

Inhalt

Vorwort	XV
Wissenswertes zu diesem Buch	XVII
1 Einleitung	1
1.1 Was sind Gruppenrichtlinien?	1
1.2 Auf welche Objekte wirken Gruppenrichtlinien?	2
1.3 Wann werden Gruppenrichtlinien verarbeitet?	2
1.4 Wie viele Gruppenrichtlinien sollte man verwenden?	3
1.5 Worauf muss man beim Ändern von Einstellungen achten?	3
1.6 Was Sie brauchen, um die Aufgaben nachvollziehen zu können	4
2 Die Gruppenrichtlinienverwaltung	5
2.1 Einführung	5
2.2 Gruppenrichtlinienverwaltung auf einem Server installieren	6
2.3 Gruppenrichtlinienverwaltung erkunden	8
2.4 Gruppenrichtlinienverknüpfungen und -objekte	8
2.5 Gruppenrichtlinienobjekte im Detail	9
2.5.1 Register BEREICH einer Gruppenrichtlinie	9
2.5.2 Register DETAILS eines GPO	10
2.5.3 Register EINSTELLUNGEN eines GPO	11
2.5.4 Register DELEGIERUNG eines GPO	12
2.5.5 Register STATUS eines GPO	12
2.6 Standorte und Gruppenrichtlinien	13
2.7 Weitere Elemente der Gruppenrichtlinienverwaltung	14
2.8 Gruppenrichtlinie erstellen	14
2.9 Gruppenrichtlinie verknüpfen	14
2.10 Gruppenrichtlinie bearbeiten	15
3 Verarbeitungsreihenfolge von Gruppenrichtlinien	17
3.1 Einführung	17
3.2 Grundlagen der Gruppenrichtlinienverarbeitung	17
3.3 Verarbeitungsreihenfolge in der Gruppenrichtlinienverarbeitung	18

3.4	Anpassungen der Verarbeitungsreihenfolge von GPOs	20
3.4.1	Bereiche von GPOs deaktivieren	20
3.4.2	Verknüpfungen aktivieren/deaktivieren	22
3.4.3	Vererbung deaktivieren	22
3.4.4	Erzwingen von GPOs	23
3.5	Loopbackverarbeitungsmodus	24
3.5.1	Loopbackverarbeitungsmodus einrichten	25
4	Gruppenrichtlinien filtern	29
4.1	Einführung	29
4.2	Filtern über Gruppenzugehörigkeiten	30
4.2.1	Sicherheitsfilterung verwenden	30
4.2.2	Berechtigungen verweigern	32
4.3	WMI-Filter	34
4.3.1	Einführung in WMI	34
4.3.2	WQL zum Filtern von GPOs	38
4.3.3	WMI-Filter erstellen	38
4.3.4	WMI-Filter anwenden	40
4.3.5	WMI-Filter entfernen	41
4.3.6	WMI-Filter exportieren	41
4.3.7	WMI-Filter importieren	42
4.3.8	Beispiele von WMI-Abfragen für WMI-Filter	42
4.3.9	WMI-Filter optimieren	43
5	Gruppenrichtlinien-Infrastruktur planen	45
5.1	Einführung	45
5.2	AD-Design und GPOs	46
5.2.1	OUs und Gruppenrichtlinien	47
5.2.2	GPOs und Sicherheitsfilterung	51
5.3	Wie viele Einstellungen gehören in ein GPO?	52
5.4	Benennung von GPOs	53
5.5	Dokumentieren von GPOs	54
5.6	Testen von GPOs	58
5.7	Empfohlene Vorgehensweisen	62
6	Softwareverteilung mit Gruppenrichtlinien	65
6.1	Einführung	65
6.2	Konzepte	66
6.2.1	Unterstützte Dateitypen	66
6.2.2	Softwareverteilung an Benutzer oder Computer	67
6.2.3	Zuweisen und Veröffentlichen	68
6.2.4	Kategorien	70
6.3	Praktisches Vorgehen	70
6.3.1	Vorbereitung	70
6.3.2	Gruppenrichtlinie für Zuweisung an Computer erstellen	71

6.3.3	Gruppenrichtlinie konfigurieren	71
6.3.4	Gruppenrichtlinienobjekt verknüpfen	73
6.3.5	Verteilung testen	73
6.3.6	Veröffentlichen für Benutzer	73
6.4	Eigenschaften von Paketen bearbeiten	74
6.4.1	Register ALLGEMEIN	74
6.4.2	Register BEREITSTELLUNG VON SOFTWARE	75
6.4.3	Register AKTUALISIERUNGEN	76
6.4.4	Register KATEGORIEN	78
6.4.5	Register ÄNDERUNGEN	78
6.4.6	Register SICHERHEIT	79
6.5	Probleme bei der Softwareverteilung	79
6.6	Software verteilen mit Specops Deploy/App	80
6.6.1	Verteilen der Client Side Extension	81
6.6.2	Erstellen eines Software-Verteilungspakets	82
6.6.3	Überprüfen der Installation	90
6.6.4	Ziele angeben mit Targetting	92
6.6.5	Konfiguration von Specops Deploy/App	94
6.6.6	Specops und PowerShell	94
6.6.7	Fazit	95
7	Sicherheitseinstellungen	97
7.1	Einführung	97
7.2	Namensauflösungsrichtlinie	98
7.3	Kontorichtlinien	100
7.3.1	Kennwortrichtlinien	101
7.3.2	Kontosperrungsrichtlinien	102
7.3.3	Kerberos-Richtlinien	103
7.3.4	Empfohlene Einstellungen für Kontorichtlinien	103
7.4	Lokale Richtlinien	104
7.4.1	Überwachungsrichtlinien	105
7.4.2	Zuweisen von Benutzerrechten	106
7.4.3	Sicherheitsoptionen	107
7.5	Ereignisprotokoll	116
7.6	Eingeschränkte Gruppen	118
7.7	Systemdienste, Registrierung und Dateisystem	120
7.7.1	Systemdienste	120
7.7.2	Registrierung	121
7.7.3	Dateisystem	122
7.8	Richtlinien im Bereich Netzwerksicherheit	123
7.8.1	Richtlinien für Kabelnetzwerke	123
7.8.2	Windows Firewall	125
7.8.3	Netzwerklisten-Manager-Richtlinien	132
7.8.4	Drahtlosnetzwerkrichtlinien	135
7.8.5	Richtlinien für öffentliche Schlüssel	139

7.8.6	Softwareeinschränkungen	150
7.8.7	Netzwerkzugriffsschutz	155
7.8.8	Anwendungssteuerung mit AppLocker	155
7.8.9	IP-Sicherheitsrichtlinien	171
7.8.10	Erweiterte Überwachungsrichtlinienkonfiguration	171
7.9	Sicherheitsvorlagen und das Security Compliance Toolkit	173
7.9.1	Sicherheitsvorlagen	173
7.9.2	Der Policy Analyzer	177
7.9.3	Security Baselines anwenden	180
8	Administrative Vorlagen	183
8.1	Einführung	183
8.2	ADMX und ADML	184
8.3	Zentraler Speicher	185
8.4	ADM-Vorlagen hinzufügen	188
8.5	Administrative Vorlagen verwalten	189
8.6	Administrative Vorlagen – Computerkonfiguration	192
8.6.1	Drucker	192
8.6.2	Netzwerkeinstellungen	194
8.6.3	Startmenü und Taskleiste	200
8.6.4	System	200
8.6.5	Systemsteuerung	216
8.6.6	Windows-Komponenten	217
8.7	Administrative Vorlagen – Benutzerkonfiguration	239
8.7.1	Desktop	239
8.7.2	Netzwerk	241
8.7.3	Startmenü und Taskleiste	241
8.7.4	System	242
8.7.5	Systemsteuerung	246
8.7.6	Windows-Komponenten	250
8.8	Einstellungen finden	253
8.8.1	Administrative Vorlagen filtern	253
8.8.2	Group Policy Settings Reference	257
8.8.3	getadmx.com	258
9	Erweitern von administrativen Vorlagen	261
9.1	Einführung	261
9.2	ADMX-Datei erweitern	262
9.3	ADML-Datei an erweiterte ADMX-Datei anpassen	265
9.4	ADM-Datei in ADMX-Datei umwandeln	267
9.5	Eigene ADMX-Dateien erstellen	267

10	Windows-Einstellungen: Benutzerkonfiguration	271
10.1	Einführung	271
10.2	An- und Abmeldeskripte	273
10.3	Softwareeinschränkungen	273
10.4	Ordnerumleitungen	273
10.4.1	Probleme, die Ordnerumleitungen lösen	275
10.4.2	Probleme, die die Ordnerumleitung schafft	275
10.5	Richtlinienbasierter QoS (Quality of Service)	283
11	Gruppenrichtlinien-Einstellungen	287
11.1	Einführung	287
11.2	Gruppenrichtlinieneinstellungen konfigurieren	288
11.2.1	Das CRUD-Prinzip	288
11.2.2	Zielgruppenadressierung auf Elementebene	291
11.2.3	Variablen	297
11.3	Die Einstellungen im Detail	298
11.3.1	Windows-Einstellungen	299
11.3.2	Systemsteuerungseinstellungen	308
11.4	Weitere Optionen	329
11.4.1	XML-Darstellung und Migration der Einstellungen	329
11.4.2	Kopieren, Umbenennen und Deaktivieren	330
11.4.3	Gemeinsame Optionen	331
11.5	Fehlersuche	333
12	Gruppenrichtlinien in Windows 10	339
12.1	Windows 10 – Software as a Service	339
12.1.1	Windows Updates verteilen	342
12.1.2	Windows Update for Business	342
12.1.3	Übermittlungsoptimierung/Delivery Optimization	349
12.1.4	Bereitstellungsringe verwenden	354
12.2	Windows 10 und die Privatsphäre	357
12.2.1	Windows-Telemetrie	358
12.2.2	Funktionsdaten	364
12.2.3	Weitere Datenschutzoptionen	367
12.2.4	Windows Defender Smartscreen konfigurieren	368
12.3	Der Microsoft Store	372
12.4	Oberfläche anpassen	376
12.4.1	Startmenü und Taskleiste	376
12.4.2	Programmverknüpfungen anpassen	382
12.5	Der alte Edge-Browser	384
12.6	Der neue Edge-Browser	389
12.6.1	Edge-Updates verwalten	390
12.6.2	Einstellungen vornehmen	392
12.6.3	Auswertung der Richtlinien	395

12.7	Virtualisierungsbasierte Sicherheit	396
12.7.1	Windows Defender Credential Guard	397
12.7.2	Windows Defender Application Control/Device Guard	398
12.7.3	Application Guard	400
12.8	Clientkonfiguration aus der Cloud	406
13	Funktionsweise von Gruppenrichtlinien	409
13.1	Die Rolle der Domänencontroller	409
13.2	Die Replikation des SYSVOL-Ordners	419
13.3	Gruppenrichtlinien auf Standorten	421
13.4	Die Rolle des Clients	422
13.4.1	Client Side Extensions	423
13.4.2	Verarbeitung der GPOs – synchron/asynchron	426
13.4.3	Verarbeitung der GPOs – Vordergrund/Hintergrund	429
13.4.4	Gruppenrichtlinien-Zwischenspeicherung	435
13.4.5	Windows-Schnellstart	436
13.4.6	Slow Link Detection	437
13.4.7	Loopbackverarbeitung	438
14	Verwalten von Gruppenrichtlinienobjekten	441
14.1	Einführung	441
14.2	Gruppenrichtlinienobjekte (GPOs) sichern und wiederherstellen	441
14.2.1	GPO sichern	442
14.2.2	Alle GPOs sichern	443
14.2.3	GPO wiederherstellen	444
14.2.4	Sicherungen verwalten	445
14.3	Einstellungen importieren und migrieren	446
14.3.1	Einstellungen importieren	446
14.3.2	Einstellungen migrieren	448
14.3.3	Einstellungen zusammenführen	450
14.4	Starter-Gruppenrichtlinienobjekte	451
14.5	Massenaktualisierung	452
15	Fehlersuche und Problembehebung	455
15.1	Einführung	455
15.2	Gruppenrichtlinienergebnisse	456
15.2.1	Gruppenrichtlinienergebnis-Assistent	457
15.2.2	Gruppenrichtlinienergebnis untersuchen	458
15.3	Gruppenrichtlinienmodellierung	465
15.3.1	Gruppenrichtlinienmodellierungs-Assistent	465
15.3.2	Gruppenrichtlinienmodellierung auswerten	469
15.4	GPRresult	471
15.5	Gruppenrichtlinien-Eventlog	472
15.6	Debug-Logging	474
15.7	Performanceanalyse	476

16	Advanced Group Policy Management (AGPM)	479
16.1	Gruppenrichtlinien in Teams bearbeiten	479
16.2	Installation von AGPM	482
16.2.1	Vorbereitende Maßnahmen	483
16.2.2	Installation des Servers	484
16.2.3	Installation des Clients	487
16.2.4	Clients konfigurieren	489
16.3	AGPM-Einrichtung	491
16.4	Der Richtlinien-Workflow (1)	494
16.5	AGPM-Rollen und Berechtigungen	495
16.6	Der Richtlinien-Workflow (2)	502
16.7	Versionierung, Papierkorb, Backup	512
16.8	Vorlagen	515
16.9	Exportieren, Importieren und Testen	517
16.10	Labeln, Differenzen anzeigen, Suchen	522
16.11	Das Archiv, Sichern des Archivs	526
16.12	Logging und Best Practices	529
16.13	Zusammenfassung	530
17	Intune einrichten	531
17.1	Azure, Azure AD und Intune	533
17.2	Integration von AD und AAD	535
17.3	Intune bereitstellen	537
17.4	Geräte für die Verwaltung registrieren	539
17.5	Eine eigene DNS-Domäne registrieren	546
17.6	Benutzer und Gruppen verwalten	549
17.6.1	Benutzer anlegen	549
17.6.2	Gruppen	552
17.6.3	Administrative Rollen	554
17.7	Berechtigungen delegieren mit Rollen, Bereichen und Bereichstags	556
17.8	Geräteregistrierung konfigurieren	563
17.9	Lokale Administratoren verwalten	566
17.10	Grundeinstellungen vornehmen	569
17.10.1	Kennwortrichtlinie	569
17.10.2	Sicherheitsstandards verwalten	571
17.10.3	Das Unternehmensportal	572
17.10.4	Portal konfigurieren	572
17.10.5	Die Sprache im Webportal anpassen	574
18	Clientverwaltung mit Intune	575
18.1	Konfigurationsprofile einrichten	576
18.1.1	Configuration Service Provider und SyncML	581
18.1.2	ADMX-basierte Konfigurationen	586
18.1.3	ADMX-basierte Richtlinien per OMA-URI ansprechen	591
18.1.4	Eigene ADMX-Dateien verwenden	595

18.1.5	Gruppenmitgliedschaften konfigurieren	601
18.1.6	Konflikte mit Gruppenrichtlinien auflösen	605
18.2	Konformitätsregeln	606
18.2.1	Erstellen einer Benachrichtigung	607
18.2.2	Erstellen einer Konformitätsrichtlinie	608
18.2.3	Prüfen von Konformitätsrichtlinien	612
18.3	Windows Update verwalten	613
18.3.1	Updaterringe	613
18.3.2	Feature Updates	616
18.3.3	Microsoft Office 365 aktualisieren	618
18.4	PowerShell-Skripte verteilen	619
18.5	Software bereitstellen	623
18.5.1	Apps aus dem Microsoft Store installieren	624
18.5.2	MSI(X)-Pakete verteilen	627
18.5.3	Win32-Anwendungen und komplexe MSI-Pakete verteilen	631
18.5.4	Anwendungen entfernen	643
18.5.5	Fehlersuche	644
18.6	Security Baselines	644
18.7	Gruppenrichtlinienanalyse	646
18.8	Einstellungen manuell synchronisieren	648
18.8.1	Sync vom Portal aus starten	648
18.8.2	Sync clientseitig starten	649
18.9	Fehlersuche	651
18.9.1	Devicemanagement-Ereignisprotokoll	652
18.9.2	Die Management Engine	652
18.9.3	Log-Daten mit dem MdmDiagnosticsTool.exe sammeln	653
18.9.4	Geplante Aufgaben	654
18.9.5	Die Registry	655
18.9.6	Zertifikate	656
18.9.7	dsregcmd.exe	657
18.9.8	SyncML-Viewer	658
18.9.9	Client-Troubleshooting aus dem Portal	658
18.9.10	Fehlercodes	665
18.10	Neuerungen nachverfolgen	666
19	Windows Auditing einrichten	667
19.1	Das erweiterte Auditing einrichten	671
19.1.1	Überwachungsrichtlinien	671
19.1.2	Den Zugriff auf Objektzugriffe (Dateien, Registry, Drucker) protokollieren	674
19.1.3	Überwachungsrichtlinien verwalten mit Auditpol	678
19.2	Die Ereignisanzeige konfigurieren	684
19.3	Das Ereignisprotokoll sichten	689
19.3.1	Die XML-Ansicht von Ereignis-Einträgen	692
19.3.2	XML-Filter und XPath-Abfragen	694

19.3.3	Mehrere XPath-Abfragen in einem XML-Filter kombinieren	700
19.3.4	Ereignisprotokolle mit PowerShell abfragen	701
19.4	Ereignisprotokoll-Weiterleitung einrichten	705
19.4.1	Manuelles Einrichten eines Sammeldienstes	707
19.4.2	Einrichten des Sammeldienstes per Gruppenrichtlinie	714
19.4.3	Anpassen der Berechtigungen des Sicherheitsprotokolls	716
19.5	PowerShell-Logging	718
19.5.1	Over the Shoulder Transcription	718
19.5.2	Skriptblock-Logging	721
19.5.3	Konfigurieren des Protokolls	728
19.6	Ereignisse auswerten	731
20	Gruppenrichtlinien und PowerShell	733
20.1	Skripte mit Gruppenrichtlinien ausführen	734
20.1.1	Das (korrekte) Konfigurieren von Anmeldeskripten	735
20.1.2	Startreihenfolge und Startzeit von Skripten	738
20.2	Windows PowerShell mit GPOs steuern und überwachen	739
20.3	Gruppenrichtlinienobjekte mit PowerShell verwalten	747
20.3.1	Dokumentieren, sichern, wiederherstellen	747
20.3.2	Health Check	754
20.3.3	Mit Kennwortrichtlinien und WMI-Filtern arbeiten	769
20.3.4	Ein neues Gruppenrichtlinienobjekt anlegen	772
20.3.5	Sonstige Cmdlets	774
20.4	Externe Ressourcen	777
20.5	PowerShell deaktivieren	780
20.6	Zusammenfassung	782
Index		783