

HANSER



Leseprobe

zu

„Gruppenrichtlinien in Windows Server und Windows 10“

von Holger Voges, Martin Dausch

ISBN (Buch): 978-3-446-45549-8

ISBN (E-Book): 978-3-446-45605-1

Weitere Informationen und Bestellungen unter

<https://www.hanser-fachbuch.de/buch/Gruppenrichtlinien+in+Windows+Server+und+Windows+10/9783446455498>

sowie im Buchhandel

© Carl Hanser Verlag, München

Inhalt

Vorwort	XIII
Wissenswertes zu diesem Buch	XV
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	174
7.9.2	Der Policy Analyzer	177
7.9.3	Security Baselines anwenden	181
7.9.4	Der Security Compliance Manager	182
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	341
12.1.2	Windows Update for Business	342
12.1.3	Übermittlungsoptimierung/Delivery Optimization	348
12.1.4	Bereitstellungsringe verwenden	352
12.2	Windows 10 und die Privatsphäre	355
12.2.1	Windows Telemetrie	355
12.2.2	Funktionsdaten	361
12.2.3	Weitere Datenschutzoptionen	363
12.2.4	Windows Defender Smartscreen konfigurieren	363
12.3	Der Microsoft Store	366
12.4	Oberfläche anpassen	371
12.4.1	Startmenü und Taskleiste	371
12.4.2	Programmverknüpfungen anpassen	376
12.5	Edge Browser	379
12.6	Virtualisierungsbasierte Sicherheit	383
12.6.1	Windows Defender Credential Guard	384
12.6.2	Windows Defender Application Control/Device Guard	385
12.6.3	Application Guard	388
12.7	Clientkonfiguration aus der Cloud	392

13	Funktionsweise von Gruppenrichtlinien	395
13.1	Die Rolle der Domänencontroller	395
13.2	Die Replikation des SYSVOL-Ordners	405
13.3	Gruppenrichtlinien auf Standorten	407
13.4	Die Rolle des Clients	408
13.4.1	Client Side Extensions	409
13.4.2	Verarbeitung der GPOs – synchron/asynchron	412
13.4.3	Verarbeitung der GPOs – Vordergrund/Hintergrund	415
13.4.4	Gruppenrichtlinien-Zwischenspeicherung	421
13.4.5	Windows-Schnellstart	422
13.4.6	Slow Link Detection	423
13.4.7	Loopbackverarbeitung	424
14	Verwalten von Gruppenrichtlinienobjekten	427
14.1	Einführung	427
14.2	Gruppenrichtlinienobjekte (GPOs) sichern und wiederherstellen	427
14.2.1	GPO sichern	428
14.2.2	Alle GPOs sichern	429
14.2.3	GPO wiederherstellen	430
14.2.4	Sicherungen verwalten	431
14.3	Einstellungen importieren und migrieren	432
14.3.1	Einstellungen importieren	432
14.3.2	Einstellungen migrieren	434
14.4	Starter-Gruppenrichtlinienobjekte	436
14.5	Massenaktualisierung	438
15	Fehlersuche und Problembehebung	441
15.1	Einführung	441
15.2	Gruppenrichtlinienergebnisse	442
15.2.1	Gruppenrichtlinienergebnis-Assistent	443
15.2.2	Gruppenrichtlinienergebnis untersuchen	444
15.3	Gruppenrichtlinienmodellierung	451
15.3.1	Gruppenrichtlinienmodellierungs-Assistent	451
15.3.2	Gruppenrichtlinienmodellierung auswerten	455
15.4	GPRresult	457
15.5	Gruppenrichtlinien-Eventlog	458
15.6	Debug-Logging	460
15.7	Performanceanalyse	462
16	Advanced Group Policy Management (AGPM)	465
16.1	Gruppenrichtlinien in Teams bearbeiten	465
16.2	Installation von AGPM	468
16.2.1	Vorbereitende Maßnahmen	469
16.2.2	Installation des Servers	470
16.2.3	Installation des Clients	473
16.2.4	Clients konfigurieren	475

16.3	AGPM-Einrichtung	477
16.4	Der Richtlinien-Workflow (1)	480
16.5	AGPM-Rollen und Berechtigungen	481
16.6	Der Richtlinien-Workflow (2)	488
16.7	Versionierung, Papierkorb, Backup	498
16.8	Vorlagen	501
16.9	Exportieren, Importieren und Testen	503
16.10	Labeln, Differenzen anzeigen, Suchen	508
16.11	Das Archiv, Sichern des Archivs	512
16.12	Logging und Best Practices	515
16.13	Zusammenfassung	516
17	Gruppenrichtlinien und PowerShell	517
17.1	Skripte mit Gruppenrichtlinien ausführen	518
17.1.1	Das (korrekte) Konfigurieren von Anmeldeskripten	519
17.1.2	Startreihenfolge und Startzeit von Skripten	522
17.2	Windows PowerShell mit GPOs steuern und überwachen	523
17.3	Gruppenrichtlinienobjekte mit PowerShell verwalten	531
17.3.1	Dokumentieren, sichern, wiederherstellen	531
17.3.2	Health Check	538
17.3.3	Mit Kennwortrichtlinien und WMI-Filtern arbeiten	553
17.3.4	Ein neues Gruppenrichtlinienobjekt anlegen	556
17.3.5	Sonstige Cmdlets	558
17.4	Externe Ressourcen	561
17.5	PowerShell deaktivieren	564
17.6	Zusammenfassung	566
18	Desired State Configuration	567
18.1	Was ist DSC?	567
18.2	Ist DSC der Ersatz für Gruppenrichtlinien?	568
18.3	Grundlagen und Einrichtung	570
18.4	Erstellen einer Computerkonfiguration	572
18.5	Konfigurieren des LCM	581
18.6	Ausblick	582
Index		583

Vorwort

Herzlichen willkommen zur vierten Auflage dieses Buches, jetzt mit dem Titel „Gruppenrichtlinien in Windows Server und Windows 10“.

Für mich ist das die zweite Auflage dieses Buches, und auch dieses Mal hat mich die Überarbeitung viel Kraft und mehr Zeit gekostet, als ich im Vorfeld dafür eingeplant hatte. Neben einem komplett neuen Kapitel über Windows 10 habe ich vor allem fast jedes Kapitel meines Vorgängers einer Renovierung – oder sollte ich eher Komplettsanierung sagen? – unterzogen. Mit dieser Auflage sind fast alle Bilder durch aktuelle Screenshots ersetzt und die Themen „Sicherheitseinstellungen“ und „Administrative Vorlagen“ komplett neu geschrieben worden. Neben diversen Korrekturen sind auch einige interessante bisher unerwähnte Themen ausführlich besprochen worden wie „Windows Remote Assistance“ oder „Windows Hello“. Außerdem habe ich die beiden Kapitel zu administrativen Vorlagen zusammengefasst. Dadurch hat das Buch genauso viele Kapitel wie die Voraufgabe, obwohl ein komplett neues hinzugekommen ist.

Trotz der Tatsache, dass mit Erscheinen dieses Buches auch Windows Server 2019 veröffentlicht wurde, hat das aktuell kaum Auswirkungen auf die Gruppenrichtlinien. Tatsächlich hat Microsoft in letzter Zeit vor allem daran gearbeitet, dass Windows 10 sich auch durch Intune, Microsofts Internet-basierte Verwaltungslösung, besser steuern lässt. Serverseitig sind kaum noch neue Erweiterungen hinzugekommen, auch wenn natürlich jedes neue Feature-Release die administrativen Vorlagen für Windows 10 erweitert. Eine zukünftige Auflage dieses Buches wird sich also vermutlich auf die neuen Features von Intune konzentrieren.

Wenn Sie Fehler in diesem Buch finden, von denen es unter Garantie einige gibt, auch wenn ich mich bemüht habe, alles so gut wie möglich zu testen und doppelt zu kontrollieren, schicken Sie mir bitte eine Mail an holger.voges@netz-weise.de. Ich werde Korrekturen als Errata unter www.gruppenrichtlinien.akademie zur Verfügung stellen.

Wenn Sie Bedarf an Schulungen zu Windows 10, Gruppenrichtlinien, PowerShell, Active Directory, Windows Server oder anderen IT-Themen wie Linux oder Scrum haben, scheuen Sie sich nicht, bei uns anzufragen. Schulungen sind unsere Profession und Leidenschaft. Neben offenen Seminaren bieten wir auch Firmenschulungen an, die auf Ihre Bedürfnisse zugeschnitten sind. Unseren aktuellen Seminarkatalog finden Sie unter <https://www.netz-weise.de>.

An dieser Stelle möchte ich meiner Freundin danken, die sich (wieder) damit abgefunden hat, dass der Anfang unseres Sommerurlaubs durch die Überarbeitung des Buches geprägt war, auch wenn ich ihr versichert habe, dass das Buch dieses Mal bis zum Urlaub mit Sicherheit lange fertig ist. Ich danke Dir für Deine Geduld, mein Sonnenschein!

Und nun viel Spaß beim Lesen.

Holger Voges

12

Gruppenrichtlinien in Windows 10



In diesem Kapitel werden folgende Themen behandelt:

- Wichtige Änderungen in Windows 10
- Startmenü, Taskleiste und Dateiverknüpfungen anpassen
- Windows Update anpassen
- Privatsphäre-Einstellungen konfigurieren
- Virtualisierungsbasierte Sicherheit in Windows 10
- Der Edge Browser

■ 12.1 Windows 10 – Software as a Service

Bevor wir in das Thema Gruppenrichtlinien in Windows 10 einsteigen, möchte ich hier einige grundlegende Konzepte von Windows 10 klären, die für das Verständnis einiger Funktionen wichtig sind.

Windows 10, so hat Microsoft es zur Veröffentlichung genannt, das letzte (Client-)Windows. Es wird also kein Windows 11 mehr geben. Wie Sie vermutlich schon gemerkt haben, heißt das aber keinesfalls, dass Microsoft Windows nicht mehr weiterentwickelt, sondern Windows 10 ist jetzt einfach ein Synonym für Windows geworden, und die Versionsnummer verbirgt sich in der Feature-Release-Nummer.

Feature Releases oder kurz FR sind halbjährlich erscheinende Updates, die das alte Feature Release vollständig ersetzen. Für den Update-Vorgang wird das neue Feature Release im Hintergrund heruntergeladen. Wenn der Update-Vorgang beginnt, wird Windows über Windows PE neu gestartet. Windows PE ist ein Mini-Windows, das seit Vista die Installation ausführt, sich aber auch für Wartungszwecke einsetzen lässt. Während des Update-Vorgangs wird der Windows-Ordner in Windows.old umbenannt. Anschließend wird das neue

Feature Release installiert und die Daten aus dem alten Windows-Ordner werden in der neuen Installation übernommen. Man spricht auch von einem In-Place-Upgrade. Genau genommen ist die Installation eines Feature Release also immer eine Neuinstallation.

Zur Drucklegung trägt das aktuelle Feature Release die Nummer 1803. Sie setzt sich aus dem Jahr und dem Monat zusammen, zu der das Release bei Microsoft freigegeben wurde, entspricht aber nicht zwingend dem Veröffentlichungsdatum. Die Version 1803 wurde z. B. erst Ende April an Endkunden verteilt. Da die Features Releases alle sechs Monate erscheinen sollen, steht die nächste Release-Nummer auch schon fest, nämlich 1809. Da Microsoft die Release-Zyklen am Anfang noch nicht so genau festgelegt hatte, gilt das halbjährliche Release erst seit 2017. Dementsprechend können wir aktuell auf folgende Releases zurückschauen:

Tabelle 12.1 Windows 10 Releases bis Sommer 2018

Quelle: https://en.wikipedia.org/wiki/Windows_10_version_history

Release	Code-Name	Marketing-Name	Erscheinungsdatum	auch LSTB
1507	Threshold 1	-	29.07.2015	x
1511	Threshold 2	November Update	20.11.2015	
1607	Redstone 1	Anniversary Update	2.08.2016	x
1703	Redstone 2	Creators Update	5.04.2017	
1709	Redstone 3	Fall Creators Update	17.10.2017	
1803	Redstone 4	April 2018 Update	20.04.2018	
1809	Redstone 5	October 2018 Update	2.10.2018	x

Neben der FR-Nummer hat Microsoft noch ein paar zusätzliche Namen eingeführt. So gibt es noch einen internen Code-Namen, der seit der Version 1607 Redstone heißt und aktuell nur hochgezählt wird. Er soll ab 2019 durch ein neues Schema ersetzt werden, das nur noch aus der Jahreszahl und dem Update des Jahres, mit einem H vorangestellt, besteht. Redstone 6 wird dann also stattdessen 19H1 heißen. Zusätzlich gibt es noch einen Marketingnamen, um die Verwirrung komplett zu machen. Ich beziehe mich daher immer auf die FR-Nummer, weil es einfach zu merken und eindeutig ist.

Tatsächlich gibt es also inzwischen schon jede Menge neue Windows-Versionen, sie heißen einfach nur alle Windows 10. Das hat natürlich auch Auswirkungen auf Gruppenrichtlinien, denn mit jedem Feature Release kommen nicht nur jede Menge neue Richtlinien hinzu, sondern es werden inzwischen leider auch alte Richtlinien entfernt, was mitunter zu Problemen führen kann.

Mit den Feature Releases hat Microsoft auch den Support-Zeitraum geändert. Im Gegensatz zu vorherigen Versionen von Windows, für die es immer zehn Jahre lang Updates gab, sind es für Windows 10 maximal zwei. Maximal heißt, dass das nur die Enterprise Edition von Windows 10 betrifft, während alle anderen Versionen nur 18 Monate mit den sogenannten Quality-Updates versorgt werden. Mit der aktuellen Version 1809 hat Microsoft den Support-Zeitraum für die Enterprise-Edition noch einmal angepasst. Für die Herbst-Versionen ist er nun 30 Monate, für die Frühjahrs-Versionen dagegen nur noch 18 Monate.

Es gibt allerdings eine Ausnahme von dieser Regel, und das ist der sogenannte Long-Term Servicing Channel (LTSC), der bis vor Kurzem noch Long-Term Service Branch hieß (LTSB). Dies sind spezielle Versionen von Windows, die es nur als Enterprise Edition gibt und die

weiterhin zehn Jahre lang von Microsoft supported werden. Das hat allerdings einen Preis, denn den LTSC-Versionen fehlen alle Features, die regelmäßig aktualisiert werden oder auf Cloud-Dienste zugreifen, also Cortana (die Windows-Sprachsteuerung), Windows Apps und der Edge Browser.



Semi-Annual Updates und der Long-Term Servicing Channel

Die Feature Releases von Microsoft erscheinen seit April 2017 in halbjährlichem Abstand. Bis zu diesem Zeitpunkt gab es für die aktuellen Versionen eine eigene Nomenklatur – das jeweils aktuellste FR wurde als Current Branch (CB) bezeichnet. Sobald das CB vier Monate verfügbar war, wurde es zum Current Branch for Business (CBB). Damit sagt Microsoft aus, dass der CB jetzt ausreichend stabil für den Unternehmenseinsatz ist. Das kann man als Empfehlung verstehen, denn natürlich bekommt man von Microsoft auch dann Support, wenn man bereits den CB einsetzt.

Die Versionen, die mit zehnjährigem Support verfügbar sind, wurden als Long-Term Service Branch (LTSB) bezeichnet. Davon gibt es aktuell zwei, 1507 LTSB und 1607 LTSB. Sie haben recht, zwischen diesen beiden Versionen liegen keine zwei Jahre, aber die nächste Version wird die 1809, und hier passt der Zeitraum jetzt. Diese Versionen sind offiziell übrigens nur für Geräte empfohlen, die Spezialsoftware betreibt, die sich schlecht warten lässt, wie Kassensysteme oder Geldautomaten.

Mit Windows 10 Version 1709 hat Microsoft die Bezeichnungen geändert. Wir sprechen jetzt von Channels und nicht mehr von Branches. Dementsprechend wird die nächste LTSB-Version auch eine LTSC-Version sein. Der Current Branch wird jetzt als Semi-Annual Update (Targetted) bezeichnet, was Microsoft im Deutschen als Zielgruppe übersetzt hat. Der ehemalige Current Branch for Business heißt jetzt nur noch Semi-Annual Update. Der Grund für die Umbenennung ist, dass Microsoft zusammen mit der Version 1709 für Clients auch für den Windows Server halbjährliche Updates eingeführt hat. Bei Office 365 gab es das Konzept auch, hieß da aber Semi-Annual Update. Um jetzt für alle Produkte eine einheitliche Benennung zu haben, wurde die Benennung von Office 365 auch Windows übergestülpt.

Alte Bezeichnung	umbenannt in
Current Branch	Semi-Annual Update (Targetted)
Current Branch for Business	Semi-Annual Update
Long-Term Service Branch	Long-Term Servicing Channel

12.1.1 Windows Updates verteilen

Neben den Feature-Updates hat Microsoft aber auch Änderungen an der Art und Weise vorgenommen, wie Sicherheitsupdates und Fehlerbereinigungen, jetzt als Quality Updates bezeichnet, verteilt werden. Quality Updates kommen nur noch in Form sogenannter kumu-

lativer Updates (CU). Ein CU beinhaltet jeweils alle Updates, die seit Erscheinen eines Release veröffentlicht wurden, also auch alle Updates, die ein Computer bereits erhalten hat. Dadurch wird sichergestellt, dass ein Computer immer alle verfügbaren Updates installiert hat – man kann kein Update mehr auslassen. Da die CUs sehr schnell sehr groß werden (bis ca. 1,2 GB), gibt es zwei weitere Update-Typen: Delta-Updates und Express-Updates. Delta-Updates enthalten nur die Updates, die seit dem Vormonat erschienen sind. Mithilfe von Express-Updates kann der Client nur die Dateien ermitteln und abrufen, die er wirklich benötigt. Express-Updates sind neuer und effizienter und werden die Delta-Updates in Zukunft komplett ersetzen. Mehr zum Thema finden Sie unter <https://techcommunity.microsoft.com/t5/Windows-IT-Pro-Blog/Windows-10-quality-updates-explained-amp-the-end-of-delta/ba-p/214426> oder kurz <https://bit.ly/2LwMMYd>. Wenn man sie mit dem WSUS einsetzen möchte, benötigt man aber bis zu achtmal mehr Speicherplatz!

Zusammengefasst verteilt Microsoft also zwei unterschiedliche Typen von Updates – Feature-Updates, die das Betriebssystem auf eine neue Version hieven, und Quality-Updates in Form von kumulativen Updates, die Fehler bereinigen. Beide Typen von Updates lassen sich nach wie vor über einen Windows Update Server (WSUS) bereitstellen. Sie benötigen für die Bereitstellung von Feature Releases mindestens WSUS 4.0. Wenn Sie Windows Server 2012 oder neuer als Betriebssystem für Ihren WSUS verwenden, aktualisiert sich der WSUS selbst auf die aktuellste Version. Windows Server 2008 R2 wird nicht mehr unterstützt.

Mehr zum Thema Servicing Channels aus Microsofts eigenem Mund finden Sie unter <https://docs.microsoft.com/en-us/windows/deployment/update/waas-overview> oder kurz <https://bit.ly/2rKZI26>.

12.1.2 Windows Update for Business

Windows Update for Business ist ein alternatives Bereitstellungsverfahren für Updates, das Microsoft mit Windows 10 eingeführt hat. Genau genommen ist Windows Update for Business eigentlich gar nicht neu, sondern ein aufgebohrter Windows Update-Client, der bessere Steuerungsmöglichkeiten mit sich bringt.

Sie beziehen mit Windows Update for Business Ihre Updates nicht über einen zentralen Update-Server wie den WSUS, sondern über einen von Microsofts Update Server oder alternativ andere Clients, die das Update bereits heruntergeladen haben (Peer-to-Peer). Das zweite Feature wird auch Delivery Optimization genannt und ähnelt ein bisschen dem BitTorrent-Verfahren, das früher auch gerne zum Teilen von Daten über das Internet verwendet wurde.

Das, was Windows Update for Business vom klassischen Windows Update unterscheidet, ist die Möglichkeit zu steuern, welche Updates wann zur Verfügung gestellt werden sollen, und zwar über einen Satz von einfachen Regeln. Das hat den Vorteil, dass Sie sich um die Freigabe von Updates nicht mehr kümmern müssen, sondern nur noch definieren, wann und wie ein Update zur Verfügung gestellt werden soll. Die Bereitstellung wird dann zeitgesteuert und automatisch vorgenommen. Das Konzept geht davon aus, dass es keine Einzelupdates mehr gibt, sondern nur noch kumulative Updates und Features, die eh eingespielt werden müssen. Warum also noch manuell freischalten? Wenn es wirklich zum Worst Case kommt und ein Update bei Ihnen nicht funktioniert, können Sie manuell eingreifen und das Bereitstellen von Updates für einen Zeitraum von bis zu 35 Tagen komplett aussetzen.

Das Windows Update for Business kann lokal in den Windows 10-Einstellungen über **Update und Sicherheit – Windows Update – Erweiterte Optionen** konfiguriert werden. Unter Windows 10 Home können Sie nur Anpassungen an der Übermittlungsoptimierung vornehmen, alle anderen Funktionen sind der Pro, Enterprise und Education Edition vorbehalten.

Updateoptionen

Updates für andere Microsoft-Produkte bereitstellen, wenn ein Windows-Update ausgeführt wird

Aus

Updates selbst über getaktete Datenverbindungen automatisch herunterladen (Gebühren können anfallen)

Aus **1**

Kurz vor dem Neustart erhalten Sie eine Erinnerung. Aktivieren Sie diese Option, wenn Sie weitere Benachrichtigungen zu Neustarts erhalten möchten.

Aus

Updates aussetzen

Sie können die Installation von Updates auf diesem Gerät vorübergehend bis zu 35 Tage aussetzen. Wenn Updates fortgesetzt werden, müssen die neuesten Updates auf das Gerät angewendet werden, bevor sie für das Gerät wieder ausgesetzt werden können.

Aus **2**

Durch das sofortige Aussetzen werden Updates bis 23.08.2018 ausgesetzt.

Installationszeitpunkt für Updates auswählen

Wählen Sie das Branch-Bereitschaftsniveau aus, um den Installationszeitpunkt von Funktionsupdates zu bestimmen. "Semi-Annual Channel (Targeted)" bedeutet, dass das Update für die meisten Benutzer geeignet ist, und "Semi-Annual Channel" bedeutet, dass es für die weitverbreitete Nutzung in Organisationen geeignet ist.

Semi-Annual Channel (Targeted) **3**

Ein Funktionsupdate enthält neue Funktionen und Verbesserungen und kann für die folgende Anzahl von Tagen verzögert werden:

0 **4**

Ein Qualitätsupdate enthält Sicherheitsverbesserungen und kann für die folgende Anzahl von Tagen verzögert werden:

0 **5**

Übermittlungsoptimierung

Datenschutzeinstellungen

Bild 12.1 Die Updateoptionen von Windows 10

In Bild 12.1 sehen Sie die lokalen Einstellungsmöglichkeiten von Windows 10. Über „Updates selbst über getaktete Datenverbindungen herunterladen“ (1) können Sie festlegen, ob ein Update auch über Mobilverbindungen heruntergeladen werden soll. Mit „Updates aussetzen“ (2) können Sie Updates für bis zu 35 Tage deaktivieren. Achten Sie darauf, dass Sie nach dem Reaktivieren immer einen Updatedurchlauf starten müssen, bevor Sie Updates wieder deaktivieren können. Ein nervöser Mausfinger kann hier unschöne Folgen haben –

ich spreche aus Erfahrung ... Unter der Option „Installationszeitpunkt für Updates auswählen“ legen Sie fest, wann Updates bezogen auf ihr Erscheinungsdatum installiert werden sollen. Das „Branch-Bereitschaftsniveau“ (3) legt fest, ob Sie Feature-Updates sofort bekommen wollen oder erst, wenn sie den Status „Semi-Annual Update“ erreicht haben. Sie können zum Bereitschaftsniveau noch eine Verzögerung konfigurieren, die bis zu 365 Tage betragen kann (4). Auch das Einspielen von Qualitätsupdates kann verzögert werden, allerdings nur bis zu 30 Tage (5).

Unter „Übermittlungsoptimierung“ (Bild 12.2) können Sie konfigurieren, ob Sie die neue Übermittlungsoptimierung nutzen wollen und von woher der Client die Updates beziehen darf.

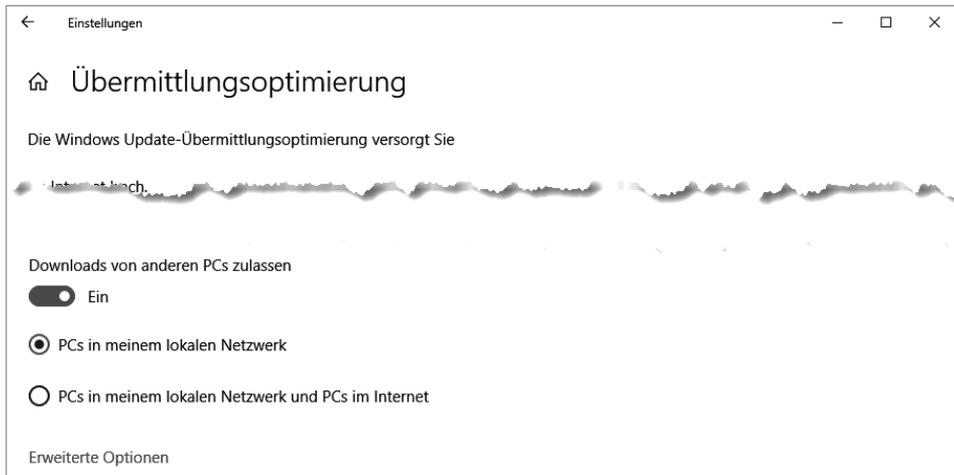


Bild 12.2 Zusätzlich zu BITS können Sie auch mit Delivery Optimization Updates beziehen.

Ab Windows 10 1709 können Sie in den erweiterten Optionen der Übermittlungsoptimierung auch steuern, wie viel von der Netzwerkbandbreite des Clients für den Up- und Download von Updates verwendet werden darf.

Ab Windows 10 1607 hat Microsoft zusätzlich die Nutzungszeit eingeführt. Sie kann direkt im Hauptfenster der Windows Update-Einstellungen konfiguriert werden. Die Nutzungszeit kann in der Version 1607 auf einen Zeitrahmen von zwölf Stunden festgelegt werden, ab 1703 kann sie bis zu 18 Stunden betragen. Mit ihr wird bestimmt, in welchem Zeitraum weder Update-Benachrichtigungen noch automatische Neustarts ausgeführt werden dürfen. Das ist notwendig, um Geräte wie Tablets aktualisieren zu können, die normalerweise nie heruntergefahren, sondern nur in den Stromsparmodus versetzt werden. Bei Windows 7 wird ein Update normalerweise immer dann installiert, wenn der Benutzer den Computer herunterfährt.

Alle diese Einstellungen können natürlich auch über eine Gruppenrichtlinie zentral gesteuert werden. Sie finden sich in den Einstellungen des Computers: **Administrative Vorlagen – Windows-Komponenten – Windows Update:**

Einstellung	Auswirkung
Automatischen Neustart nach Updates während der Nutzungszeit deaktivieren	Ist diese Einstellung aktiviert, kann Windows trotz aktivierter Nutzungszeit jederzeit neu starten.
Nutzungszeitbereich für automatische Neustarts angeben	Mit dieser Einstellung legen Sie fest, wie lang der Nutzungszeitbereich sein darf, wenn der Benutzer ihn individuell einstellt. Achten Sie darauf, dass Sie sich auch hier an die maximal unterstützten Zeitbereiche halten müssen und die Version 1607 nur zwölf Stunden unterstützt. Arbeiten Sie im Zweifelsfall mit WMI-Filtern und mehreren Richtlinien.
Automatisches Herunterladen von Updates über getaktete Verbindungen zulassen	Erlaubt das Herunterladen von Updates über Mobilfunkverbindungen. Entspricht dem Button (1) in Bild 12.1
Erinnerungsbenachrichtigungen über den automatischen Neustart zur Updateinstallation konfigurieren	Hier können Sie festlegen, wie lange vor einem geplanten Neustart eine Benachrichtigung an den Benutzer ausgegeben wird. Mit dieser Benachrichtigung kann der Benutzer den Neustart auch verschieben. Aktivieren Sie diese Richtlinie nicht, gilt der Standardwert von fünf Minuten.
Benachrichtigungen für den automatischen Neustart zur Updateinstallation deaktivieren	Schaltet jegliche Update-Benachrichtigungen aus.
Erforderliche Benachrichtigung für automatischen Neustart zur Updateinstallation konfigurieren	Sie können hier festlegen, ob für einen Neustart eine manuelle Bestätigung des Benutzers notwendig ist oder ob der Computer selbstständig neu starten kann.
Frist angeben, nach der ein automatischer Neustart zur Updateinstallation ausgeführt wird	Ist diese Option aktiviert, wird nach der angegebenen Zahl von Tagen (maximal 14) automatisch außerhalb der Nutzungszeit ein Neustart ausgeführt. Diese Option wird nicht wirksam, wenn die Richtlinie „Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet ist“ oder „Neustart immer automatisch zur geplanten Zeit durchführen“ aktiviert ist.
Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet ist	Für das Installieren des Updates muss der Benutzer den Computer manuell herunterfahren bzw. neu starten. Der Benutzer erhält hierüber eine Benachrichtigung. Diese Richtlinie ist nur gültig in Verbindung mit der Richtlinie „Automatische Updates konfigurieren“.
Neustart immer automatisch zur geplanten Zeit durchführen	Diese Richtlinie ist sehr missverständlich. Statt eine feste Zeit für das Aktualisieren des Computers angeben zu können, werden Updates im Hintergrund installiert und der Benutzer erhält eine Neustartbenachrichtigung. Mit dieser Option wird konfiguriert, wie lange der Benutzer Zeit hat, seine Daten zu speichern, bevor der Computer automatisch neu startet. Die mögliche „Gnadenfrist“ für den Benutzer kann zwischen 15 und 180 Minuten konfiguriert werden.
Zugriff auf alle Windows Update-Funktionen entfernen	Blendet die Konfigurationsmöglichkeiten für das Windows Update auf dem Client aus. Diese Konfiguration ist empfehlenswert, da Windows per Dual Scan sowohl Windows Update als auch WSUS parallel verwenden kann (s. u.).

(Fortsetzung nächste Seite)

Einstellung	Auswirkung
Keine Richtlinien für Updaterückstellungen zulassen, durch die Windows Update überprüft wird	Dieser etwas irreführende Name schaltet ab Windows 1703 (mit aktuellem CU) den Dual-Scan-Betrieb ab. Dual Scan (s. u.) heißt, dass Windows sowohl WSUS als auch Windows Update for Business zum Aktualisieren verwendet, was in den wenigsten Fällen erwünscht ist.
Keine Verbindungen mit Windows Update-Internetadressen herstellen	Diese Funktion wird nur angewendet, wenn Windows Update konfiguriert und ein WSUS-Server angegeben ist. Sie verhindert, dass der Client sich neben dem lokalen Update-Server auch noch mit Servern im Internet verbindet. Im Gegensatz zu „Keine Richtlinie für Updaterückstellungen zulassen, durch die Windows Update überprüft wird“ verhindert diese Richtlinie nicht nur den Dual Scan, sondern unterbindet auch das Herunterladen aus dem Windows Store. Im Gegensatz zur Richtlinie „Microsoft Anwenderfeatures deaktivieren“ unter Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Cloudinhalt werden beim ersten Anmelden die Download-Apps im Startmenü angezeigt, aber sie werden nicht heruntergeladen und ein manueller Download führt zu einer Fehlermeldung „Es ist keine Installation möglich, der Vorgang wird in Kürze wiederholt“. Effektiv wird der Windows Store also deaktiviert. Diese Einstellung funktioniert auch unter Windows 10 Professional! Achtung: Bei mir hat das Zurücksetzen dieser Einstellung auf „nicht konfiguriert“ weiterhin den Windows Store geblockt. Erst nachdem „deaktivieren“ konfiguriert war, konnte der Store wieder verwendet werden!
Wechsel zum erzwungenen Neustart und Benachrichtigungszeitplan für Updates festlegen	Mit dieser Einstellung können Sie festlegen, ab wann der Benutzer ein Update nicht mehr zurückstellen kann, sondern einen Neustart planen muss. Der Neustart muss nicht sofort ausgeführt werden, aber der Nutzer muss nach Ablauf der Benachrichtigungszeit einen Zeitpunkt für den Neustart definieren.
Keine Treiber in Windows-Updates einschließen	Microsoft aktualisiert auch Treiber über Windows Update, was gerade bei neuen Geräten enorm praktisch ist. Aktivieren Sie diese Option, werden Treiber nicht mehr über Windows Update verteilt. Das hat auch Auswirkungen auf die Druckerinstallation, da seit dem Druckmodell 4.0 (mit Windows 8 eingeführt) der Client sich seine Druckertreiber für Druckerfreigaben nicht mehr vom Server bezieht (auch als Point and Print bezeichnet), sondern über Windows Update. Bis Windows 10 1607 und Windows Server 2016 muss das Übermitteln von Telemetriedaten erlaubt sein (s. u.), um Treiber herunterzuladen, ab Windows 10 1703 ist das nicht mehr notwendig.
Automatische Updates sofort installieren	Ist diese Option aktiviert, werden Updates, die keinen Neustart benötigen, im Hintergrund installiert. Das betrifft z. B. Updates für den Windows Defender Antivirus und sollte aktiviert sein.

Einstellung	Auswirkung
Empfohlene Updates über automatische Updates aktivieren	Ist diese Richtlinie aktiviert, werden neben wichtigen Sicherheitsupdates auch Updates automatisch bei Windows Update heruntergeladen, die als „empfohlen“ eingestuft sind.
Warnbenachrichtigungszeitplan für den automatischen Neustart zur Updateinstallation konfigurieren	Wenn ein erzwungener Neustart aktiviert wurde, können Sie hier festlegen, ab wann der Benutzer über den Neustart informiert wird. Sie können die Frist für eine Informationsmeldung über den Neustart festlegen sowie die Frist für das Warnfenster, das den Benutzer direkt vor dem bestehenden Neustart warnt und zum Speichern seiner Daten anhält.

Um den Installationszeitplan für Feature Releases und Quality-Updates festzulegen, öffnen Sie den Knoten **Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Windows Update – Windows Update für Unternehmen** bzw. bis Windows 10 1703 **Windows Updates zurückstellen**. Hier finden Sie je nach Version zwei bzw. drei Einstellungen:

Einstellung	Auswirkung
Zeitpunkt für den Empfang von Vorabversionen und Funktionsupdates auswählen	Hier stellen Sie die Einstellungen aus Bild 1.1 (3) und (4) ein, also ab wann ein Feature-Update automatisch installiert werden soll. Mithilfe des Feldes „Vorabversionen oder Funktionsupdates aussetzen ab“ können Sie zentral alle Updates deaktivieren. Diese Funktionalität erlaubt es Ihnen, ein als problematisch erkanntes Update zu verschieben (s. Bild 1.1 (2), Updates aussetzen).
Beim Empfang von Qualitätsupdates auswählen	Hier legen Sie fest, nach wie vielen Tagen ein neues Qualitätsupdate installiert werden soll. Ich empfehle, neue Qualitätsupdates immer mindestens eine Woche zu verschieben, da Microsoft schon mehrfach problematische Updates veröffentlicht hat. Sollte ein Update zu Problemen führen, kann man die Qualitätsupdates über „Qualitätsupdates aussetzen ab“ noch bis zu 35 Tage deaktivieren. Danach wird ein Zwangsupdate durchgeführt.
Vorabversionen verwalten	Vorabversionen sind Beta-Versionen von Windows, die über den Eintrag Update und Sicherheit – Windows-Insider-Programm in den Windows-Einstellungen aktiviert werden können. Das Windows Insider-Programm ist nicht für Produktivsysteme gedacht. Um zu verhindern, dass Benutzer ihre Rechner eigenmächtig für das Windows Insider-Programm registrieren, wählen Sie in diesem Eintrag „Vorabversion deaktivieren“. Ist ein Rechner bereits im Insider-Programm, wählen Sie „Vorabversion deaktivieren, sobald die nächste Version veröffentlicht wurde“, damit der Rechner nach dem Update auf das Semi-Annual Update (Targetted) nicht wieder Teil des Insider-Programms wird.

Weitere Informationen zu Windows Update for Business-Einstellungen finden Sie in den Microsoft-Dokumentationen unter <https://docs.microsoft.com/de-de/windows/deployment/update/waas-configure-wufb> oder kurz <https://bit.ly/2A9sjaP>.

12.1.3 Übermittlungsoptimierung/Delivery Optimization

Übermittlungsoptimierung oder Delivery Optimization (DO) ist ein neues Feature, das Microsoft mit Windows 10 eingeführt hat und das die Menge an Daten, die von Windows Update und dem Windows Store heruntergeladen werden, massiv reduziert. Das Verfahren basiert auf Peer-to-Peer-Technologie, Clients teilen bereits heruntergeladene Daten also mit anderen Clients (Peers) im gleichen Netzwerk (oder auch über das Internet). Dafür werden Dateien in Blöcke aufgeteilt, gehashed – es wird eine eindeutige ID erzeugt – und dann blockweise anstatt als monolithische Datei verteilt. Damit ein Client tatsächlich nur Originaldaten erhält, sind die Dateien digital signiert, der Client kann also nach Empfang der kompletten Datei prüfen, ob er ein unverändertes Update erhalten hat.

Wenn ein Client ein Update von einem Update-Server herunterladen möchte und die Übermittlungsoptimierung aktiviert ist, erhält er über die URL `*.do.dsp.mp.microsoft.com` eine Liste von Rechnern, die bereits Blöcke der Update-Datei bezogen haben. Auf Windows 10 Pro und Enterprise ist die Einstellung dabei standardmäßig so konfiguriert, dass ein PC Daten nur von Peers aus seinem eigenen lokalen Netzwerk empfängt (s. Bild 12.2). Der Update-Service ermittelt über die IP des sich verbindenden Rechners (normalerweise die öffentliche IP des Routers oder Proxys, über den der Client sich verbindet), mit welchen Peers er Daten austauschen darf. Man kann diese automatische Gruppierung aber auch überschreiben und manuell festlegen, welche Clients miteinander Daten austauschen dürfen, indem man eine Group-ID festlegt. Die Group-ID wird dann als einziges Kriterium verwendet, um zu ermitteln, welche Clients Daten austauschen dürfen. Alternativ kann man den AD-Standort oder die Domäne verwenden oder über DHCP oder DNS eine Gruppenzuordnung festlegen. Das ist wichtig, wenn man bereits mit IPv6 arbeitet (alle Clients haben eine öffentliche IP-Adresse) oder der Zugriff nach außen über Proxy-Arrays oder Load-Balancing stattfindet, sodass ein Standort nicht über eine eindeutige ID verfügt. Die Group-ID ist eine GUID (Globally Unique Identifier), die man z.B. mit dem PowerShell-Cmdlet `New-GUID` zufällig generieren kann.

Die Übermittlungsoptimierung arbeitet höchst effizient und teilt Daten deutlich schneller als die Alternative BranchCache. Sind die Daten erst einmal im lokalen Netzwerk, dauert es nur Sekunden, bis Clients lokale Peers als Quelle verwenden können. Die Daten werden dann mit voller lokaler Netzwerkgeschwindigkeit geteilt. Der Übermittlungsoptimierungsdienst verwendet hierfür Port 7680 im lokalen Netzwerk, für den Datenaustausch mit Internet-Peers Port 3544 (Teredo-Protokoll, eine IPv6-Übergangstechnologie).

Übermittlungsoptimierung ist vor allem für große Dateien effektiv und kostet Client-Ressourcen, weshalb BranchCache standardmäßig erst aktiviert wird, wenn der Client mindestens über 4 GB RAM und 32 GB freien Speicherplatz auf dem Cache-Laufwerk verfügt. Diese Konfigurationen können über Gruppenrichtlinien angepasst werden, die Sie in der Computerkonfiguration unter **Administrative Vorlagen – Windows-Komponenten – Windows Update – Übermittlungsoptimierung** finden.

Die Übermittlungsoptimierung funktioniert übrigens genauso mit WSUS und dem Windows Store. Downloads aus dem Windows Store sind normalerweise benutzerinitiiert und werden als Vordergrundprozesse bezeichnet. Microsoft will die Übermittlungsoptimierung in Zukunft u. a. auch für Office 365 anbieten.

Einstellung	Auswirkung	FR
DownloadModus	<p>Mit dem Downloadmodus legen Sie fest, mit welchen Methoden der Windows Update Client einen Download durchführen darf.</p> <p>0: Nur HTTP: Hiermit wird der Peer-to-Peer-Datenaustausch deaktiviert, die Übermittlungsoptimierung kann aber trotzdem Daten vom Update-Server abrufen und per HTTP Daten von Peers beziehen. Welche Daten hier bezogen werden, ist leider an keiner mir bekannten Stelle dokumentiert. HTTP bedeutet, dass der Client den BITS-Dienst für den Download verwendet (das ist das Standardverhalten voriger Windows-Versionen).</p> <p>1: LAN: Der Client benutzt HTTP (BITS) und Peer-to-Peer mit Clients im gleichen Netzwerk.</p> <p>2: Gruppe: Der Client benutzt HTTP (BITS) und Peer-to-Peer mit Clients der gleichen Gruppe.</p> <p>3: Internet: Der Client benutzt HTTP (BITS) und Peer-to-Peer mit beliebigen Clients.</p> <p>99: Einfach: Mit dieser Einstellung wird die Übermittlungsoptimierung komplett deaktiviert, der Client holt Updates nur per HTTP (BITS).</p> <p>100: Überbrückung: Verwendet BITS in Verbindung mit BranchCache. Übermittlungsoptimierung ist auch hier deaktiviert.</p> <p>Mehr zu den Übermittlungsmodi finden Sie unter https://2pintsoftware.com/delivery-optimization-dl-mode/ und https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization oder kurz https://bit.ly/2mD0lot.</p>	Ab 1511
Max. Cachegröße (in Prozent)	Gibt an, wie viel Speicherplatz in Prozent vom Datenträger für den Cache verwendet werden darf. Der Windows-Standardwert ist 20%.	Ab 1511
Absolute max. Cachegröße (in GB)	Hier können Sie einen absoluten Wert für den Cache eingeben. Wird diese Option aktiviert, wird die max. Cachegröße in Prozent ignoriert.	Ab 1607
Max. Cachealter (in Sekunden)	Hier können Sie angeben, wie lange Updates lokal für andere Peers vorgehalten werden. Der Standard ist drei Tage. 0 bedeutet, dass Dateien nur bei Bedarf gelöscht werden.	Ab 1511
Cachelaufwerk ändern	Hier können Sie den Ablageort für den Cache anpassen. Ab Version 1709 ist der Standardpfad C:\Windows\Delivery Optimization.	Ab 1607
Maximale Downloadbandbreit (in KB/s)	Wie viel KB/s (absolut) der verfügbaren Netzwerkbandbreite der lokalen Netzwerkkarte von der Übermittlungsoptimierung für den Download verwendet werden darf. Diese Einstellung kann ab der Version 1709 auch lokal in den erweiterten Einstellungen der Übermittlungsoptimierung gesetzt werden.	Ab 1703

(Fortsetzung nächste Seite)

Einstellung	Auswirkung	FR
Maximale Bandbreite für Downloads im Hintergrund (Prozent)	Die Bandbreite, die für alle Downloads der Übermittlungsoptimierung in Summe von der verfügbaren Bandbreite verwendet werden darf. Ersetzt „Maximale Downloadbandbreite“ (in Prozent). Hintergrund bezieht sich auf automatische Prozesse wie das Windows Update.	Ab 1803
Maximale Bandbreite für Downloads im Vordergrund (Prozent)	Wie „Maximale Bandbreite für Download im Hintergrund“, begrenzt aber auch User-Prozesse, aktuell also den Windows Store.	Ab 1803
Maximale Downloadbandbreite (in Prozent)	Ab 1803 ersetzt durch „Maximale Bandbreite für Downloads im Hintergrund“	Ab 1607
Maximale Uploadbandbreite (in KB/s)	Gibt die Bandbreite an, die verwendet werden kann, um anderen Clients Daten zur Verfügung zu stellen. Da ein Upload immer ein Hintergrundprozess ist, gibt es hier anders als bei der Downloadbandbreite keine Unterscheidung zwischen Hintergrund- und Vordergrundverarbeitung.	Ab 1607
Max Uploadbandbreite (in KB/s) – ab 1703	Wie viel KB/s (absolut) der verfügbaren Netzwerkbandbreite der lokalen Netzwerkkarte von der Übermittlungsoptimierung für den Upload verwendet werden darf. Diese Einstellung kann ab der Version 1709 auch lokal in den erweiterten Einstellungen der Übermittlungsoptimierung gesetzt werden.	Ab 1703
Monatliche Obergrenze für Uploaddaten (in GB)	Dieser Wert kann auch auf dem Client in den erweiterten Einstellungen der Übermittlungsoptimierung konfiguriert werden und limitiert die Datenmenge, die pro Monat anderen Clients bereitgestellt werden kann. Sinnvoll ist diese Option nur, wenn man Daten auch mit Clients im Internet teilt.	Ab 1607
Gruppen-ID	Hier können Sie selber bestimmen, welche Clients als Peers fungieren können, indem alle Peers die gleiche Gruppen-ID bekommen. Die Gruppen-ID ist ein GUID-Wert, den Sie mit dem PowerShell-Cmdlet New-GUID selbstständig erstellen können. Alternativ können Sie die Gruppen-ID auch über einen Netzwerkdienst vergeben. Dann konfigurieren Sie stattdessen die Richtlinie „Quelle von Gruppen-IDs auswählen“.	Ab 1511
Methode zum Einschränken der Peer-auswahl einschränken	Ab dem Feature Release 1803 kann man jetzt die Einstellungen des Download-Modes weiter einschränken, indem man hier vorgibt, dass Clients Daten nur aus dem eigenen Subnetz beziehen können.	Ab 1803
Quelle von Gruppen-IDs auswählen	Wenn Sie als Download-Modus Gruppe (2) gewählt haben, können Sie die Gruppen-ID auch über einen Netzwerkdienst verteilen. Die ID kann entweder über den AD-Standort (AD-Site), die Windows-Domäne (authentifizierte Domänen-SID) oder das DNS-Suffix gebunden werden. Alternativ können Sie eine Gruppen-ID über DHCP (DHCP-Options-ID) verteilen. Hierzu müssen Sie die Gruppen-ID über Option 234 verteilen. Eine Anleitung zur Konfiguration Ihres DHCP-Servers finden Sie unter https://oliverkieselbach.com/2018/01/27/configure-delivery-optimization-with-intune-for-windows-update-for-business/ oder kurz https://bit.ly/2OGbaJl .	Ab 1803

Einstellung	Auswirkung	FR
Minimale Größe der Inhaltsdatei für das Peercaching (in MB)	Gibt an, wie groß eine Datei mindestens sein muss, damit die Übermittlungsoptimierung verwendet wird. Der auf dem Client gesetzte Standardwert ist 100 MB.	Ab 1703
Minimale RAM-Kapazität (einschließlich), die zur Verwendung des Peercaching erforderlich ist	Hier kann angegeben werden, wie viel GB RAM dem Client zur Verfügung stehen müssen, damit er die Übermittlungsoptimierung nutzt. Der Standardwert sind 4 GB, Sie können den Wert hier aber zwischen 1 GB und 4 GB anpassen.	Ab 1703
Geschäftszeiten festlegen, um die Bandbreite von Hintergrunddownloads zu begrenzen	Mit dieser Option können Sie unterschiedliche Bandbreiten für Tages- und Nachtzeiten festlegen. Dadurch wird es möglich, die Updates tagsüber zu begrenzen, aber nachts die volle (oder eine höhere) Bandbreite zu aktivieren. Hintergrunddownloads sind Prozesse, die vom System ausgeführt werden.	Ab 1803
Geschäftszeiten festlegen, um die Bandbreite von Vordergrunddownloads zu begrenzen	Wie „Geschäftszeiten festlegen, um die Bandbreite von Hintergrunddownloads zu begrenzen“, aber es werden Benutzerprozesse optimiert, also Downloads aus dem Microsoft Store.	Ab 1803
Hintergrunddownloads von HTTP verzögern (sek)	Wenn Peer-to-Peer-Download aktiviert ist, können Sie mit dieser Option den Download per HTTP für mehrere Sekunden verzögern. Normalerweise versucht der Client, HTTP und Peer-to-Peer parallel zu nutzen, durch diese Option wird Peer-to-Peer bevorzugt.	Ab 1803
Vordergrunddownloads von HTTP verzögern (sek)	Wenn Peer-to-Peer-Download aktiviert ist, können Sie mit dieser Option den Download per HTTP für mehrere Sekunden verzögern. Normalerweise versucht der Client, HTTP und Peer-to-Peer parallel zu nutzen, durch diese Option wird Peer-to-Peer bevorzugt. Beachten Sie, dass für den Endbenutzer während der reinen Peer-to-Peer-Verbindung kein Downloadfortschritt sichtbar ist.	Ab 1803
Uploads zulassen, während das Gerät im Akkubetrieb läuft und der minimale Akkustand (in Prozent) nicht erreicht ist.	Legen Sie einen Akkustand fest, ab dem kein Upload mehr stattfinden soll. Microsoft empfiehlt als Minimalwert 40%. Ist diese Richtlinie nicht gesetzt, ist der Upload auf mobilen Geräten deaktiviert, es findet also standardmäßig im Akkubetrieb gar kein Upload statt.	Ab 1709
Peercaching aktivieren, während das Gerät über ein VPN verbunden ist	Deaktiviert die Übermittlungsoptimierung, wenn der Client per VPN verbunden ist.	Ab 1709

Alle Übermittlungsoptimierungseinstellungen finden Sie unter <https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization> oder kurz <https://bit.ly/2mD0Iot>.

Viele weitere Informationen zur Übermittlungsoptimierung finden Sie im Video „Delivery Optimization – a deep dive“ von der Ignite 2017 unter <https://channel9.msdn.com/Events/Ignite/Microsoft-Ignite-Orlando-2017/BRK2048> oder kurz <https://bit.ly/2uFsYv6>.

12.1.4 Bereitstellungsringe verwenden

Da Windows als Feature Release regelmäßig neu bereitgestellt werden muss – ca. einmal pro Jahr, wenn Sie jeweils ein Feature Release auslassen wollen – brauchen Sie einen Plan, wie Sie die Kompatibilität der Feature-Updates mit Ihren bestehenden Anwendungen testen. Im Gegensatz zur Migration von Windows XP auf Windows 7 steht Ihnen für die Migration auf ein neues Feature Release ja nur ein relativ kurzer Zeitraum zur Verfügung. Hier stelle ich Ihnen vor, wie Microsofts Vorschlag aussieht.

12.1.4.1 Das Konzept der Bereitstellungsringe

Für das Testen und Bereitstellen von Windows 10 sieht Microsoft sogenannte Bereitstellungsringe vor. Ein Bereitstellungsring definiert zwei Dinge: die Zielgruppe (Computer bzw. Benutzer), die das Update erhalten, und den Zeitrahmen, in dem das Update ausgerollt werden soll. In Microsofts Standardmodell gibt es vier von diesen Bereitstellungsringen.

Im innersten oder ersten Ring befindet sich eine Reihe von Testrechnern, die an der Windows Insider Preview teilnehmen, also Beta-Updates bekommen. Diese Maschinen sollten in etwa Ihrem Standardclient entsprechen und werden dafür verwendet, schon einmal erste Kompatibilitätstests durchzuführen, bevor Microsofts neues Feature Release veröffentlicht wird.

Der zweite Ring besteht aus einer Reihe von ausgewählten Computern bzw. Benutzern in den unterschiedlichen Abteilungen, die mit der Veröffentlichung des neuen Feature Release sehr zeitnah ein Update bekommen. Die Benutzer des zweiten Rings sollten „Technikaffin“ sein, was bedeutet, dass sie nicht gleich beim Helpdesk anrufen, wenn ein Knopf im neuen Build ein bisschen weiter nach rechts gerückt ist. Diese Benutzer sind dafür zuständig, die Fachanwendungen ausführlich zu testen und bei Problemen Rückmeldung an das Bereitstellungsteam zu machen. Das Bereitstellungsteam sollte grundsätzlich regen Kontakt zu diesen Benutzern halten und sie auch ständig über neue Release-Pläne auf dem Laufenden halten.

Nach einer ausführlichen Testphase bekommt der dritte Ring, das Gros der Clients, das Feature-Update. Microsoft sieht diesen Zeitpunkt ungefähr gekommen, wenn das Feature-Release vom Semi-Annual Channel (Targetted) in den Semi-Annual Channel übergeht, also nach vier Monaten. Je nach eigenem Gusto können Sie diesen Zeitrahmen natürlich auch nach hinten verschieben. Für diese Clients werden auch die Qualitätsupdates um ein oder zwei Wochen verschoben, um sicherzustellen, dass ein fehlerhaftes Update nicht gleich alle Unternehmensrechner in den Abgrund reißt.

Der vierte Ring ist der Ring, auf dem unternehmenskritische Anwendungen laufen. Das können z. B. alte Anwendungen sein, die eigentlich nicht mehr mit Windows 10 kompatibel sind und nur noch mit Tricks zum Laufen gebracht werden können, für die es aber keine Alternative gibt, oder Systeme, die nicht ausfallen dürfen. Dieser Ring bekommt seine Updates noch einmal später, und Qualitätsupdates werden noch weiter hinausgezögert.

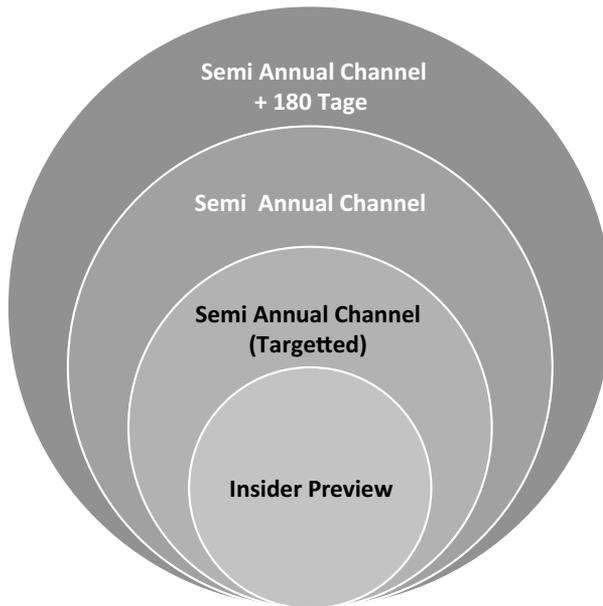


Bild 12.3 Windows-Bereitstellung in Wellen oder Ringen

Das Konzept finden Sie in Microsofts eigenen Worten unter <https://docs.microsoft.com/de-de/windows/deployment/update/waas-deployment-rings-windows-10-updates> oder kurz <https://bit.ly/2LHtpW>.

Tatsächlich ist die Bereitstellung in Ringen wohl die einzig gangbare Lösung, wenn man Feature Releases nicht einfach ohne Tests ausrollen will. Meine persönliche Empfehlung schließt noch zwei weitere Ringe mit ein. Bevor Sie die Updates in dem eben beschriebenen zweiten Ring, also für technikaffine Benutzer freigeben, sollten Sie das neue Feature Release erst einmal ausführlich auf den Arbeitsplatzrechnern der Administration und des User Helpdesk nutzen – der muss die Probleme ja hinterher eh ausbaden und sollte sich insofern sowieso am besten mit den neuen Clients auskennen. Lassen Sie sich auf jeden Fall zwei bis drei Monate (ersetzen Sie Monate mit kumulative Updates) Zeit, bevor Sie ein Feature Release auf Produktivsysteme loslassen. Die letzten Feature Releases hatten zur Veröffentlichung so viele Bugs, dass Sie die ganz sicher nicht auf Anwender-PCs haben wollen. Das Gleiche gilt für kumulative Updates – ich kann Ihnen aufgrund der Erfahrungen mit der Qualität von Updates nicht empfehlen, ein CU sofort nach Erscheinen auszurollen. Verzögern Sie die Updates um ein oder zwei Wochen und lesen Sie in dieser Zeit die einschlägigen Newsseiten wie Heise.de oder Golem.de. Wenn es zu größeren Problemen kommt, werden Sie das hier vermutlich frühzeitig erfahren und können im Zweifel die Updates einfach aussetzen.

Für sehr kritische Systeme bietet es sich eventuell an, die LTSC-Version von Windows in Betracht zu ziehen. Microsoft sieht die LTSC-Version zwar nicht gerne auf Anwenderrechnern, sondern empfiehlt sie nur für Bank- oder Kassensysteme, aber letztlich ist auch die LTSC-Version nur ein Windows 10 ohne Cortana, Apps und Edge.

12.1.4.2 Bereitstellungsringe implementieren (WSUS)

Wenn Sie Updates mit dem WSUS verteilen, legen Sie für jeden Bereitstellungsring, den Sie benötigen, eine Computergruppe auf dem WSUS an. Sie können die Gruppen von Hand zuweisen, oder Sie erstellen für jede Computergruppe auch ein GPO und weisen die Computer dann über das GPO zu. Neue Feature Releases geben Sie dann von Hand für die jeweilige Computergruppe frei.

12.1.4.3 Bereitstellungsringe implementieren – Update for Business

Wenn Sie mit Windows Update for Business arbeiten, erstellen Sie für jeden Ring ein eigenes GPO. Wenn Sie die Computer der einzelnen Update-Ringe in eigene OUs verschieben können, verknüpfen Sie die GPOs mit den zugehörigen OUs. Ansonsten wäre eine Variante, die GPOs relativ weit oben in ihrer AD-Struktur aufzuhängen und für jeden Ring auch eine globale Gruppe anzulegen. Richten Sie nun Sicherheitsfilter ein, die das GPO nur auf den Computern anwenden, die sich in der zugehörigen Sicherheitsgruppe befinden. Sie können die Computer dann Ringen zuweisen, indem Sie sie einfach in die entsprechende Sicherheitsgruppe aufnehmen. Achten Sie aber darauf, den frühesten Ring mit der niedrigsten Priorität zu verknüpfen und den spätesten Ring mit der höchsten, damit Ihnen bei einer falsch zugewiesenen Maschine nicht plötzlich die Updates um die Ohren fliegen.

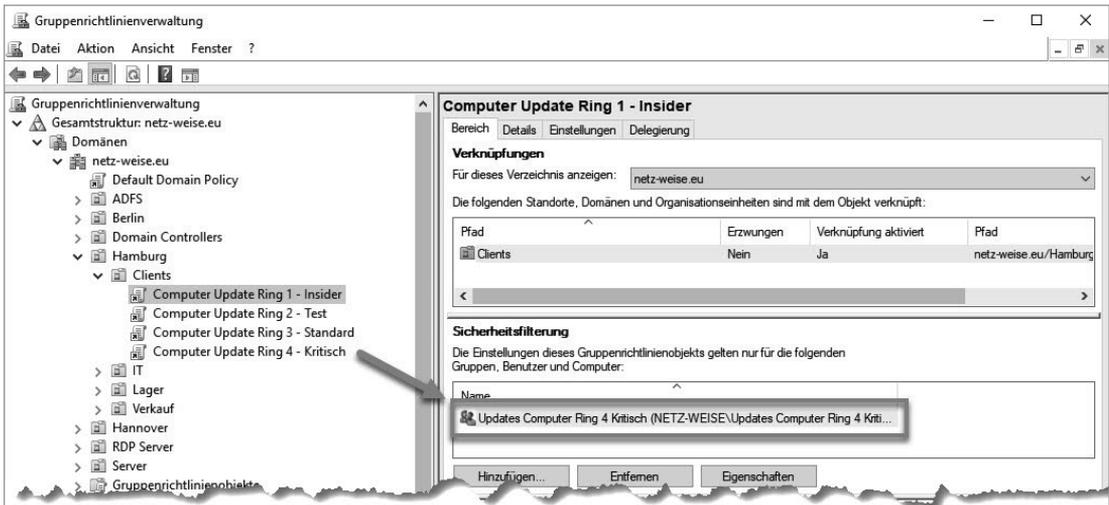


Bild 12.4 Für jeden Ring gibt es ein GPO und eine Gruppe, auf die gefiltert wird.

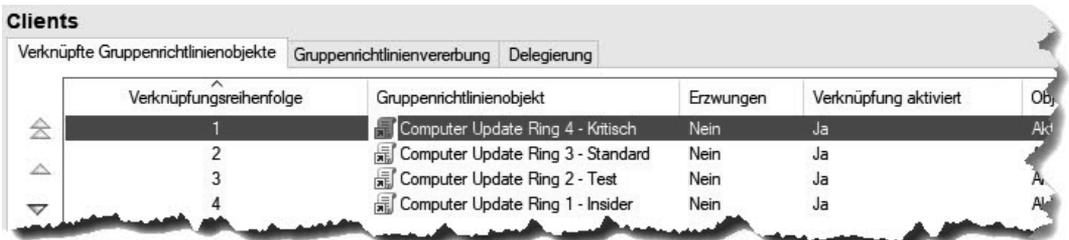


Bild 12.5 Achten Sie darauf, die kritischste Gruppe in der Verknüpfungsreihenfolge ganz nach oben zu schieben.

Nun können Sie die Windows Update for Business-Einstellungen in den einzelnen GPOs vornehmen.

■ 12.2 Windows 10 und die Privatsphäre

Windows 10 hat neben den vielen Neuerungen auch einige, die man eigentlich gar nicht haben möchte, z.B. die automatische Übertragung verschiedener Daten ins Internet. Diese Daten werden oft auch als Privatsphäre-Einstellungen bezeichnet. Dabei unterscheidet Microsoft zwei verschiedene Typen von Daten, nämlich Telemetriedaten und Funktionsdaten. Telemetriedaten sind Daten, die von Microsoft über die Funktionsweise von Windows gesammelt werden, wie installierte Programme, installierte Updates, installierte Hardware usw., aber auch und vor allem Daten über die Zuverlässigkeit von Windows wie Programmabstürze. Funktionsdaten sind Daten, die vornehmlich von Apps an den App-Hersteller übertragen werden, weil die Funktion der App eigentlich von einem Dienst irgendwo im Internet zur Verfügung gestellt wird und die App nur als Front-End fungiert. Was nach der Verwendung der Daten danach beim Hersteller passiert, ist für den Kunden normalerweise nur schwer nachvollziehbar, gelöscht werden die Daten nur in den seltensten Fällen.

12.2.1 Windows Telemetrie

Telemetriedaten sind für Microsoft extrem wichtig, seit Windows in Form von Feature Releases ausgerollt wird. Während früher jeder neuen Windows-Version eine ziemlich lange Beta-Phase vorausging, stehen Microsoft jetzt vom Beginn eines neuen Entwicklungszyklus bis zum Release nur sechs Monate zur Verfügung. Im Vorfeld finden die Tests durch freiwillige Beta-Tester statt, die Updates durch die Insider Preview beziehen. Wenn ein neues Feature Release erscheint, sind die neuen Funktionen damit nicht wirklich ausreichend getestet. Das betrifft nicht nur Fehler, sondern auch die Anwenderfreundlichkeit. Um schnell an Nutzungsdaten zu kommen, wird die Windows Home Edition quasi zwangsaktualisiert, und die Verwendungs- und Fehlerinformationen werden dann automatisch im Hintergrund an Microsoft übermittelt. Die Telemetriedaten sollten nicht anwenderspezifisch ausgewertet werden, da es Microsoft letztlich nicht darum geht, Daten über einen einzelnen Benutzer zu sammeln, sondern Windows möglichst schnell (innerhalb von vier Monaten, bis das aktuelle Feature Release zum Semi-Annual Update gereift ist) in ein für Unternehmenskunden ausreichend stabiles Release zu bringen. Ich habe hier absichtlich „sollten“ geschrieben, denn die Telemetriedaten werden verschlüsselt im Hintergrund übertragen und bis zum Release 1803 hatte man keine Möglichkeit zu prüfen, was Windows tatsächlich an Daten und wann übermittelt. Seit der Version 1803 bietet Microsoft die Möglichkeit, mithilfe einer App aus dem Windows Store die gesammelten Telemetriedaten anzuzeigen, den Diagnostic Data Viewer.

Wie viele Telemetriedaten Microsoft sammeln darf, kann man anpassen, wobei es Unterschiede in den einzelnen Windows-Versionen gibt. Die Einstellungen sind lokal auf dem Client in den Einstellungen unter **Datenschutz – Diagnose und Feedback** konfigurierbar –

s. Bild 12.6. Hier können Sie zwischen „Einfach“ und „Vollständig“ auswählen – ein vollständiges Deaktivieren der Datensammlung ist nicht vorgesehen! Über Gruppenrichtlinien haben Sie in der Enterprise Edition die Möglichkeit, die Sammlung noch weiter einzuschränken, aber komplett verhindern können Sie die Übermittlung nur, wenn Sie die Telemetrie-Server durch Ihre Firewall blocken lassen. Einen interessanten Artikel, wie Sie das mit der Windows Firewall erreichen können, finden Sie bei WinAero unter <https://winaero.com/blog/stop-windows-10-spying-on-you-using-just-windows-firewall/> oder kurz <https://bit.ly/2OrO2NZ>. Microsoft hat ebenfalls eine vollständige Liste aller URLs unter <https://docs.microsoft.com/en-us/windows/privacy/windows-endpoints-1803-non-enterprise-editions> oder kurz <https://bit.ly/2OrGATc> veröffentlicht.



Sollten Telemetriedaten abgeschaltet werden?

Telemetriedaten sind ein sehr emotionales Thema. Microsoft hat den Fehler gemacht, im Vorfeld von Windows 10 wenig darüber aufzuklären, welche Daten gesammelt werden und was mit diesen Daten dann passiert. Tatsächlich enthalten Telemetriedaten keine Benutzerdaten, sondern Verhaltensdaten über die Nutzung von Funktionen, die verwendete Hardware und Applikationsverhalten. Diese Daten werden nicht individuell ausgewertet, sondern mit anderen Daten zusammengeführt und sollen laut Microsoft größtenteils nach 30 Tagen gelöscht werden. Zusätzlich werden Programme, die ein auffälliges Verhalten an den Tag legen, von Windows Defender an Microsoft übertragen, um so Malware frühzeitig erkennen und die Defender-Antivirensignaturen entsprechend anpassen zu können.

Die Telemetriedaten können außerdem dazu verwendet werden, Features wie Windows Update for Business zu überwachen. Microsoft stellt hierfür mit den Azure Cloud-Diensten eine Funktion namens Windows Analytics zur Verfügung, die die Funktion eines WSUS Reporting-Servers übernehmen kann und anzeigt, welche Clients auf welchen Update-Ständen sind oder schon lange keine Updates mehr bezogen haben. Dafür muss auf den Clients eine Customer-ID hinterlegt werden, über die Microsoft die Clients dann einem spezifischen Kunden zuweisen kann. Hierfür muss die Telemetrie aber aktiviert sein, da Daten über den Update-Stand sonst nicht übertragen werden können.

Grundsätzlich sind Telemetriedaten also nicht schädlich, aber Sie sollten durchaus mit dem Diagnostic Data Viewer selber überwachen, was Microsoft an Daten sammelt, denn das kann sich mit jedem Windows Update ändern.

Für die manuelle Konfiguration der Telemetrie-Einstellungen stehen zwei Optionen zur Wahl – „Einfach“ oder „Vollständig“. Unter Windows 10 Professional ist standardmäßig „Vollständig“ aktiviert, unter Windows 10 Enterprise „Einfach“. Wenn der Client Updates über die Insider Preview erhält, ist „Vollständig“ Pflicht und kann nicht umgestellt werden.

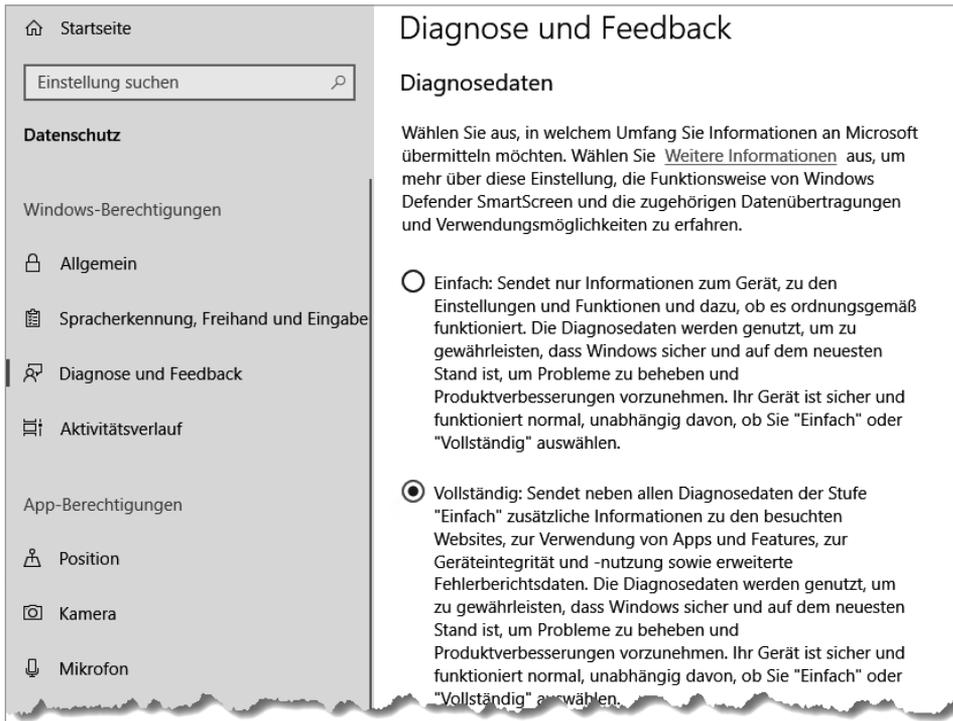


Bild 12.6 Sie können Diagnosedaten nur auf „Einfach“ stellen, sie aber nicht deaktivieren.

In den GPOs finden Sie die Telemetrie-Einstellungen in der Computerkonfiguration unter **Administrative Vorlagen – Windows-Komponenten – Datensammlung und Vorabversionen**. Unter **Telemetrie zulassen** können Sie anpassen, wie viele Daten an Microsoft übertragen werden. Ihnen stehen hier vier Stufen zur Verfügung.

Stufe	Bedeutung
0 – Sicherheit (Nur Enterprise)	Diese Einstellung sammelt nur Informationen über das Malicious Software Removal Tool (MSRT), Windows Defender und System Center Endpoint Protection sowie einige wenige Basisdaten für die Konfiguration der Telemetrie-Dienste selbst. Die Antimalwaredaten werden nicht übermittelt, wenn Sie MSRT abschalten und eine Fremdhersteller-Antiviruslösung verwenden. Diese Einstellung wird nur von Windows 10 Enterprise ausgewertet. Alle anderen Windows-Versionen ignorieren diese Einstellung.
1 – Einfach	Zu den Daten aus Stufe 0 werden Geräteinformationen gesammelt (Prozessor, Speicher, OS-Daten, Internet-Explorer-Version usw.), Informationen über Abstürze und Anwendungsfehler, Kompatibilitätsdaten und den Microsoft Store.
2 – Erweitert	Zu den Daten aus Stufe 0 und 1 werden Ereignisse (aus dem Ereignisprotokoll) gesammelt, die über Windows-Komponenten, Microsoft-Apps und -Geräte protokolliert wurden, sowie Absturz-Diagnosedaten. Diese Stufe lässt sich nicht in den Windows-Einstellungen manuell konfigurieren, sondern nur über Gruppenrichtlinien!

(Fortsetzung nächste Seite)

Stufe	Bedeutung
2 – Erweiterte Diagnosedaten auf die von Windows Analytics erforderlichen Daten beschränken	Diesen Level aktivieren Sie über die Stufe 2 und die zusätzliche Richtlinie „Erweiterte Diagnosedaten auf die von Windows Analytics erforderlichen Daten beschränken“. Sie können den Clouddienst Windows Analytics verwenden, um die Daten Ihrer Clients zentral auszuwerten. Durch Windows Analytics ist es z. B. möglich, die Windows Update for Business-Daten zentral zu sammeln. Windows Analytics benötigt für die Datensammlung mehr Informationen, als die Stufe Basis zur Verfügung stellt. Mit dieser Richtlinie schränken Sie die Einstellung „Erweitert“ auf das Minimum ein, das für Analytics notwendig ist. Diese Richtlinie steht ab Feature Release 1709 zur Verfügung.
3 – Vollständig	Die vollständige Telemetrie sammelt neben den Stufen 0 bis 2 noch Daten zu Pre-Release-Apps von Windows, die im Windows Insider-Ring ausgerollt werden. Außerdem kann Microsoft vom Client zusätzliche Daten wie Registry-Keys, vollständige Absturz-Diagnosedaten und Reports von msinfo32.exe, dxdiag.exe und powercfg.exe bei Bedarf anfordern, um Windows Fehler zu analysieren. Dies ist die Standardeinstellung in Windows 10 Pro.

Eine vollständige Auflistung, wie Microsoft die Daten auswertet und welche Daten genau übertragen werden, finden Sie unter <https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization> oder kurz <https://bit.ly/2LZbf8N>.

Unter Datensammlung und Vorabversion gibt es noch eine Reihe von weiteren interessanten Einstellungen zur Telemetrie.

Einstellung	Auswirkungen	FR
Benutzersteuerung für Insider-Builds ein-/ausschalten	Wenn Sie diese Einstellung auf deaktiviert setzen, können Benutzer Windows 10 nicht mehr selbstständig in die Insider Preview aufnehmen. Diese Einstellung wird ab Feature Release 1709 über die Einstellung „Vorabversionen verwalten“ unter Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Windows Update – Windows Update für Unternehmen konfiguriert.	Bis 1703
Übermitteln des Gerätenamens in Windows-Diagnosedaten zulassen	Hiermit können Sie aktivieren, dass der Name des Windows-Gerätes in den Telemetriedaten übermittelt werden darf. Standardmäßig wird er nicht übermittelt!	Ab 1803
Organisations-ID konfigurieren	Wenn Sie Windows Analytics verwenden, werden über die Organisations-ID Ihre Windows-Geräte Ihrer Organisation zugeordnet. Mehr dazu finden Sie unter https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-get-started oder kurz https://bit.ly/2NT67Dz und https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-privacy oder kurz https://bit.ly/2AIDhtN .	

Index

Symbole

@() 549
\$_ 533
\$AllNodes 578, 580
.aas 404
.cab 503
Configuration 573
Configuration Modes 572
[DSCLocalConfigurationManager()] 581
@GenerationHost 573
*.msi 66
*.msp 66
*.mst 66
*.zap 66

A

Abfragedefinition 39
Abfragen 42
Abmeldeskripte 273, 519
Abteilungslaufwerk 262
Active Directory 240
AD-Cmdlets 547
Add-ADFineGrainedPasswordPolicySubject 553
AD-Design 46
Add-Member 552
ADM-Datei 185, 188, 267, 404
Administrative Vorlagen 183
– Active Directory 240
– Biometrie 218
– Defender 226
– Desktop 239
– erweitern 261
– Filtern 419
– Herunterfahroptionen 225
– Optionen für das Herunterfahren 225
– Windows Update 234
Administratoren, Standort 48
Administratorkonto 102
Administrator umbenennen 113
ADML-Datei 184, 265
ADMX-Datei 184, 262
– erstellen 267
ADMX Migrator 267
ADMX und ADML erweitern 261
Adobe Flash 379
Advanced options, Specops 86
Advertise only, Specops 88
Aero Shake 239
AGPM 287
AGPM 4.0 SP3 468
AGPM, Administratorzugriff 471
agpm.admx 475
AGPM-Archiv 480
AGPM, Archivordner 469f.
AGPM-Backup 470
AGPM, Best Practices 515
AGPM-Client 466
AGPM, Clientinstallation 473
AGPM, Clientinstallation automatisieren 475
AGPM, Clientkonfiguration anpassen 475
AGPM-Dienst 467
AGPM-Einrichtung 477
AGPM, E-Mail-Server 478
AGPM-Konfiguration 514
AGPM-Logging 479, 496
AGPM-Pfad 512
AGPM, Port 472
AGPM-Server
– automatisch konfigurieren 494
– Erreichbarkeit testen 477
– Installation 470
– Standort konfigurieren 475
AGPM Service 473
agpmserv.log 515

- Aktualisierungen
 - Softwareverteilung 76
 - Aktualisierungsintervall 416
 - anpassen 416
 - AllDrives 263
 - AllSigned 525
 - Alternative Programme 69
 - Änderungen, MSI 78
 - Änderungen nachvollziehen 497
 - Änderungssteuerung 477
 - Änderungsverlauf 490
 - Anforderung GPO 491
 - Anmeldeereignisse 105
 - Anmelden 243
 - Anmeldenachricht 112
 - Anmeldeprobleme 518
 - Anmeldeskript 273, 288, 518 f.
 - Anmeldeskripte vs. Gruppenrichtlinieneinstellungen 518
 - Anmeldeskriptverzögerung 523
 - Anmeldeversuche 105
 - Anmeldezeiten 253
 - Anmeldung 2, 75, 441
 - Programme steuern 243
 - Anmeldung, Live-ID 113
 - Anpassen
 - Softwarebereitstellung 75
 - Anpassung (früher Anzeige) 247
 - Ansatz, administrativer 106
 - Ansicht, klassische 239
 - Antrag ablehnen 492
 - Antrag zum Anlegen einer neuen Richtlinie 490
 - Anwenden-Berechtigung 399
 - Anwenden, WMI-Filter 40
 - Anwenderfeatures 372
 - Anwendung
 - QoS 284
 - Anwendungseinstellungen 299
 - Anwendungs-Ereignisprotokoll 333
 - Anwendungsidentität 157
 - Anwendungsidentitätsdienst 157
 - Anwendungsprotokoll 456, 458
 - Anwendungssteuerungsrichtlinie 564
 - Anzeige 247
 - Benutzername 112
 - Application Advertisement Script 404
 - Application Control 385
 - Application Guard 388
 - AppLocker 155, 370
 - AppLocker umgehen 161
 - Approver 467, 480, 484
 - Archiv
 - Anzahl der letzten Versionen 477
 - sichern 512
 - Archivbackup 512
 - Archivbesitzer 471, 482
 - wechseln 482
 - ArchivePath 512
 - Archivierte GPO-Version 500
 - Archivierung 560
 - Archivordner 470
 - Archiv-Pfad 512
 - Array 549
 - Asynchrone Skriptverarbeitung 522
 - Auditing 171
 - Audit Mode 163
 - Aufbewahrung 117
 - Aufbewahrungsmethode 117
 - Auschecken 481, 493, 500
 - Aus dem AGPM-Archiv löschen 500
 - Ausführungsrichtlinie 524
 - Einstellungen 525
 - Gültigkeitsbereich 526
 - konfigurieren 525
 - Ausgecheckte GPO 493
 - Ausgecheckte Richtlinie verknüpfen 506
 - Auslagerungsdatei löschen 111
 - Auswerten, Gruppenrichtlinienmodellierung 455
 - Authentication Silos 316
 - Authentifizierung
 - WLAN 137
 - zertifikatsbasiert 571
 - Automatisches Erkennen
 - BranchCache 196
 - Automatische Updates
 - WSUS 238
 - Automatisch installieren 75
 - Azure AD 370
- ## B
- Backtick 549
 - Backup 275, 498
 - AGPM 514
 - aller Gruppenrichtlinien 533
 - des Archivs 512
 - für alle GPOs erstellen 533
 - kürzlich modifizierte GPOs 538
 - Backup-GPO 533
 - Bandbreite 283
 - Basisordner 276

- Bearbeiten, Pakete 74
- Bearbeiter 467, 480, 484
- Befehlszeilenreferenz 457
- Behandelter Fehler 551
- Benachrichtigung
 - Updates 238
- Benutzerauswahl 444
- Benutzerdaten 275
- Benutzerinformationen 112
- Benutzerkonfiguration 75
 - analysieren 443
 - Windows-Einstellungen 271
- Benutzerkontensteuerung 107
- Benutzeroberflächenoptionen 76
 - Softwareverteilung 75
- Benutzerprofile 243, 275
- Benutzerrechte 106
- Berechtigung 121, 442, 485
 - AGPM 482
 - auf GPO 12, 485
 - GPC 399
 - NTFS 122
 - setzen, PowerShell 557
 - verweigern 32
- Berechtigungshierarchie 498
- Bereiche, Gruppenrichtlinienverwaltungs-Editor 16
- Bereitstellen, Software 75
- Bereitstellungsart 75
- Bereitstellungsoptionen 75
- Bereitstellungsringe 352
 - implementieren 354
- Beschränkung, QoS 284
- Besitzer
 - GPO 10
 - NTFS 122
- Best Practice 62
- Best Practices Analyzer 425
- Betriebsstatus 42
- Betriebssystem 442
 - -komponenten 447
- Biometrie verwenden 234
- BitLocker 219
 - Netzwerkensperrung 221
- BITS 235
- BITS-Dienst 197
- Boolesche Operatoren 296
- BranchCache 194, 348
 - Modus 196
- Bypass 525

C

- Central Policy Store 186
- Change 466
- Change Control 477
- Chef 568
- Chronologische Auflistung aller Änderungen 498
- Clientcomputercache 196
- Clientseitige Zielzuordnung, Updates 238
- Client Side Extensions 409
- Cloud 392
- Codeintegritätsrichtlinie 387
- Code Signature Integrity 385
- comment.cmx 405
- Compliance-Server 571
- Computerauswahl 443
- ConfigurationData 578 f.
 - auslagern 581
- Configuration Drift 567, 571
- Connection Manager Administration Kit 317
- Constrained Language Mode 162
- Container
 - Definition 401
 - Unterschied OU 46
- Container-Objekte 401
- Continuum 371
- Cortana 341, 361
- Credential Guard 384, 386
- CRUD-Prinzip 288
- CSE 410
 - EnableAsynchronousProcessing 411
 - Installation überprüfen 82
 - NoBackgroundPolicy 411
 - NoSlowLink 411
 - NoUserPolicy 411
 - Specops verteilen 81
 - Systemregistrierungseinstellungen 410
- CSE-Einstellungen 205
- Current Branch 341
- Current Branch for Business 341

D

- Dateierweiterung 75
- Datei-Explorer 250
- Dateisystem 120, 122
- Dateitypen
 - designierte 153
 - Softwareverteilung 66
- Datensammlung und Vorabversion 358

- Datenverkehr 283
 - DCOM 108
 - Deaktivieren
 - Gruppenrichtlinien 20
 - Vererbung 22
 - Verknüpfungen 22
 - von Skripten 564
 - Debug-Logging 460
 - Default Domain Controllers Policy 397
 - Default Domain Policy 397
 - Defender 226
 - Deinstallation Package,Specops 92
 - Deinstallation,Specops 86
 - Deinstallieren, Softwareverteilung 75
 - Delivery Optimization 342
 - Delta-Updates 342
 - DependsOn 574
 - Deployment options, Specops 88
 - Deployments editieren, Specops 92
 - Designierte Dateitypen 153
 - Desired State Configuration 567
 - Desktop 239
 - Desktop Optimization Pack 466, 468
 - Desktopsymbole 239
 - Desktopsymbolleisten 239
 - Device Guard 386
 - DevOps 567
 - Dezimalwert 263
 - DFS 289
 - DFS-N 289
 - DFS-R 289
 - repliziert 70
 - DFSR 405
 - Diagnosedatenanzeige 360
 - Diagnostic Data Viewer 355, 360
 - Diensteinträge 441
 - Dienstgüte 283
 - Dienstkonto AGPM 469
 - Dienst, QoS 284
 - Differentiated Services Codepoint 283
 - Differenz
 - zur letzten Version 497
 - zur Vorlage 497
 - Differenzen anzeigen 508
 - zwischen Versionen eines GPO 509
 - Differenzreport 485, 509
 - Direct Access 414
 - Disable Software Updater,Specops 90
 - dism.exe 368
 - displayName-Definitionen 263
 - Distributed File System 289
 - Distributed File System Replication 405
 - DMA-Schutz 387
 - DNSAdmins 120
 - DNS-Fehler 441
 - DNSSEC 98
 - Domänenanmeldung 105
 - Domänencontroller 108
 - Funktion 395
 - Domänencontrollerwahl 451
 - Domänenmitglied 108
 - Domänenprofil, Firewall 127
 - Drahtlosnetzwerkrichtlinien 135, 398 f.
 - Drosselungsrate, QoS 284
 - Drucker 248
 - Richtlinien 399
 - zuweisen 273
 - Druckertreiber 320
 - DSC 567
 - Ersatz für Gruppenrichtlinien 568
 - Erstellen einer Konfiguration 572
 - Konfiguration 573
 - node 573
 - Unterschied zu den Windows-Gruppenrichtlinien 568
 - Unterschied zu Gruppenrichtlinien 570
 - DSC-Client 571
 - DSC-Konfiguration 575
 - DSCP 283
 - DSGVO 171
 - DSVersion 540
 - Dual-Scan 236
- ## E
- Edge 388
 - Standalone Mode 388
 - Unternehmensmodus 388
 - Edge Browser 379
 - Editor 467, 480
 - Effizienz 97
 - Eigenschaften, Softwareverteilung 74
 - Eigenschaft, gpLink 49
 - Eindeutige Versionen 500
 - Einfach, Benutzeroberflächenoptionen 76
 - Eingabeaufforderung 242
 - Eingeschränkte Gruppen 118, 315
 - Einrichten, Loopbackverarbeitungsmodus 25
 - Einschränkungen bei der Geräteinstallation 309
 - Einstellungen
 - Diagnoselog 335

- Dienste 326
- Energieoptionen 318
- Funktionstasten 312
- GEMEINSAME OPTIONEN 331
- Geplante Tasks 323
- Geräte 309
- gesichertes GPO 431
- GPO 11
- grüne Linien 311
- importieren, AGPM 494
- Ini-Dateien 303
- Internetereinstellungen 313
- kopieren 294, 330
- Lokale Benutzer und Gruppen 315
- Netzwerkooptionen 317
- Ordneroptionen 311
- regionale 323
- Register Anzeige 247
- Startmenü 328
- Tastaturlayout 323
- Verknüpfungen 306
- XML-Darstellung 329

Einwählverbindung 452

Element entfernen, wenn es nicht mehr angewendet wird 305

ELSE 544

ELSEIF 544

Empfohlene Updates, WSUS 238

Empfohlene Vorgehensweisen 62

End user interaction, Specops 88

Energieverwaltung 244

Enter-PSSession 576

Entfernen, WMI-Filter 41

Ereignisanzeige, Gruppenrichtlinienverarbeitung 449

Ereignisprotokoll 106, 116

- Umgang 117

Ereignisweiterleitung 117

Ererbte Berechtigungen entfernen 493

Ergebnis 444

Erkennung von langsamen Verbindungen 206

Erlaubte Anmeldezeiten 253

Erroraction 551

Erstellen

- von Richtlinien 484
- WMI-Filter 38

Erweiterte Bereitstellungsoptionen 76

Erweiterte Überwachungsrichtlinienkonfiguration 171

Erzwingen 153, 412

Erzwingungsmodus 164

Erzungen 10, 23, 442

Eventlog 458

Express-Updates 342

ExtensionData 542

Extra Registry Settings 187

F

Fastboot 422

Fast Logon 73

Fast Logon Optimization 201, 412

Fast Startup 412

Fast Startup Modus 68

fdeploy.ini 405

Feature Releases 339

Fehlercodes 334

Fehlersuche 441

Fehler und Warnungen protokollieren in AGPM 496

File Replication Service 405

Filtern 29

- PowerShell 535

Filteroptionen 254

FilterRunOnceID 332

Find-DSCResource 569

Flags 400

Folder Redirection 282

Foreach-Object 533, 551

Freeware 69

Freigabe

- erstellen 70

FRS 405

FullArmor 267

Funktionen 543

Funktionstrennung 484

G

Gastkonto 113

Gastkontozugriff 117

GDPR 171

Gelöschte Objekte wiederherstellen 500

Genehmigende Person 467, 480, 484, 489

Geplante Installation, Updates 238

Geplanter Neustart, Updates 238

Geräteinstallation verhindern 202

Geräte, Sicherheitsoptionen 111

Gesperrte Sitzung 112

Gesteuerte GPO 489

Get-ADDefaultDomainPasswordPolicy. 553

Get-ADDomain 547

- Get-ADFineGrainedPasswordPolicy 553
- Get-ADGPOReplication 563
- Get-ADObject 554
- Get-ADOrganizationalUnit 547f.
- Get-AppxPackage 368
- Get-AppxProvisionedPackage 368
- Get-Date 536
- Get-DscLocalConfigurationManager 571
- Get-DSCResource 568, 574
- Get-Eventlog 333
- Get-Executionpolicy-List 526
- Get-GPExtensions 409
- Get-GphPrefRunOnceKey 333
- Get-GPInheritance 558
- Get-GPO 397, 531
- Get-GpoReport 532
- Get-GPPermission 559
- Get-GPRegistryValue 550
- Get-GPResultantSetOfPolicy 560
- Get-GPStarterGPO 560
- Get-Member 537
- Getrennte administrative Rollen 480
- GPC, Berechtigungen 399
- gPCMachineExtensionNames 400
- gPCUserExtensionNames 400
- GPE
 - asynchron 413
 - GPO-Verarbeitung 400
 - GUID 417
 - synchron 413
 - Verarbeitung 417, 423
- gpLink 412, 547
- gpLink-Attribut 401
- gpLink-Flags 400
- GPMC 5
- GPO
 - abfragen 397
 - Administratorrechte 408
 - Änderungen anzeigen 467
 - anlegen mit PowerShell 556
 - Anwenden-Berechtigung 399
 - asynchrone Verarbeitung 412f.
 - aus AGPM entfernen 501
 - auschecken 481
 - bereitstellen 480
 - bereitstellen, AGPM 494
 - Dateisystem 403
 - deaktiviert 442
 - displayname 397
 - dokumentieren 54
 - domänenübergreifend 407
 - Einstellungen importieren/migrieren 432
 - ermitteln 412
 - Fastboot Verarbeitung 422
 - freigeben 467, 495
 - GUID 397
 - Hintergrundverarbeitung 415
 - History 417
 - importieren 503
 - Kommentarfunktion 405
 - kopieren 60
 - Lesen-Berechtigung 399
 - mit WMI-Filter finden 538
 - ohne Beschreibung filtern 539
 - Ordner 403
 - Planung Standorte 50
 - Registry-basierte Einstellungen 405
 - Registry-Einstellungen 418
 - Schreiben-Berechtigung 399
 - sichern und wiederherstellen 427
 - Standorte 407
 - synchrone Verarbeitung 412, 414, 421
 - synchrone Verarbeitung deaktivieren 413
 - testen 58, 506
 - Verarbeitung 395
 - Verarbeitung erzwingen 419
 - Versionsnummer 403
 - berechnen 403
 - Vordergrundverarbeitung 415
 - wiederherstellen 430
 - Zentraler Speicher 185
- GPO, Benennung 53
- GPO, Benennungsstrategie 45
- GPO, Berechtigungen auflisten 559
- gpo.cmt 405
- GPO-Differenzen 480
- GPO-Export 503
- GPO Health Check 538
- GPO-Import 503
- GPO, Kommentar 55
- GPO-Migration 562
- GPO mit WMI-Filter finden 538
- GPO, Namenskonvention 53
- GPO Reporting 563
- GPOs dokumentieren, PowerShell 531
- GPOs finden, die lange nicht geändert wurden 538
- GPOs migrieren 563
- gpostate.xml 513
- gpo-Verknüpfung erzeugen 498
- GPO-Versionen vergleichen, beliebige Versionen 509

- GPO-Vorlage 489
- GPO, wie viele Einträge 52
- GPRresult 457
- gprresult.exe 334
- GPSvc.Log 460
- GPT 412
 - Machine-Ordner 404
 - User-Ordner 404
- gptime.exe 462
- gpt.ini 405
- GPT.INI 403
- GptTmpl.inf 404
- gpupdate 73
- GPUupdate.exe
 - Force 420
- Group-ID 348
- Group Policy Caching 421
- Group Policy Container 395
- Group Policy Extensions, GPO-Verarbeitung 400
- Group Policy Preferences 287
- Group Policy Settings Reference 257
- Group Policy Template 403, 412
- Gruppen
 - eingeschränkte 118
- Gruppenrichtlinie
 - Benutzerkonfiguration 245
 - erstellen 14
 - in Teams bearbeiten 465
 - verknüpfen 14
- Gruppenrichtlinien-Aktualisierungsintervall 207
- Gruppenrichtlinienclient 395
- Gruppenrichtlinienclient, Dienst 408
- Gruppenrichtlinieneinstellungen 287, 518
 - Verarbeitungsreihenfolge 294
- Gruppenrichtlinienergebnis-Assistent 443
- Gruppenrichtlinienergebnissatz 457
- Gruppenrichtlinienergebnisse 442
- Gruppenrichtlinienergebnis untersuchen 444
- Gruppenrichtlinienerweiterung 518
- Gruppenrichtlinienmodellierung 451
 - auswerten 455
- Gruppenrichtlinienobjekt 501
 - anlegen 501
 - im AD entfernen 500
 - PowerShell 531
 - sichern 427
- Gruppenrichtlinienverarbeitung 444
 - asynchron 68
- Gruppenrichtlinien verknüpfen, Berechtigungen 47
- Gruppenrichtlinien-Verlaufsdaten 416

- Gruppenrichtlinienverwaltung 8
- Gruppenrichtlinienverwaltungs-Editor 16
- Gruppenrichtlinienverwaltungskonsole 5
- Gruppenrichtlinien zur Erkennung von langsamen Verbindungen konfigurieren 424
- Gruppenrichtlinien-Zwischenspeicherung 421
- GUIDs finden 546

H

- Hardwarekomponenten 42
- Hashregel 152
- Hash-Tabellen 579
- Herausgeber-Regel 159
- Herausgeber, vertrauenswürdige 154, 238
- Herunterfahren 111, 115, 422
- Herunterfahren-Skripte 519
- Herunterfahroptionen, Administrative Vorlagen 225
- Hiberfil.sys 422
- Hintergrundaktualisierung 2, 415, 417, 420
- Hintergrundverarbeitung 304, 415
- Historische Version 500
- Hkey_Current_User 418
- Homedirectory 262
- Hotfix KB3000850 529
- HTML-Report 494
- Hyper-V 383

I

- idempotent 571
- IF 544
- Importeinstellungen-Assistent 433
- Importieren
 - GPO-Einstellungen 432
 - in ein bestehendes GPO 505
 - in ein neues GPO 503
- Import-Module 562
- In AGPM gespeicherte Gruppenrichtlinienobjekte 512
- inf-Datei 176
- Informationen, Gruppenrichtlinienverarbeitung 445
- In-Place-Upgrade 340
- Installation AGPM 468
- Installationsfreigabe 70
- Installationsoptionen, Specops 85
- Installations-Report, Specops 91
- Installationstyp, Specops 87
- Installation überprüfen, Specops 90

Installer 66
 Installieren, GPMC 7
 Install-Module 569
 Integrated Scripting Environment 537
 Interaktive Anmeldung 111f.
 Internet Explorer 379
 – Wartung 272
 Internet Explorer Administration Kit 313
 Internet Explorer-Wartung 272
 Intranet-Speicherort, Updates 238
 Intune 392
 Inventarisierung 165
 Invoke-GPUupdate 421
 IP-Drucker 320
 IPsec 171
 – Einstellungen 131
 IPSec 398
 IP-Sicherheitsrichtlinien 171, 399
 ISE 537
 Item Level Targeting 292

J

JEA 530
 JSON 361

K

Kabelnetzwerke 123
 – Richtlinien 399
 Kategorien 70
 Kennwort
 – -alter 101
 – -chronik 101
 – Einstellungsobjekte 100
 – -länge 101
 – -richtlinie 100
 Kennwortrichtlinie
 – granuliert 553
 – Gruppenrichtlinienbasiert 553
 Kennwortrichtlinienobjekte, granuliert anlegen 553
 Kerberos-Richtlinie 100, 103
 Kernel Mode Code Integrity 385
 Kiosk-PC 25
 KiXstart 518
 Klassifizierung, Datenverkehr 283
 Klassische Ansicht 239
 Klick-und-Los 380
 Kommentar 493
 Kommentar GPO 490

Komplexitätsvoraussetzung 101
 Komponentenstatus 444
 Konfiguration 568
 – bereitstellen 576
 – mit Parametern 577
 – Specops Deploy/App 94
 Konfigurationseinstellungen ändern, AGPM 482
 Konformität, Client 176
 Konten, Sicherheitsoptionen 113
 Kontenverwaltung 105
 Kontenverwendung 113
 Kontorichtlinien 100
 Kontosperrdauer 102
 Kontosperrungsrichtlinien 100, 102
 Kontosperrungsschwelle 102
 Kontosperrungszähler 102
 Kontrollierte Richtlinien 481
 Kumulatives Update 342

L

Labeln 508
 LAN-Manager-Authentifizierungsebene 115
 LAPS-Tool 316, 385
 Laufwerke zuweisen 273
 Laufwerksbuchstaben 264
 Laufwerksmappings 288
 LCM 571
 – konfigurieren 571, 581
 LDP.exe 396
 Leere GPOs finden 539
 Leere Gruppenrichtlinie identifizieren 541
 Leere Kennwörter 113
 Lesen-Berechtigung 399
 LGPO.exe 181
 LinkGroupPolicyObjects 548
 Liste aller verknüpften GPOs 548
 Live-ID 113
 Lizenzverwaltung 165
 Local Configuration Manager 571
 Logfiles generieren 303
 Logging, AGPM 515
 Logging-Level 509
 Login-Skripte 519
 Loglevel, AGPM 515
 Lokale Benutzer 315
 Lokale Gruppen 316
 Lokale Richtlinien 104
 Lokale Sicherheitsrichtlinie 106
 Long-Term Service Branch 341

Long-Term Servicing Channel 341
Loopbackverarbeitung 424, 452
– Ersetzen 425
– RDP-Server 425
– Zusammenführen 425
Loopbackverarbeitungsmodus 24 f., 204

M

Machine-Container 398
Mailverkehr verschlüsseln 479
Malicious Software Removal Tool 357
Malware Protection Engine 230
Managed Service Account, AGPM 469
manifest.xml 513
MAPS 230
matches 548
Mausbewegung Aero Shake 239
Maximale Größe 117
Maximales Kennwortalter 101
Maximale Wartezeit für Gruppenrichtlinienskripts angeben 523
Maximum, Benutzeroberflächenoptionen 76
meta-mof-Datei 573
Methoden 536
Microsoft.GroupPolicy.ComputerConfiguration.540
Microsoft.GroupPolicy.UserConfiguration 540
Microsoft Installer 66
Microsoft-Installer-Pakete 66
Microsoft-Netzwerk 114
Microsoft Patch 66
Microsoft Security Compliance Toolkit 177
Microsoft Store 366
Microsoft Transformer 66, 78
Microsoft Updatedienst 237
Migrationstabellen 434
Migrieren, GPO-Einstellungen 432
MIME-Type 69, 153
Minimales Kennwortalter 101
Mobile Device Management 392
Mobilnutzer 275
Modul importieren 562
Modul-Logging 527
Modulprotokollierung aktivieren 527
mof-Datei 572, 576
Mount-WindowsImage 368
MSI-Datei 70
msiexec.exe 67
MSI-Paket 66, 72

MST 78
– Änderungen 78
Multioptionsfenster 312

N

Nachricht, Anmeldung 112
Nachrichtentitel 112
Namensauflösung 441
Namensauflösungsrichtlinie 98
NAP 155
NETLOGON-Freigabe 402
Network Access Protection 155
Network Location Awareness, NLA 126, 414
Netwrix Auditor 173
Netzlaufwerke zuweisen 273
Netzwerk 241
– langsames 423
Netzwerkeinstellungen 194
Netzwerkisolation für Apps 199
Netzwerklisten-Manager-Richtlinien 132
Netzwerksicherheit 114, 123
Netzwerk- und Freigabe-Center 132
Netzwerkverbindungen 241
Netzwerkzonenregel 152
Netzwerkzugriff 115
Netzwerkzugriffsschutz 155
Neues GPO anlegen, AGPM 490
Neustart 422, 441
– Updates 238
New-ADFineGrainedPasswordPolicy 553
New-GPLink 557, 560
Nicht identifizierte Netzwerke 134
Nicht verknüpfte GPOs finden 546
NLA 414
NLA-Dienst 424
NoDrivesDropDown 263
NoViewOnDrive 262
NTFS 122
Nutzungsdaten 355

O

Objektmethoden auflisten 537
Objektstatus 21
Objektverwaltung zuweisen 48
Objektzugriffsversuche 105
ODBC-Datenquellen 308
Öffentliche Schlüssel 139
Öffentliches Profil, Firewall 127
Office 365 361, 370

- Offline-Archiv 467, 512
- Offline-Dateien 275
- Offline-Kopie 467
- OMS 172
- OpenXPS 193
- Optionen, Herunterfahren 225
- Ordner 122
- Ordnerumleitung 245, 273, 405
 - Gruppenrichtlinienzwischenspeicherung 421
- Organisationseinheit abrufen 548
- OU
 - Definition 401

- P**
- Package 82
 - App-V 84
- packageRegistration-Objekt 398
- Pakete
 - Softwareverteilung 74
 - zuweisen 72
- Papierkorb 489, 498, 500
- Partielle Konfigurationen 582
- Pass the Hash 384
- Password
 - Settings Object 100
- Patches 66
- PDC-Emulator 407
- Peer-to-Peer 235, 342, 348
- Penetration-Testing 564
- Performanceanalyse, Group Policy Operational Log 462
- Personalisierung 216
- Pfadregel 151f., 160
- PKU2U 115
- Point-and-Print-Einschränkungen 320
- Policies-Container 397
- Policies, Registry 418
- Policy Analyzer 177
- PolicyDefinitions 265
- PolicyMaker 287
- Policy Rule Sets 180
- Port 4600 477
- Port, QoS 284
- Post installation command, Specops 86
- Powercfg.exe 319
- PowerShell
 - Administrative Vorlagen 523
 - blockieren 163
 - deaktivieren 564
 - für AGPM 517
 - Get-GPRegistryValue 405
 - mit GPOs steuern 523, 564
 - Set-GpRegistryValue 405
 - Specops 94
- PowerShell-Anmeldeskripte 520
- PowerShell-Aufzeichnung 530
- PowerShell-Editor 537
- PowerShell.exe verbieten 565
- PowerShell Gallery 569
- PowerShell-Module 562
- PowerShell Operational Log 530
- PowerShell Remoting 327, 576
- Powersploit 564
- Pre installation command, Specops 86
- Problembeschreibung 448
- Produktionsdelegierung 486
- Profile
 - Firewall 127
- Profilgröße beschränken 244
- Programme und Funktionen 69
- Programmverknüpfungen 310, 376
- Proxyserver 359
- Prozessnachverfolgung 105
- Prüfer 467, 485
- PSDscAllowPlainTextPassword 580
- PsDscRunAsCredentials 574
- PSO 100
- Pull-Konfiguration 568, 570
- Pull-Server 571
 - Konfiguration 571
- Pull Server Reporting 582
- Puppet 568
- Push-Konfiguration 568, 570

- Q**
- Quality of Service (QoS) 272, 283
- Quality Updates 341
- Quell-Adresse 285
- Quell-Einstellungen 432
- Quell-Starter-Gruppenrichtlinienobjekt 71
- Querladen 367

- R**
- Rapid Release Management 568
- Rechteverwendung 105
- Redstone 340
- Redteams 564
- RefreshMode 572
- Regedit 243

- Regeln, Softwareeinschränkungen 151
 - RegEx 546
 - Register Bereich, GPMC 10
 - Register Details, GPMC 10
 - Register Kategorien, Softwareverteilung 78
 - Registrierung 120 f.
 - Schlüssel 121
 - Registrierungs-Assistent 305
 - Registrierungselement 305
 - Registrierungspfade 151
 - Registry
 - bearbeiten 243
 - Einstellungen 418
 - Policies 418
 - Policies-Schlüssel 418
 - Registry-Einstellungen in Gruppenrichtlinienobjekten 550
 - registry.pol 179, 405, 410, 550
 - Reguläre Ausdrücke 546
 - Regular Expressions 546
 - Remote Desktop 155
 - Remote Differential Compression 406
 - Remote Signed 525
 - Remoteunterstützung 209
 - Remoteverwaltungsdienst 326
 - Remove-AppxProvisionedPackage 368
 - Remove-GLink 561
 - Ressource 568
 - Abhängigkeiten 574
 - erstellen 569 f.
 - Installieren 569
 - konfigurieren 574
 - Liste 569
 - Properties 574
 - Registry 575
 - Ressourcen-Module 575
 - Restore, AGPM 514
 - Restricted 525
 - Reviewer 467, 485
 - Revision 485
 - Rezepte 568
 - Richtlinie
 - als Vorlage speichern 501
 - anlegen mit AGPM 481
 - verknüpfen, AGPM 498
 - Richtlinienänderungen 105
 - Richtlinienbasierter QoS 283
 - Richtlinienersteller-Besitzer 469
 - Richtlinien für Kabelnetzwerke 398
 - Richtlinienverarbeitung 446
 - Richtlinien-Workflow 480, 488
 - Rolle 483
 - Rollen und Berechtigungen 481
 - RSAT-Tools 473, 547
 - Ruhezustand 422
 - Windows-Schnellstart 422
 - Run logon scripts synchronously 522
 - Run Scripts synchronously 521
 - Run startup scripts asynchronously 521
- ## S
- SAM-Konto 115
 - Sammlung 296
 - Sammlungselement 305
 - Sandbox 367
 - Save-Help 524
 - Schlüssel 121
 - Registrierung 121
 - Schnellstartmenü 371
 - Schreiben-Berechtigung 399
 - Secedit.exe 176
 - secpol.msc 106
 - Secure Boot 387
 - Security Baseline 177
 - Security Compliance Manager 182
 - Security GPE
 - Aktualisierung 419
 - Select-Object-ExpandProperty 540
 - Self Encrypting Devices 222
 - Semi-Annual Update (Targetted) 341
 - Service Set Identifier 136
 - Set-ADObject 553
 - Set-ExecutionPolicy 525
 - Set-GLink 561
 - Set-GPPermission 557
 - Set-GPPrefRegistryValue 557
 - Set-GPRegistryValue 557
 - Shellobjekt 306
 - Shutdown 422
 - Sicherer Kanal 110
 - Sicherheitseinstellungen 97 f.
 - Sicherheitsfilter, Planung 51
 - Sicherheitsfilterung 29 f.
 - Sicherheitsgruppenmitgliedschaft 446, 453
 - Sicherheitskonfiguration und -analyse 175
 - Sicherheit, Softwareverteilung 79
 - Sicherheitsoptionen 107
 - Geräte 111
 - Konten 113
 - Sicherheitsprinzipale 433
 - Sicherheitsprotokoll 172

- Sicherheitsrelevante Einstellungen 97
- Sicherheitsstufen 150
- Sicherheitsüberprüfungen 115
- Sicherheitsvorlagen 174
- Sichern
 - AGPM 514
 - GPOs 427, 500, 533
- Sicherungsoperatoren 469
- Sideloading 367, 383
- SIEM 172
- Signierte Updates 238
- Silent Mode 137
- Sitzung sperren 112
- Skriptausführung aktivieren 524f.
- Skriptblöcke 529
- Skriptblock-Protokollierung 529
- Skripte 273
 - einschränken 162
 - Einstellungen in der Benutzerkonfiguration 522
 - Einstellungen in der Computerkonfiguration 521f.
 - mit Gruppenrichtlinien 518
 - über GPO 519
 - weitergeben 561
- Skriptregel umgehen 565
- Skripts 98
- Skript Timeout 518
- Slow Link 419
- Slow Link Detection 423
- Smartcards 112
- Sofortiger Task 323
- Software as a Service 339
- Software-Benachrichtigung, Updates 238
- Softwareeinschränkungen 273
 - Regeln 151
- Softwareinstallation 71
- Softwarepakete 399
- Softwareverteilung 65
 - Änderungen 78
 - Eigenschaften 74
 - Kategorien 70
 - Patchmanagement 79
 - standortübergreifend 68
 - unterstützte Dateitypen 66
 - Verteilungsrichtlinie 398, 413
 - Gruppenrichtlinienzischenspeicherung 421
 - synchrone Verarbeitung 413
- Specops
 - App-V Package 84
 - Legacy Package 84
 - Package 82
 - Targets 82
- Specops Deploy
 - Softwarepaket erstellen 82
- Specops Deploy/App 80
- Speicherort 428, 441
- Speicherplatzbelegung 196
- Sperren
 - Sitzung 112
- Sperrung 112
- Splunk 172
- Sprachassistent 361
- Sprachbefehl 361
- Sprache
 - Softwareverteilung 76
- Spracherkennung 362
- Sprachleiste 305
- Sprachsteuerung 362
- SQL-Server-Treiber 308
- SSID 136
- Standard-Apps nach Protokoll auswählen 378
- Standardinstallationen 65
- Standardvorlage 502
- Standardwerte, Softwareverteilung 76
- Standort 13
- Standortübergreifende Softwareverteilung 68
- Startbildschirm 373
- Start-DSCConfiguration 570, 576
- Starter-Gruppenrichtlinienobjekte 14
- Startlayout.xml 373
- Startmenü 69, 371
 - Programme 73
- Startmenü und Taskleiste 241
- Startmodus, getriggert 408
- Startskripte 519
- Start-Transcript 530
- STRG+ALT+ENTF 112, 246
- Strings 265
- Suchbegriffe 381
- Suchen 508
 - nach Datum 512
 - über einzelne Spalten, AGPM 511
- Suchhäufigkeit, Updates 237
- Support 340
- SWITCH 544
- Switch, Kurzform 545
- Symbolleisten 239
- Synchrone Skriptverarbeitung 522
- Synchronisation 103
- Sysinternals-Tools 299

Systemdienste 120
Systemereignisse 105
Systemprotokoll 458
Systemregistrierungseinstellungen, Registry.Pol 410
Systemregistrierungswert 550
Systemrichtlinien, NT4 418
Systemsicherheit 107
Systemstart 2, 69
Systemsteuerung 69, 246
Systemsteuerungseinstellungen 308
SYSVOL
– DFS 402
– Ordner 402
– Replikation 405
SysvolVersion 540

T

Targets 82
– Filtermöglichkeiten 93
Targetting 92
Taskleiste 239
Tattooing 418f.
Teamlaufwerke 293
Technet Gallery 562
Telemetriedaten 355
– Diagnostic Data Viewer 355
Temporäres GPO 506
Testdomäne 58
Testen
– von Änderungen 503
– von Richtlinien mit AGPM 496
Testen, Softwareverteilung 73
Test-Netconnection 478
Test-OU 58
Testumgebung 4
Threshold 340
Transfer von GPOs 503
Transformer 66, 78
Trennen
– Sitzung 112
Trustlets 383

U

Übergabeparameter 543
Übermittlungsoptimierung 348
Übernehmen der Einstellungen 32
Übertragungsrate 283
Überwachung 115, 122

Überwachungsrichtlinien 105
– erweiterte 171
Überwachungsrichtlinienkonfiguration, erweiterte 171
UEFI-Firmware 383
Umbenennen, Konten 113
Umbrechen 549
Umkehrbare Verschlüsselung 101
UNC-Pfad 71, 433
Ungesteuerte GPO 489
Universal Naming Convention 71
Universal Windows Platform Apps 366
Unrestricted 525
Unternehmensstore 369
Unternehmensvorgaben 480
Untersuchen, Gruppenrichtlinienergebnis 444
Update-Help Quellpfad 524
Updates
– aussetzen 343
– WSUS steuern 234
User Account Control 408
User-Container 398
UWP-Apps 366

V

Value 263
Variablenexplorer 303
Verarbeitung
– über eine langsame Verbindung zulassen 423
– verzögerte 421
– von Skripten konfigurieren 521
Verarbeitungsreihenfolge 17f.
– anpassen 20
– von Gruppenrichtlinienerweiterungen 301
Vererbung 22, 442
– deaktivieren, AGPM 486
Vererbungsblockierung 425
Verfügbarkeit testen 515
Vergleichsoperatoren, PowerShell 535
Verhindern
– MSI-Installationspakete 155
– Programme 155
– Windows Apps 155
Verkehr, QoS 285
Verknüpfung 10
– deaktivieren 22
– Gruppenrichtlinie 8
Verknüpfungsstandort 445
Veröffentlichen 69, 73
Version 445

- Versionen, Softwareverteilung 76
 - Versionierung 465, 498
 - Versionsliste 498
 - Versionsnummer, GPT.INI 403
 - Versionsverlauf 499
 - Vertrauenswürdige Herausgeber
 - Softwareeinschränkungen 154
 - Updates 238
 - Verwaltbarkeit 97
 - Verwaltungsbereich 75
 - Verweigern, Berechtigung 32
 - Verzeichnisdienstzugriffe 105
 - Verzögerter Neustart, Updates 238
 - Vier-Augen-Prinzip 467
 - Virtual Box 387
 - Virtualisierungsbasierte Sicherheit 383
 - Virtualisierungserweiterungen 383
 - VMWare Workstation 387
 - Vorabversionen verwalten 347
 - Vordergrundaktualisierung 304, 415
 - Vordergrundprozesse 348
 - Vordergrundverarbeitung 415
 - Vorhersagen der Gruppenrichtlinienmodellierung 451
 - Vorlagen erstellen, AGPM 501
- W**
- Webserver 571
 - Wechselmedienzugriffe 215
 - Where-Object 535
 - Wiederherstellen
 - AGPM 514
 - GPO-Backups 534
 - GPOs 427
 - Wiederherstellungsinformationen 431
 - Win64, Softwareverteilung 76
 - Windows 10
 - CSE 410
 - Windows 10 Releases 340
 - Windows Analytics 358
 - Windows-Anmeldeoptionen 253
 - Windows-Apps
 - Entwickleroptionen 218
 - Windows Defender 226
 - Windows Designer für die Imageerstellung 317
 - Windows-Einstellungen 299
 - Benutzerkonfiguration 271
 - WindowsExplorer.adml 265
 - Windows Explorer, siehe Datei-Explorer 250
 - Windows Feedback-App 359
 - Windows-Fehlerberichterstattung 226
 - Windows Firewall 125
 - Windows Hello for Business 233
 - Windows Insider 347
 - Windows Installer 66
 - Windows-Installer-Dienst 74
 - Windows Passport 233
 - Windows PE 339
 - Windows Remote Management 576
 - Windows-Schnellstart 422
 - Windows-Sperrbildschirm 216
 - Windows Store for Business 370
 - Windows Update 234
 - Windows Update for Business 342
 - Windows-WLAN-Konfigurationsdienst 135
 - WinRM 576
 - WinRM Port 576
 - WMI 34
 - WMI-Erweiterung 571
 - WMI Explorer 36
 - WMI-Filter 14, 29, 34, 442, 454
 - anwenden 40
 - Beispiele 42
 - entfernen 41
 - optimieren 43
 - per PowerShell verwalten 554
 - sichern 555
 - übertragen 555
 - WMI-Klassen 34, 42, 572
 - WMI-Query, Specops 93
 - WMI, Warnung 39
 - WQL 34, 36
 - WSUS 234, 342, 354, 373
- X**
- XML 541
 - XPS 193
- Z**
- ZAP-Dateien 66
 - Zeichentypen 101
 - Zeitplan, Updates 238
 - Zentraler Policy-Speicher 404
 - Zentrale Softwareverteilung 65
 - Zertifikate 154
 - Zertifikatsfehler 382
 - Zertifikatsregel 152
 - Zertifizierungsstellenzertifikat, WSUS 238
 - Ziel-Adresse 285

- Zielgruppenadressierung 302, 442
 - Bedingungen 296
 - Reihenfolge 294
 - Sammlungen 296
- Zielgruppenadressierung auf Elementebene 292
- Zielgruppenadressierungselement Verarbeitungsmodus 304
- Zielzuordnung, Updates 238
- Zugriff AGPM 482
- Zugriffsbasierte Auflistung 70
- Zurücksetzungsdauer 102
- Zuweisen 68
- Zwischengespeicherte Anmeldeinformationen 413
- Zwischenspeicherung von Gruppenrichtlinien 205
- Zwischenspeichernde Anmeldungen 112