

Inhaltsverzeichnis

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

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

Teil II Einrichtung des Servers

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

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

Teil III Virtualisierung mit Hyper-V

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

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

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

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

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

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

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

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

Teil V Datei- und Druckserver mit Windows Server

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

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

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

Teil VI Infrastrukturen mit Windows Server

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

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

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

Kapitel 28 Remotedesktopdienste – Anwendungen virtualisieren 807

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

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

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

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

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

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

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

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