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

Inhalt

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 Vorauflage, 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 Channeln 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.

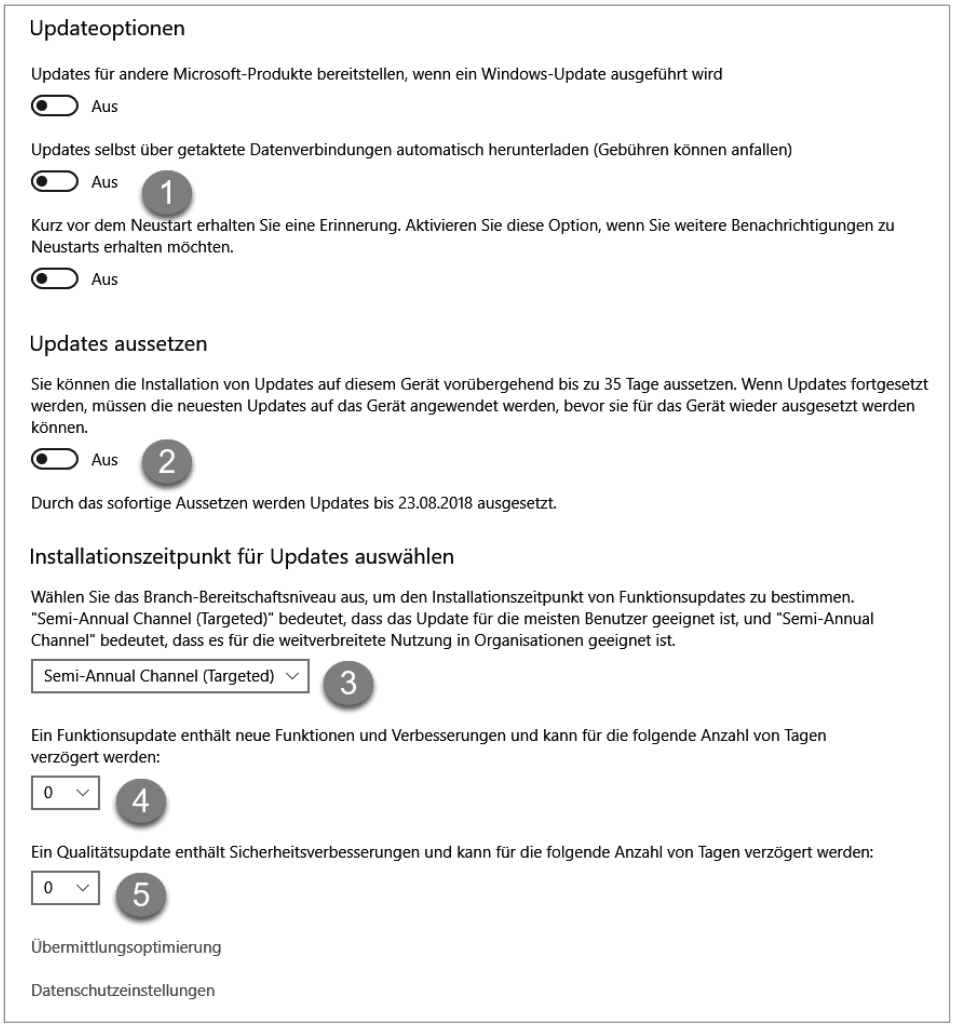

Bild 12.1 Die Updateoptionen von Windows 10

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.

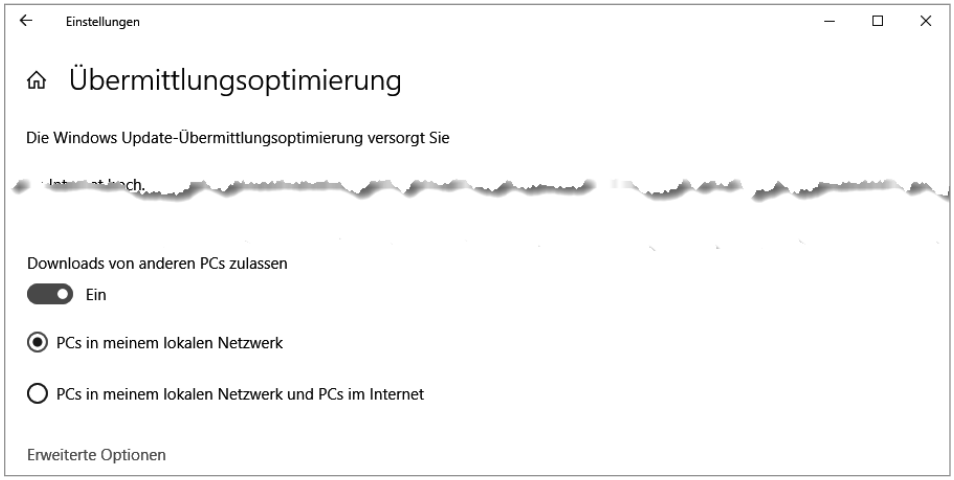

Bild 12.2 Zusätzlich zu BITS können Sie auch mit Delivery Optimization Updates beziehen.

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 betriff 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 Datentausch 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	Mit dem Downloadmodus legen Sie fest, mit welchen Methoden der Windows Update Client einen Download durchführen darf. **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). **1: LAN:** Der Client benutzt HTTP (BITS) und Peer-to-Peer mit Clients im gleichen Netzwerk. **2: Gruppe:** Der Client benutzt HTTP (BITS) und Peer-to-Peer mit Clients der gleichen Gruppe. **3: Internet:** Der Client benutzt HTTP (BITS) und Peer-to-Peer mit beliebigen Clients. **99: Einfach:** Mit dieser Einstellung wird die Übermittlungsoptimierung komplett deaktiviert, der Client holt Updates nur per HTTP (BITS). **100: Überbrückung:** Verwendet BITS in Verbindung mit BranchCache. Übermittlungsoptimierung ist auch hier deaktiviert. 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*.	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 Peerauswahl 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/2OGbalJ*.	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 zur 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.

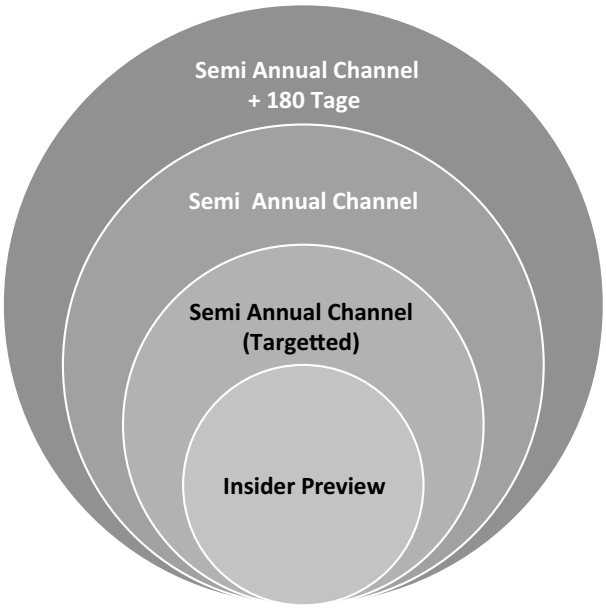

Bild 12.3 Windows-Bereitstellung in Wellen oder Ringen

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/2LHtpeW*.

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.

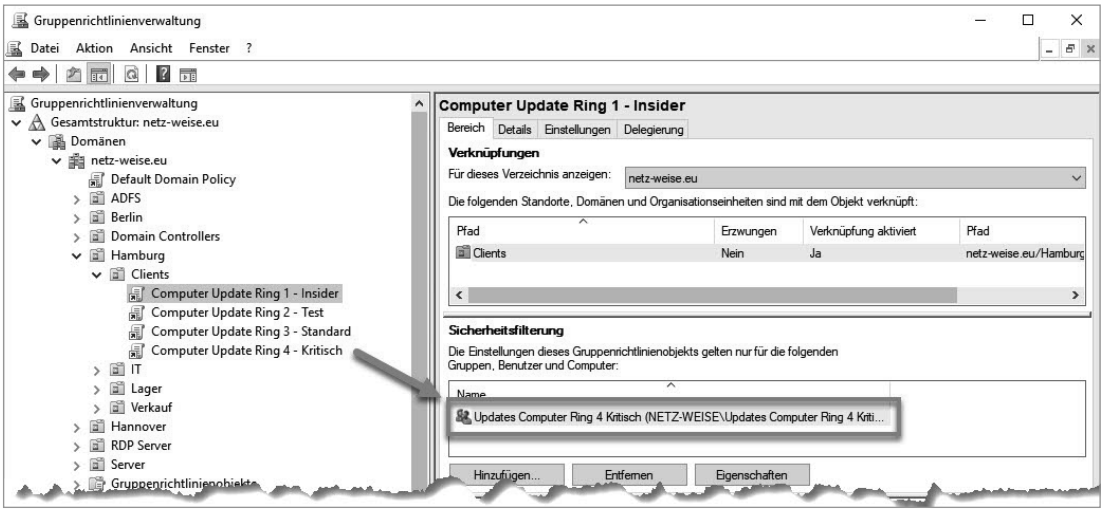

Bild 12.4 Für jeden Ring gibt es ein GPO und eine Gruppe, auf die gefiltert wird.

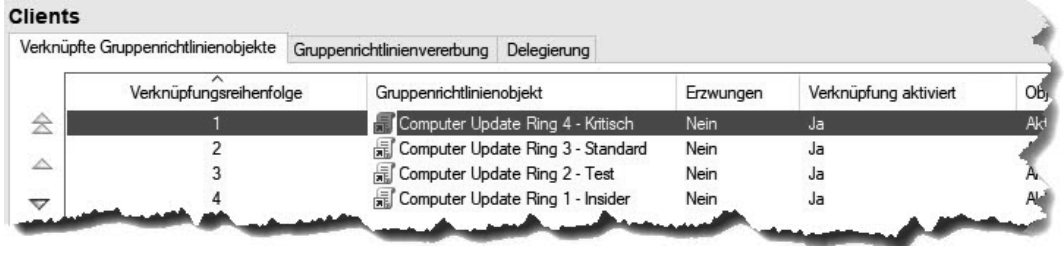

Bild 12.5 Achten Sie darauf, die kritischste Gruppe in der Verknüpfungsreihenfolge ganz nach oben zu schieben.

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.

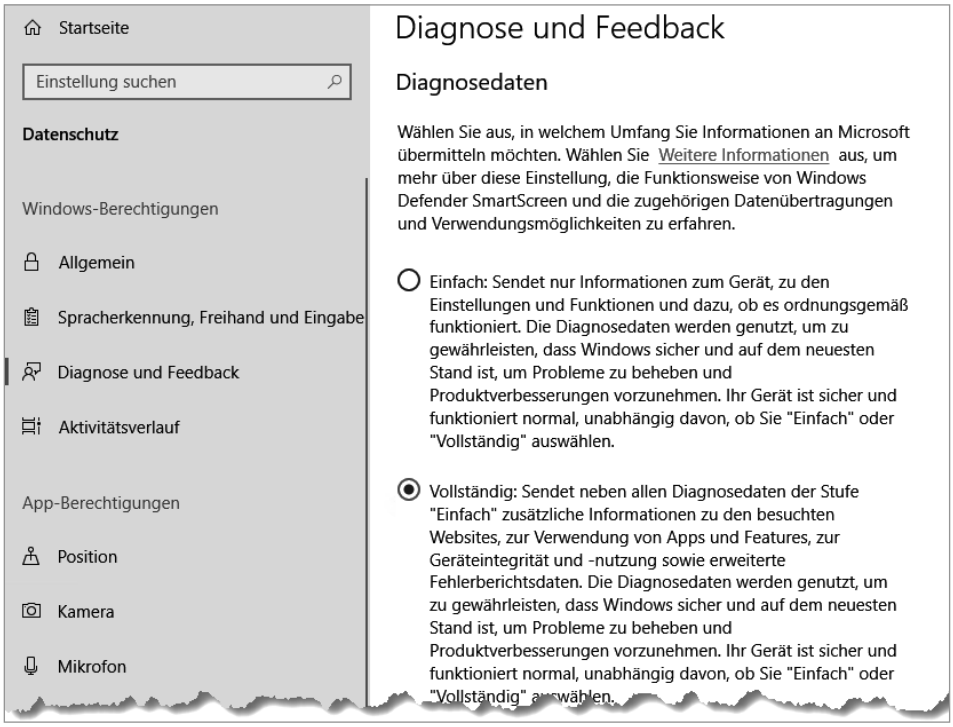

Bild 12.6 Sie können Diagnosedaten nur auf „Einfach“ stellen, sie aber nicht deaktivieren.

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/2AlDhtN*.	

Index

Symbole

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z