

O'REILLY®

Thomas Joos

Microsoft  
Windows  
Server 2022

Von der Planung und Migration bis zur  
Konfiguration und Verwaltung

DAS HANDBUCH



# Inhalt

**Cover**

**Über den Autor**

**Titel**

**Impressum**

**Inhaltsverzeichnis**

**Vorwort**

**Teil I Grundlagen und Installation**

Kapitel 1 Neuerungen und Lizenzierung

1.1 Die wichtigsten Neuerungen in Windows Server 2022

1.1.1 Neuerungen in Windows Server 2022

1.1.2 Secured-Core-Server mit Windows Server 2022

1.1.3 Neues Container-Image für Windows Server 2022

1.2 Windows Server 2022 lizenzieren

1.2.1 Editionen und Lizenzen im Vergleich

1.2.2 Clientzugriffslizenzen beachten

1.2.3 Geräte-CALs und Benutzer-CALs

1.3 Windows Server 2022 für kleine Unternehmen

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

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

1.3.3 Schneller Wechsel zu Windows Server 2022 Standard/Datacenter möglich

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

1.3.5 Zu Windows Server 2022 Essentials migrieren

1.4 Windows 11 und Windows Server 2022

1.4.1 Zu Windows 11 aktualisieren und Systemvoraussetzungen beachten

1.4.2 Weniger Updates pro Jahr mit Windows 11

1.4.3 Neuerungen in Windows 11

1.4.4 Windows 11 und Microsoft 365

1.5 Zusammenfassung

Kapitel 2 Installation und Grundeinrichtung

2.1 Grundlagen zur Installation

2.1.1 Windows Server 2022-Installation verstehen

2.1.2 Installation von Windows Server 2022 vorbereiten

2.2 Windows Server 2022 neu installieren

2.2.1 Windows Server 2022-Installation durchführen

2.2.2 USB-Stick für Windows Server 2022 erstellen

2.3 Zu Windows Server 2022 aktualisieren

2.3.1 Aktualisierung zu Windows Server 2022 durchführen

2.3.2 Upgrade von Standard- und Testversion auf Datacenter-Edition

2.4 Nacharbeiten zur Installation von Windows Server 2022

2.4.1 Windows Server 2022 aktivieren

2.4.2 Treiberinstallation überprüfen

2.4.3 Netzwerkverbindung testen

2.4.4 Windows Update aktivieren

2.4.5 Sprachpakete installieren

2.4.6 Media Player deaktivieren

2.4.7 Computernamen und Domänenmitgliedschaft festlegen

2.4.8 Aktivieren von Remotedesktop

2.4.9 WLAN-Anbindung von Windows Server 2022

2.4.10 Boot-Manager reparieren

2.5 Zusammenfassung

Kapitel 3 Erste Schritte mit Windows Server 2022

3.1 Erste Schritte nach der Installation

- 3.1.1 Windows Server 2022 mit Windows 10/11 verwalten
    - 3.2 Core-Server verwalten
      - 3.2.1 Hardware und Treiber auf Core-Servern installieren
      - 3.2.2 Windows Updates auf Core-Servern steuern
        - 3.3 Erweiterte Startoptionen nutzen
          - 3.3.1 Starten der automatischen Reparatur von Windows Server 2022
          - 3.3.2 Windows Server 2022 im abgesicherten Modus starten
          - 3.3.3 Abgesicherter Modus über msconfig.exe
          - 3.3.4 Abgesicherter Modus in das Bootmenü einbinden
          - 3.3.5 Abgesicherter Modus über automatische Reparatur starten
            - 3.4 Remote-Management aktivieren
            - 3.5 Windows Admin Center in der Praxis
              - 3.5.1 Admin Center Gateway installieren und aktualisieren
              - 3.5.2 Verbindungsaufbau zu Servern herstellen
              - 3.5.3 Fehler bei der Verbindung beheben
              - 3.5.4 Server im Windows Admin Center verwalten
              - 3.5.5 Mit Markierungen arbeiten und Objekte suchen
              - 3.5.6 Datei-Explorer, Registry-Editor, PowerShell und Remotedesktop nutzen
              - 3.5.7 Gatewayzugriff steuern
              - 3.5.8 Zertifikat für das Windows Admin Center steuern
              - 3.5.9 Erweiterungen für das Windows Admin Center
              - 3.5.10 Windows Admin Center und Microsoft Azure
              - 3.5.11 Windows Server 2022 mit Windows Admin Center überwachen
              - 3.5.12 Performance Monitor im Windows Admin Center
              - 3.5.13 Hyper-V mit dem Windows Admin Center verwalten
  - 3.6 Zusammenfassung
- Kapitel 4 Serverrollen und Features installieren und einrichten
- 4.1 Installieren von Serverrollen und Features auf einem Server

- 4.1.1 Rollen installieren
- 4.1.2 Features installieren und verwalten
- 4.1.3 Installation von Rollen und Features abschließen
  - 4.2 Rollen in der PowerShell installieren
  - 4.2.1 Serverrollen und Features in der PowerShell verwalten
  - 4.2.2 Unbeaufsichtigte Installation von Rollen und Features
    - 4.3 Rollen und Features mit DISM installieren
    - 4.3.1 Webserver mit Dism.exe remote verwalten und Serverrollen auf Core-Servern installieren
      - 4.4 Serverrollen mit dem Best Practices Analyzer überprüfen
      - 4.4.1 Überprüfen von Servern über das Netzwerk
      - 4.4.2 BPA in der PowerShell starten
      - 4.4.3 Ergebnisse exportieren
      - 4.4.4 BPA für Hyper-V nutzen
      - 4.4.5 BPA auswerten
      - 4.5 Zusammenfassung

## **Teil II Einrichtung des Servers**

### Kapitel 5 Datenträger und Speicherpools verwalten

- 5.1 Wichtige Funktionen im Storage-Bereich
  - 5.1.1 Storage Spaces Direct und Storage Replica
  - 5.1.2 Datenduplizierung erweitert
  - 5.1.3 ReFS und Speicherpools
    - 5.2 Datenträger erstellen und anpassen
    - 5.2.1 Einrichten von Datenträgern
    - 5.2.2 Konfigurieren von Laufwerken
    - 5.2.3 Komprimieren von Datenträgern und Ordnern
    - 5.2.4 Festplattenverwaltung in der PowerShell und Eingabeaufforderung
    - 5.2.5 Mit GPT-Partitionen und ReFS arbeiten

- 5.2.6 Verkleinern und Erweitern von Datenträgern
- 5.2.7 Software-RAIDs in Windows Server nutzen
  - 5.3 Verwalten von Datenträgern
    - 5.3.1 Defragmentierung verwalten
    - 5.3.2 Hardware und Richtlinie von Datenträgern verwalten
      - 5.4 BitLocker-Laufwerkverschlüsselung
        - 5.4.1 Grundlagen zu BitLocker und Trusted Platform Module (TPM)
        - 5.4.2 BitLocker schnell und einfach aktivieren
        - 5.4.3 Troubleshooting für BitLocker
        - 5.4.4 Verschlüsselndes Dateisystem (EFS) – Daten einfach absichern
      - 5.5 Speicherpools einsetzen
        - 5.5.1 Speicherpools erstellen
        - 5.5.2 Speicherplätze in Speicherpools erstellen
        - 5.5.3 Volumes auf virtuellen Datenträgern in Speicherpools erstellen
        - 5.5.4 Speicherpools verwalten und physische Festplatten hinzufügen
        - 5.5.5 Virtuelle und physische Datenträger verwalten, trennen und löschen
        - 5.5.6 Speicherpools und virtuelle Festplatten mit PowerShell verwalten
        - 5.5.7 Erstellen eines Storage Spaces mit SSD-/NVMe-Festplatten
    - 5.6 Verwenden von Schattenkopien
    - 5.7 Erstellen und Verwalten von virtuellen Festplatten
      - 5.7.1 Virtuelle Festplatten in der Datenträgerverwaltung erstellen
      - 5.7.2 VHD(X)-Festplatten konvertieren und in der PowerShell verwalten
      - 5.7.3 VHD-Dateien in den Boot-Manager einbinden
      - 5.7.4 iSCSI-Ziele über virtuelle Festplatten zur Verfügung stellen
      - 5.7.5 iSCSI-Ziele sicher zur Verfügung stellen
      - 5.7.6 iSCSI-Festplatten verbinden
    - 5.8 Datendeduplizierung einrichten
      - 5.8.1 Einstieg in die Deduplizierung

## 5.8.2 Dateneduplizierung im Server-Manager

### 5.9 Speicher-Replikation – Daten in Netzwerken replizieren

#### 5.9.1 Storage Replica verstehen

#### 5.9.2 Ablauf der Replikation

#### 5.9.3 Storage Replica in der Praxis

#### 5.9.4 Storage Replica auf alleinstehenden Servern in der PowerShell steuern

#### 5.9.5 Storage Spaces Direct und Storage Replica

### 5.10 Zusammenfassung

## Kapitel 6 Windows Server 2022 im Netzwerk betreiben

### 6.1 Grundlagen zur Netzwerkanbindung

#### 6.1.1 Installation der Netzwerkhardware

#### 6.1.2 Anbindung des Computers an das Netzwerk

#### 6.1.3 Erweiterte Verwaltung der Netzwerkverbindungen

#### 6.1.4 Eigenschaften von Netzwerkverbindungen und ihre erweiterte Verwaltung

#### 6.1.5 DNS über HTTPS – DoH

### 6.2 Netzwerkkarten zusammenfassen – NIC-Teaming

#### 6.2.1 NIC-Team erstellen

#### 6.2.2 NIC-Teams auf Core-Server und in der PowerShell

#### 6.2.3 NIC-Teams testen und konfigurieren

#### 6.2.4 Eigenschaften von TCP/IP und DHCP

### 6.3 Erweiterte Netzwerkeinstellungen – Routing und IPv6

#### 6.3.1 IP-Routing unter Windows Server 2022

#### 6.3.2 Routen verfolgen in der Eingabeaufforderung – Pathping und Tracert

#### 6.3.3 Internetprotokoll Version 6 – IPv6

### 6.4 Mit der PowerShell Netzwerkprobleme lösen

#### 6.4.1 Get-NetIPAddress und Get-NetIPConfiguration

#### 6.4.2 Test-NetConnection: Routen nachverfolgen und Verbindungen überprüfen

#### 6.4.3 Get-NetTCPConnection: Ports und TCP-Verbindungen testen

6.4.4 Get-NetFirewallRule: Windows-Firewallregeln überwachen

6.5 Windows Server 2022 Active Directory

6.5.1 Netzwerkeinstellungen für die Domänenaufnahme konfigurieren

6.5.2 Domänenaufnahme durchführen

6.5.3 Domänenaufnahme testen

6.6 Zusammenfassung

## **Teil III Virtualisierung mit Hyper-V**

Kapitel 7 Hyper-V – Installation und Server virtualisieren

7.1 Neuerungen in der Virtualisierung

7.1.1 Neue VM-Version 10 in Windows Server 2022 und Windows 11

7.1.2 Hardware-Neuerungen in Windows Server 2022 und Windows 11

7.1.3 Neuerungen bei Hyper-V-Switches

7.1.4 Microsoft sieht den Schwerpunkt von Hyper-V in Azure Stack HCI

7.2 So funktioniert Hyper-V

7.2.1 Grundlagen von Hyper-V

7.2.2 Optimale Hochverfügbarkeit

7.2.3 Sicherheit und Bandbreitenverwaltung

7.2.4 Schnellerer Datenfluss in Rechenzentren mit SAN

7.2.5 Weitere wichtige Funktionen in Hyper-V

7.2.6 Speicherorte in Hyper-V

7.3 Windows Server Virtual Machine Licensing

7.3.1 Vertriebskanäle für Windows-Server verstehen

7.3.2 Edition von Windows Server 2022 beachten

7.3.3 Container nutzen und richtig lizenzieren

7.3.4 Virtual Desktop Access und Companion Subscription License

7.3.5 Hyper-V in Windows Server 2022 nutzen

7.4 Hyper-V installieren und verwalten

7.4.1 Voraussetzungen für den Einsatz von Hyper-V

7.4.2 Hyper-V installieren

7.4.3 Erste Schritte mit Hyper-V

7.4.4 CPU-Last überwachen und Daten zu VMs anzeigen

7.5 Virtuelle Switches in Windows Server 2022

7.5.1 Network Virtualization und Extensible Switch mit Windows Server 2022

7.5.2 Hyper-V-Netzwerke planen

7.5.3 Erstellen und Konfigurieren von virtuellen Switches

7.5.4 MAC-Adressen für Hyper-V konfigurieren

7.5.5 Virtuelle LANs (VLAN) und Hyper-V

7.5.6 Switch Embedded Teaming – NIC-Teams für Hyper-V

7.5.7 NAT in Hyper-V konfigurieren

7.6 Virtuelle Server erstellen und installieren

7.6.1 IDE oder SCSI – Welcher virtuelle Controller ist besser?

7.6.2 Laufwerke mit der PowerShell hinzufügen

7.6.3 Virtualisierung von Domänencontrollern

7.6.4 Per Hyper-V-Manager virtuelle Maschinen erstellen

7.6.5 Virtuelle Server steuern

7.7 Einstellungen von virtuellen Servern anpassen

7.7.1 Hardware zu virtuellen Computern hinzufügen

7.7.2 Virtuelle Festplatten zu Servern hinzufügen

7.7.3 Speicher-Migration – Virtuelle Festplatten verschieben

7.7.4 USB-Festplatten an Hyper-V anbinden

7.7.5 Virtuelle Festplatten von Servern verwalten und optimieren

7.7.6 Dynamic Memory – Arbeitsspeicher anpassen

7.7.7 Prozessoren in Hyper-V steuern

7.7.8 Allgemeine Einstellungen von virtuellen Computern verwalten

7.7.9 Virtuelle Server in der PowerShell steuern – PowerShell Direct nutzen

7.7.10 Daten von virtuellen Servern aus Hyper-V auslesen

## 7.8 Hyper-V-Host absichern

7.8.1 Updates installieren und Lücken schließen

7.8.2 Sicherheitsempfehlungen von Microsoft mit Richtlinien absichern

7.8.3 BPA für Hyper-V nutzen

7.8.4 Sichere virtuelle Maschinen mit Secure Boot

## 7.9 Migration zu Hyper-V

7.9.1 VM in Windows Server 2022 integrieren

7.9.2 Windows Server-Migrationstools nutzen

7.9.3 Neue VM-Version mit der PowerShell steuern

7.9.4 Eingebettete Virtualisierung in Windows Server 2022

7.9.5 Festplattendateien migrieren

## 7.10 Zusammenfassung

## Kapitel 8 Hyper-V – Datensicherung und Wiederherstellung

8.1 Hyper-V und virtuelle Server richtig sichern

8.2 Prüfpunkte von virtuellen Servern erstellen

8.2.1 Produktionsprüfpunkte in Windows Server 2022 nutzen

8.2.2 Prüfpunkte verstehen

8.2.3 Produktionsprüfpunkte erstellen

8.2.4 Snapshots von virtuellen Servern erstellen

8.2.5 Verwalten der Snapshots von virtuellen Servern

8.2.6 Datensicherung und Snapshots bei Hyper-V im Cluster

8.3 Sicherung durch Export

8.4 VMs per Skript sichern

8.4.1 Snapshots erstellen in Hyper-V mit »Checkpoint-VM«

8.5 Shielded VMs und Host Guardian Service

8.5.1 Verschlüsselung ohne Shielded VMs durchführen

8.5.2 Sichere VMs mit Shielded VMs

8.5.3 Verbindung zwischen Host Guardian Service und Guarded Hosts

8.5.4 Host Guardian Service konfigurieren

8.5.5 Vertrauensstellung zwischen Host Guardian Service und Active Directory einrichten

8.5.6 Guarded Hyper-V-Hosts mit HGS verbinden

8.5.7 Shielded VMs erstellen

8.6 Virtuelle Server gruppieren

8.7 Zusammenfassung

Kapitel 9 Hyper-V – Hochverfügbarkeit

9.1 Einstieg in die Hochverfügbarkeit in Hyper-V

9.1.1 Hyper-V-Replikation und Cluster

9.1.2 Arten der Hochverfügbarkeit in Hyper-V

9.2 Hyper-V-Replikation in der Praxis

9.2.1 Hyper-V-Hosts für Replikation aktivieren

9.2.2 Hyper-V-Replikation mit SSL konfigurieren

9.2.3 Virtuelle Server zwischen Hyper-V-Hosts replizieren

9.2.4 Failover mit Hyper-V-Replica durchführen

9.3 Livemigration ohne Cluster

9.4 Hyper-V im Cluster – Livemigration in der Praxis

9.4.1 Clusterknoten vorbereiten

9.4.2 Cluster mit Windows Server 2022 installieren

9.4.3 Cluster Shared Volumes aktivieren

9.4.4 Virtuelle Server im Cluster verwalten

9.4.5 MAC-Adressen im Cluster konfigurieren

9.4.6 Nacharbeiten: Überprüfung des Clusters und erste Schritte mit der Clusterverwaltung oder der PowerShell

9.5 Zusammenfassung

## **Teil IV Active Directory**

Kapitel 10 Active Directory – Grundlagen und erste Schritte

## 10.1 Einstieg in Active Directory

### 10.1.1 Active Directory im Detail

### 10.1.2 Active Directory-Systemrollen nutzen

### 10.1.3 Active Directory mit dem Verwaltungszentrum verwalten

### 10.1.4 Active Directory für Einsteiger

### 10.1.5 PowerShell und Active Directory

### 10.1.6 Migration zu Active Directory mit Windows Server 2022

### 10.1.7 Sicheres DNS-System in Windows Server 2022

### 10.1.8 Active Directory remote verwalten

## 10.2 Active Directory mit Windows Server 2022 installieren und verstehen

### 10.2.1 Aufbau von Active Directory

### 10.2.2 Installieren einer neuen Gesamtstruktur

## 10.3 Active Directory remote mit der PowerShell verwalten

### 10.3.1 Remote-PowerShell aktivieren und Verbindungsprobleme beheben

### 10.3.2 Cmdlets für die Remoteverwaltung und Abrufen der Hilfe

## 10.4 Verwalten der Betriebsmasterrollen von Domänencontrollern

### 10.4.1 PDC-Emulator verwalten

### 10.4.2 RID-Master – Neue Objekte in der Domäne aufnehmen

### 10.4.3 Infrastrukturmater – Auflösen von Gruppen über Domänen hinweg

### 10.4.4 Schemamater – Active Directory erweitern

### 10.4.5 Domänennamenmater – Neue Domänen hinzufügen

### 10.4.6 Der globale Katalog

### 10.4.7 Verwaltung und Verteilung der Betriebsmaster

## 10.5 Schreibgeschützte Domänencontroller (RODC)

## 10.6 Zusammenfassung

## Kapitel 11 Active Directory – Installation und Betrieb

### 11.1 DNS für Active Directory installieren

#### 11.1.1 Erstellen der notwendigen DNS-Zonen für Active Directory



- 11.9.1 Microsoft empfiehlt die Aktivierung von LDAPS
- 11.9.2 Probleme nach Aktivierung von LDAPS erkennen
- 11.9.3 LDAP-Signierung und LDAP Channel Binding für mehr Sicherheit in Active Directory
- 11.9.4 LDAP over SSL in Active Directory nutzen
- 11.9.5 LDAPS zusammen mit LDAP-Signatur und LDAP Channel Binding einsetzen
- 11.9.6 LDAP-Prioritäten und -Gewichtung konfigurieren – DCs entlasten
  - 11.10 Zeitsynchronisierung in Windows-Netzwerken
  - 11.10.1 Grundlagen zur Zeitsynchronisierung in Active Directory
  - 11.10.2 Das NTP-Protokoll und Befehle zur Zeitsynchronisierung
  - 11.10.3 Net Time versus W32tm
  - 11.10.4 Funkuhr versus Internetzeit – Zeitsynchronisierung konfigurieren
  - 11.10.5 Zeitsynchronisierung bei der Virtualisierung beachten
  - 11.11 Zusammenfassung
- Kapitel 12 Active Directory – Erweitern und Absichern
  - 12.1 Offline-Domänenbeitritt – Djoin
    - 12.1.1 Vorteile und technische Hintergründe zum Offline-Domänenbeitritt
    - 12.1.2 Voraussetzungen für die Verwendung des Offline-Domänenbeitritts
    - 12.1.3 Durchführen des Offline-Domänenbeitritts
    - 12.1.4 Offline-Domänenbeitritt bei einer unbeaufsichtigten Installation über Antwortdatei
    - 12.1.5 DirectAccess Offline Domain Join
  - 12.2 Verwaltete Dienstkonten – Managed Service Accounts
    - 12.2.1 Verwaltete Dienstkonten – Technische Hintergründe
    - 12.2.2 Verwaltete Dienstkonten – Produktiver Einsatz
    - 12.2.3 Verwaltete Dienstkonten in der grafischen Oberfläche anlegen
  - 12.3 Der Active Directory-Papierkorb im Praxiseinsatz
    - 12.3.1 Active Directory-Papierkorb verstehen und aktivieren

12.3.2 Objekte aus dem AD-Papierkorb mit Bordmitteln wiederherstellen

12.3.3 Organisationseinheiten und Objekte in AD absichern und sichern

12.3.4 Erweiterte Optionen für Organisationseinheiten einblenden

12.4 Unternehmensübergreifendes Identity Management

12.5 Azure AD Connect für Synchronisierung mit Azure nutzen

12.5.1 Azure AD Connect einrichten

12.5.2 Azure AD Connect konfigurieren

12.5.3 Troubleshooting von Azure AD und Verbindungen zu Azure

12.5.4 Azure AD Connect und Azure AD Connect Cloud Sync

12.6 Zusammenfassung

Kapitel 13 Active Directory – Neue Domänen und Domänencontroller

13.1 Core-Server als zusätzlichen Domänencontroller betreiben

13.1.1 Vorbereitungen in der PowerShell durchführen

13.1.2 Active Directory auf dem Core-Server installieren und einrichten

13.2 Schreibgeschützter Domänencontroller (RODC)

13.2.1 Vorbereitungen für die Integration eines zusätzlichen Domänencontrollers in eine Domäne

13.2.2 Einstieg in schreibgeschützte Domänencontroller – RODC

13.2.3 Integration eines neuen Domänencontrollers

13.2.4 Delegierung der RODC-Installation

13.2.5 Kennwortreplikationsrichtlinien auf RODCs steuern

13.2.6 RODC löschen

13.2.7 Notwendige Nacharbeiten nach der Integration eines zusätzlichen Domänencontrollers

13.3 Erstellen einer neuen untergeordneten Domäne

13.3.1 Anpassen der DNS-Infrastruktur an untergeordnete Domänen

13.3.2 Heraufstufen eines Domänencontrollers für eine neue untergeordnete Domäne

13.4 Einführen einer neuen Domänenstruktur in einer Gesamtstruktur

- 13.4.1 Erstellen der DNS-Infrastruktur für eine neue Domänenstruktur
- 13.4.2 Optimieren der IP-Einstellungen beim Einsatz von mehreren Domänen
- 13.4.3 Erstellen der neuen Domänenstruktur

- 13.5 Das Active Directory-Schema erweitern

- 13.6 Zusammenfassung

## Kapitel 14 Active Directory – Replikation

- 14.1 Grundlagen zur Replikation

- 14.2 Konfiguration der Routingtopologie in Active Directory

- 14.2.1 Erstellen von neuen Standorten über Active Directory-Standorte und -Dienste

- 14.2.2 Erstellen und Zuweisen von IP-Subnetzen

- 14.2.3 Erstellen von Standortverknüpfungen und Standortverknüpfungsbrücken

- 14.2.4 Zuweisen der Domänencontroller zu den Standorten

- 14.2.5 Die Konsistenzprüfung (Knowledge Consistency Checker)

- 14.3 Fehler bei der Active Directory-Replikation beheben

- 14.3.1 Suche mit der Active Directory-Diagnose

- 14.3.2 Ausschließen der häufigsten Fehlerursachen

- 14.3.3 Nltest zum Erkennen von Standortzuweisungen eines Domänencontrollers

- 14.3.4 Repadmin zum Anzeigen der Active Directory-Replikation

- 14.3.5 Replikation in der PowerShell testen

- 14.3.6 Netzwerkverbindungen zwischen DCs überprüfen

- 14.3.7 Secure Channel überprüfen – Test-ComputerSecureChannel

- 14.3.8 Kerberos-Test mit Dcdiag ausführen

- 14.3.9 Überprüfung der notwendigen SRV-Records im DNS unter \_msdcs

- 14.4 Zusammenfassung

## Kapitel 15 Active Directory – Fehlerbehebung und Diagnose

- 15.1 Bordmittel zur Diagnose verwenden

- 15.1.1 Schneller Überblick zu Domänen und Gesamtstrukturen in der PowerShell – inklusive Betriebsmaster
- 15.1.2 Informationen aus Active Directory mit der PowerShell auslesen
- 15.1.3 Daten zu Computer und Benutzerkonten anzeigen
- 15.1.4 Microsoft Active Directory Documentation Script
- 15.1.5 Verwenden der Domänencontrollerdiagnose
- 15.1.6 Testen der Namensauflösung mit Nslookup
- 15.1.7 Standard-OUs per Active Directory-Benutzer und -Computer überprüfen
- 15.1.8 Überprüfen der Active Directory-Standorte
- 15.1.9 Überprüfen der Domänencontrollerliste
- 15.1.10 Überprüfen der Active Directory-Dateien
- 15.1.11 Domänenkonto der Domänencontroller überprüfen und Kennwort zurücksetzen
- 15.1.12 Überprüfen der administrativen Freigaben
- 15.1.13 Überprüfen der Gruppenrichtlinien
- 15.1.14 DNS-Einträge von Active Directory überprüfen
- 15.1.15 Testen der Betriebsmaster
- 15.1.16 Leistungsüberwachung zur Diagnose nutzen
- 15.1.17 LDAP-Zugriff auf Domänencontrollern überwachen
- 15.1.18 Zurücksetzen des Kennworts für den Wiederherstellungsmodus in Active Directory
  - 15.2 Konfiguration der Ereignisprotokollierung von Active Directory
  - 15.3 Einbrüche in Active Directory effizient erkennen
- 15.3.1 Aktivieren der einfachen Überwachung
- 15.3.2 Erweiterte Überwachung nutzen
- 15.3.3 Anmeldungen im Netzwerk überwachen
- 15.3.4 Mit Tools für mehr Sicherheit sorgen
  - 15.4 Computerkonten in Active Directory verwalten und reparieren
- 15.4.1 Computerkonten in Active Directory-Benutzer und -Computer verwalten

15.4.2 Fehlerbehebung von Computerkonten

15.4.3 Veraltete Computer finden und bei Bedarf entfernen

15.5 Bereinigung von Active Directory und Entfernen von Domänencontrollern

15.5.1 Vorbereitungen beim Entfernen eines Domänencontrollers

15.5.2 Herabstufen eines Domänencontrollers

15.5.3 Bereinigen der Metadaten von Active Directory

15.6 Zusammenfassung

Kapitel 16 Active Directory – Sicherung, Wiederherstellung und Wartung

16.1 Active Directory sichern und wiederherstellen

16.1.1 Active Directory mit der Windows Server-Sicherung sichern

16.1.2 Wiederherstellen von Active Directory aus der Datensicherung

16.2 Active Directory-Datenbank warten

16.2.1 Verschieben der Active Directory-Datenbank

16.2.2 Offlinedefragmentation der Active Directory-Datenbank

16.2.3 Reparieren der Active Directory-Datenbank

16.2.4 Erstellen von Snapshots der Active Directory-Datenbank

16.3 Zusammenfassung

Kapitel 17 Active Directory – Vertrauensstellungen

17.1 Wichtige Grundlagen zu Vertrauensstellungen in Active Directory

17.2 Varianten der Vertrauensstellungen in Active Directory

17.3 Einrichtung einer Vertrauensstellung

17.3.1 Fehler mit Vertrauensstellungen von Computern zur Domäne beheben

17.4 Automatisch aktivierte SID-Filterung

17.5 Zusammenfassung

Kapitel 18 Benutzerverwaltung und Profile

18.1 Grundlagen zur Verwaltung von Benutzern

18.1.1 Active Directory-Benutzerverwaltung

18.1.2 Benutzerkonten in der PowerShell anlegen, verwalten und löschen

18.1.3 Verwalten von Benutzerkonten

18.1.4 Benutzerverwaltung für Remotedesktopbenutzer

18.2 Benutzerprofile nutzen

18.2.1 Benutzerprofile lokal und im Profieinsatz verstehen

18.2.2 Servergespeicherte Profile für Benutzer in Active Directory festlegen

18.2.3 Anmelde- und Abmeldeskripts für Benutzer und Computer

18.3 Gruppen verwalten

18.3.1 Gruppen anlegen und verwenden

18.3.2 Berechtigungen für Benutzer und Gruppen verwalten

18.3.3 Szenario: Delegation zum administrativen Verwalten einer Organisationseinheit

18.4 Zusammenfassung

Kapitel 19 Richtlinien im Windows Server 2022-Netzwerk

19.1 Erste Schritte mit Richtlinien

19.1.1 Verwaltungswerkzeuge für Gruppenrichtlinien

19.1.2 Wichtige Begriffe für Gruppenrichtlinien

19.1.3 Gruppenrichtlinien-Preferences effizient einsetzen

19.1.4 Registry-Einstellungen von Gruppenrichtlinien herausfinden

19.1.5 BSI bietet Hilfe bei der Absicherung von Windows

19.1.6 Windows 10/11 mit Microsoft-Sicherheitsempfehlungen konfigurieren

19.2 Gruppenrichtlinien verwalten

19.2.1 Neue Gruppenrichtlinie erstellen

19.2.2 GPO mit einem Container verknüpfen

19.2.3 Gruppenrichtlinien erzwingen und Priorität erhöhen

19.2.4 Vererbung für Gruppenrichtlinien deaktivieren

19.2.5 Administration von domänenbasierten GPOs mit ADMX-Dateien

19.3 Sicherheitseinstellungen in Windows 10/11 mit Richtlinien steuern

- 19.3.1 Microsoft Store, Cortana und Datensammlungen in Windows 10/11 sperren
- 19.3.2 Sicherheitseinstellungen für das Netzwerk steuern
- 19.3.3 Überwachter Ordnerzugriff – Schutz vor Ransomware
- 19.3.4 Datenschutz in Richtlinien steuern
- 19.3.5 Benutzer und Kennwörter mit Gruppenrichtlinien absichern
- 19.3.6 OneDrive for Business nutzen
- 19.3.7 Microsoft Application Guard und Office
  - 19.4 Gruppenrichtlinien testen und Fehler beheben
  - 19.4.1 Einstieg in die Fehlerbehebung von Gruppenrichtlinien
  - 19.4.2 Vorgehensweise bei der Fehlerbehebung von Gruppenrichtlinien
  - 19.4.3 Policy Analyzer zur Fehlerbehebung nutzen
  - 19.4.4 Datensicherung und Wiederherstellung von Gruppenrichtlinien
  - 19.4.5 Gruppenrichtlinien mit der PowerShell sichern und wiederherstellen
  - 19.4.6 Gruppenrichtlinienmodellierung
  - 19.5 Softwareverteilung über Gruppenrichtlinien
  - 19.6 Geräteinstallation mit Gruppenrichtlinien konfigurieren
  - 19.6.1 Geräteidentifikationsstring und Gerätesetupklasse
  - 19.6.2 So funktioniert die Steuerungen in Geräteinstallationen über Gruppenrichtlinien
  - 19.6.3 Konfiguration von Gruppenrichtlinien für den Zugriff auf Wechselmedien
  - 19.6.4 Layered Group Policies – Mehrschichtige Gruppenrichtlinien nutzen
  - 19.6.5 Konfiguration von Gruppenrichtlinien für den Zugriff auf Wechselmedien
  - 19.7 Mit AppLocker Desktop- und Windows-Apps in Netzwerken steuern
  - 19.7.1 AppLocker in Unternehmen nutzen
  - 19.7.2 Gruppenrichtlinien für AppLocker erstellen
  - 19.7.3 Erstellen von Regeln für AppLocker
  - 19.7.4 Automatisches Erstellen von Regeln und Erzwingen von AppLocker
  - 19.7.5 Windows 10/11 Device Guard zusammen mit AppLocker nutzen

- 19.7.6 Benutzerkontensteuerung über Richtlinien konfigurieren
- 19.7.7 Erstellen einer neuen Gruppenrichtlinie für sichere Kennwörter
- 19.7.8 Firewallinstellungen über Gruppenrichtlinien setzen
- 19.8 Zusammenfassung

## **Teil V Datei- und Druckserver mit Windows Server**

### Kapitel 20 Dateiserver und Daten im Netzwerk freigeben

- 20.1 SMB 3.x in Windows Server 2022 nutzen
  - 20.1.1 Mehr Sicherheit und Leistung in SMB 3.x
  - 20.1.2 SMB 1.0 im Netzwerk ausfindig machen und deaktivieren
- 20.2 Berechtigungen für Dateien und Ordner verwalten
  - 20.2.1 Erweiterte Berechtigungen auf Ordner
  - 20.2.2 Berechtigungen verstehen
  - 20.2.3 Effektive Berechtigungen
  - 20.2.4 Tools zur Überwachung von Berechtigungen
- 20.3 Überwachung von Dateien und Ordnern
  - 20.3.1 Einstieg in die Überwachung von Verzeichnissen
  - 20.3.2 Überwachung mit Richtlinien steuern
- 20.4 Die Freigabe von Ordnern
  - 20.4.1 Freigaben erstellen
  - 20.4.2 Der Assistent zum Erstellen von Freigaben
  - 20.4.3 Anzeigen geöffneter Dateien über das Netzwerk – PsFile
  - 20.4.4 Versteckte Freigaben
  - 20.4.5 Anzeigen aller Freigaben
  - 20.4.6 Auf Freigaben über das Netzwerk zugreifen
  - 20.4.7 Offlinedateien für den mobilen Einsatz unter Windows 10/11
- 20.5 Storage Quality of Services (QoS) – Richtlinien für Datenspeicher
  - 20.5.1 Einstieg in Speicherrichtlinien
  - 20.5.2 Storage QoS in der PowerShell verwalten

- 20.5.3 Neue Richtlinien in der PowerShell erstellen und verwalten
- 20.5.4 Aggregated Policies nutzen
- 20.5.5 Storage QoS im Cluster überwachen
- 20.5.6 Speicherrichtlinien in System Center Virtual Machine Manager
  - 20.6 Dateien und Freigaben auf Windows Server 2022 migrieren
  - 20.6.1 Daten mit Robocopy übernehmen
  - 20.6.2 Nur Freigaben und deren Rechte übernehmen
  - 20.6.3 Windows Server Storage Migration Service
    - 20.7 Azure File Sync und Azure Files – Lokale Daten mit der Cloud nutzen
    - 20.7.1 So funktioniert Azure File Sync
    - 20.7.2 Azure File Sync einrichten
    - 20.7.3 Azure-Dateifreigaben nutzen
    - 20.8 Zusammenfassung
- Kapitel 21 Ressourcen-Manager für Dateiserver und DFS
  - 21.1 Kontingentverwaltung in Windows Server 2022
    - 21.1.1 Kontingentverwaltung mit FSRM
    - 21.1.2 Datenträgerkontingente für Laufwerke festlegen
    - 21.2 Dateiprüfungsverwaltung nutzen
      - 21.2.1 Erstellen einer Dateiprüfung
      - 21.2.2 Dateiprüfungsausnahmen
      - 21.2.3 Dateigruppen für die Dateiprüfung
      - 21.3 Speicherberichteverwaltung in FSRM
      - 21.4 Dateiklassifizierungsdienste einsetzen
        - 21.4.1 Klassifizierungseigenschaften und Klassifizierungsregeln verstehen und einsetzen
        - 21.4.2 Dateiverwaltungsaufgaben bei der Dateiklassifizierung einsetzen
        - 21.5 So schützen Unternehmen ihre Dateiserver vor Ransomware
          - 21.5.1 Allgemeine-Tipps für den Schutz vor Ransomware

- 21.5.2 Generelle Vorgehensweise beim Befall gegen Ransomware
- 21.5.3 Schattenkopien helfen bei Windows-Servern
- 21.5.4 Ressourcen-Manager für Dateiserver gegen Ransomware nutzen
  - 21.6 Organisieren und Replizieren von Freigaben über DFS
- 21.6.1 Einführung und wichtige Informationen beim Einsatz von DFS
- 21.6.2 DFS-Namespaces und DFS-Replikation
- 21.6.3 Voraussetzungen für DFS
- 21.6.4 Installation und Einrichtung von DFS
- 21.6.5 Einrichtung eines DFS-Namespaces
- 21.6.6 Einrichten der DFS-Replikation
  - 21.7 Zusammenfassung

## Kapitel 22 BranchCache

- 22.1 BranchCache im Überblick – Niederlassungen effizient anbinden
- 22.2 Gehosteter Cache (Hosted Cache) nutzen
- 22.3 Verteilter Cache (Distributed Cache) nutzen
- 22.4 BranchCache auf dem Hosted-Cache-Server konfigurieren
  - 22.4.1 Feature für Hosted Cache installieren
  - 22.4.2 Zertifikate auf dem Hosted-Cache-Server betreiben
  - 22.4.3 Einstellungen auf dem Hosted-Cache-Server anpassen
  - 22.4.4 Content-Server konfigurieren
  - 22.5 BranchCache auf Clients konfigurieren
- 22.5.1 Clientkonfiguration mit Gruppenrichtlinien konfigurieren
- 22.5.2 Firewallinstellungen für BranchCache setzen
  - 22.6 Leistungsüberwachung und BranchCache
  - 22.7 Zusammenfassung

## Kapitel 23 Druckerserver betreiben

- 23.1 PrintNightmare beachten
- 23.2 Drucken im Netzwerk und mit Smartphones oder Tablets

- 23.2.1 Drucker in Windows freigeben
  - 23.2.2 Drucker über WLAN anbinden
  - 23.2.3 Eigenen Netzwerkanschluss konfigurieren
  - 23.2.4 Drucken mit iPhone und iPad – AirPrint
  - 23.3 Freigegebene Drucker verwalten
    - 23.3.1 Anpassen der Einstellungen von Druckern
    - 23.3.2 Der Zugriff auf freigegebene Drucker
    - 23.3.3 Eigenschaften von Druckern in der PowerShell ändern
    - 23.3.4 Druckaufträge in der PowerShell erzeugen
    - 23.3.5 Druckberechtigungen mit Skripten setzen – SetACL.exe
  - 23.4 Verwaltung von Druckjobs
    - 23.4.1 Druckverwaltungs-Konsole – Die Zentrale für Druckerserver
    - 23.4.2 Erstellen von benutzerdefinierten Filteransichten
    - 23.4.3 Exportieren und Importieren von Druckern
    - 23.4.4 Drucker verwalten und über Gruppenrichtlinien verteilen lassen
  - 23.5 Druckprobleme im Netzwerk lösen
    - 23.5.1 Generelle Vorgehensweise beim Lösen von Druckproblemen
    - 23.5.2 Druckjobs überprüfen und löschen
    - 23.5.3 Problembehebung mit Assistenten durchführen
    - 23.5.4 Druckereinstellungen zur Fehlerbehebung überprüfen
    - 23.5.5 Berechtigungen und Sicherheitseinstellungen überprüfen
    - 23.5.6 Drucker mit WMI ansprechen
  - 23.6 Druckerserver mit Microsoft Universal Print in der Cloud betreiben
    - 23.6.1 Lizenzierung und Einstieg in Universal Print
  - 23.7 Zusammenfassung
- Teil VI Infrastrukturen mit Windows Server**
- Kapitel 24 DHCP- und IPAM-Server einsetzen
    - 24.1 DHCP-Server einsetzen

- 24.1.1 Installation eines DHCP-Servers
- 24.1.2 Grundkonfiguration eines DHCP-Servers
- 24.1.3 DHCP-Server mit Tools testen und Fehler finden
- 24.1.4 DHCP-Verkehr mit WireShark überprüfen
- 24.1.5 Core-Server – DHCP mit Netsh über die Eingabeaufforderung verwalten
- 24.1.6 Konfigurieren von DHCP mit der richtlinienbasierten Zuweisung
- 24.1.7 MAC-Filterung für DHCP in Windows Server 2022 nutzen
  - 24.2 Migration – Verschieben einer DHCP-Datenbank auf einen anderen Server
  - 24.3 Ausfallsicherheit von DHCP-Servern
    - 24.3.1 DHCP für Failover konfigurieren
    - 24.3.2 Ausfallsicherheit mit 80/20-Regel
    - 24.3.3 Bereichsgruppierung (Superscopes)
    - 24.3.4 Ausfallsicherheit bei DHCP-Servern durch verschiedene Bereiche herstellen
    - 24.3.5 Standby-Server mit manueller Umschaltung
  - 24.4 IPAM im Praxiseinsatz
    - 24.4.1 IPAM-Grundlagen
    - 24.4.2 IPAM einrichten
    - 24.4.3 Fehlerbehebung der Anbindung von IPAM-Clients
    - 24.4.4 Infrastrukturüberwachung und -verwaltung
    - 24.4.5 IP-Adressblöcke mit IPAM
  - 24.5 Zusammenfassung
- Kapitel 25 DNS einsetzen und verwalten
  - 25.1 Erstellen von Zonen und Domänen
    - 25.1.1 Erstellen von neuen Zonen
    - 25.1.2 Erstellen von statischen Einträgen in der DNS-Datenbank
    - 25.1.3 Einstellungen und Verwalten von Zonen
  - 25.2 Verwalten der Eigenschaften eines DNS-Servers

- 25.2.1 Schnittstellen eines DNS-Servers verwalten
- 25.2.2 Erweiterte Einstellungen für einen DNS-Server
- 25.2.3 Zonendaten beim Start des DNS-Servers einlesen
- 25.2.4 Protokollierung für DNS konfigurieren
- 25.2.5 Ereignisprotokollierung konfigurieren
  - 25.3 DNS-Weiterleitungen verwenden
  - 25.4 Konfiguration sekundärer DNS-Server
  - 25.5 DNS-Troubleshooting
- 25.5.1 Überprüfung und Fehlerbehebung der DNS-Einstellungen
- 25.5.2 Ipconfig für DNS-Diagnose verwenden
- 25.5.3 Domänencontroller kann nicht gefunden werden
- 25.5.4 Namensauflösung von Mitgliedsservern
- 25.5.5 Erweiterte Namensauflösung sicherstellen
- 25.5.6 Nslookup zur Auflösung von Internetdomänen verwenden
- 25.5.7 Mit Nslookup SRV-Records oder MX-Records anzeigen
- 25.5.8 Komplette Zonen mit Nslookup übertragen
- 25.5.9 Dnscmd zur Verwaltung eines DNS-Servers in der Eingabeaufforderung
  - 25.6 DNSSEC – Sicherheit in DNS
- 25.6.1 DNSSEC verstehen
- 25.6.2 DNS sicher betreiben – DNSSEC und Co. in der Praxis
- 25.6.3 DNS-Abfragen mit Richtlinien steuern
- 25.6.4 Response Rate Limiting – Schutz vor Denial of Service
- 25.7 Zusammenfassung

## Kapitel 26 Windows Server Container, Docker und Hyper-V-Container

- 26.1 Einstieg in Container und Docker
  - 26.1.1 Container im Vergleich zu virtuellen Servern
  - 26.1.2 Container-Feature installieren
  - 26.1.3 Erste Schritte mit Docker in Windows Server 2022

26.1.4 Hyper-V-Container-Host

26.1.5 Container im Windows Admin Center verwalten

26.2 Erweiterte Konfiguration von Containern

26.2.1 Neues Containerimage für Windows Server 2022 verfügbar

26.2.2 Container erstellen und Serverdienste verwalten

26.2.3 Container und eigene Images erstellen

26.2.4 Dockerfiles für eigene Images erstellen

26.2.5 Docker Push – Container in die Cloud laden

26.3 Hyper-V-Container in Windows Server 2022

26.3.1 Einstieg in Hyper-V-Container

26.3.2 Hyper-V-Container erstellen und konfigurieren

26.3.3 Docker, Hyper-V-Container und VMs parallel einsetzen

26.3.4 Windows Server Container in der PowerShell verwalten

26.4 Windows-Subsystem für Linux in Windows Server 2022 und Windows 10/11

26.4.1 Linux und Windows gemeinsam betreiben

26.4.2 Windows Subsystem for Linux installieren

26.4.3 Linux-Distributionen anzeigen und starten

26.5 Zusammenfassung

Kapitel 27 Webserver – Internetinformationsdienste (IIS)

27.1 Installation, Konfiguration und erste Schritte

27.1.1 Anzeigen der Websites in IIS

27.1.2 Hinzufügen und Verwalten von Websites

27.1.3 Starten und Beenden des Webserver

27.1.4 Systemdateien von IIS verstehen

27.1.5 Verwalten der Webanwendungen und virtuellen Ordner einer Website

27.1.6 Entwicklungstools im Internet Explorer und Microsoft Edge

27.2 Verwalten von Anwendungspools

- 27.2.1 Erstellen und Verwalten von Anwendungspools
- 27.2.2 Zurücksetzen von Arbeitsprozessen in Anwendungspools
- 27.3 Verwalten von Modulen in IIS 2022
- 27.4 Delegierung der IIS-Verwaltung
  - 27.4.1 Vorgehensweise bei der Delegierung von Berechtigungen
  - 27.4.2 Verwalten von IIS-Manager-Benutzern
  - 27.4.3 Berechtigungen der IIS-Manager-Benutzer verwalten
  - 27.4.4 Verwalten der Delegierung
  - 27.4.5 Aktivieren der Remoteverwaltung
- 27.5 Sicherheit in IIS 2022 konfigurieren
  - 27.5.1 Konfiguration der anonymen Authentifizierung
  - 27.5.2 Konfiguration der Standardauthentifizierung
  - 27.5.3 Konfiguration der Windows-Authentifizierung
  - 27.5.4 Einschränkungen für IP-Adressen und Domänen
  - 27.5.5 Sicherheitseinstellungen von IIS anpassen
  - 27.5.6 IP-Adressen, Domänen, SSL und URL Rewrite
  - 27.5.7 IIS mit kostenlosen Tools absichern
  - 27.5.8 Zed Attack Proxy Project (ZAP) und Deft-Linux – Webanwendungen testen
  - 27.5.9 Freigegebene Konfiguration
- 27.6 Konfigurieren der Webseiten, Dokumente und HTTP-Verbindungen
  - 27.6.1 Festlegen des Standarddokuments
  - 27.6.2 Das Feature »Verzeichnis durchsuchen« aktivieren und verwalten
  - 27.6.3 Konfigurieren der HTTP-Fehlermeldungen und -Umleitungen
- 27.7 IIS 2022 überwachen und Protokolldateien konfigurieren
  - 27.7.1 Ablaufverfolgungsregeln für Anforderungsfehler
  - 27.7.2 Allgemeine Protokollierung aktivieren und konfigurieren
  - 27.7.3 Überprüfen der Arbeitsprozesse der Anwendungspools
- 27.8 Optimieren der Serverleistung

27.8.1 Komprimierung aktivieren

27.8.2 Ausgabezwischenspeicherung verwenden

27.9 FTP-Server betreiben

27.9.1 Konfiguration des FTP-Servers

27.9.2 Schritt für Schritt-Anleitung zum FTP-Server in IIS 2022

27.10 Zusammenfassung

Kapitel 28 Remotedesktopdienste – Anwendungen virtualisieren

28.1 Neuerungen in RDS

28.1.1 Vergleich zu Windows Server 2016

28.1.2 Server Based Personal Desktop – Private Server für Anwender

28.2 Einstieg in die Remotedesktopdienste

28.3 Installation eines Remotedesktopservers

28.3.1 Installation und Verteilen der notwendigen Rollendienste

28.3.2 Einrichten einer neuen Sitzungssammlung

28.3.3 RemoteApp – Anwendungen bereitstellen

28.3.4 Remotedesktoplizenzierung

28.3.5 Remotedesktopsitzungen spiegeln

28.3.6 Nacharbeiten zur Installation

28.4 Drucken mit Remotedesktop-Sitzungshosts

28.4.1 Einstieg in das Drucken mit den Remotedesktopdiensten

28.4.2 Druckerprobleme auf Remotedesktop-Sitzungshosts lösen

28.4.3 Berechtigungs-Probleme auf Remotedesktop-Sitzungshosts lösen

28.5 Installation von Applikationen

28.6 Remotedesktop-Client

28.6.1 Befehlszeilenparameter für den Remotedesktop-Client

28.6.2 Umleitung von Digitalkameras und Mediaplayer

28.7 Verwaltung eines Remotedesktop-Sitzungshosts

28.7.1 Remotedesktopdienste verwalten

- 28.7.2 Single Sign-On (SSO) für Remotedesktop-Sitzungshosts
- 28.7.3 Connection Broker an Microsoft Azure anbinden
  - 28.8 RemoteApps verwalten
  - 28.8.1 Konfiguration von Remotedesktopdienste-RemoteApp
  - 28.8.2 Mit Windows 10/11 auf RemoteApps zugreifen
  - 28.8.3 Remotedesktopdienste-Webzugriff
    - 28.9 Remotedesktopgateway
    - 28.9.1 Einrichtung und Konfiguration eines Remotedesktopgateways
    - 28.9.2 Ressourcenautorisierungsrichtlinien erstellen und verwalten
      - 28.10 Remotedesktop-Verbindungsbroker
      - 28.11 Zertifikate installieren und einrichten
      - 28.11.1 RDS-Zertifikate im Überblick
      - 28.11.2 Zertifikate von den Active Directory-Zertifikatdiensten abrufen
      - 28.11.3 Eigene Zertifikate-Vorlagen für die Anmeldung an RDS verwenden
        - 28.12 Zusammenfassung

## Kapitel 29 Virtual Desktop Infrastructure – Arbeitsstationen virtualisieren

- 29.1 Einstieg in VDI
  - 29.2 Windows 10/11 als virtuellen Computer in einer VDI-Struktur einsetzen
  - 29.2.1 Installieren des Remotedesktop-Sitzungshosts
  - 29.2.2 VDI-Umgebung verwalten
  - 29.2.3 Virtuelle Computer installieren und für VDI vorbereiten
  - 29.2.4 System mit Sysprep vorbereiten
    - 29.3 Konfiguration des virtuellen Desktop-Pools
    - 29.3.1 Sammlung virtueller Pools im Server-Manager erstellen
    - 29.3.2 Desktop testen und verwenden
    - 29.3.3 Personalisierte virtuelle Rechner verwenden
    - 29.3.4 Eigenes Hintergrundbild für gehostete Desktops aktivieren

## 29.4 Zusammenfassung

### **Teil VII Sicherheit und Hochverfügbarkeit**

#### Kapitel 30 Active Directory-Zertifikatdienste

##### 30.1 Installation einer Zertifizierungsstelle

30.1.1 Serverrolle für Active Directory-Zertifikatdienste installieren

30.1.2 Zertifizierungsstelle einrichten

30.1.3 Eigenständige Zertifizierungsstellen

30.1.4 Installieren einer untergeordneten Zertifizierungsstelle

30.1.5 Migrieren des Active Directory-Zertifikatdienstes

30.1.6 Migration beginnen

30.1.7 Zielsever konfigurieren

##### 30.2 Zuweisen und Installieren von Zertifikaten

30.2.1 Zertifikate mit Assistenten aufrufen

30.2.2 Zertifikate im IIS-Manager abrufen

30.2.3 Zertifikate über Webinterface ausstellen

30.2.4 Zertifikate mit Gruppenrichtlinien verteilen

##### 30.3 Zertifizierungsstelle verwalten

30.3.1 SSL für Zertifikatdienste einrichten

30.3.2 Zertifikate von Stammzertifizierungsstellen verwalten

30.3.3 Die Zertifizierungsstellentypen und -Aufgaben

30.3.4 Verteilung der Zertifikateinstellungen über Gruppenrichtlinien

##### 30.4 Sicherheit für Zertifizierungsstellen verwalten

30.4.1 Zertifizierungsstellenverwaltung delegieren

30.4.2 Sichern von Active Directory-Zertifikatdiensten

##### 30.5 Zusammenfassung

#### Kapitel 31 Firewall, Defender und IPsec im Netzwerk einsetzen

##### 31.1 Microsoft Defender Exploit Guard

31.2 Microsoft Defender für den Virenschutz nutzen

- 31.2.1 Microsoft Defender in der GUI und Befehlszeile steuern
- 31.2.2 Definitionsdateien automatisiert herunterladen und installieren
- 31.2.3 Microsoft Defender in der PowerShell verwalten
- 31.2.4 Microsoft Defender in den Einstellungen und Gruppenrichtlinien anpassen
- 31.2.5 Ausnahmen für Serverrollen verwalten – Hyper-V
- 31.2.6 Virensuche mit dem Sysinternals Process Explorer
- 31.3 Windows Defender Credential Guard und Hypervisor-Protected Code Integrity
  - 31.3.1 Windows Defender Credential Guard aktivieren
  - 31.3.2 Kernisolierung: Hypervisor-Protected Code Integrity
- 31.4 Windows-Firewall nutzen
  - 31.4.1 Windows-Firewall in der PowerShell steuern
  - 31.4.2 IPsec mit der Windows-Firewall nutzen
  - 31.4.3 Firewallregeln für SQL Server steuern
- 31.5 Zusammenfassung

## Kapitel 32 Remotezugriff mit DirectAccess und Always On VPN

- 32.1 Always On VPN nutzen
  - 32.1.1 Vorteile von Always On VPN im Vergleich zu DirectAccess
  - 32.1.2 Gruppenrichtlinien vor dem Einsatz konfigurieren
  - 32.1.3 Zertifikatvorlagen für Always On VPN vorbereiten
  - 32.1.4 Always On VPN installieren
- 32.2 Remotezugriff installieren und einrichten – Erste Schritte
  - 32.2.1 Remotezugriff – Die Grundlagen
  - 32.2.2 Vorbereiten der Installation von DirectAccess und Remotezugriff
  - 32.2.3 Rollendienste installieren und Remotezugriff aktivieren
  - 32.2.4 DirectAccess und VPN-Zugang einrichten
  - 32.2.5 Aktualisieren von Clients mit der DirectAccess-Konfiguration
  - 32.2.6 Überprüfen der Bereitstellung

32.3 Remotezugriff verwalten

32.4 VPN verwalten

32.4.1 Verwalten und Konfigurieren der RAS-Benutzer und RAS-Ports

32.5 HTTPS-VPN über Secure Socket Tunneling-Protokoll

32.5.1 Ablauf beim Verbinden über SSTP

32.5.2 Installation von SSTP

32.5.3 Fehlerbehebung bei SSTP-VPN

32.6 Exchange und Co. veröffentlichen – Anwendungsproxy einsetzen

32.6.1 Webanwendungsproxy installieren

32.6.2 Active Directory mit dem Webanwendungsproxy einrichten

32.6.3 Active Directory-Verbunddienste einrichten

32.7 Zusammenfassung

Kapitel 33 Active Directory-Rechteverwaltungsdienste nutzen

33.1 Active Directory-Rechteverwaltung im Überblick

33.1.1 AD RMS und dynamische Zugriffssteuerung

33.2 Rechteverwaltung installieren und einrichten

33.2.1 SQL-Server für AD RMS vorbereiten

33.2.2 Konfigurieren von AD RMS

33.2.3 AD RMS nach der Installation verwalten und überprüfen

33.3 Dynamische Zugriffssteuerung nutzen

33.4 Zusammenfassung

Kapitel 34 Hochverfügbarkeit und Lastenausgleich

34.1 Grundlagen zum Lastenausgleich

34.2 Notwendige Vorbereitungen für NLB-Cluster

34.3 Netzwerklastenausgleich installieren

34.4 NLB-Cluster erstellen

34.5 NLB versus DNS-Roundrobin

34.6 Storage Spaces Direct nutzen

- 34.6.1 Einstieg in Storage Spaces Direct
- 34.6.2 So funktioniert Storage Spaces Direct
- 34.6.3 Storage Spaces Direct in der Praxis
- 34.6.4 Ausfallsicherheit bei Storage Spaces Direct
- 34.6.5 Speicherpools in Storage Spaces Direct optimieren
  - 34.7 Scale-Out File Server erstellen
  - 34.7.1 Cluster sind auch in kleinen Netzwerken sinnvoll einsetzbar
  - 34.7.2 Scale-Out File Server und Storage Spaces Direct
  - 34.7.3 Scale-Out File Server im Cluster nutzen
  - 34.7.4 Vorteile beim Einsatz eines Scale-Out File Servers: SMB-Version beachten
  - 34.7.5 Dateiserver und das Cluster Shared Volume
    - 34.8 Cluster Operating System Rolling Upgrade
    - 34.8.1 So aktualisieren Sie einen Cluster zu Windows Server 2022
    - 34.8.2 Node Fairness – Lastenausgleich aktivieren
    - 34.8.3 Startreihenfolge der VMs nach der Migration anpassen
    - 34.8.4 Compute Resiliency – Ausfallsicherheit steuern
      - 34.9 Cluster Aware Update nutzen und einrichten
      - 34.9.1 Grundlagen für die Einführung von Cluster Aware Update
      - 34.9.2 Firewallinstellungen und mehr für CAU
      - 34.9.3 CAU für den Cluster aktivieren
      - 34.9.4 CAU in der PowerShell steuern
      - 34.9.5 Fehlerbehebung der Einrichtung
      - 34.9.6 Updates mit CAU planen
        - 34.10 Cloud Witness mit Microsoft Azure
        - 34.10.1 Cluster an Microsoft Azure anbinden
        - 34.10.2 Zeugenserver überprüfen
          - 34.11 Der Netzwerkcontroller im Überblick
          - 34.12 Data Center Bridging (DCB)

### 34.13 Zusammenfassung

## Kapitel 35 Datensicherung und Wiederherstellung

### 35.1 Grundlagen zur Datensicherung

### 35.2 Windows Server-Sicherung installieren und konfigurieren

#### 35.2.1 Sicherung in der Eingabeaufforderung und PowerShell konfigurieren

#### 35.2.2 Daten mit dem Sicherungsprogramm wiederherstellen

#### 35.2.3 Kompletten Server mit dem Sicherungsprogramm wiederherstellen

### 35.3 Erweiterte Wiederherstellungsmöglichkeiten

#### 35.3.1 Schrittaufzeichnung – Fehler in Windows nachvollziehen und beheben

#### 35.3.2 Datensicherung über Ereignisanzeige starten

### 35.4 Windows-Abstürze analysieren und beheben

### 35.5 Microsoft Windows File Recovery Tool

#### 35.5.1 WinFR in der Praxis

#### 35.5.2 Alternativen für WinFR

### 35.6 Zusammenfassung

## Kapitel 36 Active Directory-Verbunddienste und Workplace Join

### 36.1 Installieren und Einrichten der Active Directory-Verbunddienste

#### 36.1.1 Einstieg in die Installation von AD FS

#### 36.1.2 Vorbereitungen für die AD FS-Infrastruktur

#### 36.1.3 SSL-Zertifikate als Vorlage in Active Directory-Zertifikatdiensten festlegen

#### 36.1.4 AD FS als Serverrolle installieren

#### 36.1.5 AD FS einrichten

#### 36.1.6 Geräteregistrierung konfigurieren

#### 36.1.7 Einrichten einer Beispiel-Webanwendung für AD FS

#### 36.1.8 Vertrauensstellung zwischen Webanwendung und AD FS einrichten

### 36.2 Fehlerbehebung und Überwachung bei einem AD FS-Server

### 36.3 Single Sign-On mit AD FS – auch mit Microsoft 365/Office 365

### 36.4 Zusammenfassung

## Kapitel 37 Updates in Microsoft-Netzwerken steuern mit WSUS und Azure

### 37.1 WSUS installieren

37.1.1 WSUS nach der Installation einrichten

37.1.2 WSUS-Grundeinrichtung über Gruppenrichtlinien

37.1.3 Upstreamserver in WSUS nutzen

37.1.4 SSL in WSUS nutzen

### 37.2 Updates im Griff behalten und steuern

37.2.1 Steuerung von Verteilungsringen

37.2.2 Steuerung von Windows-10/11-Updates mit Gruppenrichtlinien

37.2.3 Konfiguration der Übermittlungsoptimierung

37.2.4 Neue Update-Funktionen in Windows 10/11 verstehen

37.2.5 Windows-Updates in Windows 10/11 steuern

37.2.6 Installation von Funktionsupdates steuern

37.2.7 Windows 10/11 und WSUS

37.2.8 Probleme bei der Installation von Updates beheben

### 37.3 Patchverwaltung mit WSUS

37.3.1 Clientcomputer über Gruppenrichtlinien anbinden

37.3.2 Einstellungen für Windows 10/11 korrekt setzen

37.3.3 Updates genehmigen und bereitstellen

37.3.4 Berichte mit WSUS abrufen

### 37.4 WSUS in Windows Server 2022 überwachen

37.4.1 Überprüfung der Gruppenrichtlinien

37.4.2 In der Befehlszeile nach Problemen suchen

37.4.3 SSL-Port beachten

37.4.4 Diagnostic Tool for the WSUS Agent

37.4.5 WSUS mit der PowerShell verwalten

### 37.5 Azure Update Management für das Patchmanagement nutzen

37.5.1 Komponenten von Azure Update Management

37.5.2 Azure Update Management in der Praxis

37.5.3 Linux-Server automatisiert aktualisieren

37.5.4 Angebundene Server im Azure-Portal verwalten

37.5.5 Bereitstellen von Updates über Azure Update Management

37.5.6 Computer aus der Azure-Updateverwaltung entfernen

37.6 Zusammenfassung

Kapitel 38 Diagnose und Überwachung

38.1 Fehlerbehebung in Windows Server – Ereignisanzeige

38.1.1 Ereignisanzeige nutzen

38.1.2 Ereignisprotokolle im Netzwerk einsammeln

38.2 Überwachung der Systemleistung

38.2.1 Die Leistungsüberwachung

38.2.2 Indikatordaten in der Leistungsüberwachung beobachten

38.2.3 Sammlungssätze nutzen

38.2.4 Speicherengpässe beheben

38.2.5 Prozessorauslastung messen und optimieren

38.2.6 Der Task-Manager als Analysewerkzeug

38.2.7 Laufwerke und Datenträger überwachen – Leistungsüberwachung und Zusatztools

38.3 Serverüberwachung mit dem Windows Admin Center

38.3.1 Neuen Arbeitsbereich erstellen

38.3.2 Workspace speichern, herunterladen und hochladen

38.4 Aufgabenplanung – Windows automatisieren

38.4.1 Aufgabenplanung verstehen

38.4.2 Erstellen einer neuen Aufgabe

38.5 Prozesse und Dienste überwachen

38.5.1 Dienste in der PowerShell verwalten

38.5.2 Dateisystem, Registry und Prozesse überwachen – Sysinternals Process Monitor

38.5.3 Laufende Prozesse analysieren – Process Explorer

38.5.4 Wichtige Informationen immer im Blick – BgInfo

38.5.5 Systeminformationen in der Eingabeaufforderung anzeigen – PsInfo

38.6 Zusammenfassung

## **Teil VIII Bereitstellung, Verwaltung, Cloudanbindung**

### Kapitel 39 Windows-Bereitstellungsdienste

39.1 Windows Assessment and Deployment Kit (ADK)

39.1.1 Das Windows-Imageformat

39.1.2 Windows Systemabbild-Manager, Antwortdateien und Kataloge

39.1.3 Windows Assessment and Deployment Kit installieren

39.2 Automatisierte Installation von Windows 10/11 und Windows Server 2022

39.2.1 Windows System Image Manager nutzen

39.2.2 Windows 10/11 und Windows Server 2022 aktivieren

39.3 Grundlagen der Windows-Bereitstellungsdienste

39.3.1 Verwalten von Abbildern in WDS

39.3.2 So funktioniert die automatisierte Installation von Windows über WDS

39.4 Installation der Windows-Bereitstellungsdienste

39.4.1 Ersteinrichtung der Windows-Bereitstellungsdienste

39.4.2 Multicast verwenden

39.5 Verwalten und Installieren von Abbildern

39.5.1 Startabbilder verwalten

39.5.2 Installationsabbilder verwenden

39.5.3 Suchabbilder verwenden

39.5.4 Aufzeichnungsabbilder verwenden

39.5.5 Automatische Namensgebung für Clients konfigurieren

39.5.6 Berechtigungen für Abbilder verwalten

39.5.7 Virtuelle Festplatten in WDS verwenden

39.5.8 Treiberpakete in WDS verwenden

39.6 Volumenaktivierungsdienste nutzen

39.7 Zusammenfassung

Kapitel 40 Windows PowerShell

40.1 PowerShell 7 für Windows, macOS und Linux

40.1.1 Kompatibilität der PowerShell 7 mit PowerShell 5.x

40.1.2 PowerShell 7 installieren

40.1.3 Pipelines mit der PowerShell 7 und weitere neue Funktionen

40.2 Wissenswertes zur PowerShell in Windows Server 2022

40.2.1 Einstieg in die PowerShell und Eingabeaufforderung

40.3 PowerShell und PowerShell ISE – Eine Einführung

40.3.1 Mit der PowerShell ISE effizient arbeiten

40.3.2 Einstieg in die PowerShell

40.3.3 Die PowerShell über das Netzwerk nutzen

40.4 Die grundsätzliche Funktionsweise der PowerShell

40.4.1 Einstieg in die Befehle der PowerShell

40.4.2 Patches und Datensicherungen verwalten

40.4.3 Registry und Co. mit der PowerShell verwalten

40.4.4 Die PowerShell-Laufwerke verwenden

40.4.5 Skripts mit der PowerShell erstellen

40.5 Mit PowerShell Desired State Configuration Windows-Server absichern

40.5.1 MOF-Dateien für DSC erstellen und umsetzen

40.5.2 MOF-Dateien erweitern

40.6 Windows PowerShell zur Administration verwenden

40.6.1 PowerShell Direct – Virtuelle Betriebssysteme steuern

40.6.2 Software im Netzwerk verteilen

40.6.3 Software mit Chocolatey installieren und aktuell halten

- 40.6.4 Chocolatey installieren, aktualisieren und nutzen
- 40.6.5 Software mit der ChocolateyGUI installieren
- 40.6.6 Grundlagen zur Verwaltung von Servern mit der PowerShell
- 40.6.7 Mit Variablen arbeiten
- 40.6.8 Systemprozesse verwalten
- 40.6.9 Dateien und Objekte kopieren, löschen und verwalten
- 40.6.10 Dienste in der PowerShell und Befehlszeile steuern
- 40.6.11 Aus der PowerShell E-Mails schreiben
- 40.6.12 Windows-Firewall in der PowerShell steuern
  - 40.7 PowerShell Web Access
    - 40.7.1 Installieren von PowerShell Web Access
    - 40.7.2 Konfigurieren des Gateways für PowerShell Web Access
    - 40.7.3 Konfigurieren der Berechtigungen für PowerShell Web Access
  - 40.8 Eingabeaufforderung verwenden
  - 40.9 Batchdateien für Administratoren
    - 40.9.1 Grundlagen zu Batchdateien
    - 40.9.2 Netzwerkverwaltung in der Befehlszeile
    - 40.9.3 Sprungmarken und Warte-Befehle
    - 40.9.4 Wenn/Dann-Abfragen nutzen
    - 40.9.5 Informationen zum lokalen Server abrufen
    - 40.9.6 Schleifen und Variablen
      - 40.10 WMI-Abfragen nutzen
      - 40.11 Zusammenfassung

## **Index**

## 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 verzeichnishaftige 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
<span style="font-size: 1.2em;">v</span> ✓ Webserver (IIS)	8 von 43 installiert
<span style="font-size: 1.2em;">v</span> ✓ FTP-Server	0 von 2 installiert
<span style="font-size: 1.2em;">v</span> ✓ FTP-Dienst	Verfügbar
<span style="font-size: 1.2em;">v</span> ✓ FTP-Erweiterbarkeit	Verfügbar
<span style="font-size: 1.2em;">&gt;</span> ✓ Verwaltungsprogramme	1 von 7 installiert
<span style="font-size: 1.2em;">v</span> ✓ Webserver	7 von 34 installiert
<span style="font-size: 1.2em;">&gt;</span> ✓ Allgemeine HTTP-Features	4 von 6 installiert
<span style="font-size: 1.2em;">&gt;</span> ✓ Anwendungsentwicklung	0 von 11 installiert
<span style="font-size: 1.2em;">&gt;</span> ✓ Leistung	1 von 2 installiert
<span style="font-size: 1.2em;">&gt;</span> ✓ Sicherheit	1 von 9 installiert
<span style="font-size: 1.2em;">&gt;</span> ✓ 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.

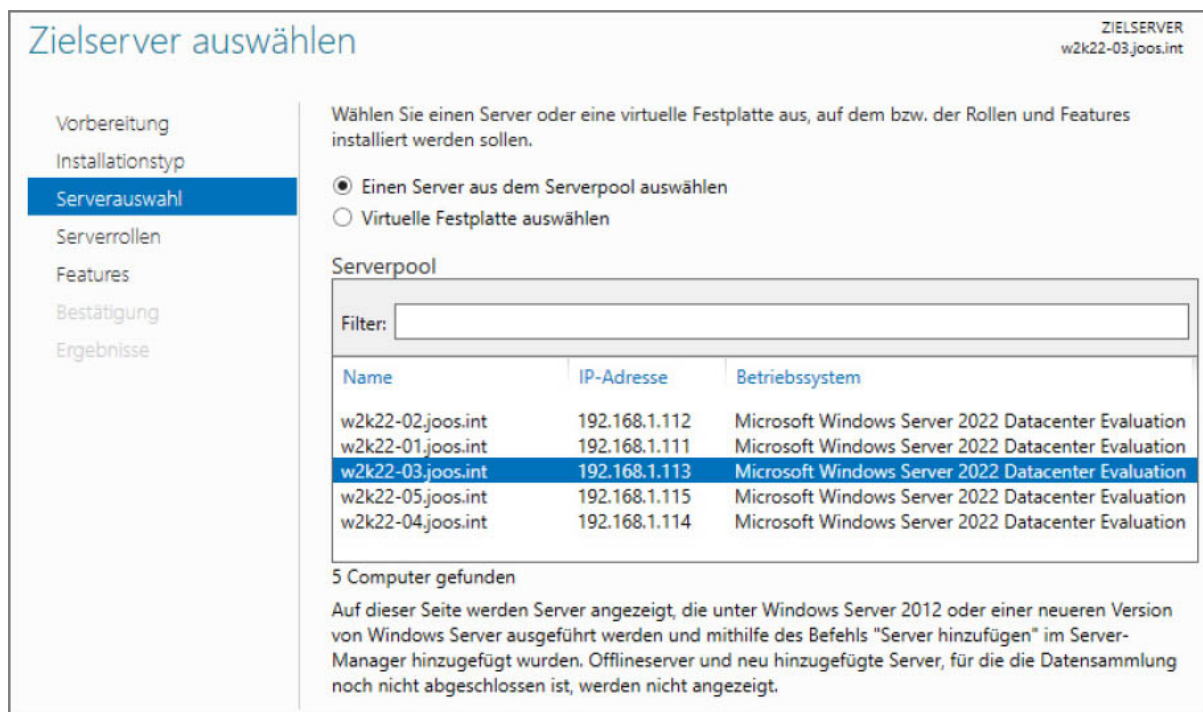
**Rollenbasierte oder featurebasierte Installation**  
 Konfigurieren Sie einen einzelnen Server, indem Sie Rollen, Rollendienste und Features hinzufügen.

**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 Zielsever 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 angebunden und online sind. Aus diesen Servern können Sie den Zielsever 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.

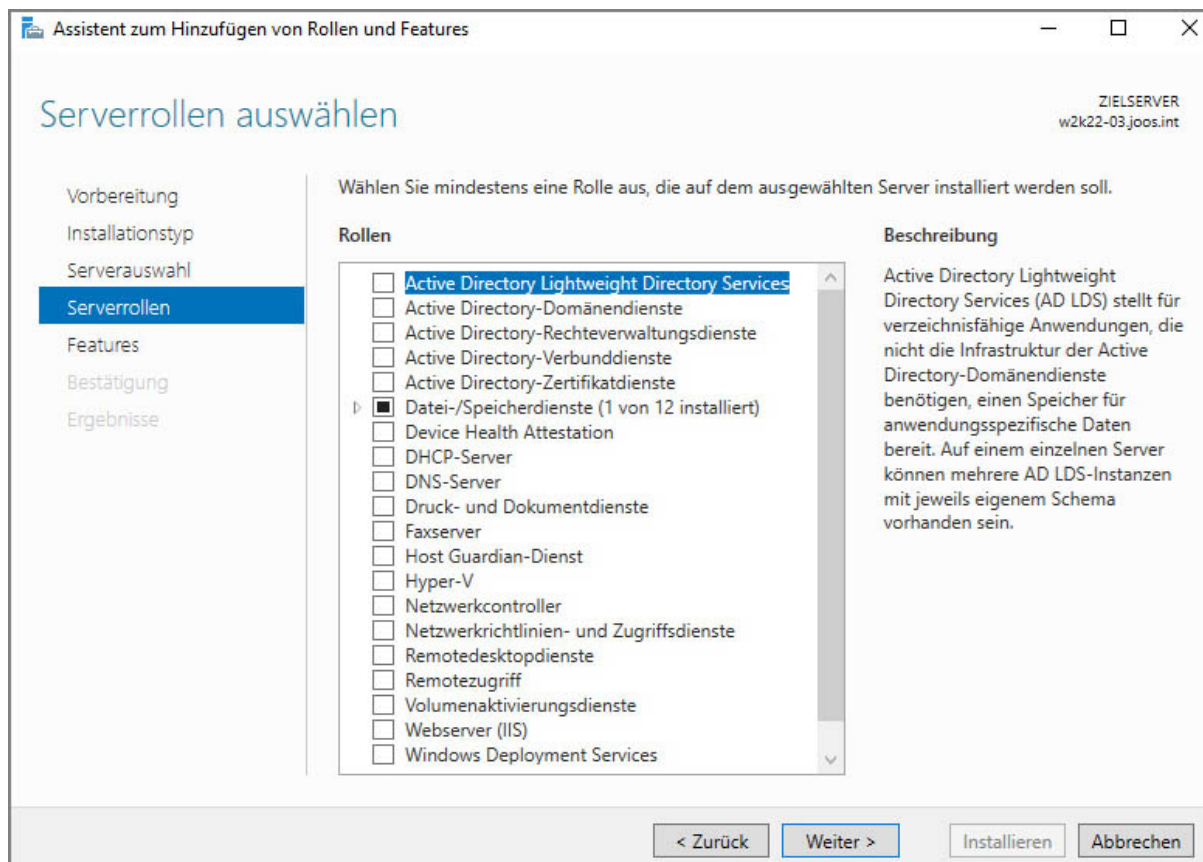


Abb. 4.5 Auswählen der zu installierenden Serverrollen in Windows Server 2022

- **Active Directory-Verbunddienste (Active Directory Federation Services, AD FS)** – Mit den AD FS 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, Datendeduplizierung 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-Sicherheitserweiterungen (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

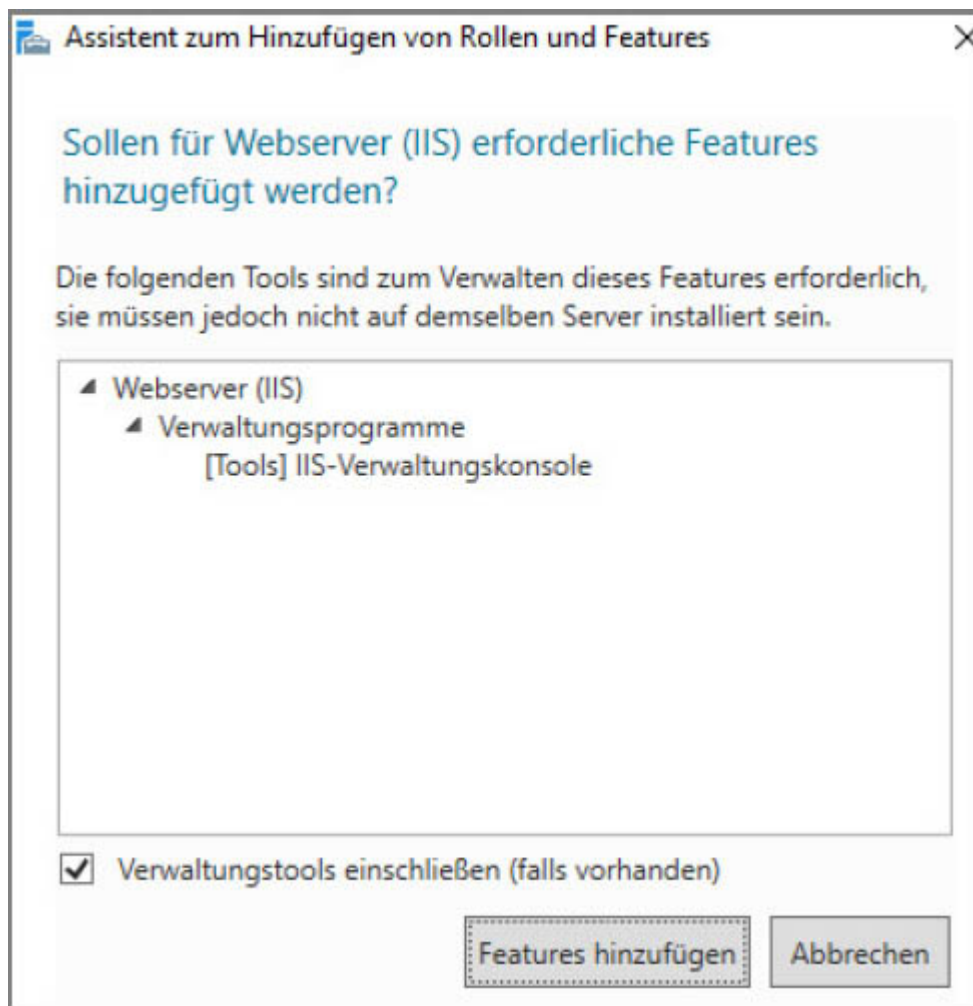
Server (Druckserver). Die Drucker können an diesen Server auch per LAN angeschlossen werden. Außerdem können Sie mit dieser Rolle Scanner im Netzwerk bereitstellen. Dokumente lassen sich durch Installation dieser Rolle an SharePoint-Webseiten weiterleiten. Außerdem verwalten Sie mit der Rolle auch andere 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 Directory 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 2012/2012 R2 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-Netzentsperrung 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 Netzwerkkadappter 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 Remotedesktop-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 Problembehandlung 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 Gruppenrichtlinienverwaltungskonsolle (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 Ausdrücke 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-Betriebssystemen 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 Nachrichtenwendungen und vieles mehr.

- **Microsoft Defender Antivirus** – Standardvirenschanner 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.
- **Speicherreplikat** – 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.

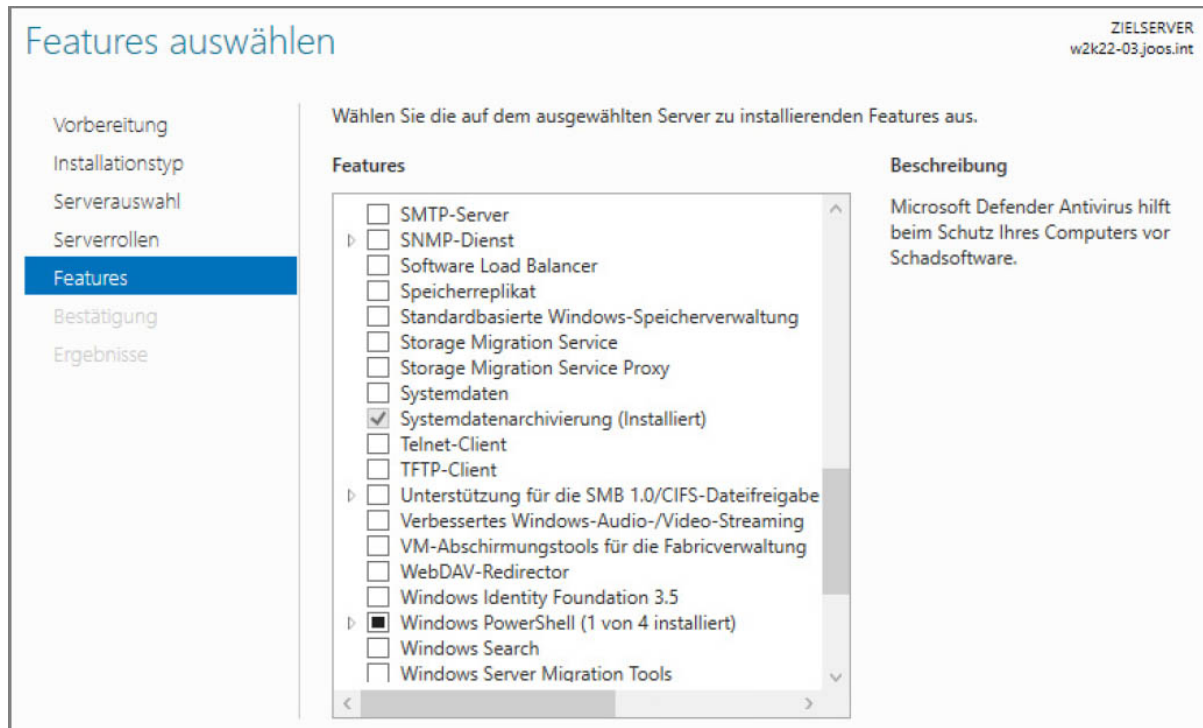


Abb. 4.7 Installieren von Features/Funktionen über den Server-Manager

- **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.

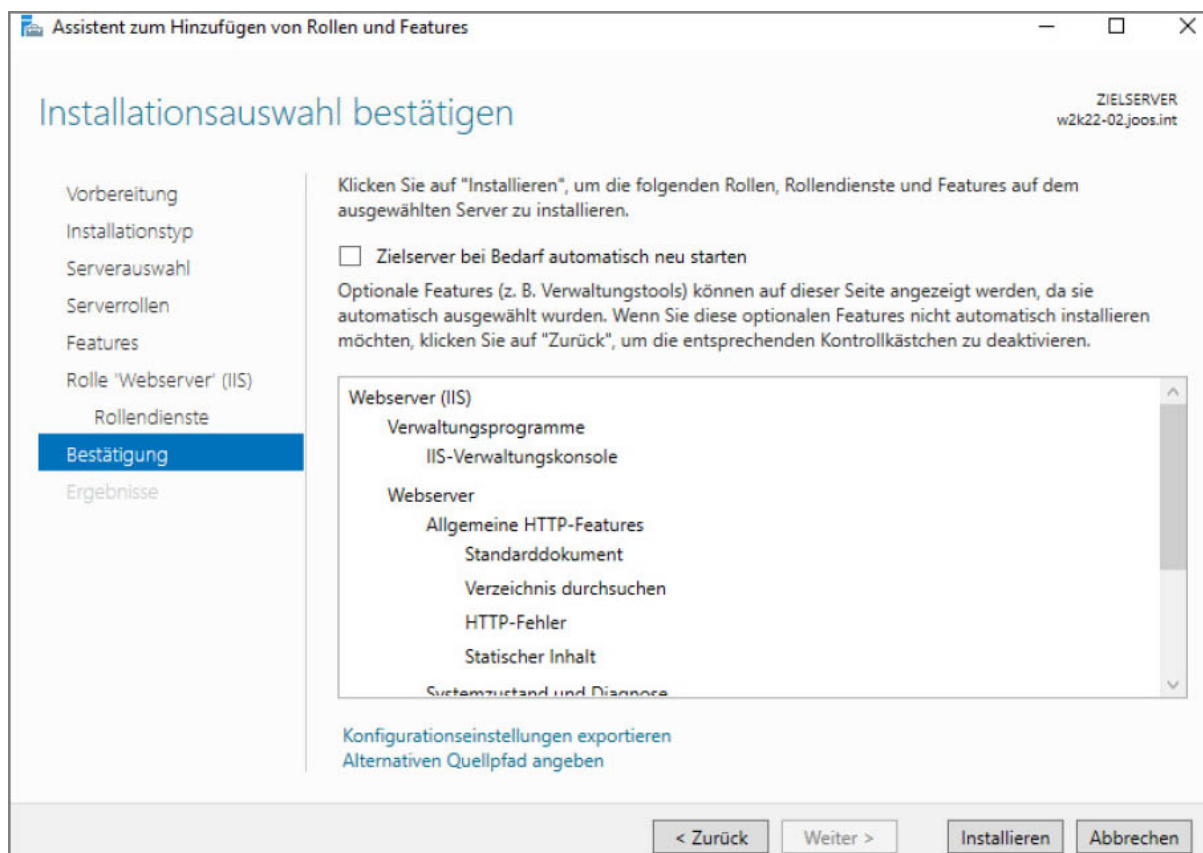
- **Windows PowerShell** – Hierbei handelt es sich um die neue PowerShell und zusätzliche Werkzeuge für die PowerShell. Sie können an dieser Stelle noch die Unterstützung der PowerShell 2.0 aktivieren und PowerShell Web Access. Installieren Sie das Feature *PowerShell Web Access* über den Server-Manager 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 Remotedesktopservern, 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.
- **WINS-Server** – Funktioniert die Namensauflösung per DNS zum Beispiel nicht mehr, kann der interne Replikationsdienst von Active Directory auf WINS zurückgreifen. WINS dient hauptsächlich der Namensauflösung von NetBIOS-Namen.
- **WLAN-Dienst** – Möchten Sie einen Server über ein Drahtlosnetzwerk in das Netzwerk einbinden, müssen Sie diese Funktion installieren. In diesem Fall kann parallel zu einer kabelgebundenen Netzwerkanbindung der Server auch über ein Drahtlosnetzwerk angebunden werden. Der WLAN-AutoConfig-Dienst steuert in diesem Fall den Zugriff des Servers auf das Netzwerk.
- **WoW64** – Das Feature unterstützt die Ausführung von 32-Bit-Anwendungen.
- **XPS-Viewer** – Der Viewer ermöglicht das Lesen von XPS-Dokumenten auf dem Server.

Rollen und Features lassen sich über den jeweiligen Assistenten hinzufügen, verwalten und wieder entfernen. In Windows Server 2022 können Sie mehrere Rollen und Features gleichzeitig installieren, indem Sie diese markieren und den Assistenten zur Installation fortsetzen.

## 4.1.3 Installation von Rollen und Features abschließen

Haben Sie im Assistenten ausgewählt, welche Rollen und Features Sie installieren wollen, bestätigen Sie auf der letzten Seite die eigentliche Installation. Über den Link *Konfigurationseinstellungen exportieren* erstellen Sie eine XML-Datei, über die Sie die Installation der ausgewählten Rollen und Features automatisieren können. Wir zeigen Ihnen in den folgenden Abschnitten, wie Sie mit der XML-Datei automatisiert Rollen, Rollendienste und Features installieren.



**Abb. 4.8** Fertigstellen der Installation von Server-Rollen

Der Link *Alternativen Quellpfad angeben* ermöglicht die Angabe eines anderen Speicherorts der Installationsdateien. Um Speicherplatz zu sparen, sind nicht alle notwendigen Binärdateien für Windows Server 2022 bereits auf dem Server vorhanden. Fehlen dem Server Binärdateien, zeigt das der Server-Manager an und Sie müssen einen alternativen Speicherort angeben.

Sie können an dieser Stelle auch die Option aktivieren, dass der Server automatisch neu starten soll, wenn dies die Installation der Rolle oder eines ausgewähltes Feature verlangt. Ein Beispiel dafür ist die Installation von Hyper-V auf einem Server.

Sie müssen das Fenster während der Installation der Rolle oder des Features nicht geöffnet lassen, sondern können es schließen. Auf diesem Weg können Sie die Installation auf mehreren Servern starten. Wollen Sie zum

Installationsfenster zurückkehren, klicken Sie im Server-Manager oben rechts auf das Benachrichtigungssymbol.

## 4.2 Rollen in der PowerShell installieren

In diesem Abschnitt zeigen wir Ihnen, wie Sie Serverrollen und Features in der PowerShell oder automatisiert installieren. Sie können dabei auch über den Assistenten zur Installation von Serverrollen eine XML-Datei erstellen und diese mit der PowerShell auf anderen Servern zur Installation von Rollen nutzen.

### 4.2.1 Serverrollen und Features in der PowerShell verwalten

Die Installation und Verwaltung von Serverrollen findet hauptsächlich über den Server-Manager oder das Windows Admin Center statt. Neben der grafischen Oberfläche für dieses Tool gibt es die Möglichkeit, Features auch in der PowerShell zu installieren.

Interessant sind vor allem die Cmdlets *Install-WindowsFeature*, *Get-WindowsFeature* und *Remove-WindowsFeature*. Und auch das Cmdlet *Uninstall-WindowsFeature* ist in dieser Hinsicht hilfreich. Hilfe zu den Cmdlets erhalten Sie wie immer über *help <Befehlsname> -detailed*.

Mit dem Befehl *Get-WindowsFeature Hyper-V\** zeigen Sie zum Beispiel an, ob die Rolle und die Verwaltungstools bereits installiert sind. In Windows Server 2022 können Sie mit *-computername* die Installation auch auf Remoteservern im Netzwerk überprüfen. Um Hyper-V oder die Verwaltungstools zu installieren, verwenden Sie das Cmdlet *Install-WindowsFeature*.

Mit *Install-WindowsFeature Hyper-V* installieren Sie die Serverrolle, mit der Option *-Include-ManagementTools* inklusive der Verwaltungstools. Soll der Server gleich noch automatisch neu starten, verwenden Sie zusätzlich die Option *-restart*. Die Verwaltungstools alleine installieren Sie mit *Install-WindowsFeature Hyper-V-Tools*.

Die Installation von Features erfolgt dann mit dem Befehl *Add-WindowsFeature <Kommagetrennte Liste>*, zum Beispiel mit *Add-WindowsFeature RSAT-AD-PowerShell,RSATAD-AdminCenter*, die Installation der Active Directory-

Verwaltungstools. Mit den Cmdlets installieren Sie auch Rollen und Features auf Core-Servern.

## 4.2.2 Unbeaufsichtigte Installation von Rollen und Features

Neben der beschriebenen Möglichkeit, Rollen und Features über die PowerShell zu installieren, indem Sie den Namen der Rolle und des Features angeben, können Sie in der PowerShell auch die XML-Steuerungsdatei verwenden, die Sie im Assistenten zum Installieren von neuen Rollen im letzten Fenster speichern können.

Um auf einem anderen Server die gleichen Rollen und Features zu installieren, verwenden Sie PowerShell und geben die XML-Datei mit. Dabei verwenden Sie das Cmdlet *Install-WindowsFeature* mit der Option *-ConfigurationFilePath*, zum Beispiel *Install-Windows-Feature -ConfigurationFilePath C:\Daten\iis.xml*.

## 4.3 Rollen und Features mit DISM installieren

Deployment Image Servicing and Management (Dism) bietet zur besseren Automatisierung der Einrichtung und Installation von Serverrollen auch für Core-Server mit Windows Server 2022 effiziente Möglichkeiten. Mit Dism lassen sich schnell und einfach wichtige Serverrollen installieren, auch skriptbasiert.

Verschiedene Verwaltungsaufgaben lassen sich mit dem Tool wesentlich schneller durchführen als in der grafischen Oberfläche. Wiederkehrende Aufgaben lassen sich mit Dism auch automatisieren. Mit Dism installieren Sie Serverrollen und Features.

Neben der Möglichkeit, Rollen zu installieren, lassen sich mit Dism auch Windows-Images einlesen. Verwenden Sie die Option */Online*, bearbeitet Dism das aktuell gestartete Betriebssystem. Um ein WIM-Image zu laden, ist der Befehl *dism /Mount-Wim /MountDir:<Ordner> /WimFile:<WIM-Datei> /Index:1* geeignet. Der Ordner zum Mounten muss vorhanden und leer sein.

Es lassen sich auch mehrere Images einlesen. Der Befehl ist dann der gleiche, aber der Wert für */Index* muss erhöht werden. Der Befehl *dism /Get-MountedWimInfo* zeigt alle gemounteten Images an. Gemountete Images lassen

sich mit dem Befehl *dism /Unmount-Wim /Mount-Dir:<Ordner> /<Option>* wieder unmounten. Als Option lassen sich mit */Commit* Änderungen speichern und mit */Discard* Änderungen ohne Speichern verwerfen. Mit der Option */Add-Driver /Driver:<INF-Datei>* lassen sich Treiber in Images integrieren.

### 4.3.1 Webserver mit Dism.exe remote verwalten und Serverrollen auf Core-Servern installieren

Wollen Sie die Internetinformationsdienste (IIS) auf einem Core-Server auch über das Netzwerk verwalten, ist die Vorgehensweise folgende:

1. Installieren der IIS-Verwaltung auf dem Core-Server mit *dism /Online /Enable-Feature /FeatureName:IIS-ManagementService*.
2. Aktivieren der Remoteverwaltung, indem Sie den Wert *1* beim Registrywert *EnableRemoteManagement* im Schlüssel *HKLM\SOFTWARE\Microsoft\WebManagement\Server* setzen.
3. Mit *Net start wmsvc* den Dienst für die Remoteverwaltung starten.

Eine Möglichkeit, DNS auf einem Core-Server zu installieren, ist der Befehl *dism /Online /Enable-Feature /FeatureName:DNS-Server-Core-Role*. Mit dem Befehl *dism /Online /Disable-Feature /FeatureName:DNS-Server-Core-Role* lässt sich die Rolle wieder entfernen.

Die Installation der DHCP-Serverrolle läuft ähnlich zur Installation eines DNS-Servers ab:

```
dism /Online /Enable-Feature /FeatureName:DHCPServerCore
```

Die Deinstallation erfolgt mit

```
dism /Online /Disable-Feature /FeatureName:DHCPServerCore
```

Zusätzlich muss der Systemdienst für DHCP noch gestartet werden:

```
sc config dhcpserver start= auto
```

```
net start dhcpserver
```

Weitere Serverrollen sind zum Beispiel:

- **Dateireplikationsdienst (File Replication Service, FRS)** – *dism /Online /Enable-Feature /FeatureName:FRS-Infrastructure*

- **Distributed File System Replication** – *dism /Online /Enable-Feature /FeatureName:DFSN-Server*
- **Network File System** – *dism /Online /Enable-Feature /FeatureName:ServerForNFS-Base* und *dism /Online /Enable-Feature /FeatureName:ClientForNFS-Base*
- **Standardrolle eines Druckservers** – *dism /Online /Enable-Feature /FeatureName:Printing-ServerCore-Role-WOW64*
- **Line Printer Daemon (LPD)** – *dism /Online /Enable-Feature /FeatureName:Printing-LPD-Print-Service*
- **Active Directory Lightweight Directory Services (AD LDS)** – *dism /Online /Enable-Feature /FeatureName:DirectoryServices-ADAM-ServerCore*
- **Active Directory-Zertifikatdienste** – *dism /Online /Enable-Feature /FeatureName:CertificateServices*

Auch diese Rollen lassen sich mit der Option *Disable-Feature* beim Einsatz von Dism deinstallieren.

## 4.4 Serverrollen mit dem Best Practices Analyzer überprüfen

Mit Windows Server 2022 erweitert Microsoft die automatische Überprüfung der Serverrollen durch Best Practices Analyzer. Diese gehören zu den Bordmitteln in Windows Server 2022 und stehen im Server-Manager auch für die Überprüfung von Serverrollen über das Netzwerk zur Verfügung. Nahezu alle Serverrollen lassen sich dadurch überprüfen und das Ergebnis zentral anzeigen.

Installieren Sie Serverrollen und konfigurieren diese, gibt es oft fehlerhafte Konfigurationen. Dazu hat Microsoft die Best Practices Analyzer entwickelt, die regelmäßig die Server auf Konfigurationsprobleme überprüfen und entsprechende Maßnahmen zur Beseitigung ausführen.

Die Ergebnisse dieser automatischen Überprüfung werden direkt in den einzelnen Kacheln der verschiedenen Serverdienste im Dashboard integriert.

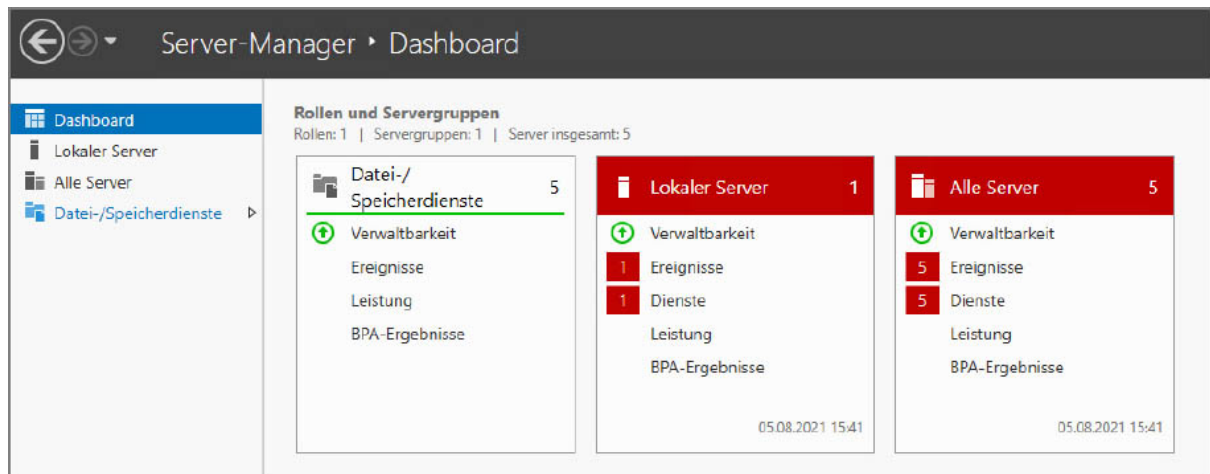


Abb. 4.9 Best Practices Analyzer in Windows Server 2022

## 4.4.1 Überprüfen von Servern über das Netzwerk

In Windows Server 2022 lassen sich Server über den Server-Manager vollständig über das Netzwerk verwalten. Über *Verwalten/Server hinzufügen* lassen sich alle Windows Server 2022-Computer im Netzwerk zum Server-Manager hinzufügen. Die Server ordnet der Server-Manager dann nach ihren Rollen und erstellt automatisch Servergruppen.

Im Dashboard des Server-Managers sind für alle Serverrollen die BPA-Ergebnisse aller Server zu sehen. Allerdings muss dazu zunächst ein Scan der Rechner im Netzwerk gestartet werden. Klicken Sie in der Ansicht *Alle Server* auf einen Server im oberen Bereich, sehen Sie unten wichtige Fehlermeldungen der Ereignisanzeige (siehe Kapitel 3).

Im oberen Bereich ist außerdem zu erkennen, ob die entsprechenden Server online sind und ob Windows Server 2022 aktiviert ist. Diese Informationen haben nichts mit dem BPA zu tun, ergänzen aber dessen Informationen.

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, die neuen 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. Die Leistungsindikatoren haben aber nur am Rande etwas mit dem BPA zu tun. Die eigentliche Aktivierung erfolgt nachträglich.

**SERVER**  
 Alle Server | 5 insgesamt

Filter

Servername	IPv4-Adresse	Verwaltbarkeit	Letztes Update	Windows-Aktivierung
W2K22-01	192.168.1.111	Online	05.08.2021 15:51:34	00455-50000-00001-AA446 (Aktiviert)
W2K22-02	192.168.1.112	Online	05.08.2021 15:51:35	00455-50000-00001-AA189 (Aktiviert)
W2K22-03	192.168.1.113	Online	05.08.2021 15:51:35	00455-50000-00001-AA540 (Aktiviert)
W2K22-04	192.168.1.114	Online	05.08.2021 15:51:35	00455-50000-00001-AA214 (Aktiviert)
W2K22-05	192.168.1.115	Online	05.08.2021 15:51:42	00455-50000-00001-AA763 (Aktiviert)

**EREIGNISSE**  
 Alle Ereignisse | 10 insgesamt

Filter

Servername	ID	Schweregrad	Quelle	Protokoll	Datum und Uhrzeit
W2K22-01	10016	Warnung	Microsoft-Windows-DistributedCOM	System	05.08.2021 13:06:40
W2K22-01	10016	Warnung	Microsoft-Windows-DistributedCOM	System	05.08.2021 11:30:30
W2K22-01	1076	Warnung	User32	System	05.08.2021 10:23:51
W2K22-01	10016	Warnung	Microsoft-Windows-DistributedCOM	System	05.08.2021 10:05:25
W2K22-01	6038	Warnung	Microsoft-Windows-LSA	System	05.08.2021 10:05:07
W2K22-01	6006	Warnung	Microsoft-Windows-Winlogon	Anwendung	05.08.2021 09:55:12
W2K22-01	6005	Warnung	Microsoft-Windows-Winlogon	Anwendung	05.08.2021 09:54:12

**DIENSTE**  
 Alle Dienste | 208 insgesamt

Filter

Servername	Anzeigenname	Dienstname	Status	Starttyp
W2K22-01	WinHTTP-Web Proxy Auto-Discovery-Dienst	WinHttpAutoProxySvc	Wird ausgeführt	Manuell
W2K22-01	Diagnosesystemhost	WdiSystemHost	Beendet	Manuell
W2K22-01	Geräteinstallations-Manager	DsmSvc	Beendet	Manuell (Ausgelöst)
W2K22-01	NLA (Network Location Awareness)	NlaSvc	Wird ausgeführt	Automatisch
W2K22-01	Diagnoserichtliniendienst	DPS	Wird ausgeführt	Automatisch (verzögerter Start)
W2K22-01	UPnP-Gerätehost	upnphost	Beendet	Deaktiviert
W2K22-01	StateRepository-Dienst	StateRepository	Wird ausgeführt	Automatisch

Abb. 4.10 Überprüfen der Funktionalität von Servern im Server-Manager

## 4.4.2 BPA in der PowerShell starten

Am schnellsten starten und aktivieren Sie den BPA für Serverrollen durch Eingabe des Befehls `Get-BPAModel | Invoke-BpaModel` in der PowerShell. Dieser Befehl versucht auch die Aktivierung von BPAs für Serverrollen, die im Netzwerk nicht installiert sind. Das bringt zwar einige Fehlermeldungen auf den Schirm, stellt aber sicher, dass alle BPAs gestartet werden.

Weitere Cmdlets für die PowerShell sind *Get-BPAResult* und *Set-BPAResult*. Diese Cmdlets zeigen Ergebnisse an oder blenden sie aus. Zur Analyse verwenden Sie aber besser den Server-Manager. Auch hier können Sie auf Windows 10/11 setzen. Der Vorteil ist, dass mit der Option *-ComputerName* eine Konfiguration und Abfrage der Ergebnisse über das Netzwerk hinweg erfolgen kann. Das funktioniert ebenfalls über die PowerShell.

Neben der PowerShell lässt sich der BPA für einzelne Serverrollen im Server-Manager starten. Dazu öffnen Sie den Server-Manager und klicken auf die Serverrolle, die überprüft werden soll. Durch einen Klick auf *Server* sind die Server mit dieser Rolle im Netzwerk zu sehen.

Hier sind allerdings nur die Server zu sehen, die Sie über *Verwalten/Server hinzufügen* dem lokalen Server-Manager hinzugefügt haben. Im unteren Bereich des Server-Managers findet sich der Bereich *Best Practices Analyzer*. Durch einen Klick auf *Aufgaben/BPA-Überprüfung starten* beginnt der Test der Serverrolle. Zunächst müssen Sie aber den Server auswählen, den der BPA überprüfen soll.

Den gleichen Assistenten finden Sie im Server-Manager über *Alle Server* im unteren Bereich von *Best Practices Analyzer*. Auch hierüber lassen sich alle Server, die an den lokalen Server-Manager angebunden sind, überprüfen.

Diese Überprüfung lässt sich ebenfalls auf Windows 10/11-Computern starten. Dazu installieren Sie die Remoteserver-Verwaltungstools für Windows 10/11 auf dem Rechner und binden über den Server-Manager die entsprechenden Server an.

Wollen Sie eine Liste der vorhandenen Überprüfungsmöglichkeiten anzeigen, lassen Sie sich die Informationen als Liste anzeigen. Hier brauchen Sie die ID eines BPA-Modells, dessen Ergebnis Sie später auslesen wollen. Dazu verwenden Sie das Cmdlet *Get-BpaModel | Format-List Name,Id*.

Wollen Sie nur für eine bestimmte Rolle einen Scan-Vorgang starten, rufen Sie wieder zunächst die ID des entsprechenden Modells ab. Danach starten Sie den oder die Tests mit dem folgenden Befehl:

```
Invoke-BPAModel -modelId  
Microsoft/Windows/DNSServer,Microsoft/Windows/FileServices
```

Sie müssen die ID immer als kompletten Pfad angeben, den Sie mit *Get-BPAModel* auslesen. Hyper-V hat zum Beispiel die ID *Microsoft/Windows/Hyper-V*. Sie können auch einen einzelnen Befehl verwenden, um das BPA-Modell auszulesen, und gleich den Scanvorgang zu starten:

```
Get-BPAModel <ID> | Invoke-BPAModel
```

Geben Sie keine ID an, werden alle Rollen gescannt, wie bereits weiter oben gezeigt. Weitere Cmdlets für die PowerShell sind *Get-BPAResult* und *Set-BPAResult*. Diese Cmdlets zeigen Ergebnisse an oder blenden sie aus. Wollen Sie zum Beispiel die Ergebnisse einer bestimmten BPA-Prüfung anzeigen, brauchen Sie zunächst die ID. Diese lesen Sie mit dem oben gezeigten Befehl aus. Danach können Sie die Ergebnisse zum Beispiel mit folgendem Befehl auslesen. Dabei können Sie gezielt nach dem Text *Fehler* suchen lassen:

```
Get-BpaResult -ModelId Microsoft/Windows/DirectoryServices | Where-Object Severity -eq "Fehler" | Format-List Title
```

Um alle Ergebnisse von bestimmten Serverrollen (BPA-Models) anzuzeigen, können Sie zum Beispiel folgenden Befehl verwenden:

```
Get-BPAResult Microsoft/Windows/DNSServer,Microsoft/Windows/FileServices
```

Sie können einzelne Ergebnisse von der Anzeige ausblenden. Das funktioniert generell ähnlich wie die gefilterte Anzeige. Dazu lassen Sie sich die Anzeige filtern und legen mit dem Cmdlet *Set-BPAResult* fest, dass diese Ergebnisse ausgeblendet werden:

```
Get-BPAResult -modelId <model ID> | Where { $_.<Field Name> -eq "Value" } | Set-BPAResult -Exclude $true
```

Um zum Beispiel unwichtige Informationen für die Dateidienste auszublenden, verwenden Sie den folgenden Befehl:

```
Get-BPAResult -Microsoft/Windows/FileServices | Where { $_.Severity -eq "Information" } | Set-BPAResult -Exclude $true
```

Viele Serverrollen verfügen über Rollendienste. Diese lassen sich ebenfalls auslesen. Ein Beispiel ist der File Server Resource Manager (FSRM) der Serverrolle *Dateidienste*. Dessen Ergebnisse lassen sich zum Beispiel folgendermaßen auslesen:

```
Get-BPAResult Microsoft/Windows/FileServices -SubmodelID FSRM
```

Ausgeblendete Informationen lassen sich wieder einblenden. Dazu steht der entsprechende Bereich im Server-Manager bei *Best Practices Analyzer* zur Verfügung. Natürlich lassen sich ausgeblendete Ergebnisse auch über die PowerShell wieder einblenden. Die Syntax dazu entspricht dem Ausblenden von Ergebnissen, die Option *-Exclude* wird dabei aber auf *\$false* gesetzt:

```
Get-BPAResult -modelId <model Id> | Where { $_.<Field Name> -eq "Value" } | Set-BPAResult -Exclude $false
```

Um die Informationen der Dateidienste wieder einzublenden, wird folgender Befehl verwendet:

```
Get-BPAResult -Microsoft/Windows/FileServices | Where { $_.Severity -eq "Information"} | Set-BPAResult -Exclude $false
```

Zur Analyse verwenden Sie aber besser den Server-Manager. Allerdings bietet auch die PowerShell Informationen, die sich wiederum mit Skripts auslesen lassen. Mit der Option `-ComputerName` kann eine Konfiguration und Abfrage der Ergebnisse über das Netzwerk hinweg erfolgen. Das funktioniert ebenfalls über die PowerShell.

### 4.4.3 Ergebnisse exportieren

Um BPA-Ergebnisse zu exportieren, zum Beispiel als HTML-Datei, können Sie ebenfalls die PowerShell verwenden. Die Syntax dazu sieht folgendermaßen aus:

```
Get-BPAResult <model ID> | convertTo-Html | Set-Content <path>
```

Als Beispiel können Sie die Informationen der Dateidienste in eine HTML-Datei exportieren:

```
Get-BPAResult Microsoft/Windows/FileServices | convertTo-Html | Set-Content C:\BPAResults\FileServices.htm
```

Die Ergebnisse lassen sich auch als CSV-Datei exportieren:

```
Get-BPAResult Microsoft/Windows/FileServices | Export-CSV C:\BPAResults\FileServices.txt
```

Die exportierten Ergebnisse lassen sich natürlich versenden, sodass IT-Profis von unterwegs auf Daten des BPA zugreifen können. Die exportierten Dateien lassen sich von externen Programmen einlesen, aber auch in Excel oder normalen Webbrowsern. Dadurch können BPA-Ergebnisse überall ausgewertet werden. Externe Hilfe kann hinzugezogen werden, indem externe Spezialisten Zugriff auf die Daten des BPA erhalten.

### 4.4.4 BPA für Hyper-V nutzen

Wie bereits erwähnt, ist der BPA für Hyper-V besonders interessant, da hier nicht nur der lokale Server optimiert werden kann, sondern auch die virtuellen Server davon profitieren. Die virtuellen Netzwerk-Switches lassen sich durch den BPA scannen. Um einen Scanvorgang für Hyper-V zu starten, verwenden Sie:

*Invoke-BpaModel -Modelld Microsoft/Windows/Hyper-V*

Die Ergebnisse des Scan-Vorgangs können in einen bestimmten Pfad umgeleitet werden. Sie müssen den Pfad aber vorher anlegen:

```
Invoke-BpaModel -Modelld Microsoft/Windows/Hyper-V -RepositoryPath C:\temp\BPA
```

Wollen Sie einen Scanvorgang für einen Server im Netzwerk starten, verwenden Sie zum Beispiel:

```
Invoke-BpaModel -ComputerName dl20 -Modelld Microsoft/Windows/Hyper-V
```

Im angegebenen Pfad werden die Ergebnisdateien nach Serverrolle und Server in Unterverzeichnisse sortiert. Die Ergebnisse liegen als XML-Dateien vor. Diese lassen sich im Browser auslesen oder mit eigenen Programmen, die auf die entsprechenden Daten direkt zugreifen können. Scanergebnisse eines Servers werden auf dem lokalen Server gespeichert, auch dann, wenn Sie einen Hyper-V-Host über das Netzwerk scannen lassen.

Wollen Sie in der PowerShell alle Scanergebnisse für Hyper-V anzeigen, verwenden Sie:

```
Get-BpaResult -Modelld Microsoft/Windows/Hyper-V
```

Haben Sie die Ergebnisse in einem Verzeichnis gespeichert, verwenden Sie:

```
Get-BpaResult -Modelld Microsoft/Windows/Hyper-V -RepositoryPath C:\temp\BPA
```

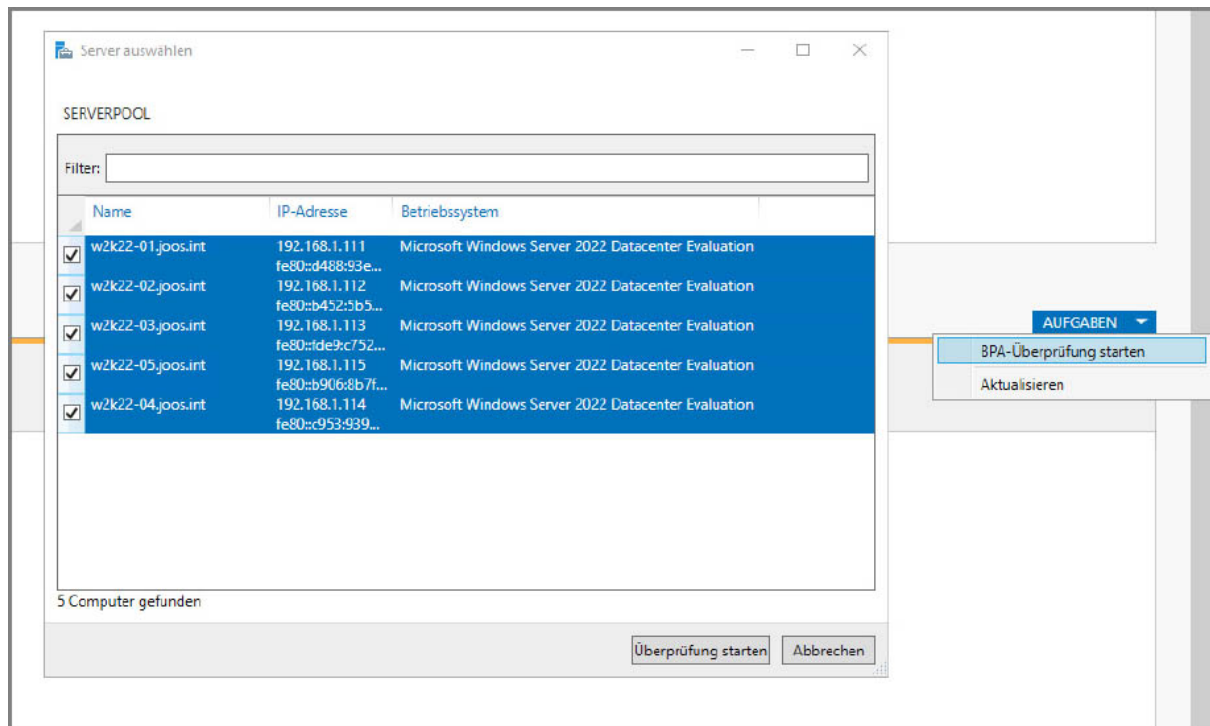
Um die Ergebnisse in der PowerShell in eine HTML-Datei zu exportieren, verwenden Sie:

```
Get-BpaResult -Modelld Microsoft/Windows/Hyper-V | ConvertTo-Html | Out-File C:\temp\BPA\results.htm
```

## **4.4.5 BPA auswerten**

Wenn Sie die BPA-Überprüfung gestartet haben, stehen auf den einzelnen Kacheln im Server-Manager die Ergebnisse zur Verfügung. Diese sind sofort ersichtlich und lassen sich durch einen Klick auf die Kachel öffnen. Klicken Sie auf das Ergebnis der BPA-Überprüfung, zeigt der Server-Manager die gefundenen Fehler an. Hierüber lassen sich auch alle Fehler von allen Servern im Netzwerk anzeigen.

Über das Kontextmenü eines Ergebnisses lässt sich eine erneute Überprüfung für den entsprechenden Server starten, das Ergebnis ausblenden oder in die Zwischenablage kopieren, zum Beispiel für eine Recherche im Internet.



**Abb. 4.11** Starten der BPA-Überprüfung im Server-Manager

Die BPA-Ergebnisse finden sich aber auch in der Ansicht *Lokaler Server* und *Alle Server* im Bereich *Best Practices Analyzer* unten im Server-Manager. Wenn für eine Serverrolle für einen der Server im Netzwerk ein BPA-Ergebnis angezeigt wird, wechselt die Kachel die Farbe. Auf diese Weise sehen Sie sofort, wenn für einen Server Verbesserungen möglich sind. Durch das Ausschließen eines Ergebnisses lassen sich die einzelnen Meldungen deaktivieren. Über die Ansicht im BPA können Sie bei *Schweregrad*, *Server* und *Kategorien* das Ergebnis filtern lassen.

Zusammenfassend stehen nach einem Scan mit dem BPA den Administratoren über *Aufgaben* im Bereich *Best Practices Analyzer im Server-Manager* starten die Ergebnisse an den verschiedenen Stellen zur Verfügung: in der Ansicht *Lokaler Server* für alle Rollen des lokalen Servers, über *Alle Server* für alle Rollen auf allen Servern und für alle Rollen. Klicken Sie im Server-Manager auf eine Serverrolle, können Sie die Ansicht nach dieser Rolle filtern lassen und erhalten hier auch alle Informationen von allen Servern.

## 4.5 Zusammenfassung

In diesem Kapitel haben Sie erfahren, welche Serverrollen und Features es gibt, was deren Funktion ist und wie diese installiert werden. Sie fanden hier eine Auflistung, welche Serverrollen und Features in Windows Server 2022 zur

Verfügung stehen und wie Sie diese integrieren. Auch die Überprüfung der Serverrollen mit Best Practices Analyzer sowie die Installation und Verwaltung über die PowerShell waren Themen in diesem Kapitel.

Ab den nächsten Kapiteln dieses Buches steigen wir etwas tiefer in die Thematik ein und erläutern Ihnen, wie Sie Windows Server 2022 produktiv einsetzen. Den Anfang macht das folgende Kapitel 5 mit der Verwaltung der Datenträger und des Dateisystems.

# Index

\_msdcs 371, 465

.dll-Datei 1080

.NET 780

.NET Framework 3.5 111

.NET Framework 4.8 111

32-Bit-System 672

512e 221

64-Bit-System 672

80/20-Regel 709

## A

Abbilddatei 250

Abbilder 1094

Ablaufverfolungsregeln 797

Abonnements 1046–1047

Abschottung 109

Abwärtskompatibilität 525

Access Control List (ACL) 537, 592

*siehe auch* Zugriffssteuerungsliste

AccessChk 598

AccessEnum 599

Active Directory 185, 206, 337, 361, 912

Benutzer und Computer 79, 347

Certificate Services 108

Datenbank 286, 343, 501

Datenbank reparieren 503

Diagnose 460

- Diagnostics 483
- Domain Services 107
- Domänen und Vertrauensstellungen 350
- Domänendienste 107
- Federation Services 108
- Installationsmedium 374
- Lightweight Directory Services 330
- Lightweight-Verzeichnisdienste 106
- Papierkorb 411, 521
- Papierkorb, Objekte wiederherstellen 412
- Rechteverwaltungsdienste 107, 330
- Registrierungsrichtlinie 305, 868
- Replikation 460
- Rights Management Services 107
- Schema 350
- Standorte 475
- Standorte und Dienste 450
- Verbunddienste 108, 331, 369, 921
- Verwaltungszentrum 384, 517
- Webdienste 332
- Zertifikatdienste 108, 861, 925
- AD CS 108
- AD DS 107
- AD FS 108, 994
- AD LDS 106
- AD RMS 107, 330, 923
  - Cluster-URL 932
  - Stammcluster 928
- Add-ADDSReadOnlyDomainControllerAccount 376, 434
- Add-ADGroupMember 295
- Add-ClusterFileServerRole 324
- Add-ClusterGroup 324
- Add-ClusterGroupSetDependency 961
- Add-ClusterNode 324, 958

Add-ClusterPrintServerRole 324  
Add-ClusterResource 324  
Add-ClusterVirtualMachineRole 324  
Add-Computer 79, 207  
Add-Content 1133  
Add-HgsAttestationHostGroup 295  
Add-KdsRootKey 408  
Add-MpPreference 880  
Add-NetNatStaticMapping 243  
Add-PhysicalDisk 166  
Add-Printer 675  
Add-PrinterDriver 675  
Add-PrinterPort 675  
Add-PswaAuthorizationRule 1140–1141  
Add-VMGroupMember 297  
Add-VMHardDiskDrive 173, 244, 274  
Add-VMSwitchTeamMember 241  
Add-VMTPM 293  
Add-WindowsFeature 119, 315, 925  
Add-WsusComputer 1029  
ADFS 331  
    Verwaltung 921  
ADK 1087  
adksetup 1090  
ADLDS 330  
Adminfreigaben 608  
Administration.config 791  
Administrator 516  
adml 559  
ADMX-Dateien 558  
adprep 335, 384  
adreplication 449  
Adresskonflikt 710  
Adressleases 696, 704

Adresspool 696, 709  
ADSI 412  
    Editor 920  
adsiedit.msc 920  
Advanced Format Technology 220  
Affinity 1078  
Aggregated Policies 617  
AirPrint 674  
Aktivierung 60, 1107  
    Hotlines 1093  
Aktualisierung 56–57  
    Intervall 724  
Alias 722  
AllowRemoteRPC 854  
Alterung 724  
AMD Nested Page Table 49  
Anforderung 870  
    Fehler 797  
Anmeldeinformationen 386  
Anmeldeskripts 532  
Anmeldeversuche 485  
Anmeldezeiten 522  
ANSI 729  
Anspruchsregeln 1001  
Anspruchstypen 934  
Antivirenschutzprogramme 57  
Antwortcode 795  
Antwortdatei 1089, 1092  
Anwendungs- und Dienstprotokolle 1042  
Anwendungsmodus 109  
Anwendungspool 117, 774, 779–780  
Anwendungsproxy 919–920  
Anwendungssteuerungsrichtlinien 580, 582  
APIPA 695

AppCMD.exe 773, 775–776  
AppData 526  
APPEND 1143  
ApplicationHost.config 777, 791  
AppLocker 580  
Approve-WsusUpdate 1029  
appwiz.cpl 574  
Arbeitsgruppe 78  
Arbeitsspeicherpuffer 262  
Arbeitsprozesse 781, 799  
Arbeitsspeicher 250, 260, 1056, 1058  
    Bereich 983  
    dynamischer 260  
    Umfang 262  
ASSIGN 1143  
ATTRIB 1144, 1150  
Attribute 352  
auditpol 487  
Aufgabenplanung 1043, 1065  
    Bibliothek 982  
Aufgabenstatus 1066  
Aufzeichnung 981  
    Abbild 1095  
    Startabbilder 1103  
Ausfallschutz 706  
Ausgabezwischenspeicherung 800  
Ausgleichsmodul 960  
Auslagerungsdatei 145, 825, 1150  
Ausnahmen 883  
Authentifizierung 786  
    Ausnahme 892  
AuthorizationRules.xml 1141  
AutoIT 533  
Autoritätsursprung 725

AutoUnattend.xml 1089  
avdx 280  
Azure 33, 754, 837, 966  
    AD Connect Cloud Sync 421  
    AD-Cloudsynchronisierung 421

## **B**

BackConnectionHostNames 873  
Backup 622, 705  
Bare-Metal-Restore 979  
Basisdatenträger 138  
Batchdatei 1068, 1146  
bcdboot 69  
Bcdedit 173, 499  
Befehlszeilenparameter 833  
Benachrichtigungsschwellenwerte 635  
Benutzergruppen 814  
    Richtlinie 826  
Benutzerisolation 804  
Benutzerkonfiguration 542, 546  
Benutzerkonten 524  
    Steuerung 585  
Benutzernamenverzeichnis 805  
Benutzerprofil  
    Datenträger 835  
    Eigenschaften 524  
Benutzerzuweisung 839  
Berechtigungen 592, 782, 1105  
    auslesen 598  
    Struktur 599  
    verweigern 592  
Bereichseigenschaften 718  
Bereichsgruppierungen 709  
Bereinigung 493

Bereitstellungs- und Imageerstellungstools 1090  
Bereitstellungseigenschaften 841, 846  
Bereitstellungsübersicht 818, 846  
Bericht 635, 1057  
Besitzer 597  
Besitzübernahme 356  
Best Practices Analyzer 121, 124  
Betriebsmaster 347, 354, 437, 481  
    Performance 353  
    Rollen 336  
Betriebssystemlaufwerke 153  
BgInfo 1080  
Bidirektional 506  
Bildschirmschoner 556  
BIND 729  
Bindungen 692, 774–775, 795, 872, 1009  
Biometrieerfassung 117  
Biometrieframework 117  
BitLocker 48, 111, 151  
    Troubleshooting 156  
BITS 113  
Blacklists 580  
Blob 404  
Blob-File 966  
Blocken 892  
Bluescreens 983  
BlueScreenView 985  
boot.wim 1089, 1101  
Boot-Manager 47  
Bootmenü 50  
Bootsect.exe 69  
Bootx64.efi 56  
BPA-Überprüfung 124  
BranchCache 108, 111, 655

Bridgeheadserver 450, 458

Brückenkopfserver 458

Builtin 475

## **C**

cab-Dateien 63

Cache 648

Cachegröße 662

Cachemodusclients 655

Cacheserver 659

CALs 37

CanPool 165, 1122

CAPs 924, 933

CAU 961

Central Access Policies 924, 933

certlm.msc 304, 663, 868, 917, 930, 996, 1147

certsrv.msc 108, 863, 872, 875, 917

certtmpl.msc 848, 875, 996

change user 830

ChDir 1143

Checkpoint-VM 253, 284

Childdomänen 338

Child-VMs 218

CHKDSK 1144

CHOICE 1144

cifs 309

cipher 158

Claim Types 934

claimapp 1001

Clear-ClusterNode 324

Clear-Content 1133

Clear-Host 1050

ClearType 832

Clientkonfiguration 665

- Cloud Witness 966
- Cloudzeugen 966
- CLS 1144
- Cluster 219, 286, 313, 323
  - Aware Update 961
  - Berechtigungen 325
  - Compute Resiliency 959
  - Gruppe 324
  - IP-Adresse 941
  - Operating System Rolling Upgrade 957
  - Quarantine 959
  - Ressourcen 302, 324
  - Rollen 962
  - Schlüsselspeicher 930
  - Shared Volumes 317
  - Volumes 318
- ClusterNode 324
- ClusterquorumEinstellungen 966
- ClusterStorage 318
- Clusterverwaltung-Pools 160
- cmd 75
- Cmdlets 345, 567
- CNA 112
- CNAME 722
- COMP 1144
- Compare-DscConfiguration 1124
- compmgmt.msc 608
- Compress-Archive 1113
- Computer 475
  - Gruppen 1023
  - Konfiguration 542, 546
  - Konten 409
  - Name festlegen 65
  - Reparaturoptionen 51, 979, 1058

Verwaltung 79  
Zertifikat 915  
ConfigEncKey.key 791  
Connection Broker 837  
Connect-PSSession 766, 1119  
Container 111, 753  
Content-Server 664  
control intl.cpl 79  
Control-Protokoll 915  
Converged Fabric 970  
Converged Network Adapter 112  
convert 142  
ConvertFrom-String 1113  
Convert-VHD 172, 274  
COPY 1144  
Copy-Item 264, 1120, 1132  
Copy-NetFirewallRule 890  
Copy-NetIPsecRule 890, 1137  
Core 861  
Core-Server 51, 61, 120, 425, 701, 976  
Cortana 560  
CSV 136, 317, 321  
Clusterlaufwerk 856  
custerr 773  
CustomDCCloneAllowList.xml 379  
Customer Address 234

## **D**

DAC 933  
Data Center Bridging 112, 970  
Data Collector Sets 1052  
Data Execution Prevention 228  
Dateiattribute 620  
Dateidienste 108

- Dateigruppen 639–640
- Dateiklassifizierungsdienste 641
- Dateiprüfung 638
  - Ausnahmen 639
  - Eigenschaften 639
  - Verwaltung 637
- Dateireplikationsdienst 121
- Dateiserver 108, 236
  - Ressourcen-Manager 631
- Dateisystem 108, 133, 637, 924
  - Berechtigungen 595
  - verteiltes 646
- Dateizugriffe 485
- Datencache 658
- Datendeduplizierung 132, 178
- Datensammlergruppen 1052
- Datensammlersatz 1055
- Datensicherung 277, 284, 314, 498, 569, 820, 975
- Datenträger 980, 1144
  - dynamische 139
  - Konfigurationen 139
  - Kontingente 632
  - Partitionsformat 137
  - Verwaltung 136
- Daytime 112
- DCB 970
- DCCloneConfig.xml 379
- DcCloneConfig.xml 378, 380
- Dcdiag 343, 348, 371, 380, 428, 460, 465, 468, 471, 738
- Dclist 738
- Ddpeval 178
- Debuggen 1116
- Debuginformationen 984
- Debugmodus 81

Debugprotokollierung 731  
Default Domain Controller Policy 478  
Default Domain Policy 478, 892  
DefaultAppPool 1001  
DefaultInstance 930  
DEFAULTIPSITELINK 453, 455  
Definitionsdateien 881  
Defragmentierung 149  
    defrag 149  
Delegierung 433, 440–441, 722, 782  
Deleted Object Lifetime 412  
Delprof2 532  
DELTREE 1144  
Deny-WsusUpdate 1029  
Deployment Image Servicing and Management 120  
Desired State Configuration 1124  
Desktophintergrund 857  
Desktop-Pools 855  
Device Health Attestion 108  
devmgmt.msc 61  
Devolo 673  
dfrgui 149  
DFS 108, 115, 180, 368, 631, 646  
DFS-Infrastruktur 649  
dfsmgmt.msc 651  
DFS-Namespace 648, 650–651  
Dfsradmin 649  
Dfsrdiag 649  
DFS-Replikation 649–650, 653  
DfsrPrivate 653  
DFS-Server 650  
DHCP 691, 1094  
    Administratoren 516  
    Benutzer 516

- Bereichskonfiguration 708
- Datenbank 699
- Failover 706
- Optionen 702
- Richtlinien 702–703
- Server 108, 691
- Serverdienst 696
- Wächter 220
- dhcpcheck.exe 699
- dhcptest.exe 699
- DHCPv6 108, 201
- Diagnose 187, 468, 1042, 1058
- Diensteigenschaften 997
- Dienststeuerung 677
- Dienstkonten, verwaltete 407
- Dienstprotokolle 583
- Dienstqualität 616
- Dienstverbindungspunkt 659, 931
- Differenzierung 256
- Differenzplatte 247
- Digitalkameras 833
- DIR 1144
- DirectAccess 109, 541, 656, 666, 899
  - Konfiguration 904
- DirectPlay 112
- DisableAutoExclusions 883
- Disable-CauClusterRole 957
- DisableLoopbackCheck 873
- Disable-NetAdapter 193
- Disable-NetAdapterQos 971
- Disable-NetFirewallRule 890
- Disable-NetQosFlowControl 970
- DisablePasswordChange 408
- Disable-PSRemoting 336, 1117

Discard 112  
Disconnect-PSSession 766, 1119  
Disk2vhd 57, 172  
Diskext 143  
Diskmgmt.msc 136, 259  
Diskpart 56, 144, 173, 259  
Dism 55, 60, 64, 120, 230, 1093  
Distributed Cache 660  
Distributed File System 180, 646  
Djoin 403, 405  
DLL-Regeln 584  
DNS 194, 362, 373, 719, 939  
    Delegierung 370  
    Domänenname 699  
    dynamische Updates 697  
    Einträge 479  
    Optionen 343  
    Round-Robin 941  
    Server 66, 78, 108, 370  
    Serveradressen 340  
    Suffix 209, 364, 445  
    Weiterleitungen 732  
    Zonen 723  
DnsAdmins 516  
DNScmd.exe 741  
Dnslint 479  
DNSSEC 108, 336, 744  
DnsUpdateProxy 516, 697, 739  
Docker 754, 757  
    Container 764  
Dockerfile 762  
Dokumentdienste 669  
DOL 412  
Domain Name System Security Extensions 108

DomainLocationDeterminationURL 908

Domäne 78, 368

Domänenadmins 515, 917

Domänenaufnahme 406

Domänencomputer 903

Domänencontroller 245, 341, 350, 361, 425, 429, 738

- herabstufen 494
- schreibgeschützter 357, 428

Domänendienste 340

Domänenfunktionsebene 384

Domänenkonto 477

Domänenlokal 534

Domänenmitgliedschaft festlegen 65

Domänenname 734

Domänennamenmaster 346, 350, 354, 357, 444

Domänenstruktur 444

Domänenzertifikat 846

DoNotRoundRobinTypes 730

Downloadmodus 1024

Downstreamserver 1009

Drahtlosnetzwerk 118

Driverquery 1149

Druck- und Dokumentdienste 108

Druckauftrag 682

- Bearbeitung 671

Druckausgabe 677

Druckdienste 108

Drucker 671, 827

- Eigenschaften 682
- Filter 678
- Installation 675
- Mapping 828
- Probleme 680
- Server 670, 678

Umleitung 828  
Druckjob 675, 677, 681  
Druckserver 108  
Druckverwaltungs-Konsole 678  
dsa.msc 347, 517  
dsac 332, 384, 386  
Dsamain.exe 503  
DSC 1124  
Dsquery 347, 481  
Dsregdns 738  
DVD-Laufwerk 50  
Dynamic Access Control 933  
Dynamische DNS-Updates 697

## **E**

E/A-Virtualisierung 220  
Easy Print Driver 827  
ECHO 1144  
Editionen 37  
EFS 111, 156  
Eingabeaufforderung 1142, 1146  
Einschränkungen 433  
Einwählen 523  
Einzelstamm 220  
EKU 915  
E-Mails 1134  
Enable-AdfsDeviceRegistration 999  
Enable-ADOptionalFeature 411  
Enable-BitLocker 155  
Enable-ClusterStorageSpacesDirect 945  
Enable-DedupVolume 179  
Enable-NetAdapter 193  
Enable-NetAdapterQos 971  
Enable-NetFirewallRule 183

Enable-Netfirewallrule 304  
Enable-NetQosFlowControl 970  
Enable-PSRemoting 323, 336, 1117, 1137  
Enable-VMMigration 311  
Encrypting File System 111, 156  
Energieverwaltung 188  
Enhanced Key Usage 915  
Enter-PSSession 253, 1119, 1128  
EPT 49  
Ereignis 981  
    Anzeige 1042  
    Katalog 718  
    Protokollierung 483, 634, 732  
    Sammeldienst 1046  
Errorlevel 1148  
Erweiterte Features 521  
Ethernet 970  
Eventcreate 1050  
Eventvwr.msc 605, 1041  
Exchange 428, 482, 919  
    Anwendungspool 780  
EXPAND 1144  
Expand-Archive 1113  
Export 287, 381  
Export-PfxCertificate 294  
Export-SmigServerSetting 271  
Extents 149

## **F**

FailedReqLogFiles 797  
Failover 300, 302, 308, 706  
    Beziehung 707  
    Clustering 112  
    Cluster-Verwaltung 303

- Konfiguration 707
- Farm 810
- Faxserver 109
- FCI 641
- Featureeinstellungen 800
- Features 74, 104, 111, 659
- Fehlerbehebung 365, 734, 918
- Fehlerseiten 795
- Festplatten 134, 172
  - differenzierende 247
  - hinzufügen 255
  - virtuelle 160, 1105
- Fibre Channels 222, 970
- File Classification Infrastructure 641
- File Server Resource Manager (FSRM) 108, 632
- Fileserver 108
- Filteransichten 678
- FIND 1144
- Find-Package 1128
- Fingerabdruck 663
- Firewall 304, 854
  - Einstellungen 660, 664, 717, 854, 1049
  - Einstellungen, BranchCache 665
  - Regeln 926
  - Status 892
- Firmware 221
- Flags 928
- Flushdns 737
- ForeignSecurityPrincipals 475
- Forest 334, 337
- FORMAT 1144
- Format-Volume 134
- Forward-Lookupzonen 362, 473, 719
- FQDN 734

Freigabe 605  
Freigabeberechtigungen 595  
Freigabecenter 589  
Freigaben 609, 623  
Frunas 386  
fsmgmt.msc 608  
fsmo maintenance 357  
FSMOs 346  
fsm.msc 632  
Fsutil 143, 636  
FTP 116, 804, 1144  
    Autorisierungsregeln 803  
    Firewallunterstützung 803  
    Server 801  
Full Qualified Domain Name 734  
Funktionen 111  
Funktionsebene 368  
Funkuhr 400

**G**

Gastbetriebssystem 246  
Gateway 199  
GCI 847  
GCM 590  
Gehosteter Cache 657  
Generation 1-VMs 243  
Generation 2-VMs 253  
Generic Routing Encapsulation 913  
Geräteidentifikationsstrings 575  
Geräte-Manager 186  
Gerätesetupklasse 575  
Gesamtstruktur 350, 368, 437, 444  
    Funktionsebene 384  
Get-ADComputer 347

Get-ADDomain 348  
Get-ADDomainController 346, 387, 426, 457  
Get-ADForest 348  
Get-ADGroup 295  
Get-ADObject 413  
Get-ADReplicationConnection 457  
Get-ADReplicationFailure 463  
Get-ADReplicationPartnerMetadata 463  
Get-ADReplicationQueueOperation 463  
Get-ADReplicationSite 463  
Get-ADReplicationUpToDateVectorTable 463  
Get-ADUser 345  
Get-BPAModel 123  
Get-BPAResult 124  
Get-CauReport 965  
Get-ChildItem 1120, 1134  
Get-Cluster 323, 959  
Get-ClusterFaultDomain 950  
Get-ClusterGroup 324  
Get-ClusterNetwork 321, 324  
Get-ClusterNode 324  
Get-ClusterQuorum 324  
Get-Clusterquorum 968  
Get-ClusterResource 324, 615  
Get-Command 143, 367, 449, 655, 696, 977  
Get-Content 676  
Get-DAConnectionStatus 909–910  
Get-Date 1131  
Get-DedupJob 179  
Get-DedupStatus 179  
Get-DedupVolume 179  
Get-Disk 143–144, 165  
Get-DnsClient 365  
Get-DnsClientNrptPolicy 908

Get-DnsClientServerAddress 365  
Get-DscConfiguration 1124  
Get-DscConfigurationStatus 1124  
Get-DscLocalConfigurationManager 1124  
Get-EventLog 1121  
Get-Eventlog 1049  
Get-ExecutionPolicy 1115  
Get-Help 193  
Get-HgsAttestationPolicy 295  
Get-HgsClientConfiguration 293, 295  
Get-HgsServer 295  
Get-HgsTrace 295  
Get-Hotfix 1031, 1120  
Get-Item 1117  
getmac 698  
Get-Member 1131  
Get-MpComputerStatus 881  
Get-MpPreference 881  
Get-MpThreat 881  
Get-MpThreatCatalog 881  
Get-MpThreatDetection 881  
Get-NCSIPolicyConfiguration 908  
Get-NetAdapter 193, 426  
Get-Netadapter 1151  
Get-NetAdapterQos 971  
Get-NetFirewallProfile 890  
Get-NetFirewallRule 183, 890  
Get-NetIPAddress 364, 910, 1120  
Get-NetIPConfiguration 78  
Get-NetLbfoTeam 191, 193  
Get-NetQosDcbxSetting 970  
Get-NetQosFlowControl 970  
Get-NetQosTrafficClass 971  
Get-NetTeredoConfiguration 912

Get-PackageSource 1128  
Get-Partition 165  
Get-PhysicalDisk 84, 143, 165, 1122  
Get-Physicaldisk 945  
Get-PnpDevice 765  
Get-PrintConfiguration 675  
Get-Printer 675  
Get-PrinterConfiguration 675  
Get-PrinterDriver 675  
Get-PrinterPort 675  
Get-PrinterProperty 675  
Get-Process 676, 1131  
Get-PSDrive 1121  
Get-PswaAuthorizationRule 1141  
Get-Random 1120  
Get-ResiliencySetting 169  
Get-Service 1131, 1134  
Get-SRGroup 182  
Get-SRPartnership 182  
Get-StorageJob 951  
Get-StoragePool 949  
Get-StorageQosFlow 616, 618  
Get-StorageQosPolicy 617-618  
Get-StorageQosPolicyStore 616  
Get-StorageQosVolume 616  
Get-StorageSubSystem 618  
Get-VirtualDisk 166, 169, 949  
Get-VM 251, 264, 266, 617  
Get-VMFibreChannelHba 266, 381  
Get-VMGroup 297  
Get-VMHardDiskDrive 264, 266, 381, 617  
Get-VMhost 266  
Get-VMIdeController 266, 381  
Get-VMNetworkAdapter 266, 274, 759

Get-VMNetworkAdapterTeamMapping 242  
Get-VMScsiController 244, 266, 275, 381  
Get-VMSnapshot 265  
Get-VMsnapshot 283  
Get-VMSwitch 241, 266  
Get-VMSwitchTeam 241  
Get-WindowsFeature 119, 230, 293, 367  
Get-WinEvent 183, 591  
Get-WmiObject 266, 683–684, 1151  
Get-WsusClassification 1029  
Get-WsusComputer 1029  
Get-WsusProduct 1029  
Get-WsusServer 1029  
Get-WsusUpdate 1029  
Gewichtung 263  
Global 534  
Globally Unique Identifier 575  
Goup Policy Management Console 112  
gpedit.msc 153, 542, 1057  
GPMC 112, 542  
GPO 542, 553  
gpresult 568  
GPT 137  
gpupdate 487, 566, 582, 716, 874, 908, 1025  
GRE 913  
Grenzwerte 637  
GroupPolicy 542, 566  
Grundeinstellungen 775  
Gruppen 534  
Gruppenmitgliedschaft 459  
Gruppenrichtlinien 153, 404, 478, 541, 657, 665, 679, 826, 848, 875, 1020  
    Modellierungsassistent 572  
    Objekte 546, 570, 1020  
    Preferences 544

Vererbung 557  
Verwaltung 112, 542, 566, 1020  
Gruppenrichtlinienbasiert 713  
GUID 575  
Partitionstabelle 137

## **H**

Haltepunkt 1116  
Handles 1080  
Hardware 149  
    Attestation 292  
HardwareIDs 576  
hasfsmo 348  
Hashveröffentlichung 662  
Hashversionsunterstützung 658  
Hauptressourcen 967  
Herunterfahren 246  
Hintergrundbild 857  
Hintergrundübertragungsdienst 113  
Histogramm  
    Ansicht 1054  
    Leiste 482  
history 773  
HKEY\_CURRENT\_USER 831  
HNV 233  
Hochverfügbarkeit 299  
Host 721  
Host A 739  
Host Guardian-Dienst 109  
Hosted Cache 657  
hostname 195, 1149  
Hot Swap 147  
Hotpatching 33  
HTTP 771

- http 403 795
- HTTP-Fehlermeldungen 794
- HTTPS 771, 899
- HTTPS-VPN 914
- HTTP-Umleitungen 794, 796
- Hyper-V 109, 215, 218, 277, 810, 851, 938
  - Container 758
  - Einstellungen 248
  - Generierungszähler 378
  - Host 287
  - Manager 219, 231, 250, 381
  - Replica 219, 300
  - Replikation 280, 302
  - Virtual Machine Management 228
  - Virtual Machine Worker Process 228
- Hypervisor 215

## I

- icacls.exe 1140
- IDE-Controller 243, 255
- Identitätsverbund 925
- IE 55
- if 1147
- IGMP 941
- IIS 109, 112, 762, 771
- IIS-Manager
  - Anmeldeinformationen 783
  - Berechtigungen 782
- iisreset 776
- IIS-Verwaltungsdienst 792
- Images 50
- import-csv 453
- Import-Module 566
  - ADDSDeployment 432

Import-SmigServerSetting 272  
Import-VM 265  
Indikator 1054  
Indikatorengruppe 1053–1054  
inetmgr 772  
inetpub 773  
inetsrv 772  
Infrastrukturmaster 346, 349, 353, 357  
Inhaltsabruf 665  
Initialisierung 138  
Initialize-ADDeviceRegistration 998  
install.wim 55, 1089  
Install-ADDSDomain 335, 376, 444  
Install-ADDSDomainController 335, 375, 387, 427  
Install-ADDSEForest 335, 375–377  
Installation 47–48, 1026  
    unbeaufsichtigte 120  
Installationsabbilder 1094, 1102  
Installationsmedium 374  
Install-HgsServer 294  
Install-Module 755  
Install-NetworkController 969  
Install-NetworkControllerCluster 969  
Install-PswaWebApplication 1139  
Install-WindowsFeature 119, 179, 229–230, 271, 292, 367, 375–376, 755, 904, 925, 944, 970, 1139  
Integrationsdienste 245, 402  
Integritätszertifikate 894  
Intel Extended Page Table 49  
Interne Windows-Datenbank 113  
Internet Information Services 771  
Internet Protocol Security 891  
Internetdruckclient 113  
Internetinformationsdienste 112, 771  
    Manager 782, 870

Internetname 940  
Internetoptionen 916, 932  
Internetprotokoll 186, 340  
Intersite Topology Generator 458, 471  
Inter-Site Transports 455  
InvocationID 378  
Invoke-BpaModel 123  
Invoke-CauRun 965  
Invoke-Command 253, 368, 1128  
Invoke-IpamGpoProvisioning 715  
Invoke-Item 1134  
Invoke-WebRequest 1112  
Invoke-WsusServerCleanup 1029  
iPad 674  
IP-Adressblöcke 718  
IP-Adressverwaltungsserver 113, 691  
IPAM 113, 691, 711  
    ASM Administrators 713  
    IP Tracking Administrators 713  
    Users 712  
IpamDhcpLog.txt 717  
IpamDnsLog.txt 717  
ipamprovisioning.ps1 717  
IPAM-Zugriff 714  
IP-Anwendungsserver 713  
IPAutoconfigurationEnabled 695  
IP-Bereiche 691  
Ipconfig 194, 346, 364, 366, 472–473, 698, 737, 910, 1148  
IP-Forwarding 938  
iPhone 674  
iphttpsinterface 910  
IPnG 200  
IPSec 656, 666, 912  
IPsec 220, 891, 893

IP-Subnetze 430, 454  
IPv4 693  
IPv6 200, 693, 903  
iSCSI 108, 112, 174  
iSCSICli 80  
iscsicpl 80  
iSCSI-Dienste 632, 650, 660  
iSCSI-Targets 80  
iSCSI-Ziele 301  
isDeleted 412  
ISO-Datei 55  
Isolierung 892  
isRecycled 412  
ISTG 458, 472  
iWARP 236

## **J**

JET-Datenbank 337

## **K**

Katalog

- Datei 1089
- globaler 350
- Server 459

KCC 449, 457, 460, 471

KDC 477

Kennwort 358, 407

- Alter 586
- Chronik 586
- Länge 586
- Replikationsgruppe 431, 433
- Richtlinien 585
- Schutz 556

Kerberos 309, 522, 894, 910

- Armoring 369

- Authentifizierung 477
- Richtlinie 397
- Schlüsselverteilungszentrum 478
- Test 465
- Verkehr 368
- Key Distribution Center 477
- Key Signing Key 744
- KiXtart 533
- Klassifizierung
  - Eigenschaften 642
  - Methode 642
  - Regeln 642
  - Verwaltung 643
  - Zeitplan 642
- KMS-Hostschlüssel 1107
- Knowledge Consistency Checker 449, 457
- Komplexitätsvoraussetzungen 586
- Komprimierung 141–142, 260, 799
- Konfiguration
  - Dateien 777
  - Datenbank 928
  - Einstellungen 118
  - freigegebene 791
- Konten
  - Operatoren 903
  - Verwaltung 485
- Kontingent 150, 632
  - Einträge 150–151
  - Ereignis 635
  - Pfad 633
  - Verwaltung 632
  - Vorlagen 635
- Kontingenteinträge 636
- Kontosperrung 522

Konvertierung 260

Kryptografie

    Dienstanbieter 870

    Modus 930

KSK 744