

Auf einen Blick

1	Windows Server 2019	29
2	Rollen und Features	59
3	Netzwerkgrundlagen und -Topologien	137
4	IP-Adressmanagement	157
5	Authentifizierungsprotokolle	231
6	Active Directory	255
7	Benutzer, Gruppen & Co im Active Directory	331
8	Virtualisierung	377
9	Dateiserver	417
10	Verwaltung	473
11	Windows PowerShell	545
12	Migration verschiedener Serverdienste auf Windows Server 2019	581
13	Hyper-V	649
14	Dateidienste	703
15	Internetinformationsdienste-Server (IIS)	763
16	PKI und Zertifizierungsstellen	805
17	Patchmanagement für Windows Server	869
18	Remotedesktopdienste	927
19	Virtuelles privates Netzwerk und Netzwerkrichtlinienserver	993
20	Integration in Azure	1083
21	Troubleshooting im Windows Server	1145
22	Security in und mit dem Windows Server	1199

Inhalt

Vorwort der Autoren	23
1 Windows Server 2019	29
1.1 What's new?	30
1.2 Die verschiedenen Editionen	32
1.2.1 Windows Server Standard	32
1.2.2 Windows Server Datacenter	33
1.3 Long Term Services Channel vs. Semi-Annual Channel	33
1.4 Lizenzierung	34
1.4.1 Verschiedene Lizenzierungsarten	34
1.4.2 Lizenzprogramme (KMS und MAK)	34
1.4.3 Active Directory Based Activation (ADBA)	38
1.4.4 VM-Based Activation	38
1.5 Systemanforderungen	38
1.6 Installation von Windows Server 2019	39
1.6.1 Installation mit grafischer Oberfläche	40
1.6.2 Windows Server Core	45
1.6.3 Nach der Installation	46
1.7 Die Installation automatisieren	48
1.7.1 Windows Assessment and Deployment Kit (ADK)	48
1.7.2 Abbildverwaltung (Deployment Image Servicing and Management)	51
1.7.3 Sysprep	53
1.8 Update-Strategie	57
2 Rollen und Features	59
2.1 Rollen und Rollendienste	59
2.2 Die Rollen im Überblick	61
2.2.1 Active Directory Lightweight Directory Services	61
2.2.2 Active Directory-Domänen Dienste	63
2.2.3 Active Directory-Rechteverwaltungsdienste	65

2.2.4	Active Directory-Verbunddienste	67
2.2.5	Active Directory-Zertifikatdienste	69
2.2.6	Datei-/Speicherdiene	72
2.2.7	Device Health Attestation	83
2.2.8	DHCP-Server	85
2.2.9	DNS-Server	87
2.2.10	Druck- und Dokumentendienste	88
2.2.11	Faxserver	89
2.2.12	Host Guardian-Dienst	91
2.2.13	Hyper-V	92
2.2.14	Netzwerkcontroller	93
2.2.15	Netzwerkrichtlinien- und Zugriffsdienste	94
2.2.16	Remotedesktopdienste	95
2.2.17	Remotezugriff	97
2.2.18	Volumenaktivierungsdienste	99
2.2.19	Webserver (IIS)	100
2.2.20	Windows Server Update Services (WSUS)	103
2.2.21	Windows-Bereitstellungsdienste	106
2.3	Features	108
2.4	Editionen und ihre Möglichkeiten	128
2.4.1	Windows Server SAC	129
2.4.2	Windows Server 2019 LTSC – Essentials	129
2.4.3	Windows Server 2019 LTSC – Standard oder Datacenter, Core oder Desktop	130
2.4.4	Vergleichen Sie die Editionen	132
2.5	Was ist neu in den unterschiedlichen SAC-Versionen?	134
2.6	Was wurde in den letzten Versionen entfernt?	134
2.7	Server- bzw. Rollen-Platzierung	134
3	Netzwerkgrundlagen und -Topologien	137
3.1	Was ist ein Netzwerk? Diese Begriffe sollten Sie kennen	137
3.2	Welche Topologien gibt es und welche werden heute in der Praxis noch genutzt?	139
3.2.1	Bus-Topologie	139
3.2.2	Ring-Topologie	140
3.2.3	Stern-Topologie	140

3.2.4	Hierarchische Topologie	141
3.2.5	Vermischte Topologie	142
3.3	Referenzmodelle	143
3.3.1	ISO-OSI-Referenzmodell	144
3.3.2	TCP/IP-Referenzmodell	154
3.3.3	Gegenüberstellung der beiden Modelle	155
3.4	Übertragungsmethoden	155
3.4.1	Unicast	155
3.4.2	Multicast	156
3.4.3	Broadcast	156

4 IP-Adressmanagement

4.1	Was ist eine MAC-Adresse?	157
4.2	Was ist TCP/IP?	159
4.3	Das IP-Protokoll genauer erklärt	160
4.3.1	IP Version 4	161
4.3.2	ARP	168
4.3.3	Subnetting	171
4.3.4	IP Version 6 (IPv6)	172
4.3.5	Aufbau eines IP-Pakets	180
4.4	Wie kommuniziert ein Computer mit einem Netzwerk?	183
4.4.1	Kabelverbindungen	184
4.4.2	WLAN und Mobilfunk	185
4.5	Netzwerkkonfiguration unter Windows	187
4.6	Namensauflösung	193
4.6.1	DNS-Namensauflösung	194
4.6.2	NetBIOS	202
4.7	DHCP	204
4.7.1	Was ist DHCP?	204
4.7.2	IP-Adressen vergeben und erneuern	204
4.7.3	Automatische Vergabe von privaten IP-Adressen (APIPA)	205
4.7.4	Aufbau eines DHCP-Datenpakets	206
4.7.5	Installation eines DHCP-Servers unter Windows Server 2019	207
4.7.6	Konfiguration eines DHCP-Servers nach der Installation der Rolle	212
4.7.7	Konfiguration eines DHCP-Failovers	223

4.8 IPAM	225
4.8.1 Vorteile des IPAM	225
4.8.2 Installation des IPAM	225
4.8.3 Konfiguration des IPAM-Servers	226
4.8.4 Mögliche Anpassungen des IPAM-Servers und Hinweise für den Betrieb	229

5 Authentifizierungsprotokolle

5.1 Domänenauthentifizierungsprotokolle	231
5.1.1 LanManager (LM)	232
5.1.2 NTLM	233
5.1.3 Kerberos	233
5.1.4 Ansprüche (Claims) und Armoring	249
5.1.5 Sicherheitsrichtlinien	252
5.2 Remotezugriffsprotokolle	253
5.2.1 MS-CHAP	253
5.2.2 Password Authentication Protocol (PAP)	253
5.2.3 Extensible Authentication Protocol (EAP)	254
5.3 Webzugriffsprotokolle	254

6 Active Directory

6.1 Geschichte des Active Directories	255
6.2 Was ist neu im Active Directory in Windows Server 2019?	256
6.3 Die Datenbank von Active Directory	257
6.4 Die Komponenten des Active Directory	258
6.4.1 Logischer Aufbau	258
6.4.2 Physischer Aufbau	262
6.4.3 Globaler Katalog	262
6.4.4 FSMO (Flexible Single Master Operations) bzw. Betriebsmaster	263
6.4.5 Standorte	265
6.4.6 Distinguished Name	265
6.4.7 Canonical Name	265
6.4.8 Common Name	265
6.5 LDAP	266

6.6	Schema	266
6.7	Replikation	267
6.7.1	Steuerung der AD-Replikation	267
6.7.2	Tool für die Überprüfung des Replikationsstatus	270
6.8	Read-Only-Domänencontroller (RODC)	270
6.8.1	Voraussetzungen für den Einsatz eines RODC	271
6.8.2	Funktionalität	272
6.8.3	RODC-Attributfilter	272
6.8.4	Wie funktioniert eine RODC-Anmeldung?	273
6.8.5	Einen schreibgeschützten Domänencontroller installieren	273
6.9	Vertrauensstellungen	280
6.9.1	Eigenschaften der Domänenvertrauensstellungen	282
6.9.2	Vertrauensstellungstypen	284
6.9.3	Vertrauensstellung in Windows-Domänen ab Windows Server 2003	284
6.9.4	Authentifizierungsvarianten in Vertrauensstellungen ab Windows Server 2003	284
6.9.5	Fehlerhafte Vertrauensstellungen	285
6.9.6	Eine Gesamtstrukturvertrauensstellung einrichten	286
6.10	Offline-Domänenbeitritt	293
6.11	Der Papierkorb im Active Directory	293
6.12	Der Wiederherstellungsmodus des Active Directory	296
6.12.1	Nicht-autorisierende Wiederherstellung	296
6.12.2	Autorisierende Wiederherstellung	297
6.12.3	Garbage Collection	297
6.12.4	Active Directory Database Mounting Tool	298
6.13	Active Directory-Verbunddienste (AD FS)	298
6.13.1	Die Komponenten des AD FS	299
6.13.2	Was ist eine Verbundvertrauensstellung?	299
6.14	Installation des Active Directory	300
6.14.1	Den ersten DC in einer Domäne installieren	300
6.14.2	Einen weiteren DC in einer Domäne installieren	311
6.14.3	Installation des ersten DCs in einer Subdomäne der Gesamtstruktur	313
6.14.4	Einen DC aus einer Domäne entfernen	315
6.14.5	Einen defekten oder nicht mehr erreichbaren DC aus einer Domäne entfernen	319
6.14.6	Die Domäne entfernen	322
6.15	Wartungsaufgaben innerhalb des Active Directories	325
6.15.1	Übertragen oder Übernehmen der FSMO	325

6.15.2	Wartung der AD-Datenbank	326
6.15.3	IFM-Datenträger	327

7 Benutzer, Gruppen & Co im Active Directory

7.1	Container	331
7.1.1	Administrative Konten und Sicherheitsgruppen im Container »Builtin«	333
7.1.2	Administrative Konten und Sicherheitsgruppen aus dem Container »Users«	336
7.2	Organisationseinheiten	338
7.2.1	Objektverwaltung delegieren	339
7.3	Benutzer	341
7.4	Computer	342
7.4.1	Sicherheitseinstellungen für den Domänenbeitritt von neuen Computern ...	343
7.5	Gruppen	345
7.5.1	Arten von Sicherheitsgruppen	346
7.5.2	Protected Users Group	347
7.6	MSA und gMSA	348
7.6.1	Managed Service Account (MSA)	348
7.6.2	Group Managed Service Account (gMSA)	349
7.7	Password Settings Objects (PSOs)	352
7.7.1	Voraussetzungen für das Anwenden der PSOs	353
7.7.2	PSOs erstellen	353
7.8	Gruppenrichtlinienobjekte (GPO)	356
7.8.1	Allgemeines zu Gruppenrichtlinien	358
7.8.2	Bestandteile einer GPO und die Ablageorte	359
7.8.3	Aktualisierungintervalle von GPOs	361
7.8.4	GPOs erstellen und löschen	361
7.8.5	Sicherheitsfilter der GPOs	363
7.8.6	Administrative Vorlagen und Central Store	363
7.8.7	Der Central Stores	365
7.8.8	Clientseitige Erweiterungen	366
7.8.9	Softwareinstallation über GPOs	367
7.8.10	Sicherheitseinstellungen innerhalb der GPOs	367
7.9	msDs-ShadowPrincipal	372
7.9.1	msDS-ShadowPrincipalContainer	372
7.9.2	Die Klasse msDS-ShadowPrincipal	372

7.9.3	Die SID msDS-ShadowPrincipal	373
7.9.4	Shadow Principals nutzen	373
7.10	Freigegebene Ordner	374
7.11	Freigegebene Drucker	374

8 Virtualisierung

8.1	Hypervisoren	377
8.1.1	Hypervisor-Typen	378
8.1.2	Hypervisor-Design	379
8.2	Hyper-V	381
8.2.1	Hyper-V-Hypervisor	381
8.2.2	Hyper-V-Architektur	391
8.2.3	Hyper-V-Anforderungen	393
8.3	Das ist neu in Windows Server 2019	401
8.4	Virtual Desktop Infrastructure (VDI)	403
8.5	Container	405
8.5.1	Windows-Container	407
8.5.2	Hyper-V-Container	408
8.6	Azure Stack	408
8.6.1	Azure Stack-Hardware	410
8.6.2	Anwendungsbeispiel	412
8.6.3	Azure Stack HCI (Hyperkonvergente Infrastruktur)	413

9 Dateiserver

9.1	Grundlagen des Dateisystems	417
9.1.1	Datenträger und Volumes	417
9.1.2	iSCSI	425
9.1.3	Schattenkopien	428
9.1.4	Freigaben	431
9.1.5	NTFS und Freigaben-Berechtigungen	436
9.1.6	Offlinedateien	443
9.1.7	Datendeduplizierung	445

9.2	Distributed File System (DFS)	447
9.2.1	DFS-N (Distributed File System Namespace)	448
9.2.2	DFS-R (Distributed File System Replication)	452
9.3	Hochverfügbarkeit (HA-Anforderungen)	457
9.4	Server Storage Migration Service	458
9.5	Azure Files	460
9.5.1	Einsatzgebiete für Azure Files	460
9.5.2	Azure-Dateifreigabeprotokolle	461
9.5.3	Kosten	469

10 Verwaltung

10.1	Windows Admin Center (WAC)	473
10.1.1	Bereitstellungsszenarien	474
10.1.2	Voraussetzungen	476
10.1.3	Die Installation des Windows Admin Centers vorbereiten	477
10.1.4	Windows Admin Center installieren	480
10.1.5	Für Hochverfügbarkeit sorgen	483
10.1.6	Einstellungen des Windows Admin Centers	485
10.1.7	Berechtigungen konfigurieren	489
10.1.8	Erweiterungen	491
10.1.9	Systeme verwalten	495
10.2	Server-Manager	512
10.2.1	Lokalen Server verwalten	512
10.2.2	Servergruppen erstellen	514
10.2.3	Remote-Server verwalten	516
10.3	Remote Server Administration Tools (RSAT)	517
10.3.1	Installation unter Windows 10	517
10.4	PowerShell	522
10.4.1	Anforderungen	523
10.4.2	Beispiele für die Verwaltung	524
10.5	WinRM und WinRS	526
10.5.1	Windows Remote Management (WinRM)	526
10.5.2	Windows Remote Shell (WinRS)	528
10.6	Windows Server-Sicherung	529
10.6.1	Die Windows Server-Sicherung installieren	530
10.6.2	Backup-Jobs erstellen	531

10.6.3	Windows Server-Sicherung auf Remote-Servern	536
10.6.4	Einzelne Dateien wiederherstellen	538
10.6.5	Recovery-Medium nutzen	541
11	Windows PowerShell	545
11.1	Windows PowerShell und PowerShell Core	545
11.2	Grundlagen zur PowerShell	555
11.2.1	Aufbau der PowerShell-Cmdlets	557
11.2.2	Skripte ausführen	559
11.2.3	Offline-Aktualisierung der PowerShell und der Hilfdateien	560
11.3	Sicherheit rund um die PowerShell	561
11.3.1	Ausführungsrichtlinien (Execution Policies)	562
11.3.2	Die PowerShell remote ausführen	564
11.3.3	Überwachung der PowerShell	567
11.4	Beispiele für die Automatisierung	569
11.5	Just enough Administration (JEA)	573
11.5.1	Einsatzszenarien	573
11.5.2	Konfiguration und Verwendung	573
11.6	Windows PowerShell Web Access	578
11.7	Windows PowerShell Version 7	580
12	Migration verschiedener Serverdienste auf Windows Server 2019	581
12.1	Einen Read-Only Domain Controller (RODC) löschen	581
12.1.1	Einen produktiven und erreichbaren RODC aus der Domäne entfernen	581
12.1.2	Einen RODC entfernen, der kompromittiert wurde bzw. einer Gefahr ausgesetzt war	582
12.2	Migration von AD-Objekten aus einem Active Directory in ein anderes Active Directory	584
12.2.1	Installation von ADMT auf einem Windows Server 2012 R2	584
12.2.2	ADMT für die Nutzermigration verwenden	585
12.3	Upgrade eines Active Directories von Windows Server 2016 auf Windows Server 2019	593

12.4 Migration eines DHCP-Servers	599
12.4.1 Migration des DHCP-Servers auf klassische Weise	599
12.4.2 Migration des DHCP-Servers mithilfe des Failover-Features	600
12.5 Migration eines Druckerservers	606
12.5.1 Migration der vorhandenen Drucker vom alten Druckerserver mithilfe des Assistenten	606
12.5.2 Migration der gesicherten Drucker auf den neuen Druckerserver mithilfe des Assistenten	608
12.5.3 Anpassung einer eventuell vorhandenen GPO für die Druckerzuweisung	611
12.6 Migration eines Dateiservers	614
12.6.1 Vorbereitungen für die Migration des Dateiservers	614
12.6.2 Daten mithilfe von robocopy auf einen neuen Dateiserver migrieren	615
12.6.3 Daten zwischen virtuellen Dateiservern migrieren	616
12.6.4 Weitere Schritte nach der Migration der Daten	616
12.6.5 Einen Dateiserver über die Domänen hinaus migrieren	616
12.6.6 Dateiserver mit dem Storage Migration Service auf Server 2019 umziehen	616
12.7 Migration eines Hyper-V-Servers	630
12.7.1 Migration einer virtuellen Maschine durch Exportieren und Importieren	630
12.7.2 Migration einer virtuellen Maschine mithilfe der PowerShell	636
12.8 Migration eines Failoverclusters	638
12.8.1 Migration des Failoverclusters mit neuer Hardware	638
12.8.2 Migration eines Failoverclusters auf Windows Server 2019 ohne neue Hardware	647
13 Hyper-V	649
13.1 Bereitstellung von Hyper-V	649
13.1.1 Hyper-V installieren	649
13.1.2 Das Hyper-V-Netzwerk konfigurieren	651
13.1.3 Hyper-V konfigurieren	661
13.1.4 Virtuelle Maschinen bereitstellen	666
13.2 Hochverfügbarkeit herstellen	671
13.2.1 Installation des Failoverclusters	671
13.2.2 Den Cluster erstellen	671
13.2.3 Cluster-Storage	676

13.2.4	Das Quorum konfigurieren	678
13.2.5	Das Cluster-Netzwerk konfigurieren	681
13.2.6	Hochverfügbare virtuelle Maschinen erstellen	681
13.3	Replikation für Hyper-V	684
13.3.1	Den Replikatserver konfigurieren	684
13.3.2	Replikation für virtuelle Maschinen starten	686
13.3.3	Die Konfiguration der virtuellen Maschine anpassen	688
13.3.4	Testfailover	689
13.3.5	Geplante Failovers	690
13.3.6	Desasterfall	692
13.4	Den Host Guardian Service bereitstellen	693
13.4.1	Installation	693
13.4.2	Initialisieren des Host Guardian Service	694
13.4.3	Den Host Guardian Service für HTTPS konfigurieren	696
13.4.4	Redundante Host Guardian Services bereitstellen	697
13.4.5	Anpassungen in der Hyper-V-Infrastruktur	698

14 Dateidienste

14.1	Die Dateiserver-Rolle installieren	703
14.1.1	Installation mit dem Server-Manager	703
14.1.2	Dateifreigaben anlegen	704
14.2	DFS-Namespaces	706
14.2.1	DFS installieren	706
14.2.2	Basiskonfiguration	707
14.2.3	DFS-Ordnerziele erstellen	710
14.2.4	Redundanzen der Namespaceserver	711
14.3	DFS-Replikation	713
14.3.1	DFS-R installieren	713
14.3.2	Die Replikation einrichten und konfigurieren	714
14.4	Ressourcen-Manager für Dateiserver	717
14.4.1	Installation des Ressourcen-Managers für Dateiserver	719
14.4.2	Kontingente	719
14.4.3	Die Dateiprüfungsverwaltung verwenden	724
14.5	Dynamische Zugriffssteuerung (Dynamic Access Control, DAC)	729

14.6 Hochverfügbare Dateiserver	737
14.6.1 Bereitstellung über einen Failovercluster	743
14.6.2 Ein Speicherreplikat einrichten	751
14.6.3 »Direkte Speicherplätze« einrichten (Storage Spaces Direct, S2D)	756
 15 Internetinformationsdienste-Server (IIS)	 763
15.1 Installation der IIS-Rolle	763
15.1.1 Installation auf einem Client	763
15.1.2 Installation auf einem Serverbetriebssystem	767
15.1.3 Remoteverwaltung des IIS	776
15.2 Konfiguration des IIS	782
15.2.1 Erstellen von Websites und virtuellen Verzeichnissen	787
15.3 Absichern des Webservers	792
15.3.1 Authentifizierungsprotokolle	792
15.3.2 Einsatz von SSL	793
15.3.3 Überwachung und Auditing	797
15.4 Sichern und Wiederherstellen	798
15.5 Hochverfügbarkeit	800
 16 PKI und Zertifizierungsstellen	 805
16.1 Was ist eine PKI?	805
16.1.1 Zertifikate	806
16.1.2 Verschlüsselung und Signatur	806
16.2 Aufbau einer CA-Infrastruktur	812
16.2.1 Installation der Rolle	820
16.2.2 Alleinstehende »Offline« Root-CA	825
16.2.3 Untergeordnete Zertifizierungsstelle als »Online«-Sub-CA	841
16.3 Zertifikate verteilen und verwenden	848
16.3.1 Verteilen von Zertifikaten an Clients	849
16.3.2 Remotedesktopdienste	850
16.3.3 Webserver	853

16.3.4	Clients	857
16.3.5	Codesignatur	857
16.4	Überwachung und Troubleshooting der Zertifikatdienste	862

17 Patchmanagement für Windows Server

17.1	Einführung	869
17.1.1	Patching in der Windows-Welt	869
17.1.2	Die Geschichte von WSUS	870
17.1.3	Patch Tuesday	870
17.1.4	Best Practices für das Patching	871
17.1.5	Begriffe im Microsoft-WSUS-Umfeld	873
17.2	Eine WSUS-Installation planen	875
17.2.1	Systemvoraussetzungen	876
17.2.2	Bereitstellungsoptionen	877
17.2.3	Installationsoptionen	879
17.3	Installation und Konfiguration von WSUS-Server	880
17.3.1	Konfigurationsassistent	883
17.3.2	Den Abruf von Updates über WSUS konfigurieren	890
17.3.3	Reporting-Funktionalität aktivieren	893
17.4	Die Administration des WSUS-Servers	893
17.4.1	Die WSUS-Konfigurationskonsole	893
17.4.2	Der WSUS-Webservice	903
17.4.3	Updates freigeben	904
17.4.4	Computer-Reports	905
17.4.5	Erstellen von zeitgesteuerten Update-Phasen	907
17.4.6	Vom Netzwerk getrennte WSUS-Server	911
17.4.7	Verschieben des WSUS-Repositorys	912
17.5	Automatisierung	913
17.5.1	E-Mail-Benachrichtigungen	913
17.5.2	Installation und Konfiguration mit der PowerShell	914
17.5.3	WSUS-Automatisierung mit der Kommandozeile	916
17.6	Azure Automation – Updateverwaltung in der Cloud	920
17.6.1	Azure Automation-Konto bereitstellen und die Basiskonfiguration vornehmen	921
17.6.2	Das Update-Verhalten konfigurieren	924
17.6.3	Designentscheidungen	926

18 Remotedesktopdienste	927
18.1 Remotedesktopdienste vs. RemoteAdminMode	928
18.1.1 Remotedesktop aktivieren	933
18.1.2 Installation der einzelnen Rollendienste	937
18.1.3 Bereitstellung einer Remotedesktop-Umgebung	939
18.2 Eine Sammlung von Anwendungen bereitstellen	948
18.2.1 Erstellen einer RD-Sammlung	948
18.2.2 RemoteApps verwenden	953
18.2.3 Den HTML5-Webclient verwenden	960
18.3 Absichern einer Remotedesktop-Umgebung	964
18.3.1 Einsatz von Zertifikaten	964
18.3.2 Verwaltung der Umgebung mithilfe von Gruppenrichtlinien	969
18.3.3 Ein RD-Gateway verwenden	973
18.3.4 Überwachung und Troubleshooting	979
18.3.5 Restricted Admin Mode	981
18.3.6 Remote Credential Guard	982
18.3.7 Multifaktor-Authentifizierung für den Zugriff auf die Remotedesktopdienste	983
18.4 Sonstige Konfigurationen	984
18.4.1 Implementieren eines RD-Lizenzservers	984
18.4.2 Aktivieren der Kennwortwechselfunktion	989
19 Virtuelles privates Netzwerk und Netzwerkrichtlinienserver	993
19.1 VPN-Zugang	994
19.1.1 VPN-Protokolle	1014
19.1.2 Konfiguration des VPN-Servers	1018
19.1.3 Konfiguration der Clientverbindungen	1019
19.1.4 Troubleshooting	1022
19.2 DirectAccess einrichten	1023
19.2.1 Bereitstellen der Infrastruktur	1025
19.2.2 Tunnelprotokolle für DirectAccess	1028
19.3 NAT einrichten	1028

19.4 Netzwerkrichtlinienserver	1032
19.4.1 Einrichtung und Protokolle	1035
19.4.2 RADIUS-Proxy-Server	1041
19.4.3 Das Regelwerk für den Zugriff einrichten	1043
19.4.4 Protokollierung und Überwachung	1047
19.5 Den Netzwerzugriff absichern	1051
19.5.1 Konfiguration der Clients	1051
19.5.2 Konfiguration der Switches	1056
19.5.3 Konfiguration des NPS	1060
19.5.4 Protokollierung und Troubleshooting	1065
19.6 Absichern des Zugriffs auf Netzwerkgeräte über das RADIUS-Protokoll	1068
19.6.1 RADIUS-Server für die Authentifizierung konfigurieren	1068
19.6.2 Definition des RADIUS-Clients	1071
19.6.3 Sicherheitsgruppen erstellen	1075

20 Integration in Azure	1083
20.1 Hybride Szenarien	1083
20.2 Azure Active Directory	1084
20.2.1 Was ist Azure Active Directory?	1084
20.2.2 Was sind die Azure Active Directory Domain Services?	1085
20.2.3 Was unterscheidet das Active Directory in Windows Server vom Azure Active Directory?	1087
20.2.4 Systemvoraussetzungen für Azure Active Directory	1088
20.2.5 Azure Active Directory initial konfigurieren	1090
20.2.6 Azure AD anpassen	1092
20.2.7 Umsetzung des Zugriffs für hybride Identitäten	1099
20.3 Azure Active Directory mit einem On-Premises-Active Directory verknüpfen	1105
20.3.1 AzureAD Connect oder AzureAD Connect Cloud Sync einsetzen	1105
20.3.2 Azure AD Connect installieren	1106
20.3.3 AzureAD Connect Cloud Sync installieren	1121
20.4 AD FS-Lab-Installation	1125
20.5 Erweitertes Monitoring	1137
20.6 Ausblick: Datacenter-Erweiterung	1143

21 Troubleshooting im Windows Server

1145

21.1	Die Windows-Ereignisanzeige	1145
21.1.1	Konfiguration der Log-Eigenschaften	1152
21.1.2	Eine Überwachung einrichten	1156
21.1.3	Verwenden des Windows Admin Centers	1161
21.2	Die Leistungsüberwachung	1161
21.2.1	Ressourcenmonitor	1166
21.2.2	Leistungsindikatoren und die »üblichen Verdächtigen«	1168
21.2.3	CPU	1171
21.2.4	Arbeitsspeicher	1173
21.2.5	Datenträger	1174
21.2.6	Netzwerk	1174
21.2.7	Datensammlersätze	1175
21.3	Erstellen und Auswerten eines Startvorgangs	1178
21.4	Erstellen und Lesen eines Netzwerktraces	1181
21.4.1	Microsoft Network Monitor 3.4	1182
21.4.2	Microsoft Message Analyzer	1184
21.4.3	Wireshark	1185
21.4.4	Beziehen einer IP-Adresskonfiguration	1186
21.4.5	Anmeldung eines Benutzers an einem System	1188
21.4.6	Zugriff auf einen Webdienst	1190
21.5	Debugging	1191
21.5.1	Aktivieren der zusätzlichen Protokollierungsoptionen	1192
21.5.2	Erzeugen und Prüfen von Memory-Dumps	1194

22 Security in und mit dem Windows Server

1199

22.1	Sicherheitsprinzipien	1199
22.1.1	Protect, Detect, Respond	1199
22.1.2	Das Least-Privilege-Prinzip	1200
22.1.3	Berechtigungssysteme innerhalb von Windows	1201
22.1.4	Stellenwert von Identitäten	1202
22.1.5	Härtung von Systemeinstellungen und Anwendungen	1204
22.1.6	Das Clean-Source-Prinzip	1205
22.1.7	Trusted Platform Modul, UEFI Secure Boot und virtualisierungsbasierte Sicherheit	1207

22.2 Das Tier-Modell und das Enterprise Access Model	1211
22.2.1 Pass the Hash und Pass the Ticket	1211
22.2.2 Schutz von privilegierten Usern durch ein Ebenenmodell	1211
22.2.3 Enterprise Access Model	1216
22.2.4 Logon-Beschränkungen	1218
22.2.5 Security Baselines anwenden	1221
22.2.6 Protected Users	1227
22.2.7 Organisationseinheiten (OUs) und Delegationen erstellen	1228
22.3 Praxisbeispiele, mit denen Sie die Sicherheit in Windows Server 2019 erhöhen	1232
22.3.1 Installation und Konfiguration von LAPS	1232
22.3.2 Windows Event Forwarding zur Zentralisierung von Log-Informationen	1245
22.3.3 Die Verwendung von Standardgruppen einschränken	1254
22.3.4 Gruppenverwaltete Dienstkonten	1256
22.3.5 Security Center in Windows Server 2019	1258
22.3.6 Cloud-basierte Erkennungsmechanismen für Windows Server 2019	1261
22.4 Erweiterte Maßnahmen zum Schutz von Windows-Umgebungen	1266
22.4.1 Sicherer Zugriff auf Windows Server 2019 durch Privilege Access Workstations	1266
22.4.2 Authentication Policies und Silos	1268
22.4.3 Defender for Identity	1273
22.4.4 Ausblick auf Red Forest	1277
Glossar	1281
Index	1305