Peter Siering

Kant-en-klaar

Windows-updates regelen via WSUS

De Windows Server Update Services (WSUS) zijn de officiële manier van Microsoft om updates los van de normale Windows Update binnen te halen, te doseren en te verdelen als je geen complexe en dure tools wilt gebruiken. Je kunt de benodigde server via trucs omzeilen.

WSUS werkt als een cache: de dienst downloadt de updatebestanden van Microsoft zodat systemen in je lokale netwerk geen contact hoeven maken met de server van Microsoft. Dat scheelt bandbreedte, maar het heeft ook andere voordelen. Via regels kun je gedetailleerd instellen welke updates de pc's krijgen vanuit WSUS en wanneer ze worden geïnstalleerd. Zo kun je signature-updates direct doorsturen naar de clients, veiligheidsupdates en belangrijke updates met twee dagen vertraging installeren en de rest pas na twee weken.

WSUS heeft een Windows-server nodig. In de huidige versie van Windows Server 2012 R2 zit WSUS geïntegreerd. Normaliter stelt zo'n server voor je lokale netwerk een Active Directory en andere diensten beschikbaar (bijvoorbeeld bij de Essentials- of SBS-versie). In dat geval is het instellen niet zo moeilijk. Maar ook zonder Active Directory binnen een Workgroup kun je een WSUS in gebruik nemen. We gaan in op de benodigde tips voor het gebruik in een Workgroup en het kader 'Instant WSUS' op de laatste pagina geeft een stappenplan om in een virtuele machine een Windows 10-updateremmer in te stellen.

Als je met WSUS aan de slag wilt, gebruik je in het ideale geval Windows Server 2012 R2 (maar het werkt ook vanaf Server 2008). Niet elke versie is geschikt: Standard, Datacenter en Essentials zijn prima, Foundation, Storage en Hyper-V niet. Maar let wel goed op: de licentievoorwaarden van Microsoft vereisen dat zodra een client door een server wordt herkend of geauthentificeerd, er een CAL (Client Access License) aanwezig moet zijn. Aangezien WSUS clients herkent, heeft

elke client dus een CAL nodig. Veel speelruimte voor creatieve uitzonderingen is er niet (zie het kader 'Instant-WSUS').

Waar te beginnen

De handmatige installatie van WSUS als rol op een server met grafische interface vereist niet alleen geduld, maar ook ontzettend veel muiskliken. De drie etappes zijn dankzij de wizard echter foolproof: de WSUS-rol toevoegen, basisconfiguratie instellen en de eerste instellingen doorlopen. De wizards vragen je om de benodigde gegevens.

Als je je aan de instructies houdt, ben je er zo doorheen. Je kunt het pad aangeven naar de map waar de updatebestanden in terecht moeten komen. Je hoeft deze map niet zelf aan te maken. Het is aan te raden om er eentje die kiezen die niet op de systeemschijf staat. Zodra een WSUS-server niet alleen de informatie over updates verzamelt maar ook zelf cache moet spelen, neemt die map al vrij snel veel ruimte in. Als je de updates lokaal mirrort, gaan talen een rol spelen. Door de taalkeuze te beperken, bespaar je ruimte.

Een WSUS-server die net is ingesteld en de eerste keer de beschikbare updates bij Microsoft ophaalt, is wel een aardig tijdje bezig, terwijl hij eerst alleen de metadata ophaalt. Het is verstandig om de keuze aan Producten te beperken tot datgene wat je echt nodig hebt. Blijf vooral weg bij Classificaties. Het is verleidelijk om flink te snoeien in deze updatecategorie (veiligheidsupdates, feature packs, drivers e.d.), maar dan loop je het gevaar dat clients updates gaan missen. Want updates die een WSUS niet aanbiedt, bestaan voor zijn clients niet.

Een basis-WSUS-installatie verdeelt standaard geen updates (in complete pakketten zoals bij de Small Business Server ligt dat anders). Om ervoor te zorgen dat dit gebeurt, heb je een aantal dingen nodig. De beheerder moet regels opgeven waarmee de WSUS updates goedkeurt, oftewel updates automatisch doorgeeft aan de clients. Het is nuttig om computers die de updates moeten krijgen in groepen te plaatsen, en daar regels aan te knopen. Regels zijn de enige zinnige manier om updates te doseren.

WSUS voor Workgroups

Om te zorgen dat de in de Windows-clients en -servers aanwezige functies niet bij officiële Microsoft-diensten naar updates vragen, maar daar een lokale WSUS-server voor gebruiken, moet je ze goed configureren. In een netwerk met Active Directory kun je de locatie van een WSUS via de Group Policy (Groepsbeleid) doorgeven aan de systemen binnen het netwerk. Complete serverpakketten zoals een SBS doen dat meestal zonder dat je daarvoor iets hoeft te doen.

Je kunt WSUS echter ook zonder een Active Directory gebruiken. In plaats van de in de Group Policy aangepaste instellingen zelf in het Windows-register in te voeren, is daar kant-en-klare software voor: de WSUS Client-Manager for Workgroups. Deze tool is via Codeplex gratis te downloaden (zie de link aan het eind).

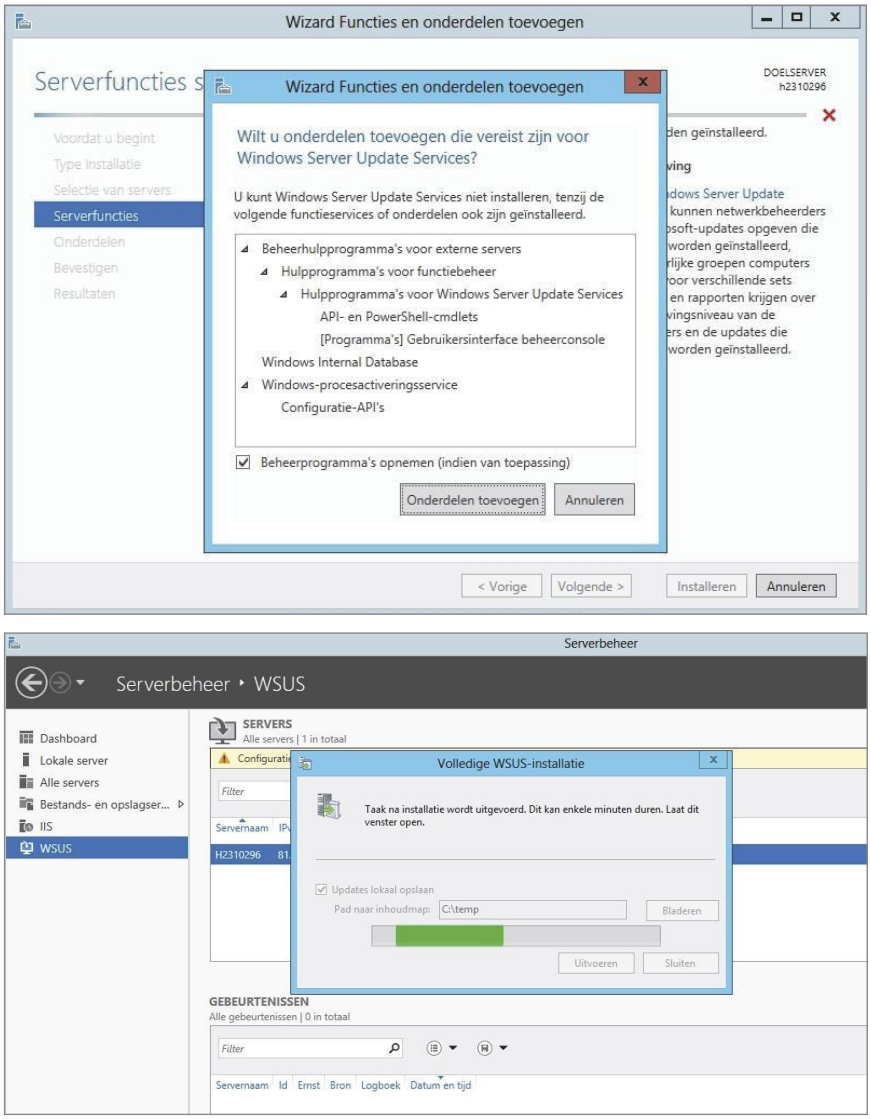
De software gaat zeer voorzichtig te werk. Voordat je veranderingen naar het register wegschrijft, wordt de betreffende sleutel in een bestand opgeslagen, zodat je altijd weer terug kunt naar de oude situatie. Het biedt allerlei opties om de updateclient in Windows te beïnvloeden en heeft ook invloed op verdere details zoals het registreren bij de WSUS. Het exporteren van alle instellingen als .reg-bestand maakt het plaatje compleet. Dit is handig om in één keer op veel systemen de instellingen toe te passen.

Over het algemeen is het voldoende om in het veld WSUS-server het IP-adres of de naam van de WSUS-server in te vullen. Zodra de client voor het eerst contact maakt met de WSUS-server wordt deze geregistreerd. Dat hij als pc wordt gemanaged zorgt dat je zeker weet dat de beide kanten met elkaar in contact staan. Nu kun je de pc op de WSUS-server in een groep opnemen waarvoor al regels staan ingesteld, en komen de updates via je eigen WSUS-server binnen.

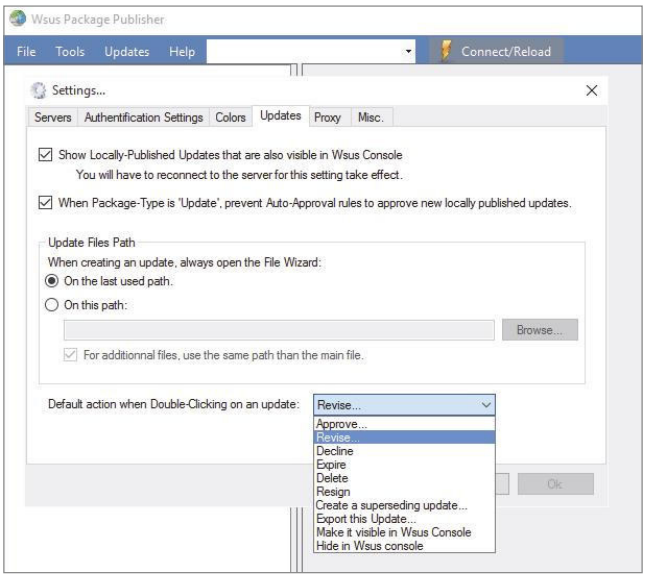
Core-WSUS

Zolang WSUS draait op een volwaardige server met desktopomgeving, kun je deze bedienen via de meegeleverde Management Console (MMC). Draait hij echter op een Core-installatie, dan moet de configuratie gebeuren via een client in het netwerk. Op deze client installeer je de Remote Server Administration Tools (RSAT), die je gratis kunt downloaden bij Microsoft (zie de link aan het eind). Voor RSAT heb je een Pro-versie van Windows nodig.

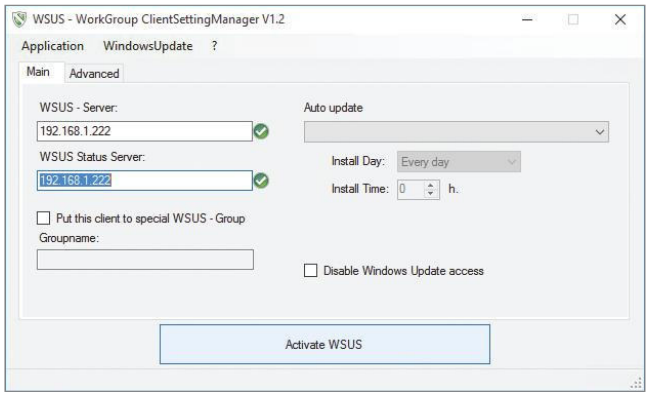
Voor Windows 10 is er alleen een Engelstalige versie van RSAT. Om deze te installeren op een Nederlandse Windows, moet je het taalpakket voor Engels (Verenigde Staten)



Het installeren van de WSUS verloopt in een paar stappen. Je begint met het toevoegen van rollen, daarna regel je basisconfiguratie en de details via de WSUS-manager.



Met de Wsus Package Publisher kun je losse MSI-, MSP- of EXE-bestanden via een WSUS laten uitrollen.



WSUS is ook zonder Active Directory te regelen door de gratis WSUS ClientManager for Workgroups te gebruiken.

toevoegen. Dat houdt in dat binnen de Instellingen onder 'Land of regio' staat aangegeven dat het taalpakket is geïnstalleerd. Nadat je het taalpakket hebt toegevoegd, moet je wel bij de opties nog op Downloaden klikken om het taalpakket daadwerkelijk te installeren.

RSAT is een los updatepakket (.msu-bestand). Het breidt de lijst met Windows-features uit die via het Configuratiescherm onder Programma's beschikbaar is. Als de installatie is gelukt, duiken de in RSAT gestopte tools op in het startmenu onder de groep Windows Systeembeheer.

Core-WSUS voor Workgroups

Als je in een Active Directory op de beheerde pc als administrator bent aangemeld, kun je zonder problemen de WSUS beheren via de Windows Server Update Services-MMC. Indien nodig voeg je de WSUS-server via een rechtermuisklik toe aan de console. Als dat niet lukt, controleer dan of je daadwerkelijk als admin bent aangemeld op het domein.

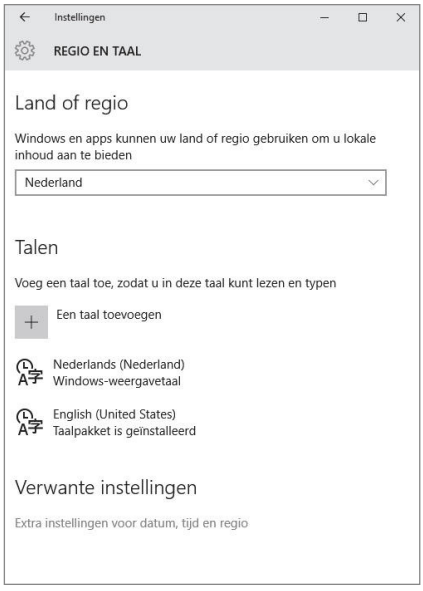
In een Workgroup zonder centrale user-database helpt de onderstaande truc om succesvol met de WSUS-server te verbinden: stel op de server een account met administratorrechten in, waarbij de gebruikersnaam en wachtwoord gelijk zijn aan de inloggegevens die op de lokale pc worden gebruikt. De MMC leidt de lokale aanmeldgegevens door naar de WSUS-server: als ze identiek zijn, kun je succesvol een verbinding maken.

Hier zit een nadeel aan: Windows-servers stellen hoge eisen aan wachtwoorden. Het aanmaken van een identiek account met administratorrechten op de server kan mislukken omdat het wachtwoord niet sterk genoeg is. Met het volgende combinatie van Powershell en Secedit (als bestand te downloaden via de link aan het eind) zorg je dat de server hier niet meer over kan struikelen:

```
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
```

Als je het script in een map als passpol.ps1 opgeslagen wordt, voert het het volgende commando uit:

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



RSAT voor Windows 10 vereist dat het taalpakket Engels (Verenigde Staten) ook daadwerkelijk is geïnstalleerd.

Daarna accepteert de server ook eenvoudige wachtwoorden. Uit veiligheidsoogpunt is het natuurlijk beter om ook op de client een sterker wachtwoord te gebruiken.

Als de server na het toevoegen aan de MMC nog steeds niet opduikt, dan zitten mogelijk de firewallregels voor privé/openbare netwerken in de weg. Als dit nog niet goed staat, kun je dat met het volgende commando in een Powershell alsnog regelen:

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

Wanneer er meerdere netwerkkaarten in de server zitten, kun je dat commando herhalen: `Get-NetAdapter` toont een lijst met de netwerkkaarten. Let wel op: je met veel pijn en moeite ingestelde firewallregels kunnen daardoor van slag raken.

Waar het fout kan gaan

Er zijn twee nadelen die we niet gaan verbloemen: als WSUS in een Workgroup draait, oftewel zonder een Active Directory op de achtergrond, dan biedt het zijn diensten alleen onversleuteld aan. Het moet mogelijk zijn om de achterliggende IIS-configuratie van certificaten te voorzien, maar vooral bij een Core-installatie is dat niet iets wat je 'even' kunt regelen. We hebben het er daarom maar bij gelaten.

Het tweede nadeel heeft betrekking op Windows 10 Home: deze editie kan niet communiceren met een WSUS-server. Dat is voorbehouden aan Pro, Enterprise en Education. Microsoft heeft de functie in Home moedwillig de nek omgedraaid. Home-edities van oudere versies van Windows kunnen wel contact maken met een WSUS als je ze bijvoorbeeld via de WSUS ClientManager for Workgroups daarvoor instelt.

Bij een upgrade naar Windows 10 Home vanuit Windows 8.1 Core, die ingesteld is voor het verkrijgen van updates via WSUS, schakelt de pc weer om naar de officiële updatediensten van Microsoft. De WSUS-console van Server 2012 R2 duidt Windows 10 aan als Vista, maar dat is slechts een cosmetisch probleem. WSUS in Server 2016 laat wel de juiste naam van de client zien.

Mocht het ombouwen van lokale updates naar WSUS toch niet werken, dan kan er een nog openstaande update dwarsliggen. Zodra op zo'n systeem de al gedownloade updates geïnstalleerd zijn, duikt het als pc in de WSUS-configuratie op. Antwoordt een geconfigureerde WSUS-server niet, dan meldt Windows op de client dat het geen updates kan binnenhalen en raadt aan om je internetverbinding te controleren. Dit ondanks dat de WSUS in het lokale netwerk staat.

In de instellingen van Windows 10 vind je op de hoofdpagina van de update-opties de checkbox om online naar updates van Microsoft Update te zoeken. Als deze geactiveerd is, stuurt de updateclient je eenmalig niet naar de eventueel ingestelde WSUS-server, maar kijkt bij Microsoft of er nog updates zijn. Dat is handig om voor Windows 10-clients gekoppeld aan de WSUS na te gaan of alles wat relevant is ook wordt aangeboden.

Speling

WSUS maakt het een administrator op een ander punt ook een stuk makkelijker: de dienst levert informatie over de staat van de updates van de geregistreerde clients. Zo kun je problemen met updates of clients die updates weigeren herkennen. Als je wilt, kun je WSUS zo instellen dat je een e-mail krijgt zodra er nieuwe updates zijn. De WSUS-console biedt ook diverse analyses, maar daarvoor heb je extra pakketten nodig (zie de link hier onder).

WSUS geeft je als beheerder veel vrijheid over hoe je het uitrollen van updates regelt. Tips voor optimale regels zijn lastig te geven. Twee dingen zijn echter erg belangrijk: de beheerder moet (vooral als WSUS de updates lokaal opslaat) regelmatig de interne databases laten opschonen. Dit doe je via de Cleanup Wizard. Een Powershell-script kan handig zijn om dit te automatiseren (commando Invoke-WsusServerCleanup).

Het tweede belangrijke punt is het monitoren. Als je clients toegang biedt tot een WSUS-server, moet je niet alleen zorgen dat de WSUS blijft draaien, maar ook dat hij alle relevante updates kan aanbieden. Als de beheerder vergeet een product aan te vinken in de configuratie, denken de systemen die aan de WSUS hangen dat alles bijgewerkt is, terwijl ze al maanden geen beveiligingsupdates meer hebben geïnstalleerd. Dat kan fatale gevolgen hebben. Het enige wat je kunt doen om dit te voorkomen is goed opletten bij het instellen. (avs)

Literatuur

[1] Windows Update Services: Client-Server Protocol: https://msdn.microsoft.com/en-us/library/cc251937.aspx
[2] Peter Siering, Kerntaken, Windows Server als Core-Installatie, c't 12/2013, p. 120
[3] Wsus Package Publisher, MSI-, MSP- of EXE-bestanden via WSUS uitrollen: https://wsuspackagepublisher.codeplex.com

www.ct.nl/softlink/1512052

Instant-WSUS Update-remmer voor Windows 10

Om WSUS als updateremmer voor Windows 10 Pro in te stellen, heb je geen fysieke server nodig. Elke moderne pc kan zonder problemen een virtuele machine draaien. Ons recept voor een versnelde basisinstallatie laat zien hoe je met Hyper-V een virtuele machine met een server-Core-installatie met actieve WSUS-rol kunt instellen. Met andere virtualisatie-oplossingen werkt het op een vergelijkbare manier. Deze WSUS laat je de update-catalogus beheren, maar je laat hem geen updates cachen.

Download via Microsoft een evaluatieversie van Windows Server 2012 R2 (die kun je 180 dagen uitproberen) of de derde preview van de aankomende Windows Server 2016, die draait tot juli 2016. Voor beide downloads moet je je registreren bij Microsoft. De links voor de beide evaluatieversies staan bij de link op deze pagina. Haal het ISO-bestand binnen om mee te installeren. VHD-bestanden, die je in theorie tijd besparen bij het inrichten, kosten je veel meer tijd om te downloaden en verspillen onnodige resources omdat ze een volledige server met grafische interface bevatten.

Maak een virtuele machine aan. Geef hem 1 GB RAM, maar stel een maximum in voor de hoeveelheid dynamisch geheugen (de WSUS-database 'vreet' geheugen). Koppel de ISO aan de virtuele machine en laat de installatie draaien. De virtuele schijf moet 32 GB aan ruimte hebben, maar er wordt bij de aanbevolen instellingen zonder update-cache echter maar een klein deel van gebruikt (ongeveer 8 GB). Zodra het set-upprogramma het vraagt, geef je aan de Core-versie of versie zonder desktop te willen gebruiken.

Nadat de installatie succesvol is afgerond meld je jezelf aan in de virtuele machine. Via de Opdrachtprompt start je met `notepad` de editor die je via het klembord met korte scripts kunt voeren. Start via `start powershell` een extra venster, zodat je er Powershell-commando's kunt intypen. Daar kun je de in het artikel besproken commando's invoeren om de firewall duidelijk te maken dat het om een vertrouwd netwerk gaat en het wachtwoordbeleid een stukje minder streng instellen.

Via de Opdrachtprompt kun je daarna met `sconfig` het hulpprogramma voor de configuratie van de Core-server opstarten [2]. Activeer daar de automatische updates, sta het verbinden via remote desktop toe en voeg een lokale administrator toe, waarbij de gebruikersnaam en wachtwoord gelijk zijn aan het account dat je gebruikt om op je lokale Windows 10-pc in te loggen (meer achtergrondinformatie daarover staat in het hoofdartikel).

De virtuele machine met de Core-server moet een verbinding met internet hebben. Daarvoor maak je in Hyper-V een virtuele switch van het type extern aan en wijs je daar de netwerkkaart van de virtuele machine aan toe. Geef de toekomstige updateremmer/WSUS-machine een vast IP-adres, waardoor deze niet onverhoopt wordt aangepast. Je kunt daarvoor `sconfig` gebruiken.

Maak daarna via Remote Desktop verbinding met de WSUS-machine. Hierdoor is het wat makkelijker om langere scripts en bestanden vanaf je pc via copy&paste naar de virtuele machine over te zetten. Download via de link aan het eind van het artikel ons Powershell-script en sla dat op in de virtuele machine als mywsus.ps1 en voer het uit via de Opdrachtprompt:

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

Het script stelt in de virtuele machine een WSUS-server in. Deze is uiteindelijk zo geconfigureerd dat hij zelfstandig de updates voor Windows 10 Security Essentials en signature-updates regelt. Het duurt ongeveer 20 minuten voordat de eerste vergelijking met wat beschikbaar is via Windows Update is afgerond. Je kunt deze WSUS-server gebruiken en beheren zoals beschreven in het hoofdartikel.

We hebben bewust geen instructies ingesteld voor het regelmatig controleren op updates en het automatisch goedkeuren ervan of groepen voor computers ingericht. Dit zul je dus zelf moeten doen op basis van je eigen persoonlijke situatie. Pas als je dat hebt ingesteld, controleert de WSUS of er nieuwe updates zijn en rolt hij ze uit naar je pc's. c't