

HANSER



Leseprobe

zu

Microsoft System Center Configuration Manager Current Branch

von Thomas Joos

ISBN (Buch): 978-3-446-45058-5

ISBN (E-Book): 978-3-446-45249-7

Weitere Informationen und Bestellungen unter

<https://www.hanser-fachbuch.de/>

sowie im Buchhandel

© Carl Hanser Verlag, München

Inhalt

Vorwort	XI
1 SCCM Current Branch kennenlernen und vorbereiten	1
1.1 Einführung in System Center Configuration Manager	1
1.1.1 Grundlagen zu SCCM	1
1.1.2 Anwendungskatalog, Softwarecenter und Unternehmensportal	2
1.1.3 Neuerungen im Vergleich zu SCCM 2012/2012 R2	3
1.1.4 Neuerungen in SCCM 1710	5
1.1.5 Verschiedene Configuration Manager-Branches	6
1.2 Netzwerk für SCCM Current Branch vorbereiten	8
1.2.1 Active Directory für SCCM vorbereiten	8
1.2.2 Neuen Container zur Verwaltung anlegen	8
1.2.3 Active Directory-Schema für SCCM erweitern	10
1.2.4 Gruppenrichtlinien für Firewallinstellungen im SCCM-Netzwerk konfigurieren und testen	13
1.3 Benutzerkonten anlegen und weitere Vorbereitungen durchführen	14
1.3.1 Notwendige Benutzerkonten für SCCM anlegen	15
1.3.2 WSUS im SCCM-Netzwerk verwenden	15
1.4 SCCM-Server für die Installation vorbereiten	16
1.4.1 Notwendige Serverrollen für SCCM installieren	17
1.4.2 Windows ADK installieren	19
1.5 Datenbankserver für SCCM installieren und einrichten	20
1.5.1 Neuen Datenbankserver installieren	21
1.5.2 Installierte Datenbankserver für SCCM anpassen	23
1.5.3 SQL-Verbindung zwischen SCCM und SQL verstehen	24
1.5.4 Portfreigaben und Firewallregeln definieren	24
1.5.5 Einstellungen für SQL Server anpassen	28
2 SCCM Current Branch installieren und einrichten	31
2.1 Voraussetzungen für SCCM prüfen	32
2.1.1 Voraussetzungen für Systemrollen überprüfen	32
2.1.2 Voraussetzungsüberprüfung erweitert nutzen und skripten	33

2.2	System Center Configuration Manager installieren	34
2.2.1	Voraussetzungen für SCCM herunterladen	35
2.2.2	Installation von SCCM durchführen	36
2.2.3	Fehler beheben	44
2.2.4	Unbeaufsichtigte Installation von SCCM	45
2.2.5	Optionen für die Installation von SCCM in der Eingabeaufforderung	46
2.2.6	Installieren eines sekundären Standorts	46
2.3	Updates und neue Versionen	
	für SCCM Current Branch installieren	51
2.3.1	Update zu SCCM Build 1710/18xx starten	53
2.3.2	Installation von Updates überwachen	56
2.3.3	Updates bei Problemen deinstallieren und Installationsprobleme beheben	57
2.3.4	Configuration Manager Trace Log Tool nutzen	58
2.3.5	Aufgaben nach der Installation von Updates	59
2.3.6	SCCM-Clients aktualisieren	59
2.4	Ermittlungsmethoden, Grenzen und Begrenzungsgruppen konfigurieren	60
2.4.1	Konfigurieren der Ermittlungsmethoden zum Anbinden von Clients	60
2.4.2	Verwalten der Standorte und angebundener Active Directory-Gesamtstrukturen	63
2.4.3	Begrenzungsgruppen definieren	63
2.5	Notwendige SCCM-Systemrollen zuweisen	65
2.6	Mit Richtlinien Clienteneinstellungen setzen	68
3	Erste Schritte mit SCCM	71
3.1	Clients an SCCM anbinden	71
3.1.1	SCCM-Agent automatisch installieren	71
3.1.2	Die Installation des SCCM-Agents verwalten	73
3.1.3	SCCM-Client manuell installieren	76
3.1.4	Geräte und Gerätesammlungen verwalten	77
3.1.5	Sammlungen erstellen	79
3.1.6	Sammlungen für das Bereitstellen von Anwendungen erstellen	82
3.2	Warnungen im SCCM-Netzwerk	84
3.3	Selbstwartung in SCCM	86
3.3.1	Wartungstasks erstellen	86
3.3.2	SCCM-Konfiguration manuell sichern	88
4	Betriebssysteme mit SCCM bereitstellen und verwalten	91
4.1	Betriebssysteme mit SCCM bereitstellen	91
4.1.1	Voraussetzungen für das Bereitstellen von Betriebssystemen	91
4.1.2	Bootimages konfigurieren	93
4.1.3	Treiber in SCCM einbinden	94

4.2	Mit SCCM eigene Installations-Images für Windows 10 erstellen	95
4.2.1	Erstellen einer neuen Tasksequenz für die Erfassung eines Images	95
4.2.2	Quell-PC mit Windows 10 als Image auf dem SCCM-Server speichern	96
4.3	Windows 10 über SCCM bereitstellen	98
4.3.1	Betriebssysteme in SCCM einbinden	99
4.3.2	Zu Windows 10 aktualisieren	102
4.3.3	Betriebssystem mit Startmedium installieren	109
4.3.4	Windows Assessment and Deployment Kit (ADK)	110
4.4	Schneller und sicherer Windows 10 installieren	112
4.4.1	Automatisierte Installation von Windows 10	113
4.4.2	Windows 10 aktivieren	116
4.4.3	ISO-Dateien mit dem Media Creation Tool kostenlos bei Microsoft herunterladen	118
4.4.4	Microsoft-Tools für die Anpassung nutzen	118
4.4.5	ISO-Datei mit WinReducer bearbeiten	119
4.4.6	Eigene Patch-CDs für Windows und Office erstellen	121
4.5	Windows 10-Wartung mit SCCM	123
4.5.1	Windows 10-Rechner optimal verwalten	123
4.5.2	Wartungspläne anpassen	126
5	Updates über SCCM mit WSUS verteilen	129
5.1	WSUS mit SCCM verbinden	129
5.1.1	SCCM an WSUS anbinden	129
5.1.2	Überwachen der Update-Installation	132
5.2	Mit Gruppenrichtlinien die Windows 10-Updates steuern	133
5.2.1	Vorlagen für Gruppenrichtlinien herunterladen	134
5.2.2	Nicht alle Gruppenrichtlinien sind in Windows 10 Pro verfügbar ..	134
5.2.3	Windows 10 Updates mit WSUS bereitstellen	135
5.2.4	Windows 10 an WSUS anbinden	135
5.2.5	Microsoft Store ist nur in den Editionen Enterprise und Education deaktivierbar	136
5.2.6	Updates steuern mit Windows Update for Business	136
5.2.7	Update-Funktionen effizient nutzen	137
5.2.8	Datenschutz verbessern	138
5.2.9	Sicherheitseinstellungen für das Netzwerk steuern	138
5.2.10	Ordnerzugriff überwachen	139
5.2.11	Exploit-Schutz per Gruppenrichtlinie steuern	139
5.2.12	Windows Defender Security Center mit Gruppenrichtlinien steuern	139
5.2.13	Sprach-Assistent Cortana zügeln	140
5.3	Skripte in Gruppenrichtlinien nutzen	142
5.3.1	Anmelde- und Abmeldeskripte für Benutzer und Computer definieren	142

5.3.2	Klassische Anmeldeskripte weiter nutzen	143
5.3.3	Skripte in Gruppenrichtlinien integrieren	144
5.3.4	Skripte kombinieren und parallel ausführen	146
5.3.5	Einstellungen für Skripte in den Gruppenrichtlinien steuern	147
5.3.6	Loopbackverarbeitung von Gruppenrichtlinien berücksichtigen ...	147
5.3.7	Sicherheitseinstellungen für Skripte in der PowerShell beachten ..	148
5.3.8	Fehler mit Group Policy Log beheben	149
5.3.9	Wichtige Informationen immer im Blick: BGInfo auch in Skripten hinterlegen	149
6	Anwendungen mit SCCM bereitstellen	153
6.1	Rollout und die Verwaltung von Office 2016 in Unternehmen	153
6.1.1	Grundlagen zur Installation	153
6.1.2	Office mobil auf dem Tablet und Smartphone nutzen	154
6.1.3	Office Click-to-Run-(C2R-)Setup anpassen	154
6.1.4	Installationsdateien von Office 365/2016 automatisiert herunterladen und Installation durchführen	157
6.2	Office 2016 mit SCCM im Netzwerk verteilen	157
6.2.1	Office Customization Tool in der Praxis	158
6.2.2	Office 2016 mit SCCM im Netzwerk automatisiert verteilen	160
6.3	Von Office 2010/2013 zu Office 2016 wechseln	164
6.3.1	Profileinstellungen und E-Mail-Konten in Outlook 2010/2013/ 2016 sichern	165
6.4	Office 2016 mit Richtlinien steuern	166
6.4.1	Grundlegende Einstellungen für Office 2016	166
6.4.2	Sicherheitseinstellungen für Office 2016 konfigurieren	167
6.4.3	Telemetrie mit Office 2016	168
6.5	Anwendungen bereitstellen	168
6.5.1	Bereitstellung von Anwendungen simulieren	168
6.5.2	Anwendungen bereitstellen	169
6.6	Pakete verteilen	173
6.6.1	Paketverteilung am Beispiel von .NET Framework	174
7	SCCM-Umgebung planen	177
7.1	Grundlagen zum Aufbau einer SCCM-Umgebung	177
7.1.1	Standorte der zentralen Verwaltung	178
7.1.2	Eigenständiger primärer Standort	178
7.1.3	Sekundäre Standorte	179
7.2	SCCM-Standorte installieren	179
7.2.1	Grundlagen zum Standortsystemserver	180
7.2.2	Standortinformationen in Active Directory veröffentlichen	180
7.3	Eine Standorthierarchie entwerfen	181
7.3.1	Eigenständige primäre Standorte verwenden	181
7.3.2	Standort der zentralen Verwaltung definieren	182

7.3.3	Primäre Standorte verwenden	183
7.3.4	Sekundäre Standorte verwenden	183
8	Standorte und Hierarchien konfigurieren	185
8.1	Standortsystemrollen verwalten	185
8.1.1	Standortsystemrollen auf neuen Standortsystemserver installieren	185
8.1.2	Dienstverbindungspunkt in SCCM	187
8.1.3	Erforderliche Berechtigungen für den Internetzugriff	188
8.2	Datenbankreplikate für Verwaltungspunkte	188
8.2.1	Standortdatenbankserver für die Veröffentlichung des Datenbankreplikats vorbereiten	189
8.2.2	Datenbankreplikatserver konfigurieren	189
8.2.3	Verwaltungspunkte für die Verwendung des Datenbankreplikats konfigurieren	191
8.2.4	SQL Server Service Broker konfigurieren	192
8.3	Standortdaten veröffentlichen	193
9	Clients verwalten und inventarisieren	197
9.1	Hardwareinventur in SCCM	197
9.1.1	Einstieg in die Hardwareinventur	198
9.1.2	Hardwareinventar mit dem Ressourcen-Explorer anzeigen	199
9.1.3	Hardwareinventur für Linux	201
9.2	Softwareinventur nutzen	202
9.2.1	Softwareinventur konfigurieren	203
9.2.2	Softwareinventar anzeigen	203
9.3	Lizenzverwaltung mit SCCM (Asset Intelligence)	204
9.4	Remotesteuerung nutzen	208
9.4.1	Remotesteuerung konfigurieren	209
9.4.2	Remoteverwaltung aktiv nutzen	209
10	Endpoint Protection mit SCCM	211
10.1	Endpoint Protection verwalten	211
10.1.1	Endpoint Protection konfigurieren	213
10.2	Windows 10 mit Bordmitteln vor Ransomware schützen	221
10.2.1	Überwachten Ordnerzugriff aktivieren	221
10.2.2	Überwachten Ordnerzugriff konfigurieren	223
10.2.3	Grundlagen zum Ransomware-Schutz	223
10.2.4	Erweiterte Einstellungen für Administratoren und Gruppenrichtlinien festlegen	223
10.2.5	Exploit-Schutz konfigurieren	224
10.2.6	Exploit Guard-Richtlinien in SCCM definieren	224
10.2.7	Vorlagen für Gruppenrichtlinien herunterladen	225
10.2.8	Windows Defender Security Center mit Gruppenrichtlinien steuern	226

11 Weiterführende Informationen	227
11.1 Internetseiten von Microsoft zum Thema SCCM	227
11.2 Schritt-für-Schritt-Anleitungen	228
11.3 Deutsche Internetseiten für SCCM	228
11.4 YouTube-Videos zu SCCM	228
Index	229

5

Updates über SCCM mit WSUS verteilen

Sie können über SCCM, zusammen mit WSUS, auch Updates für Microsoft-Produkte und Betriebssysteme verteilen lassen. In einem Netzwerk, in dem SCCM zum Einsatz kommen soll, ist es durchaus sinnvoll, auf WSUS zu setzen, um Updates effektiv zu verteilen. In diesem Kapitel lernen Sie die Vorgehensweise dazu kennen.

■ 5.1 WSUS mit SCCM verbinden

Die Einstellungen für die Zusammenarbeit von WSUS und SCCM finden Sie in SCCM unter *Softwarebibliothek/Übersicht/Softwareupdates*.

5.1.1 SCCM an WSUS anbinden

Damit Sie die Updates über SCCM mit WSUS verteilen können, benötigen Sie zunächst eine neue Serverrolle im SCCM-Netzwerk:

1. Klicken Sie auf *Verwaltung*.
2. Klicken Sie auf *Standortkonfiguration/Standorte* und markieren Sie Ihren Standort.
3. Öffnen Sie das Kontextmenü des Standorts und wählen Sie *Standortsystemrollen hinzufügen*.

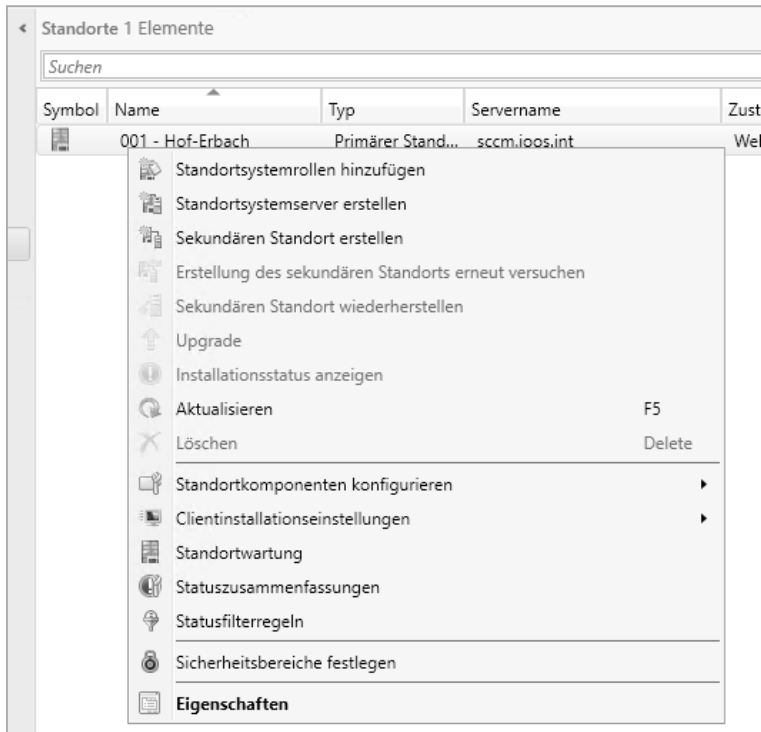


Bild 5.1 Über das Kontextmenü von Standorten führen Sie verschiedene Verwaltungsaufgaben durch, auch das Hinzufügen von zusätzlichen Systemrollen.

4. Arbeiten Sie den Assistenten durch und wählen Sie bei *Systemrollenauswahl* die Option *Softwareupdatepunkt* aus. Diese Rolle ist für die Verteilung von Updates über WSUS verantwortlich.
5. Um die Systemrolle zu konfigurieren, wählen Sie die entsprechenden Optionen aus, also auf welcher Basis Sie WSUS mit SCCM verbinden wollen.
6. Danach legen Sie noch fest, mit welchem Benutzerkonto sich der SCCM-Server mit WSUS verbinden soll.
7. Anschließend konfigurieren Sie, von wo die Updates heruntergeladen werden sollen. Diese Konfiguration steuert den lokalen WSUS-Server auf dem SCCM-Server.
8. Legen Sie noch den Zeitplan fest und wie sich WSUS bei neuen Versionen von Updates verhalten sollen.
9. Bestimmen Sie anschließend noch, welche Klassifizierungen, Produkte und Sprachen Sie über SCCM/WSUS im Netzwerk verteilen wollen.
10. Schließen Sie den Assistenten ab.

Sobald WSUS mit SCCM konfiguriert und verbunden ist, steuern Sie die Updates über *Softwarebibliothek/Übersicht/Softwareupdates*. Hier sehen Sie nach einiger Zeit die Updates, die über SCCM verteilt werden können.

Überprüfen Sie nach der Einrichtung auch die Logdatei *wsyncmgr.log* im Verzeichnis *C:\Programme\Microsoft Configuration Manager\Logs*. Hier sehen Sie, ob sich der Server mit WSUS und Windows-Update synchronisieren kann.

Auch die Datei *wcm.log* spielt bei der Überprüfung eine wichtige Rolle. Über das Kontextmenü von *Alle Softwareupdates* starten Sie eine manuelle Synchronisierung. Über den Bereich *Überwachung* sehen Sie ebenfalls den aktuellen Status der Aufgaben.

Über das Kontextmenü des Standorts können Sie die Systemrolle für den Softwareupdatepunkt anpassen. Diesen Bereich finden Sie über *Verwaltung/Standortkonfiguration/Standorte*.

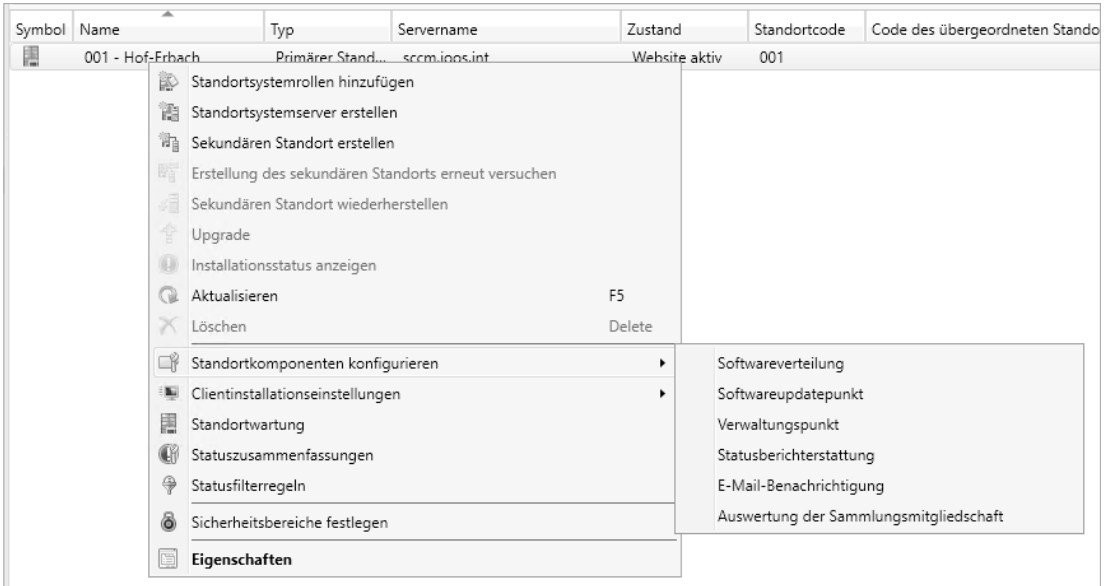


Bild 5.2 Die Einstellungen für den Softwareupdatepunkt können Sie jederzeit anpassen.

Klicken Sie wiederum auf *Softwarebibliothek/Übersicht/Softwareupdates*, erhalten Sie in der Mitte des Fensters aktuelle Warnungen angezeigt und können hier auch recht schnell Fehler finden sowie beheben.

Sobald Updates auf dem Server angezeigt werden, können Sie über Softwareupdategruppen die Updates zusammenfassen, die Sie für verschiedene Computer bereitstellen wollen.

Anschließend lassen sich die Updates über die SCCM-Infrastruktur genauso verteilen und bereitstellen wie andere Anwendungen. Der Vorteil dabei liegt in der Gruppierung der Updates. Diese werden auf den Clientcomputern nicht nur über Windows-Update angezeigt, sondern auch im Softwarecenter aufgelistet.

5.1.2 Überwachen der Update-Installation

Im *Logs*-Verzeichnis der SCCM-Installation werden verschiedene Protokolldateien hinterlegt. Die Datei *wcm.log* zeigt Informationen zur WSUS-Verbindung mit SCCM an. Und in der Datei *wsusctrl.log* finden Sie Informationen zur WSUS-Konfiguration. Auch die Synchronisierung können Sie überwachen. Dazu verwenden Sie die Datei *wsyncmgr.log*.

Einstellungen in der Konfiguration lassen sich nachträglich an verschiedenen Stellen ändern. Beispielsweise passen Sie im Bereich *Verwaltung/Standorte/Server- und Standort-systemrollen* die Eigenschaften des Softwareupdatepunkts an.

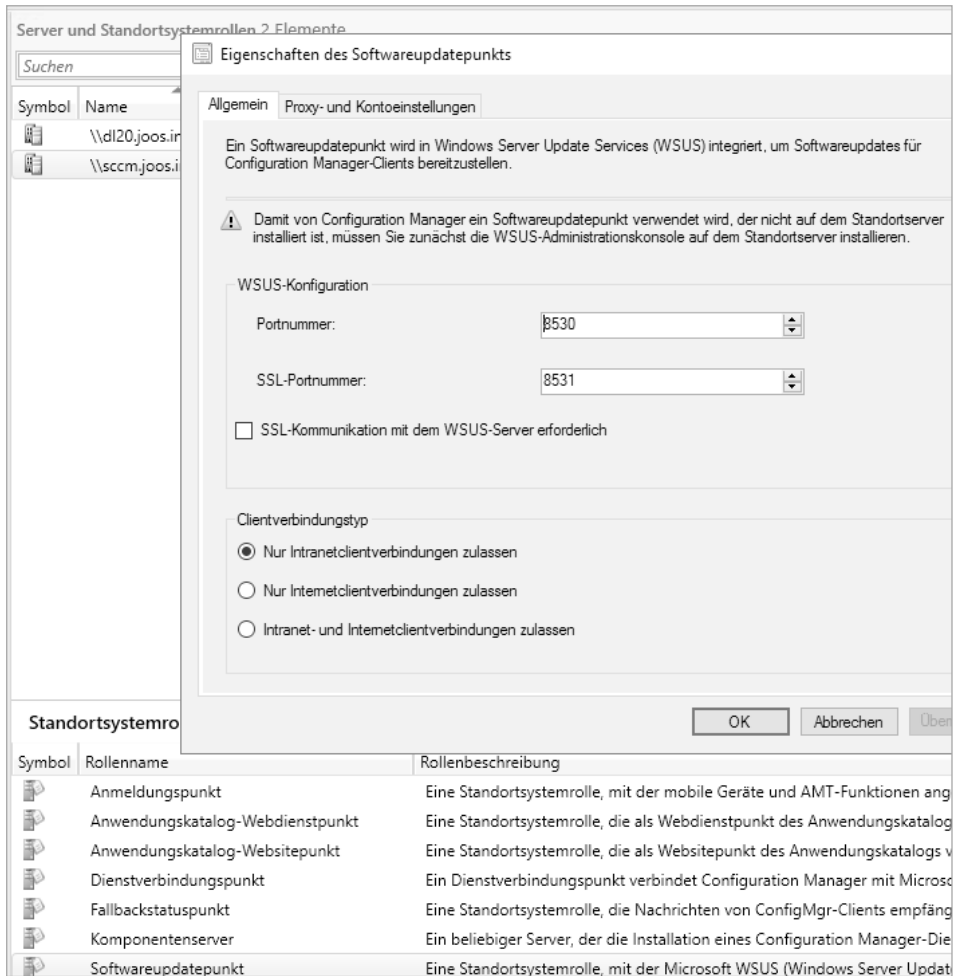


Bild 5.3 Anpassen des Softwareupdatepunkts

Die WSUS-Einstellungen passen Sie wiederum über *Verwaltung/Standorte/<Standort>/Einstellungen/Standortkomponenten konfigurieren/Softwareupdatepunkt* an.

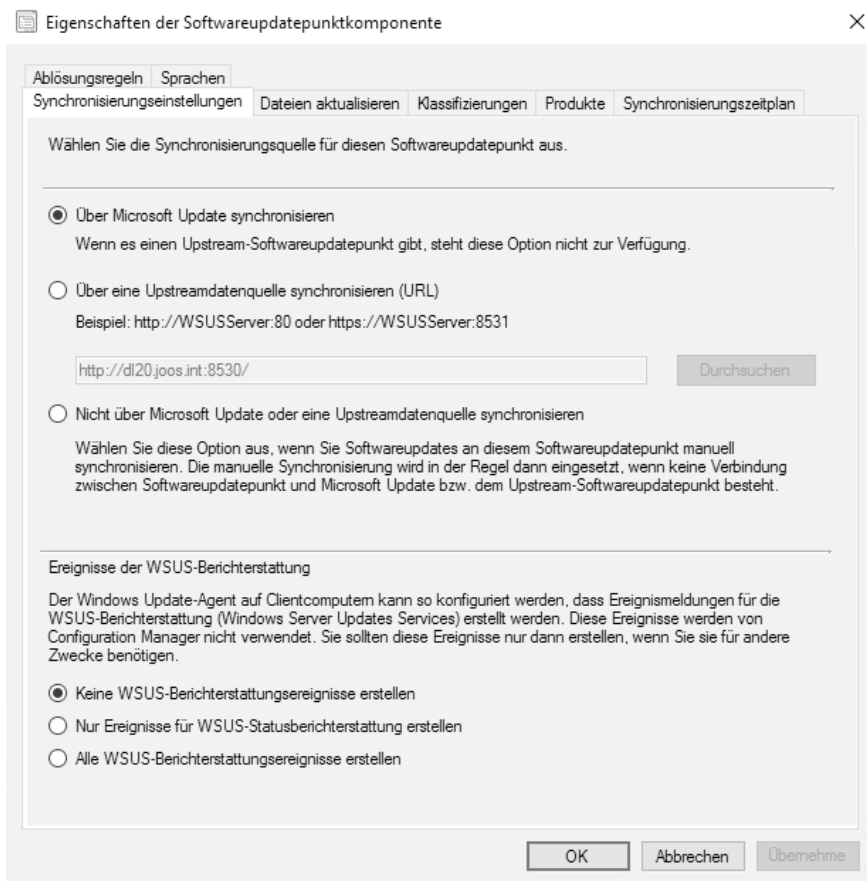


Bild 5.4 Anpassen der WSUS-Einstellungen in SCCM

Die Updates selbst verwalten Sie über *Softwarebibliothek/Softwareupdates*. Über das Kontextmenü von *Alle Softwareupdates* starten Sie eine erneute Synchronisierung. Die Updates für Windows 10 stehen wiederum über *Windows 10-Wartung/Alle Windows 10-Updates* zur Verfügung.

■ 5.2 Mit Gruppenrichtlinien die Windows 10-Updates steuern

WSUS und SCCM unterstützen Administratoren dabei, Updates für Windows 10-Rechner und Server mit Windows Server 2016, Windows Server 1709/1803 und auch Windows Server 2012 R2 im Netzwerk zu verteilen. Damit die Anbindung korrekt funktioniert, müssen die Windows 10-Rechner an WSUS beziehungsweise an SCCM angebunden sein.

Windows 10 lässt sich umfassend mit Gruppenrichtlinien steuern. Vor allem bezüglich der Sicherheit und des Datenschutzes sind einige Einstellungen für die Bereitstellung von Windows 10 interessant. Mit jeder neuen Windows 10-Hauptversion, also den Builds 1511, 1607, 1703, 1709 und den folgenden Versionen, stellt Microsoft mehr Funktionen zur Verfügung, um die Sicherheit im Netzwerk mit Gruppenrichtlinien zu verbessern.

Microsoft bietet mit jedem neuen Build von Windows 10 auch neue Funktionen bezüglich der Sicherheit. Die Funktionen lassen sich auch über Gruppenrichtlinien steuern. Dazu stellt Microsoft Vorlagen zur Verfügung, die sich in Active Directory-Umgebungen integrieren lassen. Microsoft veröffentlicht regelmäßig eine Liste der Gruppenrichtlinieneinstellungen als Excel-Tabelle (<https://tinyurl.com/y838erdq>).

5.2.1 Vorlagen für Gruppenrichtlinien herunterladen

Um die neuesten Sicherheitseinstellungen von Windows über Gruppenrichtlinien zu verteilen, ist nicht unbedingt Windows Server 2016 notwendig. Die Vorlagen, die Microsoft kostenlos zur Verfügung stellt, können auch in Windows Server 2012/2012 R2 eingebunden werden. Laden Sie dazu einfach die Vorlagen für die Gruppenrichtlinien von der Microsoft-Website herunter:

Administrative Templates (.admx) for Windows 10 Fall Creators Update (1709) - Deutsch (<https://tinyurl.com/ydx5jhfu>).

Nach dem Download müssen die *.admx*-Dateien mit den Einstellungen sowie die dazugehörigen Sprachdateien (*.adml*) auf die Domänencontroller kopiert werden. Das Standardverzeichnis dafür ist *C:\PolicyDefinitions*. Im Richtlinien-Editor sind anschließend die neuen Einstellungen verfügbar.

5.2.2 Nicht alle Gruppenrichtlinien sind in Windows 10 Pro verfügbar

Beachten Sie, dass Windows 10 Pro wesentlich weniger Gruppenrichtlinien-Einstellungen unterstützt als Windows 10 Enterprise. Dazu gehört zum Beispiel die Deaktivierung des Microsoft Store oder die Anpassung des Startmenüs. Microsoft hat im TechNet eine Liste veröffentlicht, welche GPO-Einstellungen nur mit Windows 10 Enterprise und Windows 10 Education (entspricht Windows 10 Enterprise) möglich sind (<https://tinyurl.com/yc2zsysa>). Sollen die Arbeitsstationen mit Gruppenrichtlinien angepasst werden, ist der Einsatz von Windows 10 Enterprise empfohlen.

Für Windows 10 Enterprise bietet Microsoft eine spezielle Lizenzierungsvariante an, den sogenannten Long-Term Servicing Branch (LTSB). Bei dieser Variante müssen keine neuen Funktionen und Erweiterungen installiert werden, um Support zu erhalten. Auch ohne Aktualisierung bietet die LTSB-Version zehn Jahre Support. Zwar müssen auch bei dieser Versionsvariante Sicherheits- und Stabilitätspatches installiert werden, nicht jedoch Updates, die Features installieren, oder neue Builds von Windows 10. Unternehmen mit dieser Lizenz erhalten uneingeschränkten Support für den dauerhaften Einsatz.

Einfach ausgedrückt verspricht Microsoft, dass Unternehmen mit LTSB nicht dazu gezwungen werden sollen, neue Versionen zu installieren, um innerhalb des Supportzyklus zu bleiben. Zusammen mit der Steuerung der Einstellungen über Gruppenrichtlinien bietet Windows 10 Enterprise LTSB also eine durchaus interessante Alternative für Unternehmen, die nicht ständig das Betriebssystem aktualisieren wollen.

5.2.3 Windows 10 Updates mit WSUS bereitstellen

Unternehmen, die auf Windows 10 setzen und Updates bzw. Upgrades zentral mit SCCM und WSUS verteilen wollen, müssen sicherstellen, dass das Microsoft-Update für die Entschlüsselung von ESD-Dateien auf dem WSUS-Server installiert ist. Dieses Update bringt allerdings einige Probleme mit sich, die Microsoft in der Knowledgebase behandelt (<https://tinyurl.com/ya6yc7sf>). Die Probleme bestehen vor allem darin, dass sich die WSUS-Konsole nicht mehr mit dem Server verbinden kann, sobald das Update installiert ist. In der Regel hilft es, in der Eingabeaufforderung den folgenden Befehl auszuführen:

```
C:\Program Files\Update Services\Tools\wsusutil.exe/postinstall/servicing
```

Außerdem muss über den Server-Manager das Feature *HTTP Activation* installiert werden. Dieses ist bei den .NET Framework 4.5-Features zu finden. Die genaue Anleitung zur Fehlerbehebung ist im Knowledgebase-Beitrag KB3159706 (<https://tinyurl.com/hluqrqg>) vorhanden. Voraussetzung dabei ist die Anbindung der Windows 10-Rechner an WSUS.

5.2.4 Windows 10 an WSUS anbinden

Wenn im Unternehmen bereits ein Server mit Windows Server Update Services (WSUS) in Betrieb ist, bietet es sich an, die Update-Einstellungen von Windows 10 über Gruppenrichtlinien zu setzen und die Clientrechner an WSUS anzubinden. Die wichtigsten Einstellungen dazu sind über *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Windows Update* zu finden. Die generelle Vorgehensweise entspricht generell den Vorgängerversionen. Bei der grundlegenden Anbindung an WSUS hat Microsoft an dieser Stelle nichts geändert.

Arbeitsstationen lassen sich so konfigurieren, dass diese automatisch Aktualisierungen vom WSUS herunterladen und installieren. Die erste Option ist *Internen Pfad für den Microsoft Updatendienst angeben*. Da WSUS eine Webapplikation ist, muss der Servernamen mit einer HTTP-Adresse angegeben werden: `http://<Servername>:<Port>`. WSUS lässt sich auch mit HTTPS nutzen. Dazu muss der Server entsprechend konfiguriert sein. Die zweite wichtige Option ist das Updateverhalten, das über *Automatische Updates konfigurieren* festgelegt wird. Dabei stehen hauptsächlich folgende Möglichkeiten zur Verfügung:

- *Vor Herunterladen und Installation benachrichtigen*
- *Autom. Herunterladen, aber vor Installation benachrichtigen*
- *Autom. Herunterladen und laut Zeitplan installieren*
- *Lokalem Administrator ermöglichen, Einstellung auszuwählen*

Die Einstellung zur zeitlichen Zurückstellung von Updates ist über *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Windows Update/Windows-Updates zurückstellen* zu finden. Die Einstellungen ermöglichen die verzögerte Installation von Windows-Updates auf Firmenrechnern.

5.2.5 Microsoft Store ist nur in den Editionen Enterprise und Education deaktivierbar

In Windows 10 Pro stehen nicht alle Steuerungsmöglichkeiten über Gruppenrichtlinien zur Verfügung. Nur die Editionen Windows 10 Enterprise und Education bieten die Möglichkeit, den Microsoft Store über Gruppenrichtlinien zu deaktivieren. Dieses Verhalten hat Microsoft offiziell bestätigt (<https://tinyurl.com/ydglnyj6>). Die Einstellungen sind zwar auch in Windows 10 Pro zu finden, funktionieren aber nicht. Die entsprechenden Einstellungen zur Deaktivierung des Stores in Windows 10 Enterprise sind in den Gruppenrichtlinien über die folgenden Wege zu finden:

Computer Configuration/Administrative Templates/Windows Components/Store/Turn off the Store application

User Configuration/Administrative Templates/Windows Components/Store/Turn off the Store

Auf deutschen Rechnern sind die Einstellungen über folgenden Weg zu finden:

Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Store

Unternehmen, die auf Windows 10 Enterprise setzen, können weitere Sicherheitseinstellungen definieren, die in Windows 10 Pro nicht verfügbar sind. Besonders interessant ist in diesem Bereich die Richtlinieneinstellung *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Datensammlung und Vorabversionen*. Diese Einstellungen können Sie nutzen, um den Datenschutz zu verbessern, da Windows 10 nach der Aktivierung weniger Daten ins Internet sendet.

5.2.6 Updates steuern mit Windows Update for Business

Auch die Verteilmöglichkeiten von Updates können Sie über Richtlinien steuern. Die Konfiguration ist über *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Übermittlungsoptionen* zu finden. Hier können Sie zum Beispiel festlegen, wie Windows 10 Updates heruntergeladen und anderen Arbeitsstationen mit Windows 10 zur Verfügung stellen soll.

Über *Computereinstellungen/Administrative Vorlagen/Windows-Komponenten/Übermittlungsoptimierung/Downloadmodus* lässt sich festlegen, ob und wie der Verteilungsmodus für Windows-Updates verwendet werden soll.

Durch Aktivieren der Option *Umgehen* wird der Standardmodus in Windows 10 übergangen und weiterhin die BITS-Technologie verwendet. Dadurch lässt sich einiges an Bandbreite im Netzwerk einsparen.

Windows-Updates können in Windows 10 eine Internetverbindung komplett lahmlegen. Durch Aktivieren der Option *Umgehen* bei *Downloadmodus* lässt sich das Problem beheben. Soll die neue Technologie aber verwendet werden, sollten Sie die Werte bei *Maximale Downloadbandbreite*, *Max. Uploadbandbreite* und *Minimaler Hintergrund-QoS-Wert* überprüfen und anpassen.

Besonders wichtig ist auch das Zurückstellen von Updates, die erst später oder überhaupt nicht installiert werden sollen. Die Einstellungen finden Sie über *Computereinstellungen/Administrative Vorlagen/Windows-Komponenten/Windows Update/Windows Update für Unternehmen*

In *Computereinstellungen/Administrative Vorlagen/Windows-Komponenten/Windows Update* ist auch die Einstellung *Automatischen Neustart nach Updates während der Nutzungszeit deaktivieren* zu finden. Hier können Sie einen Zeitrahmen definieren, zum Beispiel die Arbeitszeit im Unternehmen, während der die Rechner mit Windows 10 nach der Installation von Updates nicht neu gestartet werden.

Die Einstellung *Computereinstellungen/Administrative Vorlagen/Windows-Komponenten/Windows Update* und die Auswahl von *Keine Treiber in Windows-Updates einschließen* legen fest, dass Windows 10 und Windows Server 2016 keine Treiber über Windows-Updates installieren.

5.2.7 Update-Funktionen effizient nutzen

Windows 10 arbeitet für die Verteilung von Updates mit sogenannten Ringen. Dabei können Administratoren festlegen, auf welchen Rechnern welche Updates installiert werden sollen. Standardmäßig bietet Windows 10 in seinen Einstellungen die Möglichkeit, Anpassungen bezüglich von Windows-Updates vorzunehmen und Updates bis zu 35 Tage nach hinten zu verschieben. Darüber hinaus kann an dieser Stelle festgelegt werden, ob ein Rechner Updates sofort erhalten soll (*Current Branch*) oder erst nach einiger Zeit (*Current Branch for Business*), wenn diese auf Rechnern mit der Einstellung *Current Branch* getestet werden.

Neben den Einstellungsmöglichkeiten in der Einstellungen-App von Windows 10 stehen aber auch Einstellungsmöglichkeiten in den Gruppenrichtlinien zur Verfügung. Diese sind im Gruppenrichtlinieneditor unter *Computerkonfiguration/Richtlinie/Administrative Vorlagen/Windows-Komponenten/Windows-Update* zu finden. Die Einstellungen funktionieren, wie alle Gruppenrichtlinien, nur auf Rechnern mit Windows 10 Professional, Enterprise oder Education.

Mit Bereitstellungsringen (*Deployment Rings*) können Administratoren zentral festlegen, in welchen einzelnen Wellen Updates an verschiedene Rechner verteilt werden sollen. Microsoft bietet standardmäßig bereits die Ringe *Current Branch* und *Current Branch for Business* an. Ein dritter Bereitstellungsring wäre die Bereitstellung von Insider-Previews. Administratoren können aber mit weiteren Ringen arbeiten, zum Beispiel für einzelne Abteilungen im Unternehmen.

Grundsätzlich unterscheidet Windows 10 zwischen drei verschiedenen Updatetypen:

- *Feature Updates* – Diese Updates enthalten, neben Updates für mehr Sicherheit und Qualität, auch neue Funktionen. Beispiele dafür sind das *Anniversary Update* oder das *Crea-*

tors Update. Diese Updates lassen sich bis zu 365 Tage aufschieben, danach muss die Installation erfolgen.

- *Quality Updates* – Hierbei handelt es sich um herkömmliche Updates, Fehlerbehebungen und Sicherheitspatches, die keine neuen Funktionen beinhalten. Auch Updates für Microsoft Office lassen sich so bereitstellen. Quality Updates lassen sich 30 bis 35 Tage aufschieben.
- *Nicht-aufschiebbare Updates* – Dabei handelt es sich zum Beispiel um Updates für Windows Defender.

Die Einstellungen zum Aufschieben lassen sich sowohl in den Windows-Einstellungen als auch zentral über Gruppenrichtlinien vornehmen. Diese finden Sie in den Gruppenrichtlinieneinstellungen bei *Computerkonfiguration/Richtlinie/Administrative Vorlagen/Windows-Komponenten/Windows-Update*.

5.2.8 Datenschutz verbessern

Die Einstellung *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Position und Sensoren/Windows-Positionssuche* kann den Datenschutz verbessern, wenn Anwender Notebooks mit Windows 10 nutzen. Allerdings gilt auch hier, dass die Verbesserungen nicht alle Spionagefunktionen deaktivieren. In jedem Fall ist es aber sinnvoll, sich die Einstellungen genauer anzusehen und so viele wie möglich zu deaktivieren.

In Windows 10 lassen sich Datenübertragungen der integrierten Windows-Spiele steuern. Dazu steht die Einstellung *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Spiel-Explorer* zur Verfügung.

5.2.9 Sicherheitseinstellungen für das Netzwerk steuern

In manchen Situationen kann es passieren, dass Windows 10 den aktuellen Netzwerktyp nicht erkennt und so einen falschen Netzwerktyp (Öffentlich, Privat oder Arbeitsplatz) verwendet. Dies äußert sich in Problemen beim Netzwerkzugriff vor allem bei Notebooks oder Heimarbeitsplätzen. Sie haben in Windows 10 Pro und Enterprise die Möglichkeit, über Gruppenrichtlinien nicht identifizierte Netzwerke manuell zuzuordnen:

1. Navigieren Sie zu *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Netzwerklisten-Manager-Richtlinien*.
2. Öffnen Sie die Einstellung *Nicht identifizierte Netzwerke*.
3. Legen Sie hier die Einstellung fest, die Sie im Netzwerk standardmäßig nutzen wollen.

In Windows 10 Build 1709 kann das Profil in den Einstellungen der entsprechenden Netzwerkverbindung konfiguriert werden. Auch WLAN-Einstellungen bieten jetzt über das Kontextmenü mehr und einfachere Möglichkeiten.

Standardmäßig erreichen Universal-Apps das Internet nur direkt. Wenn Sie einen Proxyserver einsetzen, sollten Sie im System Änderungen vornehmen, damit die Apps eine Verbindung mit dem Internet herstellen können. Da in solchen Umgebungen normalerweise

Windows 10 Pro oder Enterprise im Einsatz sind, können Sie die Einstellungen über Gruppenrichtlinien setzen. Navigieren Sie zu *Computerkonfiguration/Administrative Vorlagen/Netzwerk/Netzwerkisolation* . Auf der rechten Seite finden Sie die Einstellungen, um die Apps über einen Proxy mit dem Internet zu verbinden. Aktivieren Sie die Einstellung für den Proxy und geben Sie den URL und den Port ein, auf den der Proxy auf Anfragen wartet.

5.2.10 Ordnerzugriff überwachen

In Windows 10 Build 1709 lassen sich Verzeichnisse vor Ransomware schützen. Wird der überwachte Ordnerzugriff aktiviert, dürfen nur noch genehmigte Apps Änderungen an den hinterlegten Ordnern vornehmen. Die Einstellungen lassen sich lokal in den Einstellungen von Windows 10 über das neue Windows Defender Security Center, in der PowerShell, oder über Gruppenrichtlinien definieren. Dazu müssen die neuen *.admx*-Dateien importiert werden. Alternativ stehen die Einstellungen auch über lokale Richtlinien zur Verfügung, die mit dem Befehl *gpedit.msc* gestartet werden.

Die neuen Optionen für den überwachten Ordnerzugriff stehen bei *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Windows Defender Antivirus/Windows Defender Exploit Guard/Überwacher Ordnerzugriff* zur Verfügung. Hier kann konfiguriert werden, welche Ordner geschützt werden sollen, welche Anwendungen Änderungen vornehmen dürfen und ob der überwachte Ordnermodus nur überwachen soll. Zusätzlich lassen sich Änderungen auch komplett blockieren.

Generell stehen bei *Windows Defender Exploit Guard* weitere Einstellungen zur Verfügung, die Windows 10-Rechner besser vor Angreifern schützen.

5.2.11 Exploit-Schutz per Gruppenrichtlinie steuern

Windows 10 Build 1709 bietet einen Exploit-Schutz, der Windows 10 vor unbekanntem Angreifern schützen soll. Auch hier finden Sie die neuen Einstellungen in der Einstellen-App über das Windows Defender Security Center. Über Gruppenrichtlinien kann diese Einstellung bei *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Windows Defender Exploit Guard/Exploit-Schutz* gefunden werden. Die Konfiguration kann anhand einer *.xml*-Datei erfolgen. Diese wird im Netzwerk gespeichert und durch die Richtlinie auf den Rechnern verteilt.

5.2.12 Windows Defender Security Center mit Gruppenrichtlinien steuern

Das Windows Defender Security Center ist ab Windows 10 Build 1709 der zentrale Bereich, wenn es um die Konfiguration und Überwachung der Sicherheit von Windows 10 geht. In den Richtlinien können umfassende Einstellungen zum Windows Defender Security Center vorgenommen werden. Die Einstellungen sind über *Computerkonfiguration/Richtlinien/*

Administrative Vorlagen/Windows-Komponenten/Windows Defender Security Center erreichbar.

Hier sind alle Bereiche des Windows Defender Security Centers aufgeführt und konfigurierbar. Zusätzlich lassen sich aus dem Windows Defender Security Anzeigen ausblenden. Dadurch werden normale Anwender nicht mit Informationen verunsichert, die für sie nicht relevant sind.

Mit Windows Defender SmartScreen lassen sich verschiedene Bereiche in Windows 10 schützen. Dazu gehören Apps, die Anwender installieren oder aus dem Store herunterladen, aber auch Webseiten und Downloads, die mit Microsoft Edge genutzt werden. Windows Defender SmartScreen kann über das Windows Defender Security Center oder mit Gruppenrichtlinien gesteuert werden. Die Einstellungen sind über *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Windows Defender SmartScreen* zu finden. Hier lässt sich der Schutz von Windows, aber auch von Microsoft Edge steuern.

5.2.13 Sprach-Assistent Cortana zügeln

Cortana soll die allumfassende sprachgestützte Assistentin für Windows 10 sein. In Unternehmen ist die Funktion aber nicht immer erwünscht. Aus diesem Grund gibt es in den Richtlinien verschiedene Einstellungsmöglichkeiten, mit denen sich Cortana etwas zügeln lässt, ohne die Suchfunktion von Windows 10 zu beeinträchtigen. Einige der Funktionen, zum Beispiel die Steuerung von Cortana auf dem Sperrbildschirm, sind erst ab Build 1607 möglich.

Über Gruppenrichtlinieneinstellungen lässt sich Cortana generell recht gut steuern. Dazu nutzen Sie die Einstellung *Nicht im Web suchen und keine Webergebnisse in der Suche anzeigen* bei *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Suche*. Durch die Aktivierung dieser Option wird verhindert, dass Anwender über Cortana im Internet nach Informationen suchen. Bei solchen Suchvorgängen werden auch Informationen des lokalen Rechners in das Internet gesendet und in der Cloud gespeichert. Das ist nicht immer im Interesse des Unternehmens.



Bild 5.5 Cortana können Sie entweder in den Windows-Einstellungen oder über Richtlinien steuern.

Mit der Richtlinieneinstellung *Cortana zulassen* können Sie mit der Option *Deaktivieren* Cortana per Richtlinie komplett abschalten. Die herkömmliche Standardsuche in Windows funktioniert danach problemlos weiterhin.

Mit der Einstellung *Cortana auf dem Sperrbildschirm zulassen* wird festgelegt, ob die neue Cortana-Funktion aus dem Anniversary Update auf Windows 10-Rechnern erlaubt sein soll. Diese bietet die Möglichkeit, Cortana auch dann zu nutzen, wenn der Rechner gesperrt ist. Auf Unternehmensrechnern sollten Sie diese Funktion in jedem Fall deaktivieren.

Manche Unternehmen wollen den Sperrbildschirm von Windows 10 nicht nutzen. Sie können diesen komplett deaktivieren. Wechseln Sie zu *Computerkonfiguration/Administrative Vorlagen/Systemsteuerung/Anpassung*. Auf der rechten Seite können Sie verschiedene Einstellungen vornehmen und auch den Sperrbildschirm deaktivieren. Zusätzlich können Sie zum Beispiel ein bestimmtes Hintergrundbild für den Anmeldebildschirm festlegen und verhindern, dass Anwender die Startseite und den Anmeldebildschirm anpassen.

Für Unternehmensrechner lassen sich Benachrichtigungen der Apps in den Gruppenrichtlinien festlegen. Dies gilt auch für Windows-Funktionen wie Cortana. Sie finden die entsprechenden Einstellungen in der Gruppenrichtlinienverwaltung im Bereich *Benutzerkonfiguration/Administrative Vorlagen/Startmenü und Taskleiste/Benachrichtigungen*. Hier lassen sich verschiedene Einstellungen vornehmen sowie verhindern, dass Anwender Einstellungen auf dem PC selbst anpassen.

■ 5.3 Skripte in Gruppenrichtlinien nutzen

Skripte zur Automatisierung von Windows-Aufgaben oder für die An- und Abmeldung von Benutzern sowie das Starten und Herunterfahren von Computern lassen sich in Gruppenrichtlinien integrieren. Zusammen mit SCCM können Sie dadurch effektiv automatische Konfigurationen umsetzen. Es ist daher sinnvoll, parallel zu den Möglichkeiten in SCCM auch mit den Funktionen in Active Directory zu arbeiten, vor allem bezüglich der Gruppenrichtlinie und Skripte.

Dadurch wird sichergestellt, dass die gewünschten Aufgaben regelmäßig und automatisch durchgeführt werden, und zwar zusammen mit den Möglichkeiten in SCCM. Microsoft bietet dazu in den Gruppenrichtlinien diverse Einstellungsmöglichkeiten und Tools an. Um Skripte in der PowerShell zu nutzen, sind keine umfassenden Entwicklerkenntnisse notwendig. PowerShell-Skripte oder normale Batchdateien lassen sich problemlos, schnell und einfach integrieren.

5.3.1 Anmelde- und Abmeldeskripte für Benutzer und Computer definieren

Sie können Benutzern in Active Directory Anmeldeskripte zuweisen, die ein Computer ausführt, sobald sich der Benutzer anmeldet. In vielen Fällen werden dazu die Einstellungen des Benutzerkontos in Active Directory genutzt. Allerdings lassen sich die Skripte ohne größere Änderungen schnell und einfach in Gruppenrichtlinien integrieren. Dies bietet sogar einige Vorteile. Sie können zum Beispiel ein umfangreiches und komplexes Anmeldeskript in verschiedene kleine Skripte aufteilen und schnell und einfach ausführen lassen. Über Gruppenrichtlinien lassen sich Skripte integrieren, die beim Starten, Herunterfahren, bei der Abmeldung und zusätzlich noch bei der Anmeldung ablaufen.

Es gibt generell fünf Möglichkeiten für Skripte, die Administratoren Anwendern oder Computern in Active Directory zuweisen können. Es ist auch möglich, mehrere Arten von Skripten zu mischen und an den verschiedenen Stellen auch mehrere Skripte gleichzeitig zu hinterlegen. Windows-Computer führen alle aus, und zwar in der vom Administrator festgelegten Reihenfolge. Um automatisch Befehle beim Anmelden von Benutzern ausführen zu lassen (oder auch wenn PCs starten), gibt es folgende Möglichkeiten:

- Das klassische Anmeldeskript, das in den Eigenschaften des Profils eingetragen ist. Die Ausführung sieht der Anwender teilweise in einem Fenster der Eingabeaufforderung.

Dieses Skript hat mit den Gruppenrichtlinien nichts zu tun, kann aber parallel eingesetzt werden. Solche Anmeldeskripte sollten Sie aber besser in die Gruppenrichtlinien integrieren.

- Anmeldeskripte in den Gruppenrichtlinien für Benutzer. Diese Skripte starten dann, wenn sich ein Benutzer anmeldet. Normalerweise sieht der Benutzer die Ausführung des Skripts nicht, da das Fenster von Windows versteckt wird.
- Abmeldeskripte in den Gruppenrichtlinien für Benutzer. Dieses Skript wird ausgeführt, wenn sich ein Benutzer abmeldet.
- Skripte in den Gruppenrichtlinien beim Hochfahren eines Computers, unabhängig vom Benutzer. Diese Skripte führt der Computer im Hintergrund aus, bevor sich ein Benutzer am Rechner anmeldet.
- Skripte in den Gruppenrichtlinien beim Herunterfahren eines Computers, unabhängig vom Benutzer. Diese Skripte werden gestartet, wenn nach der Abmeldung des Benutzers der Rechner heruntergefahren oder neu gestartet wird.

5.3.2 Klassische Anmeldeskripte weiter nutzen

Die klassischen Anmeldeskripte, die Programme und Befehle in einer Batchdatei ausführen, hinterlegen Sie auf der Registerkarte *Profil* in den Eigenschaften der Benutzer. An dieser Stelle haben Sie auch die Möglichkeit, das lokale Benutzerprofil des Anwenders auf eine Freigabe zu speichern. Damit die Skripte beim Anmelden von Benutzern auch starten, müssen Sie die Dateien und die Programme, welche die Skripte starten sollen, in der NETLOGON-Freigabe auf den Domänencontrollern speichern. Das ist beim Integrieren der Skripte in den Gruppenrichtlinien nicht notwendig, da beim Integrieren eine Kopie der Skriptdatei in den Gruppenrichtlinien erstellt und mit den Gruppenrichtlinien repliziert wird.



Bild 5.6 Anmeldeskripte unterstützen die Automatisierung mit SCCM.

Wenn Sie ein Skript in die NETLOGON-Freigabe eines Domänencontrollers kopieren, wird es durch den Dateireplikationsdienst (File Replication Service, FRS) automatisch auf die anderen Domänencontroller repliziert. Der Vorgang ist aber komplett unabhängig von Gruppenrichtlinien und erhöht die Wahrscheinlichkeit von Fehlern. Überprüfen Sie den Vorgang oder kopieren Sie das Skript manuell, wenn die Replikation nicht automatisiert stattfindet. Der lokale Speicherort der NETLOGON-Freigabe ist der Ordner `\Windows\SYSVOL\sysvol\<Domänennamen>\scripts`.

Die Skripte können entweder einfache Batchdateien, spezielle Varianten mit KiXtart (<http://www.kixtart.org>) oder AutoIT (<http://www.autoitscript.com/site>), aber auch andere Skriptdateien sein. Windows muss die Skripte nur ausführen können und über die entsprechende Erweiterung verfügen. Solche Skripte, auch AutoIT- und KiXtart-Skripte, lassen sich problemlos in Gruppenrichtlinien überführen.

Klassische Anmeldeskripte laufen sichtbar ab, wenn sich ein Anwender bei seinem Computer anmeldet. Die Anwender sehen also den Ablauf, die Befehle, eventuell hinterlegte Kennwörter und mehr. Außerdem können Anwender das Fenster beenden und damit das Skript stoppen. Das ist ein Nachteil im Vergleich zur Integration in Gruppenrichtlinien. Mit klassischen Anmeldeskripten ist es auch nicht möglich, Skripte zu schreiben, die ein Computer bereits beim Starten abarbeitet.

5.3.3 Skripte in Gruppenrichtlinien integrieren

In Active Directory können Sie neben oder anstatt der klassischen Skripte auch Skripte beim Anmelden und Abmelden sowie beim Starten und Herunterfahren eines Computers über Richtlinien festlegen. Alle Varianten lassen sich außerdem parallel einsetzen. Vorteil dabei ist, dass sich solche Skripte auch Organisationseinheiten oder ganzen Domänen zuordnen lassen. Da Sie für verschiedene Container in Active Directory auch unterschiedliche Gruppenrichtlinien zuordnen können, haben Sie auch die Möglichkeit, den Containern eigene Skript zuzuordnen. In diesem Fall sind keine komplexen Abfragen in den Skripten notwendig und die Skripte werden deutlich verkleinert. Die Skripte werden in den Gruppenrichtlinien an folgender Stelle hinterlegt:

- Skripte für Computer zum Starten und Herunterfahren werden über *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Skripts* gesteuert.
- Skripte für Anwender beim An- oder Abmelden werden über *Benutzerkonfiguration/Richtlinien/Windows-Einstellungen/Skripts* gesteuert.

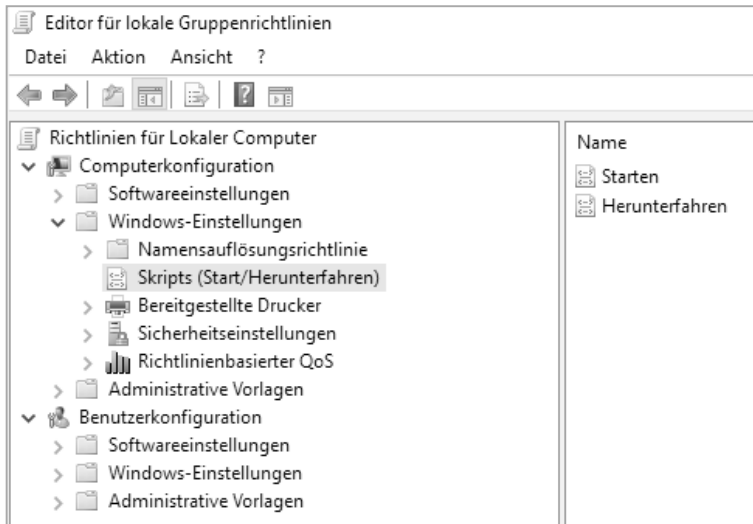


Bild 5.7 Mit Skripten kann die Automatisierung zusammen mit SCCM über Gruppenrichtlinien durchgeführt werden.

Die Abarbeitung von Skripten in den Gruppenrichtlinien hat den Vorteil, flexibler zu sein. Es besteht auch die Möglichkeit, herkömmliche Anmeldeskripte nicht über die Eigenschaften der Benutzerprofile ausführen zu lassen, sondern über Gruppenrichtlinien. Die Skripte in den Gruppenrichtlinien laufen nicht sichtbar im Hintergrund ab. Benutzer bekommen von den Skripten nichts mit, auch wenn herkömmliche *.bat*- oder *.cmd*-Dateien im Einsatz sind. Um Skripte in den Gruppenrichtlinien zu verwenden, gehen Sie folgendermaßen vor:

1. Legen Sie die entsprechende Gruppenrichtlinie an und verknüpfen Sie diese mit der Domäne oder den gewünschten Organisationseinheiten (OUs). Die Vorgehensweise entspricht dem Umgang von herkömmlichen Gruppenrichtlinien.
2. Öffnen Sie die Bearbeitung der Gruppenrichtlinie und navigieren Sie zu dem Bereich, für den Sie das Skript hinterlegen wollen, also *Computerkonfiguration* oder *Benutzerkonfiguration*. In einer Gruppenrichtlinie lassen sich Skripte gleichzeitig für Benutzer und für Computer hinterlegen.
3. Klicken Sie doppelt auf den jeweiligen Eintrag des Skripts, also *Anmelden*, *Abmelden*, *Starten* oder *Herunterfahren*. Neben herkömmlichen Skripten lassen sich an dieser Stelle auch PowerShell-Skripte anbinden. Außerdem können Sie PowerShell-Skripte mit Batchdateien und auch mit anderen Varianten wie *.exe*-Dateien vermischen.
4. Klicken Sie auf die Schaltfläche *Dateien anzeigen*. Es öffnet sich ein Explorer-Fenster, in dem das Verzeichnis der Gruppenrichtlinie geöffnet wird. In dieses Verzeichnis müssen die Skriptdateien gespeichert sein, die in den Gruppenrichtlinien ausgeführt werden sollen. Ein Beispiel dafür ist:

```
\\contoso.int\sysvol\contoso.int\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\
Machine\Scripts\Startup
```

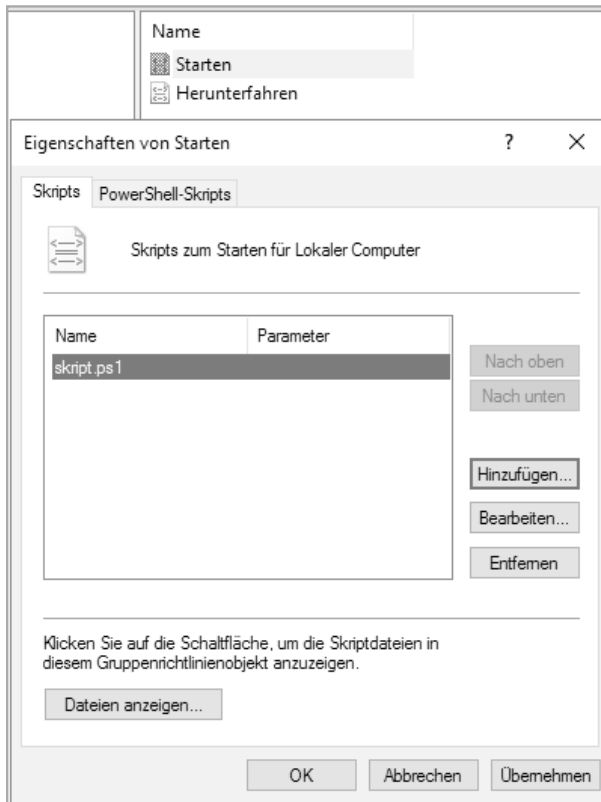



Bild 5.8 Hinzufügen von Skripten zu Gruppenrichtlinien

5. Kopieren Sie anschließend Ihre Skriptdatei in diesen geöffneten Ordner.
6. Klicken Sie danach auf die Schaltfläche *Hinzufügen* und wählen Sie das Skript aus. Das Skript wird nun im Fenster angezeigt. Sie können auch mehrere Skripte hintereinander ausführen lassen oder spezielle Parameter festlegen, die zusammen mit dem Skript ausgeführt werden sollen.

5.3.4 Skripte kombinieren und parallel ausführen

Auch die Kombination von klassischen Skripten und Skripten über Gruppenrichtlinien ist möglich. Und Sie können unterschiedliche Skripte in verschiedenen Gruppenrichtlinien auch für Computer und Benutzer kombinieren.

Das heißt, manche Skripte können in den Eigenschaften der Benutzerkonten gespeichert sein und ablaufen, andere in den Gruppenrichtlinien an verschiedenen Stellen. Es ist auch kein Problem, wenn die Skripte in den Gruppenrichtlinien von übergeordneten OUs nach unten vererbt werden und in den untergeordneten OUs weitere Skripte starten.

Sie können alle möglichen Formen miteinander kombinieren. Wenn Unternehmen mit klassischen und Gruppenrichtlinienskripten arbeiten, laufen beide parallel ab. Diesen Sachver-

halt sollten Administratoren in den Skripten beachten, wenn zum Beispiel Abhängigkeiten existieren. Skripte in den Gruppenrichtlinien werden in der Regel vor den klassischen Anmeldeskripten ausgeführt.

5.3.5 Einstellungen für Skripte in den Gruppenrichtlinien steuern

Außer speziellen Skripten lassen sich in den Gruppenrichtlinien auch diverse Einstellungen hinterlegen, die den Ablauf der Skripte steuern und entsprechend regeln. Die Einstellungen sind ebenfalls in den Gruppenrichtlinien zu finden. Die entsprechenden Erläuterungen und Hilfen finden Sie direkt in der Hilfe der jeweiligen Einstellung. Folgende Richtlinieneinstellungen spielen dabei eine Rolle:

- *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Skripts*
- *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Anmeldung*
- *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Gruppenrichtlinien*
- *Benutzerkonfiguration/Richtlinien/Administrative Vorlagen/Skripts*
- *Benutzerkonfiguration/Richtlinien/Administrative Vorlagen/Anmeldung*

5.3.6 Loopbackverarbeitung von Gruppenrichtlinien berücksichtigen

Setzen Sie Remotedesktop-Sitzungshosts zusammen mit Gruppenrichtlinien ein, bietet es sich an, die Server in einer eigenen Organisationseinheit (Organizational Unit, OU) abzulagern und für diese OUs dann Gruppenrichtlinien mit den gewünschten Einstellungen zu aktivieren. Ein solches Szenario ist nicht nur für Remotedesktopdienste sinnvoll, sondern durchaus auch beim Einsatz mehrerer Rechner.

Für Richtlinien in den Remotedesktopdiensten (oder beim Einsatz mehrerer Rechner) können Sie den Loopbackverarbeitungsmodus in den Gruppenrichtlinien aktivieren. Bei diesem Modus wendet die Gruppenrichtlinie auch Einstellungen des Benutzerbaums an, wenn das Konto der Anwender nicht in der OU gespeichert ist, in der die Richtlinie definiert ist, sondern nur der entsprechende Server oder das Computerkonto. So erhalten Sie die Möglichkeit, Benutzereinstellungen für Remotedesktopserver festzulegen, die nur bei der Anmeldung der Anwender auf den Remotedesktopservern angewendet werden, nicht bei der Anmeldung an ihren lokalen Computern.

Sie finden diese Einstellung über *Computer/Richtlinien/Administrative Vorlagen/System/Gruppenrichtlinie*. Aktivieren Sie die Richtlinie *Loopbackverarbeitungsmodus für Benutzergruppenrichtlinie*. Aktivieren Sie die Richtlinie, können Sie zwischen zwei Modi auswählen:

- *Ersetzen* - Aktivieren Sie diesen Modus, ersetzt die Richtlinie Einstellungen, die bereits von anderen Richtlinien an gleicher Stelle gesetzt sind.
- *Zusammenführen* - Bei dieser Einstellung werden die normalen Richtlinien des Anwenders angewendet und die Einstellungen für den Benutzer in der Remotedesktopserver-Richtlinie. Gibt es Konflikte, gewinnt die Richtlinie der Remotedesktopserver.

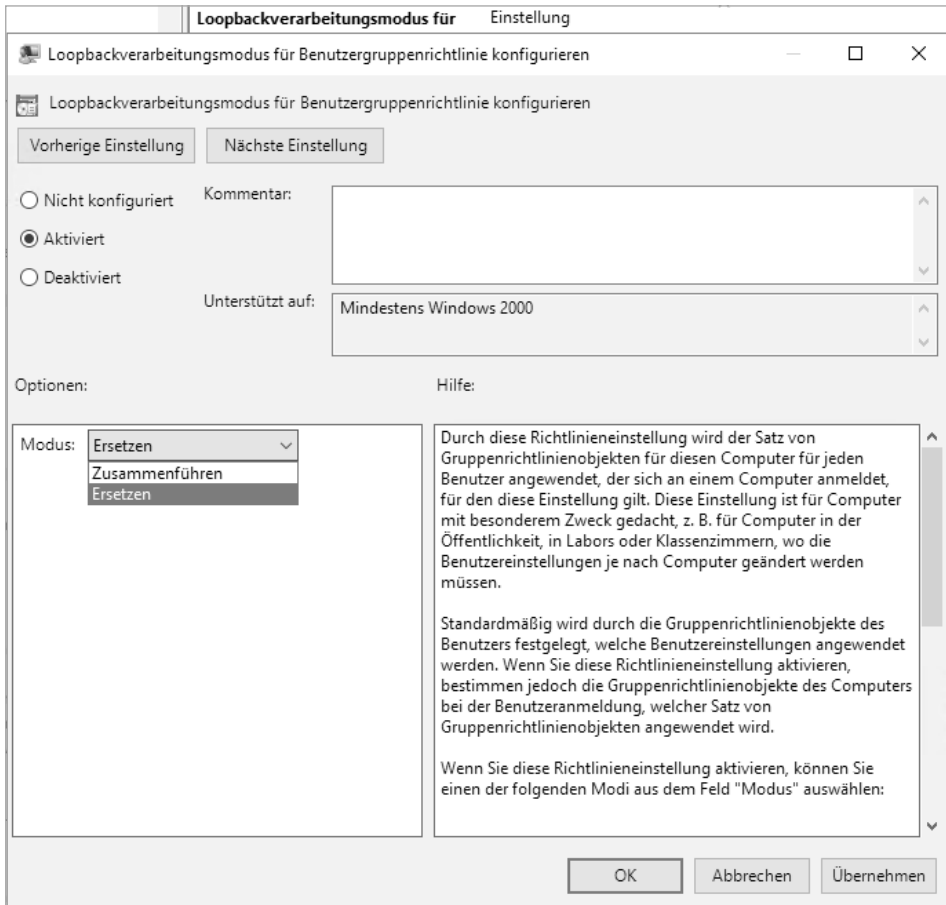


Bild 5.9 Aktivieren des Loopbackverarbeitungsmodus für Gruppenrichtlinien

5.3.7 Sicherheitseinstellungen für Skripte in der PowerShell beachten

Zum Schutz enthält die PowerShell verschiedene Sicherheitsfeatures, zu denen auch die Ausführungsrichtlinie für Skripte zählt. Die Ausführungsrichtlinie legt fest, ob Skripte ausgeführt werden dürfen, ob diese digital signiert sein müssen oder ob Skripte generell erlaubt sind. Dies gilt auch bei der Ausführung in Gruppenrichtlinien. Standardmäßig erlaubt die PowerShell nur signierte Skripte. Wollen Sie eigene Skripte schreiben, müssen Sie diese digital signieren oder für die Ausführung die Richtlinie anpassen. Für erste Schritte mit Skripten ist das der beste Weg.

Sie können die Ausführungsrichtlinie mit dem PowerShell-Cmdlet *Set-ExecutionPolicy* ändern und mit *Get-ExecutionPolicy* anzeigen. Dabei sind folgende Einstellungen möglich:

- *Restricted* – Keine Skripte erlaubt. Diese Option ist sicher, aber Sie können nicht mit Skripten arbeiten.

- *AllSigned* – Nur signierte Skripte sind erlaubt.
- *RemoteSigned* – Bei dieser Einstellung müssen Sie Skripte durch eine Zertifizierungsstelle signieren lassen.
- *Unrestricted* – Bei dieser Einstellung funktionieren alle Skripte. Die Einstellung ist optimal für eigene Tests mit Anmeldeskripten.

5.3.8 Fehler mit Group Policy Log beheben

Wenn Gruppenrichtlinien auf einzelnen Rechnern nicht korrekt angewendet werden, können Sie das kostenlose Microsoft Tool Group Policy Log View (<https://tinyurl.com/a5kvesh>) verwenden, um die Fehler genauer einzugrenzen. Das gilt vor allem dann, wenn Skripte nicht korrekt ausgeführt werden. Sie können das Tool auch mit Gruppenrichtlinien kombinieren.

Installieren Sie das Tool auf einem Rechner, den Sie analysieren wollen. Nachdem das Tool installiert ist, öffnen Sie eine Eingabeaufforderung mit Administratorrechten. Wechseln Sie in das Verzeichnis, in das Sie das Tool installiert haben. Geben Sie zur Überwachung der Gruppenrichtlinien den Befehl `Gplogview -o gpevents.txt` ein.

Das Tool analysiert alle Einträge der Gruppenrichtlinien und zeigt im Verzeichnis eine Textdatei an, in der die Fehler zu den Gruppenrichtlinien gesammelt werden. Sie können Group Policy Log auch in einem Anmeldeskript hinterlegen. Dadurch wird es auf jedem Rechner ausgeführt, der das Anmeldeskript nutzt, und Sie erhalten zentrale Informationen zu allen Rechnern im Netzwerk, die diese Richtlinie nutzen.

Wenn Sie im Anmeldeskript, das Sie über die Gruppenrichtlinie steuern, die Datei mit dem Auswertungsergebnis noch in einer Freigabe speichern, können Sie gezielt die Verwendung der Gruppenrichtlinien auf mehreren Rechnern überwachen. In diesem Fall lassen Sie die Auswertungsdatei aber nicht nur im Netzwerk speichern, sondern geben dem Dateinamen auch noch den jeweiligen Rechnernamen des ausgewerteten Rechners mit. Dazu verwenden Sie den Befehl:

```
Gplogview -o \\<Server>\<Freigabe>\%computername%-gpevent.txt
```

Sie können den Bericht auch eine HTML-Datei erstellen lassen. Die Syntax lautet in diesem Fall:

```
Gplogview -h -o \\<Server>\<Freigabe>\%computername%-gpevent.html
```

5.3.9 Wichtige Informationen immer im Blick: BGInfo auch in Skripten hinterlegen

Administratoren, die mehrere Server oder Computer von Anwendern im Netzwerk fernwarten, haben oft das Problem, dass nicht alle Informationen über den aktuell verbundenen Computer angezeigt werden, zum Beispiel IP-Adresse, Informationen zu den Laufwerken, Rechnernamen, Bootzeit, und vieles mehr. Auch wenn Anwender eine Fernwartung benö-

tigen, ist es hilfreich, wenn diese auf dem Desktop den Namen ihres Computers, die IP-Adresse und weitere Informationen auf einen Blick sehen. In vielen Fällen ist es also für Administratoren extrem hilfreich, wenn auf dem Desktop des ferngewarteten Computers nützliche Informationen angezeigt werden, allerdings ohne dass diese Informationen die Anwender stören.

Ein hilfreiches Tool für diese Zwecke ist BGInfo (<https://tinyurl.com/y7oflor9>) von Sysinternals. BGInfo kann Informationen in verschiedenen Schriftgrößen, Farben und anderen Formatierungen auf dem Desktop anzeigen. Führen Sie das Skript in einem Anmeldeskript aus, werden die Informationen bei jeder Ausführung aktualisiert.

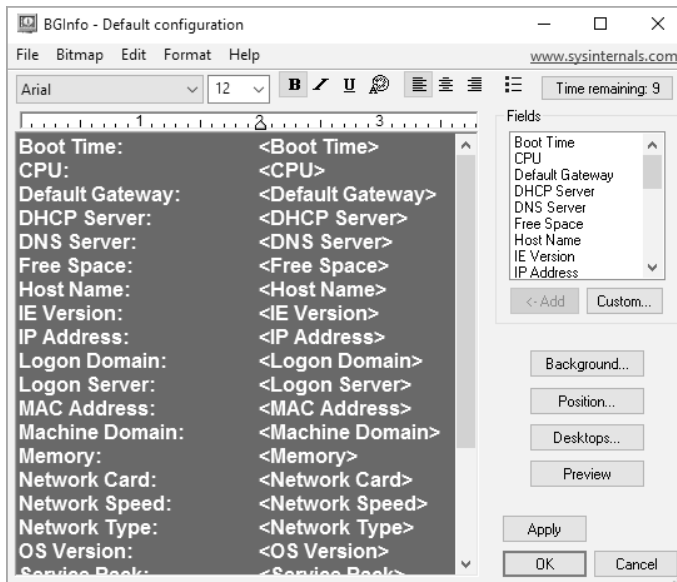


Bild 5.10 BGInfo hilft beim Identifizieren von Servern und Arbeitsstationen.

Neben vorgegebenen Feldern können Sie auch eigene Abfragen erstellen und Informationen einblenden lassen. Diese Anzeige lässt sich vor konfigurieren, als Konfigurationsdatei abspeichern und per Skript oder Gruppenrichtlinie an Computer im Netzwerk verteilen. Das Tool verbraucht keinerlei Systemressourcen, sondern erstellt beim Start aus den gewünschten Informationen ein neues Hintergrundbild auf dem Desktop und beendet sich danach wieder. Im laufenden Betrieb ist das Tool daher nicht gestartet und belegt somit keine Ressourcen.

Nach dem Start von BGInfo können Sie konfigurieren, welche Daten Sie zukünftig anzeigen wollen, und diese als Konfigurationsdatei abspeichern. Im Feld *Field* sehen Sie, welche Daten Sie in das Hintergrundbild einbinden können. Klicken Sie auf ein Feld und dann auf *<Add*, um es einzubinden.

Über die Schaltfläche *Custom* können Sie eigene Felder definieren, indem Sie mit *New* eine neue Abfrage starten. Sie haben im neuen Fenster die Möglichkeit, Umgebungsvariablen, einen Registrywert, eine WMI-Abfrage oder Daten einer Datei abzufragen. In den meisten Fällen ist dies aber nicht notwendig, da die Standardfelder bereits umfassende Informationen enthalten.

Natürlich ist es nicht sinnvoll, eine Konfiguration immer wieder neu zu erstellen oder für jeden Computer einzeln anzufertigen. Aus diesem Grund haben Sie in BGInfo auch die Möglichkeit, die von Ihnen angepassten Daten über den Menübefehl *File/Save As* als *.bgi*-Datei abzuspeichern. Sie können anschließend BGInfo so starten, dass das Tool diese *.bgi*-Datei als Konfigurationsdatei übernimmt und die ausgewählten Daten anzeigt. Dazu starten Sie BGInfo einfach mit dem Befehl:

```
Bginfo <Name der .bgi-Datei> /timer:0
```

Geben Sie keine Konfigurationsdatei an, verwendet BGInfo die Standardkonfigurationsinformationen, die in der Registrierung im Pfad *HKEY_CURRENT_USER\Software\Winternals\BGInfo* gespeichert sind.

Die Option */timer:0* bewirkt, dass das BGInfo-Konfigurationsfenster nicht erscheint, sondern sofort die Informationen übernommen werden. Sie können diesen Befehl in ein Anmeldeskript übernehmen und auf diese Weise auch Daten wie die Anmeldezeit oder Bootzeit des Computers erfassen.

Diese Zeiten sind natürlich immer nur dann aktuell, wenn Sie BGInfo bei jedem Systemstart oder jedem Anmelden starten lassen. BGInfo aktualisiert sich nicht dynamisch, sondern verwendet immer nur die Daten, die es beim Start vorfindet. Nach der Erstellung des neuen Hintergrundbilds beendet sich BGInfo wieder.

Neben Skripten können Sie BGInfo auch mit der Aufgabenplanung in Windows während des Systemstarts und im laufenden Betrieb ständig aktualisieren lassen. Das ergibt allerdings nur dann Sinn, wenn Sie auch Felder anzeigen lassen, deren Informationen sich im laufenden Betrieb ändern. Neben der Option */timer* stehen in BGInfo weitere Möglichkeiten zur Verfügung:

- */popup* - Geben Sie diese Option an, zeigt BGInfo ein Popup-Fenster an, welches die Informationen enthält. Dieses können Anwender schließen.
- */taskbar* - Bei dieser Option blendet BGInfo ein Symbol im Infobereich der Taskleiste ein. Klicken Anwender auf das Symbol, erscheinen die gewünschten Informationen genauso wie bei der Option */popup*.
- */all* - Ändert die Daten für alle aktuell angemeldeten Benutzer (zum Beispiel auf Terminalservern). Auf diese Weise erhalten also alle angemeldeten Anwender das neue Hintergrundbild.
- */log* - Erstellt eine Protokolldatei über die Ausführung, in die das Tool zusätzlich eventuell aufgetretene Fehler schreibt. Diese Option ist sinnvoll, wenn Sie das Tool im laufenden Betrieb über den Aufgabenplaner häufiger starten lassen.
- */rtf* - Erstellt eine *.rtf*-Datei. Diese Datei enthält auch die Formatierungen und Farbe zur Protokollierung.

Index

A

Abbild 100
Abbildpaket 100
Abfrage 192
Abfrageanweisung 80
Abfrageregeln 80
Abhängigkeit 176
Abonnieren 189
Active Directory 8
– Gruppenmitgliedschaft 79
Active Directory-Benutzerermittlung 61
Active Directory-Ermittlungsmethoden 60
Active Directory-Gesamtstruktur 61
Active Directory-Gesamtstrukturermittlung 60
Active Directory-Gruppenermittlung 61
Active Directory-Schema 11, 180
Active Directory-Standorte 62
Active Directory-Systemermittlung 61
AD-Gruppe 171
ADK 93, 110
Administratorkonten 15
ADMX-Dateien 139, 166
ADSI-Editor 8
Affinität 70
Agent 69
Aktualisierung 56, 60
Aktualisierungspakete 102f.
Anmeldeskripte 143
Antischadsoftware 214
Antischadsoftware-Richtlinien 211
Antwortdatei 111
Anwendungen 83, 168
Anwendungskatalog 2, 73
Anwendungskatalog-Webdienstpunkt 66

Anwendungskatalog-Websitepunkt 66
Application Compatibility Toolkit 112
Asset Intelligence 204
Assets und Konformität 73
ATP 212
Auswertungszeitplan 219
Authentifizierungszertifikatdatei 207
AutoIT 144
Automatisierung 95, 159
awebsctl.log 67
AWEBSVC 67

B

Baseline-Versionen 3
Batchdatei 143
Bedrohungsschutz 222
Begrenzungsgruppen 50, 62f.
Benutzergruppe 189
Benutzergruppenname 83
Benutzergruppenrichtlinie 147
Benutzerkonten 14
Benutzerressource 82
Benutzersammlungen 82, 171
Benutzerverwaltung 15
Berechtigungen 75
Bereinigungstask 4
Bereitstellen 91
Bereitstellung 168
Bereitstellungseinstellungen 102
Bereitstellungspakete 125
Bereitstellungsregel 218
Bereitstellungsringe 137
Bereitstellungstools 19
Bereitstellungstyp 161
Bereitstellungszeitplan 220

Betriebsmaster 11
 Betriebssystemabbilder 98
 Betriebssysteme 91, 94, 106
 Betriebssysteminstallation 95
 BGInfo 150
 Bootimages 91
 Bootp 92
 Branches 6

C

C2R 154
 Capture 95
 Ccmexec.exe 73
 Ccmsetup 72
 CD.Latest 37
 Click-to-Run 154
 Clientanwendungen 24
 Clienteinstellungen 68
 Clientinstallationseinstellungen 71
 Clientpushinstallation 71
 Clientrichtlinie 69
 Clientstandardeinstellungen 68f., 198
 Clientstatus 84
 Clientupdate 60
 CmRcViewer.exe 210
 CMTRace 96
 CMTrace.exe 44, 58
 Cmupdate.log 58
 CMUpdateReset.exe 57
 Computereinstellungen 136
 Computerinformationen 100
 Computerkonten 21, 61
 Computersammlung 108
 ConfigMgrAutoSave.ini 45
 ConfigMgr Client Health 77
 ConfigMgrPrereq.log 34
 ConfigMgrSetup.log 35, 37, 43
 ConfigMgr Task Sequence Monitor 96
 Configuration 50
 Configuration Manager Trace Log Tool 58
 CONFIGURATION_MANAGER_UPDATE 57
 Configuration.xml 155
 config.xml 158
 Current Branch 5

D

Dateireplikationsdienst 144
 Datei- und Druckerfreigabe 13

Datenbankmodulkonfiguration 22
 Datenbankreplikate 188f.
 Datenbankserver 20
 Datenquelle 93
 Datenschutz 138
 Dcdiag 12
 Defender 6, 140
 Definitionsupdate 218
 Deployment Ring 137
 Deployment Tool for Click-to-Run 164
 DHCP 92
 Dienstverbindungspunkt 52, 187
 Dism 18
 DISM 112
 Dmpdownloader.log 58
 DMTF 201
 Domänencontroller 81
 Downloadmodus 136
 Dsquery 11

E

EasySetupPayload 52
 Endpoint Protection 211
 Endpoint Protection-Dashboard 216
 Ermittlung 61, 181
 Ermittlungsmethoden 60, 183
 ESD-Dateien 135
 Excel-Tabelle 134
 Exchange 11
 execmgr.log 176
 Exploit 139
 Exploit Guard 6
 Exploit-Schutz 139, 224
 ExtADSch.exe 11
 ExtADSch.log 11

F

Fallbackstatuspunkt 66
 Favoritenordner 165
 Feature Updates 137
 Fehlerbehebung 227
 Filter 99
 Firewall 24
 Firewallinstellungen 211
 Firewallregeln 25
 Frequenzermittlung 60
 FRS 144

G

Geräte 72f.
 Gerätesammlungen 77, 99, 123
 Gesamtstruktur 180
 Gesamtstrukturermittlung 60
 Get-WmiObject 108
 Gplogview 149
 gpupdate 167
 Gpupdate 14
 Group Policy Log View 149
 Grundeinrichtung 68
 Gruppenrichtlinien 13, 134, 142, 166
 – Verwaltungskonsole 13
 GUID 57

H

Hardwareinventur 197
 Hardwareinventurklassen 199
 Hardwareverlauf 200
 Hierarchie 36, 60, 178
 – Konfiguration 60, 62
 Hierarchieeinstellungen 7
 Hierarchiekonfiguration 193
 Hintergrundübertragungsdienst 17
 Hotfixes 59
 HTTP-Umleitung 17

I

Identifikationsinformationen 204
 IIS *siehe* Internet Information Services
 Image 97
 Inhalt 98
 Inhaltsstatus 163
 Inhaltsziel 94
 Installation 31
 – Dateien 59
 – Einstellungen 39
 – Pakete 60
 – Quelldateien 48
 – Schritte 56
 – Status 50
 Installationsdateien 160
 InstallCustomSoftware.cmd 123
 Internetinformationsdienste-Manager 192
 Internet Information Services 18
 Intune 6, 187
 Intune-Connector 4

Inventurklassen 206
 Inventurverlauf 200
 iOS-App 4
 ISO 96
 ISO-Datei 118

K

kixart 144
 Klasseneigenschaften 199
 KMS 117
 Kommunikation 188
 Kommunikationseinstellungen 40
 Kompatibilitätseinstellungen 68
 Komponentenstatus 187
 Konfigurationsdaten 16
 Konformitätsauswertung 69
 Konformitätseinstellungen 69
 Konten 165
 Kriterientyp 80

L

Laufwerkseinstellungen 50
 LaunchMedia.cmd 96
 LDAP 193
 Linux 201
 Lizenzbedingungen 56
 Lizenzdetails 116
 Lizenzen 116
 Lizenzierung 7, 158
 Lizenzinformationen 116
 Long-Term Servicing Branch 7, 134
 Loopbackverarbeitungsmodus 147
 LTSB *siehe* Long-Term Servicing Branch

M

MAC-Adresse 100
 Machine Learning 212
 MDT 118
 Media Creation Tool 118
 Microsoft Deployment Toolkit 118
 msp-Datei 159

N

Named Pipes 23
 Namenskontext 9
 .NET Framework 17, 173

NETLOGON 144
 Netzwerkisolation 139
 Netzwerkschnittstellen 91
 Netzwerkzugriff 26
 Netzwerkzugriffskonto 94
 NTLite 113

O

Objekttypen 10
 Objektverwaltung 10
 OCT 158
 Office 138, 153
 Office 365 154
 Office 365 Configuration XML Editor 157
 Office 2016 167
 Office 2016 Deployment Tool 154
 Office Customization Tool 158
 Offlinebearbeitung 111
 Offlinemodus 52
 OfflineServicingMgr.log 103
 One-Click-Installer 153
 Onlinemodus 52
 Organisationseinheit 100
 Organisationseinheitsname 81

P

Pakete 173
 Paketfreigabe 50
 Paketinhalt 107
 PatchDownloader.log 127
 Planung 181
 PolicyDefinitions 134, 166
 Portfreigaben 24
 PortQry 27
 PowerShell 18, 148
 Präproduktionssammlung 4
 Prereqchk.exe 32f.
 Product Key 116
 Produktionsclients 60
 Profil 143
 proplusr.ww 160
 Protokolldatei 76, 96, 127, 132
 – awebsctl.log 67
 – Cmupdate.log 58
 – ConfigMgrPrereq.log 34, 43
 – ConfigMgrSetup.log 35, 37, 43
 – Dmpdownloader.log 58
 – öffnen 58

Provisioning Package 119
 Proxyserver 138
 Prüfung 42
 PST-Dateien 167
 Pullabonnements 190
 PXE 91
 PXE-Boot 102

Q

QoS-Wert 137
 Quality Updates 138

R

Ransomware 139
 Referenzen 65
 regedit 165
 Registerkarten 62
 Registrierungseinstellungen 14
 Registrydatei 165
 Registryschlüssel 45
 Remotecomputer 33
 Remotedesktop 208
 Remotedesktop-Sitzungshosts 147
 Remoteserverdifferenzialkomprimierung 17
 Remoteserver-Verwaltungstools 13
 Remotesteuerung 209
 Remotesteuerungssitzung 208
 Remotetools 68, 70
 Remoteunterstützung 208
 Repadmin 12
 Replikatserver 189
 Reporting Services
 – Konfiguration 23
 Report Viewer 24
 Ressourcen 181
 Ressourcen-Explorer 203
 Ressourcenklasse 82
 Richtlinien 6, 78, 214
 Rollen 17
 Rollendienste 17
 Rollenverwaltungstools 15
 Rsop.msc 14
 RuleEngine.log 127

S

- Sammlungen 80, 82
- SCCM
 - Dokumentation 227
 - Konsole 7
 - Neuerungen 3
 - Schemamaster 11
- SCCM-Standorte 63
- Schadsoftwareerkennung 217
- Schema
 - Änderung 11
 - Erweiterung 10f.
- Schemamaster 11
- Schlüsselverwaltungsdienst 117
- Schritt-für-Schritt-Anleitungen 228
- Serverkonfiguration 22
- ServiceConnectionTool.exe 53
- Set-ExecutionPolicy 148
- Set-MpPreference 223
- SetupDL.exe 35
- setuperr.log 96
- Setuptools 36
- setupwpf.exe 46
- Sicherheitseinstellungen 25, 167
- Sicherung 97
- Sicherungsdatei 87
- Signatures 165
- SIM 112
- Simulieren 168
- Single-Instance-Verfahren 110
- Skriptdatei 146
- slui 116
- SmartScreen 140
- SMS_DMP_DOWNLOADER 187
- SMSSETUP 46
- sms_site_backup 89
- Softwarebereitstellung 68, 70
- Softwarebibliothek 94, 98, 102, 130, 160, 168
- Softwarecenter 2, 74
- Softwareinventur 202
- Softwareupdates 130, 218
- Softwareupdatepunkt 105f., 4
- Softwareverteilung 62, 94
- Speicherort 160
- splash.hta 34
- SQL
 - Abwärtskompatibilität 22
 - Sortierung 22

- SQL Server 20
 - Browser 24
 - Instanz 23
 - Management Studio 23
 - Reporting Services 2
- SQL Server-Einstellungen 48
- SQL Server Reporting Services 2
- SSRS *siehe* SQL Server Reporting Services
- SQL Server Service Broker 192
- Standort 7, 47, 77, 179, 182
- Standortcode 48
- Standortdatenbankserver 189
- Standortdatenbankserverrolle 180
- Standorthierarchie 177
- Standortkomponenten 94
- Standortkonfiguration 52, 59, 71, 94, 129, 185
- Standortserverrolle 180
- Standortsicherung 88
- Standortstatus 84
- Standortsystemrollen 65, 91, 129, 179, 185, 207, 213
- Standortsystemserver 180
- Standortwartung 86
- Standortwartungstask 200
- Startabbilder 93
- Store 136
- Subnetze 193
- SUSDB 16
- Synchronisierungspunkt 204
- Sysprep 96
- Systemabbild-Manager 111
- System Center Online 205
- Systemdienst 57
- Systemressource 80
- Systemrolle 66, 131
- Systemrollenauswahl 66, 186
- Systemstatus 84
- Systemupdates 173

T

- Task-Manager 72, 74
- Tasksequenzen 5, 95, 99
- Tasksequenzmedien 95, 99, 109
- TCP/IP-Protokoll 24
- TCP-Port 188
- Telemetrieumgebung 168
- Testversion 227
- Timeout 38

Treiber 94
 Treiberpakete 94, 106
 Trust Center 167

U

Überprüfen 94
 Überwachung 56, 84, 131
 Universelle Windows-Plattform 4
 Unix 201
 Unternehmensportal 3
 UpdateGenerator.exe 121
 Updateklassifizierung 219
 Updatepaket 54
 Updates 51, 103, 130, 159
 Upgradepaket 104
 Uploadbandbreite 137
 UseWU Server 4
 UWP *siehe* Universelle Windows-Plattform

V

VAMT 112
 Veröffentlichen 194
 Verteilungspunkte 50, 91, 94, 109
 – cloudbasierte 5
 Verteilungsstatus 85, 94, 163
 Verwaltung 63
 Verwaltungspunkt 42, 109, 198
 Volume Activation Management Tool 112
 Volumenaktivierungsmethode 117
 Volumenlizenz 154
 Vorabversionen 136
 Voraussetzungen 32
 Voraussetzungsprüfung 33, 53

W

Warnungen 84
 Warnungsschweregrad 216
 Wartung 51
 Wartungspläne 123, 126f.
 Wartungsstatus 56
 Wartungstasks 86
 WCM.log 132
 wf.msc 40

WIM-Datei 96, 119
 WIM-Image 98
 Windows 10 103, 134
 – Updates 228
 Windows 10-Wartung 123
 Windows-Authentifizierung 192
 Windows-Authentifizierungsmodus 22
 Windows Configuration Designer 111
 Windows Defender Advanced Threat
 Protection 212
 Windows Defender Application Guard
 – Richtlinien 6
 Windows Defender Exploit Guard 224
 Windows Defender Security Center 140
 Windows-Firewall 13
 Windows-Positionssuche 138
 Windows-Registry 165
 Windows Server Update Services 1, 4, 15
 – Bereinigungs-task 4
 Windows System Image Manager 113
 Windows Update for Business 4
 Windows-Updates 105, 136
 Windows-Verwaltungsinstrumentation 13, 198
 Winreducer 119
 WMI 198
 WSIM 113
 WSUS *siehe* Windows Server Update Services
 WSUS Offline Update 121
 WSUS-Verbindung 132
 wsutil.exe 135
 wsyncmgr.log 132
 WUfB *siehe* Windows Update for Business

X

XML-Datei 139

Y

YouTube-Videos 228

Z

Zeitpläne 61
 Zertifikat 189