

Auf einen Blick

■ Teil 1 - Einführung und Grundlagen

1 Einführung in Windows Server 2012 R2	33
2 Einführung in Active Directory	51
3 Sicherheit in Active Directory-Domänendienst-Umgebungen	123

■ Teil 2 - Planung, Aktualisierung und Migration

4 Planung einer Active Directory-Domänendienst-Infrastruktur	156
5 Aktualisierung vorhandener Gesamt- und Domänenstrukturen	223
6 Migration von Gesamtstrukturen und Domänen	237

■ Teil 3 - Implementierung, Verwaltung und Wartung

7 Installation und Konfiguration von Windows Server 2012 R2.....	259
8 Implementierung und Verwaltung von Domain Name System (DNS)	292
9 Implementieren der Active Directory-Domänendienste (AD DS).....	322
10 Verwalten der Betriebsmasterrollen	354
11 Verwaltung globaler Katalogserver.....	373
12 Erstellen und Verwalten von Organisationseinheiten	381
13 Delegierung der Verwaltungsfunktionalität	395
14 Erstellen und Verwalten von Active Directory-Objekten.....	404
15 Erstellen und Verwalten von Gruppenrichtlinienobjekten	459
16 Verwaltung der Benutzerumgebung mit Gruppenrichtlinienobjekten.....	526
17 Planung und Einsatz von Kennworteinstellungen	565
18 Schreibgeschützte Domänencontroller.....	572
19 Domänencontroller unter Server Core.....	603
20 Verwaltung von Standorten und Replikation	631
21 Wartung und Diagnose der Active Directory-Domänendienste	645
22 Sichern und Wiederherstellen der Active Directory-Domänendienste	660
23 Weitere Active Directory-Dienste.....	685

Stichwortverzeichnis.....	691
---------------------------	-----

Inhaltsverzeichnis

Vorwort.....	29
Aufbau des Buches	30
Konventionen und Symbole.....	30
Teil 1: Einführung und Grundlagen	31
1 Einführung in Windows Server 2012 R2	33
1.2 Unterstützte Serverrollen und -funktionen.....	34
1.2.1 Unterstützte Serverrollen.....	34
1.2.1 Unterstützte Features (Funktionen)	36
1.3 Neuerungen und Verbesserungen	39
1.3.1 Der Anmeldebildschirm.....	39
1.3.2 Die grafische Benutzeroberfläche	40
1.3.3 Der grafische Server-Manager	41
1.3.4 Server Core - Grafikoberfläche nachträglich aktivierbar	42
1.3.5 Neuerungen im Windows-Explorer	43
1.3.6 Die Windows PowerShell 4.0.....	44
1.3.7 Active Directory-Verwaltungscenter	44
1.3.8 Active Directory-Papierkorb - jetzt grafisch.....	45
1.3.9 Verbesserte Kennwortrichtlinienverwaltung	46
1.3.10 Active Directory-basierte Aktivierung.....	47
1.3.11 Klonen von Domänencontrollern.....	47
1.3.12 Dynamische Zugriffssteuerung.....	48
1.3.13 Essentials Experience - für kleine Firmen und Institutionen	48
Merkmale der Essentials Experience-Serverrolle.....	48
1.3.14 Weitere Verbesserungen und Neuerungen.....	50
1.4 Zusammenfassung.....	50
2 Einführung in Active Directory	51
2.1 Was ist ein Verzeichnisdienst?	51
2.2 Merkmale der Active Directory-Domänendienste	52
2.3 Der X.500-Standard und die Microsoft Active Directory-Domänendienste.....	52
2.3.1 Das Lightweight Directory Access Protocol (LDAP)	54

2.3.2 Der Namenskontext	54
Distinguished Name (DN)	55
Relative Distinguished Name (RDN)	55
LDAP Uniform Resource Locator (URL)	55
User Principal Name (UPN)	56
2.3.3 Das Kerberos-Protokoll	56
2.4 Die Architektur	57
2.5 Die physikalischen Komponenten der Active Directory-Domänendienste	58
2.5.1 Die Datenbank	59
Aufteilung in einzelne Partitionen	59
Replikation der Partitionsinhalte	60
Das Datenspeicherungsmodell	61
Schnittstellen für den Datenbankzugriff	62
Die Datenbankdateien	63
Die Extensible Storage Engine (ESE)	64
Der Ablauf von Transaktionen	65
2.5.2 Domänencontroller	66
2.5.3 Schreibgeschützte Domänencontroller	66
Einsatzzweck von RODCs	66
Weitere Funktionen	68
Zwischenspeichern von Kennwörtern auf RODCs	68
Delegierung der Verwaltungsberechtigung	68
Einschränkungen schreibgeschützter Domänencontroller	68
2.5.4 Die Betriebsmasterrollen	69
Gesamtstrukturweite Betriebsmasterrollen	69
Domänenweite Betriebsmasterrollen	70
Tools zur Verwaltung der Betriebsmasterrollen	71
2.5.5 Der globale Katalog	72
Globaler Katalog und der Infrastruktur-Master	74
2.5.6 Zwischenspeichern der universellen Gruppenmitgliedschaft	75
Vorteile	76
Ablauf des Anmeldevorgangs	76
2.5.7 Der Replikationsdienst	77
Die Replikationstopologie	78
Inter-Site Topology Generator	80
Replikation der Inhalte von Verzeichnispartitionen	80

Multimaster-Replikation	81
Dringlichkeitsreplikation (Urgent Replication).....	81
Lokale USN.....	82
Replikationskonflikte.....	83
Replikation zwischen Standorten.....	84
Optimierung des Client-Anmeldeverkehrs.....	84
2.6 Die logischen Komponenten der Active Directory-Domänendienste.....	84
2.6.1 Das Active Directory-Schema	86
Gründe für die Änderung des Active Directory-Schemas.....	87
Tools zum Verwalten des Active Directory-Schemas	88
2.6.2 Verzeichnispartitionen	88
Tools zum Verwalten von Verzeichnispartitionen	89
2.6.3 Gesamtstrukturen	89
2.6.4 Vertrauensstellungen	91
Bidirektionale, transitive Vertrauensstellungen	92
Gesamtstrukturvertrauensstellung	93
Verknüpfte Vertrauensstellung.....	94
Externe Vertrauensstellung	95
Bereichsvertrauensstellung	96
Tools zum Verwalten von Vertrauensstellungen.....	96
2.6.6 Domänen.....	97
Tools zum Verwalten von Domänen	99
2.6.7 Authentifizierung und Autorisierung	99
Der Authentifizierungsprozess.....	99
Der Autorisierungsprozess	100
2.6.8 Organisationseinheiten	102
Beispiel für die Strukturierung von Organisationseinheiten	103
Delegierung der Verwaltungsberechtigung	104
Tools zum Verwalten von Organisationseinheiten.....	104
2.6.9 Standorte	105
Tool zum Verwalten von Active Directory-Standorten	106
2.6.10 Subnetz.....	106
Beispiel für den Einsatz von Subnetzen in Active Directory-Domänen	107
Tool zum Verwalten von Subnetzen	107
2.7.3 Heraufstufen einer Domänen- oder Gesamtstrukturfunktionsebene.....	111
Heraufstufen der Domänenfunktionsebene	112

Heraufstufen der Gesamtstrukturfunktionsebene.....	112
2.8 Active Directory- Domänendienste und das Domain Name System (DNS)	113
2.8.1 Die DNS-Namenszonen.....	114
Forward-Lookup-Zone	114
Reverse-Lookup-Zone	115
2.8.2 DNS-Zonentypen	115
2.8.3 Standardspeicherorte für DNS-Zonendaten	116
2.8.4 Dynamische oder statische Registrierung	116
DNS und DHCP	117
2.8.4.2 Sichere dynamische Aktualisierung.....	118
2.8.5 DNS-Ressourceneinträge.....	118
2.8.6 SRV-Einträge	119
Arten von Diensteinträgen.....	120
2.9 Zusammenfassung	122
3 Sicherheit in Active Directory-Domänendienst-Umgebungen	123
3.1 Grundlagen	123
3.1.1 Sicherheitsprinzipale.....	123
Beispiel für eine Sicherheitskennung (SID)	124
Standardmäßige Sicherheitskennungen	124
Löschen von Objekten	125
Discretionary Access Control List (DACL)	126
System Access Control List (SACL)	127
3.1.3 Authentifizierung & Autorisierung.....	127
3.1.4 Zugriffstoken.....	128
3.1.5 Kerberos V5-Protokoll.....	128
Kerberos - unterstützte Verschlüsselungstypen	130
Festlegen der AES-Verschlüsselung für Kerberos.....	130
Standardmäßiger Fallback zu NTLM.....	131
Kerberos-Konfiguration unter Windows Server 2012 (R2).....	131
Ports für die Kerberos-Authentifizierung.....	132
Tools für die Kerberos-Verwaltung und -Problembehandlung.....	133
3.1.6 NTLM-Protokoll	133
Situationen für die Verwendung des NTLM-Protokolls	133
Vergleich von LM, NTLM und NTLMv2	134
Verhindern der Zwischenspeicherung von LM-Hashes.....	134
Konfiguration der Lan Manager-Authentifizierungsebene	136

3.2 Domänensicherheit	138
3.2.1 Vordefinierte Sicherheit	138
3.2.2 Microsoft Security Compliance Manager (SCM) 3.0	139
Problemloser Export in Gruppenrichtlinienobjekte möglich	140
Enthaltene Tools	141
3.3.2 Sicherheitsrichtlinien für Domänencontroller.....	142
Standardmäßige Gruppenrichtlinienobjekte	142
3.3.3 SMB - Zugriff auf Freigaben erst ab Version 2.0.....	142
3.3.4 Domänencontroller als Server Core-Installation	143
Grafische Benutzeroberfläche nachträglich wieder aktivierbar	143
3.3.5 Dynamische Zugriffssteuerung	144
3.3.6 Verbesserte Kennwortrichtlinienverwaltung.....	144
Funktionsweise	145
Auswertelogik	145
Schritte zum Erstellen abgestimmter Kennwortrichtlinien	147
Anzeigen der auf einen Benutzer angewandten abgestimmten Kennwortrichtlinien.....	147
3.3.7 Sicherheitsgruppe „Protected Users“	149
Vordefinierte Schutzfunktionen	149
Voraussetzungen für den erweiterten Schutz	150
3.3.8 Überwachung der Active Directory-Domänendienste.....	150
Konfiguration der erweiterten Überwachungsrichtlinien.....	150
Zusätzliche Konfiguration für die erweiterte Überwachung	151
Aktivierung der Überwachung einzelner Active Directory-Objekte.....	152
Dokumentation der Änderungen in der Ereignisanzeige	153
3.4 Zusammenfassung.....	153
Teil 2: Planung, Aktualisierung und Migration	155
4 Planung einer Active Directory-Domänendienste-Infrastruktur	156
4.1 Planung der Active Directory-Domänendienste	156
4.1.1 Der Masterplan	157
4.1.2 Sammeln von Informationen über das Unternehmen	158
Sammeln und Analysieren von Unternehmensanforderungen	159
4.1.4 Dokumentation der vorhandenen Netzwerkinfrastruktur	160
Projektvorbereitende Dokumentation	161
4.2 Analysieren der Entwurfsoptionen	162
4.2.1 Eine oder mehrere Gesamtstrukturen?	163

Maximale Anzahl an Domänen	163
Maximale Anzahl an Domänencontrollern.....	163
Maximale Anzahl an Active Directory-Objekten	163
4.2.2 Gesamtstrukturmodelle	164
Organisations-Gesamtstrukturmodell	164
Ressourcen-Gesamtstrukturmodell	164
Gesamtstrukturmodell mit eingeschränktem Zugriff	165
4.2.3 Gesamtstrukturübergreifende Vertrauensstellung	166
SID-Filterung	166
Authentifizierungsoptionen.....	167
UPN-Suffix-Routing	167
4.2.4 Entwerfen einer Domänenstruktur	168
Das Domänenmodell	168
Anzahl der erforderlichen Domänen.....	170
Die Stammdomäne der Gesamtstruktur	171
Die Domänen- und Gesamtstrukturfunktionsebene	172
Strategien für die Planung von DNS-Namensräumen.....	177
Merkmale der verschiedenen Namensstrategien.....	178
Empfehlungen für die Namensvergabe	179
4.2.6 Entwerfen einer Standorttopologie	180
Standorte (Sites)	180
Subnetz	181
Standortverknüpfung (Site Link)	181
Standortverknüpfungsbrücke (Site Link Bridge)	183
Replikationsprotokolle.....	184
Bridgeheadserver.....	185
4.3 Platzierung von Domänencontrollern	186
4.3.1 Empfehlungen für die Anzahl von Domänencontrollern	186
4.3.2 Schreibgeschützte Domänencontroller.....	186
Voraussetzung für den Einsatz von RODCs	187
RODC als globaler Katalogserver.....	188
RODC und die Zwischenspeicherung der universellen Gruppenmitgliedschaft	189
RODC und die Betriebsmasterrollen (FSMO-Roles).....	189
RODC und die Bridgehead-Server	189
Delegierung von RODCs	189
Schreibgeschützter DNS	190

4.3.3 Platzieren globaler Katalogserver.....	190
Globaler Katalog und der Anmeldeprozess	191
Globaler Katalog und die Infrastrukturmasterrolle	192
Der globale Katalog und Remote-Standorte.....	192
Richtlinien für die Platzierung von globalen Katalogservern	192
4.3.4 Platzieren der Betriebsmasterrollen	193
Standardmäßige Platzierung von Betriebsmasterrollen.....	193
Richtlinien für die Platzierung von Betriebsmasterrollen.....	194
Active Directory-Gesamtstruktur mit einer einzigen Domäne.....	194
Active Directory-Gesamtstruktur mit mehreren Domänen	195
4.4 Entwerfen einer Verwaltungsinfrastruktur.....	196
4.4.1 Bestimmen eines Verwaltungsmodells	196
Verwaltungsmodelle.....	197
Weitere Gesichtspunkte für die Auswahl eines Verwaltungsmodells.....	198
4.4.2 Planen einer Struktur für Organisationseinheiten	198
4.4.3 Delegieren der Verwaltungsfunktionalität.....	200
Vererbung der Verwaltungsberechtigung.....	200
Empfehlungen für den Entwurf von Organisationseinheitenstrukturen.....	201
4.5 Entwerfen von Strukturen für die Verwendung von Gruppenrichtlinienobjekten ..	201
4.5.1 Empfehlungen für die Planung der Struktur der Organisationseinheiten für die Verwendung von Gruppenrichtlinienobjekten	202
4.6 Entwerfen einer Strategie für Objekte	202
4.6.1 Benutzerobjekte	202
Unterschiede zwischen lokalen und Domänenbenutzerkonten.....	202
Eindeutigkeit anhand von Benutzerobjekten	203
Namensstrategie.....	203
Teilzeitkräfte, externe Mitarbeiter, Praktikanten und Dienstkonten	204
Benutzerprinzipalnamen (UPN).....	204
Entwerfen einer Kennwortrichtlinie für Benutzerobjekte	204
4.6.2 InetOrgPerson-Objekte.....	205
4.6.3 Kontaktobjekte	206
4.6.4 Gruppenobjekte	206
Gruppentypen.....	207
Konvertierung von Gruppen.....	207
Gruppenbereiche.....	207
Delegierung der Verwaltung der Gruppenmitgliedschaft	209

Active Directory-Standardgruppen.....	209
4.6.5 Planungsstrategien für Gruppen.....	214
Die „A-G-DL-P“-Regel.....	214
Die „A-G-G-DL-P“-Regel.....	215
Die „A-G-U-DL-P“-Regel.....	215
Die „A-G-L-P“-Regel.....	216
Die „A-G-P“-Regel.....	217
Verwendung neuer oder vorhandener Gruppen?	217
4.6.6 Besondere Identitäten.....	217
4.6.7 Computerobjekte	218
Sicherheit durch Kennwortvereinbarung.....	218
Zurücksetzen von Computerkonten.....	219
Standardcontainer für Computerobjekte	219
Speicherung von Computerobjekten.....	220
4.6.8 Druckerobjekte.....	220
Gruppenrichtlinien für die Druckerkonfiguration	222
Druckerstandorte.....	222
4.6.9 Freigegebene Ordner-Objekte	222
4.7 Zusammenfassung.....	222
5 Aktualisieren vorhandener Gesamt- und Domänenstrukturen	223
5.1 Planen der Aktualisierungspfade.....	223
5.1.1 Unterstützte Aktualisierungspfade zu Windows Server 2012 R2.....	224
5.1.2 Unterstützte Aktualisierungspfade zu Windows Server 2012	225
5.2 Planen der Domänen- und Gesamtstrukturfunktionsebene	226
5.2.1 Vergleich der Domänen- und Gesamtstrukturfunktionsebenen.....	226
5.2.2 Mitgliedsserver und Clientcomputer.....	230
Windows 8/8.1 und Windows 10 als Clientbetriebssystem	231
5.3 Der Aktualisierungsvorgang.....	231
5.3.1 Aktualisierung des Betriebssystems der Domänencontroller.....	232
5.3.2 Domänenaktualisierung durch das Hinzufügen von Windows Server 2012 R2 bzw. Windows Server 2012-Domänencontrollern.....	233
5.3.3 Vorbereitung der Active Directory-Umgebung	233
Vorbereitung der Active Directory-Gesamtstruktur	234
Vorbereitung der Active Directory-Domäne	235
Vorbereitung der Domänen für den Einsatz eines RODCs.....	235

Aktualisieren der Berechtigungen für DNS-Anwendungsverzeichnispartitionen mittels adprep.exe.....	236
5.4 Zusammenfassung.....	237
6 Migration von Gesamtstrukturen und Domänen	237
6.1 Mögliche Migrationspfade.....	238
6.1.1 Neustrukturierung.....	238
SID-History und der Zugriff auf Ressourcen.....	240
6.2 Gesamtstrukturübergreifende Migration.....	240
6.2.1 Einrichtung der neuen Gesamtstruktur.....	241
6.2.2 Erstellen von Benutzerkonten für den Migrationsvorgang.....	241
6.2.3 Einrichtung von Vertrauensstellungen.....	242
6.2.4 Installation des Active Directory Migration Tools (ADMT).....	242
Mögliche Migrationsschritte mit ADMT.....	243
Migration von Benutzerkontenkennwörtern.....	244
6.2.5 Aktivierung der Überwachung in der Quell- und Zieldomäne.....	244
6.2.6 Migration der Gruppen.....	245
6.2.7 Migration der Benutzerkonten.....	247
Migration von Benutzerkonten in der Praxis.....	248
6.2.8 Migration der Computerkonten.....	248
6.2.9 Migration der Dienstkonten.....	250
6.2.10 Migration der Domänenressourcen der Quell- zur Zieldomäne.....	251
6.2.11 Auflösung der alten Gesamtstruktur.....	251
6.3 Gesamtstrukturinterne Migration.....	251
6.3.1 Wichtiger Unterschied zur gesamtstrukturübergreifenden Migration.....	252
6.4 Alternative zur Migration: Gesamtstrukturvertrauensstellungen.....	252
6.4.1 Vor- und Nachteile.....	253
6.4.2 Einrichtung von Gesamtstrukturvertrauensstellungen.....	254
6.5 Zusammenfassung.....	255
Teil 3: Implementierung, Verwaltung und Wartung	257
7 Installation und Konfiguration von Windows Server 2012 R2.....	259
7.1 Neuinstallation oder Aktualisierung?.....	259
7.2 Neuinstallation von Windows Server 2012 R2.....	259
7.2.1 Voraussetzungen.....	260
Hardwareanforderungen.....	260
7.2.2 Bestimmen der zu verwendenden Betriebssystemedition.....	261

Verfügbare Betriebssystemeditionen	261
Enthaltene Virtualisierungsrechte.....	262
Erweiterbarkeit der Virtualisierungsrechte	263
Spätere Aktualisierung von Standard- auf Datacenter-Lizenz.....	263
Spätere Aktualisierung von Essentials- auf Standard-Lizenz.....	264
7.2.3 Digital signierte Treiber erforderlich	264
7.2.4 Schritte zur Vorbereitung der Installation.....	265
7.2.5 Installationsschritte.....	266
7.2.6 Unbeaufsichtigte Installation.....	271
7.3 Konfigurationsschritte nach der Installation.....	271
7.3.1 Systemeigenschaften im Server-Manager	271
7.3.2 Schritte zur Konfiguration der Systemeigenschaften	273
7.4 Aktivierung des Betriebssystems	273
7.4.1 Produktaktivierung oder „Volume Activation“	274
Volumenaktivierung (Volume Activation)	274
7.4.2 Aktivierung über Active Directory	275
7.4.3 (Einzel-)Produktaktivierung.....	276
Aktivierung über das Internet.....	276
Telefonische Aktivierung	277
Aktivierung über die Kommandozeile	278
7.4.4 Erneute Aktivierung?.....	278
7.5 Aktualisierung vorhandener Serversysteme.....	278
7.5.1 Unterstützte Aktualisierungspfade.....	279
7.5.2 Notwendige Schritte vor der Aktualisierung.....	280
7.5.3 Digital signierte Treiber erforderlich	282
7.5.4 Vorbereitung der Active Directory-Umgebung	283
Vorbereitung der Active Directory-Gesamtstruktur (forestprep).....	284
Vorbereitung der Active Directory-Domäne (domainprep).....	284
7.5.5 Durchführung der Serveraktualisierung.....	284
7.5.6 Überprüfung der erfolgreichen Aktualisierung.....	291
7.6 Zusammenfassung	292
8 Implementierung und Verwaltung von Domain Name System (DNS)	292
8.1 Installation der DNS-Serverrolle	293
8.1.2 Installationsschritte.....	294
8.2 DNS-Namenszonen	295

8.2.1 Zonentypen.....	295
8.2.2 Forward-Lookup-Zonen.....	296
8.2.3 Reverse-Lookup-Zonen.....	296
8.3 Standardzonen.....	296
8.3.1 Primäre Standardzonen.....	297
8.3.2 Sekundäre Standardzonen.....	297
8.3.3 Erstellen von primären DNS-Namenszonen.....	297
8.3.4 Erstellen von sekundären DNS-Namenszonen.....	298
8.3.5 Umwandeln einer sekundären in eine primäre Namenszone.....	300
8.3.6 Active Directory-integrierte Zonen.....	300
8.3.7 Einrichten und Verwalten von Stub-Zonen.....	303
8.3.8 Einrichten und Verwalten von Reverse-Lookupzonen.....	305
8.4 Zonenübertragung.....	307
8.4.1 Konfiguration der Zonenübertragung.....	309
8.4.2 BIND-Sekundärzonen.....	310
8.4.3 Zonenreplikation im Vergleich zur Zonenübertragung.....	310
8.4.4 Speicherung von DNS-Namenszonen in Anwendungsverzeichnispartitionen....	311
Erstellen einer Anwendungsverzeichnispartition.....	311
Speicherung von Zonendaten in einer Anwendungsverzeichnispartition.....	312
8.5 Verwalten von DNS-Einträgen.....	312
8.5.1 Manuelles Erstellen von DNS-Einträgen.....	313
8.5.2 Dynamische Aktualisierung.....	313
8.5.3 DNSUpdateProxy.....	314
8.5.4 Änderungs- und Aufräumprozess.....	315
Konfiguration des Änderungs- und Aufräumvorgangs für eine DNS-Namenszone.....	315
Aktivierung des automatischen Aufräumvorgangs bei veralteten Ressourceneinträgen.....	316
8.6 Manuelles Löschen von DNS-Einträgen.....	317
8.7 WINS-Forward-Lookup.....	317
8.8 Bedingte Weiterleitungen.....	318
8.9 Starten und Beenden des DNS-Dienstes.....	320
8.10 Entfernen von DNS-Namenszonen.....	320
8.11 Entfernen der DNS-Dienste.....	321
8.12 Zusammenfassung.....	322
9 Implementieren der Active Directory-Domänendienste (AD DS).....	322

9.1 Installationsarten.....	323
9.2 Vorbereitende Schritte zur Installation	323
9.3 Installationsmethoden.....	324
9.3.1 Installation über den Server-Manager.....	324
Schritt 1: Installation der Serverrolle	324
Schritt 2: Heraufstufen des Servers zu einem Domänencontroller	326
9.3.2 Installation mithilfe der Windows PowerShell	330
9.3.3 Unbeaufsichtigte Installation.....	331
9.4 Überprüfung der erfolgreichen Installation	333
9.5 Installation von einem Medium.....	334
9.5.1 Erstellen eines Installationsmediums	334
Erstellen eines Installationsmediums mittels Ntdsutil.exe.....	334
Schritte zur Installation von einem Medium	336
9.6 Entfernen der Active Directory-Domänendienste	342
9.6.1 Vorbereitung des Herunterstufens eines Domänencontrollers.....	342
9.6.2 Herunterstufen eines Domänencontrollers	343
9.6.3 Entfernen der Active Directory-Domänendienste als Rolle.....	347
9.6.4 Entfernen der Active Directory-Domänendienste erzwingen.....	350
Auswirkungen nach dem erzwungenen Herabstufen eines Domänencontrollers	351
Bereinigung der Metadaten	352
9.6 Zusammenfassung.....	353
10 Verwaltung der Betriebsmasterrollen.....	354
10.1 Betriebsmasterrollen in einer Active Directory-Gesamtstruktur.....	354
10.1.1 Schemamaster.....	354
10.1.2 Domänennamenmaster.....	355
10.1.3 PDC-Emulator.....	356
10.1.4 RID-Master	357
10.1.5 Infrastrukturmater	357
Infrastrukturmater und der globale Katalog.....	358
10.2 Verschieben von Betriebsmasterrollen.....	359
10.2.1 Gründe für das Verschieben von Betriebsmasterrollen.....	359
10.2.2 Auswirkungen auf die Active Directory-Infrastruktur.....	359
Übergabe der Rollen beim Herunterstufen	359
10.2.3 Notwendige Berechtigungen.....	360
10.2.4 Ermitteln des Rolleninhabers der Betriebsmasterrollen.....	360

Ermitteln des Schemamaster-Rolleninhabers	361
Domänennamenmaster.....	363
PDC-Emulator	363
RID-Master.....	364
Infrastrukturmaster	364
10.2.5 Übertragen der Betriebsmasterrollen	364
Übertragung der Betriebsmasterrollen mittels Windows PowerShell.....	365
Schemamaster	366
Domänennamenmaster.....	367
PDC-Emulator, RID-Master und Infrastrukturmaster.....	367
10.3 Übernahme der Betriebsmasterrollen bei Ausfall des aktuellen Rolleninhabers	368
10.3.1 Gründe für die Übernahme der Betriebsmasterrollen.....	369
10.3.2 Mögliche Auswirkungen des Ausfalls.....	370
10.3.3 Übernehmen der Betriebsmasterrollen	371
Übernahme der Betriebsmasterrollen mittels Windows PowerShell erzwingen	371
Übernahme der Betriebsmasterrollen mittels ntdsutil.exe erzwingen	372
10.4 Zusammenfassung	372
11 Verwaltung globaler Katalogserver.....	373
11.1 Funktionen des globalen Katalogservers	373
11.2 Ausfall eines globalen Katalogservers	374
11.3 Zuweisen der Funktion als globaler Katalogserver	374
11.4 Anpassen des globalen Katalogs.....	376
11.5 Zwischenspeichern der universellen Gruppenmitgliedschaft	379
11.6 Zusammenfassung	380
12 Erstellen und Verwalten von Organisationseinheiten.....	381
12.1 Planen und Erstellen von Organisationseinheiten.....	381
12.2 Werkzeuge zum Erstellen und Verwalten von Organisationseinheiten.....	382
12.3 Erstellen von Organisationseinheiten	383
12.3.1 Erstellen im Active Directory-Verwaltungszentrum	383
12.3.2 Erstellen mittels MMC-Snap-In.....	384
12.3.3 Organisationseinheit erstellen mit dsadd.exe.....	384
12.3.4 Erstellen mittels Ldifde.exe.....	386
12.3.5 Verwenden der Eingabedatei mit Ldifde.exe	387
12.3.6 Erstellen mittels Windows Script Host.....	388
12.3.7 Erstellen mittels Windows PowerShell	389

12.4 Löschen von Organisationseinheiten	390
12.4.1 Löschen im Active Directory-Verwaltungscenter	390
12.4.2 Löschen mittels MMC-Snap-In.....	391
12.4.3 Löschen mittels von dsrm.exe	392
12.4.4 Löschen mittels Windows PowerShell	393
12.5 Verwaltung der Attributwerte von Organisa-tionseinheiten	393
12.6 Zusammenfassung.....	395
13 Delegierung der Verwaltungsfunktionalität	395
13.1 Schritte zur Delegierung der Verwaltungsberechtigung.....	396
13.2 Vererbung der Verwaltungsberechtigung	397
13.2.1 Blockieren der Vererbung der Verwaltungsberechtigung.....	397
Schritte zum Blockieren der Vererbung	397
13.3 Überprüfen der Delegierung der Verwaltungsberechtigung	398
13.3.1 Effektive Berechtigungen.....	399
13.4 Beendigung der Delegierung der Verwaltungsberechtigung	400
13.5 Bereitstellen angepasster Verwaltungskonsolen	400
13.5.1 Erstellen einer angepassten Verwaltungskonsole	401
13.6 Zusammenfassung.....	403
14 Erstellen und Verwalten von Active Directory-Objekten.....	404
14.1 Benutzerobjekte.....	404
14.1.1 Tools zum Erstellen und Verwalten von Benutzerobjekten	404
14.1.2 Erstellen von Benutzerobjekten mittels MMC-Snap-In.....	406
14.1.3 Erstellen von Benutzerobjekten im grafischen Active Directory-Verwaltungscenter (AD AD)	406
14.1.4 Erstellen von Benutzerobjekten mittels dsadd.exe	408
14.1.5 Erstellen von Benutzerobjekten mittels csvde.exe.....	409
Die Eingabedatei.....	409
Befehlsausführung	410
Nachteil bei der Verwendung von csvde.exe	410
14.1.6 Erstellen von Benutzerobjekten mittels ldifde.exe	411
Die Eingabedatei.....	411
Befehlsausführung	412
Nachteil bei der Verwendung von ldifde.exe	412
14.1.7 Erstellen von Benutzerobjekten mit net user.....	413
14.1.8 Erstellen von Benutzerobjekten mittels Windows Script Host (WSH)	413

Die Scriptdatei	413
Ausführung von WSH-Scripts	414
14.1.9 Erstellen von Benutzerobjekten mittels Windows PowerShell	415
14.2 Kontingente in Active Directory	415
14.2.1 Einrichtung und Verwaltung	416
14.2.2 Erstellen eines neuen Kontingenteintrags	416
14.2.3 Anzeige aller vorhandenen Kontingenteinträge	417
Ermitteln der Besitzer der meisten Active Directory-Objekte	417
14.2.4 Ändern vorhandener Kontingenteinträge	417
14.2.5 Löschen von Kontingenteinträgen	418
14.3 Verwalten von Benutzerobjekten	418
14.3.1 Attribut-Editor	418
14.3.2 Kopieren von Benutzerkonten	419
Pfadangaben in Benutzerkontenvorlagen	420
Empfehlungen für das Erstellen und Verwenden von Benutzerkontenvorlagen	420
14.3.3 Entsperren von Benutzerkonten	421
14.3.4 Zurücksetzen der Benutzerkontenkennwörter	422
14.3.5 Deaktivieren bzw. Aktivieren von Benutzerkonten	424
14.3.6 Löschen von Benutzerkonten	425
Schutz vor versehentlichem Löschen	425
14.4 Benutzerprofile und Basisverzeichnisse	426
14.5 Dienstkonten	427
14.5.1 Standardmäßig vorhandene Dienstkonten	427
14.5.2 Gruppenverwaltete Dienstkonten (Group Managed Service Accounts, gMSA)	428
Vorbereitung für den Einsatz gruppenverwalteter Dienstkonten (gMSA)	428
Speicherort gruppenverwalteter Dienstkonten	429
Erstellen gruppenverwalteter Dienstkonten	429
Schritte zur Verwendung gruppenverwalteter Dienstkonten	430
Grafische Verwaltung mittels Managed Service Accounts GUI	431
14.6 InetOrgPerson-Objekte	431
14.8 Gruppenobjekte	432
14.8.1 Gruppentypen	433
14.8.2 Gruppenbereiche	433
14.8.3 Vordefinierte Gruppen	434
Standardgruppen im Builtin-Container	435

Standardgruppen im Users-Container	437
14.8.4 Gruppenstrategien	438
14.8.5 Erstellen und Verwalten von Gruppenobjekten.....	441
Erstellen von Gruppenobjekten mittels MMC-Snap-In	442
Erstellen von Gruppenobjekten im grafischen Active Directory-Verwaltungscenter (AD AC)	443
Erstellen von Gruppenobjekten mittels dsadd.exe.....	443
Erstellen von Gruppenobjekten mit der Windows PowerShell	444
14.9 Computerobjekte	445
14.9.1 Erstellen von Computerobjekten.....	445
Erstellen von Computerobjekten mittels MMC-Snap-In.....	446
Erstellen von Computerobjekten mittels Windows PowerShell	447
Erstellen von Computerobjekten mittels net computer.....	447
14.9.2 Berechtigung zum Hinzufügen von Arbeitsstationen zur Domäne.....	449
14.9.3 Verwalten von Computerobjekten.....	449
14.10 Verwaltung von Druckerobjekten	452
14.11 Veröffentlichung von freigegebenen Ordnern	454
14.12 Suche nach Objekten	457
14.12.1 Gespeicherte Abfragen	457
14.13 Zusammenfassung	459
15 Erstellen und Verwalten von Gruppenrichtlinienobjekten	459
15.1 Einführung und Funktionsweise	460
15.1.1 Konfigurierbare Einstellungen	461
15.1.2 Speicherorte von Gruppenrichtlinienobjekten.....	462
15.1.3 Komponenten der Gruppenrichtlinienvorlagen	464
15.1.4 Neuerungen in Windows Server 2012 R2	465
15.1.5 Die Richtlinienverarbeitungsfolge.....	466
15.1.6 Die Gruppenrichtlinienverarbeitung	468
15.2 Der Gruppenrichtlinienaktualisierungsprozess	470
15.2.1 Dynamische Aktualisierung	470
15.2.2 Manuelle Aktualisierung	475
Gruppenrichtlinienupdate - aus der grafischen Konsole	475
15.3 Loopbackverarbeitungsmodus	477
15.4 Die Gruppenrichtlinienverwaltungskonsolle (GPMC).....	479
15.4.1 Verwaltungsmöglichkeiten	479

15.4.2 Installation der Gruppenrichtlinienverwaltungskonsole (GPMC)	480
15.5 Arbeiten mit Gruppenrichtlinienobjekten	482
15.5.1 Erstellen eines neuen Gruppenrichtlinienobjekts	482
15.5.2 Bearbeiten von Gruppenrichtlinienobjekten	483
15.5.3 Löschen von Gruppenrichtlinienobjekten	484
15.5.4 Wiederherstellen der Standardrichtlinienobjekte	485
15.6 Starter-Gruppenrichtlinienobjekte	486
15.6.1 Einrichten des Speicherorts für Starter-Gruppenrichtlinienobjekte	486
15.6.2 Erstellen von Starter-Gruppenrichtlinienobjekten	487
15.6.3 Bearbeiten eines Starter-Gruppenrichtlinienobjekts	488
15.6.4 Löschen eines Starter-Gruppenrichtlinienobjekts	489
15.6.5 Exportieren und Importieren von Starter-Gruppenrichtlinienobjekten	489
15.6.6 Erstellen eines neuen Gruppenrichtlinienobjekts aus einem Starter-Gruppenrichtlinienobjekt	491
15.7 Verknüpfen von Gruppenrichtlinienobjekten	493
15.7.1 Erstellen der Verknüpfung eines Gruppenrichtlinienobjekts mit einer Organisationseinheit (OU)	493
15.7.2 Löschen der Verknüpfung eines Gruppenrichtlinienobjekts	494
15.7.3 Deaktivieren einer Gruppenrichtlinienverknüpfung	495
15.7.4 Festlegen der Verknüpfungsreihenfolge	496
15.8 Gruppenrichtlinienvererbung	497
15.8.1 Vererbung deaktivieren	498
15.8.2 Erzwingen von Gruppenrichtlinien	499
15.9 Filterung von Gruppenrichtlinienobjekten	500
15.9.1 Die Sicherheitsfilterung	500
15.9.2 Die WMI-Filterung	502
15.10 Delegieren der Gruppenrichtlinienverwaltung	507
15.10.1 Delegierungsumfang	507
15.10.2 Delegierungsmöglichkeiten	507
15.10.3 Berichterstellung und Auswertung	510
15.10.4 Gruppenrichtlinien dokumentieren	520
15.10.5 Sichern und Wiederherstellen von Gruppenrichtlinienobjekten	522
15.11 Zusammenfassung	525
16 Verwaltung der Benutzerumgebung mit Gruppenrichtlinienobjekten	526

16.1 Konfigurieren der Gruppenrichtlinieneinstellungen.....527

16.1.1 Konfiguration von Einzelwerten.....527

16.1.2 Konfiguration von Mehrfachwerten.....528

16.2 Die Erweiterungen für Gruppenrichtlinienvoreinstellungen529

16.2.1 Windows-Einstellungen530

16.2.2 Systemsteuerungseinstellungen.....530

16.2.3 Beispiel für die Anwendung von Windows-Einstellungen532

16.2.4 Zielgruppenadressierung.....534

16.3 Bereitstellen und Anwenden von Skripts mithilfe von Gruppenrichtlinien537

16.3.1 Beispiel für ein Anmeldeskript.....538

16.3.2 Anwenden eines Anmeldeskripts.....539

16.3.3 Speicherorte von Skriptdateien540

16.3.4 Überlegungen zur Planung von Skriptdateien.....540

16.4 Konfigurieren der Ordnerumleitung.....541

16.4.1 Vorteile der Ordnerumleitung.....542

16.4.2 Umleitbare Ordner543

16.4.3 Zieldefinition der Ordnerumleitung.....544

16.4.4 Weitere, konfigurierbare Einstellungen545

16.4.5 Sicherheitsaspekte bei der Ordnerumleitung547

16.4.6 Beispiele für die Konfiguration der Ordnerumleitung548

16.5 Konfigurieren der Benutzerumgebung549

16.5.1 Administrative Vorlagen550

Administrative Vorlagen als XML-Dateien551

Speicherort von .ADMX-Vorlagen.....551

Verbesserungen bei der Verwendung von ADMX-Vorlagen552

Hinzufügen von Gruppenrichtlinienvorlagen für Windows 10-Computer.....553

Einrichten eines zentralen Speichers554

16.5.2 Klassische administrative Vorlagen555

Standardmäßige ADM-Vorlagen556

Erstellen von eigenen administrativen Vorlagen (ADM-Dateien).....558

Konvertierung der klassischen administrativen Vorlagen558

Hinzufügen oder Entfernen von klassischen administrativen Vorlagen.....559

Filtern von administrativen Vorlagen.....561

16.6 Zusammenfassung.....564

17 Planung und Einsatz von Kennworteinstellungen.....565

17.1 Funktionsweise	566
17.1.1 Auswertelogik	567
17.2 Schritte zum Erstellen von Objekten für Kennworteinstellungen.....	569
17.3 Anzeigen der auf einen Benutzer angewandten Kennworteinstellungen.....	569
17.4 SpecOps Password Policy Basic	571
17.5 Zusammenfassung	572
18 Schreibgeschützte Domänencontroller.....	572
18.1 Vorteile beim Einsatz von RODCs	573
18.2 Einschränkungen beim Einsatz von RODCs.....	574
18.3 Platzierung von RODCs	575
18.4 Bereitstellen schreibgeschützter Domänencontroller (RODCs).....	575
18.4.1 Überprüfung der Gesamtstrukturfunktionsebene	576
18.4.2 Aktualisieren der Berechtigungen für DNS-Anwendungsverzeichnispartitionen	577
18.4.3 Installation eines RODC unter Windows Server 2012 R2	578
Installationsschritte	578
Heraufstufen des Servers zu einem RODC	580
18.4.4 Delegierung der Installation von RODCs.....	585
18.4.5 Durchführung der delegierten RODC-Installation	588
18.5 Verwaltung schreibgeschützter Domänencontroller.....	592
18.5.1 Verwaltung der Kennwortreplikationsrichtlinie.....	592
Steuerung der Replikation von Kennwörtern.....	593
Attribute für die Steuerung der Kennwortreplikation	594
18.6 Konfigurieren der Kennwortreplikationsrichtlinie für einen RODC.....	595
18.7 Anzeige der auf einem RODC zwischengespeicherten Anmeldeinformationen..	596
18.8 Überprüfung der für einen RODC authentifizierten Konten.....	597
18.9 Auffüllen des Kennwortcache für RODCs.....	598
18.9.1 Schritte zum Auffüllen des Kennwortcache.....	598
18.10 Überprüfen den Kennwortzwischenlagerung für einzelne Benutzer	599
18.11 Zurücksetzen von zwischengespeicherten Kennwörtern.....	600
18.12 Konfiguration zur Aufteilung der Administratorrolle auf RODCs	601
18.13 Zusammenfassung.....	602
19 Domänencontroller unter Server Core.....	603
19.1 Hardware-Anforderungen.....	604

19.2 Schritte zur Vorbereitung der Installation.....	604
19.3 Installationsschritte.....	605
19.4 Unbeaufsichtigte Installation.....	608
19.4.1 Vorteile der unbeaufsichtigten Installation.....	608
19.5 Erstkonfiguration.....	609
19.5.1 Festlegen des Administratorkennworts.....	609
19.5.2 Konfiguration einer statischen IP-Adresse	610
Konfiguration mithilfe der Windows PowerShell.....	611
Konfiguration mithilfe von sconfig	613
Konfiguration mithilfe von netsh.....	614
19.5.3 Umbenennen des Servers	614
Ändern des Servernamens mithilfe der Windows PowerShell.....	615
Ändern des Servernamens mithilfe von sconfig	615
Ändern des Servernamens mithilfe von netdom	615
19.5.4 Beitreten zu einer Active Directory-Domäne.....	616
Beitritt zu einer Active Directory-Domäne mithilfe der Windows PowerShell.....	616
Beitritt zu einer Active Directory-Domäne mithilfe von sconfig	617
Beitritt zu einer Active Directory-Domäne mithilfe von netdom.....	617
19.5.5 Aktivieren von Windows Server 2012 R2 als Server Core.....	618
19.5.6 Remoteaktivierung.....	618
19.5.7 Konfigurieren der Remoteverwaltung.....	619
Remoteverwaltung mithilfe von sconfig konfigurieren.....	619
Remoteverwaltung der Firewall-Konfiguration	620
19.6 Hinzufügen der grafischen Benutzeroberfläche unter Server Core	620
19.6.1 Wechsel von der Server Core-Installation zu einer Serverinstallation mit grafischer Benutzeroberfläche.....	621
19.7 Entfernen der grafischen Benutzeroberfläche.....	623
19.8 Server Core als DNS-Server.....	624
19.8.1 Installation der DNS-Serverrolle	625
19.8.2 Verwaltung des Server Core als DNS-Server	625
Alternative Verwaltung mittels dnscmd.exe	626
Alternative Verwaltung mittels Windows PowerShell	626
19.8.3 Entfernen der DNS-Serverrolle.....	626
19.9 Server Core als Domänencontroller.....	627
19.9.1 Heraufstufen über den grafischen Server-Manager.....	627

19.9.2 Unbeaufsichtigte Installation der Active Directory-Domänendienste mittels dcpromo.exe.....	628
Beispiel für die Datei Unattend.txt	628
19.9.3 Heraufstufen über die Windows PowerShell.....	629
Installation der Serverrolle der Active Directory-Domänendienste (AD DS) mittels Windows PowerShell.....	629
Heraufstufen des Serversystems zu einem Active Directory-Domänencontroller mittels Windows PowerShell	629
19.10 Zusammenfassung.....	630
20 Verwaltung von Standorten und Replikation	631
20.1 Standorte und die Replikation.....	631
20.2 Erstellen eines Active Directory-Standorts	632
20.3 Erstellen eines Subnet-Objektes.....	632
20.4 Erstellen einer Standortverknüpfung	633
20.4.1 Hinzufügen eines Standorts zu einer Standortverknüpfung.....	634
20.4.2 Entfernen von Standorten aus einer Standortverknüpfung	635
20.5 Planen der Replikation zwischen Active Directory-Standorten.....	636
20.5.1 Notwendige Kommunikationsports für die Replikation	637
20.5.2 Replikationstransport.....	637
Konfiguration des Zeitplans für die standortübergreifende Replikation	638
Konfiguration der Häufigkeit der standortübergreifende Replikation.....	639
20.6 Überprüfung und Problembehandlung.....	639
20.6.1 Standortermittlung mit nltest.exe.....	640
20.6.2 Überprüfung der Replikation mit Repadmin.exe.....	640
20.6.3 Überprüfung der Replikation mit Dcdiag.exe	641
20.6.4 Überprüfung der Replikation mit Windows PowerShell	642
20.6.5 Überprüfung der Replikation mit dem AD Replication Status Tool.....	642
20.6.6 LDAP-Echtzeitüberwachung mit ADInsight	643
20.6.7 ADExplorer	643
20.6.8 Überprüfung des Ereignisprotokolls.....	643
20.7 Zusammenfassung	644
21 Wartung und Diagnose.....	645
21.1 Überwachung der Active Directory-Domänendienste.....	645
21.1.1 Überwachung und Diagnose mithilfe der Ereignisanzeige	646
Zu überwachende Ereignisprotokolle	647

Ereignisdetails anzeigen.....	648
21.1.3 Überwachung mithilfe der Konsole Leistung	649
Hinzufügen von Indikatoren.....	650
21.1.4 Zuverlässigkeitsüberwachung	650
21.1.5 Sammlungssätze	651
21.2 Wartung der Active Directory-Domänendienste.....	653
21.2.1 Garbage Collection	653
21.2.2 Online- und Offline-Defragmentierung.....	654
Online-Defragmentierung.....	654
Offline-Defragmentierung	655
Integritätsprüfung der Active Directory-Datenbank	657
Semantik-Prüfung der Active Directory-Datenbank.....	657
Verschieben der AD-Datenbank und -Protokolldateien	658
21.3 Zusammenfassung.....	659
22 Sichern und Wiederherstellen der Active Directory-Domänendienste.....	660
22.1 Active Directory-Datensicherung.....	660
22.1.1 Unterstützte Sicherungstypen.....	660
22.1.2 Mögliche Wiederherstellungsarten	661
22.2 Installation der Windows Server-Sicherung	661
22.2.1 Datensicherung und Wiederherstellung mit der Windows PowerShell.....	662
22.3 Durchführung der Datensicherung	662
22.3.1 Vollständige Serversicherung eines Domänencontrollers.....	662
22.3.2 Ungeplante Sicherung wichtiger Volumes eines Domänencontrollers	663
22.4 Planen der täglichen Sicherung eines Domänencontrollers.....	663
22.4.1 Online-Sicherung.....	664
22.5 Durchführung der Datenwiederherstellung	665
22.5.1 Vollständige Serverwiederherstellung eines Domänencontrollers	665
Voraussetzungen für das Ausführen einer vollständigen Wiederherstellung eines Domänencontrollers	666
22.5.2 Active Directory aus der Datensicherung wiederherstellen.....	666
Ausführen einer nicht autorisierenden Wiederherstellung der Active Directory-Domänendienste (AD DS)	666
Vorgehensweise für die Durchführung einer nicht autorisierenden Wiederherstellung der Active Directory-Domänendienste (AD DS).....	668
Ausführen einer autorisierenden Wiederherstellung gelöschter Active Directory-Objekte ..	673
22.5.3 Reanimieren von Tombstone-Objekten	675

Verwenden von Ldp.exe zum Reanimieren von Tombstone-Objekten	676
Verwenden von AdRestore.exe zum Reanimieren von Tombstone- Objekten	678
22.6 Active Directory-Papierkorb - jetzt grafisch.....	679
22.6.1 Schritte zum Aktivieren des Active Directory-Papierkorbs.....	680
Aktivierung des Active Directory-Papierkorbs mittels Windows Power-Shell	682
22.6.2 Anzeigen und Wiederherstellen gelöschter Active Directory-Objekte.....	682
Anzeigen und Wiederherstellen mittels Windows PowerShell	682
22.7 Installation der AD-Domänendienste (AD DS) von einer Sicherung.....	683
22.7.1 Verschiedene Installationsmedien.....	683
22.7.2 Erstellen eines Installationsmediums.....	684
22.7.3 Einrichten eines neuen Domänencontrollers mithilfe eines Installationsmediums	685
22.8 Zusammenfassung	685
23 Weitere Active Directory-Dienste.....	685
23.1 Die Dienste im Überblick	686
23.2.1 Active Directory Lightweight Directory Services (AD LDS)	686
23.2.2 Active Directory-Zertifikatdienste (AD CS).....	687
23.2.3 Active Directory-Rechteverwaltungsdienste (AD RMS)	688
Rechtevergabe auf digitale Inhalte	688
23.2.4 Active Directory-Verbunddienste (AD FS)	689
Unterstützte Szenarien der AD FS	689
23.3 Zusammenfassung	689
Stichwortverzeichnis.....	691