Peter Siering

Familienpackung

Windows-Updates mit WSUS organisieren

Die Windows Server Update Services (WSUS) sind das offizielle Angebot Microsofts, Updates entkoppelt vom regulären Windows Update selbstbestimmt zu beziehen, zu dosieren und zu verteilen – jedenfalls dann, wenn man sich nicht auf komplexere, kostenpflichtige, oft Cloud-basierte Werkzeuge einlassen will. Beim dafür obligatorischen Server kann man tricksen.

WSUS funktioniert wie ein Cache: Der Dienst lädt die Update-Daten bei Microsoft herunter, sodass Systeme im lokalen Netz nicht die Server bei Microsoft ansteuern müssen. Das spart Bandbreite, hat aber auch weitere Vorteile: Welche Updates die Systeme von WSUS erhalten und wann sie diese installieren, kann man im Detail mit Regeln vorgeben, zum Beispiel Signatur-Updates sofort an Clients durchreichen, Sicherheits- und wichtige Updates mit zwei Tagen Verzögerung installieren und den Rest erst nach zwei Wochen.

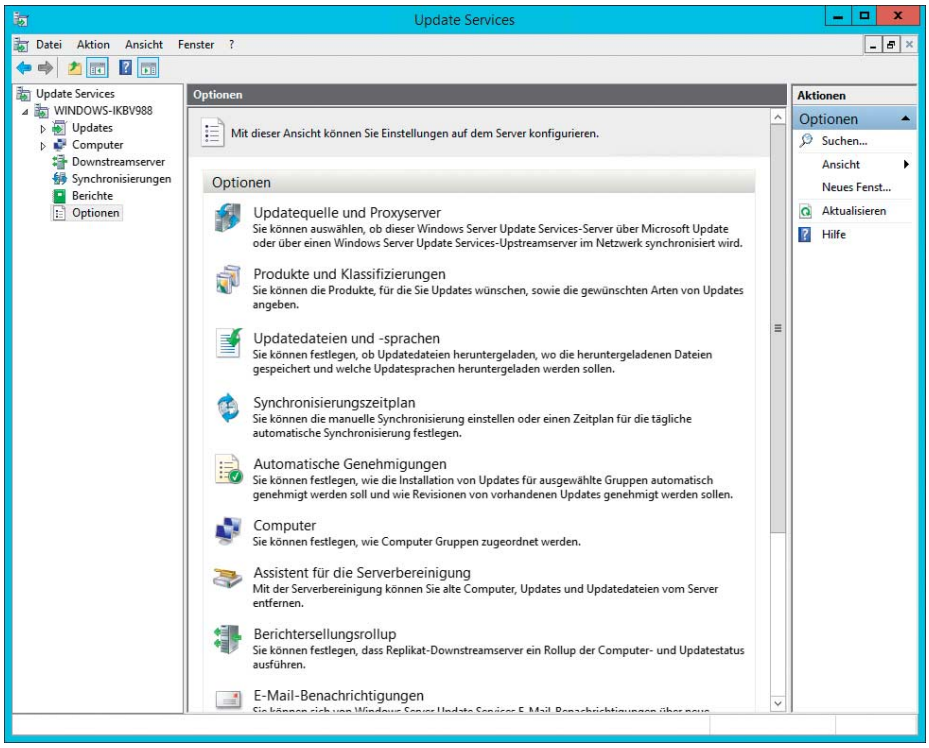
WSUS setzt einen Windows-Server als Basis voraus. Die aktuelle Version des Windows Server 2012 R2 bringt den Dienst mit. Üblicherweise stellt ein solcher Server fürs lokale Netz einen Verzeichnisdienst (Active Directory) und weitere Dienste bereit (etwa in der Essentials- oder SBS-Ausgabe). Dann ist die Einrichtung wenig kompliziert. Aber auch ohne Active Directory in einer Workgroup lässt sich ein WSUS in Betrieb nehmen: Das Folgende liefert die nötigen Tipps für den Workgroup-Einsatz und der Kasten „Instant-WSUS“ auf Seite 97 einen Rezeptvorschlag, um in einer VM eine Windows-10-Update-Bremse aufzusetzen.

Wer mit WSUS starten will, nimmt idealerweise einen aktuellen Windows Server 2012 R2 her (aber auch Server ab 2008 genügen). Nicht jede Edition eignet sich: Standard, Datacenter und Essentials reichen, Foundation, Storage sowie Hyper-V nicht. Aber Achtung: Microsofts Lizenzbedingungen fordern, sobald ein Client von einem Server wiedererkannt oder authentifiziert wird, dass eine Client-Zugriffslizenz (CAL) vorhanden ist. Da WSUS Clients wiedererkennt, braucht jeder also eine CAL. Der Spielraum für kreative Ausnahmen ist nicht allzu groß (siehe Kasten „Instant-WSUS“).

Wie es losgeht

Die manuelle Installation von WSUS als Rolle auf einem Server mit grafischer Bedienoberfläche erfordert nicht nur Geduld, sondern auch viele, viele Klicks. Die drei Etappen sind dank Assistenthilfe jedoch narrensicher: die WSUS-Rolle hinzufügen, Grundkonfiguration erledigen und Ersteinrichtung durchlaufen. Die Assistenten erfragen die wesentlichen Daten.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover



Beim Verwalten eines WSUS-Servers hilft eine spezialisierte MMC. Die kann wahlweise auf dem Server selbst oder auf einem Client im Netz laufen. Letzteres hilft, den Server schlank zu halten.

Wer sich an die Vorgaben hält, kommt heil durch. Der Pfad zu einem Verzeichnis, in dem die Update-Daten landen sollen, ist anzugeben; anlegen muss man dieses Verzeichnis nicht. Es empfiehlt sich, eines zu wählen, das nicht auf der Systemplatte liegt. Wenn ein WSUS-Server nicht nur die Informationen über die Updates sammeln, sondern auch die Updates selbst als Cache vorhalten soll, beansprucht das Verzeichnis schnell viel Speicherplatz. Sprachen spielen dann eine Rolle, wenn man die Updates lokal vorhalten will. Eine begrenzte Sprachauswahl hilft, Platz zu sparen.

Wenn ein frisch aufgesetzter WSUS-Server sich das erste Mal die Daten der bei Microsoft vorrätigen Updates abholt, kann das ewig dauern – und das, obwohl er zunächst nur die Meta-Daten holt. Man tut gut daran, die Auswahl der Produkte auf das zu begrenzen, was man braucht. Die Finger sollte man von den Klassifizierungen lassen. Das verlockende Einschränken dieser Update-Kategorien (Sicherheit, Features, Treiber usw.) birgt die Gefahr, dass Clients Updates versäumen. Denn Updates, die ein WSUS nicht anbietet, existieren für seine Clients nicht.

Von sich aus verteilt eine WSUS-Grundinstallation keine Updates (in Komplett-Paketen wie den Small Business Servern ist das anders). Damit sie das tut, sind mehrere Dinge nötig: Der Verwalter muss Regeln vorgeben, nach denen WSUS Updates genehmigt, das heißt, Updates automatisch an Client-Systeme weitergibt. Dafür ist es hilfreich, Computer, die Updates empfangen sollen, in Gruppen zusammenzufassen, um mit den Regeln daran anzuknüpfen. Regeln sind der einzig sinnvolle Weg, Updates zu dosieren.

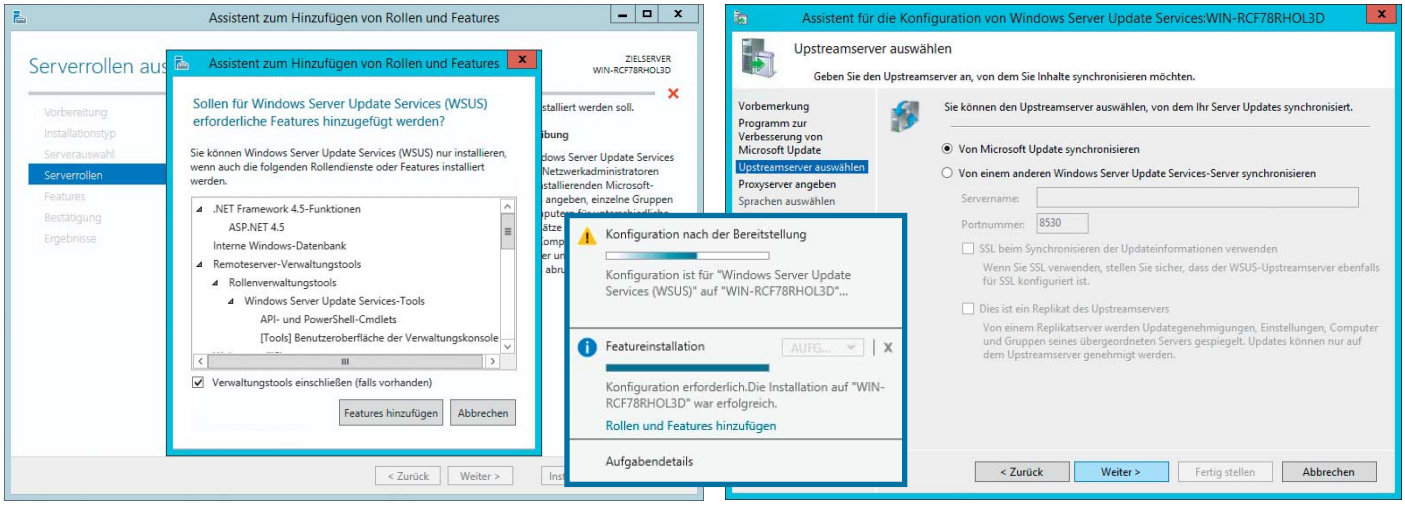
WSUS für Workgroups

Damit die in Windows-Clients und -Servern enthaltenen Funktionen nicht bei offiziellen Microsoft-Diensten nach Updates fragen, sondern dazu einen lokalen WSUS-Server konsultieren, müssen sie passend konfiguriert sein. In einem Netzwerk mit Active Directory lassen sich die Koordinaten eines WSUS über die Gruppenrichtlinien an die Systeme im Netz verteilen (Server-Komplettpakete wie ein SBS erledigen das meist ohne Zutun).

WSUS lässt sich aber durchaus auch ohne ein Active Directory betreiben. Statt die per Gruppenrichtlinie umgesetzten Änderungen an der Windows-Registry dort selbst hineinzufummeln, bietet sich fertige Software an. Daniel Bedarf hat dazu den „WSUS Client-Manager for Workgroups“ geschrieben und stellt ihn auf Codexplex zum kostenlosen Download bereit (siehe c’t-Link am Ende des Artikels).

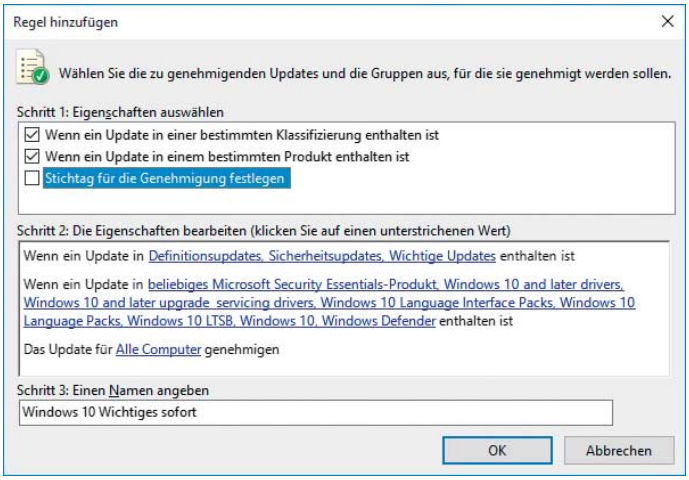
Die Software geht sehr vorsichtig zu Werke: Bevor sie Änderungen in die Registry schreibt, sichert sie die betroffenen Schlüssel in einer Datei, sodass man den Vorgang rückgängig machen kann. Sie bietet allerlei Optionen, um den Update-Client in Windows zu beeinflussen und um auf weitere Details wie die Registrierung am WSUS Einfluss zu nehmen. Ein Export als Reg-Datei für die Einstellungen rundet den Funktionsumfang ab – praktisch, um einen Satz Einstellungen auf viele Systeme anzuwenden.

Im Allgemeinen genügt es, das Feld „WSUS-Server“ mit der IP-Adresse oder dem Namen des WSUS-Servers auszufüllen. Der Erstkontakt mit dem WSUS-Server registriert einen Client dort. Dass dieser dort als Computer geführt wird, ist ein sicheres Zeichen, dass die beiden miteinander reden. Jetzt kann man den Computer auf dem WSUS-Ser-

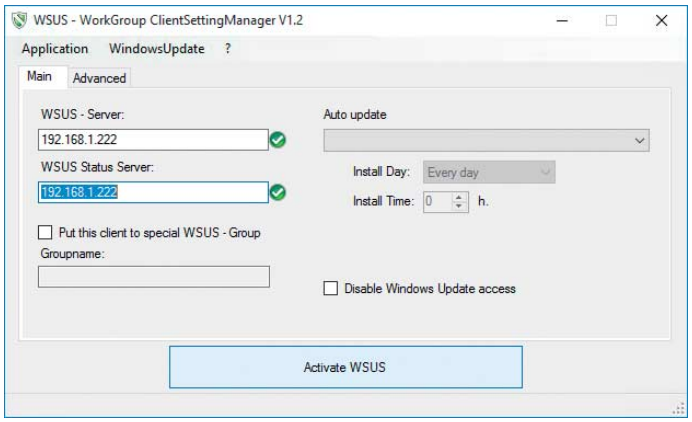


Die WSUS-Installation erfolgt in drei Etappen: Im Server-Manager die Rolle hinzufügen, ebenda die Gundkonfiguration vornehmen und die Details im WSUS-Manager erledigen.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover



Über Regeln bestimmt der WSUS-Verwalter, welche Systeme welche Sorte Update wann erhalten.



WSUS geht auch ohne Active Directory: Daniel Bedarf hat dafür ein hilfreiches Programm geschrieben.

ver in eine Gruppe packen, für die Genehmigungsregeln existieren, und die Updates trudeln über den eigenen WSUS ein.

Core-WSUS

Solange WSUS auf einem vollwertigen Server mit Desktop-Umgebung arbeitet, lässt er sich entspannt über die mitinstallierte Management Console (MMC) steuern. Läuft er allerdings auf einer Core-Installation, dann muss die Administration von einem Client-System aus übers Netz erfolgen. Auf diesem Client installiert man dazu die Remote Server Administration Tools (RSAT), die Microsoft passend für jede Windows-Version kostenlos zum Download anbietet (siehe c't-Link). RSAT setzt stets eine Pro-Version von Windows voraus.

Für Windows 10 gibt es RSAT nur in englischer Sprache. Damit es sich auf einer deutschen Version installieren lässt, muss man zunächst das Sprachpaket Englisch (United States) hinzufügen – das ist erst der Fall, wenn das in Einstellungen unter „Land oder Region" mit dem Vermerk „Sprachpaket installiert" auftaucht. Nach dem Hinzufügen des Sprachpakets muss man Windows 10 per Klick auf die Sprache und Auswahl von Optionen per Klick auf Herunterladen dazu ermuntern, die Dateien auch wirklich als Update (noch ohne WSUS-Hilfe) zu holen.

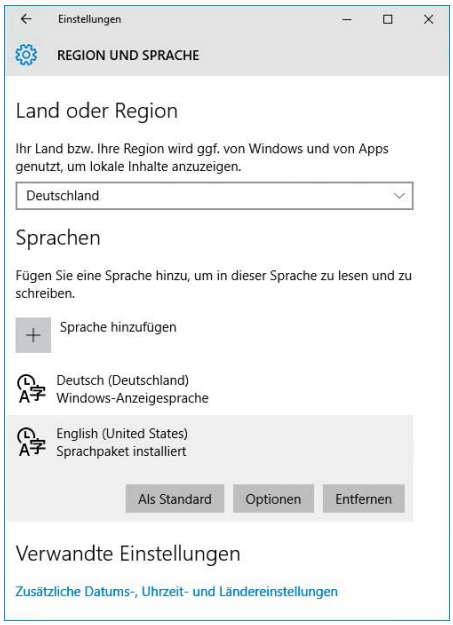
RSAT kommt als eigenständiges Update-Paket daher (.msu-Datei). Es erweitert die Liste der Windows-Features, die über die Systemsteuerung unter Programme zugänglich ist. Wenn die Installation gelingt, tauchen die in RSAT enthaltenen Werkzeuge im Startmenü als neue Gruppe „Windows-Verwaltungsprogramme" auf.

Core-WSUS für Workgroups

Wenn man in einem Active Directory auf dem verwaltenden System als Administrator angemeldet ist, so sollte es kein Problem sein, den WSUS über die „Windows Server Update Services"-MMC zu verwalten. Gegebenenfalls fügt man den WSUS-Server per Rechtsklick in der Konsole hinzu. Gelingt das nicht, ist es Zeit zu überprüfen, ob man wirklich als Admin in der Domäne angemeldet ist.

In einer Workgroup ohne zentrale Benutzerdatenbank hilft folgender Trick, damit das Verbinden mit dem WSUS-Server klappt: Man richtet dazu auf dem Server ein Konto mit Administrationsrechten ein, dessen Benutzername und Passwort identisch mit den Daten sind, die am lokalen PC verwendet werden. Die MMC leitet die lokalen Anmeldedaten an den WSUS-Server weiter – sind die gleich, gelingt der Verbindungsaufbau.

Auch hier lauert eine Tücke: Windows-Server stellen hohe Anforderungen an Passwörter – womöglich misslingt das Einrichten eines identischen Kontos mit Admin-Rechten auf dem Server, weil dessen Passwort zu trivial ist. Mit folgender Powershell- und Secedit-Melange (als Datei über den c't-Link zu bekommen) treibt man dem Server diese Ansprüche aus:



RSAT für Windows 10 setzt voraus, dass das Sprachpaket „Englisch (United States)" auch wirklich installiert ist.

```
secedit /export /cfg c:\secpol.cfg
(gc C:\secpol.cfg).replace("PasswordComplexity = 1", ↵
      "PasswordComplexity = 0") | Out-File C:\secpol.cfg
secedit /configure /db c:\windows\security\local.sdb ↵
                   /cfg c:\secpol.cfg /areas SECURITYPOLICY
rm -force c:\secpol.cfg -confirm:$false
```

Wenn das Skript in einem Verzeichnis als passpol.ps1 gespeichert wurde, führt es folgender Befehl aus:

```
powershell -ep RemoteSigned -file passpol.ps1
```

Danach frisst ein Server auch simple Kennwörter – aus Sicherheitssicht wäre es freilich eher angebracht, auf dem Client ein sicheres Kennwort zu setzen.

Taucht der Server nach dem Hinzufügen in der MMC immer noch nicht auf, sind womöglich die Firewall-Regeln für private/öffentliche Netze im Weg. Sollten die noch nicht gerade gerückt sein, so erledigt das der folgende Befehl in einer Powershell:

```
Set-NetConnectionProfile –InterfaceAlias Ethernet ↵
                                  –NetworkCategory Private
```

Wenn der Server mehrere Netzwerkkarten enthält, ist der Befehl entsprechend zu wiederholen; `Get-NetAdapter` liefert eine Liste der Karten. Vorsicht: Mühsam gehegte Firewall-Regeln gehen dabei über die Wupper.

Wo es klemmen kann

Zwei Nachteile seien nicht verschwiegen: Wenn WSUS in einer Workgroup läuft, also ohne Active Directory im Hintergrund, so bietet es die Dienste nur unverschlüsselt an. Es sollte möglich sein, die zugrunde liegende IIS-Konfiguration mit Zertifikaten zu versorgen, aber besonders bei einer Core-Installation ist das nichts, was sich zwischen Tür und Angel erledigen lässt. Wir haben es deswegen nicht durchexerziert.

Der zweite Nachteil betrifft Windows 10 Home: Diese Edition spricht nicht mit einem WSUS-Server, sondern nur Pro, Enterprise und Education. Microsoft hat die Funktion in Home mutwillig stillgelegt. Ältere Windows-Versionen sprechen auch in der Home-Edition mit einem WSUS, wenn man sie bei-

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

spielsweise über den WSUS ClientManager for Workgroups darauf einstellt.

Bei einem Upgrade auf Windows 10 Home von Windows 8.1 Core aus, das für den Update-Bezug per WSUS konfiguriert ist, wendet sich ein PC wieder den offiziellen Update-Diensten Microsofts zu. Dass die WSUS-Konsole eines Server 2012 R2 Windows 10 als Vista anzeigt, ist hingegen nur ein kosmetisches Problem (erst WSUS im Server 2016 zeigt den Namen des Clients korrekt).

Klappt das Umstellen von lokalem Upate-Bezug auf WSUS partout nicht, könnte ein noch ausstehendes Update im Weg sein. Sobald bei einem solchen System dann die bereits heruntergeladenen Updates auch installiert sind, taucht es auch als Computer in der WSUS-Konfiguration auf. Antwortet ein konfigurierter WSUS-Server nicht, so meldet Windows auf der Client-Seite, dass es keine Updates laden konnte und empfiehlt, die Internet-Verbindung zu überprüfen, auch wenn der WSUS im lokalen Netz steht.

In den PC-Einstellungen von Windows 10 findet sich auf der Hauptseite der Update-Optionen die Checkbox „Suchen Sie online nach Updates von Microsoft Update“. Wenn die aktiv ist, steuert der Update-Client einmalig nicht den eventuell eingetragenen WSUS-Server an, sondern schaut bei Microsoft nach, ob es Updates gibt. Das ist praktisch, um für Windows-10-Clients am WSUS zu prüfen, ob der alles, was relevant ist, auch im Angebot hat.

Spielraum

WSUS erleichtert einem Administrator auch das Leben in anderer Hinsicht: Der Dienst liefert Informationen über den Update-Stand der registrierten Clients. So lassen sich Probleme mit Updates oder leichtsinnige Update-Verweigerer erkennen. Wer mag, kann WSUS dazu bringen, beim Eintreffen neuer Updates, E-Mail-Benachrichtigungen zu senden. Ferner stellt die WSUS-Console diverse Auswertungen bereit, will dazu aber einige Extra-Pakete installiert haben (Download-Links dafür via c’t-Link).

WSUS lässt dem Verwalter große Freiheiten, wie er die Auslieferung von Updates gestaltet. Tipps für optimale Regeln lassen sich kaum geben. Zwei Dinge sind aber sehr wichtig: Der Verwalter sollte, besonders wenn WSUS die Updates zwischenspeichert, die internen Datenbanken regelmäßig aufräumen lassen. Das erledigt der Assistent für die Serverbereinigung; ein Powershell-Skript kann beim Automatisieren helfen (Befehl Invoke-WsusServerCleanup).

Der zweite wichtige Punkt ist die Überwachung. Wer seinen Clients einen WSUS-Server vorsetzt, muss nicht nur Sorge dafür tragen, dass er läuft, sondern auch, dass der alle relevanten Updates vorrätig hält. Versäumt der Verwalter, ein benötigtes Produkt zu abonnieren, denken die hinter dem WSUS laufenden Systeme, alles sei in bester Ordnung, obwohl sie seit Monaten keine Sicherheits-Updates mehr bezogen haben – das kann fatale Folgen haben. Hier gibt es keine Automatismen, es hilft nur ein wacher Kopf über der Tastatur. (ps@ct.de)

Literatur

[1] Windows Update Services: Client-Server Protocol: https://msdn.microsoft.com/en-us/library/cc251937.aspx
[2] Peter Siering, Schrumpfserver, Windows Server als Core-Installation, c’t 20/13, S. 180
[3] Wsus Package Publisher, MSI-, MSP- oder EXE-Dateien per WSUS veröffentlichen: https://wsuspackagepublisher.codeplex.com/

c’t Software für WSUS: ct.de/yvmx

Instant-WSUS – Update-Bremse für Windows 10

Um WSUS als Update-Bremse für Windows 10 Pro an den Start zu bringen, muss man keinen Server abstellen. Eine virtuelle Maschine dafür kann ein moderner Rechner meist wuppen. Unser Rezept für eine beschleunigte Grundinstallation zeigt, wie Sie mit Hyper-V eine VM mit einer Server-Core-Installation mit aktiver WSUS-Rolle einrichten (mit anderen Virtualisierungslösungen geht das ähnlich). Diesen WSUS lassen sie die Update-Kataloge verwalten, aber keine Updates zwischenspeichern.

Besorgen Sie sich dazu bei Microsoft entweder eine Eval-Version des Windows Server 2012 R2 (die dürfen Sie 180 Tage ausprobieren) oder die dritte Preview des kommenden Windows Server 2016 (läuft bis Juli 2016). Beide Downloads erfordern eine Registrierung bei Microsoft (siehe c’t-Link am Ende des Artikels). Laden Sie die ISO-Datei zur Installation herunter. VHD-Dateien, die theoretisch Zeit während des Einrichtens sparen, verlängern aufgrund der Größe die Downloadzeit und verschwenden Ressourcen, weil sie stets vollwertige Server mit Desktop-Umgebung enthalten.

Richten Sie eine virtuelle Maschine ein. Geben Sie Ihr 1 GByte Hauptspeicher, begrenzen Sie unbedingt den „Dynamischen Arbeitsspeicher“ nach oben (die WSUS-Datenbank „frisst“ RAM), verbinden Sie die ISO-Datei mit der VM und lassen Sie die Installation anlaufen. Die virtuelle Platte sollte 32 GByte groß sein, wird bei der empfohlenen Nutzung ohne Update-Cache aber nur einen Bruchteil belegen (zirka 8 GByte). Wenn das Setup-Programm rückfragt, wählen Sie die Variante Core beziehungsweise die Desktop-lose Installation.

Nach erfolgreicher Installation melden Sie sich an der VM an. In der Eingabeaufforderung startet `notepad` den Editor, den Sie via Zwischenablage mit kurzen Skripten füttern können. Starten Sie mit `start powershell` ein weiteres Fenster, um darin Powershell-Befehle ausführen zu können. Dort können Sie die im Hauptartikel erklärten Befehle einsetzen, um die Firewall auf ein vertrauenswürdiges Netz einzuschwören und gegebenenfalls die Passwort-Policy auf einen weniger pingeligen Standard abzusenken.

In der Eingabeaufforderung können Sie anschließend mit `sconfig` die Konfigurationshilfe für Core-Server starten [2]. Aktivieren Sie dort die automatischen Updates, erlauben Sie Verbindungen per Remotedesktop und fügen Sie einen lokalen Administrator hinzu, dessen Benutzername und Passwort identisch mit dem Konto sind, das Sie zur Anmeldung an Ihren Windows-10-PC verwenden (Hintergrund dazu im Hauptartikel).

Die virtuelle Maschine mit dem Core-Server sollte eine Verbindung zum Internet haben. Das erreichen Sie, indem Sie in Hyper-V einen virtuellen Switch des Typs „extern“ erstellen und die Netzwerkkarte der VM diesem Switch zuweisen. Sie sollten der zukünftigen Update-Bremse/WSUS-VM eine feste IP-Adresse zuweisen, damit sich die nicht durch äußere Umstände ändern kann. Dabei hilft `sconfig`.

Verbinden Sie sich anschließend per Remote Desktop auf die WSUS-VM (so fällt es leichter, längere Skript-Dateien per Copy & Paste vom Wirt in die VM zu übertragen). Laden Sie über den c’t-Link unser Powershell-Skript herunter, speichern Sie es in der VM als als mywsus.ps1 und führen es in der Eingabeaufforderung aus:

```
powershell -ep RemoteSigned -file mywsus.ps1
```

Das Skript richtet in der VM einen WSUS-Server ein. Der ist am Ende so vorkonfiguriert, dass er sich für alle Updates für Windows 10, Security Essentials und Signatur-Updates zuständig fühlt. Der ganze Prozess dauert rund 20 Minuten, bis der erste Abgleich mit Windows Update durchgelaufen ist. Sie können diesen WSUS-Server wie im Haupttext beschrieben nutzen und verwalten.

Wir haben bewusst keine Vorgaben für eine regelmäßige Update-Prüfung gesetzt und keine Regeln zur automatischen Genehmigung von Updates vorgegeben oder Gruppen für Computer eingerichtet. Das heißt, dass Sie das selbst, auf Ihre individuellen Bedürfnisse abgestimmt, erledigen müssen. Vorher prüft Ihr persönlicher WSUS nicht auf neue Updates und liefert auch keine Updates aus.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover