dem Sie festlegen, was mit dem neuen Laufwerk zu tun ist – irrt. Wie eine »echte Festplatte« ist das iSCSI-Target in der Datenträgerverwaltung zunächst zu initialisieren.

Hierzu wechseln Sie in die COMPUTERVERWALTUNG und wählen in der Baumstruktur unter DATENTRÄGERVERWALTUNG den neuen, noch nicht initialisierten Datenträger (siehe [Abbildung 9.3](#)) mit einem Rechtsklick aus. Im Kontextmenü stehen zur Initialisierung MBR oder GPT zur Auswahl. Sofern keine älteren Windows-Systeme als Windows Vista/2008 jemals auf den Datenträger zugreifen sollen, wählen Sie GPT.

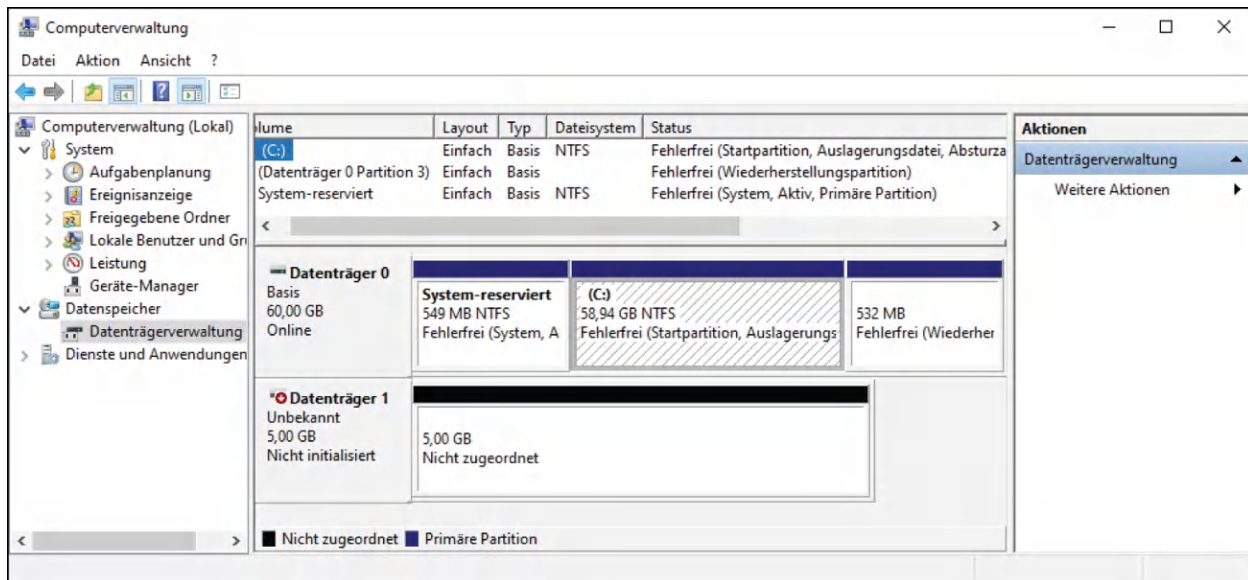


Abbildung 9.3: Wie gewöhnliche Festplatten muss der Administrator den iSCSI-Datenträger auf dem Zielrechner initialisieren.



Zur Initialisierung eines Datenträgers muss der Administrator den Partitionsstil festlegen. Zur Auswahl steht der ältere Master Boot Record (MBR) oder die modernere Variante GUID-Partitionstabelle (GPT). GPT unterstützt 128 Volumes pro Datenträger, MBR lediglich 4. Die maximale Festplattengröße beträgt unter MBR 2 TByte, während GPT 18 EByte verwalten kann. Die Limitierung auf 2 TByte macht MBR schon aus Prinzip uninteressant. Soll der Datenträger jedoch von 32-Bit-Systemen und -Tools bearbeitet werden können, ist MBR die einzige Möglichkeit.

Spannenderweise kann der Administrator das Target auch auf dem freigebenden Server selbst mit iSCSI-Initiator einbinden und einen Laufwerksbuchstaben zuweisen. Leider ist es jedoch nicht möglich, ein solches Laufwerk quasi als Cluster-Laufwerksbuchstaben von mehreren PCs aus gleichzeitig zu verwenden. Aus Client-Sicht stellen sich iSCSI-Laufwerke wie lokale Laufwerke dar. Anders als traditionelle Netzwerkfreigaben, die für Clients als Remote Volumes erkennbar sind, operiert iSCSI direkt auf der Blockebene.

Es versteht sich von selbst: Ist der Server mit dem iSCSI-Target nicht erreichbar, kann auch der Computer, der mit dem iSCSI-Initiator darauf

zugreift, das Volume nicht mehr erreichen.

Es gibt keinen Offline- oder Puffer-Modus, der Änderungen zwischenspeichert. Das heißt nicht mehr oder weniger, als dass bei iSCSI, wie bei Fibre Channel auch, die Transportprotokolle nicht in der Lage sind, sich gegenüber rivalisierenden Zugriffen zu sperren. Es ist aus diesem Grunde eine schlechte Idee, beliebige Client- oder Serversysteme ohne entsprechende Vorkehrungen mit demselben iSCSI-Target zu verbinden. Es droht ansonsten Datenverlust.

Die iSCSI-Targets kann der Administrator im SERVER-MANAGER im laufenden Betrieb vergrößern. Hierzu ist lediglich ein Rechtsklick auf den Eintrag unter ZIELE notwendig. Im Kontextmenü ist hierzu VIRTUELLEN ISCSI-DATENTRÄGER ERWEITERN erforderlich. Eine Verkleinerung sieht das Programm indes nicht vor. Die Vergrößerung ist ohne Unterbrechung des Datenstroms für den Client, jedoch gilt es für den Administrator anschließend, die Partition auf dem Zielcomputer ebenfalls zu erweitern.

Wozu dann überhaupt ein solcher Zugriff, wenn er ohnehin exklusiv sein muss?

- ✓ Sie können Storage-Speicher einfach und flexibel im Rechenzentrum verteilen.
- ✓ Sie können Storage-Speicher zügig »umhängen«.
- ✓ Blockbasierte Zugriffe erlauben die Nutzung für Datenbanksysteme und Exchange.
- ✓ Blockbasierte Freigaben sind viel schneller als SMB-Freigaben.
- ✓ Blockbasierte iSCSI-Freigaben erlauben Partitionen, eigene Rechtesteuerungen und sogar die Einbindung in komplett andere Domänenstrukturen.

iSCSI-Zielspeicheranbieter

Hinter dieser doch eher kryptischen Bezeichnung verbirgt sich eine Erweiterung für bereitgestellte iSCSI-Targets um die Funktion

Volumenschattenkopie auf der Server-Seite.

Sofern diese Server-Rolle installiert ist, können Anwendungen auf einem Server Volumenschattenkopien (VSS) von Daten auf den virtuellen iSCSI-Datenträgern erzeugen. Ebenfalls an diese Rolle gebunden ist die Möglichkeit, die virtuellen iSCSI-Datenträger mit älteren Anwendungen zu verwalten, die einen »Virtual Disk Service«-(VDS-)Hardware-Dienstanbieter erfordern. Faktisch handelt es sich hierbei um den Befehlssatz `Diskraid`.

Die Funktionalität des ISCSI-ZIELSPEICHERANBIETERS hat, auch wenn es thematisch so klingt, nichts mit den Möglichkeiten der Systemwiederherstellungspunkte oder den einfachen Schattenkopien auf der Seite der Computer mit dem iSCSI-Initiator zu tun (siehe [Abbildung 9.4](#)). Diese, quasi iSCSI-Client-Systeme, nutzen das per iSCSI bereitstellte Volume wie ein gewöhnliches Laufwerk. Folglich bietet es alle technischen Fähigkeiten, die auch eine direkt angeschlossene Platte mitbringen würde.

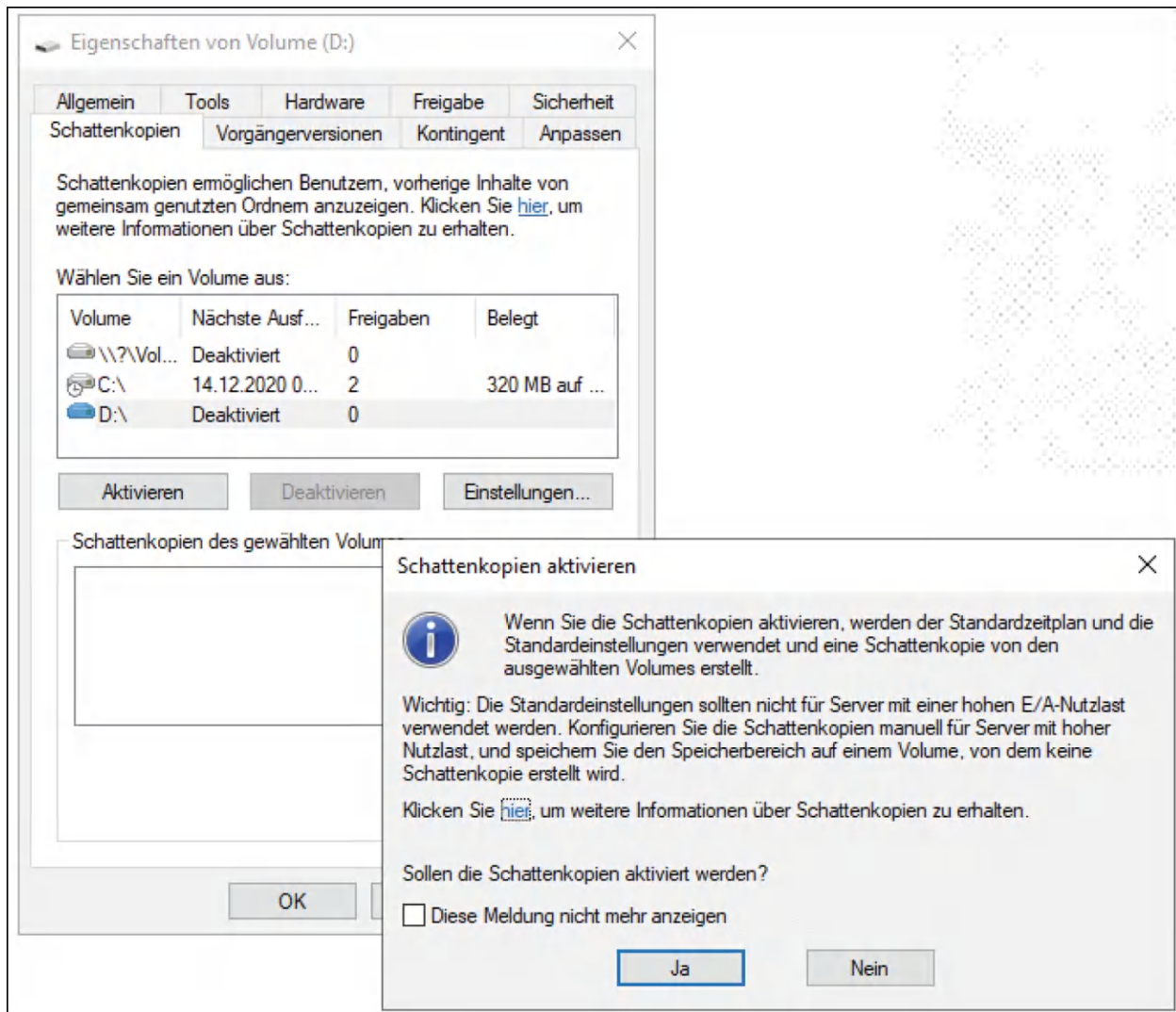


Abbildung 9.4: Schattenkopien und Vorgängerversionen funktionieren auch ohne die Rolle iSCSI-Zielspeicheranbieter.

Wer also regelmäßige Wiederherstellungspunkte auf dem Client einrichten möchte, kann dies über den Zeitplaner des Servers als Schattenkopie realisieren. Auf einem Windows-10-Computer ist hierfür die Einbindung eines Befehls in der Aufgabenplanung erforderlich (siehe [Abbildung 9.5](#)). Dieses Kommando bietet sich auch auf Windows-Servern für eine Batch-gesteuerte Erzeugung einer Volumenschattenkopien an

```
wmic shadowcopy call create Volume=Laufwerksbuchstabe:\
```

Der ISCSI-ZIELSPEICHERANBIETER liefert ein erweitertes Framework, das es insbesondere Backup-Programmen ermöglicht, Sicherungen durchzuführen, während die eigentliche Applikation,

beispielsweise ein SQL-Server, weiterarbeitet.

Der Zielspeicheranbieter stellt sicher, dass alle für die Sicherung erforderlichen Daten in der Schattenkopie konsistent sind. Spätestens die Backup-Software wird die Aktivierung dieser Server-Rolle von Ihnen einfordern. Besteht dahin gehend Unsicherheit: Installieren Sie einfach die Server-Rolle gleich mit – so ziemlich jede Quelle im Internet rät ohnehin dazu –, auch wenn der Grund sein dürfte, dass die Mehrheit der Autoren davon ausgeht, dass es sich um die Kompatibilität zur einfachen Schattenkopie handelt.

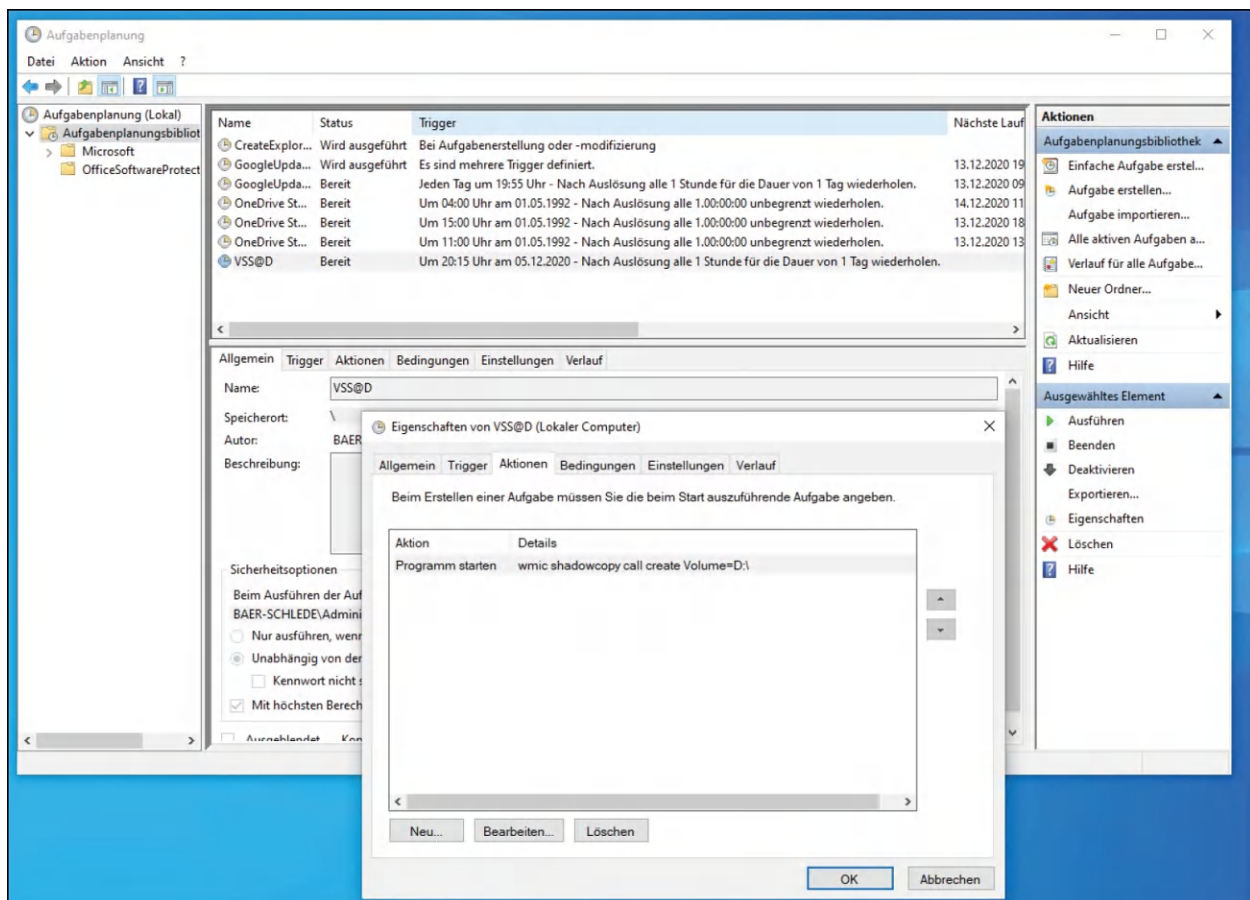


Abbildung 9.5: Automatische Erstellung von Schattenkopien unter Windows über die Aufgabenplanung



Wer sich tiefer mit dem Thema auseinandersetzen möchte, dem sei ein Beitrag in der Techcommunity von Microsoft von Jian (Jane) Yan ans Herz gelegt:

<https://techcommunity.microsoft.com/t5/storage-at-microsoft/iscsi-target-storage-vds-vss-provider/bap/424576>

Alle typischen Herausforderungen in Bezug auf das Backup im VSS-Umfeld beschreibt Michael Satran in seinem Microsoft-Docs-Dokument unter:

<https://docs.microsoft.com/de-de/windows/win32/vss/common-volume-backup-issues>

Server für NFS

In der Auflistung der Rollen im Bereich DATEI- UND ISCSI-DIENSTE finden Sie den Eintrag SERVER FÜR NFS ganz unten. Wer bereits Erfahrung mit Unix, Linux oder macOS gemacht hat, dem wird NFS durchaus ein Begriff sein. Es handelt sich um das seit vielen Jahren etablierte »Network File System«, ein Protokoll, um Dateizugriffe in Netzwerken zu ermöglichen.



Da die meisten Unix-basierten Computer nunmehr den von Microsoft üblicherweise gebräuchlichen Server Message Block (SMB) (auch CIFS genannt) unterstützen, ist die Notwendigkeit zur Installation der NFS-Kompatibilität auf Windows-Servern eher selten gegeben. Besteht die zu lösende Aufgabe beispielsweise darin, einer kleinen Anzahl von macOS-Computern Zugriff auf Dateiablagen auf einem Windows-Server zu geben, ist hierfür die Rolle SERVER FÜR NFS nicht erforderlich.

Spannender ist für Administratoren schon eher die Bedeutung von NFS im Zusammenspiel mit VMs unter vSphere von VMware. Windows Server unterstützt, sobald die Rolle aktiv ist, NFS in der Version 4.1 und eignet sich somit als File-Server für VMware ESXi und Linux im Allgemeinen.

Insbesondere für Linux-Administratoren, die sich mit Windows-Servern in ihrer Umgebung auseinandersetzen, ist diese NFS-Server-Rolle eine wichtige Funktion.

Die Installation der Rolle ist über den SERVER-MANAGER mit einem

Mausklick zu erledigen. Praktischerweise fügt der Installationsassistent automatisch die Dienste für die Netzwerkdateisystem-Verwaltungstools hinzu (siehe [Abbildung 9.6](#)).

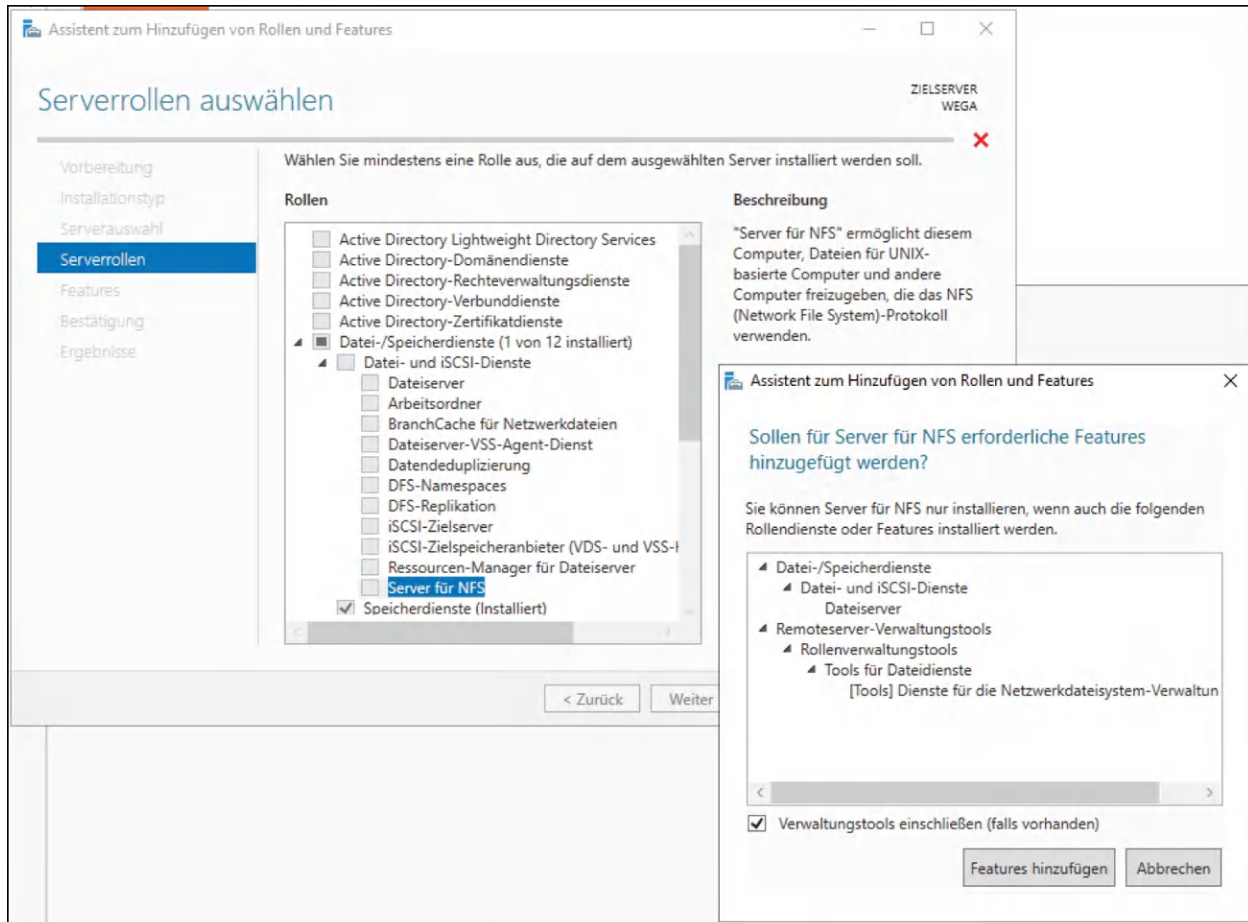


Abbildung 9.6: Die Installation über den Server-Manager fügt die Verwaltungstools für NFS automatisch mit ein.

Wer die Rolle über die PowerShell einrichtet, sollte den Aufruf um den Schalter `IncludeManagementTools` ergänzen:

```
Install-WindowsFeature FS-NFS-Service -IncludeManagementTools
```

Anschließend finden Sie die zur Konfiguration der NFS-Freigaben erforderlichen Dialogfenster im SERVER-MANAGER im Abschnitt DATEI-/SPEICHERDIENSTE im Menüpunkt FREIGABEN.

Ein Assistent unterstützt den Administrator bei der Einrichtung – der Vorgang ist für die ersten Schritte weitgehend selbsterklärend wie in [Abbildung 9.7](#) zu sehen. Bei der Definition der Freigabe schlägt das

Programm die Anlage eines lokalen Pfads für einen Share auf dem Server vor.

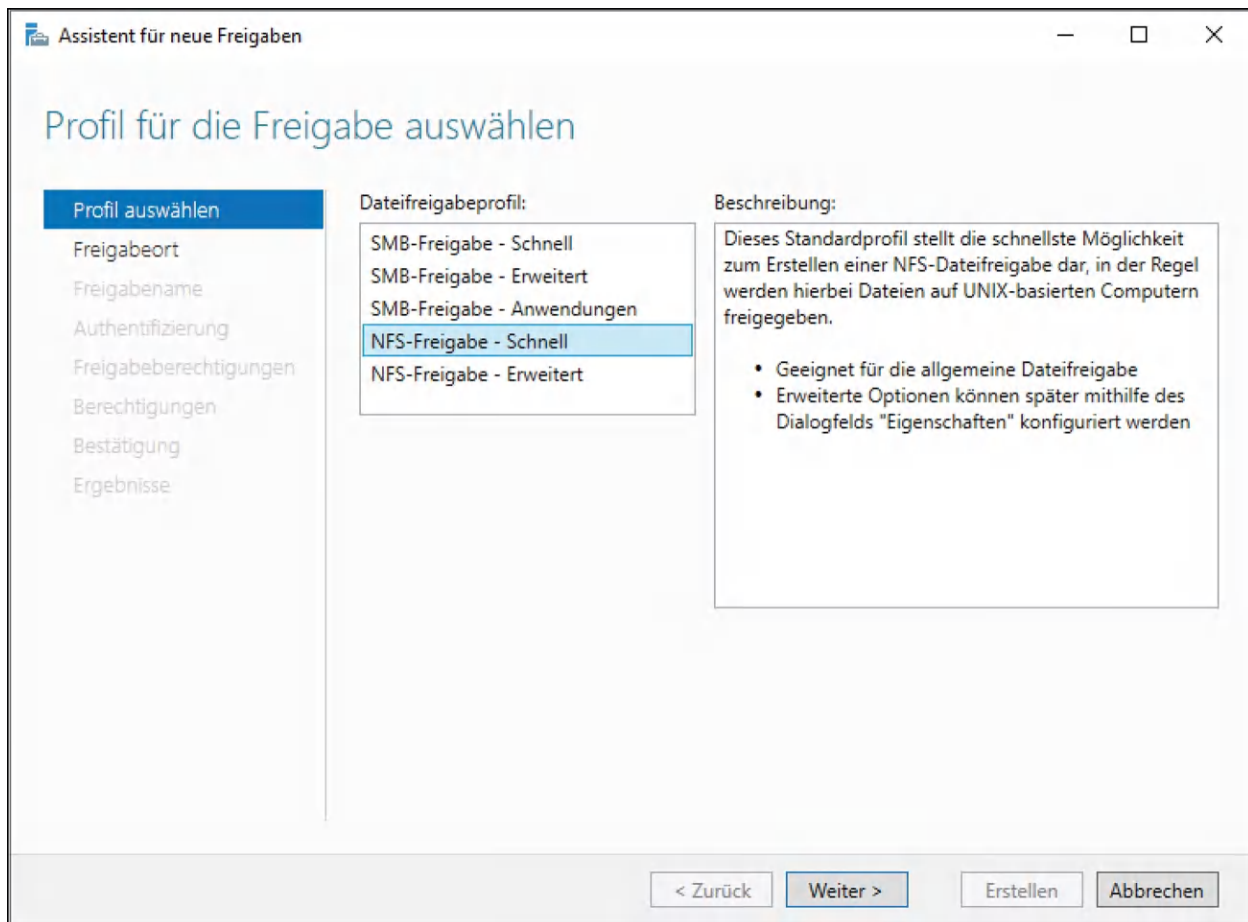


Abbildung 9.7: Dank eines Assistenten ist die Einrichtung einer NFS-Freigabe mit dem Server-Manager denkbar einfach.

Aus dem Freigabennamen TEST im lokalen Pfad c:\Shares\TEST wird so der Remote-Pfad zur Freigabe *SERVERNAME:/TEST*.



Sie können NFS-Freigaben unter Windows nur auf Volumes bereitstellen, die mit NTFS formatiert wurden. ReFS ist hierfür (noch) ungeeignet.

Im weiteren Verlauf des Assistenten wird der Administrator aufgefordert, die Authentifizierungsmethoden auszuwählen, die für diese NFS-Freigabe zugelassen sind. Die zur Auswahl stehenden Kerberos-Authentifizierungen-, Integrität- und Datenschutzooptionen sind parallel

oder getrennt aktivierbar.

Soll Kerberos im NFS-/ESXi-Umfeld zum Einsatz kommen, ist beim ESXi die Mindestversion 6.0 erforderlich. Zudem müssen die Hosts der AD-Domäne beitreten und die Freigabe mit NFS 4.1 ansprechen. Wie immer: Sicherheit und Einfachheit sind in der IT-Branche grundsätzlich gegenteiliger Natur. Alle anderen Varianten sind, was die Sicherheit angeht, nicht optimal.

Im nächsten Schritt des Einrichtungsassistenten hat der Administrator die Möglichkeit, auf die Berechtigung einzuwirken, um beispielsweise den Zugriff auf die NFS-Freigabe für einen Host, eine Client-Gruppe oder eine Netzgruppe festzulegen und die Freigabeberechtigung in drei Abstufungen einzuordnen:

- ✓ Kein Zugriff
- ✓ Schreibgeschützt
- ✓ Lesen/Schreiben

Die Sprachcodierung ist mit ANSI vorbelegt (siehe [Abbildung 9.8](#)) – diese Einstellung ist für unsere Sprachregion passend.

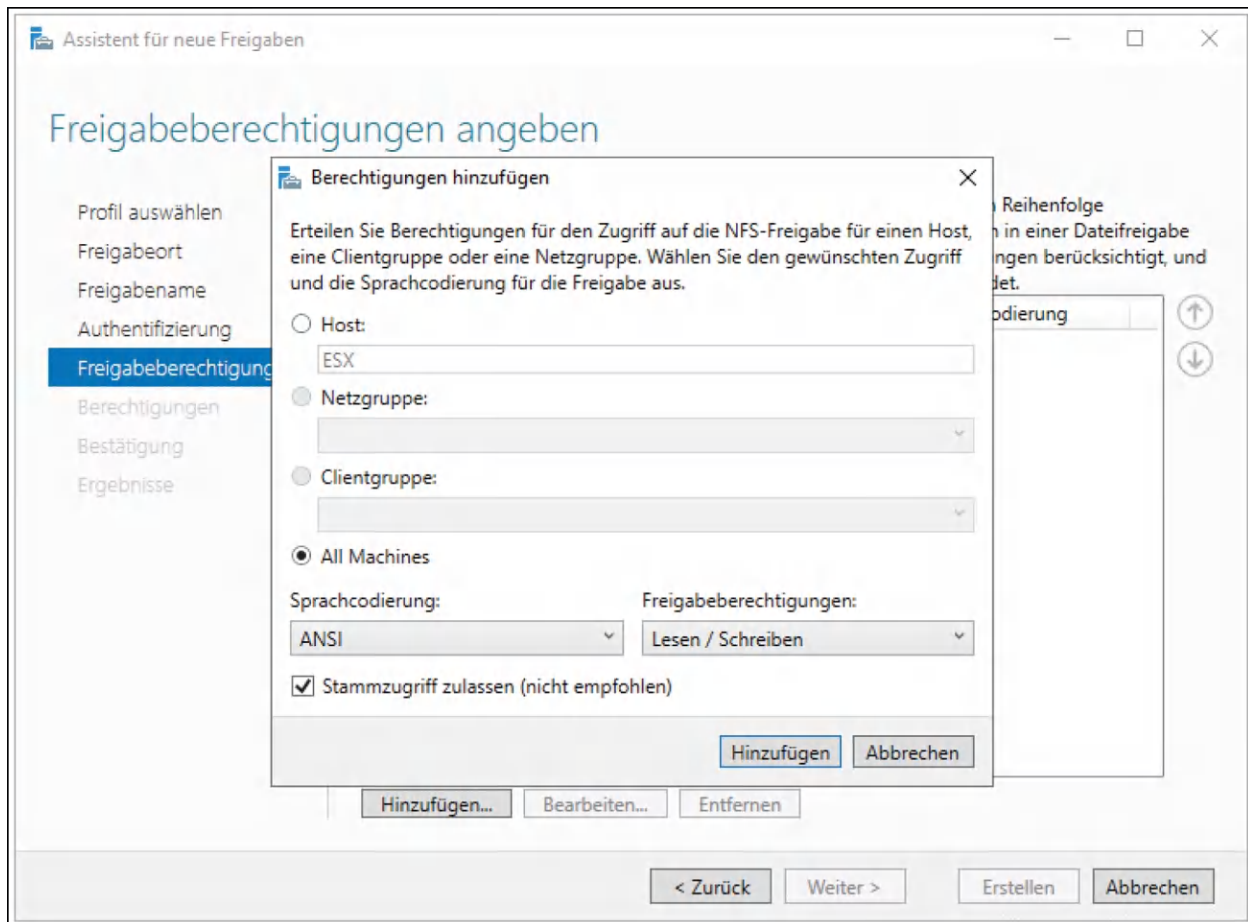


Abbildung 9.8: In der obigen Einstellung hätte jeder Computer Vollzugriff auf die NFS-Freigabe.

Die unterste Option in diesem Dialogfenster lautet STAMMZUGRIFF ZULASSEN. Es handelt sich dabei um eine wahrlich unglückliche Übersetzung ins Deutsche von »Allow root access«. Gemeint ist kein Zugriff auf den Stamm, sondern dass der Zugriff unter der root-Kennung des Clients erfolgt.

In dem bereits oben skizzierten Szenario, bei dem ein Windows-Server als NFS-Speicher für eine VMware vSphere-Umgebung dient, wäre dieses Häkchen zu setzen, sofern auf die Kerberos-Authentifizierung verzichtet wird.

Im letzten Dialog, vor der Zusammenfassung, legt der Administrator die Zugriffsrechte für die NFS-Freigabe fest. Wie bei SMB-Freigaben auch, handelt es sich um eine Kombination aus Datei- und Freigaberechten.

Im Windows Explorer kann der Administrator, nach der Einrichtung durch

den Assistenten, die NFS-Freigabe durch ein spezielles, kleines Icon erkennen. Wird der Ordner durch einen Rechtsklick geöffnet, wird eine Registerkarte sichtbar, die bei traditionellen Windows-Ordern ohne NFS-Freigabe fehlt (siehe [Abbildung 9.9](#)). In diesem Dialogfenster kann der Administrator direkt die NFS-Freigabe verwalten.

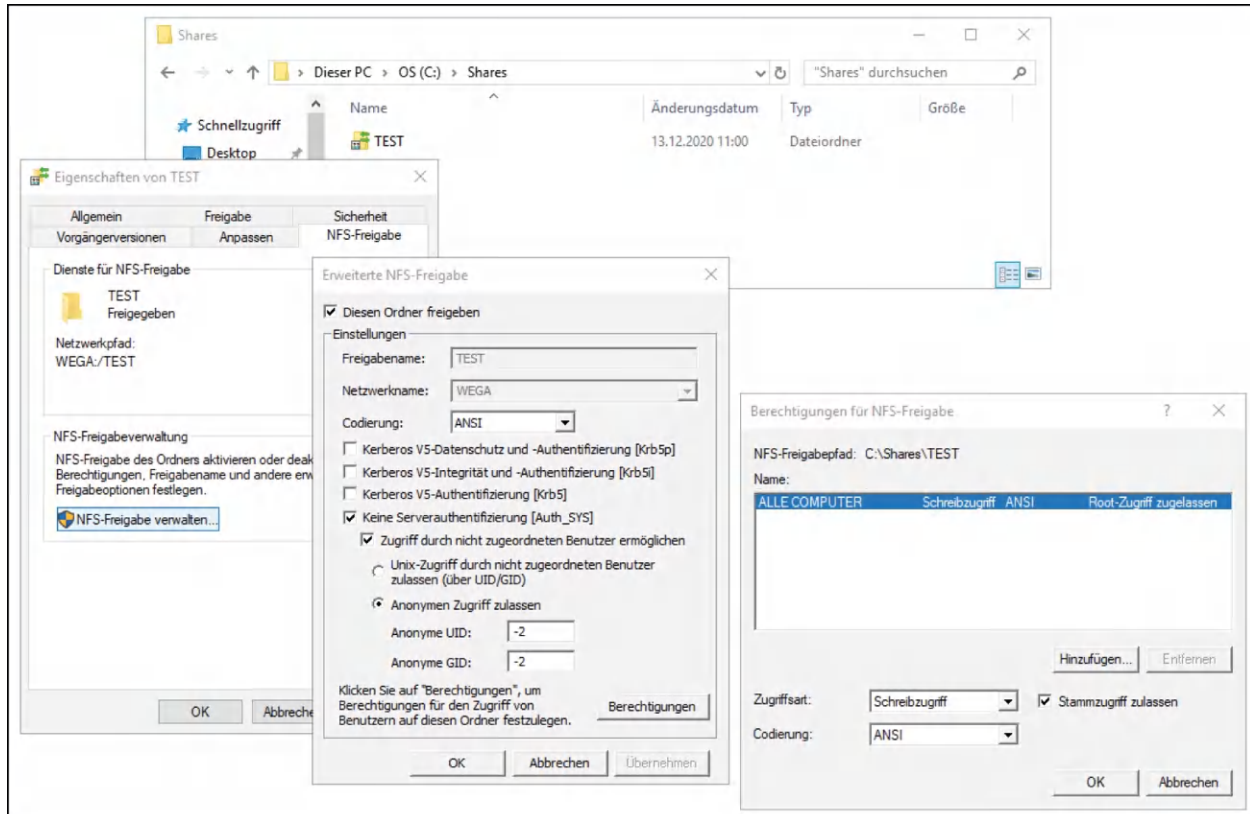


Abbildung 9.9: Die NFS-Freigabe-Verwaltung direkt im Windows Explorer

Freigaben, Datei-Server, Ressourcenmanager

Um mit einem Windows-System Dateien über das Netzwerk bereitzustellen, braucht es an sich keine eigene Rolle. Ein Benutzer kann jederzeit, entsprechende Kenntnis vorausgesetzt, einen Ordner oder ein Laufwerk mit einer Freigabe versehen, zu sehen in [Abbildung 9.10](#). Ist die Freigabe bekannt und besitzt ein Benutzer die entsprechenden Rechte, kann diese Freigabe zum Zugriff auf die Dateien genutzt werden. An dieser Stelle unterscheidet sich ein Windows-Client-Betriebssystem auch

nicht von der Server-Variante. Die Dialogfenster und Funktionen sind identisch.

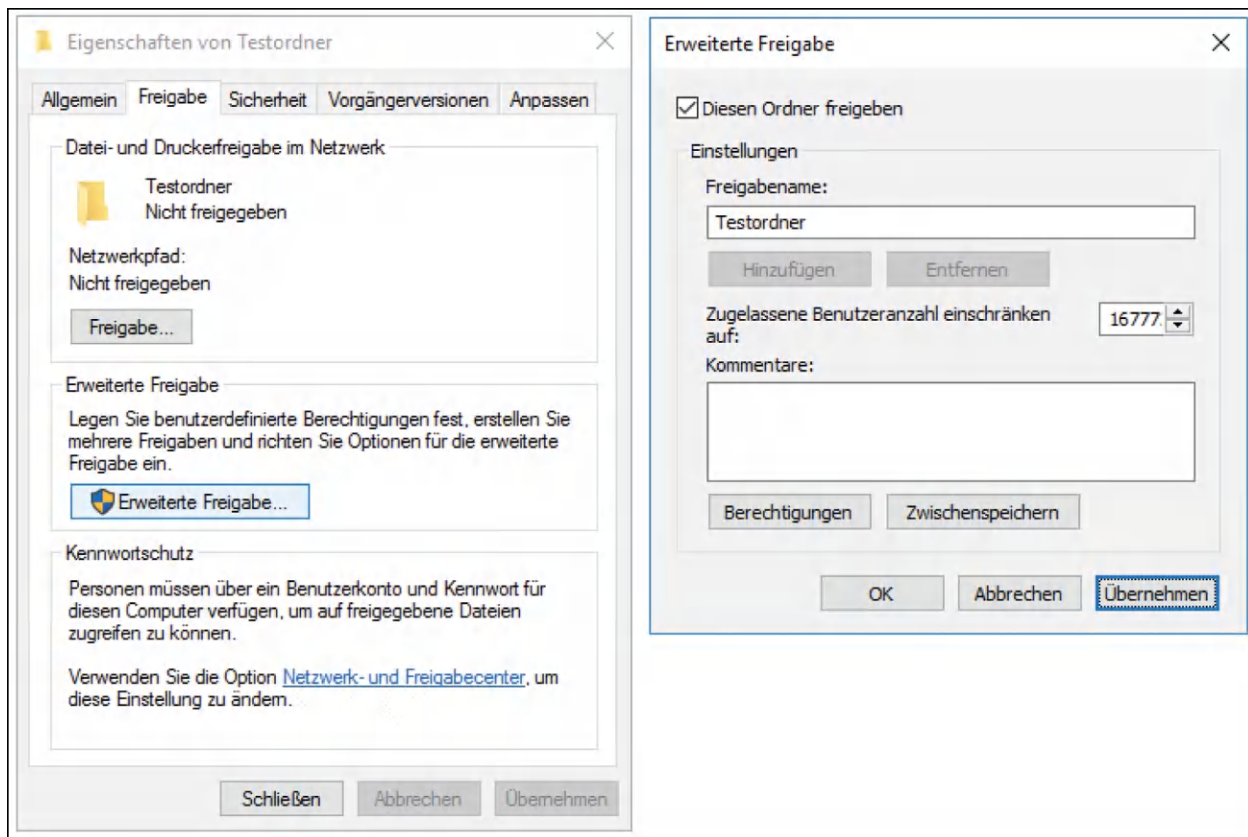


Abbildung 9.10: Die Freigabe von Ordnern und Volumes funktioniert unabhängig von der installierten Datei-Server-Rolle.

Schon zur Freigabe hat der Administrator die Möglichkeit, unterschiedliche Berechtigungen für verschiedene Benutzer oder Benutzerrollen zu definieren.

- ✓ VOLLZUGRIFF: Benutzer können lesen, ändern und Berechtigungen bearbeiten sowie die Kontrolle über Dateien übernehmen
- ✓ ÄNDERN: bedeutet, dass Benutzer Ordner und Dateien innerhalb der Freigabe lesen, ausführen, schreiben oder löschen können
- ✓ LESEN: erlaubt den Benutzern, alle Inhalte des Ordners anzuzeigen



Bei komplexen Freigabestrukturen besteht immer die Gefahr, dass

eine in der Hierarchieebene höher definierte Berechtigung in einer tieferen Ebene zu einer unerwünschten Berechtigung führt.

Auf die Freigabe wirken zudem die NTFS-Rechte ein, sofern der Datenträger nicht mit FAT/FAT32 formatiert wurde. Zu finden ist diese Rechtsteuerung in der Registerkarte SICHERHEIT:

- ✓ VOLLZUGRIFF: erlaubt Benutzern, Dateien und Unterverzeichnisse zu lesen, zu schreiben, zu ändern und zu löschen, verleiht zudem das Recht, Berechtigungseinstellungen anzupassen.
- ✓ ÄNDERN: erlaubt Benutzern, Dateien und Unterverzeichnisse zu lesen und zu schreiben; auch das Löschen des Ordners ist möglich.
- ✓ LESEN, AUSFÜHREN: erlaubt Benutzern, ausführbare Dateien inklusive Skripte anzuzeigen und auszuführen.
- ✓ ORDNERINHALT ANZEIGEN: erlaubt das Anzeigen und Auflisten von Dateien und Unterverzeichnissen sowie das Ausführen von Dateien. Wird nur auf Ordner vererbt.
- ✓ LESEN: erlaubt Benutzern, die Inhalte von Ordnern und Unterverzeichnissen anzuzeigen.
- ✓ SCHREIBEN: erlaubt Benutzern, Dateien und Unterverzeichnisse hinzuzufügen, erlaubt Ihnen, in eine Datei zu schreiben.



And the winner is: Die restriktivste Berechtigung: Im Zusammenspiel von Freigabeberechtigung und der NTFS-Rechtsteuerung gewinnt stets die restriktivste Einstellung. Wer es schlicht und einfach mag, vergibt stets in der Freigabeberechtigung Vollzugriff und schränkt über NTFS-Rechte ein. Da diese eine feinere Steuerung zulassen, stellt dies keine Limitierung dar.

Wir wollen es an dieser Stelle bei dem Thema belassen. Unmengen von Blog-Seiten sind gefüllt mit Empfehlungen und »Best Practices«, wie Freigaben und Rechte im Idealfall zu handeln sind. Die Praxis lehrt jedoch, dass die vielen Varianten nicht umsonst möglich sind – sie werden schlicht gebraucht.

Eine Prüfung der vergebenen Rechte aus der Perspektive eines Benutzers ist – insbesondere in der Einführungsphase neuer Freigaben – eine Pflichtveranstaltung. Nicht selten wird der Administrator feststellen, dass Standardbenutzer über eine **SPEZIELLE BERECHTIGUNG** Dateien ändern und Programme starten können, obwohl das so nicht vorgesehen war. Die Standardeinstellungen eines Domänenmitglied-Servers sind diesbezüglich eher weitreichend, denn limitiert.



NTFS-Sicherheitseinstellungen gelten auch für lokale Benutzer, Freigabeberechtigungen nur für Benutzer, die über das Netzwerk zugreifen!

Nun sind die Ansprüche an einen modernen Datei-Server aber nicht damit abgegolten, dass ein Benutzer über das Netzwerk auf eine Datei zugreifen kann. Möchte der Administrator einen Datei-Server sicher als Cluster betreiben oder wünscht er sich Hilfsmittel, wie beispielsweise die Kontingentverwaltung für den bereitgestellten Speicherplatz, ist die Rolle des Datei-Servers, und sinnvollerweise die des Ressourcenmanagers für Datei-Server, gefragt.

Der Ressourcen-Manager für Datei-Server bietet folgende Funktionen:

- ✓ Kontingentverwaltung, um für einen Ordner oder Volume einen zulässigen Speicherplatz festzulegen
- ✓ Dateiklassifizierung zur dynamischen Zugriffssteuerung oder Dateiverschlüsselung
- ✓ Automatisierte Dateiverwaltungsaufgaben durchführen
- ✓ Speicherberichte erstellen, um Trends bei der Dateiablage zu identifizieren
- ✓ Auf Basis der Dateinamenerweiterung Freigaben einschränken



Der Ressourcen-Manager für Datei-Server unterstützt nur Volumes, die mit dem NTFS-Dateisystem formatiert sind. Das robuste Dateisystem (ReFS) wird nicht unterstützt.

Die Installation der beiden Rollen geschieht, wie gewohnt, grafisch über den SERVER-MANAGER oder per PowerShell-Kommando.

```
Install-WindowsFeature -Name FS-Resource-Manager -  
IncludeManagementTools
```

Das augenfälligste Merkmal nach der Installation, die ein paar Minuten dauern kann, ist die Existenz des Ordners STORAGEREPORTS auf dem System-Laufwerk von Windows und die Erweiterung des Eigenschaftenfensters für ein Verzeichnis um das Register KLASSIFIZIERUNG, während das Eigenschaftenfenster für Volumes zusätzlich eine Erweiterung um KONTINGENT erfuhr.

Mit dem SERVER-MANAGER, im Abschnitt DATEI-/SPEICHERDIENSTE unter FREIGABEN hat der Administrator Zugriff auf die verschiedenen Funktionalitäten, die der Datei-Server bietet, siehe [Abbildung 9.11](#).

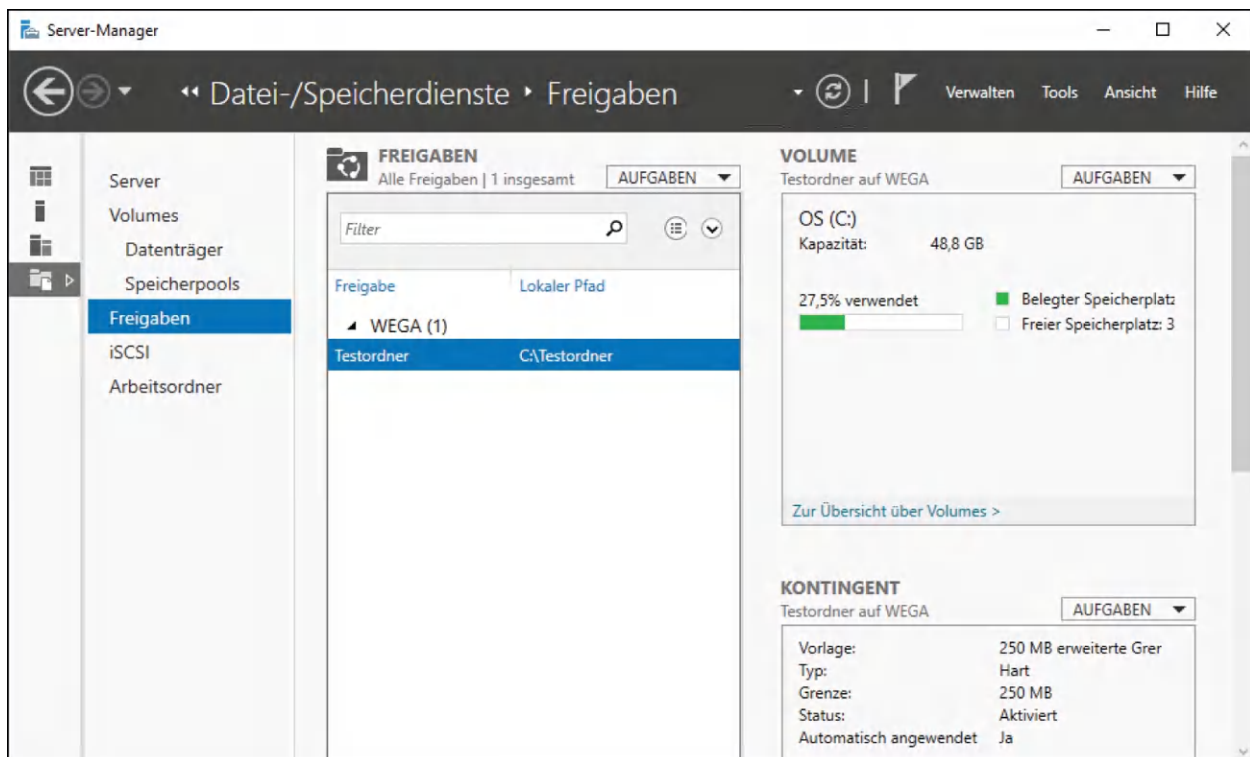


Abbildung 9.11: Der Datei-Server-Dialog erlaubt den Zugriff auf einen Teilbereich der Funktionen des Ressourcenmanagers für Datei-Server.

Wird der Ressourcenmanager nicht installiert, ist zwar das Dialogfenster für Freigaben im Servermanager sichtbar, jedoch sind Funktionen, wie

beispielsweise die Anlage von Freigaben, nur bedingt nutzbar.

Das Hauptprogramm für die Bearbeitung von Datei-Server-Eigenschaften findet der Administrator jedoch unter Tools im Snap-in RESSOURCEN-MANAGER FÜR DATEISERVER. Das Programm gliedert sich in die Teilbereiche:

- ✓ Kontingentverwaltung
- ✓ Dateiprüfungsverwaltung
- ✓ Speicherberichtsverwaltung
- ✓ Klassifizierungsverwaltung
- ✓ Dateiverwaltungsaufgaben

Der Administrator kann sich über Storage-Vorkommnisse per E-Mail informieren lassen. Auch die Speicherberichte, aus denen sich das Wachstum der Datenmengen recht gut ablesen lässt, erlauben einen regelmäßigen Versand. Um die Mail-Funktionen nutzen zu können, gilt es, den SMTP-Server unter ALLGEMEINE OPTIONEN festzulegen.

Die Kontingentverwaltung ist unter Windows denkbar einfach geregelt. Viele verschiedene Kontingentvorlagen, von der kleinen 100-MByte-Grenze über Grenzen mit Limits und Volumenbelegungsüberwachung, sind bereits vorbereitet. Der Administrator muss sie lediglich einem Pfad zuweisen.

Äußerst praktisch ist zum Beispiel die Überwachung von temporären Verzeichnissen, bei denen der Administrator sich eine Information per E-Mail oder Ereignisanzeigeneintrag wünscht, dass ein Kontingent überschritten wurde. Ein hartes Limit, bei dem der Datei-Server die weitere Speicherung unterbinden würde, ist im Zusammenspiel mit Applikationen keine sinnvolle Idee.



Die Kontingentverwaltung von Windows ist beinahe selbsterklärend. Für weitere Details sei auf die Onlinehilfe von Microsoft verwiesen: <https://docs.microsoft.com/de->

de/windows-server/storage/fsrm/quota-management.

Die Dateiprüfungsverwaltung ist eine überaus leistungsfähige Möglichkeit für den Administrator auf die Dateiablagegewohnheiten der Benutzer intelligent einzuwirken. Dank der fünf Vorlagen erklären sich sowohl die Funktion als auch der Einsatzzweck:

- ✓ Audio- und Videodateien bei Speicherung blockieren
- ✓ Ausführbare Dateien blockieren
- ✓ Bilddateien blockieren
- ✓ E-Mail-Dateien blockieren
- ✓ Ausführbare Dateien und Systemdateien überwachen

Die Dateiprüfungsverwaltung kennt den Prüfungstyp *aktiv*, der eine Speicherung beziehungsweise einen Aufruf tatsächlich blockiert, und die *passive* Prüfung, die lediglich eine Protokollierung anstößt. Für beide Prüfungstypen gibt es neben der Benachrichtigung auch die Möglichkeit, zugleich einen Befehlsstart aufzurufen.

Somit haben Administratoren eine recht gute und einfache Möglichkeit, auf das Ablageverhalten ihrer Anwender Einfluss zu nehmen.

Insbesondere Videodateien sind aufgrund ihrer Größe ungeliebte Gäste auf Dateifreigaben. Mit wenigen Mausklicks wird das Speichern verhindert oder der IT-Verantwortliche per Ereignisanzeigeneintrag oder E-Mail darüber informiert, dass etwas Ungewolltes vor sich geht.

Ganz typisch für Windows arbeitet die Erkennung von Dateitypen auf Basis der Dateinamenerweiterung (dem Suffix). In der Grundeinstellung interpretiert die Software alle Dateien mit den Erweiterungen bak, bck, bkf oder old als Sicherungsdateien oder asc, text und txt als Textdateien. Möchten Sie zum Beispiel das noch recht junge »High Efficiency Image Format« (HEIC), wird von Apples iPhone als Speicherformat für Bilder genutzt, ebenfalls aussperren, gehen Sie wie folgt vor:

1. Öffnen Sie unter DATEIPRÜFUNGSVERWALTUNG den Eintrag

DATEIGRUPPEN per Doppelklick.

2. Doppelklick auf die Dateigruppe AUDIO- UND VIDEO.
3. Tragen Sie *.heic unter »Einzuschließende Dateien« ein und klicken Sie auf HINZUFÜGEN.
4. Vorgang mit OK bestätigen.

Unter »Auszuschließende Dateien« könnte der Administrator bestimmte Dateien oder bestimmte Bezeichnungsmuster (zum Beispiel *.img oder *.bmp) wiederum aus der Liste entfernen. Die Ereignisanzeige protokolliert die Aktivitäten der Dateiprüfungen, wie in [Abbildung 9.12](#) zu sehen.

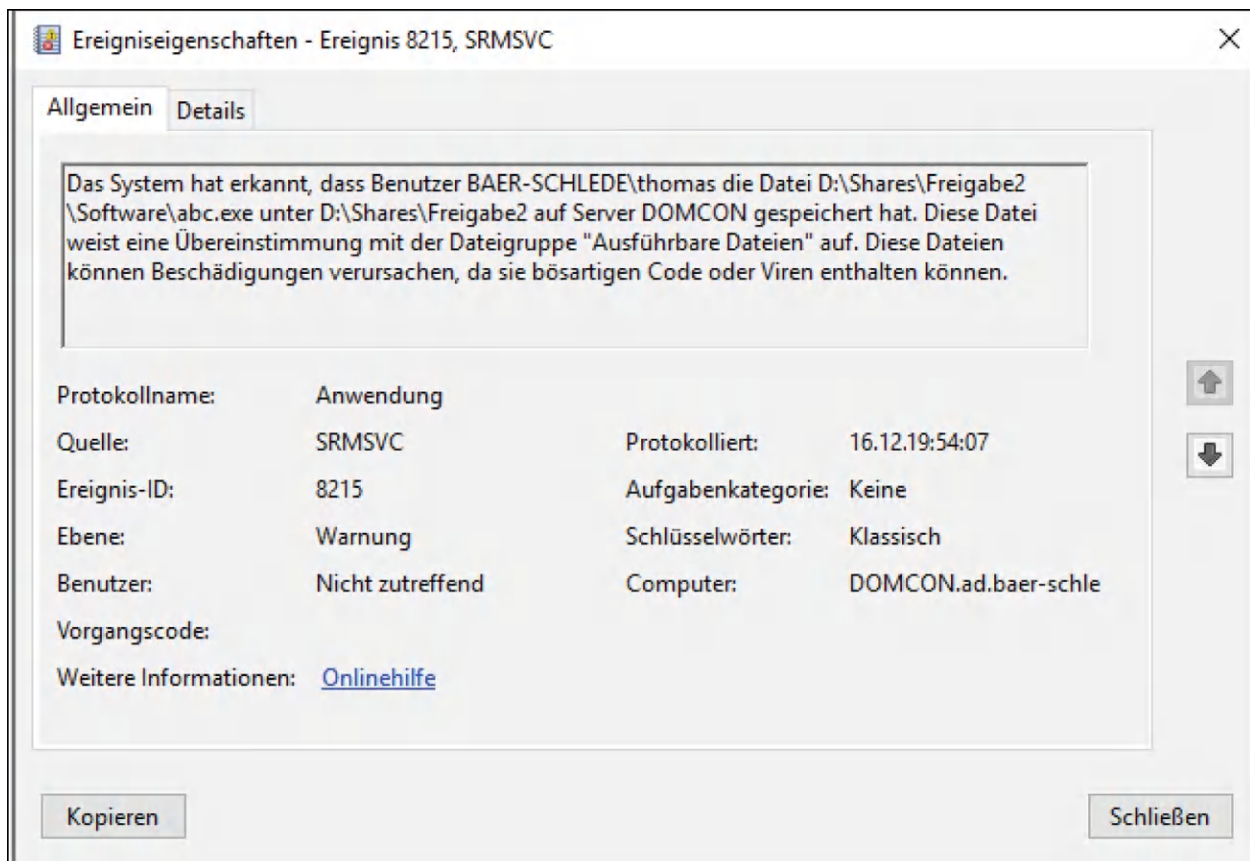


Abbildung 9.12: Je nach Einstellung protokolliert der Server in seiner Ereignisanzeige das Speichern von bestimmten Dateien.

Eine äußerst leistungsfähige Funktion bietet der RESSOURCEN-MANAGER FÜR DATEISERVER von Windows Server im Register

BEFEHL. Tritt ein anvisiertes Ereignis auf, beispielsweise dass eine ausführbare Datei in einem bestimmten Verzeichnis abgespeichert wird, soll der Server eine Aktion ausführen:

C:\Windows\System32\shutdown.exe

Mit den Befehlsargumenten /s /t 0 und der Befehlssicherheit LOKALES SYSTEM würde den Server ohne jegliche Vorwarnung sofort herunterfahren. Zugegeben eine äußerst drastische Reaktion auf ein Dateiereignis, aber es zeigt, wie weit Sie bei den Einstellungsmöglichkeiten gehen könnten. Wäre die Dateiaktion etwa die Anlage von Dateien mit einem außergewöhnlichen Suffix, könnten Sie als Administrator den Server sehr genau darauf reagieren lassen. Zudem gibt es die Option, die Dateiaktionen auf den entfernten Ordner, der als Überwachungsursprung gilt, zur Durchführung zu bringen.

Die Speicherberichtsverwaltung, siehe [Abbildung 9.13](#), ist wiederum eine Funktion, die sich weitgehend von allein erklärt. Über einen Scheduler ist der IT-Profi in der Lage, sich ein regelmäßiges Bild über die Zusammensetzung der Dateien auf dem Server geben zu lassen. Bei Bedarf erlaubt die Software auch die zeitnahe Erstellung eines Berichts, der im Dynamic HTML-, HTML-, XML-, CSV- oder Textformat erstellt wird.



Weitere Informationen zu den Speicherberichten findet der interessierte Leser in den Microsoft Docs unter <https://docs.microsoft.com/de-de/windows-server/storage/fsrm/storage-reports-management>.

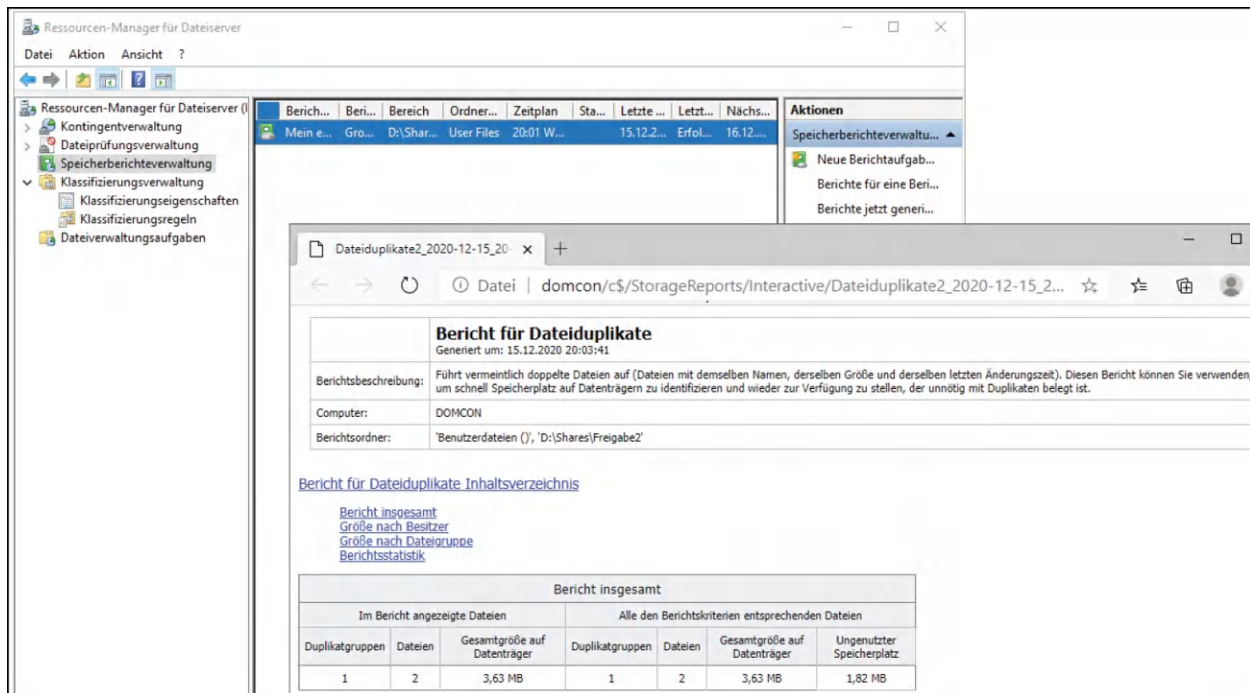


Abbildung 9.13: Die Speicherberichteverwaltung erlaubt die unkomplizierte Erstellung von Ad-hoc-Auswertungen und regelmäßigen Berichten.

Datendeduplizierung

Bei der Deduplizierung handelt es sich in der IT um einen Prozess, der redundante Daten identifiziert und löscht, ehe sie auf einen Datenträger geschrieben werden. So oder in etwa gleichbedeutend lautet die allgemeingültige Definition. Dann müssen wir uns jetzt damit abfinden, dass das identisch benannte Konzept der Firma Microsoft für die Windows-Server ein wenig anders arbeitet.

Die von Microsoft umgesetzte Technik sucht nach identischen Daten auf einem Volume und bietet hierzu vier verschiedene Aufträge an, um die mitunter doppelt vorliegenden Dateien einzusparen. Die hierzu zur Verfügung gestellten Aufträge sind:

- ✓ Der stündliche OPTIMIERUNGSAUFTRAG dedupliziert das gewählte Volume gemäß den Vorgaben des Administrators aus dem Server-Manager
- ✓ Der Auftrag GARBAGE COLLECTION gibt Speicherplatz frei, indem er unnötige Blöcke entfernt. Gibt es Dateien, die vor Kurzem

gelöscht wurden und nicht mehr auf diese Blöcke referenzieren, kann das Betriebssystem diesen Block verwerfen. Diese Aufgabe wird bei Installation automatisch in der Aufgabenplanung angelegt und startet samstags um 02:45.

- ✓ Der Auftrag INTEGRITY SCRUBBING bestimmt Beschädigungen im Blockspeicher aufgrund von Datenträgerfehlern oder fehlerhaften Sektoren – startet üblicherweise eine Stunde nach der Garbage Collection. Sofern möglich, versucht das Programm, beschädigte Dateien wiederherzustellen. Darüber hinaus werden bei der Datendeduplizierung Sicherungskopien häufig verwendeter Blöcke beibehalten, wenn diese in einem als »Hotspot« bezeichneten Bereich mehr als 100 Mal referenziert werden.
- ✓ Der Auftrag UNOPTIMIZATION ist ein bei Bedarf auszuführender Spezialauftrag. Er dient zum Rückgängigmachen der erfolgten Deduplizierung und deaktiviert die Datendeduplizierung auf dem jeweiligen Volume.

Technisch betrachtet handelt es sich bei der Deduplizierung von Microsoft Windows um zwei Dienste:

- ✓ Datendeduplizierungsdienst
- ✓ Datendeduplizierung – Volumenschattenkopie-Dienst

Die zu erwartende Einsparung des Speicherplatzes der Technik, die so etwas wie eine interessante Alternative zur Kompression darstellt, hängt stark davon ab, auf welche Dateien der Dienst im Zuge seiner Arbeit stößt. Die zu erwartende Einsparung ist, laut Hersteller, jedoch beachtlich:

- ✓ Benutzerdokumente 30–50 %
- ✓ Software, CAB, Symboldateien 70–80 %
- ✓ ISO, virtuelle Festplatten 80–95 %
- ✓ sonstige Dateien – allgemeine Dateifreigabe 50–60 %

Die Einsparung auf dem Datei-Server zieht sich, je nach verwendeter

Backup-Software, auch noch auf allen untergeordneten Speichersystemen weiter fort. Insbesondere Administratoren, die mit Hyper-V- und VDI-Konstellationen arbeiten, können durch die Aktivierung der Deduplizierung viel ansonsten erforderlichen Speicherplatz einsparen.

Eine andere typische Zielgruppe ist der Software-Entwickler, der für seine Projekte viele immer weitgehend identische Dateien nutzt, da sich von Version zu Version einer Software doch eher ein geringer Teil ändert, während viele Dateien gleichbleibend sind. Einen solchen Anwendungsfall werden wir uns nun exemplarisch genauer anschauen.



KB4025334 enthält einen Roll-up der Fehlerbehebungen für die Datendeduplizierung, einschließlich wichtiger Korrekturen der Zuverlässigkeit. Wir empfehlen dringend, diese zu installieren, wenn Sie die Datendeduplizierung mit Windows Server 2016 und Windows Server 2019 verwenden.

In der Standardeinstellung greift die Datendeduplizierung erst bei Dateien, auf die der Benutzer seit mehr als drei Tagen nicht mehr zugegriffen hat. Dies zudem nur, sofern die Datei größer als 64 KByte ist. Um sich das Verhalten des Diensts zeitnah anzuschauen, müssen wir diese Werte nun anpassen.

Verwenden Sie zur Installation den SERVER-MANAGER oder das entsprechende PowerShell-Kommando:

```
Install-WindowsFeature -Name FS-Data-Deduplication
```

Anschließend können Sie im SERVER-MANAGER unter DATEI-/SPEICHERDIENSTE im Menü VOLUMES unter DATENTRÄGER die Datendeduplizierung konfigurieren. Die Einrichtung ist Assistenten-gestützt und verlangt die Aktivierung als:

- ✓ Allgemeiner-Datei-Server
- ✓ VDI-Server
- ✓ Virtualisierter Sicherungs-Server

In unserem Fall nutzen wir die erste Option, reduzieren die Altersvorgabe für Dateien auf 0 und legen keine auszuschließenden Dateinamenerweiterungen fest. Neben dem Ausschluss des Dateisuffix besteht die Möglichkeit, einzelne Ordner und Dateien von dem Vorgang auszuschließen.

Auf unserem Test-Server gibt es auf dem Laufwerk E: im Ordner Development ein Projektverzeichnis mit den unterschiedlichen Versionen eines Entwicklungsteams. In jedem Verzeichnis findet sich eine stets identische OVA-Datei mit einer Größe von mehr als 800 MByte.

Üblicherweise startet die Datendeduplizierung vom Scheduler gesteuert, und das Ergebnis würde sich erst in ein paar Stunden zeigen. Wer schneller sehen will, wie sich die Deduplizierung zeigt, startet den Vorgang manuell über ein PowerShell-Kommando (E: ist hier das Ziellaufwerk):

```
Start-DedupJob -Type Optimization -Volume E: -Memory 100 -  
Cores 100  
-Priority High
```

Vor Aktivierung der Datendeduplizierung umfasst der belegte Speicher in unserem Test 11,7 GByte auf dem Laufwerk. Nach Aktivierung sank der Speicherplatzbedarf auf 1,74 GByte (85 %) – ohne dass es für den Anwender einen sichtbaren Unterschied gibt.

Die Datendeduplizierung können Sie auch über die grafische Oberfläche parametrieren. Verwenden Sie hierzu das entsprechende Kommando (siehe [Abbildung 9.14](#)) DATENDEDUPLIZIERUNG KONFIGURIEREN im Kontextmenü über den SERVER-MANAGER | DATEI-SPEICHERDIENSTE | VOLUMES | DATENTRÄGER.

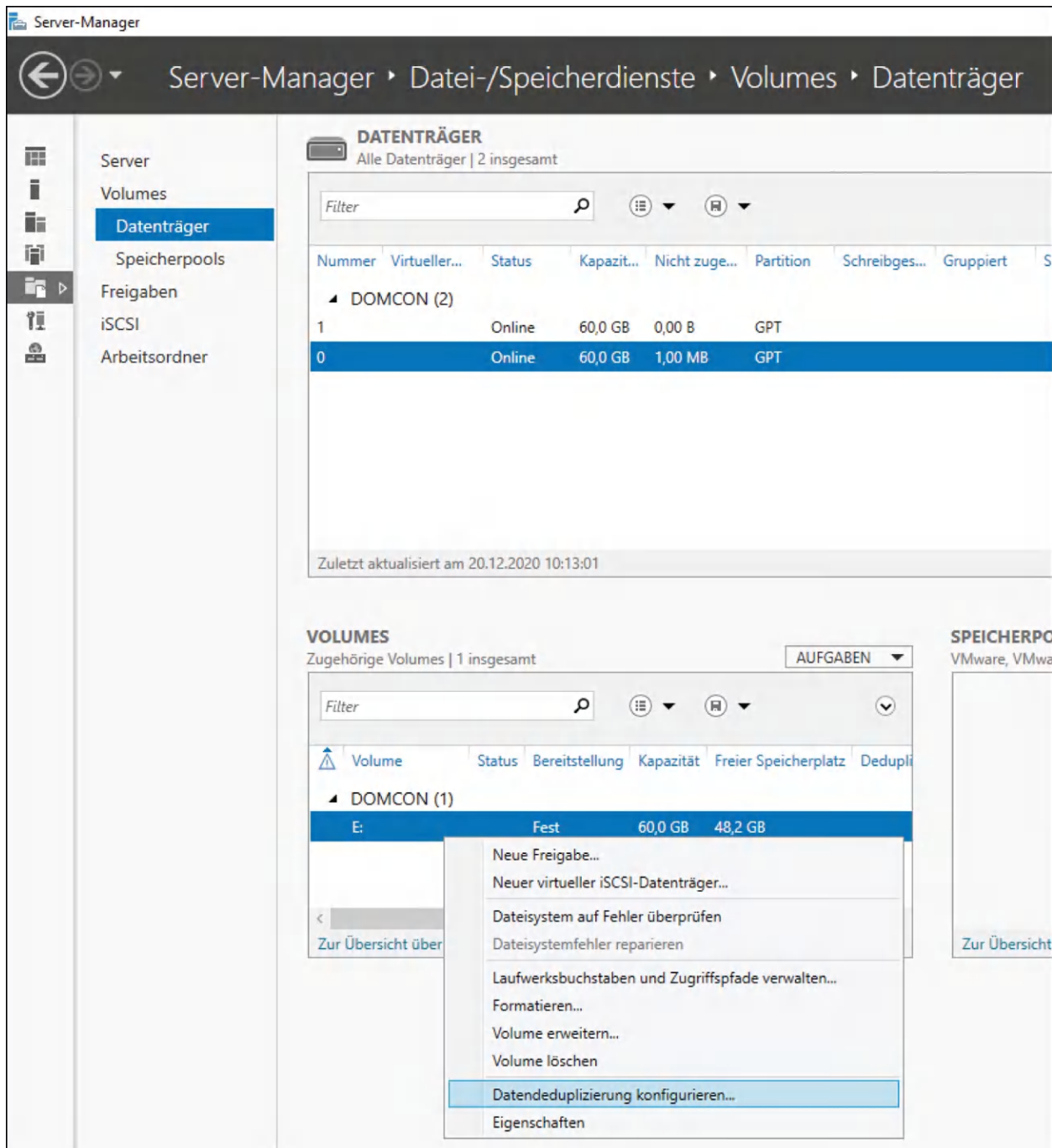


Abbildung 9.14: Die Konfiguration der Datendeduplizierung nimmt der Administrator im Server-Manager vor.

Die Datendeduplizierung unter Windows Server hat noch einige Einschränkungen, auf die wir an dieser Stelle versionsbezogen hinweisen müssen.

- ✓ ReFS wird nur ab Windows Server 2019 unterstützt.

- ✓ Findige Benutzer haben die Server-Binärdateien für die Datendeduplizierung auf Windows-10-PCs übertragen, um die Technik auf dem Client-Betriebssystem zu nutzen. Wir raten dringend von solchen Experimenten ab.
- ✓ Die Datendeduplizierung wird von Windows Search nicht unterstützt. Alle deduplizierten Dateien ignoriert der Suchdienst, daher ist das Ergebnis unvollständig.
- ✓ Die Datendeduplizierung mit Robocopy wird nicht empfohlen, da bestimmte Robocopy-Befehle Blockspeicher beschädigen können. Der Blockspeicher wird im Ordner »System Volume Information« für ein Volume gespeichert. Wenn der Ordner gelöscht wird, werden die optimierten Dateien (Analysepunkte), die aus dem Quellvolume kopiert werden, beschädigt, weil die Datenblöcke nicht auf das Zielvolume kopiert werden.



Weitere Informationen zum Thema Datendeduplizierung finden Sie in den Microsoft Docs unter <https://docs.microsoft.com/de-de/windows-server/storage/data-deduplication/overview>.

DFS-Namespaces

In wachsenden Umgebungen entstehen irgendwann Probleme, an die der IT-Administrator vor wenigen Jahren noch gar nicht gedacht hatte, da alles irgendwie in einem Fluss war. Die kleine Firma mit ihren fünf Angestellten, vier PCs und »dem Server« wuchs, dank wirtschaftlichem Erfolg, »fröhlich« vor sich hin, und irgendwann reicht »der Server« allein nicht mehr aus.

Wie griffen die Benutzer bisher auf »den Server« zu? Meist über eine Freigabe, der ein Laufwerksbuchstabe zugewiesen wurde – ganz im Stil von:

`\\server\daten`

Sofern der IT-Administrator nicht ganz von gestern ist, sollte die nächste

Freigabestruktur auf dem zweiten Server nicht wieder in diesem Schema geschehen. Denn, auch wenn es sich zum gegenwärtigen Zeitpunkt wieder keiner vorstellen kann, es wird wieder Veränderungen geben: neue Server, neue Namen, Speicherung in Cloud-Diensten – wie auch immer. Der grundsätzliche Fehler besteht immer dann, sofern der Server-Name das Ziel der Freigabe ist.



Befreien Sie sich von Server-Namen bei der Bereitstellung von Dateien. Nutzen Sie möglichst zügig DFS-Namespaces. Es erscheint Ihnen jetzt zu viel Aufwand, das zu ändern? Der Aufwand ist in einem halben Jahr nur eins: größer!

DFS-NAMESPACES ist ein Rollen-Dienst in Windows Server, der es dem Administrator ermöglicht, freigegebene Ordner, die sich auf verschiedenen Servern befinden, in einem oder mehreren logisch strukturierten Namespaces zu gruppieren. Das mündet in eine virtuelle Ansicht von freigegebenen Ordnern, in der ein einzelner Pfad zu Dateien führt, die sich auf mehreren Servern befinden können. Sprich: Wir nutzen in der IT unsere liebste Errungenschaft und legen wieder einmal eine neue Abstraktionsschicht um eine Struktur, um auf diese flexibler und dynamischer einwirken zu können.

Praktischerweise gibt es kaum nennenswerte Anforderungen an die DFS-Namespaces. Ein Namespace-Server ist dabei ein Domänen Controller oder Mitglieds-Server, der einen Namespace hostet. Server ab der Version 2008 R2 in der Datacenter- oder Enterprise-Edition oder alle darauffolgenden Windows-Server in jeder Edition sind in der Lage, einen domänenbasierten Namespace bereitzustellen.

In unserem hier skizzierten Beispiel gibt es einen Domänencontroller, der künftig als DFS-Namespace-Server fungieren wird. Zwei Datei-Server stellen Freigaben bereit, die als Namespace für das Unternehmen bereitzustellen sind. Die Freigabe auf dem ersten Datei-Server heißt Projekte, auf dem zweiten Server gibt es die Freigaben Kunden und Management.

Die Installation der DFS-NAMESPACE-Funktion geschieht wie gewohnt

entweder über den SERVER-MANAGER oder durch die Eingabe eines PowerShell-Kommandos:

```
Install-WindowsFeature "FS-DFS-Namespaces", "RSAT-DFS-Mgmt-Con"
```

Nach der Installation entdeckt der Administrator das dazugehörige Verwaltungsprogramm unter TOOLS im DATEI-MANAGER oder im Startmenü unter WINDOWS-VERWALTUNGSPROGRAMME.

Die Anlage eines neuen Namespaces für das hier beschriebene Beispiel ist glücklicherweise recht einfach:

1. Klicken Sie in der DFS-Verwaltung rechts unter AKTIONEN auf NEUER NAMESPACE...
2. Wählen Sie den gewünschten DFS-Namespaces-Server aus, in unserem Beispiel den Domänencontroller.
3. Wählen Sie den Namen für den DFS-Namespaces, in unserem Beispiel *daten*.
4. Es folgt die Festlegung des Namespace-Typs, in unserem Beispiel kommt der domänenbasierte Namespace im Windows-Server-2008-Modus zum Einsatz. Die Vorschau zeigt bereits den Namen *\\Domäne Namespace*.
5. Bestätigen Sie die Eingaben.

Wenn Sie jetzt den oben genannten Pfad über Ausführen als UNC-Adresse eingeben, wird der Windows Explorer einen leeren Ordner zeigen. Im nächsten Schritt geht es nun darum, die bereits bestehenden Freigaben der Datei-Server in diese Struktur einzufügen.

Wählen Sie den gewünschten Namespace in der DFS-Verwaltung (siehe [Abbildung 9.15](#)) aus:

1. Klicken Sie auf NEUER ORDNER...
2. Klicken Sie auf HINZUFÜGEN...
3. Wählen Sie den gewünschten Server, der die Freigabe bereitstellt.
4. Wählen Sie den Ordner aus.

5. Bestätigen Sie den gewünschten Namen und schließen Sie mit OK ab.
6. Öffnen Sie nun erneut den DFS-Namespace, in unserem Beispiel:

`\\ad.baer-schlede.de\daten`

Und die verschiedenen Freigaben der Datei-Server sind gemeinschaftlich in einer Struktur zu sehen. Soll eine Freigabe künftig von einem Server auf eine andere Maschine verlagert werden, geht diese Anpassung ohne weitreichende Änderung für die Benutzer einher.

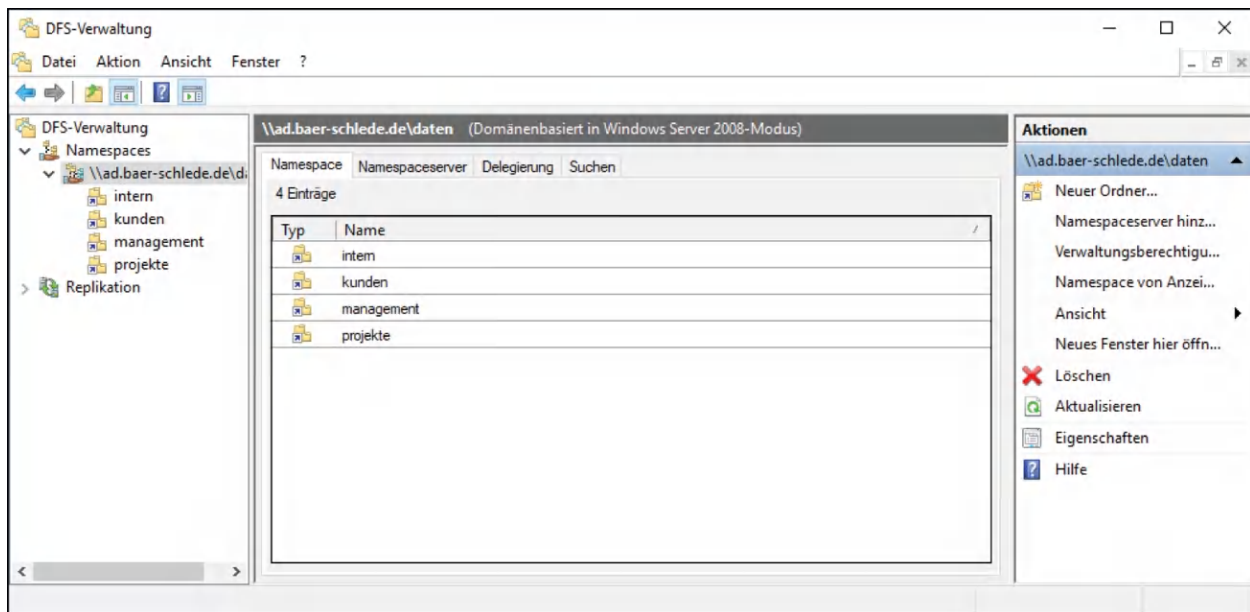


Abbildung 9.15: DFS-Namespaces erlauben eine Freigabebereitstellung, ohne aus den Server-Namen selbst zu referenzieren.



Weitere Informationen zum Thema DFS-Namespaces finden Sie in den Microsoft Docs unter <https://docs.microsoft.com/de-de/windows-server/storage/dfs-namespaces/dfs-overview>.

DFS-Replikation

Bei der DFS-Replikation handelt es sich um eine sogenannte »Multimaster-Replikation«, die die Synchronisierung von Ordnern auf mehrere Server im LAN oder WAN erlaubt. Hierbei kopiert Windows

nicht »stumpf« die komplette Datei zwischen den Orten, sondern nutzt das RDC-(Remote-Differential-Compression-)Protokoll, um nur die veränderten Bereiche einer Datei zu übertragen. Spannend: Der Administrator kann die DFS-Replikation gemeinsam mit dem DNS-Namespace nutzen, kann sie aber auch getrennt voneinander betreiben. Gemeinschaftlich ist in jedem Fall das Verwaltungsprogramm. Auf allen beteiligten Servern muss der DFS-Replikationsdienst installiert sein.

Das DFS-R wurde mit dem Erscheinen des Windows Server 2012 R2 deutlich leistungsfähiger und erlaubt bis zu 70 Millionen Dateien pro Volume und die Replikation von bis zu 100 TByte in der Gesamtheit. Die maximale Dateigröße liegt bei 250 GByte. Nach diversen Aussagen von Anwendern in den Internetforen ist in der Praxis die Replikation solch großer Dateien nicht erfolgreich.

Über die Bandbreiten- und Zeitplansteuerung kann der Administrator auf das Replikationsgeschehen sehr genau Einfluss nehmen. Je nachdem, wie in der Firma gearbeitet wird, lässt sich über diese Technik in den weniger geschäftigen Zeiten eine weitgehend automatische Übertragung von Dateien zwischen Standorten realisieren.

In unserem hier beschriebenen Beispiel soll eine Replikation einer Freigabe mit Namen Development des Domänencontrollers auf einen Datei-Server erfolgen. Ziel dieser Replikation ist die zentrale Sicherung an einem Ort. Hierbei ist Ihnen der Konfigurationsassistent behilflich, wählen Sie in den erscheinenden Dialogfenstern die hier genannten Optionen. Zuvor ist auf beiden beteiligten Servern der Dienst DFS-REPLIKATION einzurichten.

1. In der DFS-VERWALTUNG auf dem Domänencontroller (siehe [Abbildung 9.16](#)) wird eine neue Replikationsgruppe mit einem beliebigen *Namen* angelegt.
2. Als Typ kommt die MEHRZWECKREPLIKATIONSGRUPPE zum Einsatz.
3. Beide Server sind als MITGLIEDER ausgewählt.
4. Topologie VOLLSTÄNDIG VERMASCHTES NETZ.

5. Replikationszeitplan FORTWÄHREND mit VOLLSTÄNDIGER BANDBREITE.
6. Das primäre Mitglied ist in diesem Beispiel der Domänencontroller.
7. Der zu replizierende Ordner ist in unserem Beispiel die Freigabe *Development*.
8. Auf dem Datei-Server geben Sie den lokalen Pfad als Mitgliedspfad an.

Nun heißt es noch, je nach Größe des Ordners, ein wenig abwarten, und anschließend ist das Replikationsergebnis auf dem anderen Server sichtbar. Da es sich um eine Replikation handelt, können Benutzer in beiden Verzeichnissen Änderungen vornehmen. Die letzte Änderung wird auf das jeweilige Replikationsziel übertragen.

Somit handelt es sich beim Windows DFS-R nicht um eine Echtzeitreplikation, da der Inhalt erst beim Schließen der Datei übertragen wird. Im Zweifelsfall löscht der Dienst eine der beiden Änderungen, sofern auf beiden Seiten Änderungen vorgenommen werden. Insgesamt ist das System weniger für den Echtzugriff vorgesehen als für Datensammlungen oder Vorlagen. Das Verhalten steuert der Administrator über die Replikationszeitpläne.

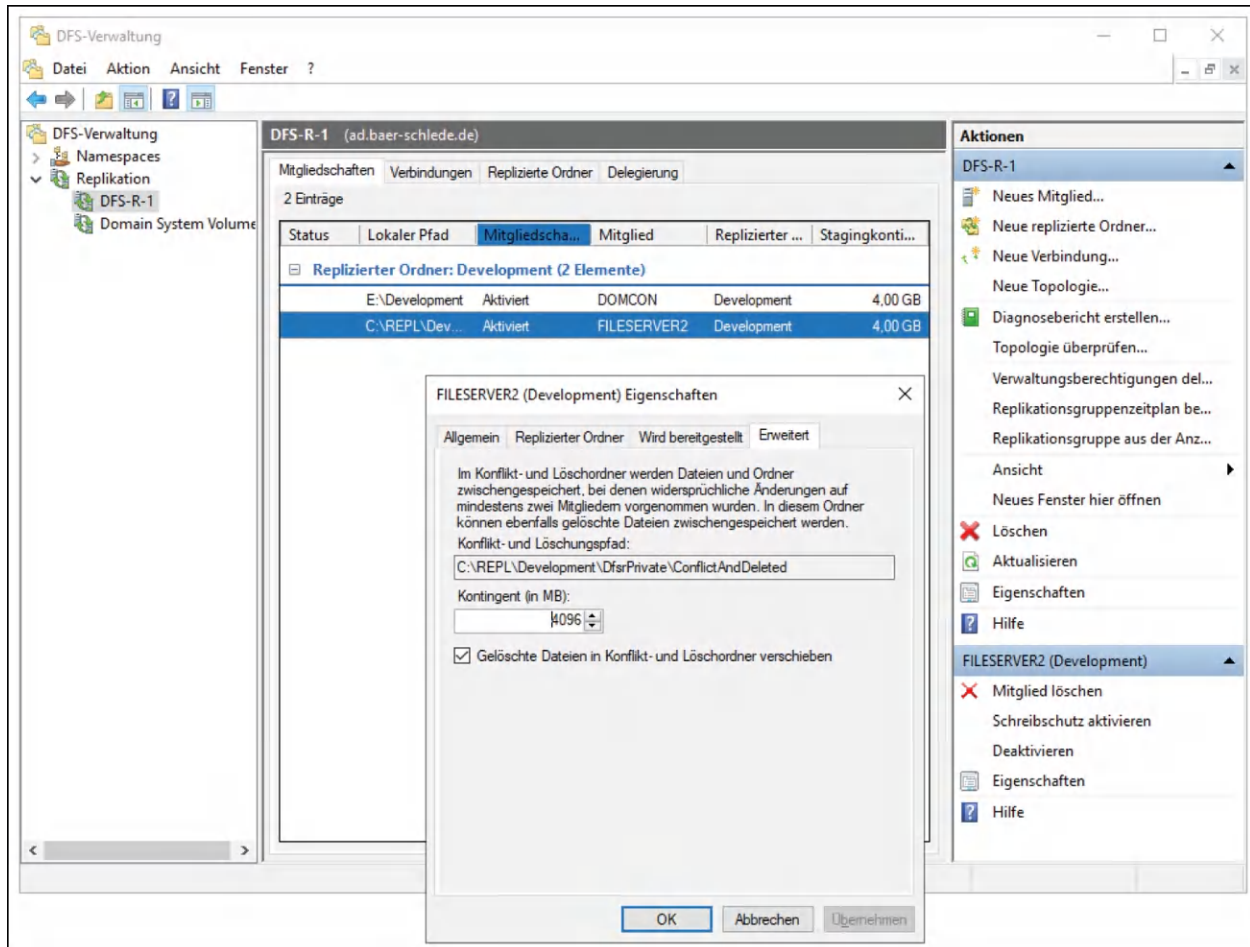


Abbildung 9.16: Der Windows-Replikationsdienst DFS-R eignet sich für eher statische Inhalte als für häufig verwendete Arbeitsdokumente.



Weitere Informationen zum Thema DFS-R finden Sie in den Microsoft Docs unter <https://docs.microsoft.com/de-de/windows-server/storage/dfs-replication/dfsr-overview>.

Grundlagen zu BranchCache für Datei-Server

BranchCache ist eine von Microsoft bereitgestellte Technologie zur Optimierung der Bandbreite in einem WAN (Wide Area Network). Erstmals vorgestellt wurde BranchCache mit dem Windows Server 2008R2 und dem dazu passenden Client-Betriebssystem Windows 7. Mit

jeder neuen Windows-Version steigert der Hersteller den Leistungsumfang von BranchCache. Die Entwicklung ist kaum verwunderlich, wird sie doch in allen Varianten mit Cloud-Verknüpfung dringend benötigt.

Um die WAN-Bandbreite zu optimieren, wenn Benutzer auf Inhalte von Remote-Servern zugreifen, ruft BranchCache Informationen von Inhaltsdaten-Servern (Datei-Server, Anwendungs-Server oder Webserver) in der Hauptniederlassung oder gehosteten Cloud-Inhalts-Servern ab und speichert sie an Filialstandorten zwischen, sodass Client-Computer in Filialen lokal und nicht über das WAN auf diese Inhalte zugreifen können.

In den Zweigstellen fungieren Server oder auch Client-Computer als Caches. Nachdem ein Client-Computer Inhalte aus der Zentrale abgerufen und empfangen hat und die Inhalte in der Filiale zwischengespeichert wurden, können andere Computer in derselben Filiale lokal auf diese Inhalte zugreifen, anstatt diese noch einmal die WAN-Verbindung vom Inhalts-Server herunterzuladen.

Um sicherzustellen, dass die im lokalen Cache vorgehaltenen Daten auch noch dem Original auf dem Inhaltsdaten-Server entsprechen, berechnen die beteiligten Server und Client-Systeme Hash-Werte. Diese sind im Vergleich zu den kompletten Datenblöcken sehr klein und können Computern auch bei leistungsschwächeren WAN-Verbindungen zügig übermitteln.

Die BranchCache-Technik bietet somit grundsätzlich die Möglichkeit,

- ✓ die Antwortzeiten zu beschleunigen,
- ✓ den Datenverkehr zu reduzieren und
- ✓ die Produktivität zu erhöhen.

Microsoft nutzt das Wort Inhaltsdaten-Server für Anwendungs-, Web- und Datei-Server im Zusammenhang mit dem BranchCache-Modul.

Grundsätzlich unterscheiden IT-Profis zwei unterschiedliche Betriebsmodi:

- ✓ Verteilter Cache: In diesem Modus laden Zweigstellen Client-

Computer Inhalte von den Inhalts-Servern in der Hauptniederlassung oder aus der Cloud herunter und speichern den Inhalt für andere Computer in derselben Zweigstelle zwischen. Für den Modus für verteilte Caches ist in der Zweigstelle kein eigener Windows-Server erforderlich.

- ✓ **Gehostete Caches:** In diesem Modus laden Client-PCs in den Zweigstellen aus der Hauptniederlassung oder der Cloud herunter. Gleichzeitig kommt ein gehosteter Cache-Server zum Einsatz, der Daten zwischenspeichert und für andere Client-Computer bereitstellt.



Um BranchCache-Technik mit Windows 10 nutzen zu können, ist zum Zeitpunkt der Manuskripterstellung Windows 10 Enterprise beziehungsweise Education erforderlich. Windows 10 Professional ist nicht geeignet, ebenso die einfachere Home-Edition.

Aufgrund der Einschränkungen bei den Betriebssystem-Edition dürfte der Einsatz in vielen Umgebungen kaum sinnvoll sein. Zumindest alle Computer in der Zweigstelle sind somit mit einer höherwertigen Windows-Client-Version auszustatten.



Weitere Informationen zum Thema BranchCache und BranchCache für Datei-Server finden Sie in den Microsoft Docs unter <https://docs.microsoft.com/de-de/windows-server/networking/branchcache/deploy/deploy-branchcache>.

Grundlagen zu Arbeitsordnern

Bisher war es in Windows-Netzwerken zumeist erforderlich, über einen Computer mit Domänenmitgliedschaft zu verfügen, um am Austausch von Dateien effektiv teilhaben zu können. Mit dem Aufkommen der SharePoint- und Cloud-Technik, aber auch der BYOD-(Bring-Your-Own-Devices-)Initiativen veränderte sich das Anforderungsprofil für Client-Systeme.

Neben Windows-Client-Computern nutzen Anwender zunehmend mobile

Geräte mit Apple IOS oder Google Android. Mit Arbeitsordnern erhalten Benutzer einen komfortablen Ort, um Arbeitsdateien zu speichern und von beliebigem Ort aus darauf zuzugreifen. Organisationen behalten dennoch die Kontrolle über Unternehmensdaten durch Speichern der Dateien auf zentral verwalteten Datei-Servern und der optionalen Festlegung von Benutzerrichtlinien für Geräte bezüglich der Verschlüsselung und oder der Sperrbildschirm-Kennwörter.

Arbeitsordner können Administratoren gemeinsam mit Freigabe, Basisordner, Ordnerumleitungen oder Offlinedateien bereitstellen. Die sogenannte Synchronisationsfreigabe verweist auch auf bereits vorhandene Benutzerdaten, sodass eine Inbetriebnahme möglich ist, auch ohne Server oder Daten im Vorfeld migrieren zu müssen.



Die Inbetriebnahme von Arbeitsordnern erfordert fundierte Kenntnis von vielen Teilbereichen wie

- ✓ Arbeitsordner selbst
- ✓ SSL-Zertifikate
- ✓ Active-Directory-Domänendienste
- ✓ IIS (Internet Information Server)
- ✓ Internet-Proxy-Dienste

Aufgrund der eher hohen Hürden und der Tatsache, dass die funktionelle Inbetriebnahme der Arbeitsordner in diesem Buch rund 100 Seiten an Umfang verschlingen würde, belassen wir es bei einer Link-Empfehlung für den angehenden »Windows-Großadministrator«.



Weitere Informationen zum Thema Arbeitsordner finden Sie in den Microsoft Docs unter <https://docs.microsoft.com/de-de/windows-server/storage/work-folders/work-folders-overview>.

Kapitel 10

Erweiterte Ressourcenfreigaben

IN DIESEM KAPITEL

Versteckte und administrative Freigaben
Dateifreigaben organisieren und ABE
Dynamic Access Control (DAC)
Prüfung des effektiven Zugriffs von Freigaben

In den [Kapiteln 7, 9 und 13](#) beschäftigt sich dieses Buch mit den verschiedenen Details zu den verschiedenen Rollen und Features von Windows Server, darunter auch die Datei- und Druckdienste. In diesem Kapitel geht es ganz schlicht um die bewusste Bereitstellung von Ressourcen und um Tricks rund um Freigaben, die von Haus aus schon auf jedem Windows-Server in einer Domäne zum Einsatz kommen.

Versteckte und administrative Freigaben

Es gibt seit den frühen Jahren von Windows die Möglichkeit, Freigaben vor den überaus neugierigen Blicken der Benutzer zu verstecken. Was die Menschen nicht sehen, klicken sie in der Regel nicht an, und macht sie auch nicht neugierig darauf, was wohl in einem Verzeichnis vor ihnen verborgen ist. Ganz frei nach dem Motto »was ich nicht weiß...«.

Und es ist tatsächlich so, dass Server- und Client-Computer in einer Windows-Domäne weit mehr zur Verfügung stellen, als es den meisten Administratoren lieb sein dürfte. Öffnen Sie auf einem Domänencontroller oder auf einem administrativen PC einmal den Windows Explorer, wählen

Sie in der Baumstruktur den Eintrag NETZWERK, und das Betriebssystem listet eine mehr oder weniger umfangreiche Anzahl von Computern auf, die in der Umgebung identifiziert werden konnten – siehe [Abbildung 10.1](#).

Durch einen Doppelklick auf einen der Computernamen können Sie sehen, welche Ressourcen die Maschine im Netzwerk freigibt. Hierbei handelt es sich in der Regel um Dateiordnerfreigaben oder um Druckerfreigaben.

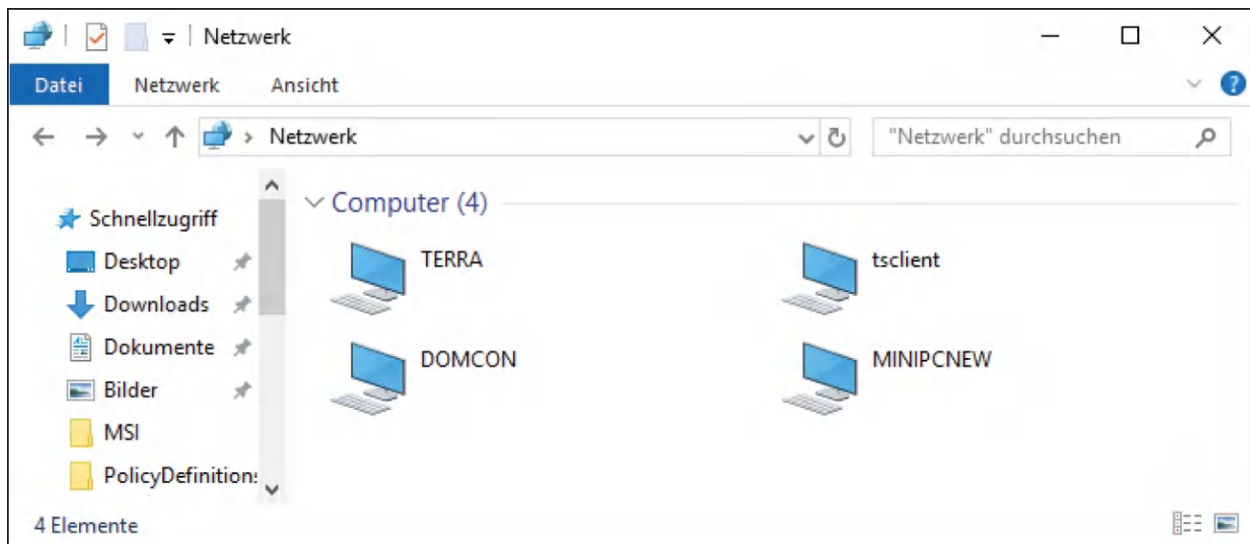


Abbildung 10.1: PCs in der Netzwerkkumgebung von Windows



Sollte Ihnen auffallen, dass PCs in dieser Netzwerkansicht fehlen, obwohl sie eingeschaltet sind, stellen Sie sicher, dass der Dienst FUNKTIONSSUCHE-RESSOURCENVERÖFFENTLICHUNG auf den Systemen eingeschaltet ist.

Aus der Liste der in dem Fenster angezeigten Computer sollten Sie sich nun exemplarisch einen Standardarbeitsplatz auswählen und über die Befehlsfolge START AUSFÜHREN einen UNC-Pfad mit dem PC-Namen gefolgt von \c\$ eingeben, beispielsweise:

\\w10clients2\c\$

Interessanterweise haben Sie nun Zugriff auf die Partition mit dem Buchstaben C auf dem entfernten Computer. Es handelt sich hierbei um

eine administrative Freigabe, die Windows standardmäßig für jede Partition anlegt und stets um das Dollarzeichen ergänzt wird.

Das Dollarzeichen sorgt dafür, dass die Freigabe in normalen Ansichten unterdrückt wird – niemand sieht auf Anhieb diese Freigabe, nicht einmal der Administrator. Zugriff auf diese administrative Freigabe haben Administratoren. Würden Sie den Vorgang andersherum wiederholen, also mit Standardbenutzerrechten von einer Workstation auf einen Server gerichtet, bekommen Sie (hoffentlich) die Warnmeldung, dass Sie Netzwerkanmeldeinformationen eingeben müssen, da der Zugriff verweigert wurde.



Die Nichtsichtbarkeit von Freigaben ist eine organisatorische Hilfestellung. Die Rechtestruktur greift dennoch.

Unsichtbare Freigaben anzulegen, ist sehr einfach:

1. Wählen Sie einen gewünschten Ordner, den Sie freigeben möchten, im Windows Explorer.
2. Klicken Sie mit der rechten Maustaste auf den Ordner.
3. Wählen Sie den Befehl EIGENSCHAFTEN aus dem Kontextmenü.
4. Wählen Sie das Register FREIGABE aus.
5. Klicken Sie die Option DIESEN ORDNER FREIGEBEN an.
6. Legen Sie einen Freigabenamen fest und ergänzen Sie diesen durch ein Dollarzeichen.
7. Bestätigen Sie die Anlage durch einen Klick auf OK.

Sie können sich, die passenden Rechte vorausgesetzt, nun auf diese Freigabe direkt verbinden. Wie bereits erwähnt, eignet sich die Unsichtbarkeit der Freigabe nicht wirklich als Schutzfunktion. Jeder Benutzer ist in der Lage, über die Anzeige der freigegebenen Ordner sich auch die versteckten Freigaben auf ihrem System anzeigen zu lassen (siehe [Abbildung 10.2](#)).

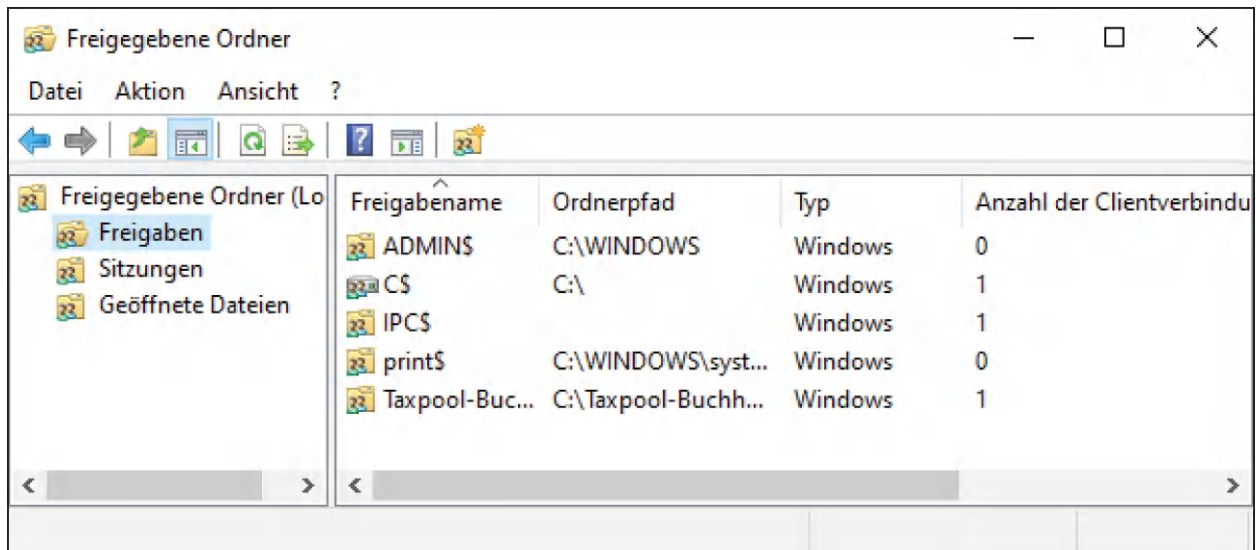


Abbildung 10.2: Auflistung aller Freigaben auf dem PC

Sie starten das Programm am einfachsten über:

1. - und die -Taste gleichzeitig drücken; ab Windows Server 2012 können Sie einfach die -Taste drücken und mit der Eingabe des gewünschten Befehlsteils beginnen.
2. `fsmgmt.msc` eingeben und mit der bestätigen.

Eine weitere Variante, alle Freigaben auf einen Blick zur Ansicht zu bringen, ist der Befehl `net share` in der Eingabeaufforderung. Recht auffällig sind neben der nun bereits bekannten Freigabe `c$` weitere Angaben, und zwar `ADMIN$`, `Print$` und `IPC$`.



Die Freigabe `IPC$` und die damit verbundene, sogenannte Null-Session, ist unter Windows für die Zusammenarbeit der Systeme erforderlich. Diese Sitzung erlaubt auch anonymen Benutzern die Durchführung einiger Aktivitäten, wie beispielsweise die Abfrage nach Freigaben oder das Auflisten von Domänenkonten.

Die `IPC$`-Freigabe wird automatisch von einem Windows-Dienst erstellt und bietet zudem sogenannte »Pipes«, hierbei handelt es sich um direkte Prozesskommunikation über das Netzwerk. Bei dieser Verbindung ist wiederum sichergestellt, dass nur berechtigte Konten

und Gruppen über diese »Inter-Process-Communication« Daten austauschen.

Die für Administratoren bekannteste »Named Pipe« existiert beim SQL-Server-Zugriff.

Mit der Freigabe IPC\$ können Sie im täglichen Praxiseinsatz als Administrator nichts unternehmen. Hingegen ist die von Windows angelegte Standardfreigabe Admin\$ äußerst hilfreich. Der Installer von Windows erzeugt diese Freigabe mit dem Ziel %SYSTEMROOT%\Windows-Verzeichnis. Neben der Freigabe selbst stellt der Installer zudem sicher, dass Administratoren Zugriff erlangen. Viele Endpoint-Management-Programme arbeiten über diese Freigabe, um Software-Verteilungsaufgaben durchzuführen.

Eine administrative und gleichzeitig versteckte Freigabe gibt es noch: print\$. Hier befinden sich die Treiberdateien für freigegebene Drucker und einige Farbprofile. Das ist quasi die technische Dateibasis für das »Point and Print« von Microsoft. Der Benutzer muss somit keine Treiberdatei vorhalten, damit Windows den Treiber direkt installieren kann.

Dateifreigaben organisieren

Das Freigeben von Verzeichnissen ist unter Windows über vielerlei Arten möglich und führt letztendlich immer zum selben Ziel. Und da es so schön einfach ist, kommt es rasch zu einem »Durcheinander«. Aus diesem Grunde empfiehlt es sich für den Administrator, frühzeitig in eine konzeptionelle Planung zu gehen: Wie soll die Freigabestruktur in unserer Domäne aussehen?

Ein Falsch oder Richtig gibt es auch hier nicht – bedeutend ist, dass es ein Konzept ist, dass dem Administrator die Ableitung von Regeln ermöglicht. Ein typischer Klassiker ist dabei eine Freigabe mit den Namen »Daten«, in dieser finden sich die Ordner für Nutzer und Abteilungen.

Im Ordner »Nutzer« wiederum gibt es Freigaben, die der Benutzer als Unterordner anschließend freigibt, um anderen den Querzugriff zu

ermöglichen. Im Ordner »Abteilungen« sind die Ordner und Dateien zusammengefasst, auf die die ganze Abteilung, gesteuert über Gruppenmitgliedschaften, Zugriff hat. Wichtig ist für den Administrator: Der gemeinsame Startpunkt ist die übergeordnete Freigabe »Daten«, die sich recht gut in ein Backup einfügt.



Bei der Planung von Berechtigungen sollten Sie als Administrator nicht Ihren Fokus auf die Zuweisung legen, sondern auf die Fragestellung, wie Sie die Berechtigung bei Bedarf wieder entziehen können.

Laufwerkfreigabe per Gruppenrichtlinie zuordnen

In den meisten Domänen verwenden Administratoren Gruppenrichtlinien, um Laufwerkzugriffe bereitzustellen. Die Zuweisung der GPOs zu Gruppenrichtlinien und die WMI-Filterfunktionen erlauben eine flexible und dynamische Zuordnung. Die Variante mit dem Anmeldeskript ist weitgehend aus der Mode gekommen – hier fehlen einfach die Möglichkeiten der Fehlerauswertungen.

In diesem Beispiel gibt es eine DFS-Freigabe, die auf den Laufwerksbuchstaben M für alle Benutzer zuzuweisen ist. Ein WMI-Filter sorgt dafür, dass die Laufwerkzuordnung nicht für Domänencontroller gilt. Praktischerweise sorgen vielen Administratoren dafür, dass ihre administrativen Benutzer ebenfalls keine Laufwerkzuordnung erhalten.

So erstellen Sie eine Laufwerksbuchstabenzuordnung:

1. Starten Sie auf dem Domänencontroller den SERVER-MANAGER.
2. Klicken Sie im Menü auf den Befehl TOOLS.
3. Wählen Sie die GRUPPENRICHTLINIENVERWALTUNG.
4. Wählen Sie in der Baumstruktur die gewünschte Gruppenrichtlinie mit der rechten Maustaste, wählen Sie den Befehl BEARBEITEN aus dem Kontextmenü.
5. Klicken Sie im Gruppenrichtlinien-Editor auf BENUTZERKONFIGURATION.

6. Wählen Sie den Zweig EINSTELLUNGEN und anschließend WINDOWS-EINSTELLUNGEN.
7. Wählen Sie in der Baumstruktur den Eintrag LAUFWERKSZUORDNUNG.
8. Klicken Sie mit der rechten Maustaste in den Detailbereich des Fensters und wählen Sie den Befehl NEU aus dem Kontextmenü und anschließen das Kommando ZUGEORDNETES LAUFWERK.
9. Füllen Sie das Fenster gemäß Ihren Vorstellungen aus – als Aktion empfiehlt sich stets »Aktualisieren« – siehe [Abbildung 10.3](#).

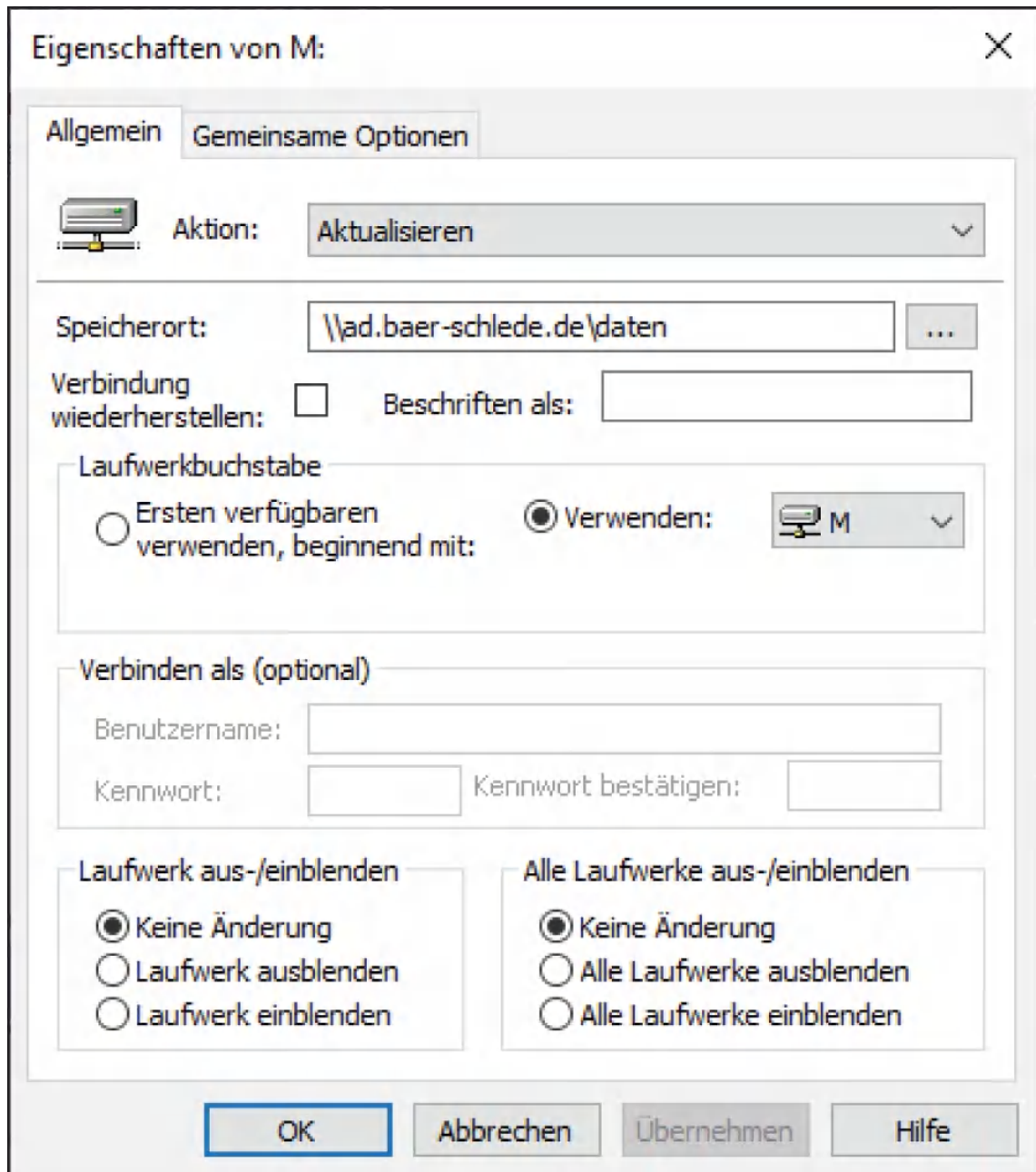


Abbildung 10.3: Laufwerkzuordnung per Gruppenrichtlinie

10. Bestätigen Sie die Eingabe durch OK.
11. Melden Sie sich zum Prüfen als Benutzer an einem Client-PC an. Sie sollten das Laufwerk zugewiesen bekommen.

Lassen Sie sich nicht ausschließen

Es gibt eine Eigenheit in Microsoft Windows, die auf den ersten Blick gar

nicht auffällt. Sofern Ihre Benutzer in der von Ihnen betreuten Umgebung nicht gerade IT-Erfahrene sind, wird aller Wahrscheinlichkeit nach gar nichts passieren.

Sofern Sie alle Freigaben mit den Standardeinstellungen von Windows bereitstellen, ist der erstellende Benutzer häufig in der Lage, Sie komplett auszusperren. Schon bei der Neuinstallation eines Fileservers ist es empfehlenswert, als Erstes den ERSTELLER-BESITZER zu entfernen oder zumindest anzupassen.

Dieser Vorlagenbenutzer bewirkt, dass die Person, die ein Dokument erstellt, auch der Besitzer wird und automatisch Vollzugriffsrechte auf diese Dateien oder Ordner erhält. In diesem Fall könnte der Ersteller auch Berechtigungen vergeben oder verweigern mit dem Ergebnis, dass Administratoren oder der Backup-User nicht mehr auf Dateien oder ganze Verzeichnisse zugreifen kann.

Die Empfehlung für die Anlage bei Freigaben lautet insgesamt:

- ✓ Verwenden Sie anstelle der Berechtigung »Jeder« auf der obersten Ebene der Freigabe zumindest »Authentifizierte Benutzer«, besser »Domänen-Benutzer« oder direkt die Abteilungsgruppen.
- ✓ Verzichten Sie auf die früher propagierte Berechtigungseinstellung VOLLZUGRIFF und nutzen Sie besser ÄNDERN.
- ✓ Entfernen Sie den ERSTELLER-BESITZER aus den erweiterten Sicherheitseinstellungen (siehe [Abbildung 10.4](#)).

Im Idealfall stellen Sie sicher, dass Freigaben so angelegt sind, dass möglichst keine Freigaben innerhalb der anderen Freigaben entstehen. Eine Verschachtelung der Freigaben hätte zur Folge, dass Benutzer möglicherweise in einer »tieferen Ebene« an Zugriffsrechte gelangen. Eine solche Maßnahme dient der Transparenz in der von Ihnen betreuten Umgebung.



Der Kerberos Token kann maximal 1024 SIDs (Security Identifiers) enthalten. Also jeder Benutzer kann folgerichtig in maximal 1024

Gruppen Mitglied sein.

Im Tagesgeschäft sollte dies (hoffentlich) kein Problem sein und ausreichen. Bei Domänenmigrationsvorhaben kann das durch die temporäre Verdoppelung der SIDs vielleicht einmal knapp sein. Gehen Sie also nicht ganz so inflationär mit den Berechtigungszugehörigkeiten um.

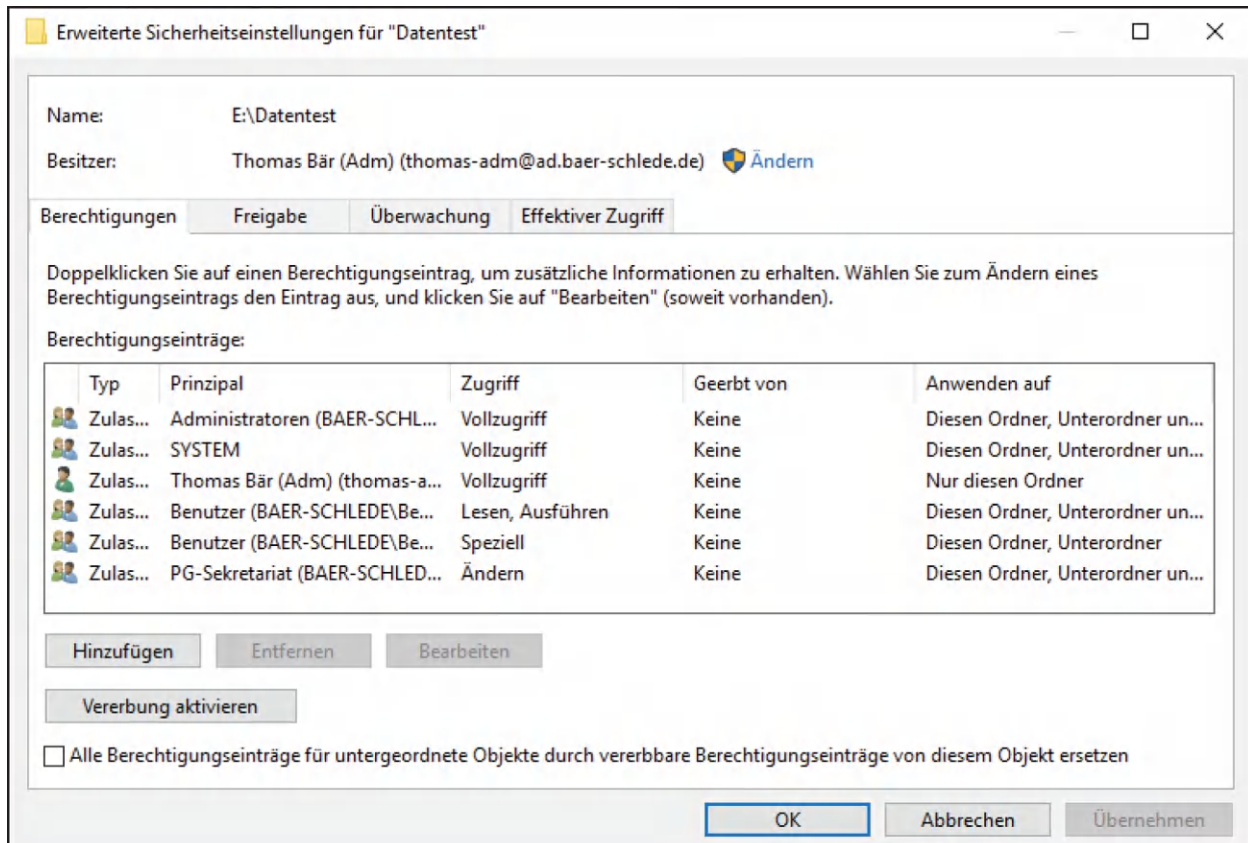


Abbildung 10.4: ERSTELLER-BESITZER wurde entfernt.

Vor Blicken schützen – ABE

Bereits am Anfang dieses Kapitels warfen wir einen Blick auf unsichtbare Freigaben. Die fehlende Sichtbarkeit einer Freigabe regelt nicht den Zugriff, wohl aber schützt sie vor unerwünschter Informationsgewinnung allein durch die Tatsache, dass ein Ordner oder eine Datei existiert.

Neben den unsichtbaren Dollar-Freigaben existiert noch eine weitaus effektivere Variante mit dem Namen »Access-based Enumeration«, abgekürzt ABE. Übersetzt bedeutet das in etwa »zugriffsbasierte

Auflistung«. Dem Benutzer werden im Windows Explorer nur noch diejenigen Verzeichnisse und Daten aufgelistet, auf die derjenige auch Zugriffsrechte besitzt.

In der Frühphase von ABE – vorgestellt mit Windows Server 2008 – hatte die Technik noch den Ruf, die Zugriffsgeschwindigkeit im Explorer drastisch zu reduzieren. Diese Sorge müssen Sie sich als Administrator heutzutage nicht mehr machen. Verschiedene Quellen im Internet besagen, dass die Performanceauswirkung bei rund drei Prozent liegen würde – das dürfte zu verschmerzen sein.

Bereiten wir – möglicherweise auch nur gedanklich – folgendes Szenario vor. Es existiert auf einem Datei-Server die Freigabe »Datentest«. In dieser Freigabe befinden sich die Ordner Projekt 1 bis 3. Auf »Projekt 2« hat die Benutzerin »Hildegard Mayer« keinen Zugriff, da sie nicht über die erforderliche Gruppenmitgliedschaft verfügt, siehe [Abbildung 10.5](#).

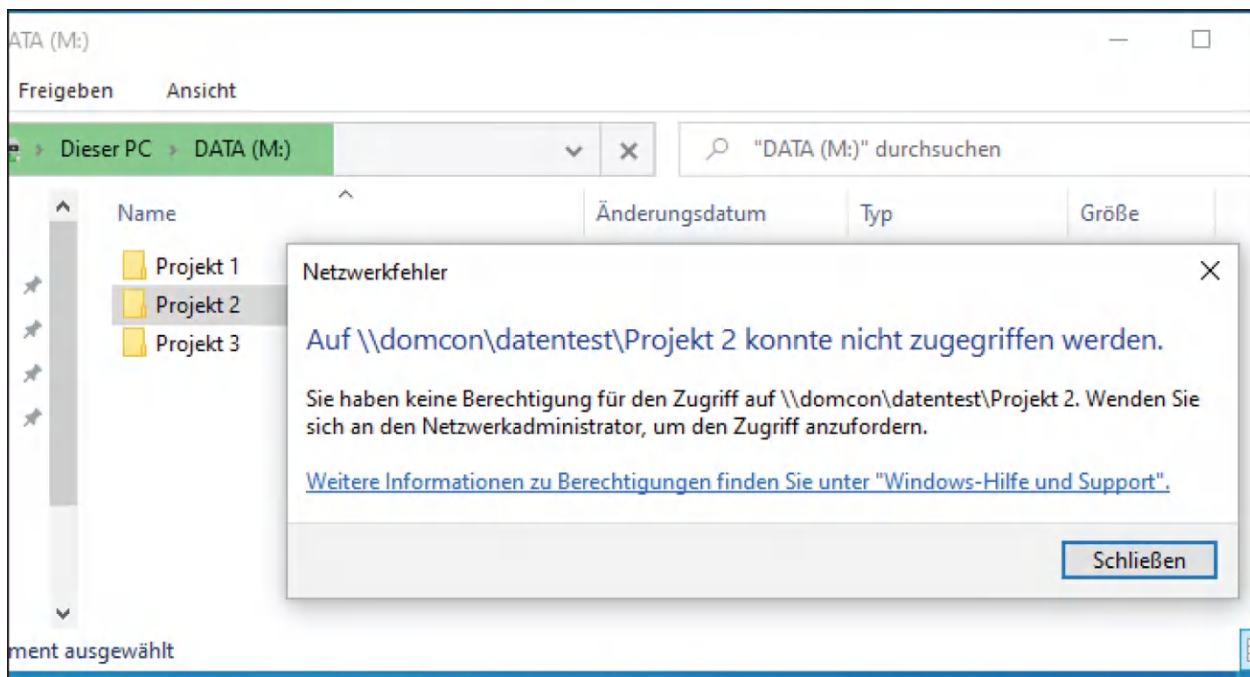


Abbildung 10.5: Obwohl kein Zugriff erlaubt, wird der Ordner dennoch angezeigt

Solange ein Ordner nur eine Bezeichnung wie »Projekt 2« besitzt, mag die bloße Sichtbarkeit vielleicht kein Problem darstellen. Anders wiederum wäre es, wenn der Ordner den Titel »Abwicklung Standort KOK Sommer 2021« haben würde. Allein die Benennung erweckt das Interesse.

Die Aktivierung von ABE auf dem Server ist ziemlich schnell erledigt.

1. Starten Sie auf dem Server den SERVER-MANAGER.
2. Wählen Sie in der linken Menüstruktur den Eintrag DATEI-/SPEICHERDIENSTE.
3. Wählen Sie in der entstandenen Menüstruktur den Eintrag FREIGABEN.
4. Klicken Sie mit der rechten Maustaste auf die gewünschte Freigabe und wählen Sie den Befehl EIGENSCHAFTEN aus dem Kontextmenü.
5. Klicken Sie in der neuen Menüstruktur im Fenster EIGENSCHAFTEN VON *Freigabename* auf EINSTELLUNGEN.
6. Bestätigen Sie die oberste Option in der Liste mit dem Titel ZUGRIFFSBASIERTE AUFZÄHLUNG AKTIVIEREN, siehe [Abbildung 10.6](#).
7. Bestätigen Sie Ihre Eingabe durch einen Klick auf OK.
8. Schließen Sie den SERVER-MANAGER.

Nach dem Einschalten von ABE bleiben die Darstellungen in den Explorer-Fenstern der Benutzer so lange in der bisherigen Form erhalten, bis sich der Anwender neu anmeldet.



Probleme im Zusammenhang mit ABE deuten in der Regel auf Fehler in der Rechtestruktur hin. Wer sich mit den technischen Details von ABE näher befassen möchte, der sei auf einen gut geschriebenen Microsoft-Docs-Beitrag auf Englisch hingewiesen: <https://bit.ly/3j0bup2>.

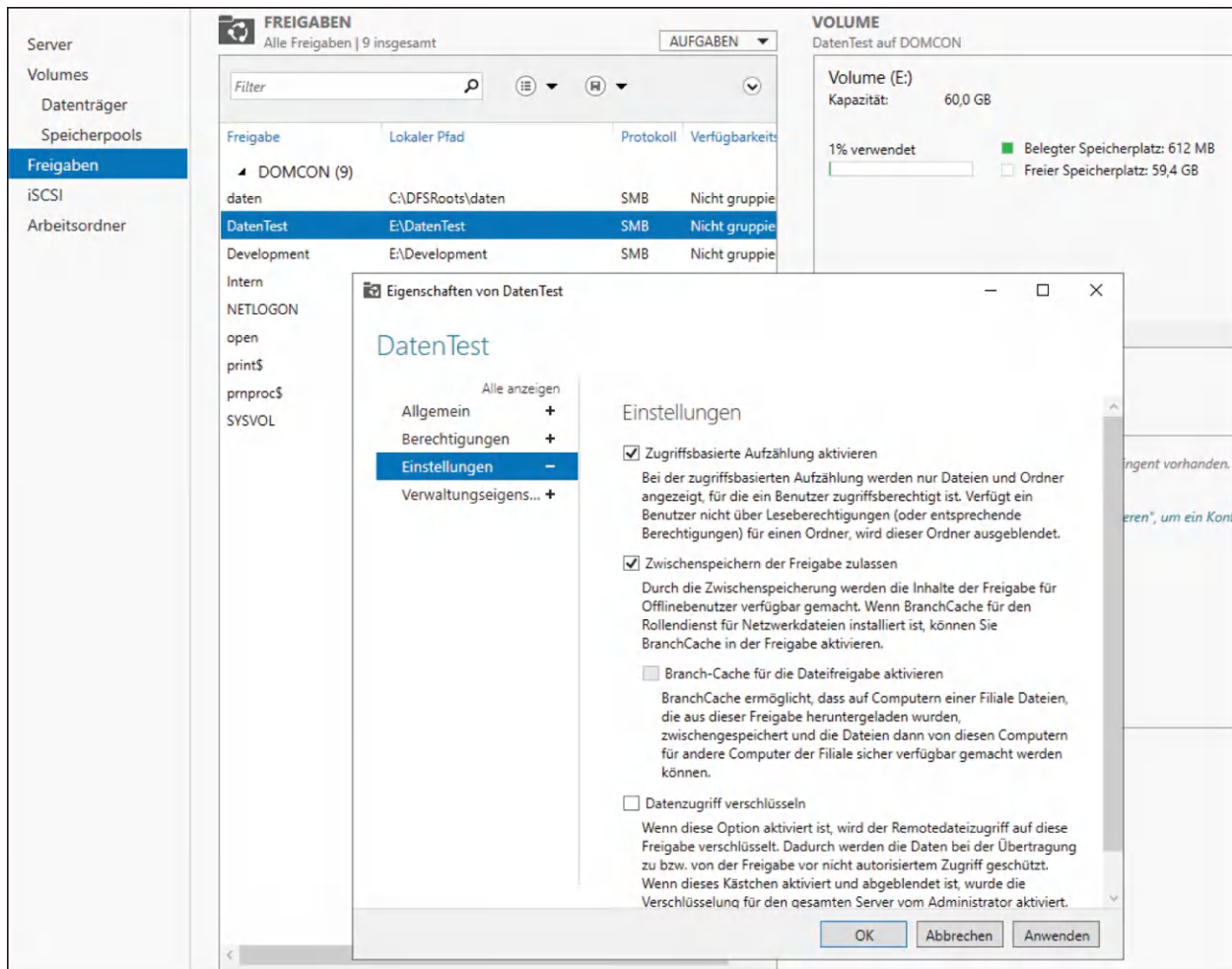


Abbildung 10.6: Aktivierung von ABE im Server-Manager

Dynamic Access Control

Das bisher in der Windows-Welt genutzte Konzept der Bereitstellung von Freigaben und die Zuordnung von Rechten ist vom Grundsatz her bereits sehr alt. Vor dem Hintergrund der Herausforderungen durch die zunehmende Cloud-Technik, für Microsoft im Wesentlichen die Azure-Strategie, offenbarten die »altehrwürdigen Freigaben« ihre statische Struktur.

Neuere Techniken wie Arbeitsordner, Scale-out File-Server oder Shared Storage für virtuelle Maschinen und Datenbanken erforderten die Aktualisierung der technischen Grundlage. Zu diesem Maßnahmenpaket gehört auch »Dynamic Access Control« (DAC).

Microsoft führte mit dem Erscheinen des Windows Servers 2012 eine neue Zugriffssteuerung für Datei-Server ein, die nicht mehr auf der doch eher statischen Zuordnung von Rechten zu Benutzern und Gruppen beruht. Vielmehr übernehmen zentral im Active Directory hinterlegte Regeln die Kontrolle, die auf Attributen basieren, die der Administrator an Benutzer und Computer sowie an Dateien und Verzeichnisse vergibt.

DAC ist dabei eine Mischung von Techniken, die es dem Administrator beispielsweise erlaubt, Konstellationen umzusetzen, bei denen quasi die Mitgliedschaft in zwei Gruppen zum Zugriff auf eine weitere Ebene führt. Bisher mussten Administratoren hierfür eine dritte Gruppe erstellen, um die erforderliche Berechtigungsstruktur so abzubilden.

Um DAC überhaupt nutzen zu können, ist im Vorfeld eine Aktivierung für die Domänencontroller und Client-Rechner erforderlich. Die erforderlichen Schritte folgen im Praxisbeispiel.

Hierzu gibt es ab Windows 8/2012 die sogenannten »Claims« – auf Deutsch »Ansprüche«. Die Einrichtung der Claims geschieht über das Active-Directory-Verwaltungscenter (siehe [Abbildung 10.7](#)).

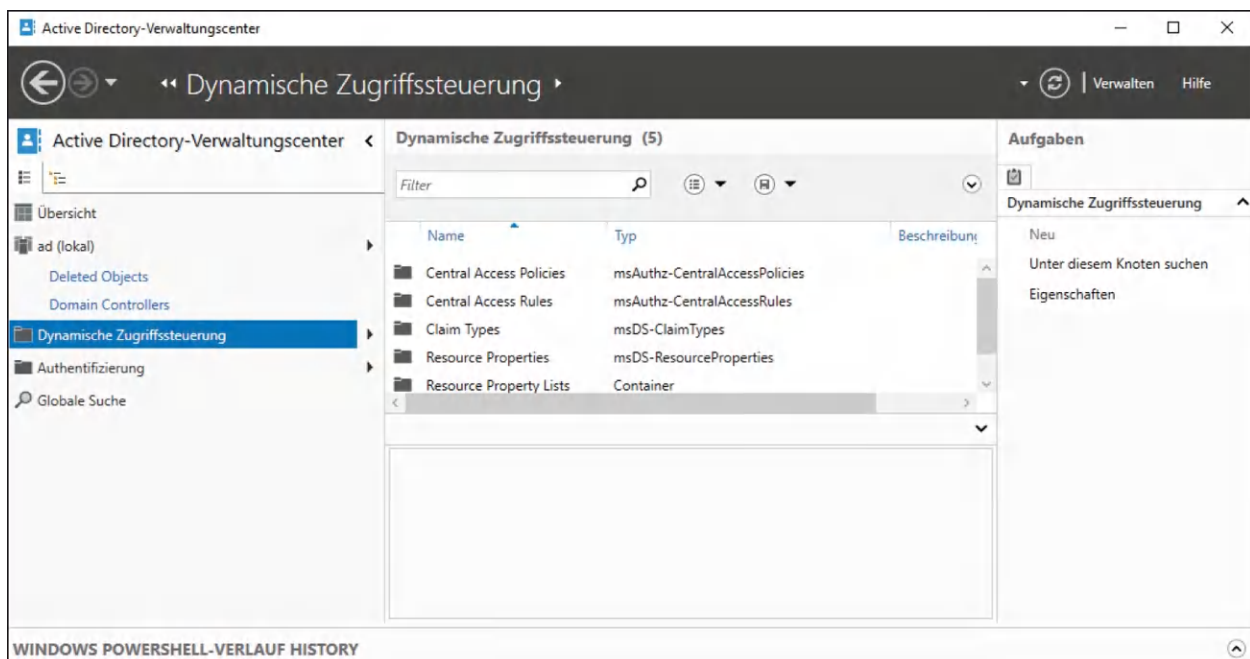


Abbildung 10.7: Möglichkeit zur Einrichtung der dynamischen Zugriffssteuerung (DAC)

Hierfür stehen fünf Container zur Verfügung:

- ✓ CENTRAL ACCESS POLICIES – Die zentralen Zugriffsrichtlinien enthalten mehrere zentrale Regeln, in denen Administratoren festlegen, wer Zugriff auf Ressourcen wie Ordner oder Dateien erhält. Die Richtlinie können Sie veröffentlichen und anschließend auf eine Ressource zur Anwendung bringen.
- ✓ CENTRAL ACCESS RULES – Mit einer zentralen Zugriffsregel definieren Sie, welche Berechtigung welcher Ressource zugewiesen wird.
- ✓ CLAIM TYPES – Sie können einen sogenannten Anspruchstyp für Benutzer oder Computer definieren.
- ✓ RESSOURCE PROPERTIES – Die Ressourceneigenschaften beschreiben das Merkmal einer Ressource, beispielsweise einer Datei oder eines Ordners. Sie wird beim Erstellen einer zentralen Zugriffsregel genutzt, um Zielressourcen und Berechtigungen zu definieren, und dient auch zur Klassifizierung der Ressource selbst.
- ✓ RESSOURCE PROPERTY LISTS – Die Ressourceneigenschaftenlisten dienen der Kategorisierung von Ressourcen.

Da haben sich die Entwickler bei Microsoft ja etwas Wundervolles einfallen lassen – etwas, das auf den ersten Blick so gar nichts sagt. Beginnen wir, das Gesamtbild im Rahmen eines Beispiels zusammenzufassen: Eine bestimmte Datei soll von einem Datei-Server aus nur dann zu öffnen sein, sofern der Benutzer Mitglied der Geschäftsführung ist, und auch nur dann, sofern er an einem PC der Geschäftsführung angemeldet ist. Für die Zuweisung dieser Eigenschaft »Geschäftsführung« nutzen wir die Attribute von Windows.

Zur Vorbereitung ordnen Sie einem Benutzer und einem Computer das Attribut »GF« zu. In der Standardeinstellung von Windows ist hierfür die erweiterte Ansicht erforderlich.

1. Starten Sie auf dem Domänencontroller den SERVER-MANAGER.
2. Klicken Sie im Menü auf den Befehl TOOLS.

3. Wählen Sie die ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
4. Klicken Sie den Menübefehl ANSICHT und stellen Sie sicher, dass die ERWEITERTEN FEATURES aktiviert sind.
5. Wählen Sie den gewünschten Benutzer aus, klicken Sie in der Registerkarte auf ATTRIBUT-EDITOR, scrollen Sie in der Liste auf den Eintrag DEPARTMENT und klicken Sie auf die Schaltfläche BEARBEITEN. Geben Sie GF ein und bestätigen Sie die Eingabe. Siehe [Abbildung 10.8](#). Wiederholen Sie den Vorgang für den ausgewählten PC der Geschäftsführung.

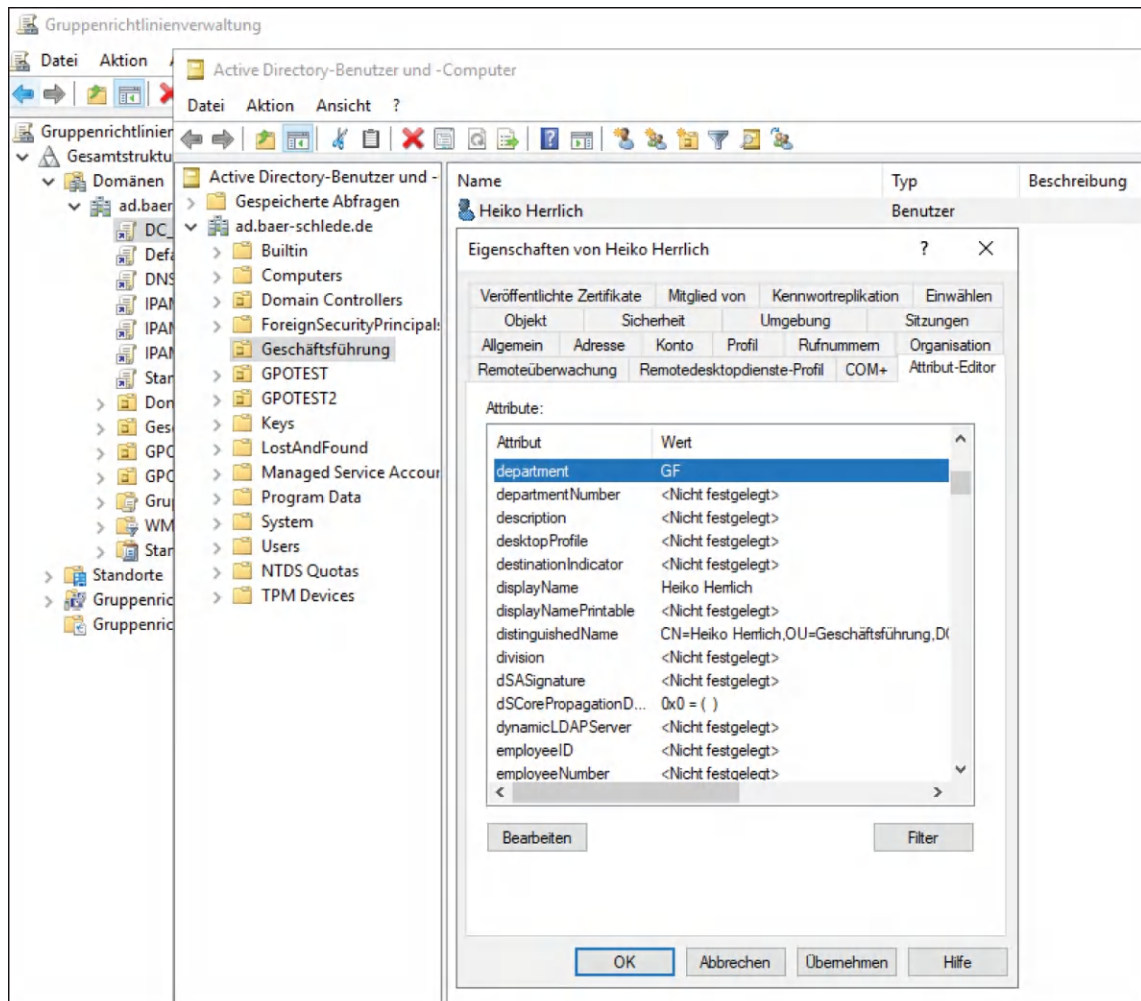


Abbildung 10.8: Eingabe eines Attributwerts in den erweiterten Features

Um überhaupt mit Claims arbeiten zu können, muss die Funktionalität auf

den Domänencontrollern aktiviert werden. Dies geschieht über eine Gruppenrichtlinie:

1. Starten Sie auf dem Domänencontroller den SERVER-MANAGER.
2. Klicken Sie im Menü auf den Befehl TOOLS.
3. Wählen Sie GRUPPENRICHTLINIENVERWALTUNG.
4. Erstellen Sie eine Gruppenrichtlinie, die auf Domänencontroller einwirkt (empfohlen), oder passen Sie die DEFAULT DOMAIN POLICY (weniger empfohlen) an.
5. Wählen Sie COMPUTERKONFIGURATION | RICHTLINIEN | ADMINISTRATIVE VORLAGEN | SYSTEM | KDC | UNTERSTÜTZUNG DES KERBEROS-DOMÄNENCONTROLLERS FÜR ANSPRÜCHE, VERBUNDAUTHENTIFIZIERUNG UND KERBEROS SCHUTZ.
6. Aktivieren Sie die Richtlinie und wählen Sie die Einstellung UNTERSTÜTZT oder IMMER ANSPRÜCHE LIEFERN – siehe [Abbildung 10.9](#).

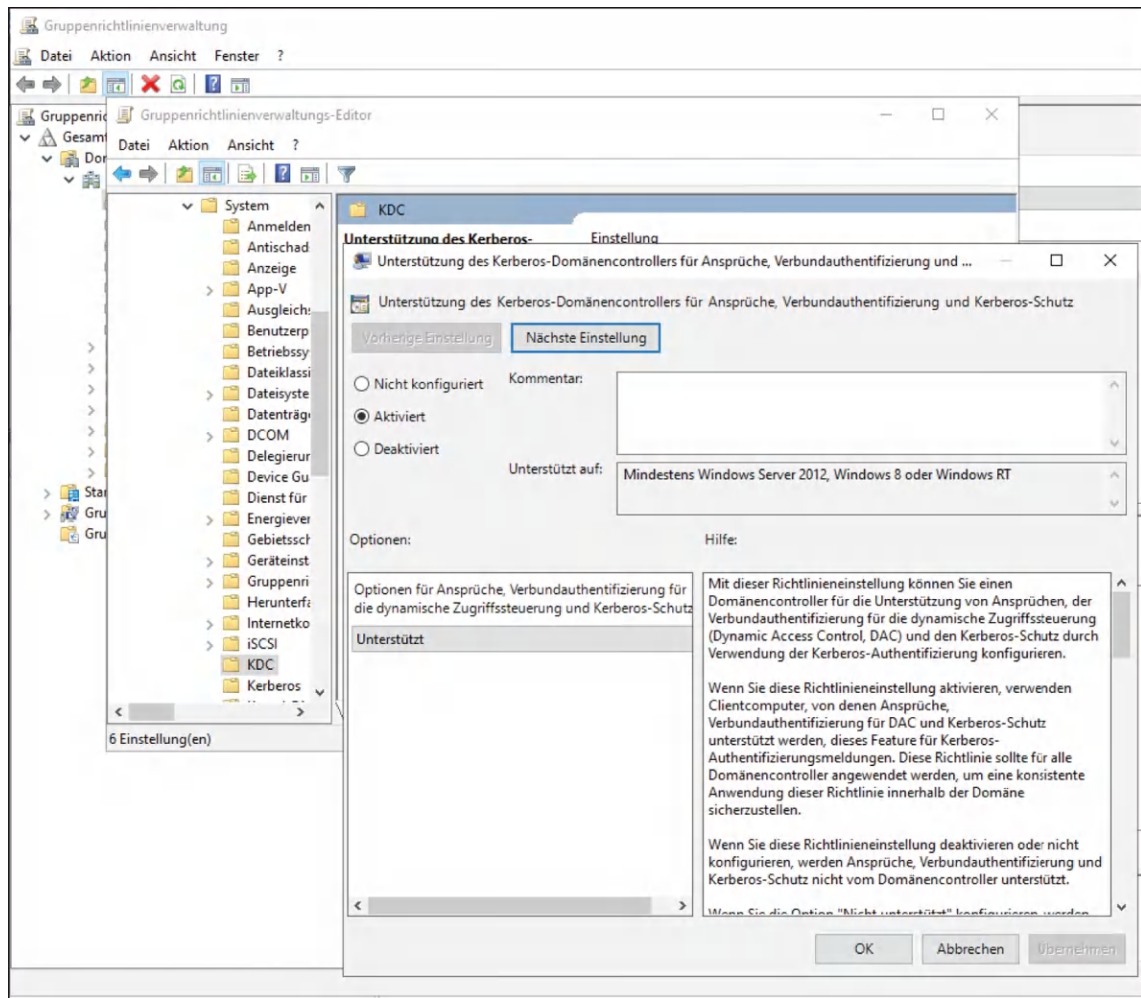


Abbildung 10.9: Die Verwendung von DCA erfordert die Aktivierung auf den DCs.

Für Client-Systeme, die auf den Datei-Server zugreifen und DAC verwenden, gilt es, ebenfalls eine Gruppenrichtlinie anzupassen:

1. Starten Sie auf dem Domänencontroller den SERVER-MANAGER.
2. Klicken Sie im Menü auf den Befehl TOOLS.
3. Wählen Sie GRUPPENRICHTLINIENVERWALTUNG.
4. Erstellen Sie eine Gruppenrichtlinie, die auf Client-Computer einwirkt (empfohlen), oder passen Sie die DEFAULT DOMAIN POLICY (weniger empfohlen) an.
5. Wählen Sie COMPUTERKONFIGURATION | RICHTLINIEN | ADMINISTRATIVE VORLAGEN | SYSTEM | KERBEROS | UNTERSTÜTZUNG DES KERBEROS-CLIENTS FÜR

ANSPRÜCHE, VERBUNDAUTHENTIFIZIERUNG UND KERBEROS SCHUTZ.

6. Aktivieren Sie die Richtlinie.
7. Warten Sie die Gruppenrichtlinienaktivierung ab oder führen Sie eine manuelle Aktualisierung mit gpupdate durch.

Nun sind alle vorbereiteten Schritte abgeschlossen – wir gehen in diesem Beispiel davon aus, dass es eine Freigabe für die Geschäftsführung bereits gibt und in dieser Freigabe die »besonders zu schützende Datei« enthalten ist.

1. Starten Sie auf dem Domänencontroller den SERVER-MANAGER.
2. Klicken Sie im Menü auf den Befehl TOOLS.
3. Wählen Sie ACTIVE DIRECTORY-VERWALTUNGSCENTER.
4. Klicken Sie auf DYNAMISCHE ZUGRIFFSSTEUERUNG (siehe [Abbildung 10.7](#)).
5. Legen Sie einen Claim-Typ an. Klicken Sie hierzu mit der rechten Maustaste auf den Eintrag CLAIM TYPES, wählen Sie im Kontextmenü den Befehl NEU | ANSPRUCHSTYP.
6. Wählen Sie unter Quellattribut DEPARTMENT aus und wählen Sie als Option sowohl BENUTZER als auch COMPUTER. Benennen Sie die Anzeige sinnvollerweise beginnend mit CT-, beispielsweise CT-department.
7. Klicken Sie anschließend auf RESSOURCE PROPERTIES und wählen Sie im Kontextmenü nach einem Rechtsklick den Befehl NEU | RESSOURCENEIGENSCHAFT.
8. Definieren Sie einen ANZEIGENAMEN, beispielsweise RP-Abteilung, vom Wertetyp Single-valued Choice und klicken Sie im Abschnitt VORGESCHLAGENE WERTE auf die Schaltfläche HINZUFÜGEN...
9. Erstellen Sie einen Eintrag mit dem Wert »GF«, dem Anzeigenamen Geschäftsführung und einer Beschreibung. Verlassen Sie den

Eingabedialog mit OK und schließen Sie das Fenster zur Anlage der Ressourceneigenschaft mit OK.

10. Klicken Sie mit der rechten Maustaste auf CENTRAL ACCESS RULES, wählen Sie im Kontextmenü den Befehl NEU | ZENTRALE ZUGRIFFSREGEL.
11. Vergeben Sie einen sinnvollen Namen, der Ihnen später bei der Identifizierung helfen wird. Klicken Sie im Bereich ZIELRESSOURCEN auf den Befehl BEARBEITEN... und anschließend auf den Link BEDINGUNG HINZUFÜGEN. Wählen Sie in dem Dialogfenster RESSOURCE | RP-ABTEILUNG | IST GLEICH | WERT | GESCHÄFTSFÜHRUNG.
12. Wählen Sie im Abschnitt BERECHTIGUNG die letztendlich gültige Zugriffsberechtigung aus. Definieren Sie hierzu unter FOLGENDE BERECHTIGUNG beispielsweise Authentifizierte Benutzer mit der grundlegenden Berechtigung ÄNDERN.
13. Klicken Sie im unteren Fensterabschnitt auf den Link BEDINGUNGEN HINZUFÜGEN und füllen Sie die Einträge gemäß der Darstellung (siehe [Abbildung 10.10](#)). Bestätigen Sie die Eingabe mit OK.

Berechtigungseintrag für "Berechtigungen"

Prinzipal: Authentifizierter Benutzer [Prinzipal auswählen](#)

Typ: Zulassen

Grundlegende Berechtigungen: [Erweiterte Berechtigungen anzeigen](#)

- ☐ Vollzugriff
- ☒ Ändern
- ☒ Lesen und Ausführen
- ☒ Lesen
- ☒ Schreiben
- ☐ Spezielle Berechtigungen

[Alle löschen](#)

Fügen Sie eine Bedingung zum Beschränken des Zugriffs hinzu. Dem Prinzipal werden die angegebenen Berechtigungen nur gewährt, wenn die Bedingungen erfüllt werden.

[Gruppierung verwalten](#)

Benutzer	CT-department	Ist gleich	Wert	GF	Entfernen
Und					
Gerät	CT-department	Ist gleich	Wert	GF	Entfernen

[Bedingung hinzufügen](#)

[OK](#) [Abbrechen](#)

Abbildung 10.10: Festlegung der Berechtigung

14. Die Bedingung wird im Fenster ERWEITERTE SICHERHEITSEINSTELLUNG FÜR BERECHTIGUNGEN in einer eigenen Syntax im Stil von »Benutzer CT-department ist gleich...« ausgeschrieben. Letztendlich bestätigen Sie auch dieses Dialogfenster mit OK und schließen den Dialog ZENTRALE ZUGRIFFSREGEL ERSTELLEN für – in unserem Fall CAR-GF-Dateizugriff – mit OK.
15. Nun gilt es, unsere frisch angelegte Central Access Rule (CAR) einem Central-Access-Policies-Eintrag zuzuordnen. Wählen Sie in der Menüstruktur den Eintrag CENTRAL ACCESS POLICIES und klicken Sie im rechten Menüband auf NEU | ZENTRALE ZUGRIFFSRICHTLINIE (oder über den Rechtsklick im Kontextmenü).
16. Es öffnet sich das Dialogfenster zur Anlage einer neuen zentralen Zugriffsrichtlinie. Dem bisherigen Benennungsschema folgend, legen Sie unter NAME einen Eintrag wie CAP-Dateizugriff an. Klicken Sie auf die Schaltfläche HINZUFÜGEN... und wählen Sie die zuvor angelegte Central Access Rule (CAR) aus. Bestätigen Sie die

Zuordnung mit OK.

17. Nun gilt es, diese Richtlinie über die Gruppenrichtlinienverwaltung auf die Datei-Server zur Anwendung zu bringen. Öffnen Sie hierzu im SERVER-MANAGER unter TOOLS die GRUPPENRICHTLINIENVERWALTUNG. Wählen Sie eine Gruppenrichtlinie aus, die nur auf die gewünschten Server wirkt.
18. Klicken Sie unter COMPUTERKONFIGURATION | RICHTLINIEN | WINDOWS-EINSTELLUNGEN | SICHERHEITSEINSTELLUNGEN | DATEISYSTEM | ZENTRALE ZUGRIFFSRICHTLINIE. Klicken Sie mit der rechten Maustaste in das Fenster für ZENTRALE ZUGRIFFSRICHTLINIE(n) und wählen Sie aus dem Kontextmenü den Befehl ZENTRALE ZUGRIFFSRICHTLINIEN VERWALTEN... Fügen Sie die erstellte CAP hinzu – siehe [Abbildung 10.11](#).

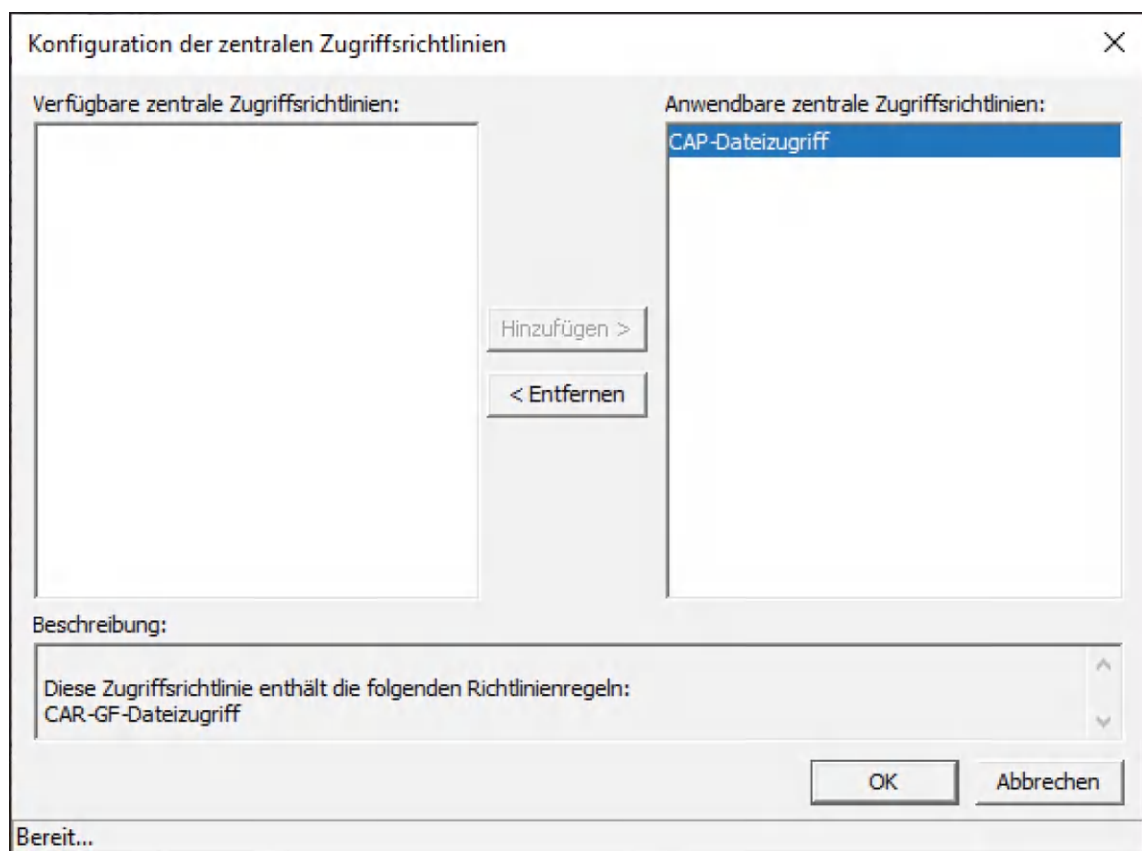


Abbildung 10.11: Zuordnung einer CAP über eine Gruppenrichtlinie

19. Führen Sie gpupdate in der Eingabeaufforderung aus.

20. Starten Sie SERVER-MANAGER | TOOLS | RESSOURCEN-MANAGER FÜR DATEISERVER.
21. Öffnen Sie in der Baumstruktur den Eintrag KLASSIFIZIERUNGSVERWALTUNG und dort den Zweig KLASSIFIZIERUNGSEIGENSCHAFTEN. In der Auflistung entdecken Sie die von Ihnen zu Beginn angelegte Ressource Property, in unserem Fall RP-Abteilung – siehe [Abbildung 10.12](#).
22. Ist dieser Eintrag nicht vorhanden, ist im Vorfeld etwas schiefgelaufen, und Sie sollten die Anwendung der Gruppenrichtlinie auf den Server prüfen.
23. Nun geht es endlich daran, die gewünschte Datei mit der erweiterten Sicherheitseinstellung zu besetzen. Wählen Sie die gewünschte Datei auf dem Datei-Server im Explorer aus. Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie EIGENSCHAFTEN aus dem Kontextmenü.

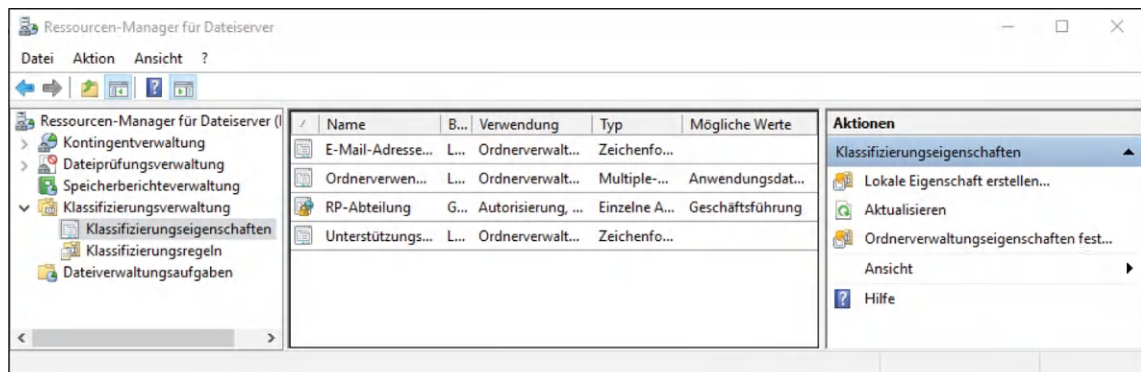


Abbildung 10.12: Der Eintrag der Ressource Property im Ressourcen-Manager

24. Wechseln Sie in die Registerkarte KLASSIFIZIERUNG und wählen Sie, für unser Beispiel, für den Eintrag RP-Abteilung den Wert Geschäftsführung aus. Bestätigen Sie mit ÜBERNEHMEN – siehe [Abbildung 10.13](#).

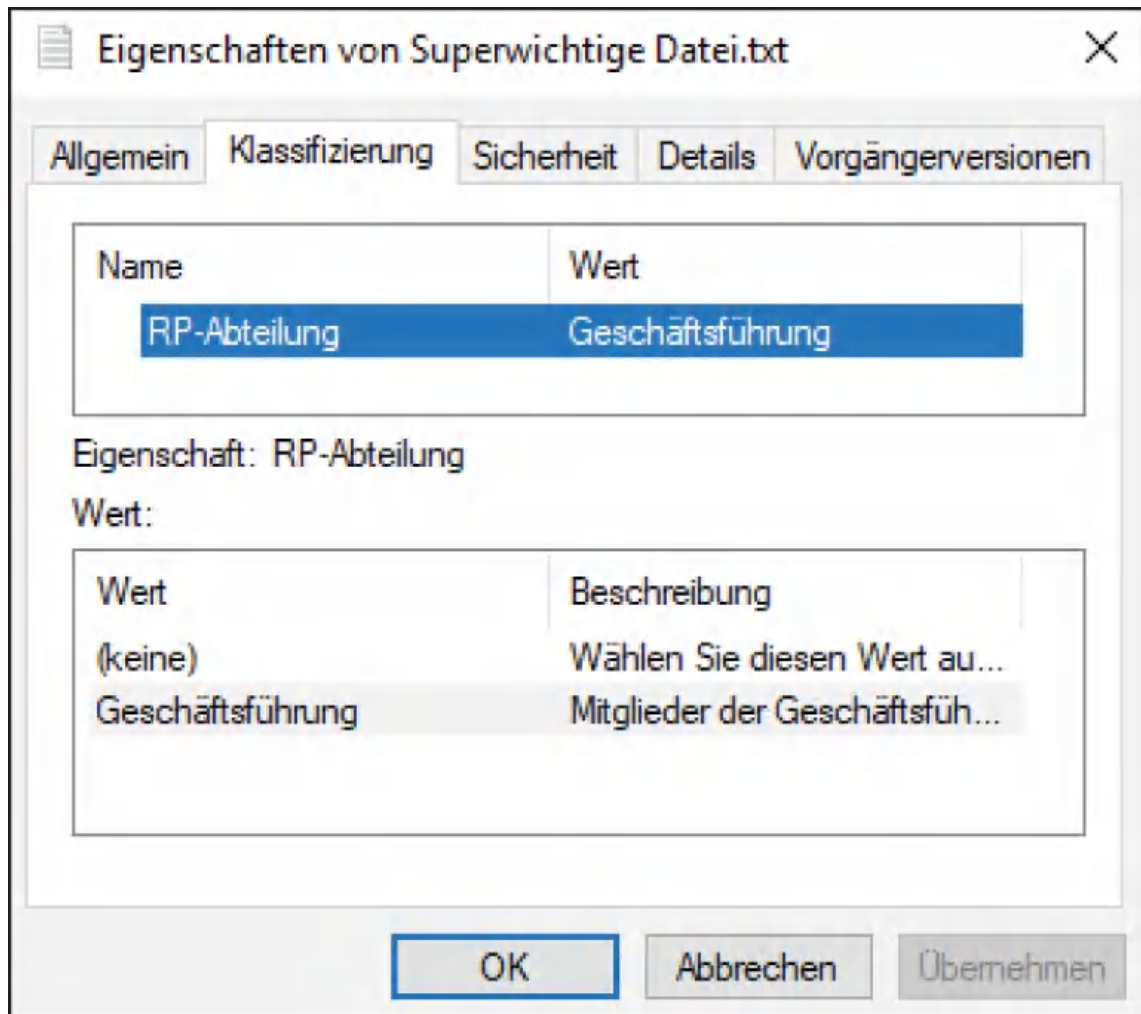


Abbildung 10.13: Zuordnung einer Ressource Property

25. Wechseln Sie in das Register SICHERHEIT.
26. Klicken Sie auf ERWEITERT.
27. Sie erkennen den Ihnen bereits bekannten Dialog, jedoch ist eine Registerkarte hinzugekommen – die mit der Bezeichnung ZENTRALE RICHTLINIE. Wechseln Sie in diese Registerkarte und klicken Sie auf das untere Schlosssymbol mit dem Link ÄNDERN.
28. Wählen Sie die im Vorfeld generierte CAP-Richtlinie im unteren Fensterbereich aus und bestätigen Sie mit OK – siehe [Abbildung 10.14](#)

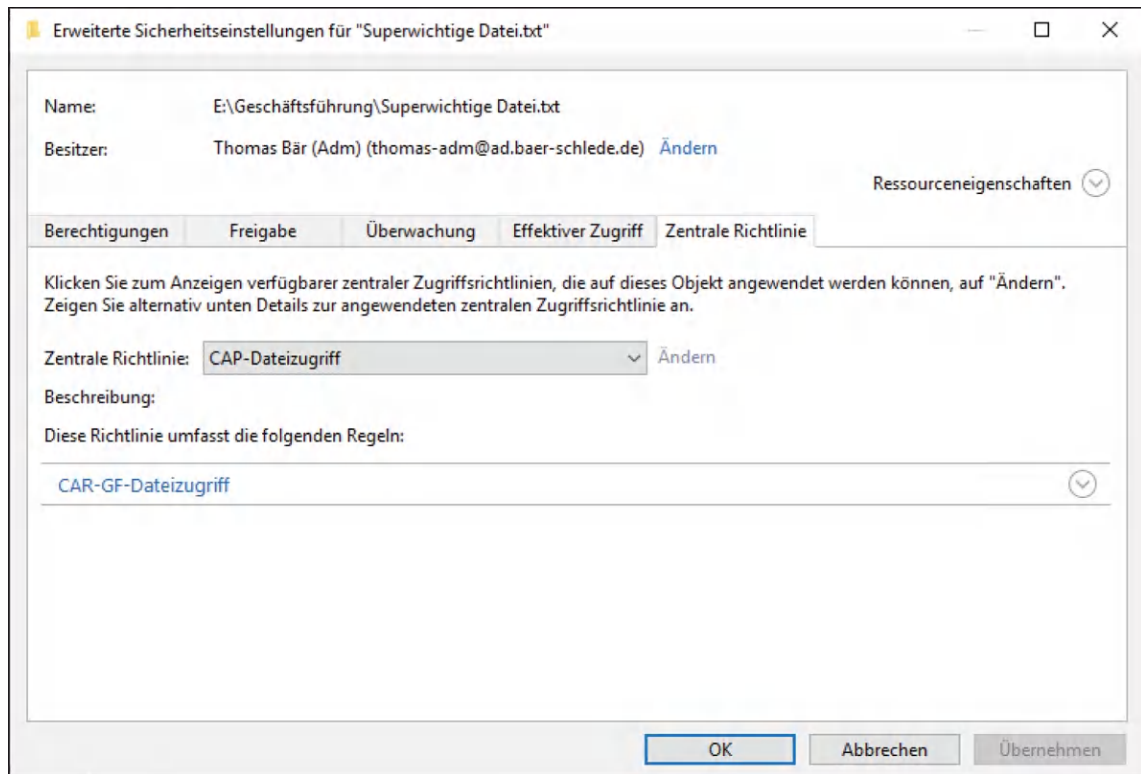


Abbildung 10.14: Zuweisung einer Richtlinie zu einer Datei

Nun haben Sie diese »Konfigurationsorgie« tatsächlich hinter sich gebracht. Wir können Ihnen versichern, dass der Vorgang tatsächlich aus dem Kopf möglich ist, wenn Sie das Konzept dahinter erst einmal verstanden haben.

Nun möchten wir jedoch noch prüfen, ob das wirklich funktioniert hat. Bekannterweise kommt die Aussage »... müsste nun klappen...« auf der Ebene der Geschäftsführung nicht ganz so gut an. Daher gibt es die Möglichkeit, den effektiven Zugriff zu prüfen.

Prüfung des effektiven Zugriffs

Auch ohne, dass Sie als Administrator die dynamische Zugriffssteuerung (DAC) verwenden, ist die Feststellung, ob ein Benutzer Zugriff auf eine Ressource nun erhält oder nicht, von vielen Faktoren abhängig. Diese im Zusammenspiel im Blick zu halten, ist mitnichten eine einfache Aufgabe.

Glücklicherweise gibt es hierfür den Dialog **EFFEKTIVER ZUGRIFF** in den **ERWEITERTEN SICHERHEITSEINSTELLUNGEN**. Sofern Sie

dem vorherigen Beispiel folgen, klicken Sie auf die entsprechende Registerkarte und geben Sie den zuvor berechtigten Benutzer der Geschäftsführung an. Wählen Sie dann dessen Computer und erweitern Sie die Links BENUTZERANSPRUCH EINSCHLIEßEN und GERÄTEANSPRUCH EINSCHLIEßEN. Wählen Sie in diesem Fall das Attribut CT-department und geben Sie in die beiden Eingabefelder den Wert GF ein. Klicken Sie anschließend auf die Schaltfläche EFFEKTIVEN ZUGRIFF ANZEIGEN – siehe [Abbildung 10.15](#).

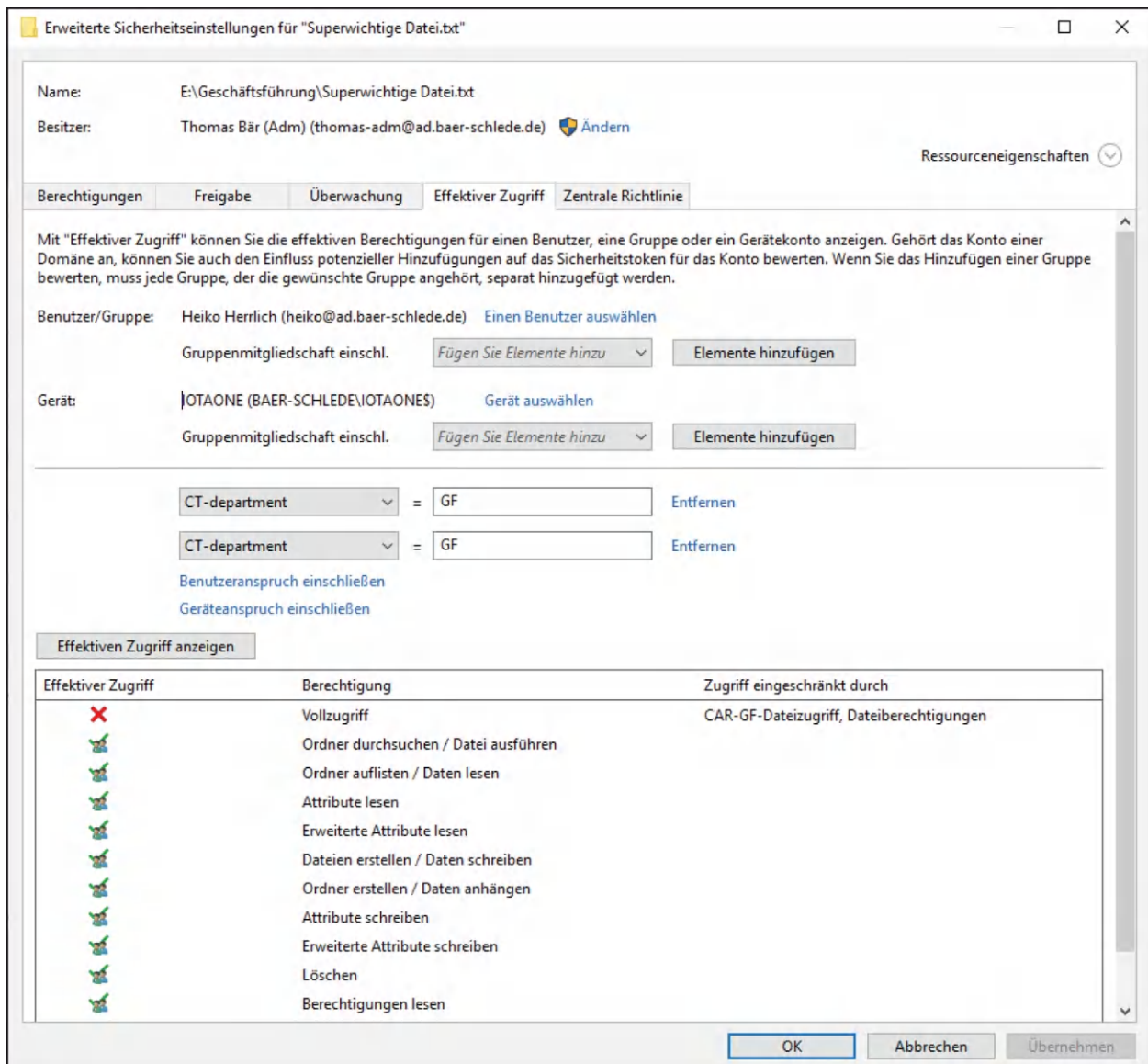


Abbildung 10.15: Anzeige des effektiven Zugriffs basierend auf Ansprüchen (Claims)

Das Dialogfenster zeigt nun die unterschiedlichen Rechte wie

VOLLZUGRIFF, ORDNER DURCHSUCHEN / DATEI AUSFÜHREN oder ATTRIBUTE LESEN an und zeigt grafisch, ob ein Zugriff erlaubt ist oder verwehrt wird. Die Begründung für eine Zugriffseinschränkung finden Sie in der dritten Spalte. Im hier dargestellten Beispiel greift die CAR-GF-Dateizugriff als Dateiberechtigung und verhindert für den oben gewählten Benutzer den Vollzugriff.

Folgende Faktoren wirken kumulativ für die effektive Freigabe zusammen:

- ✓ Zentrale Zugriffsrichtlinien – beispielsweise DAC
- ✓ Summe der NTFS-Berechtigungen
 - Zugriffsberechtigung in den verschiedenen Varianten
 - Explizite Verweigerung des Zugriffs hebt alle Zugriffsrechte wieder aus
- ✓ Vererbung
- ✓ Sicherheitseinstellungen der Freigabe



Es gewinnt das am geringsten einschränkende NTFS-Recht, übersteuert von der expliziten Verweigerung des Zugriffs!

Sie können als Administrator in diesem Dialogfenster sehr einfach Zugriffsrechte abprüfen. Wir empfehlen Ihnen wirklich, sich ein paar Minuten intensiver damit zu beschäftigen. Gern zur Wiederholung: Die Zugriffsrechte hier durchzuspielen, ist deutlich professioneller als die Rückmeldung »... sollte jetzt funktionieren« (das wissen wir, da wir diese E-Mail schon bestimmt 1.000-mal geschrieben haben).

Ansonsten haben Sie noch weitere Begleiter, die Ihnen einen Zugriff möglicherweise sperren:

- ✓ Antiviren-Software
- ✓ Makro-Schutz, der den kompletten Aufruf blockiert



Wer noch tiefer in die Möglichkeiten des zentralen Zugriffs eintauchen will, dem seien die entsprechenden Solution-Guide-Beiträge auf den Docs-Webseiten von Microsoft empfohlen:

<https://docs.microsoft.com/de-de/windows-server/identity/solution-guides/scenario--central-access-policy>

Kapitel 11

Hyper-V

IN DIESEM KAPITEL

Hyper-V – die Virtualisierung in und auf Windows Server 2019

Virtualisierung: Begriffe und Bestandteile

Vorteile beim Einsatz von Hyper-V

Einrichtung der Hyper-V-Rolle

Hyper-V konfigurieren

Manager für virtuelle Switches

Virtueller Switch und die PowerShell

Ganz gleich, wie viel Sie bisher schon mit IT und Computersystemen zu tun hatten – den Begriff »Virtualisierung« werden Sie zweifelsohne schon gehört oder gelesen haben oder Sie haben sogar schon erste Erfahrung mit virtualisierten Betriebssystemen gemacht. Grundsätzlich stellt Ihnen eine Betriebssystem-Virtualisierung die Möglichkeit zur Verfügung, auf einem physischen Server mehrere virtuelle Gastsysteme zu betreiben. Durch den Einsatz von Virtualisierungslösungen wie Xen von Citrix, vSphere (ESX/ESXi) von VMware und Hyper-V von Microsoft können Sie sogenannte virtuelle Maschinen anlegen, die dann logisch voneinander und vom darunterliegenden Hostsystem getrennt sind.

Virtualisierung: Begriffe und Bestandteile

Die Virtualisierungs-Software Hyper-V ist fester Bestandteil der Windows-Server-Betriebssysteme 2012, 2016 und 2019. Bei den Client-

Betriebssystemen stellte Microsoft sie ab Windows 8 Pro und aktuell auch in der Pro-Version von Windows 10 bereit. Da es sich bei dieser Software um einen Typ-1-Hypervisor handelt, steht er auch in eine Stand-alone-Ausführung unter dem Produktnamen Microsoft Hyper-V Server 2016 beziehungsweise 2019 zur Verfügung, die dann ohne ein Windows-Betriebssystem direkt auf der Hardware installiert und betrieben werden kann.



Keine Virtualisierungslösung funktioniert ohne einen Hypervisor, früher häufig auch als VMM (Virtual Machine Manager) bezeichnet. Seine Aufgabe besteht darin, eine Abstraktionsschicht zwischen der wirklich vorhandenen Hardware und den Betriebssystemen in den virtuellen Maschinen zu bilden.

Bei den Hypervisor-basierten Lösungen wird zwischen Typ-1- und Typ-2-Hypervisoren unterschieden. Typ 1, der auch als nativer Hypervisor oder Bare-Metal-Hypervisor bezeichnet wird, ist in der Lage, über eigene Treiber direkt mit der Hardware des Hostsystems zu interagieren. Hyper-V ist ein Typ-1-Hypervisor. Hypervisoren vom Typ 2 sind »oberhalb« des Betriebssystems des Hosts installiert und verwenden die Hardware-Treiber des Host-Betriebssystems für den Zugriff und die Verwaltung der Hardware-Ressourcen.

Neben dem Hypervisor als zentralem Baustein einer Virtualisierungslösung gehören weitere Komponenten zu Hyper-V. Unter anderem sind das:

- ✓ *Virtuelle Maschine (VM)*: Eine Software, die für das darin installierte Betriebssystem die Hardware emuliert – also ein virtueller Computer. Für das installierte Betriebssystem und die Anwendungen ist es dabei nicht ersichtlich, dass sie nicht direkt auf »echter« Hardware laufen. So kann beispielsweise auch ein Linux-Betriebssystem in einer VM auf einem Windows-Host unter Hyper-V betrieben werden. Die virtuellen Maschinen einer Lösung lassen sich zudem auf allen Hostsystemen nutzen, auf denen diese Virtualisierungslösung aktiv ist. Sie können beispielsweise virtuelle Maschinen, die Sie unter Hyper-V

auf Windows Server 2019 erstellt haben, problemlos unter Hyper-V auf einer Workstation unter Windows 10 Pro betreiben.

- ✓ *Virtueller Switch*: Die Software, die auf dem Host-Rechner läuft, ist nicht direkt mit den physikalischen Geräten gleichen Namens vergleichbar. Sie hat die Aufgabe, virtuelle Maschinen mit dem physischen Netzwerk zu verbinden und Richtlinien zur Isolierung sowie der Sicherheit der VMs durchzusetzen. Ohne einen solchen virtuellen Switch können Sie Ihre virtuellen Maschinen nicht mit dem Netzwerk verbinden.
- ✓ *Virtuelle Festplatte*: Damit die Betriebssysteme in der virtuellen Maschine arbeiten können, benötigen sie natürlich auch entsprechenden Festplattenplatz. Dieser wird von Hyper-V in Form virtueller Festplatten bereitgestellt und der jeweiligen VM zugewiesen. Die virtuellen Festplatten werden auf dem Massenspeicher als Dateien mit der Endung VHD (Virtual Hard Disk) beziehungsweise VHDX für neuere Installationen angelegt. Der Windows-Server kann ebenfalls mit diesen Formaten umgehen und erkennt diese Dateien als virtuelle Festplatten.

Vorteile beim Einsatz von Hyper-V

Vielleicht fragen Sie sich nun, warum Sie eine Virtualisierungstechnik wie Hyper-V auf Ihrem Windows Server 2019 einsetzen sollten. Grundsätzlich kann Ihnen der Einsatz virtueller Maschinen eine ganze Reihe von Vorteilen bieten:

- ✓ *Sicher testen und prüfen*: Der erste Einsatz einer Virtualisierungslösung besteht für viele Nutzer häufig darin, dass sie Testsysteme aufsetzen. Virtuelle Systeme sind ideal, um neue Betriebssysteme oder Anwendungen in geschützten, abgekapselten Umgebungen zu testen. Nach dem Test können Sie solche Systeme problemlos wieder löschen.
- ✓ *Isolation der einzelnen VMs*: Sie sind unabhängig vom Betriebssystem des Hostrechners, und Anwendungen sowie Dienste in den virtuellen

Maschinen beeinflussen weder das Hostsystem noch andere virtuelle Maschinen auf dem Hostrechner.

- ✓ *Bessere Ausnutzung und Auslastung der Hardware:* Auf der gleichen Hardware können mehrere Systeme betrieben werden. So kann beispielsweise ein Anwendungs-Server dediziert in einer virtuellen Maschine betrieben werden, während mehrere andere virtuelle Maschinen auf dem gleichen Hostsystem aktiv sind.

Ein weiterer großer Vorteil von Hyper-V besteht darin, dass Sie ihn als Server-Rolle bei jedem Windows Server 2019 mit dabei haben. Sie können mit dieser Software also die ersten Schritte in Richtung Virtualisierung wagen, ohne dass Sie dazu zusätzliche Software benötigen. In den folgenden Abschnitten zeigen wir Ihnen, wie Sie den Hyper-V auf Ihrem Server einrichten und nutzen können.

Einrichtung der Hyper-V-Rolle

Der Hyper-V ist eine Rolle, die Sie auf Ihrem Server installieren können. Sie können auch den reinen Hyper-V-Server 2019 als Stand-alone-Produkt unter der Adresse <https://www.microsoft.com/de-de/evalcenter/evaluate-hyper-v-server-2019> von der Microsoft-Webseite herunterladen. Dieser Bereich ist zwar »Windows Server Evaluierungsversionen«, aber beim reinen Hyper-V-Server handelt es sich um ein freies Produkt, das Sie unbegrenzt nutzen können. Es ist genau die gleiche Technik und das gleiche Produkt, das Ihnen auch nach der Installation der Server-Rolle auf dem Windows-Server bereitsteht. Allerdings bietet Ihnen die Stand-alone-Version von Hyper-V keine Windows-Oberfläche, sondern muss »remote« von einem anderen System aus beziehungsweise über die Kommandozeile oder PowerShell verwaltet werden. Wir raten gerade zum Einstieg dazu, zunächst auf jeden Fall mit der Server-Rolle und den damit verbundenen Verwaltungswerkzeugen zu arbeiten.

Um die Hyper-V-Rolle zu installieren, können Sie den SERVER-MANAGER oder – falls Sie diesen Zusatz bereits installiert haben – auch das neuere ADMIN CENTER wählen. Beide Ansätze führen Sie mittels

Assistenten durch die Installation und zum gleichen Ergebnis: Hyper-V wird als Server-Rolle installiert. Wir schildern hier den »traditionellen« Weg unter Einsatz des SERVER-MANAGER, der keine zusätzliche Installation einer weiteren Software erfordert. Im [Kapitel 17](#) dieses Buchs gehen wir dann auch noch genauer auf die Möglichkeiten ein, die Ihnen das ADMIN CENTER bieten kann. Für die nun folgenden Schritte müssen Sie mit einem Konto an Ihrem Server angemeldet sein, das lokale Administratorrechte besitzt:

1. Wählen Sie im Startmenü die Kachel SERVER-MANAGER.
2. Dort wählen Sie dann im Bereich SCHNELLSTART den Punkt mit der Nummer 2 ROLLEN UND FEATURES HINZUFÜGEN aus.
3. Es startet nun ein Assistent, der Ihnen zunächst unter der Überschrift VORBEMERKUNGEN einige grundsätzliche Dinge erläutert.
4. Im nächsten Schritt können Sie nun den INSTALLATIONSTYP auswählen. Wie in [Abbildung 11.1](#) zu sehen, haben Sie dort die Auswahl zwischen ROLLEN- ODER FEATURE-BASIERTE INSTALLATION und der Installation von REMOTEDESKTOPDIENSTEN. Wir wählen erstere Option.

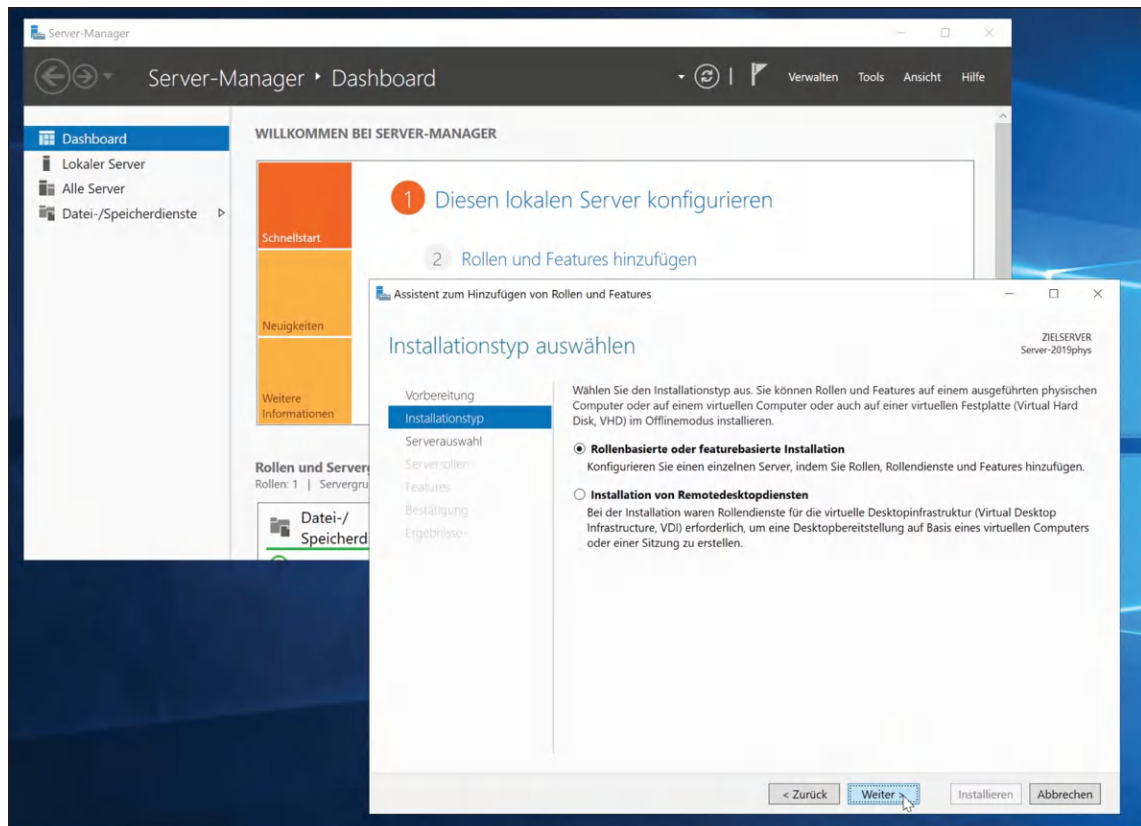


Abbildung 11.1: Der Assistent im Server-Manager führt Schritt für Schritt durch die Installation der Server-Rolle Hyper-V.

5. Die im nächsten Fenster folgende **SERVERAUSWAHL** können Sie in der Regel einfach übernehmen, da Sie zu diesem Zeitpunkt wahrscheinlich nur diesen einen Server haben werden.
6. Auf dem nächsten Bildschirm listet Ihnen der Assistent nun die unterschiedlichen Rollen und Features auf, die Ihnen zur Verfügung stehen. In dieser Liste sehen Sie zudem, welche dieser Rollen auf Ihrem Server bereits installiert sind. Bei einem neu installierten Server sind das in der Regel nur sehr wenige. Aus dieser Liste wählen Sie dann **HYPER-V** aus und markieren das Kästchen daneben.
7. Es öffnet sich nun automatisch ein Fenster, in dem Sie gefragt werden, ob die für Hyper-V erforderlichen Features ebenfalls installiert werden sollen ([Abbildung 11.2](#)). Die gezeigte Auswahl übernehmen Sie mit **FEATURES HINZUFÜGEN**. Auf diese Weise kommt nicht nur die Hyper-V-Konsole auf den Server, sondern auch die PowerShell-Cmdlets zur Verwaltung von Hyper-V werden installiert.

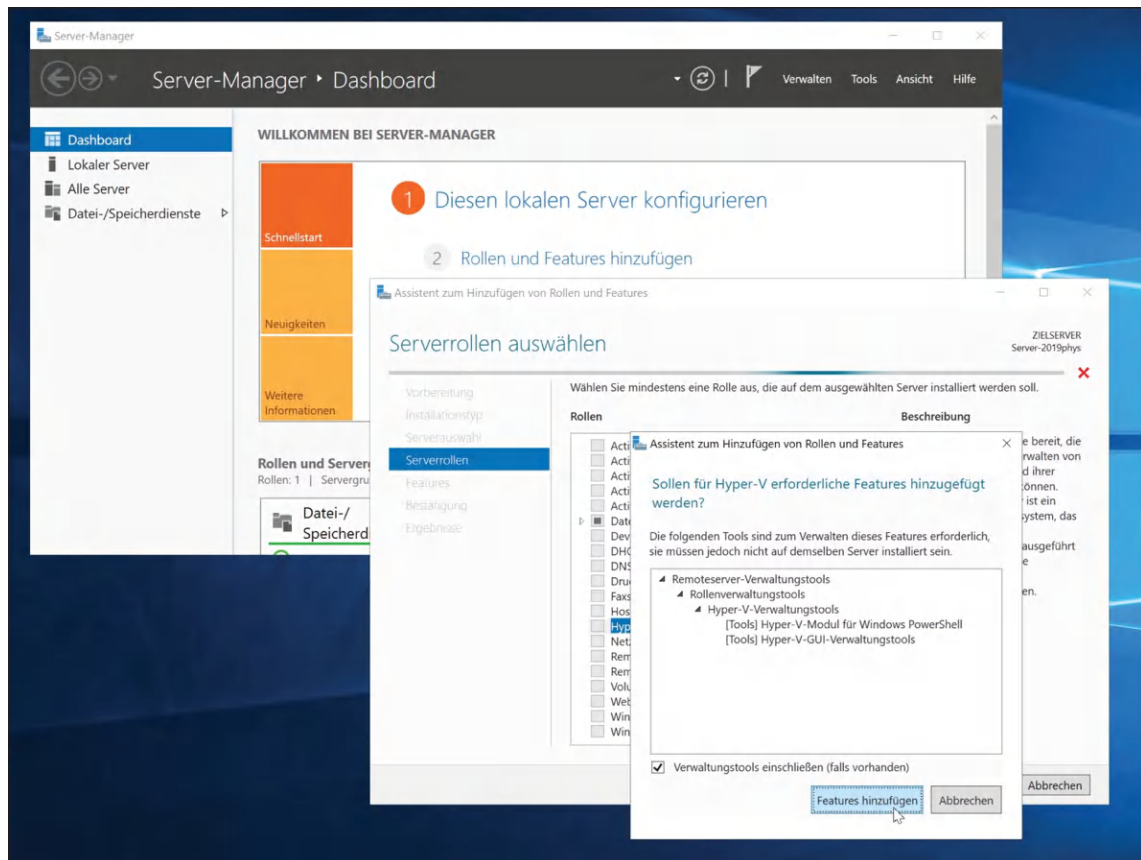


Abbildung 11.2: Die Features für den Hyper-V: Durch sie kommen die Verwaltungswerkzeuge und PowerShell-Cmdlets mit auf den Server.

8. Es folgt ein weiterer, sehr wichtiger Schritt: das Anlegen eines virtuellen Switches, der es erst ermöglicht, die virtuellen Maschinen mit dem physischen Netzwerk zu verbinden. Haben Sie – wie in der [Abbildung 11.3](#) zu sehen – nur eine Netzwerkkarte in Ihrem Server installiert, so sollten Sie natürlich diese auswählen.
9. Im nächsten Schritt geht es um die Migration der virtuellen Maschinen: Sie können Hyper-V dadurch so konfigurieren, dass eine »Live-Migration« von VMs möglich ist. Das bedeutet, dass die virtuellen Maschinen im laufenden Betrieb von einem Server auf einen anderen übertragen werden können. Da Sie diese Möglichkeit auch später, wenn Hyper-V installiert ist, einschalten und konfigurieren können, ist es zum Einstieg mit nur einem Server durchaus sinnvoll, diesen Schritt zunächst einfach mit WEITER zu überspringen.
10. Danach werden Sie gefragt, an welcher Stelle im Dateisystem des Servers die virtuellen Festplatten und die Konfigurationsdateien für

die virtuellen Maschinen abgelegt werden sollen. Auch diese Pfade können Sie später noch ändern. Standardmäßig legt Windows Server diese auf dem Laufwerk des Betriebssystems an, was ungünstig ist, weil gerade die virtuellen Festplatten doch schnell sehr groß werden können. Suchen Sie also eine Festplatte oder eine Partition auf Ihrem Server aus, die genug Platz für diese Dateien aufweist, und lenken Sie diese beiden Pfade dorthin.

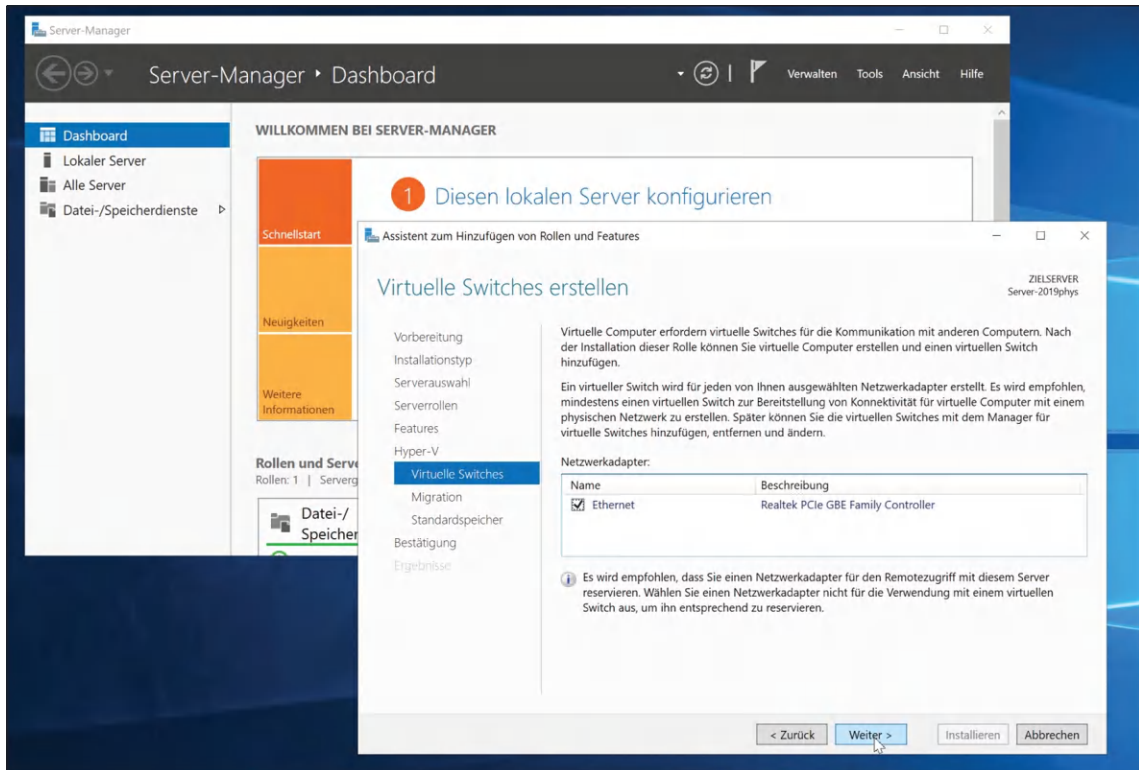


Abbildung 11.3: Ein wichtiger Schritt bei der Einrichtung von Hyper-V ist das Anlegen des virtuellen Switches, der die VMs mit dem Netzwerk verbindet.

11. Zum Abschluss bekommen Sie noch einmal eine Zusammenfassung der Dinge angezeigt, die nun installiert werden. Auf diesem Bildschirm finden Sie auch ein Kästchen, durch dessen Anwahl Sie veranlassen, dass der Server nach der Installation von Hyper-V automatisch einen Neustart ausführt. Wählen Sie diese Option nicht aus, so müssen Sie nach Abschluss der Installation »per Hand« einen Neustart ausführen, denn ohne einen solchen kann der Hyper-V nicht eingesetzt werden.
12. Mit einem Klick auf INSTALLIEREN starten Sie dann die eigentliche

Installation der Virtualisierungssoftware auf Ihrem Windows-Server.

Hyper-V konfigurieren

Nachdem Sie nun den Hyper-V auf Ihrem Server installiert haben, stehen eine ganze Reihe von Konfigurationsmöglichkeiten für diese Software zur Verfügung. Dazu rufen Sie zunächst einmal die Konsole des HYPER-V-MANAGER auf. Das können Sie über den SERVER-MANAGER machen, indem Sie dort aus der Leiste am oberen Rand das Menü TOOLS und dann im Pull-down-Menü HYPER-V-MANAGER auswählen. Sie können die Konsole aber ebenso aus dem Startmenü heraus aufrufen.

Da Sie mithilfe dieser Konsole mehrere Hyper-V-Installation auf verschiedenen Systemen über das Netz hinweg verwalten können, müssen Sie nach dem ersten Öffnen der Konsole zunächst Ihren Server auswählen ([Abbildung 11.4](#)).

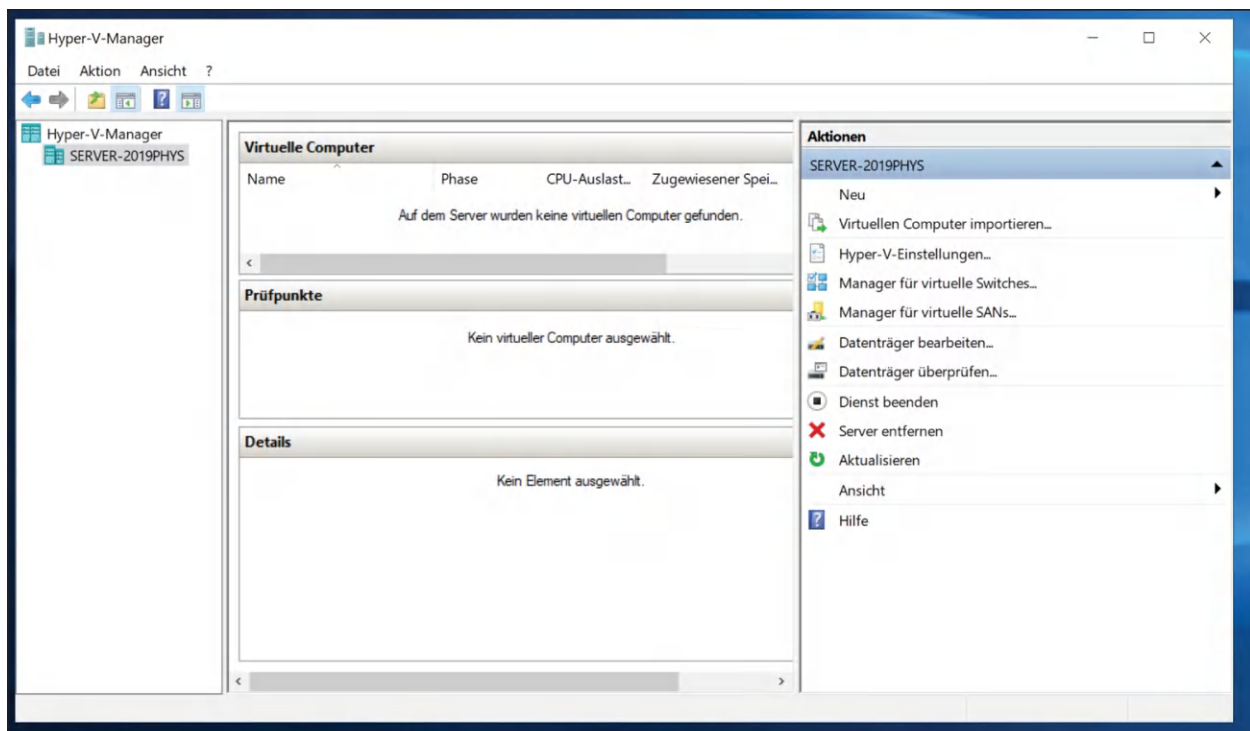


Abbildung 11.4: Die Konsole des Hyper-Managers: Sie erlaubt unter anderem das Erstellen von virtuellen Maschinen sowie deren Überwachung.

Mit einem Rechtsklick auf den Namen Ihres Servers bekommen Sie ein

Menü angezeigt, dessen Einträge Sie zudem im rechten Fenster der Konsole unter der Überschrift AKTIONEN finden können. Ein Klick auf HYPER-V-INSTALLATION präsentiert Ihnen ein Fenster, in dem Sie einige grundlegende Einstellung für die Hyper-V-Rolle vornehmen können ([Abbildung 11.5](#)). Die Einstellungen sind dabei in die Bereiche SERVER und BENUTZER aufgeteilt, je nachdem, worauf die jeweiligen Einstellungen und Features Einfluss haben.

Die ersten sieben Einträge der Liste in diesem Fenster beziehen sich auf verschiedene Bereiche des Hyper-V-Servers:

- ✓ **VIRTUELLE FESTPLATTEN und VIRTUELLE COMPUTER:**
Diese beiden Einträge ermöglichen es Ihnen, den Standard-Speicherort für die virtuellen Festplatten und virtuellen Maschinen neu festzulegen, falls Sie beispielsweise mit den bei der Installation gewählten Pfaden nicht mehr einverstanden sind. Dies sind aber nur grundsätzliche Vorgaben, die Ihnen dann beim Anlegen dieser Ressourcen angezeigt werden, Sie können bei jeder neuen virtuellen Maschine oder virtuellen Festplatte trotzdem noch individuell einen anderen Speicherplatz auswählen.
- ✓ **AUFTEILUNG AUF NUMA:** NUMA steht für »Non-Uniform Memory Access« und ist eine spezielle Architektur für den Arbeitsspeicher von Multiprozessorsystemen. Grundsätzlich ist das Zusammenspiel von virtuellen Systemen und NUMA-Architektur nicht unproblematisch, weshalb Hyper-V mit dieser Einstellung eine spezielle Unterstützung anbietet, die Sie hier aktivieren können.

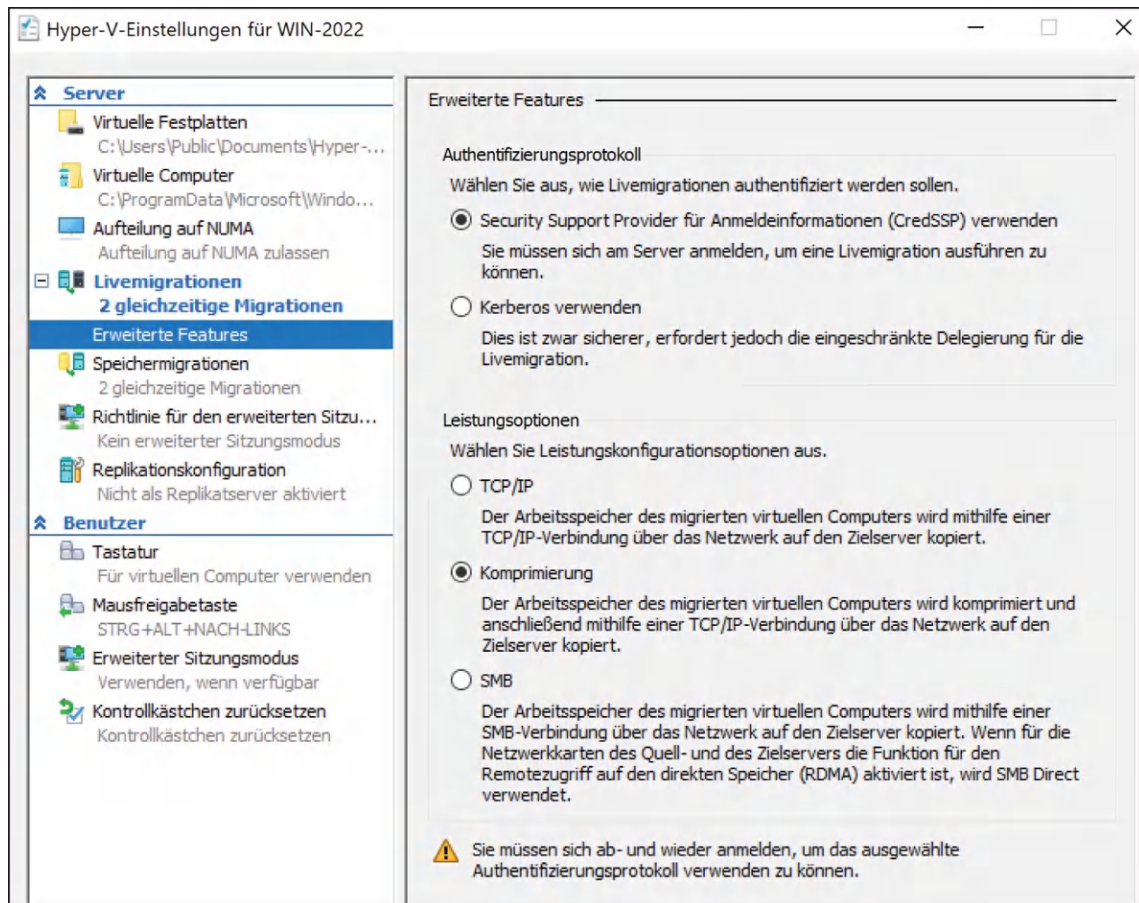


Abbildung 11.5: Etwas verborgen finden sich im Einstellungs Menü von Hyper-V auch die erweiterten Features für die Livemigration.

- ✓ **LIVEMIGRATIONEN:** Die Livemigration ermöglicht es Ihnen, virtuelle Maschinen im laufenden Betrieb von einem Hyper-V-Host auf einen anderen zu verschieben. Diese Einstellung konnten Sie auch schon bei der Installation vorwählen. Allerdings funktioniert das ausschließlich dann, wenn Ihr Server in einer Windows-Domäne angemeldet ist. Ist das der Fall, so können Sie über das Pluszeichen neben LIVEMIGRATIONEN in der linken Spalte zusätzliche Einstellungen wie beispielsweise das Authentifizierungsprotokoll für die Migration festlegen ([Abbildung 11.5](#)).
- ✓ **SPEICHERMIGRATIONEN:** Mithilfe der Speichermigration können Sie einer virtuellen Maschine neuen virtuellen Speicherplatz zuordnen, ohne dass die VM dazu heruntergefahren werden muss. Sie können an dieser Stelle eingeben, wie viele solcher Speichermigrationen gleichzeitig ausgeführt werden können. Der vorgegebene

Standardwert ist »2«.

- ✓ **RICHTLINIE FÜR DEN ERWEITERTEN SITZUNGSMODUS:** Die Aktivierung dieser Richtlinie erlaubt es Ihnen, mithilfe des RDP-Protokolls und beispielsweise dem Programm REMOTEDESKTOPVERBINDUNG auf eine virtuelle Maschine zuzugreifen. Das bietet viele Vorteile, weil Sie auf diese Art Geräte und andere Ressourcen des lokalen Systems mit dem Betriebssystem in der virtuellen Maschine verbinden können. Das muss allerdings vom Gastsystem unterstützt werden. Auch die Darstellung der virtuellen Maschinen auf einem Bildschirm mit höherer Auflösung ist auf diese Weise möglich. Diese Einstellung ist standardmäßig auf dem Windows Server 2019 zunächst deaktiviert. Wenn Sie diese Features nutzen wollen, müssen Sie hier ERWEITERTEN SITZUNGSMODUS ZULASSEN auswählen.
- ✓ **REPLIKATIONSKONFIGURATION:** Mithilfe dieser Einstellung können Sie einen Hyper-V-Server so konfigurieren, dass er als REPLIKATSERVER arbeiten kann. Dabei werden Kopien eines virtuellen Live-Computers eines primären Systems auf den Replikat-Server kopiert, der offline ist. Wenn dann auf dem primären System Probleme auftauchen, kann der Replikat-Server die gesicherten Kopien zurückspielen. Sie können in dieser Einstellung auch einstellen, ob und wie die Übertragung der VMs verschlüsselt werden soll, welche anderen Hyper-V-Systeme diesen Replikat-Server nutzen dürfen und wo die Kopien abgelegt werden.

Die nächsten vier Einstellmöglichkeiten betreffen den Benutzer und wie er mit Hyper-V und vor allen Dingen den darunter aktiven Gastsystemen arbeiten kann:

- ✓ **TASTATUR:** Hier können Sie festlegen, wie der Server mit Windows-Tastenkombinationen wie  +  umgehen soll, wenn auf dem System virtuelle Verbindungen ausgeführt werden. Sie können festlegen, dass sich eine Tastenkombination nur auf das Hostsystem oder nur auf die virtuellen Computer auswirken. Eine dritte Möglichkeit besteht darin, dass sich die Tastenkombination nur auf

virtuelle Systeme im Vollbildmodus auswirken.

- ✓ **MAUSFREIGABETASTE:** Hier können Sie festlegen, welche Tastenkombination Sie verwenden möchten, um den Mauszeiger aus der virtuellen Maschine zu »befreien« und wieder auf dem physischen Host zu verwenden. Sie sollten stattdessen jedoch lieber bei der Installation der Gastsysteme auch die sogenannten Integrationskomponenten mitinstallieren. Sie lösen derartige Probleme automatisch, indem sie beispielsweise einen nahtlosen Übergang des Mauszeigers zwischen VM und Hostsystem ermöglichen.
- ✓ **ERWEITERTER SITZUNGSMODUS:** Hier geht es noch einmal um den erweiterten Sitzungsmodus. Ist das Kästchen in dieser Einstellung aktiviert, so kann ein Benutzer den erweiterten Sitzungsmodus verwenden, wenn das Gastsystem dies erlaubt. Diese Einstellung ist auf Windows Server 2019 standardmäßig aktiviert.
- ✓ **KONTROLLKÄSTCHEN ZURÜCKSETZEN:** Mithilfe dieser Einstellung können Sie Info- und Kontrollkästchen sowie Bestätigungsmeldungen, die in Hyper-V immer wieder auftauchen und die Sie vielleicht »weggeklickt« haben, wiederherstellen.

Manager für virtuelle Switches

Wenn Sie noch einmal einen Blick auf die Menüpunkte werfen, die Ihnen der Hyper-V-Manager unter AKTIONEN anbietet, so werden Sie dort auch den MANAGER FÜR VIRTUELLE SWITCHES finden. Ein solcher virtueller Switch ist extrem wichtig für die virtuellen Maschinen, die Sie später anlegen werden. Denn nur, wenn ein solcher virtueller Switch vorhanden ist, können die installierten Gastbetriebssysteme mit dem physischen Netzwerk oder auch einem internen virtuellen Netzwerk verbunden werden. Grundsätzlich sollten Sie einen solchen virtuellen Switch bereits bei der Installation der Hyper-V-Rolle angelegt haben. Es ist aber möglich, dass Sie diesen Schritt übersprungen haben oder nun einen zweiten Switch für Ihren Server anlegen wollen. Nach einem Klick auf den Eintrag öffnet sich ein Fenster, wie Sie es in [Abbildung 11.6](#) sehen können.

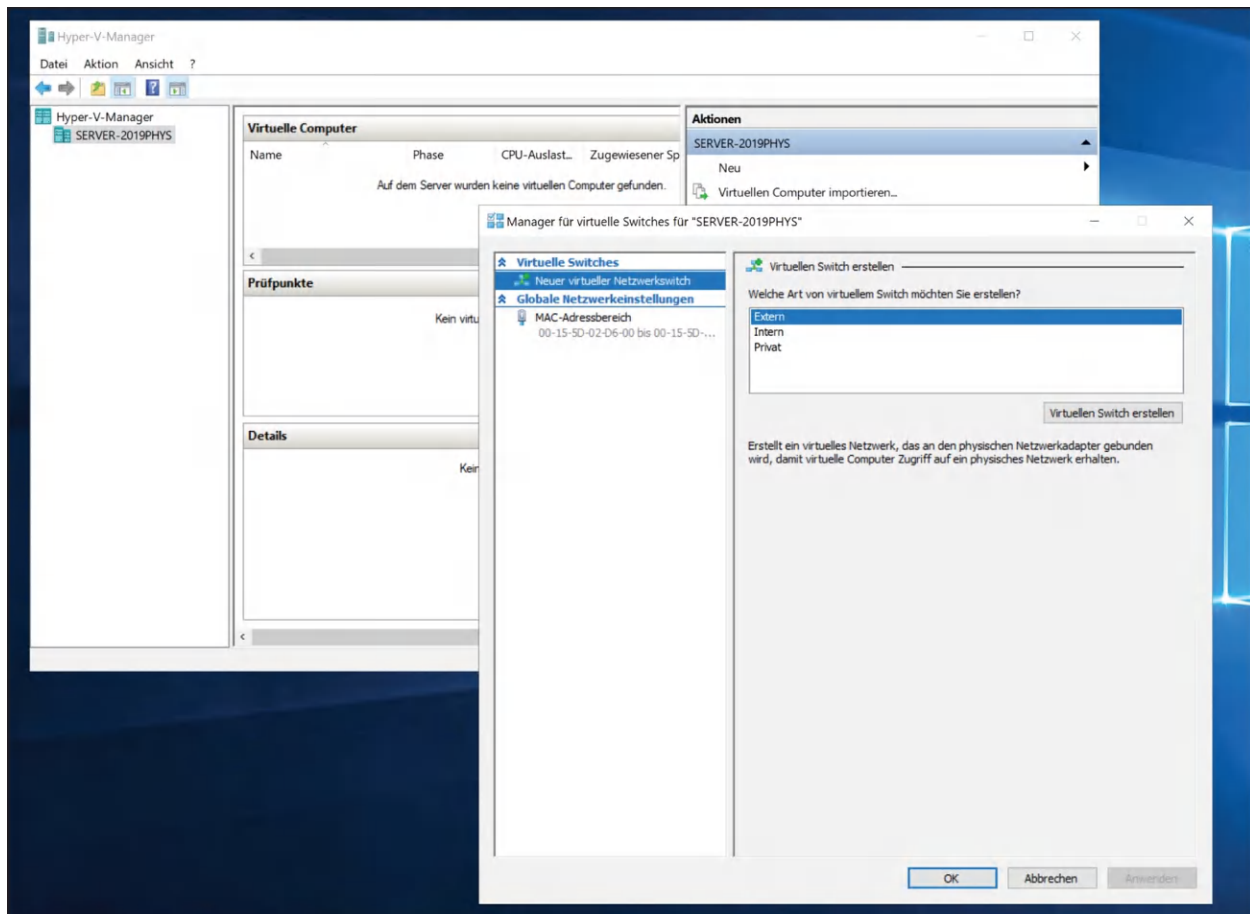


Abbildung 11.6: Der Manager für virtuelle Switches: Ohne einen solchen virtuellen Switch bekommen die VMs keinen Kontakt zum Netzwerk.

Dort haben Sie dann die Möglichkeit, einen neuen virtuellen Switch anzulegen, wobei Ihnen dafür drei Auswahlmöglichkeiten zur Verfügung stehen:

- ✓ EXTERN
- ✓ INTERN
- ✓ PRIVAT



Grundsätzlich kann Hyper-V mehrere virtuelle Switches besitzen und verwenden. Die virtuellen Maschinen verbinden sich über ihre virtuelle Netzwerkkarte mit diesem virtuellen Switch, wobei jeweils nur eine Verbindung zwischen der virtuellen Netzwerkkarte und

einem virtuellen Switch möglich ist. Soll die VM mit mehreren virtuellen Switches verbunden werden, so müssen Sie mehrere Netzwerkkarten anlegen.

Die drei unterschiedlichen Typen des virtuellen Switches unterscheiden sich durch die Art, in der sie Kommunikation mit Netzwerken erlauben: EXTERN ist die Option, die Sie in der Regel bei der Erstinstallation von Hyper-V wählen werden. Durch diesen Typ bekommen virtuelle Maschinen Zugriff auf das gesamte Netzwerk. Ein solcher externer virtueller Switch muss deshalb immer an eine physikalisch vorhandene Netzwerkkarte im Hostsystem gebunden sein. Dabei ist pro Netzwerkkarte nur die Verbindung zu einem Netzwerk möglich. Brauchen Sie Zugang zu mehreren Netzwerken, so müssen Sie weitere Netzwerkadapter im Hostrechner installieren.

Der Typ INTERN erlaubt den virtuellen Maschinen auf einem Hostsystem miteinander und mit dem Hyper-V-Host zu kommunizieren. Das Betriebssystem des Hypervisors kann dabei ebenfalls einen Adapter für dieses virtuelle Netzwerk besitzen und hat dann den entsprechenden Zugriff. Ein interner virtueller Switch wird nicht mit einem physikalischen Netzwerkadapter verbunden, sondern verwendet einen sogenannten vNIC (Virtual Network Adapter), der die Kommunikation zwischen den virtuellen Maschinen und dem Hyper-V-Host ermöglicht.

Der Typ PRIVAT weist schließlich die weitgehendsten Einschränkungen auf: In diesem Fall können nur die virtuellen Maschinen miteinander kommunizieren, das Hostsystem kann nicht daran teilnehmen. Auch ein solcher virtueller Switch hat dann keine Verbindung zu einem physikalischen Netzwerkadapter. Durch diese vollständige Isolation eignet sich dieser Typ besonders gut für abgeschottete Testnetzwerke.

Einrichten eines virtuellen Switches

Das Anlegen eines virtuellen Switches ist oftmals der erste Schritt zum Einsatz der Hyper-V-Rolle auf Windows Server 2019. Wir erläutern hier

exemplarisch die Erstellung eines externen Switches:

1. Öffnen Sie den HYPER-V-MANAGER und klicken Sie unter Aktionen auf den Eintrag MANAGER FÜR VIRTUELLE SWITCHES.
2. In der linken Spalte wählen Sie unter VIRTUELLE SWITCHES den Eintrag NEUER VIRTUELLER NETZWERKSWITCH aus.
3. Nun können Sie Ihrem neuen Switch im rechten Fensterbereich unter EIGENSCHAFTEN FÜR VIRTUELLEN SWITCH einen Namen geben und optional im Feld ANMERKUNGEN noch zusätzliche Informationen dazu eintragen ([Abbildung 11.7](#)).

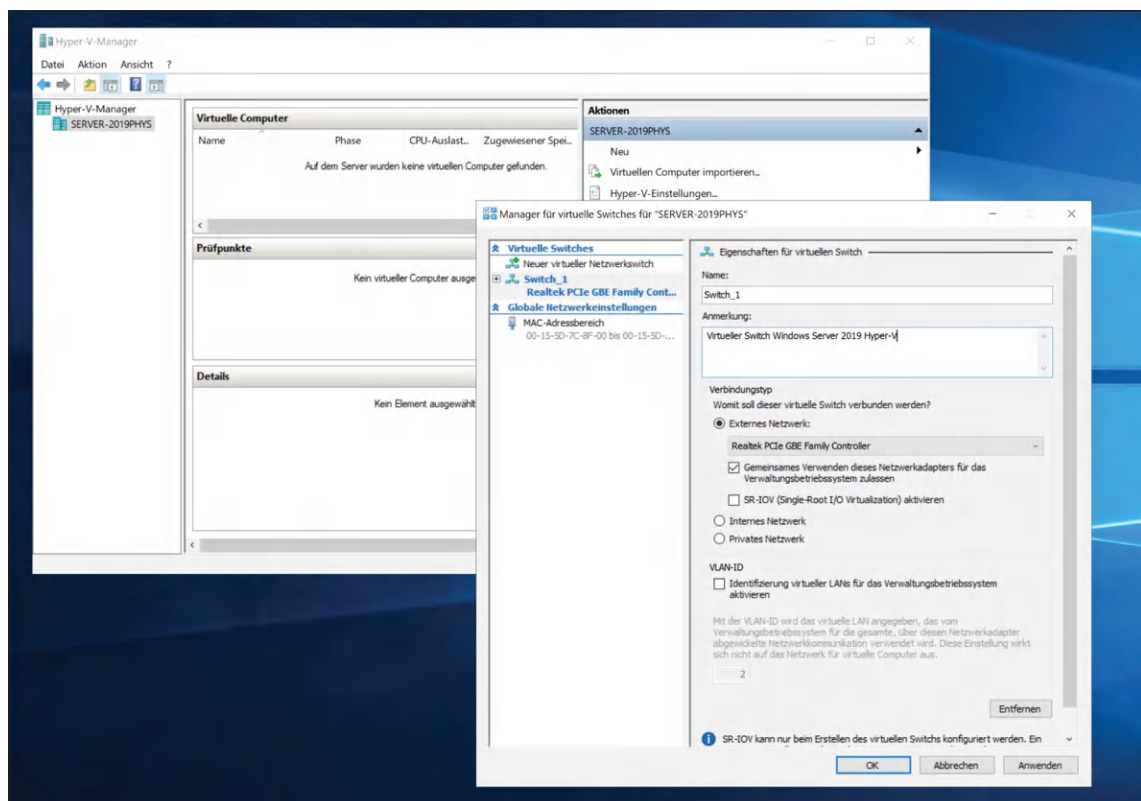


Abbildung 11.7: Das Anlegen eines ersten externen virtuellen Switches ist mit dem Hyper-V-Manager schnell erledigt.

4. Danach wählen Sie unter Verbindungstyp EXTERNES NETZWERK und aus dem Pull-down-Menü darunter Ihre Netzwerkkarte aus. Wenn Ihr Server nur mit einer Netzwerkkarte ausgestattet ist, dann müssen Sie unbedingt auch das Kästchen darunter für GEMEINSAMES

VERWENDEN DES NETZWERKADAPTERS FÜR DAS VERWALTUNGSBETRIEBSSYSTEM ZULASSEN aktivieren. Nur damit stellen Sie sicher, dass das Hostsystem nach der Erstellung des virtuellen Switches noch über die Netzwerkkarte erreichbar ist.

5. Danach können Sie die Einstellungen mit ANWENDEN und anschließendem OK übernehmen.

Sie bekommen nach eine Warnmeldung angezeigt, dass die Netzwerkverbindung zu diesem Hostsystem kurzzeitig unterbrochen wird, damit der virtuelle Switch angelegt werden kann. Nachdem der Switch angelegt wurde, finden Sie in den Netzwerkeinstellungen bei den Netzwerkadaptern des Hostsystems einen HYPER-V VIRTUAL ETHERNET ADAPTER, der vom System als VETHERNET bezeichnet wird ([Abbildung 11.8](#)). Hyper-V realisiert dieses »Teilen« des Netzwerkadapters dadurch, dass es eben diesen virtuellen Netzwerkadapter für das Betriebssystem der Management-Plattform anlegt und diesen mit dem gleichen virtuellen Switch verbindet, den auch die virtuellen Maschinen benutzen. Deshalb ist es für Sie auch nur dann notwendig, diese Checkbox auszuwählen, wenn sich nur eine Netzwerkkarte im Hostsystem befindet und Sie sicherstellen müssen, dass das Management-Betriebssystem auf diesem bestimmten physikalischen Adapter kommunizieren muss.

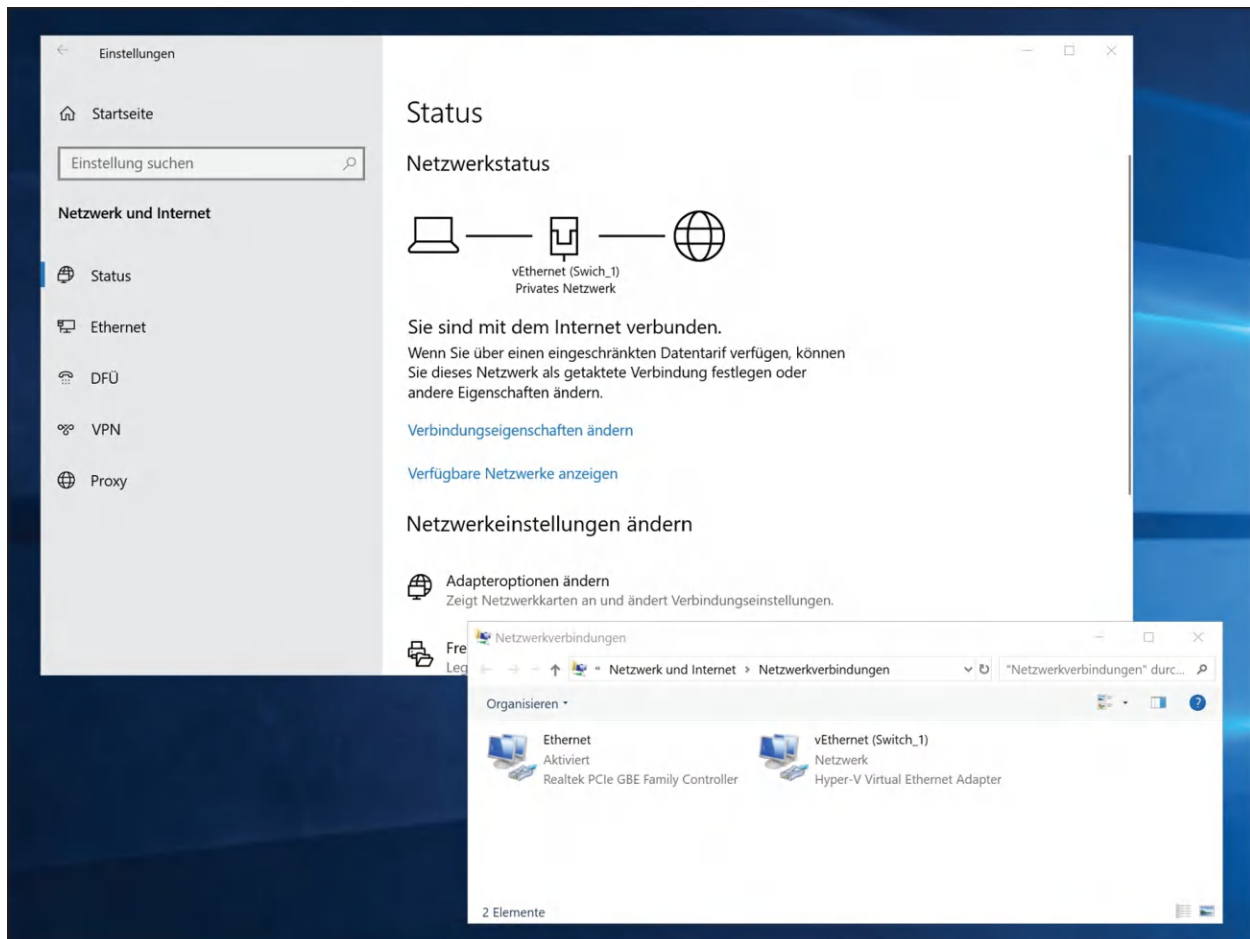


Abbildung 11.8: Nachdem der Switch angelegt wurde, existiert ein virtueller Netzwerkadapter auf dem Hostsystem, der als vEthernet bezeichnet wird.

Virtueller Switch und die PowerShell

Wie bei fast allen Systemfeatures und -möglichkeiten, die von den modernen Windows-Systemen bereitgestellt werden, können Administratoren und Anwender natürlich auch die Hyper-V-Virtualisierung mithilfe der PowerShell verwalten, einrichten, steuern und kontrollieren. Haben Sie die Server-Rolle Hyper-V konfiguriert, so können Sie auf das Modul »Hyper-V« der PowerShell zugreifen. So reicht dann der Aufruf von:

`Get-Command -Module Hyper-V`

in der PowerShell, um eine entsprechend lange Liste der verfügbaren Cmdlets auf den Bildschirm zu bringen. Geht es nur um die Cmdlets für den virtuellen Switch, so können Sie sich diese beispielsweise mit dem

folgenden Aufruf anzeigen lassen:

```
Get-Command -Module Hyper-V | select-string "switch"
```

Mithilfe der verschiedenen Cmdlets, die Sie in [Abbildung 11.9](#) sehen können, haben Sie die Möglichkeit, alle Arbeiten rund um den Virtual Switch auf diese Weise sowohl mithilfe von Skripten zu automatisieren oder auch auf Remote-Systemen auszuführen. Dabei ist es selbstverständlich notwendig, diese Kommandos in einer PowerShell mit Administratorrechten auszuführen.

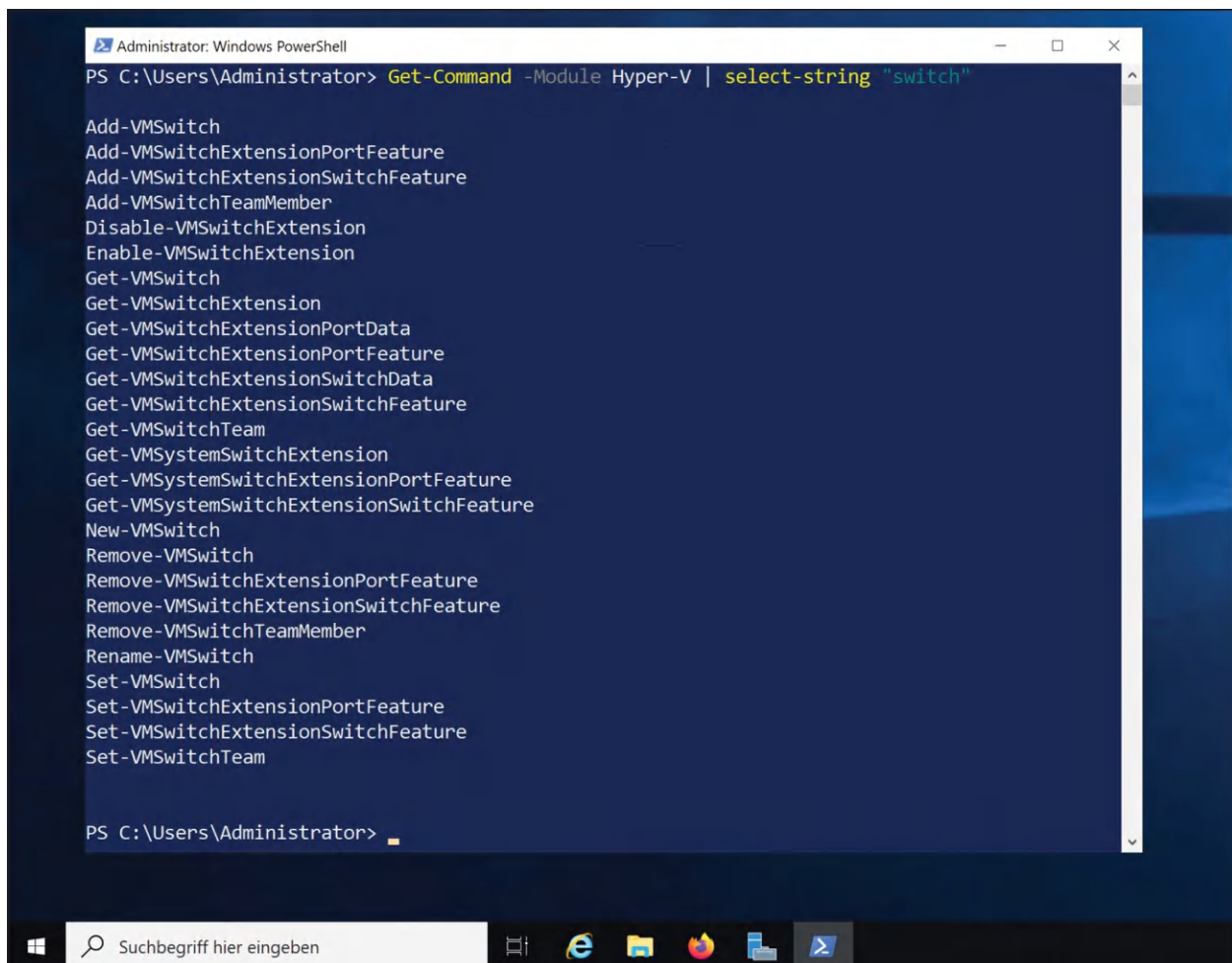


Abbildung 11.9: Das Modul Hyper-V der PowerShell stellt auch eine Reihe von Befehlen für die Arbeit mit virtuellen Switches bereit.

Dazu müssen Sie zunächst einmal feststellen, welche Netzwerkadapter im Hostsystem zu Verfügung stehen. Das gelingt am einfachsten mit dem Cmdlet `Get-Netadapter`. So können Sie beispielsweise mit dem

folgenden Aufruf die Bezeichnung des vorhandenen Ethernet-Adapters einer Variablen zugewiesen, um daran anschließend mithilfe des Kommandos New-VMSwitch einen neuen Switch anzulegen:

```
$Netzwerkkarte = Get-NetAdapter -Name Ethernet  
New-VMSwitch -Name NeuerSwitch -NetAdapterName  
$Netzwerkkarte.Name  
-AllowManagementOS $true
```

Mit diesen Kommandos wird ein neuer Switch mit dem Namen »NeuerSwitch« auf dem Hostsystem angelegt. Bei dieser Art des Aufrufs wird durch die Verwendung des Parameters -NetAdapterName implizit der Typ auf EXTERN gesetzt. Zudem bindet die Übergabe dieses Namens den virtuellen Switch an die angegebene physikalische Netzwerkschnittstelle. Der Parameter -AllowManagementOS <Boolean> erlaubt die Angabe von \$true oder \$false. Ist er »eingeschaltet« (im Beispiel mit dem Boolean-Wert »true« versehen), so steht der externe Switch sowohl dem Hostsystem als auch den virtuellen Systemen für den Netzwerkzugriff zur Verfügung. Zu Überprüfung können Sie nach der Ausführung des PowerShell-Kommandos den Hyper-V-Manager aufrufen. Dort finden Sie im Manager für virtuelle Switches den neu angelegten Switch mitsamt den entsprechend ausgewählten Kästchen bei den Einstellungen, wie in der [Abbildung 11.10](#) zu sehen.

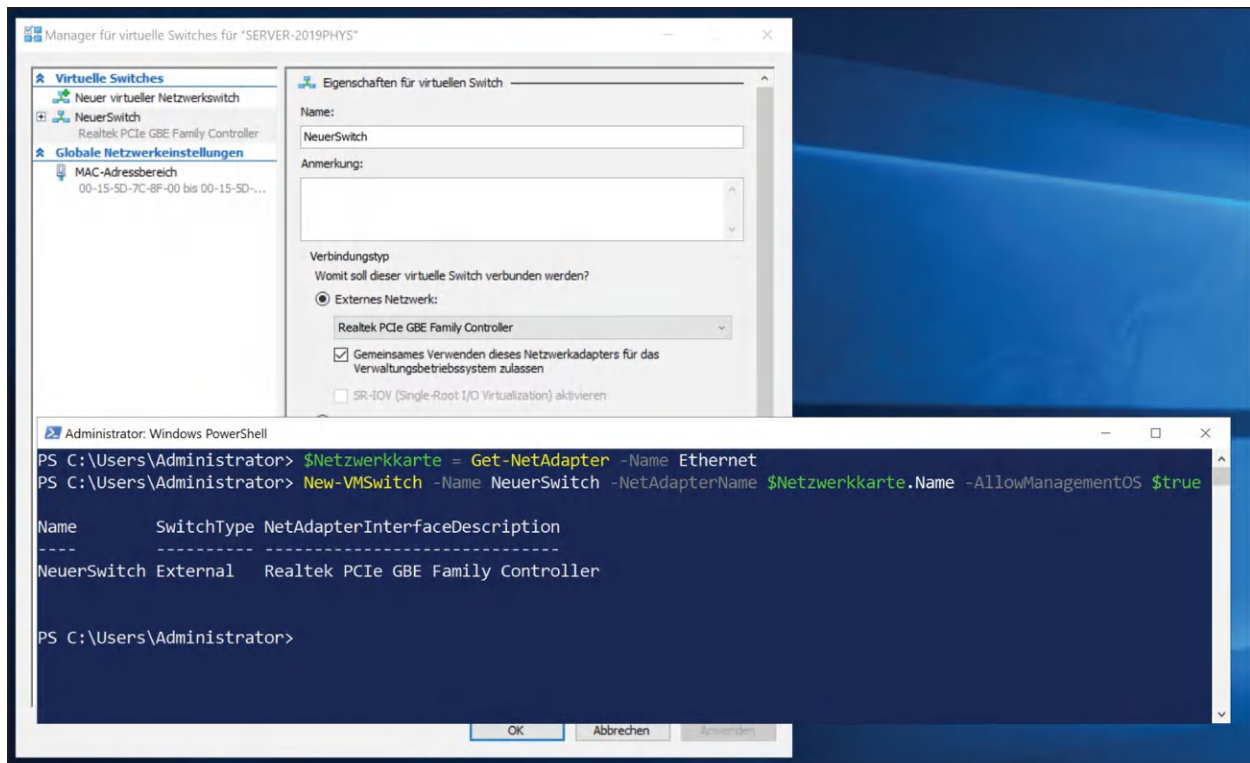


Abbildung 11.10: Das Anlegen und Zuweisen eines neuen virtuellen Switches ist mithilfe der PowerShell problemlos und schnell erledigt.

Möchten Sie mithilfe der PowerShell einen internen oder privaten Switch anlegen, so können Sie dazu den Parameter `-SwitchType <Typ des Switches>` für das Cmdlet `New-VMSwitch` verwenden. Dieser Parameter erlaubt entweder den Wert `Internal` oder `Private` als Typ, woraufhin das Cmdlet den entsprechenden Switch anlegt.

```
New-VMSwitch -name Interner -SwitchType Internal
```


Kapitel 12

Virtuelle Computer einsetzen

IN DIESEM KAPITEL

- Was eine virtuelle Maschine ausmacht
- Anlegen einer virtuellen Maschine
- Konfiguration der virtuellen Maschine
- Einen virtuellen Windows-Computer installieren

Nachdem wir nun ausführlich darüber gesprochen haben, wie Sie die Hyper-V-Rolle installieren und konfigurieren, wollen wir sie nun ihrem eigentlichen Zweck zuführen: dem Betrieb von virtuellen Maschinen samt Gastsystemen. Mithilfe des Hyper-V-Managers können diese VMs nicht nur eingerichtet, sondern auch verwaltet und betreut werden. Dabei werden die als Gastssysteme bezeichneten Betriebssysteme in den virtuellen Maschinen nicht nur auf die gleiche Art und Weise installiert, wie Sie es von einer »normalen« Installation auf PC-Hardware gewohnt sind, auch der Betrieb läuft im Großen und Ganzen ebenso so wie in der »realen Welt« ab. Damit das funktionieren kann, bieten Ihnen Hyper-V und die virtuellen Maschinen eine entsprechend umfangreiche Auswahl an Einstellmöglichkeiten und Features, die wir Ihnen in diesem Kapitel näherbringen wollen.

Anlegen einer virtuellen Maschine

Hyper-V unterstützt eine große Zahl von Gastsystemen. Neben Windows-Client-Betriebssysteme von Windows 7 mit SP1 über Windows 8.1 und Windows 10 können auch Windows-Server ab Windows Server 2008 SP2 in den virtuellen Maschinen betrieben werden. Unter <https://docs.microsoft.com/de-de/windows->

[server/virtualization/hyper-v/supported-windows-guest-operating-systems-for-hyper-v-on-windows](https://docs.microsoft.com/de-de/windows-server/virtualization/hyper-v/supported-windows-guest-operating-systems-for-hyper-v-on-windows) finden Sie die detaillierten Beschreibungen dazu. Diese Auflistung bedeutet nicht, dass Sie eine Version von Windows Vista oder gar Windows XP nicht als Gastsystem installieren könnten. Microsoft unterstützt diese Konfigurationen nur nicht mehr, und entsprechende Integrationsdienste, durch die eine Zusammenarbeit zwischen Gast- und Hostsystem deutlich erleichtert wird, stehen für solche alten Systeme ebenfalls nicht zur Verfügung.

Auch eine ganze Reihe von Linux-Derivaten können Sie als Gastsystem im Hyper-V betreiben. Hier reicht das Angebot von Red Hat Enterprise über Debian und Ubuntu bis hin zu CentOS und FreeBSD. Microsoft empfiehlt hier aber gerade im Hinblick auf die Treiber jeweils spezielle Versionen der Linux-Gastsysteme. Auch hierzu können Sie auf den Microsoft-Seiten unter <https://docs.microsoft.com/de-de/windows-server/virtualization/hyper-v/supported-linux-and-freebsd-virtual-machines-for-hyper-v-on-windows> entsprechend detaillierte Informationen finden.

Wie schon bei anderen Konfigurationen und Einstellungen stellt Ihnen der Windows-Server auch hier wieder einen entsprechenden Assistenten bereit, der Sie durch das Anlegen einer virtuellen Maschine führt.

1. Starten Sie den HYPER-V-MANAGER (entweder aus dem Menü TOOLS im SERVER-MANAGER oder direkt aus dem Startmenü heraus).
2. Wählen Sie im Pull-down-Menü unter AKTION den Eintrag NEU und dann VIRTUELLER COMPUTER... aus ([Abbildung 12.1](#)). Sie erreichen das gleiche Menü auch über einen Rechtsklick auf den Namen Ihres Servers im HYPER-V-MANAGER.

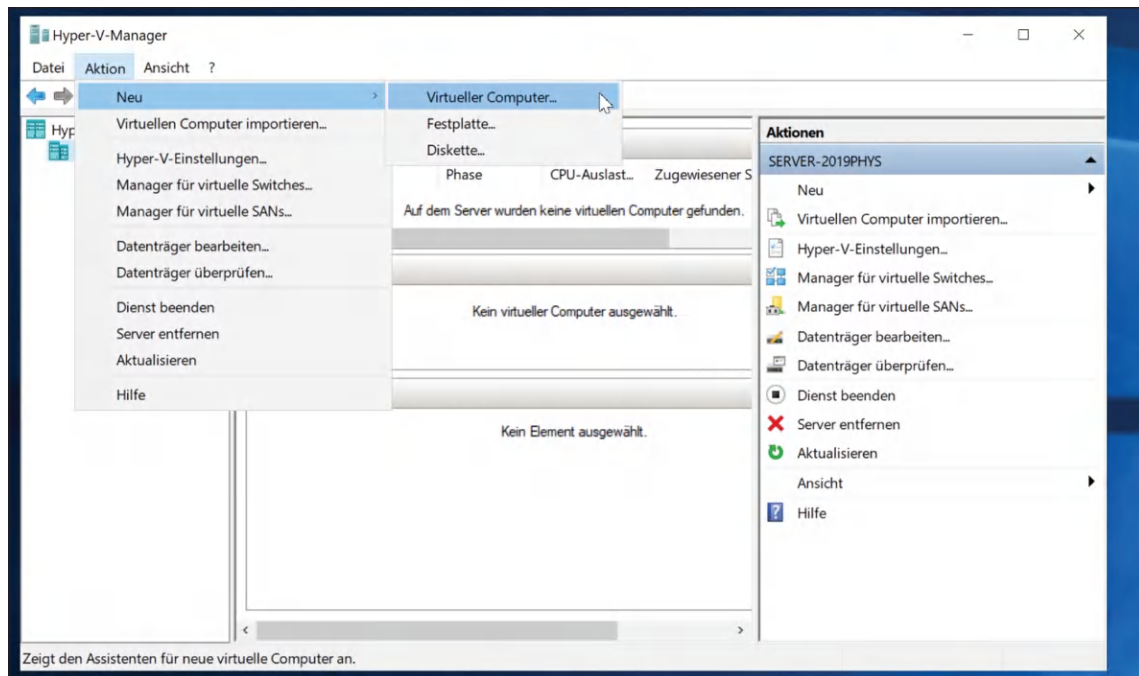


Abbildung 12.1: Der Eintrag »Virtueller Computer« führt zum Assistenten für das Anlegen einer neuen virtuellen Maschine.

3. Auch dieser Assistent startet wieder mit einem Bildschirm, der einige »Vorbemerkungen« anzeigt. Sie können diesen Bildschirm einfach mit WEITER überspringen. Möchten Sie, dass er nicht mehr bei jedem Anlegen einer neuen virtuellen Maschine angezeigt wird, so finden Sie unten auf der Seite ein kleines Kästchen mit der Beschriftung DIESE SEITE NICHT MEHR ANZEIGEN.
4. Auf dem nächsten Bildschirm können Sie nun einen Namen für Ihre virtuelle Maschine eingeben und den Speicherort ändern, an dem diese Daten auf der Festplatte abgelegt werden sollen, falls Sie nicht einfach den voreingestellten Pfad übernehmen wollen.
5. Auf dem folgenden Bildschirm müssen Sie festlegen, welche Generation Sie für Ihre virtuelle Maschine wählen wollen. Sie sollten hier grundsätzlich die GENERATION 2 wählen, die Ihnen die neueren, fortgeschritteneren Möglichkeiten und Features zu bieten hat ([Abbildung 12.2](#)). Nur wenn Sie ein älteres vielleicht auch 32-Bit-Betriebssystem als Gastsystem in der VM betreiben wollen, sollten Sie die GENERATION 1 auswählen.

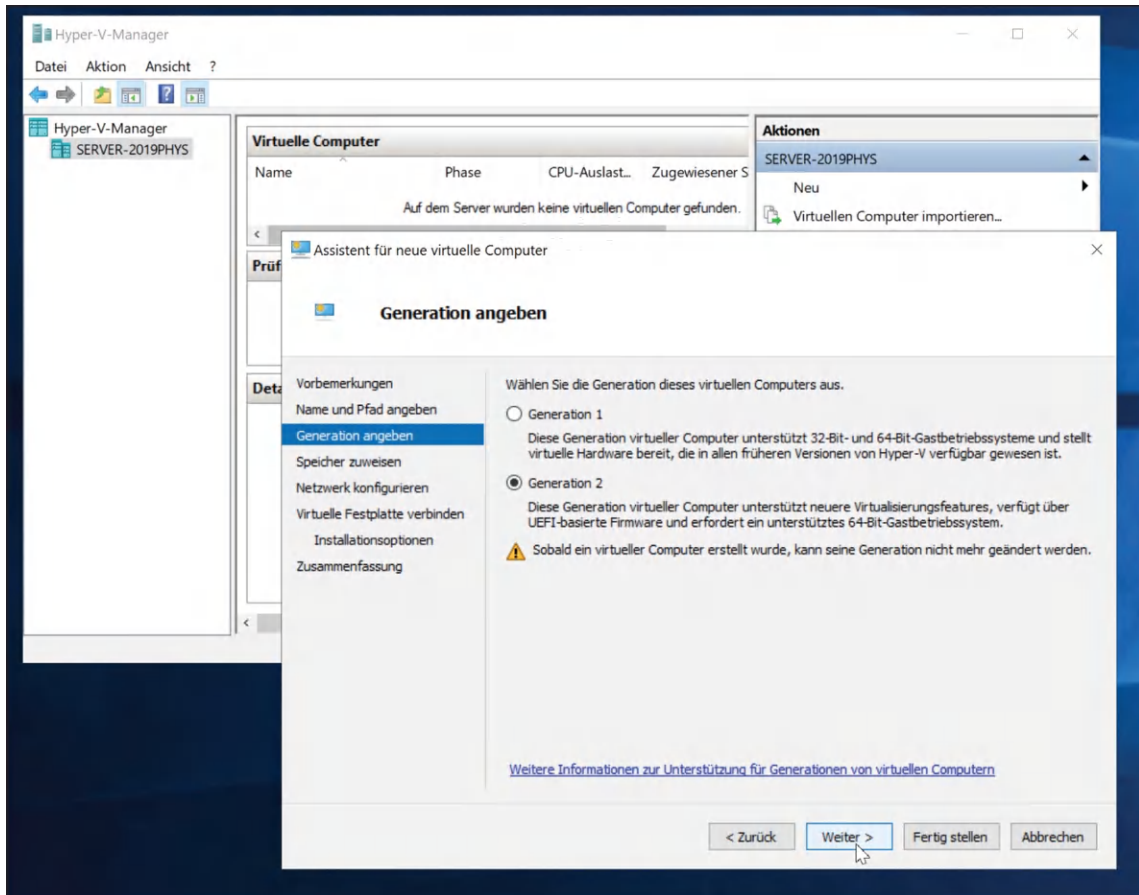


Abbildung 12.2: Die Wahl der Generation einer virtuellen Maschine ist davon abhängig, wie »modern« das zu installierende Gastsystem ist.



Hyper-V bietet auf dem Windows Server 2019 wie auch auf der Versionen 2016 und 2012 R2 zwei Typen von virtuellen Maschinen an, die als Generation 1 und Generation 2 bezeichnet werden. Handelt es sich bei Ihren Gastsystemen um moderne 64-Bit-Betriebssysteme wie beispielsweise Windows 10, so ist die Generation 2 in der Regel die richtige Wahl. In solchen virtuellen Maschinen steht Ihnen dann unter anderem auch UEFI-Unterstützung (Unified Extensible Firmware Interface) zur Verfügung. Nur mit dieser modernen Variante des Boot-Loaders (die heute auch in den meisten PC-Systemen zu finden ist) können Sie dann auch eine Secure-Boot-Option des Betriebssystems verwenden.

Viele aktuelle Linux-Derivate werden ab Windows Server 2019

auch in virtuellen Maschinen der Generation 2 unterstützt. Wollen oder müssen Sie ein Gastsystem in der 32-Bit-Variante installieren, so bleibt Ihnen nur die Wahl der Generation 1 für die virtuelle Maschine. Leider ist es nicht möglich, nach der Erstellung einer virtuellen Maschine deren Generation zu verändern. Das erfordert immer eine komplette Neuinstallation des Gastsystems.

6. Es folgt der Bildschirm für die Zuweisung von Hauptspeicher für die virtuelle Maschine. Windows Server 2019 gibt hier als Standardwert für den Start eine VM 1024 MByte vor, was für moderne Betriebssysteme doch etwas sehr knapp dimensioniert ist. Wir raten dazu, hier einen Startwert von mindestens 4096 MByte auszuwählen, und wir wählen in der Regel für alle virtuellen Maschinen das Kästchen für die Option DYNAMISCHEN ARBEITSSPEICHER FÜR DIESEN VIRTUELLEN COMPUTER VERWENDEN aus. Bei der Zuweisung von Arbeitsspeicher für die virtuellen Maschinen müssen Sie natürlich auch immer den im Hostsystem installierten Arbeitsspeicher in Ihren Berechnungen mit einbeziehen: Zwei aktive virtuelle Maschinen, die jeweils beim Start schon 16 GByte Hauptspeicher belegen, werden ein Server-System mit nur 32 GByte physikalisch vorhandenem Hauptspeicher (was für einen Windows-Server generell eher knapp bemessen ist) sehr schnell zum Stillstand bringen, auch wenn Hyper-V mit der dynamischen Zuweisung von Arbeitsspeicher sehr gut eingreifen kann.
7. Auf dem folgenden Bildschirm NETZWERK KONFIGURIEREN können Sie dann einen zuvor angelegten Virtual Switch mit dem Netzwerkadapter der virtuellen Maschine verbinden ([Abbildung 12.3](#)). Konfigurieren Sie die Netzwerkverbindung auf diesem Schirm nicht, wird Hyper-V zwar eine virtuelle Maschine anlegen, diese wird dann aber keine Verbindung zu einem Netzwerk besitzen. Wie alle anderen Einstellungen mit Ausnahme der Generation einer VM können Sie diese Werte später noch ändern.

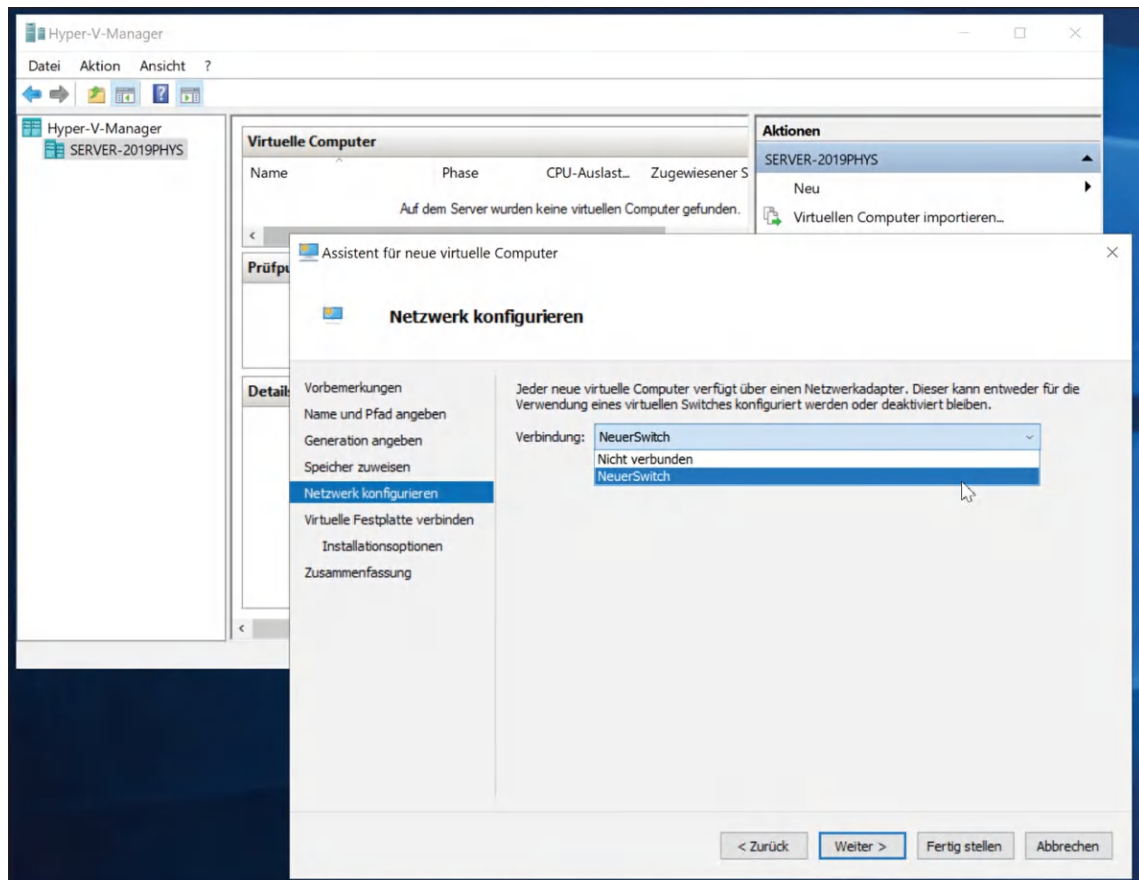


Abbildung 12.3: Unter »Netzwerk konfigurieren« legen Sie fest, ob und mit welchem virtuellen Switch Ihre virtuelle Maschine verbunden ist.

8. Nun geht es darum, Festplattenplatz für Ihre virtuelle Maschine anzulegen oder der VM eine bereits vorhandene virtuelle Festplatte zuzuweisen. Diesen Schritt können Sie auf dem Bildschirm **VIRTUELLE FESTPLATTE VERBINDEN** zunächst auch überspringen, indem Sie **VIRTUELLE FESTPLATTE SPÄTER ZUORDNEN** auswählen ([Abbildung 12.4](#)). Allerdings können Sie natürlich nur dann ein Gastsystem in der virtuellen Maschine installieren, wenn auch entsprechender Platz auf einer virtuellen Festplatte zur Verfügung steht. Falls nicht schon eine derartige Datei auf Ihrem System vorhanden ist, sollten Sie hier also die Option **VIRTUELLE FESTPLATTE ERSTELLEN** auswählen. Standardmäßig wird Ihnen hier eine Größe von 127 GByte vorgeschlagen, die Sie übernehmen oder auch verändern können. Auch bei diesen Einstellungen können Sie später noch Veränderungen vornehmen und dabei die Größe der virtuellen Festplatte verändern

oder Ihrer virtuellen Maschine eine neue virtuelle Festplatte zuordnen.

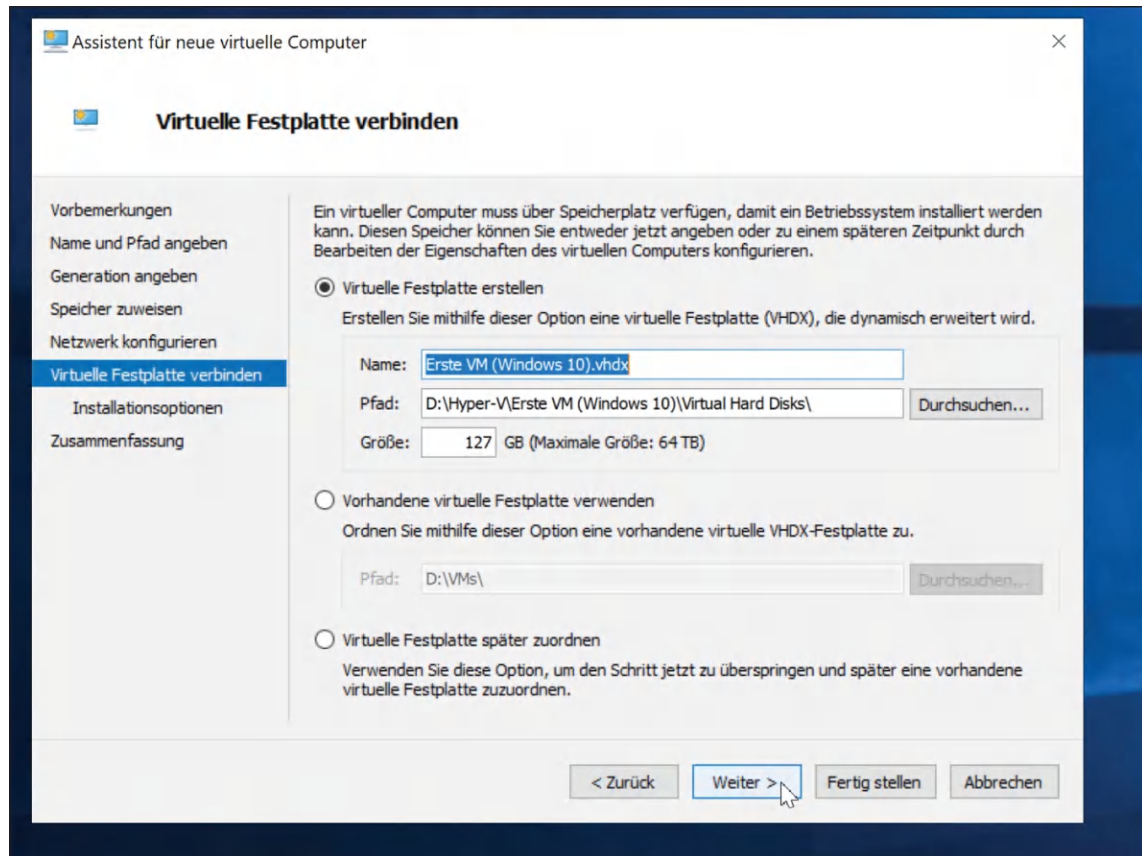


Abbildung 12.4: Hier können Sie die virtuelle Festplatte anlegen und konfigurieren, auf der später das Gastsystem installiert wird.

9. Haben Sie die Festplatte neu erstellt oder eine vorhandene virtuelle Festplatte zugeordnet, können Sie nun auf dem nächsten Bildschirm mit der Bezeichnung **INSTALLATIONSOPTIONEN** entscheiden, ob Sie sofort ein Gastsystem installieren wollen oder zunächst einfach nur die leere virtuelle Maschine (quasi den »nackten PC« ohne Betriebssystem) anlegen wollen. Entscheiden Sie sich zur sofortigen Installation nach der Fertigstellung der virtuellen Maschine, so müssen Sie nun entweder einen Pfad zu einer startbaren ISO-Datei mit dem Betriebssystem oder einen Netzwerkpfad zu einem Installationsserver angeben. Wir haben zunächst einmal die Option **BETRIEBSSYSTEM ZU EINEM SPÄTEREN ZEITPUNKT INSTALLIEREN** ausgewählt.
10. Sie sehen nun den letzten Bildschirm des Assistenten, der Ihnen unter der Überschrift **ABSCHLIEßEN DES ASSISTENTEN FÜR NEUE**

VIRTUELLE COMPUTER noch einmal die von Ihnen gewählten Einstellungen auflistet ([Abbildung 12.5](#)).

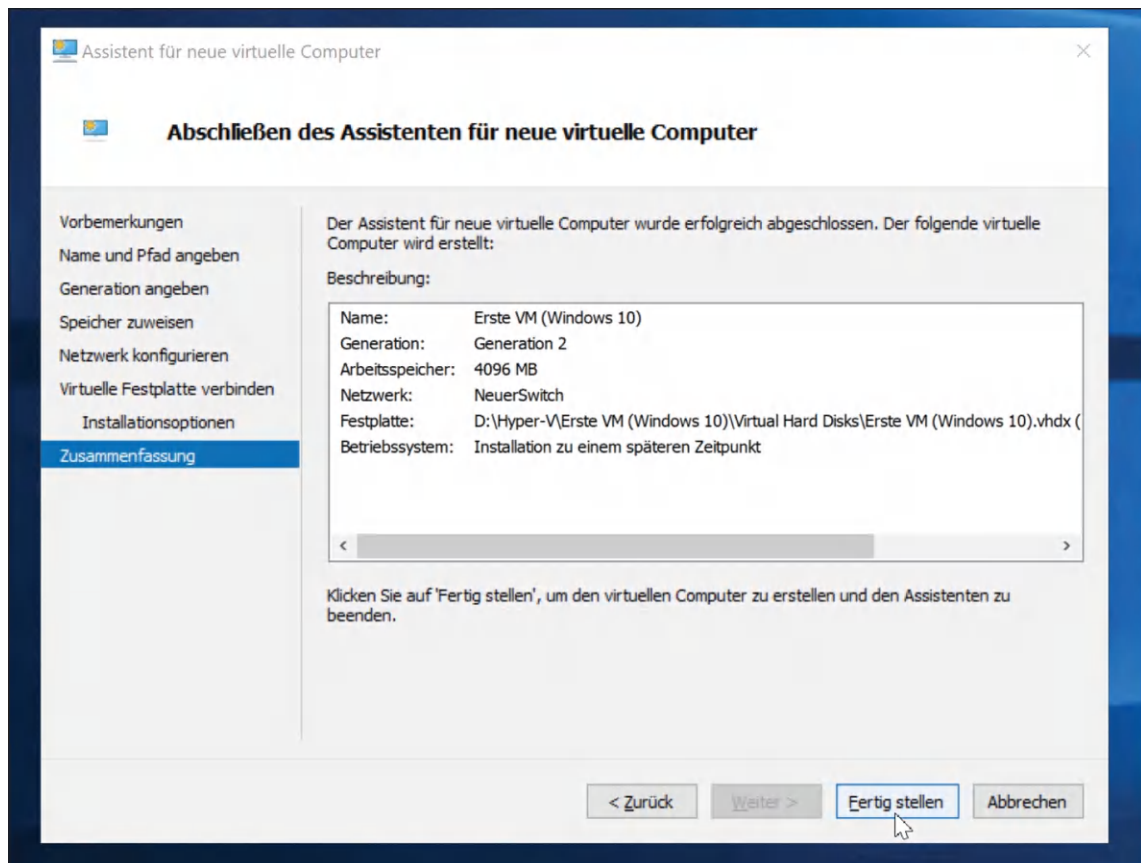


Abbildung 12.5: Die abschließende Zusammenfassung zeigt alle Einstellung, die Sie zum Anlegen der virtuellen Maschine vorgenommen haben.

11. Sind Sie der Meinung, dass alle Einstellungen richtig sind, können Sie nun durch Auswahl von FERTIG STELLEN den virtuellen Computer anlegen. Möchten Sie noch einen Wert oder eine Einstellung verändern, können Sie entweder mit ZURÜCK die einzelnen Schritte der Reihe nach rückwärts durchgehen, oder Sie klicken in der linken Spalte des Fensters direkt auf die Bezeichnung, zu deren Bildschirm Sie zurückkehren möchten.

Konfiguration der virtuellen Maschine

Sie haben beim Anlegen der virtuellen Maschine sicherlich bemerkt, dass Sie nur eine sehr begrenzte Anzahl von Konfigurationsmöglichkeiten hatten. So konnten Sie aber auch relativ schnell und leicht mithilfe des Assistenten zunächst einmal das »Grundgerüst« der virtuellen Maschine anlegen. Für die Feinarbeit können Sie nun noch weitere Einstellungen der frisch angelegten VM verändern.



Wir haben in unserem Beispiel eine virtuelle Maschine der 2. Generation angelegt, auf die wir uns im weiteren Verlauf unserer Erläuterungen beziehen. Wenn Sie hingegen eine VM der 1. Generation angelegt haben, werden Ihnen sicher einige kleine Unterschiede zu der nun folgenden Beschreibung auffallen, da diese virtuellen Maschinen einige der erweiterten Features für neuere Betriebssysteme nicht unterstützen können.

Sie finden Ihre erste virtuelle Maschine in der Konsole aufgelistet und sehen dann auch in [Abbildung 12.6](#), dass diese VM noch mit keinem Betriebssystem ausgestattet wurde. Auf der rechten Seite finden Sie jetzt Einstell- und Konfigurationsmöglichkeiten für diese VM. Das gleiche Menü bekommen Sie auch angezeigt, wenn Sie einen Rechtsklick direkt auf die virtuelle Maschine im Hyper-V-Manager ausführen ([Abbildung 12.6](#)).

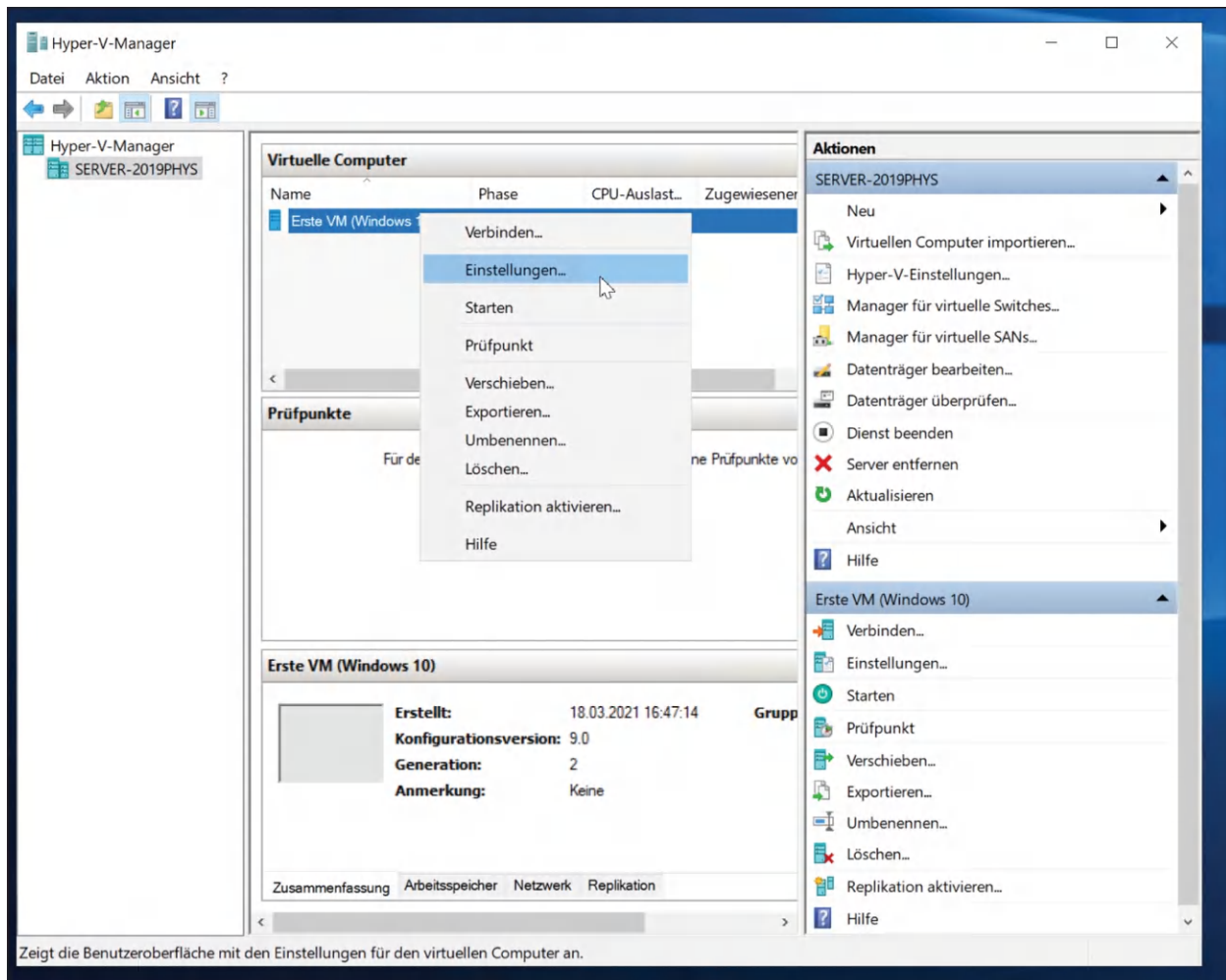


Abbildung 12.6: Die noch »leere« virtuelle Maschine kann nun über die Einstellungen weiter konfiguriert werden.

Wählen Sie aus diesem Menü den Eintrag **EINSTELLUNGEN...** aus. Dann bekommen Sie ein Fenster mit einer langen Liste mit den verschiedenen Einstellungen Ihres virtuellen PCs angezeigt. Diese Liste ist im Menü auf der linken Seite des Fensters in die Bereiche **HARDWARE** und **VERWALTUNG** aufgeteilt. ([Abbildung 12.7](#)). Auf die gleiche Art, wie Sie einen »echten« PC mit neuer oder erweiterter Hardware aufrüsten können, stehen Ihnen hier auch die verschiedenen Erweiterungen zur Verfügung.

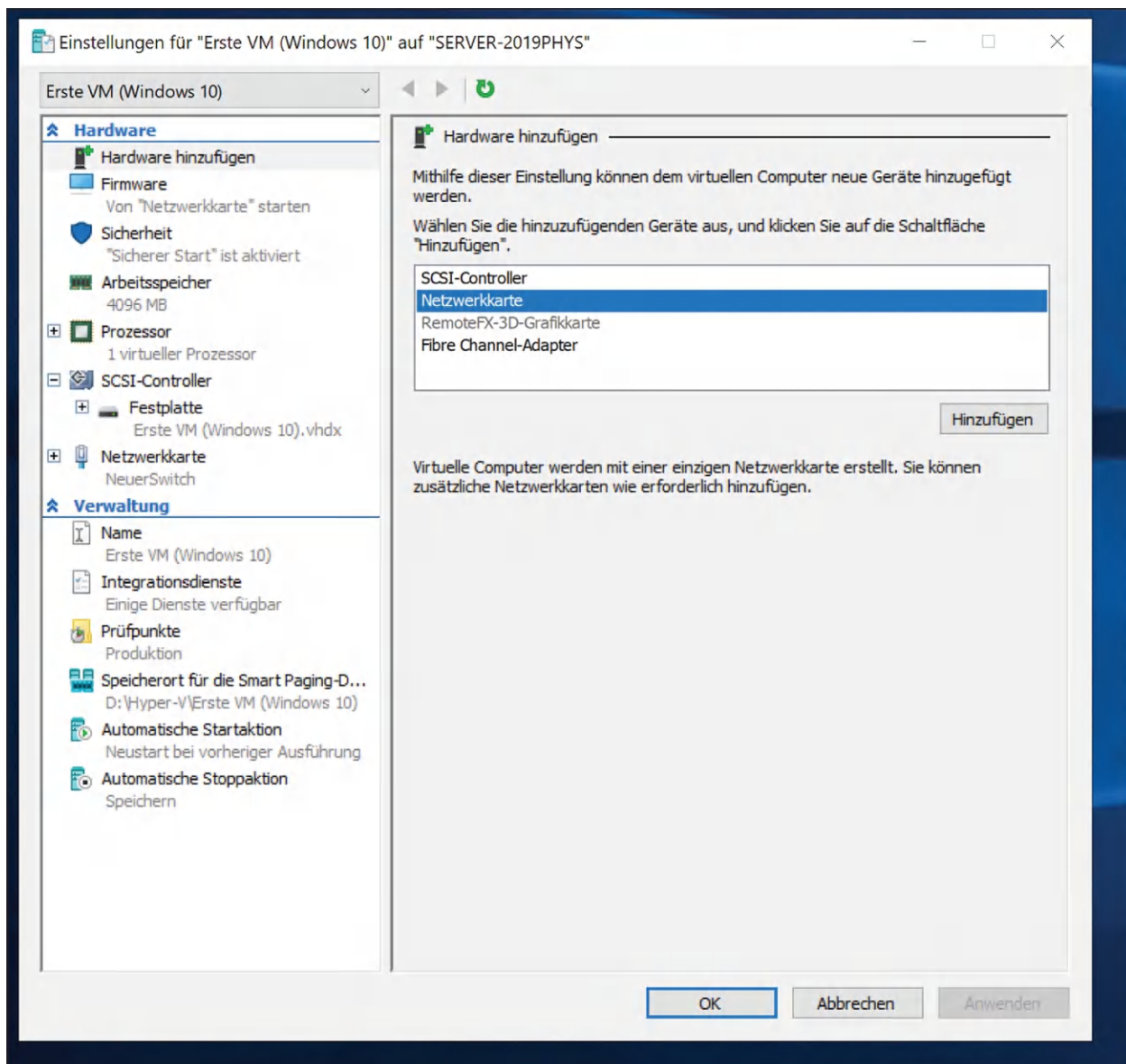


Abbildung 12.7: Konfiguration und Verwaltung wie bei einem »echten« PC: Diese Einstellungen helfen, die virtuelle Maschine richtig zu konfigurieren.

Wir schauen uns deshalb nun zunächst den Bereich **HARDWARE** etwas genau an:

- ✓ **HARDWARE HINZUFÜGEN:** Hier können Sie Ihren »virtuellen Rechner« mit weiterer Hardware ausrüsten. Besonders nützlich sind hier beispielsweise zusätzliche Netzwerkkarten, wenn es um den Einsatz komplexerer Szenarien geht. Ein zusätzlicher SCSI-Adapter (Small Computer System Interface) für die Festplattenanbindung kann sich ebenfalls als nützlich erweisen, auch wenn dieses Protokoll in den

letzten Jahren an Bedeutung verloren hat.

- ✓ **FIRMWARE:** Genau wie Sie es wahrscheinlich von Ihrem PC-System her kennen, können Sie mithilfe dieses Eintrags die Boot-Reihenfolge des Gastsystems ändern. Mithilfe der Schaltflächen NACH OBEN und NACH UNTEN können Sie die Reihenfolge der Geräte entsprechend verschieben ([Abbildung 12.8](#)).

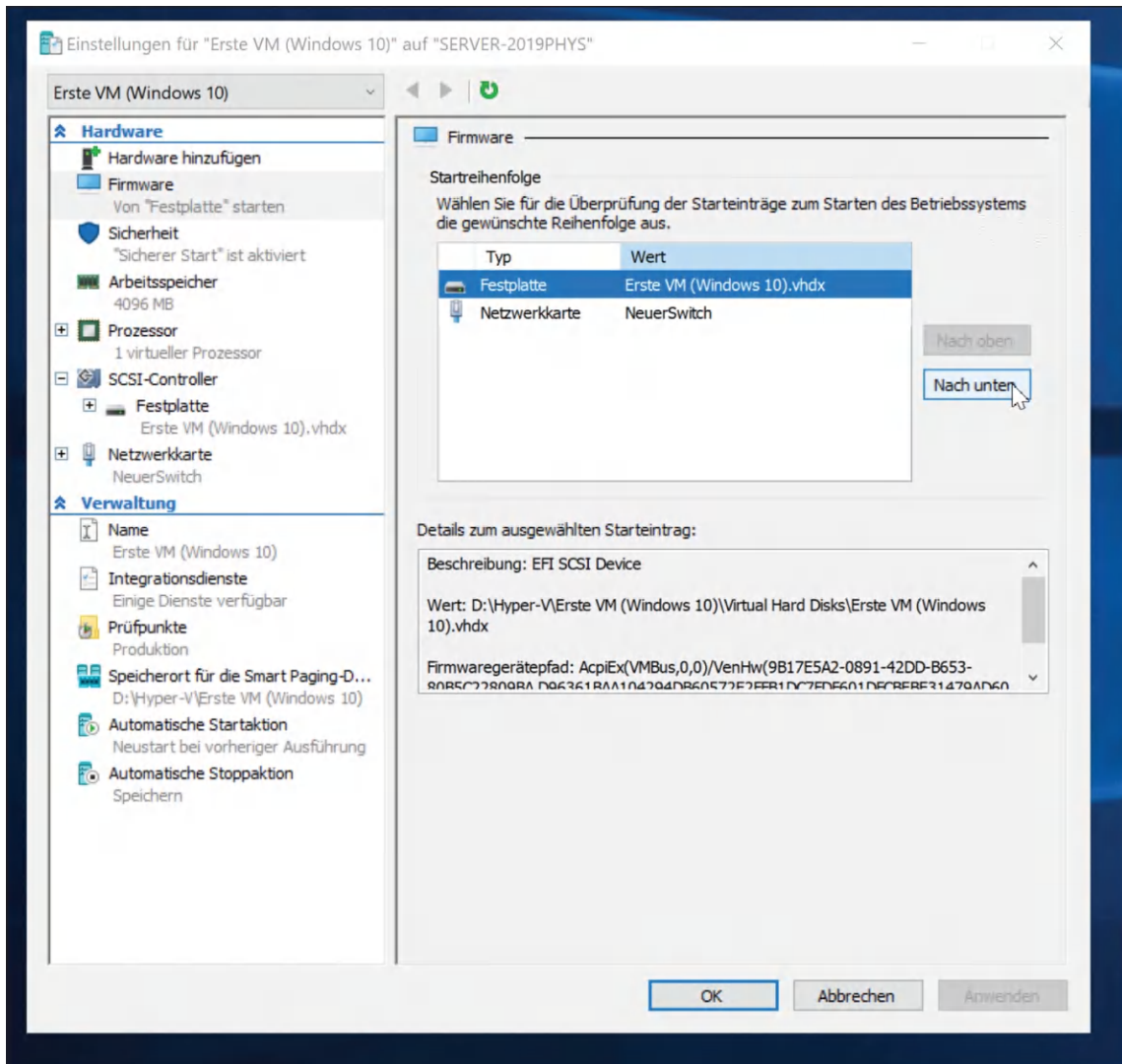


Abbildung 12.8: Im Eintrag »Firmware« können Sie die Startreihenfolge der virtuellen Maschine verändern, indem Sie die Geräte in der Liste verschieben.

- ✓ **SICHERHEIT:** In diesem Bereich geht es um zusätzliche Sicherheitsfeatures, die Sie für Ihre virtuellen Maschinen aktivieren und nutzen können. Sie haben in diesem Abschnitt die Wahl zwischen

drei Möglichkeiten:

- SICHERER START
- VERSCHLÜSSELUNGSUNTERSTÜTZUNG
- SICHERHEITSRICHTLINIE (ABGESCHIRMTE VM)



Mit der 2. Generation von virtuellen Maschinen unterstützt die Virtualisierung mit dem Hyper-V fortgeschrittene Sicherheitsoptionen, die in den VMs der 1. Generation nicht zur Verfügung stehen. Dazu gehören:

- ✓ SICHERER START: Häufig nur unter der englischen Bezeichnung »Secure Boot« bekannt. Eingeführt mit Windows Server 2012 R2 verlangt dieses Feature ein UEFI-System, damit es funktioniert. Dann stellt es sicher, dass sowohl jeder Treiber als auch weitere Software-Komponenten, die während des Boot-Vorgangs geladen werden, digital signiert sind und deren Einsatz damit zulässig ist.
- ✓ VERSCHLÜSSELUNGSUNTERSTÜTZUNG: Unter diesem Menüpunkt können Sie ein Trusted Platform Module (TPM) aktivieren. Das ist ein spezieller Chip, der heute auf den meisten Mainboards vorhanden ist und Hardware-Unterstützung für Verschlüsselungsdienste anbietet. Seit dem Windows Server 2016 ist es durch einen virtuellen TPM-Chip möglich, diese Option auch dann zu aktivieren, wenn der Hostrechner keinen solchen Chip auf dem Mainboard besitzt. TPM kann beispielsweise bei der Verschlüsselung mittels Bitlocker zum Einsatz kommen.
- ✓ SICHERHEITSRICHTLINIE: Die Möglichkeit, »abgeschirmte VMs« unter Hyper-V einzusetzen, steht ebenfalls seit der Version 2016 des Windows-Servers zur Verfügung. Aktivieren Sie diese Option, dann werden automatisch die weiteren Optionen SECURE BOOT, TRUSTED PLATFORM MODULE AKTIVIEREN sowie STATUS- UND VM-MIGRATIONSDATENVERKEHR VERSCHLÜSSELN aktiviert und durchgesetzt. So können Sie beispielsweise Administratoren, die nur den Hostrechner, aber nicht die virtuellen Maschinen verwalten sollen, davon abhalten, auf die Inhalte der VMs zuzugreifen oder deren Einstellungen zu verändern.
- ✓ ARBEITSSPEICHER: Sie konnten zwar bereits beim Anlegen der virtuellen Maschine die Starteinstellung für den Arbeitsspeicher vornehmen, aber an dieser Stelle können Sie diese Einstellungen nun noch genauer festlegen ([Abbildung 12.9](#)).



Einige Anwendungen kommen erfahrungsgemäß nur schlecht oder überhaupt nicht mit dem dynamischen Arbeitsspeicher zurecht. Im Idealfall weiß der Anbieter der entsprechenden Anwendung das und

teilt es Ihnen auch mit. So raten viele Experten davon ab, diese Option zu aktivieren, wenn in der virtuellen Maschine ein Exchange- oder SQL-Server zum Einsatz kommt.

Wenn Sie die Option DYNAMISCHEN ARBEITSSPEICHER AKTIVIEREN nicht auswählen, bekommt die virtuelle Maschine genau die Menge Arbeitsspeicher fest zugewiesen, die Sie anfangs festgelegt haben. Da auch das Host-Betriebssystem und der Hyper-V-Server Arbeitsspeicher im physikalisch vorhandenen Speicher des Hostrechners belegen, sollten Sie sehr gut überlegen, wie viel Speicher Sie Ihren virtuellen Maschinen zuordnen und ob es sinnvoll ist, die Option für die dynamische Speicherzuordnung zu aktivieren.

Haben Sie das Kästchen bei dem Eintrag DYNAMISCHER ARBEITSSPEICHER AKTIVIEREN ausgewählt, können Sie festlegen, welche minimale und welche maximale Größe des Arbeitsspeichers Sie für diese virtuelle Maschine erlauben wollen. Zudem können Sie beim Einsatz der dynamischen Zuweisung von Arbeitsspeicher noch einen Pufferbereich für diesen festlegen. Der ARBEITSSPEICHERPUFFER ist standardmäßig auf 20 Prozent des Arbeitsspeichers festgelegt. Er dient dazu, einer virtuelle Maschine, die dynamisch mehr Arbeitsspeicher anfordert, ihn aber nicht direkt vom Hyper-V bereitgestellt bekommt, sofort einen Speicherbereich zur Überbrückung zu geben. Schließlich können Sie mit einem Schieberegler im unteren Bereich dieses Abschnitts ([Abbildung 12.9](#)) den ARBEITSSPEICHERUMFANG (die »Wichtigkeit«) dieser VM festlegen. Je höher dieser Wert ist (Regler weiter rechts), desto eher bekommt sie im Vergleich zu anderen virtuellen Maschinen mehr Arbeitsspeicher zugewiesen.

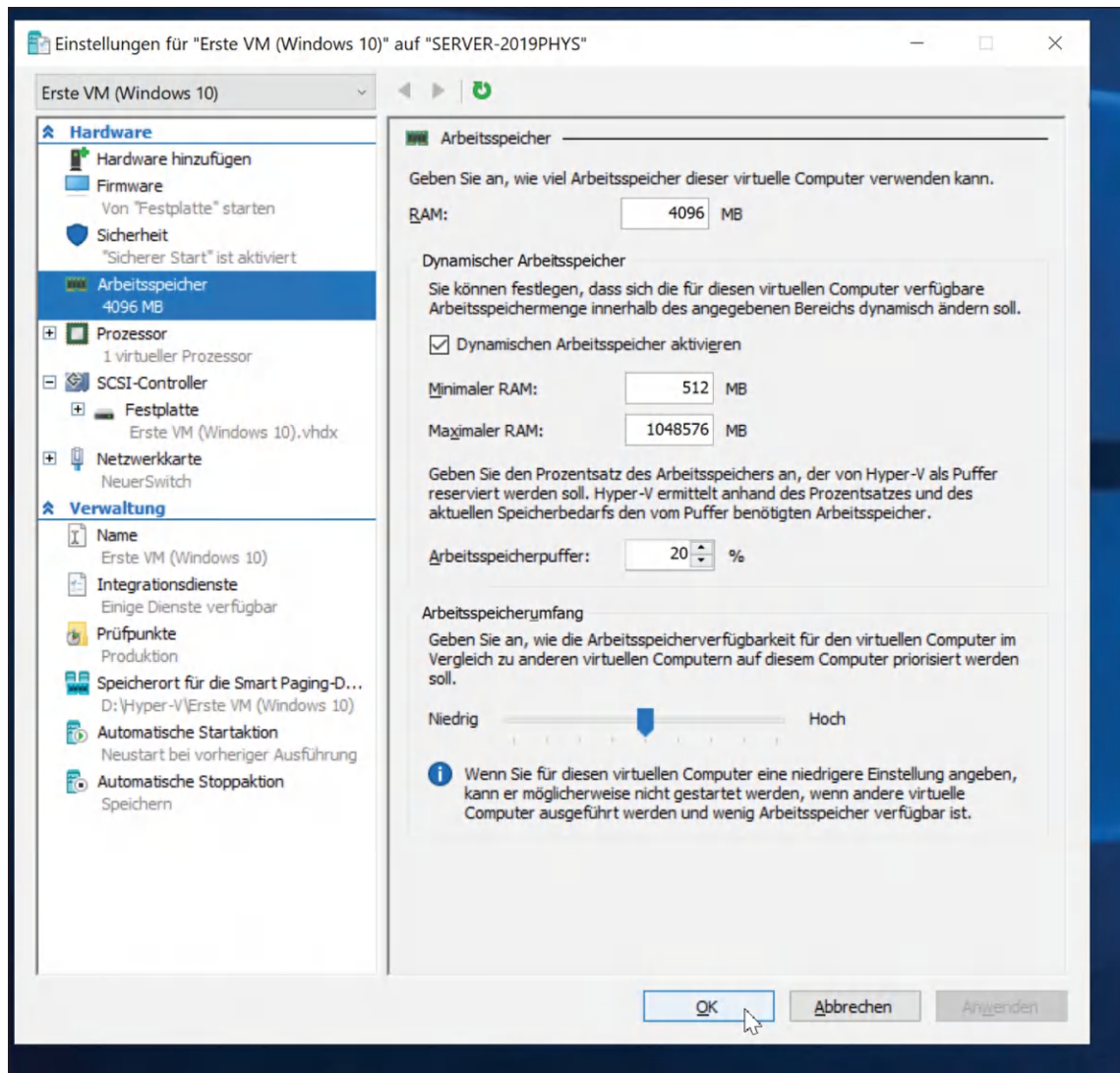


Abbildung 12.9: Die Einstellungen für den Arbeitsspeicher der virtuellen Maschinen können sehr genau vorgenommen werden.

- ✓ **PROZESSOR:** Im Abschnitt Prozessor können Sie die Zahl der virtuellen Prozessoren angeben, die Ihrer virtuellen Maschine zugeordnet werden sollen. Die Anzahl der im Hostrechner vorhandenen Prozessoren dient dabei als Grundlage. Klicken Sie auf das Pluszeichen neben dem Eintrag PROZESSOR in der linken Spalte, so bekommen Sie je ein Untermenü für die Kompatibilität und eine eventuell vorhandene NUMA-Konfiguration angeboten. Wählen Sie im Untermenü KOMPATIBILITÄTSKONFIGURATION das darunter stehende Kästchen aus, so bekommt die virtuelle Maschine nur ein begrenztes Feature-Set der CPU zur Verfügung gestellt, was

die Migration der VM auf eine andere Prozessorversion erleichtern kann.

- ✓ **SCSI-CONTROLLER:** Dieser Abschnitt erlaubt es Ihnen, zusätzliche Festplatten (sowohl virtuelle als auch physikalische), DVD-Laufwerke oder freigegeben Netzwerklaufwerke mit dieser virtuellen Maschine zu verbinden. Ein Klick auf das Pluszeichen neben dem SCSI-Controller zeigt Ihnen die mit ihm verbundenen Geräte. Nach Auswahl eines dieser Geräte bekommen Sie weitere Informationen zu diesem Gerät (in [Abbildung 12.10](#) ist es eine virtuelle Festplatte). Bei virtuellen Festplatten können Sie über BEARBEITEN diesen virtuellen Massenspeicher dann beispielsweise komprimieren oder vergrößern. Unter dem Eintrag SCSI-CONTROLLER finden Sie zudem noch die Möglichkeit, die sogenannte QUALITY OF SERVICE (QoS = Dienstqualität) für eine virtuelle Festplatte festzulegen. Das ist dann wichtig, wenn Sie in dieser virtuellen Maschine Anwendungen betreiben wollen, die eine bestimmte Anzahl von Input-/Output-Operationen pro Sekunde für das richtige Funktionieren benötigen. Sie können dann an dieser Stelle Minimal- und Maximalwerte festlegen.

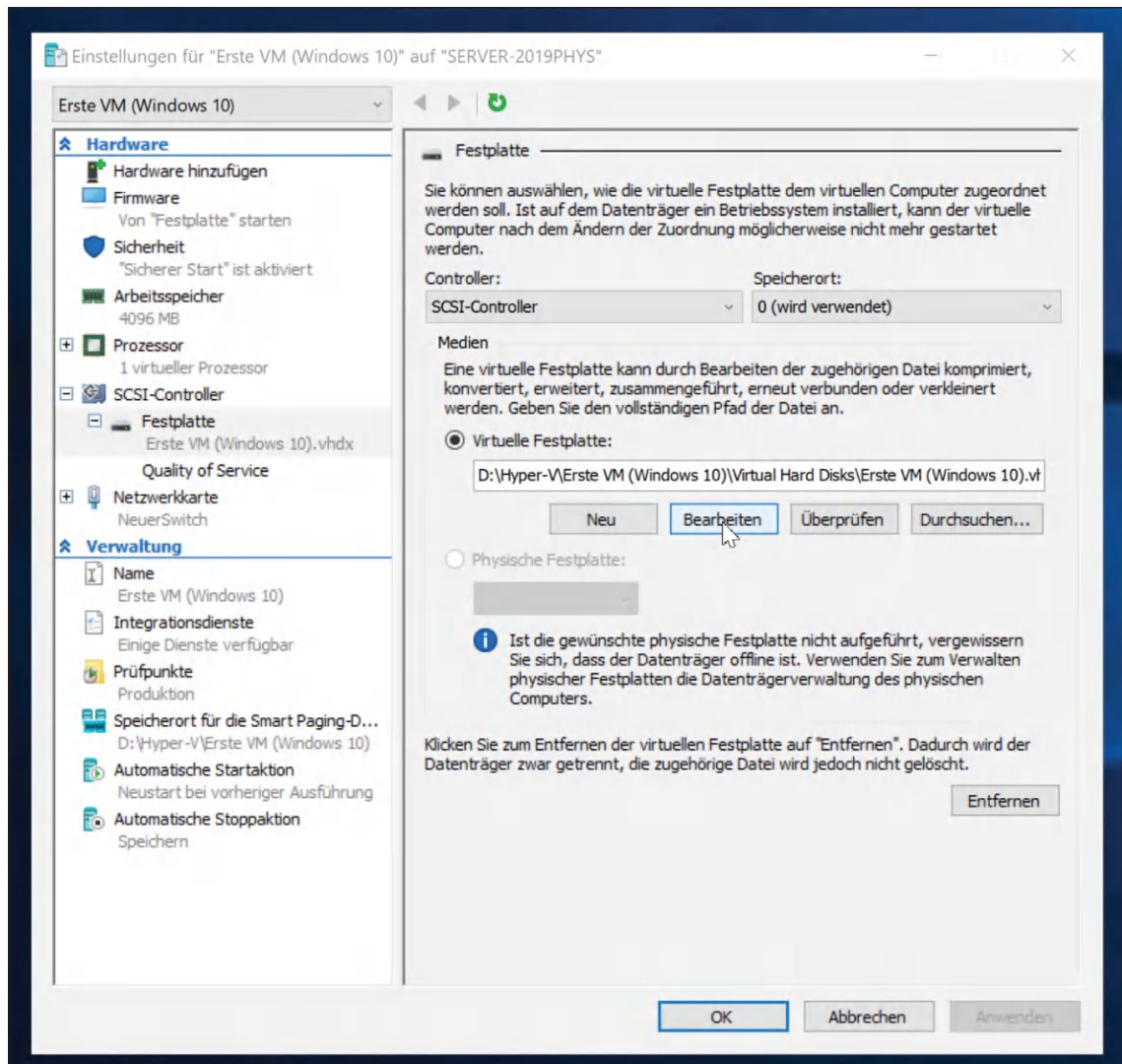


Abbildung 12.10: In den Einstellungen für den SCSI-Controller können Sie weitere Laufwerke mit der virtuellen Maschine verbinden.

- ✓ **NETZWERKKARTE:** Im Abschnitt für die Netzwerkkarte(n) können Sie eine ganze Reihe von Einstellungen vornehmen. So können Sie den virtuellen Switch ändern, mit dem die Netzwerkkarte verbunden ist. Auch die Zuordnung einer ID für den Einsatz in einem VLAN (Virtual Local Area Network) können Sie hier festlegen. Ein solches VLAN ist ein logisches Netzwerk, das auf einem physikalischen Netzwerk aufsetzt und ermöglicht, dass dieses in voneinander isolierte, logische Teilnetze aufgeteilt werden kann.



Im Abschnitt NETZWERKKARTE finden Sie nach einem Klick auf das Pluszeichen die zwei Untermenüs **HARDWAREBESCHLEUNIGUNG** und **ERWEITERTE FEATURES**.

Bei der **HARDWAREBESCHLEUNIGUNG** stehen Ihnen die folgenden Einstellungen zur Verfügung:

- ✓ **WARTESCHLANGE FÜR VIRTUELLE COMPUTER:** Dieses auch als VMQ (Virtual Machine Queue) bezeichnete Feature erhöht den Durchsatz, indem es Netzwerkpakete, die von außerhalb des virtualisierten Netzwerks kommen, direkt an das virtualisierte System liefert. Der Netzwerkkadapter des darunter liegenden physikalischen Hostsystems muss dieses Feature unterstützen, damit es auf dieser Ebene eingesetzt werden kann.
- ✓ **IPSEC-TASKABLADUNG:** Wenn die Option aktiv ist, kann Hyper-V Aufgaben, die in Zusammenhang mit der IPsec-Verschlüsselung stehen, direkt auf den Netzwerkkadapter des Hostrechners »abladen«. Dazu muss aber sowohl diese Netzwerke als das Gastsystem in der VM dieses Feature unterstützen.
- ✓ **E/A-VIRTUALISIERUNG MIT EINZELSTAMM:** Die Single Root I/O Virtualization (SR-IOV) wird seit Windows Server 2012 unterstützt, steht aber nur mit dafür geeigneter Hardware zur Verfügung. Diese Technik ermöglicht es einem PCI-Gerät, als mehrere physische Geräte zu erscheinen, wodurch Ein-/Ausgabe-Durchsätze erhöht werden können. Hyper-V stellt solchen Geräten mithilfe dieser Option dann die dazu benötigten virtuellen Funktionen und Treiber bereit.

Bei den **ERWEITERTEN FEATURES** stehen dann zudem noch die folgenden Auswahlmöglichkeiten bereit:

- ✓ Sie können festlegen, ob die eindeutige MAC-Adresse (Media Access Control), also die physikalische Adresse der

Netzwerkschnittstelle, statisch oder dynamisch vergeben werden soll. Aktivieren Sie das Kästchen neben SPOOFING VON MAC-ADRESSEN AKTIVIEREN, so können Sie diese Hardware-Adresse der Netzwerkkarte verschleiern.

- ✓ DHCP-WÄCHTER: Wenn Sie dieses Sicherheitsfeature aktivieren, werden die Server-Antworten nicht autorisierter virtueller Systeme entfernt, die sich als DHCP-Server ausgeben.
- ✓ ROUTENWÄCHTER: Arbeitet ganz ähnlich wie der DHCP-Wächter, nur dass es sich in diesem Fall um nicht autorisierte virtuelle Computer handelt, die sich als Router ausgeben. Deren Router-Ankündigungen und Umleitungsmeldungen werden nach Aktivierung des Routenwächters ebenfalls entfernt.
- ✓ GESCHÜTZTES NETZWERK: Funktioniert nur, wenn die virtuelle Maschine sich in einem Cluster befindet und hochverfügbar ist. Ist diese Option dann aktiv und die Netzwerkverbindung bricht ab, wird die virtuelle Maschine automatisch auf einen anderen Clusterknoten verschoben.
- ✓ PORTSPIEGELUNG: Dient der Überwachung des Netzwerkverkehrs eines virtuellen Computers. Ist diese Option aktiviert, werden ein- und ausgehende Netzwerkpakte kopiert und an ein anderes virtuelles System geschickt, das dann zur Überwachung dienen kann.
- ✓ NIC-TEAMVORGANG: Beim NIC-Teaming können die in einem Computer verfügbaren physische Netzwerkkarten »zusammengefasst« werden. Diese zusammengefassten NICs werden in virtuellen Netzwerkkarten dargestellt, die dann für Workloads zur Verfügung gestellt werden. Dadurch stehen so innerhalb des Servers größere Netzwerkbandbreite und höhere Resilienz zur Verfügung. Sie können durch Auswahl des Kästchens unter dieser Option zulassen, dass dieser Netzwerkkarten Teil eines Teamvorgangs im Gastbetriebssystem wird.
- ✓ GERÄTEBENENNUNG: Mithilfe der Gerätebenennung den Namen des Hyper-V-Netzwerks in das Gastsystem übertragen.

Eine Option, die zur Identifizierung nützlich ist, wenn die Gastssysteme über mehrere NICs verfügen.

Es folgen noch einige weitere Einstellmöglichkeiten unter der Überschrift VERWALTUNG:

- ✓ NAME: An dieser Stelle können Sie den Namen der virtuellen Maschine ändern oder ergänzen, den Sie beim Anlegen vergeben haben. Zudem haben Sie die Möglichkeit, hier in einem Textfeld noch Informationen zu dieser VM zu hinterlegen.
- ✓ INTEGRATIONSDIENSTE: Durch die Integrationsdienste wird es möglich, dass Sie Dienste des Hostsystems auch in der virtuellen Maschine zur Verfügung haben. Dazu gehört beispielsweise der Datenaustausch zwischen Gast- und Host-Betriebssystem über Copy-and-paste. Das Gastsystem muss selbstverständlich diese Dienste unterstützen können, sodass möglicherweise nicht alle Gastdienste zur Verfügung stehen.
- ✓ PRÜFPUNKTE: Sie sind eine der nützlichsten Einrichtungen für virtuelle Maschinen. Bei anderen Virtualisierungsprodukten und früheren Version des Windows-Servers werden sie auch als Schnappschüsse (Snapshots) bezeichnet. Ein Prüfpunkt zeichnet den aktuellen Zustand einer aktiven virtuellen Maschine auf und erlaubt es Ihnen, diesen Zustand jederzeit wiederherzustellen. Das ist besonders für Testsysteme sehr interessant. Sollte dabei beispielsweise eine Änderung ein Problem verursachen, können Sie den virtuellen Computer auf den Zustand zurücksetzen, in dem er sich bei Erstellen des Prüfpunkts befand. Hyper-V bietet Ihnen hier zwei Ausprägungen der Prüfpunkte ([Abbildung 12.11](#)) an, zwischen denen Sie in diesem Untermenü wählen können:

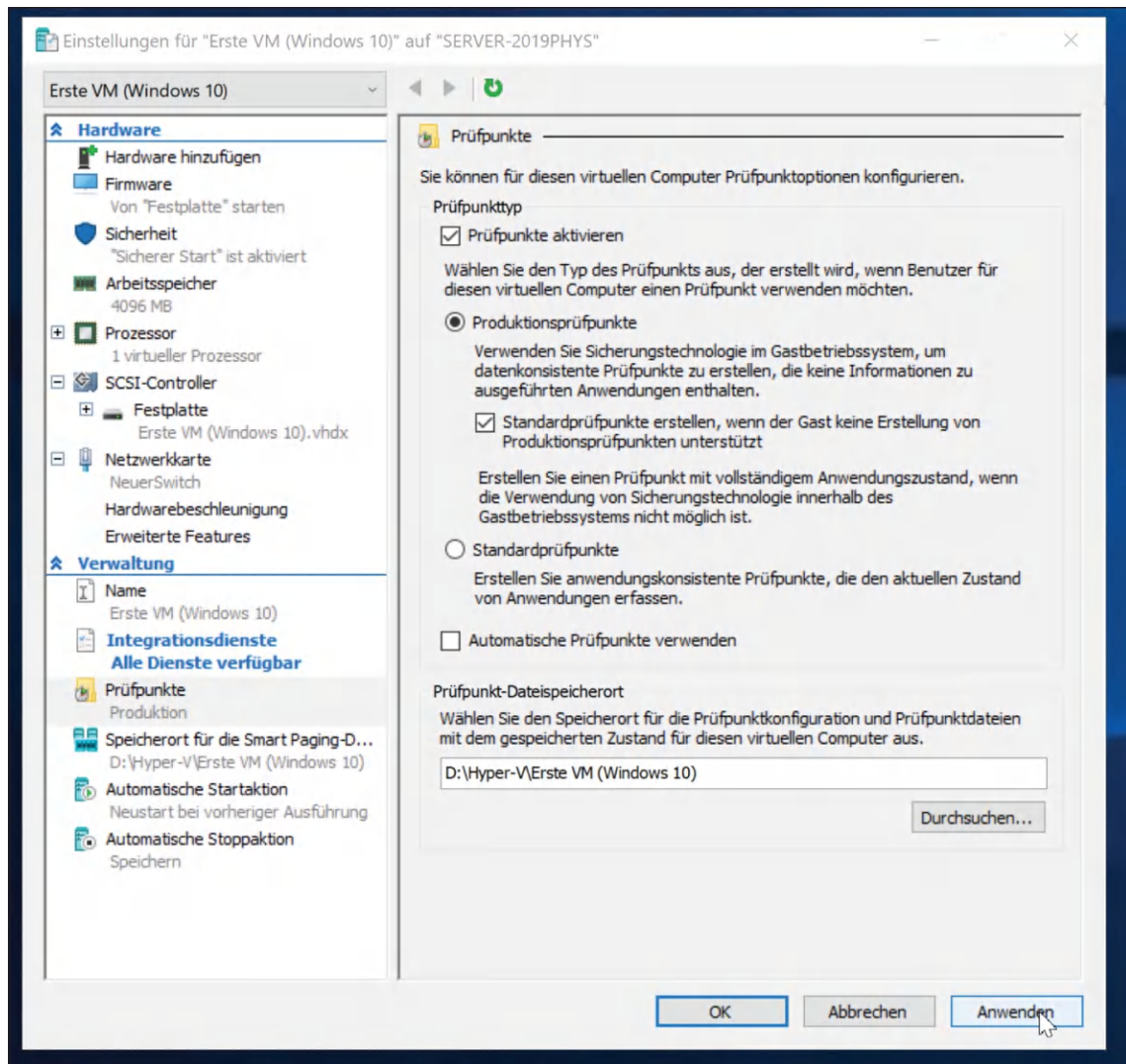


Abbildung 12.11: Prüfpunkte sind ein sehr nützliches Feature, durch das virtuelle Computer auf einen vorherigen Stand zurückgesetzt werden können.

- ✓ **PRODUKTIONSPRÜFPUNKTE:** Dies ist die Default-Voreinstellung. Dabei kommt jeweils die Backup-Technik zum Einsatz, die im Gastsystem zur Verfügung steht. Das ist dann beispielsweise der Dienst für Volumenschattenkopien bei Windows-Gästen oder das Einfrieren des Dateisystems auf einem virtuellen Linux-Computer. Der Zustand des Arbeitsspeichers des Gastsystems wird dabei nicht gesichert. Sie können bei dieser Einstellung zusätzlich aktivieren, dass Hyper-V automatisch einen Standardprüfpunkt erstellt, wenn das Gastsystem keine Produktionsprüfpunkte unterstützt.
- ✓ **STANDARDPRÜFPUNKTE:** Die hierbei erstellte Momentaufnahme

des laufenden virtuellen Computers speichert den Zustand des Arbeitsspeichers zum Zeitpunkt der Erstellung des Prüfpunkts ab. Microsoft warnt explizit, dass eine derartige Momentaufnahme keine vollständige Sicherung ist und somit auch Probleme mit der Datenkonsistenz bei Systemen wie beispielsweise Active Directory verursachen kann, die Daten zwischen verschiedenen Knoten replizieren. Grundsätzlich kann ein Prüfpunkt nie Ersatz für ein Backup sein.

- ✓ **SPEICHERORT FÜR DIE SMART PAGING-DATEI:** Die Smart-Paging-Datei kommt nur dann während des Boot-Vorgangs zum Einsatz, wenn einer virtuellen Maschine zur Startzeit nicht genügend virtueller Hauptspeicher zur Verfügung gestellt werden kann. Mit dieser Einstellung können Sie festlegen, wo diese Datei auf dem Hostrechner abgelegt werden soll.
- ✓ **AUTOMATISCHE STARTAKTION:** Mit dieser Einstellung können Sie festlegen, was die VM tun soll, wenn der Hyper-V-Host startet. Dabei haben Sie die Auswahl zwischen KEINE AKTION, AUTOMATISCH STARTEN, FALLS DIE AUSFÜHRUNG BEI BEENDUNG DES DIENSTS STATTFAND (diese Option ist standardmäßig eingestellt) und VIRTUELLEN COMPUTER IMMER AUTOMATISCH STARTEN. Zudem können Sie in diesem Menü festlegen, ob automatische Starts mit Verzögerung ablaufen sollen. Das ist besonders wichtig, um Ressourcenkonflikte zu vermeiden, wenn mehrere virtuelle Computer automatisch gestartet werden.
- ✓ **AUTOMATISCHE STOPPAKTION:** In diesem Menü können Sie einstellen, was mit den virtuellen Computern passiert, wenn der Hyper-V-Dienst gestoppt wird. Hier stehen zur Auswahl: STATUS DES VIRTUELLEN COMPUTERS SPEICHERN (dies ist die Standardeinstellung), VIRTUELLEN COMPUTER AUSSCHALTEN oder GASTBETRIEBSSYSTEM HERUNTERFAHREN. Ein Herunterfahren des Gastbetriebssystems kann aber nur funktionieren, wenn der Integrationsdienst, der das Herunterfahren in diesem virtuellen Computer steuert, dort auch installiert ist.

Nun haben Sie Ihre erste virtuelle Maschine konfiguriert und können sie

in den nächsten Schritten dann mit einem Betriebssystem Ihrer Wahl ausstatten und betreiben.

Kapitel 13

Windows und Linux als Gastsystem

IN DIESEM KAPITEL

Windows 10 als Gastsystem installieren

Virtuelle Computer mit der PowerShell im Griff

Ein genauerer Blick auf die Prüfpunkte

Ubuntu-Linux als Gastsystem installieren

Die virtuelle Maschine ist eingerichtet und konfiguriert – das bedeutet also, dass der virtuelle Computer bereitsteht und ihm nur noch das Betriebssystem fehlt, damit Sie ihn auch benutzen können. Wir zeigen Ihnen hier zunächst beispielhaft, wie Sie ein Windows-10-Betriebssystem auf einem virtuellen Computer installieren können. Dazu benötigen Sie eine ISO-Datei mit dem Betriebssystem, die Sie auf den Hostrechner kopieren oder auf einem Netzwerklaufwerk bereitstellen.



Da wir hier ein Windows 10 Professional als Gastsystem installieren wollen, wählen wir eine virtuelle Maschine der 2. Generation. Installieren Sie ein älteres Betriebssystem oder wollen Sie aus anderen Gründen lieber eine VM der 1. Generation einsetzen, so werden Sie einige kleine Unterschiede in den Konfigurationsmenüs der virtuellen Maschine finden.

1. Starten Sie den HYPER-V-MANAGER.
2. Wählen Sie zunächst einfach unter Aktionen den Eintrag VERBINDEN aus. Sie finden diesen Eintrag aber auch in dem

Kontextmenü, das sich mit einem Rechtsklick auf dem Namen ihres virtuellen Computers öffnet ([Abbildung 13.1](#)).

3. Es öffnet sich ein Fenster für den virtuellen Computer. Wenn Sie an der oberen Leiste dieses Fensters den Eintrag MEDIEN auswählen, sehen Sie, ob Ihre VM bereits mit einem virtuellen DVD-Laufwerk ausgestattet es. Ist das nicht der Fall, können Sie dieses Laufwerk über die Einstellungen der virtuellen Maschine noch hinzufügen. Wählen Sie dazu den SCSI-CONTROLLER aus und fügen Sie über das Menü ein DVD-Laufwerk hinzu ([Abbildung 13.2](#)).

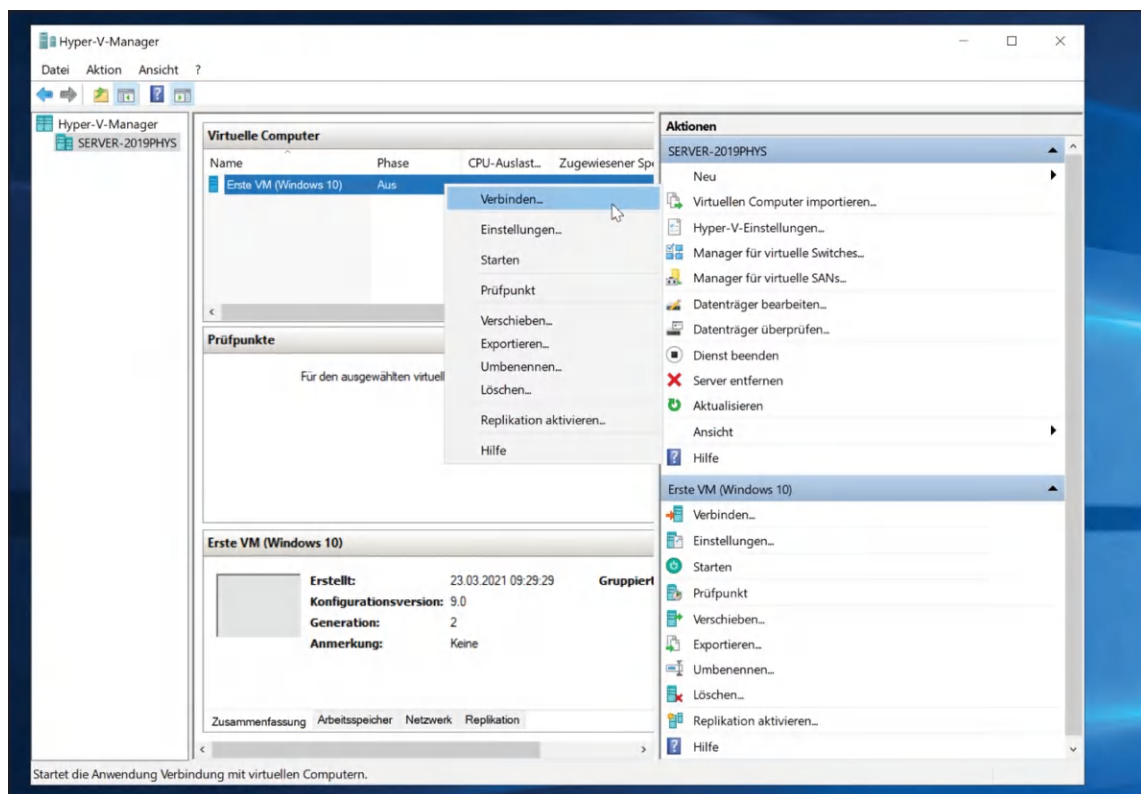


Abbildung 13.1: Um die Installation des Betriebssystems in der VM zu starten, müssen Sie zunächst eine Verbindung zu dieser aufbauen.

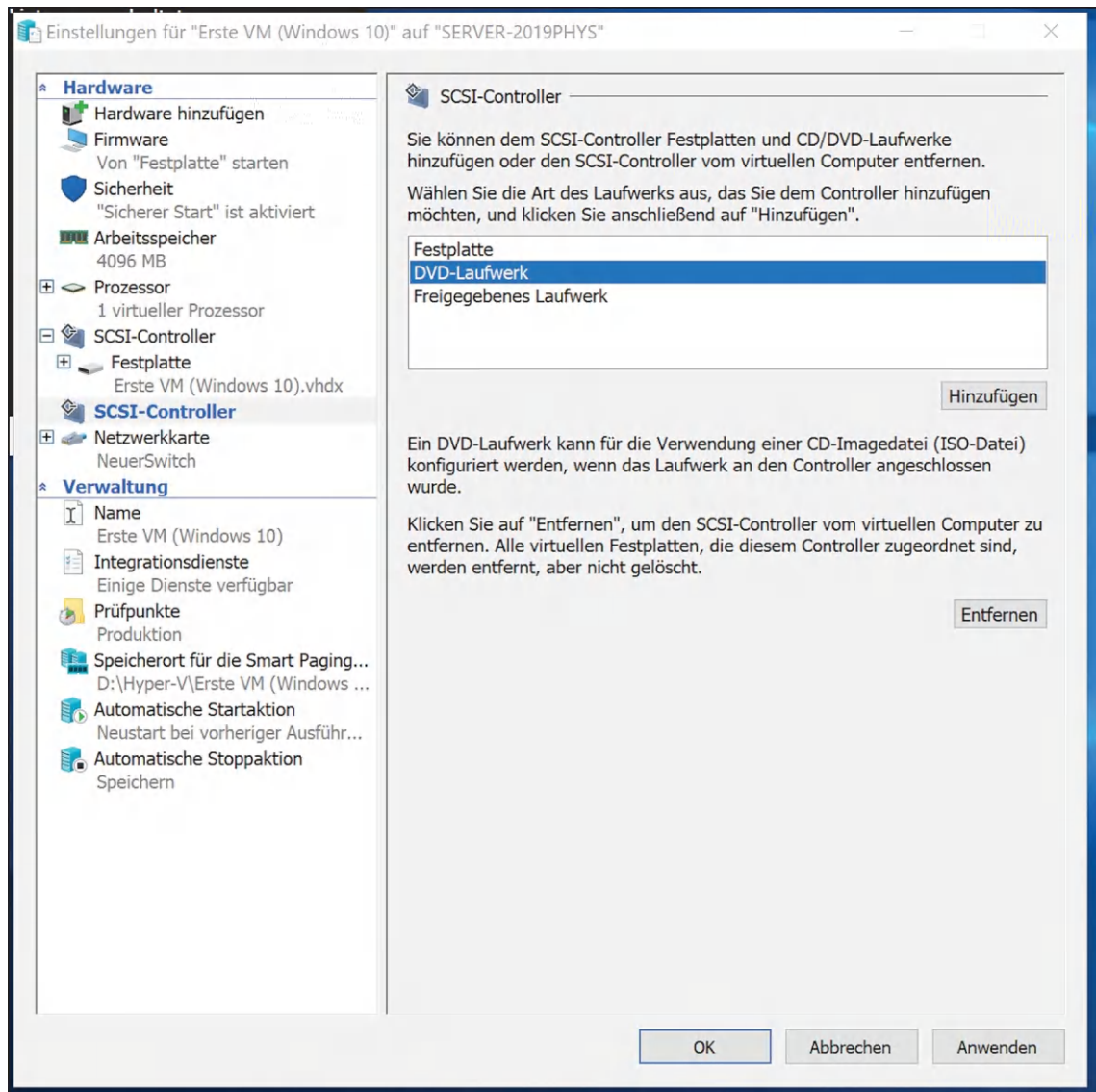


Abbildung 13.2: Ohne virtuelles DVD-Laufwerk geht es nicht. Nur so kann das Gastsystem von der ISO-Datei aus installiert werden.

4. Wählen Sie das derart installierte DVD-Laufwerk vom Eintrag MEDIEN in der Menüleiste aus. Klicken Sie dann im Menü dieses Laufwerks auf den Eintrag DATENTRÄGER. Legen Sie die virtuelle DVD in das Laufwerk ein, indem Sie die gewünschte ISO-Datei auswählen.
5. Wenn Sie nun den virtuellen Computer über die Schaltfläche STARTEN in der Mitte des VM-Fensters starten, beginnt ein Boot-Vorgang, wie Sie ihn sicher schon von der Installation eines Windows-Systems auf einem physikalischen Computersystem her

kennen. Sie werden dann vom Windows-System (in diesem Beispiel handelt es sich um Windows 10 in der Pro-Version) wie gewohnt durch die Installation geleitet ([Abbildung 13.3](#)).

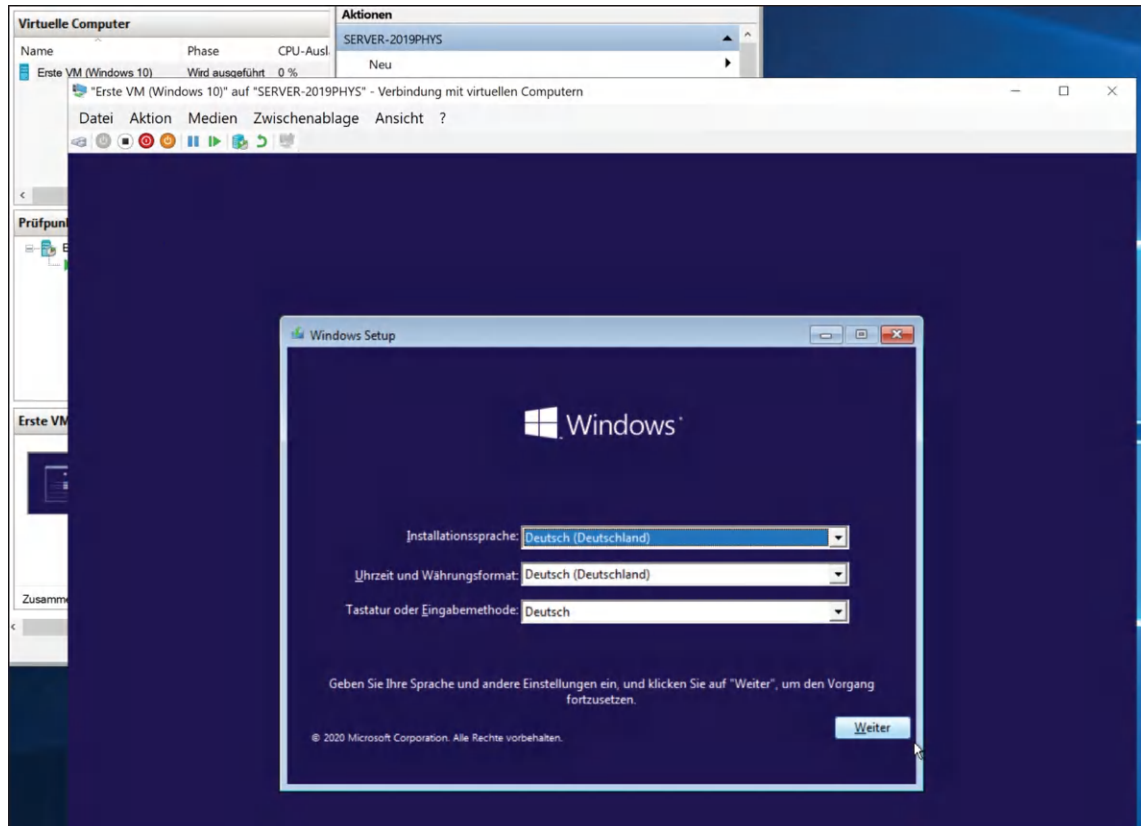


Abbildung 13.3: Kein Unterschied zu einer »normalen« Installation, sobald der virtuelle Computer von der ISO-Datei aus gestartet ist.

6. Haben Sie alle Fragen bei der Installation beantwortet, startet das Windows-Gastsystem noch einmal neu, und Sie werden vom bekannten Sperrbildschirm des Windows-10-Systems begrüßt ([Abbildung 13.4](#)). Haben Sie dabei wie wir eine VM der 2. Generation mit entsprechend modernem Betriebssystem wie Windows 10 verwendet, so wird Ihnen Hyper-V wahrscheinlich nun ein Fenster für eine sogenannte ERWEITERTE SITZUNG präsentieren, wie Sie es in der [Abbildung 13.4](#) sehen können. Damit Sie eine solche erweiterte Sitzung einsetzen können, müssen allerdings einige weitere Bedingungen erfüllt sein. Dazu kommen wir gleich.



Abbildung 13.4: Der virtuelle Computer ist aktiv und bietet bei der Anmeldung mit dem erweiterten Sitzungsmodus zusätzliche Möglichkeiten.

Sie werden sehen, dass dieser Modus sehr nützlich ist, erlaubt er doch unter anderem, dass das Fenster mit dem Gastsystem auf die vollständige Größe des Bildschirms skaliert wird, ohne dass Sie dazu zunächst explizit die Bildschirmauflösung im Gastsystem ändern müssen. Weiterhin können Sie dann wie bei einer Remotedesktop-Verbindung in einer Sitzung lokale Geräte und Features verwenden. Dazu gehören Audio, die Anzeige mit Steuerung der Auflösung, die Windows-Zwischenablage, USB- und andere »Plug-and-play«-Geräte sowie Smartcards und Drucker.



Seit der Version 2012 R2 bietet der Hyper-V den erweiterten Sitzungsmodus (Enhanced Session Mode) für die Verbindungen zu den virtuellen Computern an. Damit können Sie nun auch eine »richtige« Remotedesktop-Verbindung zu den virtuellen Maschinen verwenden. Das wird dadurch ermöglicht, dass diese Verbindungen auch den VIRTUAL MACHINE BUS nutzen können, über den die Kommunikation zwischen einer VM und dem Host-Betriebssystem

abgewickelt wird. Dadurch kann dann eine Sitzung über die Konsole des Hyper-V-Managers ähnliche Einstellungen und Möglichkeiten wie eine Sitzung mit der Remotedesktop-Verbindung bieten.

Damit Sie diesen Modus nutzen können, müssen zunächst einige Bedingungen erfüllt sein. So ist es notwendig, dass Sie im Hyper-V-Manager im Bereich Hyper-V-Einstellungen bei der RICHTLINIE FÜR DEN ERWEITERTEN SITZUNGSMODUS das Feature ERWEITERTEN SITZUNGSMODUS ZULASSEN ausgewählt haben. Diese Einstellung gilt dann für alle virtuellen Maschinen, die Sie auf diesem Host betreiben. Auch die virtuellen Maschinen müssen bestimmte Voraussetzungen erfüllen, damit Sie den erweiterten Sitzungsmodus nutzen können:

- ✓ So müssen Sie ein Gastbetriebssystem verwenden, das die Nutzung der REMOTE DESKTOP SERVICES (RDS) unterstützt. Das können beispielsweise Windows Server 2012 R2 sowie die Pro- und Enterprise-Editionen von Windows 8.1 und Windows 10 sein.
 - ✓ Zudem ist es notwendig, dass zunächst der vollständige Setup-Prozess für das Gastsystem durchlaufen wurde, bevor eine derartige Verbindung genutzt werden kann.
 - ✓ Weiterhin muss der bereits erwähnte RDS-Dienst auf dem Gastsystem gestartet sein. Dabei ist nicht notwendig, dass Sie dazu auch den Remote-Zugriff auf das Gastsystem erlauben.
 - ✓ Der angemeldete Nutzer auf dem Gastsystem muss lokale Administratorrechte besitzen oder als Remotedesktop-Anwender auf dem Gastsystem eingetragen sein.
7. Danach können Sie sich anmelden und im Konsolenfenster wie gewohnt auf dem Gastsystem arbeiten. Haben Sie es mit einem externen virtuellen Switch verbunden, der mit der physikalischen Netzwerkkarte in Ihrem Hostsystem verbunden ist, so finden Sie das Gastsystem dann auch direkt in dem Netzwerk wieder, in dem sich auch Ihr Hostsystem befindet.

8. Wechseln Sie nun einmal im Gastsystem in die WINDOWS-EINSTELLUNG und dort in den Bereich NETZWERK UND INTERNET, dann können Sie ([Abbildung 13.5](#)) sehen, dass sich die Einstellungen der virtuellen Netzwerkkarte (bis auf den Hinweis MICROSOFT HYPER-V NETWORK ADAPTER) nicht von denen eines physikalischen Systems unterscheiden. Wir haben für dieses Bild absichtlich einen Ausschnitt aus der Vollbildmodus-Darstellung gewählt, in der Sie eine Leiste des Konsolenfensters am oberen Bildrand finden, über die Sie diese Darstellung auch wieder verlassen können.
9. Auf der oberen Fensterleiste des Konsolenfensters finden Sie noch einige weitere Konfigurations- und Einstellmöglichkeiten für die in diesem Fenster aktive virtuelle Maschine ([Abbildung 13.6](#)). Wählen Sie dort den Eintrag DATEI aus, so können Sie direkt in die Einstellungen der virtuellen Maschine wechseln oder über BEENDEN das Konsolenfenster komplett schließen. Hyper-V fährt dann das Gastsystem auch automatisch herunter, wenn die Integrationsdienste dafür installiert und aktiviert sind.
10. Unter AKTION finden Sie Einträge, durch die Sie den virtuellen Computer AUSSCHALTEN (hierbei bleibt das Konsolenfenster geöffnet), HERUNTERFAHREN und SPEICHERN (der Status der VM wird gespeichert) können. Weiterhin können Sie die VM in diesem Menü ANHALTEN, NEU STARTEN oder einen PRÜFPUNKT setzen. Über MEDIEN bekommen Sie direkten Zugriff auf virtuelle DVD- oder auch Diskettenlaufwerke, wenn diese in der virtuellen Maschine konfiguriert wurden. Schließlich können Sie unter ANSICHT zwischen ERWEITERTE SITZUNG oder einem normalen Konsolenfenster wechseln. Beachten Sie bitte, dass ein solcher Wechsel jedes Mal eine neue Anmeldung am Gastsystem erfordert. Auch die Symbolleiste, die Sie unter diesen Menüeinträgen finden ([Abbildung 13.6](#)), können Sie über ANSICHT aus- und einschalten. Sie stellt Ihnen Icons für die Operationen zum An- und Abschalten sowie zum Neustart und Anhalten der virtuellen Maschine bereit. Der Wechsel in den VOLLBILDMODUS ist ebenfalls über dieses Menü möglich.

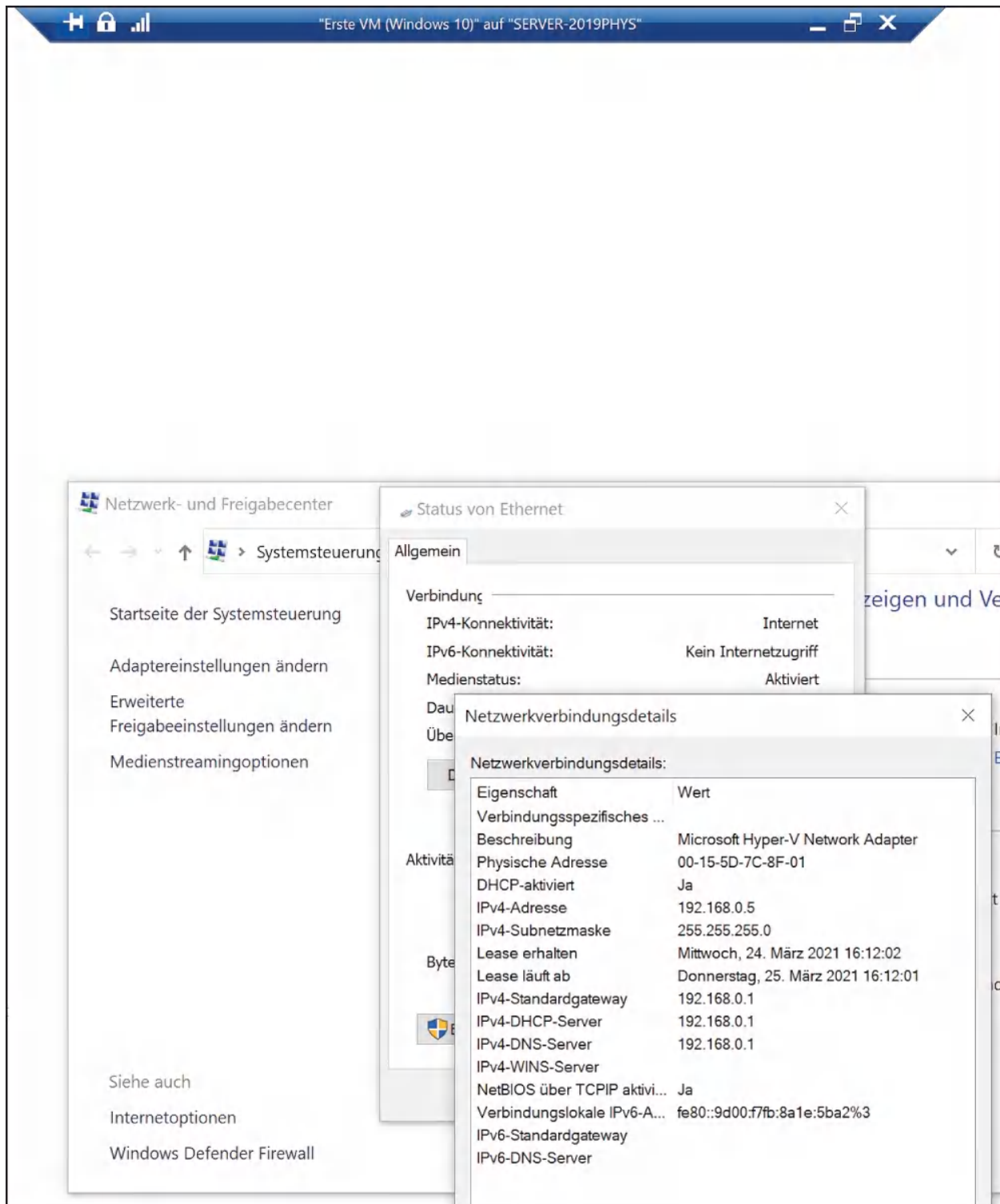


Abbildung 13.5: Der Netzwerkadapter im Gastsystem: ein Ausschnitt aus dem Vollbildmodus der VM, kenntlich an der Konsolenleiste am oberen Bildrand

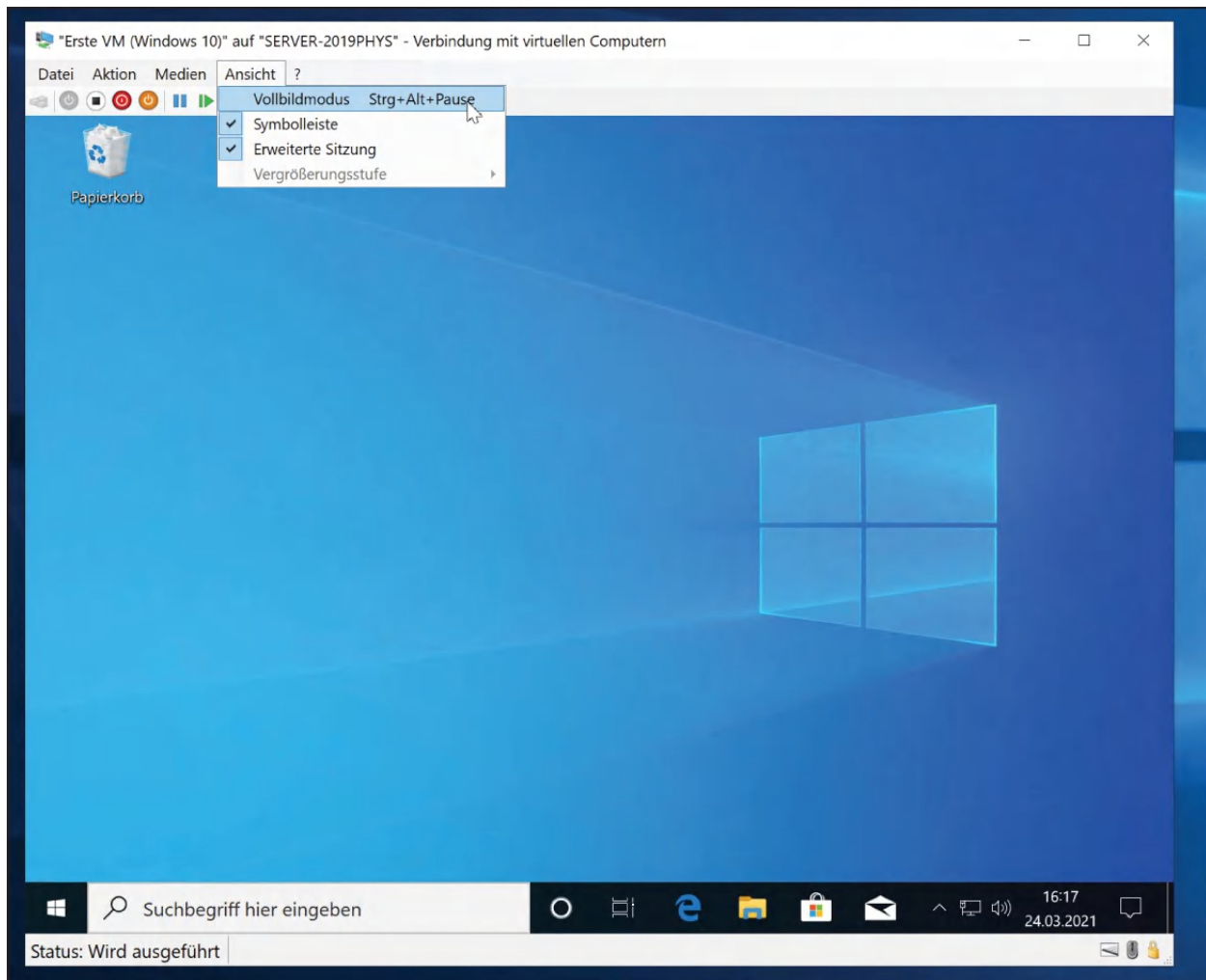


Abbildung 13.6: Das Menü an der oberen Leiste der Konsole bietet einige Einstell- und Konfigurationsmöglichkeiten rund um das Gastsystem.

Virtnelle Computer mit der PowerShell im Griff

Wie Sie es ja in der Zwischenzeit von Windows Server 2019 schon kennen, können Sie natürlich auch alle Aufgaben rund um die Virtualisierung mit dem Hyper-V mithilfe der PowerShell durchführen. Wenn Sie bei der Installation der Hyper-Rolle SERVER-MANAGER auch FEATURES HINZUFÜGEN ausgewählt haben, hat das System auch die PowerShell-Cmdlets zur Verwaltung von Hyper-V installiert. Haben Sie das noch nicht getan, können Sie es aber jederzeit nachholen (und im

Zweifelsfall noch einmal in [Kapitel 11](#) nachschlagen). Wollen Sie zunächst einmal sehen, welche Cmdlets Ihnen das PowerShell-Modul für Hyper-V zur Verfügung stellt, so können Sie dazu den folgenden Aufruf nutzen:

```
Get-Command -Module hyper-v | Out-GridView
```

Es ist sinnvoll, den Befehl mittels einer Pipe an das Cmdlet out-GridView weiterzuleiten, da das Modul Ihnen doch sehr viele spezifische Cmdlets für diese Aufgaben bereitstellt. Deshalb sehen Sie in der [Abbildung 13.7](#) auch nur einen kleinen Ausschnitt aus der langen Liste dieser Befehle.

Zu den ersten Kommandos, die Sie dann einmal ausprobieren sollten, gehört sicher

```
Get-VM
```

wodurch Ihnen alle virtuellen Maschinen auf diesem Hyper-V-Server aufgelistet werden. Sie sehen dann zwar bereits, welche VMs aktiv sind. Sie können die Ausgabe aber noch so modifizieren, dass Ihnen nur die gerade aktiven oder nur die inaktiven VMs aufgelistet werden:

```
Get-VM | where {$_.State -eq 'Running'}  
Get-VM | where {$_.State -eq 'Off'}
```

In der [Abbildung 13.8](#) sehen Sie diese Aufrufe und die entsprechende Ausgabe auf unserem Windows-Server.

Weitere nützliche Cmdlets für die Arbeit mit dem Hyper-V und den virtuellen Maschinen sind unter anderem

```
Start-VM -Name <Name der virtuellen Maschine>
```

um eine virtuelle Maschine zu starten, oder

```
Get-VM | where {$_.State -eq 'Off'} | Start-VM
```

um alle bis zu diesem Zeitpunkt ausgeschalteten virtuellen Computer zu starten.

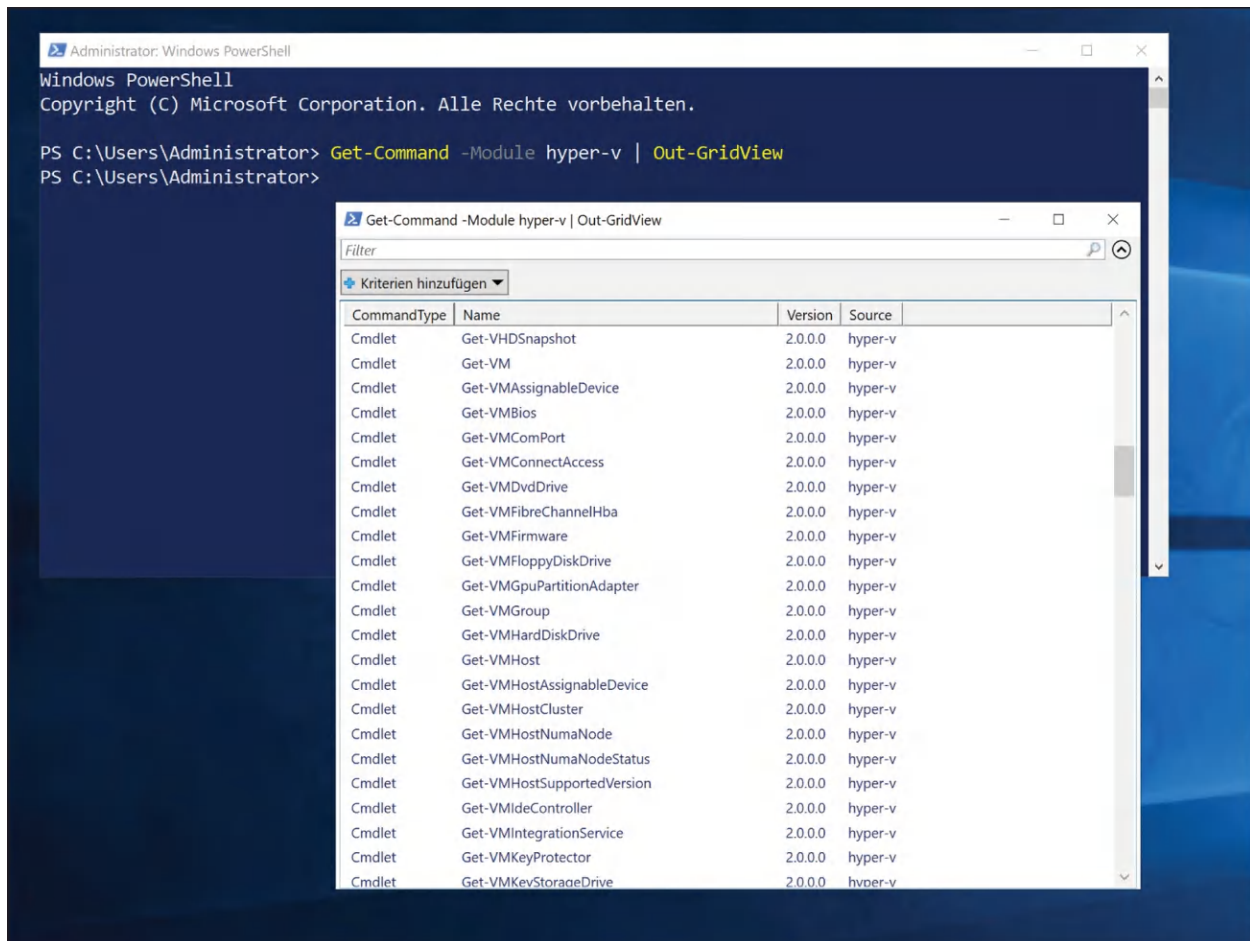
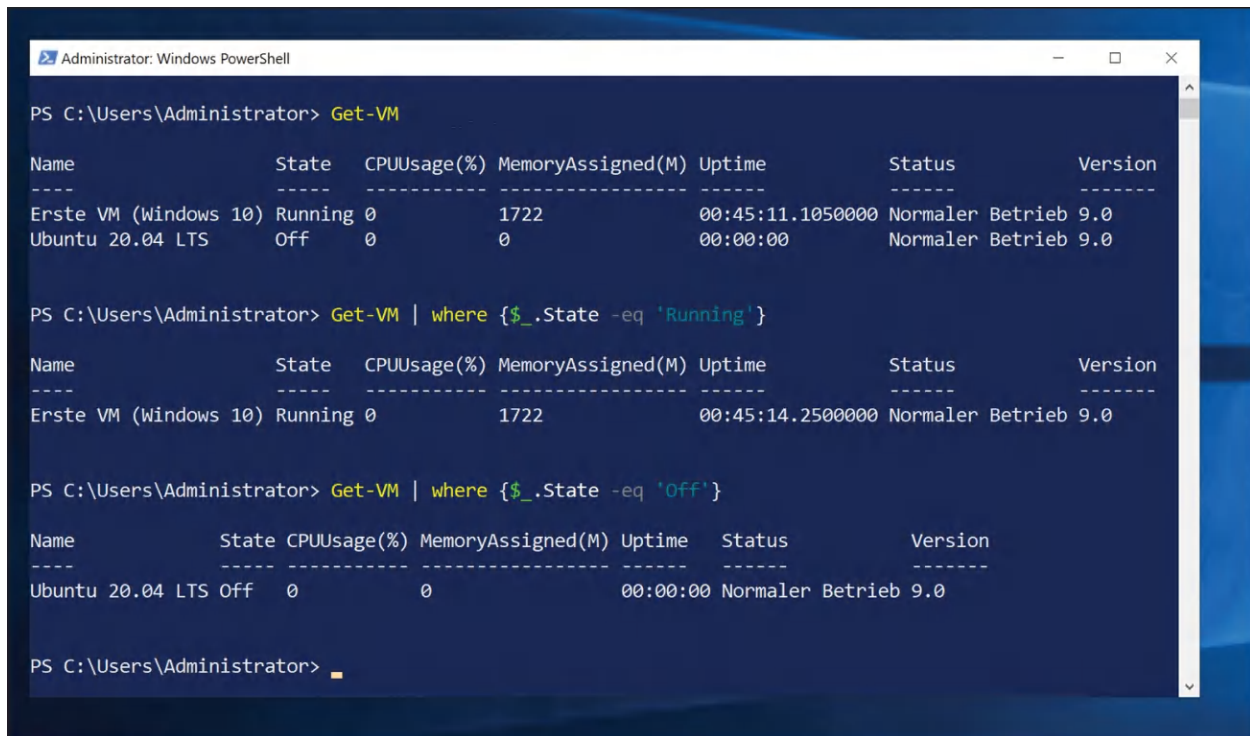


Abbildung 13.7: Das PowerShell-Modul für Hyper-V stellt eine große Auswahl an Cmdlets zur Arbeit mit Hyper-V und den virtuellen Maschinen bereit.

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window shows the output of the 'Get-VM' command, which lists two virtual machines: 'Erste VM (Windows 10)' and 'Ubuntu 20.04 LTS'. The first VM is in a 'Running' state, while the second is 'Off'. The output is formatted as a table with columns for Name, State, CPUUsage(%), MemoryAssigned(M), Uptime, Status, and Version. Subsequent commands filter the results for 'Running' and 'Off' states.

```
PS C:\Users\Administrator> Get-VM

Name                           State      CPUUsage(%) MemoryAssigned(M) Uptime                Status              Version
----                           -
Erste VM (Windows 10)          Running    0             1722              00:45:11.1050000     Normaler Betrieb    9.0
Ubuntu 20.04 LTS              Off        0             0                00:00:00             Normaler Betrieb    9.0

PS C:\Users\Administrator> Get-VM | where {$_.State -eq 'Running'}

Name                           State      CPUUsage(%) MemoryAssigned(M) Uptime                Status              Version
----                           -
Erste VM (Windows 10)          Running    0             1722              00:45:14.2500000     Normaler Betrieb    9.0

PS C:\Users\Administrator> Get-VM | where {$_.State -eq 'Off'}

Name                           State      CPUUsage(%) MemoryAssigned(M) Uptime                Status              Version
----                           -
Ubuntu 20.04 LTS              Off        0             0                00:00:00             Normaler Betrieb    9.0

PS C:\Users\Administrator>
```

Abbildung 13.8: Informationen zu den aktiven und nicht aktiven virtuellen Maschinen können Sie auch mithilfe der PowerShell anzeigen lassen.

Dabei wird die Liste der VMs, bei denen der Status `off` gefunden wird, direkt an das Cmdlet `Start-VM` übergeben. Unser Tipp: Arbeiten Sie zunächst mit dem Hyper-V-Manager, um sich mit der Virtualisierung und den virtuellen Maschinen vertraut zu machen, und nutzen Sie dann nach und nach die entsprechenden Cmdlets, die Ihnen durch das Hyper-V-Modul in der PowerShell zur Verfügung stehen. Auch hier ist der Einsatz der PowerShell besonders dann nützlich, wenn Sie Aufgaben rund um die virtuellen Computer automatisieren wollen. Unter der URL <https://docs.microsoft.com/de-de/powershell/module/hyper-v> stellt Microsoft eine umfassende Referenz dazu bereit.

Ein genauerer Blick auf die Prüfpunkte

Die Prüfpunkte, die Microsoft bis hin zu Windows Server 2012 wie andere Anbieter von Virtualisierungsprodukten als Snapshots bezeichnete, sind eine der nützlichsten Funktionen, die Ihnen mit dem Hyper-V zur

Verfügung stehen. Sie bieten Ihnen beispielsweise in Test-Szenarien eine schnelle Möglichkeit zum Zurücksetzen eines virtuellen Computers in den vorherigen Zustand. Es kann zum Beispiel sinnvoll sein, einen Prüfpunkt anzulegen, bevor Sie das Windows-Betriebssystem in der virtuellen Maschine aktualisieren oder dort neue Software installieren. Im Idealfall sind Sie auf diese Weise dazu in der Lage, den virtuellen Server bei Problemen in wenigen Sekunden auf den ursprünglichen Zustand zurückzusetzen.



Prüfpunkte können und sollen keine Sicherungskopie oder gar ein Backup ersetzen. Während bei einem Backup die Daten mindestens doppelt abgespeichert werden, sodass sie bei Beschädigung oder Verlust wiederhergestellt werden können, erzeugen die Prüfpunkte zum Zeitpunkt ihrer Erstellung nur eine Momentaufnahme des Betriebssystems. Die Daten, die diese Unterschiede abspeichern, können allerdings leicht verloren gehen oder beschädigt werden.

Prüfpunkte von virtuellen Maschinen können Sie sowohl bei eingeschalteter (online) als auch bei ausgeschalteter VM (offline) erstellen. Dabei können Sie mithilfe der sogenannten **STANDARDPRÜFPUNKTE** unter Hyper-V eine Momentaufnahme einer eingeschalteten virtuellen Maschine samt Arbeitsspeicher erstellen.

Wenn Sie einen Prüfpunkt anwenden, führt Hyper-V immer einen Kaltstart des virtuellen Computers aus dem ausgeschalteten Zustand heraus aus. Dadurch wird es auch möglich, dass die Produktionsprüfpunkte Ihnen einen konsistenten Zustand des virtuellen Computers mitsamt Dateisystem und Anwendung bieten können.



STANDARDPRÜFPUNKTE können bei verteilten Anwendungen wie Active Directory, dem SQL- oder Exchange-Server zu Problemen führen, wenn zu diesem Punkt »zurückgerollt« werden soll: Da diese VM und eine darin laufende Anwendung, die zum entsprechenden Zeitpunkt im Arbeitsspeicher Daten gehalten hat, nichts von diesem Rücksprung »wissen« können, erwarten sie die

gleichen Bedingungen wie in der Vergangenheit. Dadurch kommt es dann leicht zu Fehlern und Inkonsistenzen.

Der Technik der PRODUKTIONSPRÜFPUNKTE geht einen Schritt weiter. Sie arbeitet mithilfe des Integrationsdiensts mit dem Volume Shadow Copy Service (VSS) im Gast-Betriebssystem zusammen. Dadurch wird es möglich, dass virtuelle Maschinen den konsistenten Zustand zum Zeitpunkt ihrer Erstellung erhalten. Sie halten auf diese Weise nur den Status der virtuellen Festplatte und die Konfiguration der virtuellen Maschine und nicht den Inhalt des Arbeitsspeichers fest.

Erstellen eines Prüfpunkts

Grundsätzlich ist es möglich, einen Prüfpunkt für eine virtuelle Maschine entweder direkt aus dem Hyper-V-Manager heraus oder aber mithilfe der PowerShell zu erstellen und zu konfigurieren.

1. Starten Sie den HYPER-V-MANAGER.
2. Wählen Sie den gewünschten virtuellen Computer. Klicken Sie dann mit der rechten Maustaste auf den Namen des virtuellen Computers. Im Kontextmenü wählen Sie den Eintrag PRÜFPUNKT aus ([Abbildung 13.9](#)).

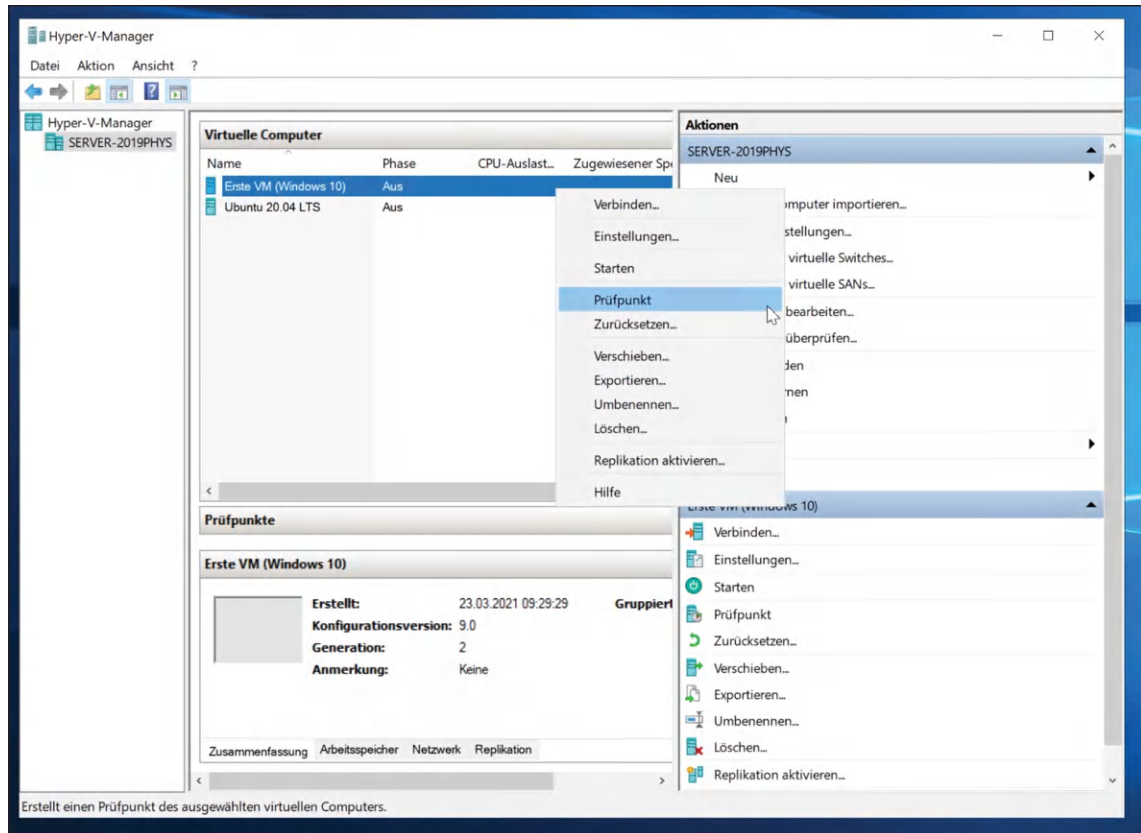


Abbildung 13.9: Prüfpunkte können im Hyper-V-Manager direkt aus dem Kontextmenü des jeweiligen virtuellen Computers heraus erstellt werden.

3. Hat Hyper-V die Erstellung des Prüfpunkts abgeschlossen, wird dieser in der Konsole des Hyper-V-Managers unter PRÜFPUNKTE angezeigt.
4. Ist der virtuelle Computer zu diesem Zeitpunkt bereits aktiv, können Sie einen Prüfpunkt auch über die Auswahl von AKTION auf der oberen Leiste des Bildschirmfensters der VM starten, indem Sie dort im Menü den Eintrag PRÜFPUNKT... auswählen.
5. Sie bekommen den Dialog PRÜFPUNKTNAME angezeigt, der es Ihnen ermöglicht, den Prüfpunkt mit einer eigenen Bezeichnung zu versehen ([Abbildung 13.10](#)).

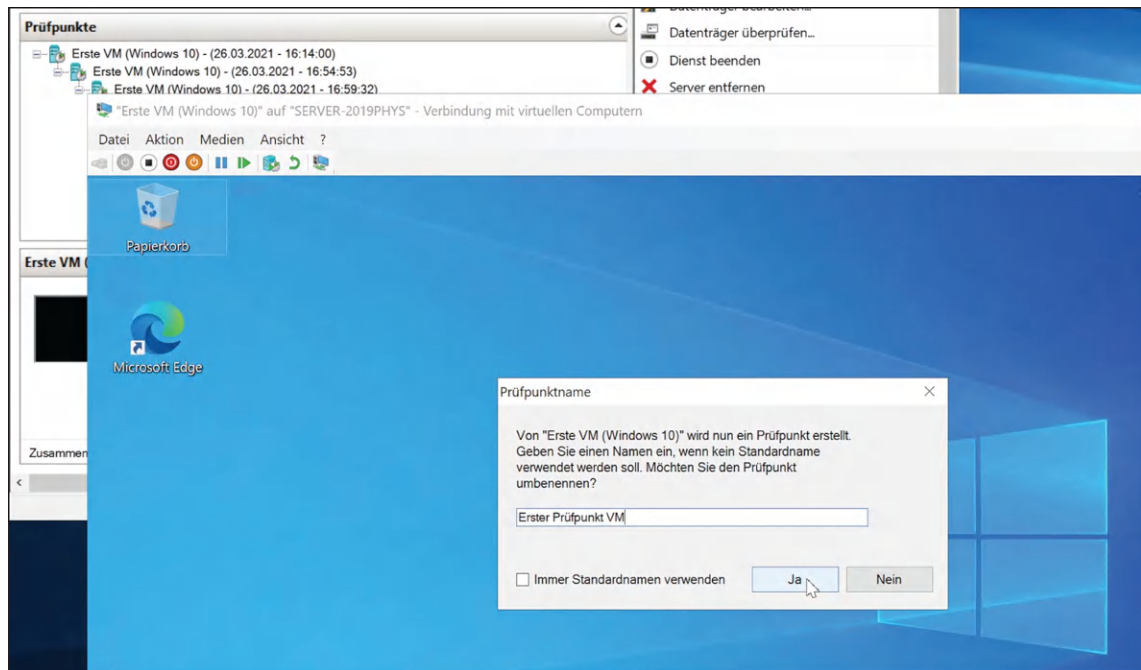


Abbildung 13.10: Der neue Prüfpunkt wurde in einer aktiven virtuellen Maschine erstellt und mit einem neuen Namen versehen.

6. Danach informiert Sie ein weiteres Fenster darüber, dass nun ein Produktionsprüfpunkt erstellt wurde. Zudem werden Sie darauf hingewiesen, dass Sie die Prüfpunktoptionen in den Einstellungen für den virtuellen Computer verändern können.

Im Bereich PRÜFPUNKTE des Hyper-V-Managers sehen Sie nun den erstellten Prüfpunkt. Ein Symbol mit einem grünen Pfeil zeigt dabei an, an welcher Stelle der Prüfpunkte, die hierarchisch dargestellt werden, sich der virtuelle Computer aktuell befindet.

Die PowerShell stellt zur Erstellung und Bearbeitung der Prüfpunkte im Hyper-V-Modul der PowerShell ebenfalls entsprechende Cmdlets bereit. Dazu dient bei PowerShell das Cmdlet `checkpoint-vm`, dem Sie den Namen der VM mitgeben müssen. Die Angabe eines Namens für den Prüfpunkt ist optional:

```
Checkpoint-VM -Name "Erste VM (Windows 10)" -SnapshotName PowerTest1
```

Mit diesem Befehl wird ein neuer Prüfpunkt für die virtuelle Maschine mit dem Namen `Erste VM (Windows 10)` erstellt ([Abbildung 13.11](#)). Den

Namen der VM müssen wir hier in Hochkommas einschließen, da er Leerzeichen beinhaltet. Ohne diese Maskierung würde die PowerShell den virtuellen Computer mit diesem Namen nicht finden können.

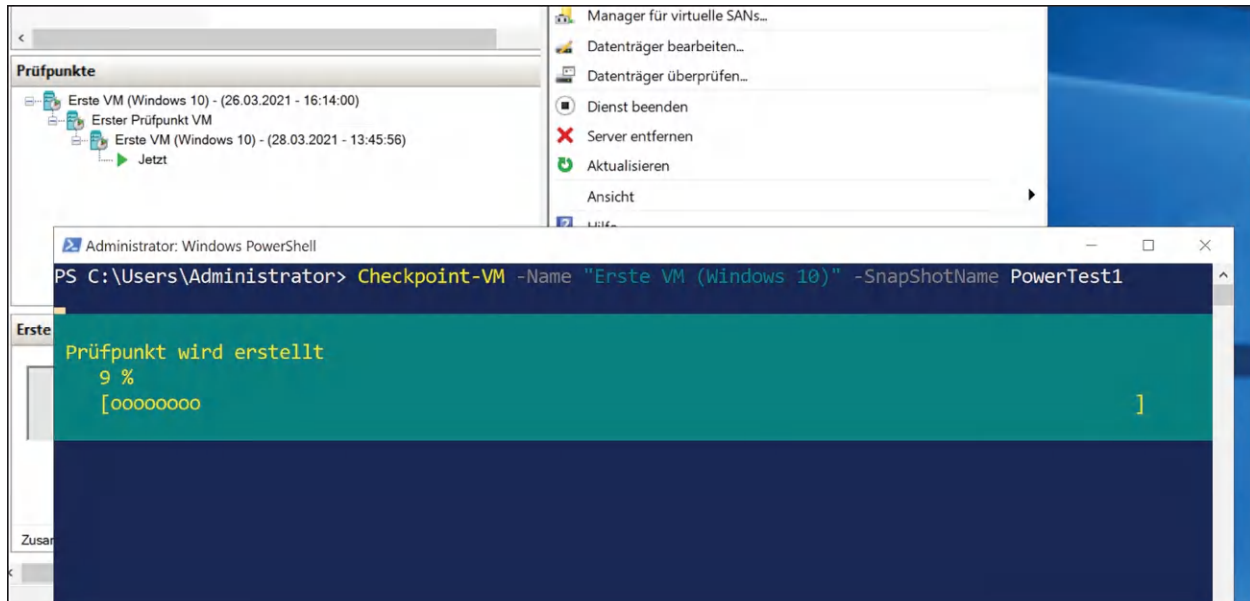


Abbildung 13.11: Das Cmdlet »Checkpoint-VM« hilft dabei, einen neuen Prüfpunkt für einen virtuellen Computer anzulegen.

Anwenden eines Prüfpunkts

Die Prüfpunkte sind dazu da, dass Sie den virtuellen Computer auf den zu diesem Zeitpunkt aktuellen Stand »zurückrollen« können. Das gelingt ganz einfach:

1. Wählen Sie im HYPER-V-MANAGER im Fenster VIRTUELLE COMPUTER die entsprechende virtuelle Maschine aus.
2. Im Fenster PRÜFPUNKTE sehen Sie jetzt die für diesen virtuellen Computer angelegten Prüfpunkte und können einen davon auswählen.
3. Mit einem Rechtsklick darauf öffnen Sie ein Kontextmenü, in dem Sie dann den Eintrag ANWENDEN... auswählen.
4. Es erscheint ein Fenster mit der Sicherheitsfrage, ob Sie den ausgewählten Prüfpunkt wirklich anwenden wollen, und Ihnen werden verschiedene Auswahlmöglichkeiten dazu angeboten ([Abbildung 13.12](#)):

- **PRÜFPUNKT ERSTELLEN UND ANWENDEN:** Dies ist die Option, die Sie in der Regel auswählen werden. Hyper-V erstellt zunächst einen neuen Prüfpunkt des virtuellen Computers, bevor dann der gewählte Prüfpunkt angewendet wird.

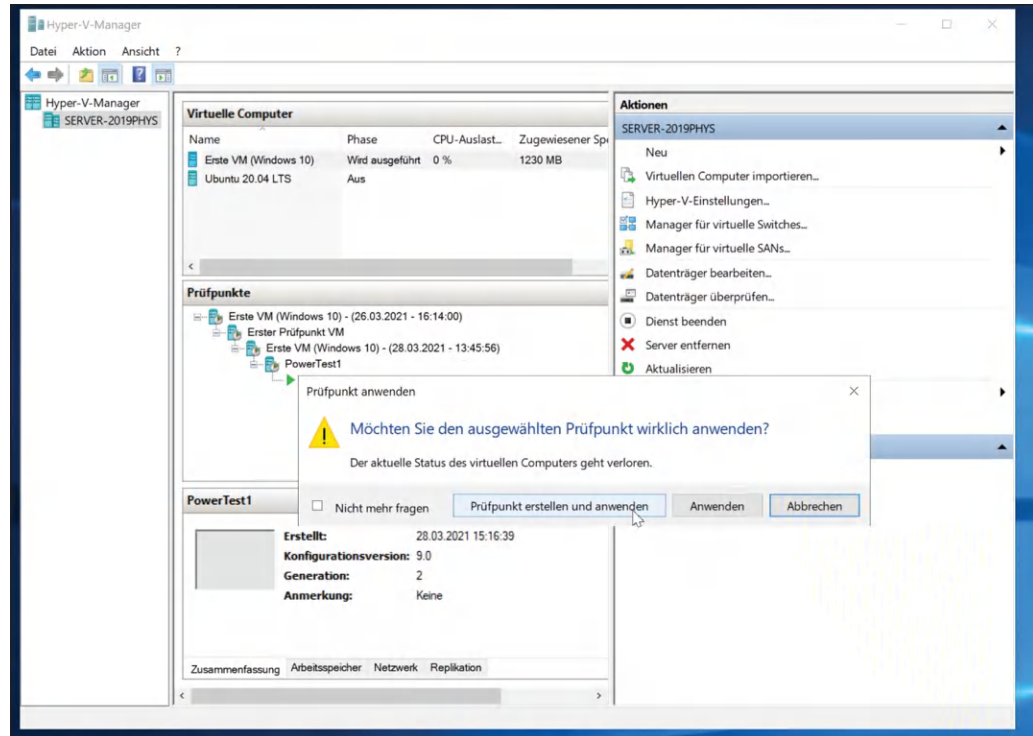


Abbildung 13.12: Das Zurücksetzen eines virtuellen Computers durch die Anwendungen eines Prüfpunkts.

- **ANWENDEN:** Hier wird nur der ausgewählte Prüfpunkt angewendet. Diese Aktion kann nicht rückgängig gemacht werden.
- **ABBRECHEN:** Das Dialogfenster wird geschlossen und die Aktion ohne Änderungen beendet.

Möchten Sie Ihren virtuellen Computer lieber mithilfe der PowerShell zurücksetzen, so können Sie sich mit folgendem Cmdlets zunächst die Liste der Prüfpunkte eines virtuellen Computers anzeigen lassen:

```
Get-VMCheckpoint -VMName <VM-Name>
```

Wollen Sie einen Prüfpunkt aus der Liste anwenden, so gelingt das mit

dem folgenden Aufruf:

```
Restore-VMCheckpoint -Name <Prüfunktname> -VMName <VM-Name> -Confirm:$false
```

Die von uns hier gewählte Option `-Confirm:$false` unterdrückt die Nachfrage, ob Sie diese Aktion wirklich ausführen wollen ([Abbildung 13.13](#)), was für den Einsatz in PowerShell-Skripten sinnvoll ist.

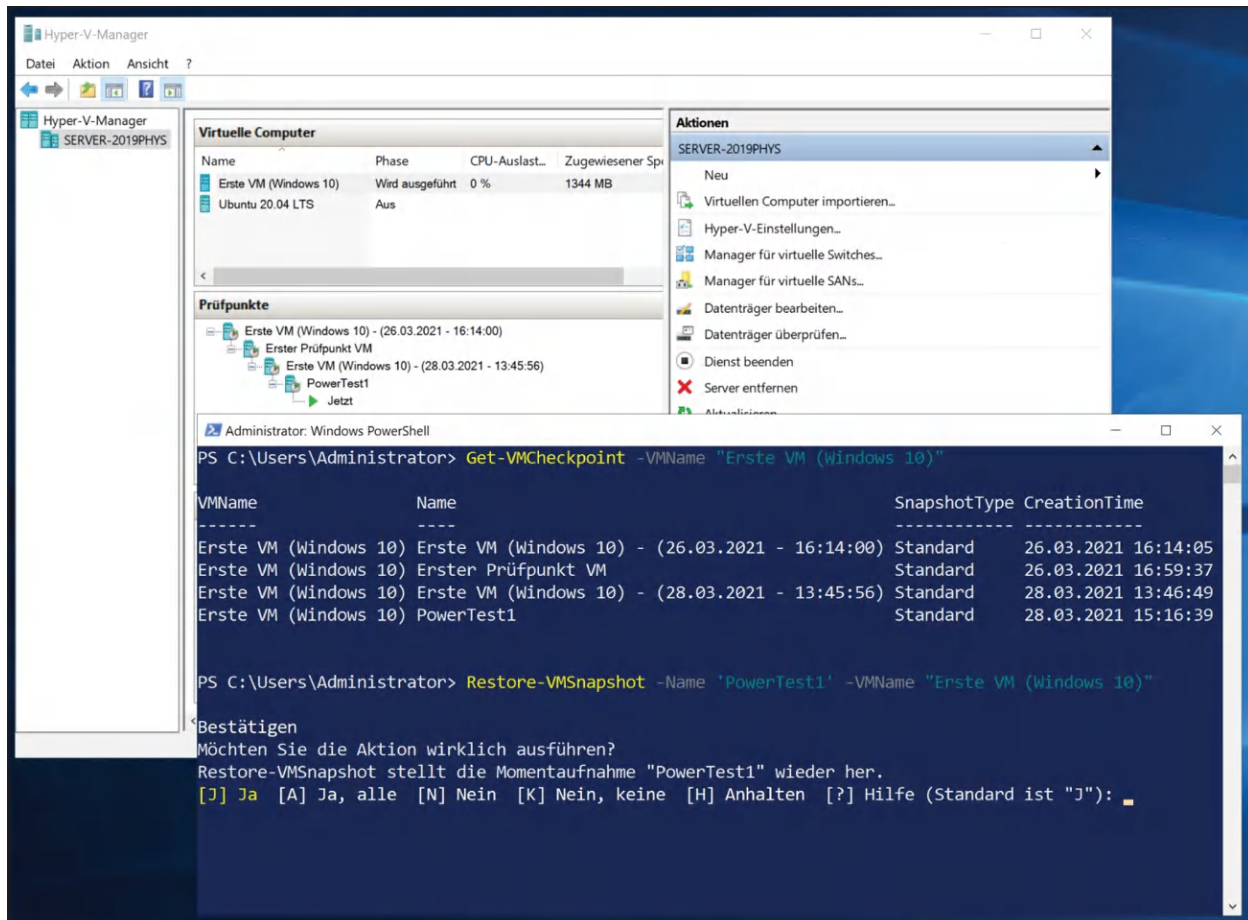


Abbildung 13.13: Auch mithilfe der PowerShell kann ein virtueller Computer auf einen Prüfpunkt zurückgesetzt werden.

Löschen eines Prüfpunkts

Natürlich können Sie einen erstellten Prüfpunkt wieder löschen. Das funktioniert grundsätzlich recht einfach direkt aus dem Hyper-V-Manager heraus:

1. Rufen Sie über einen Rechtsklick auf den gewünschten Prüfpunkt im

HYPER-V-MANAGER das Kontextmenü des Prüfpunkts auf.

2. Wählen Sie dort den Eintrag PRÜFPUNKT LÖSCHEN... aus.
3. Möchten Sie einen Prüfpunkt und alle nachfolgenden Prüfpunkte löschen, müssen Sie dazu zunächst mit der rechten Maustaste auf den frühesten zu löschenden Prüfpunkt klicken. Wählen Sie aus dem Kontextmenü dann den Eintrag PRÜFPUNKTUNTERSTRUKTUR LÖSCHEN... aus. Diese Option löscht den aktuellen Prüfpunkt sowie alle Sicherungen, die Sie nach dem Prüfpunkt erstellt haben und die auf diesem aufbauen. Der Vorgang ähnelt der Option PRÜFPUNKT LÖSCHEN, entfernt aber dabei alle zusammengehörigen Prüfpunkte auf einmal.
4. Bei beiden Einträgen werden Sie danach noch einmal gefragt, ob Sie diesen wirklich löschen wollen. Haben Sie das bestätigt, wird dieser Prüfpunkt beziehungsweise die Prüfpunktunterstruktur gelöscht.

Wer den Einsatz der PowerShell bevorzugt, kann das folgende Cmdlet einsetzen:

```
Remove-VMCheckpoint -VMName <VM-Name> -Name <Prüfpunktname>
```



Sie sollten beim Löschen der Prüfpunkte grundsätzlich mit großer Sorgfalt vorgehen. Wenn von einem Prüfpunkt ein weiterer Knoten abhängt, dann bewirkt das Löschen ein »Verschmelzen« des Prüfpunkts mit dem übergeordneten Element. Der letzte Prüfpunkt in der Reihe ist dann automatisch der aktuelle Status. Er wird im Hyper-V-Manager mit JETZT und einem grünen Pfeil dargestellt. Probleme können durch diesen Mechanismus entstehen, wenn sich beispielsweise in der Reihe eine Version des virtuellen Computers befindet, der durch fehlerhafte Konfiguration oder Schad-Software beschädigt wurde oder sich in einem inkonsistenten Zustand befindet. Wird dieser Prüfpunkt dann durch Löschen mit den anderen Versionen oder sogar der Ursprungsversion vereinigt, haben Sie im Zweifelsfall den gesamten virtuellen Computer beschädigt.

Der Einsatz der PowerShell bietet auch beim Löschen der Prüfpunkte

einige Vorteile. So können Sie beispielsweise mit nur einem Aufruf der folgenden Art alle Prüfpunkte einer virtuellen Maschine löschen, die älter als 30 Tage sind:

```
Get-VMSnapshot -VMName <VM-Name> | Where-Object  
{$_CreationTime -lt (Get-Date).AddDays(-30) } | Remove-  
VMSnapshot
```

Ubuntu-Linux als Gastsystem

Die Liste der unterstützten Gastbetriebssysteme für den Hyper-V ist in der Zwischenzeit erfreulich lang. Dadurch wird es sehr viel leichter, Windows- und Linux-Systeme auf Basis des Windows Server 2019 parallel einzusetzen. Allerdings existiert immer noch eine ganze Reihe von Linux-Distributionen, für die es keine explizite »Betriebserlaubnis« von Microsoft gibt. Das schließt allerdings nicht grundsätzlich aus, dass sie möglicherweise trotzdem als Gastsystem funktionieren könnten. Derlei Konfigurationen sind für experimentelle Einsätze sicherlich denkbar, für den produktiven Betrieb jedoch wenig zielführend.

Wer mit UEFI und anderen Sicherheitsfunktionen arbeiten möchte, wählt bei der Erstellung einer virtuellen Maschine hierzu genau wie bei den Windows-Gastmaschinen eine VM der 2. Generation aus. Wollen Sie nur mal eine Linux-VM ausprobieren, so ist die Nutzung der 1. Generation mit einem klassischen BIOS sicher auch eine gute Wahl, denn selbst bei den ansonsten von Hyper-V offiziell unterstützen Linux-Derivaten gibt es noch Versionen, die nicht für den Einsatz in den moderneren virtuellen Maschinen geeignet sind.



Um den Einsatz von Linux-Distributionen für Hyper-V-Administratoren einfacher zu gestalten, hat Microsoft unter Docs eine spezielle Seite mit dem Namen »Bewährte Methoden für die Ausführung von Linux unter Hyper-V« eingerichtet. Wer mit der englischen Sprache zurechtkommt, sollte diese Seite im Idealfall im Original unter <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/best-practices-for-running->

[linux-on-hyper-v](#) aufsuchen. Die von Microsoft auf den Webseiten mit der Dokumentation zur Verfügung gestellten maschinellen Übersetzungen führen mitunter zu seltsamen, teilweise widersprüchlichen Ergebnissen und auch Missverständnissen.

Wir haben uns entschieden, für diesen Abschnitt ein Ubuntu-Linux in der im März 2021 aktuellen Version 20.04 LTS einzusetzen. Die Abkürzung LTS steht dabei für »Long-Term Support«. Canonical, ein britischer Linux-Distributor, der die Debian-basierte Linux-Variante anbietet, verspricht LTS-Versionen des Betriebssystems in den jeweils folgenden fünf Jahren mit Updates zu versorgen. Ubuntu ist von Microsoft als Gastsystem für virtuelle Maschinen der 2. Generation freigegeben. Wer einfach in den verschiedenen Installationsanleitungen für dieses Gastsystem liest, die in großer Zahl im Internet zu finden sind, wird dabei auf vielfältige Hinweise treffen, die besagen, dass für eine solche Installation sehr spezielle Konfigurationen zwingend notwendig seien. Das trifft aber für diese Linux-Version nur noch sehr bedingt zu, sodass Sie diese prinzipiell auf die gleiche Art und Weise wie ein modernes Windows-Gastsystem installieren können.

1. Laden Sie ein Desktop- oder Server-Image (je nachdem, was Sie installieren möchten) von Ubuntu direkt unter <https://releases.ubuntu.com/20.04/> herunter und stellen Sie die ISO-Datei auf Ihrem Server oder einem Netzwerklaufwerk bereit.
2. Rufen Sie den Hyper-V-Manager auf. Über die Auswahl von AKTION, gefolgt vom Eintrag NEU und dann VIRTUELLER COMPUTER... legen Sie auf die gleiche Art, wie wir es bereits im vorherigen Kapitel gezeigt haben, eine leere virtuelle Maschine der 2. Generation an.
3. Auch die virtuelle Festplatte können Sie auf die gleiche Art und Weise wie für ein Windows-Gastsystem konfigurieren.



Wer sich etwas genauer in die Empfehlungen einliest, die Microsoft für das Anlegen der virtuellen Festplatte für die Linux-Gastsysteme angibt, findet dort ebenso wie auf vielen Webseiten

zum Thema den Hinweis, dass die VHDX-Image-Dateien, die diese virtuellen Festplatten für die Gastsysteme aufnehmen, zu schnell anwachsen könnten. Das wird damit begründet, dass einige Linux-Distributionen an dieser Stelle scheinbar beträchtliche Speicherplatzmengen verbrauchen, obwohl das Dateisystem selbst eigentlich leer ist. Experten raten in diesen Fällen zur Verringerung der Blocksize-Größe von 32 MByte – der Standardeinstellung – auf lediglich 1 MByte. Sind Sie mit diesem Problem konfrontiert, so können Sie bei Bedarf eine neue virtuelle Festplatte mithilfe dieses PowerShell-Kommandos anlegen:

```
New-VHD -Path C:\MyVHDs\test.vhdx -SizeBytes 127GB -  
Dynamic  
-BlockSizeBytes 1MB
```

Wobei Sie natürlich den Pfad passend zu Ihrem System anpassen sollten. Auf der Seite der Linux-VM sollten Sie zusätzlich noch anstelle des EXT3-Dateisystems auf das modernere EXT4 setzen. Es arbeitet laut Microsoft im Zusammenhang mit dynamischen VHDX-Festplattendateien weitaus effizienter.

4. Einen wichtigen Punkt bei der Einrichtung des virtuellen Computers der 2. Generation für ein Linux-Gastsystem finden Sie im Bereich SICHERHEIT der Einstellungen für die VM ([Abbildung 13.14](#)).

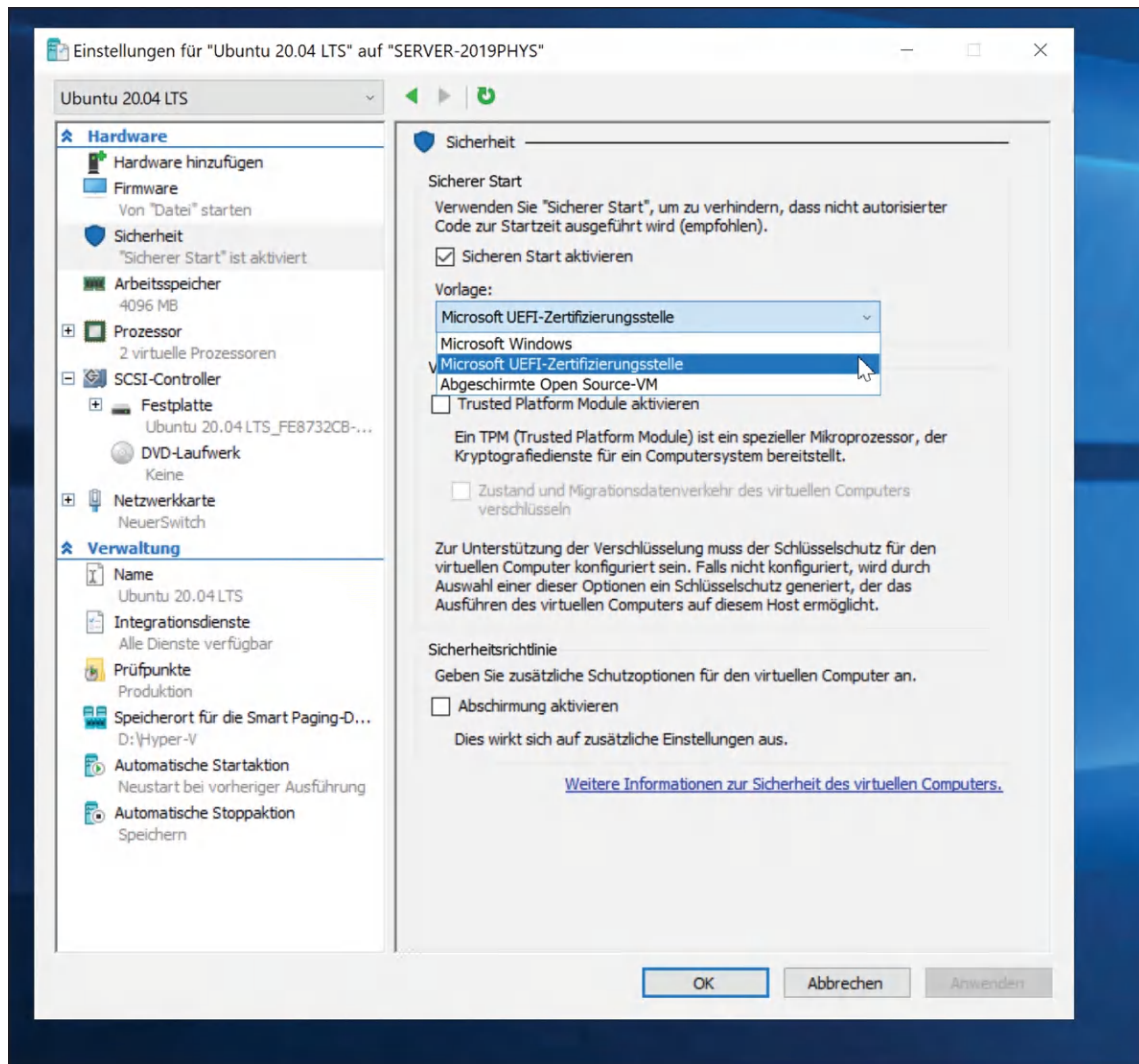


Abbildung 13.14: Ein sicherer Start für einen virtuellen Computer mit Ubuntu-Linux erfordert diese Einstellung für die UEFI-Zertifizierung.

Sie werden in diesem Zusammenhang häufig den Vorschlag lesen können, an dieser Stelle auf den sicheren Start komplett zu verzichten, indem Sie das Kästchen SICHEREN START AKTIVIEREN nicht auswählen. Das ist aber wenig sinnvoll, ist doch der sichere Start via UEFI einer der großen Vorteile der virtuellen Maschinen der 2. Generation. Deshalb sollten Sie an dieser Stelle – wie in [Abbildung 13.14](#) zu sehen – die Einstellung MICROSOFT UEFI-ZERTIFIZIERUNGSSTELLE auswählen, was sowohl mit Ubuntu 20.04 als auch mit der Vorgängerversion 18.04 problemlos funktioniert. Auch diese Einstellung können Sie mithilfe der PowerShell vornehmen:

Set-VMFirmware "VM-NAME" -SecureBootTemplate
MicrosoftUEFICertificateAuthority

5. Haben Sie Ihre VM entsprechend konfiguriert, können Sie nun die ISO-Datei in das virtuelle DVD-Laufwerk »einlegen« und die virtuelle Maschine starten.
6. Sie bekommen den Startbildschirm von Ubuntu-Linux angezeigt und können die gewohnte Installation des Betriebssystems durchlaufen ([Abbildung 13.15](#)).

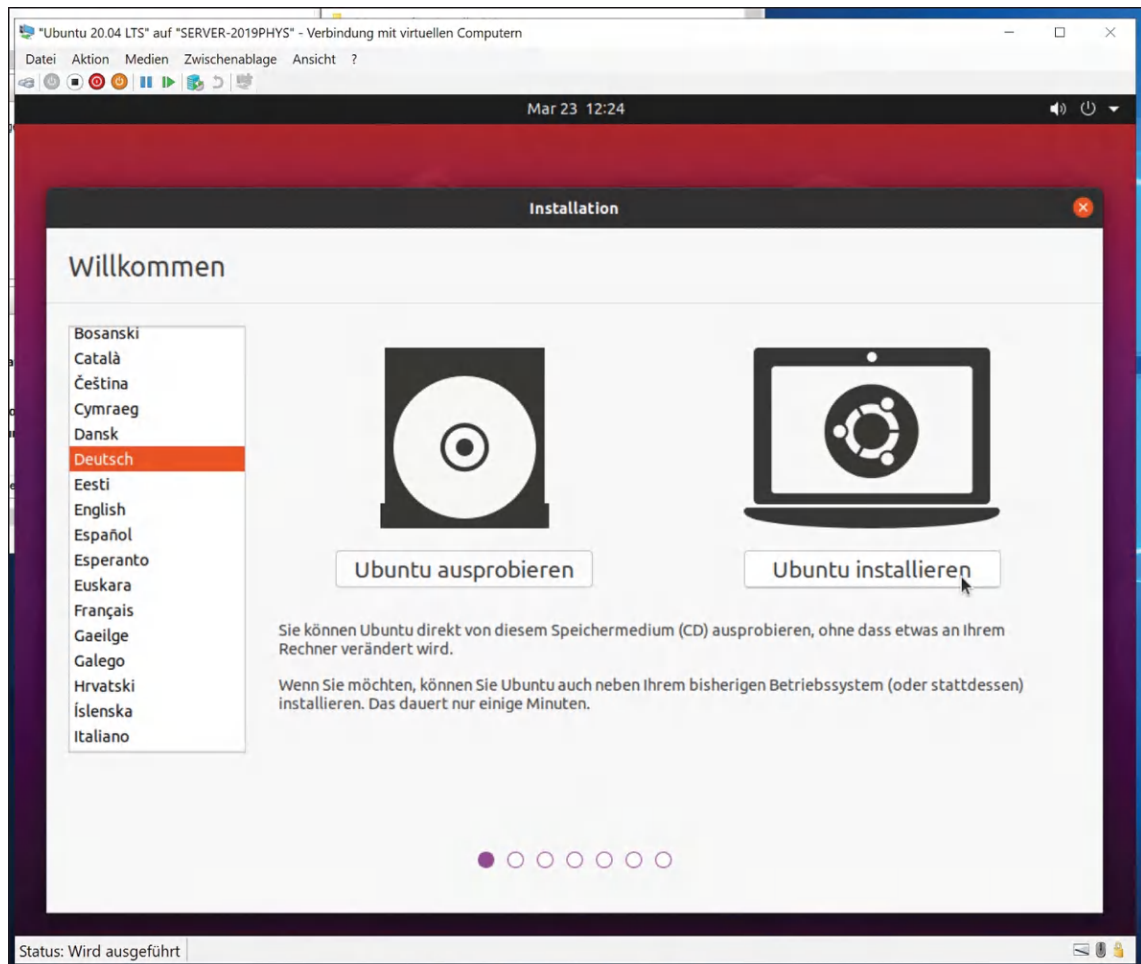


Abbildung 13.15: Die Installation einer aktuellen Linux-Version (hier Ubuntu 20.04 LTS) in einer virtuellen Maschine der 2. Generation

7. Achten Sie darauf, dass Sie auch alle INTEGRATIONSDIENSTE für Ihr Linux-System im Bereich VERWALTUNG der Einstellungen aktivieren.

8. Nach Eingabe aller Daten und einem Neustart steht das Linux-Gastsystem bereit ([Abbildung 13.16](#)).

Spätestens wenn Sie nach dem ersten Start des Linux-Systems im virtuellen Computer in den Vollbildmodus wechseln, werden Sie feststellen, dass die Standardeinstellung für die Bildauflösung dafür nicht ausreicht. Auch wenn Sie im Hyper-V-Manager im Bereich HYPER-V-EINSTELLUNGEN bei der RICHTLINIE FÜR DEN ERWEITERTEN SITZUNGSMODUS das Feature ERWEITERTEN SITZUNGSMODUS ZULASSEN ausgewählt haben (wie bei der Installation des Windows-Gastsystems geschildert), funktioniert dieser erweiterte Modus mit einem Linux- nicht so nahtlos wie mit Windows-Gastsystem oder wie unter VMware Workstation. So ist es zunächst einmal notwendig, dass Sie im Linux-Betriebssystem die Datei `/etc/default/grub` für die richtige Auflösung im Vollbildmodus anpassen:

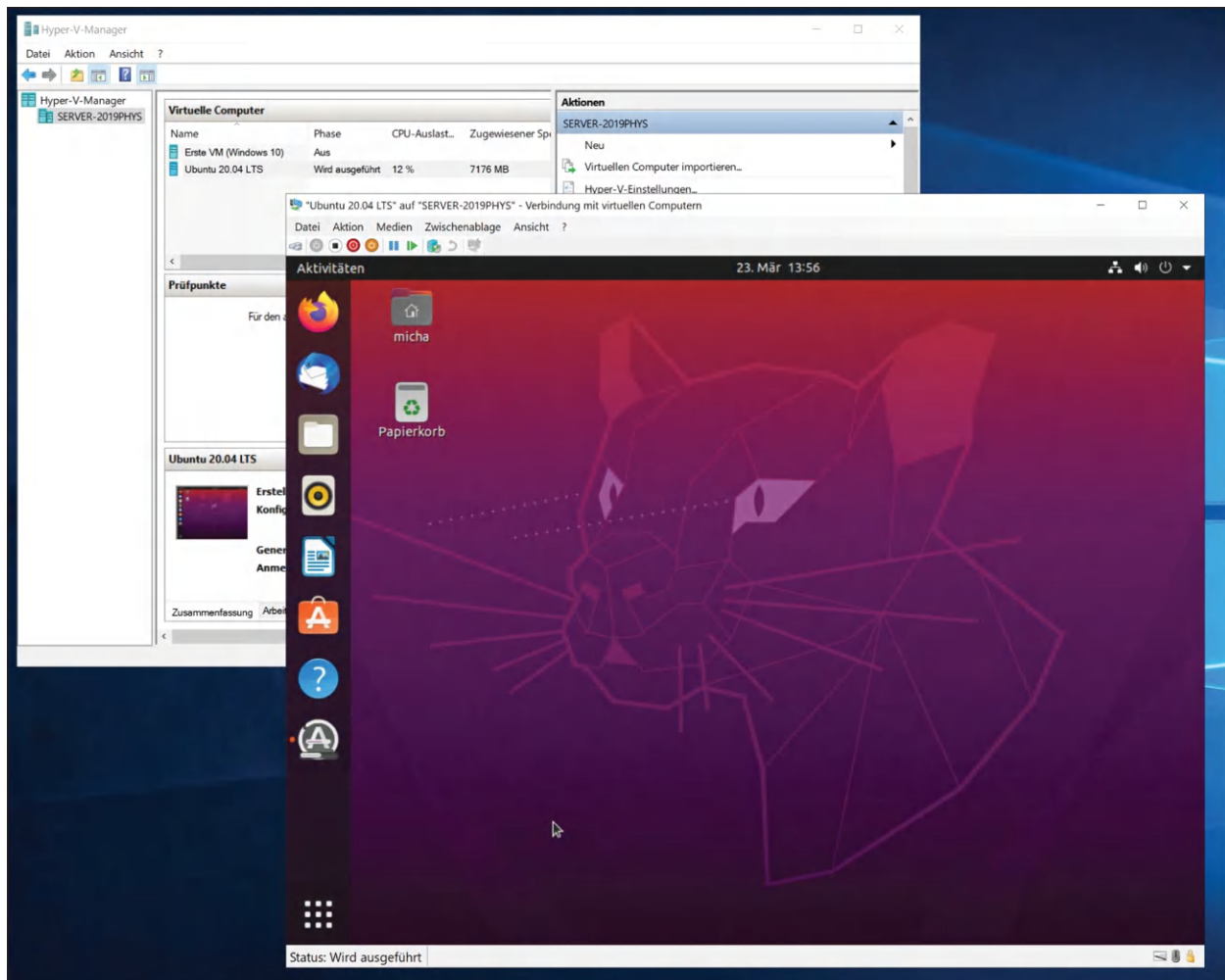


Abbildung 13.16: Nach der Installation: Ubuntu Linux in einer virtuellen Maschine auf einem Windows Server 2019

1. Öffnen Sie im Linux-System ein Terminal-Fenster.
2. Geben Sie dort an der Kommandozeile dann den folgenden Aufruf ein:

```
sudo nano /etc/default/grub
```

Den Befehl `sudo` benötigen Sie, um Administratorrechte zu bekommen, und mit `nano` starten Sie den Editor (Sie können an dieser Stelle natürlich auch den `vi` oder einen anderen Linux-Editor wählen), der dann die Konfigurationsdatei für das Linux-Bootloader-Programm »grub« öffnet.

3. Suchen Sie in dieser Datei nach der Zeile, die mit `GRUB_CMDLINE_LINUX_DEFAULT` beginnt, und fügen Sie das Folgende hinzu: `video=hyperv_fb:[Auflösung YYYYxZZZZ]`.

Das bedeutet, wenn Sie eine Auflösung von 1680 x 1050 nutzen möchten, dass diese Zeile dann so aussehen wird ([Abbildung 13.17](#)):

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet splash  
video=hyperv_fb:1680x1050"
```

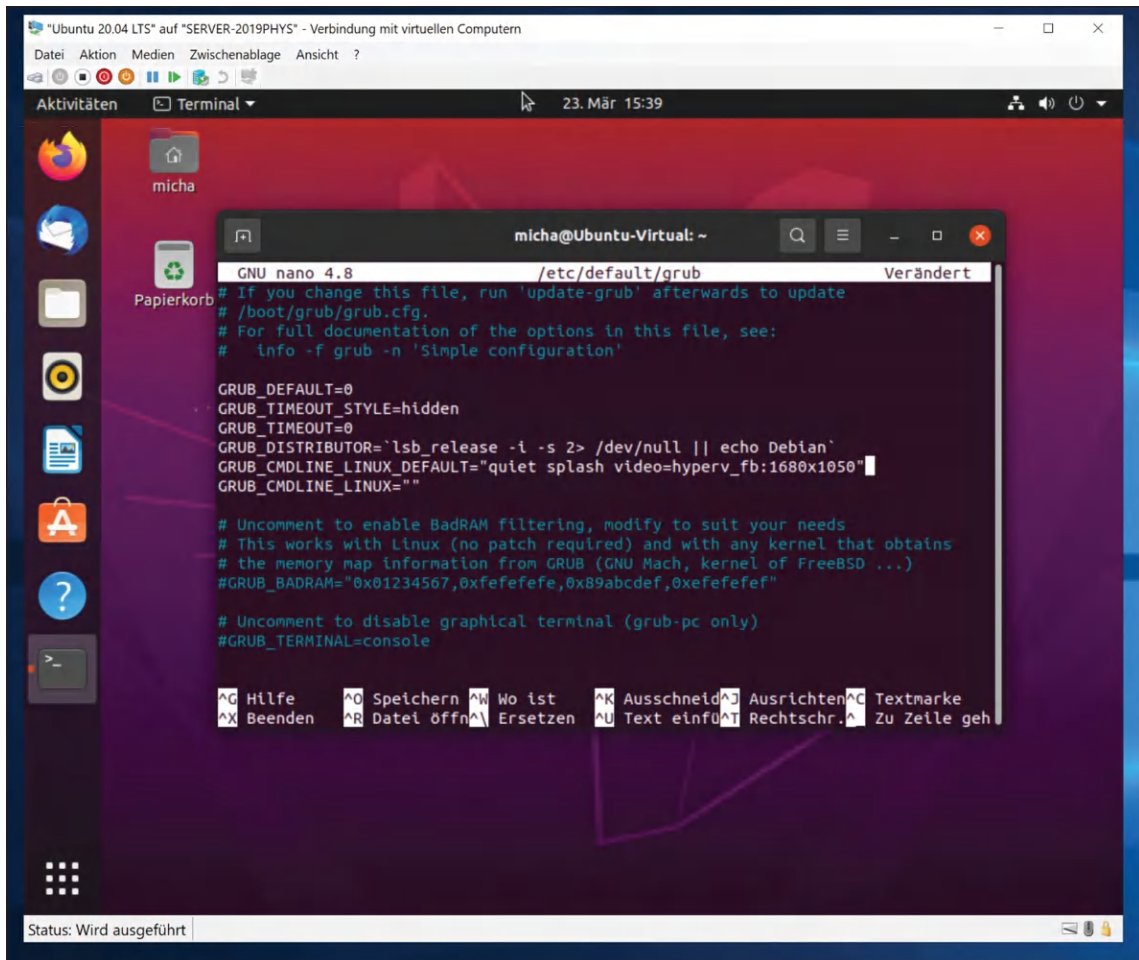


Abbildung 13.17: Mithilfe dieser Konfiguration im Linux-Gast kann dieser im Vollbildmodus auf dem Windows-Server angezeigt werden.

4. Danach speichern Sie die Datei ab und rufen den folgenden Befehl auf der Kommandozeile auf:

```
sudo update-grub
```
5. Anschließend starten Sie das Linux-System entweder über die Eingabe von

```
reboot
```

auf der Kommandozeile des Terminals oder durch Auswahl des Eintrags NEU STARTEN im Menü AKTION des Fensters des virtuellen Computers neu.

Wollen Sie den erweiterten Sitzungsmodus auch mit den Linux-Gastsystemen anwenden, müssen Sie, wie schon bei den Windows-Gastsystemen erläutert, im Hyper-V-Manager im Bereich HYPER-V-EINSTELLUNGEN bei der RICHTLINIE FÜR DEN ERWEITERTEN SITZUNGSMODUS das Feature ERWEITERTEN SITZUNGSMODUS ZULASSEN ausgewählt haben. Zusätzlich müssen Sie aber für die jeweiligen Linux-Gastsysteme noch diverse Softwarepakete nachinstallieren. Dazu müssen Sie unter anderem auch Skripte von GitHub herunterladen und installieren. Hier wird eine derartige Installation sehr gut beschrieben: <https://bit.ly/3szlDcF>.

Kapitel 14

Druckdienste

IN DIESEM KAPITEL

Brauchen wir einen Druckerserver?

Begrifflichkeiten der Druckfunktionen

Installation der Rolle »Druck- und Dokumentendienste«

Drucker bereitstellen

Google-Cloud-Druckdienste und Apple AirPrint

Im- und Export von Druckern

Druckaufträge im Spooler ansehen

Line Printer Daemon (LPD) und Line Printer Remote (LPR)

Internet-Printing

Streng genommen kommen Druckdienste in der IT-Literatur kaum zur Sprache – es gibt spannendere Themen wie virtuelle Container oder Hyperkonvergenz – das klingt schon viel spannender als »Ausdrucken«.

Aus der täglichen Praxis können wir jedoch folgende Aussage eines Mitarbeiters der Firma Siemens über Krankenhäuser nur bekräftigen: »Sollten die uns je in der Zukunft einmal ausbuddeln, dürften die diese Einrichtung für eine Papierfabrik halten.« Sie dürfen das Wort »Einrichtung« gern durch einen Firmennamen, ein Institut oder eine Verwaltung ersetzen – aller Wahrscheinlichkeit nach dürfte es passen.

Unter Windows Server müssen Administratoren:

- ✓ Druckserver installieren und bereitstellen
- ✓ Drucksysteme im Netzwerk freigeben

Grundsätzlich kann jeder Windows-Computer einen angeschlossenen Drucker, unabhängig davon, ob es sich um einen lokal angeschlossenen Drucker oder um einen über das Netzwerk genutzten Drucker handelt, über das Netzwerk für andere Benutzer und Drucker zur Verfügung stellen.



Das Windows-Client-Betriebssystem Windows 10 erlaubt ebenfalls die Freigabe von Ordner und Drucker über das Netzwerk. Aufgrund der Lizenzvereinbarungen im Abschnitt III der Microsoft-Softwarelizenzbedingungen ist der Benutzer jedoch nur berechtigt, bis zu 20 anderen Geräten Zugriff auf das lizenzierte Gerät einzuräumen. Die Anzahl der Geräte gilt für alle Windows-10-Versionen als Obergrenze – Windows Home ist jedoch aus Lizenzgründen nicht in der Lage, einer Domäne beizutreten.

Wenn jeder Server und jedes Client-System selbst die Drucker-Ressource bereitstellen kann, ist dann ein Print-Server überhaupt erforderlich?



Ob sich die Installation eines Druckservers in der Einrichtung lohnt, ist davon abhängig, wie viele Benutzer gemeinschaftlich Drucker nutzen. Möglicherweise ist der Administrator im SOHO-Umfeld (Small Office – Home Office) gut beraten, sich schlicht auf die Bordmittel der Drucker selbst zu verlassen und die wenigen Verknüpfungen von Client zu Drucker manuell einzurichten.

Ein Print-Server stellt einen zentralen Ort für Freigaben von Druckern im Netzwerk bereit. In Umgebungen, bei denen viele Benutzer auf dieselben Drucker zugreifen, ist die Einrichtung eines Druckerservers in der Domäne eine sinnvolle Entscheidung.

Das Schlüsselwort in dem vorherigen Satz ist: dieselben. Drucken mehrere Windows-Clients auf einem Drucker ohne den Einsatz von Print-Servern, gibt es je Windows-Client-System eine eigene Druckerwarteschlange. In einer Variante mit einem Print-Server gibt es eine vom Server gemeinschaftlich genutzte Druckerwarteschlange – aus Sicht des Administrators eine zu favorisierende Umsetzung, die im Fehlerfall eine

deutlich schnellere Prüfung erlaubt.

Auf Druckerserver »sammeln« Administratoren die verschiedenen Druckertreiber und stellen diese ebenfalls zentral für Client-Computer zur Verfügung. Sorgt ein Administrator für eine automatische Zuordnung eines Druckers zu einem Client-Computer wird der Druckertreiber auf dem Zielsystem zur Installation gebracht.



Das Drucksystem von Windows ist zwar leistungsfähig und robust, aber nicht besonders komfortabel für den Anwender. Das Aufkommen mobiler Computersysteme wie Laptops, Tablets oder Smartphones zwang die Druckerherstellerbranche zu technologischen Anpassungen. Infolge der Ausbreitung der Mobilgeräte kam es zu einer der dynamischsten Entwicklungen im Druckerbereich seit Jahrzehnten.

Traditionell geprägte IT-Landschaften, die eine Druckzuweisung über Gruppenrichtlinien oder Anmeldeskripte auf Basis des Client- oder Benutzer-Namens ableiten, gibt es nach wie vor, und sie bieten sich in statischen Umgebungen durchaus an. Mobilten Benutzern, die von verschiedenen Orten im Unternehmen auf einen in der Nähe positionierten Drucker zugreifen, wird der Administrator mit dieser Zuordnung jedoch kaum gerecht. Zu der wechselnden Benutzer- und Gerätelokalität gesellen sich verschiedene Zugriffsgeräte mit unterschiedlichen Betriebssystemen. Da passen statische Print-Server-Systeme im Unternehmen nicht so recht zur Anforderung.

Speziallösungen wie beispielsweise »PrinterLogic« oder »LocateMyPrinters« erweitern die vorhandene Print-Server-Landschaft um eine für den Anwender leicht zu benutzende Oberfläche, die einen schnellen Wechsel des Druckers ermöglicht. Anstatt sich durch die kryptischen Bezeichnungen der IT-Administratoren durchzukämpfen, bieten diese Programme eine zusätzliche Benennungsschicht oder unterstützen den Benutzer durch eine durchklickbare Abbildung der Unternehmensräumlichkeiten, die eine gezielte Auswahl ermöglicht.

Eine andere Variante ist »Print & Follow«: Der Druckauftrag wird an einen speziellen Druckertreiber geschickt, der vom Benutzer eine Authentifizierung am Druckgerät selbst erfordert (zum Beispiel Chip, QR-Code oder PIN) und erst dann den Druckauftrag vom Print-Server auf dieses Gerät schickt.

Begrifflichkeiten

Rund um das Thema Drucken gibt es einige Begrifflichkeiten, die Sie als Administrator unbedingt sicher beherrschen müssen. Gleichzeitig zeigt sich über diese Terminologie der Weg von der Anwendung zum Ausgabegerät:

- ✓ **Druckertreiber** – Beim Drucken eines Dokuments wird ein sogenannter Druckertreiber verwendet. Hierbei handelt es sich um eine Software, die das zu druckende Dokument in für den Drucker verständliche Daten umwandelt. Treiber sind hardwarenahe Programme, die passend zum Betriebssystem und der Architektur (ARM, x86, x64) entwickelt werden.

Seit der Version 2008 von Windows Server, respektive Windows 7 als Client-Betriebssystem, arbeitet Microsoft nach einem einheitlichen Treibermodell. Ein Basisdruckertreiber für Windows 8 wird aller Wahrscheinlichkeit nach auch unter Windows Server 2019 funktionieren. Ein Druckertreiber für Windows Server 2003 wird jedoch höchstwahrscheinlich nicht auf einem aktuellen Windows Server funktionieren.

Druckertreiber, die vom Hersteller als »paketfähig« eingestuft sind, eignen sich zur gezielten Installation im Rahmen der Bereitstellung.

Mitunter ist es möglich, einen Drucker mit dem Treiber eines »älteren Vorläufers« anzusprechen.



Nutzen Sie in professionellen Umgebungen stets nur die passenden Druckertreiber. Im Internet finden sich diverse Anleitungen, die beschreiben, wie die Signaturprüfung für einen Treiber mit BCEDIT

unterdrückt wird, um einen älteren Treiber ohne Signatur wieder zum Laufen zu bringen. Das ist, salopp gesagt, »Murks« – Sie sollten solche Modifikationen grundsätzlich ablehnen.

In der [Abbildung 14.1](#) sehen Sie einen Teil der Treiber, die sich auf einem seit Jahren in Betrieb befindlichen Druckserver gesammelt haben:

- ✓ Lokaler Druckerspooler/Druckprozessor – Benutzer drucken üblicherweise aus einer Anwendung heraus. Die Anwendung nutzt den Druckertreiber zur Konvertierung des Dokuments in ein für das ausgewählte Druckergerät interpretierbares Dateiformat. Das Dokument wird anschließend an den lokalen Druckerspooler auf dem Client/Server weitergeleitet. Dieser lokale Druckerspooler leitet den Auftrag an den Druckprozessor weiter, der die gerätespezifischen Rohdaten erzeugt.
- ✓ Druckerspooler auf dem Print-Server – Die vom Druckprozessor generierten Rohdaten gelangen, in einem Print-Server-Szenario, über das Netzwerk an den Druckerspooler des Druckerservers. In diesem Zusammenhang sei auf den WinSpool.driv hingewiesen, der den lokalen Druckauftrag an ein Remotesystem sendet und sicherstellt, dass die passenden Treiber zur Verfügung stehen.
- ✓ Druckerwarteschlange – Die Druckerwarteschlange ist die softwaretechnische Abbildung des Druckers selbst. Die Datei des Druckauftrags (Print Job) wird in die Druckerwarteschlange (Print Queue) kopiert und gemäß der Position und Priorität abgearbeitet.
- ✓ Druckmonitor – Erreicht das zu druckende Dokument in der Druckerwarteschlange den vordersten Platz, sendet der Druckmonitor (Print Monitor) das Dokument zur Ausgabe an das Druckgerät.
- ✓ Druckgerät – Beim Druckgerät (Print Device) kann es sich um einen physischen Drucker handeln, aber auch um ein »virtuelles Gerät«, das beispielsweise den Druckauftrag in eine PDF-Datei umlenkt.

Druckverwaltung							
Datei Aktion Ansicht ?							
Druckverwaltung		Treibername	Umgebung	Treiberversion	Treiberisolation	Anbieter	Druckpr... Paket
Benutzerdefinierte Filter		Apple Color LW 12/660 PS	Windows NT x86	5.2.3790.3959	Freigegeben	Microsoft	Falsch
Druckerserver		Microsoft XPS Document Write...	Windows x64	6.2.9200.16384	Kein	Microsoft	winprint Wahr
12ps01 (lokal)		OKI MICROLINE 6300F	Windows x64	6.1.7600.16385	Freigegeben	Okidata	winprint Wahr
Treiber		Microsoft enhanced Point and ...	Windows x64	6.2.9200.23194	Freigegeben	Microsoft	winprint Wahr
Formulare		Kyocera FS-1300D	Windows x64	6.1.7600.16385	Freigegeben	Kyocera	winprint Wahr
Anschlüsse		Epson LQ-500C	Windows x64	6.1.7233.0	Freigegeben	Microsoft	winprint Wahr
Drucker		Microsoft enhanced Point and ...	Windows NT x86	6.2.9200.23194	Freigegeben	Microsoft	winprint Wahr
Bereitgestellte Drucker		Brother HL-4050CDN series	Windows NT x86	1.7.0.0	Freigegeben	Brother	winprint Wahr
		TOSHIBA e-STUDIO356 PCL6 V4	Windows x64	6.2.9200.16430	Kein	TOSHIBA	winprint Wahr
		TOSHIBA e-STUDIO306 PCL6 V4	Windows x64	6.2.9200.16430	Kein	TOSHIBA	winprint Wahr
		TOSHIBA e-STUDIO305 PCL6 V4	Windows x64	6.2.9200.16430	Kein	TOSHIBA	winprint Wahr
		TOSHIBA e-STUDIO256 PCL6 V4	Windows x64	6.2.9200.16430	Kein	TOSHIBA	winprint Wahr
		TOSHIBA e-STUDIO B/W PCL6 V4	Windows x64	6.2.9200.16430	Kein	TOSHIBA	winprint Wahr
		Samsung B/W Laser PCL6 Class...	Windows x64	6.2.9200.16384	Kein	Samsung	winprint Wahr
		OKI Dot-Matrix ESC/PK Class Dr...	Windows x64	6.2.9200.16430	Kein	OKI	winprint Wahr
		OKI Dot-Matrix 24Pin ESC/P Cla...	Windows x64	6.2.9200.16430	Kein	OKI	winprint Wahr
		HP LaserJet PCLm Class Driver	Windows x64	6.2.9200.16430	Kein	HP	winprint Wahr
		HP LaserJet A4/Letter PS Class ...	Windows x64	6.2.9200.16430	Kein	HP	winprint Wahr
		HP LaserJet 6L PS Class Driver	Windows x64	6.2.9200.16430	Kein	HP	winprint Wahr
		HP LaserJet 2300 PS Class Driver	Windows x64	6.2.9200.16430	Kein	HP	winprint Wahr
		Brother Laser Type1 Class Driver	Windows x64	6.2.9200.16384	Kein	Brother	winprint Wahr
		Brother Laser Leg Type1 Class D...	Windows x64	6.2.9200.16384	Kein	Brother	winprint Wahr
		Brother Color Type3 Class Driver	Windows x64	6.2.9200.16384	Kein	Brother	winprint Wahr
		TP Output Gateway PS	Windows x64	1.0.0.12	Freigegeben	ThinPrint	Falsch
		TP Output Gateway PS	Windows NT x86	1.0.0.12	Freigegeben	ThinPrint	Falsch
		Brother HL-4050CDN series	Windows x64	1.13.0.0	Freigegeben	Brother	winprint Wahr
		Brother HL-5270DN series	Windows x64	3.25.0.0	Freigegeben	Brother	winprint Wahr
		Brother HL-5250DN series	Windows x64	3.25.0.0	Freigegeben	Brother	winprint Wahr
		Brother HL-2030 series	Windows x64	3.25.0.0	Freigegeben	Brother	winprint Wahr
		TP Output Gateway	Windows NT x86	7.15.0.6	Freigegeben	ThinPrint	Falsch

Abbildung 14.1: Mit der Zeit sammeln sich Unmengen an Druckertreibern.



An sich ist es nicht die Aufgabe des Windows-Administrators, sich über die Peripheriegeräteausrüstung großartig Gedanken machen zu müssen, doch bei der Produktauswahl von Druckern sollte er mitreden. Insbesondere günstige Geräte verfügen über technische Limitierungen, die sich im Tagesgeschäft negativ äußern werden: GDI (Graphics Device Interface).

GDI ist in erster Linie eine Komponente des Betriebssystems Microsoft Windows und dient als Programmierschnittstelle zu den logischen Grafikgeräten wie Grafikkarte oder Drucker. Bei Druckern erlaubt GDI den Aufbau sehr einfacher Hardware, da die »Intelligenz der Druckaufbereitung« nicht vom Drucker vorgenommen wird, sondern vom Betriebssystem. Der fehlende »Bildprozessor«, der die Rasterung des Ausdrucks vornimmt, mündet in einen besonders

günstigen Anschaffungspreis. Dem niedrigen Anschaffungspreis steht jedoch ein besonderes Risiko entgegen: die geringe Treiberverfügbarkeit.

Stellt der Hersteller für eine neue Windows-Version keinen Treiber bereit, so ist das Gerät nutzlos. Für den Hewlett Packard LaserJet 1010 beispielsweise gibt es keine Treiber für Windows Vista oder höher, wohl aber für den beinahe baugleichen LaserJet 1018. Der Einsatz von GDI-Druckern ist im Unternehmensumfeld kaum zu empfehlen, insbesondere dann, wenn Terminal-Services im Zusammenspiel mit ThinClients verwendet werden.

Interessanterweise sind GDI-Drucker bei kleineren Druckaufträgen in Bezug auf die Druckgeschwindigkeit größeren Druckern nicht unterlegen.

Anders als bei den GDI-Druckern handelt es sich bei PCL- und PostScript-Geräten um Drucker, die die Rasterung für den Ausdruck selbst berechnen.

PCL wird von einer großen Anzahl von Herstellern verwendet und ist aktuell der Standard für Laserdrucker. PCL, die Printer Command Language, ist eine von Hewlett-Packard entwickelte Befehlssprache zum Steuern von Laserdruckern, die aber auch bei vielen Tintenstrahldruckern eingesetzt wird.

PostScript, entwickelt von der Firma Adobe, hat sich mit den Jahren zu einem De-facto-Standard in der Druckindustrie entwickelt. In PostScript-Dateien wird das darzustellende Objekt im PostScript-Code beschrieben. PostScript ist weit mehr als eine Sprache, um einen Drucker anzusteuern – das heute sehr weit verbreitete PDF-Format basiert auf dem deutlich älteren PostScript.

Installation von Druck- und Dokumentendiensten

Der Druckdienst ist in Windows Server als Rolle implementiert. Diese umfasste bis zur Version 2016 auch den sogenannten »Distributed Scan

Server«, den die Firma Microsoft mit dem Server 2019 endgültig entfernte. Zudem entfällt auf den neueren Versionen des Servers die umfangreiche Grundausstattung mit verschiedenen Druckertreibern. Es ist nun die Aufgabe des Administrators, diese bei Bedarf nachzuinstallieren.

Nun kommen wir zur Installation der entsprechenden Rolle auf einem Windows-Server, um diesen zu einem Druckserver zu machen. In früheren Windows-Versionen war diese Funktionalität automatisch aktiv, neuere Server-Versionen erfordern das bewusste Einschalten durch den Administrator.

Im einfachsten Fall installieren Sie die Rolle über den Server-Manager:

1. Starten Sie den Server-Manager.
2. Wählen Sie oben rechts unter VERWALTEN den Eintrag ROLLEN UND FEATURES HINZUFÜGEN.
3. Bestätigen Sie den gewünschten Server/Installationstyp.
4. Wählen Sie in der Auflistung im Assistenten zum HINZUFÜGEN VON ROLLEN UND FEATURES den Eintrag DRUCK- UND DOKUMENTENDIENSTE und wundern Sie sich nicht, dass die Beschreibung auf der rechten Seite, zu sehen in [Abbildung 14.2](#), für diese Rolle auf Englisch verfasst ist.

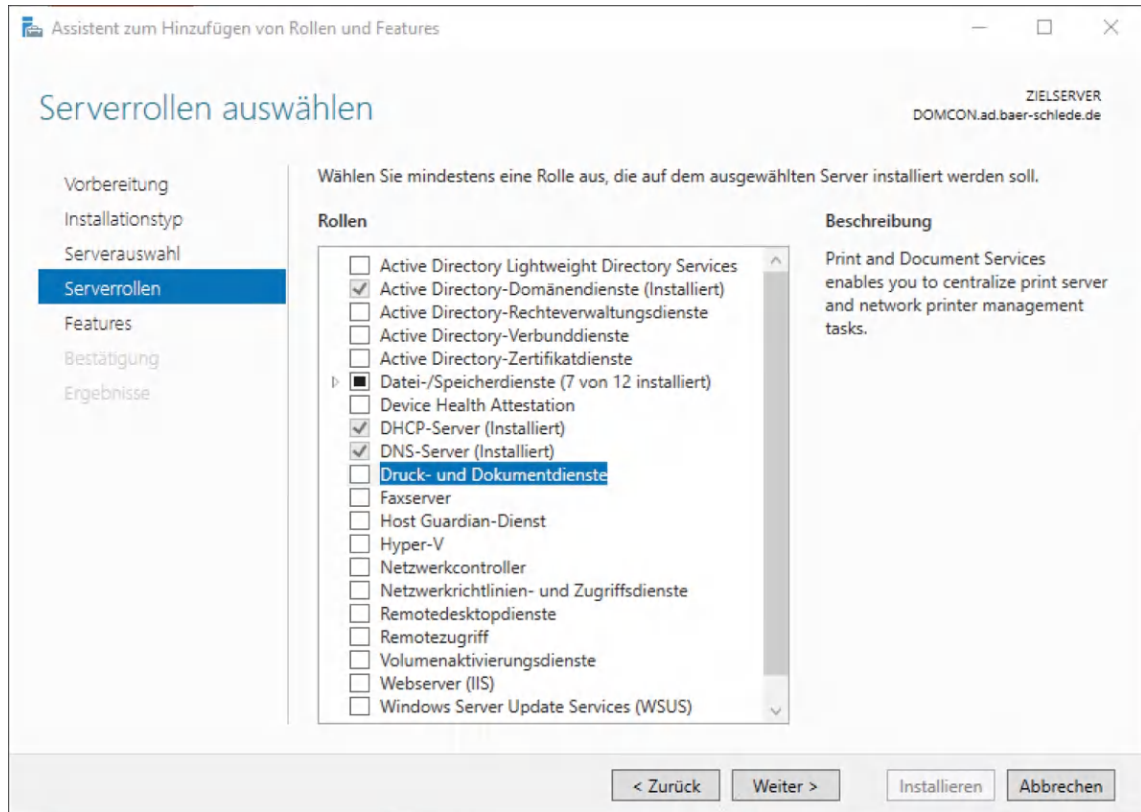


Abbildung 14.2: Bei der Rollenbeschreibung wurde der Text nicht übersetzt.

5. Nachdem Sie die Rollen/Feature-Auswahl abgeschlossen haben, erscheint ein überaus wichtiger Dialogtext:

- Windows Server 2019 (und höher) unterstützt Druckerwarteschlangen mit Druckertreibern des Typs 3 oder 4.
- Es ist empfehlenswert, Druckertreiber des Typs 4 zu verwenden. Mit diesem Typ können Benutzer, die nicht Mitglied der lokalen Administratorengruppen sind, standardmäßig eine Verbindung mit dem Drucker herstellen. Benutzer von 32-Bit-Clients können auch ohne einen 32-Bit-Treiber eine Verbindung mit dem Druckerserver herstellen.



Zu den Druckertreibern des Typs 4 hält Microsoft eine umfangreiche und äußerst detaillierte Webseite für Hardware-Entwickler bereit; auf diese sei hier hingewiesen: <https://docs.microsoft.com/en-us/windows-hardware/drivers/print/v4-printer-driver>.

Das Auffinden von Druckertreibern dieses Typs stellt sich zum Zeitpunkt der Manuskripterstellung als äußerst schwierig heraus. Die Universal-Druckertreiber der etablierten Hersteller liefern aktuell noch den Typ 3 – im Benutzermodus. In der täglichen Praxis ist es unerheblich, ob Sie mit einem Typ 3 oder Typ 4 Treiber arbeiten. Im LPR-/LPD-Umfeld sind im Zusammenspiel mit macOS Probleme bekannt, sobald es sich um einen Typ-4-Treiber handelt.

- Sie müssen signierte, paketfähige Treiber verwenden, damit Clients eine Verbindung mit freigegebenen Druckerwarteschlangen herstellen können, die den Druckertreiber des Typs 3 auf dem Druckerserver unterstützen. Falls keine signierten oder paketfähigen Treiber vorhanden sind, müssen Clientbenutzer entweder als lokale Administratoren angemeldet sein, oder Sie haben die Gruppenrichtlinie für Computer\Administrative Vorlagen\Drucker\Point-and-Print-Einschränkungen bereits für Sicherheitseingabeaufforderung konfiguriert.
 - Sie müssen eine übereinstimmende 32-Bit-Version des Druckerstreibers auf dem Druckerserver installieren, wenn Sie Druckertreiber des Typs 3 und 32-Bit-Clients einsetzen. Sollten keine 32-Bit-Treiber installiert sein, können Clients möglicherweise keine Verbindung mit dem Drucker herstellen.
6. Bestätigen Sie unter ROLLENDIENSTE, ob Sie neben dem DRUCKERSERVER auch noch das INTERNETDRUCKEN (IPP) und den LPD-DIENST für Unix-basierte Computer installieren möchten ([Abbildung 14.3](#)). In Windows-Standardumgebungen sind beide Optionen nicht erforderlich.



Die Dienste LPD und LPR gelten bei Microsoft seit Erscheinen des Windows Server 2012 als »deprecated«. Hiermit markiert der Hersteller Techniken, die in einer künftigen Produktversion, möglicherweise ohne weitere Vorankündigung, entfernt werden. Für Entwickler, IT-Architekten und Administratoren heißt dies

folgerichtig, dass sie ihre Strategie bezüglich LPD/LPR anpassen sollten.

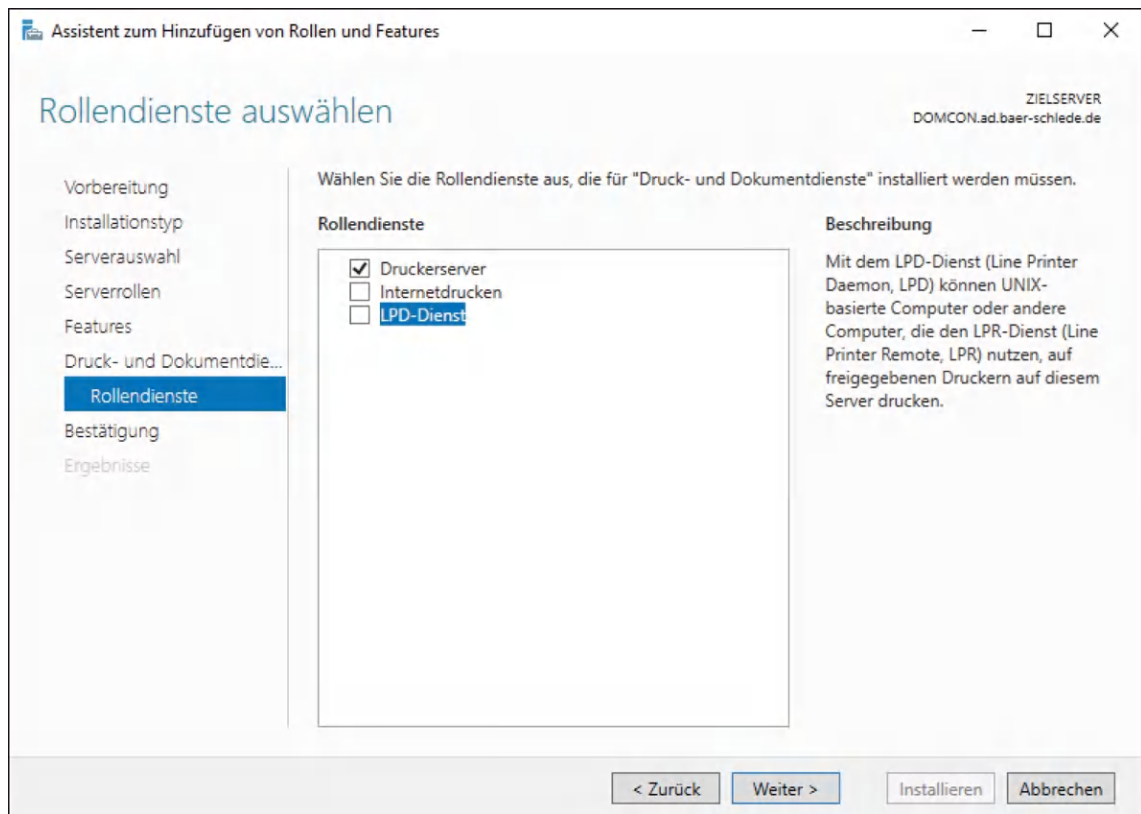


Abbildung 14.3: Die Dienste LPD und IPP werden die meisten Administratoren nicht benötigen.

7. Bestätigen Sie noch einmal die Zusammenfassung, und der Serverdienst für das Drucken wird eingerichtet.
8. Der Server ist nun ein Druckerserver/Print-Server.

Sie können, wie bei den meisten Rollen und Features, auch diese Installation über die PowerShell durchführen:

```
Install-WindowsFeature -Name Print-Server
```

Die optionalen Druckfunktionen installieren Sie mithilfe der Kommandos

```
Install-WindowsFeature -Name Print-Internet
```

beziehungsweise

```
Install-WindowsFeature -Name Print-LPD-Service
```




Sie können einen Print-Server auf einer Core-Variante von Windows Server installieren und den Server problemlos aus der Ferne verwalten. Lediglich die Aktivierung des IPP (Internet-Printings) erfordert einen Server mit grafischem Desktop.

Das sichtbarste Zeichen der erfolgreichen Installation ist das Vorhandensein der DRUCKERVERWALTUNG unter TOOLS im Server-Manager und im Ordner WINDOWS-VERWALTUNGSPROGRAMME im Startmenü.



Administratoren mit einigen Jahren Berufserfahrung dürften sich an die Cluster-HA-Funktionalitäten von Microsoft Windows Server in Bezug auf den Druckerserver erinnern. Mit der Version 2012 hat das Redmonder Unternehmen diese Technik eingestellt und verweist seither auf die Hochverfügbarkeit von Hyper-V. Dies gilt ebenso – auch wenn es nicht explizit zum Ausdruck gebracht wurde – für eine VMware-vSphere-Umgebung.

Druckerserver in der Druckerverwaltung hinzufügen

Bei der Druckerverwaltung handelt es sich um ein typisches Microsoft MMC Snap-in mit den Menübefehlen DATEI, AKTION und ANSICHT. Bei Bedarf sind Administratoren in der Lage, in diese Ansicht alle gewünschten Druckserver einzubinden oder wieder zu entfernen:

1. Klicken Sie in der Druckerverwaltungsstruktur auf DRUCKERVERWALTUNG.
2. Hier finden Sie die Option SERVER HINZUFÜGEN/ENTFERNEN.
3. Im sich öffnenden Fenster können Sie die entsprechenden Funktionen wie DRUCKERSERVER ANGEBEN oder SERVER HINZUFÜGEN auswählen.

4. Um einen Server auszuwählen, geben Sie den Namen ein oder klicken auf DURCHSUCHEN.
5. Wählen Sie nun die Option LISTE HINZUFÜGEN.
6. Fügen Sie jetzt so viele Server hinzu, wie Sie benötigen, und schließen Sie den Vorgang mit OK ab.
7. Möchten Sie einen Druckerserver entfernen, gehen Sie gleichermaßen vor. Wählen Sie statt HINZUFÜGEN jedoch ENTFERNEN/LÖSCHEN.

Arbeiten mit Druckfiltern

In größeren Umgebungen mit vielen Druckern und vielen Druckservern wird die Ansicht für den Administrator zunehmend unübersichtlich. Die Microsoft-Entwickler haben hierfür im oberen Bereich der Baumstruktur der Druckerverwaltung Filterfunktionen eingebaut. Mit deren Hilfe kann sich der IT-Profi auf die gewünschten Drucker fokussieren. Es gibt bereits vier vorgefertigte Filter:

- ✓ Alle Drucker – In Klammern steht die Gesamtzahl.
- ✓ Alle Treiber – In Klammern steht die Gesamtzahl der bekannten Treiber.
- ✓ Drucker mit Aufträgen
- ✓ Drucker nicht bereit

In der Standardeinstellung stellt Windows die Anzahl in Klammern bei den letztgenannten Filtern nicht dar. Das können Sie bei Bedarf leicht anpassen:

1. Klicken Sie mit der rechten Maustaste auf den Filter.
2. Wählen Sie im Kontextmenü EIGENSCHAFTEN.
3. Wählen Sie im Dialogfenster EIGENSCHAFTEN VON ... in der Registerkarte ALLGEMEIN unterhalb des Kastens der BESCHREIBUNG das Optionshäkchen GESAMTZAHL DER

ELEMENTE NEBEN DEM NAMEN DES FILTERS ANZEIGEN aus ([Abbildung 14.4](#)).

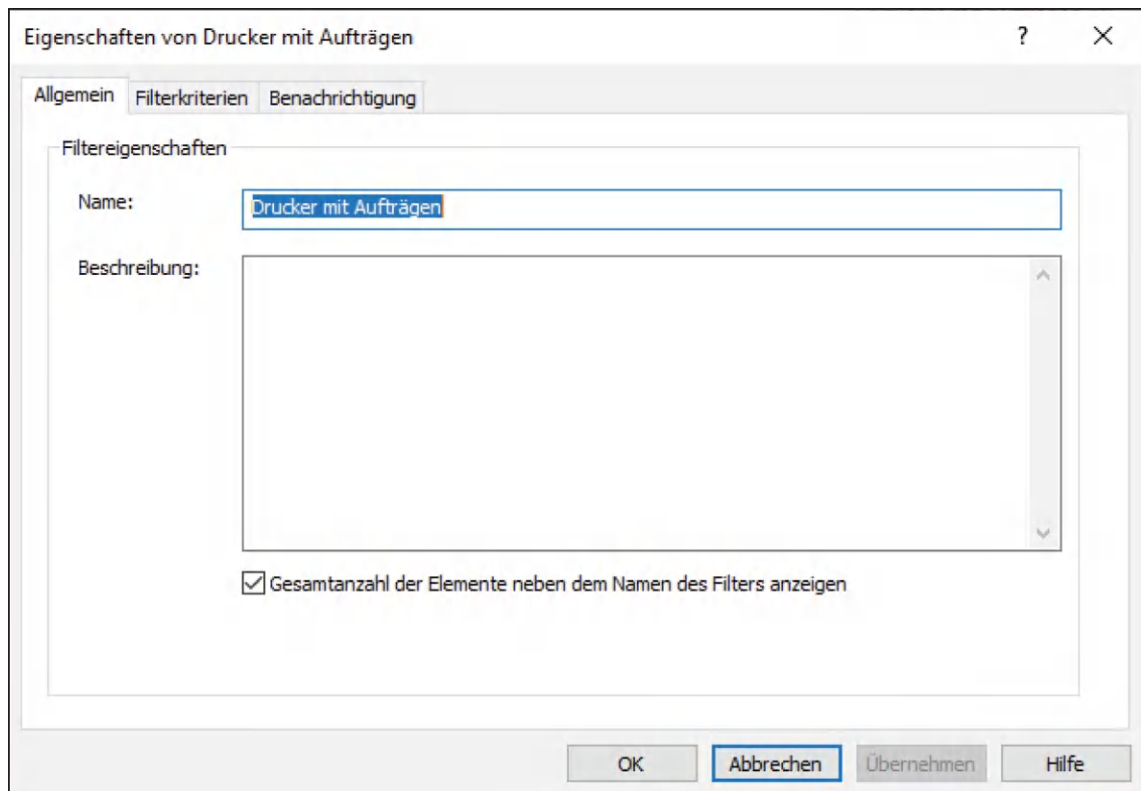


Abbildung 14.4: Bei Bedarf kann sich der Administrator die Gesamtzahl der Elemente eines Filters anzeigen lassen.

Auch die Erstellung eines eigenen Filters ist einfach möglich. Wenn Sie beispielsweise eine Aktion ausführen möchten oder eine E-Mail-Benachrichtigung erhalten wollen, wenn mehr als 25 Dokumente in einer Warteschlange auf Abarbeitung warten:

1. Mit einem Rechtsklick auf **BENUTZERDEFINIERTER FILTER** klicken.
2. Auswahl, ob es sich bei dem Filter um einen **DRUCKERFILTER** oder **TREIBERFILTER** handeln soll – in diesem Fall **DRUCKERFILTER**.
3. Benennen Sie den Filternamen – das ist der Name, der in der Baumstruktur zur Ansicht gebracht wird. Sie können eine Beschreibung eingeben und bei Bedarf die Gesamtzahl der Elemente in Klammern anzeigen lassen. Klicken Sie auf **WEITER**.

4. Im nächsten Dialogfenster ([Abbildung 14.5](#)) ASSISTENT FÜR NEUE DRUCKERFILTER haben Sie die Möglichkeit, sechs kombinierbare Filterkriterien anzugeben. In unserem Beispiel wählen wir im ersten Feld AUFTRÄGE IN WARTESCHLANGE, unter BEDINGUNG entscheiden wir uns für GRÖßER ODER GLEICH und als Wert setzen wir 25.

Assistent für neue Druckerfilter

Einen Filter definieren

Geben Sie Filterkriterien an. Die folgenden Kriterien werden gemeinsam angewendet, und nur Elemente, die allen Kriterien entsprechen, werden in der Druckverwaltungsstruktur im Ordner für die benutzerdefinierten Filter angezeigt.

Filterkriterien

Geben Sie zum Definieren des Filters das Feld, die Bedingung und den Wert in der ersten Zeile an. Fügen Sie weitere Zeilen hinzu, wenn Sie die Ergebnisse des Filters weiter eingrenzen möchten.

Feld	Bedingung	Wert
Aufträge in Warteschlange	größer oder gleich	25
Kein		
Kein		
Kein		
Kein		
Kein		

Alles löschen

< Zurück Weiter > Abbrechen Hilfe

Abbildung 14.5: Die Druckerverwaltung erlaubt die Anlage eigener Filter, die der Administrator mit Aktionen belegen kann.

5. Im dritten und letzten Abschnitt des Assistenten können Sie als Reaktion auf das Aktivwerden des Filters entweder eine E-Mail-Benachrichtigung versenden oder einen Skriptjob zur Ausführung bringen.

Drucker in der Druckerverwaltung

hinzufügen

Das Hinzufügen eines Druckers auf den Druckerserver ist ein sehr einfacher Vorgang. Typischerweise kann der Administrator einen Drucker über das Netzwerk über TCP/IP erreichen und den Drucker so einbinden. Wird der Drucker an einem Client-Computer betrieben, greift der Druckerserver über die Freigabe am PC auf den Drucker selbst zu – ein in der Praxis unerwünschtes Konzept, da der Drucker beim Ausschalten des Client-Computers nicht erreichbar ist.

Handelt es sich um einen Drucker, der an einem Linux/Unix-Computer angeschlossen ist, der selbst keine Windows/SMB-Freigaben anbietet, müssen Sie möglicherweise über einen LPR-Port die Verbindung herstellen.

Die Variante des LPR-Ports bietet sich auch für Umgebungen an, in denen ein Windows-Computer, an den der Drucker angeschlossen ist, nicht in einer Domäne mit Vertrauensstellung organisiert ist oder in überhaupt keiner Domäne betrieben wird. Auch diese Szenarien erfordern vom IT-Administrator und seinem Team eine besondere Aufmerksamkeit und sollten nur selten zum Einsatz kommen.

Normalerweise fügen Sie einen Drucker wie folgt hinzu:

1. Wechseln Sie in die DRUCKERVERWALTUNG.
2. Wählen Sie den zuständigen Druckerserver aus und klicken Sie auf den Eintrag DRUCKER in der Baumstruktur.
3. Klicken Sie mit der rechten Maustaste in das mittlere Fenster der MMC-Konsole und wählen Sie im Kontextmenü DRUCKER HINZUFÜGEN...
4. Wählen Sie im Netzwerkdruckerinstallations-Assistenten eine der vier Optionen – bei einem komplett neuen Drucker ist das häufig (b).
 - a. Das Netzwerk nach Druckern durchsuchen
 - b. Einen neuen TCP/IP- oder Webdienste-Drucker über IP-Adresse oder Hostnamen hinzufügen

- c. Neuen Drucker unter Verwendung eines vorhandenen Anschlusses hinzufügen
 - d. Neuen Anschluss erstellen und einen neuen Drucker hinzufügen
- 5. Sofern Sie die Option (b) wählen, geben Sie die IP-Adresse des Druckers ein. Der dazu passende Anschlussname wird üblicherweise selbst generiert, Sie können diesen bei Bedarf anpassen. Sofern Sie den Druckertreiber bereits installiert haben und ihn auswählen möchten, sollten Sie die Option ZU VERWENDENDEN DRUCKERTREIBER AUTOMATISCH ERMITTELN nicht aktivieren (siehe [Abbildung 14.6](#)) – das beschleunigt den Vorgang.
- 6. Die TCP/IP-Port-Erkennung versucht nun, den Drucker zu identifizieren. Bei netzwerkfähigen Druckern funktioniert dies in der Regel problemlos. Sollten Sie einen Drucker »vorbereiten« wollen, der aktuell nicht über die IP-Adresse erreichbar ist, wählen Sie im nächsten Dialogfenster den Gerätetyp STANDARD und den Eintrag GENERIC NETWORK CARD.
- 7. Im folgenden Dialogfenster können Sie einen neuen Treiber installieren oder einen bereits vorhandenen Treiber auswählen.

Netzwerkdruckerinstallations-Assistent

Druckeradresse
Sie können den Netzwerknamen des Druckers oder seine IP-Adresse eingeben.

Gerätetyp: TCP/IP-Gerät

Hostname oder IP-Adresse: 192.168.178.252

Anschlussname: 192.168.178.252

☐ Zu verwendenden Druckertreiber automatisch ermitteln

< Zurück Weiter > Abbrechen

Abbildung 14.6: Wenn es schnell gehen soll: Ohne Druckertreiberidentifikation geht das Einrichten eines neuen Druckers schneller vonstatten.

8. Sofern Sie sich für die Neuinstallation eines Druckerstreibers entschieden haben, erscheint das Auswahlfenster (siehe [Abbildung 14.7](#)) mit den bisher installierten Druckertreibern und der Möglichkeit, über DATENTRÄGER oder dem WINDOWS UPDATE neue Treiber einzufügen.

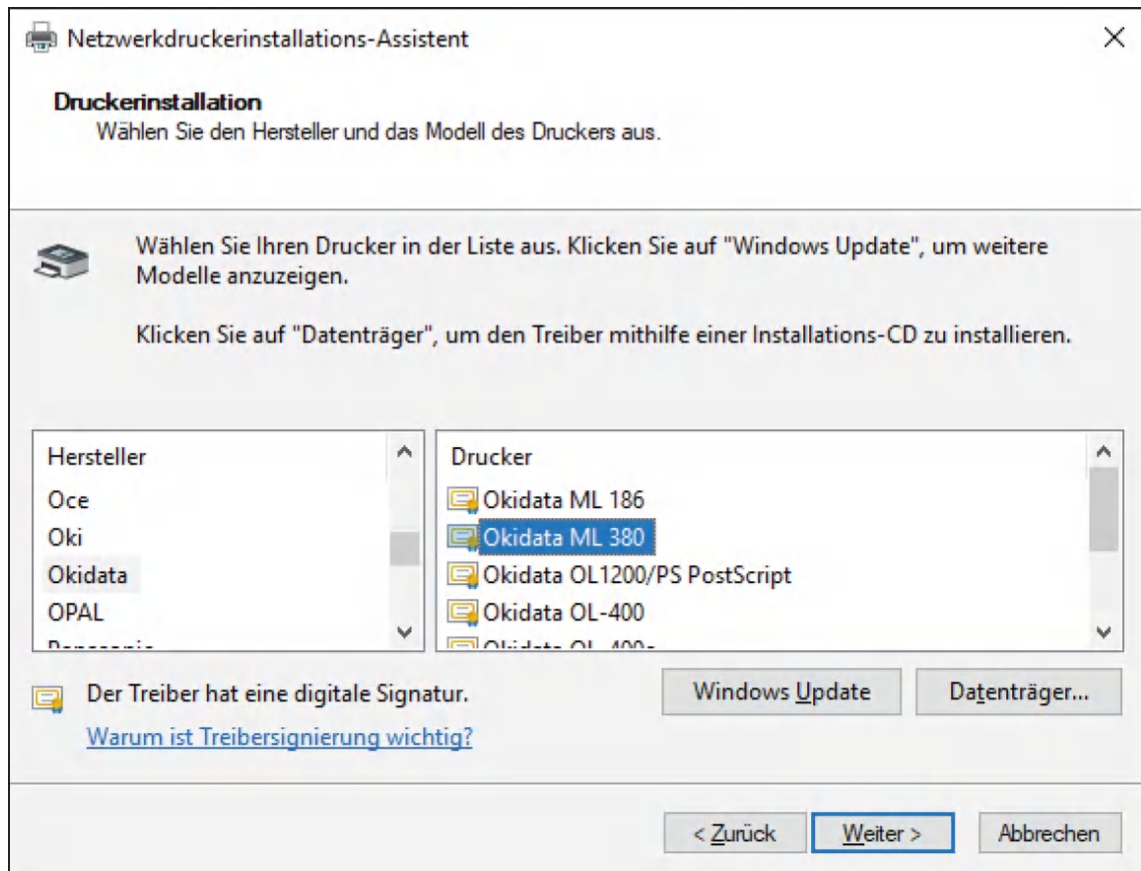


Abbildung 14.7: Druckertreiber lädt der Administrator über das »Windows Update« bei Bedarf herunter.

Die jüngeren Versionen von Windows Server verzichten darauf, alle erdenklichen Treiber schon bei der Installation einzurichten. Die Treiber stellt Microsoft noch immer für die Mehrzahl aller Geräte zur Verfügung, jedoch muss der Administrator diese bei Bedarf über das WINDOWS UPDATE herunterladen.

9. Mit der abschließenden Bestätigung beendet der Assistent seine Arbeit und installiert den Drucker.

Der Drucker ist nun auf dem Druckerserver eingerichtet und könnte von einem Client-Computer aus angesprochen werden – sofern der Administrator eine Freigabe eingerichtet hat. Die Sichtbarkeit eines freigegeben Druckers hat unter Windows leider nichts mit der Nutzbarkeit zu tun. Ein einfacher Weg, um festzustellen, welche Drucker ein Druckerserver zur Verfügung stellt, besteht darin, auf einem Client-Computer den Namen des Druckerservers als UNC-Pfad zu öffnen:

\\{NAME DRUCKER SERVER}

Benutzer sind in der Lage, durch den Befehl VERBINDEN im Kontextmenü den Drucker einzurichten. Sofern ein ordentlich signierter, paketfähiger Treiber vorliegt, geschieht die Installation des Treibers automatisch. Ein Treiber, der beispielsweise die Remote-Druck-Funktion des Herstellers verwendet und darüber eine benutzerspezifische Verwendung einer Internet-Druckerschlange nutzt, wird bei der Installation aller Wahrscheinlichkeit nach abbrechen.

Die Sicherheitseinstellungen basieren auf demselben Schema wie bei den Dokumentenfreigaben. Im Zweifelsfall gilt »Verweigern« stets höher als »Zulassen«. Es gelten folgende Möglichkeiten:

- ✓ DRUCKEN – Der Benutzer kann eine Verbindung mit einem Drucker herstellen und Dokumente ausdrucken. Standardmäßig ist die Berechtigung DRUCKEN allen Mitgliedern der Gruppe JEDER zugewiesen.
- ✓ DRUCKER VERWALTEN – Der Benutzer verfügt über die Berechtigung DRUCKEN und zudem über die volle administrative Kontrolle über den Drucker. Er kann den Drucker anhalten und neu starten, die Spooler-Einstellungen ändern, einen Drucker freigeben, die Druckerberechtigungen einstellen und die Eigenschaften des Druckers selbst ändern.
- ✓ DOKUMENTE VERWALTEN – Der Benutzer kann den Ausdruck von Dokumenten, die von anderen Benutzern an den Drucker gesendet wurden, unterbrechen, fortsetzen, neu starten und abbrechen sowie die Reihenfolge dieser Dokumente ändern. Der Benutzer kann jedoch weder Dokumente an den Drucker senden noch den Druckstatus steuern.

Standardmäßig ist die Berechtigung DOKUMENTE VERWALTEN den Mitgliedern der Sondergruppe ERSTELLER-BESITZER zugewiesen, damit Benutzer ihre eigenen Druckaufträge verwalten können.

Wenn einem Benutzer die Berechtigung DOKUMENTE VERWALTEN zugewiesen wird, kann er nicht auf Dokumente

zugreifen, die zu diesem Zeitpunkt in der Warteschlange stehen. Die Berechtigung gilt nur für Dokumente, die nach Zuweisung der Berechtigung an den Drucker gesendet werden.

- ✓ **SPEZIELLE BERECHTIGUNGEN** – Für Drucker gibt es nur sechs spezielle Berechtigungen. Neben den Standardberechtigungen sind dies Berechtigung Lesen, Berechtigungen ändern und Besitz übernehmen.



Standardmäßig haben Mitglieder der Gruppen »Administratoren« und »Hauptbenutzer« Vollzugriff auf Drucker. Sprich, diesen Benutzern sind die Berechtigungen Drucken, Dokumente verwalten und Drucker verwalten zugewiesen.



Sofern von einem Arbeitsplatz ein Drucker nur dann verwendet wird, wenn dieser Arbeitsplatz auch wirklich von einem Benutzer genutzt wird, kann der Administrator einem lokalen Anschluss über den USB-Port zustimmen. Gleichzeitig verbaut sich der Administrator jedoch die Möglichkeit auf dieses Gerät von außen administrativ zugreifen zu können, um beispielsweise Firmware-Updates einzuspielen. Weboberflächen der Drucker geben Auskunft über die bereits gedruckte Anzahl von Seiten, führen Buch über die letzten Druckaufträge oder visualisieren den Tonerstand. Wird der Drucker mit den passenden SNMP-Informationen ausgestattet, senden viele Geräte bei verschiedensten Zuständen, die vom Normalbetrieb abweichen, die dazu passende Nachricht aus. Ist in der Netzwerkumgebung keine SNMP-Überwachung aktiv, so bieten glücklicherweise viele Drucker die Nutzung von E-Mails zur Benachrichtigung.

Die Einbindung von Druckern in eine WLAN-Umgebung ist grundsätzlich bei vielen Geräten möglich und dürfte im SOHO-Bereich eine akzeptable Bereitstellungsform darstellen. In der Regel sind Drucker nicht gleichzeitig in der Lage, über beide Netzwerk-Interfaces zu arbeiten: Ethernet oder WLAN. In Umgebungen mit

Print-Servern sollten Sie den Drucker per Ethernet ansteuern und den Client-Computern den Zugriff über das WiFi-Netzwerk ermöglichen.

Müssen Sie ältere Drucksysteme per LAN ansteuern, sind sogenannte Printer-Boxen äußerst hilfreich. Der in Bielefeld ansässige Speziallösungshersteller SEH bietet eine umfangreiche Palette an verschiedenen Printer-Boxen an. In den größeren Geräten von SEH ist zudem die am Markt verbreitete ThinPrint-Technologie implementiert, die die Geschwindigkeit des Ausdrucks, besonders in WAN-Umgebungen, beschleunigen kann.

Drucker bereitstellen

Die manuelle Einbindung von Druckern in die Benutzerumgebung dürfte bereits in einer Umgebung mit mehr weniger zehn Benutzern äußerst unattraktiv sein. Machbar? – Ja! – Schön? – Nein – weil viel händischer Aufwand.

An dieser Stelle sei auf die Firmen Google und Apple hingewiesen, die für ihre Cloud-Dienste eigene Techniken auf den Weg gebracht haben.

Google und Apple haben in der jüngeren Vergangenheit ganz eigene Drucksysteme für das Cloud-Zeitalter etabliert. Diese Druckwege entziehen sich gänzlich der Ordnung durch die IT-Administratoren und zeigen einmal mehr, wie wichtig es ist, Android- und iOS-Endgeräte zu verwalten. Da sich Techniken wie »Google Cloud Print« (GCP) aber auch auf Windows-Computer nutzen lassen, sollten Sie hier besonders achtsam sein.

GCP-fähige Drucker – das sind beinahe alle modernen Geräte – verfügen über eine integrierte Client-Software, die den Drucker direkt mit der Druckerwarteschlange auf den Google-Servern verbindet. Insgesamt sprechen für die von Google aufgebaute Plattform ihre einfache Handhabung und die universelle Einsetzbarkeit. Trotz der vielen Anwendungs- und Einstellungsmöglichkeiten ist der Dienst kostenlos. Da es jedoch bei der Verknüpfung von Drucker, Google-Benutzerkonto und der Warteschlange zu einer dauerhaften Verbindung kommt, sollten sich Nutzer von sensiblen Ausdrucken gut überlegen, ob dies ein geeigneter

Weg für derlei Dokumente ist. Von der Abhängigkeit der Verfügbarkeit des Google-Diensts und der Herausforderung der DSGVO ganz zu schweigen.

Die Zeiten, in denen Apple-Druckdienste quasi synonym für PostScript standen, sind schon lang vorbei. Auch wenn Macs wohl nach wie vor das Segment Layout und Druckvorstufe beherrschen, haben die Entwickler im US-kalifornischen Cupertino eine leistungsfähige, gemeinsame Basis für ihre OS X- und IOS-Geräte geschaffen: »AirPrint«.

Die wichtigste Design-Anforderung haben die Entwickler dabei perfekt umgesetzt: Einfachheit. Wie Google, so versucht auch Apple die Hersteller zur Umsetzung einer direkten Software-Integration auf Druckern oder Multifunktionsgeräten einzustimmen. Und das gelingt dem Konzern äußerst gut, denn alle bekannten Hersteller von Brother, Hewlett Packard, Kyocera, Oki, Samsung oder Xerox sind auf der Kompatibilitätsliste und im Apple Store zu finden.

Trotz gewisser Ähnlichkeiten in der Einbindung unterscheiden sich die Plattformen von Google und Apple jedoch grundlegend. AirPrint-kompatible Drucker und die druckenden Client-Systeme müssen sich innerhalb desselben Netzwerk- oder WLAN-Bereichs befinden. Eine internetbasierte Druckerwarteschlange gibt es bei Apple nicht. Grundlage der Kommunikation ist das nicht Routing-fähige Layer-2-Protokoll »Bonjour«.

Soll der Zugriff über mehrere Netzwerksegmente hinweg möglich sein, muss ein Administrator zwangsläufig ein »Bonjour-Gateway« vorhalten. Ein kleines Zusatzprogramm mit Namen »Airprint Activator für Windows« ermöglicht auch Windows-Benutzern nicht-AirPrint-fähige Drucker bereitzustellen. Hierzu sind die Installation des Bonjour-Protokolls, die Aktivierung des Gast-Accounts und die Freischaltung von drei TCP-Ports erforderlich.

Grundsätzlich bieten sich dem Administrator verschiedene Möglichkeiten der Bereitstellung:

- ✓ Manuelle Einbindung der Freigabe im Benutzerkontext – Hoher Aufwand und stets vom angemeldeten Benutzer abhängig.

- ✓ Einbindung per net use im Anmelde-Skript – Funktioniert automatisch, ist aber nicht mehr ganz modern.

Alle gängigen Windows-Versionen unterstützen Gruppenrichtlinien, die wiederum eine viel feinere Zuordnung erlauben:

- ✓ Einbindung als benutzerspezifische Gruppenrichtlinie.
- ✓ Einbindung als computerspezifische Gruppenrichtlinie.

Moderne Administratoren nutzen in einer Active-Directory-Umgebung ausschließlich die Bereitstellung per Gruppenrichtlinien. Dies geschieht entweder über die Gruppenrichtlinienverwaltung mit einer Zielgruppenadressierung oder direkt aus dem Dialogfenster der Druckerverwaltung. Weitere Informationen finden Sie im [Kapitel 16](#) Gruppenrichtlinien.

Drucker im- und exportieren

Die Druckverwaltung von Windows erlaubt eine recht komfortable Lösung, um die kompletten Druckerobjekte von einem Server auf einen anderen Server zu übertragen. Bei diesem Vorgang bleiben sämtliche Freigaben und Treiber erhalten. Über diese Technik hat der Administrator die Möglichkeit, einen neuen Druckerserver vorzubereiten, ohne dass hierbei der bisher aktive Server beeinträchtigt wird.

Zunächst wird auf dem bisherigen Druckerserver ein Export durchgeführt:

1. Öffnen Sie die Druckerverwaltung.
2. Auswahl des gewünschten Druckerservers durch einen Rechtsklick.
3. Auswahl des Befehls DRUCKER IN DATEI EXPORTIEREN... im Kontextmenü.
4. Bestätigung Sie die Objektliste (auf die der Anwender ohnehin keinen Einfluss hat) durch einen Klick auf WEITER.
5. Festlegung des Namens für die Exportdatei im speziellen .printerExport-Format.

Die resultierende Export-Datei für die Migration kann mehrere Hundert MByte groß werden, da auch die Druckertreiber enthalten sind. Der Importvorgang auf dem neuen Server verläuft ähnlich.

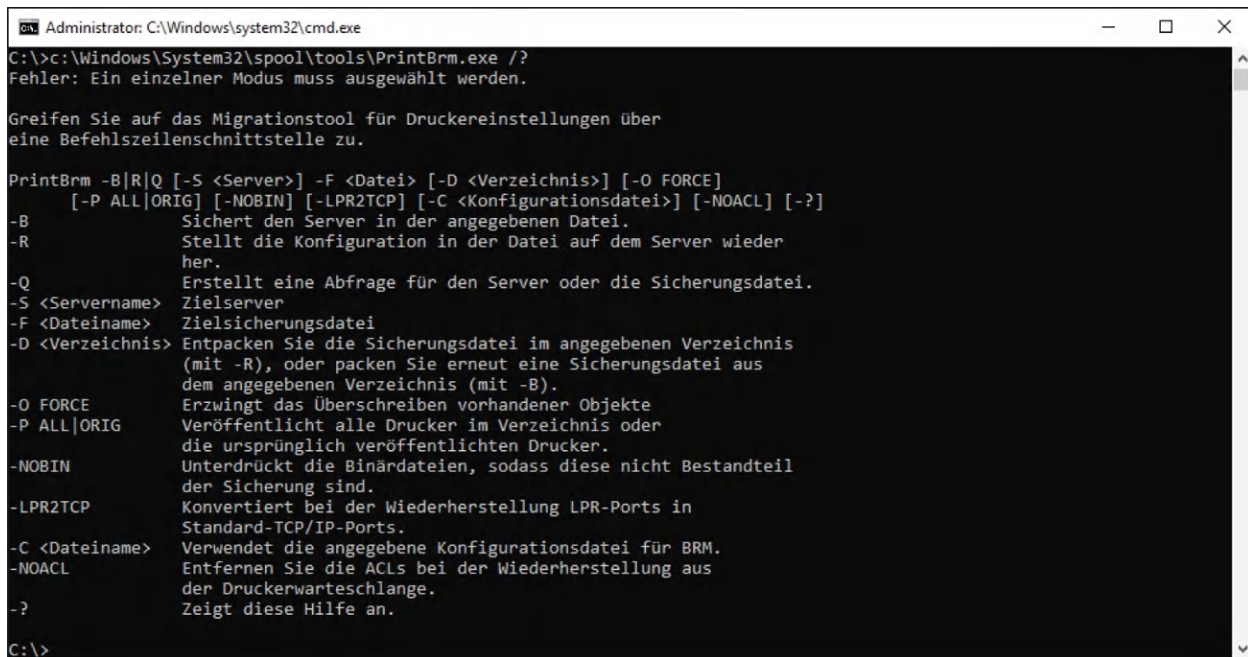
Beim Import hat der Administrator leider ebenfalls keine Möglichkeit, bestimmte Drucker aus der Migrationsdatei auszuschließen. Die Einflussnahme des IT-Profis reduziert sich auf wenige Fragen:

- ✓ LPR-Anschlüsse zu Standardanschlussmonitoren konvertieren.
- ✓ Bisherige Drucker beibehalten oder löschen.
- ✓ Neu übernommene Drucker im Active Directory auflisten oder nicht.



Nur um es noch einmal klarzustellen: Der Import der Drucker heißt nicht, dass diese bereitgestellten Drucker auf dem neuen Druckerserver vom Client angesprochen werden können. Ohne Anpassung der Zuweisung, beispielsweise durch eine Gruppenrichtlinie, nutzen alle Clients nach wie vor den vorherigen Druckerserver.

Grundsätzlich erlaubt der Export auch den Batch-Betrieb über den PrintBrm.exe-Befehl ([Abbildung 14.8](#)), somit können Administratoren ihre Druckerkonfiguration in dem Migrationsformat regelmäßig sichern und diese im Notfall schnell wiederherzustellen.



```
Administrator: C:\Windows\system32\cmd.exe
C:\>c:\Windows\System32\spool\tools\PrintBrm.exe /?
Fehler: Ein einzelner Modus muss ausgewählt werden.

Greifen Sie auf das Migrationstool für Druckereinstellungen über
eine Befehlszeilenschnittstelle zu.

PrintBrm -B|R|Q [-S <Server>] -F <Datei> [-D <Verzeichnis>] [-O FORCE]
          [-P ALL|ORIG] [-NOBIN] [-LPR2TCP] [-C <Konfigurationsdatei>] [-NOACL] [-?]
-B          Sichert den Server in der angegebenen Datei.
-R          Stellt die Konfiguration in der Datei auf dem Server wieder
          her.
-Q          Erstellt eine Abfrage für den Server oder die Sicherungsdatei.
-S <Servername> Zielsever
-F <Dateiname> Zielsicherungsdatei
-D <Verzeichnis> Entpacken Sie die Sicherungsdatei im angegebenen Verzeichnis
          (mit -R), oder packen Sie erneut eine Sicherungsdatei aus
          dem angegebenen Verzeichnis (mit -B).
-O FORCE     Erzwingt das Überschreiben vorhandener Objekte
-P ALL|ORIG Veröffentlicht alle Drucker im Verzeichnis oder
          die ursprünglich veröffentlichten Drucker.
-NOBIN      Unterdrückt die Binärdateien, sodass diese nicht Bestandteil
          der Sicherung sind.
-LPR2TCP    Konvertiert bei der Wiederherstellung LPR-Ports in
          Standard-TCP/IP-Ports.
-C <Dateiname> Verwendet die angegebene Konfigurationsdatei für BRM.
-NOACL      Entfernen Sie die ACLs bei der Wiederherstellung aus
          der Druckerwarteschlange.
-?          Zeigt diese Hilfe an.

C:\>
```

Abbildung 14.8: Das Kommandozeilentool »PrintBrm.exe« ist beim Umzug oder zur Sicherung von Druckerservern hilfreich.

Das Kommando für die Eingabeaufforderung könnte lauten:

```
c:\Windows\System32\spool\tools\PrintBrm.exe -B -S {FQDN} -F
c:\temp\printer%date%.printerexport
```

Die Option -B sorgt für eine Sicherung, die Option -S benennt den Namen des Druckerservers und kann beim lokalen Aufruf entfallen. Die Option -F benennt die Zieldatei.

Druckaufträge im Spooler ansehen

Mitunter landen über die Zeit doch einige Druckaufträge in den Druckerwarteschlangen der Druckerserver. Administratoren schmeißen die »Altlasten« irgendwann raus, sofern Sie keine besonderen Gründe haben, es nicht zu tun. Nicht wenige Administratoren nutzen das »Hängenbleiben« in den Druckerwarteschlangen, um zu prüfen, ob Umstellungen auf neue Drucker erfolgreich waren – aber das ist eine ganz eigene Vorgehensweise.

Das Betriebssystem Windows stellt leider keine direkte Möglichkeit zur Verfügung, einen Blick in diese Dokumente zu werfen. Ein kleines

Zusatzprogramm, auch als Freeware erhältlich, von Entwickler Dieter Riekert mit Namen »SPL Viewer« schafft Abhilfe.



Sie finden die Freeware »SPL Viewer« auf verschiedenen Portalen für Freeware.

Das Programm wird mit der Dateinamen-Erweiterung .SPL verknüpft und ermöglicht so einen Blick in das Spooler-Verzeichnis, das auf den Windows-Systemen unter dem Pfad `%windir%\system32\spool\printers` zu finden ist.

Die deutschsprachige Freeware ist ein schnell installiertes, einfaches Programm, das dem Nutzer einen besseren Zugriff auf die Druckaufträge in der Warteschlange zur Verfügung stellt. Einzelne Seiten aus der Warteschlange können bequem in andere Programme übernommen werden.

Die Software wird zwar auf der Webseite als »ohne Einschränkungen« dargestellt, ist aber in dieser freien Version auf 300 Seiten pro EMF-Dokument sowie 50 MByte pro RAW-Datei beschränkt. Das Programm benötigt zur ordnungsgemäßen Darstellung auf modernen Windows-Systemen zwingend den Aufruf mit Administratorrechten.

Line Printer Daemon und Line Printer Remote

Die alten Unix-Drucktechniken LPD und LPR sind von Microsoft »angezählt« und sollen, so der Hersteller aus Redmond, zu einem noch nicht näher bekannten Zeitpunkt in der Zukunft aus dem Produkt entnommen werden.

Der Hinweis, dass es sich um eine »deprecation« handelt, wurde bereits 2012 veröffentlicht. Seither sind die Unix-Druckdienste jedoch noch immer vorhanden, und es gibt seither keine weiteren Nachfragen oder Hinweise zu dem Thema bis auf die Aussage von Alan Morris aus dem »Windows Printing Team«, dass die Entfernung nicht durch ein Service-

Pack geschehen wird, sondern mit dem Erscheinen einer neuen, vollen Version von Windows.

Die Verwendung der Unix-Druckdienste ist für einige speziellere Szenarien nicht uninteressant. Insbesondere wenn Sie als Administrator komplett außerhalb jeglicher Domänenstrukturen arbeiten, sind LPD-Druckdienst und LPR-Anschlussmonitor hilfreiche Kandidaten:

- ✓ LPD-Druckdienst – Ermöglicht die Verwendung des Windows-Computers als Line Printer Daemon (LPD) und Remote Line Printer Client.
- ✓ LPR-Anschlussmonitor – Ermöglicht Clients das Drucken auf TCP/IP-Druckern, die an einem Unix-/VAX-Server angeschlossen sind.

Der komplette Druckvorgang beschränkt sich, gemäß RFC 1179, auf den Port 515. Sofern dieser Port in beiden Richtungen durchgängig ist, reicht die Kenntnis der Warteschlangenbezeichnung (Freigabename) und der IP-Adresse, um einen entfernten Drucker über einen »lokalen LPR-Port« anzusprechen.



Erwarten Sie keinerlei »mitdenkende Unterstützung«, sofern Sie LPR verwenden. Den richtigen Druckertreiber müssen Sie auf allen beteiligten Maschinen manuell installieren!

Bei der Verwendung von LPR als Drucktechnik muss jedem IT-Profi klar sein, dass es sich um einen äußerst ungeschützten Datenstrom handelt. Um es ganz schlicht auf den Punkt zu bringen:



Kennt sich jemand mit Programmen wie »WireShark« aus, ist er in der Lage, den kompletten Druckstrom eines LPR-Drucks mitzuschneiden und wieder in eine Druckerspooler-Datei zu verwandeln. Anleitung dafür findet jeder, der sich dafür interessiert, im Internet.

Von den Sicherheitsgedanken und dem möglicherweise drohenden Ende von LPR unter Windows einmal abgesehen, ist die »veraltete« Umsetzung

äußert praktisch. Schon mit einem Einzeiler auf der Eingabeaufforderung wird ein Protokoll ausgedruckt – ganz ohne Schnörkel, wie in [Abbildung 14.9](#) zu sehen.

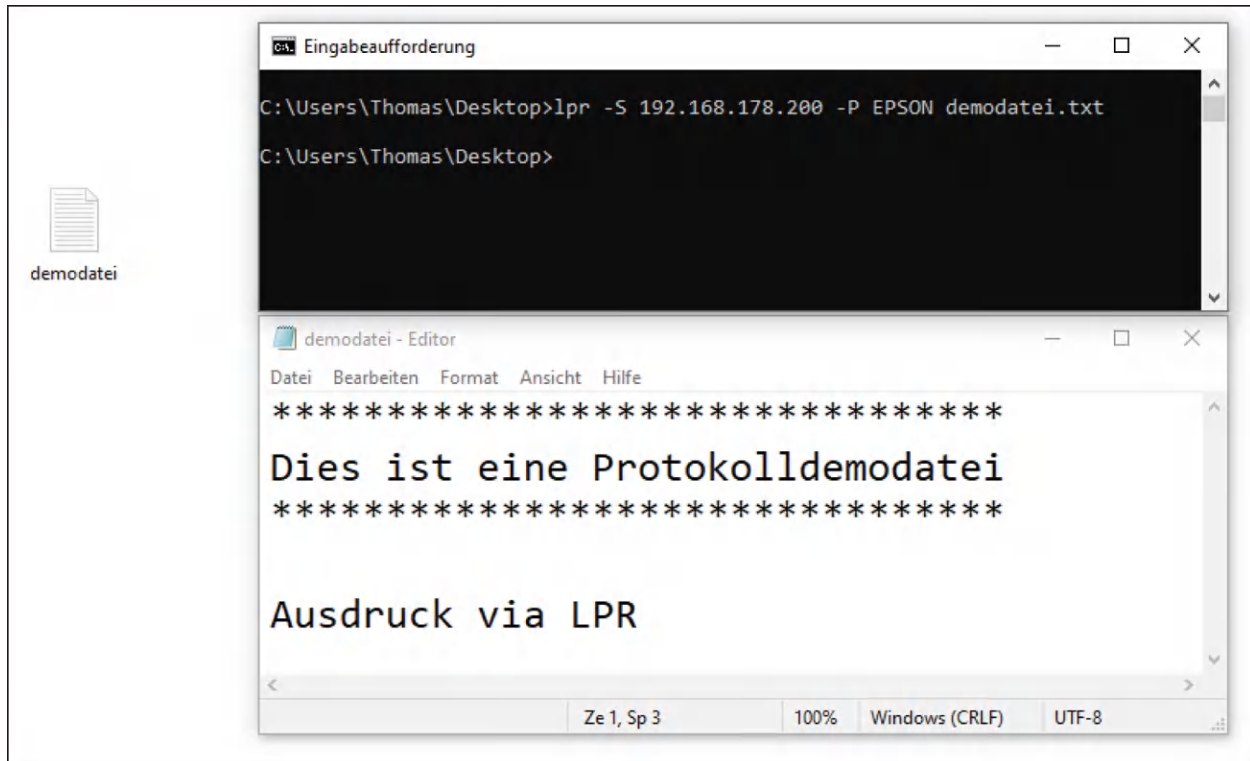


Abbildung 14.9: Altmodisch, unsicher – aber praktisch: der LPR-Druck

Druckertreiberisolation

Erstmals mit Windows 7/2008R2 stellte Microsoft die sogenannte Windows-Treiberisolation vor. Diese Funktion entfernt einen isolierten Treiber vom allgemeinen Druckerspooler-Prozess. Ein isolierter Druckertreiber arbeitet stattdessen in einem eigenen Prozessraum – typischerweise als Sandbox benannt.



In einer klassischen Büroumgebung muss sich der Administrator nicht mit dem Thema der Druckertreiberisolation auseinandersetzen. Bei Installationen mit Massendruck – beispielsweise für das Erzeugen von Produkt-Labels – kann der Einsatz dieser Technik allerdings für mehr Stabilität sorgen.

Kommt es im Zusammenhang mit einem isoliert arbeitenden Treiber zu einem Fehler, Absturz oder zu einer unerwarteten Beendigung des Druckerspools-Prozesses, wird dies keine Auswirkungen auf die anderen Drucker haben.

Ob ein Treiber diese Funktionalität grundsätzlich unterstützt, erkennt der Administrator anhand eines Schlüsselworts in der INF-Datei:

- ✓ DriverIsolation = 2 – Dieser Treiber unterstützt die Isolation.
- ✓ DriverIsolation = 0 – Dieser Treiber unterstützt die Technik nicht.

Der Wert 1 besagt, dass eine gemeinsame »Sandbox« für alle Drucker zum Einsatz kommt, ohne die gesicherte Isolation.

In der Druckerverwaltung kann der Administrator im Kontextmenü festlegen, ob der Treiber isoliert arbeiten soll oder nicht, siehe [Abbildung 14.10](#).

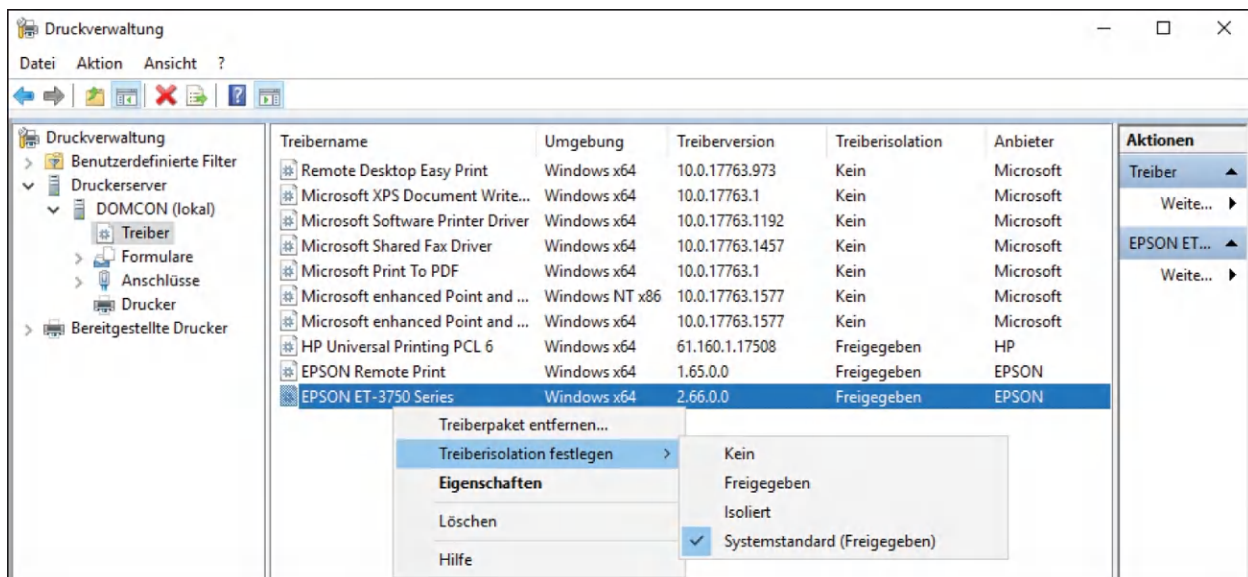


Abbildung 14.10: Den Betriebsmodus der Treiberisolation legt der Administrator pro Treiber fest.

Es existierten drei mögliche Optionen:

- ✓ Freigegeben – Der Treiber wird gemeinsam mit anderen Druckertreibern in einem gemeinsamen Prozess, unabhängig vom Spooler, ausgeführt.

- ✓ Isoliert – Windows betreibt den Treiber in einem eigenen Prozess, unabhängig vom Spooler und nicht gemeinsam mit anderen Druckertreibern.
- ✓ Keine – Der Treiber wird im Spooler-Prozess ausgeführt.

Internetdrucken

Allein schon die Bezeichnung dieses Features führt zunächst ein wenig in die Irre, da es nicht notwendigerweise um das Drucken über das Internet geht, sondern das Drucken über das Protokoll http, das nicht nur im Internet zum Einsatz kommen kann.

Mit der seit Windows Server 2008 R2 verfügbaren Intranet-Seite haben Benutzer und Administratoren die Möglichkeit, Druckaufträge über eine Webseite direkt zu verwalten. Sofern auf dem Druckerserver Internetdrucken als Feature aktiv und auch auf dem Windows-Client-Computer die Windows-Features des Internetdruckclients installiert sind, kann der Benutzer den Drucker über http einbinden.

Die Installation des Features geschieht über den Server-Manager, wie in [Abbildung 14.11](#) zu sehen.

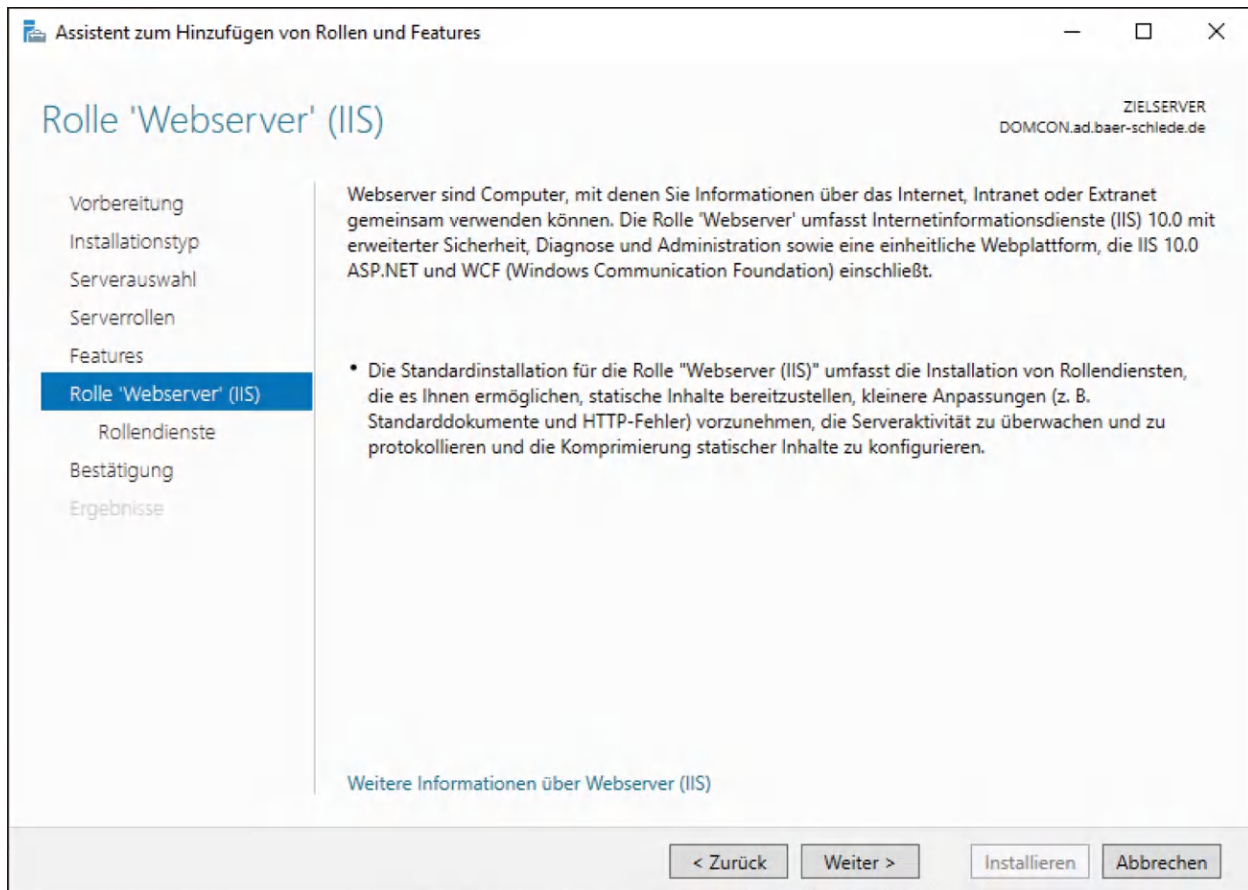


Abbildung 14.11: Um Internetdruck auf dem Server zu nutzen, ist die gleichzeitige Installation des Webservers IIS erforderlich.

Da der Internetdruck vom Vorhandensein eines Webservers abhängig ist, installiert der Server bei Bedarf den IIS mit. Für den Administrator gibt es in diesem Zusammenhang nicht viel zu konfigurieren – das übernimmt der Installer selbst.

Die Webseite des Internetdrucks ([Abbildung 14.12](#)) ist standardmäßig unter

`http://Servername/printers`

zu erreichen. Benutzer bekommen nur die Druckerobjekte angezeigt, auf die sie über die Sicherheitseinstellungen auch Zugriff haben. Auf der Webseite hat der Benutzer die Möglichkeit, den Drucker anzuhalten, Druckaufträge fortzusetzen oder Druckaufträge zu löschen.

GENERICPCL6 auf domcon

Druckerwarteschlange: **Angehalten** Wartezeit: Unbekannt
 Ausstehende Dokumente: 2 Durchschnittliche Größe: 1 Seite(n)

ANSICHT

- [Dokumentliste](#)
- [Eigenschaften](#)
- [Alle Drucker](#)

Dokument	Status	Besitzer	Seiten	Größe	Gesendet
☐ Dokument drucken		administrator	1	146,5 KB	13:51:46 09.01.2021
☐ Dokument drucken		administrator	1	146,5 KB	13:51:48 09.01.2021

DRUCKERVORGÄNGE

- [Anhalten](#)
- [Fortsetzen](#)
- [Alle Druckaufträge abbrechen](#)

DOKUMENTAKTIONEN

- [Anhalten](#)
- [Fortsetzen](#)
- [Abbrechen](#)

Abbildung 14.12: Die Verwaltungsseite für Druckaufträge

Eine Funktion zur Einrichtung eines Druckers für den eigenen Client-Computer sucht der Anwender mit einem modernen Browser an dieser Stelle vergebens. Nur wer sich mit dem Internet Explorer (nicht Edge – wirklich der IE!) auf die Intranetseite bewegt, wird unter **DRUCKERVORGÄNGE** den Befehl **VERBINDEN** finden. Ohne den Schritt über den IE bleibt die Nutzung von HTTP im **DIALOG DRUCKER & SCANNER HINZUFÜGEN**.



Um über http drucken zu können, muss auf dem Windows-Client unter **FEATURES** der **INTERNETDRUCKCLIENT** installiert sein ([Abbildung 14.13](#)). Technisch betrachtet erfolgt das Drucken über das Internet Print Protocol (IPP), das in http (Hypertext Transfer Protocol) gekapselt ist.

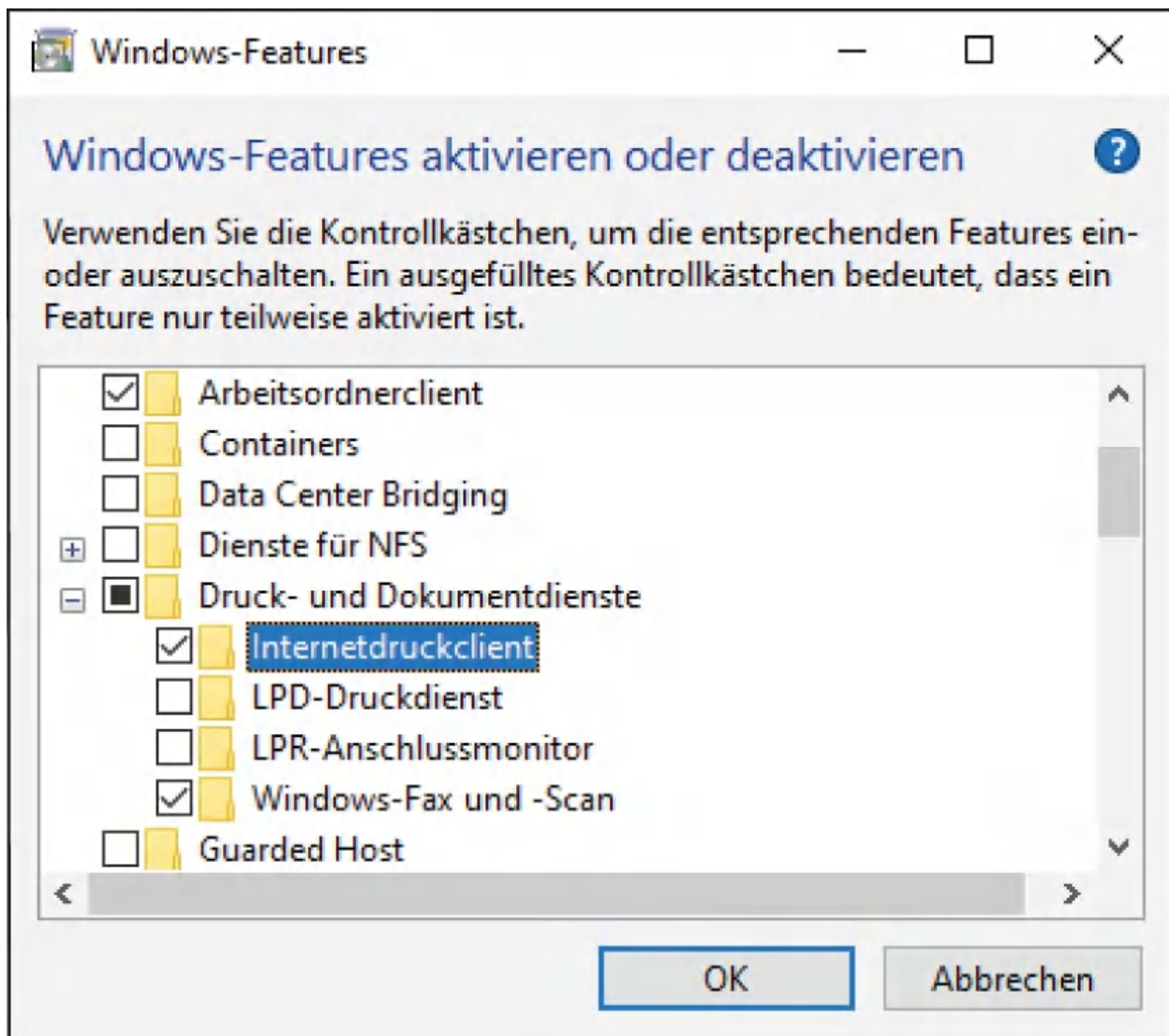


Abbildung 14.13: Der Client für den Internetdruck auf einem Windows-10-PC

Teil III

Windows-Server im Einsatz



IN DIESEM TEIL ...

- ✓ Wie kommen Server (und Clients) in die Domäne? (Domain-Join)
- ✓ Gruppenrichtlinien – was sind sie und was kann man damit machen?
- ✓ Überwachen des Betriebs: Server-Manager, Admin Center, Ereignisanzeige
- ✓ Windows-Server-Updates
- ✓ Backup für Ihren Server
- ✓ Ausfälle vermeiden und Troubleshooting

Kapitel 15

Domänen-Beitritt

IN DIESEM KAPITEL

Windows Server als Teil einer Domäne
Vorbedingungen für den Domänen-Beitritt
Einbinden in die Domäne
Offline einer Domäne beitreten

Wenn Sie Ihren Windows Server als Stand-alone-Gerät betreiben, so werden Sie ihn wahrscheinlich als Mitglied einer »Workgroup« eingerichtet haben, denn das ist die Standardeinstellung bei der Installation. Natürlich können Sie dem Server auch gleich die Rolle als Domänen-Server zugewiesen haben. In vielen Fällen wird es aber so sein, dass Sie den Server innerhalb eines Netzwerks betreiben, in dem schon ein Domänen-Server vorhanden ist, und da ist es sicher sinnvoll, dass auch Ihr neu aufgesetzter Server Teil dieser Windows-Domäne wird. Das ist sehr schnell erledigt, wenn Sie ein paar Vorbedingungen beachten.

Vorbedingungen für den Domänen-Beitritt

Bevor Ihr Server der bestehenden Domäne hinzugefügt werden kann, sollten Sie die folgenden Dinge überprüfen und gegebenenfalls entsprechend ändern:

- ✓ Der Server besitzt einen eindeutigen Namen.
- ✓ Der Server befindet sich im gleichen Netzwerk wie der Domänencontroller.

- ✓ Ganz wichtig: Die DNS-Einstellungen des Servers müssen so konfiguriert sein, dass der Domänen-Server als DNS-Server konfiguriert ist.
- ✓ Ein Nutzerkonto mit den entsprechenden Zugriffsrechten, um mit einem Server der Domäne beizutreten.

Wir wollen für dieses Kapitel unsere Testversion des Windows Server 2022, die in einer virtuellen Maschine betrieben wird, zu unserer Domäne hinzufügen. Der Domänencontroller ist ein Windows Server 2019 in der Standardversion, der ebenfalls virtualisiert ist. Um die Einstellungen des »Beitrittskandidaten« zu prüfen, können Sie beispielsweise den Server-Manager auf diesem System starten und dort vom DASHBOARD zum Eintrag LOKALER SERVER wechseln ([Abbildung 15.1](#)).

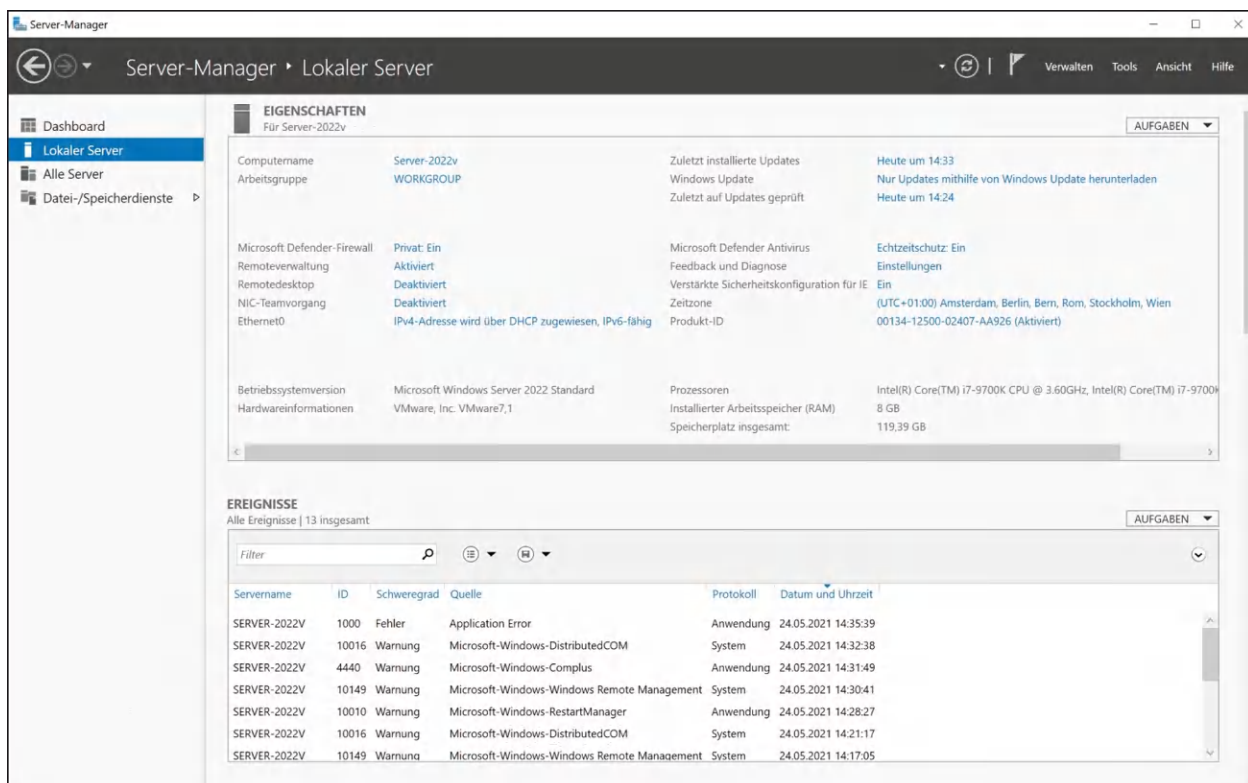


Abbildung 15.1: Vor dem Beitritt zur Domäne: Der Server besitzt bereits einen eindeutigen Namen, ist aber noch Mitglied der Workgroup.

Wenn Sie sich nicht sicher sind, ob sich Ihr Domänencontroller im gleichen Netzwerk wie Ihr neuer Server befindet, kann es manchmal hilfreich sein, dies durch ein einfaches Ping-Kommando zu bestätigen

([Abbildung 15.2](#)). Wir haben in diesem Beispiel das Kommandozeilen-Programm in der Eingabeaufforderung mit der Option -4 aufgerufen, damit die Anzeige der IP-Adresse im IPv4-Format erfolgt. Standardmäßig gibt dieser Befehl die Adresse ansonsten im IPv6-Format aus. Dadurch, dass wir hier den Namen unseres Domänencontrollers verwenden, können wir auch gleich feststellen, ob die Namensauflösung via DNS richtig funktioniert. Das kann allerdings nur dann funktionieren, wenn Sie auch den »richtigen« DNS-Server konfiguriert haben. An dieser Stelle zeigt sich ein weiteres Mal, wie eng Active Directory und DNS miteinander verknüpft sind. Deshalb werden wir im nächsten Schritt die Netzwerkeinstellungen auf unserem lokalen Server entsprechend ändern.

1. Öffnen Sie in den WINDOWS-EINSTELLUNGEN den Bereich NETZWERK UND INTERNET.
2. Dort wählen Sie unter ERWEITERTE NETZWERKEINSTELLUNGEN den Eintrag ADAPTEROPTIONEN ÄNDERN.
3. Wählen Sie Ihre Netzwerkkarte mit einem Doppelklick aus. Danach können Sie im Statusfenster die EIGENSCHAFTEN der Netzwerkkarte auswählen ([Abbildung 15.3](#)).
4. Spätesten zu diesem Zeitpunkt müssen Sie mit Administratorrechten arbeiten, was Ihnen auch das kleine Schildsymbol bei den EIGENSCHAFTEN sofort zeigt.
5. In den Eigenschaften Ihrer Netzwerkkarte wählen Sie dann den Eintrag INTERNETPROTOKOLL, VERSION 4 (TCP/IPv4) und klicken auch hier wiederum auf EIGENSCHAFTEN.

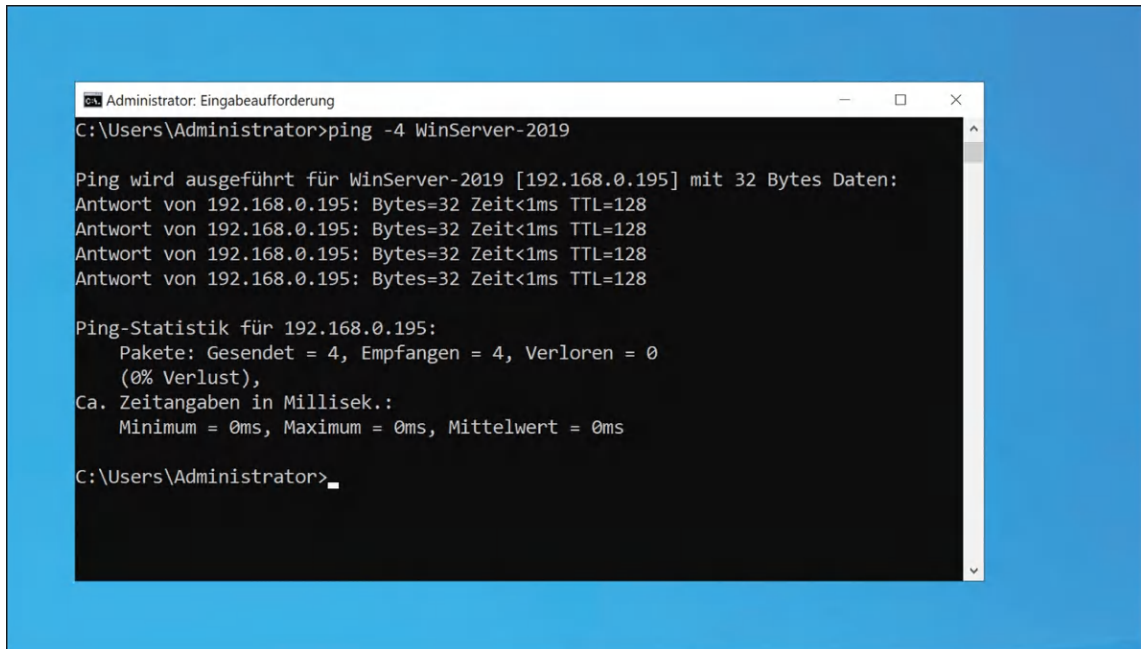


Abbildung 15.2: Ein Aufruf des Ping-Kommandos zeigt, ob der Domänencontroller vom Server aus erreichbar ist.

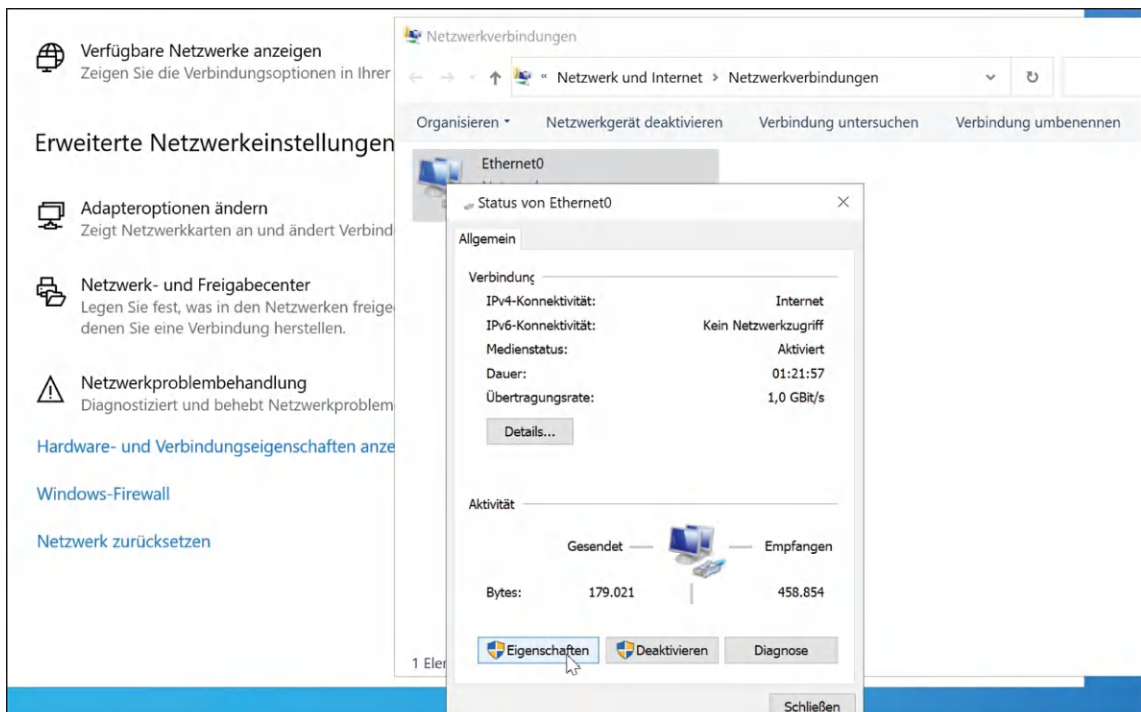


Abbildung 15.3: Damit der Server in die Domäne aufgenommen werden kann, müssen Änderungen an den Einstellungen der Netzwerkkarte vorgenommen werden.

6. Daraufhin öffnet sich ein Fenster, in dem Sie nun die TCP/IP-Konfiguration der Netzwerkkarte händisch vornehmen können

(Abbildung 15.4). In diesem Fenster konfigurieren Sie Ihre Netzwerkkarte derart, dass der Server danach keine IP-Adresse mehr vom DHCP-Server zugeteilt bekommt, sondern eine feste IP-Adresse besitzt.

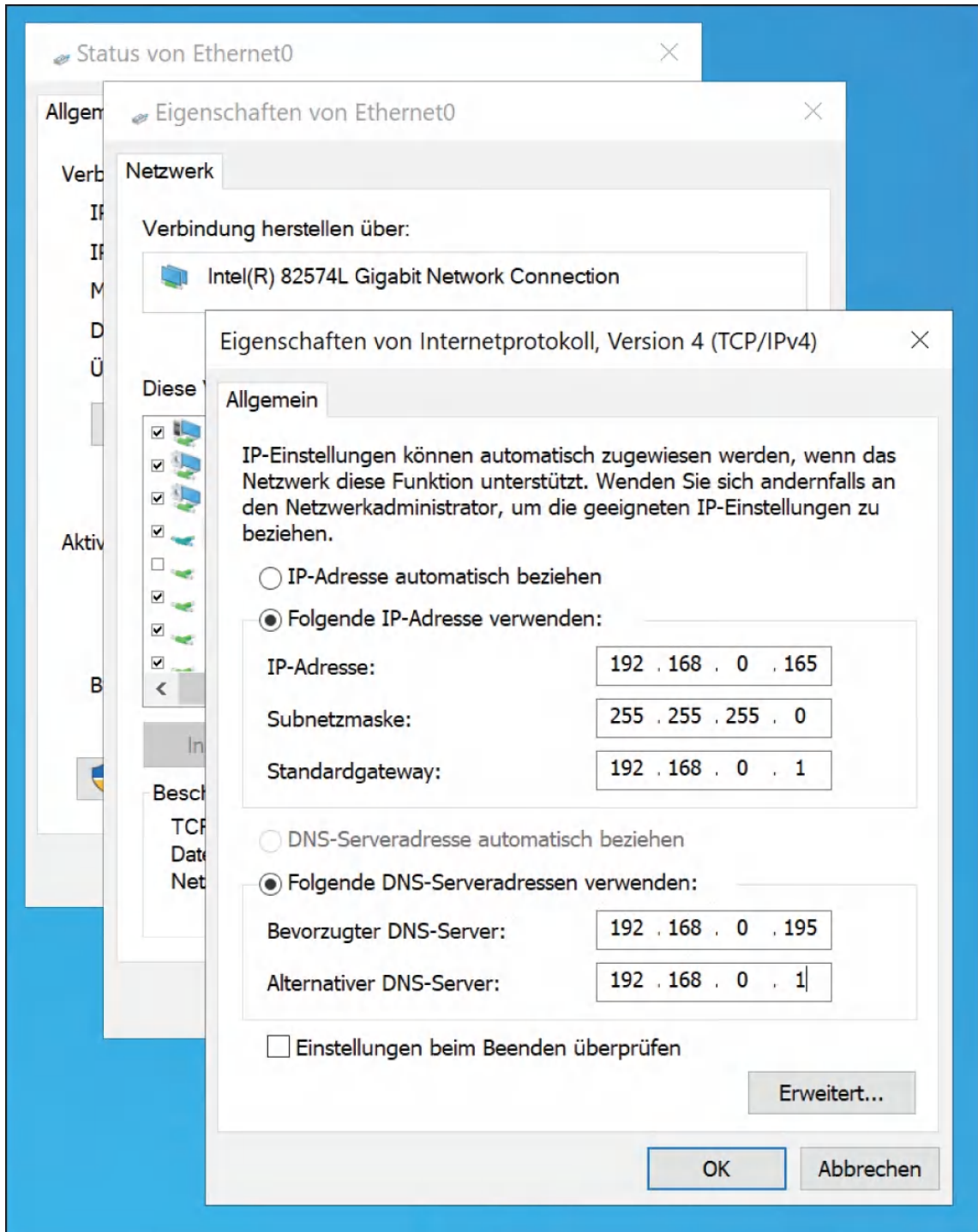


Abbildung 15.4: In den Eigenschaften des IPv4-Protokolls konfigurieren Sie Ihr

System für den Einsatz mit einer festen IP-Adresse.



Wenn Sie in Ihrem Netz beispielsweise für die Workstations und mobilen Systeme einen DHCP-Server einsetzen, dann sollten Sie darauf achten, dass die von Ihnen vergebenen festen IP-Adressen sich ausdrücklich nicht in dem Pool von Netzwerkadressen befinden, die Ihr DHCP-Server vergeben kann. Kommt die gleiche IP-Adresse in Ihrem Netzwerk zweimal zum Einsatz, so kommt es zu unvorhergesehenen Problemen, und die Systeme sind nicht mehr in der Lage, auf das Netzwerk zuzugreifen.

7. Ganz wichtig ist es hier nun auch, dass Sie den Domänencontroller als bevorzugten DNS-Server eintragen. Fungiert im Netzwerk noch ein weiteres Gerät als DNS-Server – das kann beispielsweise der Router sein, der auch als Gateway dient –, sollten Sie die Adresse dieses Systems unbedingt im Feld ALTERNATIVER DNS-SERVER eintragen. Sie können an dieser Stelle natürlich auch einen der freien DNS-Server aus dem Internet eintragen. Es ist nur wichtig, damit Ihr Server auch dann noch auf einen DNS-Server zugreifen kann, wenn der Domänencontroller einmal nicht zur Verfügung steht. Im Firmenumfeld stehen in der Regel sowieso mehrere DNS-Server zur Verfügung, die Sie hier entsprechend konfigurieren.

Ein nächster Schritt, der das weitere Arbeiten erleichtern kann, aber nicht unbedingt nötig ist, besteht darin, im Active Directory auf dem Domänencontroller eine Organisationseinheit (OU) für die Server anzulegen und darin den Server schon einmal hinzuzufügen ([Abbildung 15.5](#)).

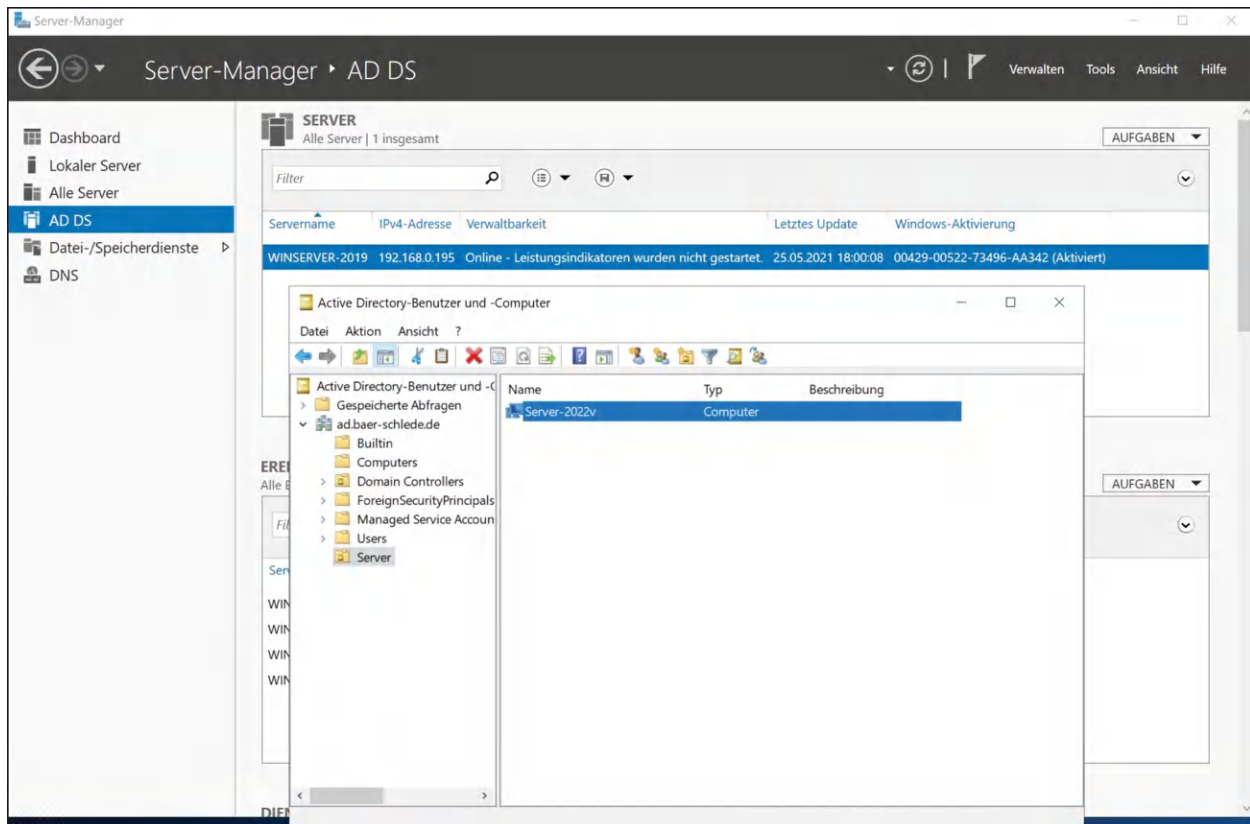


Abbildung 15.5: Es ist nicht unbedingt notwendig, aber praktisch, wenn bereits im Vorfeld die richtige OU für den Server im AD vorhanden ist.

Legen Sie keine solche OU an, dann wird Active Directory den neu hinzukommenden Server in die Organisationseinheit COMPUTERS einsortieren. Ein späteres Verschieben ist dann selbstverständlich immer noch möglich.

Einbinden in die Domäne

Nachdem nun alle Vorbereitungen getroffen sind, können Sie damit beginnen, Ihren Server zu einem Mitglied der Domäne zu machen:

1. Öffnen Sie den SERVER-MANAGER und wählen Sie in der linken Spalte LOKALER SERVER aus.
2. Klicken Sie auf den Eintrag WORKGROUP, den Sie unter den Eigenschaften Ihres Servers finden.
3. Es öffnet sich ein Fenster mit den SYSTEMEIGENSCHAFTEN. Dort

werden Ihnen der Name des Servers und seine Arbeitsgruppe angezeigt.

4. Mit einem Klick auf ÄNDERN öffnet sich ein weiteres Fenster zum ÄNDERN DES COMPUTERNAMENS BZW. DER DOMÄNE. ([Abbildung 15.6](#))
5. Klicken Sie unter MITGLIED VON auf DOMÄNE und geben Sie den Namen Ihrer Domäne ein ([Abbildung 15.6](#)).
6. Mit OK übernehmen Sie diese Einstellung.

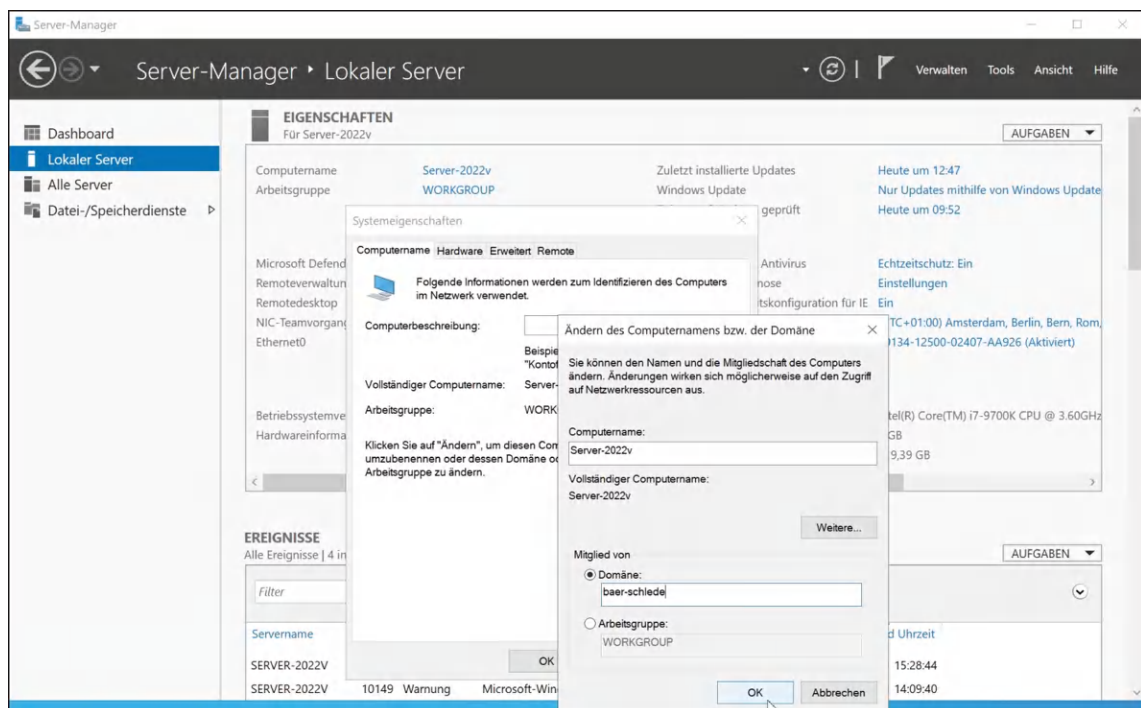


Abbildung 15.6: Der Server wird Mitglied der Domäne, deren Namen an dieser Stelle eingetragen werden muss.

7. Es öffnet sich ein Fenster der Windows-Sicherheit. Hier müssen Sie sich mit den Anmeldedaten eines Domänenadministrators an der Domäne anmelden ([Abbildung 15.7](#)).
Danach werden Sie von einem Fenster begrüßt, das Sie in der Domäne willkommen heißt.
8. Nun ist nur noch ein Neustart des neuen Domänenmitglieds notwendig. Dabei müssen Sie beachten, dass die danach folgende Anmeldung an einer Domäne immer in der Form

<DOMÄNENNAME\KONTONAME> erfolgen muss, wie in [Abbildung 15.8](#) zu sehen.

Wenn Sie es nicht durch spezielle Richtlinien unterbinden, können Sie sich an diesem System danach auch immer noch mit einem lokalen Konto anmelden.

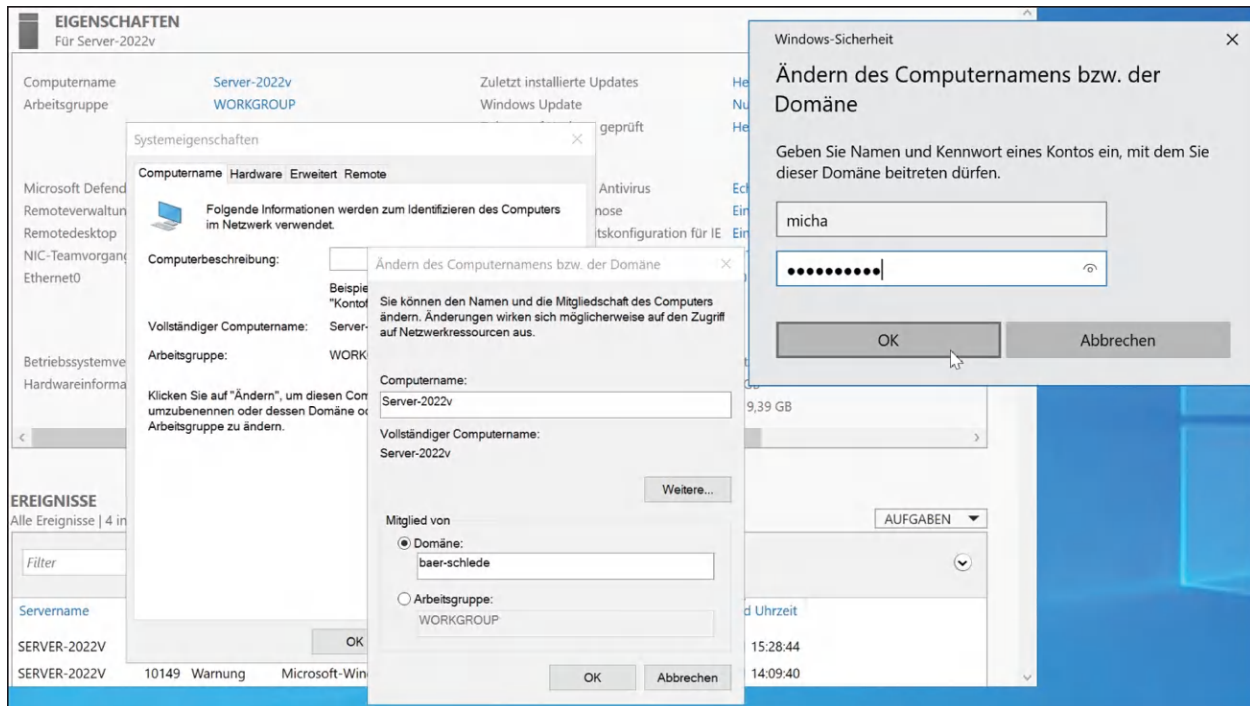


Abbildung 15.7: Die eigentliche Anmeldung an der Domäne erfolgt mit dem Konto eines Domänenadministrators.

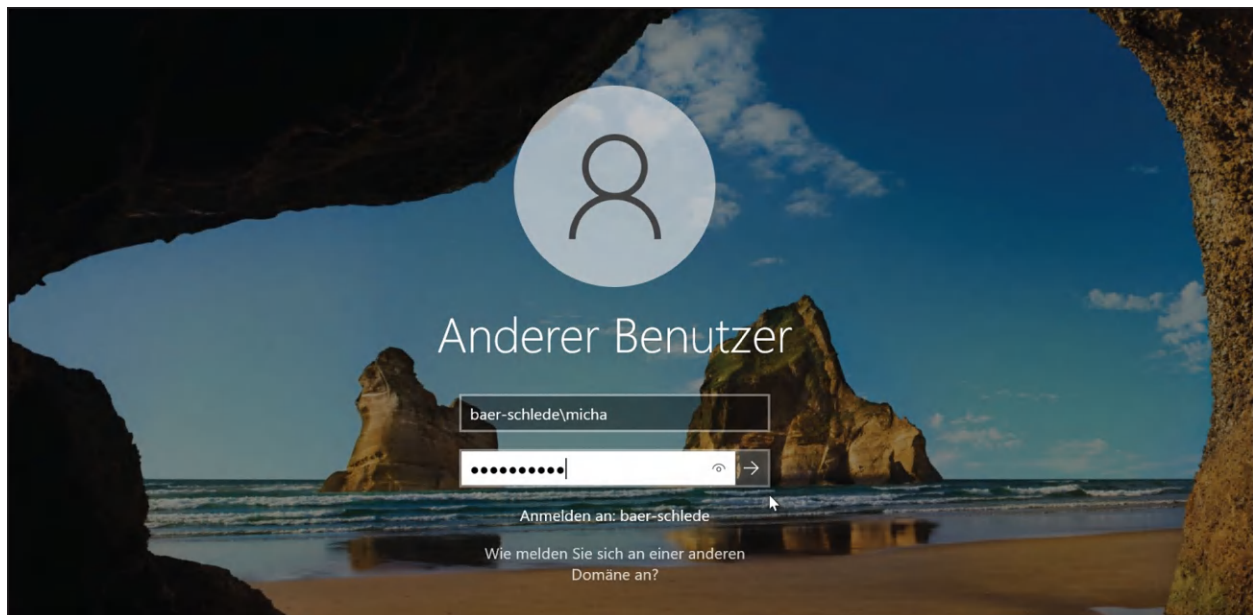


Abbildung 15.8: Die Anmeldung an einer Domäne muss immer den Namen der Domäne enthalten.

Offline einer Domäne beitreten

Normalerweise wird sich ein Computer, der einer Domäne beitreten soll, im gleichen Netzwerk wie der Domänencontroller befinden und deshalb auch eine Verbindung zu diesem haben. Es gibt aber durchaus auch Fälle, in denen es sinnvoll sein kann, diesen Vorgang offline auszuführen.

Beispielsweise, wenn der Domänenbeitritt schon einmal auf einem mobilen System konfiguriert werden soll, das nur von Zeit zu Zeit mit dem Firmennetzwerk verbunden ist. Microsoft hat mit Windows Server 2008 und Windows 7 eine solche Methode eingeführt, bei der Sie erst im letzten Schritt, nämlich bei der eigentlichen Anmeldung an der Domäne, die entsprechende Verbindung zum Domänencontroller benötigen, aber schon zuvor alles konfigurieren können. Dazu steht Ihnen in der aktuellen Version 2019 und später auch in der Version 2022 das Kommandozeilenprogramm `djoin.exe` zur Verfügung. Dabei läuft der Vorgang in zwei Schritten ab. Im ersten Schritt arbeiten Sie auf dem Domänencontroller und rufen das Programm in der Eingabeaufforderung nach dem folgenden Schema auf

```
djoin /provision /domain "baer-schlede" /maschine "Server-2019phys" /savefile server-2019phys
```


Dabei legt der Schalter /provision ein Computerkonto entsprechend der Angabe in /domain und /maschine an. An diesen Stellen setzen Sie natürlich die Angaben Ihrer Domäne und Ihres Servers ein. Schließlich müssen Sie mit /savefile noch eine Datei angeben, in der diese Daten abgespeichert werden sollen. Mit welcher Dateiendung Sie diese Datei dabei bezeichnen, ist im Prinzip unwichtig: Die Daten werden immer im BASE64-Format codiert. Viele Administratoren speichern diese Datei mit der Endung .obj ab. Wir haben für unser Beispiel die Endung .bin gewählt. In der [Abbildung 15.9](#) sehen Sie diesen Vorgang und können zugleich auch sehen, dass das Programm das neue Konto unter der OU COMPUTERS angelegt hat. Wollen Sie bei diesem Aufruf auch zugleich festlegen, in welcher Organisationseinheit der Computer angelegt werden soll, so können Sie dazu den Schalter /machineou <Name der OU> verwenden. Durch den Aufruf von

`djoin /help`

bekommen Sie alle möglichen Optionen des Kommandos mit jeweils einer kurzen Erklärung angezeigt.

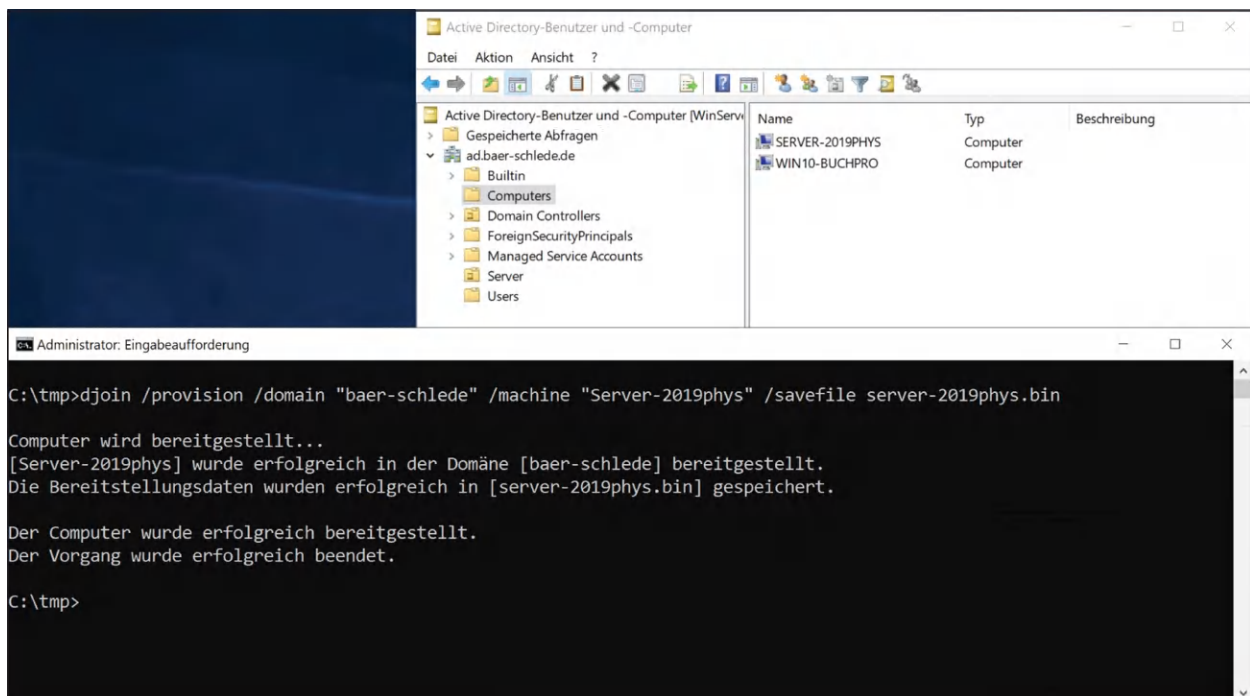


Abbildung 15.9: Ein Offline-Beitritt zu einer AD-Domäne gliedert sich in zwei Schritte: Dieser erste Schritt wird auf dem Domänencontroller ausgeführt.

Die nun erstellte Datei müssen Sie anschließend auf das System transferieren, das der Domäne beitreten soll. Dort rufen Sie dann ebenfalls das Kommando `djoin.exe` auf, wobei Sie für den Aufruf die Rechte eines lokalen Administrators besitzen müssen. Der Aufruf hat die folgende Form:

```
djoin /requestobj /loadfile ./server-2019phys.bin /windowspath  
c:\windows /localos
```

Durch den Schalter `/requestobj` wird beim nächsten Start ein Offlinebeitritt zur Domäne angefordert. Sie müssen zudem über `/loadfile` den Dateinamen der auf dem Domänencontroller erstellten Datei mitgeben. Dabei ermöglicht erst der Schalter `/localos` die Angabe des lokal ausgeführten Betriebssystems mit `/windowspath` ([Abbildung 15.10](#)).

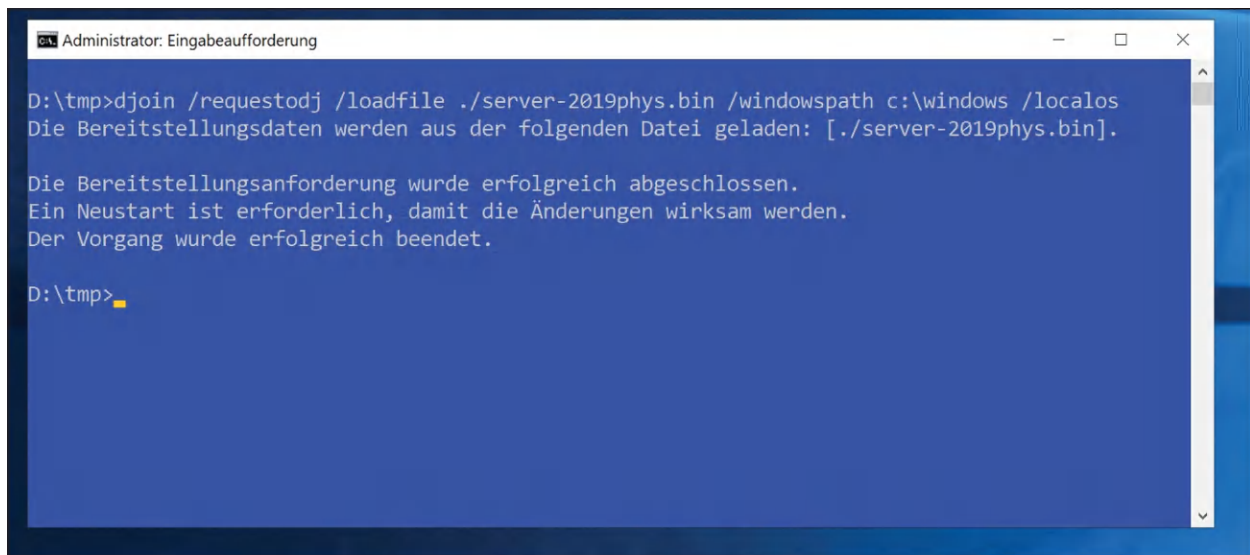


Abbildung 15.10: Der zweite Schritt: Auf dem Server wird die Datei mit den Daten zum Domänenbeitritt eingespielt.

Danach ist ein Neustart des Systems notwendig, den Sie explizit anstoßen müssen. Damit ist dieser Server nun Teil der Domäne, was Sie mit einem Aufruf des Server-Managers auch leicht feststellen können. Eine Anmeldung des Systems mittels Domänenkonto ist aber natürlich nur dann möglich, wenn Ihr Server eine Verbindung zum Domänencontroller aufbauen kann. Bis dahin bleibt Ihnen die Möglichkeit, sich weiterhin mit einem lokalen Konto auf dem System anzumelden.

Kapitel 16

Gruppenrichtlinien

IN DIESEM KAPITEL

Was sind Gruppenrichtlinien?

Anlegen, Verknüpfen und Löschen eines Gruppenrichtlinienobjekts

Gruppenrichtlinien und Gruppen

WMI-Filter

Zielgruppenadressierung

Administrative Vorlagen

Handlungsempfehlung für Gruppenrichtlinien

Praktische Empfehlungen

Troubleshooting für Gruppenrichtlinien

Gruppenrichtlinien sind, aus Sicht des Administrators, so ziemlich die wundervollste Erfindung von Microsoft, wenn es um die Steuerung von Einstellungen für Benutzer und Computer geht. Die besondere Leistungsfähigkeit ergibt sich dabei aus dem Zusammenspiel der verschiedenen Möglichkeiten.

Gruppenrichtlinienobjekte (GPO = Group Policy Objects) bestehen stets aus zwei Bereichen:

- ✓ Benutzerkonfiguration
- ✓ Computerkonfiguration



Änderungen in Gruppenrichtlinien wirken aller Wahrscheinlichkeit nach nicht sofort. In der Standardeinstellung überträgt ein

Domänencontroller üblicherweise alle 90 Minuten die Einstellungen an die Client- und Server-Systeme. Bei einem Neustart des Computers greifen wiederum sofort die verfügbaren Computerrichtlinien. Bei einer Neuansmeldung die Benutzerrichtlinien. Mehr zu diesem Thema erfahren Sie in diesem Kapitel.

Die beiden Konfigurationsbereiche unterscheiden sich auch darin, wann sie abgearbeitet werden: Die Computerkonfiguration wird beim Start des Computers abgearbeitet. Erst nach Abschluss dieses Vorgangs steht der Anmeldedialog für den Anwender zu Verfügung. Bei Anmeldung des Benutzers greifen die Einstellungen aus der Benutzerkonfiguration.

Starten wir ein praktisches Beispiel, um in das Thema Gruppenrichtlinien einzusteigen. Hierfür sind einige Rahmenbedingungen vorzubereiten:

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND COMPUTER.
4. Klicken Sie mit der rechten Maustaste auf die Bezeichnung Ihrer Domäne und wählen Sie im Kontextmenü den Befehl NEU | ORGANISATIONSEINHEIT. Benennen Sie die OU als »GPOTEST«.
5. Verschieben Sie nun einen Testbenutzer aus dem Container USERS in die OU »GPOTEST«. Der Windows-Server zeigt Ihnen daraufhin einen Warndialog an, dass das Verschieben von Objekten möglicherweise Auswirkungen auf den ordnungsgemäßen Betrieb haben wird. Da wir bewusst eine Verschiebung durchführen, bestätigen Sie diesen Dialog mit JA.
6. Verschieben Sie nun einen Testcomputer aus dem Container COMPUTERS in die OU »GPOTEST«. Es erscheint erneut der Dialog aus Schritt 5, bestätigen Sie diesen wieder mit JA.
7. Schließen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND COMPUTER.

8. Wählen Sie das Verwaltungsprogramm GRUPPENRICHTLINIENVERWALTUNG.
9. Klicken Sie mit der rechten Maustaste auf die von Ihnen erzeugte OU »GPOTEST« und wählen Sie GRUPPENRICHTLINIENOBJEKT HIER ERSTELLEN UND VERKNÜPFEN... Benennen Sie das Gruppenrichtlinienobjekt beispielweise »GPO1« und bestätigen Sie den Dialog mit OK.
10. Klicken Sie mit der rechten Maustaste auf das erzeugte Gruppenrichtlinienobjekt und wählen Sie im Kontextmenü den Befehl BEARBEITEN – siehe [Abbildung 16.1](#).
11. Es öffnet sich der GRUPPENRICHTLINIENVERWALTUNGS-EDITOR, aufteilt in die beiden Abschnitte COMPUTERKONFIGURATION und BENUTZERKONFIGURATION jeweils mit den Unterordnern RICHTLINIEN und EINSTELLUNGEN.

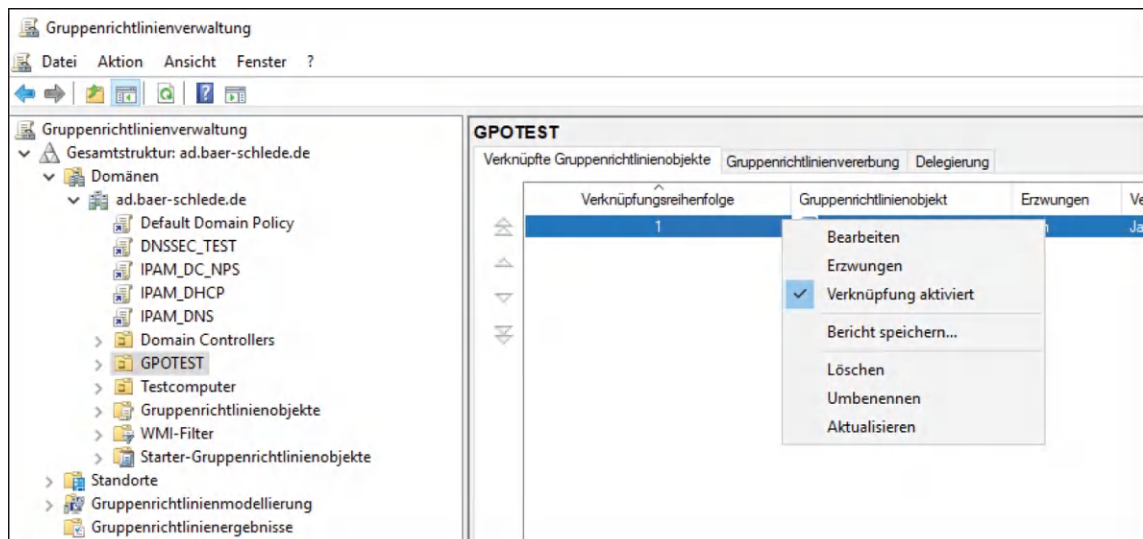


Abbildung 16.1: Gruppenrichtlinienobjekte sind OUs in der Gruppenrichtlinienverwaltung zugeordnet.



Bedenken Sie die Abarbeitungsreihenfolge der Gruppenrichtlinienobjekte: Erst die Computerkonfiguration, dann die Benutzerkonfiguration. Die zuletzt gesetzte Einstellung stellt die tatsächlich aktive Einstellung dar.

Neben der Computer- und Benutzerkonfiguration gibt es in Bezug auf die GPOs noch eine weitere Reihenfolge: lokale Sicherheitsrichtlinie, gefolgt von Standort, Domäne und letztendlich OU. Die gesetzten Einstellungen in unserem Beispiel übersteuern somit die vordefinierten Einstellungen.

12. Öffnen Sie einmal alle Unterordner und Sie werden sehen, dass die Grundstruktur weitgehend identisch ist.
13. Erstellen wir exemplarisch eine Verknüpfung auf dem Desktop auf das Programm Notepad. Wählen Sie hierzu
BENUTZERKONFIGURATION | EINSTELLUNGEN | WINDOWS-EINSTELLUNGEN | VERKNÜPFUNGEN.
14. Es erscheint das Dialogfenster zur Anlage von Verknüpfungen. Klicken Sie mit der rechten Maustaste in das Fenster und wählen Sie im Kontextmenü den Eintrag NEU. Es erscheint der Anlagedialog für eine NEUE VERKNÜPFUNGSEIGENSCHAFT. Legen Sie die Einträge an, wie in [Abbildung 16.2](#) zu sehen. Bestätigen Sie die Eingabe mit OK.
15. Melden Sie sich mit dem Benutzer an, der von der Gruppenrichtlinie betroffen sein wird. Auf dem Desktop erscheint der Link auf das Programm Notepad mit einem vom Standard abweichenden Icon.



Die Anmeldung kann in unserem Beispiel an jedem PC oder Server in der Domäne erfolgen, da wir eine Benutzerkonfiguration angelegt haben!

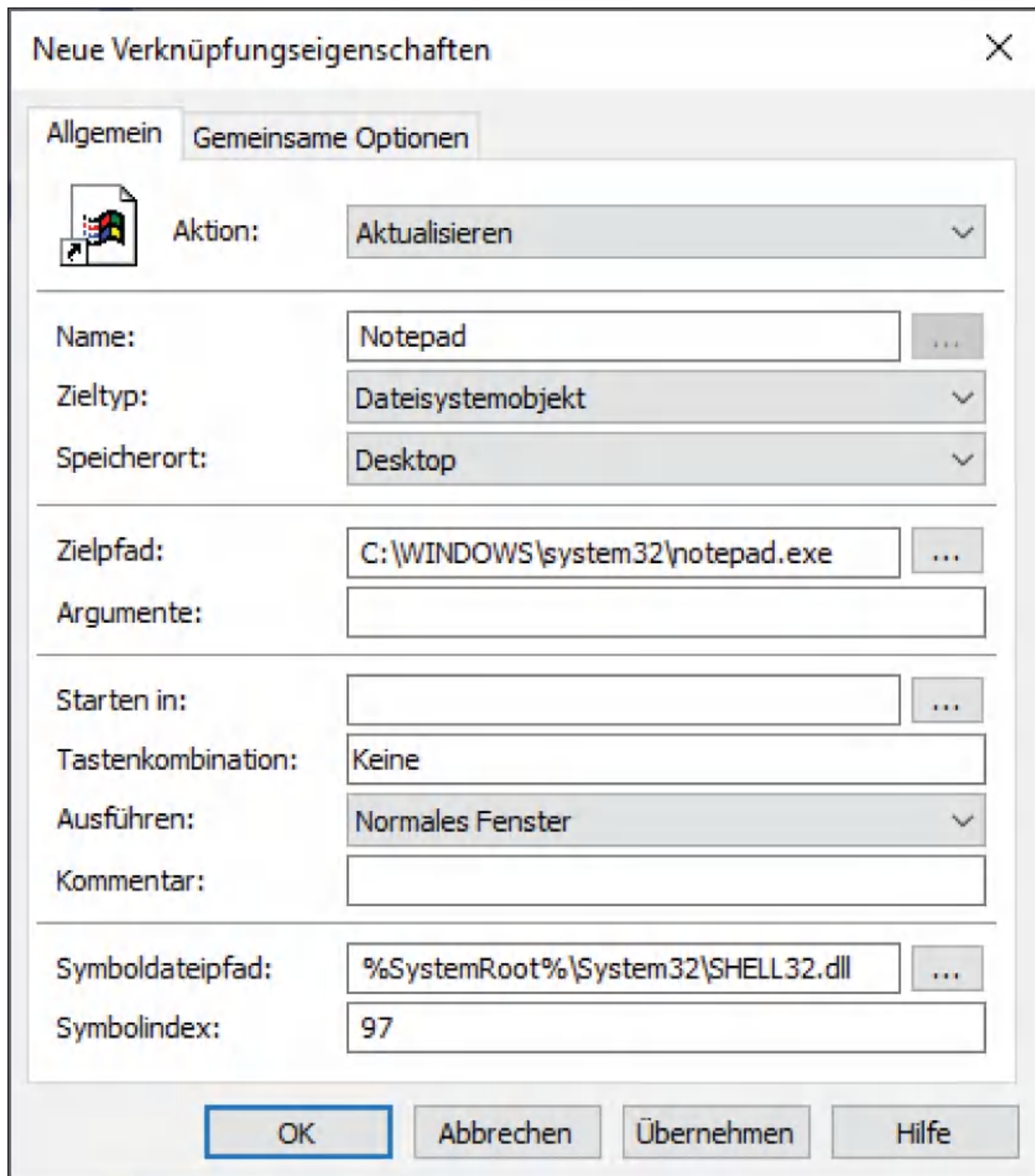


Abbildung 16.2: Anlage einer Verknüpfung für eine Gruppenrichtlinie

Wie Sie bereits im Dialogfenster GRUPPENRICHTLINIENVERWALTUNGS-EDITOR sehen konnten, gibt es eine sehr große Anzahl von möglichen Einstellungen. Wir werden darauf noch zurückkommen, aber zunächst wollen wir einen Blick auf die

»grundlegende Anatomie« einer Gruppenrichtlinie.

Öffnen Sie noch einmal die Gruppenrichtlinienverwaltung und klicken Sie auf »GPOTEST« und wählen Sie die zweite Registerkarte GRUPPENRICHTLINIENVERERBUNG – siehe [Abbildung 16.3](#).

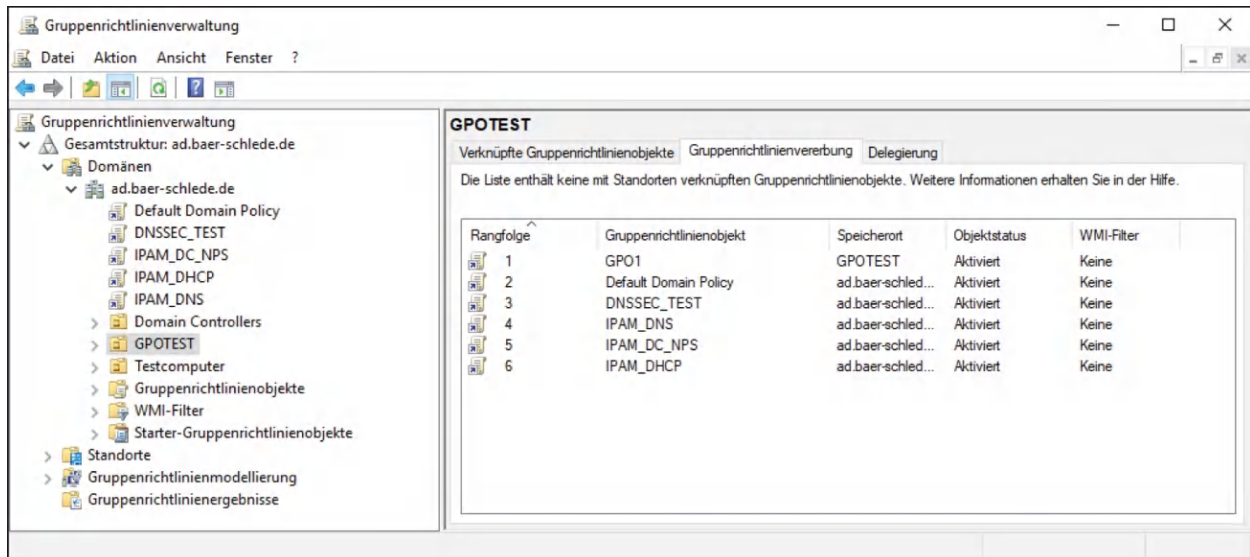


Abbildung 16.3: Die Abarbeitungsreihenfolge verläuft von unten nach oben.

Es gibt, wie Sie sehen können, eine Reihe von Gruppenrichtlinie, die auf die OU einwirken, und diese werden in Bezug auf die Reihenfolge von »große Zahl« nach »kleiner Zahl« abgearbeitet. Sollte also an Position 6 festgelegt worden sein, dass eine Eigenschaft den Wert 5 haben mag und in der Richtlinie am Rangfolgenplatz 1 für dieselbe Eigenschaft der Wert 3 gelten möge – so gewinnt 3.



Bei den Gruppenrichtlinien ist es wie beim Sport: Der auf Platz 1 gewinnt!



Es gibt zwei verschiedene Möglichkeiten, die Reihenfolge der Gruppenrichtlinienabarbeitung zu beeinflussen. Aktivieren Sie das Häkchen ERZWUNGEN, sorgen Sie dafür, dass im AD diese Gruppenrichtlinie stets an die oberste Stelle verschoben wird.

Die andere Variante ist das Deaktivieren der Vererbung: Es wird

nicht die von ihr ausgehende Vererbung deaktiviert, sondern das darüber liegende Richtlinienerbe wird nicht geerbt. Sie wird »blockiert« (engl. Block Inheritance).

Hinter einem Gruppenrichtlinienobjekt verbirgt sich schlicht eine XML-Einstellung, die vom Windows-Computer abgearbeitet wird. Sie können den Inhalt über einen Zugriff auf die Freigabe SYSVOL auf einem Domänencontroller betrachten. Öffnen Sie dort den Ordner mit dem DOMÄNENNAMEN | POLICIES und suchen Sie anschließend den Ordner mit dem »jüngsten Datum« auf ([Abbildung 16.4](#)).

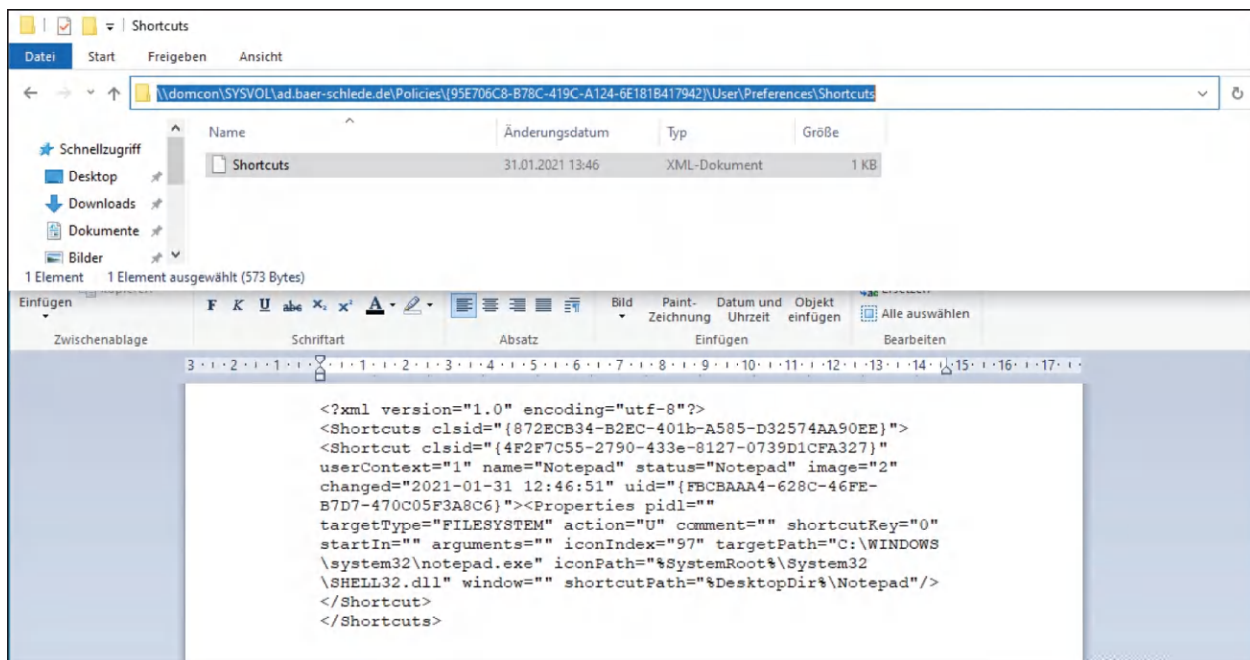


Abbildung 16.4: Inhalt und Ablageort des Gruppenrichtlinienobjekts

Richtlinien sind sicher vor dem direkten Benutzerzugriff, sie schreiben die Werte in die .Policies-Schlüssel der Registry-Datenbank, in denen der Benutzer selbst innerhalb der eigenen `ntuser.dat` nur über Leserechte verfügt, und der Besitzer dieses Teilschlüssels ist das System selbst. Das Objekt speichert die aus einer Gruppenrichtlinie stammenden Daten in eine lokale Datei mit Namen `ntuser.pol` im Verzeichnis `%userprofile%`, und der Benutzer kann sie deswegen auch gezielt löschen – was aber ohne negative Folgen bleibt.

Richtlinien muss der Computer nur dann verarbeiten, wenn sie aktualisiert

wurden. Sofern der Versionszähler unverändert ist, passiert nichts. Jede Anpassung einer Gruppenrichtlinie sorgt folglich für die Erhöhung des individuellen Zählers. Jede Richtlinie hat einen eindeutige Identifier (UID) – die der Default Domain Policy lautet beispielsweise 31B2F340-016D-11D2-945F-00C04FB984F9.



Wenn Sie eine GPO anpassen, sind die Einstellungen sofort vor Ort verfügbar und werden im nächsten Replikationszeitfenster auf die anderen DCs übertragen. Jede Änderung ist sofort aktiv – die Änderung wird gespeichert, ohne dass dazu das Fenster geschlossen werden muss. Fall ein Benutzer oder ein Computer zum Zeitpunkt der Änderung die GPO abruft, erhält er sofort die neuesten Einstellungen. Es empfiehlt sich daher, zunächst neue Objekte zu erstellen, anschließend die Einstellung zu konfigurieren und sie dann zu verknüpfen.

Gruppenrichtlinienobjekt verknüpfen

Im vorherigen Beispiel legten wir zunächst eine OU an, füllten sie mit einem Benutzer- und einem Computerobjekt und legten anschließend ein Gruppenrichtlinienobjekt (GPO) an. Sie können ein bereits vorhandenes GPO aber auch einer anderen OU zuweisen. Hierzu erstellen wir exemplarisch eine zweite OU und ordnen dieser einen Benutzer zu.

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm GRUPPENRICHTLINIENVERWALTUNG.
4. Wählen Sie Ihre Domäne aus und klicken Sie mit der rechten Maustaste auf den Namen der Domäne. Wählen Sie den Befehl NEUE ORGANISATIONSEINHEIT aus dem Kontextmenü.
5. Wählen Sie einen beliebigen Namen – in diesem Beispiel wählen wir »GPOTEST-2«.

6. Klicken Sie in der Baumstruktur mit der rechten Maustaste auf die soeben angelegte Organisationseinheit und wählen Sie **VORHANDENES GRUPPENRICHTLINIENOBJEKT VERKNÜPFEN...** aus dem Kontextmenü.
7. Wählen Sie das zuzuordnende GPO – in diesem Beispiel »GPO1«. Bestätigen Sie die Auswahl mit einem Doppelklick oder durch Auswahl mit abschließendem Klick auf OK.
8. Aus dem Dialog **GRUPPENRICHTLINIENVERWALTUNG** heraus haben Sie keine Möglichkeit, eine Benutzerzuordnung zur OU vorzunehmen. Klicken Sie mit der rechten Maustaste noch einmal auf die Domänenbezeichnung und wählen Sie **ACTIVE DIRECTORY-BENUTZER UND COMPUTER**, um in den Dialog zu wechseln.
9. Verschieben Sie ein Benutzerobjekt aus dem Container **USERS** in die neue OU. Es erscheint wieder der bekannte Warnhinweis.
10. Melden Sie sich mit dem Benutzerkonto an einem beliebigen Computer in der Domäne an – die verknüpfte Gruppenrichtlinie wirkt auch auf die neue OU.



In einer kleinen Umgebung mit nur einem Domänencontroller sind die Änderungen sofort wirksam. In größeren Umgebungen kann es bis zum nächsten Replikationszyklus dauern, ehe das GPO wirkt.

Gruppenrichtlinienobjekt löschen

Das Löschen eines Gruppenrichtlinienobjekts ist denkbar einfach. Hier gilt es zu unterscheiden, ob lediglich die Verknüpfung auf eine OU zu entfernen oder das ganze Gruppenrichtlinienobjekt zu verwerfen ist.

Die Verknüpfung entfernen Sie über folgende Befehlskette:

1. Starten Sie den **SERVER-MANAGER**.
2. Wählen Sie oben rechts im Menü den Befehl **TOOLS**.
3. Wählen Sie das Verwaltungsprogramm

GRUPPENRICHTLINIENVERWALTUNG.

4. Wählen Sie in der Baumstruktur die gewünschte OU aus, markieren Sie das zu entfernende GPO in der Auflistung der verknüpften Gruppenrichtlinienobjekte und drücken Sie die Taste .
5. Bestätigen Sie das Löschen der Verknüpfung mit OK.

Das GPO entfernen Sie über folgende Befehlskette:

1. Starten Sie den SERVER-MANAGER.
 2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
 3. Wählen Sie das Verwaltungsprogramm GRUPPENRICHTLINIENVERWALTUNG.
 4. Wählen Sie in der Baumstruktur den Ordner GRUPPENRICHTLINIENOBJEKTE.
 5. Wählen Sie aus dem Kontextmenü nach einem Rechtsklick den Befehl LÖSCHEN oder drücken Sie nach Auswahl des Eintrags die Taste .
- Es erscheint ein Warndialog (zu sehen in [Abbildung 16.5](#)), der Sie darauf hinweist, dass das Löschen des GPO nur dafür sorgt, dass es als Verknüpfung aus allen Gruppenrichtlinien in der eigenen Domäne entfernt wird, nicht aber aus anderen Domänen.
6. Sie müssen diesen Dialog mit JA bestätigen, um das Löschen abzuschließen.

Möglicherweise erreichen Sie durch das Löschen eines GPOs oder der zu der Einstellung führenden Verknüpfung nicht unbedingt den gewünschten Effekt, denn die von dem GPO angepassten Einstellungen wurden nicht rückgängig gemacht, sondern nur die Neuausführung wurde aufgehoben.

In unserem Beispiel verbleibt die Verknüpfung auf dem Desktop, sofern diese nicht explizit gelöscht wird. Wenn beispielsweise eine Verknüpfung wieder zurückgenommen werden soll, brauchen Sie hierfür zunächst ein Löschkommando.

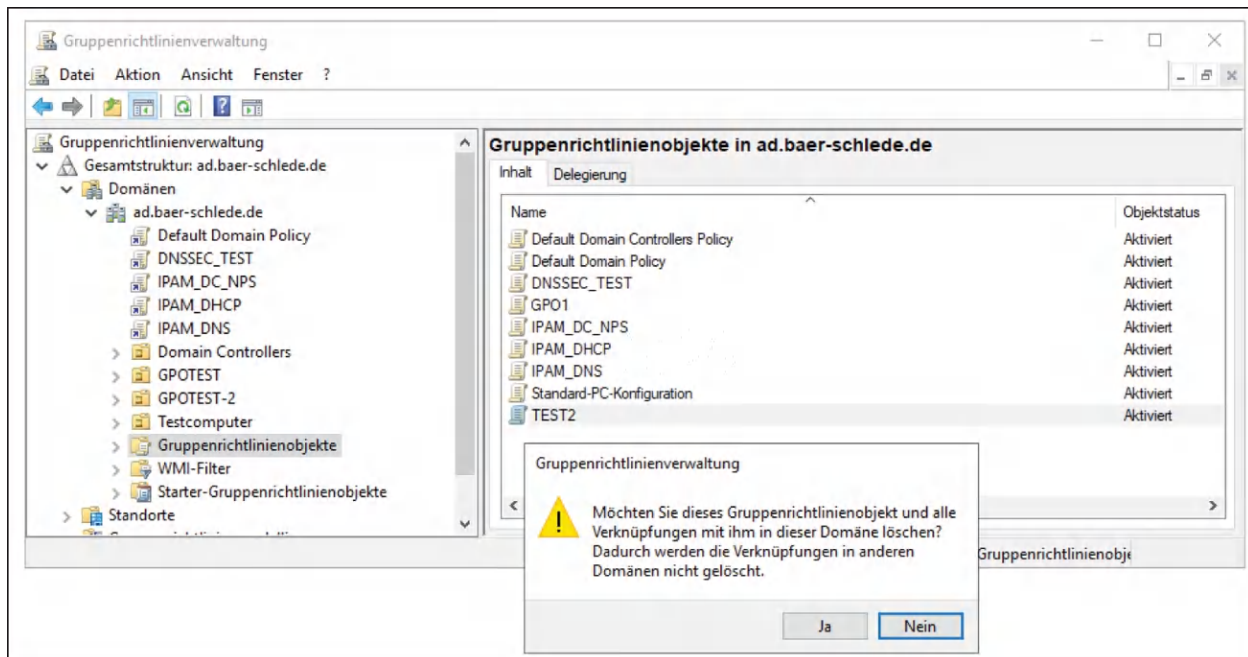


Abbildung 16.5: Beim Löschen eines Gruppenrichtlinienobjekts entfernt Windows automatisch alle Verknüpfungen innerhalb der eigenen Domäne.

In unserem zuvor beschriebenen Beispiel wäre es also schlichtweg sinnvoller, im GPO die Verknüpfung auf dem Desktop über Löschen zu entfernen, anstatt das Gruppenrichtlinienobjekt oder die Verknüpfung der OU auf das Gruppenrichtlinienobjekt zu löschen.



Einstellungen per Gruppenrichtlinie sind schnell eingerichtet, und ohne die notwendige Struktur durch den Administrator entsteht sehr schnell Chaos. Sorgen Sie in einer größeren IT-Gruppe dafür, dass nur wenige ausgewiesene Experten Gruppenrichtlinien anpassen dürfen. Es gibt mit dem »Group Policy Advanced Management«-Tool (AGPM) von Microsoft sogar die Möglichkeit, eine Genehmigungsstruktur für Gruppenrichtlinien aufzubauen. Sie finden das Tool bei Microsoft unter dem Link <https://bit.ly/3oCzps9>.

Gruppenrichtlinien und Gruppen

Vielleicht ist es Ihnen aufgefallen, dass das Wort Gruppen bisher noch gar nicht vorkam.



Die Abarbeitungsreihenfolge ist Standort (Site) | Domäne | Organisationseinheit.

Das bedeutet nichts anderes, als dass eine Gruppenrichtlinie auf Domänenebene auf alle untergeordneten Organisationseinheiten wirkt, sofern diese Vererbung nicht explizit außer Kraft gesetzt wird. Spannend: In der Reihenfolge kommt das Wort »Gruppe« gar nicht vor, weil Gruppen eben nicht vorgesehen sind. Gruppenrichtlinien stehen, so in einem Internetforum treffende Aussage, für »Gruppen von Richtlinien« und nicht für »Richtlinie von Gruppen«.

Diese Umsetzung würde jedoch eine dramatische Limitierung der Technik zur Folge haben, wenn es nicht die Möglichkeit gäbe, eine Zuordnung auch außerhalb der Organisationseinheiten darzustellen. Glücklicherweise gibt es die Möglichkeit, die Wirksamkeit einer Gruppenrichtlinie, die auf eine OU einwirkt, auf die Zugehörigkeit einer Gruppe zu limitieren.

Erweitern wir hierzu das bereits angeführte Beispiel in diesem Kapitel. Stellen Sie sicher, dass mindestens zwei Benutzer der OU »GPOTEST« zugeordnet sind. Die Benutzerobjekte müssen sich hinsichtlich der Gruppenzugehörigkeit unterscheiden. In unserem Beispiel ist das Benutzerkonto von »Julia Schmidt« Mitglied der Gruppe »PG-Chefsekretariat«.

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm GRUPPENRICHTLINIENVERWALTUNG.
4. Wählen Sie in der Baumstruktur den Eintrag der gewünschten Organisationseinheit, in unserem Beispiel »GPOTEST«, und markieren Sie das darunter zugeordnete Gruppenrichtlinienobjekt, in unserem Beispiel »GPO1«.
5. In der rechten Fensterseite wird in der Registerkarte BEREICH in der Mitte die Einstellung für die SICHERHEITSFILTERUNG sichtbar. In der Standardeinstellung ist hier die Zuordnung für authentifizierte

Benutzer zugewiesen. Markieren Sie die Gruppe und klicken Sie die Schaltfläche ENTFERNEN.

6. Es erscheint ein Warndialog, der darlegt, dass Leserechte für Domänencomputer erforderlich sind. Bestätigen Sie den Hinweis mit OK.
7. Klicken Sie auf die Schaltfläche HINZUFÜGEN und wählen Sie die gewünschte Gruppe, in unserem Beispiel »PG-Chefsekretariat«, siehe [Abbildung 16.6](#).

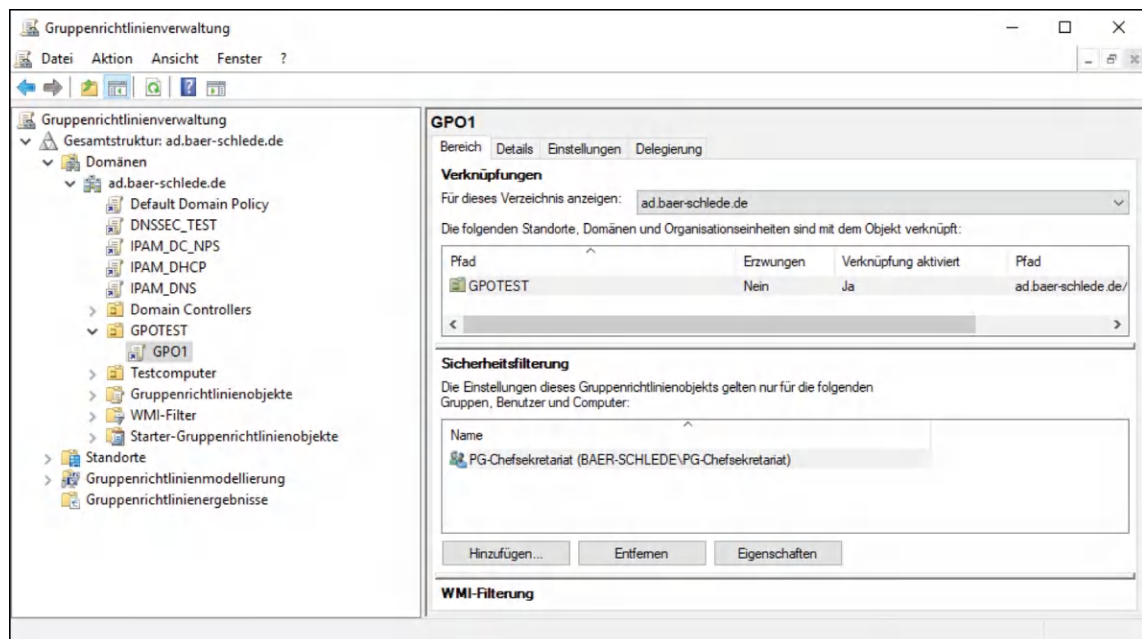


Abbildung 16.6: Mit der Sicherheitsfilterung wirken Gruppenrichtlinien direkt auf Gruppen, Benutzer oder Computer.

8. Nun gilt es noch, den zuvor bestätigten Warndialog zu berücksichtigen und in der Registerkarte DELEGIERUNG sicherzustellen, dass authentifizierte Benutzer über die zwei Rechte *Lesen* und *Gruppenrichtlinie übernehmen* verfügen. Klicken Sie hierzu in die Registerkarte DELEGIERUNG, wählen Sie den Befehl HINZUFÜGEN und suchen Sie nach DOMÄNENCOMPUTER.
9. Wählen Sie im Dialog BENUTZER ODER GRUPPE HINZUFÜGEN die Berechtigung LESEN aus der Auswahlliste aus.
10. Selektieren Sie den Eintrag DOMÄNENCOMPUTER und klicken Sie auf die Schaltfläche ERWEITERT... Wählen Sie in dieser Liste erneut

den Eintrag DOMÄNENCOMPUTER und markieren Sie in der unteren Auswahlbox den Eintrag GRUPPENRICHTLINIE ÜBERNEHMEN. Bestätigen Sie die Auswahl durch OK.

11. Prüfen Sie auf einem Computer die Funktionalität der Einstellung.

Die Auswertung einer Gruppenzuordnung in einer Gruppenrichtlinie selbst ist nicht möglich. Dank der Filterfunktion ist es jedoch sehr wohl möglich, gruppenabhängig ein Gruppenrichtlinienobjekt zur Ausführung zu bringen. Letztendlich ist diese Variante sogar in der Praxis attraktiver, da Sie als Administrator die erstellten GPOs viel besser »wiederverwerten« können.

WMI-Filter

Die Filterung über Gruppen, Benutzer oder Computer wurde im vorherigen Kapitel bereits dargestellt. Es existiert jedoch eine noch viel mächtigere Filterfunktion, um GPOs nur in ganz spezifischen Konstellationen zur Ausführung zu bringen: der WMI-Filter.



Die Windows Management Instrumentation (WMI) ist eine Implementierung von Microsoft und auch Erweiterung des Common Information Models (CIM), einer Kernfunktionalität des standardisierten Web Based Enterprise Managements (WBEM) für die Windows-Plattform. WMI ermöglicht den schreibenden und lesenden Zugriff auf nahezu alle Einstellungen von Windows-Systemen. Verständlicherweise ist es damit im Windows-Umfeld die wichtigste Schnittstelle zur Administration und Fernwartung von Windows-Computern, unabhängig davon, ob es sich um PCs oder Server handelt. WMI wird typischerweise per PowerShell, VBScript oder schlicht über das Kommandozeilenprogramm Windows Management Instrumentation Command-line (WMIC) angesprochen.

WMI ist in einem dreischichtigen Modell aufgebaut: Provider, CIM Object Manager (CIMOM) und die »Konsumenten« der WMI-Informationen. Provider, die unterste WMI-Schicht, sind Software-

Agenten, die Informationen beispielsweise über das Betriebssystem, Dienste, Programme oder Systemtreiber verarbeiten und an den CIM Objekt Manager weiterreichen. Provider extrahieren die Management-Informationen aus den verschiedenen Datenquellen über verschiedene Software-Interfaces. Dank dieser Abstraktionsschicht ist die versionsübergreifende Nutzung einfacher. Der CIMOM ist ein Informations- und Anfrage-Broker, der über eigene Repository-Datenbanken verfügt. Der CIMOM selbst ist ein Systemdienst, der auch als »WinMgmt« bezeichnet wird. Provider verbinden sich mit dem CIMOM über COM-Schnittstellen.

CIMOM speichert alle Informationen in strukturierte Klassen und ermöglicht einen gezielten Zugriff auf gewünschte Management-Informationen. Eigenschaften, im englischen Original als »Properties« bezeichnet, sind sowohl eine beschreibende als auch operative Information einer Klasse. Ein gutes Beispiel ist die Instanz einer Klasse von Win32_DiskDrive. In dieser Klasse gibt es eine Eigenschaft mit der Bezeichnung InterfaceType – diese Eigenschaft hat üblicherweise einen Wert – beispielsweise »IDE« oder »USB«.

Geben Sie in der PowerShell folgendes Kommando ein:

```
Get-WMIObject -Class Win32_DiskDrive | Select  
InterfaceType, Caption, Size
```

Sie erhalten eine Auflistung des Interface-Anschlusses, Bezeichnung und der Kapazität in Bytes. In der Eingabeaufforderung ergibt das Kommando

```
wmic diskdrive get InterfaceType, Caption, Size
```

dasselbe Ergebnis.

Erstellen wir, wieder einmal rein exemplarisch, einen WMI-Filter für eine GPO, die nur dann in Aktion treten soll, wenn es sich bei dem Zielcomputer um einen Domänencontroller handelt.

Es ist an sich kaum zu glauben, aber hierfür gibt es tatsächlich keinen vorgefertigten Filter. Der Administrator muss sich der WMI bedienen.

1. Starten Sie den SERVER-MANAGER.

2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm GRUPPENRICHTLINIENVERWALTUNG.
4. Wählen Sie den Eintrag WMI-FILTER in der Baumstruktur.
5. Klicken Sie mit der rechten Maustaste in die rechte Fensterhälfte und wählen Sie aus dem Kontextmenü den Befehl NEU...
6. Benennen Sie Ihren WMI-Filter, beispielsweise mit »DOMAIN-CONTROLLER«.
7. Klicken Sie auf HINZUFÜGEN.
8. Belassen Sie den NAMESPACEWERT auf der Auswahl root\CIMv2.
9. Geben Sie in das Textfeld ABFRAGE folgenden Text ein, ProductType 2 ist ein Domänencontroller, 1 wäre eine normale Arbeitsstation und 3 ein Server, der kein Domänencontroller ist:

```
select * from Win32_OperatingSystem where  
ProductType ="2"
```
10. Klicken Sie auf OK, um die Abfrage im Filter zu speichern.
11. Klicken Sie auf die Schaltfläche SPEICHERN, um die Anlage abzuschließen.
12. Wählen Sie nun eine Gruppenrichtlinienobjekt aus, das Sie nur auf einem DC zur Ausführung bringen möchten, und wählen Sie im Abschnitt WMI-FILTERUNG den passenden WMI-Filter aus der Liste und bestätigen Sie mit JA.



In der Praxis werden Sie eher das genaue Gegenteil in einem WMI-Filter zum Ausdruck bringen wollen. Dann lautet die Syntax
`ProductType <>"2"`.

Wie bereits geschrieben – es handelt sich bei dem Ausschluss der Domänencontroller für diese Gruppenrichtlinie um ein Beispiel. Es gibt viele verschiedene Anwendungsfälle, die Sie als Administrator recht einfach umsetzen können.

WMI Query Language

Die Basis sind die verschiedenen Informationen aus WMI und die sogenannte WMI Query Language (WQL), eine SQL-ähnliche Abfragesprache für das Windows Management Instrumentation. Beispielsweise könnte ein anderer Filter heißen:

```
select * from Win32_OperatingSystem where OSArchitecture="64-Bit"
```

Bei diesem Filter stellen Sie sicher, dass die Gruppenrichtlinie ausschließlich auf Computer mit einer 64-Bit-Version von Windows zum Einsatz kommt (zugegeben, es dürfte zunehmend schwieriger werden, überhaupt noch eine 32-Bit-Maschine zu finden).

Der wirklich große Vorteil von WMI-Filtern besteht darin, dass Administratoren nicht Unmengen von Gruppenrichtlinien erstellen müssen, sondern über einen dynamischen Prozess für eine gezielte Limitierung sorgen können.

Nun stellt sich die Frage: Woher soll ich alle Klassen, Objekte und Eigenschaften von WMI in Erfahrung bringen? Bei gefühlten Tausenden von Attributen ist die Suche wahrlich nicht einfach. Zudem unterscheiden sich die Bezeichner zwischen der älteren WMIC-Konsolen-Software und der modernen PowerShell-Syntax. Wer hat also nun recht?



Zwei gute Hilfsmittel im Umgang mit WMI sind: WMI Code Creator 1.0 von Microsoft (<https://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=8572>) und der WMI multi Query von Tools4Net, zu finden unter (<https://www.tools4net.de/index.php/wmimulti.html>).

Beim Erstellen von WQL-Abfragen muss der Administrator sicherstellen, dass das Ergebnis kein Array zurückgibt, also keine Gruppe von Werten. Praktischerweise liefert der Select einen Wert, den der Filter dann als »True« identifiziert. Kommt kein Ergebnis vom Select zurück, so interpretiert der Filter dies als »False«.

Leider gibt es keine einfache Art und Weise, die Filter mit Bordmitteln zu testen. Aber es gibt im Internet ein Freeware-Tool, das diese Aufgabe mit Bravour meistert – »WMI Filter Validation Utility«, zu sehen im Einsatz in [Abbildung 16.7](#).

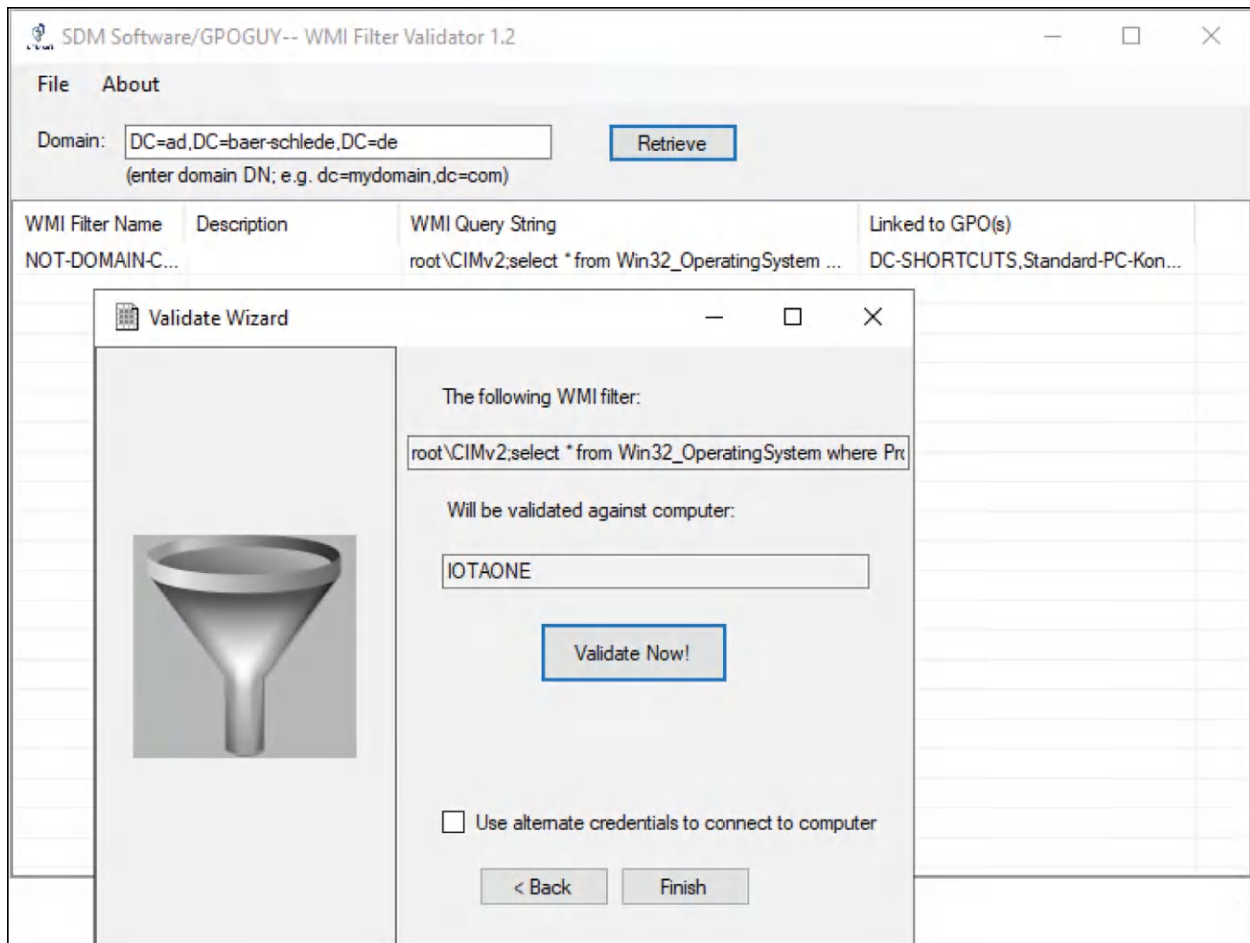


Abbildung 16.7: Das WMI Filter Validation Utility ersetzt die fehlende Testfunktion für WQL-basierte Filter.



Die Download-Adresse für das »WMI Filter Validation Utility« von sdm Software lautet <https://sdmsoftware.com/389932-gpo-freeware-downloads/>.

Neben der Auswahl des Filters selbst können Sie alternativ auch den Computernamen eingeben, gegen den der Filter zu prüfen ist.

Hübsch im Konzept der negierten Ausdrucksweise, liefert der Filter

```
select * from Win32_OperatingSystem where ProductType <>"2"
```

gegen einen Domänencontroller geprüft ein »False«, da es sich ja um ein ProductType 2 handelt.

Es gibt noch einen Filter, der in der Praxis öfter zum Einsatz kommt, der aber schon so manchen Administrator gefühlt an den Rand der Verzweiflung gebracht hat: Wie finde ich raus, ob es sich bei dem Gerät um einen Laptop handelt? Windows liefert hierfür kein vordefiniertes Attribut, und keines der vielen Hardware-Merkmale bietet sich zunächst an. Die wirklich einfachste Art, um Laptops und andere tragbare Geräte zu identifizieren, ist:

```
Select * from Win32_Battery
```

Ziemlich einfach – aber funktionell!

Anwendungsfall	Statement
Deutschsprachiges Tastaturlayout	SELECT * FROM Win32_OperatingSystem WHERE CountryCode = '49'
Computernamen beginnt mit win	SELECT * FROM Win32_ComputerSystem WHERE Name LIKE 'win%'
Windows-Client-Computer / Workstation	SELECT * FROM Win32_OperatingSystem WHERE ProductType = '1'
Windows-Member-Server, keine DC	SELECT * FROM Win32_OperatingSystem WHERE ProductType = '3'
Windows Vista und höher	SELECT * FROM Win32_OperatingSystem WHERE BuildNumber > '5000'
Netzwerkkarte von Realtek	SELECT * FROM Win32_NetworkAdapter WHERE MACAddress LIKE '00:E0:4C%'

Tabelle 16.1: Typische WQL-Statements für WMI-Filter

Noch ein paar klassische Beispiele – siehe [Tabelle 16.1](#).



Gern würden wir auch ein WQL-Statement für die Identifikation von Cisco- oder Broadcom-Netzwerkkarten abdrucken, jedoch verwenden die beiden Hersteller eine solche Unsumme an MAC-Präfixen, dass dies den Rahmen sprengen würde. Eine passende Suchfunktion – hier vorbelegt mit Cisco – finden Sie unter:

Zielgruppenadressierung

Nun, da wir verschiedene Möglichkeiten der WMI-basierten Filter im Zusammenhang mit Gruppenrichtlinien gesehen haben, stellt sich dem praxiserprobten Administrator zwangsläufig eine Frage: »Wie soll ich über eine solche Zuordnung Drucker systemspezifisch verbinden?«

Diese Fragestellung ist vollkommen berechtigt – wir setzen hier stillschweigend voraus, dass Sie eine Verbindung von Druckern zu Arbeitsplätzen auf Computerbasis und nicht auf Benutzerbasis wünschen.

Wir kennen viele Umgebungen, in denen genau dies erforderlich ist. Eher mobil arbeitende Benutzer melden sich an verschiedenen Computerarbeitsplätzen an und möchten stets den Ausdruck an dem Drucker erzeugen, der dem PC am nächsten steht.

Glücklicherweise ist es für ein solches Szenario nicht erforderlich, eine unendliche Kette von verschachtelten WMI-Filtern aufzubauen, sondern es ist die Funktion der Zielgruppenadressierung zu verwenden – im Englischen lautet die Bezeichnung »Item Level Targeting« (ITL).

Die Funktionalität eröffnet sich anhand eines Beispiels für Drucker – Sie können ITL jedoch an vielen Stellen verwenden.

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm GRUPPENRICHTLINIENVERWALTUNG.
4. Klicken Sie auf den Ordner GRUPPENRICHTLINIENOBJEKTE.
5. Erstellen Sie ein neues Gruppenrichtlinienobjekt oder wählen Sie ein bereits erstelltes Objekt aus. Klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie im Kontextmenü den Befehl BEARBEITEN aus.
6. Es öffnet sich der GRUPPENRICHTLINIEN-EDITOR. Wählen Sie

unter COMPUTERKONFIGURATION den Ordner EINSTELLUNGEN und öffnen Sie das Element SYSTEMSTEUERUNGSEINSTELLUNGEN.

7. Öffnen Sie den Eintrag DRUCKER durch einen Doppelklick.
8. Klicken Sie mit der rechten Maustaste in das Fenster und wählen Sie aus dem Kontextmenü den Befehl NEU | TCP/IP-DRUCKER.
9. Sparen Sie sich das Aktualisieren und füllen Sie das Fenster mit den erforderlichen Informationen für einen Druckerzugriff aus. In unserem Fall selektieren wir die Option DNS-NAMEN VERWENDEN, geben den Namen des DC ein, wählen als lokalen Namen den Freigabennamen und im Druckpfad alle Angaben noch einmal in UNC als *\\Servername\Freigabename*.
10. Nun zum entscheidenden Teil für die Zielgruppenadressierung! Hierzu öffnen Sie die Registerkarte GEMEINSAME OPTIONEN.
11. Aktivieren Sie die Option ZIELGRUPPENADRESSIERUNG AUF ELEMENTEBENE. Daraufhin wird die Schaltfläche ZIELGRUPPENADRESSIERUNG... nutzbar. Klicken Sie an.
12. Es öffnet sich der Dialog ZIELGRUPPENADRESSIERUNGSEEDITOR.
13. Klicken Sie auf die Schaltfläche oben links mit der Bezeichnung NEUES ELEMENT, um eine Auswahlliste zur Ansicht zu bringen.
14. Wählen Sie den Eintrag COMPUTERNAMEN. Die Auswahl wird direkt in das Fenster eingeblendet. Der angezeigte »Satz« lautet nun »Computername des NetBIOS ist ...« Vervollständigen Sie den Eintrag durch eine manuelle Eingabe oder über eine Auswahl über die Schaltfläche mit den drei Punkten.
15. Wählen Sie erneut die Schaltfläche oben links mit der Bezeichnung NEUES ELEMENT, um eine Auswahlliste zur Ansicht zu bringen.
16. Wählen Sie den Eintrag TERMINALSITZUNG aus.
17. Wählen Sie als Parameter die Auswahl CLIENTNAMEN und geben Sie den Namen erneut in das Eingabefeld ein.
18. Drücken Sie unbedingt auf der Tastatur die Taste , um das

entstandene Satzkonstrukt von

»Computernamen des NetBIOS ist *Computernamen* AND
Terminalsession ist beliebig mit Computernamen = *Computernamen*«

in

»Computernamen des NetBIOS ist *Computernamen* OR Terminalsession
ist beliebig mit Computernamen = *Computernamen*«

umzustellen (siehe [Abbildung 16.8](#)).

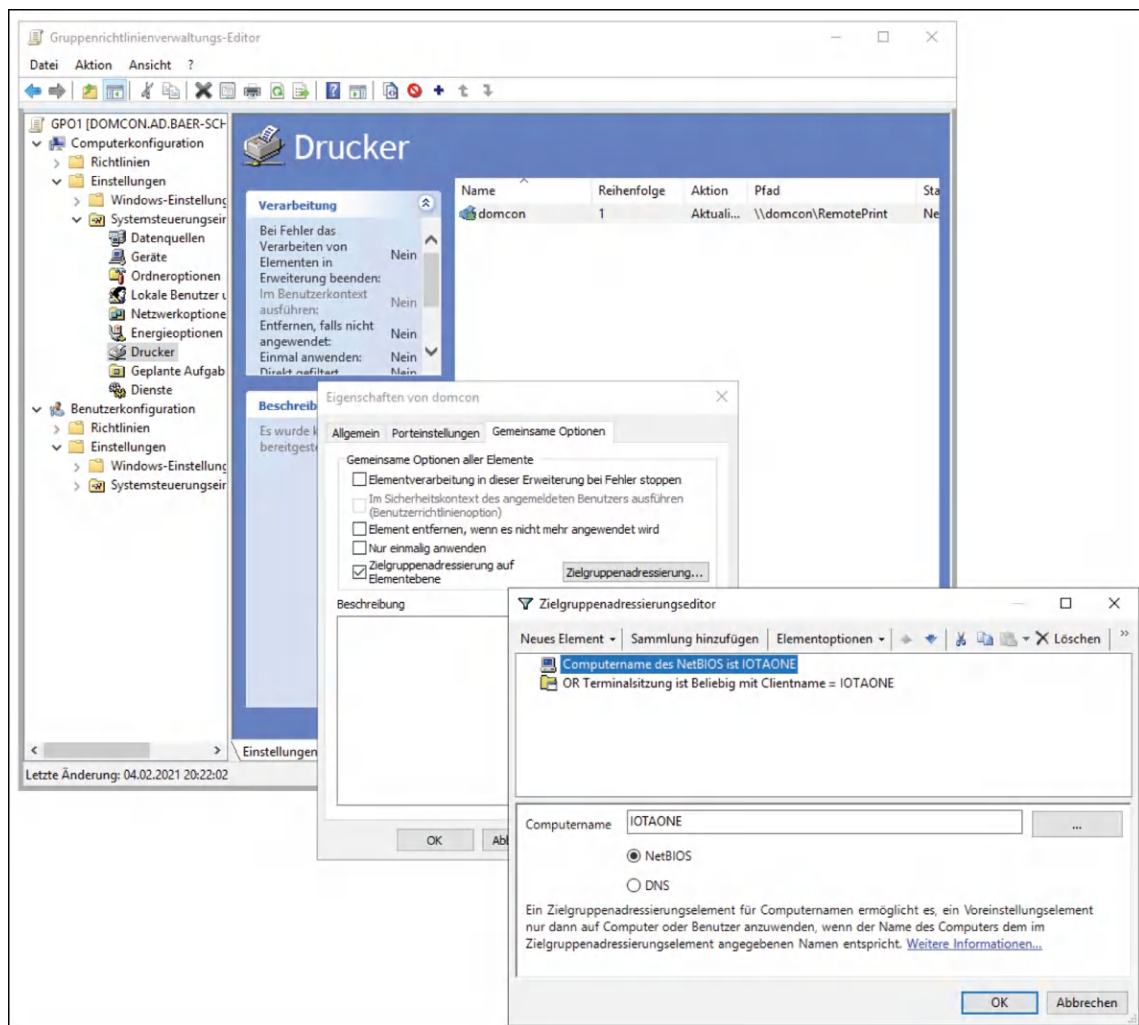


Abbildung 16.8: Zielgruppenadressierung mit zwei Eigenschaften in einer ODER-Verknüpfung.



Bei der Anlage mehrerer Elemente legt Windows als Verknüpfung stets den Boolean-Wert »UND« an. Durch die Taste **F6** wechseln

Sie in eine ODER-Verknüpfung. Alternativ verwenden Sie einen Rechtsklick mit Auswahl des Befehls ELEMENTOPTIONEN, um eine boolesche Variable auszuwählen.

Mit der oben beschriebenen Zielgruppenadressierung stellen wir sicher, dass ein Computer mit dem gewählten Namen den gewünschten Drucker zugewiesen bekommt. Auch in einer Remotedesktop-Session, bei der der Computernamen als Clientname durchgereicht wird, greift die Richtlinie entsprechend, und auch auf dem Terminalserver wird der Drucker verbunden.

Natürlich ist es auch möglich, verschiedene Computernamen in der Druckerzuweisung zu berücksichtigen. Hier gilt es wieder, mit der ODER-Verknüpfung zu arbeiten.



Die Zielgruppenadressierung richtet keine Rechte ein! Sofern der Benutzer kein Recht hat, eine Ressource, in diesem Fall den Drucker, zu verwenden, nützt auch die Zuordnung per Gruppenrichtlinienzielgruppenadressierung nichts.

Administrative Vorlagen

Für die Konfiguration von GPOs können Sie als Administrator sogenannte administrative Vorlagen verwenden. In diesen Vorlagen sind bereits viele Einstellungsmöglichkeiten für unterschiedliche Einstellungen vorhanden und, das ist beinahe noch wichtiger, dokumentiert.

Schauen wir uns eine solche Vorlage einmal näher an, indem wir zu dem hier beschriebenen Beispiel eine weitere Einstellung auf Benutzerkonfigurationsbasis hinzufügen:

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm GRUPPENRICHTLINIENVERWALTUNG.
4. Wählen Sie in der Baumstruktur den Eintrag der gewünschten

Organisationseinheit, in unserem Beispiel »GPOTEST«. Klicken Sie in der rechten Fensterhälfte in der Registerkarte VERKNÜPFTE GRUPPENRICHTLINIENOBJEKTE das gewünschte Gruppenrichtlinienobjekt, hier GPO1, an und wählen Sie aus dem Kontextmenü den Befehl BEARBEITEN.

5. Wählen Sie unter BENUTZERKONFIGURATION den Ordner RICHTLINIEN.

6. Öffnen Sie ADMINISTRATIVE VORLAGEN und darunter DESKTOP.

Im Detailbereich erscheint eine Auflistung von Einstellungen ([Abbildung 16.9](#)).

7. Wählen Sie den Eintrag PAPIERKORBSYMBOL VOM DESKTOP entfernen.

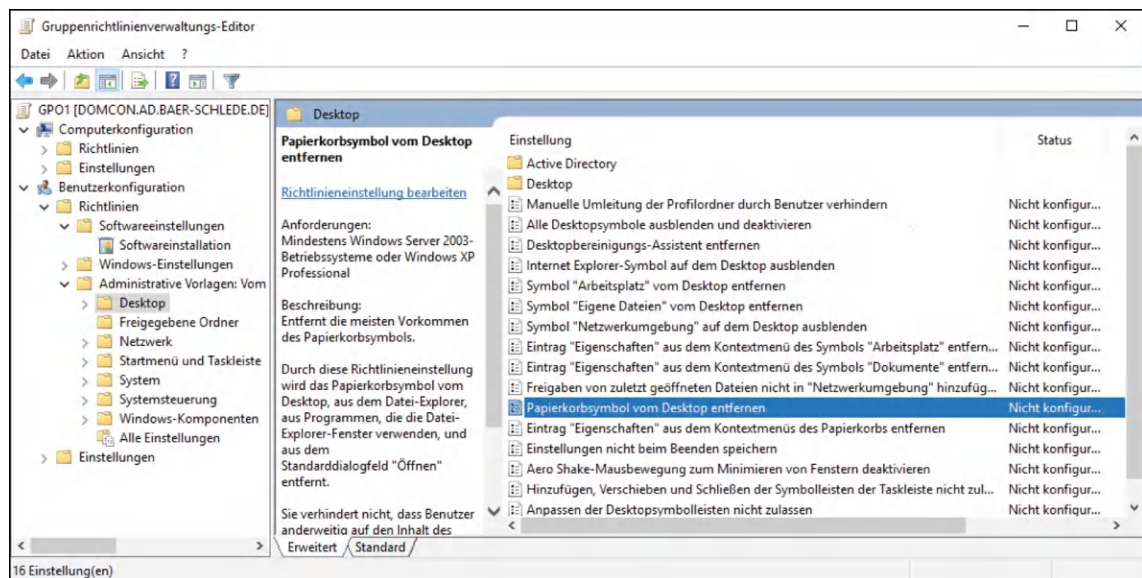


Abbildung 16.9: Administrative Vorlagen erlauben eine einfache Einstellungssteuerung.

8. Nach einem Doppelklick öffnet sich der entsprechende Konfigurationsdialog. Aufgrund der Hilfetexte erklären sich die administrativen Vorlagen beinahe von selbst. Es gibt zumeist drei Optionen: NICHT KONFIGURIERT, AKTIVIERT oder DEAKTIVIERT. In unserem Beispiel wählen wir AKTIVIERT, um den Papierkorb vom Desktop zu entfernen.



Administrative Vorlagen sind sprachenunabhängig, auch wenn Hilfe- und Dialogtexte etwas anderes erahnen lassen.

Praktischerweise empfiehlt es sich für Administratoren, eine Anpassung mit einem Kommentar zu versehen.

Die gesamte Thematik der administrativen Vorlagen und Gruppenrichtlinien hat Microsoft »verkompliziert«: Seit der Festlegung, dass Windows 10 für sehr viele Windows-Versionen als Name erhalten blieb und nur durch regelmäßige Builds vom Hersteller aktualisiert wird, ist es für den Administrator schwieriger geworden, da mit jedem neuen Build auch die Anzahl der verwendbaren Gruppenrichtlinien tendenziell steigt. Wiederum gibt es eine deutlichere Trennung der möglichen Anpassungsmöglichkeiten je nach Edition. Windows 10 Pro unterstützt wesentlich weniger Gruppenrichtlinien-Einstellungen als Windows 10 Enterprise. Dazu gehört etwa das Deaktivieren des Stores oder die Anpassung des Startmenüs. Die volle Steuerbarkeit, wie sie einst mit Windows XP/7 Professional möglich war, bleibt heute den Education- und Enterprise-Editionen von Windows 10 vorbehalten. Wie sich die Benennung mit Windows 11 verhält, ist zum Zeitpunkt der Manuskripterstellung noch nicht klar.

Ob eine Einstellung steuerbar ist, erkennt der Administrator am Eintrag UNTERSTÜTZT AUF: – siehe [Abbildung 16.10](#)

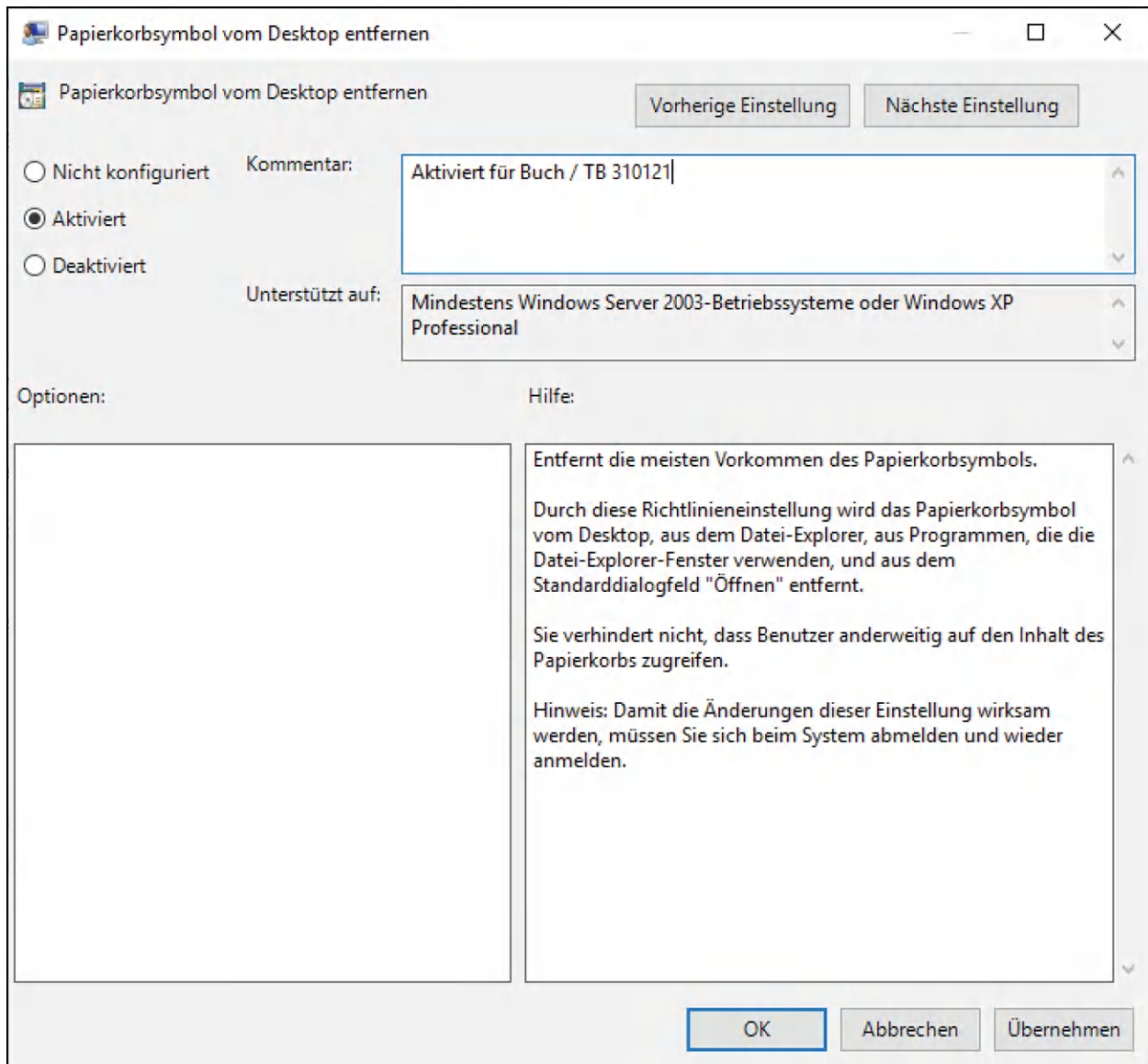


Abbildung 16.10: Das Dialogfenster für administrative Vorlagen

Alle Richtlinien, Erklärungstexte, Anforderungen und Oberflächeninteraktionen von Gruppenrichtlinien, die mithilfe des Gruppenrichtlinieneditors und auf einer administrativen Vorlage definiert wurden, basieren auf sogenannten ADMX-Dateien. Die Einstellungen selbst, die im Bereich der administrativen Vorlagen vorgenommen wurden, werden nicht in den ADMX-Dateien gespeichert, sondern in den sogenannten registry.pol-Dateien. Diese befinden sich in den entsprechenden Ordnern im SYSVOL-Verzeichnis.

Central Store

Werden administrative Vorlagen verändert oder erweitert, sind die entsprechenden Einstellungen nur dann für alle Client-Systeme in der Domäne sichtbar, wenn diese über einen sogenannten Central Store zur Verfügung gestellt werden. Der Central Store dient dabei als zentrale Quelle für alle ADMX- und ADML-Dateien, die zum Bearbeiten der Gruppenrichtlinien zur Verfügung stehen. In dieser einmal erstellt, werden lediglich die zu verwendenden ADMX-Dateien sowie zu unterstützenden ADML-Dateien in den Central Store kopiert. Der Central Store befindet sich im SYSVOL-Verzeichnis der Domänencontroller und wird automatisch über die Domäne repliziert.

Moderne Windows-Client- und -Server-Computer prüfen beim Öffnen einer Gruppenrichtlinie mit dem Gruppenrichtlinienverwaltungs-Editor, ob ein Central Store auf den DCs existiert, und verwenden diesen automatisch. Nur wenn es keinen Central Store gibt, finden die lokalen administrativen Vorlagen Anwendung.

So erstellen Sie einen Central Store in Ihrer Domäne:

1. Navigieren Sie mit dem Windows-Explorer zu dem Pfad *\\Name des Domänencontrollers\SYSVOL\Name der Domäne\Policies*.
2. Erstellen Sie einen Ordner mit Namen *PolicyDefinitions*.
3. Kopieren Sie den Inhalt aus dem lokalen Ordner des DC unter *%windir%\PolicyDefinitions* in den soeben erstellten Ordner.

Ob ein Computer beim Öffnen des Gruppenrichtlinienverwaltungs-Editors auf die administrativen Vorlagen im Central Store oder auf die Vorlagen aus dem lokalen Verzeichnis zugreift, sehen Sie an der Erweiterung des Ordernamens unter »Administrative Vorlagen«.

Handlungsempfehlung für Gruppenrichtlinien

Unglücklicherweise gibt es kein allgemein gültiges Patentrezept für die richtige Anwendung von Gruppenrichtlinien. Was in einem Anwendungsfall sinnvoll und vertretbar ist, entscheidet ganz allein das Szenario und das Know-how der Mitarbeiter, die mit der Verwaltung der Gruppenrichtlinien betraut sind. Das massive Schachteln von Gruppenrichtlinien erfordert von Administratoren eine höhere Aufmerksamkeit, und möglicherweise ist es klüger, kleinere und überschaubarere Varianten zu wählen.

Üblicherweise gilt die Empfehlung, die »Default Domain Policy«, quasi die von Microsoft vorgegebene Grundlage, nicht zu verändern, um im Zweifelsfall auf den »garantiert funktionierenden Urzustand« zurückspringen zu können. Wer sich bei der Änderung jedoch auf eine angepasste Kennwortrichtlinie beschränkt, dürfte in der GRUPPENRICHTLINIENVERWALTUNG keinen größeren Schaden anrichten, der die Domäne in einen unkontrollierbaren Zustand bringt. Alle anderen Anpassungen sollten jedoch in explizit dafür angelegten und zugewiesenen Richtlinien geschehen.



Ein guter Rat von der Webseite www.gruppenrichtlinien.de von Mark Heitbrink zur »Default Domain Policy« lautet »Ich ändere, was drin ist, aber ich füge nichts hinzu.«.

Es gibt kein »Jetzt« bei Gruppenrichtlinien, was angesichts von Installationen mit mehreren Tausend PCs in einem international verteilten Unternehmen auch logisch ist. Wird eine Richtlinie angepasst, vergehen mehrere Minuten, bis diese zur Anwendung kommt. Bei der Anmeldung an eine Windows-Sitzung, also während ihrer Initialisierung, fragt das lokale Windows-Betriebssystem die Einstellungen aktiv an. Während der Verarbeitung der Computerrichtlinien ist keine Benutzeroberfläche sichtbar und nutzbar.

Nach der Authentifizierung durch den Benutzer wendet das Betriebssystem die Benutzerrichtlinien an. Dieser Reihenfolge zum Trotz haben Computerrichtlinien in der Grundeinstellung Vorrang vor Benutzerrichtlinien. Gruppenrichtlinien werden standardmäßig aktualisiert, sobald sich ein Benutzer abmeldet oder der Computer neu

startet. Zudem kommt es in einem Intervall von 90 bis 120 Minuten zu einer automatischen Aktualisierung der Einstellung. Domänencontroller aktualisieren sich alle fünf Minuten.

Sie können das Update-Intervall anpassen, sollten jedoch stets bedenken, dass ein zu rasches Intervall möglicherweise negative Auswirkung auf Anwender haben könnte. Sie finden die Einstellungen unter: COMPUTER | BENUTZER-KONFIGURATION | ADMINISTRATIVE VORLAGEN | SYSTEM | GRUPPENRICHTLINIE | GRUPPENRICHTLINIEN-AKTUALISIERUNGSINTERVALL FÜR COMPUTER FESTLEGEN

Sie können das Intervall über einen Minutenwert anpassen. Microsoft erklärt diese Aktualisierungs-GPO für die Computerkonfiguration wie folgt:



Diese Richtlinieneinstellung legt fest, wie oft Gruppenrichtlinien für Computer (im Hintergrund) aktualisiert werden, wenn der Computer verwendet wird. Diese Richtlinieneinstellung gibt die Hintergrundaktualisierungsrate nur für Gruppenrichtlinien im Ordner »Computerkonfiguration« an.

Zusätzlich zu den Hintergrundaktualisierungen wird die Gruppenrichtlinie für den Computer bei jedem Systemstart aktualisiert.

Standardmäßig werden Computergruppenrichtlinien alle 90 Minuten im Hintergrund (mit einem zufälligen Versatz von 0 bis 30 Minuten) aktualisiert.

Wenn Sie diese Einstellung aktivieren, können Sie eine Aktualisierungsrate von 0 bis 64.800 Minuten (45 Tage) angeben. Wenn Sie 0 Minuten angeben, wird eine Aktualisierung alle 7 Sekunden angestrebt. Da Aktualisierungen jedoch die Benutzer beim Arbeiten beeinträchtigen und zu einer Erhöhung des Netzwerkdatenverkehrs führen können, sind sehr kurze Aktualisierungsintervalle für die meisten Installationen nicht geeignet.

Wenn Sie diese Einstellung deaktivieren, werden Gruppenrichtlinien alle 90 Minuten (dies ist der Standardwert) aktualisiert. Verwenden Sie die Richtlinie »Hintergrundaktualisierung der Gruppenrichtlinien deaktivieren«, wenn die Gruppenrichtlinien nie aktualisiert werden sollen, während der Computer verwendet wird.

Mit der Richtlinieneinstellung »Gruppenrichtlinien-Aktualisierungsintervall für Computer festlegen« können Sie außerdem angeben, inwieweit das tatsächliche Aktualisierungsintervall variiert. Das Aktualisierungsintervall unterscheidet sich von Client zu Client um eine zufällige Anzahl von Minuten, damit Clients mit demselben Aktualisierungsintervall nicht gleichzeitig Aktualisierungen anfordern. Mithilfe der von Ihnen im Feld für die Zufallszeit eingegebenen Zahl wird die Obergrenze für den Schwankungsbereich festgelegt. Wenn Sie beispielsweise 30 Minuten eingeben, wird vom System eine Schwankung von 0 bis 30 Minuten ausgewählt. Wenn Sie einen hohen Wert eingeben, wird eine hohe Schwankungsbreite verwendet, sodass es unwahrscheinlich ist, dass sich Client-Anforderungen überschneiden. Allerdings können Aktualisierungen dadurch erheblich verzögert werden.

Diese Einstellung bestimmt eine Aktualisierungsrate für die Computergruppenrichtlinien. Verwenden Sie die Einstellung »Gruppenrichtlinien-Aktualisierungsintervall für Benutzer festlegen« (unter BENUTZERKONFIGURATION | ADMINISTRATIVE VORLAGEN | SYSTEM | GRUPPENRICHTLINIEN), wenn Sie eine Aktualisierungsrate für Benutzerrichtlinien festlegen möchten.

Diese Einstellung wird nur angewendet, wenn die Richtlinieneinstellung HINTERGRUNDAKTUALISIERUNG DER GRUPPENRICHTLINIEN DEAKTIVIEREN nicht aktiviert ist.



Einige Benutzereinstellungen, wie zum Beispiel die Ordnerumleitung, können von Windows zur Laufzeit nicht geändert werden, solange der Benutzer angemeldet ist. Wiederum andere Computereinstellungen erfordern zwingend einen Neustart.

Viele mittlere und große Unternehmen verwenden zur Bereitstellung von Client-Computern sogenannte »Endpoint-Management-Systeme« (vormals Client-Lifecycle-Management-(CLM-)Lösungen). Wer eine solche Software zur Ferninstallation von Betriebssystemen und Softwarepaketen sein Eigen nennt, hat faktisch eine weitere Möglichkeit, um Einstellungen für Computersysteme auszubringen. Die Verwendung dieser Produkte bietet zumeist den Charme, dass eine Einstellung wirklich »jetzt sofort« greift.

Nachteilig ist jedoch, dass der Administrator sicherstellen muss, dass der Agent für die Software auf dem Server oder PC auch wirklich aktiv ist – das Basis-Windows arbeitet immer mit den lokalen Gruppenrichtlinien oder denen der Domäne zusammen.

Praktische Empfehlungen

Im Zuge dieses Kapitels wurden im Zusammenspiel mit WMI-Filter und der Zielgruppenadressierung schon einige Beispiele aus der Praxis aufgeführt. Diesbezüglich sind Sie als Leser quasi im »Flow«, daher sollen noch weitere Szenarien folgen.

Anmeldung am Computer verweigern

In der Standardeinstellung von Windows und der Domäne kann sich ein Domänenbenutzer über die Kombination Benutzername und Kennwort an jedem Domänencomputer anmelden. Über die Benutzerprofile und die Zugriffsrechte auf Ressourcen ist das normalerweise auch überhaupt kein Problem. Jedoch gibt es, wenn auch eher selten, Programme die ihre Daten nicht anhand von Windows-Berechtigung ausrichten. Schlussendlich – Sie müssen als Administrator dafür sorgen, dass sich an den Computern der Geschäftsführung auch nur Gruppenmitglieder der Geschäftsführung anmelden können.

Für dieses Szenario brauchen wir zwei Voraussetzungen:

- ✓ Eine Organisationseinheit für die Computer der Geschäftsführung.
- ✓ Eine Gruppe für die Mitglieder Geschäftsführung.

Die Einrichtung geschieht, wie gewohnt, über die Gruppenrichtlinienverwaltung:

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm GRUPPENRICHTLINIENVERWALTUNG.
4. Selektieren Sie mit der rechten Maustaste in der Baumstruktur die gewünschte Organisationseinheit – in unserem Beispiel »Geschäftsführung«.
5. Klicken Sie auf den Befehl GRUPPENRICHTLINIENOBJEKT HIER ERSTELLEN UND VERKNÜPFEN... aus dem Kontextmenü.
6. Benennen Sie das Objekt nach Ihren Vorstellungen, zum Beispiel ANMELDUNG_NUR_GF. Klicken Sie mit der rechten Maustaste auf das soeben erzeugte Objekt in der Auflistung und wählen Sie den Befehl BEARBEITEN aus dem Kontextmenü.
7. Öffnen Sie folgenden Zweig: COMPUTERKONFIGURATION | RICHTLINIEN | WINDOWS-EINSTELLUNGEN | SICHERHEITSEINSTELLUNGEN | LOKALE RICHTLINIEN | ZUWEISEN VON BENUTZERRECHTEN.
8. Doppelklicken Sie den Eintrag LOKAL ANMELDEN ZULASSEN.
9. Aktivieren Sie die Option DIESE RICHTLINIENEINSTELLUNGEN DEFINIEREN.
10. Klicken Sie auf die Schaltfläche BENUTZER ODER GRUPPEN HINZUFÜGEN... und fügen Sie die im Vorfeld definierte Gruppe, in unserem Beispiel »Geschäftsführung« hinzu. Fügen Sie zusätzliche die Gruppe der »Administratoren« hinzu, da ansonsten die Aktivierung nicht funktioniert ([Abbildung 16.11](#)). Schließen Sie die Auswahl mit OK ab.



Durch die Zuweisung des expliziten Rechts zur Anmeldung wird automatisch ein Anmeldeverbot für die anderen Domänenbenutzer

erreicht.

Somit ist die Einrichtung der besonderen Gruppenrichtlinie, die die Anmeldung von »normalen Domänenbenutzern« verhindert, bereits abgeschlossen. Idealerweise testen Sie vor der Verwendung solcher Einschränkungen die Richtlinie in einer Testumgebung – bei uns funktionierte es auf Anhieb ([Abbildung 16.12](#)).



Wird diese Richtlinie versehentlich auf eine falsche Organisationseinheit oder auf alle Computer angewandt, kann sich die Mehrheit der Benutzer nicht mehr anmelden.

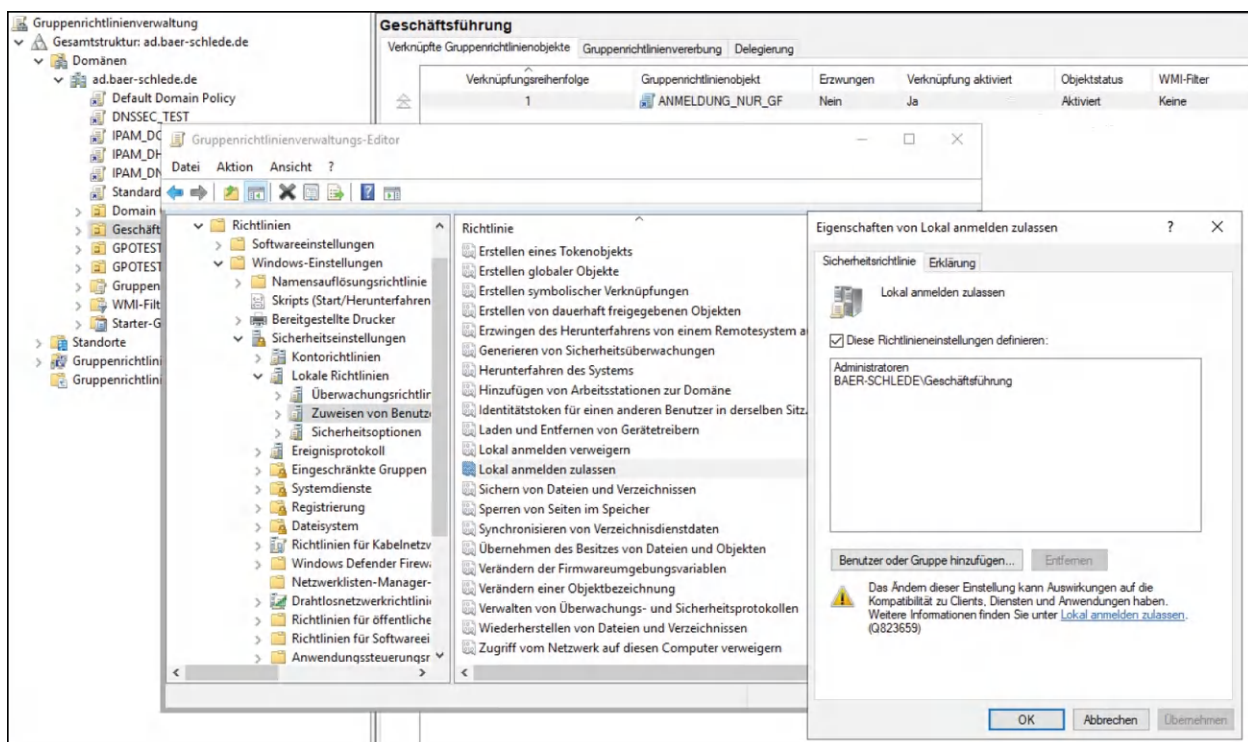


Abbildung 16.11: Mithilfe der expliziten Zuweisung von Anmelderechten wird die Anmeldung von anderen Domänenbenutzern ausgeschlossen.



Abbildung 16.12: Nur bestimmte Personen dürfen sich an diesem Computer anmelden.



Neben der Richtlinie »Lokal anmelden zulassen« existiert auch eine Richtlinie »Lokal anmelden verweigern«. Diese ist aber nur dann sinnvoll im Einsatz, wenn Sie einzelnen Benutzern die Anmeldung am Computer verweigern möchten.

Desktophintergrundbild festlegen

Die Festlegung des Desktophintergrundbilds ist ein wahrer Klassiker unter den Gruppenrichtlinien. Insbesondere Firmen haben eine Vorliebe dafür, der Individualisierung der Arbeitsumgebung durch striktere Vorgaben einen Strich durch die Rechnung zu machen.

Unsere dringende Empfehlung: Bevor Sie auf die Idee kommen, den Domänenbenutzern ein verbindliches Hintergrundbild »aufzudrücken«, stellen Sie sicher, dass Sie für eine solche Maßnahme die entsprechende Rückendeckung der Geschäftsführung oder Unternehmensleitung haben.



Der heutige Begriff der Individualität leitet sich vom lateinischen Adjektiv *individuus* ab, was so viel wie unteilbar bedeutet. Entsprechend lässt sich bei der Individualität von der »Ungeteiltheit«

oder auch Unteilbarkeit sprechen. Der Wunsch nach Individualität ist in unserem Kulturkreis stark verankert.

Die Einrichtung einer Gruppenrichtlinie ist schneller erledigt, als die Rahmenbedingungen zu klären sind. Sie brauchen in jedem Fall ein JPEG- oder BMP-Bild in einer ausreichend hohen Auflösung an einem Speicherort, auf den Benutzer zugreifen können.

In unserem Fall handelt es sich um eine Datei auf dem Domänencontroller, die sich in einem freigegebenen Ordner mit Leserechten für Domänenbenutzer und der Gruppe »Jeder« befindet:

\\domcon.ad.baer-schlede.de\open\background.jpg



Unsere Versuche, das Bild über das SYSVOL-Verzeichnis über einen beliebigen Domänencontroller anzusprechen, sind allesamt gescheitert.

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm GRUPPENRICHTLINIENVERWALTUNG.
4. Selektieren Sie mit der rechten Maustaste in der Baumstruktur die gewünschte Organisationseinheit oder die Domäne und wählen Sie die gewünschte Gruppenrichtlinie. In unserem Beispiel lautet der Name »Standard-PC-Konfiguration«. Klicken Sie im Kontextmenü nach einem Rechtsklick auf den Befehl BEARBEITEN.
5. Öffnen Sie den Ordner RICHTLINIEN unter Benutzerkonfiguration.
6. Öffnen Sie den Ordner ADMINISTRATIVE VORLAGEN.
7. Öffnen Sie DESKTOP und anschließend noch einmal DESKTOP.
8. Doppelklicken Sie das Element DESKTOPHINTERGRUND.



Um diese Einstellung zu verwenden, geben Sie den vollqualifizierten Pfad und den Namen der Datei ein, in der das

Hintergrundbild gespeichert ist. Sie können einen lokalen Pfad wie »C:\Windows\web\wallpaper\home.jpg« oder einen UNC-Pfad wie »\\Server\Freigabe\Corp.jpg« eingeben. Wenn die angegebene Datei bei der Benutzeranmeldung nicht verfügbar ist, wird kein Hintergrundbild angezeigt. Benutzer können kein alternatives Hintergrundbild angeben. Mit dieser Einstellung können Sie auch angeben, dass das Hintergrundbild zentriert, nebeneinander wiederholt oder gestreckt angezeigt werden soll. Benutzer können diese Festlegung nicht ändern.

9. Aktivieren Sie oben links die Option AKTIVIERT.
10. Fügen Sie den Pfad für das Bild unter HINTERGRUNDNAME ein. Sofern es sich um einen UNC-Pfad handelt, prüfen Sie mit dem Startmenübefehl »Ausführen«, ob der Pfad passt. Der Eintrag sollte dem in [Abbildung 16.13](#) entsprechen.

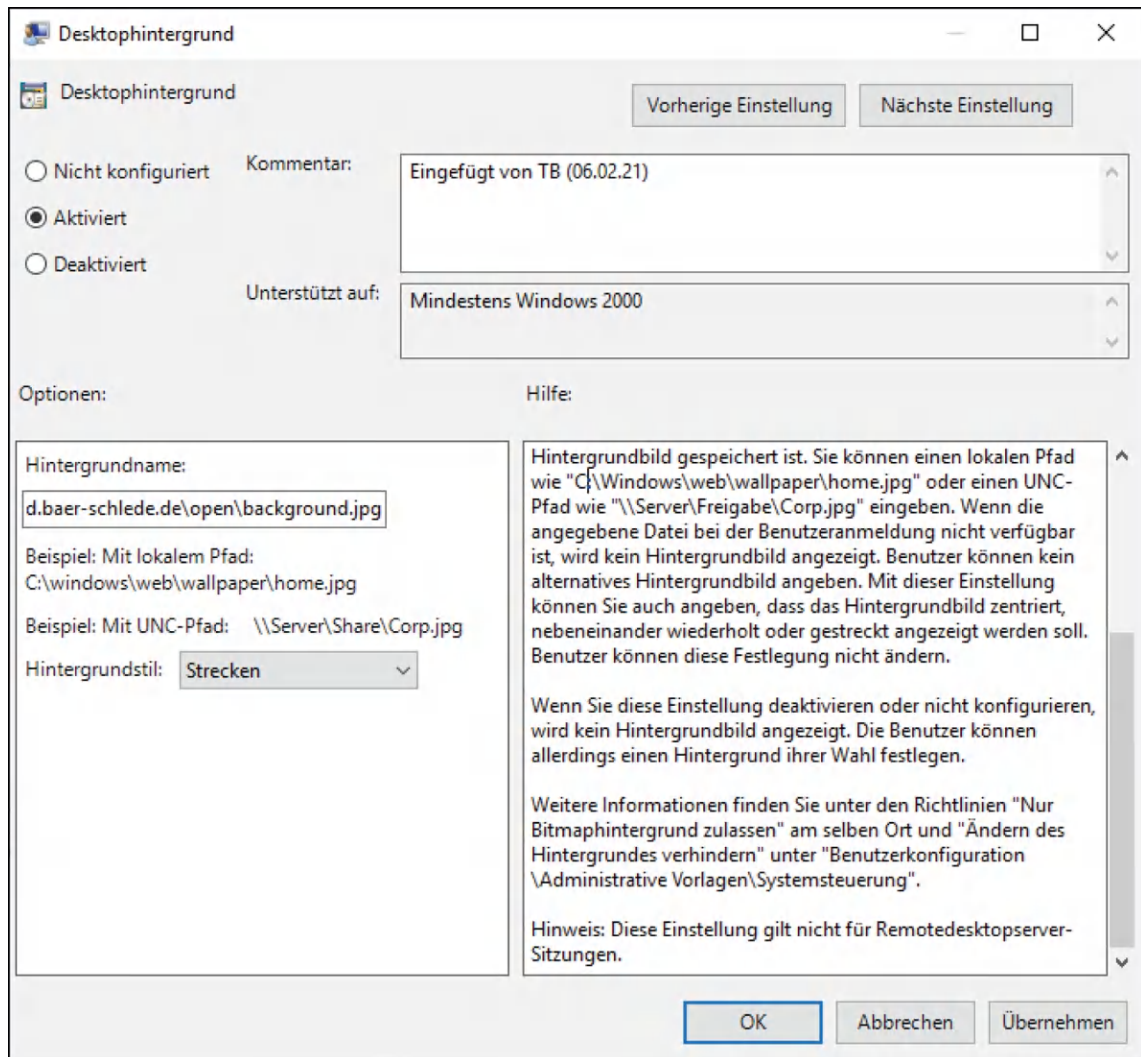


Abbildung 16.13: Ein Desktophintergrund, der per Gruppenrichtlinie festgelegt wurde

11. Bestätigen Sie die Anpassung mit OK.
12. Prüfen Sie die Funktionalität auf einem Desktop-PC.

Wie schon im letzten Satz des Infotexts zu lesen ist: Die Einstellung gilt nicht für Remotedesktop-Serververbindungen. Angesichts der Tatsache, dass ein komplexes Hintergrundbild bei der Übertragung von Bildinhalten über ein Netzwerk nur eine Belastung darstellt, ist das Fehlen dieser Funktion durchaus verständlich.

In Zeiten permanenten Streamens von hochauflösenden Videos über das Internet mag das nicht mehr nachvollziehbar sein. Aber: Die Latenz ist beim Streaming von Videodaten nicht so negativ spürbar wie die

Reaktionszeit bei einer Interaktion zwischen einer Anwendung des Benutzers und dem Desktop.

Administratoren können in einer Remotedesktop-Umgebung Hintergrundbilder generell abschalten. Die hierfür erforderliche Richtlinie finden Sie unter: COMPUTERKONFIGURATION | ADMINISTRATIVE VORLAGEN... | WINDOWS KOMPONENTEN | REMOTEDESKTOPDIENSTE | REMOTEDESKTOPSITZUNGS-HOST | UMGEBUNG FÜR REMOTESITZUNG | ENTFERNEN DES REMOTEDESKTOP ERZWINGEN.

Aktivieren Sie diese Richtlinie, und die Standardhintergrundbilder von Windows kommen auch nicht mehr zum Einsatz.

Sicherheitsrelevante Gruppenrichtlinien

In den vorherigen Abschnitten wurde die grundlegende Methodik der Konfiguration, Filterung und Zuweisung von Gruppenrichtlinien hinreichend dargestellt. Nutzen wir nun die Gelegenheit, einige äußerst spannende GPOs vorzustellen, die in einer auf Sicherheit ausgelegten Umgebung sicherlich von Interesse sind:

- ✓ Zugriff auf die Systemsteuerung verhindern – Setzen Sie dazu die Option »Aktiviert« über BENUTZERKONFIGURATION | RICHTLINIEN | ADMINISTRATIVE VORLAGEN | ZUGRIFF AUF SYSTEMSTEUERUNG UND PC-EINSTELLUNGEN NICHT ZULASSEN.
- ✓ Unterdrücken Sie die zusätzliche Zwischenspeicherung der Hash-Werte von Anmeldedaten (SAM) im sogenannten »LAN Manager von Windows«. Aktivieren Sie die Option unter: COMPUTERKONFIGURATION | RICHTLINIEN | WINDOWS-EINSTELLUNGEN | SICHERHEITSEINSTELLUNGEN | LOKALE RICHTLINIEN | SICHERHEITSOPTIONEN | KEINE LAN MANAGER-HASHWERTE FÜR NÄCHSTE KENNWORTÄNDERUNG SPEICHERN.
- ✓ Deaktivieren Sie die Möglichkeit, die SID von anonymen Konten aus aufzulisten: COMPUTERKONFIGURATION | RICHTLINIEN |

WINDOWS-EINSTELLUNGEN |
SICHERHEITSEINSTELLUNGEN | LOKALE RICHTLINIEN |
SICHERHEITSOPTIONEN | ANONYME AUFGÄBEN VON
SAM-KONTEN UND FREIGABEN NICHT ERLAUBEN. Sie
sollten diese Richtlinieneinstellung aktivieren.

- ✓ Deaktivieren Sie für Standardbenutzer die Eingabeaufforderung. Zwar berücksichtigt die Kommandozeile die Benutzerrechte, jedoch wird es durch das Ausschalten erschwert, unerwünschte Änderungen am System auszuführen. Sie schalten die Eingabeaufforderung wie folgt aus: BENUTZERKONFIGURATION | RICHTLINIEN | ADMINISTRATIVE VORLAGEN | SYSTEM | ZUGRIFF AUF EINGABEAUFFORDERUNG VERHINDERN ([Abbildung 16.14](#)) – Die Option, gleichzeitig die Ausführung von Batch-Jobs zu deaktivieren, wäre eine weitere Variante, die Betriebssicherheit Ihrer Umgebung zu erhöhen. In »gewachsenen Strukturen«, bei denen sich Mitarbeiter und Anwender mit höheren IT-Skills Abläufe in Form von Batch-Skripten erstellt haben, ist die Umsetzung der Deaktivierung nur im Dialog möglich.

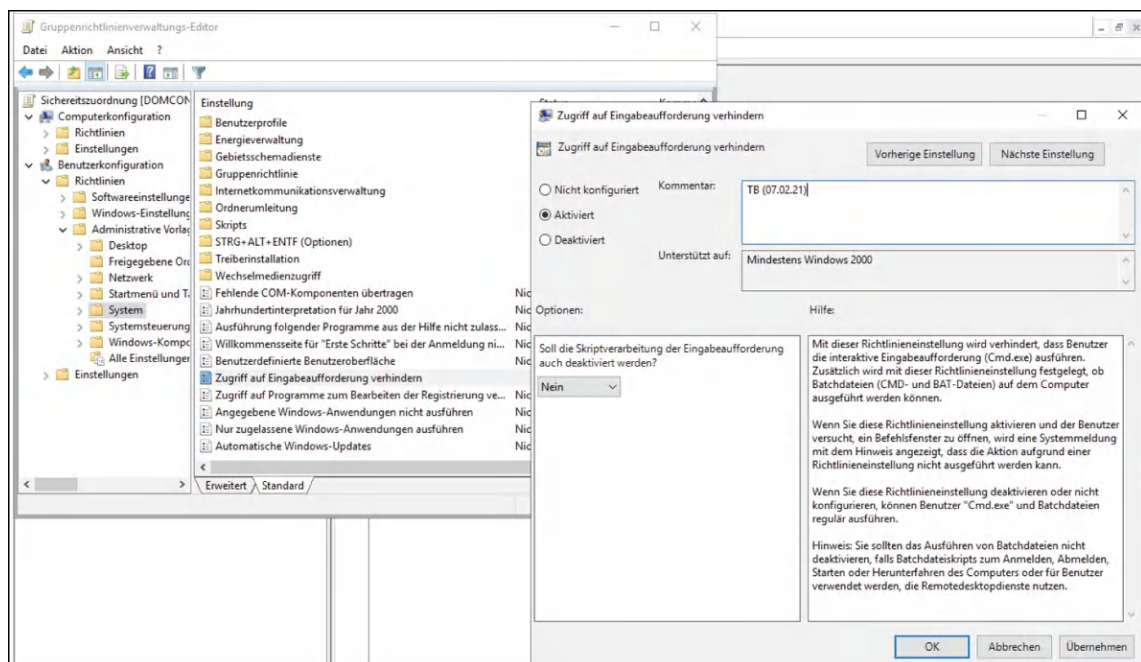


Abbildung 16.14: Windows bietet viele Möglichkeiten, die Sicherheit zu erhöhen: beispielsweise die Deaktivierung der Eingabeaufforderung für Standardbenutzer.

- ✓ Über einen recht einfachen Weg haben Sie die Möglichkeit, Wechseldatenträgerlaufwerke (CD, DVD, Diskettenlaufwerk (oh – wer hat sie noch?)) zu deaktivieren. Aktivieren Sie hierzu die GPO: BENUTZERKONFIGURATION | RICHTLINIEN | ADMINISTRATIVE VORLAGEN | SYSTEM | WECHSELMEDIENZUGRIFF | ALLE WECHSELMEDIENKLASSEN: JEGLICHEN ZUGRIFF VERWEIGERN.
- ✓ Deaktivieren Sie das Gastkonto komplett, sofern Sie keinen sinnvollen Einsatzzweck dafür haben. COMPUTERKONFIGURATION | RICHTLINIEN | WINDOWS-EINSTELLUNGEN | SICHERHEITSEINSTELLUNGEN | LOKALE RICHTLINIEN | SICHERHEITSOPTIONEN | GASTKONTENSTATUS.

Im nächsten Schritt gilt es, die Anforderungen bezüglich der Kennwörter zu erhöhen. Auf den ersten Blick scheint es zudem sinnvoll zu sein, die Anwender zur regelmäßigen Änderung der Passwörter zu »erziehen«. In der Praxis offenbart sich jedoch eine neue Erkenntnis: Zwingen wir den Anwender zu regelmäßiger Änderung der Passwörter, neigt dieser dazu, eher schwache Passwörter zu wählen, die er sich leichter merken kann.

Während die US-amerikanische Standardisierungsbehörde NIST im Jahr 2017 und die britische CESG bereits im Jahr zuvor die Empfehlung zur regelmäßigen Änderung gestrichen haben, brauchte das in Deutschland beheimatete BSI (Bundesamt für Sicherheit in der Informationstechnik) dazu bis zum Jahr 2020.

Empfehlungen für ein gutes Kennwort:

- ✓ Gut zu merken.
- ✓ Je länger, desto besser – mindestens acht Zeichen.
- ✓ Für ein Passwort können in der Regel alle verfügbaren Zeichen genutzt werden:
 - beispielsweise Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ?!%+...).

- 20 bis 25 Zeichen lang, und zwei Zeichenarten sollen genutzt werden (beispielsweise eine Folge von Wörtern). Es ist dann lang und weniger komplex.
 - 8 bis 12 Zeichen lang, und vier Zeichenarten sollen genutzt werden. Es ist dann kürzer und komplex.
- ✓ Nicht als Passwörter geeignet sind Namen von Familienmitgliedern, des Haustiers, des besten Freunds, des Lieblingsstars, Geburtsdaten und so weiter. Das vollständige Passwort sollte möglichst nicht in Wörterbüchern vorkommen. Es sollte zudem nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern wie »asdfgh« oder »1234abcd« bestehen. Manche Anbieter von Webseiten gleichen Passwörter beispielsweise gegen eine sogenannte »black list« ab, in der genau solche nicht geeigneten Passwörter hinterlegt sind. Möchte man sie nutzen, erhält man einen Hinweis, dass das Passwort in dieser Form nicht zugelassen wird beziehungsweise nicht sicher ist. Microsoft Windows gibt an dieser Stelle keinen Hinweis!



Alle bisherigen Anpassungen wurden stets außerhalb der »Default Domain Policy« vorgenommen. Die Einstellungen zu den Kennwortrichtlinien steuern die meisten Administratoren aber genau über die Standardrichtlinie.

Die Anpassung der Anforderungen bezüglich der Kennwörter erledigt der Administrator in einer Domäne ebenfalls über Gruppenrichtlinien:

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts im Menü den Befehl TOOLS.
3. Wählen Sie das Verwaltungsprogramm GRUPPENRICHTLINIENVERWALTUNG.
4. Wählen Sie unterhalb der Domänenbezeichnung in der Baumstruktur den Eintrag DEFAULT DOMAIN POLICY. Klicken Sie diese Standardrichtlinie mit der rechten Maustaste an und wählen Sie im Kontextmenü den Befehl BEARBEITEN.

5. Wechseln Sie in die COMPUTERKONFIGURATION und klicken Sie auf RICHTLINIEN.
6. Klicken Sie auf WINDOWS-EINSTELLUNGEN.
7. Doppelklicken Sie SICHERHEITSEINSTELLUNGEN.
8. Doppelklicken Sie KONTORICHTLINIEN.
9. Doppelklicken Sie KENNWORTRICHTLINIEN.
10. Passen Sie die Richtlinien Ihren Vorstellung nach an und beenden Sie den Vorgang.

Standardbrowser per Gruppenrichtlinie

Die Zuweisung des Standardbrowsers ist unnötigerweise komplizierter, als man es sich auf den ersten Blick vorstellen könnte. Glücklicherweise ist der altehrwürdige Microsoft Internet Explorer auf dem sicheren Weg zum Ruhestand, und mit Microsoft Edge steht ein steuerbarer und auf der Chrome-Engine basierender, moderner Browser als Ersatz zur Verfügung – und dennoch möchten Sie möglicherweise Googles Chrome als Standardbrowser festlegen.

1. Erstellen Sie eine XML-Datei mit folgendem Inhalt:

```
<?xml version="1.0" encoding="UTF-8"?>
<DefaultAssociations>
  <Association Identifier=".htm"
ProgId="ChromeHTML"
  ApplicationName="Google Chrome"/>
  <Association Identifier=".html"
ProgId="ChromeHTML"
  ApplicationName="Google Chrome"/>
  <Association Identifier="http"
ProgId="ChromeHTML"
  ApplicationName="Google Chrome"/>
  <Association Identifier="https"
ProgId="ChromeHTML"
  ApplicationName="Google Chrome"/>
</DefaultAssociations>
```

2. Speichern Sie diese Datei als chromedefault.xml auf dem

Domänencontroller.

3. Erstellen Sie ein Gruppenrichtlinienobjekt oder wählen Sie ein Gruppenrichtlinienobjekt aus und bearbeiten Sie dieses in der GRUPPENRICHTLINIENVERWALTUNG.
4. Wechseln Sie in den Zweig COMPUTERKONFIGURATION | RICHTLINIEN | ADMINISTRATIVE VORLAGEN | WINDOWS-KOMPONENTEN | DATEI-EXPLORER | KONFIGURATIONSDATEI FÜR STANDARDZUORDNUNGEN FESTLEGEN. Aktivieren Sie die Richtlinie, und die Auswahl der Datei wird aktiv.
5. Kopieren Sie die erstellte `chromedefault.xml`-Datei in ein für alle Benutzer freigegebenes Verzeichnis und geben Sie den Pfad in der Gruppenrichtlinie an ([Abbildung 16.15](#)).
6. Prüfen Sie die Funktionalität der Richtlinie – bei uns hat es geklappt!



Kaum ein Bereich in der Gruppenrichtlinienverwaltung hat sich in den vergangenen Jahren so oft verändert wie die Browser-Steuerung. Möglicherweise gibt es, bis Sie dieses Kapitel lesen, schon wieder eine andere Variante. Am besten suchen Sie direkt mit dem Suchbegriff `Make <Browsername> default browser (Windows 10)` nach der aktuell gültigen Vorgehensweise.

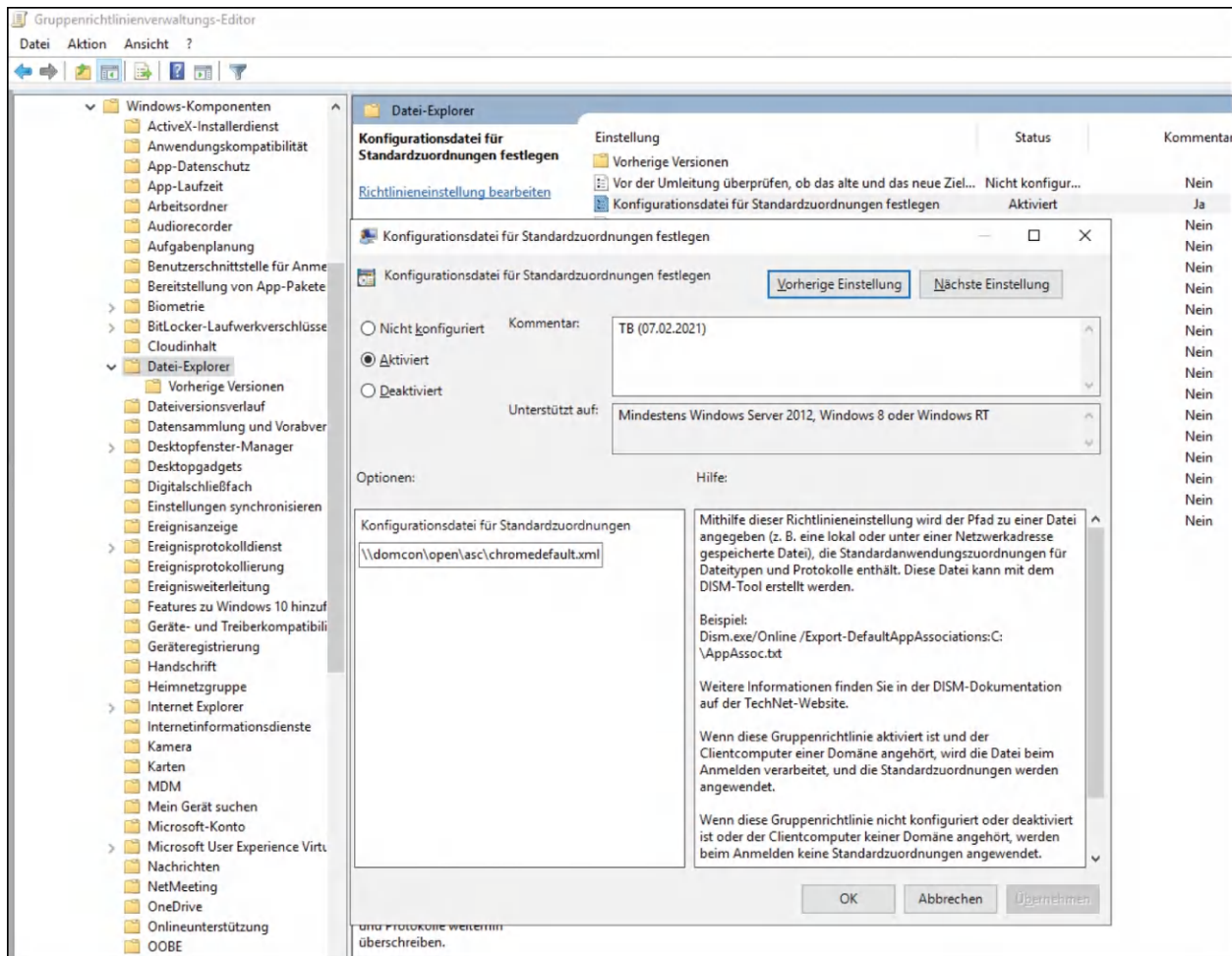


Abbildung 16.15: Hier ist die Zuordnung des Browsers über die Dateinamenerweiterungszuordnung zu sehen.

Office-VBA per Gruppenrichtlinie ausschalten

Es gibt leider eine äußerst große Angriffsfläche für jede Domäne, und diese Gefahr geht von Makroviren aus dem Office-Umfeld aus. Die technischen Möglichkeiten, die Visual Basic for Applications (VBA) bietet und somit auch der »kleine Bruder« Visual Basic Script (VBS), sind wahrlich beeindruckend.

Während sich die .net-Plattform immer weiter entwickeln konnte und sogenannter »Managed Code« dem Administrator heute quasi mitteilt, welche programmtechnischen Erfordernisse zu erfüllen sind, ist so etwas beim Vorläufer nicht möglich.

Wenn Sie mit Ihrer Umgebung auf der sprichwörtlichen »grünen Wiese« beginnen, schalten Sie Makros am besten komplett aus. Sie sparen sich

möglicherweise eine ganze Menge Ärger, der von den Verschlüsselungstrojanern ausgeht.

Sind fortgeschrittene Benutzer in den Fachabteilungen am Werk, bauen diese per VBA gern maßgeschneiderte Lösungen für das Unternehmen. Aus diesem Grund kommt das komplette Deaktivieren von Makros für viele Firmen leider nicht in Betracht.

Wer glaubt, es würde ausreichen, den Mitarbeitern und Kollegen mitzuteilen, dass sie Office-Dateien mit aktivem Inhalt (beispielsweise .docm als Word-Datei mit Makro oder .doc – das ältere Format, bei dem keine Unterscheidung zwischen Makro enthaltenen Dateien oder programmtechnisch aufgewerteten Office-Dokumenten gemacht wird) aus unbekannten Quellen nicht öffnen sollen, irrt gewaltig. Insbesondere Personalabteilung erhalten laufend Material aus unbekannten Quellen – das ist im Bewerbermanagement schlicht der Regelfall.

Und erwarten Sie als Administrator keine besondere Hilfe durch »kostengünstige Virens Scanner«! Nur professionelle Varianten mit Überwachung des »Behaviorismus« entdecken das Werk eines Verschlüsselungstrojaners und sind in der Lage, nach der dritten oder vierten bearbeiteten Datei einzugreifen, den Schädling zu eliminieren und den Schaden zu korrigieren.

Sie können mit einer Erweiterung der administrativen Vorlagen für Office 2007 und höher das Verhalten der Office-Programme steuern. In einer idealen Welt gibt es nur per Zertifikat geschützte Office-Dokumente mit Makroprogrammierung. In der Praxis empfiehlt es sich, die zulässigen Speicherorte für Makrodateien zu definieren.

1. Laden Sie zur Bereitstellung der Gruppenrichtlinie die passenden administrativen Vorlagen für Microsoft Office herunter und wählen Sie die gewünschte Architektur x86/x64. Für Office 2016/2019 lautet der Link <https://www.microsoft.com/en-us/download/details.aspx?id=49030>.
2. Starten Sie die heruntergeladene Datei durch einen Doppelklick und extrahieren Sie den Inhalt an einer Stelle im Dateisystem, auf die Sie von einem Domänencontroller aus zugreifen können.

3. Der nächste Arbeitsschritt unterscheidet sich, je nachdem ob Sie einen Central Store für administrative Vorlagen angelegt haben oder nicht:
 - Ohne Central Store: Verbinden Sie sich mit Ihrem Domänencontroller und kopieren Sie die Dateien im Verzeichnis admx in das Verzeichnis %systemroot%\PolicyDefinitions\. Sie brauchen gewöhnlich nur die Unterverzeichnisse für de und en, die anderen Sprachen müssen Sie nicht mit kopieren.
 - Mit Central Store: Verbinden Sie sich auf einem DC mit \\Names des Domänencontrollers\sysvol\Name der Domäne\Policies und kopieren Sie die Dateien im Verzeichnis admx in das SYSVOL-Verzeichnis. Sie brauchen gewöhnlich nur die Unterverzeichnisse für de und en, die anderen Sprachen müssen Sie nicht mit kopieren.
4. Starten Sie den SERVER-MANAGER.
5. Wählen Sie oben rechts im Menü den Befehl TOOLS.
6. Wählen Sie das Verwaltungsprogramm GRUPPENRICHTLINIENVERWALTUNG.
7. Sie entdecken nun unter ADMINISTRATIVE VORLAGEN die Einträge für die Office-Programme.
8. Über den Eintrag COMPUTER- ODER BENUTZERKONFIGURATION | RICHTLINIEN | ADMINISTRATIVE VORLAGEN | MICROSOFT OFFICE VERSIONSNUMMER | SICHERHEITSEINSTELLUNGEN erhalten Sie Zugriff auf die EINSTELLUNG VBA FÜR OFFICE-ANWENDUNGEN DEAKTIVIEREN.



Für eine detaillierte Steuerung, beispielsweise für das Blockieren von Office-Dateien aus Internet-Quellen oder der Festlegung von sicheren Speicherorten, verweisen wir auf einen ausgezeichneten Blog-Eintrag von Wolfgang Sommergut unter <https://bit.ly/39XsKos>.

Softwareinstallation per Gruppenrichtlinie

Grundsätzlich ist es möglich, dass Administratoren über Gruppenrichtlinienzuweisungen auch Programminstallation anstoßen können. Wir sagen es hier in aller Deutlichkeit: Wir halten nicht sonderlich viel von dieser Basisfunktionalität, da sie eher so einem »Fire and Forget«-Vorgang ähnelt.

Sie bekommen von den Client-Computern keinerlei Rückmeldung – weder im positiven noch im negativen Installationsfall. Sie können als Administrator schlichtweg nur hoffen, dass die Installation umfassend und erfolgreich verläuft. Die Installation findet typischerweise beim Neustart eines Computers statt. Sollten Sie größere Software-Pakete installieren wollen, kann es, abhängig von Computer- und Netzwerkgeschwindigkeit, einige Minuten dauern, ehe der Benutzer sich anmelden kann.



Informieren Sie Ihre Benutzer in jedem Fall, bevor Sie erstmalig Programme per Software-Verteilung bereitstellen, ansonsten dürften Sie recht schnell Rückfragen über den Support erhalten. Über WMI-Filter können Sie die Bereitstellung von Programmen auch zunächst auf eine Testumgebung begrenzen.

Trotz der eher negativen Grundstimmung des Autorenduos in Bezug auf die Software-Verteilung per Gruppenrichtlinie: Um Programme wie einen »Mozilla Firefox« oder »Notepad++« auf viele Computer zu bekommen, ist die Verteilung per Gruppenrichtlinie möglicherweise doch attraktiver, als alles per Hand zu machen. Bereits in mittleren Umgebungen sind Software-Verteilungskonzepte im Endpoint-Management sinnvoller – wohlwissend, dass vor dem Hintergrund der zunehmenden Bereitstellung von Cloud-basierten Applikationen das traditionelle Installationspaket auf dem »Rückmarsch« ist.

Sie können verschiedene Installationspakete verteilen:

- ✓ MSI – Klassische Windows-Installationspakete von Microsoft
- ✓ MST – Transformationsdateien von Microsoft
- ✓ MSP – Patch-Pakete von Microsoft

Hinter diesen Pakettypen verbirgt sich die Technologie des »Microsoft Installers«.



Das Thema MSI und Windows Installer füllt für gewöhnlich ein eigenes Buch und ist für den technisch geprägten Administrator sicherlich ein spannendes Thema. Daher weisen wir besonders gern auf die dazu passenden Microsoft Docs hin:

<https://docs.microsoft.com/en-us/windows/win32/msi/windows-installer-portal>

1. Zunächst einmal gilt es, ein geeignetes MSI-Paket für eine Ferninstallation zu bekommen. Ein idealer Kandidat für die ersten Versuche ist dabei »Notepad++«. Sinnvollerweise suchen Sie im Internet nach den Suchbegriffen:

`Notepad++ msi installer`

Zum Zeitpunkt der Erstellung wurden wir auf Source Forge fündig und entdeckten das passende Paket.

2. Das ZIP-Archiv entpacken und das MSI-Paket extrahieren.
Praktischerweise legen Sie die Datei an einem Ort ab, auf den alle später anvisierten Computer und Benutzer Zugriff haben. In unserem Fall gibt es hierzu auf dem Domänencontroller eine Freigabe mit dem Namen »open« und darunter eine Ebene mit der Bezeichnung »msi«. Bezüglich der Leserechte darf großzügig mit »Jeder« gearbeitet werden.
3. Der nächste Schritt führt in den SERVER-MANAGER, dort unter TOOLS die GRUPPENRICHTLINIENVERWALTUNG starten.
4. In der Baumstruktur wählen Sie die gewünschte Gruppenrichtlinie aus, klicken das Gruppenrichtlinienobjekt mit der rechten Maustaste an und wählen anschließend BEARBEITEN.



Arbeiten Sie an dieser Stelle mit WMI-Filtern, um die Installationsvorgänge genau zu planen. Sollten Sie noch zwischen x86- und x64-Windows unterscheiden müssen, wäre dies ein

Filterkriterium. Zudem können Sie Member-Server, Workstations oder Desktops, Laptops und Domänencontroller voneinander trennen.

5. Es öffnet sich der GRUPPENRICHTLINIEN-EDITOR.
6. Wählen Sie COMPUTERKONFIGURATION | RICHTLINIEN | SOFTWAREEINSTELLUNGEN und dort den Eintrag SOFTWAREINSTALLATION aus.
7. Klicken Sie mit der rechten Maustaste in das möglicherweise noch komplett leere Ergebnisfenster und wählen Sie aus dem Kontextmenü den Befehl NEU | PAKET... aus.
8. Es öffnet sich der Auswahldialog für Pakete. Wählen Sie das von Ihnen heruntergeladene Notepad++-MSI-Paket aus, indem Sie den Pfad UNC-codiert eingeben – in unserem Fall
`\\domcon\open\MSI\Notepad++7_8_9.msi`
Schließen Sie die Auswahl mit ÖFFNEN ab.
9. Bezüglich der Bereitstellungsmethode bietet Ihnen das Dialogfeld zwei Optionen an: ZUGEWIESEN oder ERWEITERT. Wählen Sie die letztgenannte Option aus und bestätigen Sie die Auswahl mit OK.
10. Es erscheint das Dialogfenster mit den EIGENSCHAFTEN VON NOTEPAD++ (64-BIT X64). Schauen Sie sich die verschiedenen Optionen an. In diesem Fall gibt es weder Änderungen noch Aktualisierungen, die es zu beachten gäbe.
11. Stellen Sie sicher, dass in der Registerkarte BEREITSTELLUNG VON SOFTWARE die BEREITSTELLUNGSART ZUGEWIESEN aktiv ist.
12. Klicken Sie auf OK und Sie haben Ihr erstes Paket zur Festinstallation vorbereitet.

Software-Installationen geschehen, wie bereits erwähnt, beim Neustart des Computers, und es kann durchaus einige Zeit vergehen, ehe das Paket tatsächlich auf die von der Gruppenrichtlinie betroffenen Richtlinien verteilt ist.

Wiederholen Sie, eher aus didaktischen Gründen, Ihr Vorhaben mit dem Mozilla Firefox und Sie landen beinahe automatisch auf der entsprechenden Support-Webseite:

<https://support.mozilla.org/de/kb/firefox-uber-msi-installationspakete-bereitstellen>

Praktischerweise beschreibt die Mozilla-Support-Seite unterhalb des Downloadlinks recht passend, wie Sie mit einem Programm wie MS Orca die MSI-Transformationsdateien erstellen können.

Die automatische Verteilung von Programmen ist, wie bereits erwähnt, eine komplexe Aufgabe. Allein schon die Bereitstellung eines Standardprogramms wie Adobe Acrobat in der DC-Variante »mutiert mitunter zum Intelligenztest«. Dagegen ist die Verteilung von Libre Office als MSI-Paket einfach, wenn man erst einmal verstanden hat, dass man per SuperOrca die überflüssigen Sprachvarianten entfernen muss. Microsoft Office wiederum – lassen wir das ...



Eine praktische Beschreibung zur Verteilung von Adobe Acrobat finden Sie unter

https://community.spiceworks.com/how_to/37690-how-to-deploy-acrobat-reader-with-gpo.

Entfernen eines Pakets und Updates

Führen Sie die folgenden Schritte aus, um ein veröffentlichtes oder zugewiesenes Paket wieder aus der Auflistung zu entfernen:

1. Starten Sie den SERVER-MANAGER, klicken Sie dort unter TOOLS auf die GRUPPENRICHTLINIENVERWALTUNG.
2. Klicken Sie auf das Gruppenrichtlinienobjekt, das Sie zum Bereitstellen des Pakets verwendet haben, und klicken Sie dann auf BEARBEITEN.
3. Erweitern Sie den Container SOFTWAREEINSTELLUNGEN, der das Software-Installationselement enthält, das Sie zum Bereitstellen des Pakets verwendet haben.

4. Klicken Sie mit der rechten Maustaste auf den Software-Installationscontainer, der das Paket enthält, wählen Sie ALLE AUFGABEN und klicken Sie dann auf ENTFERNEN.
5. Führen Sie eine der folgenden Aktionen aus:
 - Klicken Sie auf SOFTWARE SOFORT DEINSTALLIEREN von BENUTZERN UND COMPUTERN und klicken Sie dann auf OK.
 - Klicken Sie auf BENUTZER DÜRFEN WEITERHIN DIE SOFTWARE VERWENDEN, ABER NEUE INSTALLATIONEN VERHINDERN und klicken Sie dann auf OK.
6. Schließen Sie die Gruppenrichtlinienverwaltung.

Möchten Sie beispielsweise eine neue Version von Notepad++ ausbringen, entfernen Sie die ältere Version mit der Option »sofort deinstallieren« und legen Sie anschließend das neue Paket an. Windows steuert die Reihenfolge glücklicherweise, sodass Benutzer nach einem Neustart, nach etwas Wartezeit bei der Anmeldung, die neue Version zur Verfügung haben.

Loopback

Mit dem bisher dargestellten Wissen sind Sie in der Lage, so ziemlich jede Konstellation per Gruppenrichtlinie darzustellen. Wer sich zu dem Thema im Internet bedient, wird zwangsläufig auf den Punkt Loopbackverarbeitungsmodus stoßen.

Dieses beinahe »legendäre« Wort – Loopbackverarbeitungsmodus – werden Sie nicht brauchen, da Sie anhand von WMI-Filtern recht gut zwischen Servern und normalen Arbeitsrechnern unterscheiden können.

In der frühen Phase des Active Directory und der Gruppenrichtlinien war dem nicht so – unter Windows 2000 war es nicht so leicht möglich, eine Konstellation aufzubauen, bei der ein Benutzer auf seiner Arbeitsstation das Recht besaß, den Computer herunterzufahren, während derselbe Benutzer in einer Remotedesktop-Terminalserver-Umgebung den Server eben nicht herunterfahren durfte.

Durch den sogenannten »Loop« wird eine bewusste Schleife eingebaut:
COMPUTERKONFIGURATION | ADMINISTRATIVE VORLAGEN |
SYSTEM | GRUPPENRICHTLINIEN |
LOOPBACKVERARBEITUNGSMODUS FÜR
BENUTZERGRUPPENRICHTLINIE = AKTIVIERT

Diese Schleife sorgt dafür, dass die Gruppenrichtlinienverarbeitung nach Abarbeiten der Benutzeranmeldung noch einmal in die Liste der Gruppenrichtlinien für Computerobjekte springt. Klingt kompliziert? Ist es auch.



Wer es gern detailliert zur Loopbackverarbeitung mag, der sei auf einen sehr gelungenen Blog-Beitrag von Mark Heitbrink hingewiesen:

<https://www.gruppenrichtlinien.de/artikel/loopbackverarbeitung-mode/>.

Programme per GPO sperren

Typischerweise installieren Administratoren Computer in der Form, dass die Programme, die ein Anwender zu sehen bekommt, auch bedienen darf oder soll. Eine solche Bereitstellung von Programmen erleichtert schlichtweg das Lizenzmanagement. Sie müssen einen solchen Rat ja nicht beherzigen und können mit Gruppenrichtlinien dafür sorgen, dass einzelne Programme von Benutzern nicht verwendet werden können.

In unserem Beispiel möchten wir sicherstellen, dass niemand das Programm `wordpad.exe` einsetzen kann.

1. Starten Sie den SERVER-MANAGER, klicken Sie dort unter TOOLS auf die GRUPPENRICHTLINIENVERWALTUNG.
2. Wählen Sie die gewünschte Gruppenrichtlinie in der Baumstruktur aus und wählen Sie das zu bearbeitende Gruppenrichtlinienobjekt mit der rechten Maustaste aus. Wählen Sie aus dem Kontextmenü den Befehl BEARBEITEN.
3. Wechseln Sie in die BENUTZERKONFIGURATION | RICHTLINIEN | ADMINISTRATIVE VORLAGEN.

4. Wählen Sie SYSTEM und anschließend den Eintrag ANGELEGENE WINDOWS-ANWENDUNGEN NICHT AUSFÜHREN.
5. Wählen Sie die Option AKTIVIERT und klicken Sie anschließend auf die Schaltfläche ANZEIGEN...
6. Geben Sie den Programmnamen wordpad.exe ein (siehe [Abbildung 16.16](#)).

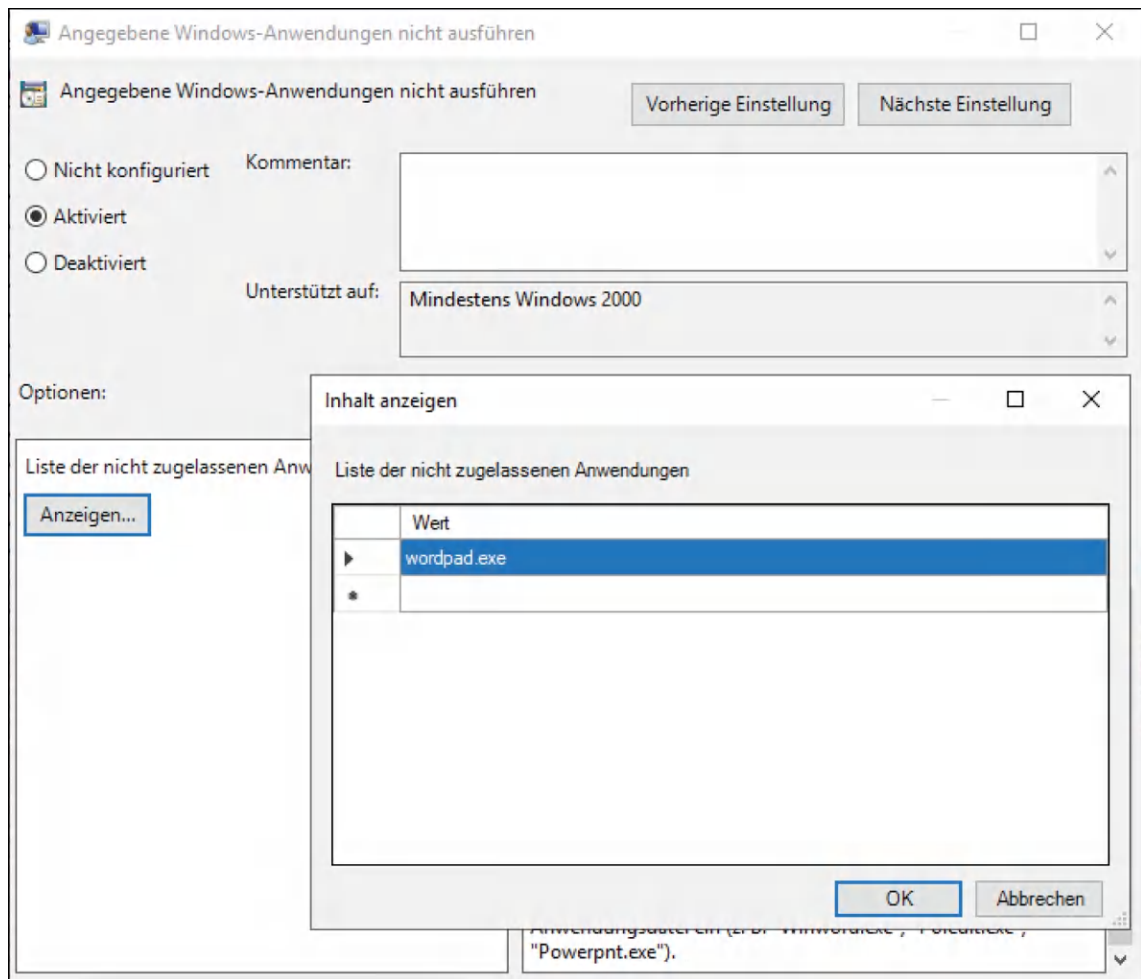


Abbildung 16.16: Programme im Griff: Wordpad kann nun nicht mehr gestartet werden.

Ein Startversuch von Wordpad wird nun mit dem Dialogfenster EINSCHRÄNKUNGEN beantwortet mit dem Hinweis, dass aufgrund einer aktuellen Beschränkung auf dem Computer der Vorgang abgebrochen wurde. Der Anwender möge sich doch an den Systemadministrator wenden.

Troubleshooting für Gruppenrichtlinien

Die Fehlersuche bei Gruppenrichtlinien ist nicht besonders attraktiv, das mögen wir gleich vorwegschicken. Und hier kommen häufig »Weichmacher« in Dialogen vor: »Komisch, eigentlich hätte es klappen sollen...« Wie so oft sitzt das Problem vor dem Computer, und es ist die Überlagerung der verschiedenen Gruppenrichtlinienobjekte, die zur Anwendung kommen, und das simple »die zuletzt schreibende Gruppenrichtlinie ist die aktive Gruppenrichtlinie«, das zu Chaos führen kann.

Bevor wir auch nur ein einziges Kommando in die Tastatur klopfen werden, benutzen wir das Gehirn:

- ✓ Hat sich der Benutzer schon neu angemeldet, seit die Gruppenrichtlinie angepasst wurde?
- ✓ Wurde der Computer neu gestartet, seit die Gruppenrichtlinie geändert wurde?

Die einfachste Fehlerbeseitigungsvariante für einen Standardcomputer, auf dem nur ein Anwender aktiv ist, lautet: »Starten Sie den Computer bitte noch einmal neu!«

Mit etwas »Glück und digitaler Spucke« zieht nun die Gruppenrichtlinie, und das Problem hat sich erledigt. Auf Computern mit mehreren Benutzern, insbesondere Terminalservern, reduziert sich der Lösungsvorschlag auf Ab- und Neuansmeldung. GPOs, die auf der Computerkonfiguration basieren, kommen somit leider nicht zur Ausführung, und der in Internetforen inflationär verwendete Hinweis, man möge doch mit

`gpupdate /force`

in der Eingabeaufforderung für ein nachträgliches und erzwungenes Neueinlesen der Gruppenrichtlinie setzen, bleibt zumeist erfolglos. Neustart und die damit verbundene Neuansmeldung des Benutzers

bewirken mehr – versprochen.

Als administrativ berechtigter Benutzer können Sie sich durch Eingabe von

`rsop.msc`

in der Eingabeaufforderung den Richtlinienprotokollierungssatz zum Sammeln von Computerrichtlinieninformationen anzeigen lassen. RSOP steht hier für »Resultant Set of Policy«. Ein nettes Tool, jedoch ohne administrative Rechte so stark limitiert, dass die Aussagefähigkeit nicht überzeugend ist.

Die tatsächliche »Allzweckwaffe« ist ein anderes Programm, das Sie – auch als Benutzer – wieder über die Eingabeaufforderung aufrufen:

`gpresult /h Ausgabedateiname.html`

Sie können sich anschließend das Ergebnis bequem mit einem Browser anschauen – und haben den Report für den Computer, auf dem Sie den Befehl ausgeführt haben, und als der Benutzer, der aktuell angemeldet ist.

Etwas spannender ist für Sie als Administrator die Möglichkeit, die Auswirkungen auf die Konstellation Benutzer/Computer simuliert zu betrachten. Hierzu ist ein Befehl wie

`gpresult /S iotaone /USER schmidt /h ausgabe2.html`

interessant. Hier werten wir für den PC `iotaone` für einen angemeldeten Benutzer `schmidt` die Auswirkungen von Richtlinien aus ([Abbildung 16.17](#)).

BAER-SCHLEDE\schmidt auf BAE

← → ↺ ⓘ Datei | C:/Users/Thomas%20Bär/Desktop/ausgabe2.html

Sicherheitsgruppenmitgliedschaft

Einblenden

Komponentenstatus

Komponentenname	Status	Erstellungszeit	Letzter Prozess am	Ereignisprotokoll
Gruppenrichtlinieninfrastruktur	Erfolgreich	4 Sekunde(n) 845 Millisekunde(n)	10.02.2021 19:36:30	Protokoll anzeigen
Group Policy Shortcuts	Erfolgreich	3 Sekunde(n) 453 Millisekunde(n)	10.02.2021 19:36:29	Protokoll anzeigen
Registrierung	Erfolgreich	329 Millisekunde(n)	10.02.2021 19:36:26	Protokoll anzeigen

Einstellungen

Richtlinien

Administrative Vorlagen

Richtliniendefinitionen (ADMX-Dateien) wurden beim lokalen Computer abgerufen.

System

System/Wechselmedienzugriff

Richtlinie	Einstellung	Ausschlaggebendes Gruppenrichtlinienobjekt
Alle Wechselmedienklassen: Jeglichen Zugriff verweigern	Aktiviert	Sicherheitszuordnung

Systemsteuerung

Einstellungen

Windows-Einstellungen

Verknüpfungen

Gruppenrichtlinienobjekte

Angewendete Gruppenrichtlinienobjekte

Sicherheitszuordnung [{8F389E6F-C315-4D6B-8711-D44C6DF2DED3}]

Standard-PC-Konfiguration [{1EDED01A-E97C-4A4D-9092-88B892433714}]

Abgelehnte Gruppenrichtlinienobjekte

Richtlinien der lokalen Gruppe [LocalGPO]

WMI-Filter

Name	Wert	Gruppenrichtlinienobjekt-Referenz
NOT-DOMAIN-CONTROLLER	Wahr	Standard-PC-Konfiguration

Abbildung 16.17: Eine Auswertung von Gruppenrichtlinien per »gpresult«

Wir finden den Bericht an sich selbsterklärend.



Weitere Informationen finden Sie in den Microsoft Docs unter <https://docs.microsoft.com/de-de/windows-server/administration/windows-commands/gpresult>.

Kapitel 17

Überwachung des Server-Betriebs

IN DIESEM KAPITEL

- Der Server-Manager
- Verwalten des lokalen Servers
- Server-Manager-Eigenschaften konfigurieren
- Überblick über das Tools-Menü
- Windows Admin Center – Installation
- Windows Admin Center – erster Einsatz

Der Betrieb eines Windows-Servers erfordert regelmäßig Kontrolle. Dafür steht eine fast unüberschaubare Zahl von Anwendungen oder auch SaaS-Lösungen (Software as a Service) von Drittanbietern zur Verfügung, aber Microsoft stattet die Server-Systeme schon standardmäßig mit einer Reihe von Programmen aus, die Ihnen bei der Verwaltung und Betreuung Ihres Windows Server 2019 sehr nützlich sein können.

Der Server-Manager

Bereits mit der Version 2008 des Windows-Servers hat Microsoft den Administratoren erstmals einen eigenständigen Server-Manager zur Verfügung gestellt, der den IT-Fachleuten eine Verwaltung ihrer Server auch ohne die umfangreiche und kostenintensive Lösung System Center ermöglicht. Stellte sich die Software aber auf den Systemen unter Windows Server 2008 und 2008 R2 noch als eine »erweiterte MMC« (Microsoft Management Console) dar, haben die Entwickler aus Redmond

ab den Server-Versionen 2012 und 2012 R2 ein Werkzeug bereitgestellt, das Ihnen die Verwaltung eines oder mehrerer Windows-Server mittels moderner Oberfläche und vielen Features deutlich erleichtert.

Wenn Sie sich an Ihrem Windows Server mit dem Administratorkonto anmelden, startet das System automatisch den Server-Manager mit seinem sogenannten »Dashboard«, das Ihnen einen ersten Überblick über den Zustand des Systems präsentiert. Mit dem Windows Server 2019 und auch dem Windows Server 2022 bekommen Sie dabei standardmäßig auch immer ein Fenster präsentiert, das Sie darauf hinweist, dass Microsoft mit dem WINDOWS ADMIN CENTER ein Nachfolgeprodukt für diese Software anbietet, und Sie dazu veranlasst, dieses doch direkt herunterzuladen und zu installieren ([Abbildung 17.1](#)). Wir gehen auf dieses Nachfolgeprodukt für den Server-Manager im Verlauf dieses Kapitels noch näher ein und zeigen auch, wie Sie es parallel zum Server-Manager installieren und nutzen können. Sie können dieses kleine Fenster deshalb beruhigt schließen oder gleich das Kästchen **DIESE MELDUNG NICHT MEHR ANZEIGEN** auswählen, damit wir uns zunächst einmal ungestört dem Server-Manager widmen können.

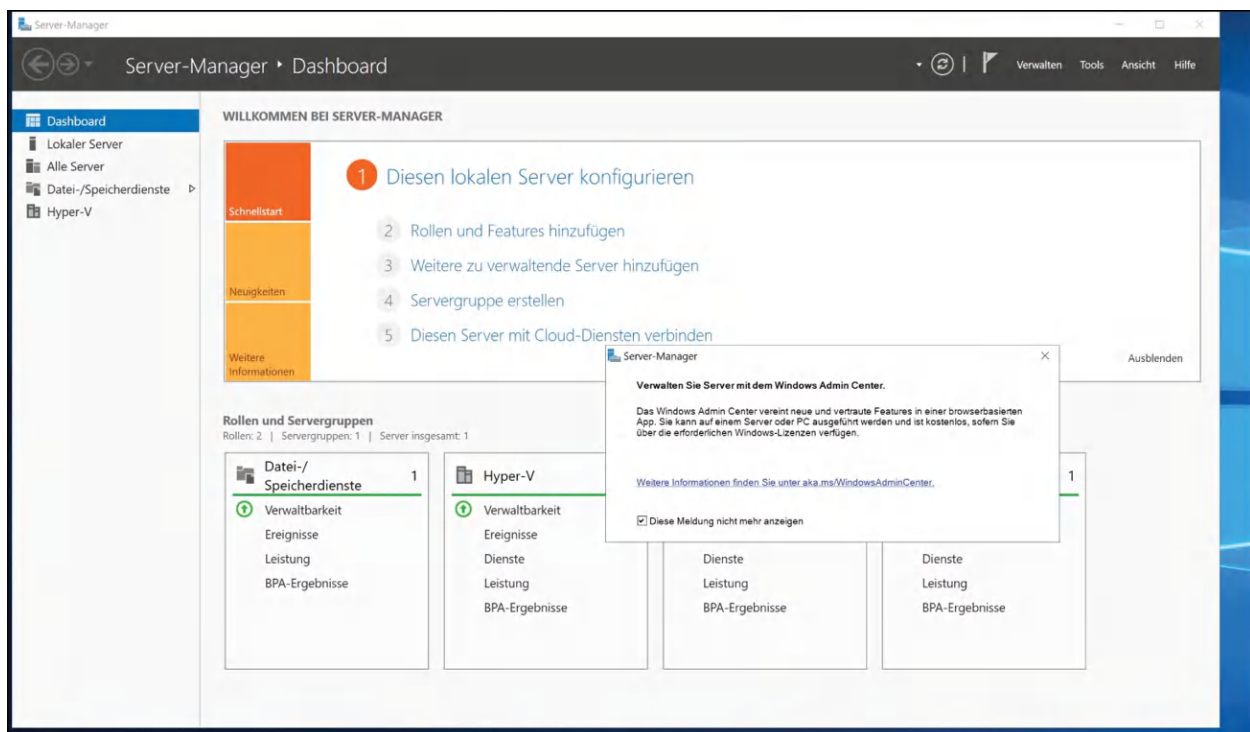


Abbildung 17.1: Beim ersten Start meldet sich der Server-Manager mit einem Dashboard

und »Werbung« für den Nachfolger Admin Center.

Ein großer Vorteil des Server-Managers besteht darin, dass er nach wie vor standardmäßig zur Ausstattung des jeweils aktuellen Windows-Servers gehört. Auch wenn Microsoft immer wieder betont, dass das Admin Center ein wichtiger Teil der kommenden Server-Versionen sei, ist der Server-Manager auf dem 2019-Nachfolger, der in einer Vorabversion als Windows Server 2022 bereitsteht, nach wie vor zu finden.

Das übersichtliche Dashboard ist mit vielen Assistenten ausgestattet, die auch weniger erfahrene Administratoren sicher durch komplexe Aufgaben wie das Anlegen eines Domänen-Servers für Active Directory leiten. Erläuterungen zu Best-Practices-Maßnahmen in der Praxis stehen ebenfalls direkt innerhalb der Oberfläche des Managers bereit. Nach wie vor stehen viele Software-Werkzeuge für die Verwaltung eines Windows-Servers auch als Snap-ins für die Microsoft Management Console (MMC) bereit. Die meisten Einstellungen und Konfigurationen können Sie aber direkt über das TOOLS-Menü des Server-Managers erreichen. Dabei startet dann in vielen Fällen – wie beispielsweise beim Eintrag COMPUTERKONFIGURATION – ein Fenster mit der altbekannten MMC-Darstellung, wie Sie es vielleicht bereits von Ihrem Windows-10-Rechner her kennen ([Abbildung 17.2](#)).

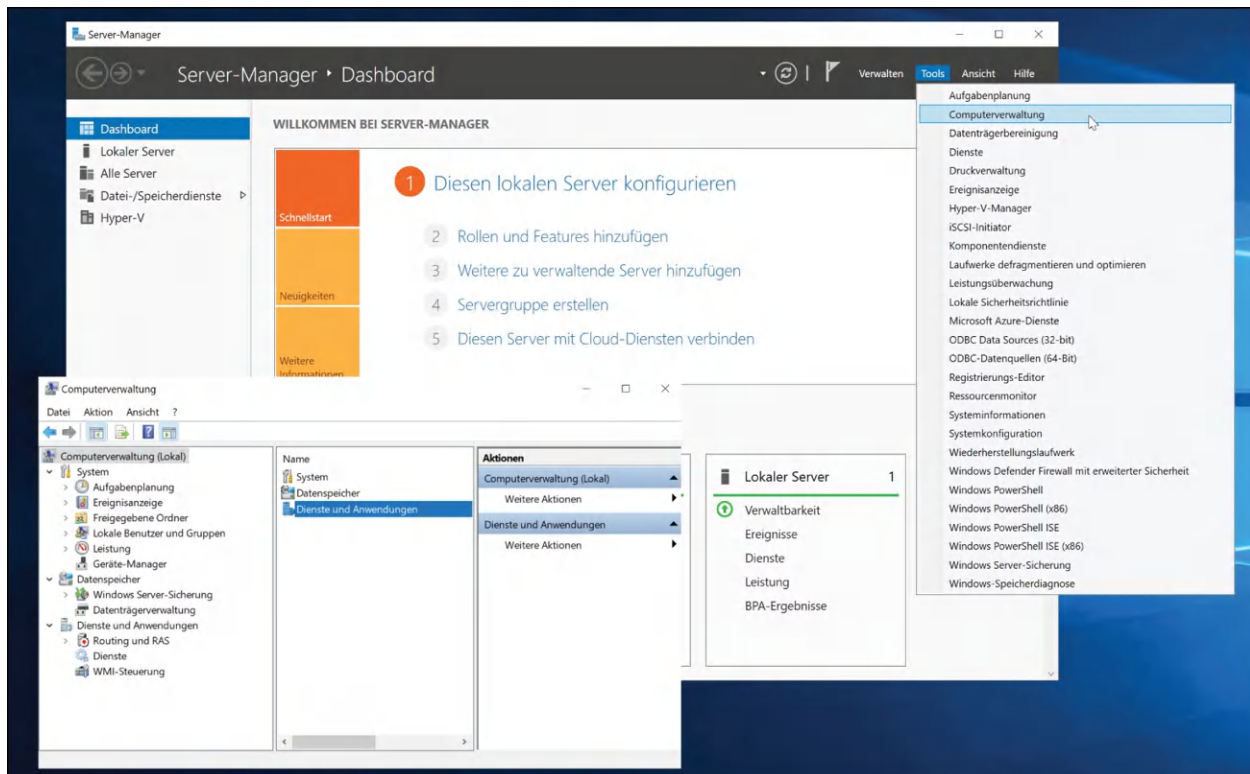


Abbildung 17.2: Fast alle Einstellungen und Konfigurationsmöglichkeiten sind direkt aus dem Server-Manager heraus erreichbar.

In den Server-Manager können Sie mehrere Server innerhalb eines AD-Verbunds oder einer Workgroup einbinden und verwalten. Sie können diese Server dann auch in Gruppen zusammenfassen und gemeinsam bearbeiten und verwalten. Sie können mit dem Server-Manager Aufgaben wie die Installation und Deinstallation von Server-Features und -Rollen ebenso gut im Griff behalten wie eine Überwachung der Festplatten in den Systemen. Allerdings haben Sie dabei keinen direkten Zugriff auf weitere Hardware-Features Ihres Servers.

Die Kacheln auf dem Dashboard signalisieren mit ihrer Farbe den jeweiligen Zustand eines Servers oder einer Server-Gruppe und werden dann beispielsweise bei Problemen rot dargestellt. Für jede installierte Rolle sowie für jeden Server, der mit dem Werkzeug verwaltet wird, finden Sie im Dashboard eine eigene Kachel. Diese beinhaltet dann Links zu Übersichten der aufgetretenen Ereignisse, zu Leistungsdaten und Ergebnissen des für die Rolle zuständigen BEST PRACTICE ANALYZER. Diese Software analysiert die Konfiguration der Rollen auf dem Server und vergleicht sie mit den gesammelten Daten einer Best-

Practice-Datenbank. So erfahren Sie nicht nur etwas über das Funktionieren der Rollen hinaus, Sie bekommen auch Informationen dazu, wo Nachbesserungsbedarf bei der Konfiguration besteht, ob eventuell Sicherheitslücken bestehen oder ob es Optimierungsmöglichkeiten gibt. Die entsprechenden Daten werden dabei nicht in Echtzeit angezeigt, sondern standardmäßig alle 10 Minuten durch den Server-Manager abgefragt. Sie können dieses Intervall aber leicht verändern:

1. Starten Sie den Server-Manager und wählen Sie auf der oberen Leiste des Fensters den Eintrag VERWALTEN aus.
2. Im Pull-down-Menü klicken Sie dann auf SERVER-MANAGER EIGENSCHAFTEN.
3. Es öffnet sich ein weiteres Fenster ([Abbildung 17.3](#)), in dem das Kästchen neben der Beschreibung DATENAKTUALISIERUNGSPERIODE FÜR DEN SERVER-MANAGER ANGEBEN (IN MINUTEN) angewählt ist. Auf der rechten Seite finden Sie nun ein Feld mit den Minuten für das Intervall. Wenn Sie dort einen neuen Wert eintragen, nehmen Sie die Warnung darunter ernst, dass ein zu kurzes Intervall den Server und das Netzwerk deutlich belasten wird. Unserer Erfahrung nach sollten Sie keinen Wert unter 5 Minuten wählen.

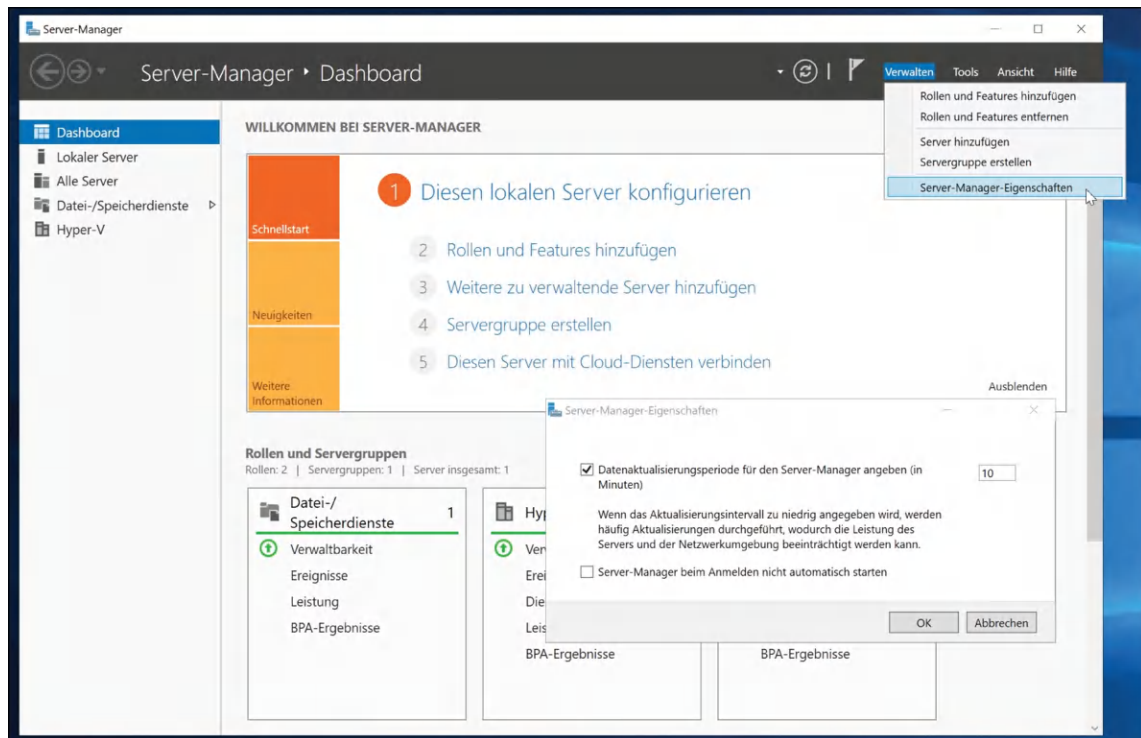


Abbildung 17.3: Bei den Eigenschaften des Server-Managers ist es möglich, das Aktualisierungsintervall für die Abfrage der Daten zu verändern.

4. Sie können in diesem Fenster dann noch die Auswahl treffen, dass der Server-Manager nicht mehr automatisch beim Anmelden gestartet wird. Da Sie das Programm jederzeit wieder aus dem Startmenü heraus aufrufen können, ist es unproblematisch, den automatischen Start an dieser Stelle abzuschalten.

Eine der wichtigsten Aufgaben des Server-Managers besteht darin, dem Windows-Server Aufgaben und Features hinzuzufügen oder zu entfernen. Bei den Versionen vor Windows Server 2012 waren es noch zwei Assistenten, die den Nutzer jeweils durch das Hinzufügen beziehungsweise Entfernen einer Rolle oder eines Features führten. Das führte dazu, dass die Nutzer immer erst einmal suchen mussten, ob das, was ihr Server brauchte, in einer Rolle oder einem Feature zu finden war. Dies ist seit Windows Server 2012 und damit auch auf Ihrem Windows Server 2019 und dem Windows Server 2022 nicht mehr so: Sie finden alle Rollen und Features in einem Assistenten, den Sie aus dem Dashboard direkt unter **DIESEN LOKALEN SERVER KONFIGURIEREN** oder aus dem Menü **VERWALTEN** heraus aufrufen können ([Abbildung 17.3](#)).

Verwalten des lokalen Servers

Wenn Sie Ihren lokalen Server verwalten wollen, dann können Sie dazu aus der linken Spalte des Server-Manager-Dashboards den Eintrag **LOKALER SERVER** auswählen. Darauf öffnet sich eine Seite, auf der Ihnen Eigenschaften, Ereignisse, Dienst- und Leistungsdaten sowie die Ergebnisse des Best Practices Analyzer (BPA) für den lokalen Server angezeigt werden ([Abbildung 17.4](#)).

The screenshot displays the Windows Server Manager interface for a local server. The left sidebar contains navigation links: Dashboard, Lokaler Server (selected), Alle Server, Datei-/Speicherdienste, and Hyper-V. The main content area is titled 'Server-Manager - Lokaler Server' and features a top navigation bar with 'Verwalten', 'Tools', 'Ansicht', and 'Hilfe' buttons. The 'EIGENSCHAFTEN' (Properties) section is active, showing a grid of server details. A context menu is open over the 'AUFGABEN' (Tasks) button in this section, listing actions such as 'Lokalen Server herunterfahren', 'Windows PowerShell', 'Computerverwaltung', 'Hyper-V-Manager', and 'Aktualisieren'. Below the properties, the 'EREIGNISSE' (Events) and 'DIENSTE' (Services) sections are visible, each with a filter and a list of items.

Category	Value
Computernamen	Server-2019phys
Arbeitsgruppe	WORKGROUP
Zuletzt installierte Updates	26.03.2021 15:31
Windows Update	Nur Updates mithilfe von Microsoft Update
Zuletzt auf Updates geprüft	Gestern um 13:50
Windows Defender Firewall	Privat: Ein
Remoteverwaltung	Aktiviert
Remotedesktop	Aktiviert
NIC-Teamvorgang	Deaktiviert
vEthernet (NeuerSwitch)	192.168.0.250, IPv6-fähig
Windows Defender Antivirus	Echtzeitschutz: Ein
Feedback und Diagnose	Einstellungen
Verstärkte Sicherheitskonfiguration für IE	Ein
Zeitzone	(UTC+01:00) Amsterdam, Berlin, Rom, Stockholm, Wien
Produkt-ID	00429-00521-75746-AA209 (Aktiviert)
Betriebssystemversion	Microsoft Windows Server 2019 Standard
Prozessoren	Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz
Hardwareinformationen	ASUS All Series
Installierter Arbeitsspeicher (RAM)	15,66 GB
Speicherplatz insgesamt	2708,5 GB

Servername	ID	Schweregrad	Quelle	Protokoll	Datum und Uhrzeit
SERVER-2019PHYS	1008	Warnung	Microsoft-Windows-PerfLib	Anwendung	01.04.2021 10:21:04
SERVER-2019PHYS	2004	Fehler	Microsoft-Windows-PerfNet	Anwendung	01.04.2021 10:20:42
SERVER-2019PHYS	1008	Warnung	Microsoft-Windows-PerfLib	Anwendung	01.04.2021 10:20:42
SERVER-2019PHYS	1008	Warnung	Microsoft-Windows-PerfLib	Anwendung	01.04.2021 10:20:42
SERVER-2019PHYS	7023	Fehler	Microsoft-Windows-Service Control Manager	System	01.04.2021 10:20:37
SERVER-2019PHYS	134	Warnung	Microsoft-Windows-Time-Service	System	01.04.2021 10:20:37
SERVER-2019PHYS	10149	Warnung	Microsoft-Windows-Windows Remote Management	System	31.03.2021 17:35:04

Servername	Anzeigenname	Dienstname	Status	Starttyp
SERVER-2019PHYS	Anwendungsidentität	AppIDSvc	Beendet	Manuell (Ausgelöst)
SERVER-2019PHYS	Anwendungsverwaltung	AppMgmt	Beendet	Manuell
SERVER-2019PHYS	Microsoft App-V Client	AppVClient	Beendet	Deaktiviert

Abbildung 17.4: Die Seite »Lokaler Server« des Server-Managers bietet viele Informationen und Einstellmöglichkeiten.



Die im Abschnitt **EIGENSCHAFTEN** angezeigten Einstellungen wirken sich ausschließlich auf den lokalen Server aus, da an dieser

Stelle auch nur dessen Eigenschaften angezeigt werden.
Veränderungen dieser Einstellungen sind von einem Remote-System aus nicht möglich.

Alle Bereiche auf der Seite LOKALER SERVER besitzen jeweils ein eigenes AUFGABEN-Menü. Bei den Eigenschaften für Ihren Server stehen Ihnen dort die folgenden Möglichkeiten zur Verfügung:

- ✓ LOKALEN SERVER HERUNTERFAHREN: Dient dem Herunterfahren des Systems.
- ✓ WINDOWS POWERSHELL: Hier können Sie eine lokale PowerShell-Sitzung starten.
- ✓ COMPUTERVERWALTUNG: Öffnet das MMC-Snap-in für die Verwaltung des lokalen Systems.
- ✓ HYPER-V-MANAGER: Direkter Wechsel zur Verwaltung des Hyper-V-Servers.
- ✓ AKTUALISIERUNG: Durch Auswahl dieses Eintrags werden die Daten im Abschnitt EIGENSCHAFTEN auf den aktuellen Stand gebracht.

Wenn Sie einen Server über den Menüeintrag LOKALER SERVER HERUNTERFAHREN beenden, sehen Sie als Neuerung in der Version 2019 nun ein Fenster, in dem Sie direkt den Grund für das Herunterfahren angeben können, der dann bei den Ereignissen auf dem Server protokolliert wird – zu sehen in [Abbildung 17.5](#). Mittels eines kleinen Kästchens können Sie an dieser Stelle festlegen, ob das Herunterfahren grundsätzlich geplant war, und bekommen auch die entsprechenden Auswahlmöglichkeiten mit dem Zusatz »geplant« präsentiert. Weiterhin steht Ihnen ein Feld für Kommentare zur Verfügung.

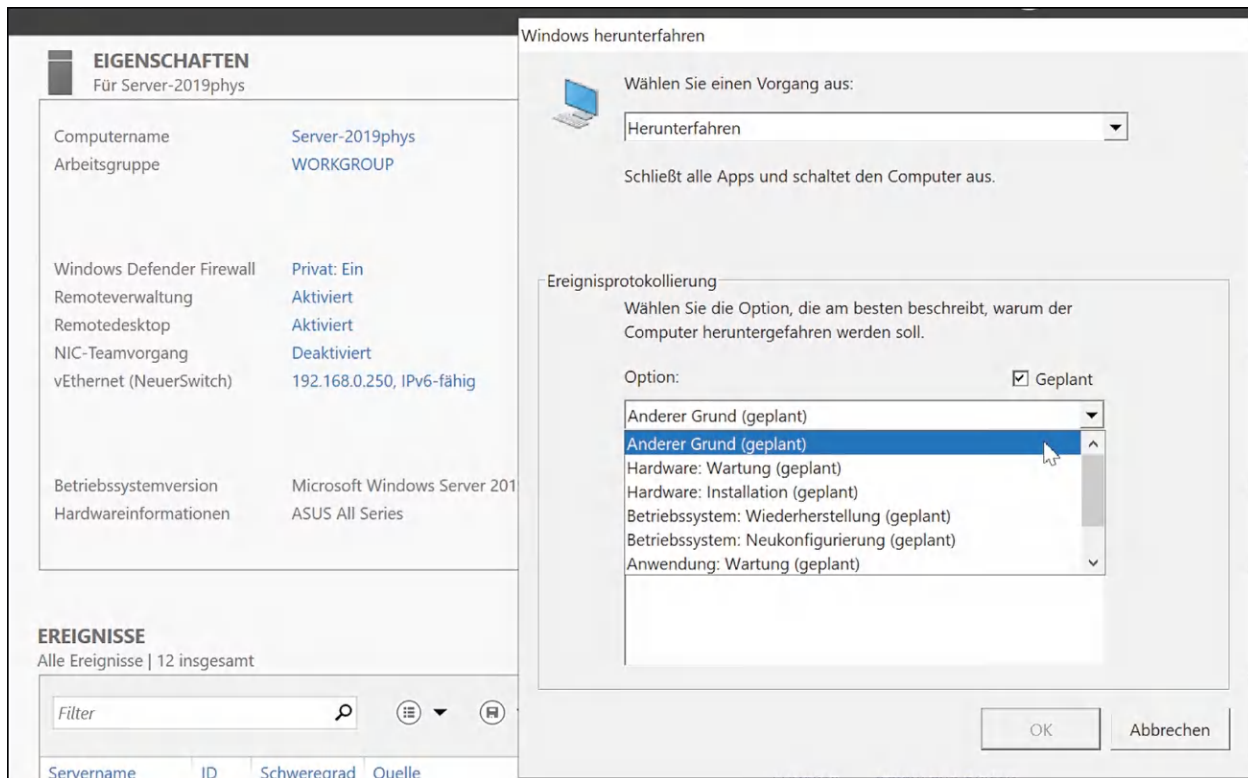


Abbildung 17.5: Nach der Auswahl von »Lokaler Server herunterfahren« können Sie den Grund für diesen Vorgang angeben.



Ein Windows-Server kann nur von Mitgliedern der Gruppe ADMINISTRATOREN heruntergefahren werden. Klicken Sie beispielsweise als Standardbenutzer auf den Eintrag **LOKALEN SERVER HERUNTERFAHREN**, so werden Sie automatisch von der Server-Sitzung abgemeldet.

Lokalen Server konfigurieren

Im Bereich **EIGENSCHAFTEN** steht Ihnen eine ganze Reihe von Einstellungen zur Verfügung, die Sie für diesen lokalen Server vornehmen können:

- ✓ **COMPUTERNAME:** Dort wird Ihnen der Namen des Servers angezeigt. Wenn Sie auf diesen Namen klicken, öffnet sich das Fenster **SYSTEMEIGENSCHAFTEN** mit der Registerkarte **COMPUTERNAME**. Dort können Sie dann beispielsweise den

Namen Ihres Servers ändern (was einen Neustart erfordert) oder auch den Server aus einer Arbeitsgruppe (Workgroup) in eine Windows-Domäne verschieben ([Abbildung 17.6](#)).

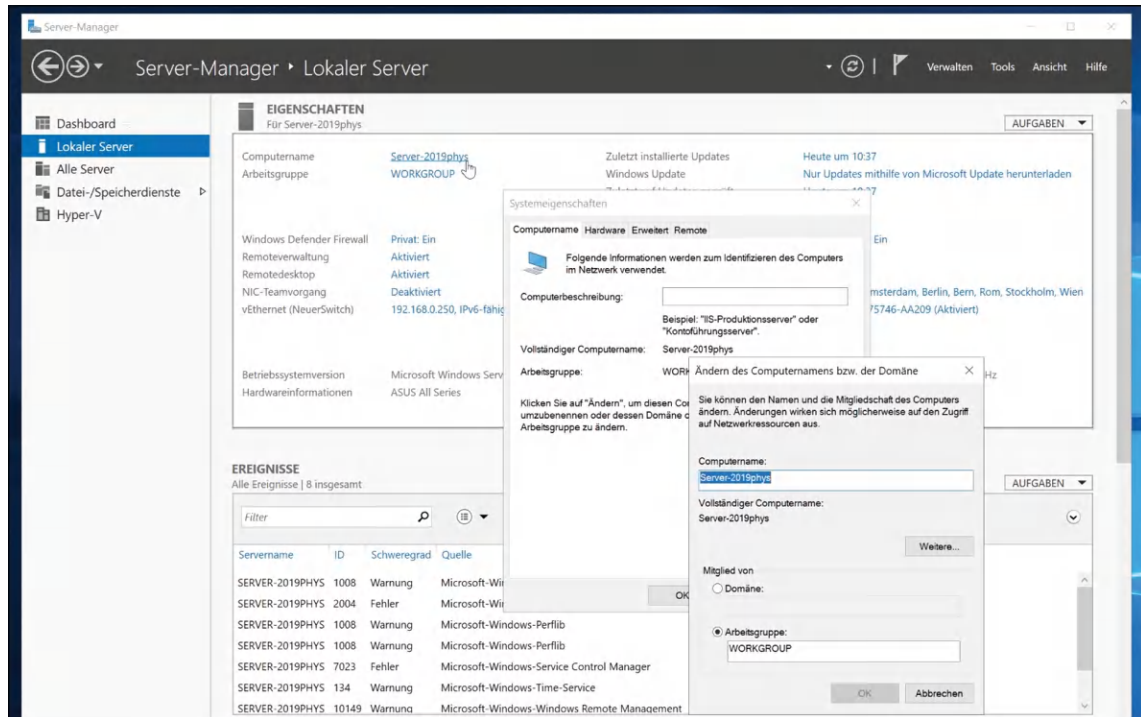


Abbildung 17.6: Bei den Eigenschaften des lokalen Servers sind die Einträge als Hyperlinks ausgeführt, die dann direkt zu den Einstellungen führen.

- ✓ **ARBEITSGRUPPE/DOMÄNE:** An dieser Stelle wird die Arbeitsgruppe oder die Domäne angezeigt, in der sich der Server aktuell befindet. Auch hier wird bei einem Klick auf den Namen das Fenster SYSTEMEIGENSCHAFTEN geöffnet.
- ✓ **WINDOWS DEFENDER FIREWALL:** Zeigt an, ob die Windows-Firewall aktiv ist und für welche Art des Netzwerks (DOMÄNE, PRIVAT, ÖFFENTLICH) die Einstellung gilt. Die Auswahl des Eintrags führt in der Bereich WINDOWS-SICHERHEIT|FIREWALL & NETZWERKSCHUTZ.
- ✓ **REMOTEVERWALTUNG:** Zeigt an, ob die Remoteverwaltung aktiviert wurde. Wird der Eintrag ausgewählt, öffnet sich das Fenster REMOTEVERWALTUNG KONFIGURIEREN. Ist das Kästchen in diesem Fenster ausgewählt, ist es möglich, diesen Server von anderen Computern aus zu verwalten.

- ✓ REMOTEDESKTOP: Zeigt an, ob Remotedesktop-Verbindungen auf diesen Server zugelassen sind. Öffnet das Fenster SYSTEMEIGENSCHAFTEN mit der Registerkarte REMOTE, sodass Sie dort weitere Einstellungen vornehmen können.
- ✓ NIC-TEAMVORGANG: Zeigt an, ob dieser Server an einem NIC-Teamvorgang teilnimmt, bei dem bis zu 32 physische Ethernet-Netzwerkadapter in einem oder mehreren softwarebasierten virtuellen Netzwerkadaptern zusammengefasst werden können. Ein Klick darauf öffnet das Fenster NIC-TEAMVORGANG des Server-Managers, in dem Sie dann eine oder mehrere Netzwerkkarten zu einem Team hinzufügen können.
- ✓ ETHERNET (NAME DES KONFIGURIERTEN NETZWERKADAPTERS): Bei dieser Einstellung wird der Netzwerkstatus Ihres Servers angezeigt. Sie finden dort auch die Netzwerkadresse sowie eine Meldung, falls der Adapter IPv6-fähig ist. Ein Klick darauf öffnet das Fenster SYSTEMSTEUERUNG\NETZWERK UND INTERNET\NETZWERKVERBINDUNGEN.
- ✓ BETRIEBSSYSTEMVERSION: Stellt ebenso wie das nächste Feld HARDWAREINFORMATIONEN einen geschützten Bereich dar: Sie können hier die Informationen zum Betriebssystem und den Vendor-String des Motherboard-Herstellers nur auslesen, aber keine Änderungen vornehmen.
- ✓ ZULETZT INSTALLIERTE UPDATES: Tag und Uhrzeit der zuletzt auf diesem Server installierten Updates. Ein Klick darauf führt Sie in das Untermenü UPDATE UND SICHERHEIT\WINDOWS UPDATE der WINDOWS-EINSTELLUNGEN.
- ✓ WINDOWS UPDATE: Zeigt an, welche Update-Einstellungen auf diesem Server aktiv sind. Der Link führt in das Menü WINDOWS-UPDATE.
- ✓ ZULETZT AUF UPDATES GEPRÜFT: Tag und Uhrzeit der letzten Prüfung auf Updates. Wiederum führt der Link zum Menü WINDOWS-UPDATE.

- ✓ **WINDOWS DEFENDER ANTIVIRUS:** Zeigt den Status des Antivirus-Schutzes an. Der Link führt direkt zum Menü **WINDOWS-SICHERHEIT** und dort in das Untermenü **VIREN- UND BEDROHUNGSSCHUTZ/EINSTELLUNGEN FÜR VIREN- UND BEDROHUNGSSCHUTZ**.
- ✓ **FEEDBACK UND DIAGNOSE:** Ein Klick auf den Link **EINSTELLUNGEN** führt Sie in das Menü **DIAGNOSE UND FEEDBACK**, das Sie im Bereich **DATENSCHUTZ** der **WINDOWS-EINSTELLUNGEN** finden. Hier können Sie wie bei den Windows-10-Systemen auswählen, welche Diagnosedaten Ihr Server wie häufig an Microsoft senden darf.
- ✓ **VERSTÄRKTE SICHERHEITSKONFIGURATION FÜR IE:** Diese Einstellung zeigt an, ob die sogenannte »verstärkte Sicherheitskonfiguration« für den Browser Internet Explorer (IE) auf Ihrem Server aktiviert (Standardeinstellung) oder deaktiviert ist. Ein Klick auf den Link öffnet das Dialogfeld **VERSTÄRKTE SICHERHEITSKONFIGURATION** im Internet Explorer.



Einige Quellen im Internet behaupten zwar etwas anderes – aber der »altgediente« Microsoft-Browser Internet Explorer (IE) ist immer noch Teil der Windows-Distributionen und kommt aktuell auch bei der Installation der Vorabversion des Windows Server 2022 mit auf das System. Ab Windows Server 2019 gilt das allerdings dann nicht, wenn Sie die Core-Version des Servers installieren. Bei der GUI-Version ist der Browser hingegen nach wie vor vorhanden, weshalb Sie dann in den Einstellungen des Server-Managers auch noch die Möglichkeit finden, die verstärkte Sicherheitskonfiguration für diesen Browser ein- beziehungsweise auszuschalten.

Ist diese Funktion eingeschaltet, so ist es praktisch nicht mehr möglich, damit Webseiten aus der **SICHERHEITZONE INTERNET** anzuzeigen. Gerade wenn Sie dann auch mit dem neuen Admin Center auf dem Server arbeiten möchten, raten wir dringend dazu, einen anderen Browser herunterzuladen und zu installieren. Die

aktuelle 64-Bit-Version des Edge-Browsers von Microsoft wird auch auf dem Windows Server 2019 vollständig unterstützt. Dabei eignet sich besonders die Edge-Version, die Microsoft unter der URL <https://www.microsoft.com/de-de/edge/business/download> für Unternehmen bereitstellt. Dort finden Sie auch weitere Informationen zu Versionen und Builds des Browsers.

ZEITZONE: An dieser Stelle wird die Zeitzone des lokalen Servers angezeigt. Ein Klick auf die Daten öffnet das Fenster DATUM UND UHRZEIT.

PRODUKT-ID: Zeigt den Status der Windows-Aktivierung und die Produkt-ID des Betriebssystems Windows Server 2019 an, wenn Sie Ihr System aktiviert haben. Ein Klick darauf führt Sie in den Bereich UPDATE UND SICHERHEIT\AKTIVIERUNG der WINDOWS-EINSTELLUNG.

Bei den drei folgenden Feldern PROZESSOREN, INSTALLIERTER ARBEITSSPEICHER (RAM) und SPEICHERPLATZ INSGESAMT handelt es sich wieder um schreibgeschützte Felder, die Ihnen die Werte dieser Hardware-Ressourcen Ihres Servers anzeigen.

Sind Sie sich nicht sicher, ob die Daten, die im Bereich Eigenschaften angezeigt werden, alle noch auf dem aktuellen Stand sind, so können Sie im Pull-down-Menü von AUFGABEN die Daten durch Auswahl von AKTUALISIEREN auf den neuesten Stand bringen.



Haben Sie den automatischen Start des Server-Managers bei der Anmeldung am Server ausgeschaltet, können Sie ihn ganz einfach sofort starten, indem Sie `servermanager` in der Eingabeaufforderung, an der Kommandozeile einer PowerShell-Sitzung oder im AUSFÜHREN-Fenster, das Sie durch  +  aufrufen, eintippen. Auch im Startmenü Ihres Servers finden Sie eine Kachel für den Server-Manager.

Überblick über das Tools-Menü

Wenn Sie das Tools-Menü des Server-Managers öffnen, bekommen Sie eine ziemlich lange Liste von Programmen und Features angezeigt. Sie können alle diese Werkzeuge – von denen Sie sehr viele auch auf den Windows-10-Systemen finden können – aber auch direkt aus dem STARTMENÜ aufrufen. Rufen Sie das Startmenü des Windows-Servers auf und scrollen Sie in der Liste der Programme nach unten, bis zum Eintrag WINDOWS-VERWALTUNGSPROGRAMME, öffnen Sie diesen Eintrag und Sie werden dort die gleichen Programme finden, die Ihnen auch das Tools-Menü präsentiert hat ([Abbildung 17.7](#)).

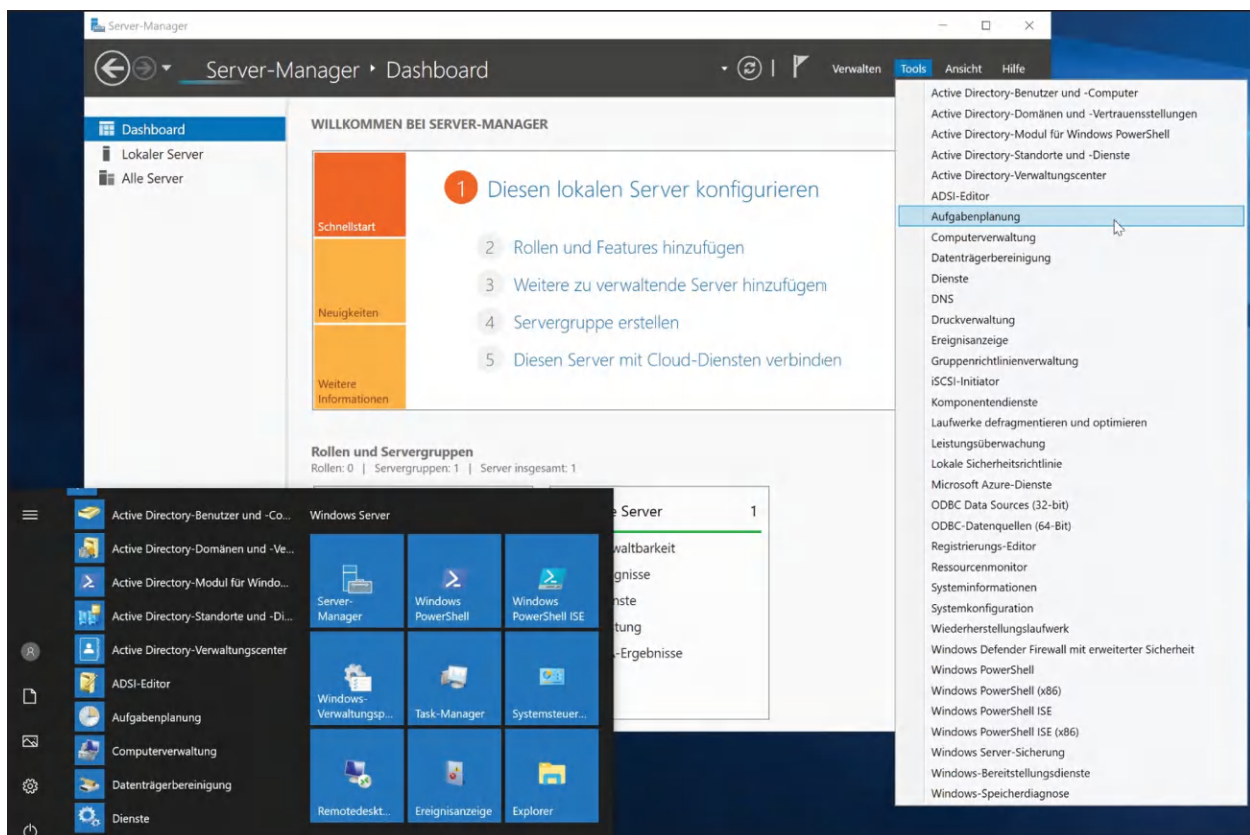


Abbildung 17.7: Mehrere Wege führen zu den Server-Tools: Sie sind aus dem Server-Manager und auch aus dem Startmenü heraus zu erreichen.

Der in [Abbildung 17.7](#) gezeigte Windows Server ist als Domänen-Controller (DC) eingerichtet. Haben Sie Ihren Server nicht als DC konfiguriert, so werden Ihnen die entsprechenden Werkzeuge für die Verwaltung und Betreuung des Verzeichnisdiensts weder im Tools- noch im Startmenü angezeigt.

Viele dieser Tools kennen Sie sicher auch bereits von den Windows-Client-Systemen, auf denen die meisten auch in der gleichen Form zu finden sind. Der Großteil davon präsentiert sich nach dem Aufruf noch in der »alten« Form als Snap-in in einer MMC (Microsoft Management Console), wie es schon seit Windows NT üblich ist. Mit dem voranschreitenden Umbau der Oberfläche der Windows-Systeme werden wir hier in den nächsten Jahren und im Verlauf der kommenden Server-Versionen sicher auch noch einige Änderungen vorfinden. Wir werden im Folgenden einige dieser Software-Werkzeuge, die zum Teil auch in anderen Kapiteln dieses Buchs beschrieben werden, exemplarisch vorstellen:

- ✓ *Computerverwaltung*: Die Computerverwaltung dürfte eines der bekanntesten Werkzeuge sein, das auf allen Windows-Systemen zum Einsatz kommt. Nach wie vor ist es ein sehr nützliches Werkzeug, wenn es um die Verwaltung Ihres lokalen Servers geht. Bietet es Ihnen doch unter anderem Zugriff auf andere Tools wie den Aufgabenplaner oder die Ereignisanzeige ([Abbildung 17.8](#)). Weiterhin können Sie von dort aus auf den Gerätemanager und damit die Hardware des Servers zugreifen und lokal freigegebene Ordner anzeigen und verwalten. Viele der hier vorhandenen Software-Werkzeuge können Sie zudem über einen eigenen Eintrag im Tools-Menü aufrufen.

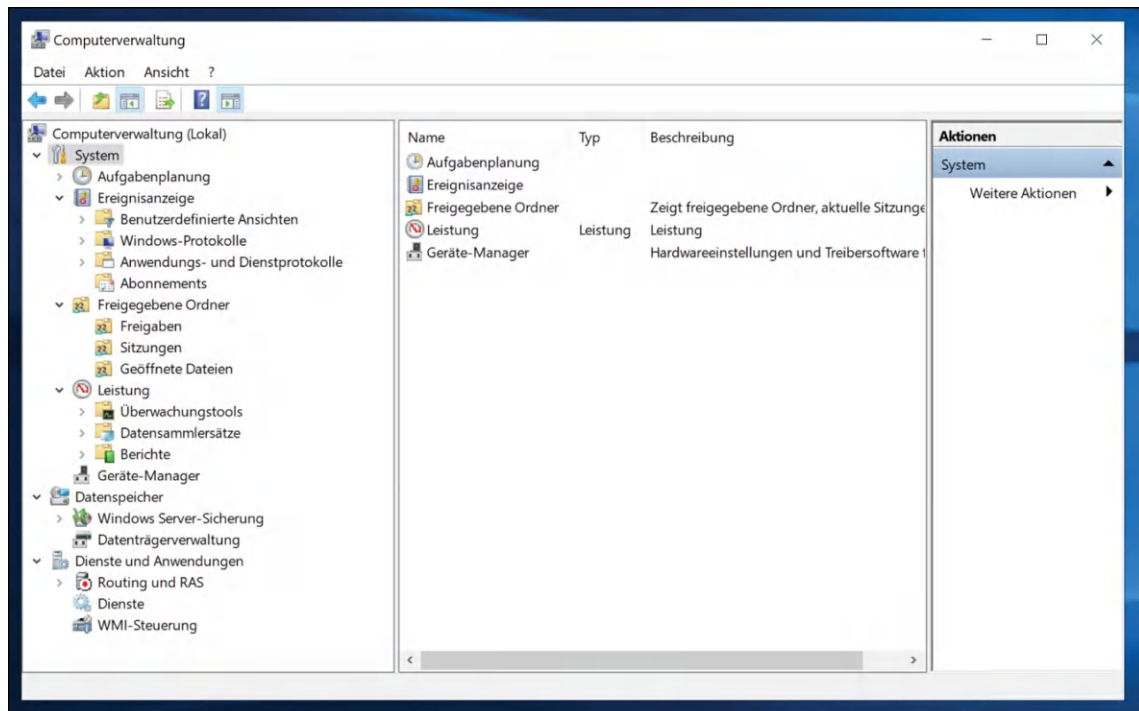


Abbildung 17.8: Viele Tools – wie hier die Computerverwaltung – werden in einer MMC angezeigt und sind auch in anderen Windows-Versionen zu finden.

- ✓ **Ereignisanzeige:** Die Ereignisanzeige (Event Viewer) ist sicher eines der wichtigsten Werkzeuge, wenn es darum geht, den Betrieb aufrechtzuerhalten und Fehler zu lokalisieren. Das Betriebssystem hält im dazugehörigen Protokoll alle Vorgänge fest, die auf Ihrem Server ablaufen. Zudem erfasst es auch noch die unterschiedlichen Warnungen des Systems. So wird die Ereignisanzeige zu einem mächtigen Fehleranalyse-Werkzeug, das Sie bei der Lösung von Hard- und Software-Problemen unterstützen kann. Wer erstmals mit diesem Werkzeug arbeitet, wird sich in der Regel auf die »Standardbereiche« ANWENDUNG, SICHERHEIT und SYSTEM konzentrieren ([Abbildung 17.9](#)), die unter WINDOWS-PROTOKOLLE zu finden sind. Dabei werden unter ANWENDUNG die Informationen zu den Anwendungen und Programmen protokolliert. Unter SICHERHEIT finden Sie Meldungen und Protokolle, die die Sicherheit des Servers betreffen. In diesem Protokoll können Sie dann beispielsweise auch die Meldungen über erfolgreiche oder fehlgeschlagene Anmeldeversuche finden. Unter SYSTEM protokolliert der Server Fehlermeldungen, Warnungen und Informationen des Betriebssystems

und der Systemdienste.

Neben diesen drei Hauptbereichen protokolliert Ihr Windows-Server noch sehr viel mehr Daten, die Sie mithilfe der Ereignisanzeige durchforsten können. Im mittleren Bereich der MMC werden alle Informationen angezeigt, die zu diesem Protokoll gehören. Dabei werden drei Arten unterschieden und entsprechend angezeigt:

- ✓ *Ein Fehler*, dargestellt durch einen roten Kreis mit Ausrufezeichen: Dieses Symbol zeigt Ihnen immer ein größeres Problem an (beispielsweise einen Datenverlust) und erfordert in der Regel ein Eingreifen.

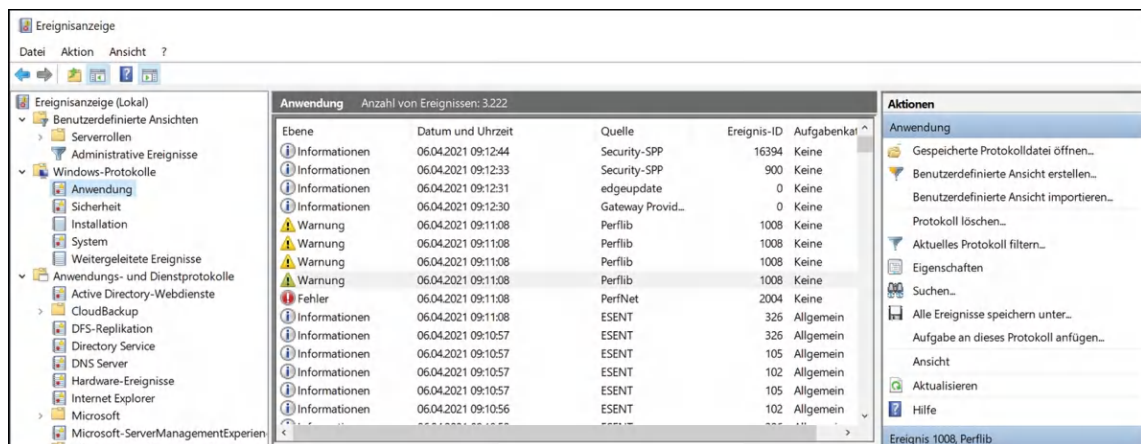


Abbildung 17.9: Die drei Windows-Protokolle »Anwendung«, »Sicherheit« und »System« zeigen bereits viele Vorgänge auf, die auf dem Server ausgeführt wurden.

- ✓ *Eine Warnung*, die durch ein gelbes Dreieck dargestellt wird: Sie weist auf ein Ereignis hin, das zum aktuellen Zeitpunkt nicht unbedingt ein Problem darstellt, sich aber zukünftig zu einem entwickeln könnte.
- ✓ *Informationen*, die durch ein blaues Ausrufezeichen in einem Kreis dargestellt werden: Sie signalisieren Ihnen, dass ein Dienst, ein Treiber oder auch ein Programm erfolgreich ausgeführt wurde.

Weitere Werte, die wichtig werden können, sind die Quelle und die Ereignis-ID. Durch diese Daten bekommen Sie Informationen zur jeweils betroffenen Systemkomponente sowie zur möglichen Ursache für ein Ereignis.

In der rechten Spalte der Ereignisanzeige finden Sie die AKTIONEN: Sie können an dieser Stelle die Protokolle beispielsweise nach Schlüsselwörtern durchsuchen oder bei Bedarf auch gleich komplett löschen. Dazu dient der Eintrag PROTOKOLL LÖSCHEN, den Sie ebenfalls bei den Aktionen finden. Das ist von Zeit zu Zeit durchaus sinnvoll, da auf einem Windows-Server sehr viele solcher Meldungen auftreten und in die Protokolle wandern. Mit dem Eintrag ALLE EREIGNISSE SPEICHERN UNTER... können Sie diese Daten zuvor noch in einer Datei mit der Endung *.evtx ablegen und diese dann später über GESPEICHERTE PROTOKOLLDATEN ÖFFNEN... wieder in die Ereignisanzeige hineinladen.

Kapitel 18

Das Windows Admin Center

IN DIESEM KAPITEL

Was ist das Windows Admin Center (WAC)?

Installation und Einrichtung des Admin Centers

Konfiguration und erster Einsatz

Grundsätzliche Einstellungen und Erweiterungen

Tools und Features

Wer eine Software sucht, um einen oder auch mehrere Windows Server zu verwalten, wird bei einem schnellen Blick ins World Wide Web eine große und kaum zu überschauende Zahl an entsprechend Lösungen finden. Aber auch Microsoft ist nicht untätig: So zeigen alle aktuellen Versionen von Windows Server von der Version 2012 über 2016 bis hin zu 2019 und 2022 beim Start des Server-Managers einen Hinweis auf das sogenannte Windows Admin Center (WAC), das als »Nachfolgeversion« des Server-Managers zum Download bereitsteht.

Aber auch wenn es aktuell so aussehen mag, als ob Microsoft dann irgendwann in der näheren Zukunft die Verwaltung des Servers ganz auf diesen Ansatz umstellen möchte, bietet die Vorabversion des Windows Server 2022 nach wie vor den Server-Manager als Standardanwendung für die Verwaltung des Betriebssystems an.

Was ist das Windows Admin Center (WAC)?

Trotzdem ist es natürlich sinnvoll, sich schon einmal etwas genauer mit

dieser »moderner« Version der Server-Verwaltung zu befassen. Da das Admin Center problemlos und ohne Datenverlust parallel zum Server-Manager genutzt werden kann, sollten Sie unbedingt einen Blick darauf werfen. Dabei müssen Sie sich aber immer bewusst machen, dass die Software – wie alle Produkte aus dem Cloud-Umfeld von Microsoft – laufend weiterentwickelt wird. So kann es Ihnen durchaus passieren, dass ein Feature plötzlich an andere Stelle zu finden ist oder von den Entwicklern herausgenommen wurde.



Sie können mit dem Windows Admin Center Systeme unter Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows 10 sowie Azure Stack HCI (Hyperconverged Infrastruktur) verwalten. Weitere Versionen können beispielsweise auch über in Domänen eingebundene Windows-10-Instanzen verwaltet werden, auf denen das Windows Admin Center Gateway installiert ist. Der Zugriff auf das WAC erfolgt immer über einen Browser, wobei Microsoft hier den eigenen Edge- oder den Google-Chrome-Browser als »moderne Browser« empfiehlt. Wir haben im Testbetrieb auf allen Windows-Systemen den aktuellen Edge-Browser eingesetzt, der ja auf Chromium aufbaut und Teil der aktuellen Server-Distributionen ist. Dabei gab es weder bei der Darstellung noch bei den Zugriffen irgendwelche Probleme. Wer den Mozilla Firefox einsetzen will, der von Microsoft offiziell für WAC nicht unterstützt wird, kann in der Dokumentation ([Abbildung 18.1](#)) auf den Microsoft-Seiten unter »Bekannte Probleme im Windows Admin Center« einige Hinweise zu dessen Einsatz finden: <https://docs.microsoft.com/de-de/windows-server/manage/windows-admin-center/support/known-issues>.

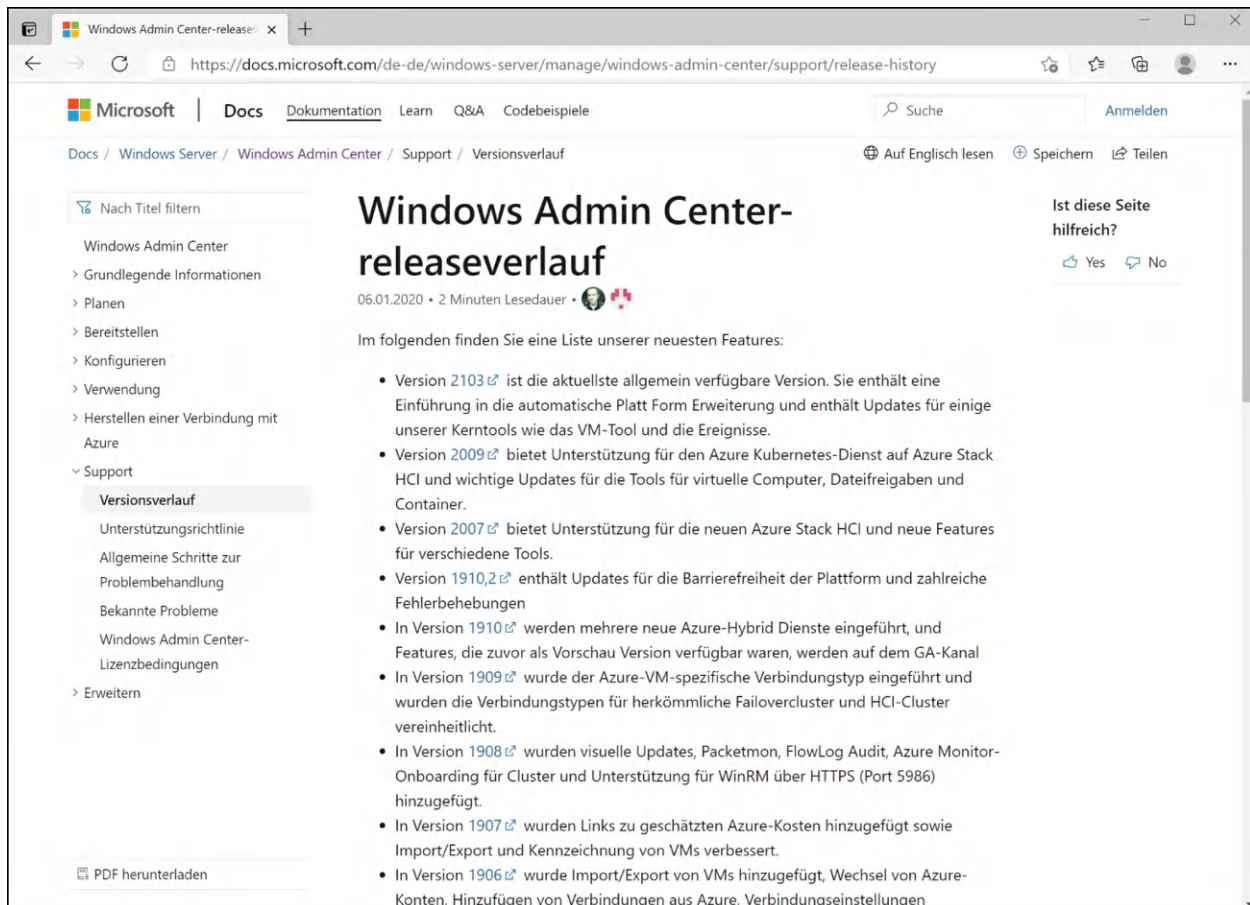


Abbildung 18.1: Wer das Windows Admin Center einsetzen will, kann sich auf Microsofts Webseiten über den jeweiligen Stand der Software informieren.

Installation

Wenn Sie dem von Microsoft angebotenen Link zum Download des Admin Centers folgen, landen Sie im sogenannten »Windows Server Evaluation Center«. Dort finden Sie die Software dann in der Kategorie der Server-Testversionen. Die Bezeichnung als Evaluierungsversion ist dabei allerdings etwas missverständlich: Es handelt sich bei dieser Lösung um eine Freeware-Version, die unbeschränkt und – anders als die anderen Programme auf dieser Webseite – nicht nur 180 Tage verwendet werden kann. Zudem steht dieses Tool ausdrücklich auch für den produktiven Einsatz zur Verfügung. Seit März 2021 ist die Lösung unter der Versionsnummer 2103 auch allgemein verfügbar.

Nachdem Sie Ihren Namen und die E-Mail-Adresse in einem

Onlineformular eingegeben haben, können Sie die nur circa 70 MByte große MSI-Datei dann installieren. Dabei haben Sie die Wahl, wo Sie die Software installieren möchten. Microsoft schlägt vier unterschiedliche Szenarien für die Installation vor:

- ✓ direkt auf einem lokalen Client-Rechner unter Windows 10,
- ✓ auf einem sogenannten Gatewayserver mit Zugriff von den Clients,
- ✓ direkt auf einem der verwalteten Server im Netzwerk, beispielsweise auf dem Mitglieds-knoten eines Clusters, oder
- ✓ Bereitstellung auf einem Failover-Cluster.

Die unterschiedlichen Installationen unterscheiden sich nur unwesentlich voneinander. Wir beschreiben die Installation auf einem Windows Server 2019 beziehungsweise Windows Server 2022 als Gatewayserver:

1. Nach dem Download starten Sie die MSI-Datei mit einem Doppelklick.
2. Ein Setup-Assistent startet und präsentiert Ihnen die Lizenzbedingungen, denen Sie zustimmen müssen, damit die Installation beginnen kann.
3. Danach müssen Sie entscheiden, ob Sie mit dieser Software nur **ERFORDERLICHE DIAGNOSEDATEN** oder **ERFORDERLICHE UND OPTIONALE DIAGNOSEDATEN** an Microsoft übersenden wollen – ganz ohne Datenübermittlung geht es nicht.
4. Nun folgt die Frage, ob Sie Updates durch Microsoft Update zulassen möchten ([Abbildung 18.2](#)). Diese Einstellung sollten Sie auf jeden Fall auswählen.
5. Im nächsten Fenster treffen Sie dann die wichtige Entscheidung, wo Ihr Admin Center installiert wird. Haben Sie die Installation auf einem Windows-Server gestartet, so schlägt Ihnen das Programm gleich die sinnvolle Installation als Gatewayserver vor ([Abbildung 18.3](#)). Ein Link in diesem Fenster zeigt Ihnen zudem den Weg zu mehr Informationen in Verbindung mit den verschiedenen Installationsmöglichkeiten.

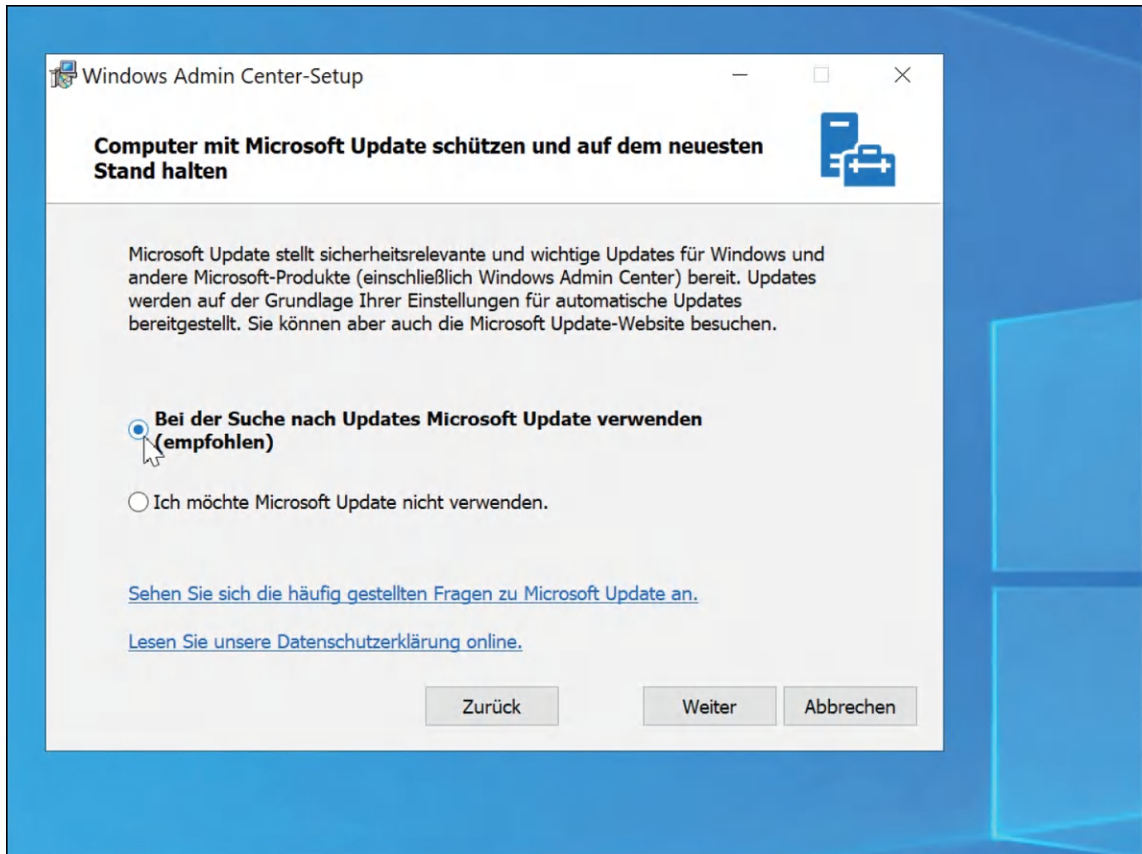


Abbildung 18.2: Bei der Installation des WAC entscheiden Sie auch, ob Sie Microsoft Update einsetzen möchten.

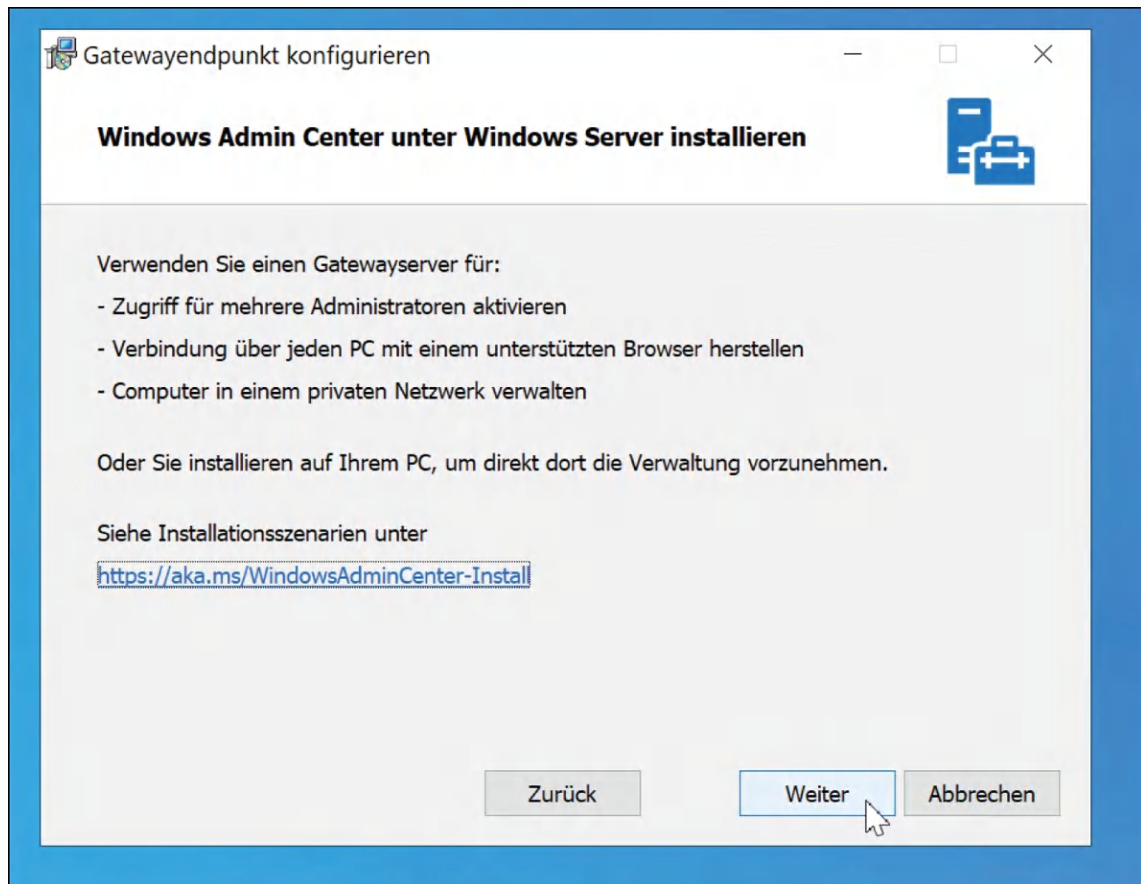


Abbildung 18.3: Für die Installation auf einem Stand-alone-Server ist der Einsatz als Gatewayserver eine sinnvolle Wahl.

6. Im nächsten Schritt dreht sich alles um die Remote-Verwaltung: Sie können hier festlegen, ob Sie dem Windows Admin Center das Ändern der vertrauenswürdigen Hosts erlauben. Wenn diese Option nicht schon automatisch ausgewählt ist ([Abbildung 18.4](#)), ist es sinnvoll, sie einzuschalten, damit Sie keine Probleme bei der Erreichbarkeit der Systeme bekommen. In diesem Fenster können Sie dann ebenfalls festlegen, dass WinRM (Windows Remote Management) ausschließlich über eine HTTPS-Verbindung möglich ist. Diese Einstellung sollten Sie dann wählen, wenn Sie sicher sind, dass alle mit diesem WAC zu verwaltenden Systeme auch auf diese Weise erreichbar sind.

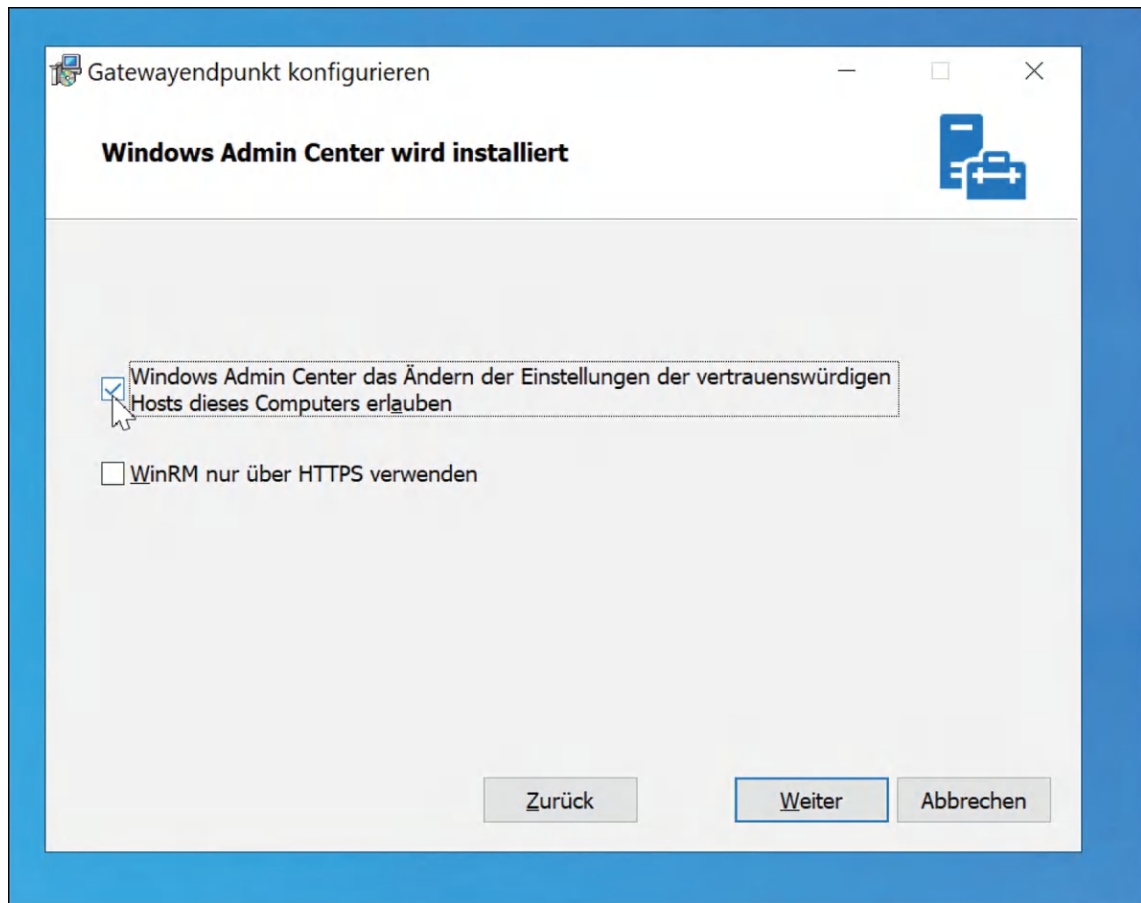


Abbildung 18.4: Es erleichtert die Verwaltung entfernter Systeme mit dem WAC, wenn Sie das Ändern der vertrauenswürdigen Hosts erlauben.

7. Das Windows Admin Center wird auf einem Windows-Server als Netzwerkdienst installiert. Deshalb müssen Sie im letzten Schritt der Installation den Port angeben, den der Dienst überwacht. Dies ist in der Regel der Port 443 und erfordert ein Zertifikat für das Protokoll HTTPS. Dazu kann das Installationsprogramm zu Testzwecken ein selbst signiertes Zertifikat erstellen, das dann 60 Tage gültig ist ([Abbildung 18.5](#)). Sie können aber auch den Fingerabdruck eines Zertifikats bereitstellen, der bereits auf dem Computer installiert ist. Wenn Sie das generierte Zertifikat verwenden, wird es dadurch dem DNS-Namen des Servers entsprechen. Danach können Sie INSTALLATION auswählen, und das Windows Admin Center wird auf Ihrem Server installiert.

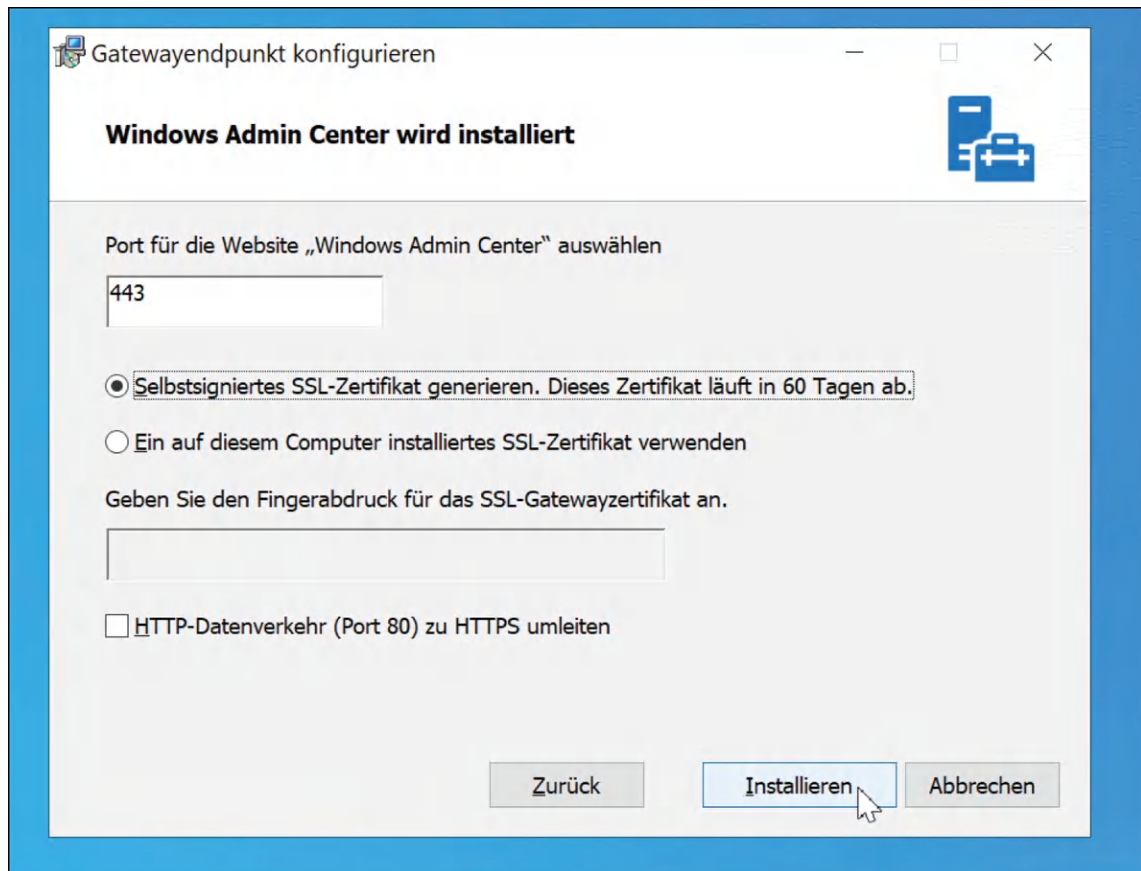


Abbildung 18.5: Der letzte Schritt: Port für den Dienst angeben und Zertifikat zuweisen

Konfiguration und erster Einsatz

Leider taucht das Windows Admin Center nach der Installation nicht automatisch in der Liste der installierten Apps des Startmenüs aus. Darum ist es wichtig, dass Sie den letzten Bildschirm der Installation des WAC beachten. Denn dort ([Abbildung 18.6](#)) bekommen Sie die Information, wie Sie das Admin Center starten und Zugriff auf die Informationen bekommen. Mit dieser Adresse können Sie sich dann natürlich ebenso von einem anderen Rechner aus, der sich in Ihrem Netzwerk befindet, mit dem Admin Center verbinden. Anschließend müssen Sie sich noch mit einem Konto aus der Gruppe der Administratoren ([Abbildung 18.6](#)) im Browser-Fenster anmelden.

Nach der Anmeldung bekommen Sie eine Übersicht über alle Verbindungen angezeigt, die Sie in Ihrem Admin Center konfiguriert

haben. Diese Übersicht wird beim ersten Start nur das System anzeigen, auf dem Ihr Admin Center installiert ist. In unserem Fall ist es ein Windows Server 2019, den wir als Gateway eingerichtet haben ([Abbildung 18.7](#)).

Auf dieser Übersichtsseite können Sie nun Server und Workstations hinzufügen, die Sie mit WAC überwachen und verwalten wollen.

1. Wählen Sie auf der oberen Leiste unter ALLE VERBINDUNGEN den Eintrag +HINZUFÜGEN aus.

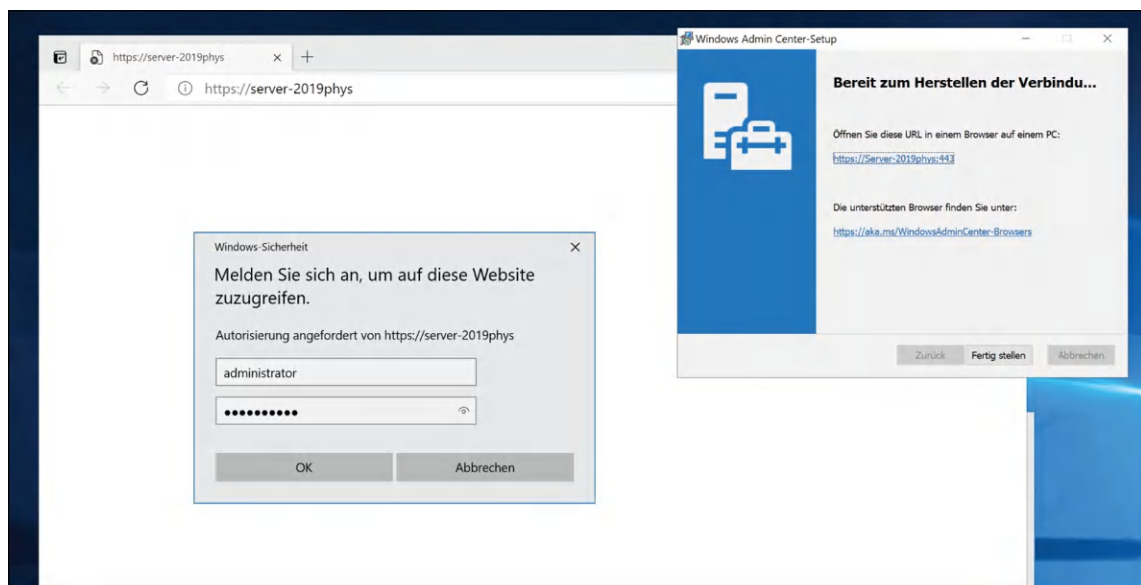


Abbildung 18.6: Wie starte ich das Windows Admin Center? Der Setup-Assistent gibt Auskunft.

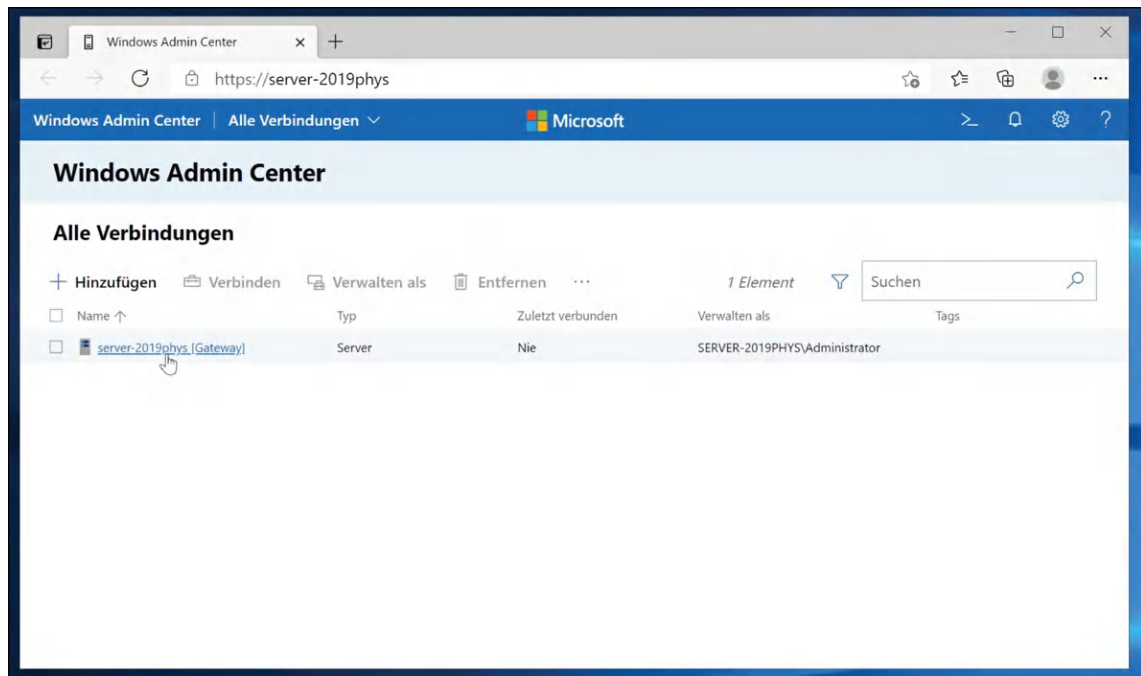


Abbildung 18.7: Der erste Start: Noch ist nur der Windows-Server, auf dem das WAC installiert ist, in der Übersicht zu sehen.

2. Sie können nun einen Server, einen Windows-10-PC, ganze Server-Cluster oder auch eine virtuelle Maschine unter Azure hinzufügen, indem Sie die entsprechende Kachel auswählen ([Abbildung 18.8](#)). Wir haben für dieses Beispiel eine Installation des Windows Admin Centers auf der Vorabversion des Windows Server 2022 gewählt. Das Vorgehen unterscheidet sich dabei in keiner Weise von dem auf einem Windows Server 2019.

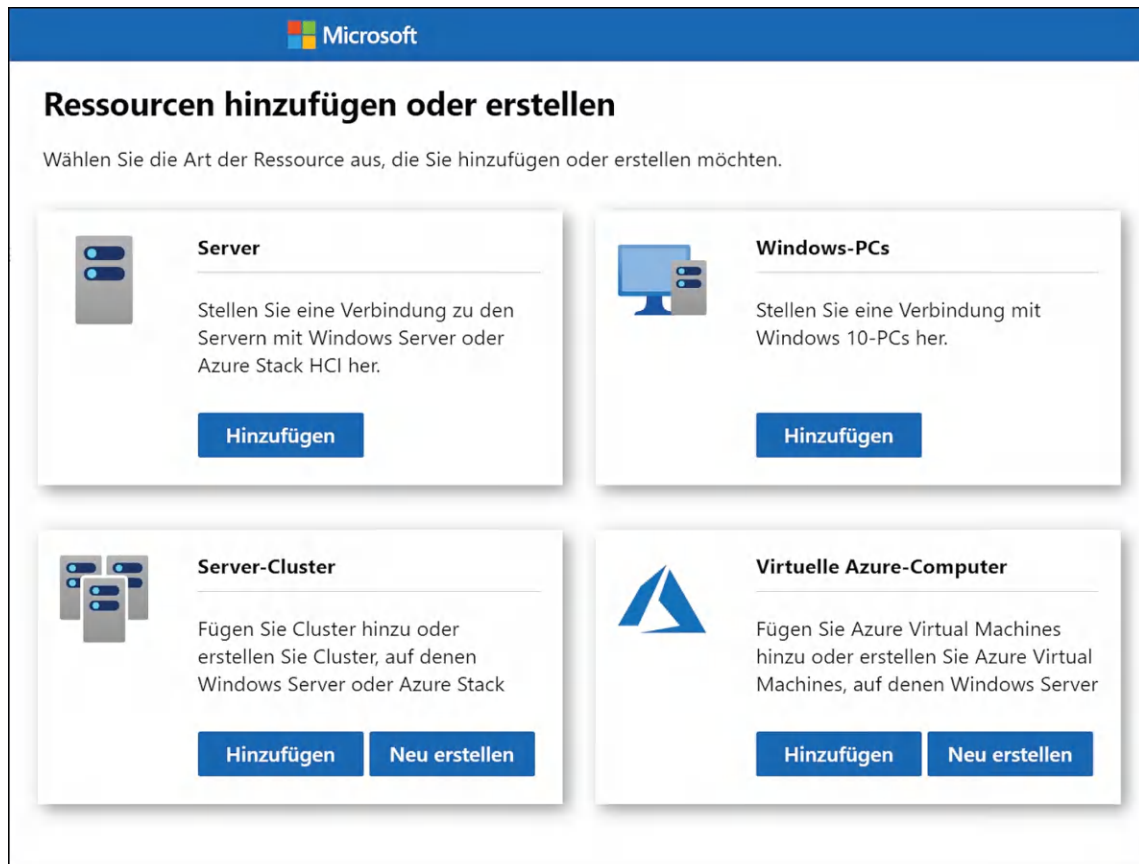


Abbildung 18.8: Auswahl und Hinzufügen einer Ressource zum WAC auf einem Windows Server 2022

3. Wir haben einen Windows Server 2016 in unserem Netzwerk ausgewählt, den wir hier hinzufügen wollen. Das gelingt über Eingabe des Namens des Servers oder auch durch Suche eines Systems im Active Directory, wenn die Rechner in einer AD-Domäne eingebunden sind. Als dritte Möglichkeit steht Ihnen wie in [Abbildung 18.9](#) zu sehen, unter LISTE IMPORTIEREN die Möglichkeit zur Verfügung, eine ganze Liste mit Servern zu importieren. Diese können dann alle auf einmal in das Admin Center hineingebracht werden. Dazu kann eine Text- oder .csv-Datei (*comma-separated values*) verwendet werden. In dieser Datei sind dann die Systeme mit ihren FQDN (Fully-Qualified Host Name – »vollständig angegebener Rechnername«) aufgelistet.
4. Wählen Sie dann MIT ANMELDEINFORMATIONEN HINZUFÜGEN oder nur HINZUFÜGEN aus, und das System erscheint unter »Alle Verbindungen« in der Übersicht. Diesen

Vorgang zeigt das WAC auch noch einmal an, wie Sie in [Abbildung 18.10](#) sehen können. Alle Benachrichtigungen des Admin Centers finden Sie, wenn Sie auf das Glocken-Symbol rechts oben in der blauen Leiste klicken.



Wenn Sie mehrere Systeme mit dem Windows Admin Center von Ihrem Windows-Server aus verwalten wollen, ist das Thema »Authentifizierung« wichtig. Das WAC bietet Ihnen unterschiedliche Möglichkeiten der Anmeldung bei den Remote-Systemen. Die Standardeinstellung ist ein »Single Sign-on«, bei dem Sie Ihre aktuellen Windows-Anmeldeinformationen zur Authentifizierung verwenden. Haben Sie WAC auf einem Windows-Server als Dienst installiert, ist für eine einmalige Anmeldung eine zusätzliche Konfiguration notwendig: Nähere Informationen dazu finden Sie unter <https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/configure/user-access-control> (nutzen Sie bitte diese englischsprachige Version, die maschinelle deutsche Übersetzung ist in einigen Punkten missverständlich). Schließlich bietet Ihnen das Admin Center als dritte Methode noch die Möglichkeit, in der oberen Leiste unter ALLE VERBINDUNGEN den Eintrag VERWALTEN ALS auszuwählen. Dazu müssen Sie allerdings zunächst die Kästchen vor den Systemen markieren, die Sie damit bearbeiten wollen ([Abbildung 18.11](#)). Sie können diese Anmeldeinformationen auch für alle Ihre Verbindungen nutzen. Dadurch werden sie für diese Browser-Sitzung im Cache abgespeichert. Starten oder laden Sie den Browser neu, so müssen Sie die Anmeldedaten für VERWALTEN ALS neu eingeben. Ausführlichere Information dazu finden Sie in der Microsoft-Dokumentation unter <https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/use/get-started>.

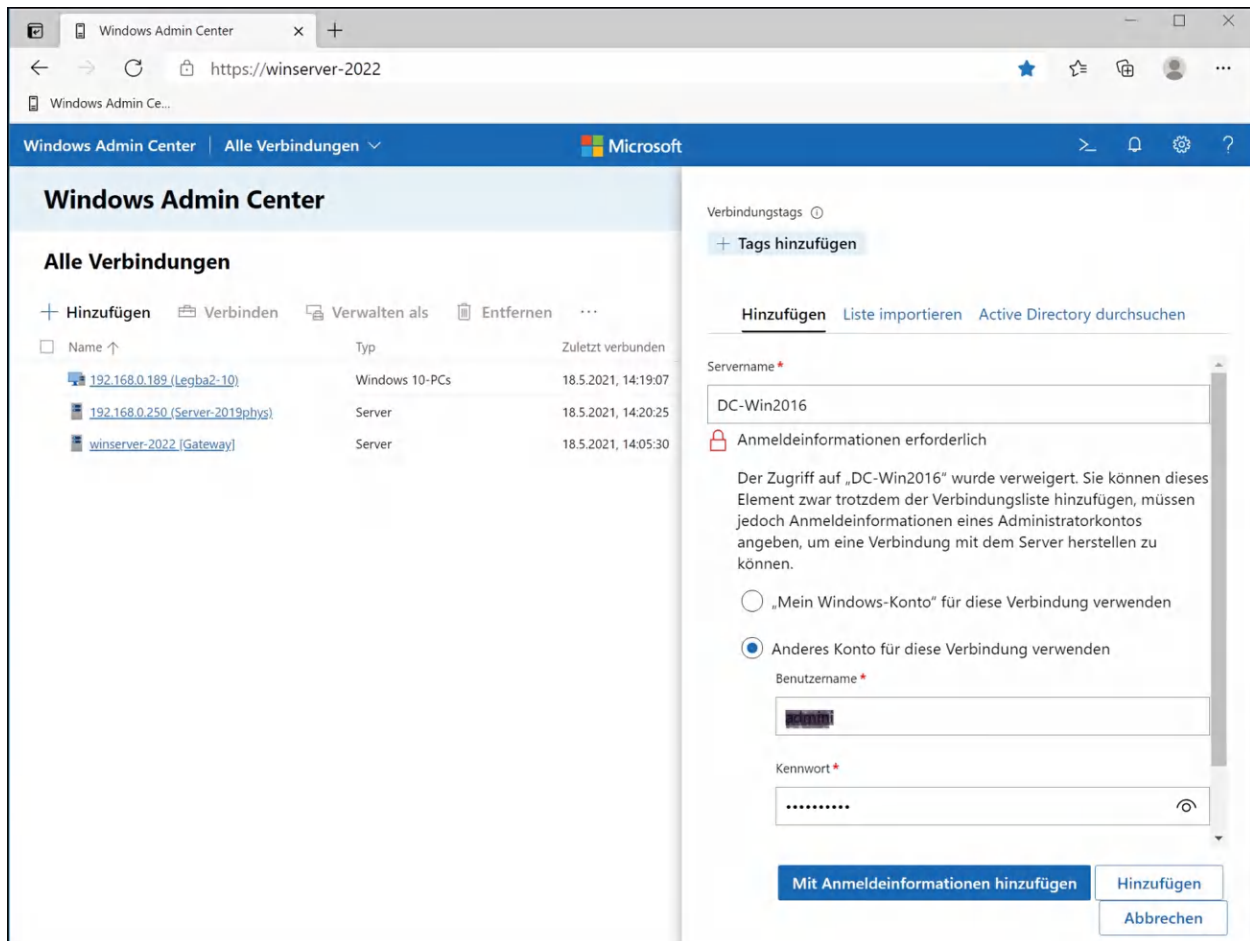


Abbildung 18.9: Das Hinzufügen eines Servers zum Windows Admin Center

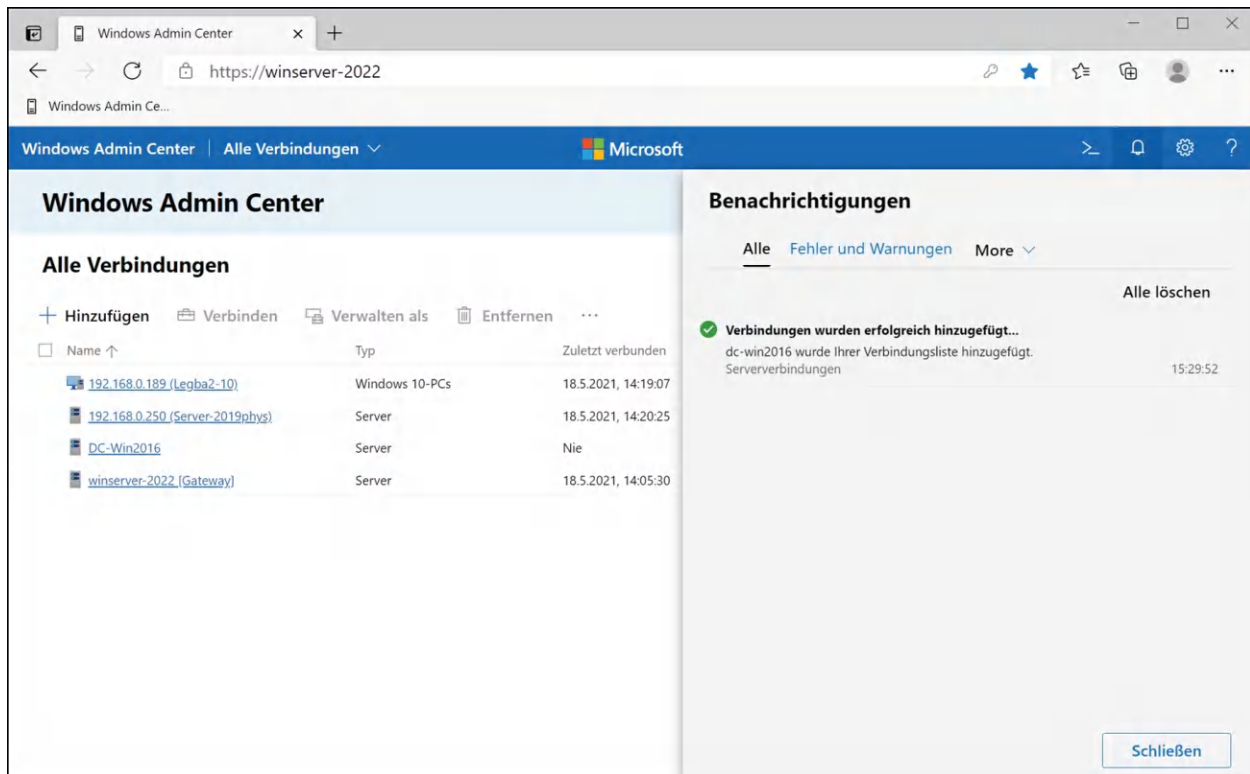


Abbildung 18.10: Der neue Server wurde hinzugefügt und erscheint in der Übersicht. WAC gibt dazu die entsprechende Meldung aus.

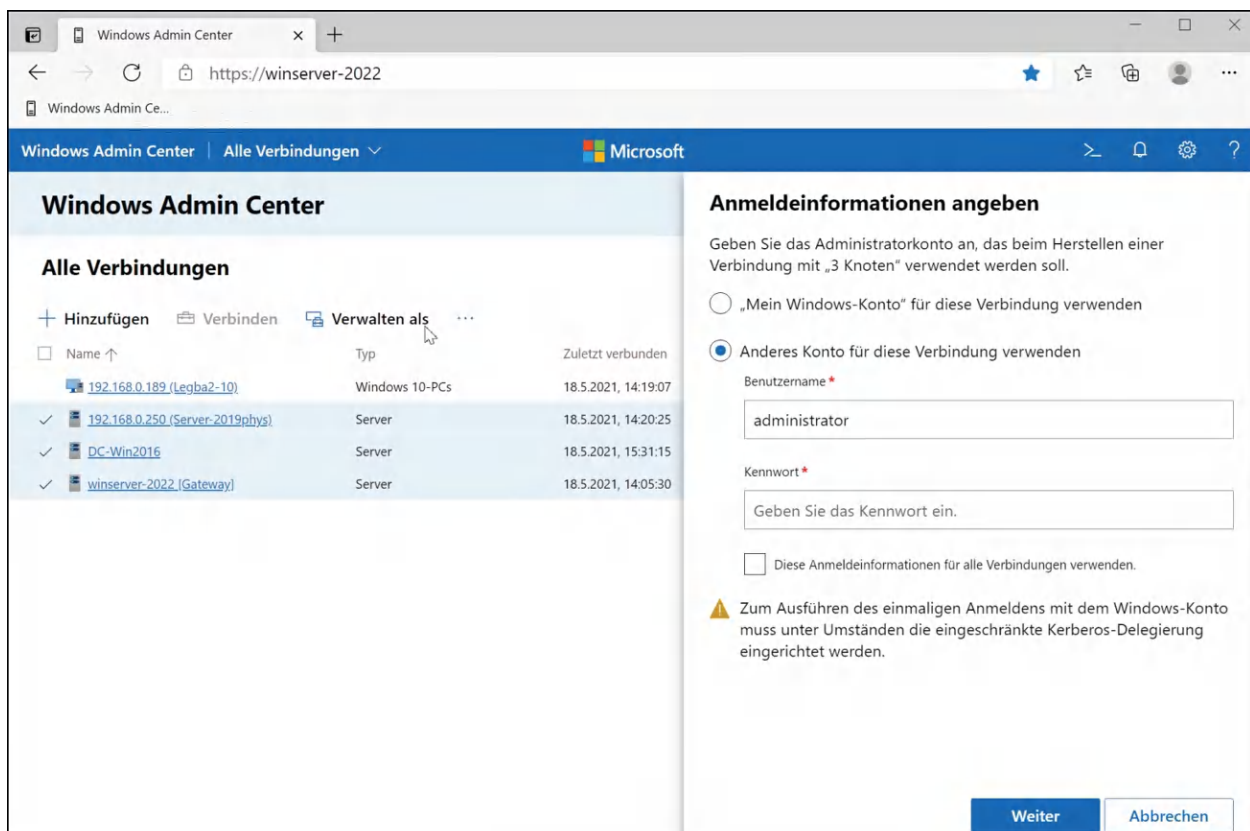


Abbildung 18.11: Mehrere Systeme mit den gleichen Anmeldedaten einzubinden, gelingt unter anderem über die Einstellung »Verwalten als«.

Grundsätzliche Einstellungen und Erweiterungen

Wie alle Anwendungen unter Windows können Sie auch das Windows Admin Center in gewissem Umfang nach Ihren Vorstellungen einstellen. Die grundsätzlichen Einstellungen für das WAC finden Sie, wenn Sie das Zahnradsymbol wählen, das Sie rechts in der blauen Leiste im oberen Bereich des Browser-Fensters finden.

Nach dieser Auswahl bekommen Sie zunächst Ihre Kontoinformationen präsentiert ([Abbildung 18.12](#)). Zudem können Sie in diesem Fenster erkennen, dass die Einstellungen des Windows Admin Centers hier in die drei Bereiche BENUTZER, ENTWICKLUNG und GATEWAY unterteilt sind. Wenn Sie im Bereich BENUTZER Änderungen vornehmen, so wirken sich diese dann nur auf den aktuell angemeldeten Benutzer aus. Ändern Sie hingegen Einstellungen im Bereich GATEWAY, so wirken sich diese auf alle Nutzer dieses WAC-Gateways aus. Im Bereich ENTWICKLUNG können Sie unter anderem das sogenannte Entwicklerhandbuch laden und sich dieses dann anzeigen lassen.

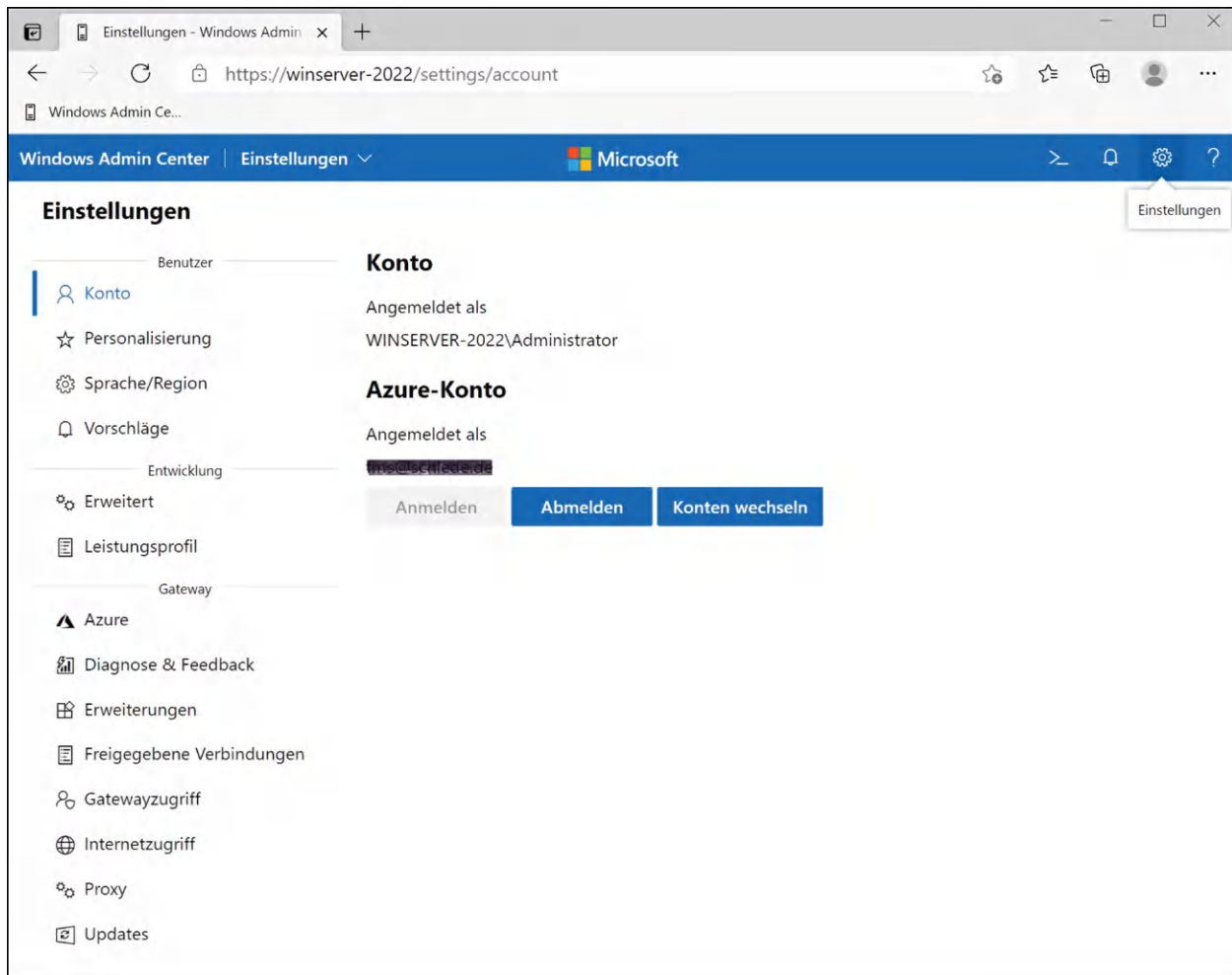


Abbildung 18.12: Nach Auswahl der Einstellungen werden dem Nutzer zunächst die Konten im Bereich »Benutzer« präsentiert.

Wie Sie in [Abbildung 18.12](#) sehen können, wird Ihnen unter KONTTO die Anmeldeinformation angezeigt, mit der Sie sich beim Windows Admin Center authentifiziert haben. Wollen Sie sich von hier aus mit Ihrem Azure-Konto an- beziehungsweise abmelden, so muss das Azure Active Directory als Identitätsanbieter konfiguriert sein. Diese Einstellung können Sie wiederum im Bereich GATEWAY beim Eintrag AZURE vornehmen.

Hinter PERSONALISIERUNG im Bereich BENUTZER verbirgt sich nur die Möglichkeit, WAC im sogenannten »dunklen Modus«, also mit einer Oberfläche in dunklen Farben, zu verwenden. Schließlich können Sie in diesem Menübereich noch die SPRACHE/REGION für Ihr Admin Center konfigurieren und unter VORSCHLÄGE die verschiedenen Mitteilungen

an- beziehungsweise ausschalten, die Ihnen über das WAC mitgeteilt werden. Stört es Sie beispielsweise, dass die Software Sie regelmäßig (alle 90 Tage) dazu auffordert, ein Feedback abzugeben, so können Sie das an dieser Stelle abstellen.

Im Bereich GATEWAY können Sie unter dem Menüpunkt AZURE das Gateway bei der Cloud-Plattform Azure registrieren, sodass Sie diese Dienste im Windows Admin Center nutzen und integrieren können. Genau wie auf dem Server selbst, können Sie unter DIAGNOSE & FEEDBACK auswählen, welche Diagnosedaten Sie an Microsoft senden wollen. Unter GATEWAYZUGRIFF können Sie festlegen, welche Nutzer und Gruppen auf das Windows Admin Center Gateway zugreifen dürfen und welcher Identitätsanbieter zum Authentifizieren verwendet wird. Wie Ihr WAC-Gateway auf das Internet zugreifen kann, können Sie unter INTERNETZUGRIFF festlegen ([Abbildung 18.13](#)).

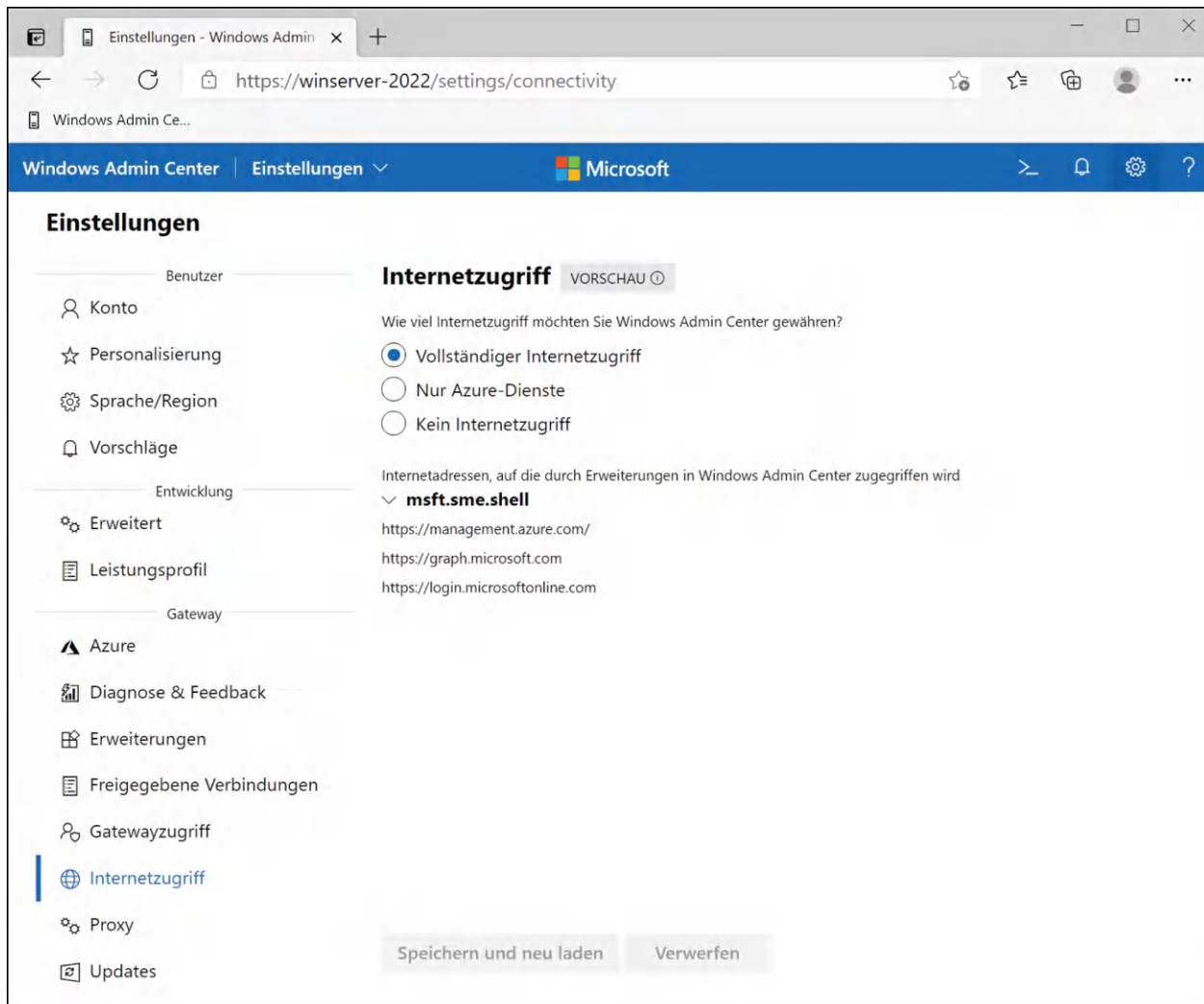
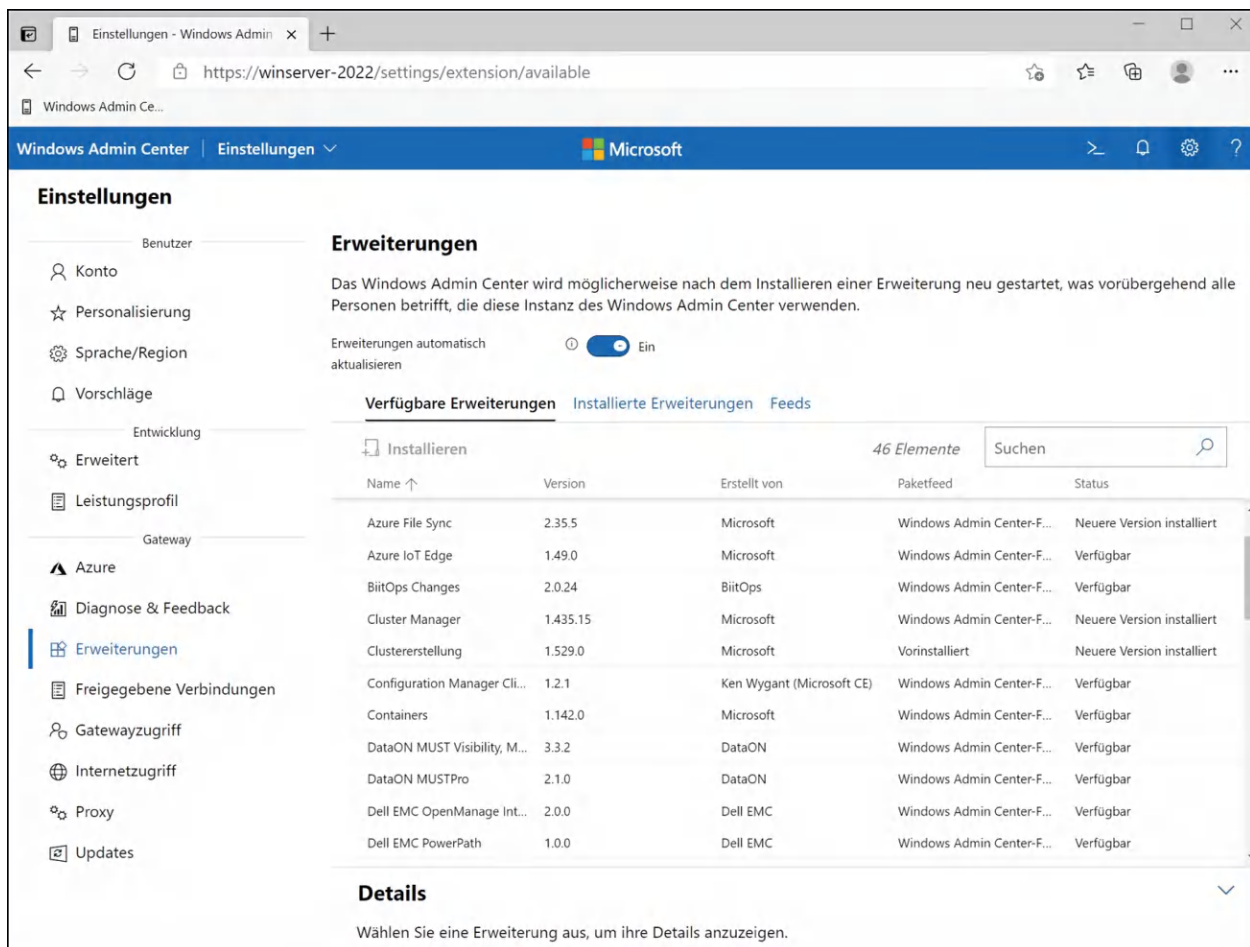


Abbildung 18.13: Wie kann das WAC auf das Internet zugreifen? Manchmal kann es durchaus sinnvoll sein, nur Azure-Dienste zu erlauben.

Einen sehr wichtigen Bereich finden Sie unter dem Eintrag **ERWEITERUNGEN** in diesem Menü. Microsoft hat das WAC als erweiterbare Plattform konzipiert. Schon bei der Installation haben Sie vermutlich bemerkt, dass Ihr Windows Admin Center standardmäßig eine ganze Anzahl von Erweiterung mitbringt und installiert. Laut der Microsoft-Dokumentation (<https://docs.microsoft.com/de-de/windows-server/manage/windows-admin-center/configure/using-extensions>) kann jeder Verbindungstyp ebenso wie jedes Tool eine solche Erweiterung darstellen. Sie können diese einzeln installieren, deinstallieren und auch aktualisieren. Wählen Sie im Menübereich **GATEWAY** die **ERWEITERUNGEN** aus, so bekommen Sie zunächst

eine Übersicht über verfügbare Erweiterungen präsentiert ([Abbildung 18.14](#)). Sie bekommen nicht nur den Namen der jeweiligen Erweiterung angezeigt, Sie sehen auch sofort in der Spalte STATUS, ob diese Erweiterung aktuell verfügbar ist oder eine neue Version bereits installiert wurde. Woher kommen diese Erweiterungen? Das können Sie dann in der Spalte PAKETFEED sehen. Dort sehen Sie auch, dass bei einem Großteil der Erweiterungen als Quelle Windows Admin Center ausgewiesen wird, es aber auch vorinstallierte Erweiterungen gibt.



Einstellungen

Benutzer

- Konto
- Personalisierung
- Sprache/Region
- Vorschläge

Entwicklung

- Erweitert
- Leistungsprofil

Gateway

- Azure
- Diagnose & Feedback
- Erweiterungen**
- Freigegebene Verbindungen
- Gatewayzugriff
- Internetzugriff
- Proxy
- Updates

Erweiterungen

Das Windows Admin Center wird möglicherweise nach dem Installieren einer Erweiterung neu gestartet, was vorübergehend alle Personen betrifft, die diese Instanz des Windows Admin Center verwenden.

Erweiterungen automatisch aktualisieren ☒ Ein

Verfügbare Erweiterungen **Installierte Erweiterungen** **Feeds**

46 Elemente

Name ↑	Version	Erstellt von	Paketfeed	Status
Azure File Sync	2.35.5	Microsoft	Windows Admin Center-F...	Neuere Version installiert
Azure IoT Edge	1.49.0	Microsoft	Windows Admin Center-F...	Verfügbar
BitOps Changes	2.0.24	BitOps	Windows Admin Center-F...	Verfügbar
Cluster Manager	1.435.15	Microsoft	Windows Admin Center-F...	Neuere Version installiert
Clustererstellung	1.529.0	Microsoft	Vorinstalliert	Neuere Version installiert
Configuration Manager Cli...	1.2.1	Ken Wygant (Microsoft CE)	Windows Admin Center-F...	Verfügbar
Containers	1.142.0	Microsoft	Windows Admin Center-F...	Verfügbar
DataON MUST Visibility, M...	3.3.2	DataON	Windows Admin Center-F...	Verfügbar
DataON MUSTPro	2.1.0	DataON	Windows Admin Center-F...	Verfügbar
Dell EMC OpenManage Int...	2.0.0	Dell EMC	Windows Admin Center-F...	Verfügbar
Dell EMC PowerPath	1.0.0	Dell EMC	Windows Admin Center-F...	Verfügbar

Details

Wählen Sie eine Erweiterung aus, um ihre Details anzuzeigen.

Abbildung 18.14: Das Windows Admin Center kann mit vielen Erweiterungen ergänzt werden.



Für die Erweiterungen des Windows Admin Centers kommen sogenannte NuGet-Feeds zum Einsatz. Bei NuGet handelt es sich um ein System, das die freie Verteilung von Software-Komponenten in

Form von Paketen ermöglicht. NuGet ist der von Microsoft unterstützte Mechanismus zur Freigabe von Programmcode für .NET und .NET Core (<https://docs.microsoft.com/de-de/nuget/what-is-nuget>). Administratoren können im WAC weitere NuGet-Feeds oder auch eine gesonderte Dateifreigabe konfigurieren. Das ist besonders dann sinnvoll, wenn auf diese Weise Erweiterungen zur internen Verwendung innerhalb einer Firma verteilt werden sollen.

Wenn Sie eine neue Erweiterung installieren wollen, können Sie folgendermaßen vorgehen:

1. Wechseln Sie in die EINSTELLUNGEN und wählen Sie dort in der linken Spalte ERWEITERUNGEN aus.
2. Wechseln Sie nun zur Registerkarte VERFÜGBARE ERWEITERUNGEN ([Abbildung 18.15](#)).

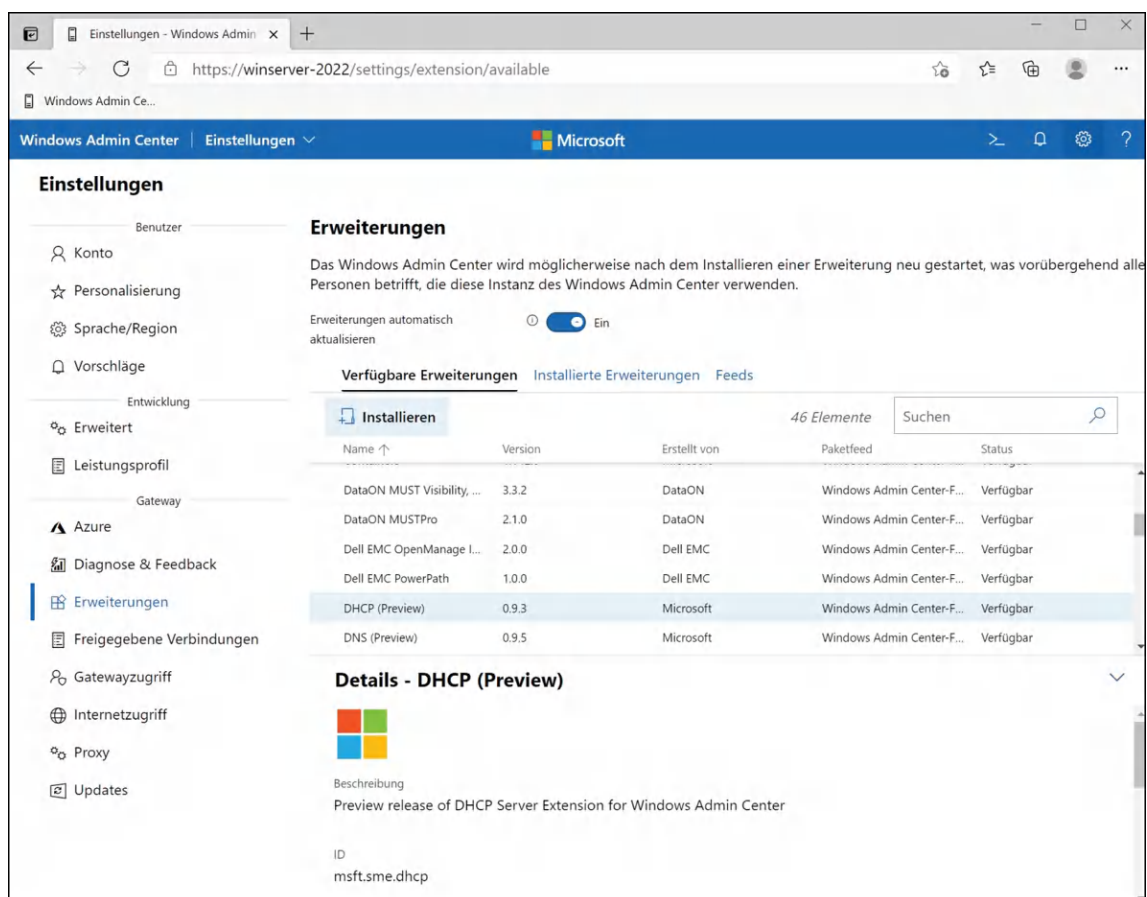


Abbildung 18.15: WAC zeigt die verfügbaren Erweiterungen mitsamt deren Details an.

3. Mit einem Klick auf die entsprechende Erweiterung bekommen Sie unter DETAILS eine Beschreibung der Erweiterung, deren Version, den Herausgeber und weitere Informationen angezeigt.
4. Klicken Sie dann auf INSTALLIEREN. Ist dieses Feld ausgegraut, ist die Erweiterung bereits auf Ihrem WAC-Gateway installiert.
5. Ist es notwendig, dass Ihr Gateway für diese Installation mit erhöhten Rechten ausgeführt werden muss, bekommen Sie an dieser Stelle dann eine Eingabeaufforderung der Benutzerkontensteuerung (UAC) für erhöhte Rechte angezeigt.
6. Nach Abschluss der Installation wird der Browser automatisch aktualisiert, und das Windows Admin Center wird mit der installierten neuen Erweiterung erneut geladen.

Weitere Einstellungen und Features

Nach dieser Einführung möchten wir Ihnen im folgenden Abschnitt nur einen kurzen Überblick darüber geben, welche Möglichkeiten Ihnen das WAC noch zur Verfügung stellt. Diese Software bietet so viele Möglichkeiten und Unterstützung für so viele Bereiche des Windows-Servers, dass eine vollständige Auflistung aller Einstellungen auf jeden Fall den Rahmen dieses Buchs sprengen würde.

Das liegt nicht zuletzt daran, dass Microsoft das Windows Admin Center auch sehr eng mit den Möglichkeiten der Cloud-Plattform Azure verbunden hat. Grundsätzlich bietet Ihnen das WAC eine große Anzahl von Software-Werkzeugen, mit denen Sie unter anderem Ereignisse und Prozesse ebenso wie die virtuellen Maschinen unter Hyper-V auf den verbundenen Maschinen verwalten und betreuen können. Sie können aber auch Updates und Geräte sowie Zertifikate verwalten. Dadurch, dass Sie das Admin Center nicht nur auf einem Windows-10-Rechner installieren können, sondern diese Client-Systeme damit ebenso wie die Server verwalten können, steht die Lösung in direkter Konkurrenz zu den vielen professionellen Lösungen für die Server-Verwaltung – mit dem großen Vorteil, dass sie kostenlos bereitsteht und sehr gut mit den Windows-Systemen zusammenarbeitet. Auch wenn Windows Server in der Version 2022 noch den traditionellen Server-Manager als Standardlösung

verwendet, ist es doch abzusehen, dass Microsoft in den kommenden Jahren mehr und mehr in Richtung WAC schwenken wird.

Wenn Sie auf der ersten Seite des Windows Admin Centers auf den Link eines Servers klicken, gelangen Sie auf eine Übersichtsseite, die Ihnen die grundlegenden Dateien zu diesem System präsentiert ([Abbildung 18.16](#)). So können Sie beispielsweise sofort sehen, mit welcher CPU das System ausgestattet ist und wie groß der Ausbau des Hauptspeichers ist. Schauen Sie sich in der [Abbildung 18.16](#) die Einträge für Hersteller und Modell dieses Systems an, dann sehen Sie auch, dass wir diesen Windows Server 2022 in einer virtuellen Maschine unter VMware betreiben. Es handelt sich hier also nicht um ein physikalisch vorhandenes System.

Auf der linken Seite des Browser-Fensters finden Sie zudem eine Auflistung der Systemwerkzeuge, die Ihnen an dieser Stelle zur Verfügung stehen. Die ersten fünf Einträge im Tools-Menü beziehen sich auf die Verbindung zur Cloud-Plattform Azure, durch die im WAC eine hybride Verwaltung von lokalen Systemen und solchen in der Azure-Cloud möglich wird. Darunter finden Sie dann Werkzeuge, wie Sie sie vielleicht schon aus dem Server-Manager oder anderen Verwaltungsanwendungen kennen: Sie können dort auf Dateien und Dateifreigaben ebenso zugreifen wie auf die Firewall des Servers oder die Geräte. Weiterhin können Sie unter anderem lokale Nutzer und Gruppen sowie die installierten Apps auf dem entsprechenden System verwalten. Wir möchten Ihre Aufmerksamkeit aber zunächst einmal auf das ganz untere Ende dieser Liste lenken, denn dort finden Sie das bekannte Zahnradsymbol, das Sie zu den Einstellungen für die Tools führt.

Wählen Sie die Einstellungen im Tools-Bereich aus, so bekommen Sie ein Menü mit sechs Einträgen unter der Überschrift ALLGEMEIN präsentiert ([Abbildung 18.17](#)).

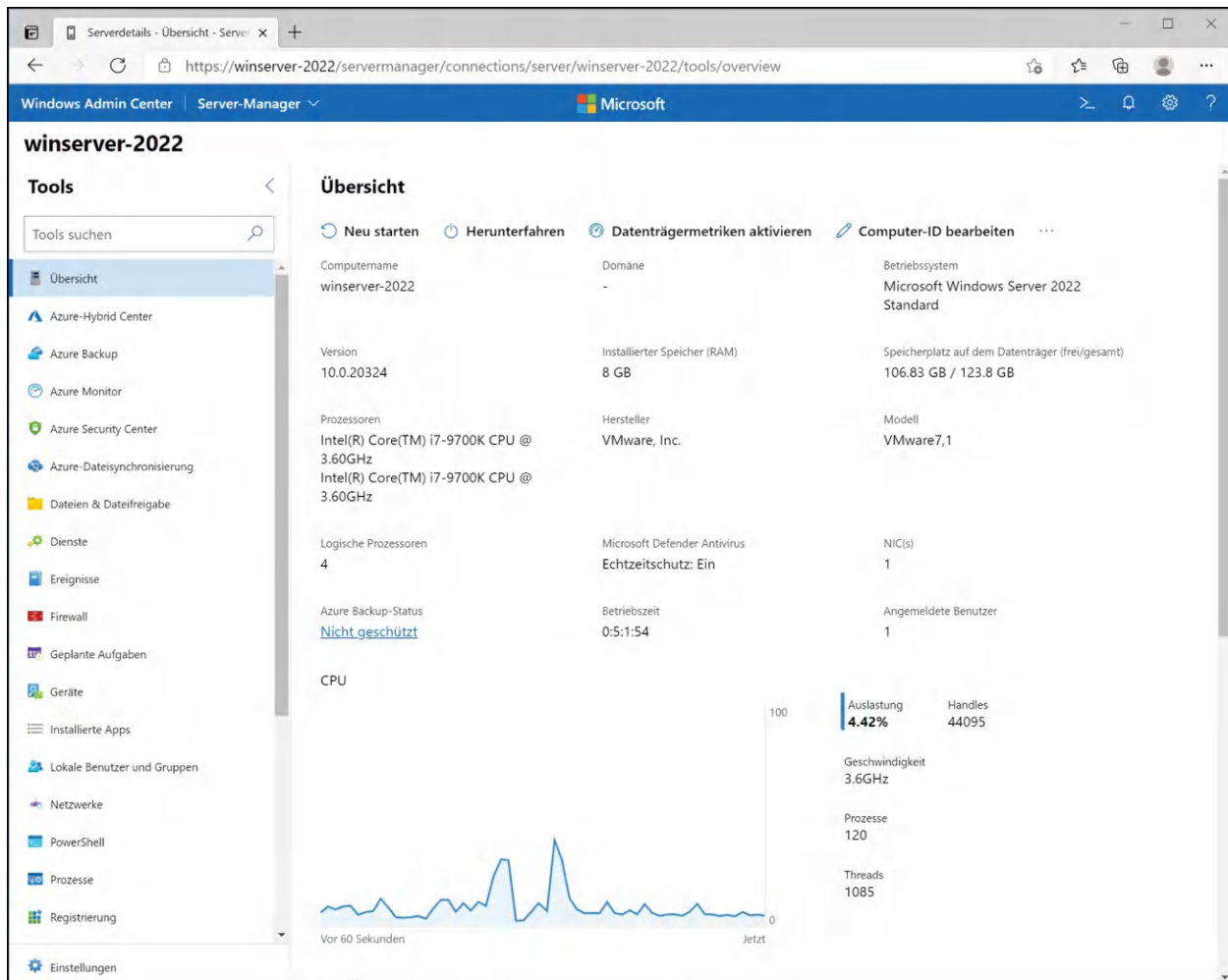


Abbildung 18.16: Die Übersichtsseite eines Servers zeigt im Windows Admin Center alle grundlegenden Daten eines Systems und alle Tools an.

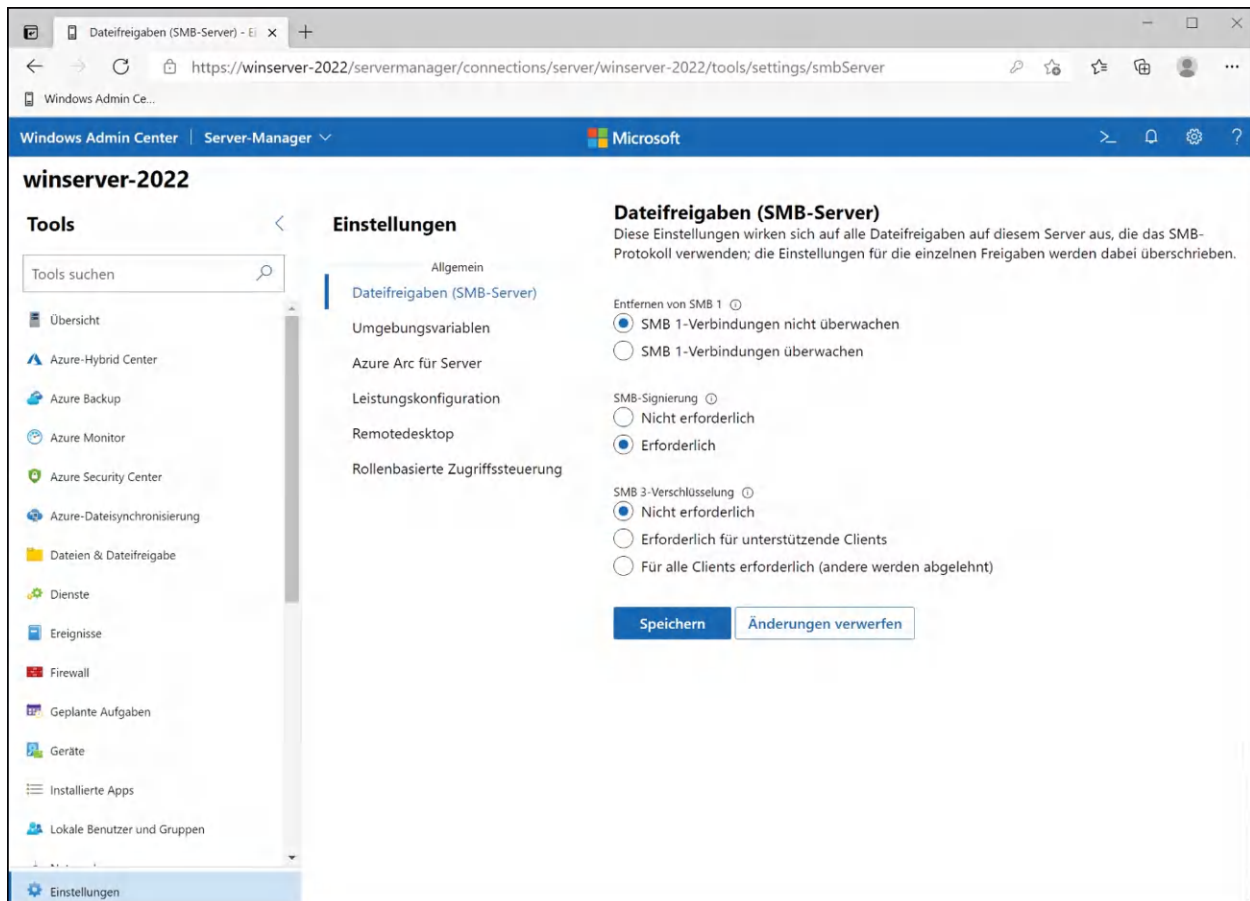


Abbildung 18.17: Das Menü »Einstellungen« ermöglicht es Ihnen, einige wichtige Bereiche des Servers zu konfigurieren.

Der erste Eintrag im Menü EINSTELLUNGEN bezieht sich auf die Version des bei Dateifreigaben verwendeten SMB-Protokolls (Server Message Block). Die Überwachung des SMB-1-Protokolls ist standardmäßig unter Windows Server 2019 und 2022 nicht aktiviert. Bereits mit der Version 1709 von Windows Server wird es nicht mehr installiert. Wenn es auf einem Ihrer Server doch noch zum Einsatz kommt (wovon aber aus Sicherheitsgründen abzuraten ist), so können Sie an dieser Stelle die Überwachungsfunktion aktivieren.

Besonders interessant ist in diesem Menü die Einstellung ROLLENBASIERTE ZUGRIFFSSTEUERUNG (Role-Based Access Control, RBAC), die in [Abbildung 18.18](#) zu sehen ist. Diese Einstellung steht allerdings nur dann zur Verfügung, wenn Sie das Admin Center im Gateway-Modus auf Ihrem Server installiert haben. Mithilfe dieses Features können Sie ein rollenbasiertes Rechtemanagement umsetzen, das

es Ihnen erlaubt, bestimmte Aufgaben an andere Nutzer zu delegieren, auch wenn diese keine Administratorrechte auf dem Server oder im Active Directory besitzen. Durch Auswahl von **ÜBERNEHMEN** ([Abbildung 18.18](#)) muss diese Funktion zunächst einmal aktiviert werden. Das WAC meldet dann, dass »unter Umständen« der Dienst WinRM (Windows Remote Management) neu gestartet werden muss. Das kann dann bis zu zehn Minuten dauern. Danach ändert sich der Status der Zugriffssteuerung im Fenster auf **ANGEWENDET**.

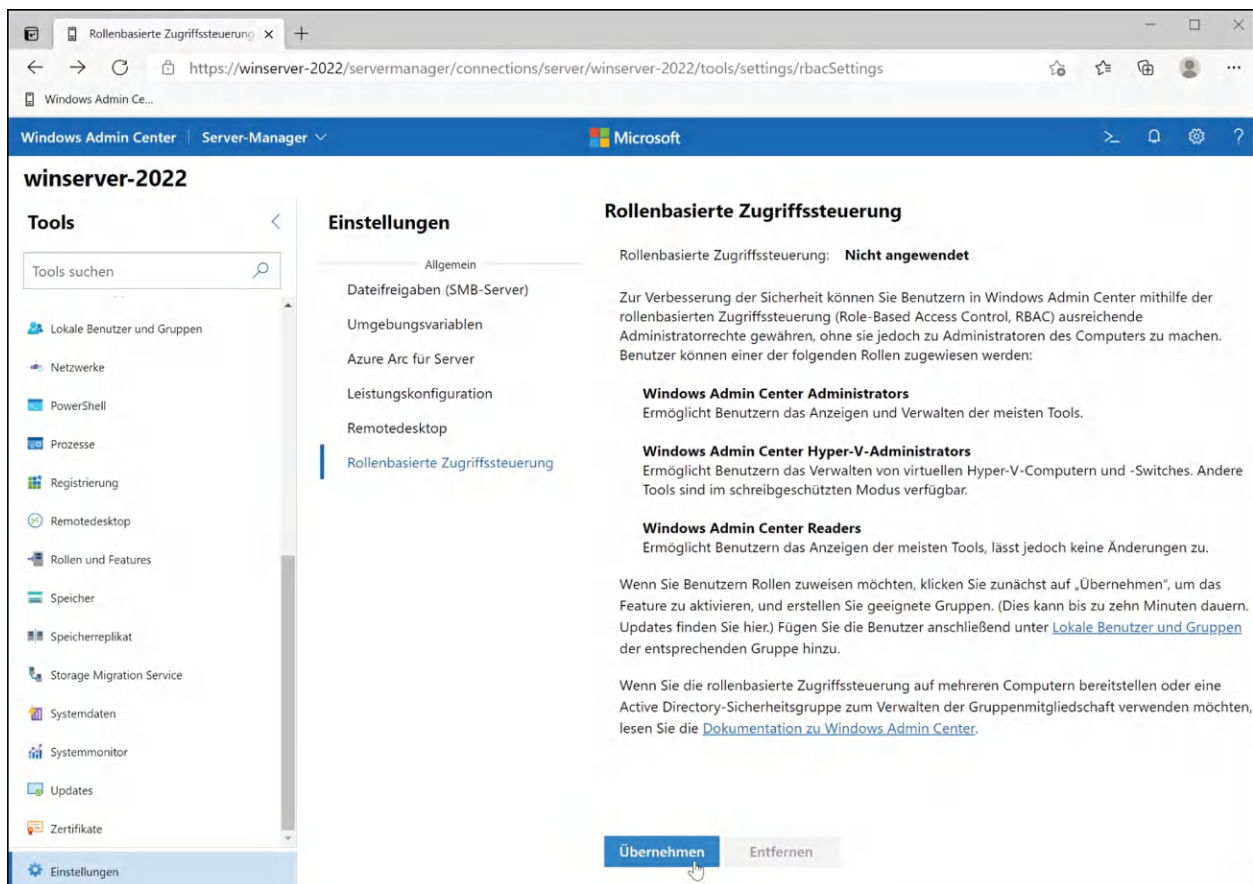


Abbildung 18.18: Die »Rollenbasierte Zugriffssteuerung« ermöglicht es Nutzern, bestimmte Zugriffsrecht im WAC zuzuordnen.

Danach stehen drei neue lokale Nutzergruppen zur Verfügung ([Abbildung 18.19](#)). Ihre Namen entsprechen dabei den Rollen:

- ✓ Windows Admin Center Administrators,
- ✓ Windows Admin Center Hyper V Administrators und

✓ Windows Admin Center Readers.

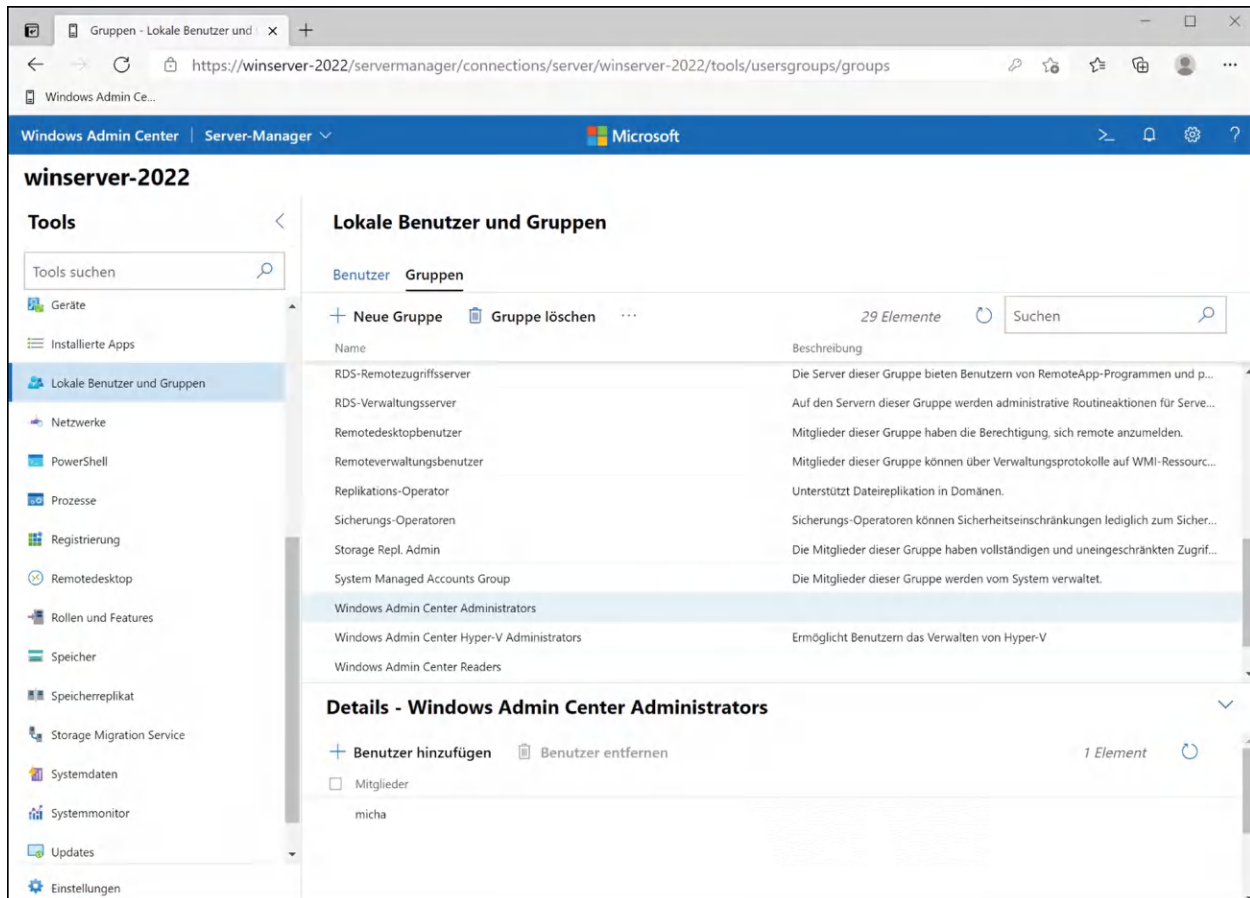


Abbildung 18.19: Nachdem die »Rollenbasierte Zugriffssteuerung« aktiviert wurde, stehen drei neue lokale Nutzergruppen bereit.



Wenn Sie die rollenbasierte Zugriffssteuerung auf Ihrem Server aktivieren wollen, müssen Sie mit einem Konto angemeldet sein, das über lokale Administratorenrechte auf diesem Rechner verfügt.

Wenn Sie nun Benutzer oder Gruppen mit den Berechtigungen dieser Rollen auszustatten wollen, müssen Sie diese in eine der neu erstellten lokalen Gruppen aufnehmen:

1. Dazu wählen Sie aus dem Tools-Menü **LOKALE BENUTZER UND GRUPPEN** aus ([Abbildung 18.19](#)). In diesem Zusammenhang möchten wir noch auf ein Feature hinweisen, das WAC erst seit der Anfang 2021 verfügbarer Version 2103 zur Verfügung stellt: Sie

können jedes der Tools, die Ihnen in der linken Spalte des Fensters zur Verfügung stehen, nun auch in einem neuen separaten Fenster öffnen.

2. Dazu zeigen Sie mit dem Mauszeiger auf den Eintrag und klicken auf das kleine Fenstersymbol, das dann erscheint ([Abbildung 18.20](#)).

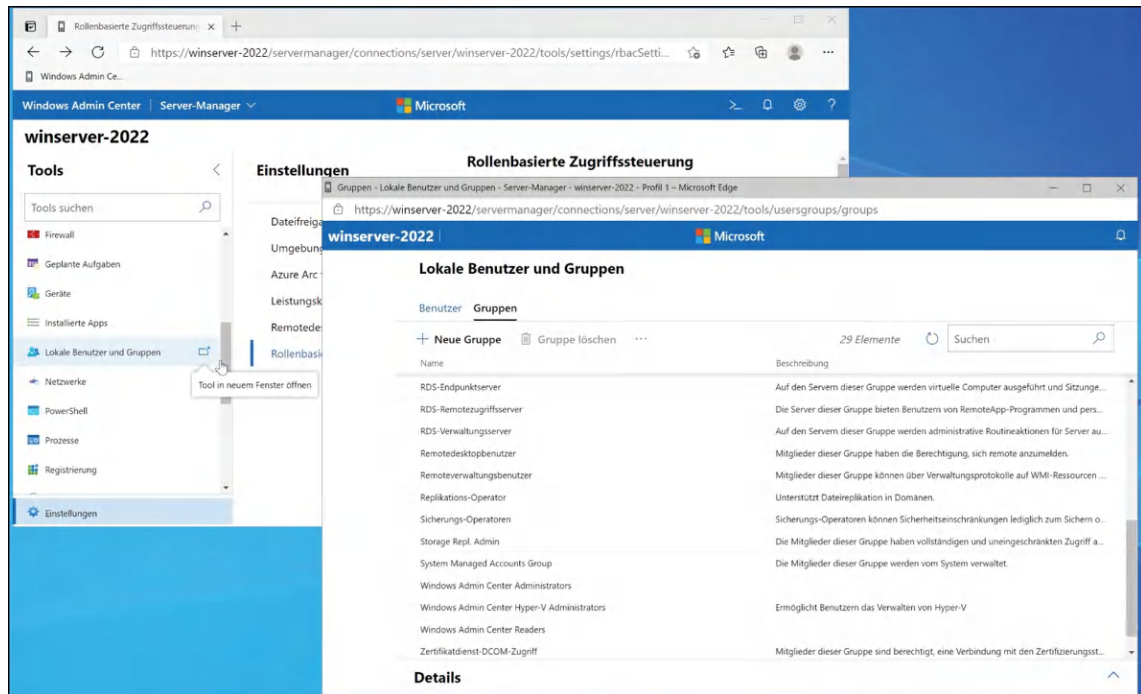


Abbildung 18.20: WAC erlaubt es dem Nutzer, jedes Tool aus der Liste in einem eigenen Fenster zu starten.

3. In dem neuen Fenster können Sie dann die Registerkarte GRUPPEN wählen.
4. Ein Klick auf dem Namen der entsprechenden Gruppe öffnet ein Fenster mit den Details zu dieser Gruppe.
5. Über +BENUTZER hinzufügen können Sie anschließend den gewünschten Nutzer als Mitglied dieser Gruppe eintragen und ihm so die damit verbundenen Rechte geben.

Die Nutzer der Gruppe WINDOWS ADMIN CENTER READERS können dabei nur lesend auf die Daten im Admin Center zugreifen. Der Zugriff der Nutzer der Gruppe WINDOWS ADMIN CENTER HYPER V ADMINISTRATORS beschränkt sich auf die Wartung und Betreuung des Hyper-V und seiner virtuellen Maschinen. Für andere Features steht

diesen Nutzern nur der schreibgeschützte Zugriff zur Verfügung. Nur die WINDOWS ADMIN CENTER ADMINISTRATORS können dann die meisten Features in Windows Admin Center verwenden. Allerdings besitzen auch sie keinen Zugriff auf Remotedesktop oder die PowerShell.

Kapitel 19

Windows-Server-Updates

IN DIESEM KAPITEL

Einstellungen und Features für die Updates

Update-Richtlinien verändern

Update-Einstellungen mittels sconfig ändern

Neben den Backups, auf die wir später noch eingehen werden, gehören auch die Updates zu den eher »ungeliebten« Aufgaben bei der Verwaltung und Betreuung von Windows-Systemen – was auch für die Server gilt. Dabei ist es unbestritten, dass regelmäßige Updates ein entscheidender Faktor für die Sicherheit von IT-Systemen sind. Während Microsoft bei dem Client-Betriebssystem auch aus diesem Grund immer mehr dazu übergeht, alle Update-Vorgänge einschließlich des Herunterladens und des Installierens möglichst vollautomatisch ablaufen zu lassen, kann das bei einem Server-System nicht der Fall sein. Hier besitzt der Administrator mehr und bessere Auswahlmöglichkeiten, den Update-Prozess nach seinen Vorstellungen zu konfigurieren.



Wenn die Rede auf die Updates der Windows-Systeme kommt, dann taucht auch schnell der Begriff WSUS auf. WSUS ist die Abkürzung für »Windows Server Update Services«. Dieser Dienst wurde mit der Version 2003 von Windows Servers als Nachfolger der »Software Update Services« eingeführt. Er steht auf allen aktuellen Windows-Server-Systemen als Server-Rolle bereit. Mithilfe des WSUS ist es möglich, die eigenen Systeme (Server und Clients) mit Updates, die über Microsoft Update veröffentlicht werden, auf den Computern im eigenen Netzwerk zu versorgen und somit die Update-Verteilung besser zu kontrollieren. In einem solchen

Netzwerk muss dann wenigstens einer der vorhandenen WSUS-Server eine Verbindung zu Microsoft-Update besitzen. Auch Software-Produkte anderer Hersteller können mittels WSUS verteilt werden. Der Einsatz einer solchen Update-Infrastruktur ist besonders im Unternehmensumfeld sinnvoll. Wollen oder müssen Sie diese Form der Update-Verteilung einsetzen, so finden Sie im Internet – neben vielen anderen Angeboten – auch alle nötigen Informationen zu WSUS in der Microsoft-Dokumentation:

<https://docs.microsoft.com/de-de/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus>.

Einstellungen und Features für die Updates

Windows Server 2019 und auch die kommende Version 2022 verwenden eine Oberfläche, wie sie viele Anwender von Windows 10 her kennen dürften. Die uns bei der Erstellung dieses Buchs zur Verfügung stehende Vorabversion des Windows Server 2022 aus dem Insider-Programm von Microsoft setzt dabei bereits auf die Version 21H1. Dabei konnten wir im Bereich der Update-Verwaltung noch keine Veränderungen im Vergleich zur aktuellen Version 2019 des Servers finden. Allerdings hat Microsoft auch schon bei früheren Release-Wechseln deutliche Änderungen im Bereich Updates durchgeführt, sodass Sie auf jedem Fall aufmerksam bleiben sollten.

Grundsätzlich finden Sie die Einstellungen für die Update-Verwaltung Ihres Windows-Servers in den WINDOWS-EINSTELLUNGEN im Bereich UPDATE UND SICHERHEIT. Wenn Sie dorthin wechseln, werden Sie in der Regel auch gleich über den Stand der Updates und eventuell anstehende neue Updates informiert ([Abbildung 19.1](#)). Auch im Info-Center am rechten Bildrand erhalten Sie eine neue Nachricht, falls Updates für Ihren Server zur Verfügung stehen. Wenn Sie bisher nur mit Windows-Client-Systemen gearbeitet haben, dann werden Sie in der [Abbildung 19.1](#) bereits einige Unterschiede beispielsweise im Vergleich

zu den Einstellungen bei einem Windows-10-Rechner finden. Zunächst einmal werden Sie auf dem Windows-Server standardmäßig nur darüber informiert, dass neue Updates zu Installation bereitstehen.

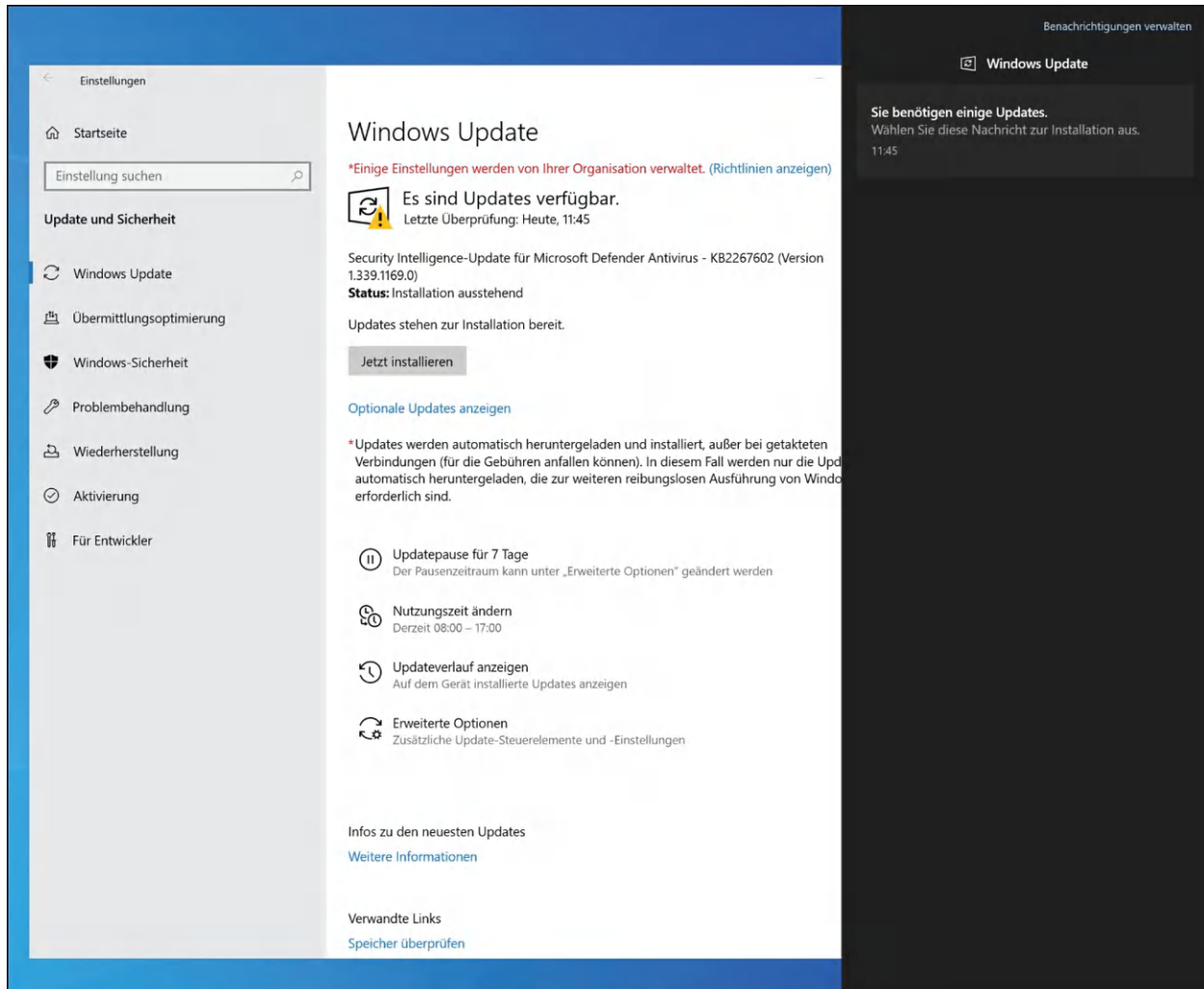


Abbildung 19.1: Gibt es Updates für meinen Server? Die Windows-Einstellungen und das Info-Center geben Auskunft.

Den eigentlichen Installationsvorgang müssen Sie manuell anstoßen, indem Sie **JETZT INSTALLIEREN** auswählen. Den zweiten Unterschied werden Sie in der Regel direkt unter der Überschrift **WINDOWS UPDATE** finden: Dort wird Ihnen mitgeteilt, dass »einige Einstellungen von Ihrer Organisation verwaltet werden«. Diese recht allgemeine Aussage werden Sie auch dann vorfinden, wenn Ihr Server aktuell kein Mitglied einer Organisation oder Firma ist. Wollen Sie wissen, um welche Einstellungen es sich dabei handelt, dann können Sie den Link hinter

dieser Aussage auswählen. Sie werden dann ein Bild ähnlich dem in [Abbildung 19.2](#) zu sehen bekommen.

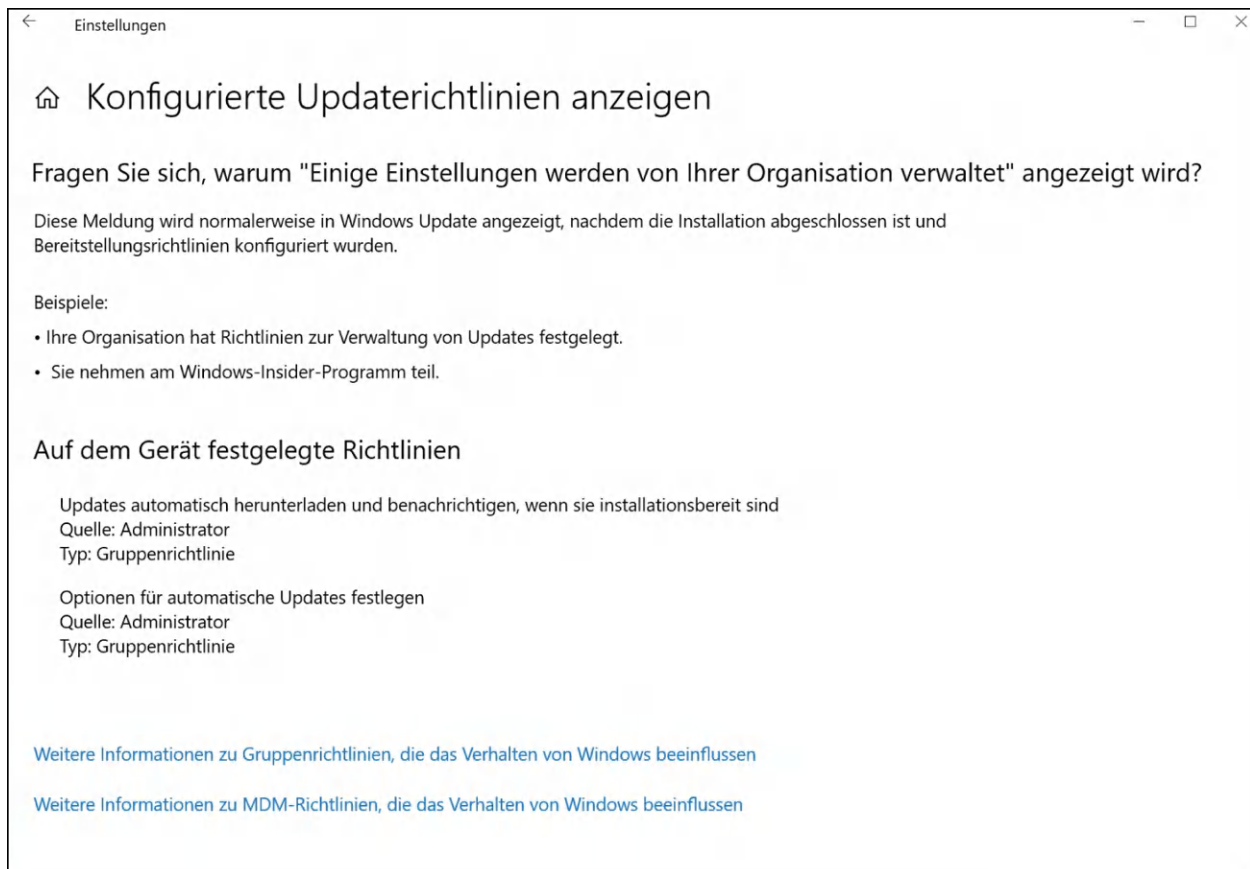


Abbildung 19.2: Windows Server zeigt Ihnen an, welche Richtlinien für die Updates auf Ihrem System automatisch festgelegt wurden.

Dort finden Sie dann eine kurze Erläuterung mit Beispielen zu dieser Einstellung und können sehen, welche Richtlinien für diesen Server von wem festgelegt wurden. Wir werden uns im Verlauf dieses Kapitels noch genauer damit beschäftigen, wie Sie diese Gruppenrichtlinien, die in einem Unternehmensnetzwerk zumeist mittels Active Directory auf Ihren Server gelangen, auch lokal einsetzen und verwalten können.

Zunächst wechseln wir aber zurück in den Update-Bereich unter UPDATE UND SICHERHEIT der WINDOWS-EINSTELLUNGEN. Wenn Ihr System sich in dem aktuellen Zustand befindet, werden Sie hier ein Bild wie in der [Abbildung 19.3](#) finden. Sie können dann an dieser Stelle auch manuell mittels NACH UPDATES SUCHEN eine Suche nach neuen Updates anstoßen, die der Server ansonsten automatisch ausführen würde.

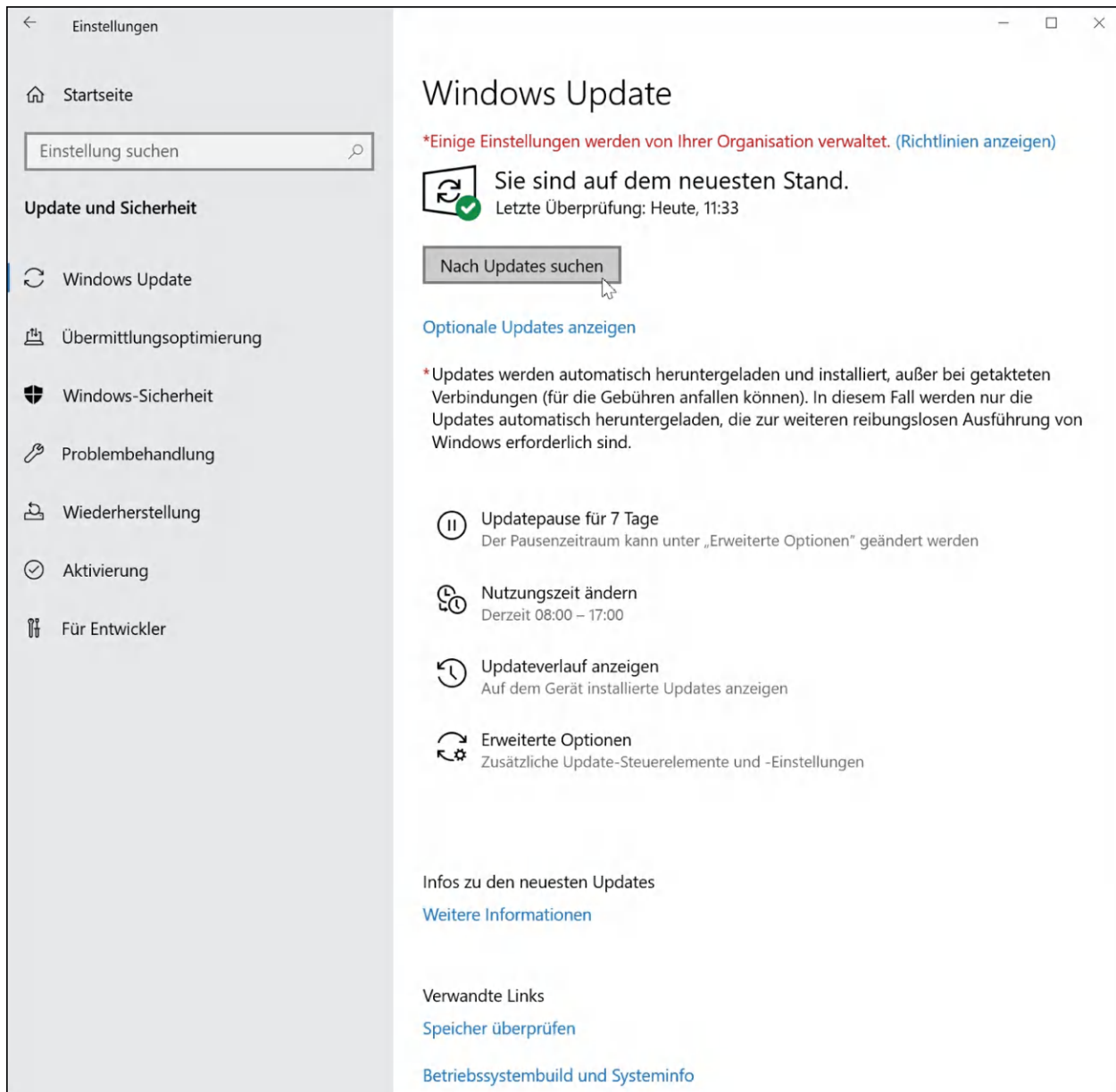


Abbildung 19.3: Auf der Seite »Update und Sicherheit« finden Sie unter »Windows Update« eine ganze Reihe weiterer Einstellmöglichkeiten.

Mit der Einstellung UPDATEPAUSE FÜR 7 TAGE können Sie das Herunterladen von Updates für sieben Tage unterbrechen. Danach aktiviert Windows das Herunterladen der Updates wieder automatisch. Sie können auf der Seite nun auch sehen, dass die Updates ausgesetzt wurden. Wollen Sie diese Pause früher beenden, können Sie das jederzeit durch Auswahl von UPDATES FORTSETZEN erreichen ([Abbildung 19.4](#)). Beachten Sie dabei aber, dass der Windows-Server in diesem Fall sofort eine Suche nach neuen Updates startet und diese auch herunterlädt.

Wollen Sie die Updates für einen längeren Zeitraum aussetzen, können Sie das erreichen, indem Sie ERWEITERTE OPTIONEN auswählen.

Auf der Seite ERWEITERTE OPTIONEN finden Sie eine ganze Reihe weiterer Einstellmöglichkeiten für die Updates, zu denen auch UPDATES AUSSETZEN gehört ([Abbildung 19.5](#)). Dort können Sie über ein Pull-down-Menü ein Datum auswählen, bis zu dem die Installation von Updates auf diesem Rechner nicht mehr stattfinden soll. Dabei steht Ihnen ein Zeitraum von bis zu 35 Tagen zur Verfügung. Ähnlich wie bei der siebentägigen Pause können Sie hier ebenfalls die Pausierung jederzeit beenden: Auch bei dieser Vorgehensweise wird Windows Server auf jedem Fall nach dem Abbrechen oder nach Ablauf der 35 Tage zunächst einmal automatisch nach Updates suchen und diese herunterladen. Danach können Sie dann natürlich wieder einen bis 35 Tage dauernden Stopp für das automatische Herunterladen der Updates aktivieren.

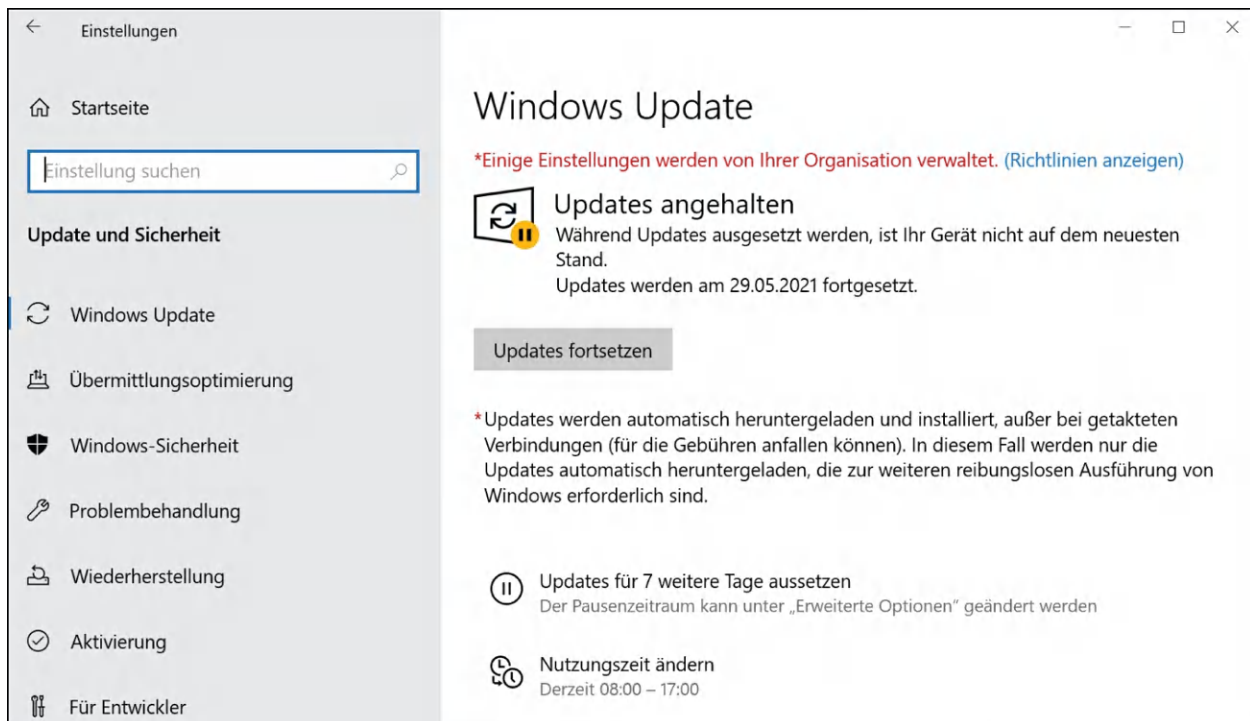


Abbildung 19.4: Sie können das Herunterladen der Updates auf dieser Seite für sieben Tage unterbrechen.

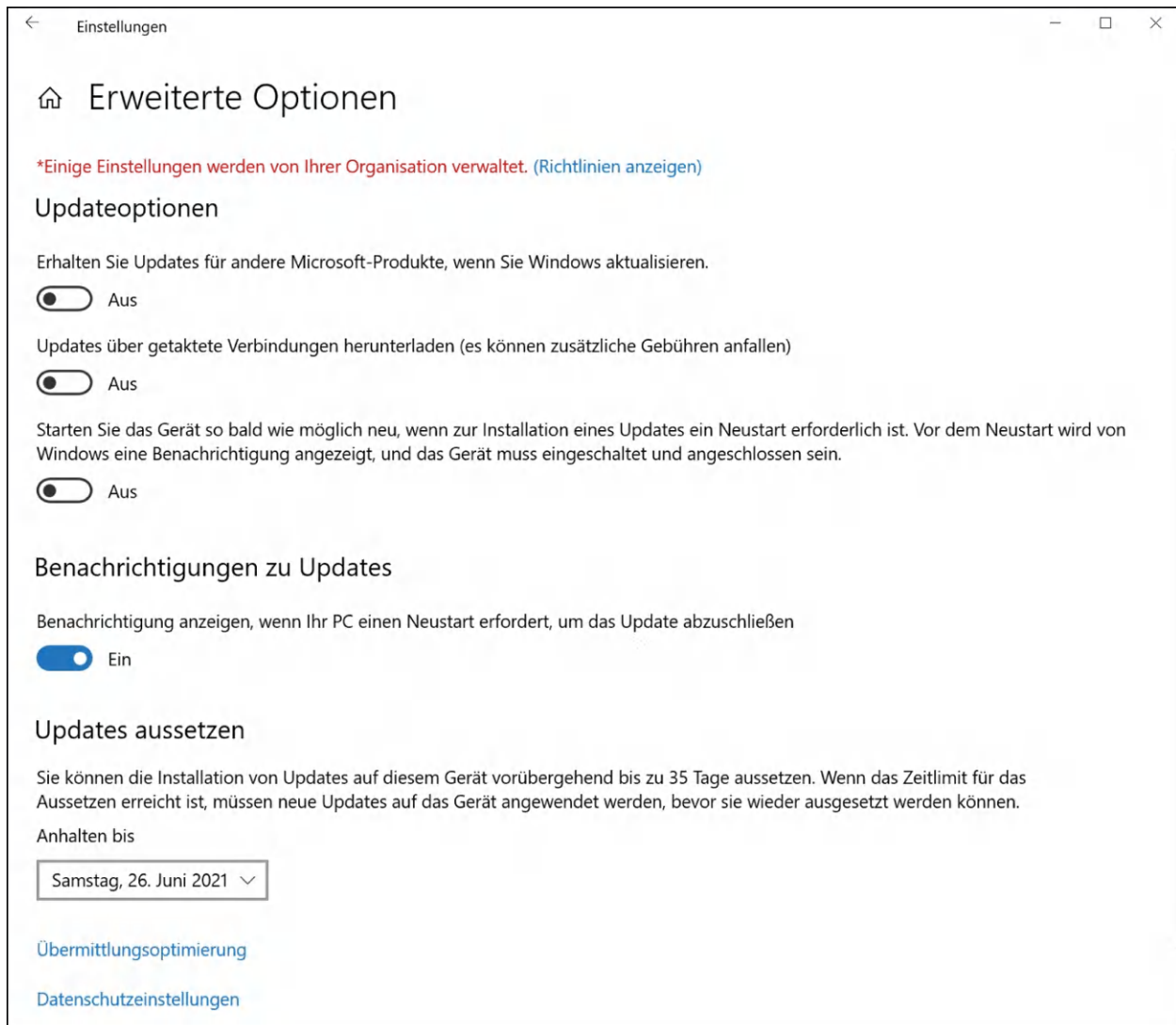


Abbildung 19.5: Mithilfe der »Erweiterten Optionen« ist es möglich, die Installation von Updates auf dem Server für bis zu 35 Tage auszusetzen.

Unter ERWEITERTE OPTIONEN stehen Ihnen noch weitere Konfigurationsmöglichkeiten zur Verfügung. Unter der Überschrift UPDATEOPTIONEN ist es zum Beispiel möglich, mittels Schiebeschalter eine Option zu aktivieren, die sicherstellt, dass auch andere Microsoft-Produkte, die sich auf dem Server befinden, bei der Aktualisierung von Windows automatisch Updates erhalten. Die Einstellung UPDATES ÜBER GETAKTETE VERBINDUNG HERUNTERLADEN dürfte für Server seltener relevant sein, da es eher mobile Systeme sind, die solche Verbindungen nutzen. Auch die Möglichkeit, die der dritte Schalter bietet, nämlich einen automatischen

Neustart so schnell wie möglich auszuführen, wird auf einem Server sicher nicht so häufig zum Einsatz kommen.

Hingegen ist es in der Regel durchaus sinnvoll, den Schalter unter BENACHRICHTIGUNGEN ZU UPDATES auf EIN zu setzen, sodass Sie benachrichtigt werden, wenn der Rechner aufgrund eines Updates einen Neustart benötigt.

Ganz unten auf dieser Seite finden Sie neben einem Link, der in das Menü DATENSCHUTZ der Windows-Einstellungen führt, auch einen Link mit der Bezeichnung ÜBERMITTLUNGSOPTIMIERUNG. Dieser führt Sie in ein Menü, in dem Sie dieses Feature – das standardmäßig auf dem Windows-Server nicht aktiviert ist – für Ihren Server einschalten können ([Abbildung 19.6](#)).

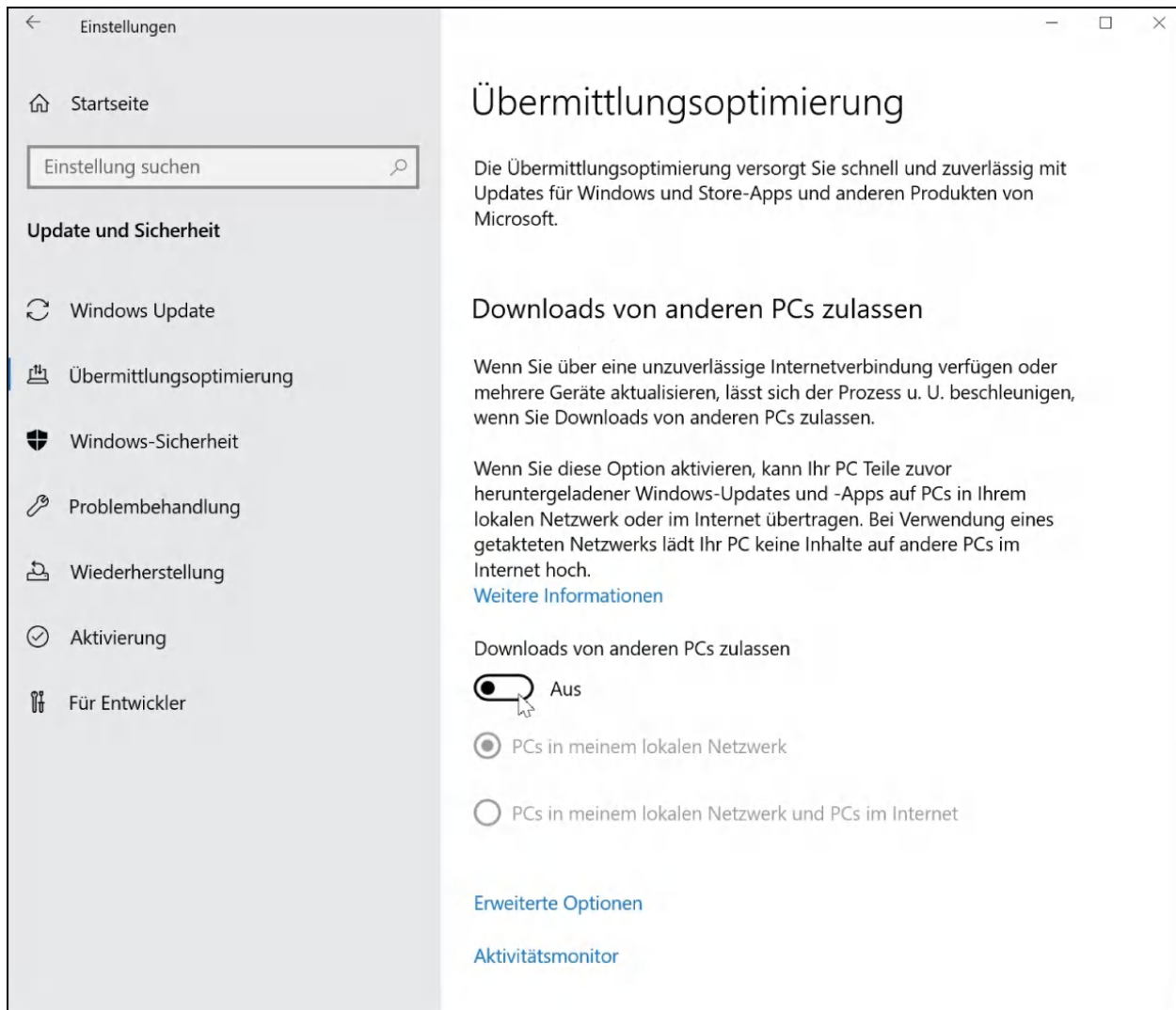


Abbildung 19.6: Die Übermittlungsoptimierung kann Downloads von Updates beschleunigen, muss aber explizit aktiviert werden.

Die Übermittlungsoptimierung bietet Ihnen die Möglichkeit, Ihre Updates nicht nur von Microsoft, sondern auch von anderen PCs zu erhalten. Das ist prinzipiell gerade für kleine Unternehmen mit nur einer, vielleicht auch nicht so leistungsfähigen Internet-Verbindung eine gute Lösung: Sie können dabei die Rechner im eigenen Netzwerk oder auch diese und weitere Systeme im Internet als Quelle wählen. Der Vorteil besteht darin, dass Ihr System sich dann beispielsweise Updates, die sich schon auf einem dieser Rechner befinden, von diesem System holen kann. Es braucht dazu nicht extra eine weitere Verbindung zum Microsoft-Server im Internet aufzubauen. Die Option, sowohl Rechner im eigenen Netzwerk als auch solche im Internet als Quelle zu nutzen, dürfte aber in

den meisten Fällen wegen Bedenken in Bezug auf den Datenschutz für die meisten Anwender nicht infrage kommen,



Windows nutzt eine aktivierte Übermittlungsoptimierung sowohl für den Download von Windows-Update als auch für das Herunterladen von Store-Apps aus dem Microsoft Store. Diese Technik funktioniert in beide Richtungen: Haben Sie die Übermittlungsoptimierung aktiviert, so sendet Ihr Server ebenfalls Updates und Apps an andere Rechner in Ihrem Netzwerk oder auch im Internet (je nachdem, welche Einstellung Sie gewählt haben). Lädt Windows unter Einsatz der Übermittlungsoptimierung ein Update herunter, sucht es zunächst auf den anderen Systemen, ob einer dieser Rechner dieses Update bereits erhalten hat. Dabei lädt das Betriebssystem nicht die komplette Datei von einer Quelle herunter, sondern teilt den Download in kleinere Teile auf. Diese Teile werden dann sowohl von den anderen Systemen als auch direkt von Microsoft abgerufen. Dabei soll das System so optimiert sein, dass es jeweils die schnellste und zuverlässigste Quelle verwendet. Intern erstellt die Übermittlungsoptimierung dafür einen lokalen Cache, in dem die heruntergeladenen Teile zwischengespeichert werden.

Microsoft betont dabei außerdem, dass diese Technik nicht dazu verwendet werden kann, persönliche Daten herunterzuladen oder zu versenden. Weiterhin ist diese Technik laut Microsoft auch grundsätzlich nicht dazu in der Lage, auf persönliche Dateien oder Ordner auf dem Server zuzugreifen. Die Übermittlungsoptimierung prüft zudem die Echtheit der Downloads vor jeder Installation ein weiteres Mal.

Auf der Seite WINDOWS UPDATE finden Sie weiterhin noch die Möglichkeit, die Nutzungszeit Ihres Systems festzulegen. In diesem Zeitraum ([Abbildung 19.7](#)) wird der Server nach der Installation von Updates dann nicht automatisch neu gestartet, wenn ein Update einen Neustart notwendig macht. Sie sollten grundsätzlich automatische Neustarts für Ihren Server verbieten, indem Sie auch bei Software anderer Anbieter, die auf dem System installiert ist, diese Option immer

ausschließen. Während Sie auf den Client-Rechnern beispielsweise unter Windows 10 dem System erlauben können, diesen Zeitraum automatisch anhand Ihrer Nutzungsgewohnheiten zu ermitteln, steht diese Option auf den Server-Versionen nicht zur Verfügung. Voreingestellt ist an dieser Stelle bei allen Server-Versionen eine Nutzungszeit von 8:00 bis 17:00 Uhr.

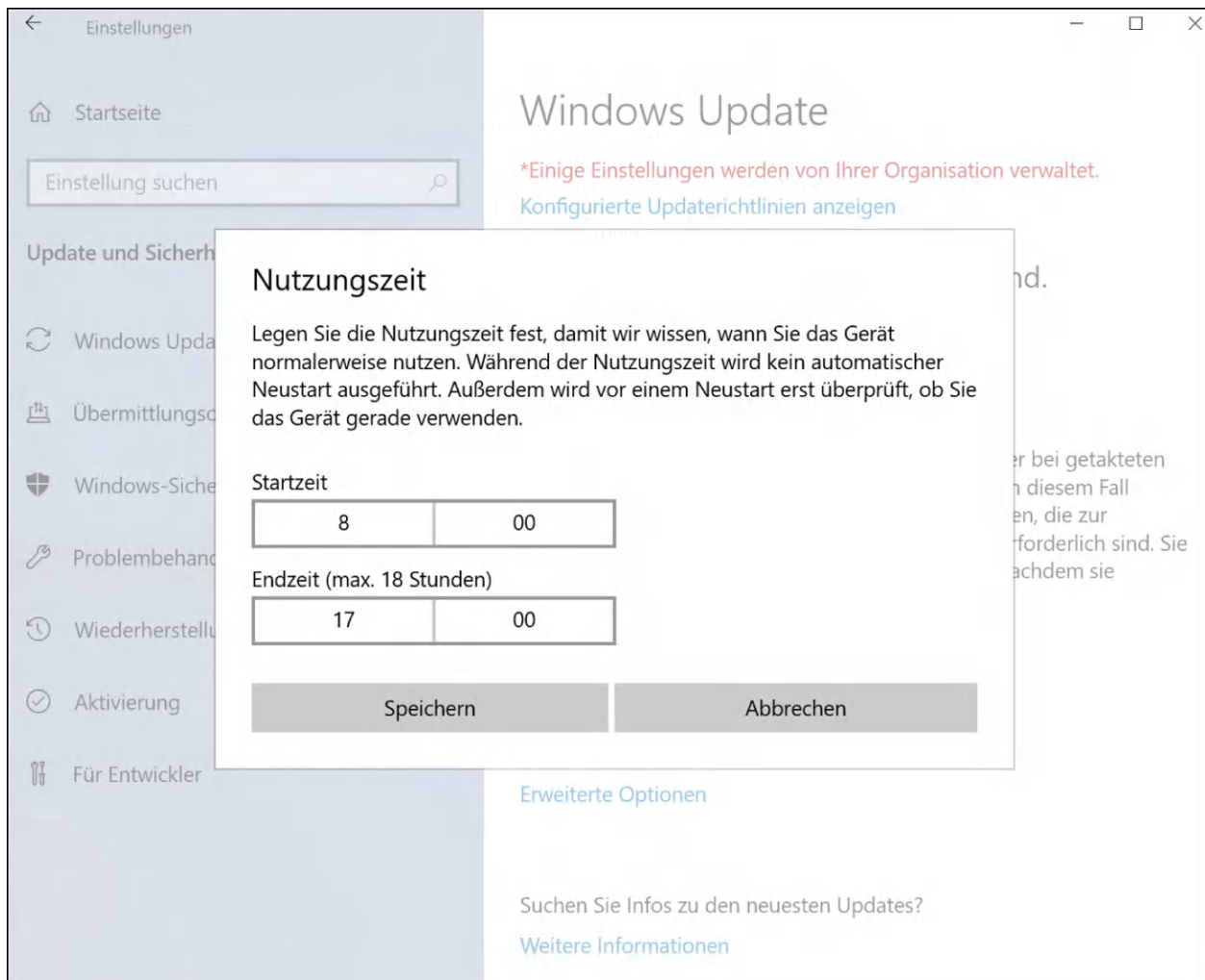


Abbildung 19.7: Kein automatischer Neustart für den Server: Der Zeitraum für diese Regel kann unter »Windows Update« festgelegt werden.

Es gibt immer wieder Fälle, in denen ein Windows-Update nicht die versprochene Verbesserung bringt oder schlimmer noch, das System derart verändert, dass es nicht mehr richtig arbeitet. Dann muss es auch möglich sein, Updates wieder vom System zu entfernen.

1. Wechseln Sie dazu in den WINDOWS-EINSTELLUNGEN in den Bereich UPDATE UND SICHERHEIT.
2. Dort wählen Sie den Eintrag UPDATEVERLAUF ANZEIGEN.
3. Auf der folgenden Seite finden Sie dann die auf Ihrem Server installierten Updates unterteilt in die Kategorien QUALITÄTSUPDATES, TREIBERUPDATES, DEFINITIONSUPDATES und WEITERE UPDATES ([Abbildung 19.8](#)).

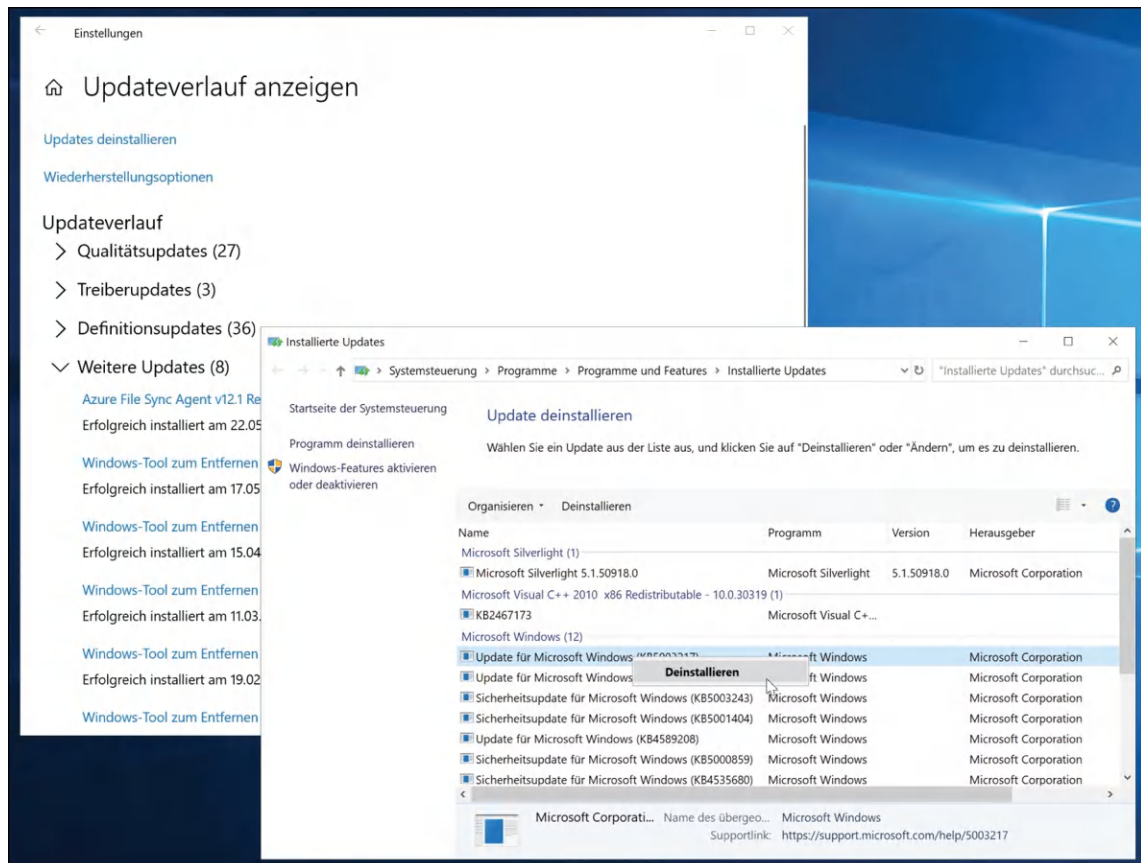


Abbildung 19.8: Wenn Updates wieder entfernt werden müssen, kommt auf dem Server noch ein Programm mit der »alten« Oberfläche zum Einsatz.

4. Klicken Sie auf den Link UPDATES DEINSTALLIEREN.
5. Daraufhin öffnet sich ein Fenster der App SYSTEMSTEUERUNG ([Abbildung 19.8](#)), wie sie auch noch auf älteren Server-Versionen wie Windows Server 2012 R2 zum Einsatz kommt.
6. Dort können Sie dann ein installiertes Update auswählen und wieder

vom System entfernen.

Beachten Sie dabei bitte, dass sich nicht alle Updates so ohne Weiteres wieder entfernen lassen. So ersetzen einige Feature-Updates auch auf den Server-Versionen das komplette Betriebssystem mit neuen Versionen, sodass ein Zurückrollen nur eine begrenzte Zeit möglich ist. Aber gerade, wenn ein sogenanntes Qualitäts-Update Probleme auf dem Server verursacht, kann eine Deinstallation ein gutes Mittel sein, um die Zeit zu überbrücken, bis Microsoft eine neue, reparierte Version des Updates bereitstellt.

Update-Richtlinien verändern

Es kann überhaupt nicht oft genug betont werden: Auf einem Server-System ist es in der Regel unerwünscht, dass die Updates automatisch und ohne Kontrolle durch den Administrator auf den Rechner gelangen und vielleicht sogar direkt installiert werden. Deshalb wird die Update-Verwaltung von Windows Server auch bereits standardmäßig über Gruppenrichtlinien geregelt. Während deren Einsatz in einem Netzwerk mit Active Directory »gang und gäbe« ist, fragen sich Anwender, die Windows Server ohne diesen Verzeichnisdienst nutzen, oft, wie sie diese Einstellungen nach ihren Vorstellungen konfigurieren können.

Auf den Server-Versionen von Windows steht Ihnen mit dem Editor für lokale Gruppenrichtlinien (siehe [Abbildung 19.9](#)) ein Software-Werkzeug zur Verfügung, mit dessen Hilfe Sie diese Richtlinien einsehen und auch für Ihren Server verändern können.

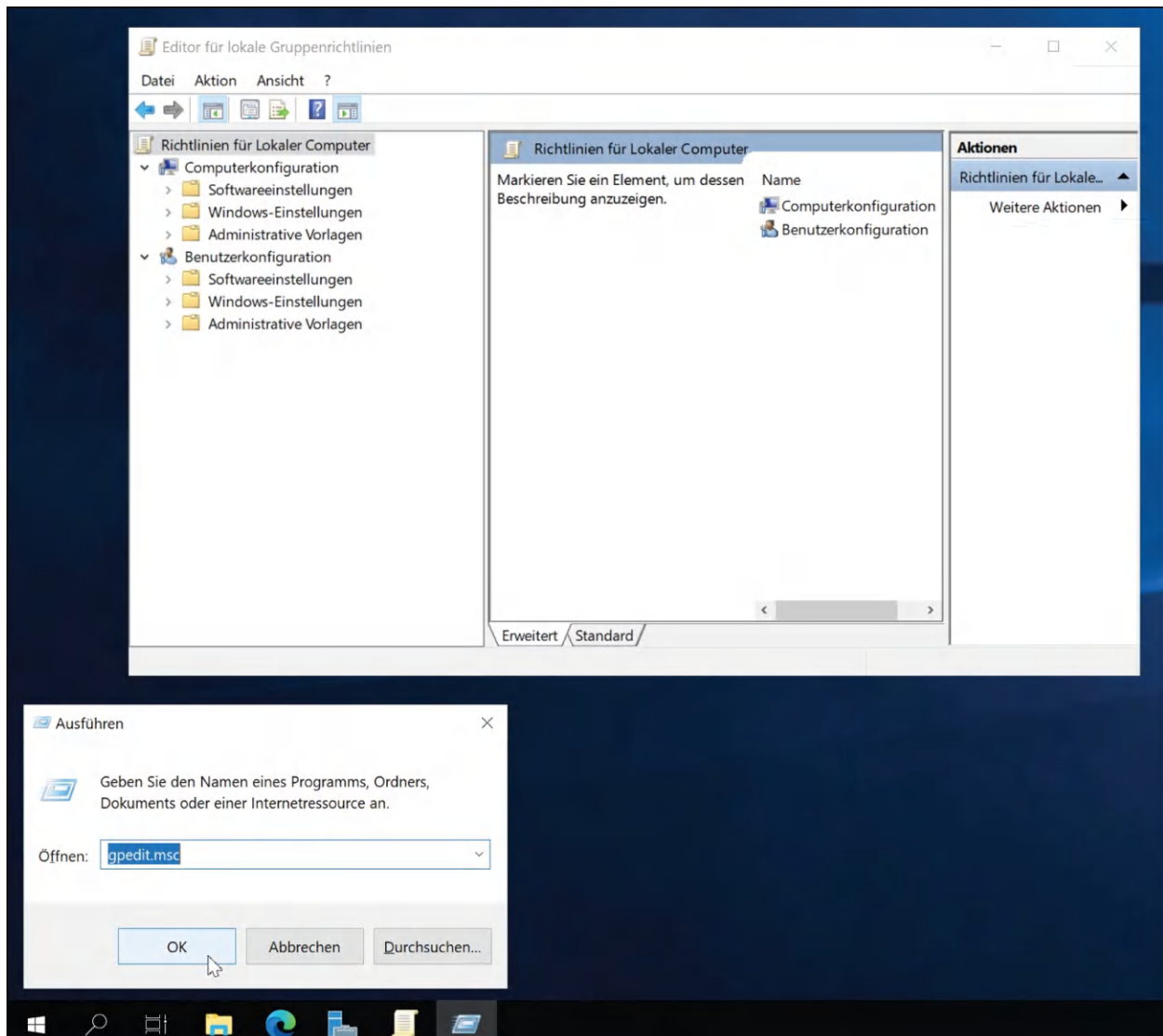


Abbildung 19.9: Über den Aufruf von »gpedit.msc« kann auf Windows Server der Editor für lokale Gruppenrichtlinien aufgerufen werden.

1. Um diesen Editor zu starten, rufen Sie mithilfe der Tastenkombination  +  das Fenster zum Ausführen von Befehlen auf. Sie können aber auch eine Eingabeaufforderung starten und den Aufruf dort auf der Kommandozeile eingeben.
2. Im Editor navigieren Sie zu folgendem Pfad:
COMPUTERKONFIGURATION\ADMINISTRATIVE
VORLAGEN\WINDOWS-KOMPONENTEN\WINDOWS UPDATE.
3. Nun wählen Sie im rechten Fenster des Editors den Eintrag
AUTOMATISCHE UPDATES KONFIGURIEREN aus ([Abbildung](#)

19.10).

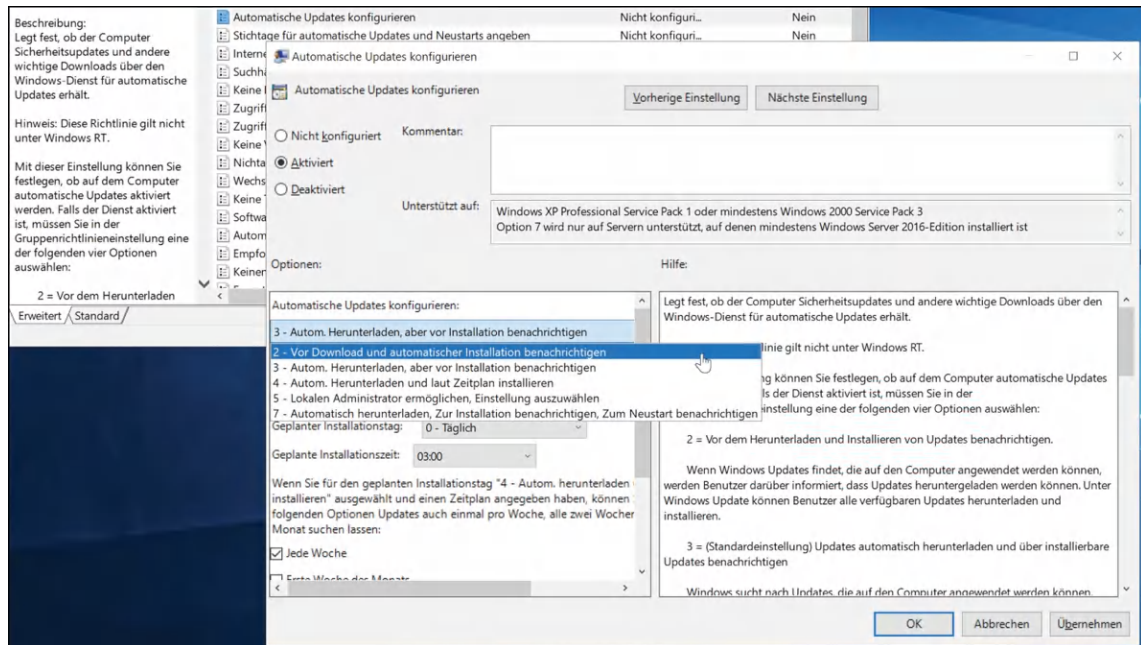


Abbildung 19.10: Mit dem Eintrag »Automatische Updates konfigurieren« können Sie genau festlegen, wie und wann Updates auf den Server gelangen.

4. In dem Fenster, das sich nun öffnet, finden Sie eine ganze Reihe von Optionen und Einstellmöglichkeiten. Ist der Status dieser Richtlinie auf NICHT KONFIGURIERT festgelegt, so wurde die Verwendung von automatischen Updates auf diesem System nicht auf Gruppenrichtlinienebene festgelegt. Allerdings können Sie als Administrator automatische Updates weiterhin über die Systemsteuerung konfigurieren.
5. Aktivieren Sie diese Richtlinie, so wird automatisch die Standardeinstellung AUTOM. HERUNTERLADEN, ABER VOR INSTALLATION BENACHRICHTIGEN eingestellt.

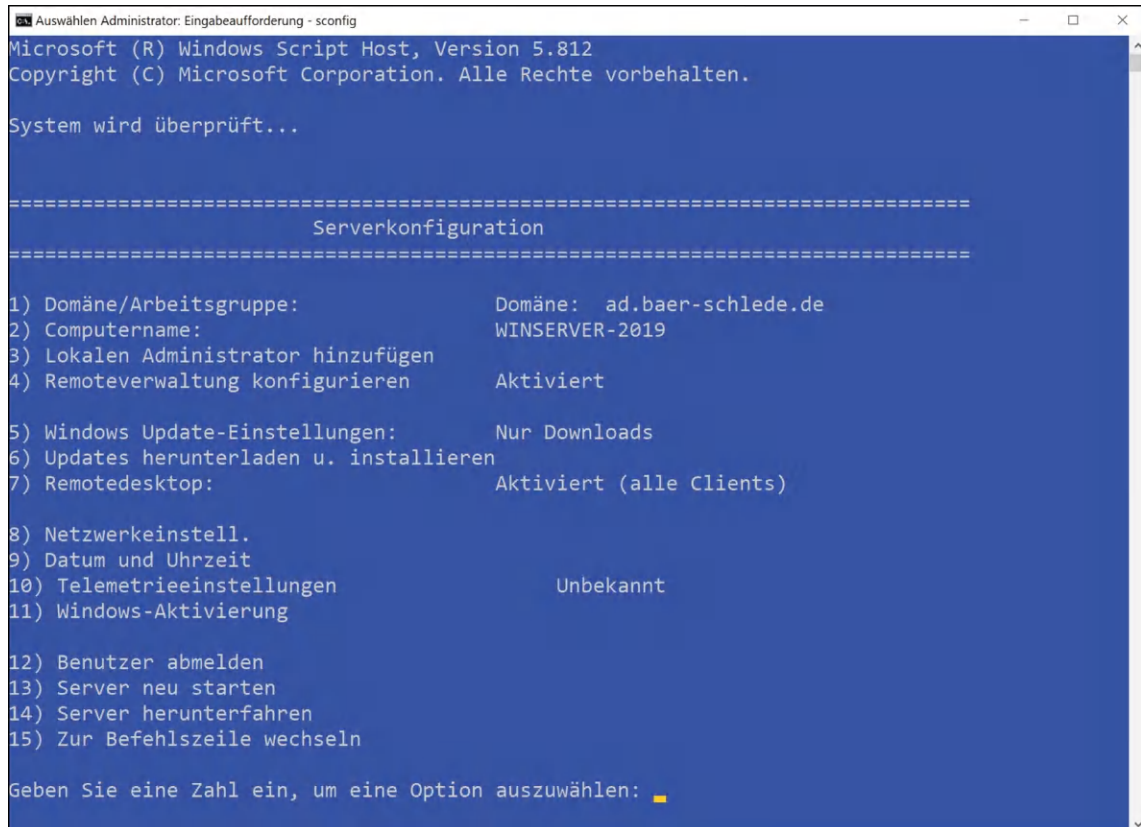
Insgesamt stehen Ihnen nach der Aktivierung dieser Richtlinie sieben verschiedene Möglichkeiten für die Konfiguration der automatischen Updates zur Verfügung. Dabei können Sie beispielsweise auch die Updates automatisch herunterladen und laut einem Zeitplan installieren, den Sie ebenfalls an dieser Stelle konfigurieren können. Nur für die Server-Versionen von Windows steht dabei unter anderem die Möglichkeit VOR DEM INSTALLIEREN VON UPDATES UND VOR

NEUSTARTS BENACHRICHTIGEN zur Verfügung. Lesen Sie bitte auf jeden Fall die Beschreibungen genau durch, die Ihnen hier bei den lokalen Gruppenrichtlinien angezeigt werden. Microsoft ändert sowohl diese Einstellungen als auch deren Wirkungsbereich immer wieder einmal mit den Release-Wechseln.

Update-Einstellungen mittels sconfig ändern

Wenn Ihnen die zuvor erläuterten Einstellmöglichkeiten für die automatischen Updates mithilfe der lokalen Gruppenrichtlinien zu kompliziert erscheinen, so bietet Ihnen Windows Server noch eine weitere Möglichkeit zur Änderung dieser Einstellungen: das Kommandozeilen-Programm sconfig.

1. Rufen Sie eine Eingabeforderung mit Administratorrechten auf und geben an der Kommandozeile sconfig ein.
2. Daraufhin startet das Programm mit einer textorientierten Oberfläche ([Abbildung 19.11](#)). Es wird deshalb auch gern für die Konfiguration eines Windows-Servers in der Core-Variante verwendet.



```
Auswählen Administrator: Eingabeaufforderung - sconfig
Microsoft (R) Windows Script Host, Version 5.812
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

System wird überprüft...

=====
                          Serverkonfiguration
=====

1) Domäne/Arbeitsgruppe:          Domäne: ad.baer-schlede.de
2) Computernamen:                WINSERVER-2019
3) Lokalen Administrator hinzufügen
4) Remoteverwaltung konfigurieren  Aktiviert

5) Windows Update-Einstellungen:  Nur Downloads
6) Updates herunterladen u. installieren
7) Remotedesktop:                Aktiviert (alle Clients)

8) Netzwerkeinstell.
9) Datum und Uhrzeit
10) Telemetrie-einstellungen      Unbekannt
11) Windows-Aktivierung

12) Benutzer abmelden
13) Server neu starten
14) Server herunterfahren
15) Zur Befehlszeile wechseln

Geben Sie eine Zahl ein, um eine Option auszuwählen: 
```

Abbildung 19.11: Auch das Kommandozeilen-Programm »sconfig« bietet recht komfortable Möglichkeiten für die Update-Einstellungen.

3. Um einen Eintrag auszuwählen, müssen Sie die entsprechende Zahl aus dem Menü unten bei der Eingabeaufforderung eingeben.
4. Für die Windows-Update-Einstellungen ist das die 5. Sie sehen hier auch, dass die aktuelle Einstellung den Wert NUR DOWNLOADS hat.
5. Nach der Auswahl stehen Ihnen dann drei Optionen für die Update-Einstellung zur Verfügung: (A)UTOMATISCH, NUR (D)OWNLOADS, (M)ANUELLE UPDATES.

Wir haben in der [Abbildung 19.12](#) die Option für manuelle Updates gewählt. Das System teilt uns danach mit, dass es von nun an nie nach Update suchen wird.

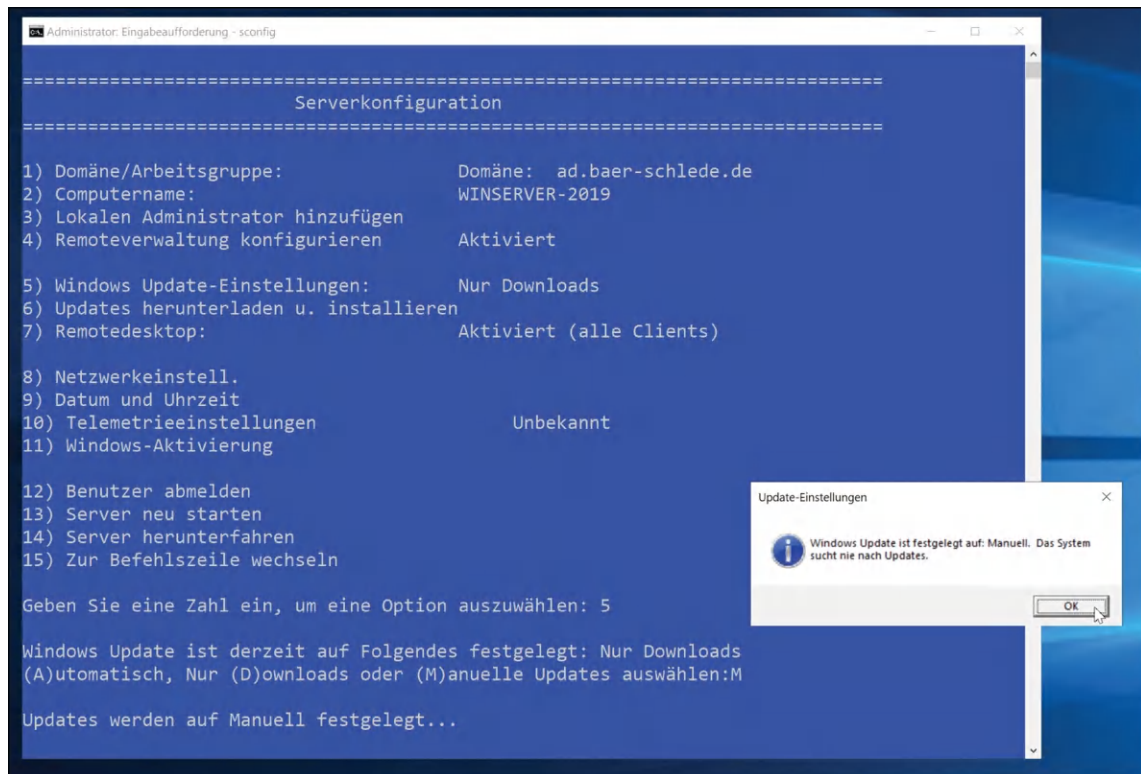


Abbildung 19.12: Mithilfe von »sconfig« können Sie die Update-Einstellungen sehr schnell und einfach ändern – in diesem Beispiel auf »Manuell«.

Sie können mit diesem Programm natürlich durch die Wahl der Einstellung AUTOMATISCH den Update-Prozess Ihres Windows-Servers auch derart konfigurieren, dass er wie bei den Windows-10-Systemen abläuft: Updates werden immer und ohne weiteres Zutun automatisch heruntergeladen und auch installiert. Wir raten jedoch davon ab, diese Einstellung für Server-Systeme zu nutzen. Es ist nach unserer Erfahrung immer sicherer, wenn der Systemverantwortliche zuvor noch einen Blick auf die Updates werfen kann, bevor diese auf einem so wichtigen System installiert werden.

Kapitel 20

Backup

IN DIESEM KAPITEL

Grundlagen der Sicherung und Wiederherstellung

Windows-Server-Sicherung

Worum handelt es sich beim Azure-Backup-Dienst?

Sie dürfen sich als Administrator sicher sein, es gibt kein Thema, das schwerer, quasi wie Blei, auf diesem Berufsstand lastet, als Sicherung und Wiederherstellung. Backup interessiert in der Regel niemanden, und wir meinen das wirklich genauso, wie wir es geschrieben haben:

NIEMANDEN! Aber das nur so lange, bis jemand gelöscht, entweder versehentlich oder durch Fremdverschulden, Informationen wieder benötigt. Wehe dem Systemverantwortlichen, der dann nicht über die notwendigen Sicherungskopien der Daten verfügt. Schließlich ist die Durchführung der Sicherung eine »selbstverständliche Aufgabe« des Administrators.



Kein Backup – kein Mitleid! Es gibt T-Shirts und Aufkleber mit diesem Spruch. Sie sollten ihn unbedingt beherzigen. Sie wollen ja nicht als der IT-Profi in Ihrem Unternehmen in die Geschichte eingehen, der dafür verantwortlich ist, dass Daten verloren gingen.

Aufgrund der hohen Wichtigkeit sollten Sie an diesem Punkt nicht mit sich verhandeln lassen. Ist nicht genügend Speicherplatz für das Backup vorhanden oder werden Ihnen die Ressourcen (Geld, Material oder Schulung) nicht zur Verfügung gestellt, lassen Sie es sich von Geschäftsführung oder dem Kunden unterschreiben, dass Sie jegliche Verantwortung für den sicheren Betrieb der Server von sich weisen.



Informieren Sie sich zum aktuellen Stand aus dem Bereich »Konzepte und Vorgehensweisen« des Bundesamts für Sicherheit in der Informationstechnik (BSI). In der Beschreibung von »CON.3: Datensicherungskonzept« erhalten Sie einen hervorragenden Überblick und können ein Gespür dafür entwickeln, welche Anforderungen wirklich als MUSS-Kriterien gelten.

Grundlagen der Sicherung und Wiederherstellung

Ohne nun alle Empfehlungen und Hinweise des BSI im Detail durchzugehen, gibt es ein paar zwingende Grundlagen, die vor der Einrichtung einer Sicherung bedacht werden müssen:

- ✓ Was wollen Sie sichern? Die Daten oder den ganzen Server?
- ✓ Wo soll die Sicherung gelagert werden?
- ✓ Welchen Zeitraum wollen Sie sichern?
- ✓ Wie lange dauert es, bis Sie eine Wiederherstellung durchgeführt haben?
- ✓ Wie und wie oft werden Sie den Wiederherstellungsfall proben?
- ✓ Auf welches Medium soll gesichert werden?
- ✓ Sie kennen die Begriffe Vollsicherung, inkrementelles Backup und differenzielles Backup?

Im einfachsten Fall richten Sie einen Sicherungsjob ein, der den kompletten Server regelmäßig sichert. Üblicherweise führen Administratoren, sofern es keine anderen Vorgaben gibt, eine Sicherung in der Nachtzeit durch, wenn die Last auf den Servern in den Nachtstunden geringer ist. Praktischerweise legen Sie zusätzlich untertägige Zwischensicherungen mit Schattenkopien an, um einzelne Dateien oder Ordner zügig wiederherstellen zu können.

Falls es keine anderslautenden Vorgaben gibt, sollten Sicherungen in einem anderen »Brandabschnitt« gelagert werden. Es nützt wenig, wenn sich die kompletten Sicherungsbänder oder -platten auf dem Tisch neben dem Server befinden. Im Katastrophenfall wäre nicht nur die Maschine betroffen, sondern auch die Sicherung. Je nach Firmengröße kann es auch sinnvoll sein, dass ein Mitarbeiter täglich das Backup-Medium tauscht und mit sich führt. Achten Sie bei solchen Szenarien auf die Verschlüsselung der Sicherung – nicht, dass durch Unachtsamkeit der komplette Datenstand der Firma als Backup in falsche Hände gerät.

Die Frage des Zeitraums ist pauschal nicht zu beantworten. Manche Missstände zeigen sich erst nach einem längeren Zeitraum, sodass ein möglicher Wiederherstellungszeitraum von einer Woche vielleicht zu kurz sein könnte. Klassischerweise greifen Administratoren auf das »Generationenprinzip« zurück, bei dem mit 20 Speichermedien ein Zeitraum von zwei Jahren abgedeckt wird.



Infos zum »Generationenprinzip« finden Sie im Internet – einfach in eine Suchmaschine eingeben!

Die Wiederherstellungszeit (Recovery Time Objective (RTO)) ist letztendlich das entscheidende Kriterium für den grundsätzlichen Aufbau der Sicherung. Hierbei geht es darum, wie lange es dauern darf, bis verloren gegangene Daten wieder verfügbar sind. Wenn der Ausfall eines Systems beziehungsweise dessen Datenstände für 48 Stunden vertretbar ist, können Sie deutlich günstigere Technologie zum Einsatz bringen, als wenn das Unternehmen bereits nach 4 Stunden durch den Ausfall massiv an Geld, Daten oder Reputation verliert.

Eben der RTO-Wert bricht vielen »Cloud First«-Konzepten im ländlichen Raum das sprichwörtliche Genick. Wer nur mit einem 25-MBit-DSL-Anschluss und einem durchschnittlichen Upload von 2 MBit auf Internet-Ressourcen zugreift, kann die Wiederherstellung eines SQL-Servers mit 800 GByte Datenbankgröße in 8 Stunden schlichtweg vergessen. Als zusätzliche »Offsite«-Sicherung der Daten für den Katastrophenfall sind Cloud-Systeme wiederum äußerst hilfreich.

Hand aufs Herz: Wenn ein Standort durch einen Brandschaden oder durch eine Naturkatastrophe komplett vernichtet ist, dürfte die Wiederherstellung eines Servers in 4 Stunden zunächst einmal das geringere Problem darstellen. Ganz anders sieht es jedoch 14 Tage später aus – wenn Ersatzräumlichkeiten bezogen sind und die Kundendaten nicht bearbeitet werden könnten, weil es gar keine Daten mehr gibt.



Führen Sie laufende Recovery-Tests durch. Sie werden es nicht für möglich halten, dass es Kollegen gibt, denen über Monate niemals auffiel, dass ihr Backup fast auf die Sekunde genau immer die gleiche Zeit braucht wie die Sicherung.

Wie oft sollten Sie die Wiederherstellung von Daten proben? Ehrlich gesagt, sind Sie den meisten Kollegen bereits weit voraus, wenn Sie es überhaupt schon einmal gemacht haben. Im Tagesgeschäft geht so etwas gern unter, und wenn es dann passieren muss, entsteht zeitlicher Druck, und es drohen Bedienungsfehler. Erstellen Sie sich einen regelmäßigen Termin im Kalender, blockieren Sie sich die Zeit und führen Sie Recovery-Tests durch. Hierfür erstellen Sie sich eine genaue To-do-Liste, die Sie stur abarbeiten. Wenn diese Anleitung perfekt ist, sollten Sie sie so deponieren, dass auch andere Administratoren mit der Anleitung arbeiten könnten – vielleicht sind Sie auf dem Weg auf den K2, während die Wiederherstellung der Sicherung ansteht.

Nun steht noch eine weitere Frage im Raum: Auf welche Medien sollten Sie als Administrator Ihre Server sichern. Typischerweise wählen IT-Profis in größeren Umgebungen LTO-Bänder. Dank ihres günstigen Preises pro GByte, dem hohen Tempo, der Beständigkeit und der Tatsache, dass sogenannte Bandroboter existieren, die bei Bedarf das nächste Band ins Laufwerk einschieben, eine technisch gute Wahl.

In kleineren Umgebungen sind LTOs jedoch kaum zu finden. Hier wird eher direkt auf die Festplatte von einem anderen Server oder auf mobile Festplatten (USB) gesichert. RDX-Medien, quasi Festplatten in einem staub- und stoßsicheren Auswurfgehäuse, sind eine gute Alternative. RDX bietet den Vorteil, dass die Medien ebenfalls seit vielen Jahren auf dem Markt sind und es de facto keine Limitierungen in Bezug auf neue

Versionen gibt. Kaum verwunderlich, es steckt in Wirklichkeit nur ein verlängerter SATA-Anschluss im Gehäuse. Externe Laufwerke mit einem USB-2.0-Anschluss sind einfach etwas langsamer als interne SATA-beziehungsweise externe USB-3.0-Varianten.

Die Unterstützung für Wechselmedien, insbesondere von Bändern, ist ein Leistungsmerkmal der teuren, professionellen Backup-Lösungen.

Dahingegen geht das RDX als »fixed Disk« durch, was die Verwendung des Mediums auch mit günstigen Backup-Programmen, also auch den Bordmitteln von Microsoft Windows, ermöglicht.



Nun noch die drei Begrifflichkeiten:

- ✓ *Vollbackup*: Der komplette gewünschte Datenbereich wird stets vollumfänglich gesichert. Nachteilig ist der Umstand, dass es lang dauert. Der Vorteil wiederum ist, dass Sie stets nur die eine Sicherung brauchen, um den ganzen Datenbereich wiederzustellen.
- ✓ *Differenzielles Backup*: Sie beginnen mit einem Vollbackup und speichern beim nächsten Sicherungsvorgang nur die Veränderung (Differenz) zur Vollsicherung. Vorteil des Verfahrens: Weniger Speicherplatzbedarf als beim Vollbackup, es sind nur das Vollbackup und die Differenzsicherung für die Wiederherstellung erforderlich. Nachteil ist, dass sich stets verändernde Daten immer wieder neu gesichert werden.
- ✓ *Inkrementelles Backup*: Sie beginnen mit einem Vollbackup und speichern anschließend beim nächsten Sicherungslauf nur die Veränderung zur letzten Sicherung. Vorteil: recht einfaches Verfahren mit wenig Speicherplatzbedarf. Nachteil: Sie benötigen jede Sicherung für die Wiederherstellung (Vollbackup und ALLE inkrementellen Sicherungen).

Windows-Server-Sicherung

Um die Windows Server-Sicherung nutzen zu können, müssen Sie diese zunächst installieren. Im einfachsten Fall installieren Sie die Rolle über den Server-Manager:

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie oben rechts unter VERWALTEN den Eintrag ROLLEN UND FEATURES HINZUFÜGEN.
3. Bestätigen Sie den gewünschten Server/Installationstyp.
4. Klicken Sie im Dialog SERVERROLLEN auf WEITER.
5. Wählen Sie unter FEATURES den Eintrag WINDOWS SERVER-SICHERUNG.
6. Bestätigen Sie die Eingabe mit WEITER.
7. Klicken Sie auf INSTALLIEREN. Sie können das Dialogfenster schließen, auch wenn die Installation selbst noch nicht abgeschlossen ist.



Sie können die Windows-Server-Sicherung auch auf einem Windows-Core-Server ohne grafische Oberfläche installieren. Wählen Sie hierzu in der PowerShell den Befehl `Install-WindowsFeature Windows-Server-Backup` an.

Da der Einsatz der MMC für das Bearbeiten von Sicherungs- und Wiederherstellungsjobs jedoch auf einem Core-Server nicht möglich ist, müssen Sie als Administrator hierzu einen anderen Server mit Desktop-Installation oder die Remoteserver-Verwaltungstools für Windows 10 nutzen.

Auch wenn es sich bei der Windows-Server-Sicherung lediglich um ein Feature des Betriebssystems Windows handelt, ist das Programm eine vollwertige Backup- und Wiederherstellungslösung. Seit Windows Server 2008 haben Administratoren mit der Software die Möglichkeit, folgende Sicherungsjobs durchzuführen:

- ✓ Komplettsicherung des Servers, inklusive Betriebssystem

- ✓ Einzelne Dateien und Ordner sichern
- ✓ Applikations-konsistente Sicherungen durchführen (zum Beispiel SQL-Server)

Der Hersteller Microsoft empfiehlt gar, die Sicherung des Active Directory, Exchange-Server und Hyper-V-Hosts mit diesen Bordmitteln zu sichern, selbst wenn bereits andere Lösungen im Einsatz sind. Dabei ist das technische Fundament der Windows-Server-Sicherung auch die Basis der professionellen Drittanbieter.



Die Windows-Server-Sicherung ist seit einigen Windows-Versionen faktisch unverändert geblieben. Die Strategie von Microsoft liegt in der Nutzung der Cloud-Speicher als zentrales Sicherungsziel. Microsoft setzt vor allem auf »Azure Site Recovery«, andere Hersteller propagieren ähnliche Lösungen. Wenn Sie über das Windows Admin Center die Option SICHERN installieren, richten Sie nicht das Feature WINDOWS SERVER-SICHERUNG ein, sondern das Azure-basierte Speicherkonzept von Microsoft.

Einrichten von Backup-Jobs

Nachdem das Feature installiert ist, können Sie über den MMC-Dialog WINDOWS SERVER-SICHERUNG Jobs anlegen. Zur Auswahl stehen:

- ✓ Einzelsicherungen
- ✓ Sicherungszeitplan

Der komplette Vorgang ist, wie bei Windows üblich, auf einen Software-Assistenten gestützt (siehe [Abbildung 20.1](#)). Sie müssen lediglich ein paar Fragen beantworten und haben eine Einzelsicherung oder einen Zeitplan angelegt.

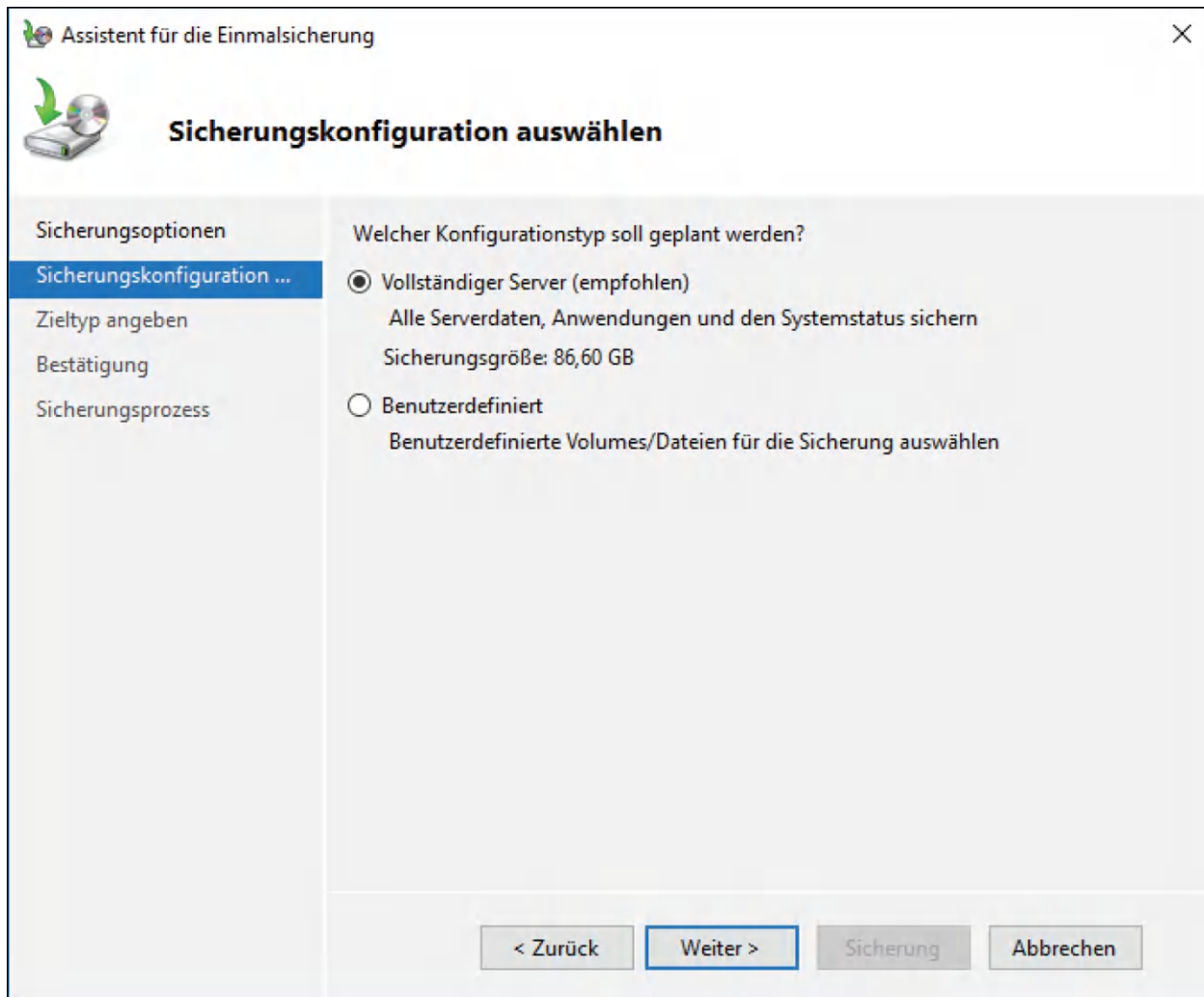


Abbildung 20.1: Die »Windows Server-Sicherung« ist komplett assistentengestützt und erklärt sich glücklicherweise von allein.

Bei der Anlage eines Sicherungsjobs haben Sie die Möglichkeit, festzulegen, wie sich das Backup in Bezug auf die Zugriffssteuerung verhalten soll. Die typische Einstellung lautet VERERBEN – jeder Benutzer, der Zugriff auf das Backup-Ziel hat, darf auch auf die Daten zugreifen. Die zweite verfügbare Option lautet NICHT VERERBEN, hierbei wird bei der Anlage des Jobs ein Benutzername ausgewählt, der auf die Daten zugreifen darf.

Sofern Sie einzelne Elemente für die Sicherung ausgewählt haben, gibt es die Möglichkeit, Dateitypen auszuschließen. Ein Beispiel für ausschließbare Elemente wären Log- oder Temporär-Dateien, da diese üblicherweise für eine Wiederherstellung nicht von Bedeutung sind. Wer

sich unsicher ist, schließt besser keine Dateien oder Dateitypen aus.

In [Abbildung 20.2](#) sind die beiden Optionen für die Volumenschattenkopie-Einstellungen ersichtlich. Sofern Sie keine andere Sicherungslösung im Einsatz haben, wählen Sie den Eintrag VOLLSTÄNDIGE VSS-SICHERUNG. Hiermit signalisieren Sie dem Betriebssystem, dass die Merkmale, die den Backup-Vorgang dokumentieren, entsprechend durch das Betriebssystem gesetzt werden.

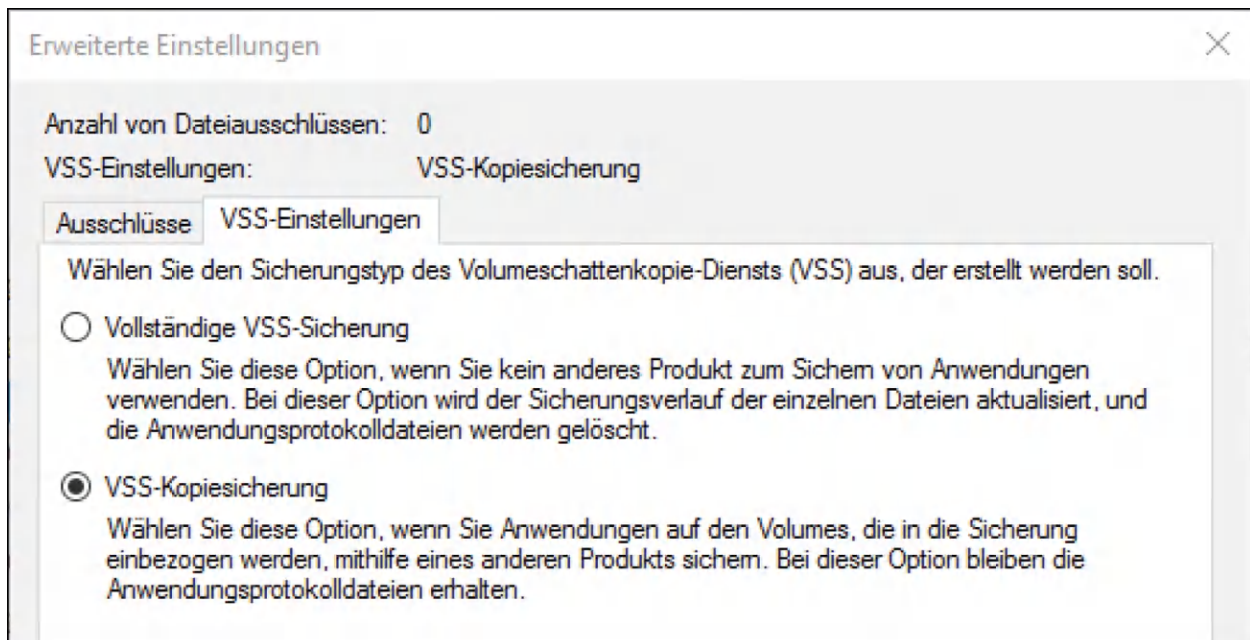


Abbildung 20.2: VSS-Optionen für die Sicherung von einzelnen Elementen

Backup-Jobs können Sie entweder für einen ganzen Computer oder einzelne Datei- und Ordnerbereiche erstellen. Über die Schaltfläche ELEMENTE HINZUFÜGEN können Sie festlegen, welche Teile gesichert werden sollen. Sofern Sie sich im Zuge der Auswahl in der Dateiliste für den Eintrag BARE-METAL-RECOVERY entscheiden, können Sie kein Element ausschließen. Bei dieser Sicherung handelt es sich um ein Backup, das eine 1:1-Wiederherstellung – auch auf einer anderen Hardware – ermöglicht.

Recovery-Medium nutzen

Nicht selten findet eine solche Wiederherstellung gar nicht auf der

originalen Maschine statt, sondern auf einem anderen System oder direkt in einer virtuellen Umgebung. Während andere Backup-Programme spezielle Wiederherstellungs-Boot-Datenträger erzeugen, dient bei Microsoft der Installationsdatenträger von Windows als Boot-beziehungsweise Recovery-Medium. Nach dem Start über den Datenträger wählen Sie im Dialogfenster WINDOWS-SETUP unten links COMPUTERREPARATUROPTIONEN aus, anschließend PROBLEMBEHANDLUNG und dann in der Auswahl ERWEITERTE OPTIONEN den Eintrag SYSTEMIMAGE-WIEDERHERSTELLUNG. Sie können den UNC-Pfad einer Dateifreigabe auswählen, wenn Sie lokal keinen Zugriff auf das Systemabbild haben.



Wie bereits erwähnt: Das sollten Sie schon einmal »trocken« geübt haben. Nur dann löst der Dialog »Partitionierung« auf dem neuen Server keine Schweißperlen auf der Stirn aus. Ohne Partition, kann Windows keine Daten speichern – und somit auch nicht wiederherstellen.

Einzelne Dateien wiederherstellen

Eine einzelne, verloren gegangene Datei stellt ein erfahrener Administrator stets über Vorgängerversionen und Schattenkopien her, sofern er die Wahl hat. Das geht einfach am schnellsten – und wenn Sie es klug anstellen, bringen Sie es Ihren Benutzern gleich selbst bei. Das erspart Meldungen im Ticketsystem!

Der komplette Wiederherstellungsvorgang für Ordner und Dateien ist faktisch selbsterklärend. Zunächst gilt es, den Speicherorttyp auszuwählen – hierbei handelt es sich um den Medientyp, beispielsweise lokale Platte oder Netzwerklaufwerk, dann das Sicherungsverzeichnis über den Ordner selbst. Es folgt die Auswahl des Speicherzeitpunkts (siehe [Abbildung 20.3](#)) und der gewünschten Wiederherstellungselemente. Keine Sorge – Sie haben als Administrator die Möglichkeit, die Daten an einem anderen Speicherplatz wiederzustellen.

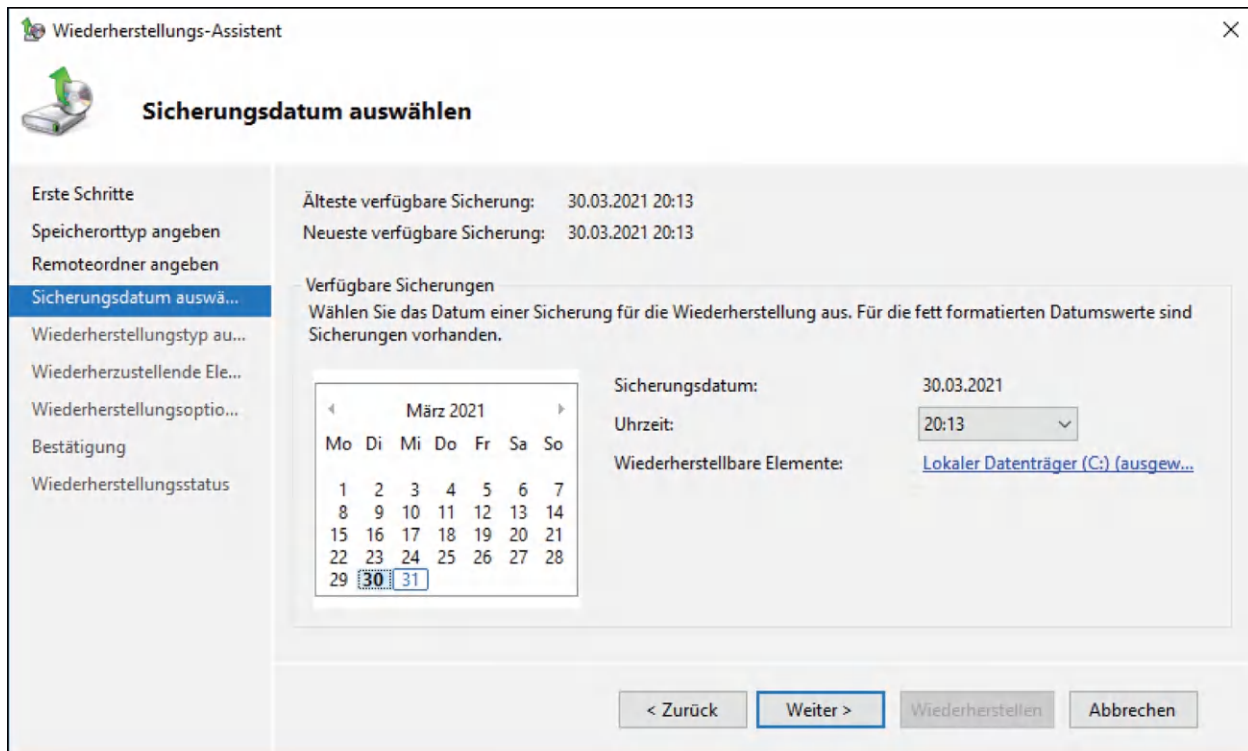


Abbildung 20.3: Zunächst gilt es, den Speicherort für das Backup auszuwählen, dann folgt der Sicherungszeitpunkt.

Nun haben wir so viel über Sicherung geschrieben und an keiner Stelle kam die Auswahl, ob Sie Vollbackups oder inkrementell sichern möchten. Die Differenzmethode bietet das Bordwerkzeug von Microsoft gleich gar nicht erst an. Die Einstellung haben die Entwickler unter **LEISTUNGSEINSTELLUNGEN** im Hauptdialog des MMC-Fensters auf der rechten Seite versteckt, siehe [Abbildung 20.4](#).

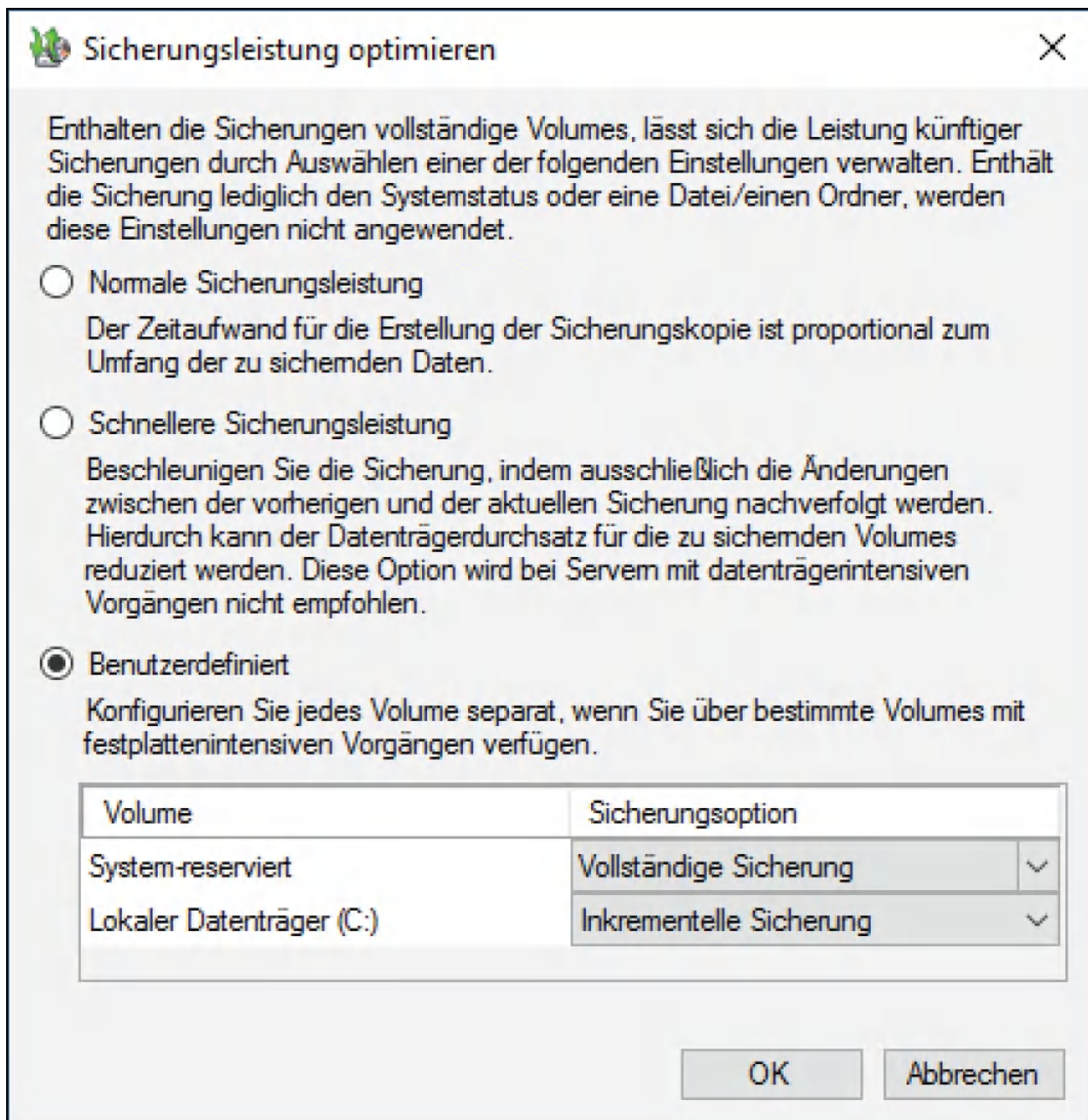


Abbildung 20.4: Die »Windows Server-Sicherung« bietet die Optionen zur vollständigen und inkrementellen Sicherung.

Worum handelt es sich beim Azure-Backup-Dienst?

Der Azure Backup-Dienst bietet einfache, sichere und kostengünstige Lösungen, um Ihre Daten zu sichern und aus der Microsoft-Azure-Cloud

wiederherzustellen. Das Azure-Backup kostet somit stets einen gewissen Obolus. Neben Cloud-Ressourcen wie Azure-VMs, Azure Managed Disks, Azure-File-Freigaben, SQL-Server auf Azure-VMs oder SAP-HANA-Datenbanken auf Azure-VMs können Sie auch lokale Dateien, Ordner oder den Systemstatus sichern. Hierzu benötigen Sie jedoch den sogenannten Microsoft Azure Recovery Services-Agent (MARS). Alternativ können Sie den DPM- oder Azure Backup Server-Agent (MABS) verwenden, um lokale VMs (Hyper-V und VMware) und andere lokale Workloads zu schützen.

Tatsächlich gibt es eine Vielzahl guter Gründe, die für die Verwendung von Azure Backup sprechen, beispielsweise:

- ✓ **Auslagerung lokaler Sicherungen:** Azure Backup bietet eine einfache Lösung, mit der Sie Ihre lokalen Ressourcen in der Cloud sichern können. Mit Azure Backup erhalten Sie kurz- und langfristige Sicherungen, ohne komplexe lokale Sicherungslösungen vor Ort einrichten zu müssen.
- ✓ **Sicherung virtueller Azure-IaaS-Computer:** Azure Backup bietet unabhängige und isolierte Sicherungen zum Schutz vor dem versehentlichen Löschen von Originaldaten. Sicherungen werden in einem »Recovery Services-Tresor« mit integrierter Verwaltung von Wiederherstellungspunkten gespeichert. Konfiguration und Skalierung sind unkompliziert. Sicherungen werden außerdem optimiert und können bei Bedarf wiederhergestellt werden.
- ✓ **Unkomplizierte Skalierung:** Dank der Leistung und unbegrenzten Skalierbarkeit der Azure-Cloud bietet Azure Backup Hochverfügbarkeit ohne Wartungs- oder Überwachungsaufwand. Sprich: Ihr Backup-Bereich wächst dynamisch mit Ihren Anforderungen mit.
- ✓ **Unbegrenzte Datenübertragungen:** Die Menge an übertragenen ein- oder ausgehenden Daten wird vom Anbieter Microsoft nicht beschränkt, und es fallen keine weiteren Kosten für die übertragenen Daten an. An diesem Punkt unterscheidet sich das Angebot von Microsoft von den »Marktbegleitern«, zumindest zum Zeitpunkt der

Manuskripterstellung.

- ✓ Ausgehende Daten sind Daten, die während eines Wiederherstellungsvorgangs aus einem Recovery-Services-Tresor übertragen werden.
- ✓ Wenn Sie mit dem Import-/Export-Dienst von Azure eine erste Sicherung im Offlinemodus ausführen, um große Datenmengen zu importieren, fallen Kosten für eingehende Daten an.
- ✓ Mehrere Speicheroptionen: Azure Backup bietet drei Replikationsarten, um die Hochverfügbarkeit Ihres Speichers beziehungsweise Ihrer Daten sicherzustellen:
 - Lokal redundanter Speicher (Locally Redundant Storage, LRS) repliziert Ihre Daten dreimal in einer Speicherskalierungseinheit in einem Datacenter. (Es werden also drei Kopien Ihrer Daten erstellt.) Alle Kopien der Daten befinden sich in derselben Region. LRS ist eine kostengünstige Möglichkeit, um Daten vor lokalen Hardware-Fehlern zu schützen.
 - Geografisch redundanter Speicher (Geo-Redundant Storage, GRS) ist die standardmäßige und empfohlene Replikationsoption. GRS repliziert Ihre Daten in einer sekundären Region, die mehrere Hundert Kilometer vom primären Speicherort der Quelldaten entfernt ist. GRS führt zu höheren Kosten als LRS, bietet aber eine höhere Dauerhaftigkeit Ihrer Daten (auch im Falle eines regionalen Ausfalls).
 - Zonenredundanter Speicher (ZRS) repliziert Ihre Daten in Verfügbarkeitszonen und gewährleistet dadurch Data Residency und Resilienz in derselben Region. Bei ZRS gibt es keine Downtime. Daher können Ihre kritischen Workloads, die Data Residency erfordern und für die keine Downtime auftreten darf, in ZRS gesichert werden.



Die Kombination aus der Windows-Server-Sicherung und dem

Azure-Dienst stellt bereits eine leistungsfähige Lösung dar. Nichtsdestotrotz möchten wir darauf hinweisen, dass es viele gute Backup- und Recovery-Lösungen am Markt gibt. Es muss nicht immer Microsoft sein. Insbesondere die doppelte Sicherungsstrategie bestehend aus der Windows-Server-Sicherung und einer zusätzlichen Backup-Software ist verlockend.

Wir kommen nicht umhin, zumindest einmal den Namen eines besonders am Markt etablierten Anbieters zu nennen: Veeam!

Kapitel 21

Ausfälle und deren Vermeidung

IN DIESEM KAPITEL

Ursachen von Ausfällen

Vermeidung

Monitoring

Jeder Server wird irgendwann einmal in eine »Fehlstellung« geraten und mit ziemlicher Sicherheit auch einmal ausfallen. Als Administrator müssen Sie dafür sorgen, dass ein Server möglichst niemals ausfällt und die bereitgestellten Dienste stets zur Verfügung stehen – ein hochgestecktes Ziel.

Leider gibt es kaum aktuelle Daten, die Server-Ausfälle analysieren. Einzig eine Studie von Hewlett Packard aus dem Jahr 2013 gibt für Deutschland einige interessante Anhaltspunkte. Für die Studie wurden rund 300 mittelständische Unternehmen mit 200 bis 4.999 Angestellten zur Häufigkeit und zu den Gründen für einen Server-Ausfall befragt. Mehr als drei Viertel aller Teilnehmer gaben an, dass innerhalb der letzten 12 Monate mindestens ein Ausfall in systemkritischen Bereichen aufgetreten sei.



Dreiviertel der Unternehmen gaben in einer Studie an, dass innerhalb eines Jahrs mindestens ein systemkritisches Server-System ausfiel.

Zu den möglichen genannten Auslösern zählen unter anderem in dieser Studie:

- ✓ Angriffe wie eine DDoS-Attacke

- ✓ Versagen der Hardware inklusive CPU, Festplatten oder Expansion Cards
- ✓ Bugs in der Software
- ✓ Probleme im Netzwerk durch Router, Switches, Security-Server oder Verkabelung
- ✓ Menschliches Versagen
- ✓ Gezielte Cyberkriminalität oder -spionage wie Spear Phishing, Social Engineering oder Datendiebstahl durch Man-in-the-Middle-Angriffe
- ✓ Infiltration kritischer Bereiche durch Viren, Würmer, Ransomware oder Trojaner
- ✓ Unfälle wie Brand oder Wasserschaden
- ✓ Versagen von externen Dienstleistern, etwa Stromausfälle
- ✓ Innere oder äußere Sabotage durch Manipulation von SCADA-Systemen
- ✓ Ausnutzen von Sicherheitslücken für das Eindringen in das Netzwerk
- ✓ Probleme beim Betriebssystem (Windows Blue Screen, Linux Kernel Panic)

Wie unschwer zu erkennen ist, handelt es sich um ein weit gestreutes Feld an möglichen Ursachen für Server-Ausfälle. Weiter heißt es in der Erhebung, dass die Reparatur für einen Server-Ausfall rein statistisch in etwa 3,8 Stunden dauert. Wie hoch der finanzielle Schaden ist, wird in der Studie zwar ebenfalls berechnet, jedoch sind diese Ausformulierungen meistens nur noch »Schall und Rauch«, da es äußerst schwierig ist, die wirtschaftlichen Folgen für vollkommen unterschiedliche Firmen und Institutionen über einen Durchschnittswert zu ermitteln.

Wichtig für Sie als Administrator ist: Ihre Systeme werden einmal ausfallen, und alle Eventualitäten zu berücksichtigen, ist eine nur schwer zu lösende Aufgabe. Einige der genannten Ursachen haben wenig mit dem eigentlichen Server-Management zu tun, darum mögen sich die jeweiligen Abteilungen bemühen, bei anderen Aufgaben steht der Server-Administrator ganz klar in der Pflicht.

Vermeidung von Ausfällen

Bei Autos, Maschinen und Heizanlagen ist es vollkommen normal, dass diese Maschinen regelmäßig einer Wartung unterzogen werden. Interessanterweise ist die Wartung in der IT nicht in diesem Maße verbreitet – das hat einen ganz simplen Grund, wie der Definition zu entnehmen ist:



Als Wartung werden gemäß DIN 31051 (Stand 2003) Maßnahmen zur Verzögerung des Abbaus des vorhandenen Abnutzungsvorrats der Betrachtungseinheit verstanden. Sie wird während der Nutzung eines Objekts angewandt.

Server-Systeme haben, mit Blick auf die Hardware, in dem Sinne keine echte Abnutzung – von mechanischen Belastungen für Lüfter und dem thermischen Einwirken auf das Gesamtsystem einmal abgesehen. Sehr wohl gibt es aber eine Software-Wartung, die eine laufende Veränderung eines Software-Produkts nach dessen Auslieferung darstellt. Grund dieser Maßnahme ist es, Fehler zu beheben, die Performanz zu steigern oder andere Attribute zu verbessern.

Natürlich können Sie, als pflichtbewusster Administrator, einen Instandhaltungs- oder Wartungsplan für Server-Komponenten erstellen, um beispielsweise

- ✓ Lüfter,
- ✓ drehende Festplatten und
- ✓ Bandlaufwerke

regelmäßig zu ersetzen. Aber, das soll nicht unerwähnt bleiben, ist der zu erwartende Produktlebenszyklus in der Regel so bemessen, dass während der zu erwartenden Laufzeit des Server-Systems zwischen drei und fünf Jahren keine dieser Komponenten ausfallen sollte.

Da ist die Einhaltung der regelmäßigen Wartungsintervalle einer Klimaanlage im Server-Raum beziehungsweise Rechenzentrum schon

deutlich wichtiger. Von den Handfeuerlöschern ganz zu schweigen – auch diese müssen im Ernstfall garantiert funktionieren und bedürfen daher der regelmäßigen Prüfung mit dem entsprechenden Instandhaltungsnachweis.



Die regelmäßigen Wartungsarbeiten als Administrator betreffen in erster Linie das Betriebssystem und die darauf aufsetzenden Applikationen.

Bevor wir uns thematisch auf die Vermeidungstätigkeiten stürzen, sei noch kurz auf ein anderes Thema hingewiesen: Zugriff. Natürlich betreiben IT-Profis einen großen Aufwand, um sicherzustellen, dass keine unbefugten Personen Zugriff auf ein Server-System erhalten. Firewalls, Zugriffsregeln und Passwörter sind dabei nur das allgemeingültige Repertoire.

Mit derselben Aufmerksamkeit sollten Sie sich jedoch auch einmal die Frage stellen, welche Personen die IT-Räumlichkeiten, inklusive Rechenzentrum oder Server-Raum betreten können! In der Praxis haben die Autoren hier schon die seltsamsten Formen von organisatorischer Inkompetenz erleben dürfen. Ferner sollte man nicht davon ausgehen, dass das gesamte Personal stets die nötige Aufmerksamkeit an den Tag legt: Da kann auch mal die Serverraumtür über das Wochenende unverschlossen bleiben.

Ein Schlüsselverzeichnis, besser noch ein Code-gestütztes Zugangssystem mit Protokollierung, Tür- und Fenstersensoren, Video-Überwachung im Rechenzentrum und ein simpler Knauf, anstelle einer Klinke, sind Maßnahmen, um sicherzustellen, dass nur ausgewähltes Personal die jeweiligen Räume betreten kann.



Wenn Sie sich thematisch mit den Rahmenbedingungen eines geordneten IT-Betriebs auseinandersetzen möchten, werfen Sie einen Blick in das »IT-Grundschutz-Kompendium« des Bundesamts für Sicherheit in der Informationstechnik.

Windows aktuell halten

Die wichtigste Pflicht als Administrator besteht darin, den Systembetrieb aufrechtzuerhalten – Punkt. Die wichtigste Maßnahme des Windows-Administrators besteht darin, die betreuten Systeme auf dem aktuellen Stand zu halten. Da beinahe jedes Update von Microsoft Sicherheitsverbesserungen enthält, erhöhen Sie durch das zeitnahe Installieren automatisch die Betriebssicherheit, siehe [Abbildung 21.1](#).

Das Eigenschaftswort »zeitnah« ist wieder einmal individuell für die spezifische Anlage zu sehen. Wer als Administrator eine kleine Firma mit zwei Servern betreut, kann sich keine Analyse auf Testservern leisten. Hier gilt in der Installationsregel »direkt nach der Bereitstellung, nach einer ordentlichen Sicherung, in einem regelmäßigen Intervall«. In größeren IT-Umgebungen erstellen Administratoren Zeitpläne für »Downtimes« und bewerten neu erschienene Updates von Microsoft einzeln.

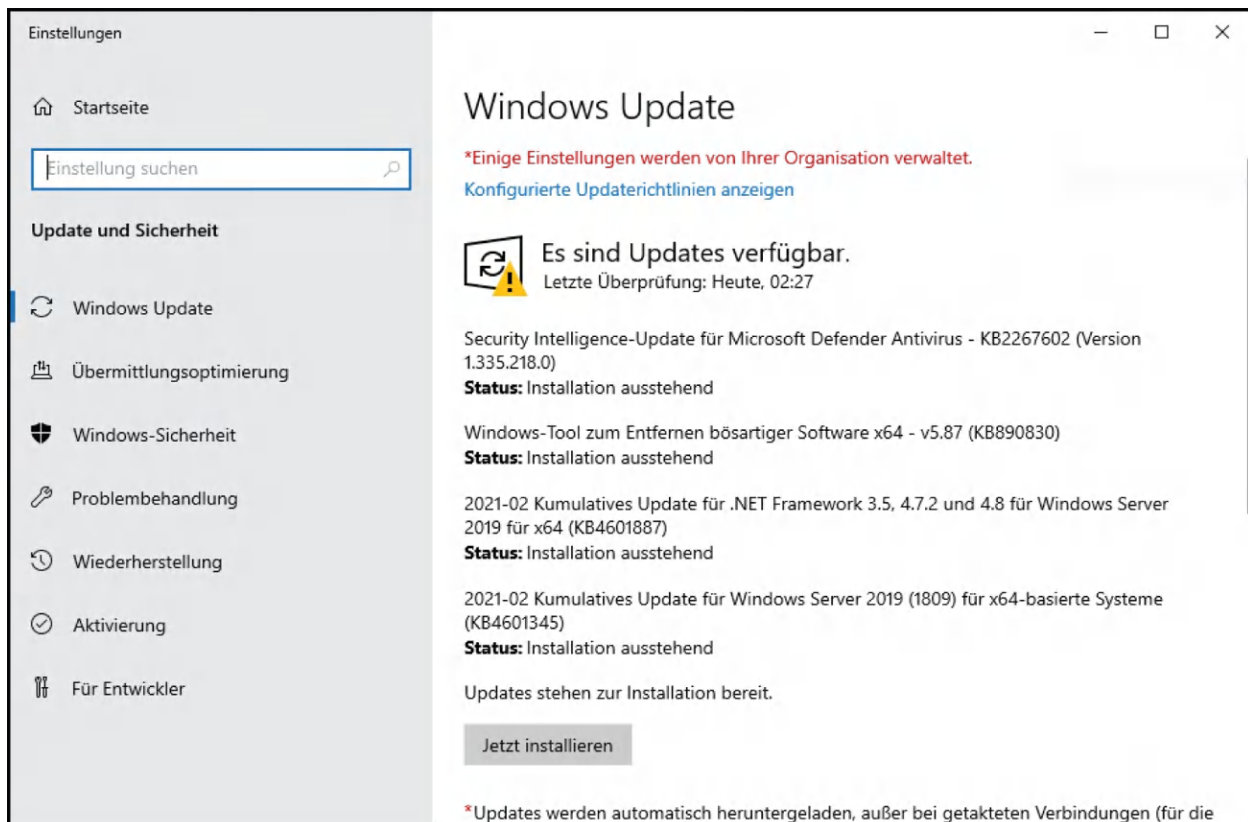


Abbildung 21.1: Die schnelle Installation von Updates ist die wichtigste Maßnahme eines Administrators gegenüber sicherheitsvorfallbedingten Server-Ausfällen.

Applikationen aktuell halten

Sofern Ihr Server nur Basisdienste von Microsoft bereitstellt, enthalten die Updates, die der Hersteller zur Verfügung stellt, auch die Aktualisierung für die bereitgestellte Applikation. Ein Microsoft-SQL- oder Exchange-Server erhält seine Aktualisierungen ebenfalls über den Update-Dienst, sofern in den Optionen das entsprechende Häkchen gesetzt ist, siehe [Abbildung 21.2](#).

Leider ist es für den Administrator an der Stelle mit dem »guten Service« bereits erledigt. Für Branchenlösungen oder Zusatzprogramme gilt es, regelmäßig selbst auf die Suche zu gehen. Selbst Updates für die Firmware von Festplatten, des Servers oder RAID-Controller gibt es häufiger.



Prüfen Sie regelmäßig, ob Updates für Branchenprogramme und die eingesetzte Server-Plattform bereitstehen. Dokumentieren und planen Sie die Installation sowie den jeweils aktuellen Stand. Updates verhindern schlichtweg Ausfälle!

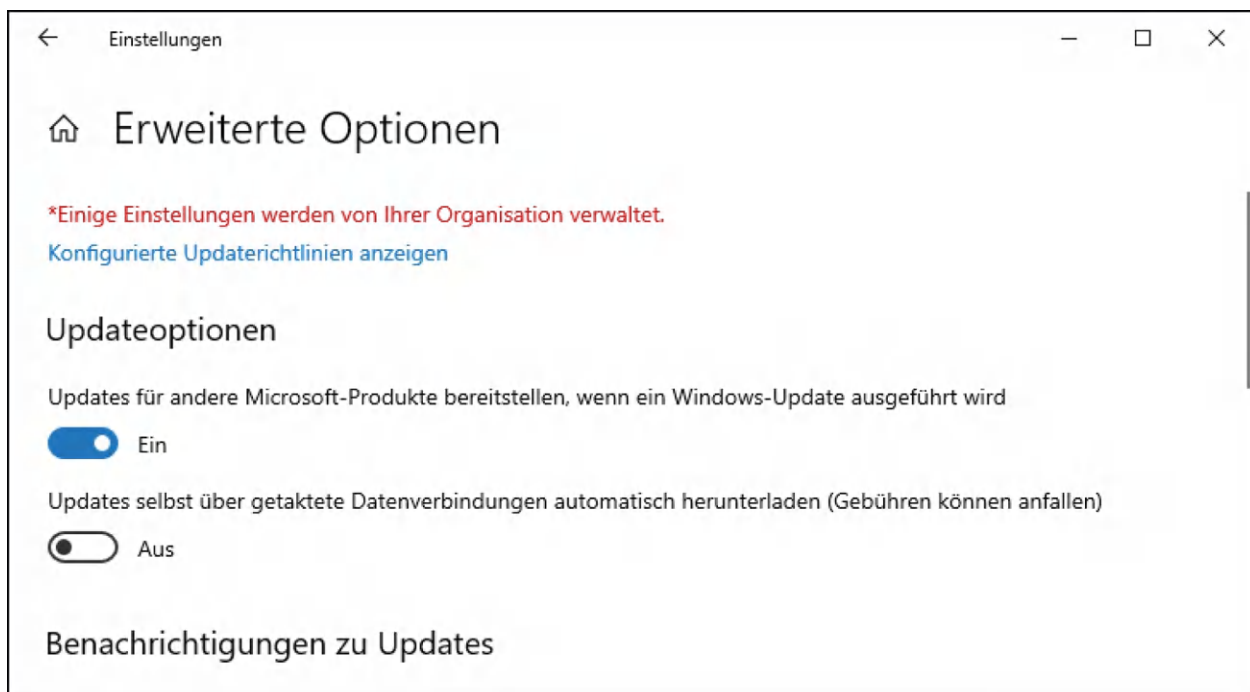


Abbildung 21.2: Wird die entsprechende Option aktiviert, erhält der Server auch Updates für Office, Exchange oder SQL.

RAM-Test

Unerklärliche und gänzlich ohne Systematik auftretende Schwierigkeiten eines Servers können auf Fehler im Arbeitsspeicher hindeuten. Das seit Windows Server 2012 R2 integrierte RAM-Diagnoseprogramm rufen Sie über mdsched in der Eingabeaufforderung auf.



Während des RAM-Tests wird der Windows-Server heruntergefahren. Der Vorgang kann mehrere Minuten, aber auch bis zu einer halben Stunde dauern!

Sie können den Server nach dem Aufrufen des Tools entweder sofort neu starten und eine Diagnose durchführen oder festlegen, dass die Diagnose erst beim nächsten Systemstart ablaufen soll. Während der Speicherdiagnose prüft das Werkzeug automatisch und ausführlich, ob der eingebaute Arbeitsspeicher Fehler aufweist, siehe [Abbildung 21.3](#).

Nachdem der Server neu gestartet ist, beginnt der Test und zeigt den aktuellen Status auf dem Bildschirm. Über die Funktionstaste **F1** gelangen Sie zu den Optionen der Überwachung und können verschiedene Überprüfungsmethoden auswählen und mit **F10** starten.

Ist der Test beendet, startet der Server automatisch wieder und meldet das Ergebnis des Tests im Infobereich der Taskleiste. Unabhängig davon, ob Sie das Ergebnisfenster beachten, das Windows bei Problemen anzeigt, protokolliert das Betriebssystem die Testergebnisse in der Ereignisanzeige. Sie finden die Einträge unter WINDOWS-PROTOKOLLE und SYSTEM als Ereignis-ID 1201 und 1101 unter der Quelle MEMORYDIAGNOSTICRESULTS.



Abbildung 21.3: Mit »mdsched« können Sie den Betriebszustand des Arbeitsspeichers prüfen.

Festplattenspeicherplatz beachten

In der Auflistung der bereits genannten Studie der Firma Hewlett Packard kommt der Grund »Server-Ausfall wegen voller Festplatte« als einzelne Nennung überhaupt nicht vor. Wahrscheinlich läuft ein solcher Fehler unter der Kategorie »Menschliches Versagen«.

Es ist aber so, dass Server noch immer ausfallen, weil niemand bemerkt hat, dass der Speicherplatz ausging. Unglücklicherweise sind Sie Mitglied der nicht-personifizierten Gruppe »Niemand«. Administratoren sind verantwortlich, wenn der Speicherplatz zur Ablage von Daten ausgeht. Dabei müssen zwei unterschiedliche Speicherbereiche bedacht werden:

- ✓ Systemrelevante Speicher
- ✓ Speicher zur Datenablage

Sofern Speicherbereiche für Benutzerdaten aufgrund mangelnden Platzes nicht mehr nutzbar sind, haben Benutzer noch die Möglichkeit, selbst einzuwirken, indem sie nicht mehr benötigte Daten löschen. Das ist zwar unangenehm – IT-Profis sprechen von »betriebsbehindernd« –, aber noch keine Katastrophe. Stellt ein Server seinen Betrieb ein, weil er keinen Platz mehr auf seiner Systemplatte hat, um beispielsweise Log-Daten zu erzeugen, wird ein »betriebsverhindernder« Zustand erreicht, bei dem Benutzer keine Möglichkeit haben, selbst einzugreifen.



Richten Sie unbedingt Quoten und Kontingente ein: für Benutzerdaten, um das Datenwachstum im Griff zu behalten, und für die Systemplatten, um rechtzeitig eine Warnung zu bekommen, ehe das System zum Stillstand kommt.

Am einfachsten überwachen Sie die Auslastung der Systemplatte eines Servers mit dem Ressourcen-Manager für Dateiserver. Diesen installieren Sie, sofern noch nicht vorhanden, über den Server-Manager. Über **BENUTZERDEFINIERT EIGENSCHAFTEN** im Dialog **KONTINGENT ERSTELLEN** können Sie sich eine **WEICHE KONTINGENTGRENZE** einrichten. Als Reaktion bieten sich E-Mails, Skript-Jobs oder Ereignisanzeigeneinträge an, siehe [Abbildung 21.4](#).

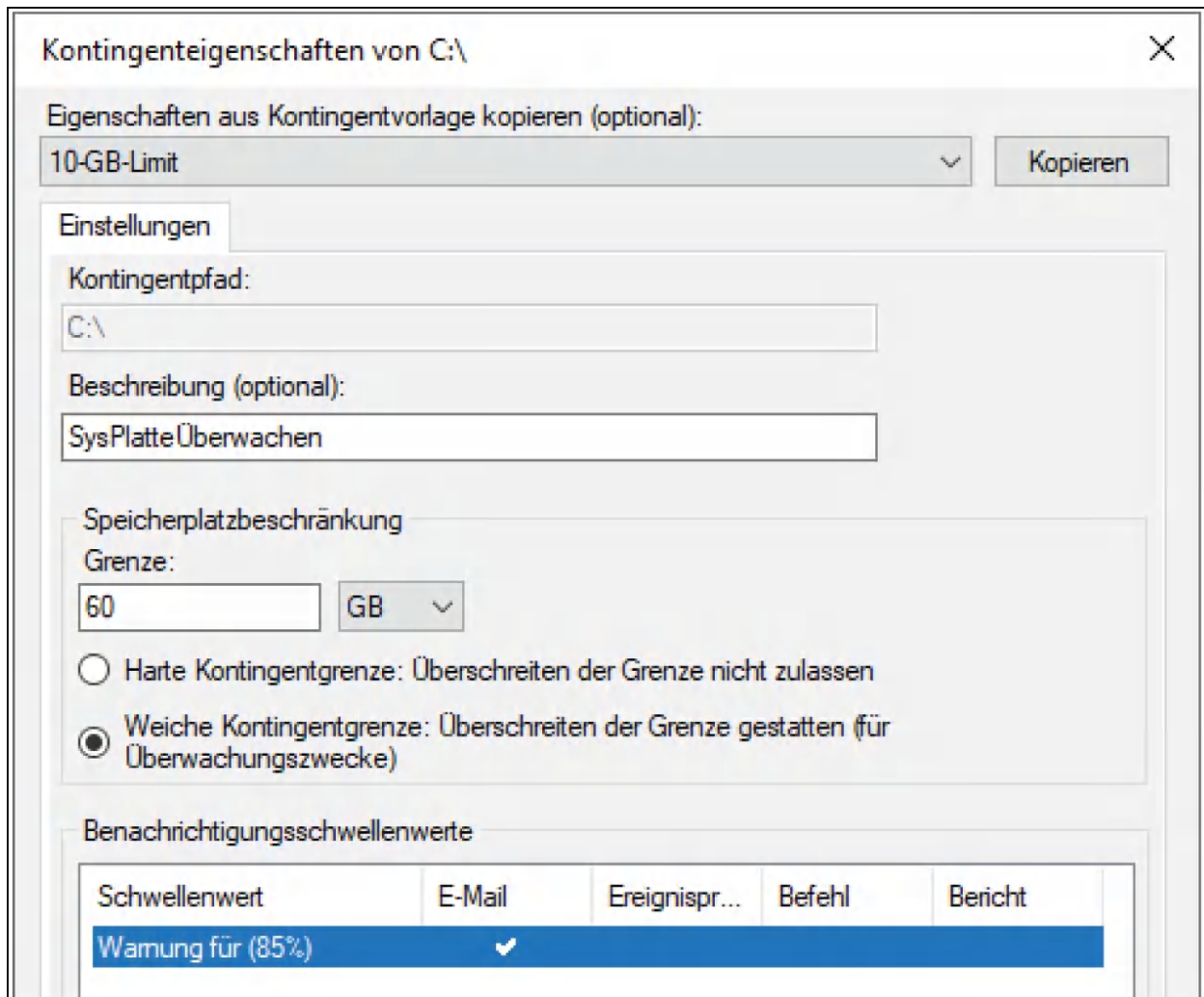


Abbildung 21.4: Die Windows-Bordmittel bieten eine laufende Überwachung, um Server-Ausfälle aufgrund mangelnden Speicherplatzes auf der Systemplatte zu verhindern.

Jedoch empfiehlt es sich in der Praxis, eine Monitoring-Umgebung aufzubauen, in der die verschiedenen zu überwachenden Parameter in einer Zeitachse gemeinschaftlich betrachtet werden können. Zudem bieten Überwachungsprogramme die Möglichkeit, einheitliche Vorgaben zu nutzen, statt individuellen Einstellungen pro Server vorzunehmen.

Monitoring

Microsoft bietet viele gute Software-Produkte an, und die zur Verfügung gestellten Schnittstellen erlauben eine hohe Integration. Im Bereich des Monitorings verlässt sich das Software-Unternehmen aus Redmond auf

seine Integrationsfähigkeit. Dank WMI stellt das Betriebssystem faktisch alle relevanten Informationen zur Überwachung zur Verfügung.

Klassisch überwachen Windows-Administratoren:

- ✓ Festplattenspeicher
- ✓ CPU-Last
- ✓ RAM-Ausnutzung
- ✓ Netzwerkdurchsatz
- ✓ Erreichbarkeit per IP-Adresse
- ✓ Erreichbarkeit per Hostnamen
- ✓ Verfügbarkeit von Diensten

Schon die wenigen Tests liefern, sofern regelmäßig ausgeführt, ein gutes Bild über die Verfügbarkeit des Servers und dessen Dienste. Insbesondere im Zusammenspiel mit anderen Überwachungswerten, beispielsweise der Netzwerkauslastung, der Stabilität der Namensauflösung und der Stabilität der Internet-Anbindung, helfen die Werte und Ergebnisse bei der Eingrenzung von Problemen. Es gibt viele ausgereifte Überwachungs- und Monitoring-Lösungen am Markt, einige Namen möchten wir hier dennoch hervorheben:

PRTG

Das in Deutschland beheimatete Unternehmen Paessler hat sich mit dem Produkt PRTG weltweit einen Namen gemacht und gehört zu den etabliertesten Monitoring-Lösungen am Markt. Praktischerweise benötigt PRTG unter Windows keine Agent-Installation, um an die zu überwachenden Daten zu gelangen.

PRTG wird typischerweise auf einem Windows-Server im Netzwerk installiert. Ein Vorgang, der in wenigen Minuten erledigt ist und kaum fachliche Expertise verlangt. Bereits in der »Freeware«-Edition ist ein Administrator in der Lage, 100 verschiedene Parameter über sogenannte Sensoren kostenfrei zu überwachen.

Besonders beeindruckt die Software durch ihre gut programmierten

Assistenten, die es Ihnen als Administrator ermöglichen, in wirklich kurzer Zeit eine Überwachung Ihrer Umgebung aufzubauen, ohne sich mit den Details auseinandersetzen zu müssen.

Nagios und Nagios XI

Nagios ist mit Sicherheit eines der bekanntesten Monitoring-Produkte für komplexe IT-Infrastrukturen. Das System besteht dabei aus einer ganzen Sammlung von Modulen zur Überwachung von Hosts, Netzwerken und Diensten, eingebettet in eine gemeinsame Weboberfläche zur Konfiguration und Datenvisualisierung.

Das Basissystem, der Nagios Core steht unter GNU GPL als freie Software für Unix-ähnliche Betriebssysteme kostenfrei zur Verfügung. Die Firma Nagios Enterprises LLC bietet seit mehr als 10 Jahren technische Unterstützung rund um das Thema Nagios als kommerzielle Dienstleistung an. Neben dieser Support-Leistung bietet die Firma, gegründet von Ethan Galstad, dem ursprünglichen Entwickler und Erfinder von Nagios, eine schlüsselfertige Version von Nagios – Nagios XI – in den Ausbaustufen Standard und Enterprise. Einen Teil der früheren Wegbegleiter hat die Firma bereits verloren, und aus Nagios gingen verschiedene weitere, eigenständige Zweige hervor: Icinga, Shinken und zuletzt Naemon.

Nagios XI ist eine kostenpflichtige Ergänzung zu Nagios Core und erlaubt dem Administrator einen schnelleren Einstieg in die Überwachung. Um Windows-Server ordentlich ins Monitoring zu bekommen, ist die Installation des sogenannten NCPA-Agent empfehlenswert. Im Zusammenspiel von XI und NCPA klickt der Administrator sich die gewünschten Überwachungsparameter zusammen, siehe [Abbildung 21.5](#).

☒ **Swap Usage**
 Monitor the percentage of allocated swap used.


 %


 %

Current Swap Usage

Disk Metrics
 Specify the disks the the warning and critical percentages for disk capacity.

Disk/Mount	Current Usage	Thresholds
☒ E:\	1 % 	 70 %  90 %
☒ D:\	1.5 % 	 15 %  90 %
☒ C:\	58.4 % 	 70 %  90 %

Network Interface Metrics
 Specify bandwidth limits for your network interfaces. Note that these measurements are per second, not a counter.

Interface Name	Thresholds
Show all interfaces	

Services
 Specify which services should be running or stopped. Depending on the selected state you will receive an OK when the process

Service Description	Service Name	Expected Status
☒ Microsoft iSCSI-Zielerserver	WinTarget	☒ Running ☐ Stopped

Abbildung 21.5: Nagios XI und NCPA helfen dem Windows-Administrator beim Monitoring.

Syspectr

Die in Berlin ansässigen Software- und Windows-Spezialisten von O&O Software bieten seit einigen Jahren eine weitere, äußerst spannende Monitoring-Lösung mit dem Namen Syspectr an. Das Programm ist eine kostenfreie Cloud-Lösung, die es einem Systembetreuer ermöglicht, viele Systemparameter und wichtige Funktionen der Windows-Systeme – wie Updates und deren Status – über das Web zu kontrollieren und dann im Zweifelsfall auch einzugreifen.

Dazu benötigt der Systemverwalter an seinem jeweiligen Arbeitsplatz lediglich einen Browser, der HTML5 unterstützt, um mit diesem dann im Prinzip von überall her solche Aufgaben ausführen zu können. Auf den zu überwachenden Windows-Systemen, Client- oder Server-Version, muss

nur jeweils ein kleines Agent-Programm installiert sein. Als Systemvoraussetzung gilt es lediglich, ein halbwegs aktuelles .net-Framework und eine Internetanbindung vorzuhalten. Zwischen dem Rechenzentrum von O&O und den verschiedenen Windows-Systemen besteht eine verschlüsselte Verbindung.

Je nach Einstellung wird der Administrator bei Problemen, beispielsweise bei zu hoher Temperatur der Festplatten, automatisch per E-Mail informiert. Eine Fernwartungsmöglichkeit, Update-Überwachung und Hard- und Software-Inventarisierung runden das Produkt ab, siehe [Abbildung 21.6](#).

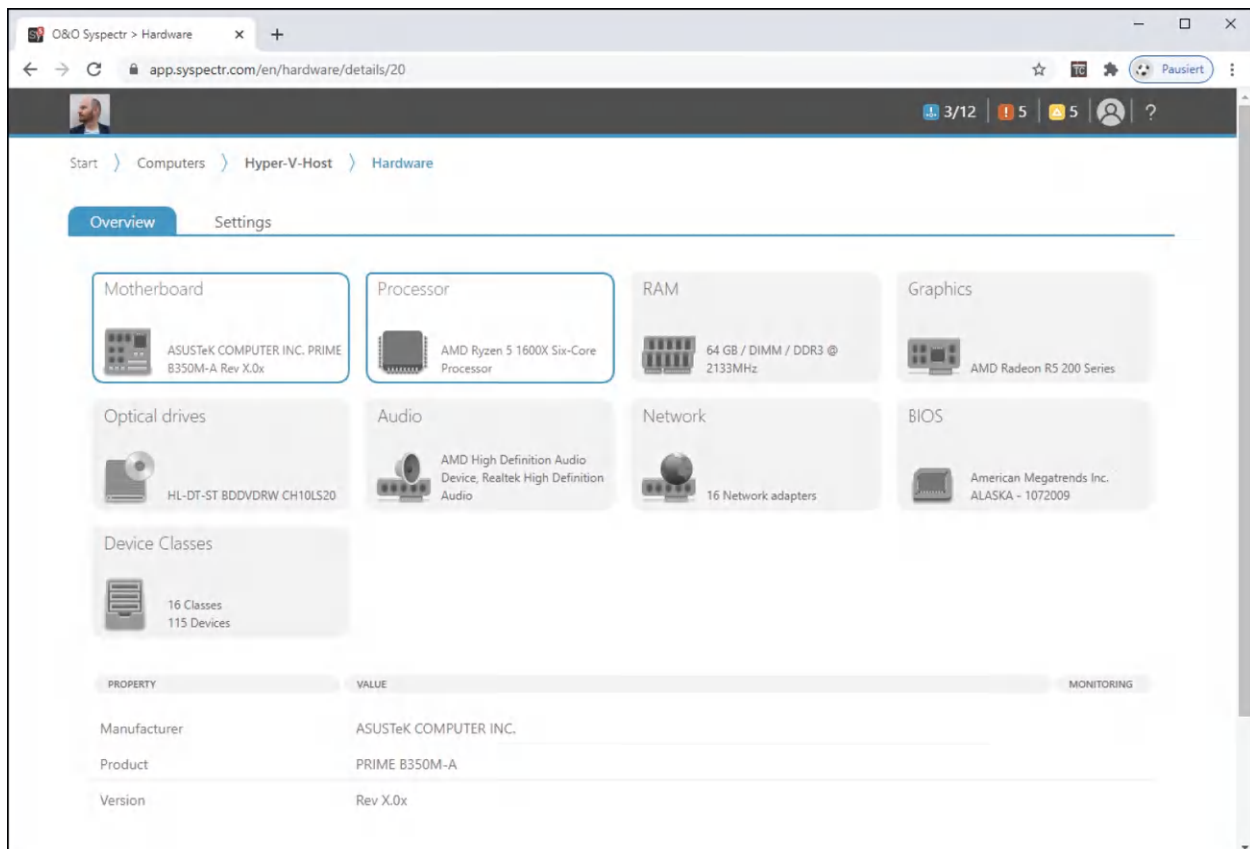


Abbildung 21.6: O&O Syspectr eignet sich besonders für verteilte Umgebungen.

Kapitel 22

Fernzugriffe

IN DIESEM KAPITEL

Art und Zielsetzung eines Fernzugriffs

Konsolenzugriffe

MMC

Remote Desktop

Dritthersteller-Tools

Fernzugriff ist nicht gleich Fernzugriff, auch wenn die Mehrheit der Benutzer und Administratoren typischerweise damit die Darstellung des kompletten Windows-Desktops verbindet. Insbesondere im Support-Umfeld ist die Betrachtung des kompletten Desktops für eine zielgerichtete Unterstützung wichtig – viele administrative Tätigkeiten verlangen jedoch nicht zwangsläufig die volle grafische Darstellung.

Allein die Existenz der Core-Server, sprich Windows-Server ohne grafische Oberfläche, verdeutlicht, dass der komplette Desktop nicht unbedingt erforderlich ist, um mit einem Server erfolgreich zu arbeiten. Da den meisten Servern ohnehin nur noch ein virtuelles Dasein zugestanden wird und eine physische Grafikkarte nur selten verbaut ist, muss es wohl ausreichend funktionelle Fernzugriffstechniken geben.

Viele administrative Verwaltungsaufgaben werden Sie als Administrator über das Admin Center, den Server-Manager oder über die MMC-Konsolen durchführen. Hierfür ist es kaum erforderlich, sich direkt mit dem entfernten System zu verbinden. Virtuelle Server in der Installationsphase erreichen Administratoren mit den Bordmitteln von Hyper-V und VMware ESX und bereits nach wenigen Minuten über erweiterte Remote-Zugriffe, in der Regel RDP (Remote Desktop

Protocol).

Insgesamt ist der RDP-Zugang für Windows-Computer das, was in der Unix-/Linux-Umgebung der SSH-Zugang ist. Auch Windows-Server, die in der Azure-Cloud residieren, erreichen die Administratoren über RDP-Zugriffe. Hierzu sei jedoch schon jetzt gesagt, dass Sie als Systemverantwortlicher sicherstellen müssen, dass nicht von jedem beliebigen Ort ein RDP-Zugriff auf die Server-Konsolen aus möglich sein sollte.



Ein Windows-Server mit dem lokalen Zugang Administrator und dem Passwort abc123 mit einem über das Internet erreichbaren RDP-Zugang war in einem Test der Autoren binnen weniger als einem Tag komplett durch Schad-Software »verseucht«.

Stellen Sie sicher, dass RDP-Zugriffe nur aus »halbwegs« vertrauensvollen Netzwerken aus möglich sind.

Konsolenzugriffe

Aber – auch wenn es die besonders in der Unix-/Linux-Welt anzutreffenden Konsolenadministratoren nicht gern hören – es ist meist schlichtweg viel angenehmer, die komplette Arbeitsumgebung, den Desktop, vor sich zu wissen, als sich mit minimalistischen Hilfsmitteln durchzuschlagen.

Wenn es wahrlich nur um den »Konsolenzauber« geht, gibt es zwei probate Hilfsmittel:

- ✓ PsExecute von Mark Russinovich
- ✓ PowerShell

Der Name Mark Russinovich ist in der Windows-Welt »well-known«. Der IT-Sicherheitsexperte ist unter anderem auch Autor, Programmierer und Journalist. Die PsTools sind eine Sammlung von Fernverwaltungs- und Managementprogrammen, die Microsoft direkt über die Docs-Webseite

zum Download zur Verfügung stellt:

<https://docs.microsoft.com/en-us/sysinternals/downloads/psexec>

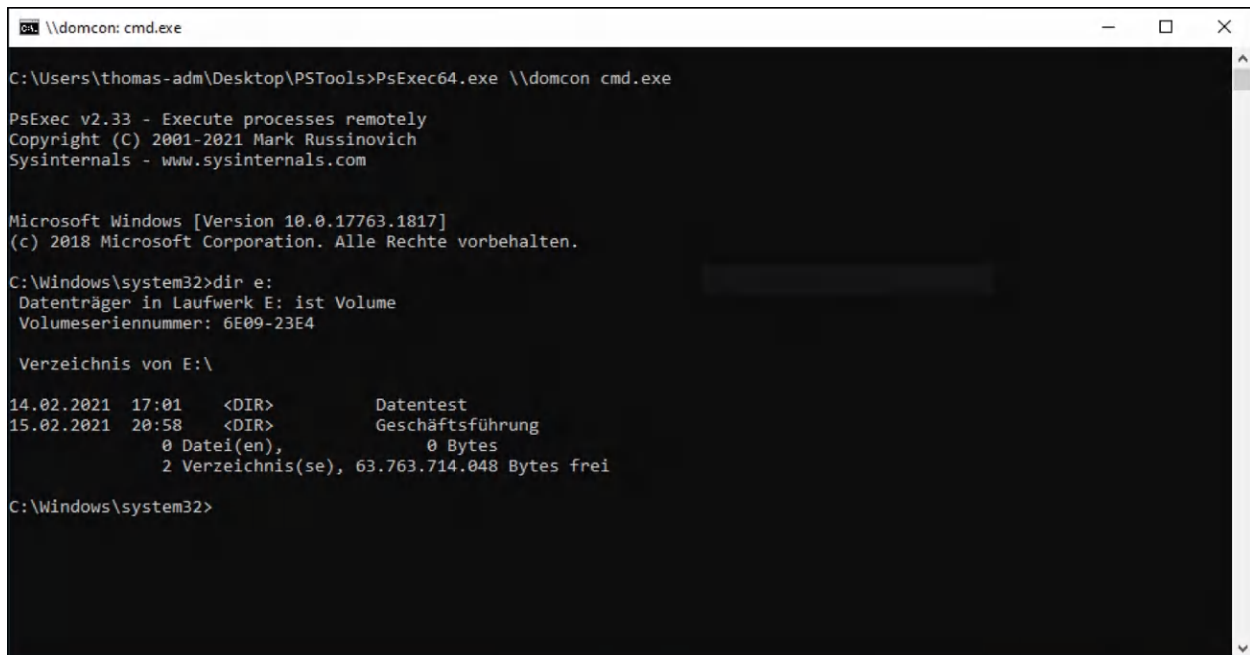
PSEXEC, wie das Programm abgekürzt genannt wird, hat schon gut zwei Dekaden auf dem »digitalen Buckel«, wird aber nach wie vor regelmäßig aktualisiert. Die zur Erstellung dieses Manuskripts gängige Version 2.33 ist gerade einmal zwei Monate alt und funktioniert auch mit dem neuesten Windows-Server hervorragend zusammen.

PSEXEC ist ein Ersatz für Telnet und bietet die Fähigkeit, eine vollwertige Konsole (Eingabeaufforderung) für ein entferntes System aufzubauen, ohne dass dafür auf dem zu steuernden Windows-Server oder -PC eine Client-Komponente zu installieren wäre.



Einige Antiviren-Programme reagieren auf das Vorfinden von PSEXEC mit einer Warnmeldung, dass ein »remote admin«-Virus vorliegen würde. Es handelt sich bei dieser Warnung um einen Fehler – PSEXEC ist kein Virus, jedoch ein äußerst mächtiges Werkzeug, das auch von einigen Schadprogrammen genutzt wird.

Nach dem Herunterladen des Programmpakets gilt es, den kompletten Inhalt des ZIP-Archivs in einen gewünschten Ordner abzuspeichern. Dort aufgerufen steht der Befehl psexec in der Eingabeaufforderung des lokalen Computers zur Verfügung, siehe [Abbildung 22.1](#).



```
C:\Users\thomas-adm\Desktop\PSTools>PsExec64.exe \\domcon cmd.exe

PsExec v2.33 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 10.0.17763.1817]
(c) 2018 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>dir e:
Datenträger in Laufwerk E: ist Volume
Volumeserienummer: 6E09-23E4

Verzeichnis von E:\

14.02.2021  17:01    <DIR>          Datentest
15.02.2021  20:58    <DIR>          Geschäftsführung
               0 Datei(en),               0 Bytes
               2 Verzeichnis(se), 63.763.714.048 Bytes frei

C:\Windows\system32>
```

Abbildung 22.1: Zugriff auf die Konsole über PS-Execute

Ein exemplarischer Aufruf der Software lautet beispielsweise:

```
psexec -i \\computername c:\bin\test.exe
```

oder

```
psexec -i \\ computername cmd
```

oder

```
psexec -i -d -s c:\windows\regedit.exe
```

Sinnvollerweise wird Psexec innerhalb einer Windows-Domäne genutzt, da nur hier die entsprechenden Firewall-Regeln gesetzt sein dürften, die einen fehlerfreien Betrieb ermöglichen. Mit der PowerShell existiert heute eine modernere Variante für die Fernausführung und den Fernzugriff in Windows-Umgebungen.



Wer sich dafür interessiert, wie PsExecute genau funktioniert, der sei auf einen Artikel von Mark Russinovich hingewiesen:
<https://www.itprotoday.com/windows-server/psexec-explainer-mark-russinovich>.

Dank der PowerShell ist es für Administratoren heute sehr einfach, sich

auf die Konsole eines anderen Servers zu verbinden, um Verwaltungsaufgaben wahrzunehmen. Aktuelle Server-Betriebssysteme verfügen über die entsprechenden Systemvoraussetzungen – hier geht es insbesondere um Microsoft .NET-Framework, die Windows-PowerShell selbst und die Windows-Remoteverwaltung.

- ✓ Windows-Remoteverwaltung (WinRM) 3.0 und Microsoft .NET Framework 4 sind in Windows 8, Windows Server 2012 und neueren Versionen des Windows-Betriebssystems enthalten.
- ✓ WinRM 3.0 ist in Windows Management Framework 3.0 für ältere Betriebssysteme enthalten.
- ✓ Wenn der Computer nicht über die erforderliche Version von WinRM oder das Microsoft .NET Framework verfügt, schlägt die Installation fehl.

Um Remotesitzungen zu erstellen und Remotebefehle auszuführen, muss der aktuelle Benutzer Mitglied der Gruppe Administratoren auf dem Remotecomputer sein oder die Anmeldeinformationen eines Administrators angeben. Andernfalls führt der Befehl möglicherweise zu einem Fehler.

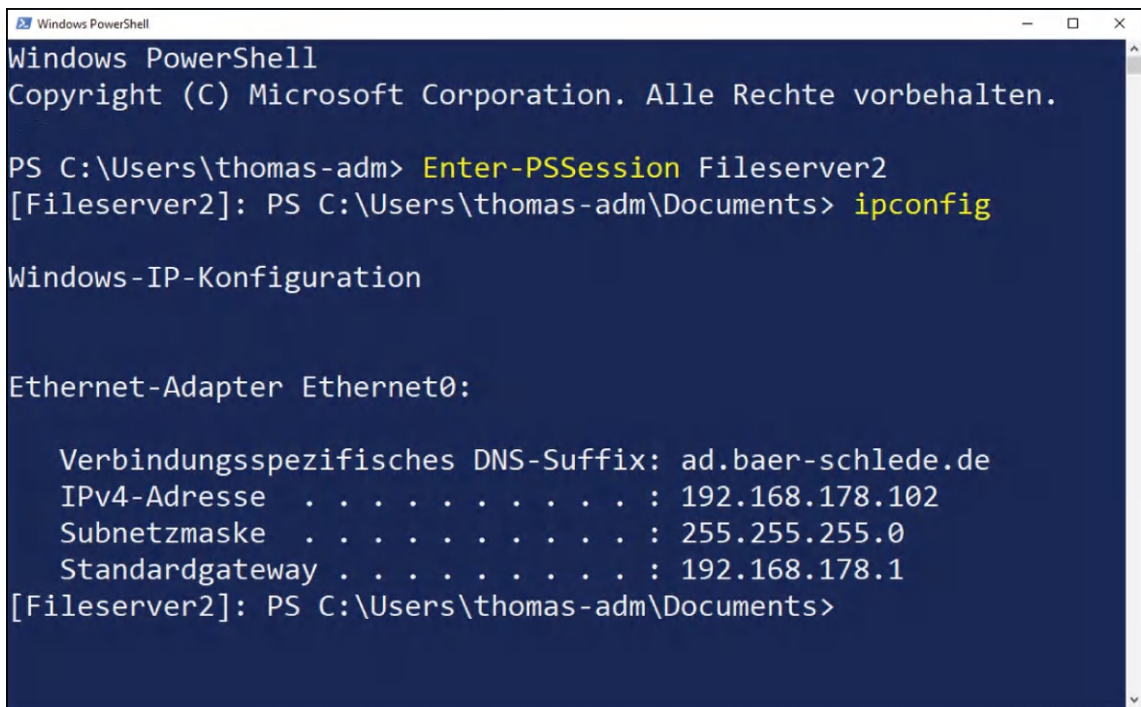
Die Berechtigungen, die zum Erstellen von Sitzungen und Ausführen von Befehlen auf einem Remotecomputer oder in einer Remotesitzung auf dem lokalen Computer erforderlich sind, werden durch die Sitzungskonfiguration – auch als »Endpunkt« bezeichnet – auf dem Remotecomputer eingerichtet, mit dem die Sitzung eine Verbindung herstellt. Insbesondere bestimmt die Sicherheitsbeschreibung für die Sitzungskonfiguration, wer Zugriff auf die Sitzungskonfiguration hat und wer sie zum Herstellen einer Verbindung verwenden kann.



Das klingt nun möglicherweise alles viel komplizierter, als es letztendlich ist: In einer Windows-Domäne mit Standardeinstellungen werden Sie problemlos in der Lage sein, aus einer PowerShell-Sitzung heraus interaktiv auf die Konsole eines anderen Servers zuzugreifen.

Starten wir ein praktisches Beispiel: Melden Sie sich auf einem Server als administrativer Benutzer an.

1. Starten Sie die POWERSHELL, indem Sie die -Taste drücken, PowerShell als Begriff eingeben und die Windows-PowerShell starten.
2. Geben Sie in dem PowerShell-Fenster das Kommando `Enter-PSsession computername` ein (siehe [Abbildung 22.2](#)) und bestätigen Sie Eingabe mit der -Taste.



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

PS C:\Users\thomas-adm> Enter-PSsession Fileserver2
[Fileserver2]: PS C:\Users\thomas-adm\Documents> ipconfig

Windows-IP-Konfiguration

Ethernet-Adapter Ethernet0:

    Verbindungsspezifisches DNS-Suffix: ad.baer-schlede.de
    IPv4-Adresse . . . . . : 192.168.178.102
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.178.1
[Fileserver2]: PS C:\Users\thomas-adm\Documents>
```

Abbildung 22.2: Zugriff über Windows-PowerShell-Remoting

3. Versichern Sie sich, beispielsweise durch die Eingabe des Befehls `ipconfig`, dass Sie sich nicht mehr auf dem lokalen Server befinden, sondern über Windows-PowerShell-Remoting mit der Konsole eines anderen Servers verbunden sind.

Die Eingabeaufforderung ändert sich, und es wird der Name des Remotecomputers angezeigt. Alle Befehle, die Sie an der Eingabeaufforderung eingeben, werden auf dem Remotecomputer ausgeführt, und die Ergebnisse werden auf dem lokalen Computer

angezeigt.

Beenden Sie die interaktive Sitzung mit dem Kommando:

`Exit-PSSession`

Microsoft Management Console (MMC)

Administratoren benötigen für viele Verwaltungsaufgaben eigentlich gar keinen Zugriff auf den tatsächlichen Desktop des Systems. Für die Einrichtung einer Druckerwarteschlange, die Anpassung von DNS- oder DHCP-Einträgen oder um die Ereignisanzeige eines anderen Servers zu öffnen, ist es nicht notwendig, sich direkt auf den Desktop des Servers zu verbinden. Die Dialogfenster, typischerweise MMC-Fenster – Microsoft Management Console 3.0 – lassen sich auf andere Computer »umlenken«, ähnlich der Steuerung durch den Server-Manager.

In diesem Beispiel greifen wir auf die Dienste-Steuerung auf einem entfernten Server zu. Melden Sie sich dazu auf einem Server als administrativer Benutzer an.

1. Starten Sie die MMC der Dienste-Verwaltung, indem Sie die -Taste drücken, Dienste als Begriff eingeben und in den Suchergebnissen unter APPS den Punkt DIENSTE auswählen.

Binnen weniger Sekunden wird Ihnen der Zustand der aktuellen Dienste-Verwaltung auf dem lokalen Server angezeigt.

2. Wählen Sie im Menü AKTIONEN den Befehl VERBINDUNG MIT ANDEREN COMPUTERN HERSTELLEN... (sollten Sie den Befehl nicht sehen, stellen Sie sicher, dass Sie keinen Dienst ausgewählt haben, indem Sie auf eine freie Stelle im Dialogfenster klicken). Es öffnet sich das Dialogfenster COMPUTER AUSWÄHLEN – siehe [Abbildung 22.3](#).

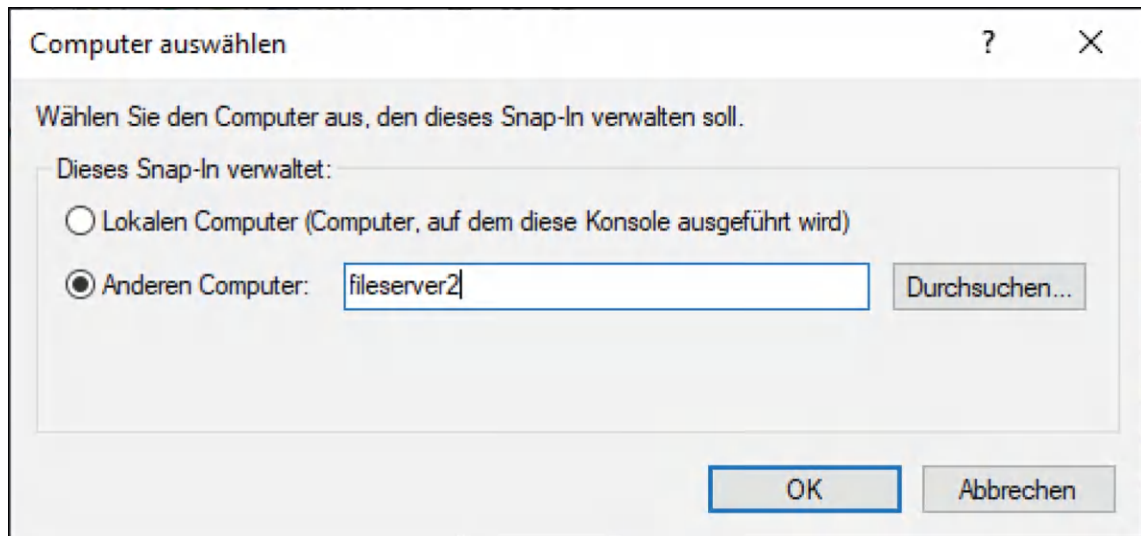


Abbildung 22.3: Verbindung mit einem anderen Computer in der MMC herstellen

3. Wählen Sie den gewünschten Computer aus oder geben Sie den Namen ein und klicken Sie auf OK.
4. Anschließend können Sie die Dienste auf dem entfernten Server einsehen und steuern.

Remote Desktop (RDP)

Das Remote Desktop Protocol (RDP) ist ein von Microsoft entwickeltes Protokoll für den Fernzugriff auf einen Rechner mit Windows-Betriebssystem. Mithilfe des Protokolls lassen sich Bildschirmdarstellungen und Steuerungsbefehle verschlüsselt über IP-Netze hinweg – auch über das Internet – übertragen. RDP ist ein äußerst wichtiges Protokoll für den administrativen Zugriff. Was für Linux-/Unix-Administratoren SSH ist, ist für den Windows-Administrator RDP.

In größeren Betriebsumgebungen wird das RDP-Protokoll nicht nur für den Administratorzugriff genutzt, sondern die komplette Windows-Benutzerumgebung über dieses Protokoll als Remote-Desktop-beziehungsweise Terminalserver-Farm zur Verfügung gestellt.



RDP arbeitet typischerweise auf TCP-Port 3389, es kann jedoch bei Bedarf das verbindungslose UDP, ebenfalls auf Port 3389, zum

Einsatz kommen.

Entstanden ist das Remote Desktop Protocol aus einer Erweiterung eines Protokolls der T.120-Protokollfamilie der internationalen Fernmeldeunion (ITU). Das Remote Desktop Protocol arbeitet als Terminalserver-Protokoll im Client-Server-Modus. Die per RDP übertragenen Daten sind grundsätzlich verschlüsselt. De facto gibt es für jedes im Einsatz befindliche Betriebssystem einen RDP-Client – für Apple macOS wird der Client direkt von Microsoft zur Verfügung gestellt.

Damit Sie als Administrator die Benutzeroberfläche eines Windows-Servers erreichen können, benötigen Sie

- ✓ eine durchgängige Verbindung TCP/3389, die nicht von einer Firewall blockiert wird,
- ✓ einen RDP-Client »Remotedesktop-Verbindung«, wie er in allen gängigen Windows-Versionen enthalten ist, zu starten durch Drücken der -Taste und Eingabe von `mstsc` (Microsoft Terminal Server Client), und
- ✓ einen aktivierten REMOTEDESKTOP auf dem Server.

So stellen Sie sicher, dass die RDP-Verbindung aktiviert ist:

1. Drücken Sie die -Taste in einer lokalen Anmeldung auf dem Server, für den Sie die Remotedesktop-Verbindung freigeben wollen.
2. Geben Sie »Remoteeinstellungen« als Suchbegriff ein.
3. Wählen Sie den entsprechenden Dialog aus den SYSTEMEINSTELLUNGEN aus – siehe [Abbildung 22.4](#).

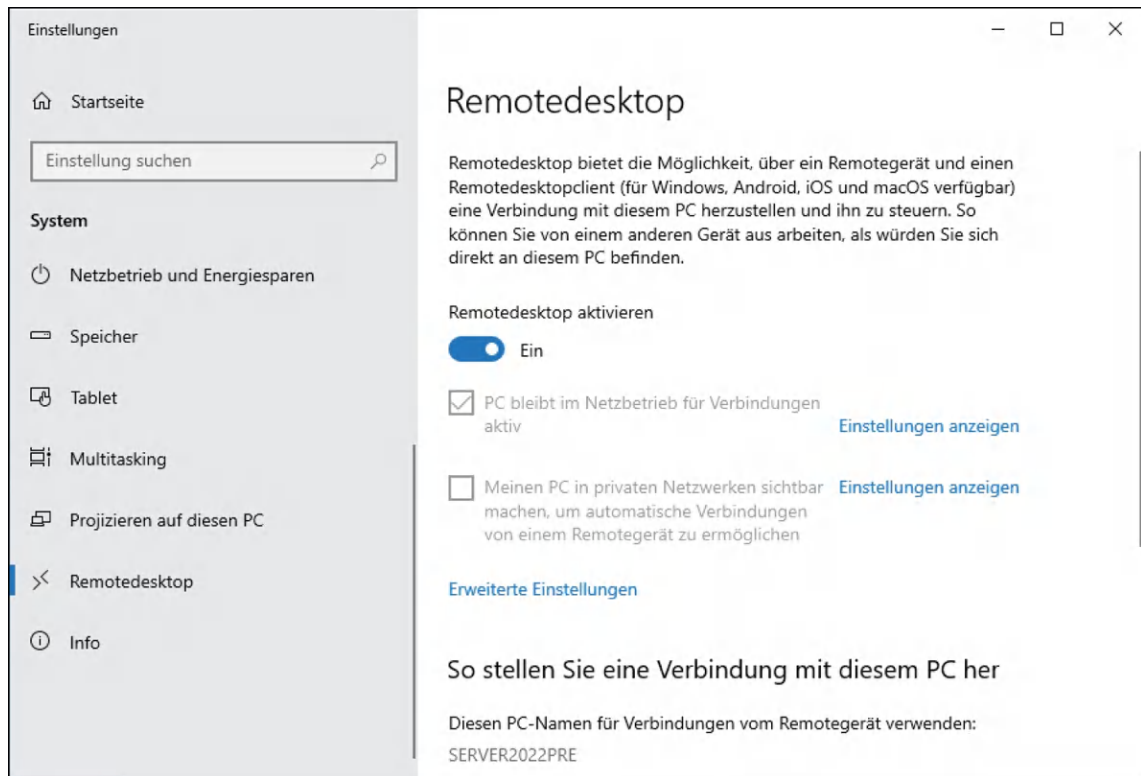


Abbildung 22.4: Aktivierte Remotedesktop-Verbindung auf einem Windows Server 2022.

4. Prüfen Sie, ob die Aktivierung eingeschaltet ist.

Sofern der Remotedesktop-Zugriff erstmalig aktiviert wurde, ist es sinnvoll, zu prüfen, welche Benutzer für den Zugriff freigeschaltet sind. Hierzu gibt es etwas weiter unten in dem Dialogfenster einen entsprechenden Befehl. Letztendlich handelt es sich jedoch um die Mitglieder der Benutzergruppe REMOTEDESKTOPBENUTZER.

Dritthersteller-Tools

Es existiert eine große Anzahl verschiedenerer Lösungen für den Fernzugriff auf Computer am Markt. Diese lassen sich ganz grob in zwei Gruppen einteilen:

- ✓ Programme, die eine Internetanbindung benötigen
- ✓ Lokale Fernwartungsprogramme

In die letzte Gruppe fallen vor allem ältere Programme. Das bekannteste unter ihnen dürfte VNC (Virtual Network Computing) sein. VNC geht auf eine Entwicklung von Olivetti aus den 1980er-Jahren zurück und ist faktisch für alle Betriebssysteme verfügbar. Die Software basiert auf einem Konzept mit Namen Remote Framebuffer in einer Client-Server-Architektur, bei dem prinzipbedingt auch die Tastatur- und Mauseingaben des Viewers in der Regel unverschlüsselt über das Netzwerk übermittelt werden. Zur Absicherung der Verbindung besteht die Möglichkeit, eine SSL-Verschlüsselung zu aktivieren, siehe [Abbildung 22.5](#).

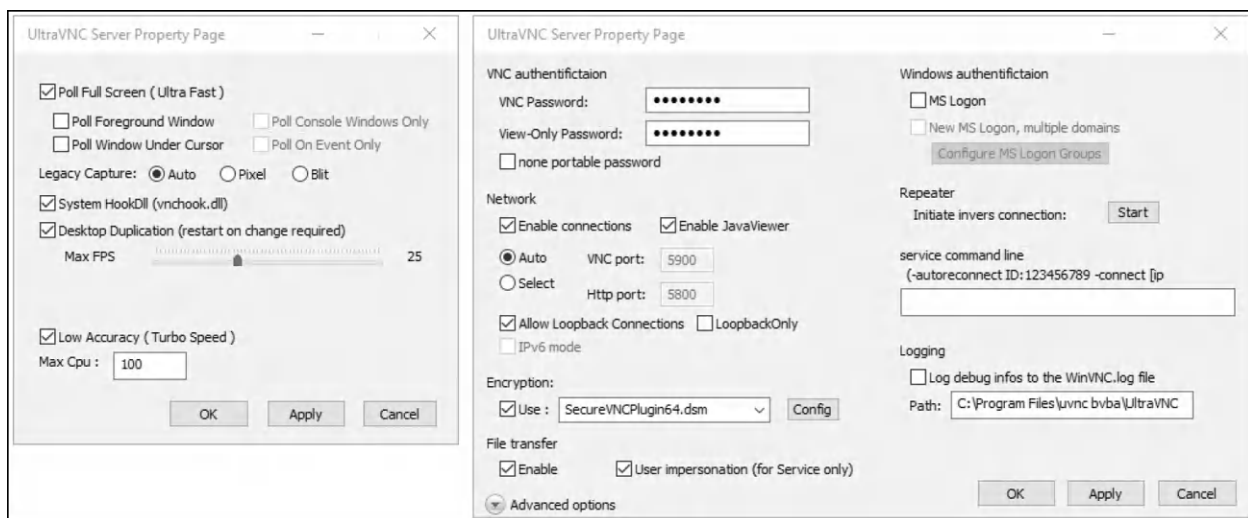


Abbildung 22.5: Das kostenlose Ultra-VNC bietet ebenfalls die Funktion zur Verschlüsselung (Encryption).

Die Internet-basierten Fernwartungs- beziehungsweise Remote-Administrations-Tool-(RAT-)Programme bieten gegenüber den lokalen Programmen einen entscheidenden Vorteil: Die zu installierenden Client-Komponenten sind im laufenden Datenaustausch mit einer zentralen Instanz im Internet. Somit können sich Computersysteme miteinander verbinden, die sich normalerweise nicht über eine direkte Netzwerkverbindung erreichen ließen – sprich über das Internet.

Im deutschsprachigen Bereich ist der Anbieter Teamviewer bekannt und populär (siehe [Abbildung 22.6](#)). Die Verwendung ist für Privatpersonen kostenfrei und erlaubt eine Betriebsvariante, bei der die Software nur bei Bedarf gestartet wird. Somit sind spontane Support-Sitzungen möglich, falls beispielsweise der Bruder den neuen Drucker nicht zum Laufen

bringt.

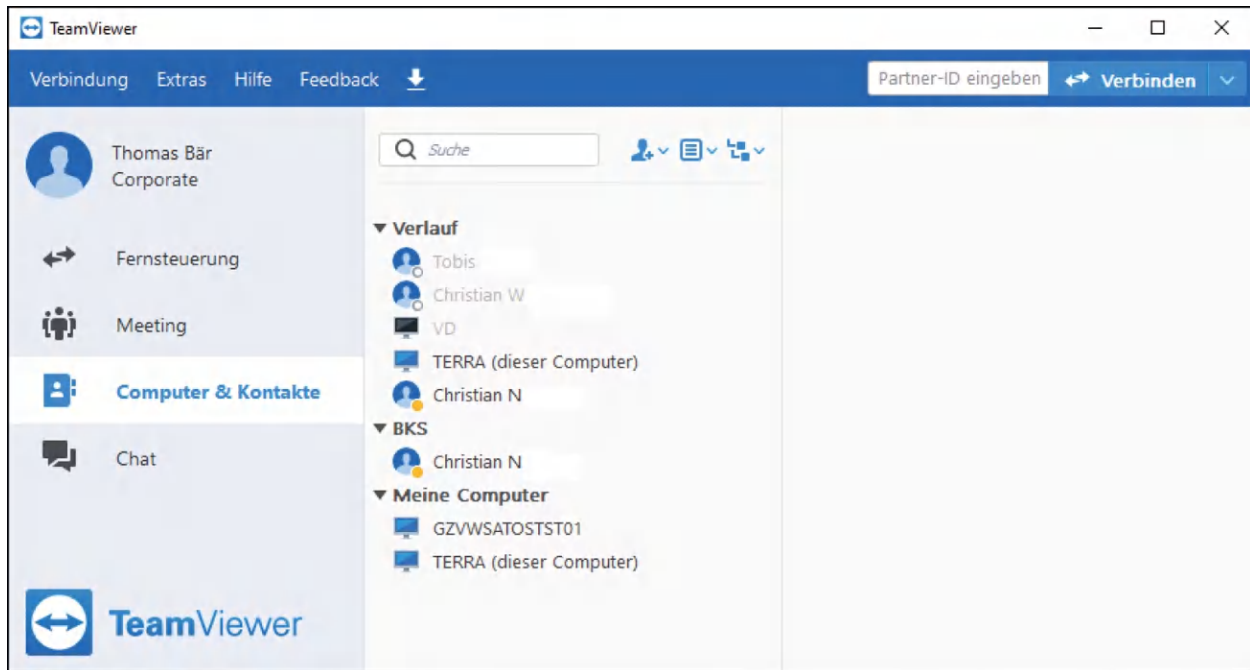


Abbildung 22.6: Bekannte Fernzugriffslösung aus Deutschland: Teamviewer

Fest installiert kann sich ein IT-Profi auch auf Computer aufschalten, ohne dass beispielsweise am Telefon eine Benutzerkennung und ein Passwort verraten werden müssten.

Eine regelmäßige Nutzung der Software könnte auf eine gewerbsmäßige Nutzung hindeuten. Der geschäftsmäßige Einsatz der Software ist kostenpflichtig.



Richten Sie Internet-basierte Fernwartungsprogramme nur ein, wenn Sie dem Anbieter zu 100 Prozent Vertrauen schenken können. Immerhin installieren Sie einen Client, der einen Fernzugriff ermöglicht.

Im Vergleich zu Teamviewer geht das Angebot »Syspectr« des ebenfalls in Deutschland ansässigen Herstellers O&O Software noch einen deutlichen Schritt weiter – jedoch beschränkt auf Windows-Computer. Der Administrator meldet sich beim kostenlosen Service des Herstellers an und lädt eine für den Mandanten spezifische Client-Version herunter und installiert diese auf den gewünschten Computern.

Für das Ausrollen von O&O Syspectr über das Active Directory von Windows stellt der Hersteller eine spezielle MSI-Datei zur Verfügung, sodass der gesamte Installationsvorgang zentral verwaltet und durchgeführt werden kann.

Anschließend sind Sie als IT-Profi in der Lage, im Dashboard von O&O Syspectr über den Browser die Endgeräte zu verwalten, inklusive einer Remotedesktop-Verbindung, ebenfalls im Browser und einer Remote Console. Zu jedem verwalteten Computer gibt es die Möglichkeit, Prozesse und Dienste zu beobachten, die Speicherplatznutzung zu überwachen, Windows-Updates zu installieren oder PowerShell-Skripte zur Ausführung zu bringen, siehe [Abbildung 22.7](#).

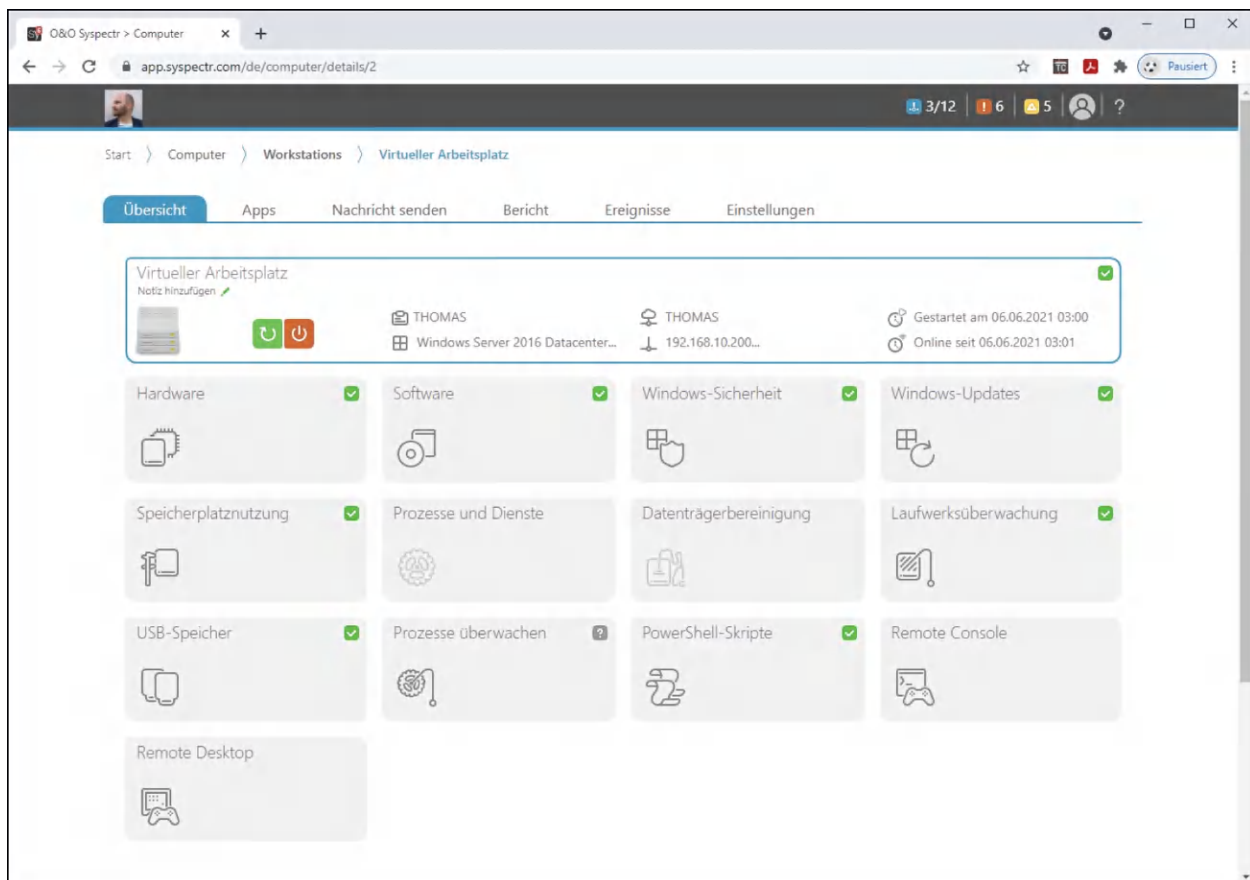


Abbildung 22.7: Kostenfreie Fernwartungs-Software von O&O Software – Syspectr

Insbesondere, wenn Sie als Administrator verschiedene Umgebungen bei verschiedenen Kunden betreuen, ist Syspectr eine interessante Überwachungs- und Fernwartungslösung.

Kapitel 23

Troubleshooting

IN DIESEM KAPITEL

Gibt es schon ein Update?
Könnte dieser Tipp passen?
Erst die Ereignisanzeige – dann der Rest!
Eigene Dokumentationen
Server-Manager als Hilfestellung
IPv6 unterdrücken
Wo finde ich die richtige Unterstützung?

Unglücklicherweise befasst sich ein Administrator auch beim neuesten Windows-Server eine äußerst lange Zeit mit der Fehlersuche. Nicht umsonst gibt es Aussagen wie »Try and error« oder »never change a running system« – diese salopp ausgedrückten Binsenweisheiten haben in der IT ihre Daseinsberechtigung. Natürlich ist der Mensch ein »Gewohnheitstier« und zieht aus der Wiederholung erlernter Aufgaben seine Routine und damit so etwas wie »Betriebssicherheit«, aber ohne stete Anpassung wird die von Ihnen betreute Server-Anlage zunehmend in Schieflage geraten.

Möglicherweise werden Sie sich wundern, warum wir ausgerechnet mit einem solchen Absatz das Kapitel »Troubleshooting« begonnen haben. Wir dürfen Ihnen versichern, wir haben uns etwas dabei gedacht. Ein wichtiger Grundsatz beim Troubleshooting ist:



Updates installieren – Stoßen Sie auf Anomalien auf einem System und haben Sie die Möglichkeit, noch Aktualisierungen an

Betriebssystem oder der Applikation vorzunehmen, dann sollte dies Ihr erster Schritt sein. Release Notes und Hotfix-Beschreibungen geben oft Hinweise darauf, ob das von Ihnen festgestellte Problem über diesen Weg lösbar sein wird.

Immer wieder ist in Onlineforen zu lesen, dass ein Problem wieder verschwand, sobald ein Update von Microsoft gezielt vom Administrator deinstalliert wurde. Und ja – es stimmt –, auch Microsoft hat seinen Benutzern mehr als einmal bewiesen, dass dem Unternehmen beim Ausbringen von Updates ein Fehler unterlaufen ist. Manchmal mit mehr oder weniger schwerwiegenden Folgen.

Die Deinstallation eines Updates, um ein Problem aus der Welt zu schaffen, sollte stets die allerletzte Reaktion für Sie als Administrator darstellen. Typischerweise fasst Microsoft in ein Update viele einzelne Patches zusammen, und Sie handeln sich als Administrator möglicherweise andere Risiken ein, sofern Sie eine Deinstallation in Erwägung ziehen.

Bei diesen Deinstallationsdebatten gibt es vor allem eine Komponente zu bedenken, und zwar den Zeitpunkt. Wenn das von Ihnen festgestellte Problem direkt nach der Installation eines vor wenigen Tagen bereitgestellten Updates auftritt, mag das Entfernen des Updates die naheliegende Lösung darstellen.

Handelt es sich bei der im Onlineforum benannten Empfehlung zur Deinstallation um ein Update, das vor mehreren Monaten vorgestellt wurde, können Sie diesen Hinweis getrost vergessen. Sicherlich hat es in der Zwischenzeit diverse Aktivitäten vonseiten des Herstellers gegeben, um den Fehler anderweitig zu beheben.



Achten Sie immer darauf, wann eine Empfehlung in einem Onlineforum zur Fehlerbehebung gepostet wurde. Ein sechs Monate alter Tipp ist möglicherweise eher ein Risiko als die Lösung. Unglücklicherweise werden Tipps von ihren Autoren in den allerseltensten Fällen angepasst.

Auch wir unterliegen in diesem Kapitel den Limitierungen der

Manuskripterstellung, aus diesem Grunde verzichten wir auf spezifische Lösungsvorschläge, sondern bewegen uns eher allgemeingültig und zeitlos durch das Thema Troubleshooting.



Applikationen und Betriebssysteme haben eine »Lebenserwartung«. Dies äußert sich jedoch anders als bei Hardware-Produkten – da die Software-Produkte ja weiterhin funktionieren. Sofern Sie jedoch Produkte außerhalb ihres Produktlebenszyklus weiterbetreiben möchten, müssen Sie damit rechnen, dass Sie bei allen Veränderungen auf sich selbst gestellt sind.

Ein veralteter Windows-Server, der nur mit sich und seiner Applikation ohne Zugriff durch einen aktualisierten Client arbeitet, ist kein Problem. Ein Windows-2000-Server in einer Windows-Server-2016-Domäne mit Windows-10-Clients wird nicht mehr ordentlich arbeiten können, da Sie hoffentlich die Unterstützung für SMB v1 deaktiviert haben.

Als Administrator ist es Ihre Pflicht, sicherzustellen, dass die von Ihnen betreute Landschaft technologisch den Anschluss hält. Das gilt für das Wissen um moderne Technologien gleichermaßen.

Troubleshooting in einer mehr als zwei Entwicklungsgenerationen rückständigen Umgebungen ist eher ein Glücksspiel denn eine gezielte Maßnahme!

Erst die Ereignisanzeige – dann der Rest!

Das wichtigste Hilfsmittel bei der Problemlösung auf Windows-Servern ist Ihnen bestimmt bekannt, und dennoch wollen wir es noch einmal in den Vordergrund holen: die Ereignisanzeige – zu sehen in [Abbildung 23.1](#).

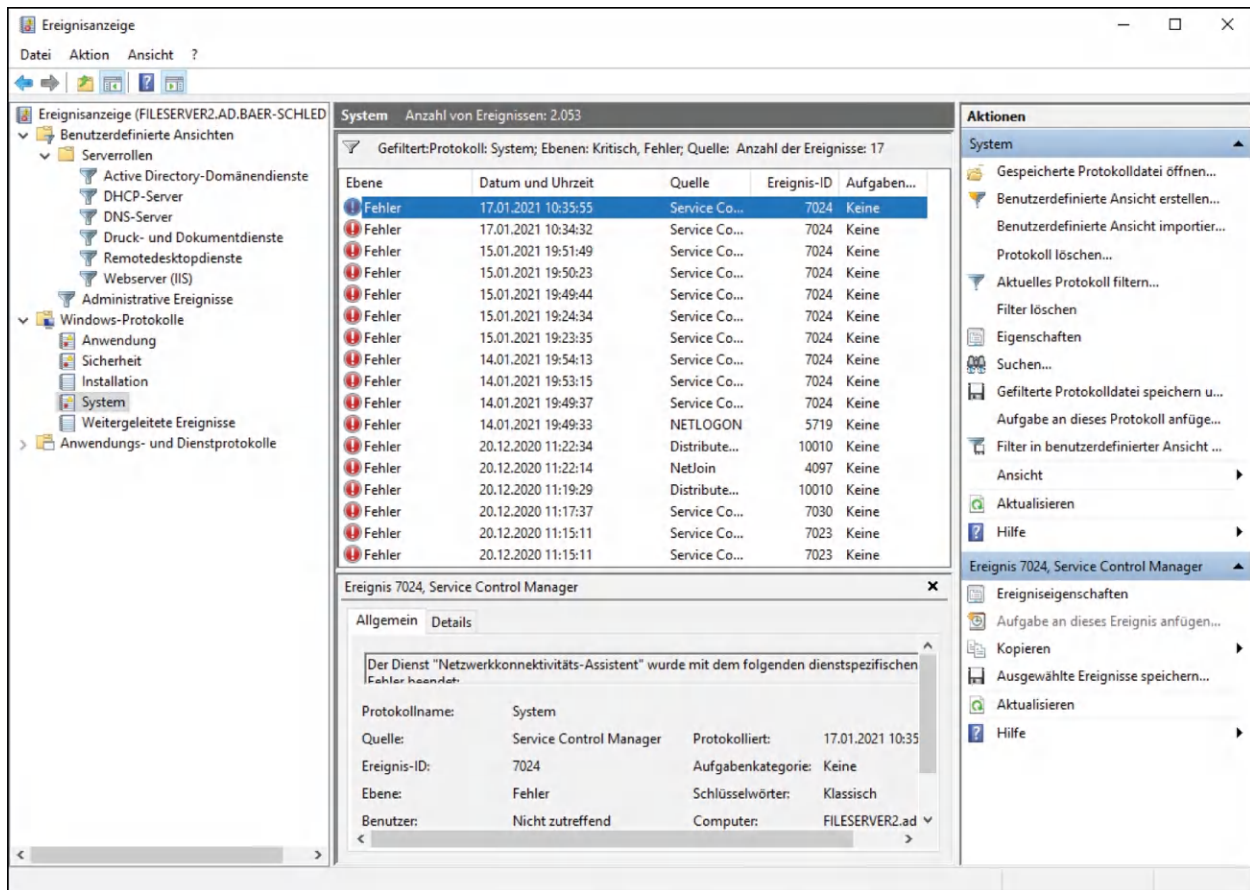


Abbildung 23.1: Erste Anlaufstelle bei Fehlverhalten: das Eventlog

Die Ereignisanzeige, englisch Eventlog, ist die wichtigste Informationsquelle, wenn es um ein Fehlverhalten von Servern geht. Praktischerweise kann sich der Administrator von einer MMC-Konsole aus auch mit den Ereignisanzeigen anderer Computer in der Domäne verbinden. Über die beinahe selbsterklärenden Filterfunktionen und die Zeitstempel können Sie sich schnell dem »Geschehen nähern«.



Die Vorgaben für die Protokollgrößen in der Ereignisanzeige wurden von Microsoft eher konservativ gewählt. Auf wichtigen Servern, die viele Aktionen ausführen, empfiehlt es sich, die Protokollgröße zu erhöhen, um einen längeren Zeitraum retrospektiv betrachten zu können.

Client-Computer zeigen Fehlermeldung in der Regel direkt an und präsentieren ihrem Benutzer einen entsprechenden Fehlerdialog. Dieses

Verhalten ist für Client-Systeme sinnvoll, da der Entwickler davon ausgehen kann, dass der Anwender zum Zeitpunkt des Fehlers vor dem Bildschirm sitzt.

Bei Servern ist das jedoch ganz anders – in den seltensten Fällen sitzt jemand direkt von dem Gerät. Daher protokollieren Anwendungen und Server-Dienste alle Fehler in der Ereignisanzeige.



Ohne zuvor die Ereignisanzeige nach Missständen untersucht zu haben und sich mit den Ereignis-IDs und deren Bedeutungen vertraut gemacht zu haben, sollten Sie weder mit Kollegen über Ihr Problem sprechen noch in Internet-Foren nach Antworten suchen.



Die Ereignis-IDs in der Ereignisanzeige sind sprachunabhängig. Sie können, wenn Sie möchten, die Suche auf englischsprachigen Seiten beginnen. Lediglich die Fehlertexte unterscheiden sich in den Sprachversionen.

Eigene Dokumentationen

Es liegt wohl in der Natur der Sache begründet, dass wir Menschen, wenn keine Probleme auftauchen, auch keine Notwendigkeit sehen, diesen einwandfreien Zustand besonders hervorzuheben oder festzuhalten.

Und auch auf die Gefahr hin, dass das Autorengespann nun den sprichwörtlichen Oberlehrerfinger hebt (sofern Sie den Eindruck haben, beteuern wir, es war nicht in unserem Sinn): Dokumentieren Sie!

Denn leider mussten wir im Rahmen der Fehlersuche nur allzu oft feststellen, dass der ursprüngliche Zustand – also der Zeitpunkt, an dem ein Problem noch nicht bestand – nicht ordentlich protokolliert ist.

Für IT-Administratoren ist jedoch die Dokumentation des Normalzustands von essenzieller Bedeutung. Aufgrund der entstehenden Komplexität von Computersystemen in ihrer, zumeist individuellen Zusammenstellung, gibt es außer dem Administrator niemanden, der die »Normwerte« kennt

beziehungsweise kennen muss.

Stellen Sie sich als Administrator dieser Herausforderung und erstellen Sie Ihre Dokumentation:

- ✓ Exportieren Sie zu Dokumentations- und Vergleichszwecken die Protokolle der Ereignisanzeige.
- ✓ Dokumentieren Sie den Funktionszustand der Domäne mit dem Tool `dcdiag.exe` und leiten Sie das Ergebnis in eine Datei um, zum Beispiel `dcdiag.exe > dcdiag-auswertung-kw05.txt`.
- ✓ Dokumentieren Sie in einer simplen Liste, zu welchen Zeitpunkten neue Programmversionen zum Einsatz kamen oder neue Server-Systeme in Betrieb genommen wurden.
- ✓ Erweitern Sie sukzessiv Ihre Dokumentation, beispielsweise durch Protokollierung von Routing-Einträgen.



Die Dokumentation der Funktions- und Leistungsdaten wird Ihnen bei der Suche nach einem aktuellen Problem heute vielleicht nicht helfen. Dafür sind Sie für die zukünftigen Problemlösungen besser gewappnet.

Server-Manager als Hilfestellung

Die Ereignisanzeige ist eher der Protokollführer, der Server-Manager der Helfer. Allein schon die Farbwahl zur Begrüßung offenbart den aktuellen Status. Sofern Sie als Administrator alle für den Betrieb wichtigen Server in den Manager eingebunden haben, sollte der erste Blick des Tages dieser Software gelten – siehe [Abbildung 23.2](#).

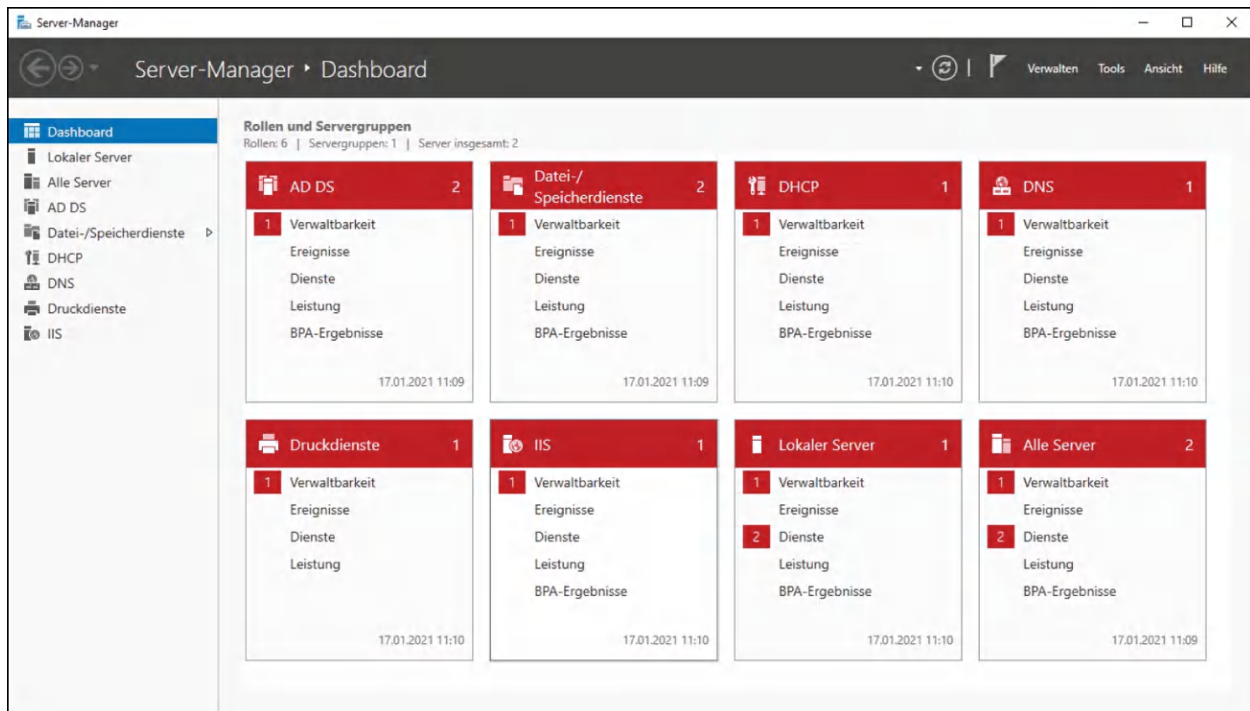


Abbildung 23.2: Die Zeichen stehen auf Rot – der Server-Manager erinnert den Administrator an ausstehende Tätigkeiten.

Glücklicherweise verrät der Server-Manager dem Administrator in den meisten Fällen, was es zu tun gibt. Bei dem hier gezeigten Screenshot steht bei einem Domänencontroller, der gleichzeitig als Druck-, DNS-, Datei- und DHCP-Server fungiert, ein Neustart aus. Allein diese eine ausstehende Maßnahme sorgt somit für eine ganze Menge »roter Kacheln«.

Sollte einer der verwalteten Server komplett fehlen, löst dies im Server-Manager ebenfalls einen rotfarbenen Eintrag aus, der darauf hinweist, dass die vom Administrator gewünschte Server-Sammlung nicht vollständig ist.



Die Zusammenstellung (Serverpool) der Server im Server-Manager wird in Windows pro Benutzer angelegt. Sollten Sie in Ihrer Abwesenheit von einem Kollegen vertreten werden, stellen Sie sicher, dass ihm alle von Ihnen zur Überwachung vorgesehenen Server ebenfalls bekannt sind.

Der Server-Manager hat jedoch noch mehr drauf, als dem Administrator

mit ein paar roten Kacheln anzuzeigen, dass etwas möglicherweise nicht richtig funktioniert. Microsoft hat dem Programm eine automatische Prüfung gegen die »Best Practices Settings« in Form eines Analyzers mit auf den Weg gegeben.

1. Starten Sie den SERVER-MANAGER.
2. Wählen Sie in der linken Menüleiste den Bereich, für den Sie eine Analyse ermitteln möchten, beispielsweise DHCP. Scrollen Sie das rechte Ergebnisfenster herunter, bis Sie den Eintrag BEST PRACTICES ANALYZER sehen. Klicken Sie rechts auf die Auswahl Schaltfläche AUFGABEN.
3. Wählen Sie BPA-PRÜFUNG STARTEN und bestätigen Sie die gewünschte Maschine. Starten Sie den Vorgang durch einen Klick auf ÜBERPRÜFUNG STARTEN.

Nach der BPA-Prüfung findet der Administrator das Ergebnis, aufgelistet nach Problem, Auswirkung und Lösung – zu sehen in [Abbildung 23.3](#).

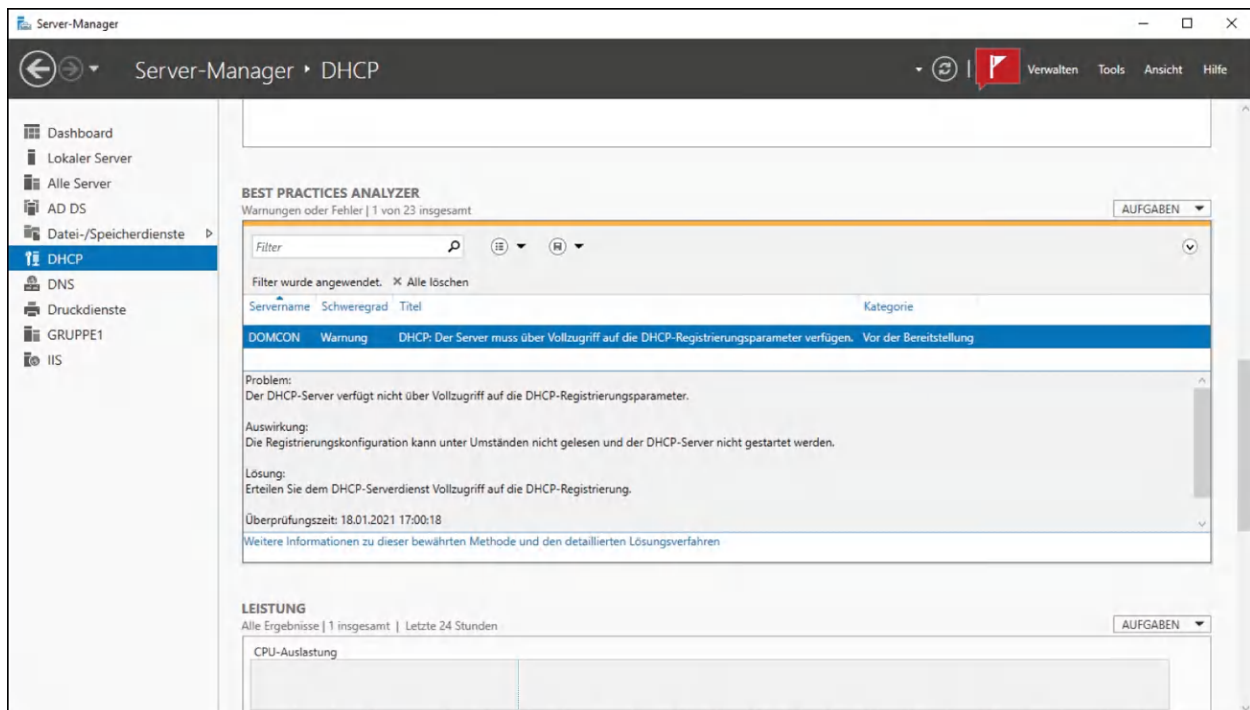


Abbildung 23.3: Ergebnis einer BPA-Prüfung des DHCP-Service

Bevor die Suche nach einem Lösungsvorschlag in einem freien

Internetforum beginnt, sollten versierte Administratoren zunächst die Betriebsempfehlungen des Herstellers Microsoft umsetzen.

IPv6 unterdrücken

IPv6, der jüngere Vertreter des IP-Protokolls, ist seit Jahren in aller Munde, und was für die Anbindung von Web-Services oder IoT-Gerätschaften sinnvoll ist, wird in manch kleiner Umgebung bei der Fehlersuche zu einer Herausforderung.

Seit Windows Server 2008 und dem dazu passenden Client-Betriebssystem bevorzugt Windows globale IPv6-Unicast-Adressen gegenüber IPv4-Adressen. Insgesamt stellt es sich so dar, dass IPv6 immer dominanter wird, während IPv4 zunehmend ins »Hintertreffen« gerät. Das mag den Azure-Aktivitäten von Microsoft geschuldet sein und der damit verbundenen Tatsache, dass in Cloud-Umgebungen IPv6 eher zum Einsatz kommt.

Mitunter wird der Administrator bei der Fehlersuche allein schon von Ping-Antworten im IPv6-Format genervt. Und die Praxis zeigt: In manchen Fällen scheint das Betriebssystem die Metrik-Vorgaben des Administrators pro Interface vollkommen zu ignorieren – oder schlimmer noch – es sind so viele NICs verbaut, dass der Administrator die Übersicht verliert.

Sie deaktivieren die automatische Metrik pro Netzwerkkarte und Protokoll wie folgt:

1. Öffnen Sie den Status des LAN-Dialogs über den Ethernet-Adapter.
2. Wählen Sie EIGENSCHAFTEN und das gewünschte Protokoll, zum Beispiel TCP/IPv6.
3. Klicken Sie erneut auf EIGENSCHAFTEN.
4. Klicken Sie auf die Schaltfläche ERWEITERT...
5. Deaktivieren Sie die »Automatische Metrik« und geben Sie einen Wert ein – beispielsweise 20. Wiederholen Sie den Vorgang für das Protokoll IPv4 mit dem Wert 10, und Sie geben IPv4 den Vorzug.



Als obligatorischer Bestandteil des Windows-Betriebssystems wird vor der kompletten Deaktivierung von IPv6 oder seiner Komponenten von Microsoft explizit gewarnt. Sofern es für die Fehlersuche hilfreich ist, können Sie dafür sorgen, dass Windows IPv4 bevorzugt.

Wie gesagt, muss der Administrator unglücklicherweise diese kleine »Konfigurationsorgie« pro Protokoll und Adapter durchführen. Wenn es einmal schneller gehen soll – beim Troubleshooting sehr hilfreich –, kann der IT-Profi dafür sorgen, dass IPv4 generell der Vorzug gegeben wird.

1. Öffnen Sie RegEdit über START | AUSFÜHREN.
2. Wechseln Sie in den Pfad HKLM\ System\ CurrentControlSet\ services\ TCPIP6\ Parameters und suchen Sie den Schlüssel DISABLEDCOMPONENTS.
3. In der Standardeinstellung »0« ist IPv6 voll aktiviert, mit »32« wird IPv4 der Vorzug gegeben, und »4294967295« würde IPv6 gänzlich deaktivieren (nicht empfohlen).
4. Nach einem Neustart des Computers greifen die neuen Einstellungen für alle Netzwerkkarten im System gleichermaßen.



Grundsätzlich ließe sich die Bevorzugung von IPv4 oder die komplette Deaktivierung von IPv6 auch per Gruppenrichtlinie umsetzen. Hierzu verweisen wir auf einen entsprechenden Blog-Beitrag von Mark Heitbrink:
<https://www.gruppenrichtlinien.de/artikel/ipv6-deaktivieren-das-protokoll-nicht-die-bindung>.

Wo finde ich Unterstützung?

Sofern Sie die Hilfestellungen der Bordmittel von Windows ausgeschöpft haben oder einfach bei der Fehlersuche nicht weiterkommen – was nun?

Ihre erste Anlaufstelle sind stets die Microsoft Docs:

<https://docs.microsoft.com/en-us/windows-server/> oder auf Deutsch unter <https://docs.microsoft.com/de-de/windows-server/>.

Ausgestattet mit den richtigen Suchbegriffen, finden Sie hier viele gute, spannende und tiefgehende Informationen – direkt vom Hersteller. Die Microsoft Docs haben jedoch auch etwas von einer »losen Blattsammlung« ohne ordnenden Rahmen, und natürlich finden Sie nur sehr geringe Hinweise auf Produkte von Drittherstellern. Es gibt auch einige wenige Troubleshooting-Dokumente.

Glücklicherweise ist das Internet voller Foren mit vielen mehr oder minder qualitativen Vorschlägen zur Problemlösung. Es empfiehlt sich, insbesondere bei Forenbeiträgen, den kompletten Verlauf durchzulesen, ehe in einem Anfall von Aktionismus Änderungen an den Systemeinstellungen erfolgen.



Da die Qualität von Internetseiten stets schwankend ist, finden Sie hier keine generellen Empfehlungen für Foren- oder Blog-Seiten. Die Suchmaschine Ihrer Wahl wird Sie – mit den passenden Suchbegriffen gefüttert – zum Ziel führen.



Einträge von Benutzern mit einem MVP-Logo dürften hier besonders hilfreich sein.

Microsoft Most Valuable Professionals, kurz MVPs, sind Technologieexperten, die ihr Wissen leidenschaftlich mit der Community teilen. Sie sind immer auf dem neuesten Stand der Technik und haben den unaufhaltsamen Drang, neue, spannende Technologien kennenzulernen. Sie verfügen über ein sehr fundiertes Wissen über Microsoft-Produkte und -Dienste und sind gleichzeitig in der Lage, verschiedene Plattformen, Produkte und Lösungen zusammenzuführen, um Probleme aus der Praxis zu lösen. MVPs bilden eine globale Community aus über 4.000 technischen Experten und Community Leaders in 90 Ländern und Regionen, und sie werden von ihrer Leidenschaft, ihrem Gemeinschaftssinn und ihrer

Suche nach Wissen angetrieben. Neben ihren erstaunlichen technischen Fähigkeiten sind MVPs vor allem immer bereit, anderen zu helfen – und das zeichnet sie aus, so Microsoft.

Grundsätzlich kann jeder zu einem aktiven und kompetenten Teil der Tech-Community werden. Weitere Informationen findet der angehende MVP auf der Seite <https://mvp.microsoft.com/de-de/overview>.

Sie werden sich wundern, aber je größer eine IT-Abteilung ist, desto mehr externe Berater, IT-Experten und Personen, die sich für IT-Experten halten, gehen ein und aus. Irgendwann ist für jeden eine Kapazitätsgrenze erreicht, und der finanzielle Aufwand, externe IT-Berater zu suchen und zu beauftragen, ist geringer als die zeitlich erforderliche interne Lernkurve, um dasselbe Ziel zu erreichen.

Bei der Suche nach einem passenden Partner ist der Hersteller Microsoft auch zur Hand und bietet eine praktische Suchfunktion auf der Webseite (siehe [Abbildung 23.4](#)) <https://www.microsoft.com/de-de/solution-providers/home> an.

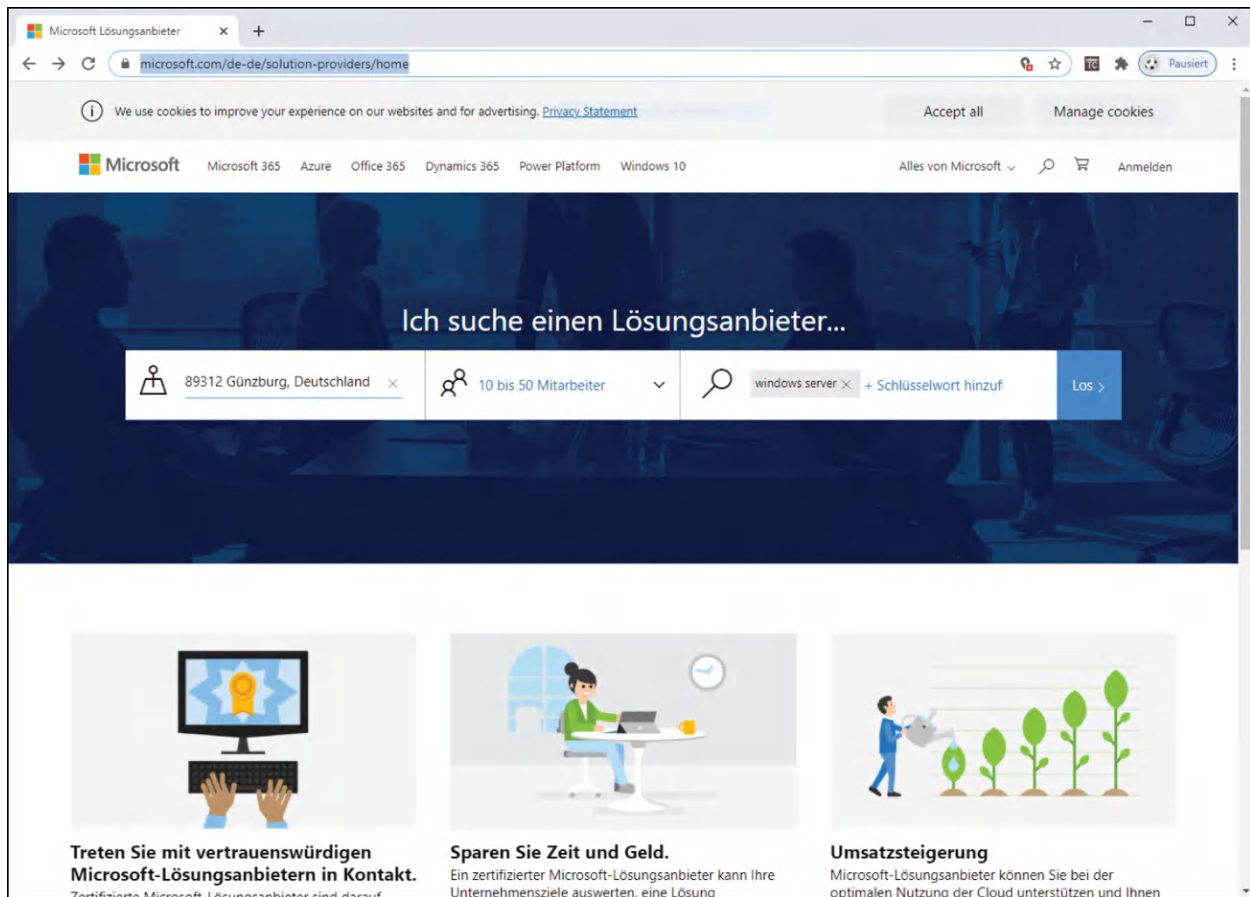


Abbildung 23.4: Microsoft hilft bei der Suche nach dem einen passenden Partner.

Die Wahl eines passenden IT-Beraters ist von vielen Faktoren abhängig:

- ✓ Erfahrung des Partners
- ✓ Kennzahlen des Partners in Bezug auf Mitarbeiter, Umsatz, Projektanzahl, Marktbeständigkeit
- ✓ Preisgestaltung
- ✓ Termintreue
- ✓ Anzahl nachweislich durchgeführter ähnlicher Projekte
- ✓ Branchenkenntnis

Neben diesen hoffentlich passenden Skills geht es schlussendlich aber um den Faktor Vertrauen. Ist der Berater ein »Newbie« mit wenig Erfahrung, aber Sie haben ein absolut gutes Gefühl, dass Sie gemeinsam das Ziel schnell und sicher erreichen werden, dann ist das vielleicht die passende

Person.

Wir möchten aber nicht die Erkenntnis unter den Tisch kehren, dass der soeben beschriebene »Youngster« möglicherweise nicht das Maximum aus dem Vorhaben rausholt, weil es dazu schlicht an Erfahrung mangelt.



Natürlich möchten IT-Administratoren am liebsten alles selbst machen – dem Unternehmen ist es, zumindest in der nachträglichen Betrachtung, aber herzlich egal, wer es war. Hauptsache es hat funktioniert.

Bye bye

Vielen Dank für Ihr Interesse, für Ihre Zeit und für das Vertrauen. Uns hat es sehr viel Spaß gemacht – wir hoffen Ihnen auch. Wir übergeben nun voller Vertrauen an die »dicken Brummer« von Fachbüchern mit thematischen Schwerpunkten zur weiteren Vertiefung des Wissens. Viel Erfolg!

Teil IV

Der Top-Ten-Teil



Der
Top-Ten-
Teil



Besuchen Sie uns doch einmal auf
www.facebook.de/fuerdummies!

IN DIESEM TEIL ...

- ✓ Zehn Software-Werkzeuge aus der Praxis, die bei der Arbeit mit einem Windows-Server sehr hilfreich sein können.

Kapitel 24

Die 10 besten Server-Tools

Manchmal brauchen Sie mehr als den Windows-Server. Dann sollten Sie sich hier mal umschauen.

Veeam Backup & Replication Community Edition

Alle Sicherheitsvorkehrungen sind sinnlos ohne ein funktionierendes Backup. Die freie Lösung der Veeam-Software kann nicht nur den Server, sondern auch die virtuellen Maschinen sichern und wiederherstellen:

<https://www.veeam.com/de/virtual-machine-backup-solution-free.html>

AD Replication Status Tool

Wollen Administratoren Fehler im Netzwerk finden oder sicherstellen, dass alles funktioniert, kann das Werkzeug AD Replication Status Tool den Replikationsstand aller Domänencontroller anzeigen.

<https://www.microsoft.com/en-us/download/details.aspx?id=30005>

Specops Password Auditor für Active Directory

Hilft dem Administrator, schwache Passwörter im AD zu finden.

<https://specopssoft.com/de/specops-password-auditor-fur-active-directory/>

Winscp

Ein Open-Source-SFTP-, FTP- und SCP-Client.

<https://winscp.net/eng/docs/lang:de>

Microsoft Security Compliance Toolkit 1.0 (SCT)

Eine Reihe von Tools, mit der Sicherheitsadministratoren von Microsoft empfohlene Konfigurations-Sicherheitsgrundwerte für Windows und andere Microsoft-Produkte herunterladen, analysieren, testen, bearbeiten und speichern können.

<https://www.microsoft.com/en-us/download/details.aspx?id=55319>

WiseDataman Password Control

Software, die bei Verwaltung und Betreuung von Passwörtern auch in AD-Domänen helfen kann.

<https://wisedataman.com/password-control>

WireShark

Eine Art »Schweizer Taschenmesser«, wenn es um Analyse und Arbeit der Netzwerkprotokolle geht.

<https://www.wireshark.org/>

RSAT

RSAT, die Remote Server Administration Tools sind eine Windows-Server-Komponente für die Verwaltung entfernter Computer, die auch Teil von Windows 10 »bei Bedarf« ist.

<https://www.microsoft.com/de-DE/download/details.aspx?id=45520>

SysMon

Der Systemmonitor aus der Sammlung der Sysinternals-Tools hilft dabei, Prozesse und Ereignisse auf dem Server zu überwachen.

<https://docs.microsoft.com/de-de/sysinternals/downloads/sysmon>

SysInternals Suite (komplett)

Die komplette Suite der Hilfeprogramme von Sysinternals bietet eine Sammlung von Programmen, die bei Systemproblemen und deren Analyse helfen und in jeden »Werkzeugkasten« für den Windows-Server gehören.

<https://docs.microsoft.com/de-de/sysinternals/downloads/sysinternals-suite>

Dummies Junior – die frechen »... für Dummies« für interessierte Kids und Jugendliche

- » Projekte zum Ausprobieren, Programmieren und Experimentieren
- » Mit pädagogischem Konzept
- » Viele Abbildungen
- » Verständliche Texte
- » In Workshops erprobt



C. Ermel, N. Rosenfeld

Spaß mit Elektronik für Dummies Junior

1. Auflage 2020 ISBN: 978-3-527-71705-7

198 Seiten

Format: 176 mm x 240 mm

Ladenpreis: 15,- €*

In diesem Buch lernst du, Schaltungen für coole Gadgets aufzubauen: eine Glückwunschkarte, die leuchtet, eine blinkende Weihnachtsbaumkugel, einen klingenden Draht und anderes mehr.



M. Ponce Kärger

Hörspiel und Podcast selber machen für Dummies Junior

1. Auflage 2020 ISBN: 978-3-527-71704-0

192 Seiten

Format: 176 mm x 240 mm

Ladenpreis: 16,- €*

Sein eigener Produzent sein, wer will das nicht? Steig ein in die Welt der Hörspiele und Podcasts. Dieses Buch zeigt dir Schritt für Schritt, wie du deine eigenen Audiobeiträge produzieren und veröffentlichen kannst.



U. Schmid, K. Weitz, M. Siebers

Künstliche Intelligenz selber programmieren für Dummies Junior

1. Auflage 2019 ISBN: 978-3-527-71573-2

134 Seiten

Format: 140 mm x 216 mm

Ladenpreis: 12,99 €*

Mit diesem Buch verstehst du, was Künstliche Intelligenz ist. Du findest heraus, ob es Künstliche Intelligenz bereits gibt. Und das Beste: Mit Hilfe kleiner Programme erkennst du, wie durch Computerprogramme Künstliche Intelligenz entsteht



V. Borngässer

Stop-Motion-Trickfilme selber machen für Dummies Junior

1. Auflage 2018 ISBN: 978-3-527-71484-1

144 Seiten

Format: 140 mm x 216 mm

Ladenpreis: 11,99 €*

Schritt für Schritt zum eigenen Stop-Motion-Video mit der richtigen Beleuchtung, krassen Geräuschen und Spezialeffekten. Hier erfährst du, wie es geht.



N. Bergner, Th. Leonhardt

Eigene Apps programmieren für Dummies Junior

2. Auflage 2019 ISBN: 978-3-527-71596-1

136 Seiten

Format: 140 mm x 216 mm

Ladenpreis: 11,99 €*

Hast du Lust, deine eigene App zu programmieren, die dann auch wirklich auf einem Android-Smartphone läuft? Mit dem kostenlosen App Inventor ist das gar nicht schwer.



* Der €-Preis gilt nur für Deutschland. Preisänderungen und Irrtümer vorbehalten.

Stichwortverzeichnis

64-Bit-Prozessor [27](#)

A

AAAA [159](#)

Access-based Enumeration (ABE) [231](#)

Active Directory [105](#)

 Funktionsebene [112](#)

 Papierkorb [133](#)

 Verwaltungscenter [134](#)

Administrator [118](#)

ADML [351](#)

ADMX [351](#)

AGULP [140](#)

Airprint [312](#)

Alias [65](#)

Anmeldebildschirm [101](#)

APIPA [179](#)

Arbeitsgruppe (Workgroup) [379](#)

Arbeitsordner [223](#)

Arbeitsspeicherpuffer [270](#)

Authentifizierung [392](#)

Autorisierung [182](#)

Autoritätenursprung [167](#)

Azure [399](#)

Azure Arc [41](#)

Azure Stack HCI (Hyperconverged Infrastruktur) [386](#)

B

Backup

 differenzielles [422](#)

 inkrementelles [422](#)

Bare-Metal-Installation [95](#)

BCEDIT [299](#)

Benutzer [137](#)

 anlegen [113](#)

 Gruppenzuweisung [140](#)

Benutzerkontentypen [143](#)

Best Practice Analyzer [375](#)

Betriebsbehindernd [436](#)

Betriebsmasterrollen [128](#)

Branchcache [221](#)

C

CALs (Client-Zugriffslizenzen) [37](#)

Central Access Policies (CAP) [234](#), [238](#)

Central Access Rule (CAR) [234](#), [238](#)

Central Store [351](#)

CIFS [107](#)

CIMOM [342](#)

Claim Types [234](#)

Client-Server-Modell [26](#)

- cmd [56](#)
- Cmdlet [64](#)
- CNAME [159](#)
- Common Information Models (CIM) [60](#)
- Computeranmeldung
 - verweigern [354](#)
- Computerverwaltung [117](#) [382](#)
- CoreInfo [27](#)
- Core-Server installieren [101](#)

D

- DAC [233](#)
- DANE [172](#)
- Deduplizierung [214](#)
- Default Domain Policy [352](#)
- Desktopdarstellung [98](#)
- Desktophintergrundbild [357](#)
- DFS
 - Namespaces [217](#)
 - Replikation [219](#)
- DHCP [178](#)
 - Failover [187](#)
 - Installation [180](#)
 - Optionen [186](#)
 - Reservierungen [183](#)
- DHCP-Server [326](#)

DHCP-Wächter [273](#)

DIN 31051 [432](#)

Directory Service [106](#)

Diskraid [201](#)

djoin.exe [330](#)

DNS [147](#)

- Cache Poisoning [172](#)

- Installation [150](#)

- Konfiguration [155](#)

- Sicherheit [172](#)

- Spoofing [173](#)

- Stammhinweise [153](#)

- Tunneling [173](#)

- Weiterleitungen [155](#)

DNSSEC [172](#)

- Konfiguration [173](#)

DNS-Server [323](#)

Domain Name Service *siehe* [DNS](#)

Domäne [107](#)

Domänen-Admins [119](#)

Domänencontroller

- entfernen [130](#)

Domänennamenmaster [128](#)

Druckaufträge

- betrachten [314](#)

Druckdienste

- Installation [301](#)

Drucker

bereitstellen [311](#)

Export [313](#)

hinzufügen [307](#)

Import [313](#)

Druckerserver [298](#)

Druckerspooler [299](#)

Druckertreiber [299](#)

Isolation [318](#)

Druckerverwaltung via PowerShell [83](#)

Druckerwarteschlange [302](#)

Druckfilter [307](#)

Druckmonitor [302](#)

Dynamic Access Control [233](#)

Dynamic Hardware Pool (DHP) [47](#)

Dynamischen Arbeitsspeicher aktivieren [270](#)

E

Editor für lokale Gruppenrichtlinien [414](#)

Effektiver Zugriff [241](#)

Eingabeaufforderung

deaktivieren [359](#)

Ereignisanzeige (Event Viewer) [383](#)

Ereignis-ID [384](#)

Erweiterter Sitzungsmodus (Enhanced Session Mode) [280](#)

Execution Policy [78](#)

ext3 [292](#)

ext4 [292](#)

F

Firmware [268](#)

Forward-Lookupzone [153](#)

Fernzugriff [441](#)

FQDN [109](#)

Freigaben [225](#)

 versteckte [226](#)

Fully-Qualified Host Name (FQDN) [392](#)

G

Gast [144](#)

Gastkonto

 deaktivieren [360](#)

Gastsysteme [261](#)

Gatewayserver [387](#)

Geschütztes Netzwerk [274](#)

GNU-/Linux-Umgebung [38](#)

Google Cloud Print (GCP) [311](#)

gpresult [372](#), [371](#)

GPT [200](#)

gpupdate [370](#)

Graphics Device Interface (GDI) [301](#)

Group Policy Objects (GPO) [335](#)

 administrative Vorlagen [349](#)

 Aktualisierungsintervall [353](#)

Handlungsempfehlung [354](#)

löschen [339](#)

verknüpfen [338](#)

Gruppen [138](#)

erstellen [138](#)

Gruppenrichtlinien

Fehlersuche [370](#)

Gruppenrichtlinienobjekte *siehe* [Group Policy Objects \(GPO\)](#)

Gruppenrichtlinienverwaltungs-Editor [336](#)

H

Hardware hinzufügen [268](#)

Hardwarebeschleunigung [273](#)

HCL (Hardware Compatibility List) [29](#)

Hintergrundaktualisierungen [353](#)

Hosteintrag

anlegen [160](#)

hosts-Datei [148](#)

Hyper-V [245](#), [257](#)

Hyper-V-Container [39](#)

Hypervisor [246](#)

Hyper-V-Rolle [247](#)

I

Infrastructure as a Service (IaaS) [44](#)

Infrastrukturmaster [128](#)

Integrationsdienste [274](#)

Internet Explorer (IE) [380](#)

Internetdrucken [317](#)

IPAM [190](#)

IPC\$ [227](#)

IPP [319](#)

IPsec-Taskabladung [273](#)

iSCSI

- Initiator [196](#)

- Target [199](#)

- Zielserver [196](#)

- Zielspeicheranbieter [201](#)

Item Level Targeting (ITL) [346](#)

IT-Grundschutz-Kompendium [433](#)

K

Kerberos [107](#)

Kerberos Token [230](#)

Konsolenfenster [57](#)

Kontingentverwaltung [211](#)

L

Laufwerkfreigabe

- per Gruppenrichtlinie [228](#)

LDAP [107](#)

Lease [178](#)

Legacyconsole [58](#)

Line Printer Daemon [315](#)
Line Printer Remote [315](#)
Linux-Container [39](#)
Linux-Gastsysteme [292](#)
Livemigration [252](#)
Lokaler Dienst [144](#)
Lokaler Server [377](#)
Long-Term Servicing Channel (LTSC) [36](#)
Long-Term Support [292](#)
Loopback [368](#)
LPD [303](#), [315](#)
LPR [303](#), [315](#)

M

MBR [200](#)
Medien [277](#)
Microsoft UEFI-Zertifizierungsstelle [293](#)
Mitglieder [141](#)
Module [66](#)
Monitoring [437](#)
MS-DOS [55](#)
MS-DS-MachineAccountQuota [115](#)
MSI [365](#)
MSP [365](#)
MST [365](#)
Multiprocessing [34](#)

MX [159](#), [161](#)

N

Nagios [438](#)

Named Pipe [227](#)

Namensauflösung [147](#)

Netzwerkdienst [144](#)

Netzwerkkarten [88](#)

NFS [203](#)

NIC-Teamvorgang [274](#), [380](#)

nslookup [160](#)

NTFS

Rechte [208](#)

ntuser.dat [337](#)

NuGet-Feeds [397](#)

NUMA [251](#)

O

Objekte [63](#)

On-premise [43](#)

Organisations-Admins [120](#)

Organization Unit (OU) [136](#)

P

Passwörter [360](#)

PDC-Emulationsmaster [128](#)

Ping-Kommando [324](#)
Pipelines [65](#)
Platform as a Service (PaaS) [44](#)
Portspiegelung [274](#)
PostScript [303](#)
PowerShell-Modul für Hyper-V [283](#)
Primäre Zone [162](#)
Print Queue [300](#)
PrintBrm.exe [313](#)
Printer Command Language (PCL) [301](#)
Print-Server [298](#)
Produktionsprüfpunkte [275](#), [286](#)
Programmzugriff
 sperren [368](#)
Provider [65](#)
PRTG [438](#)
Prüfpunkte [274](#), [285](#)
 anwenden [288](#)
 löschen [290](#)
PTR [154](#)
PXE [186](#)

Q

Quality of Service (QoS) [272](#)
Quoten und Kontingente [436](#)

R

RAID [196](#)
RAM-Diagnoseprogramm [435](#)
Rechte [145](#)
Reguläre Ausdrücke [72](#)
Remote Desktop Services (RDS) [281](#)
Remote Server Administration Tools [132](#)
Replikation [107](#), [126](#)
Replikat-Server [253](#)
Ressource Properties [234](#)
Ressource Property Lists [234](#)
Reverse-Lookupzone [154](#)
 anlegen [159](#)
RID-Master [128](#)
RISC (Reduced Instruction Set Computer) [34](#)
Robocopy [217](#)
RODC [107](#), [164](#)
 Limitierungen [123](#)
Role-Based Access Control (RBAC) [401](#)
Routenwächter [273](#)
RSAT [132](#)
rsop.msc [370](#)
Rufus [96](#)

S

SAM [143](#)
Schattenkopie [202](#)
Schema-Admins [120](#)

- Schemamaster [128](#)
- sconfig [416](#)
- Scope [178](#)
- SCSI-Controller [272](#)
- Sekundäre Zone [162](#)
- Server-Ausfälle [431](#)
 - wegen voller Festplatte [436](#)
- Server-Gruppe [375](#)
- Server-Manager [455](#)
 - Dashboard [373](#)
 - Tools-Menü [381](#)
- shutdown.exe [213](#)
- Sicherer Start [269](#)
- Sicherheitsgruppe
 - Global [138](#)
 - Lokal (in Domäne) [138](#)
 - Universal [139](#)
- Sicherheitsrichtlinie [270](#)
- Sicherheitszone Internet [381](#)
- Single Root I/O Virtualization (SR-IOV) [273](#)
- Single Sign-on [392](#)
- Skriptsprachen [61](#)
- SMB-Protokolls (Server Message Block) [401](#)
- SOA [167](#)
- Software as a Service (SaaS) [373](#)
- Softwareinstallation [365](#)
- Speicherberichtsverwaltung [213](#)

Speicherdienste [195](#)
Speichermigration [252](#)
SPL Viewer [314](#)
SSD [196](#)
Stammhinweise
 wiederherstellen [157](#)
Standardbrowser [362](#)
Standardprüfungspunkte [275](#), [285](#)
Syspectr [439](#), [449](#)
Systemsteuerung
 Zugriff deaktivieren [359](#)
SYSVOL [337](#)

T

TPM-Chip [29](#)
Trusted Platform Module (TPM) [270](#)

U

Übermittlungsoptimierung [410](#), [411](#)
UCS [105](#)
Updates [405](#)
 erweiterte Optionen [408](#)
 suchen [407](#)

V

VBA deaktivieren [363](#)

Verzeichnisdienst [106](#)
VHDX-Image-Dateien [292](#)
Virtual Machine Bus [280](#)
Virtual Machine Queue (VMQ) [273](#)
Virtualcore [48](#)
Virtualisierung [245](#)
Virtuelle Computer [251](#)
Virtuelle Festplatte [246](#), [251](#)
Virtuelle Maschine (VM) [246](#)
 anlegen [262](#)
 Generation 1 [263](#)
 Generation 2 [263](#), [267](#)
Virtueller Switch [246](#), [254](#)
Vollbackup [422](#)
Vollbildmodus [283](#)

W

Web Based Enterprise Managements (WBEM) [60](#)
Wechseldatenträgerlaufwerke
 deaktivieren [360](#)
whoami [146](#)
Windows Admin Center (WAC) [385](#)
 Erweiterungen [396](#)
Windows Hardware Compatibility Program [29](#)
Windows Management Instrumentation [342](#)
Windows NT [33](#)
Windows PowerShell ISE [62](#)

Windows Remote Management (WinRM) [389](#)
Windows Server 2022 [40](#)
Windows Server Evaluation Center [387](#)
Windows Server Update Services (WSUS) [405](#)
Windows Subsystem for Linux (WSL) [38](#)
Windows-Container [39](#)
WMI Query Language [344](#)
WMI-Filter [342](#)
WPAD [187](#)
WQL [346](#)

Z

Zielgruppenadressierung [346](#)
Zoneneigenschaften [165](#)

Diese Bücher könnten Sie auch interessieren

A. Dittfurth

PowerShell für Dummies

1. Auflage 2019 ISBN: 978-3-527-71471-1

370 Seiten

Format: 176 mm x 240 mm

Ladenpreis: 24,99 €*

Diese leicht verständliche Einführung in PowerShell mit vielen Praxisbeispielen beschreibt die wichtigsten Commandlets und erläutert die Arbeit mit Objekten und den Gebrauch von Skripten. Finden Sie heraus, was die neue PowerShell auf verschiedenen Betriebssystemen kann.



D. Lowe

Netzwerke für Dummies

10. Auflage 2021 ISBN: 978-3-527-71772-9

528 Seiten

Format: 176 mm x 240 mm

Ladenpreis: 24,99 €*

Der ideale Einstieg für alle, die ein Netzwerk einrichten möchten! Mit diesem Buch gelingt Ihnen die Installation und Konfiguration von Servern und Clients. Router, Switch und Access-point gehören bald zu Ihren besten Freunden.



J. Steinberg und M. Haller

Cyber-Sicherheit für Dummies

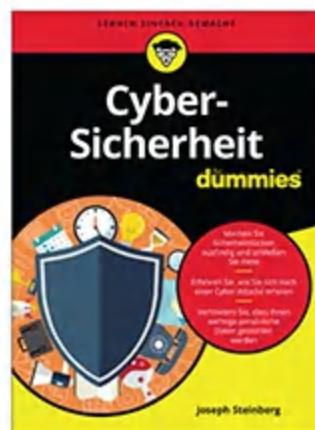
1. Auflage 2020 ISBN: 978-3-527-71665-4

294 Seiten

Format: 176 mm x 240 mm

Ladenpreis: 20,- €*

In diesem Buch erfahren Sie, welchen Gefahren Sie und Ihr Computer ausgesetzt sind, wie Sie sich davor schützen, wie Sie Schwachstellen in Ihren Geräten erkennen und was Sie – wenn es zum Fall der Fälle kommt – tun müssen, um Ihre Daten möglichst wiederherzustellen.



K. Beaver und G. Franken

Hacken für Dummies

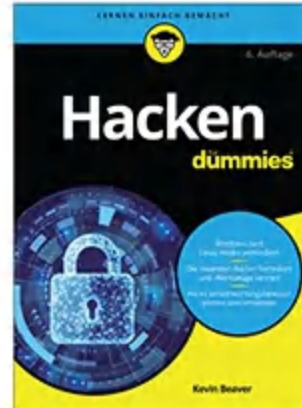
6. Auflage 2020 ISBN: 978-3-527-71795-8

396 Seiten

Format: 176 mm x 240 mm

Ladenpreis: 25,- €*

Erfahren Sie in diesem Buch, wie Hacker denken, wo sie in Ihren IT-Systemen Angriffsstellen suchen (und finden) und wie Sie sich dagegen schützen können.



F. Geisler und B. Kettner

Microsoft Azure für Dummies

1. Auflage 2021 ISBN: 978-3-527-71835-1

384 Seiten

Format: 176 mm x 240 mm

Ladenpreis: 28,- €*

Dieses Buch bietet einen Überblick über die grundlegenden Cloud-Betriebsmodelle und die wichtigsten Dienste von Microsoft Azure. Auf Grundlage der CLI-Code-Beispiele können Sie eine eigene Azure-Umgebung aufbauen.



E. Freeman

DevOps für Dummies

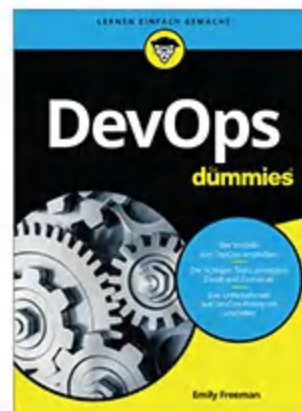
1. Auflage 2019 ISBN: 978-3-527-71624-1

328 Seiten

Format: 176 mm x 240 mm

Ladenpreis: 26,99 €*

Finden Sie mit diesem Buch den Einstieg in DevOps: Wie Sie DevOps-Arbeitsweisen praktisch implementieren, wo die Hürden sind und wie Sie sie überwinden können.



*Der €-Preis gilt nur für Deutschland. Preisänderungen und Irrtümer vorbehalten.

WILEY END USER LICENSE AGREEMENT

Besuchen Sie www.wiley.com/go/eula, um Wiley's E-Book-EULA einzusehen.