

O'REILLY®

Thomas Joos

Microsoft
Windows
Server 2022

Von der Planung und Migration bis zur
Konfiguration und Verwaltung

DAS HANDBUCH

The background of the cover is a high-angle, night-time photograph of a city. The city lights are visible as a dense grid of small white and yellow dots. Overlaid on this are several major highways, their paths captured as long, glowing streaks of red and white light, indicating the movement of traffic. The overall color palette is dominated by the cool blues and purples of the night sky, contrasted with the warm oranges and reds of the light trails.



Thomas Joos

ist selbstständiger IT-Consultant und seit 20 Jahren in der IT-Branche tätig. Er schreibt Fachbücher und berät Unternehmen im Mittelstands- und Enterprise-Bereich in den Themenfeldern Active Directory, Exchange Server und IT-Sicherheit. Durch seinen praxisorientierten und verständlichen Schreibstil sind seine Fachbücher für viele IT-Spezialisten eine wichtige Informationsquelle geworden. Seinen Blog finden Sie auf <http://thomasjoos.wordpress.com>. Neben vielen erfolgreichen Büchern schreibt er für zahlreiche IT-Publikationen wie z.B. *c't*, *iX*, *IT Administrator* und *tecchannel.de*.

Papier
plus⁺
PDF.

Zu diesem Buch – sowie zu vielen weiteren O'Reilly-Büchern – können Sie auch das entsprechende E-Book im PDF-Format herunterladen. Werden Sie dazu einfach Mitglied bei oreilly.plus⁺:

www.oreilly.plus

Thomas Joos

Microsoft Windows Server 2022 – Das Handbuch

Von der Planung und Migration
bis zur Konfiguration und Verwaltung

O'REILLY®

Thomas Joos

Lektorat: Sandra Bollenbacher

Fachlektorat: Georg Weiherer und Rainer G. Haselier

Korrektorat: Petra Heubach-Erdmann, Düsseldorf

Satz: Gerhard Alfes, mediaService, Siegen, www.mediaservice.tv

Herstellung: Stefanie Weidner

Umschlaggestaltung: Michael Oréal, www.oreal.de

Bildnachweis: buranatrakul, Stock-Fotografie-ID: 508671177

Druck und Bindung: C.H.Beck, Nördlingen

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.

ISBN:

Print 978-3-96009-182-0

PDF 978-3-96010-616-6

ePub 978-3-96010-617-3

mobi 978-3-96010-618-0

1. Auflage 2022

Copyright © 2022 dpunkt.verlag GmbH

Wieblinger Weg 17

69123 Heidelberg

Dieses Buch erscheint in Kooperation mit O'Reilly Media, Inc. unter dem Imprint »O'REILLY«. O'REILLY ist ein Markenzeichen und eine eingetragene Marke von O'Reilly Media, Inc. und wird mit Einwilligung des Eigentümers verwendet.

Hinweis:

Der Umwelt zuliebe verzichten wir auf die Einschweißfolie.

Schreiben Sie uns:

Falls Sie Anregungen, Wünsche und Kommentare haben, lassen Sie es uns wissen:

komentar@oreilly.de.

Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung des Verlags urheberrechtswidrig und daher strafbar. Dies gilt insbesondere für die Vervielfältigung, Übersetzung oder die Verwendung in elektronischen Systemen.

Es wird darauf hingewiesen, dass die im Buch verwendeten Soft- und Hardware-Bezeichnungen sowie Markennamen und Produktbezeichnungen der jeweiligen Firmen im Allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz unterliegen.

Alle Angaben und Programme in diesem Buch wurden mit größter Sorgfalt kontrolliert.

Weder Autor noch Verlag können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Buches stehen.

5 4 3 2 1 0

Inhaltsverzeichnis

| | |
|--|----|
| Vorwort | 29 |
| Teil I Grundlagen und Installation | |
| Kapitel 1 Neuerungen und Lizenzierung | 33 |
| 1.1 Die wichtigsten Neuerungen in Windows Server 2022 | 33 |
| 1.1.1 Neuerungen in Windows Server 2022 | 34 |
| 1.1.2 Secured-Core-Server mit Windows Server 2022 | 34 |
| 1.1.3 Neues Container-Image für Windows Server 2022 | 35 |
| 1.2 Windows Server 2022 lizenzieren | 36 |
| 1.2.1 Editionen und Lizenzen im Vergleich | 37 |
| 1.2.2 Clientzugriffslizenzen beachten | 37 |
| 1.2.3 Geräte-CALs und Benutzer-CALs | 38 |
| 1.3 Windows Server 2022 für kleine Unternehmen | 39 |
| 1.3.1 Neue und nicht mehr vorhandene Funktionen in Windows Server 2022 Essentials | 40 |
| 1.3.2 Wann lohnt sich der Einsatz von Windows Server 2022 Essentials? | 40 |
| 1.3.3 Schneller Wechsel zu Windows Server 2022 Standard/Datacenter möglich | 41 |
| 1.3.4 Das muss beim Einsatz von Windows Server 2022 Essentials beachtet werden ... | 42 |
| 1.3.5 Zu Windows Server 2022 Essentials migrieren | 42 |
| 1.4 Windows 11 und Windows Server 2022 | 42 |
| 1.4.1 Zu Windows 11 aktualisieren und Systemvoraussetzungen beachten | 43 |
| 1.4.2 Weniger Updates pro Jahr mit Windows 11 | 43 |
| 1.4.3 Neuerungen in Windows 11 | 44 |
| 1.4.4 Windows 11 und Microsoft 365 | 44 |
| 1.5 Zusammenfassung | 45 |
| Kapitel 2 Installation und Grundeinrichtung | 47 |
| 2.1 Grundlagen zur Installation | 47 |
| 2.1.1 Windows Server 2022-Installation verstehen | 48 |
| 2.1.2 Installation von Windows Server 2022 vorbereiten | 49 |
| 2.2 Windows Server 2022 neu installieren | 50 |
| 2.2.1 Windows Server 2022-Installation durchführen | 50 |
| 2.2.2 USB-Stick für Windows Server 2022 erstellen | 55 |
| 2.3 Zu Windows Server 2022 aktualisieren | 56 |
| 2.3.1 Aktualisierung zu Windows Server 2022 durchführen | 57 |
| 2.3.2 Upgrade von Standard- und Testversion auf Datacenter-Edition | 59 |
| 2.4 Nacharbeiten zur Installation von Windows Server 2022 | 60 |
| 2.4.1 Windows Server 2022 aktivieren | 60 |
| 2.4.2 Treiberinstallation überprüfen | 61 |
| 2.4.3 Netzwerkverbindung testen | 62 |
| 2.4.4 Windows Update aktivieren | 62 |
| 2.4.5 Sprachpakete installieren | 63 |
| 2.4.6 Media Player deaktivieren | 64 |
| 2.4.7 Computernamen und Domänenmitgliedschaft festlegen | 65 |

| | | |
|------------------|--|------------|
| 2.4.8 | Aktivieren von Remotedesktop | 66 |
| 2.4.9 | WLAN-Anbindung von Windows Server 2022 | 68 |
| 2.4.10 | Boot-Manager reparieren | 68 |
| 2.5 | Zusammenfassung | 69 |
| Kapitel 3 | Erste Schritte mit Windows Server 2022 | 71 |
| 3.1 | Erste Schritte nach der Installation | 71 |
| 3.1.1 | Windows Server 2022 mit Windows 10/11 verwalten | 71 |
| 3.2 | Core-Server verwalten | 76 |
| 3.2.1 | Hardware und Treiber auf Core-Servern installieren | 79 |
| 3.2.2 | Windows Updates auf Core-Servern steuern | 80 |
| 3.3 | Erweiterte Startoptionen nutzen | 80 |
| 3.3.1 | Starten der automatischen Reparatur von Windows Server 2022 | 81 |
| 3.3.2 | Windows Server 2022 im abgesicherten Modus starten | 81 |
| 3.3.3 | Abgesicherter Modus über msconfig.exe | 82 |
| 3.3.4 | Abgesicherter Modus in das Bootmenü einbinden | 82 |
| 3.3.5 | Abgesicherter Modus über automatische Reparatur starten | 83 |
| 3.4 | Remote-Management aktivieren | 84 |
| 3.5 | Windows Admin Center in der Praxis | 84 |
| 3.5.1 | Admin Center Gateway installieren und aktualisieren | 85 |
| 3.5.2 | Verbindungsaufbau zu Servern herstellen | 87 |
| 3.5.3 | Fehler bei der Verbindung beheben | 88 |
| 3.5.4 | Server im Windows Admin Center verwalten | 89 |
| 3.5.5 | Mit Markierungen arbeiten und Objekte suchen | 91 |
| 3.5.6 | Datei-Explorer, Registry-Editor, PowerShell und Remotedesktop nutzen | 92 |
| 3.5.7 | Gatewayzugriff steuern | 92 |
| 3.5.8 | Zertifikat für das Windows Admin Center steuern | 93 |
| 3.5.9 | Erweiterungen für das Windows Admin Center | 93 |
| 3.5.10 | Windows Admin Center und Microsoft Azure | 94 |
| 3.5.11 | Windows Server 2022 mit Windows Admin Center überwachen | 97 |
| 3.5.12 | Performance Monitor im Windows Admin Center | 98 |
| 3.5.13 | Hyper-V mit dem Windows Admin Center verwalten | 99 |
| 3.6 | Zusammenfassung | 101 |
| Kapitel 4 | Serverrollen und Features installieren und einrichten | 103 |
| 4.1 | Installieren von Serverrollen und Features auf einem Server | 104 |
| 4.1.1 | Rollen installieren | 104 |
| 4.1.2 | Features installieren und verwalten | 111 |
| 4.1.3 | Installation von Rollen und Features abschließen | 118 |
| 4.2 | Rollen in der PowerShell installieren | 119 |
| 4.2.1 | Serverrollen und Features in der PowerShell verwalten | 119 |
| 4.2.2 | Unbeaufsichtigte Installation von Rollen und Features | 120 |
| 4.3 | Rollen und Features mit DISM installieren | 120 |
| 4.3.1 | Webserver mit Dism.exe remote verwalten und Serverrollen auf Core-Servern installieren | 120 |
| 4.4 | Serverrollen mit dem Best Practices Analyzer überprüfen | 121 |
| 4.4.1 | Überprüfen von Servern über das Netzwerk | 122 |
| 4.4.2 | BPA in der PowerShell starten | 123 |
| 4.4.3 | Ergebnisse exportieren | 125 |
| 4.4.4 | BPA für Hyper-V nutzen | 126 |
| 4.4.5 | BPA auswerten | 126 |
| 4.5 | Zusammenfassung | 127 |

Teil II Einrichtung des Servers

| | | |
|------------------|---|------------|
| Kapitel 5 | Datenträger und Speicherpools verwalten | 131 |
| 5.1 | Wichtige Funktionen im Storage-Bereich | 131 |
| 5.1.1 | Storage Spaces Direct und Storage Replica | 132 |
| 5.1.2 | Datendeduplizierung erweitert | 132 |
| 5.1.3 | ReFS und Speicherpools | 133 |
| 5.2 | Datenträger erstellen und anpassen | 136 |
| 5.2.1 | Einrichten von Datenträgern | 137 |
| 5.2.2 | Konfigurieren von Laufwerken | 139 |
| 5.2.3 | Komprimieren von Datenträgern und Ordnern | 141 |
| 5.2.4 | Festplattenverwaltung in der PowerShell und Eingabeaufforderung | 142 |
| 5.2.5 | Mit GPT-Partitionen und ReFS arbeiten | 144 |
| 5.2.6 | Verkleinern und Erweitern von Datenträgern | 145 |
| 5.2.7 | Software-RAIDs in Windows Server nutzen | 147 |
| 5.3 | Verwalten von Datenträgern | 148 |
| 5.3.1 | Defragmentierung verwalten | 149 |
| 5.3.2 | Hardware und Richtlinie von Datenträgern verwalten | 149 |
| 5.4 | BitLocker-Laufwerkverschlüsselung | 151 |
| 5.4.1 | Grundlagen zu BitLocker und Trusted Platform Module (TPM) | 152 |
| 5.4.2 | BitLocker schnell und einfach aktivieren | 153 |
| 5.4.3 | Troubleshooting für BitLocker | 156 |
| 5.4.4 | Verschlüsselndes Dateisystem (EFS) – Daten einfach absichern | 156 |
| 5.5 | Speicherpools einsetzen | 159 |
| 5.5.1 | Speicherpools erstellen | 159 |
| 5.5.2 | Speicherplätze in Speicherpools erstellen | 160 |
| 5.5.3 | Volumes auf virtuellen Datenträgern in Speicherpools erstellen | 163 |
| 5.5.4 | Speicherpools verwalten und physische Festplatten hinzufügen | 164 |
| 5.5.5 | Virtuelle und physische Datenträger verwalten, trennen und löschen | 165 |
| 5.5.6 | Speicherpools und virtuelle Festplatten mit PowerShell verwalten | 165 |
| 5.5.7 | Erstellen eines Storage Spaces mit SSD-/NVMe-Festplatten | 167 |
| 5.6 | Verwenden von Schattenkopien | 169 |
| 5.7 | Erstellen und Verwalten von virtuellen Festplatten | 171 |
| 5.7.1 | Virtuelle Festplatten in der Datenträgerverwaltung erstellen | 171 |
| 5.7.2 | VHD(X)-Festplatten konvertieren und in der PowerShell verwalten | 172 |
| 5.7.3 | VHD-Dateien in den Boot-Manager einbinden | 173 |
| 5.7.4 | iSCSI-Ziele über virtuelle Festplatten zur Verfügung stellen | 174 |
| 5.7.5 | iSCSI-Ziele sicher zur Verfügung stellen | 176 |
| 5.7.6 | iSCSI-Festplatten verbinden | 177 |
| 5.8 | Datendeduplizierung einrichten | 178 |
| 5.8.1 | Einstieg in die Deduplizierung | 178 |
| 5.8.2 | Datendeduplizierung im Server-Manager | 179 |
| 5.9 | Speicher-Replikation – Daten in Netzwerken replizieren | 180 |
| 5.9.1 | Storage Replica verstehen | 180 |
| 5.9.2 | Ablauf der Replikation | 181 |
| 5.9.3 | Storage Replica in der Praxis | 181 |
| 5.9.4 | Storage Replica auf alleinstehenden Servern in der PowerShell steuern | 182 |
| 5.9.5 | Storage Spaces Direct und Storage Replica | 183 |
| 5.10 | Zusammenfassung | 184 |

| | | |
|------------------|---|------------|
| Kapitel 6 | Windows Server 2022 im Netzwerk betreiben | 185 |
| 6.1 | Grundlagen zur Netzwerkanbindung | 185 |
| 6.1.1 | Installation der Netzwerkhardware | 186 |
| 6.1.2 | Anbindung des Computers an das Netzwerk | 186 |
| 6.1.3 | Erweiterte Verwaltung der Netzwerkverbindungen | 187 |
| 6.1.4 | Eigenschaften von Netzwerkverbindungen und ihre erweiterte Verwaltung | 188 |
| 6.1.5 | DNS über HTTPS – DoH | 189 |
| 6.2 | Netzwerkkarten zusammenfassen – NIC-Teaming | 190 |
| 6.2.1 | NIC-Team erstellen | 191 |
| 6.2.2 | NIC-Teams auf Core-Server und in der PowerShell | 193 |
| 6.2.3 | NIC-Teams testen und konfigurieren | 193 |
| 6.2.4 | Eigenschaften von TCP/IP und DHCP | 194 |
| 6.3 | Erweiterte Netzwerkeinstellungen – Routing und IPv6 | 198 |
| 6.3.1 | IP-Routing unter Windows Server 2022 | 198 |
| 6.3.2 | Routen verfolgen in der Eingabeaufforderung – Pathping und Tracert | 199 |
| 6.3.3 | Internetprotokoll Version 6 – IPv6 | 200 |
| 6.4 | Mit der PowerShell Netzwerkprobleme lösen | 204 |
| 6.4.1 | Get-NetIPAddress und Get-NetIPConfiguration | 204 |
| 6.4.2 | Test-NetConnection: Routen nachverfolgen und Verbindungen überprüfen | 204 |
| 6.4.3 | Get-NetTCPConnection: Ports und TCP-Verbindungen testen | 205 |
| 6.4.4 | Get-NetFirewallRule: Windows-Firewallregeln überwachen | 206 |
| 6.5 | Windows Server 2022 Active Directory | 206 |
| 6.5.1 | Netzwerkeinstellungen für die Domänenaufnahme konfigurieren | 206 |
| 6.5.2 | Domänenaufnahme durchführen | 207 |
| 6.5.3 | Domänenaufnahme testen | 207 |
| 6.6 | Zusammenfassung | 211 |

Teil III Virtualisierung mit Hyper-V

| | | |
|------------------|--|------------|
| Kapitel 7 | Hyper-V – Installation und Server virtualisieren | 215 |
| 7.1 | Neuerungen in der Virtualisierung | 215 |
| 7.1.1 | Neue VM-Version 10 in Windows Server 2022 und Windows 11 | 216 |
| 7.1.2 | Hardware-Neuerungen in Windows Server 2022 und Windows 11 | 216 |
| 7.1.3 | Neuerungen bei Hyper-V-Switches | 216 |
| 7.1.4 | Microsoft sieht den Schwerpunkt von Hyper-V in Azure Stack HCI | 217 |
| 7.2 | So funktioniert Hyper-V | 218 |
| 7.2.1 | Grundlagen von Hyper-V | 218 |
| 7.2.2 | Optimale Hochverfügbarkeit | 219 |
| 7.2.3 | Sicherheit und Bandbreitenverwaltung | 220 |
| 7.2.4 | Schnellerer Datenfluss in Rechenzentren mit SAN | 222 |
| 7.2.5 | Weitere wichtige Funktionen in Hyper-V | 222 |
| 7.2.6 | Speicherorte in Hyper-V | 223 |
| 7.3 | Windows Server Virtual Machine Licensing | 224 |
| 7.3.1 | Vertriebskanäle für Windows-Server verstehen | 224 |
| 7.3.2 | Edition von Windows Server 2022 beachten | 224 |
| 7.3.3 | Container nutzen und richtig lizenzieren | 225 |
| 7.3.4 | Virtual Desktop Access und Companion Subscription License | 225 |
| 7.3.5 | Hyper-V in Windows Server 2022 nutzen | 226 |
| 7.4 | Hyper-V installieren und verwalten | 228 |
| 7.4.1 | Voraussetzungen für den Einsatz von Hyper-V | 228 |
| 7.4.2 | Hyper-V installieren | 229 |

| | | |
|------------------|---|------------|
| 7.4.3 | Erste Schritte mit Hyper-V | 231 |
| 7.4.4 | CPU-Last überwachen und Daten zu VMs anzeigen | 231 |
| 7.5 | Virtuelle Switches in Windows Server 2022 | 232 |
| 7.5.1 | Network Virtualization und Extensible Switch mit Windows Server 2022 | 233 |
| 7.5.2 | Hyper-V-Netzwerke planen | 234 |
| 7.5.3 | Erstellen und Konfigurieren von virtuellen Switches | 237 |
| 7.5.4 | MAC-Adressen für Hyper-V konfigurieren | 238 |
| 7.5.5 | Virtuelle LANs (VLAN) und Hyper-V | 239 |
| 7.5.6 | Switch Embedded Teaming – NIC-Teams für Hyper-V | 241 |
| 7.5.7 | NAT in Hyper-V konfigurieren | 242 |
| 7.6 | Virtuelle Server erstellen und installieren | 243 |
| 7.6.1 | IDE oder SCSI – Welcher virtuelle Controller ist besser? | 243 |
| 7.6.2 | Laufwerke mit der PowerShell hinzufügen | 244 |
| 7.6.3 | Virtualisierung von Domänencontrollern | 245 |
| 7.6.4 | Per Hyper-V-Manager virtuelle Maschinen erstellen | 248 |
| 7.6.5 | Virtuelle Server steuern | 251 |
| 7.7 | Einstellungen von virtuellen Servern anpassen | 253 |
| 7.7.1 | Hardware zu virtuellen Computern hinzufügen | 254 |
| 7.7.2 | Virtuelle Festplatten zu Servern hinzufügen | 255 |
| 7.7.3 | Speicher-Migration – Virtuelle Festplatten verschieben | 257 |
| 7.7.4 | USB-Festplatten an Hyper-V anbinden | 259 |
| 7.7.5 | Virtuelle Festplatten von Servern verwalten und optimieren | 260 |
| 7.7.6 | Dynamic Memory – Arbeitsspeicher anpassen | 260 |
| 7.7.7 | Prozessoren in Hyper-V steuern | 262 |
| 7.7.8 | Allgemeine Einstellungen von virtuellen Computern verwalten | 263 |
| 7.7.9 | Virtuelle Server in der PowerShell steuern – PowerShell Direct nutzen | 264 |
| 7.7.10 | Daten von virtuellen Servern aus Hyper-V auslesen | 265 |
| 7.8 | Hyper-V-Host absichern | 267 |
| 7.8.1 | Updates installieren und Lücken schließen | 268 |
| 7.8.2 | Sicherheitsempfehlungen von Microsoft mit Richtlinien absichern | 268 |
| 7.8.3 | BPA für Hyper-V nutzen | 268 |
| 7.8.4 | Sichere virtuelle Maschinen mit Secure Boot | 269 |
| 7.9 | Migration zu Hyper-V | 270 |
| 7.9.1 | VM in Windows Server 2022 integrieren | 270 |
| 7.9.2 | Windows Server-Migrationstools nutzen | 270 |
| 7.9.3 | Neue VM-Version mit der PowerShell steuern | 272 |
| 7.9.4 | Eingebettete Virtualisierung in Windows Server 2022 | 273 |
| 7.9.5 | Festplattendateien migrieren | 274 |
| 7.10 | Zusammenfassung | 275 |
| Kapitel 8 | Hyper-V – Datensicherung und Wiederherstellung | 277 |
| 8.1 | Hyper-V und virtuelle Server richtig sichern | 277 |
| 8.2 | Prüfpunkte von virtuellen Servern erstellen | 278 |
| 8.2.1 | Produktionsprüfpunkte in Windows Server 2022 nutzen | 279 |
| 8.2.2 | Prüfpunkte verstehen | 280 |
| 8.2.3 | Produktionsprüfpunkte erstellen | 282 |
| 8.2.4 | Snapshots von virtuellen Servern erstellen | 283 |
| 8.2.5 | Verwalten der Snapshots von virtuellen Servern | 285 |
| 8.2.6 | Datensicherung und Snapshots bei Hyper-V im Cluster | 286 |
| 8.3 | Sicherung durch Export | 287 |
| 8.4 | VMs per Skript sichern | 289 |
| 8.4.1 | Snapshots erstellen in Hyper-V mit »Checkpoint-VM« | 289 |

| | | |
|-------------------|---|------------|
| 8.5 | Shielded VMs und Host Guardian Service | 290 |
| 8.5.1 | Verschlüsselung ohne Shielded VMs durchführen | 291 |
| 8.5.2 | Sichere VMs mit Shielded VMs | 292 |
| 8.5.3 | Verbindung zwischen Host Guardian Service und Guarded Hosts | 293 |
| 8.5.4 | Host Guardian Service konfigurieren | 293 |
| 8.5.5 | Vertrauensstellung zwischen Host Guardian Service und Active Directory einrichten | 294 |
| 8.5.6 | Guarded Hyper-V-Hosts mit HGS verbinden | 295 |
| 8.5.7 | Shielded VMs erstellen | 296 |
| 8.6 | Virtuelle Server gruppieren | 297 |
| 8.7 | Zusammenfassung | 298 |
| Kapitel 9 | Hyper-V – Hochverfügbarkeit | 299 |
| 9.1 | Einstieg in die Hochverfügbarkeit in Hyper-V | 300 |
| 9.1.1 | Hyper-V-Replikation und Cluster | 300 |
| 9.1.2 | Arten der Hochverfügbarkeit in Hyper-V | 302 |
| 9.2 | Hyper-V-Replikation in der Praxis | 302 |
| 9.2.1 | Hyper-V-Hosts für Replikation aktivieren | 303 |
| 9.2.2 | Hyper-V-Replikation mit SSL konfigurieren | 304 |
| 9.2.3 | Virtuelle Server zwischen Hyper-V-Hosts replizieren | 305 |
| 9.2.4 | Failover mit Hyper-V-Replica durchführen | 308 |
| 9.3 | Livemigration ohne Cluster | 309 |
| 9.4 | Hyper-V im Cluster – Livemigration in der Praxis | 313 |
| 9.4.1 | Clusterknoten vorbereiten | 314 |
| 9.4.2 | Cluster mit Windows Server 2022 installieren | 314 |
| 9.4.3 | Cluster Shared Volumes aktivieren | 317 |
| 9.4.4 | Virtuelle Server im Cluster verwalten | 322 |
| 9.4.5 | MAC-Adressen im Cluster konfigurieren | 323 |
| 9.4.6 | Nacharbeiten: Überprüfung des Clusters und erste Schritte mit der Clusterverwaltung oder der PowerShell | 323 |
| 9.5 | Zusammenfassung | 325 |
| Teil IV | Active Directory | |
| Kapitel 10 | Active Directory – Grundlagen und erste Schritte | 329 |
| 10.1 | Einstieg in Active Directory | 329 |
| 10.1.1 | Active Directory im Detail | 329 |
| 10.1.2 | Active Directory-Systemrollen nutzen | 330 |
| 10.1.3 | Active Directory mit dem Verwaltungscenter verwalten | 331 |
| 10.1.4 | Active Directory für Einsteiger | 333 |
| 10.1.5 | PowerShell und Active Directory | 335 |
| 10.1.6 | Migration zu Active Directory mit Windows Server 2022 | 335 |
| 10.1.7 | Sicheres DNS-System in Windows Server 2022 | 336 |
| 10.1.8 | Active Directory remote verwalten | 336 |
| 10.2 | Active Directory mit Windows Server 2022 installieren und verstehen | 337 |
| 10.2.1 | Aufbau von Active Directory | 337 |
| 10.2.2 | Installieren einer neuen Gesamtstruktur | 339 |
| 10.3 | Active Directory remote mit der PowerShell verwalten | 344 |
| 10.3.1 | Remote-PowerShell aktivieren und Verbindungsprobleme beheben | 344 |
| 10.3.2 | Cmdlets für die Remoteverwaltung und Abrufen der Hilfe | 345 |

| | | |
|-------------------|--|------------|
| 10.4 | Verwalten der Betriebsmasterrollen von Domänencontrollern | 346 |
| 10.4.1 | PDC-Emulator verwalten | 347 |
| 10.4.2 | RID-Master – Neue Objekte in der Domäne aufnehmen | 348 |
| 10.4.3 | Infrastrukturmaster – Auflösen von Gruppen über Domänen hinweg | 349 |
| 10.4.4 | Schemamaster – Active Directory erweitern | 349 |
| 10.4.5 | Domänennamenmaster – Neue Domänen hinzufügen | 350 |
| 10.4.6 | Der globale Katalog | 350 |
| 10.4.7 | Verwaltung und Verteilung der Betriebsmaster | 353 |
| 10.5 | Schreibgeschützte Domänencontroller (RODC) | 357 |
| 10.6 | Zusammenfassung | 359 |
| Kapitel 11 | Active Directory – Installation und Betrieb | 361 |
| 11.1 | DNS für Active Directory installieren | 362 |
| 11.1.1 | Erstellen der notwendigen DNS-Zonen für Active Directory | 362 |
| 11.1.2 | Überprüfung und Fehlerbehebung der DNS-Einstellungen | 365 |
| 11.2 | Installation der Active Directory-Domänendienste-Rolle | 366 |
| 11.2.1 | Test der Voraussetzungen zum Betrieb von Active Directory | 367 |
| 11.2.2 | Starten der Installation von Active Directory | 368 |
| 11.2.3 | DNS in Active Directory integrieren und sichere Updates konfigurieren | 371 |
| 11.2.4 | DNS-IP-Einstellungen anpassen | 373 |
| 11.3 | Active Directory von Installationsmedium installieren | 374 |
| 11.3.1 | Vorbereiten des Active Directory-Installationsmediums | 374 |
| 11.3.2 | Domänencontroller mit Medium installieren | 374 |
| 11.4 | Active Directory mit PowerShell installieren | 375 |
| 11.5 | Virtuelle Domänencontroller betreiben – Klonen und Snapshots | 377 |
| 11.5.1 | Möglichkeiten zur Virtualisierung von Domänencontrollern | 378 |
| 11.5.2 | Bereitstellung virtueller Domänencontroller vorbereiten – XML-Dateien erstellen | 379 |
| 11.5.3 | Quelldomänencontroller vor dem Klonen überprüfen und vorbereiten | 380 |
| 11.5.4 | Festplatten von virtuellen Domänencontrollern kopieren | 381 |
| 11.5.5 | Geklonten Domänencontroller für die Aufnahme in Active Directory vorbereiten | 381 |
| 11.6 | Domänencontroller entfernen | 382 |
| 11.6.1 | Herabstufen eines Domänencontrollers in der PowerShell | 383 |
| 11.6.2 | Entfernen von Active Directory über den Server-Manager | 383 |
| 11.7 | Migration zu Windows Server 2022-Active Directory | 384 |
| 11.7.1 | Domänen zu Windows Server 2022 aktualisieren | 384 |
| 11.8 | Das Active Directory-Verwaltungszentrum und PowerShell | 384 |
| 11.8.1 | Active Directory und die PowerShell | 387 |
| 11.8.2 | Objekte schützen und wiederherstellen | 388 |
| 11.8.3 | Andere Objekte schützen – Active Directory-Standorte und -Dienste | 389 |
| 11.8.4 | Löschsicherheit in der PowerShell abfragen und setzen | 389 |
| 11.9 | Sicherheit in LDAP für Domänencontroller nutzen | 390 |
| 11.9.1 | Microsoft empfiehlt die Aktivierung von LDAPS | 390 |
| 11.9.2 | Probleme nach Aktivierung von LDAPS erkennen | 391 |
| 11.9.3 | LDAP-Signierung und LDAP Channel Binding für mehr Sicherheit in Active Directory | 391 |
| 11.9.4 | LDAP over SSL in Active Directory nutzen | 393 |
| 11.9.5 | LDAPS zusammen mit LDAP-Signatur und LDAP Channel Binding einsetzen | 395 |
| 11.9.6 | LDAP-Prioritäten und -Gewichtung konfigurieren – DCs entlasten | 395 |

| | | |
|-------------------|--|------------|
| 11.10 | Zeitsynchronisierung in Windows-Netzwerken | 396 |
| 11.10.1 | Grundlagen zur Zeitsynchronisierung in Active Directory | 396 |
| 11.10.2 | Das NTP-Protokoll und Befehle zur Zeitsynchronisierung | 398 |
| 11.10.3 | Net Time versus W32tm | 400 |
| 11.10.4 | Funkuhr versus Internetzeit – Zeitsynchronisierung konfigurieren | 400 |
| 11.10.5 | Zeitsynchronisierung bei der Virtualisierung beachten | 402 |
| 11.11 | Zusammenfassung | 402 |
| Kapitel 12 | Active Directory – Erweitern und Absichern | 403 |
| 12.1 | Offline-Domänenbeitritt – Djoin | 403 |
| 12.1.1 | Vorteile und technische Hintergründe zum Offline-Domänenbeitritt | 403 |
| 12.1.2 | Voraussetzungen für die Verwendung des Offline-Domänenbeitritts | 404 |
| 12.1.3 | Durchführen des Offline-Domänenbeitritts | 404 |
| 12.1.4 | Offline-Domänenbeitritt bei einer unbeaufsichtigten Installation über Antwortdatei | 405 |
| 12.1.5 | DirectAccess Offline Domain Join | 406 |
| 12.2 | Verwaltete Dienstkonten – Managed Service Accounts | 407 |
| 12.2.1 | Verwaltete Dienstkonten – Technische Hintergründe | 407 |
| 12.2.2 | Verwaltete Dienstkonten – Produktiver Einsatz | 408 |
| 12.2.3 | Verwaltete Dienstkonten in der grafischen Oberfläche anlegen | 409 |
| 12.3 | Der Active Directory-Papierkorb im Praxiseinsatz | 411 |
| 12.3.1 | Active Directory-Papierkorb verstehen und aktivieren | 411 |
| 12.3.2 | Objekte aus dem AD-Papierkorb mit Bordmitteln wiederherstellen | 412 |
| 12.3.3 | Organisationseinheiten und Objekte in AD absichern und sichern | 414 |
| 12.3.4 | Erweiterte Optionen für Organisationseinheiten einblenden | 415 |
| 12.4 | Unternehmensübergreifendes Identity Management | 417 |
| 12.5 | Azure AD Connect für Synchronisierung mit Azure nutzen | 418 |
| 12.5.1 | Azure AD Connect einrichten | 418 |
| 12.5.2 | Azure AD Connect konfigurieren | 419 |
| 12.5.3 | Troubleshooting von Azure AD und Verbindungen zu Azure | 419 |
| 12.5.4 | Azure AD Connect und Azure AD Connect Cloud Sync | 421 |
| 12.6 | Zusammenfassung | 423 |
| Kapitel 13 | Active Directory – Neue Domänen und Domänencontroller | 425 |
| 13.1 | Core-Server als zusätzlichen Domänencontroller betreiben | 425 |
| 13.1.1 | Vorbereitungen in der PowerShell durchführen | 426 |
| 13.1.2 | Active Directory auf dem Core-Server installieren und einrichten | 427 |
| 13.2 | Schreibgeschützter Domänencontroller (RODC) | 428 |
| 13.2.1 | Vorbereitungen für die Integration eines zusätzlichen Domänencontrollers in eine Domäne | 428 |
| 13.2.2 | Einstieg in schreibgeschützte Domänencontroller – RODC | 429 |
| 13.2.3 | Integration eines neuen Domänencontrollers | 429 |
| 13.2.4 | Delegierung der RODC-Installation | 433 |
| 13.2.5 | Kennwortreplikationsrichtlinien auf RODCs steuern | 434 |
| 13.2.6 | RODC löschen | 435 |
| 13.2.7 | Notwendige Nacharbeiten nach der Integration eines zusätzlichen Domänencontrollers | 435 |
| 13.3 | Erstellen einer neuen untergeordneten Domäne | 437 |
| 13.3.1 | Anpassen der DNS-Infrastruktur an untergeordnete Domänen | 437 |
| 13.3.2 | Heraufstufen eines Domänencontrollers für eine neue untergeordnete Domäne .. | 443 |

| | | |
|-------------------|---|------------|
| 13.4 | Einführen einer neuen Domänenstruktur in einer Gesamtstruktur | 444 |
| 13.4.1 | Erstellen der DNS-Infrastruktur für eine neue Domänenstruktur | 445 |
| 13.4.2 | Optimieren der IP-Einstellungen beim Einsatz von mehreren Domänen | 445 |
| 13.4.3 | Erstellen der neuen Domänenstruktur | 446 |
| 13.5 | Das Active Directory-Schema erweitern | 447 |
| 13.6 | Zusammenfassung | 448 |
| Kapitel 14 | Active Directory – Replikation | 449 |
| 14.1 | Grundlagen zur Replikation | 449 |
| 14.2 | Konfiguration der Routingtopologie in Active Directory | 451 |
| 14.2.1 | Erstellen von neuen Standorten über Active Directory-Standorte und -Dienste ... | 452 |
| 14.2.2 | Erstellen und Zuweisen von IP-Subnetzen | 454 |
| 14.2.3 | Erstellen von Standortverknüpfungen und Standortverknüpfungsbrücken | 455 |
| 14.2.4 | Zuweisen der Domänencontroller zu den Standorten | 457 |
| 14.2.5 | Die Konsistenzprüfung (Knowledge Consistency Checker) | 457 |
| 14.3 | Fehler bei der Active Directory-Replikation beheben | 460 |
| 14.3.1 | Suche mit der Active Directory-Diagnose | 460 |
| 14.3.2 | Ausschließen der häufigsten Fehlerursachen | 460 |
| 14.3.3 | Nltest zum Erkennen von Standortzuweisungen eines Domänencontrollers | 461 |
| 14.3.4 | Repadmin zum Anzeigen der Active Directory-Replikation | 461 |
| 14.3.5 | Replikation in der PowerShell testen | 463 |
| 14.3.6 | Netzwerkverbindungen zwischen DCs überprüfen | 464 |
| 14.3.7 | Secure Channel überprüfen – Test-ComputerSecureChannel | 464 |
| 14.3.8 | Kerberos-Test mit Dcdiag ausführen | 465 |
| 14.3.9 | Überprüfung der notwendigen SRV-Records im DNS unter <i>_msdcs</i> | 465 |
| 14.4 | Zusammenfassung | 465 |
| Kapitel 15 | Active Directory – Fehlerbehebung und Diagnose | 467 |
| 15.1 | Bordmittel zur Diagnose verwenden | 468 |
| 15.1.1 | Schneller Überblick zu Domänen und Gesamtstrukturen in der PowerShell – inklusive Betriebsmaster | 468 |
| 15.1.2 | Informationen aus Active Directory mit der PowerShell auslesen | 469 |
| 15.1.3 | Daten zu Computer und Benutzerkonten anzeigen | 469 |
| 15.1.4 | Microsoft Active Directory Documentation Script | 470 |
| 15.1.5 | Verwenden der Domänencontrollerdiagnose | 471 |
| 15.1.6 | Testen der Namensauflösung mit Nslookup | 472 |
| 15.1.7 | Standard-OU's per Active Directory-Benutzer und -Computer überprüfen | 475 |
| 15.1.8 | Überprüfen der Active Directory-Standorte | 475 |
| 15.1.9 | Überprüfen der Domänencontrollerliste | 476 |
| 15.1.10 | Überprüfen der Active Directory-Dateien | 476 |
| 15.1.11 | Domänenkonto der Domänencontroller überprüfen und Kennwort zurücksetzen | 477 |
| 15.1.12 | Überprüfen der administrativen Freigaben | 478 |
| 15.1.13 | Überprüfen der Gruppenrichtlinien | 478 |
| 15.1.14 | DNS-Einträge von Active Directory überprüfen | 479 |
| 15.1.15 | Testen der Betriebsmaster | 481 |
| 15.1.16 | Leistungsüberwachung zur Diagnose nutzen | 481 |
| 15.1.17 | LDAP-Zugriff auf Domänencontrollern überwachen | 483 |
| 15.1.18 | Zurücksetzen des Kennworts für den Wiederherstellungsmodus in Active Directory | 483 |
| 15.2 | Konfiguration der Ereignisprotokollierung von Active Directory | 483 |

| | | |
|-------------------|--|------------|
| 15.3 | Einbrüche in Active Directory effizient erkennen | 484 |
| 15.3.1 | Aktivieren der einfachen Überwachung | 485 |
| 15.3.2 | Erweiterte Überwachung nutzen | 486 |
| 15.3.3 | Anmeldungen im Netzwerk überwachen | 488 |
| 15.3.4 | Mit Tools für mehr Sicherheit sorgen | 488 |
| 15.4 | Computerkonten in Active Directory verwalten und reparieren | 490 |
| 15.4.1 | Computerkonten in Active Directory-Benutzer und -Computer verwalten | 491 |
| 15.4.2 | Fehlerbehebung von Computerkonten | 491 |
| 15.4.3 | Veraltete Computer finden und bei Bedarf entfernen | 492 |
| 15.5 | Bereinigung von Active Directory und Entfernen von Domänencontrollern | 493 |
| 15.5.1 | Vorbereitungen beim Entfernen eines Domänencontrollers | 493 |
| 15.5.2 | Herabstufen eines Domänencontrollers | 494 |
| 15.5.3 | Bereinigen der Metadaten von Active Directory | 495 |
| 15.6 | Zusammenfassung | 496 |
| Kapitel 16 | Active Directory – Sicherung, Wiederherstellung und Wartung | 497 |
| 16.1 | Active Directory sichern und wiederherstellen | 498 |
| 16.1.1 | Active Directory mit der Windows Server-Sicherung sichern | 498 |
| 16.1.2 | Wiederherstellen von Active Directory aus der Datensicherung | 499 |
| 16.2 | Active Directory-Datenbank warten | 501 |
| 16.2.1 | Verschieben der Active Directory-Datenbank | 501 |
| 16.2.2 | Offlinedefragmentation der Active Directory-Datenbank | 502 |
| 16.2.3 | Reparieren der Active Directory-Datenbank | 503 |
| 16.2.4 | Erstellen von Snapshots der Active Directory-Datenbank | 503 |
| 16.3 | Zusammenfassung | 504 |
| Kapitel 17 | Active Directory – Vertrauensstellungen | 505 |
| 17.1 | Wichtige Grundlagen zu Vertrauensstellungen in Active Directory | 505 |
| 17.2 | Varianten der Vertrauensstellungen in Active Directory | 508 |
| 17.3 | Einrichtung einer Vertrauensstellung | 509 |
| 17.3.1 | Fehler mit Vertrauensstellungen von Computern zur Domäne beheben | 512 |
| 17.4 | Automatisch aktivierte SID-Filterung | 512 |
| 17.5 | Zusammenfassung | 513 |
| Kapitel 18 | Benutzerverwaltung und Profile | 515 |
| 18.1 | Grundlagen zur Verwaltung von Benutzern | 515 |
| 18.1.1 | Active Directory-Benutzerverwaltung | 517 |
| 18.1.2 | Benutzerkonten in der PowerShell anlegen, verwalten und löschen | 519 |
| 18.1.3 | Verwalten von Benutzerkonten | 520 |
| 18.1.4 | Benutzerverwaltung für Remotedesktopbenutzer | 523 |
| 18.2 | Benutzerprofile nutzen | 524 |
| 18.2.1 | Benutzerprofile lokal und im Profieinsatz verstehen | 524 |
| 18.2.2 | Servergespeicherte Profile für Benutzer in Active Directory festlegen | 526 |
| 18.2.3 | Anmelde- und Abmeldeskripts für Benutzer und Computer | 532 |
| 18.3 | Gruppen verwalten | 534 |
| 18.3.1 | Gruppen anlegen und verwenden | 534 |
| 18.3.2 | Berechtigungen für Benutzer und Gruppen verwalten | 536 |
| 18.3.3 | Szenario: Delegierung zum administrativen Verwalten einer Organisationseinheit | 538 |
| 18.4 | Zusammenfassung | 540 |

| | | |
|-------------------|---|------------|
| Kapitel 19 | Richtlinien im Windows Server 2022-Netzwerk | 541 |
| 19.1 | Erste Schritte mit Richtlinien | 541 |
| 19.1.1 | Verwaltungswerkzeuge für Gruppenrichtlinien | 542 |
| 19.1.2 | Wichtige Begriffe für Gruppenrichtlinien | 542 |
| 19.1.3 | Gruppenrichtlinien-Preferences effizient einsetzen | 544 |
| 19.1.4 | Registry-Einstellungen von Gruppenrichtlinien herausfinden | 547 |
| 19.1.5 | BSI bietet Hilfe bei der Absicherung von Windows | 547 |
| 19.1.6 | Windows 10/11 mit Microsoft-Sicherheitsempfehlungen konfigurieren | 549 |
| 19.2 | Gruppenrichtlinien verwalten | 553 |
| 19.2.1 | Neue Gruppenrichtlinie erstellen | 553 |
| 19.2.2 | GPO mit einem Container verknüpfen | 554 |
| 19.2.3 | Gruppenrichtlinien erzwingen und Priorität erhöhen | 556 |
| 19.2.4 | Vererbung für Gruppenrichtlinien deaktivieren | 557 |
| 19.2.5 | Administration von domänenbasierten GPOs mit ADMX-Dateien | 558 |
| 19.3 | Sicherheitseinstellungen in Windows 10/11 mit Richtlinien steuern | 560 |
| 19.3.1 | Microsoft Store, Cortana und Datensammlungen in Windows 10/11 sperren | 560 |
| 19.3.2 | Sicherheitseinstellungen für das Netzwerk steuern | 560 |
| 19.3.3 | Überwacher Ordnerzugriff – Schutz vor Ransomware | 561 |
| 19.3.4 | Datenschutz in Richtlinien steuern | 562 |
| 19.3.5 | Benutzer und Kennwörter mit Gruppenrichtlinien absichern | 563 |
| 19.3.6 | OneDrive for Business nutzen | 564 |
| 19.3.7 | Microsoft Application Guard und Office | 564 |
| 19.4 | Gruppenrichtlinien testen und Fehler beheben | 566 |
| 19.4.1 | Einstieg in die Fehlerbehebung von Gruppenrichtlinien | 566 |
| 19.4.2 | Vorgehensweise bei der Fehlerbehebung von Gruppenrichtlinien | 567 |
| 19.4.3 | Policy Analyzer zur Fehlerbehebung nutzen | 568 |
| 19.4.4 | Datensicherung und Wiederherstellung von Gruppenrichtlinien | 569 |
| 19.4.5 | Gruppenrichtlinien mit der PowerShell sichern und wiederherstellen | 572 |
| 19.4.6 | Gruppenrichtlinienmodellierung | 572 |
| 19.5 | Softwareverteilung über Gruppenrichtlinien | 573 |
| 19.6 | Geräteinstallation mit Gruppenrichtlinien konfigurieren | 574 |
| 19.6.1 | Geräteidentifikationsstring und Gerätesetupklasse | 575 |
| 19.6.2 | So funktioniert die Steuerungen in Geräteinstallationen über Gruppenrichtlinien | 577 |
| 19.6.3 | Konfiguration von Gruppenrichtlinien für den Zugriff auf Wechselmedien | 577 |
| 19.6.4 | Layered Group Policies – Mehrschichtige Gruppenrichtlinien nutzen | 577 |
| 19.6.5 | Konfiguration von Gruppenrichtlinien für den Zugriff auf Wechselmedien | 579 |
| 19.7 | Mit AppLocker Desktop- und Windows-Apps in Netzwerken steuern | 580 |
| 19.7.1 | AppLocker in Unternehmen nutzen | 580 |
| 19.7.2 | Gruppenrichtlinien für AppLocker erstellen | 580 |
| 19.7.3 | Erstellen von Regeln für AppLocker | 582 |
| 19.7.4 | Automatisches Erstellen von Regeln und Erzwingen von AppLocker | 583 |
| 19.7.5 | Windows 10/11 Device Guard zusammen mit AppLocker nutzen | 584 |
| 19.7.6 | Benutzerkontensteuerung über Richtlinien konfigurieren | 585 |
| 19.7.7 | Erstellen einer neuen Gruppenrichtlinie für sichere Kennwörter | 585 |
| 19.7.8 | Firewalleinstellungen über Gruppenrichtlinien setzen | 586 |
| 19.8 | Zusammenfassung | 586 |

Teil V Datei- und Druckserver mit Windows Server

| | |
|---|------------|
| Kapitel 20 Dateiserver und Daten im Netzwerk freigeben | 589 |
| 20.1 SMB 3.x in Windows Server 2022 nutzen | 589 |
| 20.1.1 Mehr Sicherheit und Leistung in SMB 3.x | 589 |
| 20.1.2 SMB 1.0 im Netzwerk ausfindig machen und deaktivieren | 591 |
| 20.2 Berechtigungen für Dateien und Ordner verwalten | 592 |
| 20.2.1 Erweiterte Berechtigungen auf Ordner | 593 |
| 20.2.2 Berechtigungen verstehen | 595 |
| 20.2.3 Effektive Berechtigungen | 597 |
| 20.2.4 Tools zur Überwachung von Berechtigungen | 598 |
| 20.3 Überwachung von Dateien und Ordnern | 604 |
| 20.3.1 Einstieg in die Überwachung von Verzeichnissen | 604 |
| 20.3.2 Überwachung mit Richtlinien steuern | 605 |
| 20.4 Die Freigabe von Ordnern | 605 |
| 20.4.1 Freigaben erstellen | 606 |
| 20.4.2 Der Assistent zum Erstellen von Freigaben | 607 |
| 20.4.3 Anzeigen geöffneter Dateien über das Netzwerk – PsFile | 607 |
| 20.4.4 Versteckte Freigaben | 608 |
| 20.4.5 Anzeigen aller Freigaben | 608 |
| 20.4.6 Auf Freigaben über das Netzwerk zugreifen | 609 |
| 20.4.7 Offlinedateien für den mobilen Einsatz unter Windows 10/11 | 610 |
| 20.5 Storage Quality of Services (QoS) – Richtlinien für Datenspeicher | 614 |
| 20.5.1 Einstieg in Speicherrichtlinien | 614 |
| 20.5.2 Storage QoS in der PowerShell verwalten | 616 |
| 20.5.3 Neue Richtlinien in der PowerShell erstellen und verwalten | 616 |
| 20.5.4 Aggregated Policies nutzen | 617 |
| 20.5.5 Storage QoS im Cluster überwachen | 618 |
| 20.5.6 Speicherrichtlinien in System Center Virtual Machine Manager | 619 |
| 20.6 Dateien und Freigaben auf Windows Server 2022 migrieren | 619 |
| 20.6.1 Daten mit Robocopy übernehmen | 619 |
| 20.6.2 Nur Freigaben und deren Rechte übernehmen | 623 |
| 20.6.3 Windows Server Storage Migration Service | 623 |
| 20.7 Azure File Sync und Azure Files – Lokale Daten mit der Cloud nutzen | 627 |
| 20.7.1 So funktioniert Azure File Sync | 627 |
| 20.7.2 Azure File Sync einrichten | 628 |
| 20.7.3 Azure-Dateifreigaben nutzen | 628 |
| 20.8 Zusammenfassung | 629 |
| | |
| Kapitel 21 Ressourcen-Manager für Dateiserver und DFS | 631 |
| 21.1 Kontingentverwaltung in Windows Server 2022 | 632 |
| 21.1.1 Kontingentverwaltung mit FSRM | 632 |
| 21.1.2 Datenträgerkontingente für Laufwerke festlegen | 636 |
| 21.2 Dateiprüfungsverwaltung nutzen | 637 |
| 21.2.1 Erstellen einer Dateiprüfung | 638 |
| 21.2.2 Dateiprüfungsausnahmen | 639 |
| 21.2.3 Dateigruppen für die Dateiprüfung | 640 |
| 21.3 Speicherberichtverwaltung in FSRM | 640 |
| 21.4 Dateiklassifizierungsdienste einsetzen | 641 |
| 21.4.1 Klassifizierungseigenschaften und Klassifizierungsregeln verstehen und einsetzen | 642 |
| 21.4.2 Dateiverwaltungsaufgaben bei der Dateiklassifizierung einsetzen | 643 |

| | | |
|-------------------|--|------------|
| 21.5 | So schützen Unternehmen ihre Dateiserver vor Ransomware | 644 |
| 21.5.1 | Allgemeine-Tipps für den Schutz vor Ransomware | 644 |
| 21.5.2 | Generelle Vorgehensweise beim Befall gegen Ransomware | 644 |
| 21.5.3 | Schattenkopien helfen bei Windows-Servern | 645 |
| 21.5.4 | Ressourcen-Manager für Dateiserver gegen Ransomware nutzen | 645 |
| 21.6 | Organisieren und Replizieren von Freigaben über DFS | 646 |
| 21.6.1 | Einführung und wichtige Informationen beim Einsatz von DFS | 646 |
| 21.6.2 | DFS-Namespaces und DFS-Replikation | 648 |
| 21.6.3 | Voraussetzungen für DFS | 650 |
| 21.6.4 | Installation und Einrichtung von DFS | 650 |
| 21.6.5 | Einrichtung eines DFS-Namespace | 651 |
| 21.6.6 | Einrichten der DFS-Replikation | 653 |
| 21.7 | Zusammenfassung | 654 |
| Kapitel 22 | BranchCache | 655 |
| 22.1 | BranchCache im Überblick – Niederlassungen effizient anbinden | 655 |
| 22.2 | Gehosteter Cache (Hosted Cache) nutzen | 657 |
| 22.3 | Verteilter Cache (Distributed Cache) nutzen | 660 |
| 22.4 | BranchCache auf dem Hosted-Cache-Server konfigurieren | 662 |
| 22.4.1 | Feature für Hosted Cache installieren | 662 |
| 22.4.2 | Zertifikate auf dem Hosted-Cache-Server betreiben | 663 |
| 22.4.3 | Einstellungen auf dem Hosted-Cache-Server anpassen | 663 |
| 22.4.4 | Content-Server konfigurieren | 664 |
| 22.5 | BranchCache auf Clients konfigurieren | 664 |
| 22.5.1 | Clientkonfiguration mit Gruppenrichtlinien konfigurieren | 665 |
| 22.5.2 | Firewalleinstellungen für BranchCache setzen | 665 |
| 22.6 | Leistungsüberwachung und BranchCache | 666 |
| 22.7 | Zusammenfassung | 667 |
| Kapitel 23 | Druckerserver betreiben | 669 |
| 23.1 | PrintNightmare beachten | 669 |
| 23.2 | Drucken im Netzwerk und mit Smartphones oder Tablets | 670 |
| 23.2.1 | Drucker in Windows freigeben | 671 |
| 23.2.2 | Drucker über WLAN anbinden | 672 |
| 23.2.3 | Eigenen Netzwerkanschluss konfigurieren | 673 |
| 23.2.4 | Drucken mit iPhone und iPad – AirPrint | 674 |
| 23.3 | Freigegebene Drucker verwalten | 674 |
| 23.3.1 | Anpassen der Einstellungen von Druckern | 674 |
| 23.3.2 | Der Zugriff auf freigegebene Drucker | 674 |
| 23.3.3 | Eigenschaften von Druckern in der PowerShell ändern | 675 |
| 23.3.4 | Druckaufträge in der PowerShell erzeugen | 676 |
| 23.3.5 | Druckberechtigungen mit Skripts setzen – SetACL.exe | 677 |
| 23.4 | Verwaltung von Druckjobs | 677 |
| 23.4.1 | Druckverwaltungs-Konsole – Die Zentrale für Druckerserver | 678 |
| 23.4.2 | Erstellen von benutzerdefinierten Filteransichten | 678 |
| 23.4.3 | Exportieren und Importieren von Druckern | 679 |
| 23.4.4 | Drucker verwalten und über Gruppenrichtlinien verteilen lassen | 679 |
| 23.5 | Druckprobleme im Netzwerk lösen | 680 |
| 23.5.1 | Generelle Vorgehensweise beim Lösen von Druckproblemen | 681 |
| 23.5.2 | Druckjobs überprüfen und löschen | 681 |
| 23.5.3 | Problembhebung mit Assistenten durchführen | 682 |

| | | |
|--------|--|-----|
| 23.5.4 | Druckeinstellungen zur Fehlerbehebung überprüfen | 682 |
| 23.5.5 | Berechtigungen und Sicherheitseinstellungen überprüfen | 683 |
| 23.5.6 | Drucker mit WMI ansprechen | 683 |
| 23.6 | Druckerserver mit Microsoft Universal Print in der Cloud betreiben | 685 |
| 23.6.1 | Lizenzierung und Einstieg in Universal Print | 685 |
| 23.7 | Zusammenfassung | 687 |

Teil VI Infrastrukturen mit Windows Server

| | | |
|-------------------|---|------------|
| Kapitel 24 | DHCP- und IPAM-Server einsetzen | 691 |
| 24.1 | DHCP-Server einsetzen | 691 |
| 24.1.1 | Installation eines DHCP-Servers | 691 |
| 24.1.2 | Grundkonfiguration eines DHCP-Servers | 692 |
| 24.1.3 | DHCP-Server mit Tools testen und Fehler finden | 699 |
| 24.1.4 | DHCP-Verkehr mit WireShark überprüfen | 700 |
| 24.1.5 | Core-Server – DHCP mit Netsh über die Eingabeaufforderung verwalten | 701 |
| 24.1.6 | Konfigurieren von DHCP mit der richtlinienbasierten Zuweisung | 702 |
| 24.1.7 | MAC-Filterung für DHCP in Windows Server 2022 nutzen | 704 |
| 24.2 | Migration – Verschieben einer DHCP-Datenbank auf einen anderen Server | 705 |
| 24.3 | Ausfallsicherheit von DHCP-Servern | 706 |
| 24.3.1 | DHCP für Failover konfigurieren | 706 |
| 24.3.2 | Ausfallsicherheit mit 80/20-Regel | 709 |
| 24.3.3 | Bereichsgruppierung (Superscopes) | 709 |
| 24.3.4 | Ausfallsicherheit bei DHCP-Servern durch verschiedene Bereiche herstellen | 710 |
| 24.3.5 | Standby-Server mit manueller Umschaltung | 711 |
| 24.4 | IPAM im Praxiseinsatz | 711 |
| 24.4.1 | IPAM-Grundlagen | 712 |
| 24.4.2 | IPAM einrichten | 713 |
| 24.4.3 | Fehlerbehebung der Anbindung von IPAM-Clients | 716 |
| 24.4.4 | Infrastrukturüberwachung und -verwaltung | 717 |
| 24.4.5 | IP-Adressblöcke mit IPAM | 718 |
| 24.5 | Zusammenfassung | 718 |
| Kapitel 25 | DNS einsetzen und verwalten | 719 |
| 25.1 | Erstellen von Zonen und Domänen | 719 |
| 25.1.1 | Erstellen von neuen Zonen | 719 |
| 25.1.2 | Erstellen von statischen Einträgen in der DNS-Datenbank | 721 |
| 25.1.3 | Einstellungen und Verwalten von Zonen | 723 |
| 25.2 | Verwalten der Eigenschaften eines DNS-Servers | 728 |
| 25.2.1 | Schnittstellen eines DNS-Servers verwalten | 729 |
| 25.2.2 | Erweiterte Einstellungen für einen DNS-Server | 729 |
| 25.2.3 | Zonendaten beim Start des DNS-Servers einlesen | 730 |
| 25.2.4 | Protokollierung für DNS konfigurieren | 731 |
| 25.2.5 | Ereignisprotokollierung konfigurieren | 732 |
| 25.3 | DNS-Weiterleitungen verwenden | 732 |
| 25.4 | Konfiguration sekundärer DNS-Server | 733 |
| 25.5 | DNS-Troubleshooting | 734 |
| 25.5.1 | Überprüfung und Fehlerbehebung der DNS-Einstellungen | 734 |
| 25.5.2 | Ipconfig für DNS-Diagnose verwenden | 737 |
| 25.5.3 | Domänencontroller kann nicht gefunden werden | 738 |

| | | |
|-------------------|--|------------|
| 25.5.4 | Namensauflösung von Mitgliedsservern | 738 |
| 25.5.5 | Erweiterte Namensauflösung sicherstellen | 739 |
| 25.5.6 | Nslookup zur Auflösung von Internetdomänen verwenden | 740 |
| 25.5.7 | Mit Nslookup SRV-Records oder MX-Records anzeigen | 740 |
| 25.5.8 | Komplette Zonen mit Nslookup übertragen | 740 |
| 25.5.9 | Dnscmd zur Verwaltung eines DNS-Servers in der Eingabeaufforderung | 741 |
| 25.6 | DNSSEC – Sicherheit in DNS | 744 |
| 25.6.1 | DNSSEC verstehen | 744 |
| 25.6.2 | DNS sicher betreiben – DNSSEC und Co. in der Praxis | 745 |
| 25.6.3 | DNS-Abfragen mit Richtlinien steuern | 749 |
| 25.6.4 | Response Rate Limiting – Schutz vor Denial of Service | 751 |
| 25.7 | Zusammenfassung | 752 |
| Kapitel 26 | Windows Server Container, Docker und Hyper-V-Container | 753 |
| 26.1 | Einstieg in Container und Docker | 754 |
| 26.1.1 | Container im Vergleich zu virtuellen Servern | 754 |
| 26.1.2 | Container-Feature installieren | 755 |
| 26.1.3 | Erste Schritte mit Docker in Windows Server 2022 | 756 |
| 26.1.4 | Hyper-V-Container-Host | 758 |
| 26.1.5 | Container im Windows Admin Center verwalten | 759 |
| 26.2 | Erweiterte Konfiguration von Containern | 760 |
| 26.2.1 | Neues Containerimage für Windows Server 2022 verfügbar | 760 |
| 26.2.2 | Container erstellen und Serverdienste verwalten | 761 |
| 26.2.3 | Container und eigene Images erstellen | 762 |
| 26.2.4 | Dockerfiles für eigene Images erstellen | 762 |
| 26.2.5 | Docker Push – Container in die Cloud laden | 763 |
| 26.3 | Hyper-V-Container in Windows Server 2022 | 764 |
| 26.3.1 | Einstieg in Hyper-V-Container | 764 |
| 26.3.2 | Hyper-V-Container erstellen und konfigurieren | 765 |
| 26.3.3 | Docker, Hyper-V-Container und VMs parallel einsetzen | 766 |
| 26.3.4 | Windows Server Container in der PowerShell verwalten | 766 |
| 26.4 | Windows-Subsystem für Linux in Windows Server 2022 und Windows 10/11 | 767 |
| 26.4.1 | Linux und Windows gemeinsam betreiben | 767 |
| 26.4.2 | Windows Subsystem for Linux installieren | 768 |
| 26.4.3 | Linux-Distributionen anzeigen und starten | 769 |
| 26.5 | Zusammenfassung | 770 |
| Kapitel 27 | Webserver – Internetinformationsdienste (IIS) | 771 |
| 27.1 | Installation, Konfiguration und erste Schritte | 772 |
| 27.1.1 | Anzeigen der Websites in IIS | 773 |
| 27.1.2 | Hinzufügen und Verwalten von Websites | 774 |
| 27.1.3 | Starten und Beenden des Webserver | 776 |
| 27.1.4 | Systemdateien von IIS verstehen | 776 |
| 27.1.5 | Verwalten der Webanwendungen und virtuellen Ordner einer Website | 778 |
| 27.1.6 | Entwicklungstools im Internet Explorer und Microsoft Edge | 779 |
| 27.2 | Verwalten von Anwendungspools | 779 |
| 27.2.1 | Erstellen und Verwalten von Anwendungspools | 780 |
| 27.2.2 | Zurücksetzen von Arbeitsprozessen in Anwendungspools | 781 |
| 27.3 | Verwalten von Modulen in IIS 2022 | 781 |
| 27.4 | Delegierung der IIS-Verwaltung | 782 |
| 27.4.1 | Vorgehensweise bei der Delegierung von Berechtigungen | 782 |

| | | |
|--------|--|-----|
| 27.4.2 | Verwalten von IIS-Manager-Benutzern | 782 |
| 27.4.3 | Berechtigungen der IIS-Manager-Benutzer verwalten | 782 |
| 27.4.4 | Verwalten der Delegierung | 783 |
| 27.4.5 | Aktivieren der Remoteverwaltung | 784 |
| 27.5 | Sicherheit in IIS 2022 konfigurieren | 785 |
| 27.5.1 | Konfiguration der anonymen Authentifizierung | 785 |
| 27.5.2 | Konfiguration der Standardauthentifizierung | 786 |
| 27.5.3 | Konfiguration der Windows-Authentifizierung | 787 |
| 27.5.4 | Einschränkungen für IP-Adressen und Domänen | 787 |
| 27.5.5 | Sicherheitseinstellungen von IIS anpassen | 788 |
| 27.5.6 | IP-Adressen, Domänen, SSL und URL Rewrite | 789 |
| 27.5.7 | IIS mit kostenlosen Tools absichern | 790 |
| 27.5.8 | Zed Attack Proxy Project (ZAP) und DefT-Linux – Webanwendungen testen | 791 |
| 27.5.9 | Freigegebene Konfiguration | 791 |
| 27.6 | Konfigurieren der Webseiten, Dokumente und HTTP-Verbindungen | 792 |
| 27.6.1 | Festlegen des Standarddokuments | 792 |
| 27.6.2 | Das Feature »Verzeichnis durchsuchen« aktivieren und verwalten | 793 |
| 27.6.3 | Konfigurieren der HTTP-Fehlermeldungen und -Umleitungen | 794 |
| 27.7 | IIS 2022 überwachen und Protokolldateien konfigurieren | 796 |
| 27.7.1 | Ablaufverfolgsregeln für Anforderungsfehler | 797 |
| 27.7.2 | Allgemeine Protokollierung aktivieren und konfigurieren | 797 |
| 27.7.3 | Überprüfen der Arbeitsprozesse der Anwendungspools | 799 |
| 27.8 | Optimieren der Serverleistung | 799 |
| 27.8.1 | Komprimierung aktivieren | 799 |
| 27.8.2 | Ausgabezwischen speichern verwenden | 800 |
| 27.9 | FTP-Server betreiben | 801 |
| 27.9.1 | Konfiguration des FTP-Servers | 802 |
| 27.9.2 | Schritt für Schritt-Anleitung zum FTP-Server in IIS 2022 | 802 |
| 27.10 | Zusammenfassung | 805 |

| | | |
|-------------------|--|------------|
| Kapitel 28 | Remotedesktopdienste – Anwendungen virtualisieren | 807 |
| 28.1 | Neuerungen in RDS | 807 |
| 28.1.1 | Vergleich zu Windows Server 2016 | 807 |
| 28.1.2 | Server Based Personal Desktop – Private Server für Anwender | 809 |
| 28.2 | Einstieg in die Remotedesktopdienste | 810 |
| 28.3 | Installation eines Remotedesktopservers | 811 |
| 28.3.1 | Installation und Verteilen der notwendigen Rollendienste | 811 |
| 28.3.2 | Einrichten einer neuen Sitzungssammlung | 814 |
| 28.3.3 | RemoteApp – Anwendungen bereitstellen | 815 |
| 28.3.4 | Remotedesktoplizenzierung | 817 |
| 28.3.5 | Remotedesktopsitzungen spiegeln | 820 |
| 28.3.6 | Nacharbeiten zur Installation | 825 |
| 28.4 | Drucken mit Remotedesktop-Sitzungshosts | 827 |
| 28.4.1 | Einstieg in das Drucken mit den Remotedesktopdiensten | 827 |
| 28.4.2 | Druckerprobleme auf Remotedesktop-Sitzungshosts lösen | 828 |
| 28.4.3 | Berechtigungs-Probleme auf Remotedesktop-Sitzungshosts lösen | 829 |
| 28.5 | Installation von Applikationen | 830 |
| 28.6 | Remotedesktop-Client | 831 |
| 28.6.1 | Befehlszeilenparameter für den Remotedesktop-Client | 833 |
| 28.6.2 | Umleitung von Digitalkameras und Mediaplayer | 833 |

| | | |
|-------------------|---|------------|
| 28.7 | Verwaltung eines Remotedesktop-Sitzungshosts | 833 |
| 28.7.1 | Remotedesktopdienste verwalten | 835 |
| 28.7.2 | Single Sign-On (SSO) für Remotedesktop-Sitzungshosts | 836 |
| 28.7.3 | Connection Broker an Microsoft Azure anbinden | 837 |
| 28.8 | RemoteApps verwalten | 838 |
| 28.8.1 | Konfiguration von Remotedesktopdienste-RemoteApp | 839 |
| 28.8.2 | Mit Windows 10/11 auf RemoteApps zugreifen | 839 |
| 28.8.3 | Remotedesktopdienste-Webzugriff | 840 |
| 28.9 | Remotedesktopgateway | 841 |
| 28.9.1 | Einrichtung und Konfiguration eines Remotedesktopgateways | 843 |
| 28.9.2 | Ressourcenautorisierungsrichtlinien erstellen und verwalten | 843 |
| 28.10 | Remotedesktop-Verbindungsbroker | 845 |
| 28.11 | Zertifikate installieren und einrichten | 845 |
| 28.11.1 | RDS-Zertifikate im Überblick | 846 |
| 28.11.2 | Zertifikate von den Active Directory-Zertifikatdiensten abrufen | 846 |
| 28.11.3 | Eigene Zertifikate-Vorlagen für die Anmeldung an RDS verwenden | 848 |
| 28.12 | Zusammenfassung | 849 |
| Kapitel 29 | Virtual Desktop Infrastructure – Arbeitsstationen virtualisieren | 851 |
| 29.1 | Einstieg in VDI | 851 |
| 29.2 | Windows 10/11 als virtuellen Computer in einer VDI-Struktur einsetzen | 852 |
| 29.2.1 | Installieren des Remotedesktop-Sitzungshosts | 852 |
| 29.2.2 | VDI-Umgebung verwalten | 853 |
| 29.2.3 | Virtuelle Computer installieren und für VDI vorbereiten | 853 |
| 29.2.4 | System mit Sysprep vorbereiten | 854 |
| 29.3 | Konfiguration des virtuellen Desktop-Pools | 855 |
| 29.3.1 | Sammlung virtueller Pools im Server-Manager erstellen | 855 |
| 29.3.2 | Desktop testen und verwenden | 856 |
| 29.3.3 | Personalisierte virtuelle Rechner verwenden | 857 |
| 29.3.4 | Eigenes Hintergrundbild für gehostete Desktops aktivieren | 857 |
| 29.4 | Zusammenfassung | 857 |
| Teil VII | Sicherheit und Hochverfügbarkeit | |
| Kapitel 30 | Active Directory-Zertifikatdienste | 861 |
| 30.1 | Installation einer Zertifizierungsstelle | 861 |
| 30.1.1 | Serverrolle für Active Directory-Zertifikatdienste installieren | 862 |
| 30.1.2 | Zertifizierungsstelle einrichten | 863 |
| 30.1.3 | Eigenständige Zertifizierungsstellen | 866 |
| 30.1.4 | Installieren einer untergeordneten Zertifizierungsstelle | 866 |
| 30.1.5 | Migrieren des Active Directory-Zertifikatdienstes | 866 |
| 30.1.6 | Migration beginnen | 867 |
| 30.1.7 | Zielservers konfigurieren | 867 |
| 30.2 | Zuweisen und Installieren von Zertifikaten | 868 |
| 30.2.1 | Zertifikate mit Assistenten aufrufen | 868 |
| 30.2.2 | Zertifikate im IIS-Manager abrufen | 869 |
| 30.2.3 | Zertifikate über Webinterface ausstellen | 871 |
| 30.2.4 | Zertifikate mit Gruppenrichtlinien verteilen | 871 |
| 30.3 | Zertifizierungsstelle verwalten | 872 |
| 30.3.1 | SSL für Zertifikatdienste einrichten | 872 |

| | | |
|-------------------|---|------------|
| 30.3.2 | Zertifikate von Stammzertifizierungsstellen verwalten | 873 |
| 30.3.3 | Die Zertifizierungsstellentypen und -Aufgaben | 874 |
| 30.3.4 | Verteilung der Zertifikateinstellungen über Gruppenrichtlinien | 875 |
| 30.4 | Sicherheit für Zertifizierungsstellen verwalten | 875 |
| 30.4.1 | Zertifizierungsstellenverwaltung delegieren | 875 |
| 30.4.2 | Sichern von Active Directory-Zertifikatdiensten | 876 |
| 30.5 | Zusammenfassung | 876 |
| Kapitel 31 | Firewall, Defender und IPsec im Netzwerk einsetzen | 877 |
| 31.1 | Microsoft Defender Exploit Guard | 877 |
| 31.2 | Microsoft Defender für den Virenschutz nutzen | 878 |
| 31.2.1 | Microsoft Defender in der GUI und Befehlszeile steuern | 879 |
| 31.2.2 | Definitionsdateien automatisiert herunterladen und installieren | 880 |
| 31.2.3 | Microsoft Defender in der PowerShell verwalten | 880 |
| 31.2.4 | Microsoft Defender in den Einstellungen und Gruppenrichtlinien anpassen | 881 |
| 31.2.5 | Ausnahmen für Serverrollen verwalten – Hyper-V | 883 |
| 31.2.6 | Virensuche mit dem Sysinternals Process Explorer | 886 |
| 31.3 | Windows Defender Credential Guard und Hypervisor-Protected Code Integrity | 888 |
| 31.3.1 | Windows Defender Credential Guard aktivieren | 888 |
| 31.3.2 | Kernisolierung: Hypervisor-Protected Code Integrity | 889 |
| 31.4 | Windows-Firewall nutzen | 889 |
| 31.4.1 | Windows-Firewall in der PowerShell steuern | 890 |
| 31.4.2 | IPsec mit der Windows-Firewall nutzen | 891 |
| 31.4.3 | Firewallregeln für SQL Server steuern | 894 |
| 31.5 | Zusammenfassung | 898 |
| Kapitel 32 | Remotезugriff mit DirectAccess und Always On VPN | 899 |
| 32.1 | Always On VPN nutzen | 900 |
| 32.1.1 | Vorteile von Always On VPN im Vergleich zu DirectAccess | 900 |
| 32.1.2 | Gruppenrichtlinien vor dem Einsatz konfigurieren | 900 |
| 32.1.3 | Zertifikatvorlagen für Always On VPN vorbereiten | 901 |
| 32.1.4 | Always On VPN installieren | 901 |
| 32.2 | Remotезugriff installieren und einrichten – Erste Schritte | 902 |
| 32.2.1 | Remotезugriff – Die Grundlagen | 902 |
| 32.2.2 | Vorbereiten der Installation von DirectAccess und Remotезugriff | 903 |
| 32.2.3 | Rollendienste installieren und Remotезugriff aktivieren | 904 |
| 32.2.4 | DirectAccess und VPN-Zugang einrichten | 904 |
| 32.2.5 | Aktualisieren von Clients mit der DirectAccess-Konfiguration | 908 |
| 32.2.6 | Überprüfen der Bereitstellung | 910 |
| 32.3 | Remotезugriff verwalten | 911 |
| 32.4 | VPN verwalten | 912 |
| 32.4.1 | Verwalten und Konfigurieren der RAS-Benutzer und RAS-Ports | 912 |
| 32.5 | HTTPS-VPN über Secure Socket Tunneling-Protokoll | 914 |
| 32.5.1 | Ablauf beim Verbinden über SSTP | 915 |
| 32.5.2 | Installation von SSTP | 916 |
| 32.5.3 | Fehlerbehebung bei SSTP-VPN | 918 |
| 32.6 | Exchange und Co. veröffentlichen – Anwendungsproxy einsetzen | 919 |
| 32.6.1 | Webanwendungsproxy installieren | 919 |
| 32.6.2 | Active Directory mit dem Webanwendungsproxy einrichten | 920 |
| 32.6.3 | Active Directory-Verbunddienste einrichten | 921 |
| 32.7 | Zusammenfassung | 921 |

| | |
|---|------------|
| Kapitel 33 Active Directory-Rechteverwaltungsdienste nutzen | 923 |
| 33.1 Active Directory-Rechteverwaltung im Überblick | 923 |
| 33.1.1 AD RMS und dynamische Zugriffssteuerung | 924 |
| 33.2 Rechteverwaltung installieren und einrichten | 925 |
| 33.2.1 SQL-Server für AD RMS vorbereiten | 925 |
| 33.2.2 Konfigurieren von AD RMS | 928 |
| 33.2.3 AD RMS nach der Installation verwalten und überprüfen | 931 |
| 33.3 Dynamische Zugriffssteuerung nutzen | 933 |
| 33.4 Zusammenfassung | 935 |
| | |
| Kapitel 34 Hochverfügbarkeit und Lastenausgleich | 937 |
| 34.1 Grundlagen zum Lastenausgleich | 937 |
| 34.2 Notwendige Vorbereitungen für NLB-Cluster | 938 |
| 34.3 Netzwerklastenausgleich installieren | 939 |
| 34.4 NLB-Cluster erstellen | 939 |
| 34.5 NLB versus DNS-Roundrobin | 941 |
| 34.6 Storage Spaces Direct nutzen | 943 |
| 34.6.1 Einstieg in Storage Spaces Direct | 943 |
| 34.6.2 So funktioniert Storage Spaces Direct | 944 |
| 34.6.3 Storage Spaces Direct in der Praxis | 944 |
| 34.6.4 Ausfallsicherheit bei Storage Spaces Direct | 949 |
| 34.6.5 Speicherpools in Storage Spaces Direct optimieren | 951 |
| 34.7 Scale-Out File Server erstellen | 951 |
| 34.7.1 Cluster sind auch in kleinen Netzwerken sinnvoll einsetzbar | 952 |
| 34.7.2 Scale-Out File Server und Storage Spaces Direct | 952 |
| 34.7.3 Scale-Out File Server im Cluster nutzen | 954 |
| 34.7.4 Vorteile beim Einsatz eines Scale-Out File Servers: SMB-Version beachten | 955 |
| 34.7.5 Dateiserver und das Cluster Shared Volume | 956 |
| 34.8 Cluster Operating System Rolling Upgrade | 957 |
| 34.8.1 So aktualisieren Sie einen Cluster zu Windows Server 2022 | 957 |
| 34.8.2 Node Fairness – Lastenausgleich aktivieren | 959 |
| 34.8.3 Startreihenfolge der VMs nach der Migration anpassen | 960 |
| 34.8.4 Compute Resiliency – Ausfallsicherheit steuern | 961 |
| 34.9 Cluster Aware Update nutzen und einrichten | 961 |
| 34.9.1 Grundlagen für die Einführung von Cluster Aware Update | 961 |
| 34.9.2 Firewallinstellungen und mehr für CAU | 963 |
| 34.9.3 CAU für den Cluster aktivieren | 963 |
| 34.9.4 CAU in der PowerShell steuern | 964 |
| 34.9.5 Fehlerbehebung der Einrichtung | 964 |
| 34.9.6 Updates mit CAU planen | 965 |
| 34.10 Cloud Witness mit Microsoft Azure | 966 |
| 34.10.1 Cluster an Microsoft Azure anbinden | 966 |
| 34.10.2 Zeugenserver überprüfen | 967 |
| 34.11 Der Netzwerkcontroller im Überblick | 968 |
| 34.12 Data Center Bridging (DCB) | 970 |
| 34.13 Zusammenfassung | 971 |
| | |
| Kapitel 35 Datensicherung und Wiederherstellung | 973 |
| 35.1 Grundlagen zur Datensicherung | 973 |
| 35.2 Windows Server-Sicherung installieren und konfigurieren | 974 |
| 35.2.1 Sicherung in der Eingabeaufforderung und PowerShell konfigurieren | 976 |

| | | |
|-------------------|--|-------------|
| 35.2.2 | Daten mit dem Sicherungsprogramm wiederherstellen | 977 |
| 35.2.3 | Kompletten Server mit dem Sicherungsprogramm wiederherstellen | 979 |
| 35.3 | Erweiterte Wiederherstellungsmöglichkeiten | 980 |
| 35.3.1 | Schrittaufzeichnung – Fehler in Windows nachvollziehen und beheben | 981 |
| 35.3.2 | Datensicherung über Ereignisanzeige starten | 981 |
| 35.4 | Windows-Abstürze analysieren und beheben | 983 |
| 35.5 | Microsoft Windows File Recovery Tool | 987 |
| 35.5.1 | WinFR in der Praxis | 988 |
| 35.5.2 | Alternativen für WinFR | 990 |
| 35.6 | Zusammenfassung | 991 |
| Kapitel 36 | Active Directory-Verbunddienste und Workplace Join | 993 |
| 36.1 | Installieren und Einrichten der Active Directory-Verbunddienste | 994 |
| 36.1.1 | Einstieg in die Installation von ADFS | 994 |
| 36.1.2 | Vorbereitungen für die ADFS-Infrastruktur | 995 |
| 36.1.3 | SSL-Zertifikate als Vorlage in Active Directory-Zertifikatdiensten festlegen | 995 |
| 36.1.4 | ADFS als Serverrolle installieren | 996 |
| 36.1.5 | ADFS einrichten | 997 |
| 36.1.6 | Geräteregistrierung konfigurieren | 998 |
| 36.1.7 | Einrichten einer Beispiel-Webanwendung für ADFS | 999 |
| 36.1.8 | Vertrauensstellung zwischen Webanwendung und ADFS einrichten | 1001 |
| 36.2 | Fehlerbehebung und Überwachung bei einem ADFS-Server | 1002 |
| 36.3 | Single Sign-On mit ADFS – auch mit Microsoft 365/Office 365 | 1003 |
| 36.4 | Zusammenfassung | 1004 |
| Kapitel 37 | Updates in Microsoft-Netzwerken steuern mit WSUS und Azure | 1005 |
| 37.1 | WSUS installieren | 1005 |
| 37.1.1 | WSUS nach der Installation einrichten | 1006 |
| 37.1.2 | WSUS-Grundeinrichtung über Gruppenrichtlinien | 1008 |
| 37.1.3 | Upstreamserver in WSUS nutzen | 1008 |
| 37.1.4 | SSL in WSUS nutzen | 1009 |
| 37.2 | Updates im Griff behalten und steuern | 1010 |
| 37.2.1 | Steuerung von Verteilungsringen | 1012 |
| 37.2.2 | Steuerung von Windows-10/11-Updates mit Gruppenrichtlinien | 1013 |
| 37.2.3 | Konfiguration der Übermittlungsoptimierung | 1014 |
| 37.2.4 | Neue Update-Funktionen in Windows 10/11 verstehen | 1014 |
| 37.2.5 | Windows-Updates in Windows 10/11 steuern | 1015 |
| 37.2.6 | Installation von Funktionsupdates steuern | 1017 |
| 37.2.7 | Windows 10/11 und WSUS | 1018 |
| 37.2.8 | Probleme bei der Installation von Updates beheben | 1019 |
| 37.3 | Patchverwaltung mit WSUS | 1019 |
| 37.3.1 | Clientcomputer über Gruppenrichtlinien anbinden | 1020 |
| 37.3.2 | Einstellungen für Windows 10/11 korrekt setzen | 1023 |
| 37.3.3 | Updates genehmigen und bereitstellen | 1025 |
| 37.3.4 | Berichte mit WSUS abrufen | 1027 |
| 37.4 | WSUS in Windows Server 2022 überwachen | 1027 |
| 37.4.1 | Überprüfung der Gruppenrichtlinien | 1027 |
| 37.4.2 | In der Befehlszeile nach Problemen suchen | 1028 |
| 37.4.3 | SSL-Port beachten | 1028 |
| 37.4.4 | Diagnostic Tool for the WSUS Agent | 1029 |
| 37.4.5 | WSUS mit der PowerShell verwalten | 1029 |

| | | |
|-------------------|--|-------------|
| 37.5 | Azure Update Management für das Patchmanagement nutzen | 1031 |
| 37.5.1 | Komponenten von Azure Update Management | 1032 |
| 37.5.2 | Azure Update Management in der Praxis | 1033 |
| 37.5.3 | Linux-Server automatisiert aktualisieren | 1035 |
| 37.5.4 | Angebundene Server im Azure-Portal verwalten | 1035 |
| 37.5.5 | Bereitstellen von Updates über Azure Update Management | 1036 |
| 37.5.6 | Computer aus der Azure-Updateverwaltung entfernen | 1038 |
| 37.6 | Zusammenfassung | 1039 |
| Kapitel 38 | Diagnose und Überwachung | 1041 |
| 38.1 | Fehlerbehebung in Windows Server – Ereignisanzeige | 1041 |
| 38.1.1 | Ereignisanzeige nutzen | 1041 |
| 38.1.2 | Ereignisprotokolle im Netzwerk einsammeln | 1044 |
| 38.2 | Überwachung der Systemleistung | 1050 |
| 38.2.1 | Die Leistungsüberwachung | 1052 |
| 38.2.2 | Indikatorendaten in der Leistungsüberwachung beobachten | 1054 |
| 38.2.3 | Sammlungssätze nutzen | 1055 |
| 38.2.4 | Speicherengpässe beheben | 1055 |
| 38.2.5 | Prozessorauslastung messen und optimieren | 1058 |
| 38.2.6 | Der Task-Manager als Analysewerkzeug | 1059 |
| 38.2.7 | Laufwerke und Datenträger überwachen – Leistungsüberwachung und Zusatztools | 1061 |
| 38.3 | Serverüberwachung mit dem Windows Admin Center | 1062 |
| 38.3.1 | Neuen Arbeitsbereich erstellen | 1063 |
| 38.3.2 | Workspace speichern, herunterladen und hochladen | 1064 |
| 38.4 | Aufgabenplanung – Windows automatisieren | 1065 |
| 38.4.1 | Aufgabenplanung verstehen | 1066 |
| 38.4.2 | Erstellen einer neuen Aufgabe | 1068 |
| 38.5 | Prozesse und Dienste überwachen | 1070 |
| 38.5.1 | Dienste in der PowerShell verwalten | 1070 |
| 38.5.2 | Dateisystem, Registry und Prozesse überwachen – Sysinternals Process Monitor | 1073 |
| 38.5.3 | Laufende Prozesse analysieren – Process Explorer | 1077 |
| 38.5.4 | Wichtige Informationen immer im Blick – BgInfo | 1080 |
| 38.5.5 | Systeminformationen in der Eingabeaufforderung anzeigen – PsInfo | 1083 |
| 38.6 | Zusammenfassung | 1084 |
| Teil VIII | Bereitstellung, Verwaltung, Cloudanbindung | |
| Kapitel 39 | Windows-Bereitstellungsdienste | 1087 |
| 39.1 | Windows Assessment and Deployment Kit (ADK) | 1087 |
| 39.1.1 | Das Windows-Imageformat | 1088 |
| 39.1.2 | Windows Systemabbild-Manager, Antwortdateien und Kataloge | 1089 |
| 39.1.3 | Windows Assessment and Deployment Kit installieren | 1089 |
| 39.2 | Automatisierte Installation von Windows 10/11 und Windows Server 2022 | 1090 |
| 39.2.1 | Windows System Image Manager nutzen | 1090 |
| 39.2.2 | Windows 10/11 und Windows Server 2022 aktivieren | 1093 |
| 39.3 | Grundlagen der Windows-Bereitstellungsdienste | 1094 |
| 39.3.1 | Verwalten von Abbildern in WDS | 1094 |
| 39.3.2 | So funktioniert die automatisierte Installation von Windows über WDS | 1095 |

| | | |
|-------------------|---|-------------|
| 39.4 | Installation der Windows-Bereitstellungsdienste | 1096 |
| 39.4.1 | Ersteinrichtung der Windows-Bereitstellungsdienste | 1096 |
| 39.4.2 | Multicast verwenden | 1099 |
| 39.5 | Verwalten und Installieren von Abbildern | 1100 |
| 39.5.1 | Startabbilder verwalten | 1100 |
| 39.5.2 | Installationsabbilder verwenden | 1102 |
| 39.5.3 | Suchabbilder verwenden | 1103 |
| 39.5.4 | Aufzeichnungsabbilder verwenden | 1103 |
| 39.5.5 | Automatische Namensgebung für Clients konfigurieren | 1104 |
| 39.5.6 | Berechtigungen für Abbilder verwalten | 1105 |
| 39.5.7 | Virtuelle Festplatten in WDS verwenden | 1105 |
| 39.5.8 | Treiberpakete in WDS verwenden | 1106 |
| 39.6 | Volumenaktivierungsdienste nutzen | 1107 |
| 39.7 | Zusammenfassung | 1107 |
| Kapitel 40 | Windows PowerShell | 1109 |
| 40.1 | PowerShell 7 für Windows, macOS und Linux | 1109 |
| 40.1.1 | Kompatibilität der PowerShell 7 mit PowerShell 5.x | 1110 |
| 40.1.2 | PowerShell 7 installieren | 1111 |
| 40.1.3 | Pipelines mit der PowerShell 7 und weitere neue Funktionen | 1111 |
| 40.2 | Wissenswertes zur PowerShell in Windows Server 2022 | 1112 |
| 40.2.1 | Einstieg in die PowerShell und Eingabeaufforderung | 1113 |
| 40.3 | PowerShell und PowerShell ISE – Eine Einführung | 1115 |
| 40.3.1 | Mit der PowerShell ISE effizient arbeiten | 1116 |
| 40.3.2 | Einstieg in die PowerShell | 1117 |
| 40.3.3 | Die PowerShell über das Netzwerk nutzen | 1117 |
| 40.4 | Die grundsätzliche Funktionsweise der PowerShell | 1119 |
| 40.4.1 | Einstieg in die Befehle der PowerShell | 1119 |
| 40.4.2 | Patches und Datensicherungen verwalten | 1120 |
| 40.4.3 | Registry und Co. mit der PowerShell verwalten | 1120 |
| 40.4.4 | Die PowerShell-Laufwerke verwenden | 1121 |
| 40.4.5 | Skripts mit der PowerShell erstellen | 1122 |
| 40.5 | Mit PowerShell Desired State Configuration Windows-Server absichern | 1124 |
| 40.5.1 | MOF-Dateien für DSC erstellen und umsetzen | 1125 |
| 40.5.2 | MOF-Dateien erweitern | 1126 |
| 40.6 | Windows PowerShell zur Administration verwenden | 1127 |
| 40.6.1 | PowerShell Direct – Virtuelle Betriebssysteme steuern | 1127 |
| 40.6.2 | Software im Netzwerk verteilen | 1128 |
| 40.6.3 | Software mit Chocolatey installieren und aktuell halten | 1129 |
| 40.6.4 | Chocolatey installieren, aktualisieren und nutzen | 1129 |
| 40.6.5 | Software mit der ChocolateyGUI installieren | 1130 |
| 40.6.6 | Grundlagen zur Verwaltung von Servern mit der PowerShell | 1130 |
| 40.6.7 | Mit Variablen arbeiten | 1131 |
| 40.6.8 | Systemprozesse verwalten | 1131 |
| 40.6.9 | Dateien und Objekte kopieren, löschen und verwalten | 1132 |
| 40.6.10 | Dienste in der PowerShell und Befehlszeile steuern | 1134 |
| 40.6.11 | Aus der PowerShell E-Mails schreiben | 1134 |
| 40.6.12 | Windows-Firewall in der PowerShell steuern | 1136 |
| 40.7 | PowerShell Web Access | 1138 |
| 40.7.1 | Installieren von PowerShell Web Access | 1139 |
| 40.7.2 | Konfigurieren des Gateways für PowerShell Web Access | 1139 |
| 40.7.3 | Konfigurieren der Berechtigungen für PowerShell Web Access | 1140 |

| | |
|---|-------------|
| 40.8 Eingabeaufforderung verwenden | 1142 |
| 40.9 Batchdateien für Administratoren | 1146 |
| 40.9.1 Grundlagen zu Batchdateien | 1146 |
| 40.9.2 Netzwerkverwaltung in der Befehlszeile | 1146 |
| 40.9.3 Sprungmarken und Warte-Befehle | 1147 |
| 40.9.4 Wenn/Dann-Abfragen nutzen | 1147 |
| 40.9.5 Informationen zum lokalen Server abrufen | 1148 |
| 40.9.6 Schleifen und Variablen | 1149 |
| 40.10 WMI-Abfragen nutzen | 1150 |
| 40.11 Zusammenfassung | 1152 |
| Index | 1153 |

Vorwort

Mit Windows Server 2022 stellt Microsoft die neue Version seines Server-Betriebssystems vor. In der neuen Version hat Microsoft Neuerungen im Bereich der Virtualisierung, Container und im Storage-Bereich integriert, aber auch neue Funktionen mit eingebunden.

Die Container-Technologie wurde verbessert, arbeitet mit Kubernetes zusammen und wurde noch enger mit dem Windows-System verknüpft.

In diesem Buch habe ich für Sie alle Neuerungen aufgenommen sowie deren praktische Umsetzung erläutert. Auch die Zusammenarbeit der neuen Funktionen mit bewährten Technologien von Windows Servern sind im Buch zu finden.

Freuen Sie sich auf Windows Server 2022 und die vielen Praxisworkshops und Anleitungen in diesem Buch. Ich habe viele Vorgehensweisen in der PowerShell erläutert und bin auch darauf eingegangen, wie Sie Windows Server umfassend mit der PowerShell und dem Windows Admin Center verwalten.

Ich hoffe, Sie haben beim Lesen so viel Spaß wie ich beim Schreiben.

Ihr Thomas Joos

Teil I

Grundlagen und Installation

Kapitel 1

Neuerungen und Lizenzierung

In diesem Kapitel widmen wir uns unter anderem den Neuerungen in Windows Server 2022 im Vergleich zu Windows Server 2019. Windows Server 2022 unterstützt die effektivere Bereitstellung von Containern, vor allem auf Basis von Linux. Auch Kubernetes wird in Windows Server 2022 unterstützt.

Der Nachfolger von Windows Server 2019 bietet Neuerungen im Bereich der Virtualisierung, Sicherheit und der Zusammenarbeit von Servern im Netzwerk. Um die neue Version einzusetzen, müssen Unternehmen aber nicht alle Server ersetzen. Windows Server 2022 lässt sich sowohl als Mitgliedsserver als auch als Domänencontroller in gemischten Netzwerken betreiben. Alle Vorteile erreichen Sie allerdings nur, wenn Sie alle Server auf die neue Version umstellen. Natürlich können Sie Windows Server 2022 auch zusammen mit Windows Server 2012/2012 R2/2016 und Windows Server 2019 betreiben.

Von Windows Server 2022 gibt es die Editionen Standard und Datacenter. Zusätzlich bietet Microsoft noch eine Essential-Lizenz für kleine Unternehmen an sowie die Azure-Edition, die nur als VM in Microsoft Azure genutzt werden kann. Diese ermöglicht zum Beispiel »Hotpatching«, also das Aktualisieren des Servers im laufenden Betrieb. Das ist mit den anderen Editionen derzeit nicht möglich. Die Azure-Edition entspricht vom Funktionsumfang der Datacenter-Edition. Neben dem Betrieb in Microsoft Azure steht Windows Server 2022 Azure Edition ebenfalls in Azure Stack HCI zur Verfügung.

In Windows Server 2022 gibt es Unterschiede zwischen den Editionen bei den Speicherfunktionen. Es lassen sich weiterhin mit der Standard-Edition Cluster, die Rechteverwaltung und alle Funktionen der Active Directory-Zertifikatdienste betreiben. Wer alle Funktionen von Windows Server 2022 nutzen will, muss daher zur Datacenter-Edition greifen.

1.1 Die wichtigsten Neuerungen in Windows Server 2022

Mit Windows Server 2022, dem LTSC-Nachfolger von Windows Server 2019, stellt Microsoft auch das dazugehörige Container-Image zur Verfügung. Wir geben einen Überblick zur Einrichtung und Installation.

Der LTSC-Nachfolger von Windows Server 2019 steht als Servervariante, aber auch als Container-Image zur Verfügung. Microsoft gewährt fünf Jahre Standard-Support und weitere fünf Jahre erweiterten Support.



Natürlich hat Microsoft bei der unterstützten Hardware einiges verändert. Windows Server 2022 kann bis zu 48TB Arbeitsspeicher verwalten. Das gilt auch für Windows Server 2022 Essentials und natürlich für Datacenter. Insgesamt lassen sich bis zu 64 CPUs mit Windows Server 2022 nutzen.

1.1.1 Neuerungen in Windows Server 2022

Wesentliche Sprünge von Windows Server 2019 gibt es in Windows Server 2022 nicht. Die Änderungen liegen im Detail. Zunächst hat Windows Server 2022 eine engere Verbindung zu Microsoft Azure erhalten, die wiederum mit neuen Versionen des Windows Admin Centers verwaltet werden sollen. Ab Version 2103.2 ist das Windows Admin Center kompatibel mit den Funktionen in Windows Server 2022 und ermöglicht auch die Anbindung von Azure-Funktionen wie Azure Arc oder Storage Migration Service (Speichermigrationsdienst) an Windows Server 2022. Einfach ausgedrückt soll Azure Arc Funktionen und Technologien aus Microsoft Azure direkt in lokalen Rechenzentren zur Verfügung stellen.

Neue Sicherheitsfunktionen unterstützen Sicherheitsoptionen der Hardware. Der Secured-Core-Server und Secured-Connectivity sollen vor allem die Angriffe auf Server reduzieren. Für den Einsatz ist aber Hardware notwendig, die die Funktionen unterstützt. Basis sind das Trusted Platform Module (TPM) und System Guard. Die Server nutzen Technologien aus Hyper-V für den sicheren Betrieb.

Windows Server 2022 setzt auf TLS 1.3 und eine sichere Kommunikation per HTTPS sowie AES-256-Verschlüsselung bei SMB-Verbindungen.

Die Installation von Windows Server 2022 unterscheidet sich nicht von der aus Windows Server 2019. Es stehen weiterhin die Editionen Standard und Datacenter mit und ohne Desktop zur Verfügung. Die neue Windows Server-Version verfügt bereits über eine Installation von Microsoft Edge, dem Nachfolger des Internet Explorers. Auch der Server-Manager ist noch an Bord. Microsoft erweitert allerdings die Möglichkeiten des Windows Admin Centers, sodass in Zukunft immer mehr Verwaltungsfunktionen in die webbasierte Oberfläche wandern.

Eine der zentralen neuen Funktionen in Windows Server 2022 ist der Secured-Core-Server. Dabei handelt es sich um eine neue Sicherheitsebene für Windows-Server, die auch in Azure Stack HCI Einzug findet. Mit Secured-Core-Server erhalten Unternehmen eine Kombination aus Hardware, Treiber, Software und Windows Server 2022.

1.1.2 Secured-Core-Server mit Windows Server 2022

Kunden, die einen Secured-Core-Server erwerben, erhalten in Zusammenarbeit mit einem Hardware-Hersteller Serverhardware, die mit den Funktionen umgehen kann. Die neuen Funktionen sind vor allem über das Windows Admin Center steuerbar.

Im Windows Admin Center ist auf der linken Seite der Menüpunkt *Security* verfügbar, wenn Hardware die Sicherheitsfunktionen von Windows Server 2022 unterstützt. Die Erweiterung kann über das Windows Admin Center auch nachträglich eingebunden werden. Hier ist mit Icons zu erkennen, ob Sicherheitsfunktionen wie HVCI (Hypervisor-basierte Code-Integrität), Boot DMA Protection, System Guard, Secure Boot, VBS (Virtualisierungsbasierte Sicherheit) und TPM 2.0 aktiviert sind.

Secured-Core-Server ist vor allem für Server sinnvoll, auf denen heikle Daten betrieben werden sollen. Trusted Platform Module 2.0 (TPM 2.0) sind standardmäßig in Secured-Core-Servern enthalten.

Durch die Unterstützung des Prozessors für die DRTM-Technologie (Dynamic Root of Trust for Measurement) zusammen mit dem DMA-Schutz isolieren Secured-Core-Systeme den sicherheitskritischen Hypervisor von Angriffen.

Secured-Core-Server unterstützen VBS und Hypervisor-basierte Code-Integrität (HVCI). Virtualisierungsbasierte Sicherheit (VBS) ermöglicht eine Isolierung zwischen den privilegierten Teilen des Betriebssystems, wie dem Kernel und dem Rest des Systems.

Natürlich nutzen Secured-Core-Server auch andere Sicherheitsfunktionen von Windows Server 2022, die ebenso den anderen Servern zur Verfügung stehen. Die Verwaltung wird ebenfalls hier im Windows Admin Center integriert. Windows Server 2022 unterstützt TLS 1.3 und aktiviert TLS automatisch beim Neustart.

Windows Server 2022 bietet neue gruppenverwaltete Dienstkonten (Group Managed Service Accounts, gMSA) für Windows-Container, ohne den Host in die Domäne aufnehmen zu müssen.

Wer Windows Server 2022 in Microsoft Azure bereitstellt, kann Images auswählen, auf denen Azure-Sicherheitsrichtlinien automatisch aktiviert sind. Das ermöglicht die Optimierung einer Windows Server 2022-Installation für Microsoft Azure.

1.1.3 Neues Container-Image für Windows Server 2022

Mit Windows Server 2022 erscheint außerdem ein neues Container-Image. Neben den bekannten Core- und Nano-Images bietet Windows Server 2022 das neue Windows Server-Image. Dieses soll innerhalb eines Containers recht umfassende Möglichkeiten bieten, die bisher nur vollständig installierten Servern mit grafischer Oberfläche vorbehalten waren.

Die neue Version bietet eine Unterstützung für nahezu alle Windows-APIs, die im Nano- und Core-Image fehlen. Basis des Images ist eine vollständig installierte Version von Windows Server 2022. Daher hat das Image fünf Jahre Support, genauso wie Windows Server 2022 selbst. Auf Containern, die mit diesem Image erstellt werden, soll es möglich sein, ebenfalls Serverdienste zu installieren, zum Beispiel eine nahezu uneingeschränkte IIS-Installation mit unbegrenzten, gleichzeitigen Verbindungen.

Das Image hat eine Größe von 3,1 GB. Container auf der Basis des Images sollen eine Grafikbeschleunigung bieten. Aktuell lässt sich das Image nur auf Windows Server 2022 installieren und starten. Um Windows Server 2022 zu einem Container-Host für das neue Image zu machen, sind in der PowerShell folgende Befehle notwendig:

```
Install-Module -Name DockerMsftProvider -Repository PSGallery -Force
```

```
Install-Package -Name docker -ProviderName DockerMsftProvider
```

```
Restart-Computer -Force
```

Nach dem Neustart kann die installierte Docker-Version mit dem folgenden Befehl überprüft werden:

```
Get-Package -Name Docker -ProviderName DockerMsftProvider
```

```
Find-Package -Name Docker -ProviderName DockerMsftProvider
```

Docker wird anschließend mit dem folgenden Befehl gestartet:

```
Start-Service Docker
```

Anschließend kann auf dem Windows-Server das Image über Docker heruntergeladen werden, zum Beispiel mit:

```
docker pull mcr.microsoft.com/windows/server/insider:10.0.20348.1
```

Beim Download ist es natürlich wichtig, die jeweils aktuelle Version zu verwenden. Die Version ist im Docker-Hub zu finden (https://hub.docker.com/_/Microsoft-Windows-server-insider). Um einen Container auf Basis des Images zu starten, wird der folgende Befehl verwendet:

```
docker run -it mcr.microsoft.com/windows/server/insider:10.0.20348.1 cmd
```

Auch hier ist selbstverständlich die Angabe der jeweilig heruntergeladenen Version notwendig. Der Container kann überdies im Hyper-V-Isolationsmodus gestartet werden. Dazu ist auf dem Server natürlich noch die Installation von Hyper-V notwendig.



Neben Windows Server 2019 hat Microsoft halbjährlich neue Server-Versionen veröffentlicht, die über neue Funktionen verfügen. Diese tragen die Bezeichnung »Semi-Annual-Channel-Versionen« (SAC). Im Gegensatz zu den Hauptversionen von Windows Server Long Term Servicing Channel, LTSC, tragen die SAC-Versionen nicht nur die Jahreszahl der Veröffentlichung im Namen, sondern auch, in welchem Halbjahr die Version erschienen ist. So wurde etwa Windows Server 20H2 im 2. Halbjahr in 2020 veröffentlicht.

Mit Windows Server 2022 stellt Microsoft diese Versionen ein. Neue Funktionen integriert Microsoft in Azure Stack HCI. Es wird keine SAC-Versionen mehr für Windows Server 2022 geben.

1.2 Windows Server 2022 lizenzieren

Eines ändert sich auch mit Windows Server 2022 nicht: die Komplexität der Lizenzierung. Es gibt zahlreiche Verträge und viele Möglichkeiten, Windows 10/11 und Windows Server 2022 zu lizenzieren. Verantwortliche im Unternehmen sollten sich darüber informieren, welche Lizenzverträge und Möglichkeiten es gibt.

Generell ist davon auszugehen, dass der Einsatz von Windows Server 2022 teurer wird. Das liegt vor allem an der Prozessor-Kern-Lizenzierung. Der CAL-Zugriff der Anwender bleibt in Windows Server 2022 generell gleich zu den Vorgängern. Die unterschiedlichen Windows-Editionen bieten für Unternehmen verschiedene Möglichkeiten und Auswahlkriterien.

1.2.1 Editionen und Lizenzen im Vergleich

Microsoft hat mit Windows Server 2022 Unterschiede in den Storage-Funktionen integriert. So unterstützt nur die Datacenter-Edition alle Funktionen. In der Standard-Edition gibt es weder Storage Spaces Direct noch Storage Replica. Auch Shielded Virtual Machines fehlen in der Standard-Edition. Die anderen Funktionen hat Microsoft in der Standard-Edition integriert. Diese verfügt zum Beispiel ebenfalls über die Container-Technologie und die Nano-Images.

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

Die Lizenzierung erfolgt nicht mehr auf Basis der CPUs, sondern auf Basis der CPU-Kerne. In Hyper-V werden die logischen Prozessoren lizenziert, da diese das Pendant zu den physischen Prozessorkernen darstellen.

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

Sie müssen für jeden Server mindestens vier Lizenzen erwerben, also für acht Kerne. Setzen Sie einen Dual-Prozessor mit je acht Kernen ein, müssen Sie also acht Lizenzen für diese 16 Kerne erwerben. Für jeden Kern mehr müssen Sie ein Core-Pack kaufen, damit alle Kerne lizenziert sind. In Windows Server 2022 Standard dürfen Sie pro Lizenz zwei VMs installieren, Windows Server 2022 Datacenter kennt kein Limit. Hier müssen Sie lediglich alle Prozessorkerne des Servers lizenzieren.

Lizenzen von Windows Server 2022 sind direkt auf die physische Hardware gebunden. Jede Lizenz deckt zwei physische Prozessorkerne ab. Sie dürfen mit der Standard-Edition außerdem bis zu zwei virtuelle Server auf dem lizenzierten Host betreiben. Beim Einsatz der Datacenter-Edition dürfen Sie so viele virtuelle Server auf dem Host betreiben, wie die Hardware hergibt.

1.2.2 Clientzugriffslizenzen beachten

Für die Editionen Standard und Datacenter benötigen Sie weiterhin Clientzugriffslizenzen (CALs). Auch in Windows Server 2022 können Sie diese benutzerbasiert oder pro Gerät erwerben, dürfen sie aber nicht aufsplitten. Clientzugriffslizenzen (CALs) und Remotedesktop-Clientzugriffslizenzen (RDCALs) sowie Lizenzen für die Active Directory-Rechteverwaltung (AD RMS) sind auch in Windows Server 2022 weiterhin notwendig, aber nur in den Editionen Standard und Datacenter. Hier gibt es gleichfalls Gerätelizenzen oder Benutzerlizenzen für den Zugriff. Sie müssen bereits bei der Bestellung Ihrer Lizenzen im Voraus planen, welchen Lizenztyp Sie einsetzen wollen.

Sie können die verschiedenen Lizenzen miteinander mischen. Es ist jedoch nicht erlaubt, die einzeln erhältlichen Lizenzpakete in Geräte- und Benutzerlizenzen aufzusplitten. Sie dürfen also ein 5er-Paket Gerätelizenzen und ein 5er-Paket Benutzerlizenzen für einen Ser-

ver kaufen und lizenzieren. Es ist aber nicht erlaubt, diese Pakete aufzusplitten und zum Beispiel als 2er-Gerätelizenz und 8er-Benutzerlizenz zu verwenden. Genauso ist nicht zulässig, mit CALs von Vorgängerversionen auf Server mit Windows Server 2022 zuzugreifen.

1.2.3 Geräte-CALs und Benutzer-CALs

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



CALs sind bei Microsoft an die Version gebunden. Sie dürfen daher CALs für Windows Server 2019 nicht für Windows Server 2022 nutzen. Allerdings ist es erlaubt, mit CALs für Windows Server 2022 auf Server mit Windows Server 2019 zuzugreifen. Sie sollten daher möglichst immer die aktuellsten CALs einsetzen bzw. erwerben.

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

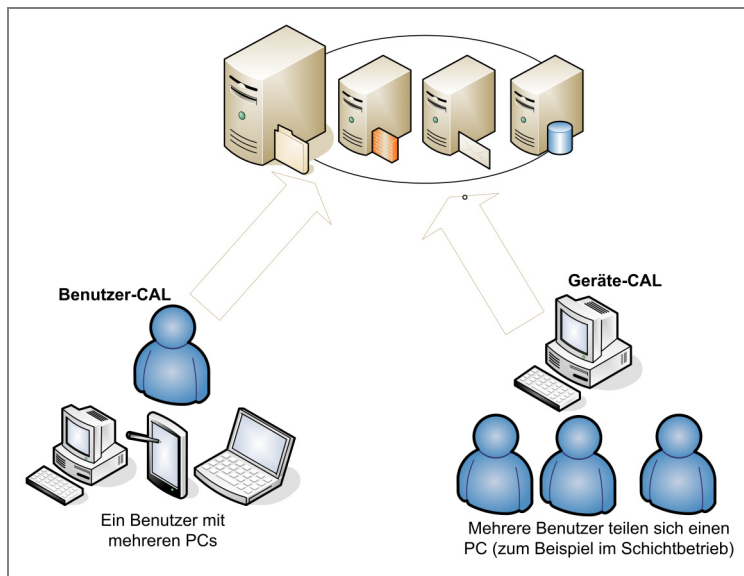


Abb. 1.1 Windows Server 2022 lässt sich weiterhin mit Benutzer-CALs und Geräte-CALs lizenzieren.

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

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

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

1.3 Windows Server 2022 für kleine Unternehmen

Sehr kleine Unternehmen können Windows Server 2022 Standard mit der sogenannten Essentials-Lizenz verwenden. Einen Nachfolger für SBS mit Exchange und einem SQL-Server gibt es nicht mehr. Unternehmen, die Microsoft Exchange nutzen wollen, müssen auf Microsoft 365 setzen oder Exchange auf einer eigenen Servermaschine getrennt lizenzieren.



Grundsätzlich entspricht Essentials dem Funktionsumfang von Windows Server 2022 Standard. Es gibt lizenztechnische Einschränkungen, die wir in den nächsten Abschnitten genauer vorstellen.

Der Server erlaubt die Anbindung von maximal 25 Benutzern und 50 PCs sowie 10 CPU-Kerne. Wenn mehr im Einsatz sind, müssen Unternehmen auf die Standard-Edition von Windows Server 2022 erhöhen. CALs sind für die Benutzer nicht notwendig und auch nicht verfügbar. Allerdings können Sie Essentials als RDS-Host (siehe Kapitel 28) verwenden. In diesem Fall brauchen Sie aber RDS-CALs.

Wenn Sie Windows Server 2022 als Hyper-V-Host nutzen, dürfen Sie auf dem Server einen weiteren Server virtualisieren.

Vom Funktionsumfang entspricht Windows Server 2022 Essentials in etwa den Funktionen der Standard-Edition. Allerdings verfügt Windows Server 2022 Essentials über deutlich weniger Funktionen als der Vorgänger Windows Server 2016 Essentials. Diese Edition ist nur als OEM-Version verfügbar und darf nur auf Servern mit einer CPU und maximal zehn Kernen zum Einsatz kommen.

1.3.1 Neue und nicht mehr vorhandene Funktionen in Windows Server 2022 Essentials

Generell handelt es sich bei der Essentials-Edition von Windows-Servern um eine funktionsreduzierte Version des ehemaligen Small Business Servers. Man merkt schnell, dass Microsoft diese Edition nicht mehr großartig unterstützen will und dass sie vermutlich in den nächsten LTSC-Versionen wegfallen wird. Die Lizenz darf nur auf Servern mit maximal zwei CPUs installiert werden. Es gibt keinerlei Zusatzfunktionen im Vergleich zur Standard-Edition.

Zunächst gibt es in Windows Server 2022 Essentials kein Dashboard mehr und keine Möglichkeit, auf den angebotenen Arbeitsstationen einen Agenten zu installieren, der den Rechner an den Server anbindet und sogar eine Sicherung und Wiederherstellung ermöglicht. Auch der Zugriff über das Internet ist nicht mehr verfügbar, genauso wie der Einrichtungs-Assistent. Microsoft hat die komplette »Essentials-Experience« entfernt, sodass die Installation von Windows Server 2022 Essentials der Installation eines herkömmlichen Servers mit grafischer Oberfläche entspricht.

Microsoft hat das Dashboard ersatzlos gestrichen und weist darauf hin, dass Unternehmen zur Verwaltung das Windows Admin Center nutzen sollen. Nur ist dieses vom Funktionsumfang eher eingeschränkt und bietet auch keine Assistenten zum Anlegen neuer Freigaben mit entsprechenden Berechtigungen. Ebenso wurde die Essentials-Serverrolle in Windows Server 2022 Datacenter und Standard gestrichen.

Windows Server 2022 Essentials unterstützt dafür alle Neuerungen, die auch Windows Server 2022 Standard bietet. Allerdings kann Windows Server 2022 Essentials nicht als Core-Server installiert werden. Bei der Installation wird automatisch die grafische Oberfläche mit installiert. Vom Funktionsumfang entspricht Windows Server 2016/2019/2022 Essentials ansonsten der Standard-Edition. Eine Aktualisierung von Windows Server 2016/2019 Essentials zur Standard- und Datacenter-Edition ist natürlich möglich.

1.3.2 Wann lohnt sich der Einsatz von Windows Server 2022 Essentials?

Der Einsatz von Windows Server 2022 Essentials lohnt sich vor allem dann, wenn in einem kleinen Netzwerk bis maximal 25 Benutzer und 50 Geräte mit Standardaufgaben angebunden werden sollen. Zu den Geräten zählt aber auch der Zugriff mit Smartphones und Tablets. Der Preis der Edition ist günstiger, und wenn die Installation auf einem kleinen Server mit maximal zwei CPUs erfolgt, reicht die Edition oft aus. Sind auf Dauer doch mehr Benutzer auf den Server angewiesen, kann dieser jederzeit zur Standard- oder Datacenter-Edition aufgewertet werden. Dieser Vorgang kann in der PowerShell und Befehlszeile erfolgen. Wir zeigen die Vorgehensweise im nächsten Abschnitt. Wenn in kleinen Netzwerken ein Server gesucht wird, auf dem Dateifreigaben und Druckerfreigaben erstellt werden, kann Windows Server 2022 Essentials hilfreich sein.

Soll auf dem Server aber noch andere Software betrieben werden, ist es sinnvoll, auf weitere Server zu setzen oder die Dienste in der Cloud zu buchen. Vor allem der Einsatz eines E-Mail-Servers inklusive Absicherung und Datensicherung ist auf einem kleinen Server nicht unbedingt sinnvoll. Hier kann es auch für kleine Netzwerke sinnvoll sein, zu Microsoft 365 zu wechseln. Bezüglich der Datensicherung scheiden sich die Geister. Die Daten

lassen sich problemlos lokal sichern, aber vor allem bei kleinen Unternehmen kann es empfehlenswert sein, die Sicherung ebenfalls in der Cloud abzulegen. Allerdings erfordert die Anbindung der Datensicherung an die Cloud eine entsprechend schnelle Datenleitung.

1.3.3 Schneller Wechsel zu Windows Server 2022 Standard/Datacenter möglich



Sie können einen Server mit einer Essentials-Lizenz von Windows Server 2022 ohne Neuinstallation zur Standard-Edition heraufstufen. Von der Standard-Edition können Sie wiederum zur Datacenter-Edition wechseln, ebenfalls ohne erneute Installation.

Nach der Installation eines Windows-Servers müssen Sie die Aktivierung von Windows Server 2022 durchführen. Das gilt für alle Editionen von Windows Server 2022. Mehr Informationen erhalten Sie, wenn Sie im Suchfeld der Taskleiste nach *slui* suchen.

Sie können Windows Server 2022 entweder über das Internet aktivieren oder per Telefon. Bei der Aktivierung per Telefon werden Sie mit einem automatischen Telefonsystem verbunden. Sollten Sie Probleme bei der Aktivierung bekommen, überprüfen Sie die Uhrzeit und die Zeitzone Ihres Servers. Sind die entsprechenden Einstellungen nicht korrekt, können Sie Windows nicht aktivieren.

Über den Befehl *slui* wird ein Dialogfeld geöffnet, um einen neuen Produktschlüssel einzugeben. Starten Sie das Tool über die Suchfunktion des Startmenüs mit Administratorrechten über das Kontextmenü. In diesem Bereich aktivieren Sie Windows Server 2022 dann mit dem neuen Key. Der Befehl *slui 4* öffnet die Auswahl der Aktivierungshotlines.

Wollen Sie sich die aktuelle Windows Server 2022-Edition anzeigen lassen, die auf dem Computer installiert ist, öffnen Sie eine Eingabeaufforderung mit Administratorrechten und geben den Befehl *dism /online /Get-CurrentEdition* ein. Sie erhalten daraufhin die Edition und weitere Information zur Installation angezeigt. Wollen Sie anzeigen, zu welchen Editionen Sie die installierte Version aktualisieren können, verwenden Sie den Befehl *dism /online /Get-TargetEditions*.

Für die Verwaltung und die Abfrage von Lizenzinformationen auf Windows Server 2022-Computern stellt Microsoft das Skript *slmgr.vbs* zur Verfügung, das Sie über die Eingabeaufforderung oder das Dialogfeld *Ausführen* aufrufen. Auch in Windows Server 2022 Essentials ist das Skript verfügbar. Dieses starten Sie mit der Tastenkombination  + . Das Tool kennt verschiedene Optionen:

/ato – Windows online aktivieren

/dli – Zeigt die aktuellen Lizenzinformationen an

/dlv – Zeigt noch mehr Lizenzdetails an

/dlv all – Zeigt detaillierte Infos für alle installierten Lizenzen an

Möchten Sie den Status der Aktivierung von Windows Server 2022 Essentials anzeigen, geben Sie in der Befehlszeile den Befehl *slmgr.vbs /dli* ein und führen diesen aus. Anschließend werden der Name und die Beschreibung des Betriebssystems, aber auch ein Teil des Product Key und der Lizenzstatus angezeigt.

Haben Sie den Produktschlüssel eingetragen, führen Sie die Aktivierung über die beschriebenen Wege durch. Verfügt der Computer über eine Internetverbindung, führt der Assistent die Aktivierung automatisch aus, sobald der korrekte Product Key eingegeben wurde.

1.3.4 Das muss beim Einsatz von Windows Server 2022 Essentials beachtet werden

Entscheiden sich Unternehmen in kleinen Netzwerken, auf Windows Server 2022 Essentials zu setzen, dürfen sich nicht mehr als 25 Benutzer mit 50 PCs mit dem Server verbinden. Eine Installation als Core-Server ist nicht möglich. Wird der Server zum Domänencontroller heraufgestuft, darf es im Active Directory nur einen Domänencontroller geben, auf dem alle Betriebsmasterrollen installiert sind. Fällt der Domänencontroller aus, ist bei kleinen Netzwerken oft guter Rat teuer.

Dazu kommt, dass es keine bidirektionalen Vertrauensstellungen zu anderen Domänen geben darf. Aus diesen Gründen ist es sinnvoll, den Server zu virtualisieren. Als Basis kann der kostenlose Hyper-V-Server 2019 genutzt werden, oder Sie verwenden Windows Server 2022 Essentials als Hyper-V-Host und virtualisieren Ihren eigentlichen Server als VM, ebenfalls mit Windows Server 2022 Essentials.



Mit Windows Server 2022 wird es keinen Nachfolger von Hyper-V Server 2019 geben.

Auf diesem wird Windows Server 2022 Essentials virtualisiert. Durch die Sicherung dieses virtuellen Servers kann die Umgebung nach der Einrichtung einfacher wiederhergestellt werden. Die Sicherung der VM mit Windows Server 2022 Essentials ersetzt aber nicht die Sicherung der Daten auf dem Server. Hier sollte auf jeden Fall auf eine Datensicherung gesetzt werden, die entweder VM und Daten parallel sichern kann oder die nur die Daten sichert.

1.3.5 Zu Windows Server 2022 Essentials migrieren

Da Windows Server 2022 über die gleichen Funktionen wie Windows Server 2022 Standard verfügt, mit sehr wenigen Ausnahmen wie die Core-Installation, lassen sich auch Daten leichter migrieren. Entweder aktualisieren Unternehmen ihren Server direkt zu Windows Server 2022 Essentials oder sie installieren einen neuen Server und übernehmen die Daten mit dem Storage Migration Service in Windows Server 2022. Allerdings kann der Storage Migration Service nur Freigaben und Rechte übernehmen. Er kann natürlich keine Serverdienste, Benutzer oder Domänen migrieren.

1.4 Windows 11 und Windows Server 2022

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

Bei der Umstellung zu Windows 11 müssen Administratoren und Profis natürlich zunächst einiges beachten. Die guten Nachrichten zuerst: Windows 11 steht als kostenloses Update für Windows 10 zur Verfügung. Die meisten Tools, Treiber und Vorgehensweisen, die für

Windows 10 entwickelt sind, funktionieren genauso mit Windows 11. Das Betriebssystem baut direkt auf Windows 10 auf. Windows 11 steht als Featureupdate für Windows 10 zur Verfügung.

Im Grunde genommen ist Windows 11 vor allem nur ein großes Update für Windows 10, ähnlich wie Windows 8.1 das Update für Windows 8 war. Microsoft orientiert sich bei den Bezeichnungen etwas an macOS. Einfach ausgedrückt:

Für Administratoren und Support-Mitarbeiter gibt es keine riesigen Neuerungen. Die Anpassungen sind im Detail zu finden und später vor allem in der Zusammenarbeit mit Windows Server 2022. Während Windows 10 vor allem für Windows Server 2016/2019 optimiert ist, unterstützt Windows 11 natürlich vor allem die neuen Funktionen der neuen Serverversion von Microsoft.

1.4.1 Zu Windows 11 aktualisieren und Systemvoraussetzungen beachten

Windows 10-Rechner lassen sich direkt zu Windows 11 aktualisieren und natürlich soll auch eine Neuinstallation mit Windows 11 kein Problem sein. Für die Aktualisierung zu Windows 11 ist eine installierte Version von Windows 10 Version 2004 notwendig. Derzeit funktioniert die direkte Aktualisierung aber auch von Versionen wie Windows 10 Version 1909. Der neue Cloud-PC von Microsoft mit der Bezeichnung Windows 365 steht nach der Erscheinung von Windows 11 ebenfalls für dieses Betriebssystem zur Verfügung.

Das kleine Open Source-Tool »WhyNotWin11« des Entwicklers Robert C. Maehl (<https://github.com/rcmaehl/WhyNotWin11>) testet ohne Installation, ob die Hardware eines Computers für Windows 11 geeignet ist. Die aktuellen Anforderungen listet Microsoft auf der Seite »Windows 11-Spezifikationen, -Funktionen und -Computeranforderungen suchen« (<https://www.microsoft.com/de-de/windows/windows-11-specifications>) auf. Microsoft Endpoint Manager wird in diesem Zug erweitert und erhält Funktionen, mit denen vorhandene Computer auf die Kompatibilität mit Windows 11 überprüft werden.

Generell ist es aktuell noch möglich, Windows 7 kostenlos zu Windows 10 zu aktualisieren. Ist die Hardware kompatibel, kann über diesen Weg eine kostenlose Aktualisierung zu Windows 11 erfolgen. Wer eine gültige Lizenz für Windows 10 einsetzt, zum Beispiel über Microsoft Enterprise E3 oder E5, kann problemlos zu Windows 11 wechseln.

1.4.2 Weniger Updates pro Jahr mit Windows 11

Was für Administratoren sicher interessant ist, das ist die neue Updatepolitik. Es wird nur noch ein Feature-Update pro Jahr für Windows 11 erscheinen. Das erleichtert Administratoren natürlich die Bereitstellung enorm. Die Updates erhalten von Microsoft eine Unterstützung von 24 bis 36 Monaten.

1.4.3 Neuerungen in Windows 11

Spektakuläre Neuerungen gibt es in Windows 11 nicht. Das Erste, was nach der Installation auffällt, ist das neue Startmenü, das mehr in die Mitte des Bildschirms gerückt ist und grafisch ein bisschen aufgebebbert ist. Auch hier erinnern die Vorgehensweise und das Aussehen etwas an macOS.

Was viele Admins und Benutzer interessiert, ist die Möglichkeit, das Startmenü wieder an seiner angestammten Stelle zu positionieren. Das ist problemlos möglich. Die Einstellungen sind über das Kontextmenü der Taskleiste und der Auswahl von *Taskleisteneinstellungen* zu finden. Über den Menüpunkt *Personalisierung* steht das Menü *Taskleiste* zur Verfügung. Hier sind *Verhalten der Taskleiste* und anschließend *Taskleistenausrichtung* zu finden. Der Standardwert *Zentriert* lässt sich an dieser Stelle zu *Links* ändern.

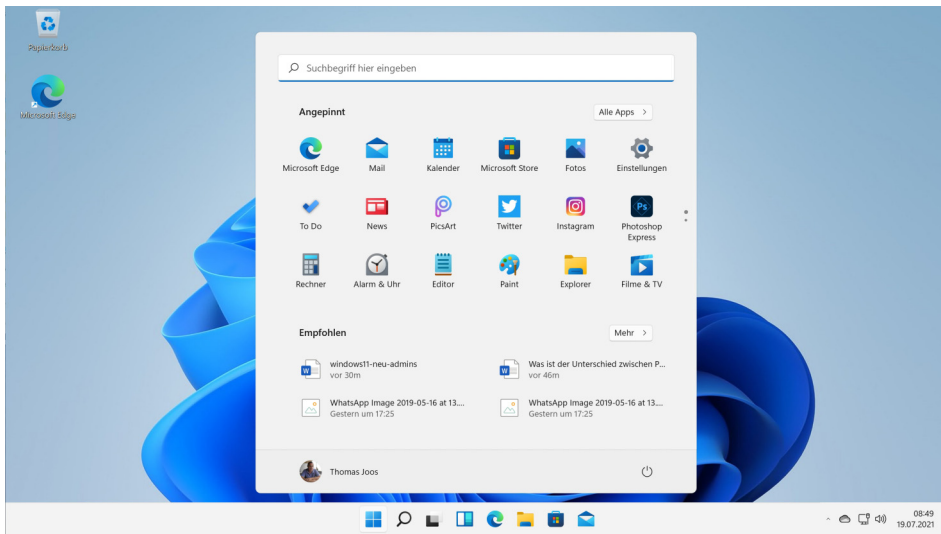


Abb. 1.2 Das neue Startmenü lässt sich auf Wunsch wieder nach links verschieben.

1.4.4 Windows 11 und Microsoft 365

Microsoft bindet Windows 11 noch enger an die Azure-Cloud an. Die Verwaltung des Betriebssystems kann über Microsoft Endpoint Manager erfolgen, genauso wie in Windows 10. Die Anmeldung von Windows 11 Pro/Enterprise ist auch mit einem Benutzerkonto aus Microsoft Azure Active Directory möglich. Ist Microsoft 365 im Einsatz, verbindet sich das Betriebssystem ebenfalls mit verbundenen Bibliotheken in SharePoint Online und zeigt die gespeicherten und häufig verwendeten Dokumente im Startmenü an. Das funktioniert generell einfacher und übersichtlicher als in Windows 10.

Die Icons im Windows-Explorer hat Microsoft in Windows 11 ebenfalls angepasst, das gilt auch für das Kontextmenü von Ordnern und Dateien. Hier sind die wichtigsten Icons in den oberen Bereich gewandert und Microsoft hat das Kontextmenü für das Arbeiten mit Dateien etwas angepasst. Das neue Kontextmenü ist allerdings nicht in Windows Server 2022 integriert.

Neben der engeren Anbindung von Dokumenten aus Microsoft 365 integriert Microsoft auch Kommunikationsmöglichkeiten enger direkt in das Startmenü und die Windows-Oberfläche. Microsoft Teams kann leichter und wesentlich enger in das Betriebssystem und die Benutzerkonten integriert werden.

1.5 Zusammenfassung

In diesem Kapitel haben wir Ihnen die wichtigsten Neuerungen von Windows Server 2022 gezeigt, damit Sie einen Überblick haben, welche neuen Funktionen es gibt. Wir sind in diesem Kapitel auch auf die Editionen und die Lizenzierung eingegangen. In den weiteren Kapiteln des Buchs vertiefen wir die Neuerungen und zeigen die Verwaltung von Windows Server 2022.

Im nächsten Kapitel erfahren Sie, welche Möglichkeiten Sie haben, um Windows Server 2022 zu installieren und einzurichten.

Kapitel 2

Installation und Grundeinrichtung

In diesem Kapitel zeigen wir Ihnen, wie Sie Windows Server 2022 installieren. Wir gehen auch darauf ein, wie Sie erweiterte Installationen durchführen, zum Beispiel mit einem USB-Stick oder auf virtuelle Festplatten, was zum Beispiel für Testumgebungen interessant ist. Wir zeigen Ihnen anschließend, wie Sie Core-Server installieren.



Sie können sich auf der Seite <https://www.microsoft.com/de-de/evalcenter> Testversionen von Windows Server 2022 Standard und Datacenter herunterladen. Auf dieser Seite finden Sie auch die Testversion von Windows 10/11 Enterprise.

Sie können die Testversion bis zu 180 Tage kostenlos einsetzen, müssen sie aber nach spätestens 10 Tage aktivieren. Sie sehen die noch zur Verfügung stehende Testzeit auf dem Desktop oder wenn Sie in der Eingabeaufforderung `slmgr.vbs /dlv` eingeben.

2.1 Grundlagen zur Installation

Windows Server 2022 verfügt wie dessen Vorgängerversionen ab Windows Server 2012/2012R2 über einen Boot-Manager, mit dessen Hilfe Sie auch mehrere Betriebssysteme parallel auf einem Server einsetzen können. Das gilt ebenso für Windows Server 2022. Sie haben die Möglichkeit, das Bootverhalten zu konfigurieren, festzulegen, wie lange der Boot-Manager eingeblendet bleiben soll, um eine Auswahl zu treffen, und können auch das Standardbetriebssystem festlegen. Und auch zusätzliche Betriebssysteme lassen sich einbinden. Interessant ist das vor allem für Entwicklungs- oder Testumgebungen.

2.1.1 Windows Server 2022-Installation verstehen

Windows Server legt eine versteckte Partition auf der Startfestplatte an. In diesem Bereich liegen die Startdateien von Windows und Daten zum Entschlüsseln von BitLocker-Laufwerken (siehe Kapitel 5). Aktualisieren Sie einen Rechner, belässt der Assistent die Startpartition auf einer geringeren Größe. Auch in Windows Server 2022 wird eine solche Partition angelegt.

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

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



Microsoft empfiehlt generell eine Neuinstallation anstelle einer Aktualisierung zu Windows Server 2022 über eine frühere Server-Version.

Die zweite Möglichkeit zum Installieren von Windows Server 2022 ist eine komplette Neuinstallation von Windows Server 2022 auf einem Computer, auf dem bereits eine ältere Version von Windows Server vorhanden ist. In diesem Fall sollten Sie ebenfalls vorher alle Daten von Windows Server sichern. Sie müssen zwar nach der Installation von Windows Server 2022 alle Programme neu installieren und die Daten manuell übernehmen, erhalten dafür aber ein neues, sauberes System. Der Nachteil ist, dass Ihr bisheriges Windows Server-System dann verloren ist. Sie können allerdings das erstellte Image im Notfall verwenden und zurücksichern.

Die dritte Möglichkeit, um Windows Server 2022 zu testen oder in einer Entwicklungsumgebung zu betreiben, ist die Installation auf einer zweiten Partition oder Festplatte des Rechners. Auch hier können Sie eine Neuinstallation von Windows Server 2022 durchführen, eine frühere Windows Server-Version (ab 2012) verbleibt dabei auf der Festplatte. Bei der Installation von Windows Server 2022 wird auch der Boot-Manager durch die Windows Server 2022-Version ersetzt. Daten können Sie per Kopiervorgang übernehmen und Ihr bestehendes Windows-System bleibt erhalten.

Die vierte Möglichkeit, um Windows Server 2022 zu testen, entspricht in etwa der Parallelinstallation aus dem vorherigen Absatz. Hier nutzen Sie aber keine zweite Partition, sondern erstellen während der Installation eine virtuelle Festplatte (VHDX) und installieren Windows Server 2022 in diese VHDX-Datei. Der Vorteil ist, dass Sie dabei die Hardware Ihres Computers nutzen, das parallele Windows unangetastet bleibt und Sie dennoch Windows Server 2022 produktiv nutzen, zum Beispiel für eine Entwicklungsumgebung. Dabei speichert Windows Server 2022 alle Daten in einer VHDX-Datei, ersetzt aber den alten Boot-Manager. Sie können über diesen Weg auch Hyper-V testen, also in der virtuellen Festplatte die Virtualisierung installieren. Allerdings ist das nur für Testumgebungen oder zur Entwicklung sinnvoll, nicht für den produktiven Einsatz.

Starten Sie Windows Server 2022, mountet das System die VHDX-Datei und Sie können fast genauso schnell arbeiten wie mit einer echten Festplatte. Die meisten Administratoren werden keine Einschränkungen bemerken. Windows Server 2022 verfügt bereits standardmäßig über eine Vielzahl an Treibern.

Finden Sie beim Hersteller des Geräts keinen passenden Treiber und ist in Windows Server 2022 kein Treiber integriert, können Sie auch Windows Server 2016/2019-Treiber in Windows Server 2022 nutzen. Das sollten Sie aber nur in Ausnahmefällen tun. Programme, die in alten Versionen von Windows laufen, funktionieren oft auch in Windows Server 2022. Allerdings sollten Sie unter keinen Umständen Systemprogramme wie Virens Scanner, Optimierungstools oder Anwendungen für die Datensicherung in Windows Server 2022 nutzen, die der Hersteller nicht für diese Version freigegeben hat. Auch ältere Serverprodukte sollten Sie erst mit Windows Server 2022 betreiben, wenn Updates oder Patches verfügbar sind.

2.1.2 Installation von Windows Server 2022 vorbereiten

Damit Sie Windows Server 2022 installieren können, müssen Sie zunächst die Systemvoraussetzungen beachten und einige Dinge vorbereiten. Unabhängig von den Neuerungen in Windows Server 2022 und den verwendeten Serverdiensten muss der Prozessor des Servers gewisse Mindest-Voraussetzungen erfüllen, damit er kompatibel mit der neuen Server-Version ist:

- 1,4-GHz-64-bit-Prozessor
- 64-Bit-Kompatibilität
- NX und DEP
- CMPXCHG16b, LAHF/SAHF und PrefetchW
- Second Level Address Translation (Intel Extended Page Table (EPT) oder AMD Nested Page Table (NPT)).
- 512 MB RAM

Bei der Installation eines Plug-and-play-Geräts werden Sie unter Umständen darauf hingewiesen, dass der Treiber nicht digital signiert ist. Bei der Installation einer Anwendung, die einen nicht digital signierten Treiber enthält, wird beim Setup kein Fehler angezeigt. In beiden Fällen wird der nicht signierte Treiber von Windows Server nicht geladen. Wollen Sie diese Funktion umgehen, deaktivieren Sie die Prüfung für nicht signierte Treiber:

1. Starten Sie den Computer neu, und drücken Sie beim Start die **F8**-Taste.
2. Wählen Sie im Fenster *Erweiterte Startoptionen* den Eintrag *Erzwingen der Treibersignatur deaktivieren* aus.
3. Starten Sie Windows Server 2022.

Wenn der Computer mit einer unterbrechungsfreien Stromversorgung (USV) verbunden ist, trennen Sie vor dem Ausführen von Setup das serielle oder USB-Kabel dieses Geräts. Das Installationsprogramm von Windows Server 2022 versucht automatisch, die Geräte an den seriellen Anschlüssen oder USB-Geräten zu erkennen. Eine USV kann zu Problemen bei diesem Vorgang führen und die Installation deutlich ausbremsen oder sogar mit einem Fehler abbrechen lassen.

Sichern Sie den Server. Ihre Sicherung sollte alle erforderlichen Daten und Konfigurationsdateien für eine ordnungsgemäße Ausführung des Servers einschließen. Daten wie die Einstellungen von DHCP-Servern, Netzwerkeinstellungen, aber auch andere Daten sind wichtig für den Betrieb des Servers nach der Installation.

Deaktivieren Sie die Virenschutzsoftware des Netzwerks für diesen Server, genauso wie die Überwachung durch Managementlösungen.

2.2 Windows Server 2022 neu installieren

In diesem Abschnitt erläutern wir Ihnen, wie Sie Windows Server 2022 neu installieren. Wir zeigen Ihnen auch, wie Sie Windows Server 2022 über einen USB-Stick installieren. Die Installation über einen USB-Stick läuft schneller ab und Sie können damit Windows Server 2022 auch auf Geräten installieren, die über kein DVD-Laufwerk verfügen. Generell lässt sich die ISO-Datei von Windows Server 2022 ohnehin schwer auf DVD brennen, da deren Größe die Kapazität der meisten Rohlinge übersteigt.

Die Windows Server 2022-Bereitstellung basiert auf Images. Bei Images handelt es sich quasi um eine Kopie eines installierten Betriebssystems. Windows Server 2022 arbeitet (wie bereits die Vorgängerversionen ab 2012) mit dem WIM-Imageformat (Microsoft Windows Imaging). Statt eines sektorbasierten Imageformats ist das WIM-Format dateibasiert. Dies hat mehrere Vorteile:

- **WIM ist hardwareunabhängig** – Das bedeutet, Sie brauchen nur ein Image für verschiedene Hardwarekonfigurationen. Mit WIM können mehrere Images in einer Datei gespeichert werden. Sie können Images mit und ohne Anwendungen in einer Datei speichern. WIM nutzt eine Kompression und ein Single-Instance-Verfahren. So wird die Größe von Imagedateien deutlich reduziert. Single-Instancing ist eine Technologie, bei der jede Datei nur einmal gespeichert wird. Wenn zum Beispiel Image 1, 2 und 3 alle die Datei A enthalten, dann sorgt Single-Instancing dafür, dass Datei A tatsächlich nur einmal gespeichert wird.
- **WIM ermöglicht die Offlinebearbeitung von Images** – Sie können Betriebssystemkomponenten, Patches und Treiber hinzufügen oder löschen, ohne ein neues Image erstellen zu müssen. Mit WIM können Images auf Partitionen jeder Größe installiert werden. Sektorbasierte Imageformate benötigen eine Partition der gleichen Größe oder eine größere Partition. Mit WIM können auf dem Zielvolumen vorhandene Daten beibehalten werden. Das Einrichten eines Images löscht nicht zwingend alle vorhandenen Daten auf der Festplatte.

2.2.1 Windows Server 2022-Installation durchführen

Unabhängig davon, ob Sie Windows Server 2022 über eine DVD oder einen USB-Stick installieren, müssen Sie den entsprechenden Datenträger mit dem Computer verbinden und im BIOS oder den Booteinstellungen vom Datenträger aus starten. Das gilt auch für den Start mit einer ISO-Datei. Anschließend beginnt der Installations-Assistent von Windows Server 2022 mit seiner Arbeit. In den meisten Fällen erscheint das Bootmenü nach dem Drücken einer Taste auf der Tastatur. Welche das ist, sehen Sie beim Starten des Rechners.

Die Installation von Windows Server 2022 findet bereits beim Starten in einer grafischen Oberfläche statt, es gibt keinen textorientierten Teil mehr. Außerdem werden weniger Fenster angezeigt und es sind weniger Eingaben für die Installation erforderlich. Es werden die meisten Eingaben bereits vor Beginn der Installation durchgeführt, sodass der Computer während der Installation nicht die ganze Zeit beaufsichtigt werden muss. Sie benötigen für die Installation ein bootfähiges DVD-Laufwerk oder einen USB-Stick.



Abb. 2.1 Starten einer Windows Server 2022-Installation

Im ersten Schritt wählen Sie die Installationsprache, das Uhrzeit- und Währungsformat sowie die Tastatur- oder Eingabemethode aus und klicken auf *Weiter*.

Auf der nächsten Seite starten Sie entweder mit *Jetzt installieren* die eigentliche Installation oder durch Auswahl von *Computerreparaturoptionen* die Systemwiederherstellung von Windows Server 2022.

Starten Sie die Installation, müssen Sie im nächsten Schritt den Product Key eingeben, wenn Sie keine spezielle Edition von Windows Server 2022 einsetzen. Sie können dazu entweder die Tastatur des Rechners oder die Bildschirmtastatur nutzen. Den Produktschlüssel können Sie aber auch jederzeit nach der Installation eingeben.

Im nächsten Schritt wählen Sie aus, ob Sie eine Server Core-Installation durchführen wollen (Standardauswahl) oder eine Installation eines Servers mit grafischer Oberfläche (*Desktopdarstellung*). Die Installation als Core-Server ist standardmäßig ausgewählt.



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

Zu installierendes Betriebssystem auswählen

| Betriebssystem | Architektur | Geändert am |
|--|-------------|-------------------|
| Windows Server 2022 Standard Evaluation | x64 | 08.05.2021 |
| Windows Server 2022 Standard Evaluation (Desktopdarstell... | x64 | 08.05.2021 |
| Windows Server 2022 Datacenter Evaluation | x64 | 08.05.2021 |
| Windows Server 2022 Datacenter Evaluation (Desktopdarstell... | x64 | 08.05.2021 |

Beschreibung:
Durch diese Option wird die vollständige grafische Umgebung von Windows installiert, wodurch zusätzlicher Speicherplatz verbraucht wird. Sie kann hilfreich sein, wenn Sie den Windows-Desktop verwenden möchten oder über eine App verfügen, die die grafische Umgebung benötigt.

Abb. 2.2 Auswählen der Installationsvariante von Windows Server 2022

Ein Core-Server verfügt über keine grafische Oberfläche, keine Shell, keine Mediafunktionen und keinerlei Zusatzkomponenten, außer den notwendigen Serverdiensten. Der Anmeldebildschirm sieht allerdings identisch aus, Sie müssen sich nach der Installation über die Tastenkombination **[Strg] + [Alt] + [Entf]** anmelden. Sobald Sie sich angemeldet haben, sehen Sie in Windows Server 2019 nur eine Eingabeaufforderung. In Windows Server 2022 wird automatisch Sconfig geöffnet.

Zur Bearbeitung der Einstellungen des Servers kann es manchmal notwendig sein, den Editor (Notepad) zu nutzen, das ist in der Core-Installation möglich. Es gibt aber keinen Windows-Explorer oder Internet Explorer, Microsoft Edge und keinen Registrierungseditor (Regedit). Durch diese Funktion können die Standardfunktionen von Windows Server 2022 betrieben werden, ohne dass der Server durch unwichtige Komponenten belastet oder kompromittiert werden kann. Als Serverrollen können Sie auf Core-Servern folgende Rollen installieren:

- Active Directory-Zertifikatdienste (siehe Kapitel 30)
- Active Directory-Domänendienste (siehe Kapitel 11 bis 19)
- DHCP-Server (siehe Kapitel 24)
- DNS-Server (siehe Kapitel 25)
- Dateidienste (einschließlich Ressourcen-Manager für Dateiserver, siehe Kapitel 20 bis 23)
- Active Directory Lightweight Directory Services (AD LDS)

- Hyper-V (siehe Kapitel 7, 8 und 9)
- Druck- und Dokumentdienste (siehe Kapitel 20 bis 23)
- Streaming Media-Dienste
- Webserver (einschließlich ASP.NET, siehe Kapitel 27)
- Windows Server Update Services (siehe Kapitel 37)
- Active Directory-Rechteverwaltungsserver (siehe Kapitel 33)
- Routing- und RAS-Server (siehe Kapitel 32)

Mehr zu diesem Thema lesen Sie auch in Kapitel 3 und 4.

Um einen Server neu zu installieren, wechseln Sie zur nächsten Seite des Assistenten und akzeptieren Sie die Lizenzbedingungen. Wählen Sie danach aus, ob Sie ein bereits installiertes Betriebssystem aktualisieren oder Windows Server 2022 neu installieren möchten. Bei einer Neuinstallation wählen Sie *Benutzerdefiniert* aus. Wollen Sie eine Aktualisierung durchführen, wählen Sie *Upgrade*.

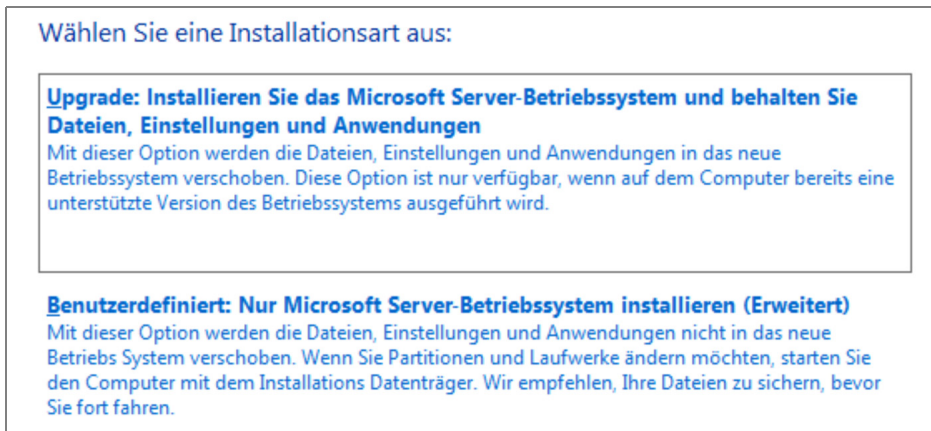


Abb. 2.3 Auswählen der Installationsvariante

Durch diese Auswahl haben Sie auch die Möglichkeit, erweiterte Einstellungen für die Partitionierung durchzuführen. Die *Upgrade*-Option steht nur dann zur Verfügung, wenn Sie das Setupprogramm aus jener Windows-Installation heraus starten, die Sie aktualisieren wollen. Booten Sie das Windows Server 2022-Installationsprogramm von DVD, ist nur die Option *Benutzerdefiniert* sinnvoll.

Nachdem Sie die Installationsart ausgewählt haben, gelangen Sie zum nächsten Fenster der Installationsoberfläche. Hier wählen Sie die Partition aus, auf der Windows Server 2022 installiert werden soll. In diesem Fenster können Sie auch zusätzliche Treiber laden, wenn die Controller für die Festplatten nicht erkannt werden. Klicken Sie dazu auf den Link *Treiber laden*.

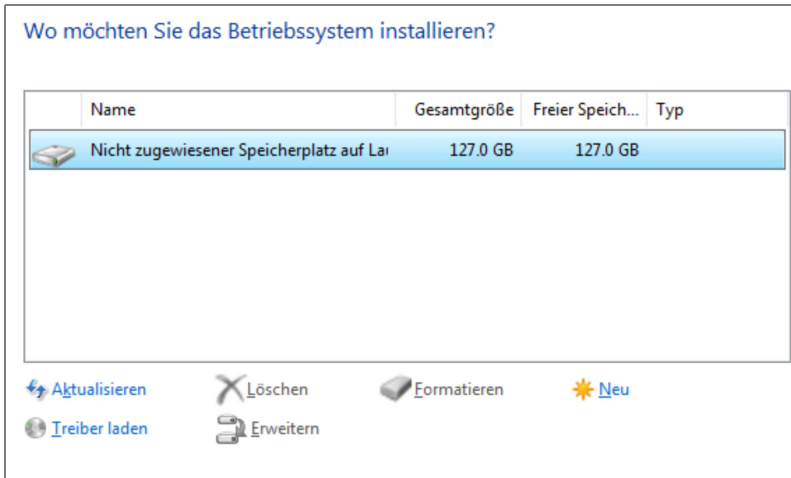


Abb. 2.4 Auswählen der Partition für die Installation

Wollen Sie die Partitionierung ändern, klicken Sie auf den Link *Neu*.

Systempartitionen und Startpartitionen sind Bezeichnungen für Partitionen oder Volumes auf einer Festplatte, die zum Starten von Windows verwendet werden. Die Systempartition enthält die hardwarebezogenen Dateien, die einem Computer mitteilen, von wo aus Windows gestartet werden kann. Eine Startpartition ist eine Partition, die die Windows-Betriebssystemdateien enthält, die sich im Windows-Dateiordner befinden.

Wenn Sie den Computer einschalten, werden die auf der Systempartition verwendeten Informationen zum Starten des Computers verwendet. Auf einem Windows-basierten Computer ist nur eine Systempartition vorhanden, auch wenn auf dem Computer verschiedene Windows-Betriebssysteme installiert sind. Nicht-Windows-Betriebssysteme verwenden andere Systemdateien.

Wenn auf einem Multiboot-Computer ein Nicht-Windows-Betriebssystem installiert ist, befinden sich die dazugehörigen Systemdateien auf einer eigenen Partition, getrennt von der Windows-Systempartition.

Mit einem Klick auf *Weiter* beginnt die Installation. Diese ist seit der Version 2012 von Windows Server imagebasiert. Abhängig von der Leistung des Rechners startet die Installationsroutine den Computer nach 10 bis 20 Minuten automatisch neu. Sie müssen keine weiteren Eingaben durchführen und keine Taste drücken. Sollten Sie versehentlich eine Taste gedrückt haben und die Installation startet wieder von der DVD, schalten Sie den Rechner aus und starten ihn erneut.

Der Computer bootet und es wird ein Fenster geöffnet, über das Sie informiert werden, dass der Rechner für den ersten Start von Windows vorbereitet wird. Lassen Sie den Rechner am besten ungestört weiterarbeiten. Es kann sein, dass der Bildschirm während der Installation der Monitor- und Grafikkartentreiber ein paar Mal flackert oder schwarz wird. Dies ist normal und muss Sie nicht beunruhigen.

Sobald der Assistent seine Arbeit abgeschlossen hat, erscheint die Abfrage für das gewünschte Administrator Kennwort, das Sie zur Sicherheit zwei Mal nacheinander eingeben müssen. Achten Sie beim Kennwort darauf, mindestens einen Großbuchstaben und eine Zahl oder ein Sonderzeichen zu verwenden.

Anschließend melden Sie sich mit der Tastenkombination **Strg** + **Alt** + **Entf** am Server an. Als Anmeldenamen verwenden Sie *Administrator* und das zuvor festgelegte Kennwort. Nach der Anmeldung startet automatisch der Server-Manager (siehe Kapitel 3). Wollen Sie das nicht, können Sie die Willkommen-Kachel und den Autostart verhindern.



Über das Menü *Ansicht* können Sie die Willkommen-Kachel deaktivieren. Und wenn Sie verhindern wollen, dass der Server-Manager automatisch mit Windows startet, wählen Sie im Menü *Verwalten* den Eintrag *Server-Manager-Eigenschaften* und aktivieren das Kontrollkästchen *Server-Manager beim Anmelden nicht automatisch starten*.

Für die Installation von Treibern benötigen Sie teilweise Microsoft Edge. Bei Windows Server 2022 ist automatisch die verstärkte Sicherheit des Internet Explorers aktiv, was beim Herunterladen von Treibern oder bei Test- und Entwicklungsumgebungen durchaus stören kann, auch wenn in Windows Server 2022 Microsoft Edge als Browser bereits vorinstalliert ist. Sie können die erweiterte Sicherheit des Internet Explorers/Microsoft Edge im Server-Manager deaktivieren. Allerdings ist das aus Sicherheitsgründen nicht empfehlenswert. Die Sicherheit sollte im produktiven Betrieb eingeschaltet bleiben.

1. Öffnen Sie den Server-Manager.
2. Klicken Sie auf der linken Seite auf *Lokaler Server*.
3. Klicken Sie im rechten Bereich im Abschnitt *Eigenschaften* neben *Verstärkte Sicherheitskonfiguration für IE* auf den Link *Ein*. Es ist zu erwarten, dass Microsoft in Updates für Windows Server 2022 hier auch Microsoft Edge als Bezeichnung integriert.
4. Wählen Sie im daraufhin geöffneten Dialogfeld die Option *Aus* für alle Benutzer oder nur für Administratoren.

2.2.2 USB-Stick für Windows Server 2022 erstellen

Liegen Ihnen die Windows Server 2022-Installationsdateien im ISO-Format vor, können Sie die ISO-Datei im Betriebssystem bereitstellen und auf deren Basis einen bootfähigen USB-Stick erstellen. Damit die Image-Datei von Windows Server 2022 (*install.wim*) auf einen USB-Stick mit dem FAT32-Dateisystem passt, müssen Sie diese unter Umständen aufteilen. Das hängt von der Größe des Installationsimages ab. Ansonsten können Sie die Datei nicht kopieren. Das Aufteilen ist aber kein komplizierter Vorgang. Sie können in einem ersten Schritt versuchen, ob die WIM-Datei problemlos kopierbar ist. Erhalten Sie einen Kopierfehler, teilen Sie die Datei auf und gehen dazu vor, wie nachfolgend erläutert.

Der Befehl dazu sieht zum Beispiel folgendermaßen aus:

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

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

USB-Stick manuell erstellen – auch mit gesplitteten SWM-Dateien

Sie können den USB-Stick auch zukünftig für das Speichern von Daten nutzen, zum Beispiel für Treiber. Die Installationsdateien belegen etwa einen Platz von 3,5 GB:

1. Starten Sie eine Eingabeaufforderung über das Kontextmenü im Administratormodus.
2. Geben Sie *diskpart* ein.
3. Geben Sie *list disk* ein.
4. Geben Sie den Befehl *select disk <Nummer des USB-Sticks aus list disk>* ein. Sie erkennen den Stick an dessen Größe.
5. Geben Sie *clean* ein.
6. Geben Sie *create partition primary* ein.
7. Geben Sie *active* ein, um die Partition zu aktivieren. Dies ist für den Bootvorgang notwendig, denn nur so kann der USB-Stick booten.
8. Formatieren Sie den Datenträger mit *format fs=fat32 quick*.
9. Geben Sie den Befehl *assign* ein, um dem Gerät im Explorer einen Laufwerksbuchstaben zuzuordnen.
10. Beenden Sie Diskpart mit *exit*.
11. Kopieren Sie den kompletten Inhalt der Windows Server 2022-DVD/ISO-Datei in den Stammordner des USB-Sticks. Anstatt der Datei *install.wim* aus dem Verzeichnis *sources* kopieren Sie aber die beiden erstellten SWM-Dateien. Der Installations-Assistent erkennt die Dateien und verwendet sie, wie die *install.wim*.
12. Booten Sie einen Computer mit diesem Stick, startet die Windows Server-Installation.



Soll der Stick auch UEFI beherrschen, sollte überprüft werden, ob die Datei *Bootx64.efi* im Verzeichnis *\efi\boot* auf dem Stick vorhanden ist. Ist sie das nicht, kann die Datei von jedem Windows 10/11 auf den Stick kopiert werden.

Dazu wird auf dem Rechner das Verzeichnis *C:\Windows\Boot\Efi* geöffnet. Hier befindet sich die Datei *bootmgfw.efi*. Die Datei muss auf den USB-Stick in das Verzeichnis *\EFI\BOOT* kopiert und in *BOOTX64.EFI* umbenannt werden. Ist das Verzeichnis nicht vorhanden, muss es angelegt werden. Danach ist der Stick UEFI-fähig.

2.3 Zu Windows Server 2022 aktualisieren

Im folgenden Abschnitt zeigen wir Ihnen, wie Sie ein bestehendes Windows Server-System direkt zu Windows Server 2022 aktualisieren.



Sie können von Windows Server 2012/2016/2019 direkt zu Windows Server 2022 aktualisieren, ohne das Betriebssystem neu installieren zu müssen.

Sie können entweder identische Editionen aktualisieren, also Windows Server 2016/2019 Standard zu Windows Server 2022 Standard, oder zu höherwertigen Editionen, also Standard-Edition zu Datacenter-Edition. Vor der Aktualisierung sollten Sie das Quell-Betriebssystem auf den neuesten Stand bringen.



Core-Installationen von Windows Server 2016/2019 lassen sich nur zu Core-Installationen von Windows Server 2022 aktualisieren.

Starten Sie das Installationsprogramm im laufenden Betrieb von Windows Server 2016/2019. Sie werden auf eventuelle Probleme hingewiesen und müssen diese vor der Aktualisierung bestätigen.



Bevor Sie zu Windows Server 2022 aktualisieren, sollten Sie eine Systemabbildsicherung Ihres aktuellen Server-Betriebssystems erstellen. Der Vorteil dabei ist, dass Sie bei Problemen schnell und einfach Ihr bisheriges Windows Server-System wiederherstellen können.

Mit dem kostenlosen Tool Disk2vhd von Sysinternals können Sie physische Festplatten in eine VHDx-Datei sichern und diese später zur Wiederherstellung von Daten nutzen. Die VHDx-Datei können Sie auch in Windows Server 2022 als Festplatte einbinden. Dazu starten Sie durch Eingabe von `diskmgmt.msc` auf der Startseite den Festplatten-Manager und fügen die virtuelle Festplatte an.

Nach dem Download von Disk2vhd (<https://docs.microsoft.com/en-us/sysinternals/downloads/disk2vhd>) können Sie das Tool direkt ohne Installation starten. Legen Sie zunächst den Pfad und den Namen der anzulegenden VHDx-Datei fest.

Beachten Sie vor der Aktualisierung die folgenden wichtigen Aktionen:

- Bevor Sie einen Server direkt auf Windows Server 2022 aktualisieren, sollten Sie zunächst installierte Sicherheitsprogramme und Antivirenschutzprogramme deaktivieren.
- Arbeiten Sie mit Netzwerküberwachungsprogrammen, sollten Sie beachten, dass Sie den zu aktualisierenden Computer in den Wartungsmodus versetzen.
- Achten Sie darauf, dass alle installierten Anwendungen, Management Packs für Netzwerküberwachungsprogramme und Tools kompatibel zu Windows Server 2022 sind. Aktualisieren Sie die Programme nach der Installation von Windows Server 2022.
- Achten Sie darauf, dass die Windows-Firewalleinstellungen Verbindungen zu anderen Servern nicht blockieren und bestimmte IPsec-Regeln nicht gesetzt sind.

2.3.1 Aktualisierung zu Windows Server 2022 durchführen

In diesem Abschnitt zeigen wir Ihnen, wie Sie zu Windows Server 2022 aktualisieren. Dazu muss Windows Server gestartet sein und fehlerfrei funktionieren.

Starten Sie Windows Server und legen Sie die Windows Server 2022-DVD in das DVD-Laufwerk. Alternativ starten Sie den Server mit einem USB-Stick. Klicken Sie dann auf `setup.exe`, um die Installation zu starten. Klicken Sie auf *Jetzt installieren*. Im nächsten Schritt erhalten Sie die Möglichkeit, die Installationsdateien zu aktualisieren. Dazu sollten Sie die Option *Online gehen, um jetzt Updates zu installieren* auswählen. Anschließend sucht der Assistent nach Updates und bindet diese in die Installation mit ein. Dies ist nicht

zwingend notwendig, aber empfohlen. Im Rahmen der Aktualisierung fragt Sie der Assistent auch, ob Sie die installierten Programme und Einstellungen erhalten wollen oder ob er alles entfernen soll.

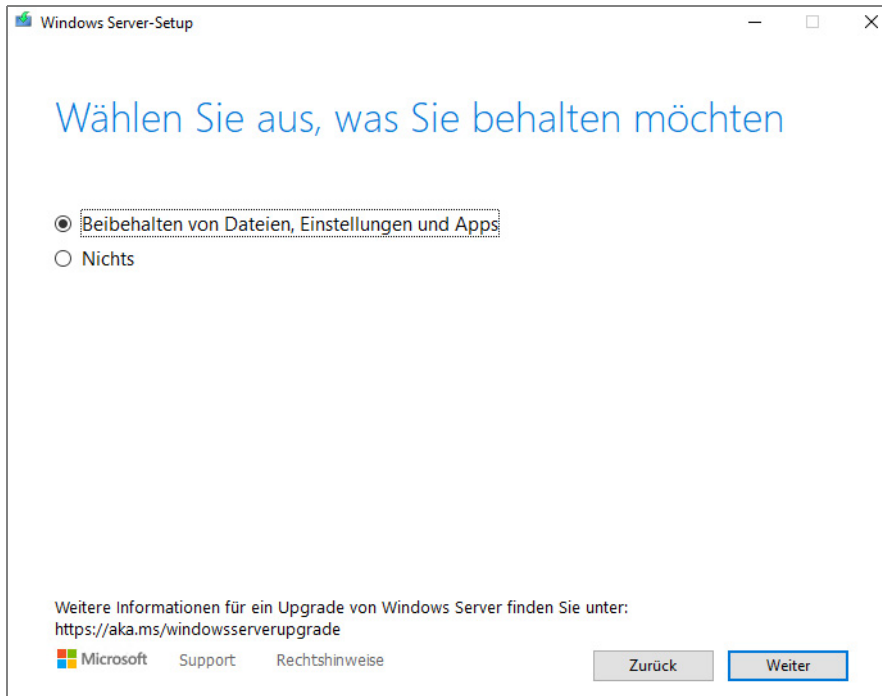


Abb. 2.5 Aktualisieren auf Windows Server 2022

Erscheint die Abfrage des Product Keys für die Installation, geben Sie die Seriennummer ein. Auf Basis der Seriennummer entscheidet es sich, ob Sie Windows Server 2022 in der Standard- oder Datacenter-Edition installieren. Im unteren Feld erhalten Sie nach wenigen Sekunden den Hinweis, dass der Installations-Assistent den Schlüssel verifiziert hat. Klicken Sie dann auf *Weiter*.

Im nächsten Fenster wählen Sie aus, ob Sie einen Core-Server oder einen Server mit grafischer Benutzeroberfläche installieren wollen. Sie können von einem herkömmlichen Server nicht zu einer Core-Installation von Windows Server 2022 aktualisieren.

Im nächsten Schritt bestätigen Sie die Lizenzbedingungen. Danach erscheint ein Fenster, in dem Sie auswählen können, welche Daten Sie übernehmen wollen. Am besten belassen Sie hier die Auswahl auf *Upgrade: Windows installieren und Dateien, Einstellungen und Anwendungen behalten*. Klicken Sie auf *Weiter*, führt der Assistent noch verschiedene Vorbereitungen zur Installation durch. Nach der Installation startet der Einrichtungs-Assistent von Windows Server 2022, genauso wie bei einer Neuinstallation.

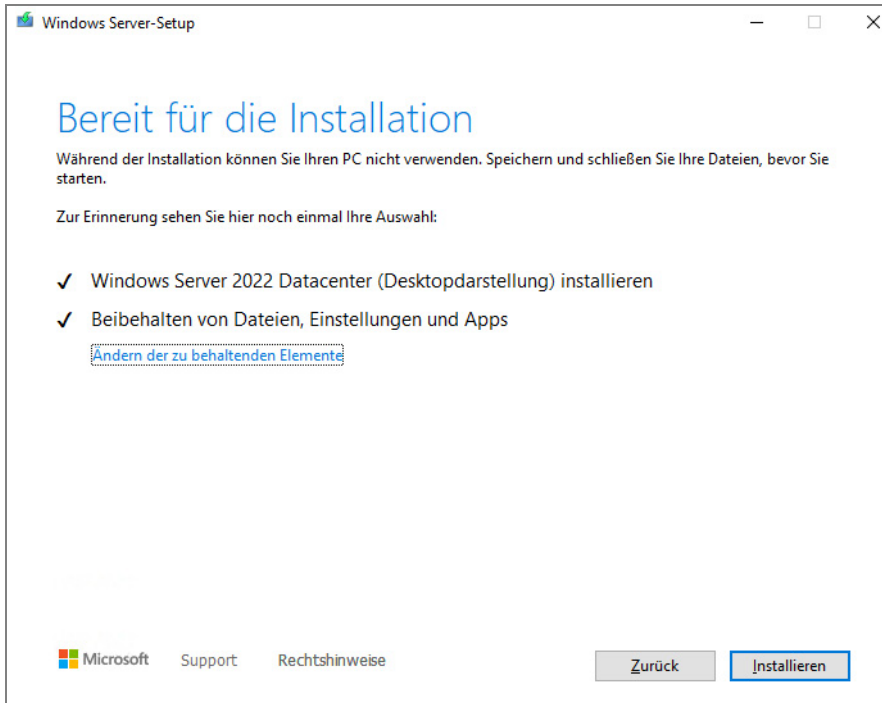


Abb. 2.6 Erfolgreiche Überprüfung einer möglichen Aktualisierung zu Windows Server 2022

2.3.2 Upgrade von Standard- und Testversion auf Datacenter-Edition

Haben Sie Windows Server 2022 Standard installiert, können Sie auf die Datacenter-Edition aktualisieren. Sie müssen dazu Windows nicht neu installieren, die Aktualisierung kann im laufenden Betrieb erfolgen. Sie müssen lediglich nach der Aktualisierung den Server neu starten.

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

Sie haben auch die Möglichkeit, die Testversionen von Windows Server 2022 zu einer vollwertigen Version umzuwandeln. Ob es sich bei der Version um eine Testversion handelt, sehen Sie durch Eingabe des Befehls `slmgr.vbs /dlv`. Auch in der Testversion sehen Sie mit `dism /online /Get-TargetEditions`, auf welche Edition Sie aktualisieren können. Die aktuelle Edition lassen Sie mit `dism /online /Get-CurrentEdition` anzeigen.

Eine Aktualisierung nehmen Sie mit dem gleichen Befehl vor wie bei der Aktualisierung von Standard zu Datacenter. Sie können auf diesem Weg von der Testversion von Windows Server 2022 Datacenter zur lizenzierten Version von Windows Server 2022 Datacenter wechseln. Der Server muss dazu mindestens zweimal neu starten.

2.4 Nacharbeiten zur Installation von Windows Server 2022

Bevor wir in den nächsten Kapiteln ausführlicher auf die Einrichtung und Verwaltung von Windows Server 2022 eingehen, zeigen wir Ihnen in den nächsten Abschnitten die wichtigsten Schritte, die nach der Installation notwendig sind.

Haben Sie die Installation von Windows Server 2022 abgeschlossen, sollten Sie einige erste Aufgaben durchführen, um zu überprüfen, ob das System funktioniert. Auch die Aktivierung gehört zu diesen Aufgaben.

2.4.1 Windows Server 2022 aktivieren

Nach der Installation müssen Sie die Aktivierung von Windows Server 2022 durchführen. Installieren Sie eine VM auf einem Hyper-V-Host, der über eine aktivierte Lizenz von Windows Server 2022 verfügt, wird die VM automatisch aktiviert. In den meisten Fällen müssen Sie aber den Produktschlüssel manuell eingeben und das Betriebssystem aktivieren. Mehr Informationen erhalten Sie, wenn Sie im Startmenü nach *slui* suchen.

Sie können Windows Server 2022 entweder über das Internet aktivieren oder per Telefon. Bei der Aktivierung per Telefon werden Sie mit einem automatischen Telefonsystem verbunden.




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

Über den Befehl *slui 3* wird ein Dialogfeld geöffnet, um einen neuen Produktschlüssel einzugeben. Starten Sie das Tool über die Suchfunktion des Startmenüs mit Administratorrechten über das Kontextmenü. In diesem Bereich aktivieren Sie Windows Server 2022 dann mit dem neuen Key.

Der Befehl *slui 4* öffnet die Auswahl der Aktivierungshotlines. Wollen Sie sich die aktuelle Windows Server 2022-Edition anzeigen lassen, die auf dem Computer installiert ist, öffnen Sie eine Eingabeaufforderung mit Administratorrechten und geben den Befehl *dism /online /Get-CurrentEdition* ein. Sie erhalten daraufhin die Edition und weitere Information zur Installation angezeigt.

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

Für die Verwaltung und die Abfrage von Lizenzinformationen auf Windows Server 2022-Computern stellt Microsoft das Skript *slmgr.vbs* zur Verfügung, das Sie über die Eingabeaufforderung oder das Dialogfeld *Ausführen* aufrufen. Dieses starten Sie mit der Tastenkombination  + [R]. Das Tool kennt verschiedene Optionen:

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

Möchten Sie den Status der Aktivierung von Windows Server 2022 anzeigen, geben Sie in der Befehlszeile den Befehl `slmgr.vbs /dli` ein und führen diesen aus. Anschließend werden der Name und die Beschreibung des Betriebssystems, aber auch ein Teil des Product Keys und der Lizenzstatus angezeigt.

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

Sie können den Product Key einer Windows Server 2022-Installation ändern. Über diesen Weg aktivieren Sie Windows Server 2022 auch auf einem Core-Server:

1. Geben Sie zum Löschen des alten Product Keys in der Eingabeaufforderung den Befehl `slmgr /upk` ein. Zwar ersetzen die nächsten Punkte den vorhandenen Product Key. Allerdings funktioniert das nicht immer, wenn nicht zuvor die alte Nummer gelöscht wurde.
2. Bestätigen Sie das Löschen.
3. Den neuen Product Key geben Sie dann mit `slmgr /ipk xxxxx-xxxxx-xxxxx-xxxxx-xxxxx` ein.
4. Mit `slmgr /ato` aktivieren Sie Windows Server 2022.

Da ein Core-Server über keine grafische Oberfläche verfügt, müssen Sie einen solchen Server über die Eingabeaufforderung aktivieren. Verwenden Sie zur lokalen Aktivierung des Servers den Befehl `slmgr.vbs -ato`.

Nach Eingabe des Befehls wird die Aktivierung durchgeführt. Sie können Windows Server 2022 auch remote über das Netzwerk aktivieren. Verwenden Sie dazu den Befehl `slmgr.vbs <ServerName> <Benutzername> <Kennwort> -ato`.

Um einen Server lokal über das Telefon zu aktivieren, verwenden Sie den Befehl `slmgr -dti`. Notieren Sie sich die ID, die generiert wird, und rufen Sie die Aktivierungsnummer von Microsoft an. Geben Sie über die Telefontasten die ID ein und Sie erhalten vom Telefoncomputer eine Aktivierungs-ID. Diese geben Sie mit dem Befehl `slmgr -atp <Aktivierungs-ID>` ein. Sie können die Edition eines Core-Servers auch aktualisieren, indem Sie in der Eingabeaufforderung Änderungen vornehmen:

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

2.4.2 Treiberinstallation überprüfen

Nach der Installation sollten Sie auch überprüfen, ob Windows Server 2022 alle Geräte erkannt hat, die in Ihrem Computersystem verbaut sind. Geben Sie dazu im Suchfeld der Taskleiste `devmgmt.msc` ein und stellen Sie sicher, dass keine unbekanntenen Geräte vorhanden und alle Treiber installiert sind. Vor allem den Treiber des Netzwerkadapters und der Systemgeräte sollten Sie überprüfen.

Mit dem Befehl `Msinfo32` können Sie eine sehr ausführliche Übersicht über die eingebaute Hardware und die Ressourcen eines PC abrufen.

Mit dem Befehl *Systeminfo* zeigen Sie alle Informationen Ihres Computers in der Eingabeaufforderung an. Darunter finden sich Infos über Hotfixes, Netzwerkkarten, Prozessor, Betriebssystem, Hersteller usw. – sogar die aktuelle Systembetriebszeit (also wie lange Sie schon arbeiten) und das ursprüngliche Installationsdatum lässt sich anzeigen.

Hier empfiehlt sich die Umleitung in eine Textdatei, wobei Sie zusätzlich den Parameter */FO list* angeben sollten, um die Informationen formatiert zu speichern. Um alle Infos in die Textdatei *C:\sysinfo.txt* zu speichern, müssen Sie den Befehl *systeminfo /FO list > C:\sysinfo.txt* verwenden.

2.4.3 Netzwerkverbindung testen

Um Windows Server 2022 aktuell zu halten, ist eine Verbindung mit dem Internet und damit mit dem Netzwerk notwendig. Nachdem Sie die Treiberinstallation kontrolliert haben, überprüfen Sie über das Symbol der Netzwerkverbindung in der Taskleiste, ob Windows Server 2022 mit dem Netzwerk und dem Internet kommunizieren kann. Zeigt Windows ein Netzwerksymbol ohne Fehler an, kann der Rechner mit dem Netzwerk und dem Internet kommunizieren.

Kann der Computer mit dem Netzwerk kommunizieren, aber nicht mit dem Internet, wird das Netzwerksymbol mit einem Ausrufezeichen gekennzeichnet. In diesem Fall überprüfen Sie die Einstellungen der Netzwerkkarte. Am schnellsten geht dies, wenn Sie über das Suchfeld der Taskleiste nach *ncpa.cpl* suchen. Verfügt der Computer über keine physische Netzwerkverbindung, ist das Netzwerksymbol mit einem roten X gekennzeichnet. In diesem Fall überprüfen Sie die Installation des Treibers und des Netzwerkkabels beziehungsweise der WLAN-Verbindung.

2.4.4 Windows Update aktivieren

Im nächsten Schritt sollten Sie, unabhängig davon, ob Sie Treiber manuell oder über Windows Update installieren wollen, die Windows Update-Funktion in den Einstellungen aufrufen. Sie können diese Einstellungen zwar auch über Richtlinien durchführen, aber nach der Installation von Windows Server 2022 ist es empfehlenswert, diese Funktion sofort zu aktivieren, zumindest wenn der Server Zugriff auf das Internet hat.

Nach der Installation sollten Sie die aktuellsten Windows-Updates installieren, um sicherzustellen, dass das Betriebssystem auf dem neuesten Stand ist. Rufen Sie dazu über das Startmenü die Einstellungen über das Zahnradsymbol auf und wechseln danach zu *Update und Sicherheit/Windows Updates*. Lassen Sie nach Updates suchen und installieren Sie diese gleich. Nach der Installation der Updates lassen Sie erneut nach Updates suchen, um sicherzustellen, dass keine weiteren mehr gefunden werden.

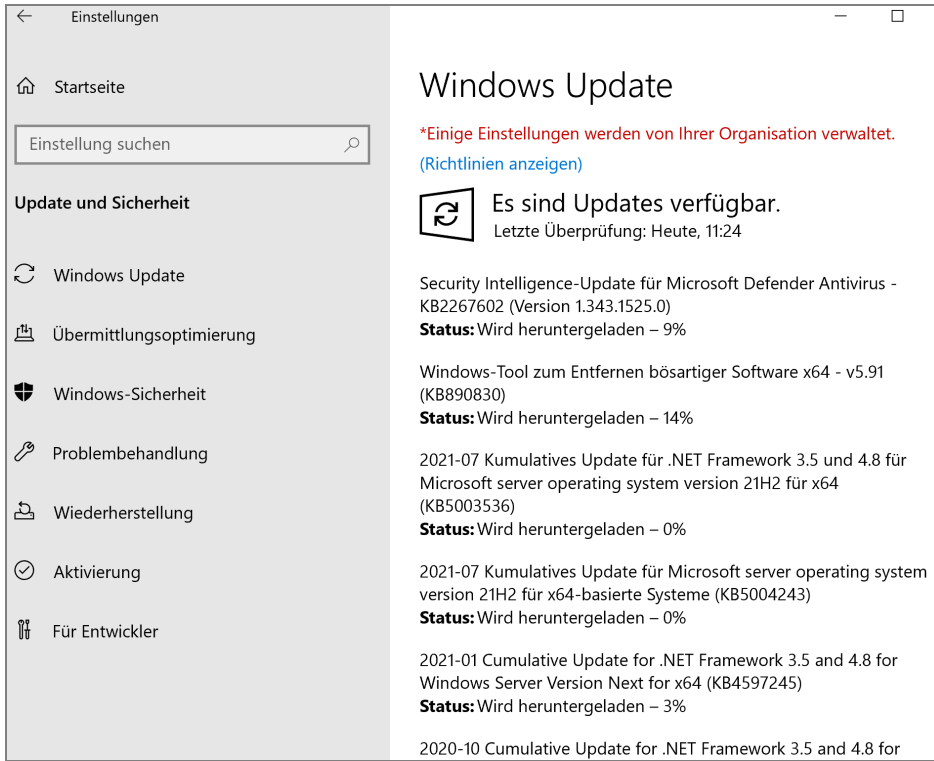


Abb. 2.7 Nach der Installation sollten Sie den Server aktualisieren.

2.4.5 Sprachpakete installieren

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

Liegt Ihnen die Sprachdatei vor, suchen Sie auf der Startseite nach *lpksetup*. Hier können Sie anschließend die Sprache installieren.

In der Einstellungen-App von Windows Server 2022 können Sie bei funktionierender Internetverbindung auch online zusätzliche Sprachen hinzufügen. Die Einstellungen dazu finden Sie bei *Zeit und Sprache*.

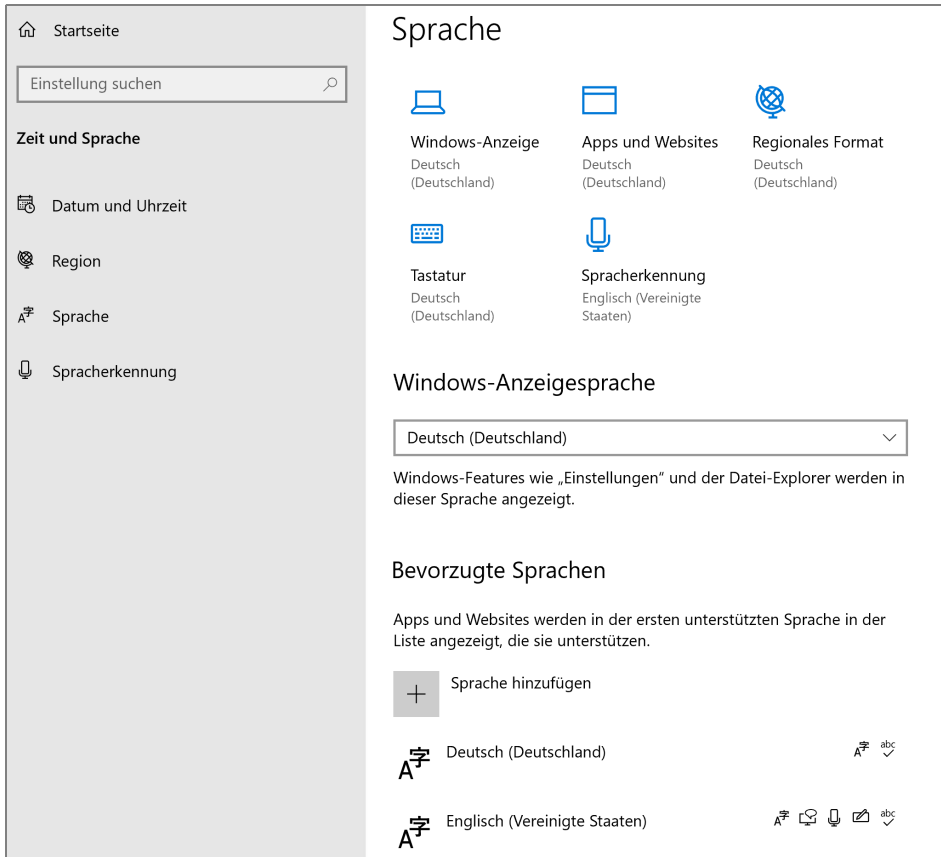


Abb. 2.8 Zusätzliche Sprachen für Windows Server 2022 installieren

2.4.6 Media Player deaktivieren

Standardmäßig ist in Windows Server 2022 der Windows Media Player aktiv. Auf produktiven Servern wird dieser nicht benötigt. Um den Media Player zu deinstallieren, verwenden Sie:

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



```

Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.20348.1]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Administrator>dism /online /Disable-Feature /FeatureName:WindowsMediaPlayer /norestart

Tool zur Imageverwaltung für die Bereitstellung
Version: 10.0.20348.1

Abbildversion: 10.0.20348.1

Features werden deaktiviert
[=====100.0%=====]
Der Vorgang wurde erfolgreich beendet.

C:\Users\Administrator>_

```

Abb. 2.9 Media Player in Windows Server 2022 deaktivieren

2.4.7 Computernamen und Domänenmitgliedschaft festlegen

Sie müssen den Computernamen und die Domänenmitgliedschaft nach der Installation manuell festlegen. Gehen Sie dazu folgendermaßen vor:

1. Starten Sie den Server-Manager.
2. Klicken Sie auf *Lokaler Server*, dann im mittleren Bereich auf den Namen des Servers.
3. Klicken Sie im neuen Fenster auf *Ändern*.
4. Geben Sie den neuen Namen des Computers ein und booten Sie den Rechner neu.



Sie erreichen die Systemeinstellungen und auch die Aktivierung für den Remote-Desktop am schnellsten, wenn Sie aus dem Startmenü heraus *sysdm.cpl* aufrufen.

Wollen Sie den Server auch in eine Domäne aufnehmen, gehen Sie folgendermaßen vor:

1. Tippen Sie in das Suchfeld der Taskleiste *ncpa.cpl* ein und rufen Sie die Eigenschaften der Netzwerkverbindung und von IPv4 auf.
2. Stellen Sie sicher, dass als DNS-Server mindestens ein Server eingetragen ist, der die DNS-Zone der Windows-Domäne auflösen kann, der Sie beitreten wollen.
3. Klicken Sie im Server-Manager auf *Lokaler Server* und dann auf den Link bei *Workgroup*. Sie finden die Einstellungen auch über *sysdm.cpl*.
4. Klicken Sie danach auf *Ändern*. Geben Sie bei *Computernamen* den neuen Namen des Servers in der Domäne ein und aktivieren Sie die *Domäne*.
5. Geben Sie den Namen der Domäne ein.

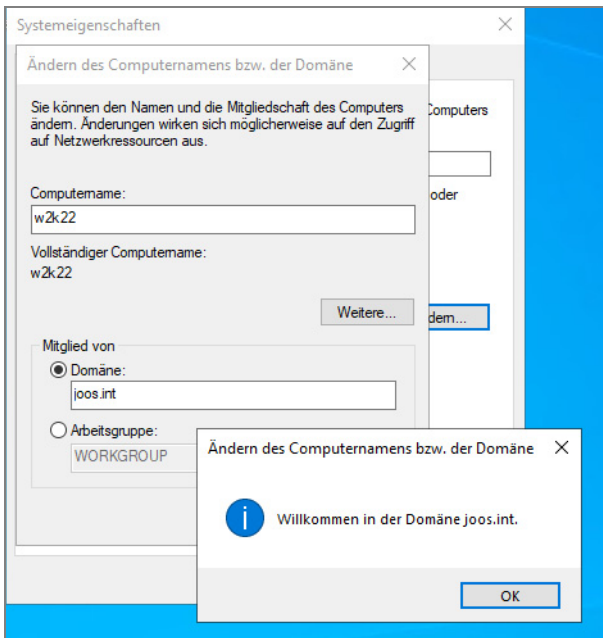


Abb. 2.10 Aufnehmen eines Computers in eine Domäne

6. Kann der Server über seinen DNS-Server die Domäne auflösen, erscheint ein Authentifizierungsfenster. Wenn nicht, erscheint ein Fehler. In diesem Fall überprüfen Sie, ob der DNS-Server korrekt ist. Authentifizieren Sie sich an der Domäne. Kann der DNS-Server den Namen der Domäne auflösen und haben Sie sich korrekt authentifiziert, erhalten Sie eine Rückmeldung der Domänenaufnahme und können den Server neu starten.

2.4.8 Aktivieren von Remotedesktop

Die Einrichtung von Servern direkt im Serverraum oder Rechenzentrum ist nicht gerade sehr bequem. Hier bietet es sich an, eine Remotedesktopverbindung zu aktivieren und von Ihrem Computer aus auf den Server zuzugreifen. Das hat den Vorteil, dass Sie auf dem Server mit Maus und Tastatur arbeiten können und Treiber, die Sie mit dem Computer herunterladen, per Kopieren/Einfügen über den Remotedesktop auf den Server kopieren können. Um nach der Netzwerkverbindung eine Remotedesktopverbindung herzustellen, gehen Sie folgendermaßen vor:

1. Sie erreichen die Systemeinstellungen auch durch Eingabe von *sysdm.cpl* im Startmenü.
2. Klicken Sie in den Systemeigenschaften auf die Registerkarte *Remote*. Aktivieren Sie die Option *Remoteverbindung mit diesem Computer zulassen*. Funktioniert die Verbindung nicht, deaktivieren Sie noch die Option *Verbindungen nur von Computern zulassen, auf denen Remotedesktop mit Authentifizierung auf Netzwerkebene ausgeführt wird*. Bestätigen Sie die Eingabe mit *OK*.

Sie finden diese Einstellungen auch in der Einstellungen-App von Windows Server 2022 im Bereich *System/Remotedesktop*.

3. Stellen Sie im unteren Bereich der Taskleiste sicher, dass eine Netzwerkverbindung hergestellt ist.

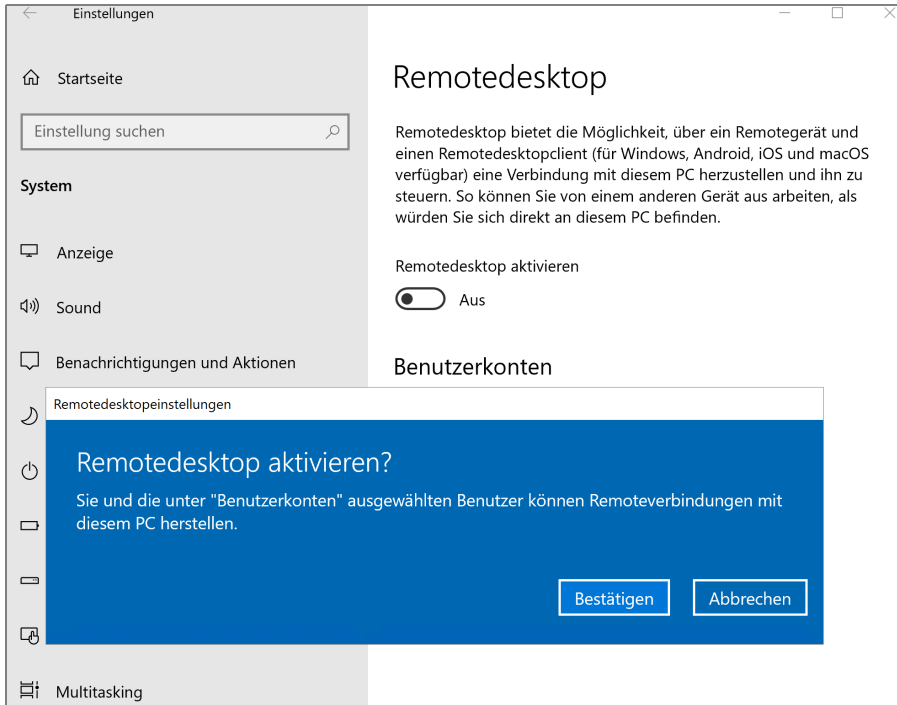


Abb. 2.11 Aktivieren des Remotedesktops in Windows Server 2022

Um zum Beispiel von einem Windows 10/11-Computer aus eine Remotedesktopverbindung herzustellen, geben Sie auf der Startseite *mstsc* ein. Es öffnet sich der Client für die Remotedesktopverbindung. Verwenden Sie den internen Remotedesktopclient in Windows 10/11, geben Sie bei *Computer* die IP-Adresse des Servers ein und bei *Benutzername* den Anmeldenamen mit der Syntax `<Name des Servers oder der Domäne>\<Anmeldename>`. Auf Wunsch aktivieren Sie noch *Speichern der Anmeldeinformationen zulassen*.

Wechseln Sie zur Registerkarte *Anzeige* und verwenden Sie entweder den Vollbildmodus oder setzen Sie die Anzeige auf die Auflösung, die auch der Server hat.

Auf der Registerkarte *Lokale Ressourcen* sollten Sie die Option *Auf dem Remotecomputer anwenden bei Windows-Tastenkombinationen anwenden* aktivieren.

Auf der Registerkarte *Leistung* aktivieren Sie die Option *LAN (10MBit/s oder höher)* und stellen sicher, dass alle Optionen aktiviert sind. Wechseln Sie dann zur Registerkarte *Allgemein* und speichern Sie die Verbindung mit *Speichern unter*.

Starten Sie die Verbindung, müssen Sie einmalig eine Ausnahme für die Windows-Firewall eintragen lassen, das Kennwort für das Benutzerkonto angeben und das Zertifikat bestätigen. Anschließend wird eine Remotedesktopverbindung hergestellt. Bei weiteren Verbindungen sind diese Eingaben nicht mehr notwendig, wenn Sie die entsprechenden Optionen speichern lassen.

In vielen Unternehmen wird mit dem Remotedesktopzugriff gearbeitet. In vielen Fällen wird dieser über die grafische Oberfläche des Servers aktiviert oder über das textbasierte Menü auf Core-Servern. Auf Servern mit grafischer Oberfläche wird die Einstellung am schnellsten durch Aufrufen von *sysdm.cpl* erreicht.

Die Aktivierung des Remotedesktops kann auch über die Registry erfolgen. Die Einstellungen dazu sind im folgenden Schlüssel zu finden:

HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server

Durch Skripts oder Tools kann dadurch der Remotedesktop auch über das Importieren von Einträgen aktiviert werden.

Der wichtigste Eintrag ist *fDenyTSConnection*. Durch den Wert *0* wird der Remotedesktop aktiviert. Der Wert *1* deaktiviert den Remotedesktop.

Welche Benutzer mit einem Server verbunden sind, kann in der Befehlszeile mit dem folgenden Befehl angezeigt werden:

Qwinsta /server:<Servername>

Wer den Zugriff von bestimmten Benutzern verweigern will, zum Beispiel für alle Administratoren, kann das über Gruppenrichtlinien erledigen. Um den Zugriff auf die Remotedesktopdienste für lokale Administratoren zu blockieren, werden die Rechte am besten zentral gesteuert. Der Pfad zu den Einstellungen ist:

Computerkonfiguration/Windows Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien/Zuweisen von Benutzerrechten

Wichtig sind die beiden Einstellungen:

Anmelden über Remotedesktopdienste verweigern

Lokal anmelden verweigern

Hier kann konfiguriert werden, welche Benutzer sich lokal am Server anmelden dürfen, also direkt an der Konsole, und welche Benutzer sich per Remotedesktop mit dem Server verbinden dürfen. Remotedesktopverbindungen lassen sich auch über den Webbrowser nutzen, wenn auf das Windows Admin Center gesetzt wird. Hier steht der Menüpunkt *Remotedesktop* zur Verfügung, mit dem der Aufbau erfolgt.

2.4.9 WLAN-Anbindung von Windows Server 2022

Sie können einen Server mit Windows Server 2022 auch an WLANs anbinden. Zuvor müssen Sie über den Server-Manager das Feature *WLAN-Dienst* installieren.

Haben Sie eine WLAN-Karte installiert oder verwenden Sie einen WLAN-USB-Stick, können Sie den Server jetzt mit einem WLAN verbinden. Dazu klicken Sie auf das Netzwerksymbol und wählen das entsprechende WLAN aus.

2.4.10 Boot-Manager reparieren

Teilweise kann es passieren, dass Windows Server 2022 nicht mehr startet. In diesem Fall liegt ein Problem mit dem Boot-Manager vor. Dieser lässt sich aber über die Computerreparaturoptionen in Windows Server 2022 oder aber über das Installationsmedium reparieren.

Startet der Boot-Manager nicht, sollten Sie in den Computerreparaturoptionen zur Eingabeaufforderung wechseln. Um den Boot-Manager zu reparieren, geben Sie folgenden Befehl ein:

```
bcdboot C:\Windows /s C: /f BIOS
```

Erscheint ein Fehler, geben Sie *bcdboot D:\Windows /s C: /f BIOS* ein. Die Befehle funktionieren auf Rechnern mit UEFI nicht. Weitere Befehle, die den Boot-Manager reparieren, sind:

```
bootsect.exe /nt60 ALL /force
```

```
bootsect.exe /nt60 C: /mbr /force
```

In den Computerreparaturoptionen von Windows Server 2022 steht auch der Menüpunkt *Starthilfe* zur Verfügung. Mit diesem Bereich lässt sich Windows häufig wieder reparieren, wenn das Betriebssystem nicht startet.

2.5 Zusammenfassung

In diesem Kapitel wurde Ihnen anhand diverser Anleitungen gezeigt, wie Sie Windows Server 2022 installieren, aber auch parallel mit älteren Windows-Versionen betreiben. Außerdem wurde Ihnen erläutert, welche wichtigen Aufgaben Sie nach der Installation durchführen müssen und wie Sie Windows Server 2022 aktivieren. Des Weiteren sind wir darauf eingegangen, wie Sie Windows Server 2022 über einen USB-Stick installieren.

Im nächsten Kapitel lesen Sie, wie Sie Windows Server 2022 so einrichten, dass Sie nach der Installation optimal mit dem Server arbeiten können. Außerdem gehen wir näher auf die Einrichtung und Installation des Windows Admin Centers ein.

Kapitel 3

Erste Schritte mit Windows Server 2022

In diesem Kapitel zeigen wir Ihnen die ersten Schritte, die zur Verwaltung eines Servers mit Windows Server 2022 notwendig sind. Bereits in Kapitel 1 haben wir Ihnen Neuerungen gezeigt. In diesem Kapitel gehen wir auf erste Schritte bei der Verwaltung von Windows Server 2022 ein. Wir zeigen auch die Installation und Einrichtung des Windows Admin Centers. Mit dieser webbasierten Verwaltungsoberfläche können Sie Netzwerke mit Windows Server 2022 parallel zu den anderen Verwaltungswerkzeugen verwalten.

3.1 Erste Schritte nach der Installation

Während der Installation legt Windows Server 2022 automatisch einen Namen für den Server fest, der nachträglich angepasst werden sollte. Wie Sie dabei vorgehen, lesen Sie in Kapitel 2. Viele Aufgaben, die zur Grundkonfiguration des Servers gehören, nehmen Sie direkt im Server-Manager oder im Windows Admin Center vor. Dazu klicken Sie auf *Lokaler Server*. Im mittleren Bereich sehen Sie die verschiedenen Aufgaben, deren Assistenten Sie über einen Klick auf den entsprechenden Link erreichen. Alternativ rufen Sie das Tool *system.cpl* auf. Auch hier können Sie den Namen des Servers ändern.

3.1.1 Windows Server 2022 mit Windows 10/11 verwalten

Um Windows Server 2022 mit Windows 10/11 zu verwalten, bietet Microsoft die Remote-server-Verwaltungstools (Remote Server Administration Tools, RSAT) an. Achten Sie darauf, die neueste Version der Tools zu verwenden, die mit Windows 10/11 und Windows Server 2022 kompatibel sind. Die Tools müssen Sie in Windows 10/11 nicht mehr installieren, sondern können diese als optionale Features aktivieren, wenn Sie auf Windows 10/11 Pro setzen.

Mit den Tools aktivieren Sie auf einer Arbeitsstation mit Windows 10/11 Verwaltungsprogramme, die zur Verwaltung von Windows Server 2022 notwendig sind. Mit den Tools verwalten Sie auch die Serverdienste in Windows Server 2012/2012 R2/2016/2019.

Neben den verschiedenen Verwaltungstools der Serverrollen bieten RSAT auch den Server-Manager von Windows Server 2022 in Windows 10/11. Über den Server-Manager binden Sie die verschiedenen Server im Netzwerk an, auf denen Windows Server 2022 installiert

ist. Sie können mit dem Server-Manager auf diesem Weg ebenso über Windows 10/11-Arbeitsstationen aus Serverrollen auf Servern installieren. Auch im Server-Manager von Windows Server 2022 können Sie andere Server mit Windows Server 2022 im Netzwerk verwalten. Sie können ebenfalls das Windows Admin Center auf Windows 10/11 installieren und Ihre Server parallel mit dem Windows Admin Center verwalten.

Die Remoteserver-Verwaltungstools für Windows 10/11 umfassen Server-Manager, Verwaltungstools der Serverrollen und Features von Windows Server 2016/2019/2022, PowerShell-Cmdlets und Befehlszeilentools für die Verwaltung von Rollen und Features.

Die Remoteserver-Verwaltungstools lassen sich sogar in der kleinsten Version Windows 10/11 installieren, allerdings bietet nur die Enterprise-Version alle Funktionen.

Remoteserver-Verwaltungstools installieren

In aktuellen Windows 10/11-Versionen sind die Remote Server Administration Tools bereits integriert, sie müssen als optionale Funktionen nur aktiviert werden. Auf diesem Weg lassen sich Windows-Server mit dem Server-Manager und Storage-Tools verwalten. Dazu müssen sich aber Server und Arbeitsstation im gleichen Active Directory befinden. Die Installation erfolgt über die Einstellungs-App von Windows 10/11, die über das Startmenü aufgerufen wird:

1. Klicken Sie auf *Apps*.
2. Wählen Sie in der Mitte des Fensters die Option *Optionale Features*.
3. Klicken Sie auf *Feature hinzufügen* oder auf *Optionales Feature hinzufügen*.

Im Fenster stehen jetzt die Verwaltungstools zur Verfügung. Um zum Beispiel mit dem Server-Manager Funktionen wie Freigaben oder Storage-Bereiche zu verwalten, klicken Sie auf *RSAT: Server Manager*. Zusätzlich steht hier auch das Modul für die Speicherreplikation und die Storage Migration Service Management Tools zur Verfügung. Natürlich können Sie auch alle weiteren Remoteserver-Verwaltungstools aktivieren.

Remoteverwaltung mit dem Server-Manager

Im Vergleich zu den Vorgängern sind keine Neuerungen im Server-Manager zu sehen, außer, die Informationen zur Verwaltung der Umgebung noch auf das Windows Admin Center zu setzen. Die Server im Netzwerk lassen sich zentral im Server-Manager verwalten.

Klicken Sie im Server-Manager auf *Dashboard*, können Sie über das Menü *Ansicht* die Willkommen-Kachel ausblenden und gewinnen Platz zur Verwaltung von Servern. Über das Menü *Verwalten* erstellen Sie eigene Servergruppen.

Dazu gruppiert der Server-Manager die verschiedenen Serverfunktionen zur besseren Verwaltung. Alle installierten Serverrollen zeigt er automatisch gruppiert an. Verwaltungswerkzeuge zeigt er direkt über das Menü *Tools* an. Hierüber lassen sich alle wichtigen Werkzeuge starten. So stört auch die neue Oberfläche nicht, da alle Verwaltungsaufgaben zentral im Server-Manager stattfinden. Diese Funktionen sind nach der Installation von RSAT auch in Windows 10/11 verfügbar.

Um im Server-Manager in Windows Server 2022 und Windows 10/11 weitere Server anzubinden, klicken Sie auf *Verwalten* und dann auf *Server hinzufügen*. Im Fenster können Sie anschließend nach Servern suchen, um sie im lokalen Server-Manager zu verwalten. Auf diesem Weg erstellen Sie auch eigene Servergruppen, die Sie im Server-Manager zusam-

menfassen. Von diesen Gruppen können Sie dann Ereignismeldungen anzeigen lassen. Über diesen Weg binden Sie Server mit Windows Server 2022 in allen Editionen, aber auch Windows Server 2012/2012 R2/2016/2019 an.

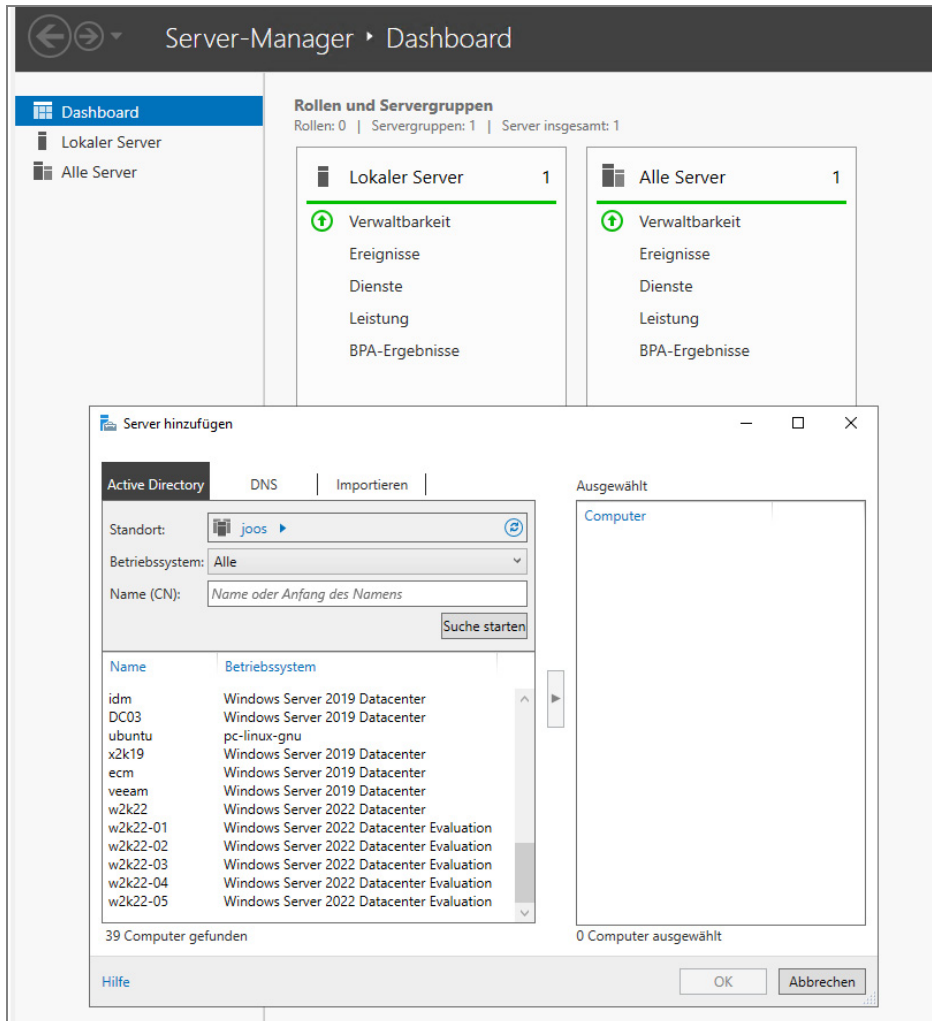


Abb. 3.1 Verwalten von zusätzlichen Servern im Server-Manager

Um auf Servern im Netzwerk über den Server-Manager remote Rollen oder Features zu installieren, ist eine vorherige Anbindung notwendig. Im Assistenten zum Hinzufügen von zusätzlichen Rollen erscheint ein Fenster, über das Sie den Server auswählen können, auf dem Sie eine neue Rolle oder ein neues Feature installieren wollen. Dazu klicken Sie auf *Verwalten/Rollen und Features hinzufügen*.

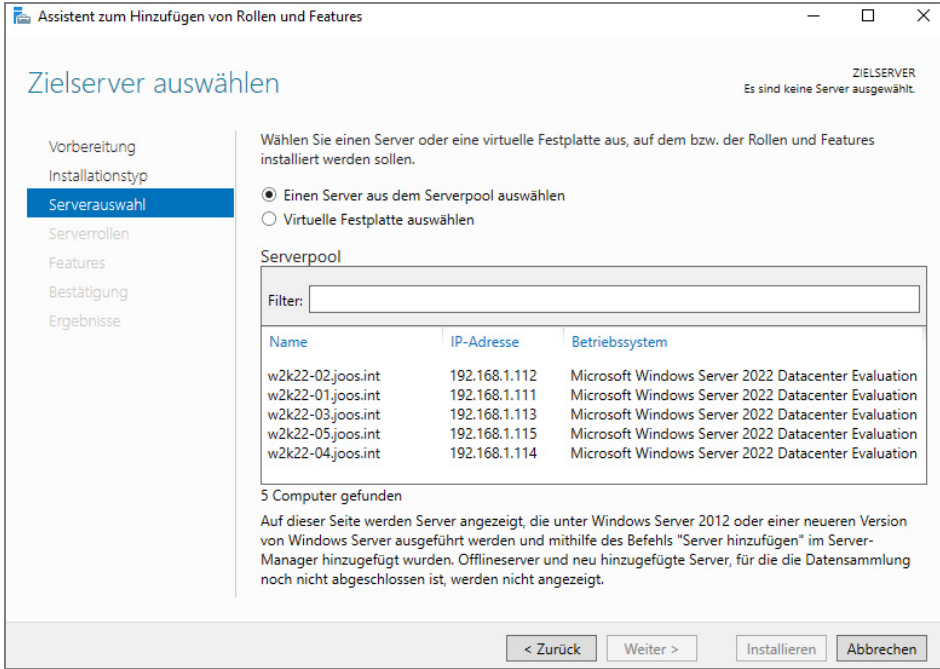


Abb. 3.2 Auswählen des Zielservers zur Installation von Serverrollen

In Windows Server 2022 sind die Assistenten zum Hinzufügen von Rollen und Features zusammengefasst. Das heißt, Sie können über einen einzelnen Assistenten mehrere Serverrollen und Features gemeinsam und auf einmal installieren. Das erspart unnötige Neustarts und Installationen, da alles in einem Arbeitsschritt erfolgt. Im Assistenten lassen sich aber nicht nur physische Server im Netzwerk auswählen, um Serverrollen zu installieren, sondern auch virtuelle Festplatten auf Hyper-V-Hosts.

Beim Abschluss der Installation von Serverrollen und Features erhalten Sie eine Zusammenfassung angezeigt und die Möglichkeit geboten, die Konfiguration in XML-Dateien zu exportieren. Mit dieser Datei können Sie dann die gleichen Rollen oder Features auf einem anderen Server installieren. Zusätzlich haben Sie die Möglichkeit, einen alternativen Pfad zu den Installationsdateien von Windows Server 2022 anzugeben. Hier sollten Sie auch die Option zum automatischen Neustart aktivieren.

In diesem Fall starten die Server automatisch neu, falls dies notwendig ist. Vor allem, wenn Sie Installationen von Serverrollen über das Netzwerk oder über eine RDP-Verbindung ausführen, ist dies sinnvoll, da viele Rollen die Netzwerkverbindung kappen können, zum Beispiel die Installation von Hyper-V. Damit der Assistent seine Arbeit erfolgreich fortsetzt, müssen Sie das Fenster nicht geöffnet lassen, sondern können es nach dem Start der Installation schließen.

Überall im Server-Manager lassen sich die anderen Server im Netzwerk schnell und einfach integrieren sowie verwalten. Über das Kontextmenü von Servern können Sie Server über das Netzwerk remote neu starten lassen, eine PowerShell-Sitzung auf dem Server starten oder eine RDP-Verbindung öffnen. Auch die Installation von Rollen und Features über das Netzwerk ist mit dem Kontextmenü möglich.

The screenshot shows the Windows Server Manager interface. The left sidebar contains navigation options: Dashboard, Lokaler Server, Alle Server (selected), and Datei-/Speicherdienste. The main area displays a list of servers under the heading 'SERVER Alle Server | 5 insgesamt'. A table lists server details, with 'W2K22-02' selected and its context menu open. The context menu includes options like 'Rollen und Features hinzufügen', 'Server neu starten', 'Computerverwaltung', 'Remotedesktopverbindung', 'Windows PowerShell', 'NIC-Teamvorgang konfigurieren', 'Verwalten als...', 'Server entfernen', 'Aktualisieren', and 'Kopieren'. Below the server list, an 'EREIGNISSE' section shows a list of events with columns for Servername, ID, Schweregrad, Quelle, Protokoll, and Datum und Uhrzeit.

| Servername | IPv4-Adresse | Verwaltbarkeit | Letztes Update | Windows-Aktivierung |
|------------|---------------|----------------|---------------------|-------------------------------------|
| W2K22-01 | 192.168.1.111 | Online | 05.08.2021 11:41:57 | 00455-50000-00001-AA446 (Aktiviert) |
| W2K22-02 | 192.168.1.112 | Online | 05.08.2021 11:43:49 | 00455-50000-00001-AA189 (Aktiviert) |
| W2K22-03 | | | 05.08.2021 11:43:53 | 00455-50000-00001-AA540 (Aktiviert) |
| W2K22-04 | | | 05.08.2021 11:43:59 | 00455-50000-00001-AA214 (Aktiviert) |
| W2K22-05 | | | 05.08.2021 11:43:57 | 00455-50000-00001-AA763 (Aktiviert) |

| Servername | ID | Schweregrad | Quelle | Protokoll | Datum und Uhrzeit |
|------------|-------|-------------|--|-----------|---------------------|
| W2K22-02 | 1076 | Warnung | User32 | System | 05.08.2021 10:23:53 |
| W2K22-02 | 10016 | Warnung | Microsoft-Windows-DistributedCOM | System | 05.08.2021 10:05:11 |
| W2K22-02 | 6038 | Warnung | Microsoft-Windows-LSA | System | 05.08.2021 10:05:06 |
| W2K22-02 | 15 | Fehler | Microsoft-Windows-CertificateServicesClient-CertEnroll | Anwendung | 05.08.2021 09:57:22 |
| W2K22-02 | 6 | Fehler | Microsoft-Windows-CertificateServicesClient-AutoEnrollment | Anwendung | 05.08.2021 09:57:22 |
| W2K22-02 | 70 | Fehler | Microsoft-Windows-CertificateServicesClient-CertEnroll | Anwendung | 05.08.2021 09:57:22 |
| W2K22-02 | 68 | Fehler | Microsoft-Windows-CertificateServicesClient-CertEnroll | Anwendung | 05.08.2021 09:57:22 |

Abb. 3.3 Über das Kontextmenü von Servern lassen sich Verwaltungswerkzeuge von Windows Server 2022 auch in Windows 10/11 starten.

Im Server-Manager sehen Sie am Wartungszentrumsymbol im oberen Bereich, ob Fehler auf einem angebotenen Server vorliegen oder Maßnahmen zur Verwaltung notwendig sind. Sie können sich über diesen Weg in Windows 10/11 auch gesammelt alle Fehlermeldungen aller Server anzeigen lassen.

Klicken Sie in der Ansicht *Alle Server* auf einen Server im oberen Bereich, sehen Sie unten wichtige Fehlermeldungen der Ereignisanzeige. Im oberen Bereich ist außerdem zu sehen, ob die entsprechenden Server online sind und ob Windows Server 2022 aktiviert ist.

Nach der Installation von Windows Server 2022 sollten Sie im Server-Manager über das Kontextmenü der Server den Befehl *Leistungsindikatoren starten* ausführen, damit der Server über das Netzwerk überwachbar ist und die Best Practices Analyzer funktionieren und Daten abrufen können. Über das Kontextmenü der Server können Sie sich auch mit einem anderen Benutzernamen am Server anmelden, um diesen zu administrieren.



Wenn Sie auf einem Core-Server nur einen schwarzen Bildschirm sehen, ist die Eingabeaufforderung geschlossen. Um diese zu öffnen, drücken Sie **[Strg] + [Alt] + [Entf]** und starten den Task-Manager. Mit *Mehr Details* und Eingabe von `cmd` über *Datei/Neuen Task ausführen* starten Sie die Eingabeaufforderung neu.

Um das Verwaltungsprogramm von Core-Servern aufzurufen, geben Sie `sconfig` ein. Das Befehlszeilentool `sconfig` steht in Windows Server 2022 auch auf Servern mit grafischer Benutzeroberfläche zur Verfügung. Auf diesem Weg können Sie zum Beispiel in Fernwartungen Einstellungen vornehmen, wenn die Verbindung für grafische Werkzeuge zu langsam ist.

3.2 Core-Server verwalten

Core-Server hat Microsoft mit Windows Server 2008 R2 eingeführt und in den Nachfolgeversionen verbessert. In Windows Server 2022 bieten Core-Server ähnliche Funktionen wie in Windows Server 2016/2019 und noch einiges mehr. So unterstützt etwa auch Exchange Server 2022 die Installation auf Core-Servern mit Windows Server 2022. Exchange Server 2019 kann auch auf Core-Servern mit Windows Server 2019 installiert werden.

Den Core-Servern fehlt die grafische Oberfläche. Sie verwalten diese Server mit der Eingabeaufforderung, der PowerShell oder über das Netzwerk von anderen Servern oder Windows 10/11-Arbeitsstationen. Hier stehen die Remote Server-Verwaltungstools zur Verfügung sowie das Windows Admin Center über einen Webbrowser.

Core-Server werden vor allem mit Windows Admin Center verwaltet. Hier steht über den Webbrowser von Arbeitsstationen alles zur Verfügung, was Administratoren benötigen. Auch die Anbindung an den Server-Manager ist möglich.



Core-Server lassen sich in Windows Server 2022 nicht zu Servern mit grafischer Oberfläche aktualisieren, und umgekehrt lässt sich die grafische Oberfläche nach der Einrichtung nicht deinstallieren.

Haben Sie aber die Remoteserver-Verwaltungstools (Remote Server Administration Tools, RSAT) in Windows 10/11 installiert, können Sie die Verwaltungstools auch von einer Windows 10/11-Arbeitsstation aus verwenden, ohne dass auf dem Core-Server eine grafische Oberfläche zur Verfügung steht. Auch das Windows Admin Center steht in Windows Server 2022 und Windows 10/11 zur Verfügung, um Core-Server umfassend zu verwalten.

Sie können Core-Server 2022 mit dem Hyper-V-Manager in Windows 10/11 verwalten, auch ohne RSAT zu nutzen. Das gilt auch für das Windows Admin Center. Wichtig für die Verwaltung von Core-Servern über das Netzwerk sind noch die Punkte 4 und 7 in Sconfig. Hierüber aktivieren Sie die Remoteverwaltung mit Tools wie den Hyper-V-Manager. Durch Aktivierung des Remotedesktops lässt sich Hyper-V-Server auch darüber verwalten. Wie Sie dabei vorgehen, lesen Sie in Kapitel 2.

Haben Sie sich mit einem Core-Server verbunden und versehentlich die Eingabeaufforderung geschlossen, drücken Sie die Tastenkombination `[Strg]+[Alt]+[Entf]` und starten den Task-Manager. Klicken Sie danach auf *Mehr Details* und dann auf *Datei/Neuen Task ausführen*. Geben Sie `cmd` ein, um die Eingabeaufforderung erneut zu öffnen.

Haben Sie einen Core-Server installiert, legen Sie zunächst die IP-Adresse fest, konfigurieren den DNS-Server, ändern den Namen und nehmen den Server in die Active Directory-Domäne auf. Aktivieren Sie noch die Remoteverwaltung, können Sie den Server mit grafischen Verwaltungstools verwalten, wie in den ersten Abschnitten in diesem Kapitel behandelt.

```

Administrator: C:\Windows\system32\cmd.exe
WARNUNG: Um den Start von SConfig bei der Anmeldung zu verhindern, geben Sie „Set-SConfig -AutoLaunch $false“ ein.
-----
Willkommen bei Windows Server 2022 Datacenter Evaluation
-----
1) Domäne/Arbeitsgruppe:           Arbeitsgruppe: WORKGROUP
2) Computername:                   WIN-44JDM3BHH6
3) Lokalen Administrator hinzufügen
4) Remoteverwaltung:               Aktiviert
5) Einstellung aktualisieren:      Nur Herunterladen
6) Updates installieren
7) Remotedesktop:                  Deaktiviert
8) Netzwerkeinstellungen
9) Datum und Uhrzeit
10) Telemetrie-Einstellung:        Erforderlich
11) Windows-Aktivierung
12) Benutzer abmelden
13) Server neu starten
14) Server herunterfahren
15) In Befehlszeile (PowerShell) beenden

Geben Sie eine Zahl ein, um eine Option auszuwählen: _

```

Abb.3.4 Die erste Verwaltung und Einrichtung von Core-Servern erfolgt unter anderem mit Sconfig.

Um Core-Server zu verwalten, geben Sie zunächst in der Eingabeaufforderung *sconfig* ein, wenn Sconfig nicht automatisch startet. Danach binden Sie den Server an das Netzwerk an und konfigurieren IP- und DNS-Adressen:

1. Zur Konfiguration der Netzwerkeinstellungen wählen Sie den Menüpunkt 8) *Netzwerkeinstellungen*
2. Wählen Sie die Nummer des Adapters aus.
3. Wählen Sie 1) *Netzwerkadapteradresse festlegen* aus, um die Adresse zu ändern.
4. Geben Sie *S* ein, um eine statische IP-Adresse zu konfigurieren.
5. Geben Sie die statische IP-Adresse ein und danach die Subnetzmaske.

```

Administrator: C:\Windows\system32\cmd.exe
-----
Netzwerkadaptereinstellungen
-----
NIC-Index: 1
Beschreibung: Intel(R) 82574L Gigabit Network Connection
IP-Adresse: 192.168.1.87,
             fe80:d00d:1ff9:7413:6e28
Subnetzmaske: 255.255.255.0
DHCP aktiviert: True

Standardgateway: 192.168.1.1
Bevorzugter DNS-Server: 8.8.8.8
Alternativer DNS-Server: 8.8.4.4

1) Netzwerkadapteradresse festlegen
2) DNS-Server festlegen
3) DNS-Servereinstellungen löschen

Auswahl eingeben (Leer=Abbrechen): 1
(D)HCP- oder (s)tatische IP-Adresse auswählen (Leer=Abbrechen): s
Geben Sie die statische IP-Adresse ein (Leer=Abbrechen): 192.168.1.117
Subnetzmaske eingeben (Leer=255.255.255.0): 255.255.255.0
Standardgateway eingeben (Leer=Abbrechen): 192.168.1.1
NIC wird auf die statische IP-Adresse festgelegt...
DHCP-Lease erfolgreich freigegeben.
Die statische Adressierung wurde erfolgreich aktiviert. DHCP ist für diesen Netzwerkadapter deaktiviert.
Gateway wurde erfolgreich festgelegt.
Netzwerkadapteradresse erfolgreich festgelegt.
(Drücken Sie die EINGABETASTE, um den Vorgang fortzusetzen): _

```

Abb.3.5 Festlegen einer statischen IP-Adresse für einen Core-Server

Anschließend tragen Sie über den Menüpunkt 2) *DNS-Server festlegen* einen DNS-Server ein, der die Active Directory-Domäne auflösen kann. Danach können Sie den Server in die Active Directory-Domäne aufnehmen:

1. Im Hauptmenü zurück nehmen Sie den Server mit dem Punkt 1) *Domäne/Arbeitsgruppe* in die Domäne auf und ändern den Servernamen. Anschließend starten Sie den Server neu.
2. Über die Menüpunkte 4 und 7 im Sconfig-Hauptmenü aktivieren Sie die Verwaltung des Remotedesktops und die Remoteverwaltung über grafische Tools wie den Server-Manager oder das Windows Admin Center.

Die Verwaltung eines Core-Servers läuft hauptsächlich über die Eingabeaufforderung oder PowerShell ab, beziehungsweise mit Verwaltungstools über das Netzwerk, also in Windows Server 2022 vor allem über das Windows Admin Center.



Mit dem Befehl `start cmd /separate` öffnen Sie ein paralleles Fenster der Eingabeaufforderung, wenn Sie zwei Fenster benötigen. Wird das eine Fenster geschlossen, lässt sich über den Task-Manager durch Erstellen eines neuen Tasks mit dem Befehl `cmd` ein neues Fenster starten, aber mit einem zweiten Fenster ersparen Sie sich diesen Aufwand und können bei der Arbeit mit einem Skript parallel mit einer zweiten Oberfläche arbeiten.

Alle Tools, die eine grafische Oberfläche verwenden oder den Datei-Explorer benötigen, funktionieren auf einem Core-Server nicht. Aus diesem Grund werden auch keine Meldungen angezeigt, wenn neue Updates zur Verfügung stehen oder das Kennwort eines Benutzers abgelaufen ist. Einige Fenster funktionieren auch auf einem Core-Server. So kann zum Beispiel der Editor (Notepad) verwendet werden, um Skripts oder Dateien zu bearbeiten. Der Task-Manager steht ebenfalls zur Verfügung.

Um das lokale Administratorkennwort eines Servers anzupassen, gehen Sie folgendermaßen vor:

1. Geben Sie in der Eingabeaufforderung den Befehl `net user administrator *` ein. Durch die Eingabe des Platzhalters `*` wird das eingegebene Kennwort nicht in Klartext angezeigt.
2. Geben Sie das neue Kennwort ein und bestätigen Sie.
3. Geben Sie das Kennwort noch mal ein und bestätigen Sie erneut.

Sie können natürlich auch Einstellungen des Servers in der Eingabeaufforderung anpassen. Das Kennwort des angemeldeten Benutzers ändern Sie über die Tastenkombination `[Strg]+[Alt]+[Entf]`. Die PowerShell ist in Core-Installationen automatisch aktiviert. Daher verwenden Sie zur Konfiguration der IP-Einstellungen nicht mehr das Befehlszeilentool `Netsh`, sondern besser die Cmdlets `New-NetIPAddress` und `Get-NetIPConfiguration`.

Ein Beispiel für die Einrichtung ist `New-NetIPAddress -InterfaceIndex 12 -IPAddress 192.168.178.2 -PrefixLength 24 -DefaultGateway 192.168.1.10`.

Die DNS-Server tragen Sie mit `Set-DNSClientServerAddress -InterfaceIndex 12 -ServerAddresses 192.168.1.4` ein. Mehrere DNS-Server trennen Sie jeweils mit einem Komma. Das Cmdlet `Set-DnsClientServerAddress -InterfaceIndex 12 -ResetServer` wechselt zu DHCP. Achten Sie darauf, jeweils die korrekte Indexnummer für den Netzwerkkadapter zu verwenden. Diesen erhalten Sie mit `Get-NetIPConfiguration`.

Einer Windows-Domäne treten Sie mit *Add-Computer* bei. Um der lokalen Administratorgruppe ein Domänenkonto hinzuzufügen, verwenden Sie den Befehl `net localgroup administrators /add <Domäne>\<Benutzername>`. Mit dem Befehl `net localgroup administrators` können Sie sich alle Gruppenmitglieder anzeigen lassen. Die Aufnahme funktioniert auch über Sconfig, geht aber mit der Eingabeaufforderung schneller.

Mit dem Befehl `net localgroup` können Sie sich alle lokalen Gruppen auf dem Server anzeigen lassen. So können Sie mit diesem Befehl schnell feststellen, welche Gruppen es gibt und welche Benutzerkonten enthalten sind. Außerdem lassen sich neue Benutzerkonten hinzufügen. Sie können die Benutzerverwaltung auch über die grafische Oberfläche von einem anderen Server aus durchführen, wenn Sie die Remoteverwaltung auf dem Server aktiviert haben. Mit dem Befehl `net localgroup administrators /delete <Domäne>\<Benutzername>` entfernen Sie ein Benutzerkonto wieder aus der Gruppe.

Den Namen von Servern ändern Sie mit *Rename-Computer*. Der Aufruf von *Set-Date* ändert die Zeitzone, und die Spracheinstellungen ändern Sie mit *control intl.cpl*.



Installieren Sie Windows-Installer-Pakete auf einem Core-Server, verwenden Sie beim Aufruf die Option `/qb`.

Die Computerverwaltung starten Sie zum Beispiel über das Snap-In *Active Directory-Benutzer und -Computer*. Klicken Sie den Core-Server in der Konsole mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag *Verwalten*. Anschließend kann der Server über eine grafische Oberfläche konfiguriert werden. Über diesen Weg lassen sich zum Beispiel wesentlich einfacher Freigaben und Systemdienste verwalten als über die Eingabeaufforderung des Core-Servers. Auf dem gleichen Weg funktioniert das auch im Windows Admin Center. Hier spielt es keine Rolle, ob die angebundenen Server Core-Server sind oder Server mit grafischer Oberfläche.

3.2.1 Hardware und Treiber auf Core-Servern installieren

Installieren Sie neue Hardware, können Sie die grafische Oberfläche verwenden oder die Eingabeaufforderung. Auf Core-Servern bleibt Ihnen keine andere Wahl, als die Eingabeaufforderung zu verwenden. Haben Sie die neue Hardware mit dem Server verbunden, wird diese durch das Plug-and-play automatisch erkannt und der Treiber installiert, das gilt auch auf Core-Servern. Allerdings muss in diesem Fall der Treiber in Windows Server 2022 integriert sein. Ist er das nicht und müssen Sie den Treiber manuell nachinstallieren, gehen Sie folgendermaßen vor:

1. Entpacken Sie die Treiberdateien und kopieren Sie diese in einen Ordner auf dem Server.
2. Geben Sie den Befehl `pnputil -i -a <*.inf-Datei des Treibers>` ein. Mit diesem neuen Tool können Treiber in Windows Server 2022 hinzugefügt und entfernt werden.
 - Über den Befehl `sc query type= driver` können Sie sich alle installierten Treiber auf einem Server anzeigen lassen (achten Sie auf das Leerzeichen nach dem Gleichheitszeichen).
 - Mit dem Befehl `sc delete <Treibername>` können Sie den Treiber entfernen, den Sie sich zuvor über den Befehl `sc query type= driver` anzeigen lassen können.

Für die Anbindung an iSCSI-Targets (siehe auch Kapitel 5) steht auf Core-Servern eine grafische Oberfläche zur Verfügung. Diese starten Sie durch Eingabe des Befehls *iscsicpl*. Für die Anbindung von Core-Servern an iSCSI-Targets steht auch der Befehl *iscsicli* zur Verfügung. Über *iscsicli /?* erhalten Sie eine ausführliche Hilfe zum Befehl (siehe Kapitel 5).

3.2.2 Windows Updates auf Core-Servern steuern

Um Windows-Updates zu steuern, verwenden Sie auf Core-Servern ebenfalls Sconfig. Mehr zu diesem Thema lesen Sie in Kapitel 37. Alternativ können Sie auch hier das Windows Admin Center verwenden.

Um eine sofortige Installation von Updates durchzuführen, geben Sie den Befehl *wuauctl /detectnow* ein. Die installierten Updates lassen sich durch den Aufruf von *systeminfo* oder *wmic qfe list* anzeigen.

3.3 Erweiterte Startoptionen nutzen

Die erweiterten Startoptionen bieten Möglichkeiten zur Reparatur des Servers. Wir werden in Kapitel 35 noch ausführlicher auf das Thema zu sprechen kommen. Die Optionen lassen sich zum Beispiel aufrufen, wenn der Server beim Starten einige Male abstürzt oder Sie den Windows-Start dreimal oder viermal abbrechen. Mit der Auswahl von *Problembehandlung* starten Sie die Reparatur des Servers.



Abb. 3.6 Problembehandlung in Windows Server 2022 starten

3.3.1 Starten der automatischen Reparatur von Windows Server 2022

Hier stehen verschiedene Möglichkeiten zur Verfügung:

- **Computer reparieren** – Startet die Reparatur des Betriebssystems in der Recovery-Oberfläche
- **Abgesicherter Modus** – Startet Windows mit den mindestens erforderlichen Treibern und Diensten.
- **Abgesicherter Modus mit Netzwerktreibern** – Startet Windows im abgesicherten Modus zusammen mit den für den Zugriff auf das Internet oder auf andere Computer im Netzwerk erforderlichen Netzwerktreibern und -diensten.
- **Abgesicherter Modus mit Eingabeaufforderung** – Startet Windows im abgesicherten Modus mit einem Eingabeaufforderungsfenster anstelle der normalen Windows-Benutzeroberfläche.
- **Startprotokollierung aktivieren** – Erstellt die Datei *Nbtlog.txt*, in der alle Treiber aufgelistet werden, die beim Starten installiert werden und für die erweiterte Problembehandlung nützlich sein können.
- **Videomodus mit niedriger Auflösung aktivieren** – Startet Windows mithilfe des aktuellen Videotreibers und mit niedrigen Einstellungen für Auflösung und Aktualisierungsrate. Mithilfe dieses Modus können Sie die Anzeigeeinstellungen zurücksetzen.
- **Letzte als funktionierend bekannte Konfiguration** – Startet Windows mit der letzten funktionsfähigen Registrierungs- und Treiberkonfiguration.
- **Debugmodus** – Startet Windows in einem erweiterten Problembehandlungsmodus.
- **Automatischen Neustart bei Systemfehler deaktivieren** – Verhindert, dass Windows nach einem durch einen eigenen Fehler verursachten Absturz automatisch neu gestartet wird. Wählen Sie diese Option nur aus, wenn Windows in einer Schleife festgefahren ist, die aus Absturz, Neustart und erneutem Absturz besteht.
- **Erzwingen der Treibersignatur deaktivieren** – Ermöglicht, dass Treiber mit ungültigen Signaturen installiert werden.
- **Frühen Start des Treibers der Antischadsoftware deaktivieren** – In Windows Server 2022 startet der installierte Virensch scanner wesentlich früher als in den Vorgängerversionen. Das kann zu Problemen führen, wenn der Computer nicht mehr startet. Hier deaktivieren Sie diesen Schutz.

3.3.2 Windows Server 2022 im abgesicherten Modus starten

Der abgesicherte Modus lässt sich in Windows Server 2022 auf mehreren Wegen starten.

Wenn Windows Server 2022 nicht mehr ordnungsgemäß funktioniert, hilft oft der Start im abgesicherten Modus. In diesem werden nur notwendige Systemtreiber geladen. Administratoren haben in diesem Modus die Möglichkeit, Programme oder Treiber zu deinstallieren oder das Betriebssystem zu reparieren, damit es wieder optimal funktioniert. Wir zeigen, welche Möglichkeiten es gibt, den abgesicherten Modus zu starten.

Der einfachste Weg, den abgesicherten Modus zu starten, ist das Verwenden der Tastenkombination **STRG**+**F8** während des Starts von Windows Server 2022. Allerdings ist es bei aktuellen Rechnern sehr schwer, den richtigen Moment zu treffen, da das Betriebssystem schneller startet als in den Vorgängerversionen. Es gibt aber noch mehr Möglichkeiten, den abgesicherten Modus zu starten.

3.3.3 Abgesicherter Modus über msconfig.exe

Startet Windows Server 2022 noch, können Sie den abgesicherten Modus auch über die Systemkonfiguration (*msconfig.exe*) im Suchfeld des Startmenüs starten. Rufen Sie das Tool auf und wechseln Sie zur Registerkarte *Start*. Aktivieren Sie das Kontrollkästchen *Abgesicherter Start*.

Klicken Sie auf *OK* und starten Sie dann den Rechner neu. Damit Windows 10/11 wieder normal startet, rufen Sie im abgesicherten Modus erneut *msconfig* auf und deaktivieren Sie den Modus wieder.

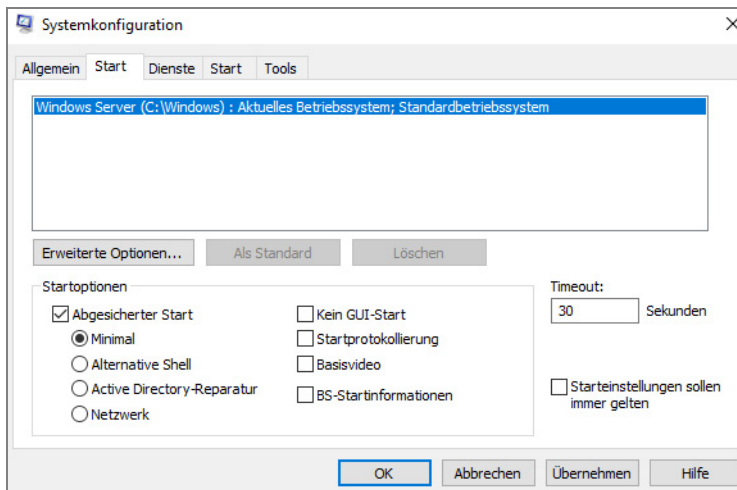


Abb. 3.7 Abgesicherter Modus über *msconfig* starten

3.3.4 Abgesicherter Modus in das Bootmenü einbinden

Wer den abgesicherten Modus oft benötigt, kann ihn auch in das Bootmenü einbinden:

1. Starten Sie eine Eingabeaufforderung mit Administratorrechten. Klicken Sie dazu die Eingabeaufforderung mit der rechten Maustaste an und wählen Sie die Option *Als Administrator ausführen*.
2. Geben Sie den Befehl `bcdedit /enum /v` ein.
3. Kopieren Sie den Eintrag der Zeile *Bezeichner* im Bereich *Windows-Startladeprogramm* für die Windows-Partition, für die Sie den abgesicherten Modus einbinden wollen.

4. Geben Sie danach den Befehl `bcdedit /copy {<Bezeichner>} /d "Windows Abgesicherter Modus"` ein, etwa `bcdedit /copy {2704757d-cf94-11e7-91d8-d41045f10ffd} /d "Windows Abgesicherter Modus"`. Sie sollten eine erfolgreiche Rückmeldung erhalten. Geben Sie `bcdedit` ein, sollte der Eintrag bereits erscheinen.
5. Starten Sie als Nächstes `msconfig` und wechseln Sie zur Registerkarte *Start*. Auch hier sehen Sie den Eintrag. Markieren Sie den neuen Eintrag des abgesicherten Modus. Aktivieren Sie die Option *Abgesicherter Modus* und *Minimal*.
6. Legen Sie noch den Timeout fest, nach dem Windows automatisch das Standardbetriebssystem starten soll. Aktivieren Sie das Kontrollkästchen *Starteinstellungen sollen immer gelten*.
7. Stellen Sie sicher, dass Ihr normales Windows als Standard definiert ist.

Booten Sie den Rechner, können Sie zukünftig den abgesicherten Modus direkt auswählen.

3.3.5 Abgesicherter Modus über automatische Reparatur starten

Brechen Sie den Startvorgang von Windows zwei- bis dreimal ab, startet automatisch die *Automatische Reparatur* von Windows. Um hier in den abgesicherten Modus zu wechseln, rufen Sie im Reparaturmenü zunächst *Problembehandlung* auf.

Anschließend wählen Sie *Erweiterte Optionen* und danach *Starteinstellungen*. Klicken Sie danach auf *Neu starten*, erscheint ein Systemmenü, in dem Sie auch den abgesicherten Modus starten können.



Abb. 3.8 Die erweiterten Optionen der Systemreparatur in Windows

3.4 Remote-Management aktivieren

Über Windows Remote Management (WinRM) lassen sich Cmdlets auch remote auf Core-Servern, aber auch auf herkömmlichen Windows-Servern ausführen. Damit das funktioniert, muss auf dem Server, der eine Verbindung zum Core-Server aufbaut, WinRM konfiguriert werden. Auch für die Verwendung des Windows Admin Centers ist das möglich. Die folgenden Befehle dazu müssen in einer Befehlszeile mit administrativen Rechten eingegeben werden:

```
winrm quickconfig
winrm set winrm/config/client @{TrustedHosts="*"}
chcp 65001
```

Anschließend lässt sich in der Befehlszeile eine Verbindung aufbauen:

```
winrs -r:<IP-Adresse des Core-Servers> -u:Administrator -p:<Kennwort> <Befehl, zum Beispiel ipconfig>
```

Der Befehl wird in diesem Fall auf dem Core-Server ausgeführt. So lassen sich auch Skripts für die Ausführung von Befehlen schreiben. WMI steht aber auch in der PowerShell zur Verfügung, wenn Administratoren eine Verbindung zum Core-Server aufbauen.

Wollen Sie auf einem Core-Server Daten von Festplatten auslesen, stehen verschiedene Möglichkeiten zur Verfügung. Der einfachste Weg ist die Verwendung des Cmdlets *Get-PhysicalDisk*. Dieses Cmdlet steht auch bei herkömmlichen Servern zur Verfügung und lässt sich natürlich auch lokal einsetzen. Die PowerShell zeigt eine Liste der Laufwerke an, ob diese Mitglied eines Speicherpools sein können oder sind, wie der Status des Laufwerks ist, und dessen maximale Größe. Noch mehr Informationen erhalten Sie mit *Get-PhysicalDisk |fl*.

3.5 Windows Admin Center in der Praxis

Das Windows Admin Center ist das empfohlene Werkzeug, mit dem Sie über einen Webbrowser die verschiedenen Server und Arbeitsstationen zentral verwalten können. Microsoft erweitert seine Funktionen mit jeder neuen Version. Die Installation des Windows Admin Centers erfolgt zunächst über die Installation eines Admin Center-Gateways. Dieses stellt den Zugriffspunkt für Webbrowser dar. Die Installation kann dabei auf einem Core-Server erfolgen, aber auch auf Hyper-V Server 2019/2022 oder Windows 10/11.



Das Windows Admin Center funktioniert optimal mit Google Chrome und Microsoft Edge. Andere Browser unterstützen die Funktionen in der Verwaltungslösung derzeit noch nicht ausreichend. Im Internet Explorer kann das Admin Center nicht genutzt werden.

Das heißt, auf einem Server kann das Admin Center nur dann direkt geöffnet werden, wenn Chrome oder Edge installiert sind. Das ist natürlich für den Gatewayendpunkt nicht notwendig. Der Browser wird nur auf dem zugreifenden Client benötigt.

Da bei Windows Server 2022 automatisch Microsoft Edge installiert ist, können Sie auch die grafische Oberfläche des Windows Admin Centers auf Servern öffnen.

Wenn im Webbrowser im Windows Admin Center eine Verbindung zu einem Server erfolgt, wird die Verbindung zwischen dem Gateway und dem entsprechenden Server hergestellt. Das heißt, alle Server kommunizieren mit dem Gateway, die Administratoren verwenden Webbrowser, zum Beispiel Google Chrome, und verbinden sich ebenfalls mit dem Gateway. Das Gateway kann auf Servern mit grafischer Oberfläche installiert werden, aber auch auf Core-Servern und Arbeitsstationen mit Windows 10/11.

Bei Servern mit grafischer Oberfläche wird das Gateway über eine MSI-Datei in der grafischen Oberfläche installiert. Hier kann auch der Port für den Zugriff festgelegt werden. Das Gateway kann auf Servern mit Windows Server ab der Version 2012R2 installiert werden, aber ebenso auf Arbeitsstationen mit Windows 10/11 ab Version 1709.

Am besten ist natürlich die Installation auf einem Server mit Windows Server 2022. Das Windows Admin Center bietet nahezu die gleichen Möglichkeiten wie der herkömmliche Server-Manager. Auch PowerShell-Sitzungen und Remotedesktopverbindungen lassen sich direkt über das Windows Admin Center aufrufen. Dazu kommen Funktionen zur Verwaltung von Windows 10/11-Arbeitsstationen, Clustern und Hyper-Converged-Clustern. Ebenso lassen sich VMs in Microsoft Azure verwalten und mit lokalen Rechnern synchronisieren.

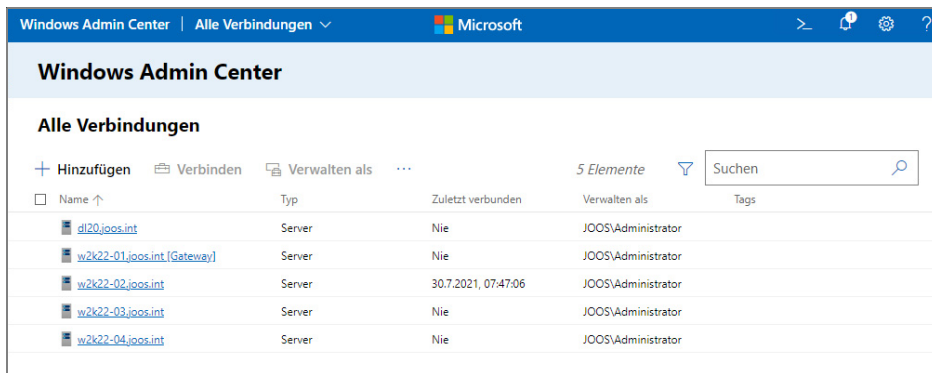


Abb. 3.9 Das Verwalten von lokalen Servern mit dem Windows Admin Center

Über das Zahnradsymbol am oberen rechten Bereich sind Einstellungen für das Windows Admin Center-Gateway zu finden. Hier lassen sich Einstellungen für einzelne Administratoren anpassen, zum Beispiel die jeweilige Sprache, in der das Windows Admin Center angezeigt wird. Die Anbindung an Microsoft Azure wird ebenfalls hier konfiguriert.

3.5.1 Admin Center Gateway installieren und aktualisieren

Die Installation des Gateways besteht aus der Bestätigung weniger Fenster. Hier werden auch Zertifikate und Ports gesteuert. Erscheint eine neue Version des Windows Admin Centers, können Sie diese auf dem Gateway installieren. Dadurch wird die alte Version aktualisiert und Sie können die neuen Funktionen nutzen. Die vorhandenen Einstellungen bleiben dabei erhalten.

Innerhalb des Windows Admin Centers gibt es die Möglichkeit, in den Einstellungen über die Option *Updates* die Aktualisierung des Windows Admin Centers zu automatisieren.



Nicht möglich ist die Installation des Windows Admin Centers auf Domänencontrollern und keinesfalls empfohlen ist die Installation des Windows Admin Centers auf Rechnern, mit denen webbasierte Dienste genutzt werden, wie zum Beispiel Exchange oder der IIS.

Das Gateway kann jederzeit wieder deinstalliert werden. Auch die vertrauenswürdigen Hosts auf einem Host lassen sich automatisch pflegen, zum Beispiel in Umgebungen ohne Domänen oder mit mehreren Gesamtstrukturen. Betreiben Sie das Windows Admin Center in einer Active Directory-Domäne, müssen Sie keine vertrauenswürdigen Hosts definieren. In diesem Fall arbeitet das Windows Admin Center mit den Berechtigungen in Active Directory.

Die aktuellen Installationsdateien für das Windows Admin Center finden Sie auf der Seite <https://www.microsoft.com/de-de/windows-server/windows-admin-center>.

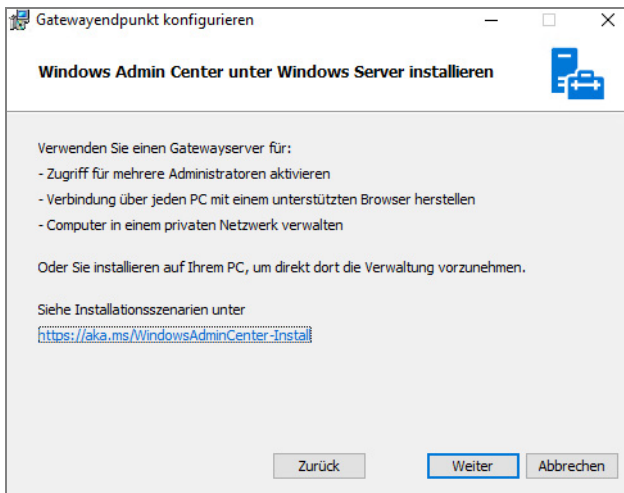


Abb. 3.10 Installieren des Gateways für das Windows Admin Center

Im Rahmen der Installation wird auch der Port festgelegt und das Zertifikat angegeben, mit dem die Verbindung über SSL abgesichert wird. Wenn bei der Installation kein Zertifikat angegeben wird, verwendet das Admin Center ein selbstsigniertes Zertifikat. Verbinden sich Administratoren mit dem Gateway, erhalten sie über den Webbrowser eine Zertifikatwarnung.



Die Verbindung des Webbrowsers von Administratoren erfolgt über das Gateway. Dieses verbindet sich wiederum mit WinRM und Remote-PowerShell oder WMI mit dem jeweiligen Server.

Damit die Remoteverbindung zwischen den Servern funktioniert, müssen die Remoteverwaltungen auf den beteiligten Servern aktiviert sein.

Das Admin Center können Sie auch über die Befehlszeile installieren. Das ist zum Beispiel sinnvoll, wenn das Gateway auf einem Core-Server installiert werden soll. Die Installation erfolgt in der Befehlszeile mit

```
msiexec /i <InstallerName>.msi /qn /L*v log.txt SME_PORT=<port> SSL_CERTIFICATE_OPTION=generate
```

Zum Beispiel:

```
msiexec /i WindowsAdminCenter2103.2.msi /qn /L*v log.txt SME_PORT=6516 SSL_CERTIFICATE_OPTION=generate
```

```
msiexec /i WindowsAdminCenter2103.2.msi /qn /L*v log.txt SME_PORT=<port> SME_THUMBPRINT=<thumbprint> SSL_CERTIFICATE_OPTION=installed
```

Wenn das Admin Center auf dem Core-Server installiert ist, kann auch hier der Zugriff über das Netzwerk mit einem Webbrowser erfolgen. Um Core-Server wiederum mit dem Admin Center zu verwalten, muss auf dem entsprechenden Server die Remoteverwaltung aktiviert sein.

Eine zusätzliche Software ist auf den Servern, die mit dem Admin Center verwaltet werden, nicht notwendig. Nur das Gateway muss auf einem Computer im Netzwerk installiert sein, die Verwaltung der angebotenen Server erfolgt mit den Standard-Verwaltungstools von Windows-Servern, die Verbindung über Browser wie Google Chrome oder Microsoft Edge. Natürlich muss zur Verwaltung auf einem Server kein Google Chrome installiert werden, Microsoft Edge ist auf Windows Server 2022 ohnehin automatisch installiert.



Die Verbindung des Webbrowsers erfolgt über das Gateway. Dieses verbindet sich wiederum mit WinRM und Remote-PowerShell oder WMI mit dem jeweiligen Server. Damit die Remoteverbindung zwischen den Servern funktioniert, müssen die Remoteverwaltungen auf den beteiligten Servern aktiviert sein.

3.5.2 Verbindungsaufbau zu Servern herstellen

Sobald der Gatewayendpunkt für das Windows Admin Center installiert ist, kann über das Netzwerk mit der URL `https://<Gatewayendpunkt>:Port` auf das Windows Admin Center zugegriffen werden. Erscheint ein Fenster zur Anmeldung, muss der Benutzername eines Administrators eingegeben werden. Das Windows Admin Center nutzt zur Authentifizierung das Active Directory.

Im Windows Admin Center lassen sich alle aktuellen Windows-Server im Netzwerk verbinden. Dazu gehören, neben Windows Server 2022, auch Server mit Windows Server 2012/2012R2 und Windows Server 2016/2019. Dazu nutzt das Admin Center zwischen dem Gateway und den Servern die standardmäßigen Remoteverbindungen von Windows-Servern.

Funktioniert eine Verbindung nicht, kann es auf dem entsprechenden Server helfen, mit `winrm quickconfig` die Remoteverwaltung zu aktivieren. Sobald ein Server verbunden ist, lässt er sich im Admin Center verwalten.

Das Hinzufügen von Servern erfolgt über den Link *Hinzufügen* und der anschließenden Auswahl des Objekts, das hinzugefügt werden soll.

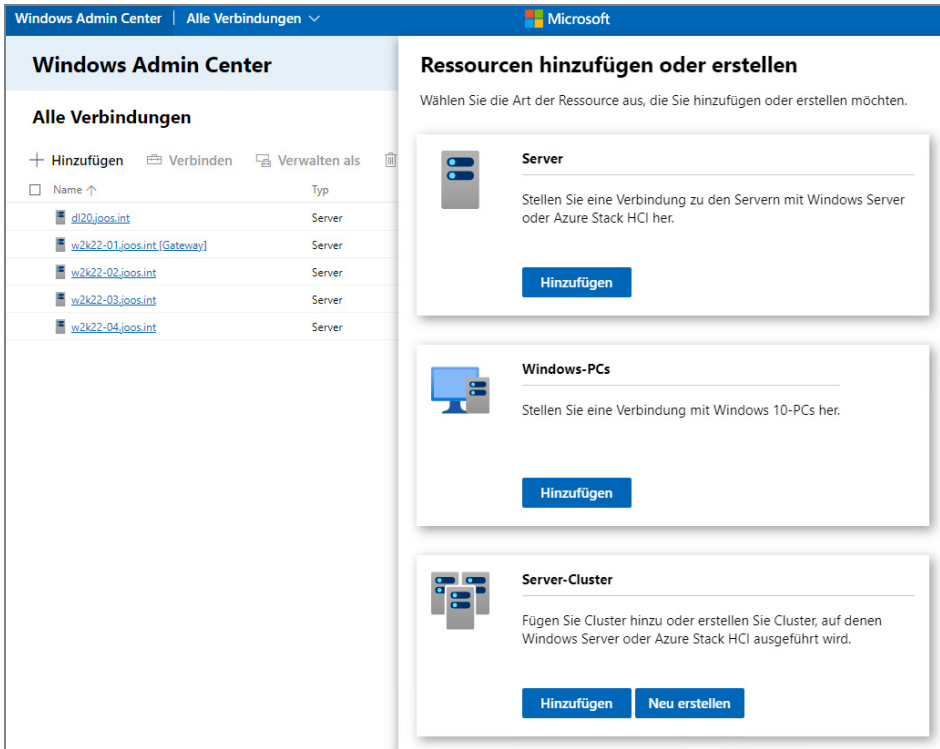


Abb. 3.11 Hinzufügen von neuen Objekten zum Windows Admin Center

Beim ersten Start erscheint ein Assistent, der über die Möglichkeiten des Windows Admin Centers informiert. Mit *Weiter* kann zur nächsten Seite des Fensters gewechselt werden. Ist die Einrichtung nach wenigen Sekunden abgeschlossen, zeigt der Browser das Startfenster des Windows Admin Centers an. Der Server, auf dem der Gatewayendpunkt installiert ist, wird automatisch hinzugefügt. Weitere Server können jederzeit hinzugefügt werden.

Das Admin Center kann nicht nur Server hinzufügen, sondern auch ganze Cluster und Arbeitsstationen. Alle Objekte lassen sich zentral im Webbrowser verwalten, sobald sich ein Administrator mit dem Gateway verbindet. Bei der Anbindung geben Sie den Namen des Servers ein oder dessen IP-Adresse. Auch die Anmeldeinformationen können Sie hier angeben und für Ihr Konto zwischenspeichern. Dadurch können Sie Server mit unterschiedlichen Benutzerkonten verwalten. Neben der manuellen Eingabe von IP-Adresse oder Servername können Sie das Active Directory nach neuen Servern durchsuchen.

3.5.3 Fehler bei der Verbindung beheben

Wenn keine Verbindung zum Windows Admin Center-Gateway erfolgen kann, sollte zunächst mit dem folgenden Befehl überprüft werden, ob die Firewallregeln korrekt gesetzt sind:

```
Get-NetFirewallRule -DisplayName "SmeInboundOpenException"
```

Vom Rechner aus, mit dem eine Verbindung hergestellt werden soll, kann die Verbindung in der PowerShell getestet werden:

`Test-NetConnection -Port <Port> -ComputerName <Gateway> -InformationLevel Detailed`
Beispiel:

`Test-NetConnection -Port 443 -ComputerName s1.joos.int -InformationLevel Detailed`

Wenn auf dem Server die Installation nicht funktioniert, können Sie den Port löschen und für das Windows Admin Center neu belegen:

`netsh http delete sslcert ipport=0.0.0.0:443`

`netsh http delete urlacl url=https://+:443/`

Kann keine Verbindung zu einem zu verwaltenden Server aufgebaut werden, kann vom Windows Admin Center Gateway getestet werden, ob eine Remote-PowerShell-Sitzung funktioniert:

`Enter-PSSession <Server>`

3.5.4 Server im Windows Admin Center verwalten

Durch einen Klick auf den Server, der im Windows Admin Center bereits verbunden ist, öffnet sich die Hauptseite des Admin Centers. Hier sind auf der linken Seite zunächst alle Bereiche zu sehen, die für die einzelnen Server konfiguriert werden können.

Im oberen Bereich kann zwischen dem webbasierten Server-Manager, dem Failovercluster-Manager, dem Hyper-Converged Cluster Manager und der Computerverwaltung von PCs umgeschaltet werden.

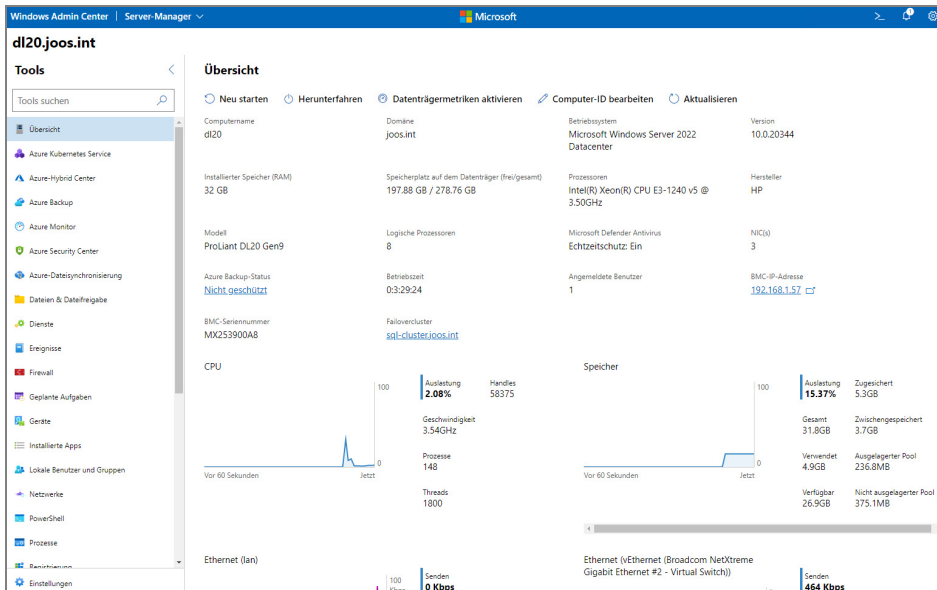


Abb. 3.12 Verschiedene Werkzeuge im Windows Admin Center

In der Mitte des Fensters werden weitere Befehle und Informationen zum jeweiligen Server oder PC angezeigt. Hier sind im oberen Bereich verschiedene Befehle zu sehen und im unteren Bereich Informationen und Optionen zum Server.

Um Server anzubinden, wird zunächst über *Hinzufügen* im Hauptfenster von Windows Admin Center eine neue Server-Verbindung hinzugefügt. Im Folgenden gehen wir von der Anbindung weiterer Server aus, die mit Windows Admin Center verwaltet werden sollen. Auch Tags (Markierungen) sind für Server möglich. So lassen sich etwa alle Hyper-V-Hosts mit dem Tag *Hyper-V-Host* markieren. Wird ein Import der Server durchgeführt, besteht der einfachste Weg darin, eine Textdatei zu erstellen, in der alle Server kommagetrennt oder in eigenen Zeilen aufgelistet werden.

Anschließend wird der Name des anzubindenden Servers angegeben sowie die Anmelde-daten. Windows Admin Center ermöglicht also die Anbindung von verschiedenen Servern mit unterschiedlichen Berechtigungen.

Nach der erfolgreichen Anbindung werden die Server im Fenster angezeigt. Durch das An-klicken eines Servers wird eine Verbindung aufgebaut. Der Zeitpunkt der letzten Verb-in-dung wird im Windows Admin Center angezeigt. Das Windows Admin Center verfügt auch über einen Benachrichtigungsbereich. Durch einen Klick auf das Icon mit der Glocke oben rechts zeigt das Admin Center die durchgeführten Aktionen und Infos zu den Aktio-nen an.

Wird ein Server angeklickt, kann ein Verbindungsaufbau erfolgen. Außerdem kann über *Verwalten als* ein alternatives Benutzerkonto ausgewählt werden, mit dem der Server ver-bunden wird. Ebenso ist die Bearbeitung der Tags auf der Startseite des Windows Admin Centers möglich. Sobald der Server verbunden ist, kann er über die Befehle am linken Rand verwaltet werden. Hier lassen sich Serverrollen installieren, die Windows-Firewall anpas-sen, die Registry öffnen und vieles mehr.

Auf der Übersichts-Seite können Sie den Server neu starten oder herunterfahren. Auch den Servernamen, inklusive Domänenmitgliedschaft können Sie über *Computer-ID bearbeiten* ändern.

Durch einen Klick auf einen Menüpunkt, zum Beispiel *Rollen und Features* oder *Firewall*, erscheinen auf der rechten Seite weitere Befehle und Informationen. Hier stehen die Menü-punkte *Übersicht*, *Regeln für eingehende Verbindungen* und *Regeln für ausgehende Verbin-dungen* zur Verfügung. Mit diesen Menüpunkten können nicht nur die Regeln überprüft, sondern auch angepasst, deaktiviert und aktiviert werden. Bei *Übersicht* ist zu sehen, wel-che Firewall-Profile aktiv sind. Die Firewallregeln können im Webbrowser zusätzlich ange-passt werden. Das Erstellen von neuen Regeln ist ebenso möglich.

Auf diesem Weg lassen sich über das Netzwerk zahlreiche Einstellungen auf Servern vor-nehmen, bis hin zur Installation von Server-Rollen und der Verwaltung von Windows-Up-dates. Für Hyper-V-Hosts lassen sich über den Server-Manager auch die virtuellen Switches konfigurieren. Warnungen und Fehler werden hier ebenfalls angezeigt und lassen sich kor-rigieren.

Um mit dem Windows Admin Center Rollen zu installieren, wird der Menüpunkt *Rollen und Features* angeklickt. Danach zeigt das Fenster in der Mitte alle verfügbaren Serverrollen an. Hier ist bei *Status* zu sehen, welche Rollen bereits installiert sind. Durch einen Klick auf eine Server-Rolle kann diese über das Fenster installiert oder deinstalliert werden. Auch einzelne Rollendienste lassen sich an dieser Stelle installieren oder deinstallieren.

| Rollen und Features | |
|---|-----------------------|
| + Installieren — Deinstallieren | |
| Name | Status |
| <input type="checkbox"/> Rollen | 11 von 92 installiert |
| Active Directory Lightweight Directory Services | Verfügbar |
| Active Directory-Domänendienste | Verfügbar |
| > Active Directory-Rechteverwaltungsdienste | 0 von 2 installiert |
| Active Directory-Verbunddienste | Verfügbar |
| > Active Directory-Zertifikatdienste | 0 von 6 installiert |
| > Datei-/Speicherdienste | 2 von 12 installiert |
| Device Health Attestation | Verfügbar |
| <input checked="" type="checkbox"/> DHCP-Server | Verfügbar |
| DNS-Server | Verfügbar |
| > Druck- und Dokumentdienste | 0 von 3 installiert |
| Faxserver | Verfügbar |
| Host Guardian-Dienst | Verfügbar |
| Hyper-V | Installiert |
| Netzwerkcontroller | Verfügbar |
| Netzwerkrichtlinien- und Zugriffsdienste | Verfügbar |
| > Remotedesktopdienste | 0 von 6 installiert |
| Details - DHCP-Server (1 Ausgewählt) | |
| Beschreibung | |
| Der Dynamic Host Configuration-Protokoll (DHCP)-Server ermöglicht das zentrale Konfigurieren, Clientcomputer. | |

Abb. 3.13 Serverrollen im Windows Admin Center installieren

3.5.5 Mit Markierungen arbeiten und Objekte suchen

Sie können im Windows Admin Center den einzelnen Objekten und Servern Markierungen (Tags) zuweisen. Das geht beim Hinzufügen eines Servers, aber auch jederzeit nachträglich. Markierungen werden in der Übersicht des Windows Admin Centers in der Spalte *Tags* angezeigt. Über den Menüpunkt *Tags bearbeiten* können Sie Servern Markierungen zuweisen, zum Beispiel *dc* oder *Hyper-V-Host*, *Dateiserver* oder *Rechenzentrum1*. Sie können Servern und Objekten wie Clustern natürlich mehrere Markierungen zuweisen.

Auf der ganz rechten Seite können Sie mehrere Server auf einmal markieren. Klicken Sie auf *Tags bearbeiten*, können Sie den Servern gleichzeitig ein Tag zuweisen. Einmal erstellte Tags werden im Fenster angezeigt und müssen nicht neu eingetippt werden.

Sie sehen die Tags nicht nur im Windows Admin Center in der Spalte *Tags*, sondern können auch nach Tags im Suchfeld suchen. Das erleichtert die Navigation im Windows Admin Center.

3.5.6 Datei-Explorer, Registry-Editor, PowerShell und Remotedesktop nutzen

Neben der Verwaltung von Serverrollen und Einstellungen für den Server kann über das Windows Admin Center auch auf das Dateisystem des Servers zugegriffen werden. Hier sind Dateiaktionen auf dem jeweiligen Server möglich und Dateien lassen sich vom PC, der mit dem Windows Admin Center verbunden ist, hoch- und herunterladen. Informationen zu Dateien können angezeigt und Ordner erstellt, Daten gelöscht und umbenannt werden. Den webbasierten Datei-Explorer finden Sie über den Menüpunkt *Dateien*.

Wenn Sie mit einem Webbrowser mit dem Windows Admin Center verbunden sind, lassen sich Dateien auf die Arbeitsstationen des Administrators herunter- und von der Arbeitsstation des Administrators zum verbundenen Server hochladen. Die Verbindung läuft auch hier über das Gateway. Für den Down- und Upload steht der Bereich *Dateien* zur Verfügung. Hierüber starten Sie den webbasierten Datei-Explorer des Windows Admin Centers. Über den Menüpunkt *Registrierung* können Sie wiederum den webbasierten Registry-Editor auf dem Server öffnen. Sie können Einträge in der Registry lesen, exportieren und importieren und Schlüssel und Werte bearbeiten sowie Werte erstellen.

Zusätzlich kann über *PowerShell* eine PowerShell-Sitzung im Webbrowser geöffnet werden, der Befehle auf dem remotegesteuerten Server ausführt. Mit *Remotedesktop* kann im Webbrowser eine Remotedesktop-Verbindung zum jeweiligen Server aufgebaut werden.

3.5.7 Gatewayzugriff steuern

Natürlich kann festgelegt werden, welche Administratoren Zugriff auf das Admin Center erhalten sollen und welche Server sie verwalten dürfen. Dazu steht im Admin Center die rollenbasierte Zugriffssteuerung zur Verfügung. In den Einstellungen des Gateways finden Sie links den Menüpunkt *Gatewayzugriff*. Hier können Sie steuern, welche Benutzergruppen das Recht erhalten, auf das Gateway zuzugreifen.

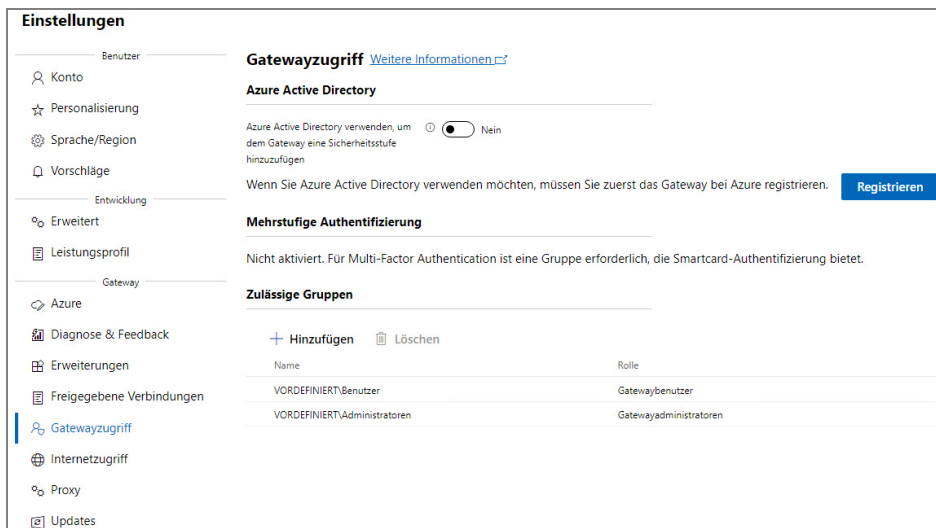


Abb. 3.14 Konfigurieren der Rechte für den Zugriff auf das Gateway

Mit der rollenbasierten Zugriffssteuerung kann über *Active Directory-Benutzer und -Gruppen* gesteuert werden, wer das Windows Admin Center nutzen darf.

3.5.8 Zertifikat für das Windows Admin Center steuern

Wer das Windows Admin Center dauerhaft produktiv im Netzwerk einsetzt, sollte ein Zertifikat verwenden. Hier lassen sich auch die Active Directory-Zertifikatdienste verwenden. Dazu muss dem Server mit dem Windows Admin Center-Gateway zunächst ein Zertifikat zugewiesen werden. Das Zertifikat kann über *certlm.msc* verwaltet werden.

Auch das Abrufen von neuen Zertifikaten kann hier erfolgen. In den Eigenschaften eines Zertifikats kann anschließend der Fingerabdruck auf der Registerkarte *Details* abgerufen werden.

Der Fingerabdruck wird danach im Windows Admin Center hinterlegt. Dazu rufen Sie das Installationsprogramm auf und wählen die Option *Ändern* aus. Bei einer Neuinstallation verwenden Sie das Zertifikat, indem im entsprechenden Feld sein Fingerabdruck genutzt wird.

Anschließend steht das Zertifikat zur Verfügung und das Windows Admin Center verwendet es in Zukunft für Verbindungen der Administratoren.

3.5.9 Erweiterungen für das Windows Admin Center

Im Windows Admin Center finden sich oben rechts seine Optionen. Hier können Erweiterungen installiert werden und die Verbindung zu Microsoft Azure erfolgen.

Auch hier erweitert Microsoft die Funktionen mit jeder neuen Version. In den Erweiterungen werden Funktionen von Drittherstellern integriert, aber genauso erweiterte Funktionen von Windows-Servern, wie zum Beispiel der Windows Server Storage Migration-Assistent von Windows Server 2022.

Microsoft bietet auch eine API, mit der sich Erweiterungen für das Admin Center programmieren lassen. Diese können direkt im Windows Admin Center hinzugefügt werden. Dazu steht ein eigener Menüpunkt zur Verfügung.

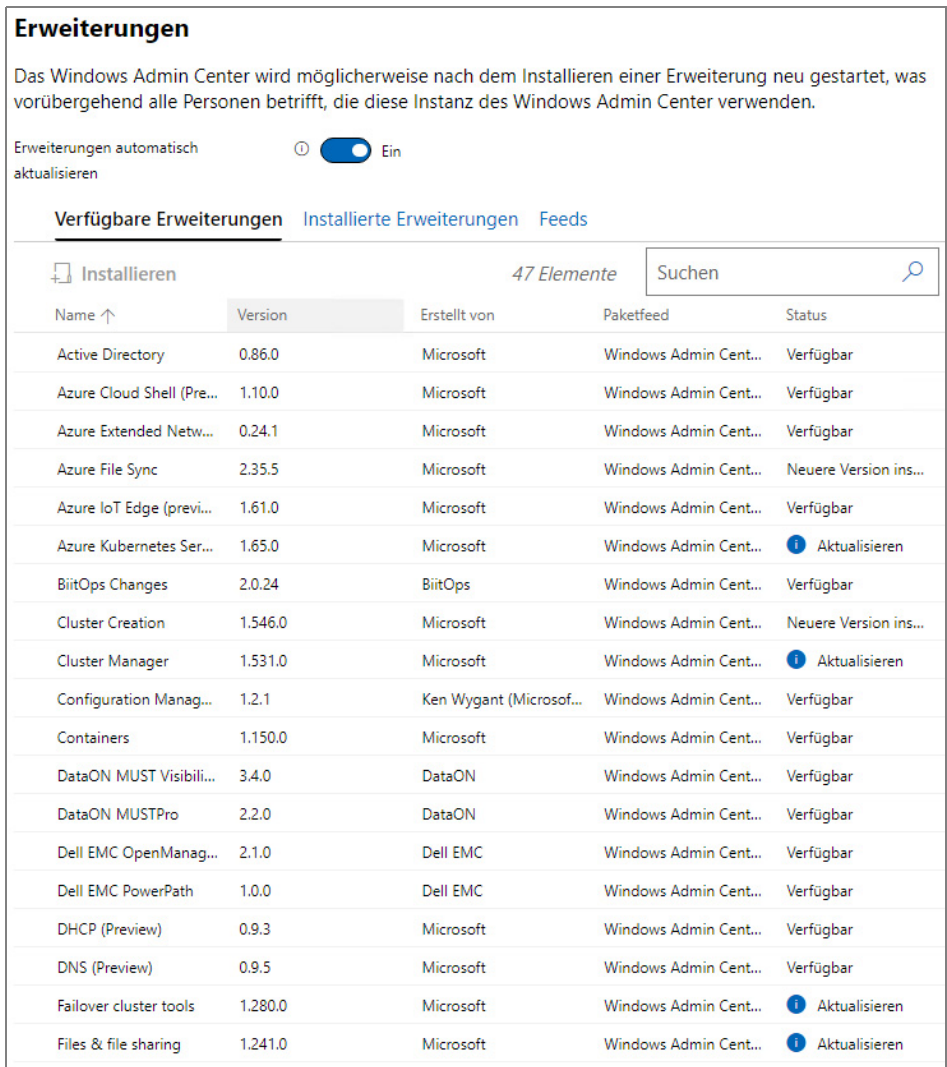


Abb. 3.15 Erweiterungen im Windows Admin Center installieren

3.5.10 Windows Admin Center und Microsoft Azure

Verbinden Sie das Windows Admin Center mit Microsoft Azure, können Sie nicht nur Azure-VMs im Windows Admin Center verwalten. Sie können Server im lokalen Netzwerk mit Azure Backup sichern, VMs mit Azure Site Recovery VMs in Azure hochverfügbar replizieren und andere Funktionen von Microsoft Azure nutzen. Die interessantesten Funktionen in Microsoft Azure zur Unterstützung von lokalen Netzwerken sind Azure Backup, Azure Monitor, Azure Security Center und Azure Site Recovery. Es gibt weitaus mehr Funktionen, aber mit diesen Diensten aus Azure können auch lokale Netzwerke schnell profitieren.

Um das Windows Admin Center mit Microsoft Azure zu verbinden, müssen Sie die entsprechende Konfiguration nur auf dem Server vornehmen, auf dem das Admin Center-Gateway verbunden ist. Sobald die Anbindung einmal erfolgt ist, erhalten Administratoren, die mit dem Webbrowser auf das Gateway zugreifen, auch Zugriff auf die Funktionen in Microsoft Azure, wenn sie dazu berechtigt sind.

Zur Anbindung rufen Sie im Windows Admin Center über das Zahnradsymbol die Einstellungen auf.

Der Vorteil dabei besteht darin, dass die Anbindung an Microsoft Azure nur einmal für das WAC-Gateway durchgeführt werden muss. Danach stehen die Azure-Funktionen an den verschiedenen Stellen zur Verfügung und können auf lokalen Servern eingebunden werden. Die Anbindung an Microsoft Azure wird mit jeder neuen Version des Windows Admin Centers einfacher.

Über die Einstellungen des Gateways ist bei *Azure* der Assistent zu finden, mit dem die Anmeldung an Azure erfolgen kann. Danach stehen die verschiedenen Azure-Dienste im Netzwerk zur Verfügung.

Zur Anbindung des Windows Admin Center-Gateways werden im Windows Admin Center über das Zahnradsymbol die Einstellungen aufgerufen. Über den Menüpunkt *Azure* kann der Vorgang zum Registrieren gestartet werden. Danach erscheint auf der rechten Seite ein Code, der für die Anmeldung an Microsoft Azure benötigt werden. Den Code sollten Sie in die Zwischenablage kopieren.

Durch einen Klick auf den Link *Geräteanmeldung* kann die Anmeldung an Microsoft Azure erfolgen. Zunächst müssen Sie Anmeldedaten für ein Azure-Konto angeben. Außerdem muss der Code im Fenster eingegeben werden. Dadurch registriert sich das Windows Admin Center-Gateway mit dem angegebenen Azure-Konto.

Nach dieser Aktion ist das Windows Admin Center mit dem entsprechenden Azure-Abonnement verbunden und kann genutzt werden. Allerdings sind zuvor noch Anpassungen im Webportal von Microsoft Azure notwendig. Das verbundene Gateway muss erst Rechte erhalten, Dienste in Microsoft Azure zu nutzen. Verbinden sich Administratoren im lokalen Rechenzentrum mit dem Gateway, können sie die Funktionen nutzen, ohne erneut Anpassungen oder Verwaltungen vorzunehmen.

Sobald das lokale Windows Admin Center-Gateway in Microsoft Azure registriert ist, wird der Status im Windows Admin Center angezeigt. An dieser Stelle kann die Registrierung auch wieder aufgehoben werden. Wenn die lokale Installation des Windows Admin Centers aktualisiert wird, übernimmt der Installationsassistent die Registrierung, sodass keine erneute Anmeldung an Microsoft Azure erfolgen muss.

Im Azure-Portal müssen anschließend noch die Berechtigungen für das Windows Admin Center freigeschaltet werden. Dazu klicken Sie im Windows Admin Center in den Einstellungen bei auf *In Azure anzeigen*.

Im Azure-Portal müssen Sie außerdem bei der registrierten App für das Windows Admin Center auf *Einstellungen* und dann auf *Erforderliche Berechtigungen* klicken. Durch die Bestätigung von *Berechtigungen erteilen* können Sie die Azure-Funktionen nutzen.

Nach der Registrierung des Admin Centers mit einem Azure-Abonnement steht der Menüpunkt *Azure-Hybriddienste* zur Verfügung. Hier können Sie über Assistenten die Funktionen von Azure im lokalen Rechenzentrum einbinden und diese auch mit dem Windows Admin Center verwalten:

- **Azure Backup** – Sicherung von lokalen Servern und Arbeitsstationen in einen sicheren Cloud-Speicher
- **Azure Site Recovery** – Virtuelle Server in Hyper-V in die Cloud synchronisieren, für Hochverfügbarkeit und Wiederherstellung
- **Azure-Netzwerkadapter** – Point-to-Site-VPNs mit Azure einrichten
- **Azure Monitor** – Lokale Server überwachen

Azure Backup mit dem Windows Admin Center steuern

Ein Vorteil bei der Integration von Azure im Windows Admin Center besteht auch darin, dass die Azure-Dienste genauso verwaltet werden wie lokale Dienste. Nach der Anbindung an Microsoft Azure steht nach der Anbindung eines Servers im WAC zum Beispiel *Azure Backup* zur Verfügung. Hierüber können Sie den ausgewählten Server in die Cloud sichern. Die Einrichtung erfolgt durch einen Assistenten. Danach können Sie die Sicherung des Servers jederzeit im Windows Admin Center steuern. Auch Wiederherstellungen von Servern sind hier verfügbar.

Azure Monitor und Azure Security Center

Neben den Bordmitteln im Windows Admin Center können Windows-Server mit Ressourcen aus Microsoft Azure überwacht werden. Azure Monitor zum Überwachen von Servern und Azure Security Center zum Anzeigen von Sicherheitslücken und Sicherheitsgefahren sind über die entsprechenden Menüpunkte im Windows Admin Center verfügbar. Lokale Server können auf diesem Weg problemlos angebunden und überwacht werden. Auch hier übernimmt das WAC die Anmeldedaten des Gateways.

Azure Site Recovery – Azure in die Hyper-V-Hochverfügbarkeit einbinden

Mit Azure Site Recovery ist es möglich, einzelne VMs in die Azure-Cloud zu replizieren. Dadurch wird eine Hochverfügbarkeit für VMs erreicht, ohne einen internen Cluster aufbauen zu müssen. Parallel zu einem Cluster können mit Azure Site Recovery VMs repliziert werden, und zwar ebenfalls wieder komplett über das Windows Admin Center.

Wenn im Windows Admin Center ein Hyper-V-Host hinzugefügt wird, stehen die Menüpunkte *Virtuelle Computer* und *Virtuelle Switches* zur Verfügung. Hierüber verwalten Administratoren die lokalen VMs in Hyper-V. Über den Menüpunkt *Verwalten* beim Öffnen einer VM im WAC steht der Menüpunkt *Mithilfe von Azure Site Recovery replizieren* zur Verfügung. Hierüber kann die Replikation von VMs über das Windows Admin Center zu Microsoft Azure gesteuert werden. Die Einrichtung kann komplett im WAC erfolgen und danach auch verwaltet werden.

Angebundene Azure-Dienste zentral verwalten

Um einen Überblick darüber zu behalten, welche Dienste auf Servern in Microsoft Azure genutzt werden, steht der Menüpunkt *Azure Hybriddienste* zur Verfügung. Hier zeigt das WAC die Azure-Dienste an, die auf dem verbundenen Server angebunden wurden. Durch einen Klick auf den jeweiligen Dienst können Sie direkt zur entsprechenden Azure-Ressource im WAC wechseln.

Netzwerke im Windows Admin Center verwalten – Azure und virtuelle Switches

Über den Menüpunkt *Netzwerke* werden die Netzwerk-Einstellungen des lokalen Servers angezeigt und verwaltet. Handelt es sich bei diesem Server um einen Hyper-V-Host, sind hier auch die virtuellen Switches und die verwendeten virtuellen Adapter zu finden. Virtuelle Switches werden wiederum über den Menüpunkt *Virtuelle Switches* im WAC verwaltet. Natürlich lassen sich hier auch die Einstellungen der Netzwerke anpassen.

Über *Azure-Netzwerkanschluss hinzufügen* können Sie lokale Netzwerke mit einem VPN an Azure anbinden. Das ermöglicht die Verwendung von Ressourcen in der Cloud direkt auf dem Server.

Windows-Updates zentral im Windows Admin Center verwalten

Über den Menüpunkt *Updates* können Sie bei einem verbundenen Server die Windows-Updates steuern. Das ist schon lange im Windows Admin Center möglich. Soll die Installation von Updates automatisiert werden, steht die Azure-Updateverwaltung zur Verfügung. Auch diese können Sie über das Windows Admin Center nutzen. Dadurch können Administratoren mit Azure Automation Verwaltungsaufgaben auf lokalen Servern durchführen, zum Beispiel das Installieren von Updates zentral verwalten.

Über den Menüpunkt *Updates* ist zu sehen, ob für einen Server Updates zur Verfügung stehen. Die Updates können an dieser Stelle über den Webbrowser und das Windows Admin Center gleich installiert werden. Außerdem kann über diesen Bereich die Anbindung eines Servers an die Azure-Updateverwaltung erfolgen.

Über den Menüpunkt *Einstellungen* werden die Konfigurationen für die Installation von Updates für den entsprechenden Server erreicht. Hier können Sie festlegen, ob der Server automatisch nach Updates suchen und diese installieren soll oder ob das manuell erfolgen soll.

Mit dem Link *Online nach Updates von Microsoft Update suchen* können Sie über den Webbrowser nach Updates für den Server suchen, der Menüpunkt *Updateverlauf* zeigt die bereits installierten Updates auf dem Server an.

3.5.11 Windows Server 2022 mit Windows Admin Center überwachen

Mit dem webbasierten Windows Admin Center können Server mit Windows Server 2012 R2 und Windows Server 2016/2019 verwaltet werden. Setzen Unternehmen auf Windows Server 2022, kann die Erweiterung Windows Server System Insights noch mehr Überwachungsfunktionen nutzen.

Administratoren müssen regelmäßig dafür sorgen, dass Server fehlerfrei und optimal funktionieren. Viele Unternehmen setzen dazu auf Überwachungslösungen von Drittherstellern oder auf Produkte der System Center-Reihe von Microsoft. Die Überwachung, ob eine Festplatte keinen Speicherplatz mehr hat, eine Festlegung, wie viel Speicherplatz verbraucht ist, und die Kontrolle eines Hyper-V-Hosts, um neue VMs zu planen, sind nur einige Beispiele.

3.5.12 Performance Monitor im Windows Admin Center

Mit dem Windows Admin Center steht auch der Performance Monitor zur Verfügung. Das heißt, Sie können im Browser mit der Leistungsüberwachung (*perfom.msc*) arbeiten, genauso wie bei der lokalen Verbindung mit dem Server. Nachdem ein Dashboard erstellt wurde, können Counter hinzugefügt werden, und die Leistung des Servers wird in Echtzeit überwacht. Die Überwachung kann pausiert werden. Die Workspaces und auch Einstellungen können für die Leistungsüberwachung gespeichert werden. Durch das Speichern bietet sich natürlich die Möglichkeit, die Leistungsmonitore wieder zu laden. Der Vorteil dabei ist, dass Administratoren die Oberfläche nicht immer neu zusammenstellen müssen.

Funktionen von Windows Server System Insights

Windows Server System Insights ist eine neue Funktion in Windows Server 2022, die lokale prädiktive Analysefunktionen nativ auf Windows-Server bringt. Diese vorausschauenden Funktionen, die jeweils durch ein Modell zum maschinellen Lernen unterstützt werden, analysieren lokal Windows Server-Systemdaten. Dazu gehören Leistungsindikatoren und Ereignisse. Die Funktionen in Windows Server System Insights liefern Vorhersagen, die dabei helfen, Windows-Server effektiver zu betreiben.

Diese Funktionen werden lokal ausgeführt. Das heißt, alle Daten werden direkt auf der lokalen Windows Server-Instanz gesammelt, gespeichert und analysiert. Die Analysefunktionen können daher gänzlich ohne Cloud-Konnektivität genutzt werden. Mit Windows Server 2022 kann System Insights zukünftige Nutzung für Auslastung des Servers, Netzwerkverkehr und Datenspeicherung vorhersagen.

Systeminformationen, die Windows Server System Insights von Servern mit Windows Server 2022 bietet, lassen sich vollständig über Windows Admin Center verwalten. System Insights bietet darüber hinaus auch eine PowerShell-Schnittstelle, mit der sich Automatisierungen durchführen lassen. Wie das Windows Admin Center auch, entwickelt Microsoft Windows Server System Insights ständig weiter und integriert neue Funktionen.

So können Sie durch die Vorhersagefunktionen blättern und rufen entweder eine Funktion bei Bedarf auf oder konfigurieren sie so, dass sie nach einem regelmäßigen Zeitplan ausgeführt wird. Sie können die Vorhersageergebnisse auch visualisieren, sobald genügend Messdaten vorhanden sind. Das hilft dabei, die Entwicklung des Kapazitätsverbrauchs zu verstehen. Bis genügend Daten gemessen wurden, kann es einige Zeit dauern.

Windows Server System Insights kann aber nicht nur über die Auslastung von Servern informieren, sondern aktiv in die Serverkonfiguration eingreifen. Sie können zum Beispiel Korrekturaufträge so konfigurieren, dass sie automatisch ausgeführt werden, nachdem eine Funktion ein bestimmtes Ergebnis erzeugt hat. Für Skripts lassen sich auch Anmelde-daten hinterlegen, mit deren Berechtigungen anschließend Anpassungen am Server vorgenommen werden.

Sie können auch die PowerShell auf Remote-Instanzen verwenden, um Vorhersageergebnisse zu erhalten und zu aggregieren. Auf diesem Weg können Sie eine Gruppe von Windows Server-Instanzen zur Überwachung koppeln. Beispiele dafür sind Cluster, gruppierte Anwendungs-Server, Server in einem bestimmten Rack oder Rechenzentrum. Hier kann flexibel gesteuert werden. Microsoft plant, in Zukunft Cluster-Speicherprognosen, PowerShell-Skript zur Fehlerbehebung und die Möglichkeit der dynamischen Installation neuer Vorhersagefunktionen in Windows Server System Insights zu integrieren.

Windows Server System Insights installieren

Für Windows Server System Insights wird zunächst eine Installation des Windows Admin Centers im Netzwerk benötigt. Idealerweise sollten hier möglichst aktuelle Versionen verwendet werden.

Sobald ein Server mit Windows Server 2022 angebunden ist, steht im Windows Admin Center bei der Anbindung von deutschen Servern der Menüpunkt *Systemdaten* zur Verfügung. Durch einen Klick auf diesen Menüpunkt können Sie im aktuellen Windows Admin Center die Erweiterung für Windows Server System Insights installieren. Anschließend steht der Bereich zur Verfügung, zeigt aber noch keine Daten an.

Durch einen Klick auf einen der Bereiche zur Überwachung der CPU-Last, der Netzwerk-Auslastung oder des Speicherverbrauchs kann ein Zeitplan festgelegt werden, der steuert, wann ein Server Vorhersagen erstellt.

Über *Aktionen* werden wiederum die Skripts hinterlegt, die ausgeführt werden, wenn ein Server einen bestimmten Status erreicht. Über den Menüpunkt *Aufrufen* können Sie eine sofortige Vorhersage erstellen und anzeigen lassen.

Neben Windows Server System Insights spielen natürlich auch die Daten eine Rolle, die das Windows Admin Center im Bereich *Übersicht* anzeigt, wenn ein Server im Windows Admin Center angeklickt wird. Hier werden Laufzeitdaten der CPU-Belastung, des Netzwerks und des Speichers angezeigt sowie eine Vielzahl weiterer Informationen über den lokalen Server.

Neben Windows Server System Insights und der Übersicht zu den Servern im Windows Admin Center können Sie in den Einstellungen noch Erweiterungen installieren. Auch hier integriert Microsoft regelmäßig neue Erweiterungen und bindet auch solche von Drittherstellern an. Dazu gehören aktuell zum Beispiel Überwachungsfunktionen von Fujitsu-Servern und andere Technologien.

Dienste und Prozesse überwachen

Mit den beiden Menüpunkten *Dienste* und *Prozesse* können die Verwaltung von Systemdiensten und die Überwachung von Prozessen durchgeführt werden. Sobald der entsprechende Menüpunkt ausgewählt wurde, stehen im oberen Bereich des Fensters wieder weitere Befehle zur Verfügung, um Dienste und Prozesse zu verwalten. Hier lassen sich zum Beispiel Systemdienste starten, beenden sowie deren Einstellungen anpassen. Bei Prozessen können Filter erstellt werden. Außerdem können Administratoren Prozesse beenden oder einen Dump des Prozesses erstellen.

3.5.13 Hyper-V mit dem Windows Admin Center verwalten

Über das Windows Admin Center kann auf einem Server mit Windows Server 2022 Hyper-V installiert und verwaltet werden. Dazu wird der Bereich *Rollen und Funktionen* genutzt. Hier sehen Sie, ob auf einem Server bereits Hyper-V installiert ist. Wenn das nicht der Fall ist, kann die Installation über den Webbrowser erfolgen.

Nach der Installation finden Sie auf einem Server die beiden Menüpunkte *Virtuelle Computer* und *Virtuelle Switches*. Hierüber werden die VMs und virtuellen Switches des ausgewählten Hyper-V-Hosts verwaltet.

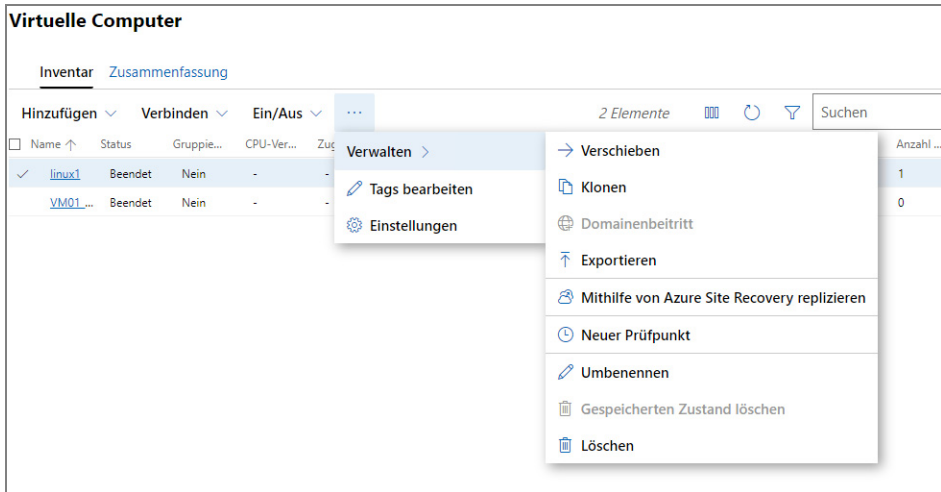


Abb. 3.16 Hyper-V im Windows Admin Center verwalten

Mit dem Menüpunkt *Inventar* erhalten Sie Zugriff auf die VMs des Servers und können diese über den Menüpunkt *Mehr* auch verwalten.

Über den Menüpunkt *Einstellungen* unten links lassen sich serverspezifische Einstellungen im Windows Admin Center vornehmen. Hier können Sie zum Beispiel auch die Hyper-V-Einstellungen eines Hyper-V-Hosts definieren.



Abb. 3.17 Einstellen von Servern im Windows Admin Center

Im Windows Admin Center ist die neue Funktion Windows Server System Insights über den Menüpunkt *Systemdaten* integriert. Hier können Sie über einen Assistenten zum maschinellen Lernen einen Hyper-V-Host überwachen. Dazu kann Insights auch Prognosen erstellen, wann es zum Beispiel auf einem Server zu Engpässen kommen kann.

3.6 Zusammenfassung

In diesem Kapitel haben wir Ihnen grundsätzlich gezeigt, wie Sie mit der Oberfläche von Windows Server 2022 umgehen. Wir sind darauf eingegangen, wie Sie Server im Netzwerk verwalten und mit dem Server-Manager in Windows Server 2022 umgehen.

Auch die Verwaltung und Einrichtung von Core-Servern sowie die Verwaltung von Windows Server mit den Remoteserver-Verwaltungstools in Windows ist Bestandteil des Kapitels.

Im nächsten Kapitel erfahren Sie, wie Serverrollen und Features in Windows Server 2022 installiert werden.

Kapitel 4

Serverrollen und Features installieren und einrichten

In diesem Kapitel zeigen wir Ihnen, welche verschiedenen Serverrollen und Features es gibt und wie Sie diese installieren. Serverrollen beschreiben die primäre Funktion eines Servers, zum Beispiel Webserver oder Domänencontroller. Features ergänzen das Betriebssystem um weitere Funktionen. Rollendienste erweitern wiederum die Serverrollen um weitere Funktionen.

Oft verschwimmen die Grenzen zwischen Features und Rollen sowie Rollendiensten. Die notwendigen Dateien für die Installation eines Windows-Clusters werden zum Beispiel als Feature und nicht als Serverrolle installiert.



Sie benötigen für die Installation von neuen Rollen und Diensten keine Installationsdateien von Windows Server 2022. Die notwendigen Dateien sind in der Installation eines Servers bereits verfügbar.

In Windows Server 2022 installieren Sie Rollen und Features über einen gemeinsamen Assistenten, bei Bedarf auch beides gemeinsam. Das erspart Neustarts und unnötige Konfigurationen. Sie können in Windows Server 2022 Rollen und Features über den Server-Manager oder das Windows Admin Center auch auf anderen Servern im Netzwerk installieren. Haben Sie die Remoteserver-Verwaltungstools von Windows 10/11 im Einsatz, können Sie die Installation ebenso von Arbeitsstationen aus starten. Über Arbeitsstationen können Sie mit einem Browser ebenfalls das Windows Admin Center nutzen.

In den einzelnen Kapiteln in diesem Buch gehen wir auf die Installation der jeweiligen Serverrolle ausführlich ein. In diesem Kapitel erfahren Sie wiederum generelle Vorgehensweisen, um Serverrollen zu installieren. In Kapitel 2 und 3 sind wir darauf eingegangen, wie Sie Serverrollen auch auf Core-Servern installieren.

4.1 Installieren von Serverrollen und Features auf einem Server

Auf einem Server lassen sich mehrere Rollen parallel und gleichzeitig über den Assistenten zum Hinzufügen von Rollen und Features installieren. In Windows Server 2022 können Sie Features zusammen mit Rollen installieren, wenn Sie den Server-Manager verwenden. Über den Eintrag *Verwalten/Rollen und Features hinzufügen* im Server-Manager startet ein Assistent, über den Sie einzelne Rollen auswählen und installieren können, auch mehrere Rollen auf einmal.

Im Windows Admin Center sind Rollen und Features untereinander angeordnet und lassen sich über *Rollen und Features* installieren. Dazu verbinden Sie sich mit dem Server im Windows Admin Center und klicken auf *Rollen und Features*. Setzen Sie einen Haken bei der Rolle, die Sie installieren wollen, und klicken Sie danach auf *Installieren*. Auf dem gleichen Weg können Sie mit *Deinstallieren* Serverrollen auch wieder entfernen.

Rollen und Features

+ Installieren — Deinstallieren 268 Elemente 46 ausgewählt ✕ ↻

| Name | Status | Typ |
|---|-----------------------|--------------|
| ▼ Rollen | 11 von 92 installiert | |
| ✓ Active Directory Lightweight Directory Services | Verfügbar | Role |
| Active Directory-Domänendienste | Verfügbar | Role |
| ✓ Active Directory-Rechteverwaltungsdienste | 0 von 2 installiert | Role |
| ✓ Active Directory-Rechteverwaltungsserver | Verfügbar | Role Service |
| ✓ Unterstützung für Identitätsverbund | Verfügbar | Role Service |
| Active Directory-Verbunddienste | Verfügbar | Role |
| > Active Directory-Zertifikatdienste | 0 von 6 installiert | Role |
| > Datei-/Speicherdienste | 2 von 12 installiert | Role |
| Device Health Attestation | Verfügbar | Role |
| DHCP-Server | Verfügbar | Role |
| DNS-Server | Verfügbar | Role |
| > Druck- und Dokumentdienste | 0 von 3 installiert | Role |
| Faxserver | Verfügbar | Role |
| Host Guardian-Dienst | Verfügbar | Role |
| Hyper-V | Installiert | Role |
| Netzwerkcontroller | Verfügbar | Role |

Details - Active Directory Lightweight Directory Services (46 Ausgewählt)

Beschreibung
 Active Directory Lightweight Directory Services (AD LDS) stellt für verzeichnisfähige Anwendungen, die nicht die Infrastruktur der Active Directory-Domänendienste benötigen, einen Speicher für anwendungsspezifische Daten bereit. Auf einem einzelnen Server können mehrere AD LDS-Instanzen mit jeweils eigenem Schema vorhanden sein.

Abb. 4.1 Rollen im Windows Admin Center installieren und verwalten

4.1.1 Rollen installieren

Rollen sind meistens in mehrere Rollendienste aufgeteilt, die Sie nachträglich noch hinzufügen können. Auch das kann im Server-Manager und im Windows Admin Center erfolgen. Dazu müssen Sie einfach den entsprechenden Assistenten erneut starten oder die Rolle im Windows Admin Center auswählen und installieren lassen.

Wählen Sie eine Rolle aus, wird der Assistent im Server-Manager erweitert, um die Rolle zu konfigurieren oder weitere Rollendienste zur Rolle hinzuzufügen. Im Windows Admin Center sind die einzelnen Rollendienste unter den jeweiligen Rollen angeordnet und können jederzeit installiert werden.

| Rollen und Features | |
|--|-----------|
| + Installieren — Deinstallieren | |
| Name | Status |
| Volumenaktivierungsdienste | Verfügbar |
| <ul style="list-style-type: none"> ✓ ✓ Webservers (IIS) 8 von 43 installiert <ul style="list-style-type: none"> ✓ ✓ FTP-Server 0 von 2 installiert <ul style="list-style-type: none"> ✓ FTP-Dienst Verfügbar ✓ FTP-Erweiterbarkeit Verfügbar > ✓ Verwaltungsprogramme 1 von 7 installiert <ul style="list-style-type: none"> ✓ ✓ Webserver 7 von 34 installiert <ul style="list-style-type: none"> > ✓ Allgemeine HTTP-Features 4 von 6 installiert > ✓ Anwendungsentwicklung 0 von 11 installiert > ✓ Leistung 1 von 2 installiert > ✓ Sicherheit 1 von 9 installiert > ✓ Systemzustand und Diagnose 1 von 6 installiert | |

Abb. 4.2 Installieren von Rollendiensten unterhalb von Serverrollen im Windows Admin Center

Sie können in Windows Server 2022 natürlich weiterhin Serverrollen über den Server-Manager installieren. Auf der ersten Seite des Assistenten wählen Sie in diesem Fall zunächst aus, ob Sie eine Serverrolle oder die Remotedesktopdienste installieren möchten. Diese werden in Windows Server 2022 über den Assistenten zur Installation von Serverrollen getrennt eingerichtet.

Installationstyp auswählen

ZIELSERVER
 Es sind keine Server ausgewählt.

- Vorbereitung
- Installationstyp
- Serverauswahl
- Serverrollen
- Features
- Bestätigung
- Ergebnisse

Wählen Sie den Installationstyp aus. Sie können Rollen und Features auf einem ausgeführten physischen Computer oder auf einem virtuellen Computer oder auch auf einer virtuellen Festplatte (Virtual Hard Disk, VHD) im Offlinemodus installieren.

- Rollenbasierte oder featurebasierte Installation**
 Konfigurieren Sie einen einzelnen Server, indem Sie Rollen, Rollendienste und Features hinzufügen.
- Installation von Remotedesktopdiensten**
 Bei der Installation waren Rollendienste für die virtuelle Desktopinfrastruktur (Virtual Desktop Infrastructure, VDI) erforderlich, um eine Desktopbereitstellung auf Basis eines virtuellen Computers oder einer Sitzung zu erstellen.

Abb. 4.3 Auswählen des Installationstyps

Haben Sie den Installationstyp ausgewählt, können Sie auf der nächsten Seite des Assistenten den Zielserver auswählen, auf dem Sie die Serverrolle installieren wollen. Sie sehen im Fenster aber nur Server, die Sie im Server-Manager bereits hinzugefügt haben (siehe Kapitel 3). Außerdem müssen die Server gestartet sein. Server, die nicht eingeschaltet sind, blendet der Assistent aus.

Um Server im Server-Manager hinzuzufügen, klicken Sie auf *Verwalten/Server hinzufügen*. Anschließend können Sie im Fenster eine Suche nach den Servern in der Domäne starten und diese im Assistenten hinzufügen. Damit die Server im Assistenten zum Hinzufügen von Rollen angezeigt werden, müssen Sie teilweise etwas warten und den Assistenten dann neu starten. Mehr zu diesem Thema lesen Sie in den Kapiteln 2 und 3.

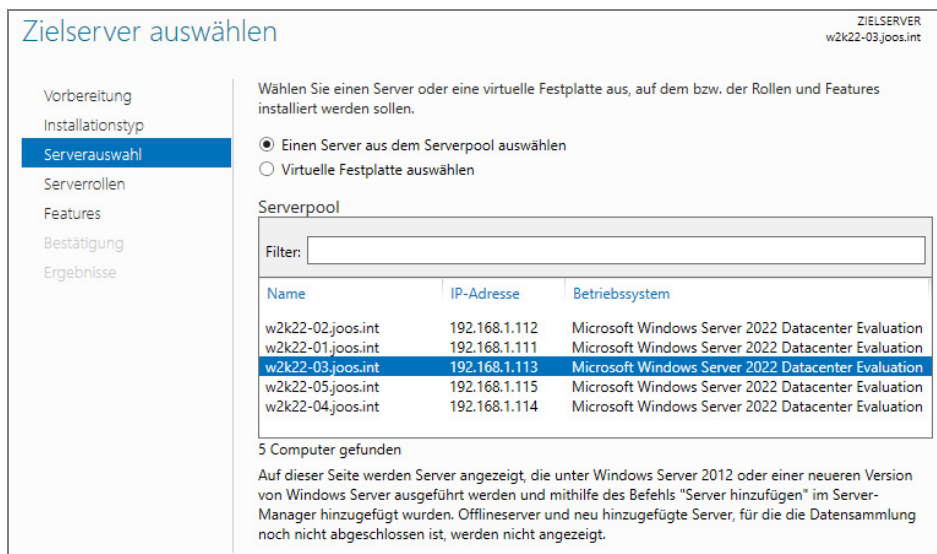


Abb. 4.4 Auswählen des Servers zur Installation von Serverrollen

Starten Sie den Installations-Assistenten für Rollen und Features, scannt er nach Servern, die im lokalen Server-Manager angebonden und online sind. Aus diesen Servern können Sie den Zielserver auswählen, um Rollen und Features zu installieren.

Sie können an dieser Stelle aber nicht nur einen Server auswählen, der gerade online ist, sondern auch virtuelle Festplatten, auf denen Windows Server 2022 installiert ist. Wählen Sie diese Option aus, müssen Sie im unteren Eingabefeld den Speicherort der virtuellen Festplatte angeben. Dabei kann es sich auch um eine Netzwerkfreigabe handeln.

Haben Sie den Server oder die virtuelle Festplatte ausgewählt, auf dem Sie Serverrollen und Features installieren wollen, wählen Sie auf der nächsten Seite aus, welche Rolle Sie installieren wollen.

Wählen Sie eine Rolle zur Installation aus, zeigt der Assistent alle abhängigen Rollendienste und Features an, die durch Auswahl dieser Rolle auf dem Server ebenfalls notwendig sind. Folgende Rollen stehen für Windows Server 2022 zur Verfügung:

- **Active Directory Lightweight Directory Services (AD LDS)** – Mit diesen Diensten können Applikationen arbeiten, die Informationen in einem Ordner speichern. Im Gegensatz zu den Active Directory-Domänendiensten wird der Ordner nicht als Dienst

ausgeführt. Diese Dienste benötigen keinen reinen Domänencontroller. Auf einem Server können mehrere Instanzen laufen. Bei AD LDS handelt es sich sozusagen um ein »Mini«-Active Directory ohne große Verwaltungsfunktionen. AD LDS ist eine Low-End-Variante von Active Directory. Es basiert auf der gleichen Technologie und unterstützt ebenfalls Replikation. Mit AD LDS können LDAP-Ordner für Anwendungen erstellt werden, die wiederum mit Active Directory synchronisiert werden und dieses auch für die Authentifizierung nutzen können. Auf einem Server lassen sich parallel mehrere Instanzen betreiben. Der Dienst ist für Organisationen entwickelt, die eine flexible Unterstützung ordnerfähiger Anwendungen benötigen. Damit können Unternehmen zum Beispiel andere LDAP-Ordner in Testumgebungen installieren, ohne auf Software eines Drittanbieters zurückgreifen zu müssen.

- **Active Directory-Domänendienste (Active Directory Domain Services, AD DS)** – Hierbei handelt es sich um die Rolle eines Domänencontrollers für das Active Directory. Bevor Sie einen Server zum Domänencontroller für das Active Directory heraufstufen können, muss diese Rolle installiert sein. Sie finden diese Rolle in den verschiedenen Kapiteln dieses Buchs wieder. Mehr zu diesem Thema lesen Sie auch in den Kapiteln 10 bis 19.
- **Active Directory-Rechteverwaltungsdienste (Active Directory Rights Management Services, AD RMS)** – Mit dieser Technologie werden Daten mit digitalen Signaturen versehen, um sie vor unerwünschtem Zugriff zu sichern. Besitzer von Dateien können basierend auf Benutzerinformationen exakt festlegen, was andere Benutzer mit den Dateien machen dürfen. Dokumente können mit »Nur Lesen«-Rechten konfiguriert werden. Mehr zu diesem Thema lesen Sie in Kapitel 33.

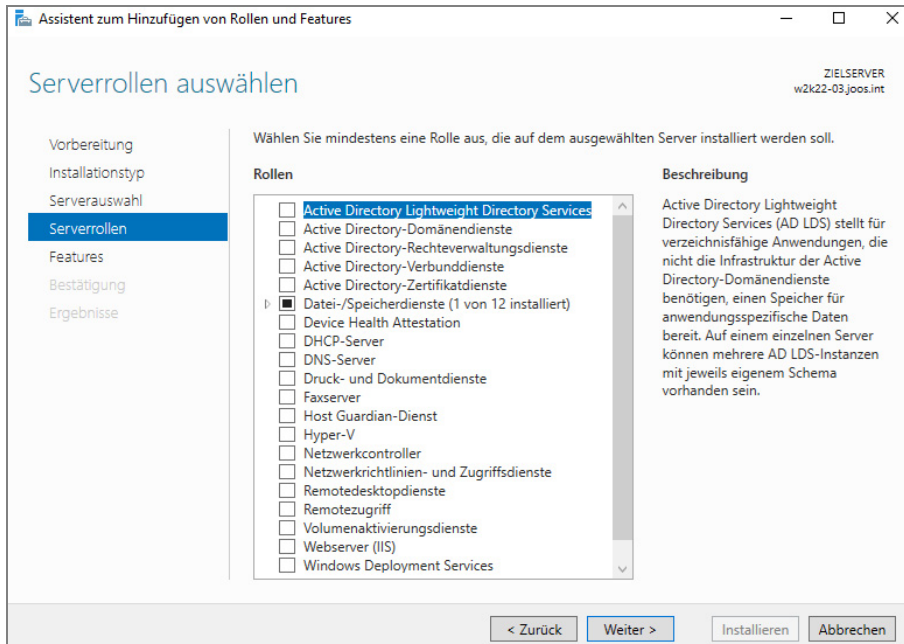


Abb. 4.5 Auswählen der zu installierenden Serverrollen in Windows Server 2022

- **Active Directory-Verbunddienste (Active Directory Federation Services, ADFS)** – Mit den ADFS können Sie eine webbasierte Single Sign-On-(SSO-)Infrastruktur aufbauen. Profitieren sollen hauptsächlich unternehmensinterne Verbände (auch mit mehreren Gesamtstrukturen) sowie Cloudplattformen. Der Identitätsverbund ermöglicht es Unternehmen, die in Active Directory gespeicherten Identitätsinformationen eines Benutzers auf sichere Weise über Verbundvertrauensstellungen gemeinsam zu nutzen, wodurch die Zusammenarbeit erheblich vereinfacht werden soll. Eingesetzt werden die Dienste zum Beispiel, wenn Authentifizierungsdaten zwischen lokalen Installationen und Office 365 oder Microsoft Azure ausgetauscht werden sollen.
- **Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS)** – Diese Rolle installiert eine Zertifizierungsstelle in Windows Server 2022. Viele Serverdienste wie Exchange und SQL benötigen Zertifikate, das gilt auch für Dienste wie DirectAccess. In Active Directory-Gesamtstrukturen sind oft Zertifikate unerlässlich. Aus diesem Grund kann es sich anbieten, diese Serverrolle auf Domänencontrollern mit zu installieren. Auch unter Windows Server 2022 können Sie über einen Browser auf die Zertifizierungsstelle zugreifen. Diese Funktionalität wird allerdings nicht automatisch installiert, sondern muss über den Rollendienst *Zertifizierungsstellen-Webregistrierung* installiert werden. Nach der Installation des Rollendienstes steht die Webseite der Zertifizierungsstelle zur Verfügung. Die Adresse lautet <http://<Servername>/certsrv>. Mehr zu diesem Thema lesen Sie auch in Kapitel 30.
- **Datei- und Speicherdienste** – Installieren Sie diese Rolle, können Sie den Server als Dateiserver verwenden, um Freigaben zu erstellen. Die Dateidienste beinhalten Erweiterungen wie die Dateiklassifizierungsdienste oder Funktionen zur Unterstützung von iSCSI und Speicherpools. Auch BranchCache, Datenduplizierung und der Ressourcen-Manager für Dateiserver (Fileserver Resource Manager, FSRM) gehört zu dieser Serverrolle. Das verteilte Dateisystem (Distributed File System, DFS) installieren Sie als Rollendienst über diese Rolle. Mehr zu diesem Thema lesen Sie in den Kapiteln 5 und 20 bis 22.
- **Device Health Attestion** – Diese Serverrolle ist neu seit Windows Server 2016. Sie bietet Mobile Device Management-Funktionen für Windows 10/11.
- **DHCP-Server** – Diese Rolle beinhaltet die Funktion eines DHCP-Servers für das Netzwerk. Unter Windows Server 2022 kann der DHCP-Server auch IPv6-Adressen verteilen, ist also vollständig DHCPv6-kompatibel. Mehr zu diesem Thema lesen Sie in Kapitel 24.
- **DNS-Server** – Installieren Sie diese Rolle, erhält der Server die Möglichkeit, DNS-Zonen zu verwalten. Das ist zum Beispiel auch für Domänencontroller notwendig, da hier wichtige Daten in DNS gespeichert werden. DNS-Server und -Clients mit Windows Server 2022 bieten auch eine Unterstützung für die Domain Name System-Sicherheits-erweiterungen (Domain Name System Security Extensions, DNSSEC). Sie können DNSSEC-Zonen signieren und hosten, um Sicherheit für die DNS-Infrastruktur bereitzustellen. In Windows Server 2022 sind diese Funktionen direkt in der grafischen Oberfläche integriert. Außerdem unterstützt DNSSEC Active Directory und schreibgeschützte Domänencontroller. Mehr zu diesem Thema lesen Sie in den Kapiteln 25 und 26.
- **Druck- und Dokumentdienste** – Mit dieser Rolle ermöglichen Sie die Verwaltung von mehreren lokal angeschlossenen Druckern an einem Server (Druckserver). Die Drucker können an diesen Server auch per LAN angeschlossen werden. Außerdem können Sie mit dieser Rolle Scanner im Netzwerk bereitstellen. Dokumente lassen sich durch In-

Installation dieser Rolle an SharePoint-Webseiten weiterleiten. Außerdem verwalten Sie mit der Rolle auch andere Druckserver im Netzwerk zentral von einem Server aus. Mehr zu diesem Thema lesen Sie in Kapitel 23.

- **Faxserver** – Diese Server senden und empfangen Faxe. Auch die Verwaltung von Faxressourcen über das Netzwerk wird durch diese Rolle installiert.
- **Host Guardian-Dienst** – Mit dieser neuen Serverrolle ermöglichen Sie die Abschottung einzelner VMs von anderen VMs. Solche VMs werden in Windows Server 2022 auch als »Shielded VMs« bezeichnet und bieten eine besondere Sicherheit.
- **Hyper-V** – Mit dieser Rolle installieren Sie Hyper-V mit den notwendigen Verwaltungsprogrammen auf dem Server. Mehr zu diesem Thema lesen Sie in den Kapiteln 7 bis 9.
- **Netzwerkcontroller** – Der Network Controller-Dienst erlaubt die zentrale Verwaltung, Überwachung und Konfiguration von Netzwerkgeräten. Anbinden lassen sich physische Netzwerkgeräte, aber auch virtuelle Netzwerke sowie Netzwerke in Microsoft Azure. Neben Hardware-Geräten lassen sich softwarebasierte Netzwerkdienste verwalten.
- **Netzwerkrichtlinien- und Zugriffsdienste (Network Policy and Access Services)** – Hierbei handelt es sich um eine Sicherheits-Funktion von Windows Server 2022. Mit dieser Rolle können Sie Benutzern Zugriff auf verschiedene Netzwerksegmente gewähren. Auch wenn Sie einen Server als Router zwischen verschiedenen Netzwerken einsetzen, verwenden Sie diese Rolle.
- **Remotedesktopdienste** – Bei dieser Funktion werden die Remotedesktopdienste im Anwendungsmodus installiert. Mehr zu diesem Thema lesen Sie in Kapitel 28.
- **Remotezugriff** – Sie installieren mit dieser Rolle DirectAccess und normale RAS-Verbindungen gemeinsam. In Windows Server 2022 erfolgt die Konfiguration von RAS und DirectAccess in einer gemeinsamen Oberfläche. Mehr zu diesem Thema lesen Sie in Kapitel 32.
- **Volumenaktivierungsdienste** – Mit dieser Serverrolle installieren Sie einen Schlüsselverwaltungsdienst (Key Management Service, KMS) im Netzwerk. Der Server verwaltet dann zentral die Produktschlüssel für alle Clients, die Sie über KMS aktivieren. In Active Directorys sorgt der Dienst für eine Überwachung und Aktivierung der Rechner.
- **Webserver (IIS)** – Installieren Sie diese Rolle, werden die Internetinformationsdienste (Internet Information Services, IIS) auf dem Server aktiviert. Mehr zu diesem Thema lesen Sie in Kapitel 27.
- **Windows Server Update Services (WSUS)** – Unternehmen, die mehrere Microsoft-Produkte und Clientsysteme im Netzwerk einsetzen, kommen um eine zentrale Verwaltung der Patches kaum herum. Windows Server 2022 bietet dazu, wie bereits der Vorgänger, die Windows Server Update Services. Die grundlegende Funktion hat sich von Windows Server 2008 R2 zu Windows Server 2022 nicht geändert. Mehr zu diesem Thema lesen Sie in Kapitel 37.
- **Windows-Bereitstellungsdienste (Windows Deployment Services, WDS)** – Hiermit können Sie Images von Windows 7/8, Windows 10/11, aber auch Windows Server 2012/2012R2 und Windows Server 2016/2019/2022 im Netzwerk verteilen und die Installation von Servern und Arbeitsstationen automatisieren. Mehr zu diesem Thema lesen Sie in Kapitel 39. WDS wird in Windows Server 2022 als veraltet markiert. Das heißt, in Zukunft wird es diesen Dienst nicht mehr geben. Windows 11 lässt sich nur eingeschränkt mit WDS bereitstellen.

Wenn Sie eine Serverrolle auswählen, erscheint ein Fenster, in dem der Assistent anzeigt, welche Features und Rollendienste noch zusätzlich notwendig sind. In diesem Fenster können Sie zudem festlegen, ob auf dem entsprechenden Server die notwendigen Verwaltungswerkzeuge installiert werden sollen. Das ist nicht auf allen Servern notwendig, wenn Sie zum Beispiel von einem zentralen Server aus verschiedene Server verwalten wollen.

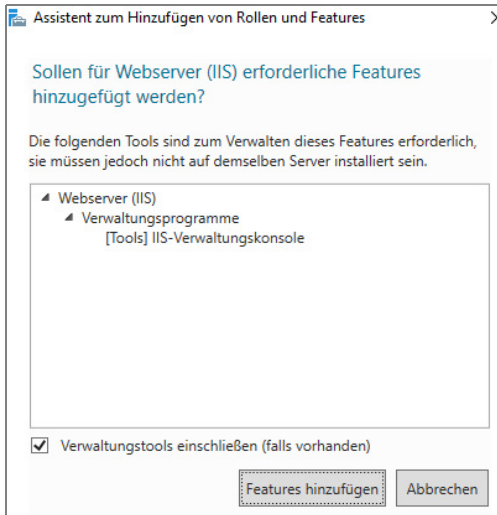


Abb. 4.6 Hinzufügen von notwendigen Features für eine Serverrolle

Sobald Sie eine Serverrolle auswählen, erweitert sich der Assistent automatisch um weitere Seiten, auf denen Sie die entsprechende Rolle bereits während der Installation konfigurieren oder zumindest Hinweise erscheinen, was Sie für den Betrieb der Rolle beachten müssen.

Um den Assistenten abzuschließen, bestätigen Sie die weiteren Fenster. Auf Core-Servern stehen weniger Serverrollen zur Verfügung. Auch diese können Sie über den Server-Manager oder das Windows Admin Center installieren, wenn Sie Core-Server über das Netzwerk angebunden haben. Die wichtigsten Rollen für Core-Server sind:

- Active Directory-Zertifikatdienste (siehe Kapitel 30)
- Active Directory-Domänendienste (siehe die Kapitel 10 bis 19)
- DHCP-Server (siehe Kapitel 24)
- DNS-Server (siehe Kapitel 25)
- Dateidienste (einschließlich Ressourcen-Manager für Dateiserver, siehe Kapitel 20 und 21)
- Active Directory Lightweight Directory Services (AD LDS)
- Hyper-V (siehe Kapitel 7 bis 9)
- Druck- und Dokumentdienste (siehe Kapitel 23)
- Streaming Media-Dienste
- Webserver (einschließlich ASP.NET, siehe Kapitel 27)
- Windows Server Update Services (siehe Kapitel 37)
- Active Directory-Rechteverwaltungsserver (siehe Kapitel 33)
- Routing- und RAS-Server (siehe Kapitel 32)

4.1.2 Features installieren und verwalten

Serverrollen bestimmen den primären Verwendungszweck eines Servers. Mit den Rollendiensten im Server-Manager werden untergeordnete Funktionen zu Rollen hinzugefügt. Features erweitern unabhängig von Serverrollen das Betriebssystem um zusätzliche Möglichkeiten.

Verwechseln Sie Features/Funktionen nicht mit Rollendiensten. Features sind einzelne Funktionen, die einen Server erweitern. Auch sie werden über den Server-Manager installiert, indem Sie den gleichen Assistenten wie bei der Installation von Serverrollen verwenden. Im Windows Admin Center sind die Features unterhalb der Rollen bei *Rollen und Funktionen* angeordnet.

Wählen Sie über *Verwalten/Rollen und Features hinzufügen* auf der Seite *Features auswählen* die neuen Features aus, die Sie installieren wollen. Im folgenden Abschnitt zeigen wir Ihnen, welche Features in Windows Server 2022 zur Verfügung stehen:

- **.NET Framework 3.5-Funktionen** – Dieses Feature erweitert den Server um die Funktionen von .NET Framework 3.5. und 2.0. Viele Anwendungen benötigen noch die älteren Versionen von .NET Framework.
- **.NET Framework 4.8-Features** – Neu in Windows Server 2022 ist das Feature zur Installation von .NET Framework 4.8 für neue Anwendungen, die für Windows Server und Windows 10/11 optimiert sind.
- **BitLocker-Laufwerkverschlüsselung** – BitLocker bietet eine Verschlüsselung für lokale Festplatten und im Gegensatz zum verschlüsselten Dateisystem (Encrypting File System, EFS) auch Schutz vor Diebstahl oder dem Ausbau des Datenträgers. Server in Niederlassungen lassen sich mit BitLocker besser verschlüsseln. BitLocker unterstützt auch Hardwareverschlüsselungstechnologien von Festplatten und eine inkrementelle Verschlüsselung. Bei Aktivierung verschlüsselt das System nur verwendete Bereiche der Festplatte und erweitert die Verschlüsselung, wenn neue Daten auf der Festplatte gespeichert werden. Mehr zu diesem Thema lesen Sie in Kapitel 5.
- **BitLocker-Netzwerkentsperrung** – BitLocker-Netzwerkentsperrung kann verschlüsselte Domänencomputer zentral entsperren. Das ist zum Beispiel sinnvoll, wenn Computer im Netzwerk gewartet werden sollen und neu starten müssen. Mit der zentralen Entsperrung optimieren Sie diesen Vorgang.
- **BranchCache** – Durch die Aktivierung von BranchCache als Feature kann ein Server als Client für BranchCache dienen. Um BranchCache als Server einzusetzen, müssen Sie noch den Rollendienst für BranchCache aus der Serverrolle der Dateidienste installieren. BranchCache bietet eine Zwischenspeicherung von Dateien für den schnelleren Zugriff von Windows 7/8- und Windows 10/11-Computern in Niederlassungen. Mehr zu diesem Thema lesen Sie in Kapitel 33.
- **Client für NFS** – Mit dem Client für NFS lassen sich Server mit UNIX-NFS-Freigaben verbinden.
- **Container** – Mit diesem Feature installieren Sie die Docker-Container-Technologien auf Servern mit Windows Server 2022.

- **Data Center Bridging** – Mit dieser Funktion erweitern Sie den Server, um den Datenverkehr in großen Netzwerken steuern zu können. Unterstützt der Netzwerkadapter die Funktion Converged Network Adapter (CNA), lassen sich Daten wie iSCSI oder RDMA besser nutzen (siehe Kapitel 1). Außerdem lassen sich Bandbreiten für die verschiedenen Funktionen festlegen.
- **DirectPlay** – Mit diesem neuen Feature integrieren Sie DirectPlay als Komponente auf einem Server. Bei diesem Protokoll können verschiedene Transport- und Übertragungsaufgaben zwischen Servern realisiert werden. Das Feature ergibt vor allem auf Remote-desktop-Servern Sinn.
- **E/A-QoS** – Definieren von Bandbreitengrenzwerten für Anwendungen auf dem Server.
- **Einfache TCP/IP-Dienste** – Installieren Sie diese Funktionen, werden auf dem Server noch einige zusätzliche Dienste für TCP/IP aktiviert. Sie sollten diese Dienste nur dann installieren, wenn sie von einer speziellen Applikation benötigt werden. Folgende Funktionen sind in den einfachen TCP/IP-Diensten enthalten: Der *Zeichengenerator (CHARGEN)* sendet Daten, die sich aus einer Folge von 95 druckbaren ASCII-Zeichen zusammensetzen. Dieses Protokoll wird als Debuggingtool zum Testen oder zur Problembearbeitung bei Zeilendruckern verwendet. *Daytime* zeigt Meldungen mit Wochentag, Monat, Tag, Jahr, aktueller Uhrzeit (im Format HH:MM:SS) und Informationen zur Zeitzone an. Einige Programme können die Ausgabe dieses Dienstes zum Debuggen oder Überwachen von Abweichungen der Systemuhr oder auf einem anderen Host verwenden. *Discard* verwirft alle über diesen Anschluss empfangenen Meldungen, ohne dass eine Antwort oder Bestätigung gesendet wird. Die Funktion kann als Nullanschluss für den Empfang und die Weiterleitung von TCP/IP-Testnachrichten während der Netzwerkinstallation und -konfiguration verwendet werden. *Echo* erzeugt Echorückmeldungen zu allen über diesen Serveranschluss empfangenen Nachrichten. Der *Echo*-Befehl kann als Debugging- und Überwachungstool in Netzwerken eingesetzt werden. Das *Zitat des Tages (QUOTE)* gibt ein Zitat in Form eines ein- oder mehrzeiligen Texts in einer Meldung zurück. Die Zitate werden nach dem Zufallsprinzip aus der folgenden Datei ausgewählt: `C:\Windows\System32\Drivers\Etc\Quotes`. Eine Beispieldatei mit Zitaten wird mit den einfachen TCP/IP-Diensten installiert. Wenn diese Datei fehlt, kann der Zitatdienst nicht ausgeführt werden.
- **Erweitertes Speichern** – Mit dieser Funktion können Sie die Zusammenarbeit von Windows Server 2022 mit externen Speichergeräten verbessern, indem die beteiligten Komponenten Berechtigungen austauschen.
- **Failoverclustering** – Mit dieser Funktion installieren Sie die Clusterfunktionalität von Windows Server 2022. Wie andere frühere Enterprise-Funktionen steht auch das Clustering in Windows Server 2022 in der Standard-Edition zur Verfügung. Mehr zu diesem Thema lesen Sie in Kapitel 9.
- **Gruppenrichtlinienverwaltung** – Mit dieser Funktion installieren Sie die Gruppenrichtlinienverwaltungskonsole (Group Policy Management Console, GPMC), mit der Sie die Gruppenrichtlinien in Active Directory verwalten können. Auf Domänencontrollern wird das Feature automatisch installiert. Mehr zu diesem Thema lesen Sie in Kapitel 19.
- **Hostfähiger Webkern für Internetinformationsdienste** – Dieses Feature ermöglicht Serveranwendungen, eigene Konfigurationsdateien für den IIS zu verwenden, die sich von den anderen Konfigurationsdateien unterscheiden. Arbeitsordner in Windows Server 2022 und Windows 10/11 nutzen zum Beispiel diese Funktion.

- **Hyper-V-Unterstützung durch Host Guardian** – Installiert notwendige Funktionen, um den Hyper-V-Host an den Host Guardian Service anzubinden, mit dem wiederum VMs verschlüsselt werden können.
- **IIS-Erweiterung für OData Services for Management** – Mit dieser Funktion stellen Sie PowerShell-Cmdlets für einen Webdienst zur Verfügung. Mehr zu diesem Thema lesen Sie in Kapitel 27.
- **Intelligenter Hintergrundübertragungsdienst** – Bei dieser Technologie kann ein Server im Hintergrund Daten empfangen, ohne die Bandbreite im Vordergrund zu beeinträchtigen. Ein Server kann dadurch – zum Beispiel bei installiertem WSUS – Patches aus dem Internet herunterladen. Dazu wird nur so viel Bandbreite verwendet, wie derzeit bei dem Server ungenutzt ist. Andere Netzwerkanwendungen können so auf einem Server weiterhin auf die volle Netzwerkperformance zugreifen.
- **Interne Windows-Datenbank** – Hierbei handelt es sich um eine kostenlose relationale Datenbank, die einige Serverdienste nutzen. Die Datenbank kann allerdings nicht von Drittherstellerprodukten verwendet werden, sondern nur von den Funktionen und Rollen in Windows Server 2022.
- **Internetdruckclient** – Mit diesem Feature können Sie über das HTTP-Protokoll auf die Drucker des Servers zugreifen. Dadurch wird Anwendern ermöglicht, über das Internet auf die Drucker zuzugreifen. Diese Funktion ist zum Beispiel für mobile Mitarbeiter sinnvoll, die Dokumente von unterwegs in der Firma ausdrucken wollen, wie Ausdrucke für Aufträge oder Ähnliches.
- **IP-Adressenverwaltungsserver (IPAM-Server)** – Die Serverlösung hat die Aufgabe, Infrastrukturserver, die die IP-Adressen im Netzwerk verwalten, in einer gemeinsamen Oberfläche zusammenzuführen und zentral zu verwalten und zu überwachen. Natürlich gibt es weiterhin Verwaltungskonsolen für DHCP und DNS. Zwar lassen sich viele Einstellungen von DHCP auch in der IPAM-Konsole vornehmen, aber für erweiterte Aufgaben wie Ausfallsicherheit von DHCP-Servern ist weiterhin die DHCP-Konsole notwendig. IPAM dient nicht nur der Überwachung von DNS- und DHCP-Servern, sondern bietet auch eine effiziente Verwaltungsmöglichkeit dieser Server, und zwar in einer gemeinsamen Oberfläche. Microsoft geht mit der neuen Serverrolle auf die ständig wachsende Anzahl an DNS- und DHCP-Servern in Unternehmen und der damit verbundenen komplizierteren Verwaltung ein. Damit Administratoren einen Überblick über die verschiedenen IP-Adressbereiche und DNS-Domänen erhalten, sind oft Zusatztools im Einsatz oder Excel-Tabellen, in denen die Daten aufgelistet sind. Damit soll IPAM Schluss machen. IPAM verfügt generell über folgende Funktionen: Automatisches Auffinden der IP-Adresse-Infrastruktur im Unternehmen, Erstellen von Berichten für IP-Infrastruktur, Überwachung der Infrastruktur-Server im Netzwerk und der vorhandenen IP-Adressen, Überwachung von Netzwerkzugriffsschutz-Servern, Überwachung von Domänencontrollern. Mehr zu diesem Thema lesen Sie in Kapitel 24.
- **LPR-Portmonitor** – Windows-Betriebssysteme unterscheiden zwischen lokalen und Netzwerkdruckern. Für andere Druckprotokolle, also auch für das LPR-Druckprotokoll, werden die Verbindungen zu Druckern über sogenannte Ports (Anschlüsse) abgewickelt. Sie ergänzen die standardmäßig vorhandenen lokalen Ports. Die Druckerports für das LPR-Protokoll werden LPR-Ports genannt. Jeder LPR-Port verweist auf eine Queue eines Remotedruckerservers. LPR-Ports werden also unter Windows-Betriebssys-

temen wie lokale Anschlüsse behandelt. Deshalb werden auch Drucker, die über das LPR-Protokoll angesprochen werden, als lokale Drucker angesehen. Mehr zu diesem Thema lesen Sie in Kapitel 23.

- **Media Foundation** – Dieses Feature bietet die Möglichkeit, dass Anwendungen Miniaturansichten für Mediendateien zur Verfügung stellen können. Das Tool arbeitet mit der Desktopdarstellung zusammen und ist auf Remotedesktopservern sinnvoll.
- **Message Queuing** – Mit dieser Funktion können Nachrichten gesichert und überwacht zwischen Applikationen auf dem Server ausgetauscht werden. Nachrichten können priorisiert werden und es gibt eine Vielzahl an Möglichkeiten, um die Konfiguration anzupassen. Message Queuing (auch als *MSMQ* bezeichnet) ist sowohl eine Kommunikationsinfrastruktur als auch ein Entwicklungswerkzeug. Für Systemadministratoren als auch für Softwareentwickler bietet Message Queuing Möglichkeiten wie Installation und Verwaltung der Infrastruktur, Entwicklung von Nachrichtenanwendungen und vieles mehr.
- **Microsoft Defender Antivirus** – Standardvirens scanner von Microsoft, der auch in Windows Server 2022 installiert ist.
- **Multipfad-E/A** – Durch Multipfad wird die Verfügbarkeit erhöht, weil mehrere Pfade (Pfad-Failover) von einem Server oder Cluster zu einem Speichersubsystem zugelassen werden. Unterstützt ein Server im SAN die Funktion Microsoft Multipfad-E/A (Multipath I/O, MPIO), können Sie mehr als einen Pfad zum Lesen und Schreiben für eine LUN (Logical Unit Number, logische Gerätenummer) aktivieren, indem Sie auf diesem Server mehrere Fibrechannel-Ports oder iSCSI-Adapter derselben LUN zuweisen. Dies gilt auch für das Zugreifen auf die LUN von einem Cluster. Stellen Sie zum Vermeiden von Datenverlust vor dem Aktivieren von Zugriff über mehrere Pfade sicher, dass der Server oder Cluster die Funktion Multipfad-E/A unterstützt.
- **MultiPoint Connector** – Dieses neue Serverfeature arbeitet mit den MultiPoint-Services zusammen. Mit den Funktionen lassen sich zum Beispiel MultiPoint-Server im Netzwerk verwalten.
- **Netzwerklastenausgleich** – Mit dieser Funktion können Sie einen Lastenausgleich zwischen mehreren Servern im Netzwerk bereitstellen. Zu den Anwendungen, die vom Netzwerklastenausgleich profitieren können, zählen IIS, Remotedesktopserver sowie virtuelle private Netzwerke, Windows Media-Dienste und viele Server mehr. Mithilfe des Netzwerklastenausgleichs können Sie außerdem die Serverleistung skalieren, sodass der Server mit den steigenden Anforderungen der Internetclients Schritt halten kann. Ausgefallene oder offline geschaltete Computer werden automatisch erkannt und wiederhergestellt. Die Netzwerklast wird nach dem Hinzufügen oder Entfernen von Hosts automatisch umverteilt. Mehr zu diesem Thema lesen Sie in Kapitel 34.
- **Netzwerkvirtualisierung** – Bietet die Möglichkeit, mehrere virtuelle Netzwerke in einem physischen Netzwerk zu betreiben. Das Feature ist vor allem für Netzwerke mit Software Defined Networking interessant, in denen Windows-Server integriert werden sollen.
- **Peer Name Resolution-Protokoll** – PNRP ermöglicht die verteilte Auflösung eines Namens in eine IPv6-Adresse und Portnummer. Einfach betrachtet ist PNRP eine P2P-Anwendung, die die Form eines Windows-Dienstes annimmt. PNRP baut auf IPv6 auf.

- **RAS-Verbindungs-Manager-Verwaltungskit** – Mit dem Toolkit erstellen Sie ausführbare Dateien, die auf Clientcomputern Einstellungen für RAS-Verbindungen und Direct Access automatisieren.
- **Remotedifferenzialkomprimierung** – Dieses Feature ermöglicht die verbesserte Übertragung von geänderten Daten in schmalbandigen Netzwerken. Ist zum Beispiel ein Server über ein langsames WAN angebunden, erkennt dieses Feature, wenn Änderungen an Dateien vorgenommen wurden, und kopiert nur die geänderten Daten über das Netzwerk, nicht die komplette Datei. Diese Funktion wird zum Beispiel von DFS (Distributed File System, verteiltes Dateisystem) verwendet.
- **Remoteserver-Verwaltungstools** – Diese Funktion wird auf normal installierten Servern automatisch installiert. Sie können mit diesen Tools die Funktionen über das Netzwerk auf einem Windows Server 2022 verwalten. Mehr zu diesem Thema lesen Sie in Kapitel 3.
- **Remoteunterstützung** – Installieren Sie diese Funktion, können Sie an Kollegen eine Remoteunterstützungsanforderung schicken, damit sich diese per Remotedesktop auf den Server verbinden können. Diese Funktion wird normalerweise eher für Arbeitsstationen verwendet als auf Servern. Es spielt keine Rolle, ob die Verbindung mit dem entfernten Rechner über das Netzwerk, Internet oder via Modem per Telefonleitung erfolgt. Auf Remotedesktopservern kann die Funktion durchaus sinnvoll sein.
- **RPC-über-HTTP-Proxy** – Mit dieser Funktion werden Remoteprozeduraufrufe (Remote Procedure Call, RPC) in HTTP-Pakete gekapselt. Die Remotedesktopgateway-Rolle baut ebenfalls auf diese Funktion auf.
- **Sammlung von Setup- und Startereignissen** – Dieses Feature kann Setup-Protokolldateien und andere Logdateien im Netzwerk auslesen und erfassen.
- **Simple TCP/IP Services** – Installiert die einfachen TCP/IP-Dienste in Windows Server 2022. Das Feature wird aber nur für die Rückwärtskompatibilität benötigt.
- **SMB 1.0/CIFS File Sharing Support** – Installiert die Unterstützung für SMB 1.0, ebenfalls für die Rückwärtskompatibilität.
- **SMB-Bandbreitengrenzwert** – Hier steuern Sie die Bandbreite, die Servern und Computern über das SMB-Protokoll im Netzwerk zur Verfügung stehen.
- **SMTP-Server** – Über diese Funktion installieren Sie einen Mailserver auf dem Server.
- **SNMP-Dienst** – Das Simple Network Management-Protokoll (SNMP) ist ein Standard, mit dem SNMP-fähige Applikationen, hauptsächlich Überwachungsprogramme für Server, Informationen von einem Server abfragen können. Hierbei handelt es sich um einen optionalen Dienst, der im Anschluss an eine erfolgreiche Konfiguration des TCP/IP-Protokolls installiert werden kann. Der SNMP-Dienst stellt einen SNMP-Agenten bereit, der eine zentrale Remoteverwaltung von Computern ermöglicht. Wenn Sie auf die vom SNMP-Agent-Dienst bereitgestellten Informationen zugreifen möchten, benötigen Sie eine Softwareanwendung des SNMP-Verwaltungssystems. Der SNMP-Dienst unterstützt zwar SNMP-Verwaltungssoftware, diese ist jedoch derzeit noch nicht im Lieferumfang enthalten.
- **Software Load Balancer** – Bietet Lastenausgleich für Netzwerkressourcen.
- **Speicherreplikation** – Ermöglicht die Replikation kompletter Datenträger auf andere Server oder Rechenzentren.

- **Standardisierte Windows-Speicherverwaltung** – Mit dem Feature lassen sich Hardwarespeichergeräte, die SMI-S unterstützen, an Windows Server 2022 anbinden und über Windows-Tools verwalten. Es stehen auch Befehle über WMI und der PowerShell zur Verfügung.
- **Storage Migration Service** – Ermöglicht die Migration von älteren Dateiservern zu Windows Server 2022 oder Microsoft Azure. Bei der Migration lassen sich Daten, Berechtigungen und Freigaben über einen Assistenten migrieren.
- **Storage Migration Service Proxy** – Stellt den Dienst zur Verfügung, mit dem Server über Storage Migration Service verbunden und Daten migrieren können.
- **Systemdaten** – Installiert Windows Server System Insights (siehe Kapitel 3).
- **Systemdatenarchivierung** – Arbeitet mit Windows Server System Insights aus dem Windows Admin Center zusammen (siehe Kapitel 3).
- **Telnet-Client** – Mit dem Telnet-Client können Sie sich per Telnet auf einen anderen Server verbinden. Standardmäßig ist dieser Client unter Windows Server 2022 nicht installiert.
- **TFTP-Client** – Bei dieser Funktion handelt es sich um einen eingeschränkten FTP-Client, der hauptsächlich für die Updates von Firmware oder das Übertragen von Informationen zu Systemen gedacht ist, auf denen ein TFTP-Server läuft.

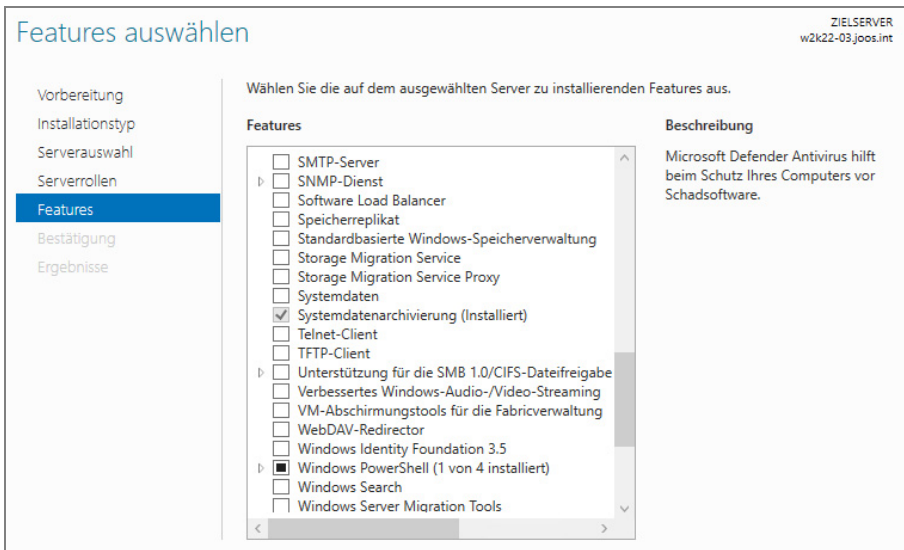


Abb. 4.7 Installieren von Features/Funktionen über den Server-Manager

- **Unterstützung für das SMB 1.0/CIFS-Protokoll** – Nach Aktivierung steht SMB 1 auch in Windows Server 2022 zur Verfügung.
- **Verbessertes Windows-Audio-/Video-Streaming** – Diese Funktion ist für die Verteilung von Audio- oder Videostreams in Netzwerken vorgesehen. Mit dieser Funktion können Streams auch überwacht und konfiguriert werden.
- **VM-Abschirmungstools für die Fabricverwaltung** – Dieses Feature wird zusammen mit dem Host Guardian-Dienst eingesetzt, um Shield-VMs (abgeschottete VMs) zu erstellen und zu verwalten.

- **WebDAV-Redirector** – Ermöglicht die Verbindung eines Servers mit WebDAV-Freigaben im Internet, um mit dem Explorer auf Dateien im Internet oder in Cloud-Speichern zugreifen zu können.
- **Windows Identity Foundation 3.5** – Ermöglicht, einige .NET Framework 4.5-Funktionen auch für .NET Framework 3.5 und 4 zu nutzen. Allerdings ist das nur sinnvoll, wenn die entsprechende Serveranwendung kein .NET Framework 4.5 unterstützt.
- **Windows PowerShell** – Hierbei handelt es sich um die neue PowerShell und zusätzliche Werkzeuge für die PowerShell. Sie können an dieser Stelle noch die Unterstützung der PowerShell 2.0 aktivieren und PowerShell Web Access. Installieren Sie das Feature *PowerShell Web Access* über den Server-Manager oder die PowerShell, kann auf die PowerShell über einen Webbrowser zugegriffen werden. So können Verwaltungsaufgaben auf einem Server auch von Tablet-PCs oder nicht kompatiblen Systemen durchgeführt werden. Mehr zu diesem Thema lesen Sie auch in Kapitel 40.
- **Windows Search** – Mit diesem Feature installieren Sie die Funktionen der Windows-Suche auf dem Server. Die Funktion ist für kleinere Dateiserver geeignet oder Remote-Desktopservern, auf denen indexierte Dateien für die Anwender zur Verfügung stehen müssen, damit diese nach Dateien und Inhalten suchen können.
- **Windows Server-Migrationstools** – Die Migrationstools unterstützen bei der Migration älterer Server zu Windows Server 2022. Zum Migrieren von Rollen, Features und Daten über die Windows Server-Migrationstools müssen Sie die Tools auch auf den Quellservern installieren, von denen Sie Daten migrieren wollen. Die Tools sind vor allem bei der Migration wertvoll, da keine Zusatzwerkzeuge lizenziert werden müssen.
- **Windows Server-Sicherung** – Das standardmäßige Datensicherungsprogramm von Windows Server wird nicht mehr automatisch installiert, sondern muss manuell nachinstalliert werden. Das Programm wurde für Windows Server 2022 überarbeitet. Die Sicherung unterstützt jetzt besser die Schattenkopien sowie die integrierten Sicherungsfunktionen von SQL-Server und Exchange. Die Verwaltung der Sicherung findet über die MMC oder die Eingabeaufforderung statt. So können Sie auch über das Netzwerk mit der MMC die Datensicherung von mehreren Servern verwalten. Mehr zu diesem Thema lesen Sie in Kapitel 35.
- **Windows Subsystem für Linux** – Die Möglichkeit, Linux-Distributionen auf Windows zu installieren und damit Linux-Tools auch in Windows einzusetzen.
- **Windows-TIFF-IFilter** – Dieses Feature benötigen Sie für die OCR-Erkennung von eingescannten Dokumenten im Zusammenspiel mit der verbesserten Suche und der Indexierung. Eingescannte Dokumente lassen sich so automatisch indexieren und über Windows Search (Rollendienst der Dateidienste) besser durchsuchen.
- **Windows-Biometrieframework** – Bietet die Unterstützung von Geräten zum Erfassen von Biometriedaten in Windows-Netzwerken, zum Beispiel Fingerabdruckscanner.
- **Windows-Prozessaktivierungsdienst** – Bei der Installation der IIS in Windows Server 2022 fordert Windows als Grundlage die Installation des Windows-Prozessaktivierungsdienstes (Windows Process Activation Service, WPAS). WPAS ist der Systembaustein, der für die IIS die Anwendungspools und Prozesse verwaltet.
- **Windows-Tiff-Filter** – Möglichkeit, mit OCR gescannte Dokumente zu verarbeiten.
- **WinRM-IIS-Erweiterung** – Hierbei handelt es sich um die IIS-Erweiterung zur Remoteverwaltung der Dienste im Netzwerk.