Inhalt

Zielsetzung

IST-Situation

Meine Windows Infrastruktur soll auf Windows Server 2019 aktualisiert werden. Nur noch zwei Server sind mit Windows Server 2016 unterwegs. Einer davon ist mein Server WS-CM. Auf ihm läuft mein Windows Server Update Service (WSUS) und mein Windows Deployment Service (WDS)

Der WSUS hat derzeit Updates für Windows Server 2016 und 2019 geladen. Er braucht also recht viel Platz. Der WDS hat ebenfalls einige Betriebssysteme im Katalog, die ich nicht mehr benötige.

SOLL-Situation

Der Service WSUS muss unbedingt weiter betrieben werden. Idealerweise natürlich nur noch mit Updates für Windows Server 2019 und mein Windows 10. Natürlich könnte ich den Service auf einen neuen Server portieren, aber durch eine Neuinstallation kann ich nur noch die erforderlichen Produkte im WSUS hinzufügen und einfach alles neu herunterladen lassen. Und auch die ganzen Server und Clients melden sich wieder im WSUS – dank der Gruppenrichtlinien.

Wenn ich also einfach einen neuen Server für WSUS installiere, dann kann ich eine gute Bereinigung durchführen. Aber was ist dann mit dem Service WDS? Derzeit habe ich für ihn keine Verwendung mehr. Und sollte ich ihn dennoch wieder benötigen, dann würde ich ihn gerne auf einem anderen Windows Server betreiben. Damit könnte ich den alten Server WS-CM einfach abschalten und einen WS-WSUS und optional einen WS-WDS neu installieren.

Migrationsszenario

Und genau das wird mein Migrationsszenario: Es wird bis auf die Scriptlogik keine Datenübernahme geben. Der alte Server WS-CM wird abgeschaltet und ich installiere heute einen neuen WS-WSUS. Dort werde ich auch das Layout des WSUS etwas anpassen.

Und später werde ich bei Bedarf einen WS-WDS bereitstellen.

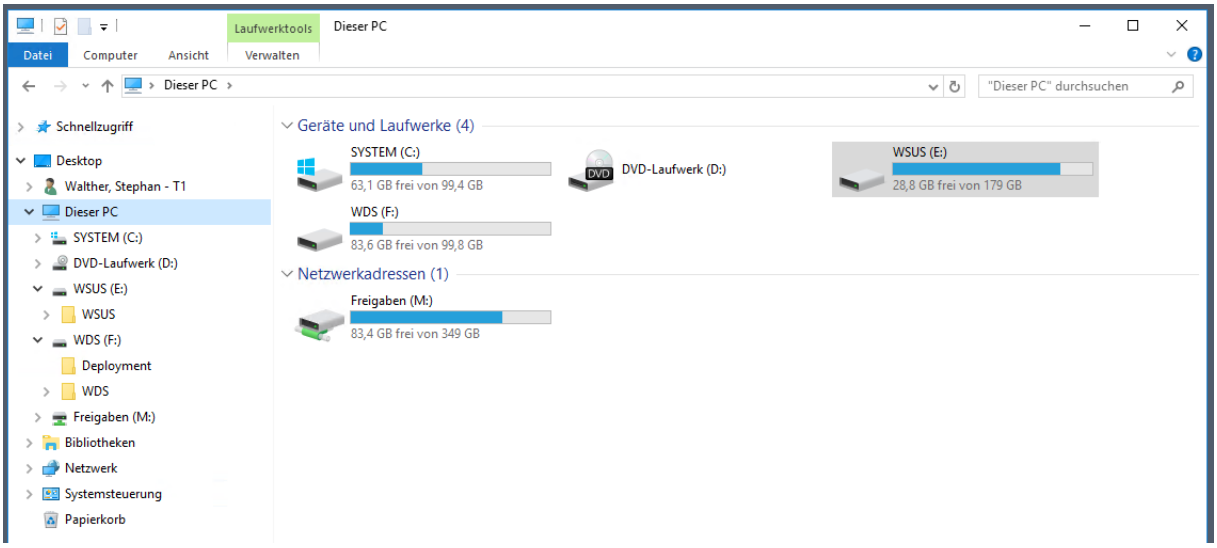
Vorarbeiten

Sichtung der Basisinfos

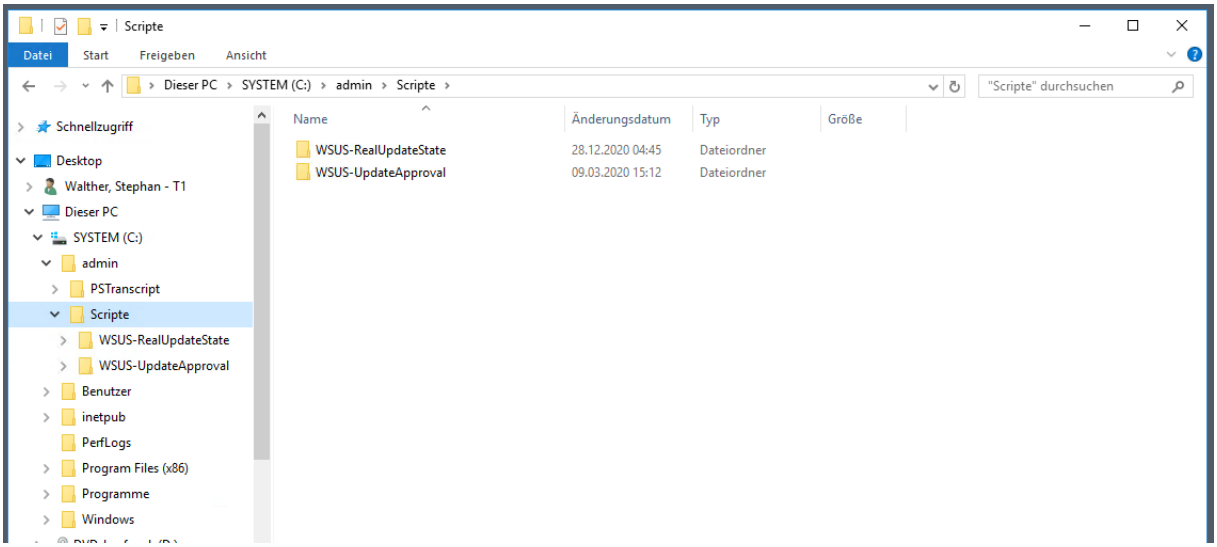
Für eine Neuinstallation sammle ich erst einmal einige Daten. Der aktuelle Server hat eine IPv4 in meinem Servernetz. An dieser hängt die Freigabe in meiner Firewall für die WSUS-Netzwerkverbindungen. Die IPv4 gebe ich später dem neuen Server:

```
PS C:\Users\stephan-ad> ipconfig /all

Windows-IP-Konfiguration

   Hostname  . . . . . . . . . . . . : WS-CM
   Prim„res DNS-Suffix . . . . . . . : ws.its
   Knotentyp . . . . . . . . . . . . : Peer-Peer
   IP-Routing aktiviert  . . . . . . : Nein
   WINS-Proxy aktiviert  . . . . . . : Nein
   DNS-Suffixsuchliste . . . . . . . : ws.its

Ethernet-Adapter Ethernet:

   Verbindungsspezifisches DNS-Suffix:
   Beschreibung. . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physische Adresse . . . . . . . . : 00-15-5D-F9-A7-11
   DHCP aktiviert. . . . . . . . . . : Nein
   Autokonfiguration aktiviert . . . : Ja
   Verbindungslokale IPv6-Adresse  . : fe80::a86a:6300:131b:a28e%2(Bevorzugt)
   IPv4-Adresse  . . . . . . . . . . : 192.168.100.4(Bevorzugt)
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . : 192.168.100.252
   DHCPv6-IAID . . . . . . . . . . . : 50337117
   DHCPv6-Client-DUID. . . . . . . . : 00-01-00-01-26-18-04-F8-00-15-5D-F9-A7-11
   DNS-Server  . . . . . . . . . . . : 192.168.100.2
                                       192.168.100.1
   NetBIOS ber TCP/IP . . . . . . . : Aktiviert

Tunneladapter isatap.{067D5D53-2107-4551-9430-A7E122416A3F}:

   Medienstatus. . . . . . . . . . . : Medium getrennt
   Verbindungsspezifisches DNS-Suffix:
   Beschreibung. . . . . . . . . . . : Microsoft ISATAP Adapter #2
   Physische Adresse . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP aktiviert. . . . . . . . . . : Nein
   Autokonfiguration aktiviert . . . : Ja
```

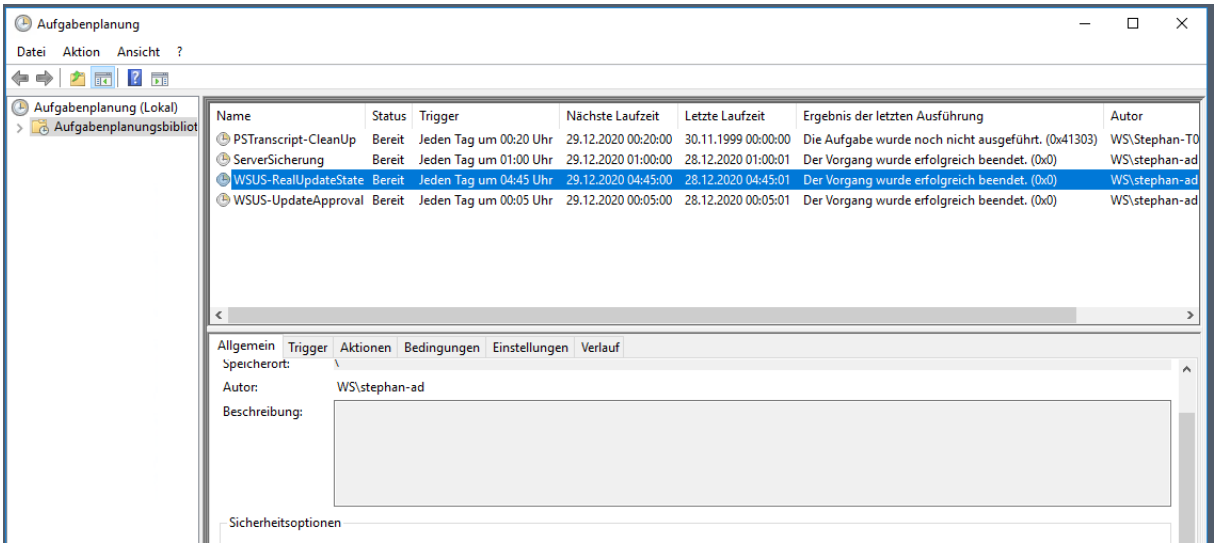
Aktuell sind für jeden der Services eine eigene VHDX-Datei im Hyper-V vorhanden. Diese sind als eigene Volumes eingebunden. Hier kann man gut den Platzbedarf ablesen und eine Ersparnis durch die Neuinstallation erahnen:



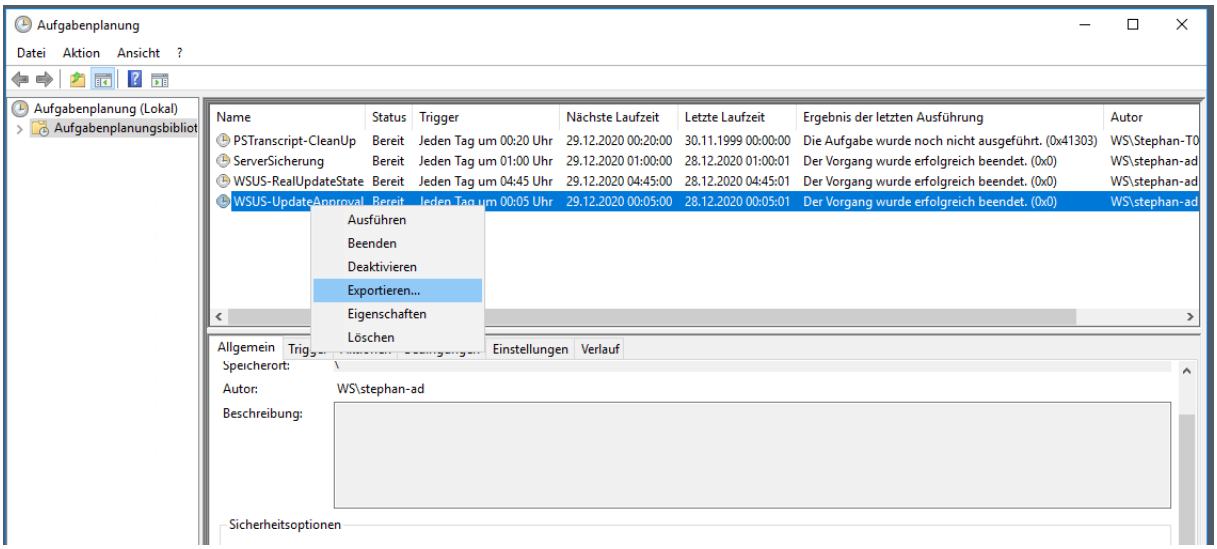
Meinen WSUS habe ich mit 2 kleinen PowerShell-Scripten verbessert. Eines ist für die tageweise Genehmigung der neuen Updates gedacht. Und das andere zeigt mir den realen Updatestand bereinigt um die noch nicht genehmigten Updates an (das schafft Microsoft bis heute nicht). Diese Scripte muss ich auf dem neuen Server wieder einspielen:

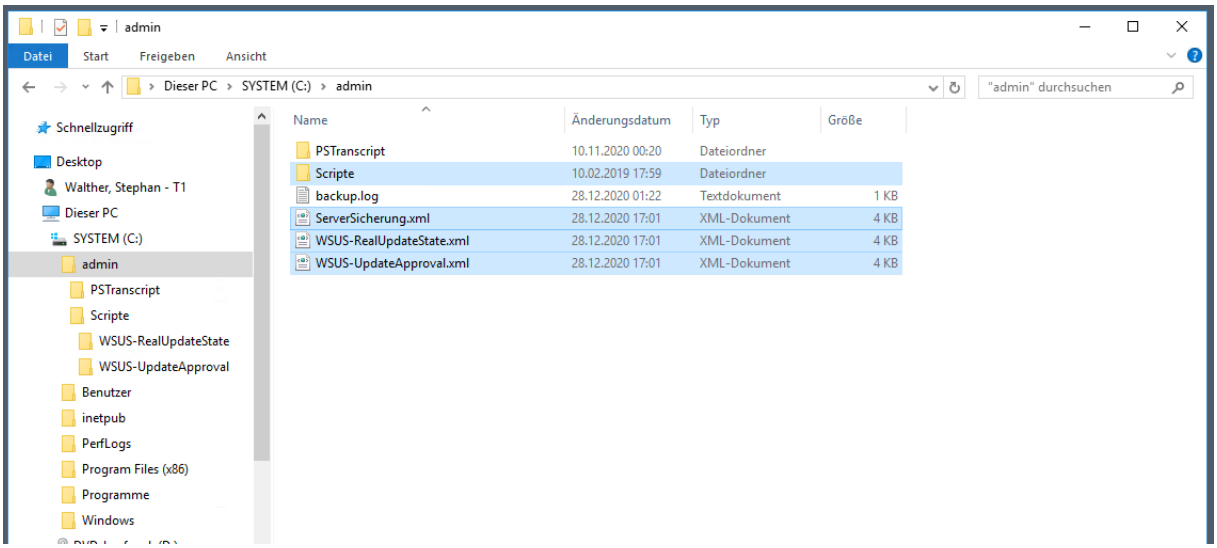


Die Scripte werden als Script-Tasks automatisch ausgeführt:

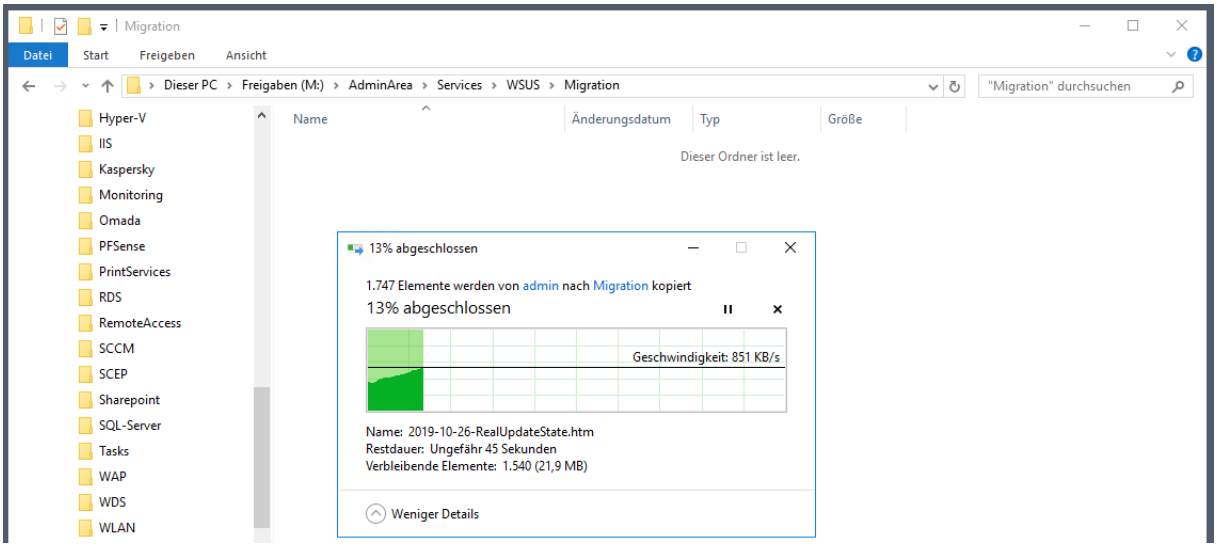


Ich exportiere hier beide Aufgaben in je eine XML-Datei. So kann ich sie auf dem neuen Server leicht wieder importieren:

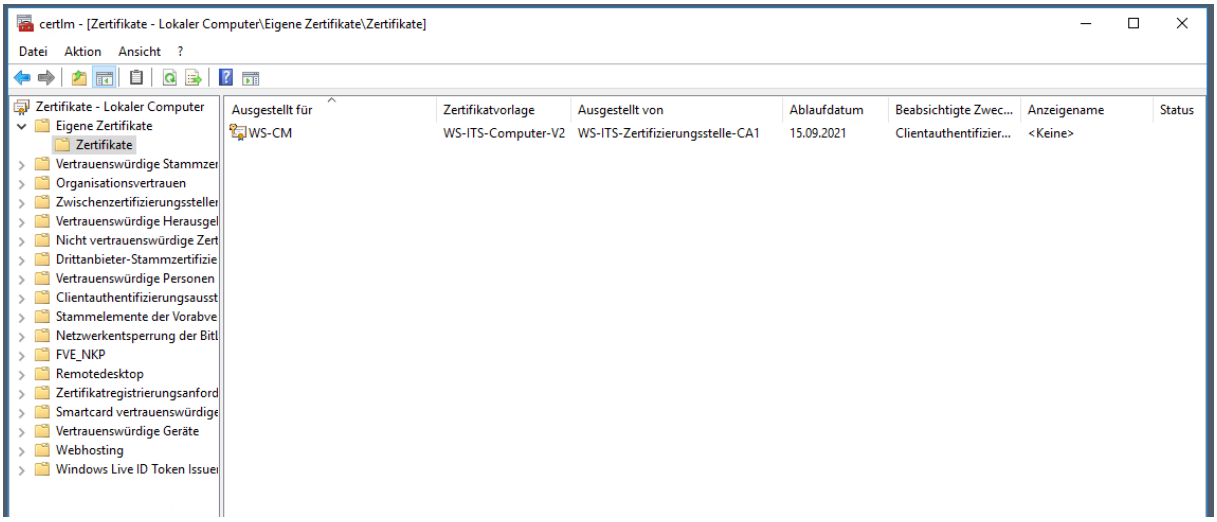




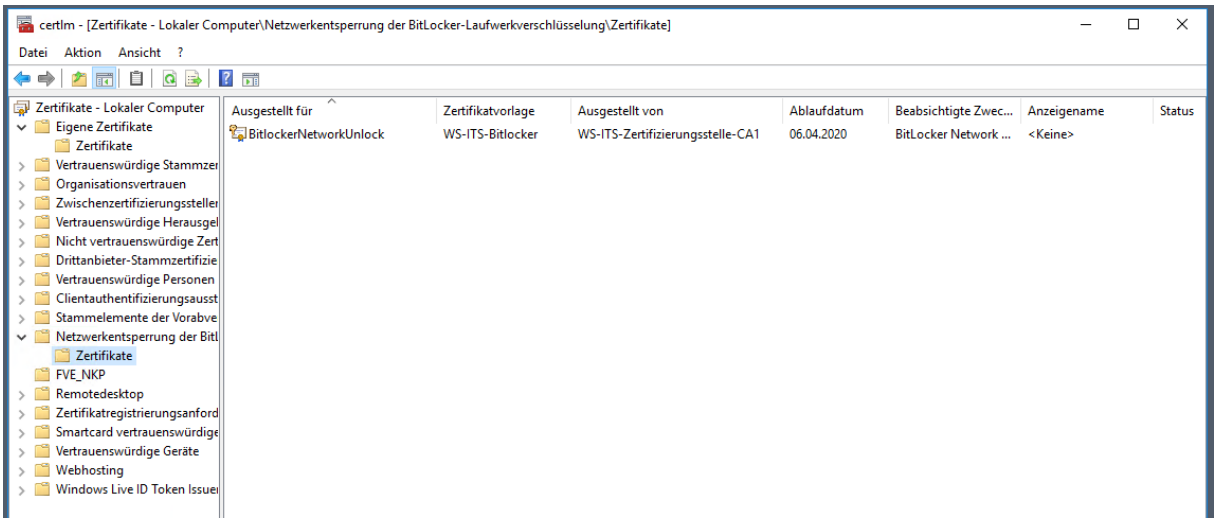
Dann kopiere ich die Scriptverzeichnisse auf mein AdminShare:



Mein WSUS kann direkt über den Standardport 8530 angesprochen werden. Daher hat er keine weiteren interessanten Zertifikate im persönlichen Speicher:



Früher hatte ich den WDS auch für einen Bitlocker-NetworkUnlock-Service verwendet. Dabei konnte ein Client über eine GPO angewiesen werden, beim Start via PXE-Boot einen WDS mit einem Sicherheitszertifikat zu suchen. Wenn er diesen findet und das Sicherheitszertifikat passt, dann war für den Bitlocker-Prozess keine Start-PIN-Eingabe erforderlich. Das Zertifikat hatte ich in einem Container erstellt:



Wie man aber erkennen kann, ist das Zertifikat seit einigen Monaten abgelaufen. Ich habe den Service deaktiviert, da er den Startprozess unangenehm lang verzögert. Da gebe ich lieber die PIN beim Hochfahren ein. Das Feature wird also nicht mehr benötigt.

Zuletzt sichte ich noch die installierten Rollen und Features. Dies gibt ggf. Aufschluss auf Services, die nicht so offensichtlich sind:

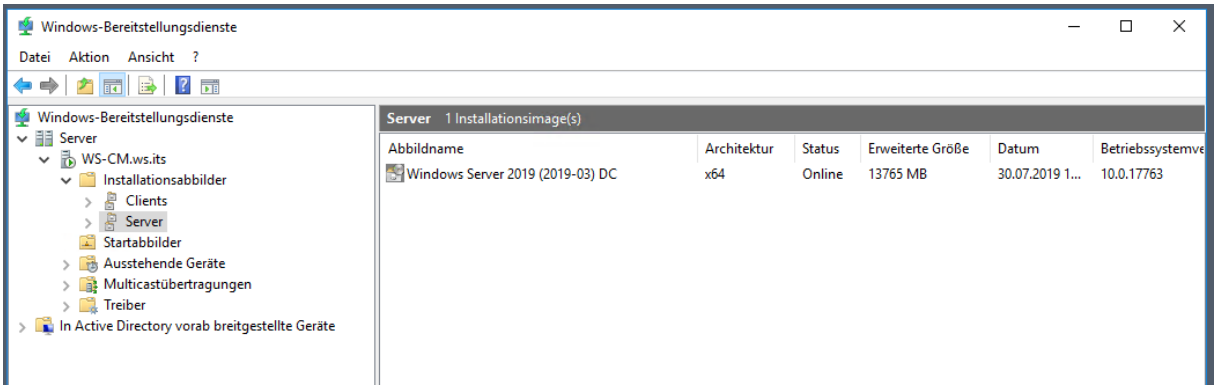
```
PS C:\Users\stephan-ad> Get-WindowsFeature | where installed

Display Name                                            Name                       Install State
------------                                            ----                       -------------
[X] Datei-/Speicherdienste                              FileAndStorage-Services        Installed
    [X] Datei- und iSCSI-Dienste                        File-Services                  Installed
        [X] Dateiserver                                 FS-FileServer                  Installed
        [X] Datendeduplizierung                         FS-Data-Deduplication          Installed
    [X] Speicherdienste                                 Storage-Services               Installed
[X] Webserver (IIS)                                     Web-Server                     Installed
    [X] Webserver                                       Web-WebServer                  Installed
        [X] Allgemeine HTTP-Features                    Web-Common-Http                Installed
            [X] Standarddokument                        Web-Default-Doc                Installed
            [X] Statischer Inhalt                       Web-Static-Content             Installed
        [X] Leistung                                    Web-Performance                Installed
            [X] Komprimieren dynamischer Inhalte        Web-Dyn-Compression            Installed
        [X] Sicherheit                                  Web-Security                   Installed
            [X] Anforderungsfilterung                   Web-Filtering                  Installed
            [X] Windows-Authentifizierung               Web-Windows-Auth               Installed
        [X] Anwendungsentwicklung                       Web-App-Dev                    Installed
            [X] .NET-Erweiterbarkeit 4.6                Web-Net-Ext45                  Installed
            [X] ASP.NET 4.6                             Web-Asp-Net45                  Installed
            [X] ISAPI-Erweiterungen                     Web-ISAPI-Ext                  Installed
            [X] ISAPI-Filter                            Web-ISAPI-Filter               Installed
    [X] Verwaltungsprogramme                            Web-Mgmt-Tools                 Installed
        [X] IIS-Verwaltungskonsole                      Web-Mgmt-Console               Installed
        [X] Kompatibilität mit der IIS 6-Verwaltung     Web-Mgmt-Compat                Installed
            [X] IIS 6-Metabasiskompatibilität           Web-Metabase                   Installed
[X] Windows Server Update Services (WSUS)               UpdateServices                 Installed
    [X] WID Connectivity                                UpdateServices-WidDB           Installed
    [X] WSUS Services                                   UpdateServices-Services        Installed
[X] Windows-Bereitstellungsdienste                      WDS                            Installed
    [X] Bereitstellungsserver                           WDS-Deployment                 Installed
    [X] Transportserver                                 WDS-Transport                  Installed
[X] .NET Framework 4.6-Funktionen                       NET-Framework-45-Fea...        Installed
    [X] .NET Framework 4.6                              NET-Framework-45-Core          Installed
    [X] ASP.NET 4.6                                     NET-Framework-45-ASPNET        Installed
    [X] WCF-Dienste                                     NET-WCF-Services45             Installed
        [X] HTTP-Aktivierung                            NET-WCF-HTTP-Activat...        Installed
        [X] TCP-Portfreigabe                            NET-WCF-TCP-PortShar...        Installed
[X] BitLocker-Netzwerkentsperrung                       BitLocker-NetworkUnlock        Installed
[X] Interne Windows-Datenbank                           Windows-Internal-Dat...        Installed
[X] Remoteserver-Verwaltungstools                       RSAT                           Installed
    [X] Rollenverwaltungstools                          RSAT-Role-Tools                Installed
        [X] Windows Server Update Services-Tools        UpdateServices-RSAT            Installed
            [X] API- und PowerShell-Cmdlets             UpdateServices-API             Installed
            [X] Benutzeroberfläche der Verwaltungsko... UpdateServices-UI              Installed
        [X] Tools für Windows-Bereitstellungsdienste    WDS-AdminPack                  Installed
[X] Unterstützung für die SMB 1.0/CIFS-Dateifreigabe    FS-SMB1                        Installed
[X] Windows Defender-Features                           Windows-Defender-Fea...        Installed
    [X] Windows Defender                                Windows-Defender               Installed
    [X] GUI für Windows Defender                        Windows-Defender-Gui           Installed
[X] Windows PowerShell                                  PowerShellRoot                 Installed
    [X] Windows PowerShell 5.1                          PowerShell                     Installed
    [X] Windows PowerShell ISE                          PowerShell-ISE                 Installed
[X] Windows Server-Sicherung                            Windows-Server-Backup          Installed
[X] Windows-Prozessaktivierungsdienst                   WAS                            Installed
    [X] Prozessmodell                                   WAS-Process-Model              Installed
    [X] Konfigurations-APIs                             WAS-Config-APIs                Installed
[X] WoW64-Unterstützung                                 WoW64-Support                  Installed
```

Sonst ist auf dem Server aber nichts weiter zu finden.

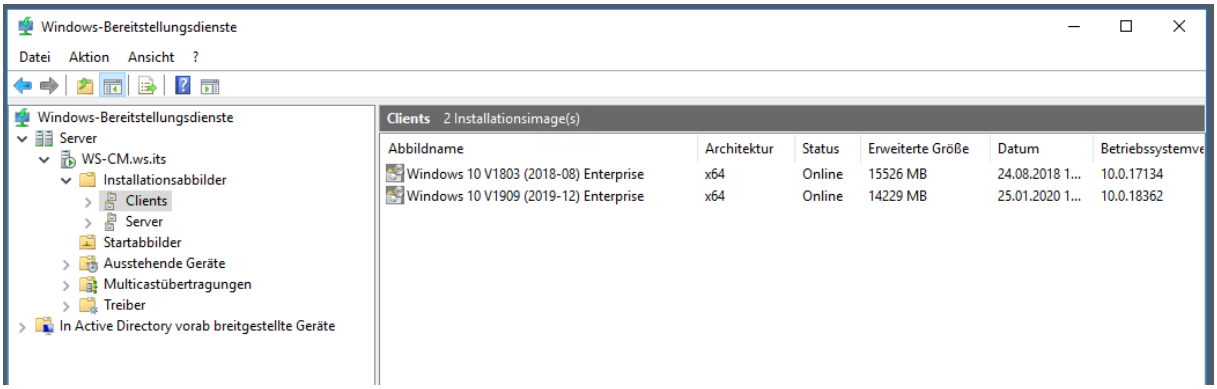
Sichtung der Rolle WDS

Ich werde heute die Rolle Windows Deployment Service nicht mit migrieren. Aber dennoch werde ich den aktuellen Stand hier dokumentieren. Das kann bei einer neuen Bereitstellung durchaus helfen.

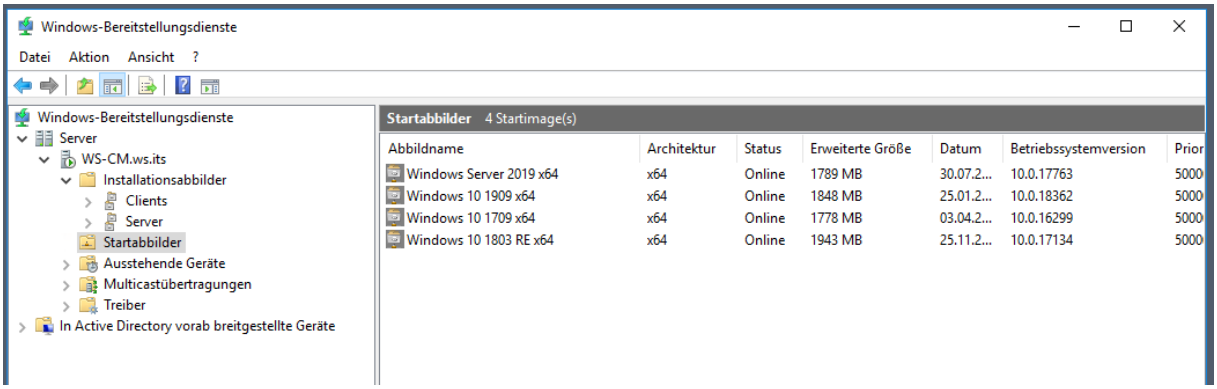
Im WDS ist ein Server-Image vorhanden. Das ist schon fast zwei Jahre alt:



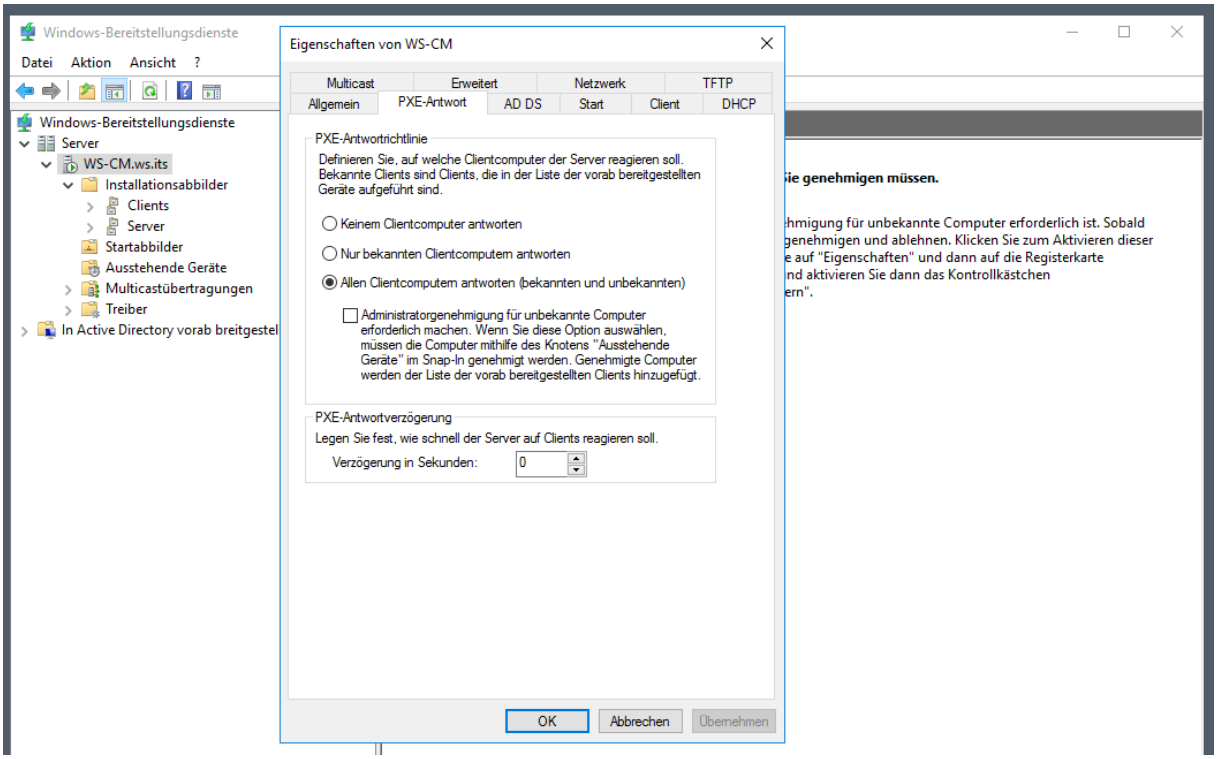
Bei den Clients sieht es nicht viel besser aus:

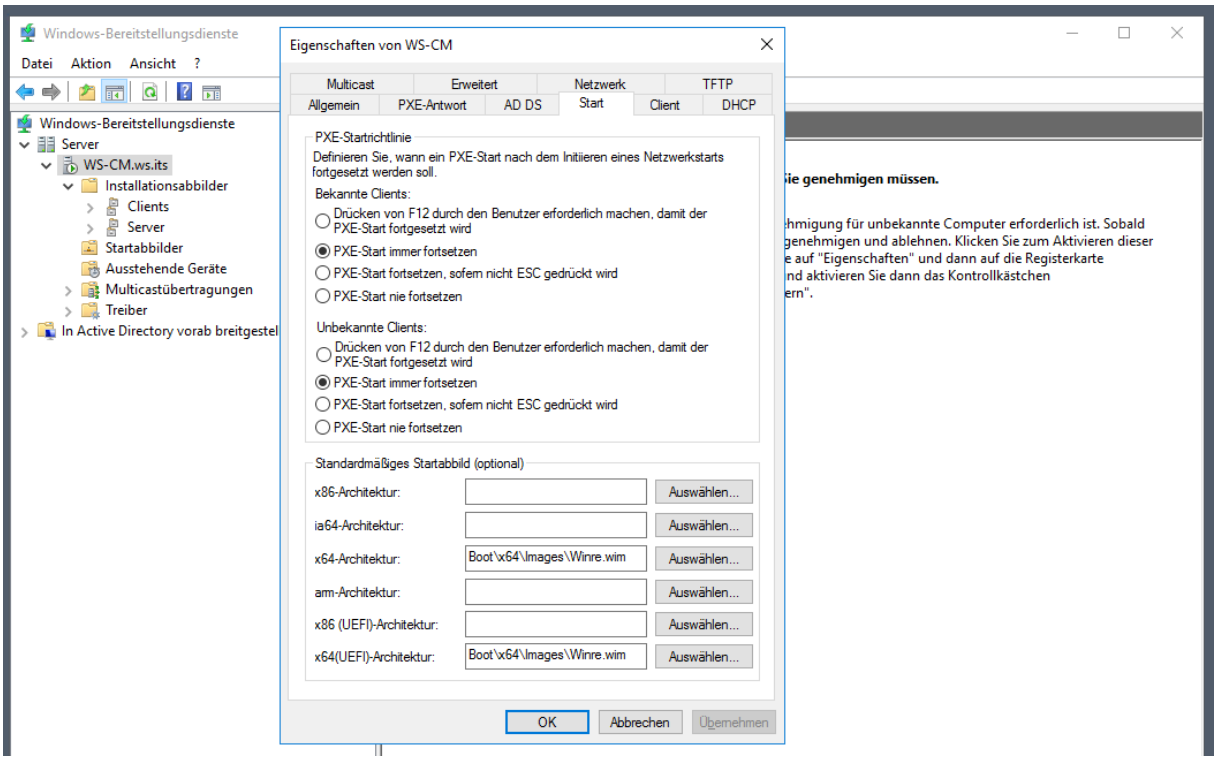


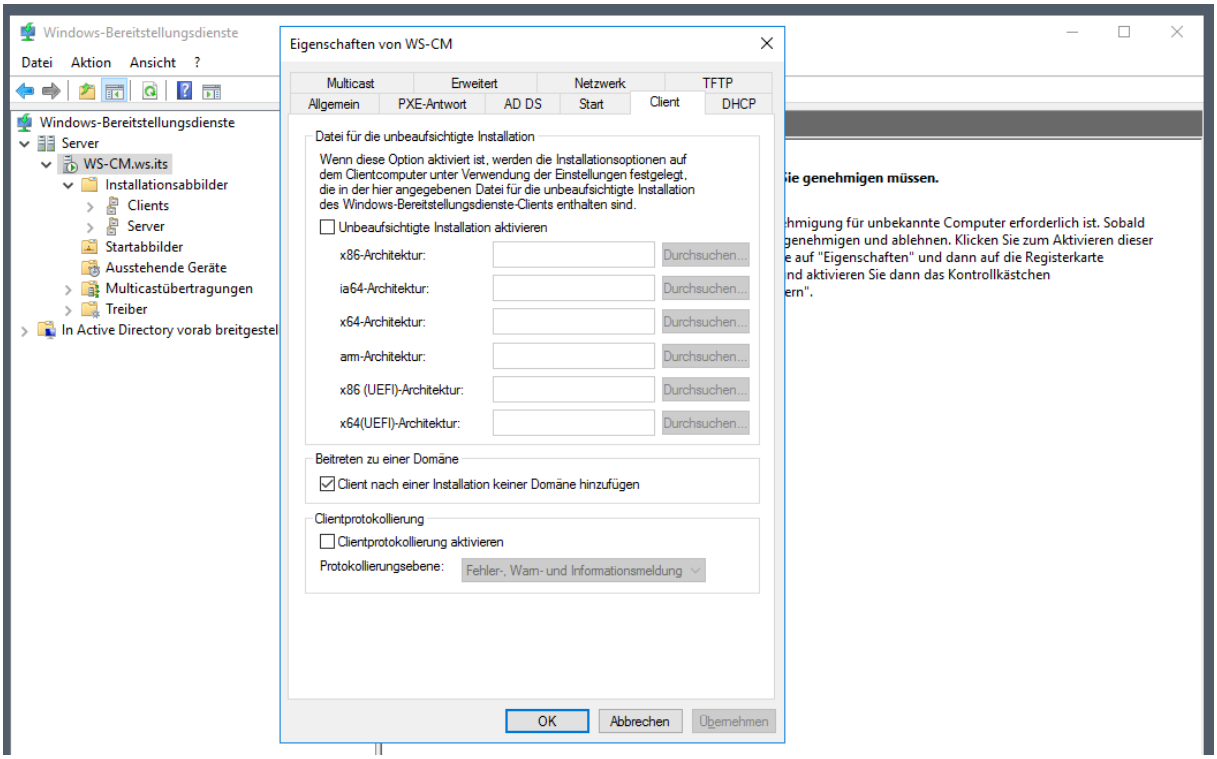
Dann gibt es noch diverse Start-Images. Eines davon ist eine Recovery Environment. Mit dieser kann eine Bare Metal Recovery durchgeführt werden. Alles ist aber veraltet:

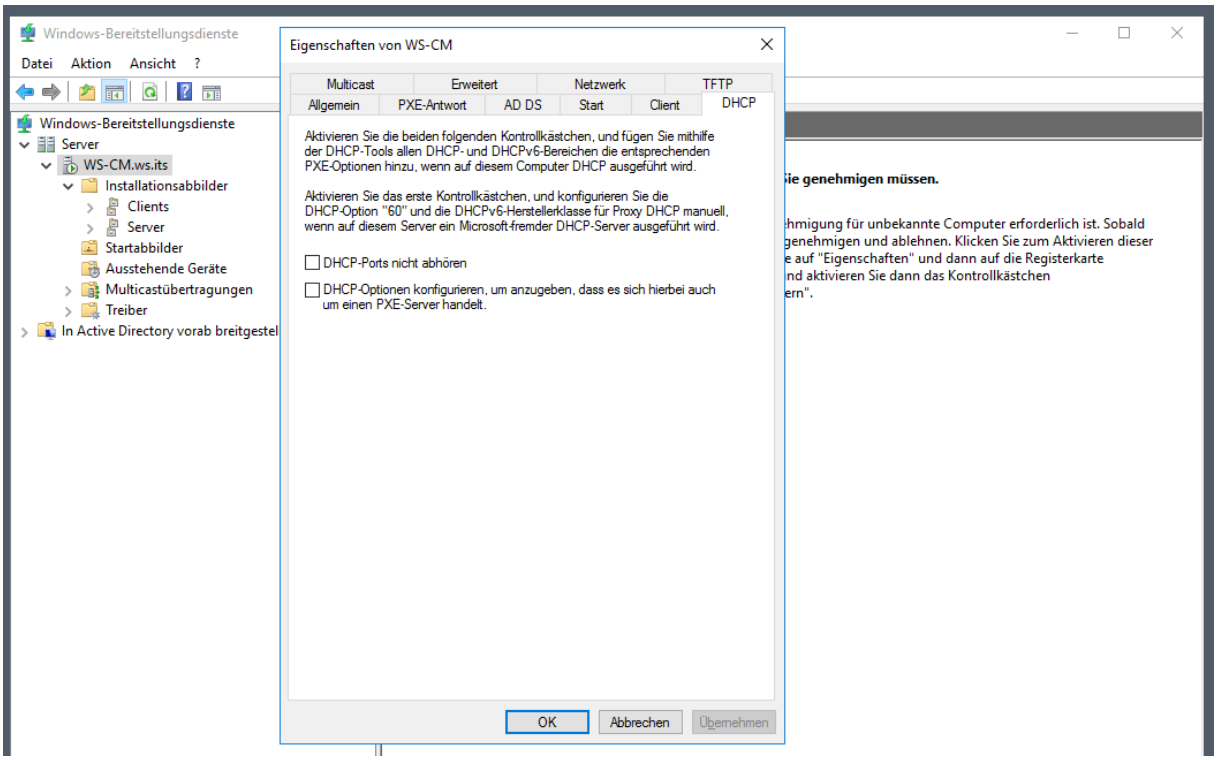


In den Optionen sammle ich noch einige Screen-Shots:


Windows-Bereitstellungsdienste
Datei Aktion Ansicht ?
Windows-Bereitstellungsdienste
Server
WS-CM.ws.its
Installationsabbilder
Clients
Server
Startabbilder
Ausstehende Geräte
Multicastübertragungen
Treiber
In Active Directory vorab breitgestel
Eigenschaften von WS-CM
Multicast Erweitert Netzwerk TFTP
Allgemein PXE-Antwort AD DS Start Client DHCP
PXE-Antwortrichtlinie
Definieren Sie, auf welche Clientcomputer der Server reagieren soll. Bekannte Clients sind Clients, die in der Liste der vorab bereitgestellten Geräte aufgeführt sind.
Keinem Clientcomputer antworten
Nur bekannten Clientcomputern antworten
Allen Clientcomputern antworten (bekannten und unbekannten)
Administratorgenehmigung für unbekannte Computer erforderlich machen. Wenn Sie diese Option auswählen, müssen die Computer mithilfe des Knotens "Ausstehende Geräte" im Snap-In genehmigt werden. Genehmigte Computer werden der Liste der vorab bereitgestellten Clients hinzugefügt.
PXE-Antwortverzögerung
Legen Sie fest, wie schnell der Server auf Clients reagieren soll.
Verzögerung in Sekunden: 0
OK Abbrechen Übernehmen
ie genehmigen müssen.
hmigung für unbekannte Computer erforderlich ist. Sobald
genehmigen und ablehnen. Klicken Sie zum Aktivieren dieser
e auf "Eigenschaften" und dann auf die Registerkarte
nd aktivieren Sie dann das Kontrollkästchen
ern".


Windows-Bereitstellungsdienste
Datei Aktion Ansicht ?
Windows-Bereitstellungsdienste
Server
WS-CM.ws.its
Installationsabbilder
Clients
Server
Startabbilder
Ausstehende Geräte
Multicastübertragungen
Treiber
In Active Directory vorab breitgestel
Eigenschaften von WS-CM
Multicast Erweitert Netzwerk TFTP
Allgemein PXE-Antwort AD DS Start Client DHCP
PXE-Startrichtlinie
Definieren Sie, wann ein PXE-Start nach dem Initiieren eines Netzwerkstarts fortgesetzt werden soll.
Bekannte Clients:
Drücken von F12 durch den Benutzer erforderlich machen, damit der PXE-Start fortgesetzt wird
PXE-Start immer fortsetzen
PXE-Start fortsetzen, sofern nicht ESC gedrückt wird
PXE-Start nie fortsetzen
Unbekannte Clients:
Drücken von F12 durch den Benutzer erforderlich machen, damit der PXE-Start fortgesetzt wird
PXE-Start immer fortsetzen
PXE-Start fortsetzen, sofern nicht ESC gedrückt wird
PXE-Start nie fortsetzen
Standardmäßiges Startabbild (optional)
x86-Architektur: Auswählen...
ia64-Architektur: Auswählen...
x64-Architektur: Boot\x64\Images\Winre.wim Auswählen...
arm-Architektur: Auswählen...
x86 (UEFI)-Architektur: Auswählen...
x64(UEFI)-Architektur: Boot\x64\Images\Winre.wim Auswählen...
OK Abbrechen Übernehmen
ie genehmigen müssen.
hmigung für unbekannte Computer erforderlich ist. Sobald
genehmigen und ablehnen. Klicken Sie zum Aktivieren dieser
e auf "Eigenschaften" und dann auf die Registerkarte
nd aktivieren Sie dann das Kontrollkästchen
ern".

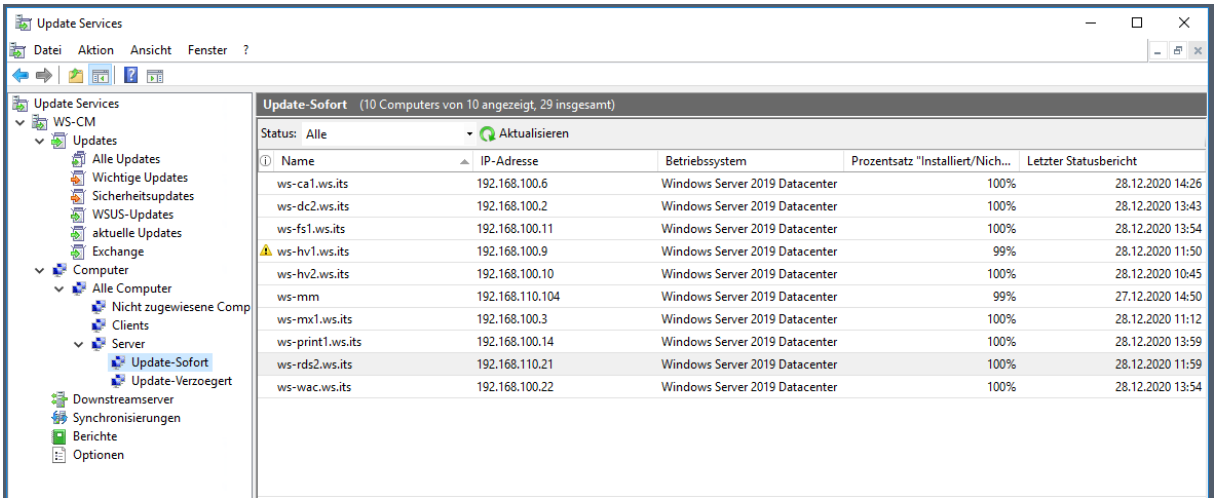


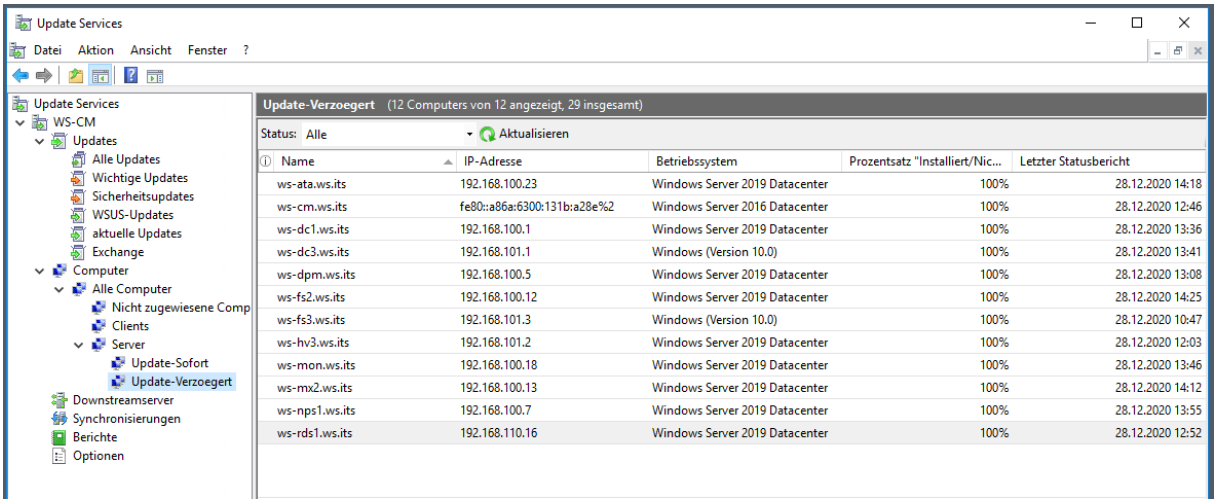


Das soll dann aber auch genügen.

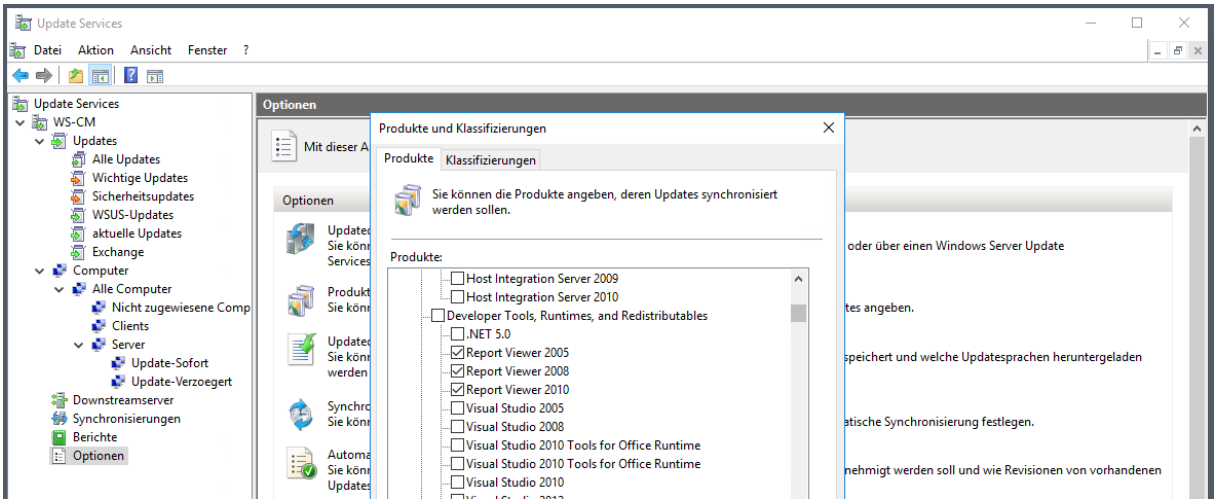
Sichtung der Rolle WSUS

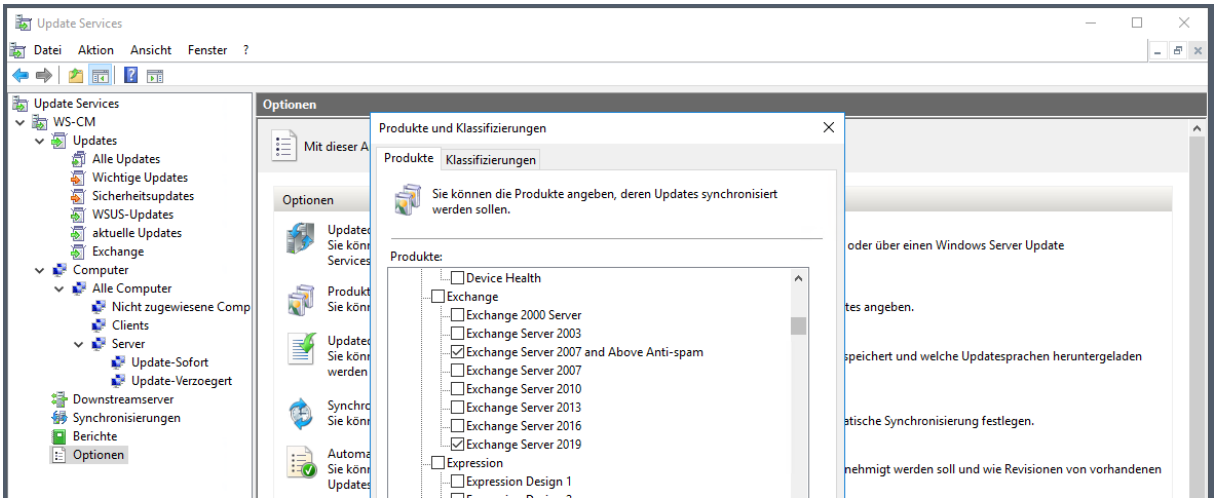
Im Service WSUS dokumentiere ich auch noch einmal den aktuellen Stand. Derzeit habe ich für meine Windows Server 2 Container für die Aktualisierung. Mein Genehmigungs-Script wird die neuen Updates nach 7 Tagen Liegezeit auf dem Container „Updates-Sofort“ genehmigen. Erst weitere 7 Tage später ist der Container „Updates-Verzoegert“ an der Reihe. Durch eine gezielte Platzierung meiner Windows Server kann ich so steuern, wann welcher Server seine Updates installiert. Cluster-Systeme lassen sich so schön voneinander trennen:

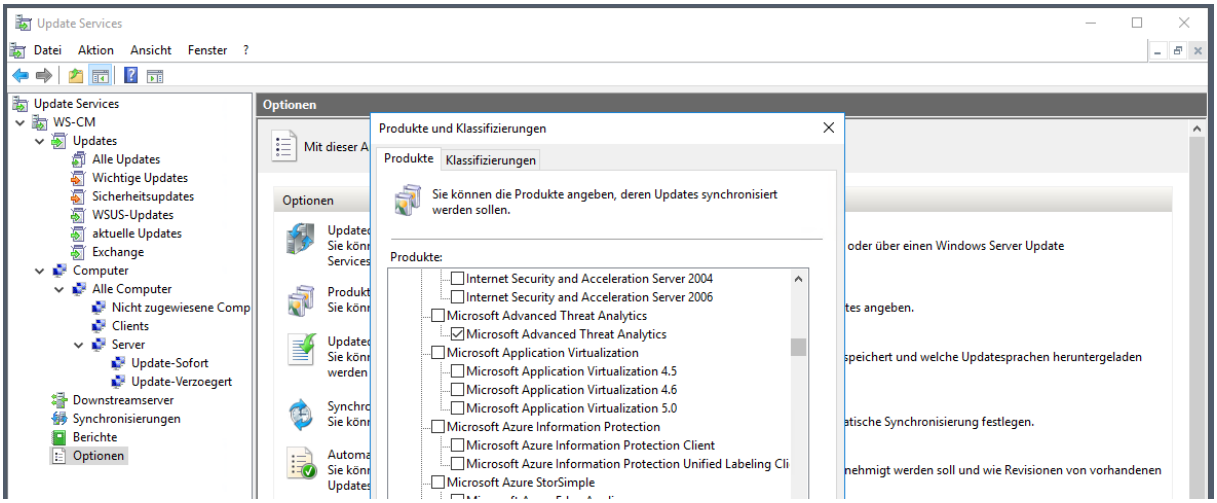


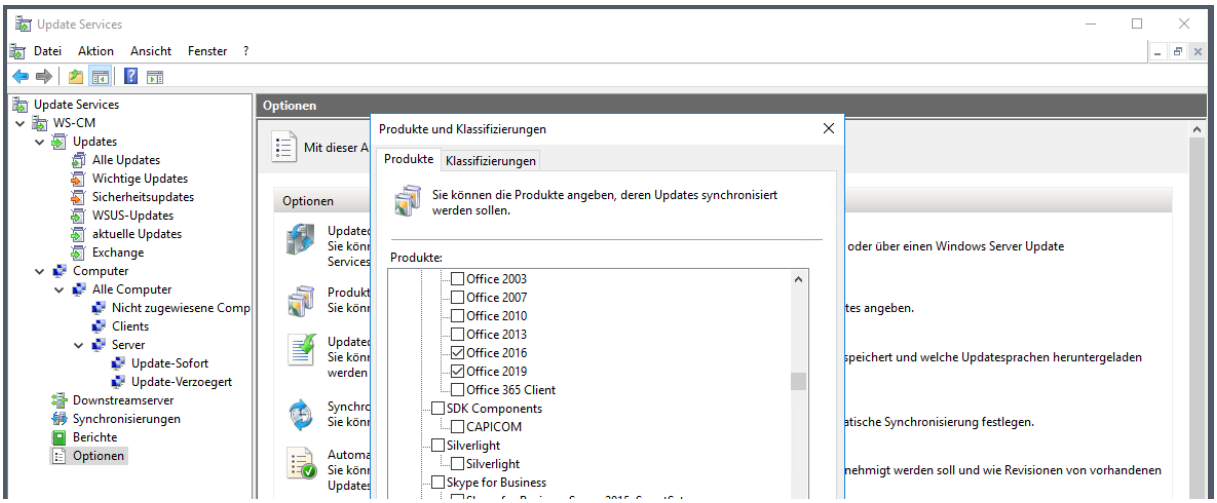


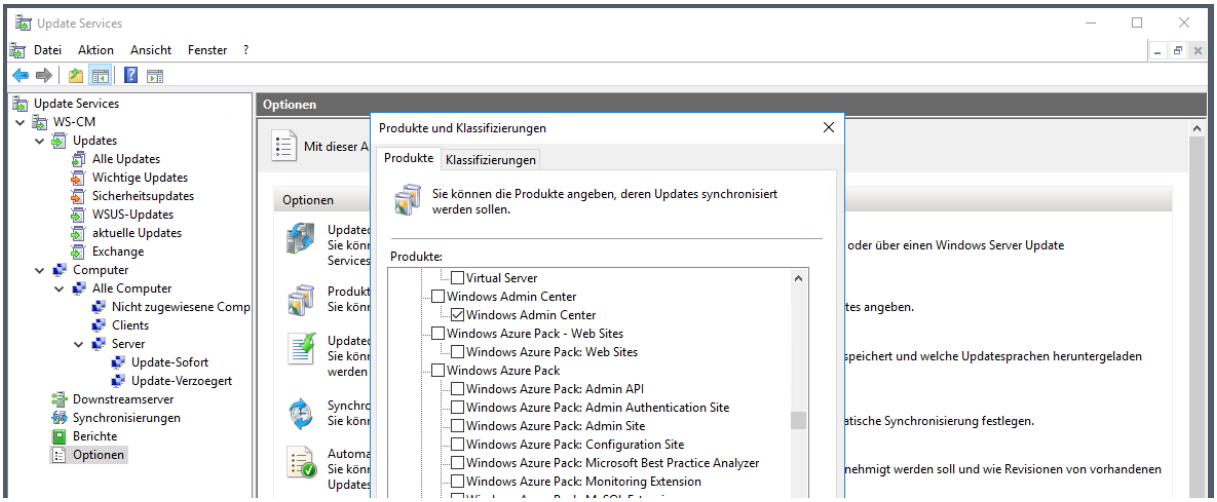
In meinem aktuellen WSUS lade ich für diese Produkte Updates herunter:

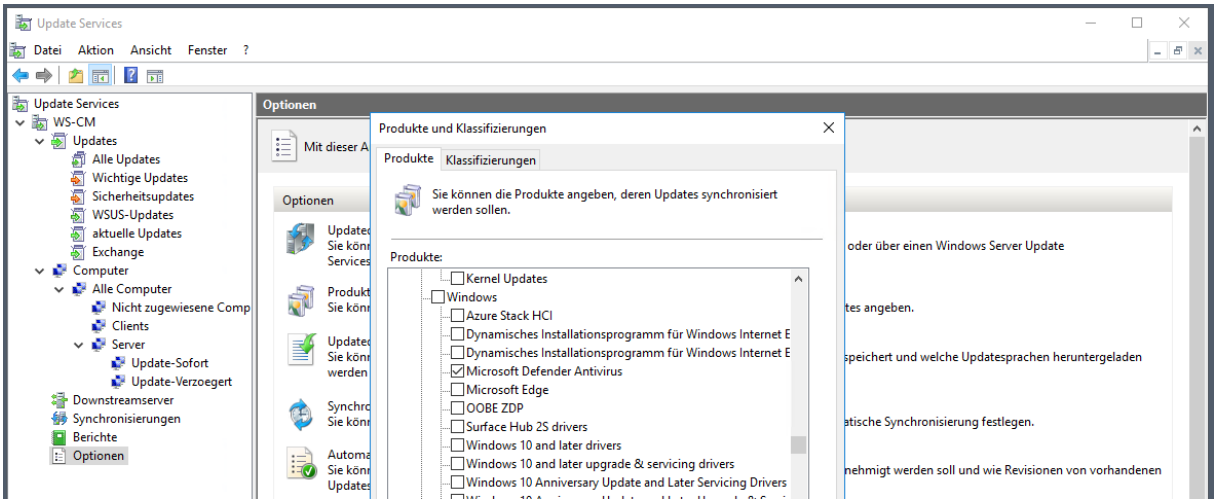


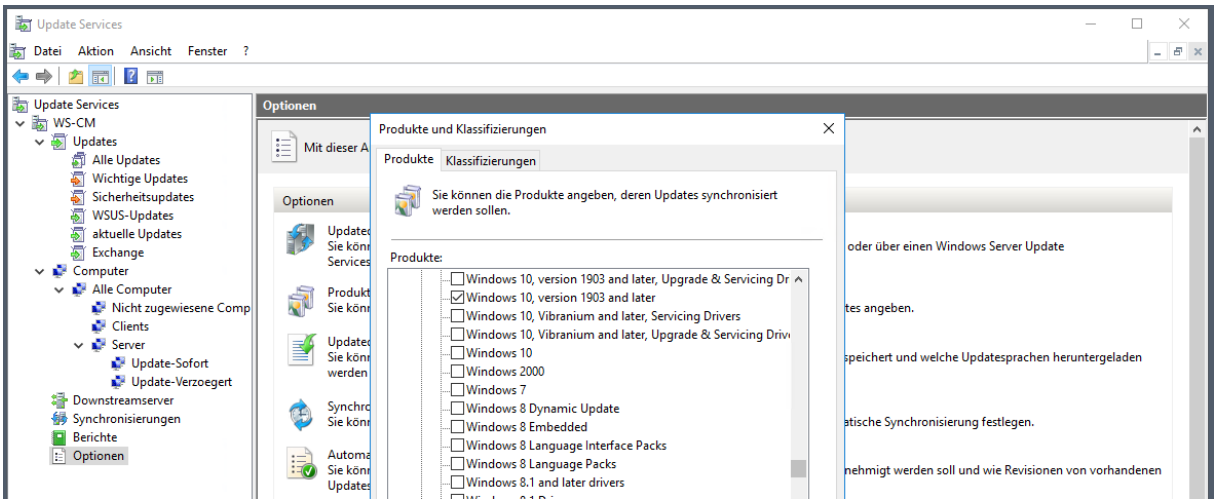

Update Services
Datei Aktion Ansicht Fenster ?
Update Services
WS-CM
Updates
Alle Updates
Wichtige Updates
Sicherheitsupdates
WSUS-Updates
aktuelle Updates
Exchange
Computer
Alle Computer
Nicht zugewiesene Comp
Clients
Server
Update-Sofort
Update-Verzoegert
Downstreamserver
Synchronisierungen
Berichte
Optionen
Optionen
Produkte und Klassifizierungen
Produkte
Klassifizierungen
Sie können die Produkte angeben, deren Updates synchronisiert werden sollen.
Produkte:
Device Health
Exchange
Exchange 2000 Server
Exchange Server 2003
Exchange Server 2007 and Above Anti-spam
Exchange Server 2007
Exchange Server 2010
Exchange Server 2013
Exchange Server 2016
Exchange Server 2019
Expression
Expression Design 1

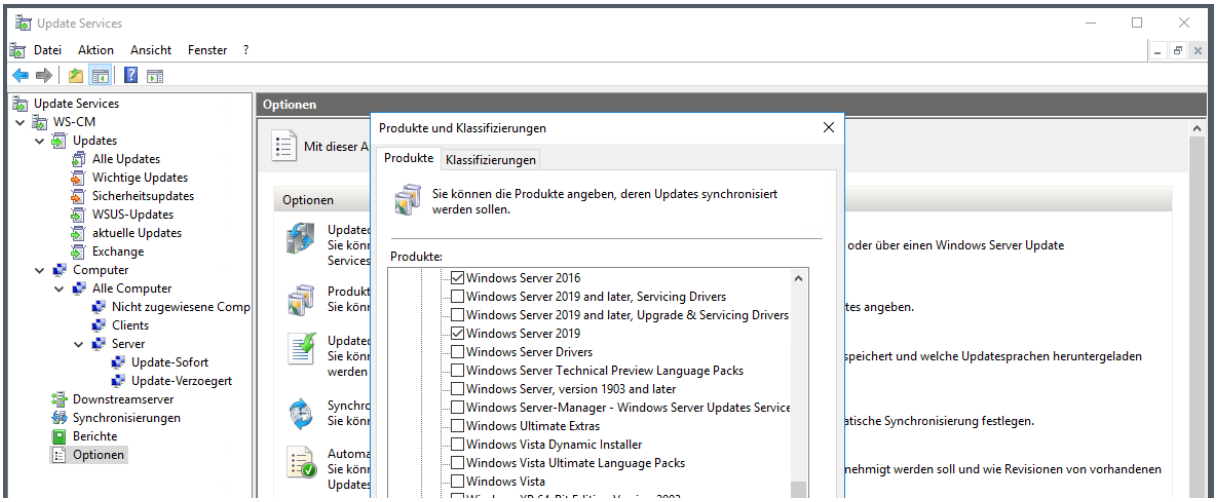

Update Services
Datei Aktion Ansicht Fenster ?
Update Services
WS-CM
Updates
Alle Updates
Wichtige Updates
Sicherheitsupdates
WSUS-Updates
aktuelle Updates
Exchange
Computer
Alle Computer
Nicht zugewiesene Comp
Clients
Server
Update-Sofort
Update-Verzoegert
Downstreamserver
Synchronisierungen
Berichte
Optionen
Optionen
Produkte und Klassifizierungen
Produkte
Klassifizierungen
Sie können die Produkte angeben, deren Updates synchronisiert werden sollen.
Produkte:
Internet Security and Acceleration Server 2004
Internet Security and Acceleration Server 2006
Microsoft Advanced Threat Analytics
Microsoft Advanced Threat Analytics
Microsoft Application Virtualization
Microsoft Application Virtualization 4.5
Microsoft Application Virtualization 4.6
Microsoft Application Virtualization 5.0
Microsoft Azure Information Protection
Microsoft Azure Information Protection Client
Microsoft Azure Information Protection Unified Labeling Cli
Microsoft Azure StorSimple


Update Services
Datei Aktion Ansicht Fenster ?
Update Services
WS-CM
Updates
Alle Updates
Wichtige Updates
Sicherheitsupdates
WSUS-Updates
aktuelle Updates
Exchange
Computer
Alle Computer
Nicht zugewiesene Comp
Clients
Server
Update-Sofort
Update-Verzoegert
Downstreamserver
Synchronisierungen
Berichte
Optionen
Optionen
Produkte und Klassifizierungen
Produkte
Klassifizierungen
Sie können die Produkte angeben, deren Updates synchronisiert werden sollen.
Produkte:
Office 2003
Office 2007
Office 2010
Office 2013
Office 2016
Office 2019
Office 365 Client
SDK Components
CAPICOM
Silverlight
Silverlight
Skype for Business

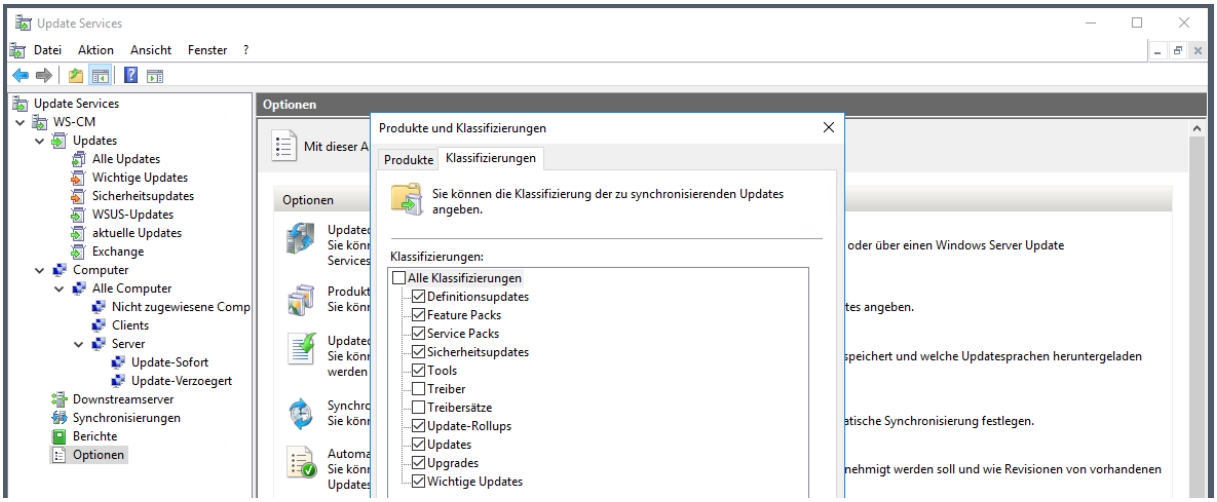

Update Services
Datei Aktion Ansicht Fenster ?
Update Services
WS-CM
Updates
Alle Updates
Wichtige Updates
Sicherheitsupdates
WSUS-Updates
aktuelle Updates
Exchange
Computer
Alle Computer
Nicht zugewiesene Comp
Clients
Server
Update-Sofort
Update-Verzoegert
Downstreamserver
Synchronisierungen
Berichte
Optionen
Optionen
Produkte und Klassifizierungen
Produkte
Klassifizierungen
Sie können die Produkte angeben, deren Updates synchronisiert werden sollen.
Produkte:
Virtual Server
Windows Admin Center
Windows Admin Center
Windows Azure Pack - Web Sites
Windows Azure Pack: Web Sites
Windows Azure Pack
Windows Azure Pack: Admin API
Windows Azure Pack: Admin Authentication Site
Windows Azure Pack: Admin Site
Windows Azure Pack: Configuration Site
Windows Azure Pack: Microsoft Best Practice Analyzer
Windows Azure Pack: Monitoring Extension


Update Services
Datei Aktion Ansicht Fenster ?
Update Services
WS-CM
Updates
Alle Updates
Wichtige Updates
Sicherheitsupdates
WSUS-Updates
aktuelle Updates
Exchange
Computer
Alle Computer
Nicht zugewiesene Comp
Clients
Server
Update-Sofort
Update-Verzoegert
Downstreamserver
Synchronisierungen
Berichte
Optionen
Optionen
Produkte und Klassifizierungen
Produkte
Klassifizierungen
Sie können die Produkte angeben, deren Updates synchronisiert werden sollen.
Produkte:
Kernel Updates
Windows
Azure Stack HCI
Dynamisches Installationsprogramm für Windows Internet E
Dynamisches Installationsprogramm für Windows Internet E
Microsoft Defender Antivirus
Microsoft Edge
OOBE ZDP
Surface Hub 2S drivers
Windows 10 and later drivers
Windows 10 and later upgrade & servicing drivers
Windows 10 Anniversary Update and Later Servicing Drivers

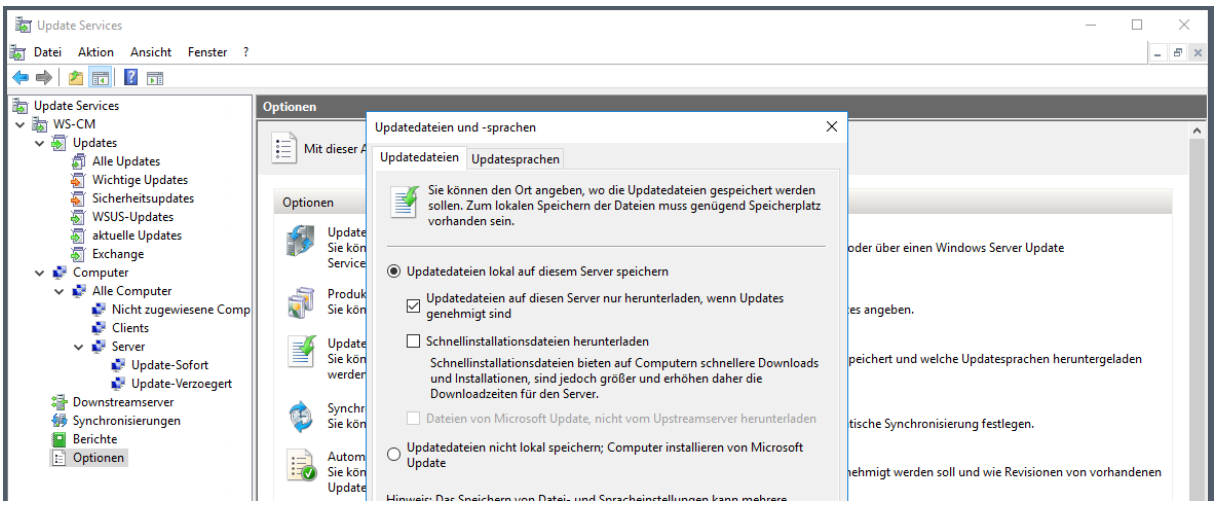

Update Services
Datei Aktion Ansicht Fenster ?
Update Services
WS-CM
Updates
Alle Updates
Wichtige Updates
Sicherheitsupdates
WSUS-Updates
aktuelle Updates
Exchange
Computer
Alle Computer
Nicht zugewiesene Comp
Clients
Server
Update-Sofort
Update-Verzoegert
Downstreamserver
Synchronisierungen
Berichte
Optionen
Optionen
Produkte und Klassifizierungen
Produkte
Klassifizierungen
Sie können die Produkte angeben, deren Updates synchronisiert werden sollen.
Produkte:
Windows 10, version 1903 and later, Upgrade & Servicing Dr
Windows 10, version 1903 and later
Windows 10, Vibranium and later, Servicing Drivers
Windows 10, Vibranium and later, Upgrade & Servicing Driv
Windows 10
Windows 2000
Windows 7
Windows 8 Dynamic Update
Windows 8 Embedded
Windows 8 Language Interface Packs
Windows 8 Language Packs
Windows 8.1 and later drivers



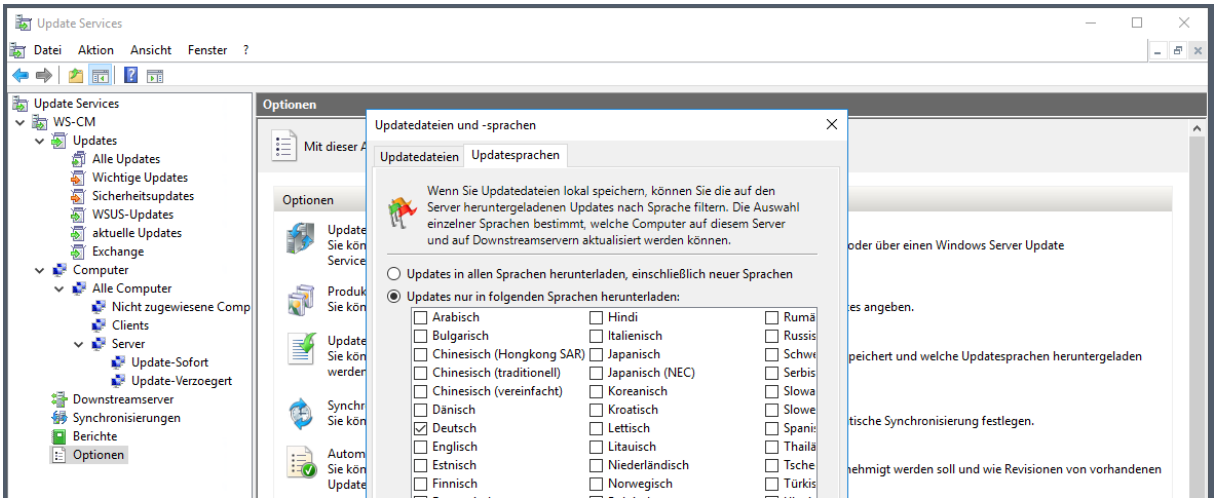
Die Updates sind in einzelne Klassifizierungen aufgeteilt. Hier fahre ich sehr gut mit dieser Einstellung:



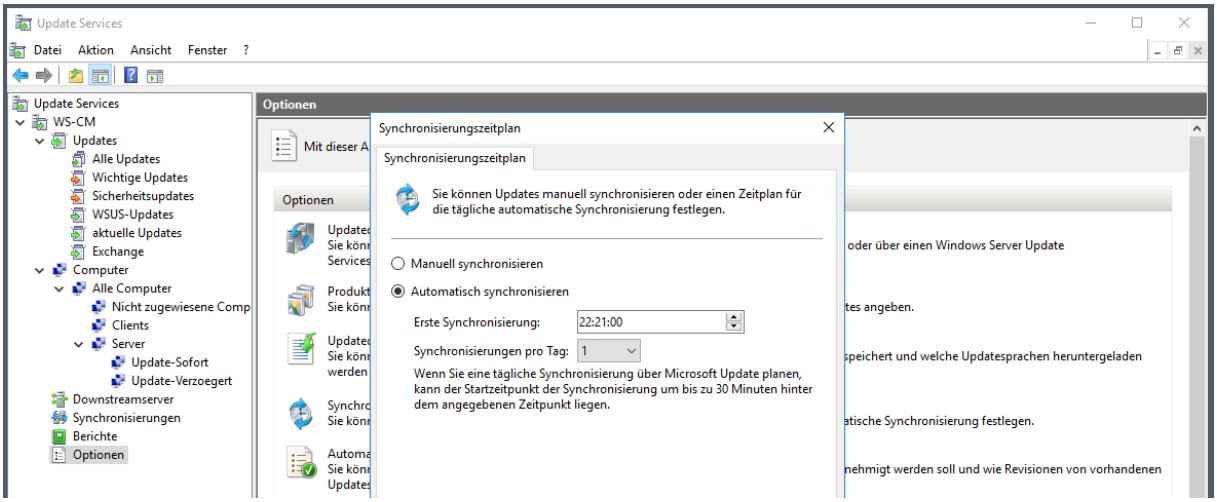
Die Updates werden erst nach der Genehmigung geladen. Das macht mit meinem Genehmigung-Script besonders Sinn, denn dieses lehnt nicht erwünschte Updates ab. So kann ich viel Speicherplatz und Bandbreite sparen:



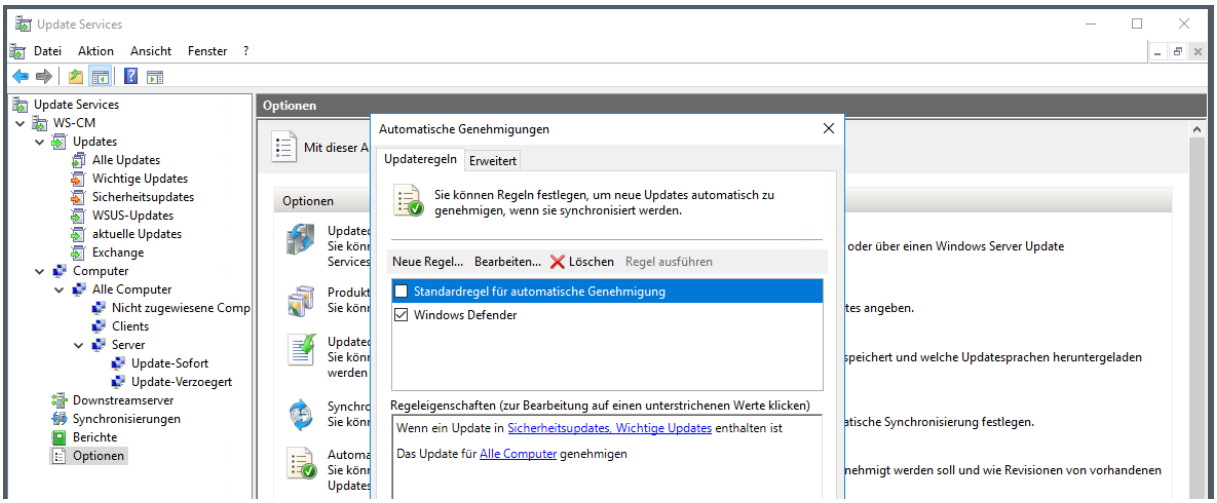
Meine eigene Umgebung enthält ausschließlich deutsche Installationen. Daher kann ich hier gut filtern:



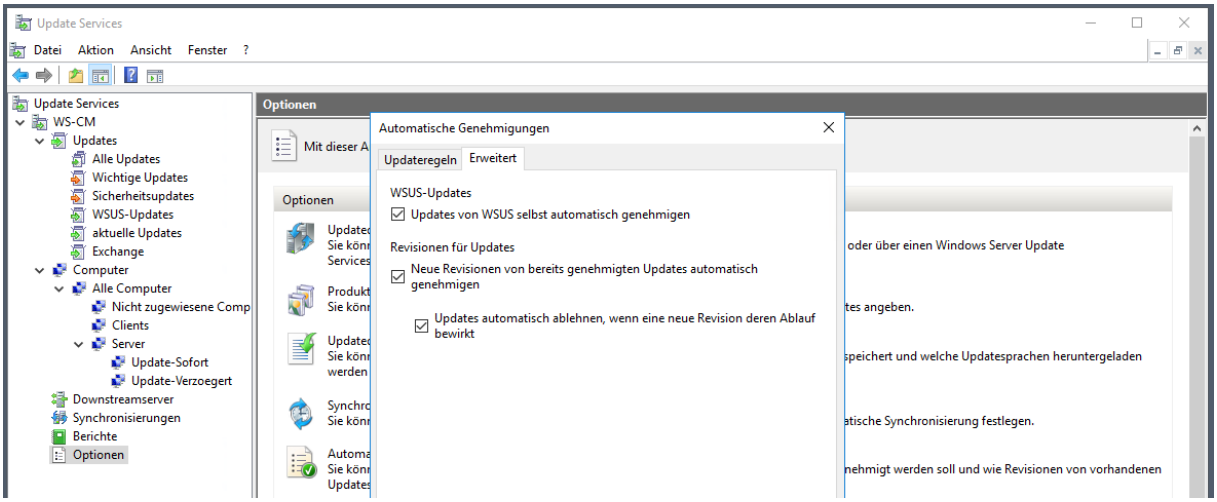
Mein WSUS schaut einmal am Tag nach neuen Updates. Die Zeit ist kein Zufall. Nach der Synchronisierung läuft das Genehmigungsscript und kann bei Bedarf Updates genehmigen. Diese werden dann heruntergeladen. Und wenn dann am Folgetag 03:00 die Update-Installationen beginnen, dann hab ich die Server gleich mit dem Setup versorgt.



Ich verwende die Standardgenehmigung nur für die Updates von Windows Defender. Den Rest erledigt mein Script:



Diese Einstellung hatte ich nicht verändert:

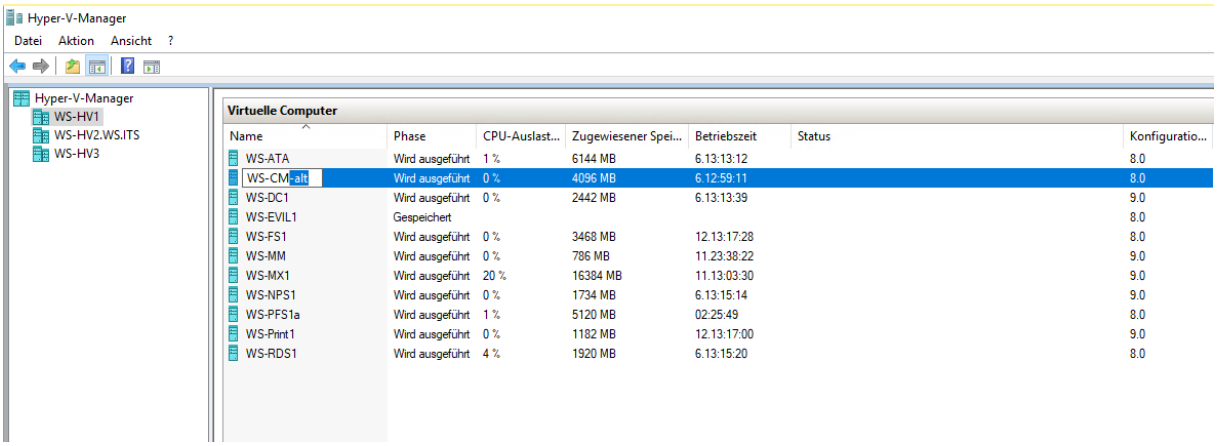


Bei dem neuen WSUS werde ich einige Anpassungen vornehmen.

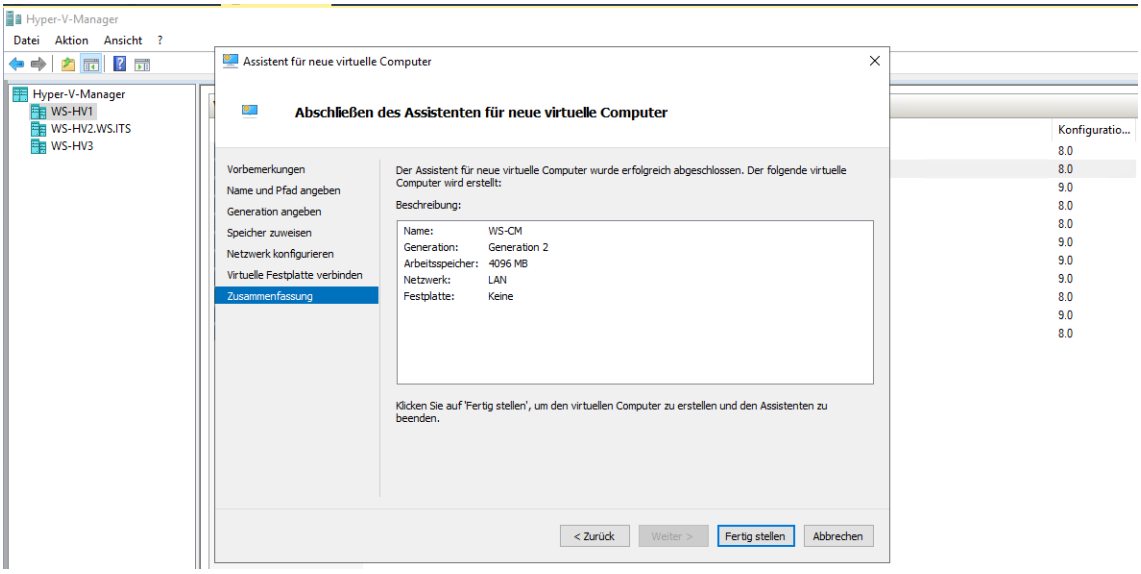
Migration

Bereitstellung der neuen VM

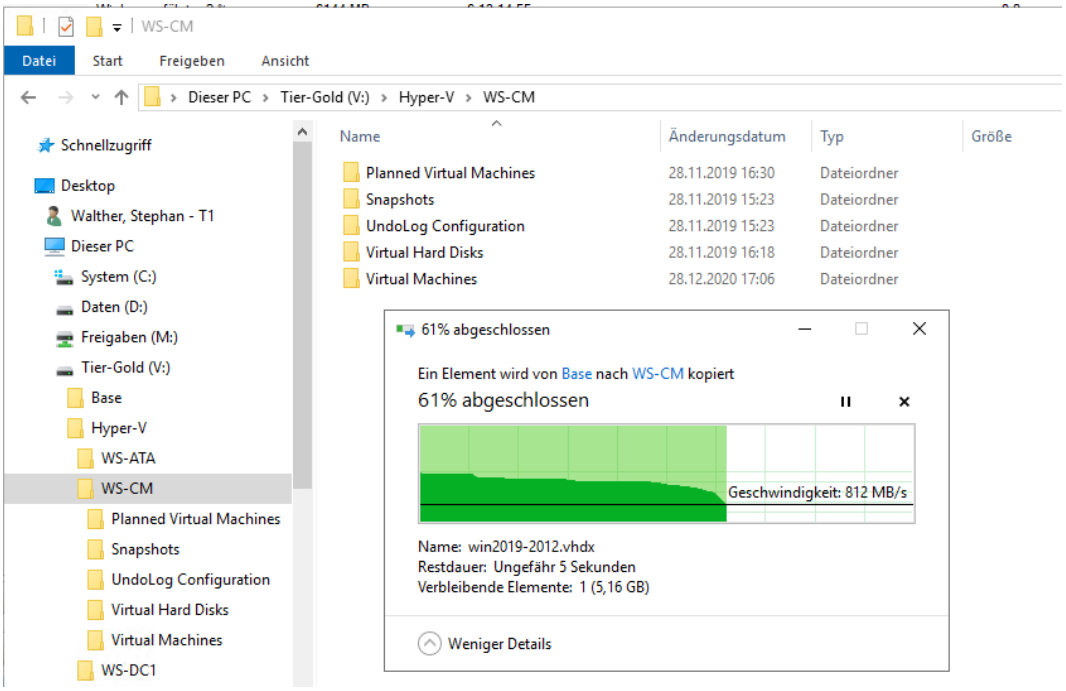
In meinem Hyper-V benenne ich den aktuellen Server um:



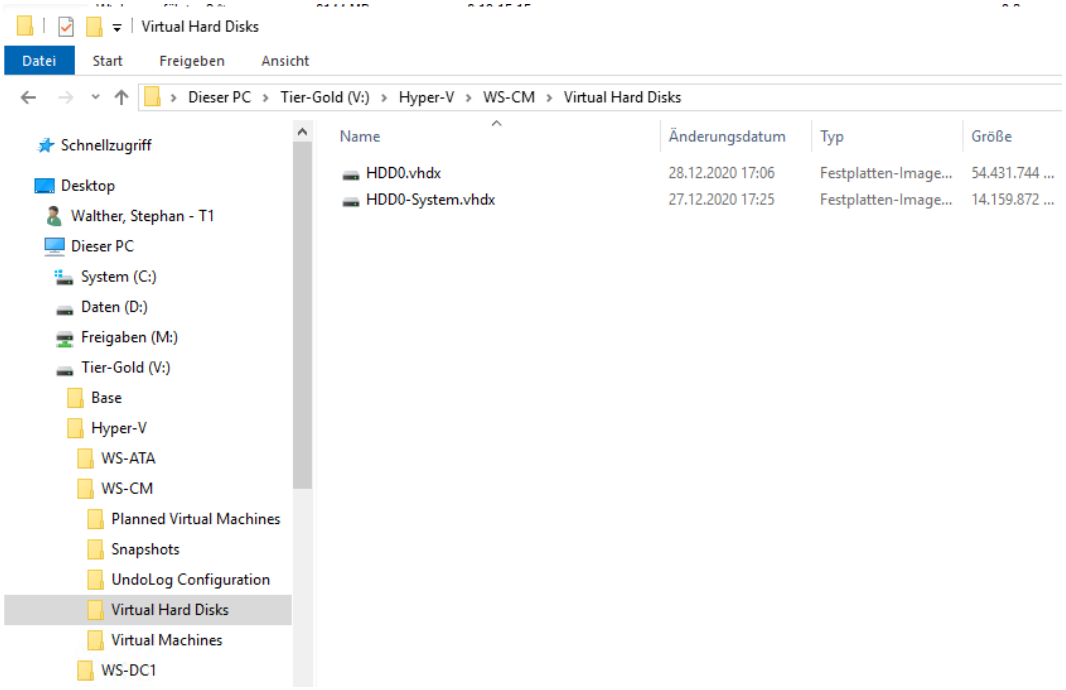
Dann erstelle ich eine neue VM:



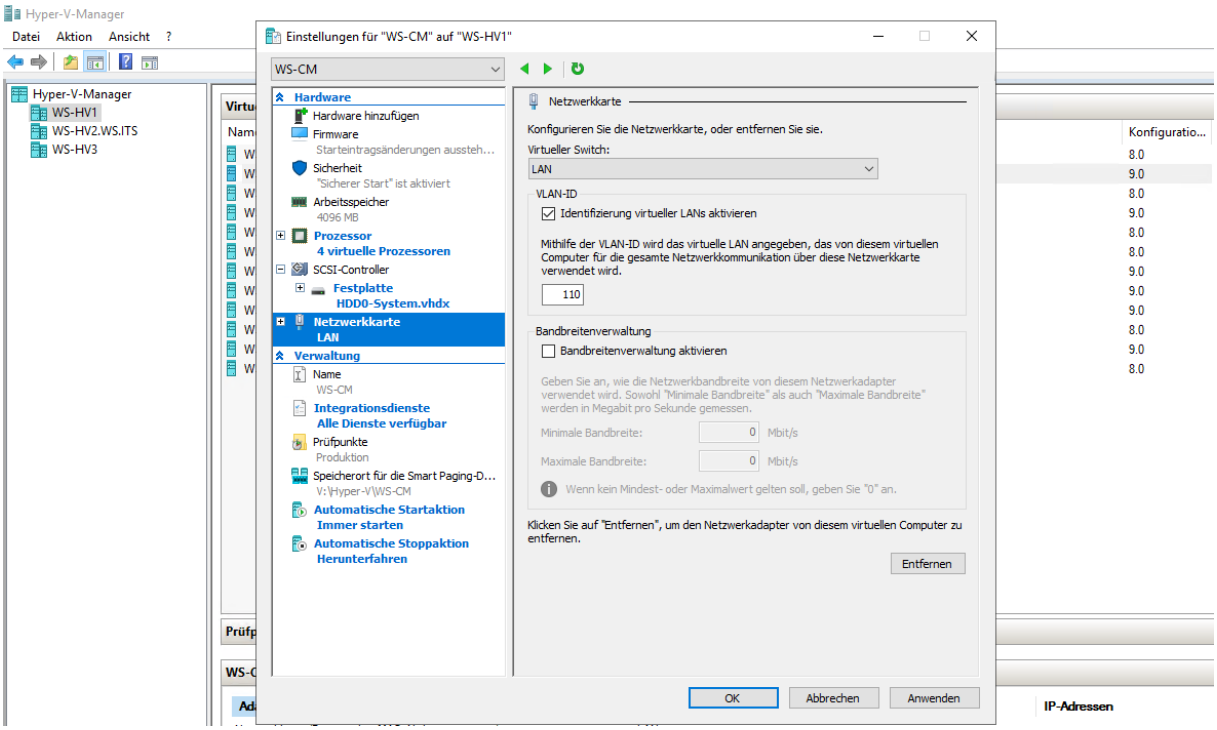
Als Betriebssystemdatenträger kopiere ich mein vorbereitetes Master-Image als VHDX in den VM-Ordner:



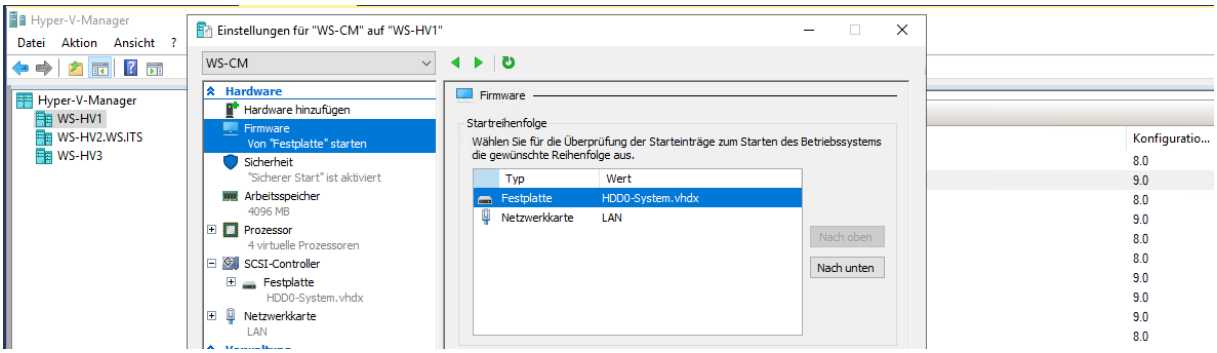
Die neue System-Partition liegt nun an der richtigen Stelle:



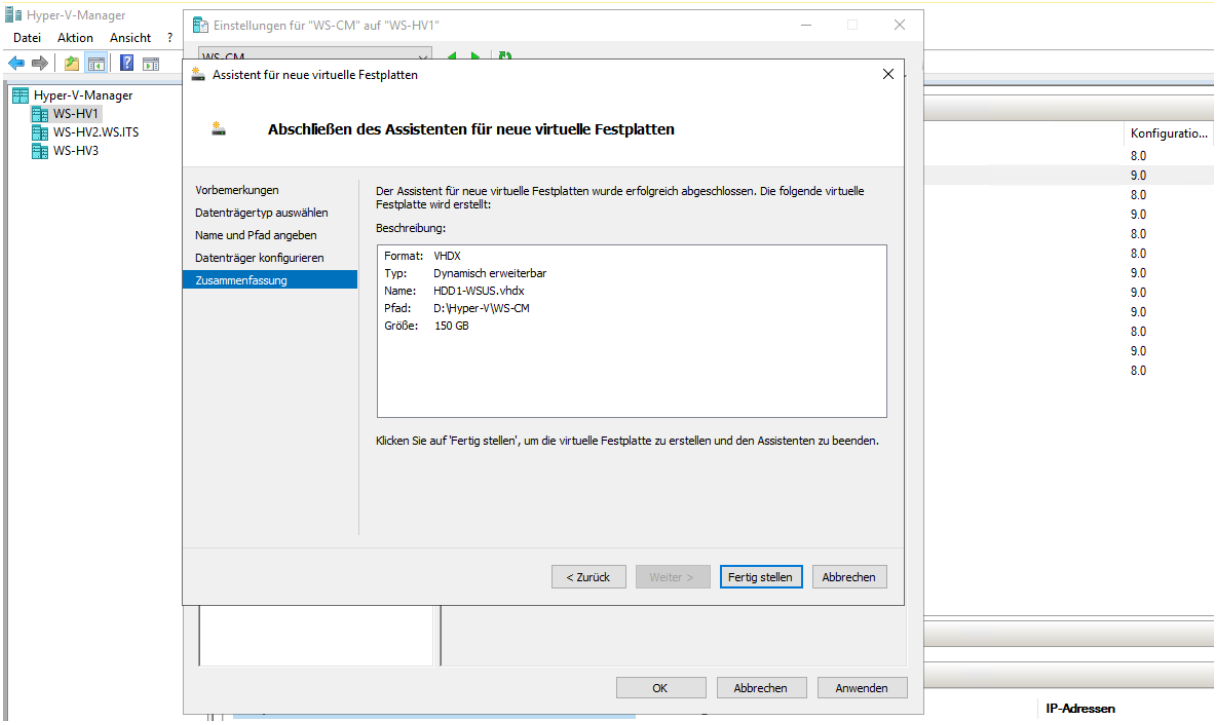
Jetzt bekommt die VM den Feinschliff: etwas mehr CPU, die neue VHDX und einige Konfigurationsanpassungen für z.B. den automatischen Start gehören eingetragen. Ebenso braucht der Server eine Netzwerkverbindung. Für die Aktivierung kommt er erst einmal in mein Client-VLAN 110:



Dann passe ich die Boot-Reihenfolge an:



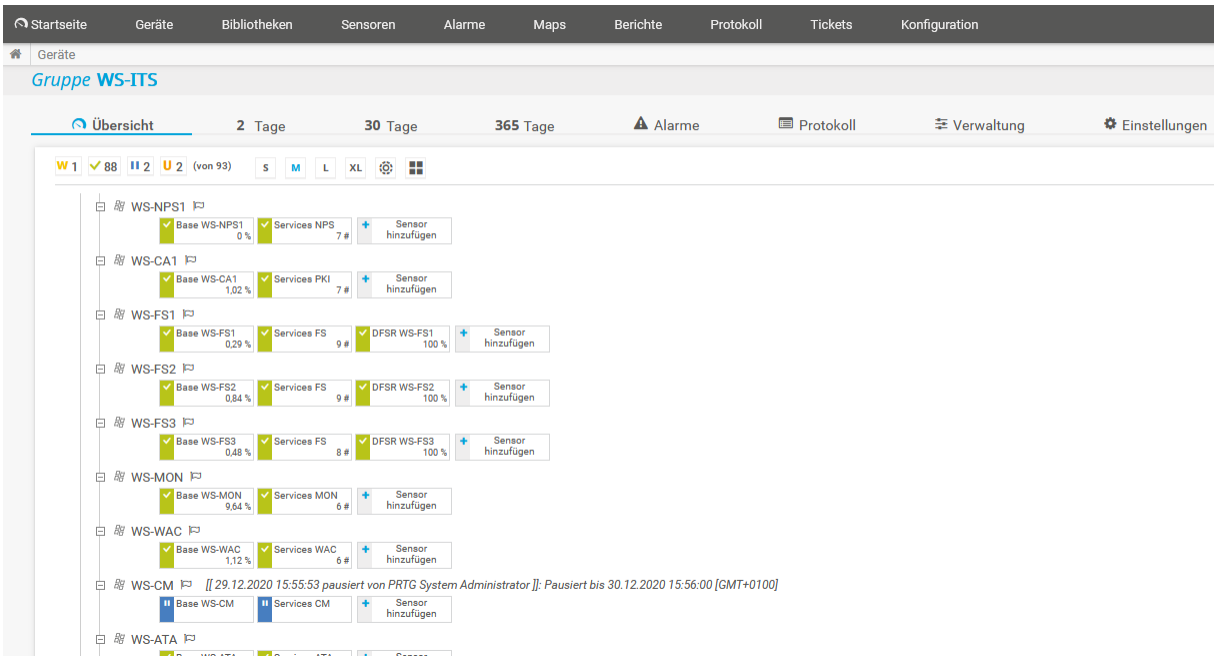
Und danach erhält der Server eine zusätzliche VHDX, in der er die Updates abspeichern kann. Diese lege ich auf einem langsameren Datenträger ab – ein NVMe-Storage ist mir dafür zu schade:



An dieser Stelle habe ich mich dann dazu entschlossen, den Servernamen nicht zu übernehmen. Die VM WS-CM habe ich jetzt in WS-WSUS geändert. Ebenso habe ich die Dateien der VM in einen passenden Ordner auf meinem Dateisystem im Hyper-V verschoben.

Abschaltung des alten Servers & Maintenance

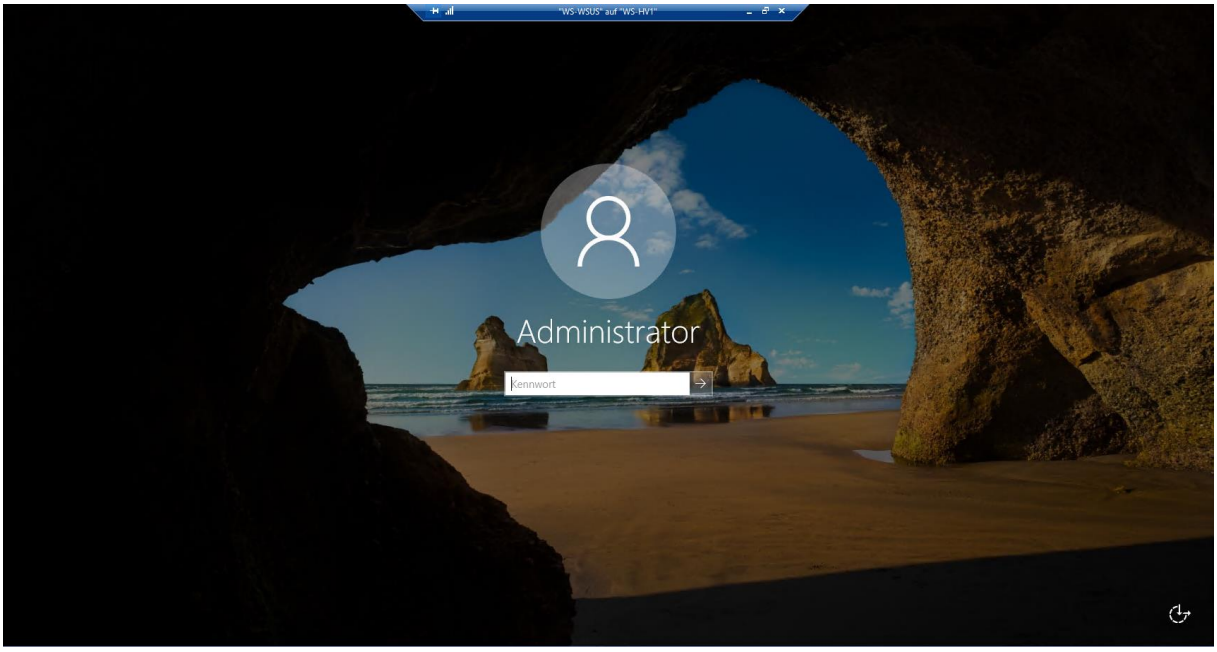
Der alte Server kann einfach abgeschaltet werden, denn er hat keine weiteren Abhängigkeiten. Damit mich mein Monitoring nicht permanent anpiept, pausiere ich die Sensoren für den alten WSUS:



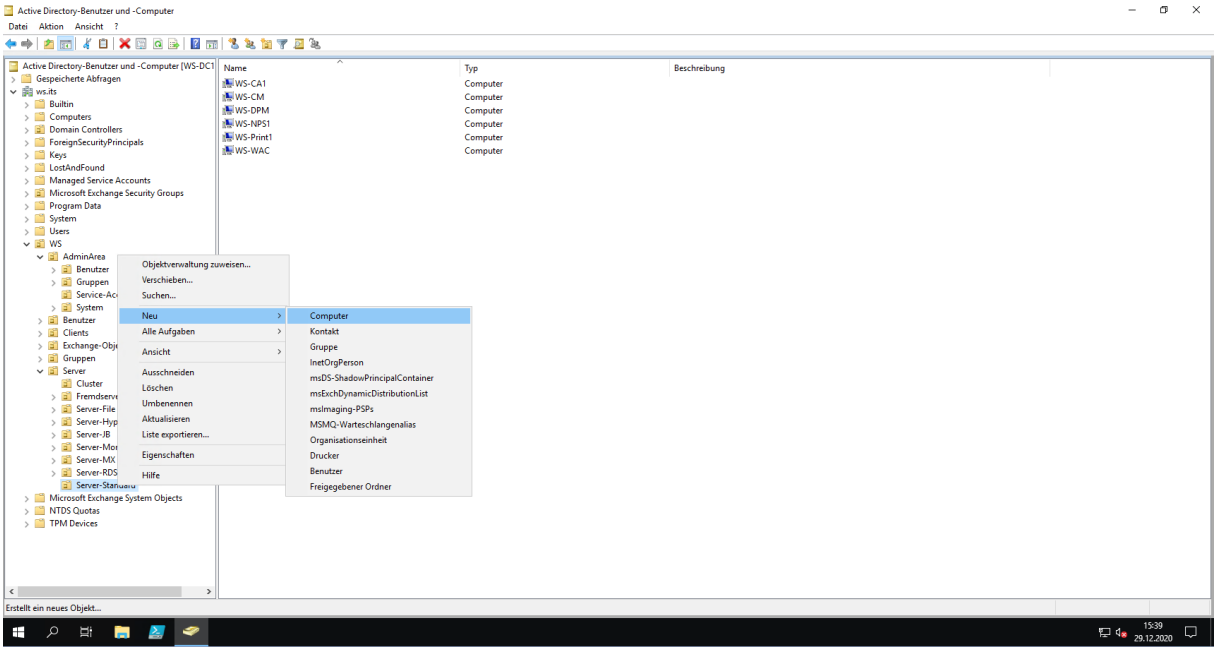
Jetzt fahre ich den alten Server einfach herunter.

Betriebssystemvorbereitung

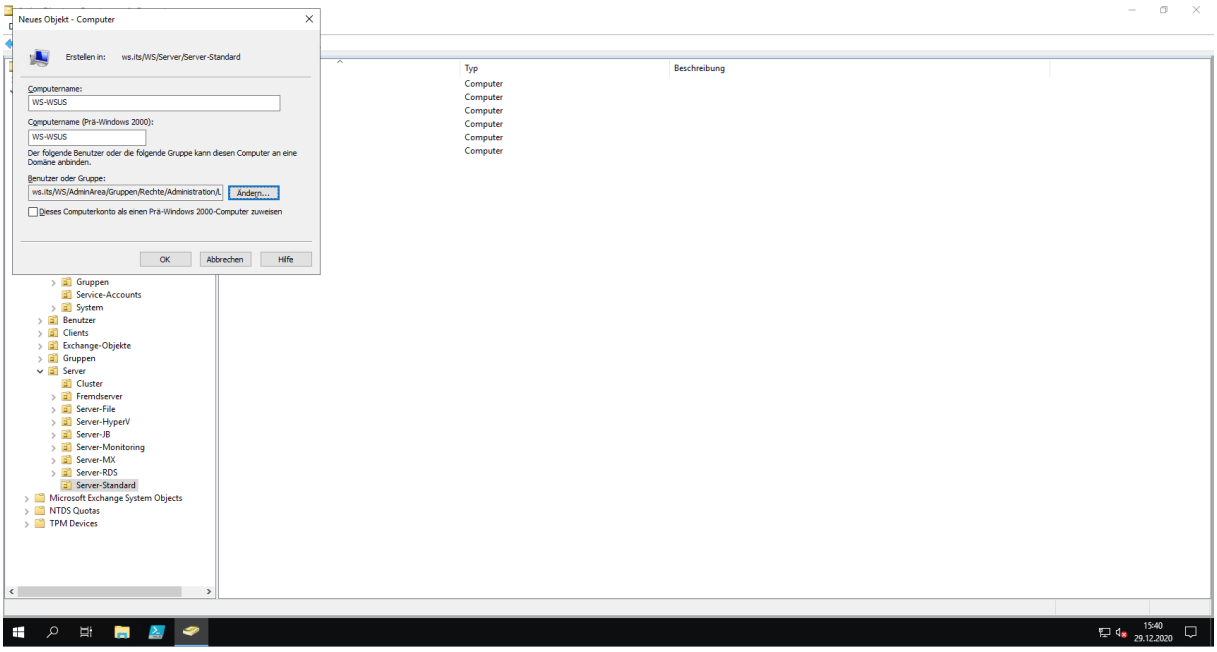
Danach starte ich den neuen Server. Das Setup wird mit einer Out-of-Box-Konfiguration abgeschlossen. Danach kann ich mich lokal anmelden:



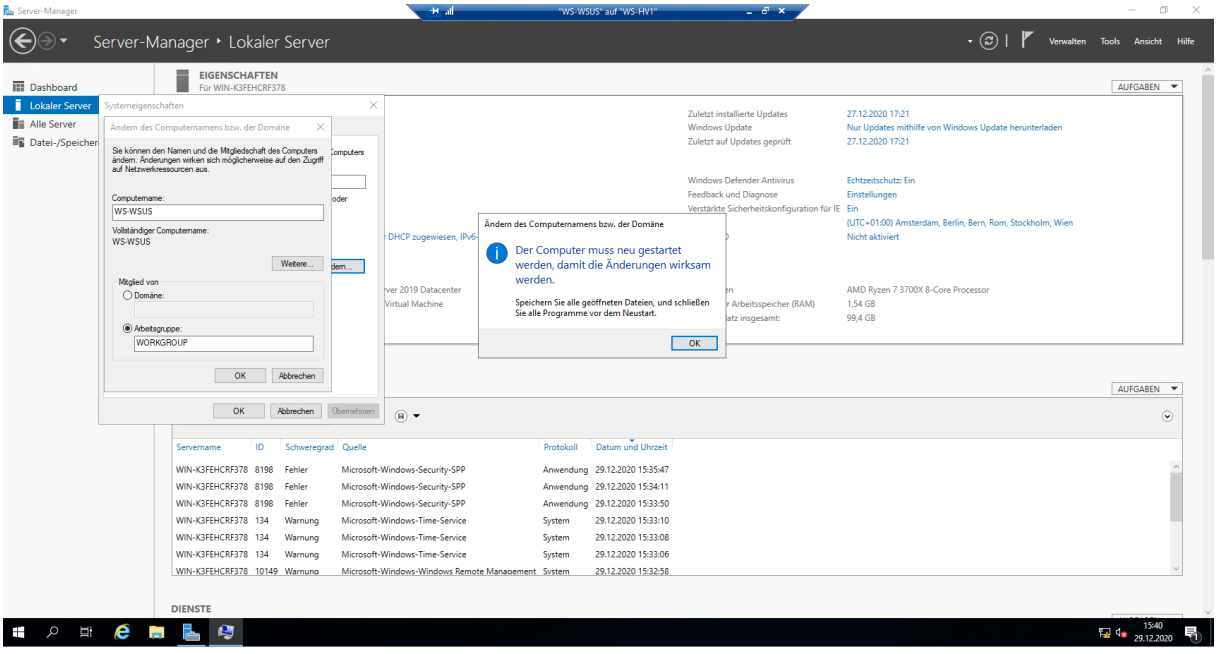
Durch den neuen Servernamen wird auch ein neues Computerkonto im Active Directory benötigt. Dieses erstelle ich VOR dem Domain Join in der richtigen Organisationseinheit. So kann ich sicherstellen, dass der neue Server von der ersten Minute an die für ihn richtigen Gruppenrichtlinien bezieht. Der Server kommt in meinen Standard-Tier-ServerContainer:



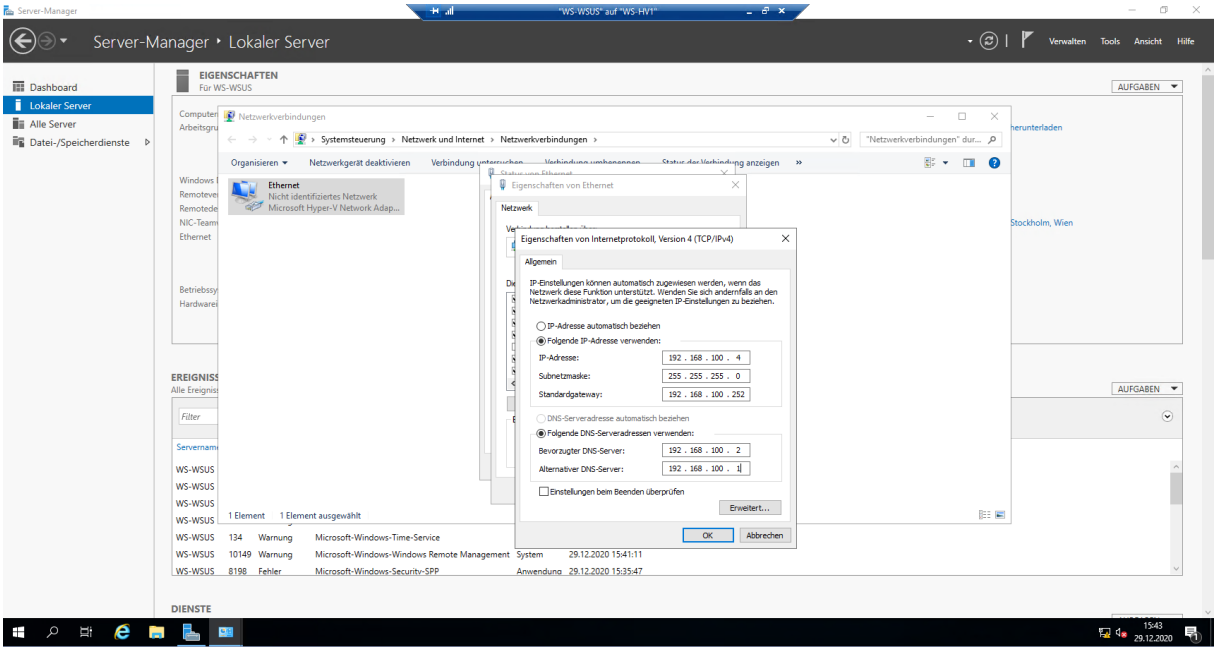
Dann passe ich noch im gleichen Dialog den Namen der für den Domain Join berechtigten AD-Gruppe an. Das muss ja nicht immer ein Domain Admin erledigen:



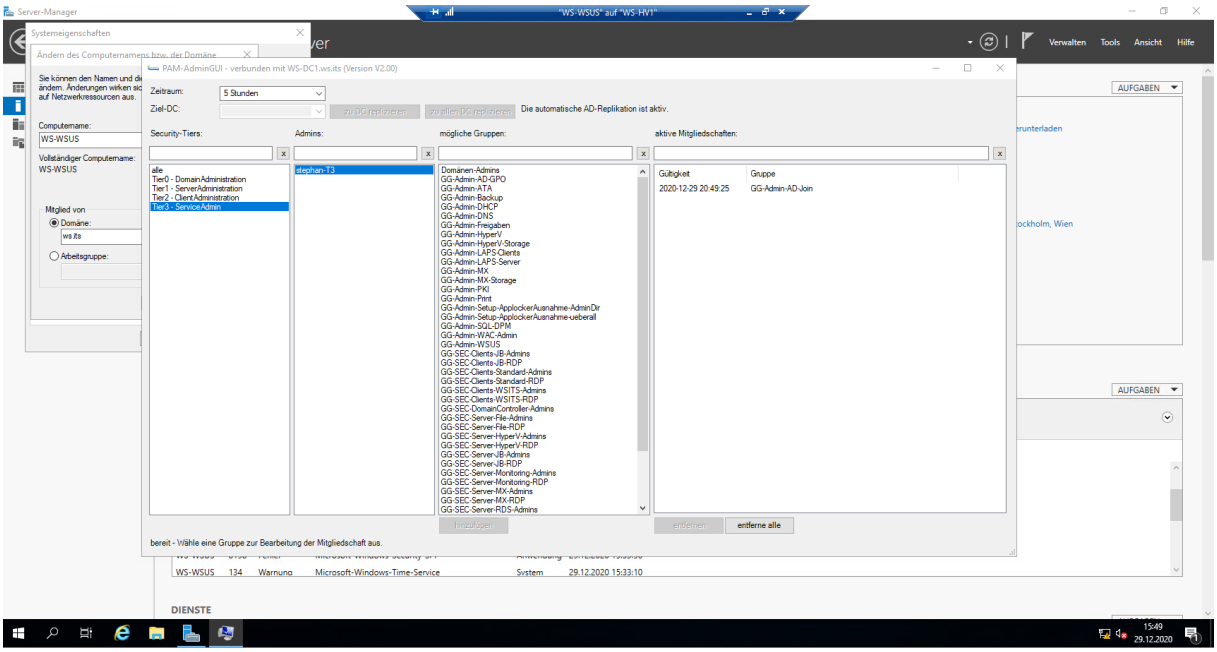
Der nächste Schritt ist das Ändern des Servernamens. Dabei verzichte ich bewusst auf den Domain Join: Der Server würde sonst mit seinem generischen Namen ins AD wechseln und sich DANACH umbenennen. Er würde also ein eigenes Computerkonto im Standard-Container „CN=Computers“ erstellen und würde so nicht in meiner Wunsch-Organisationseinheit landen. Zudem würde der Rename fehlschlagen, denn es gibt ja schon einen anderen Computer mit diesem Namen – den habe ich ja eben im AD vorprovisioniert… Also lieber eins nach dem Anderen:



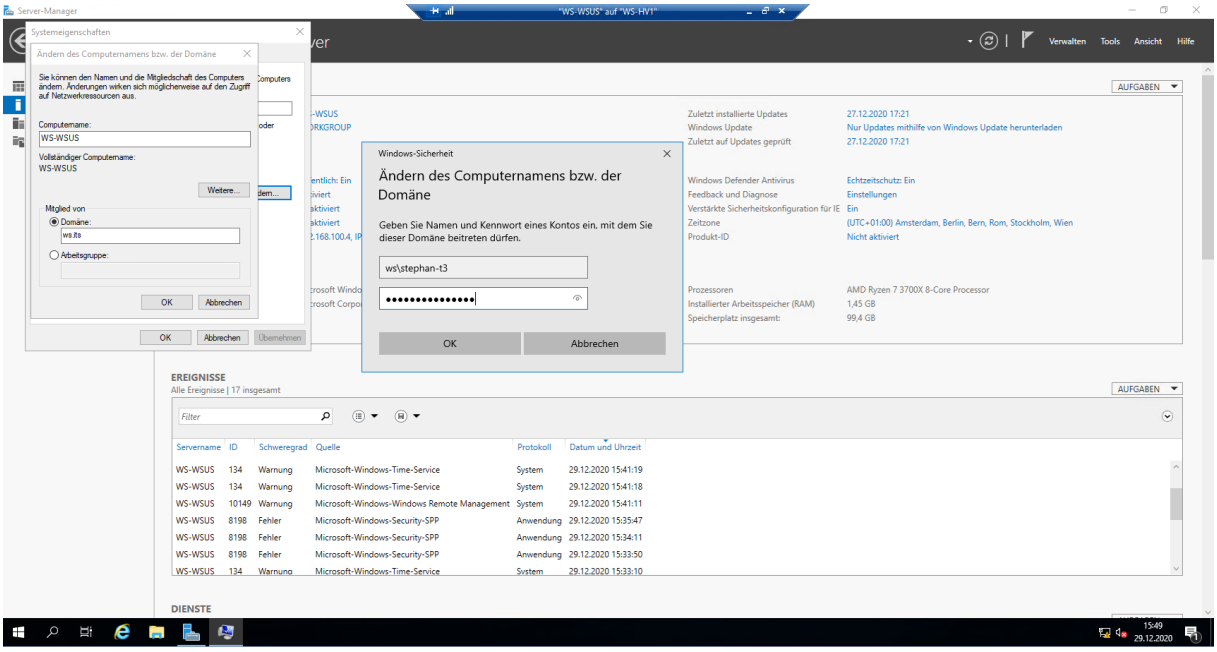
Vor dem Neustart bekommt der Server die alte IPv4 des Servers WS-CM. Damit spare ich mir in der Firewall die Anpassungen der Ausnahmen:



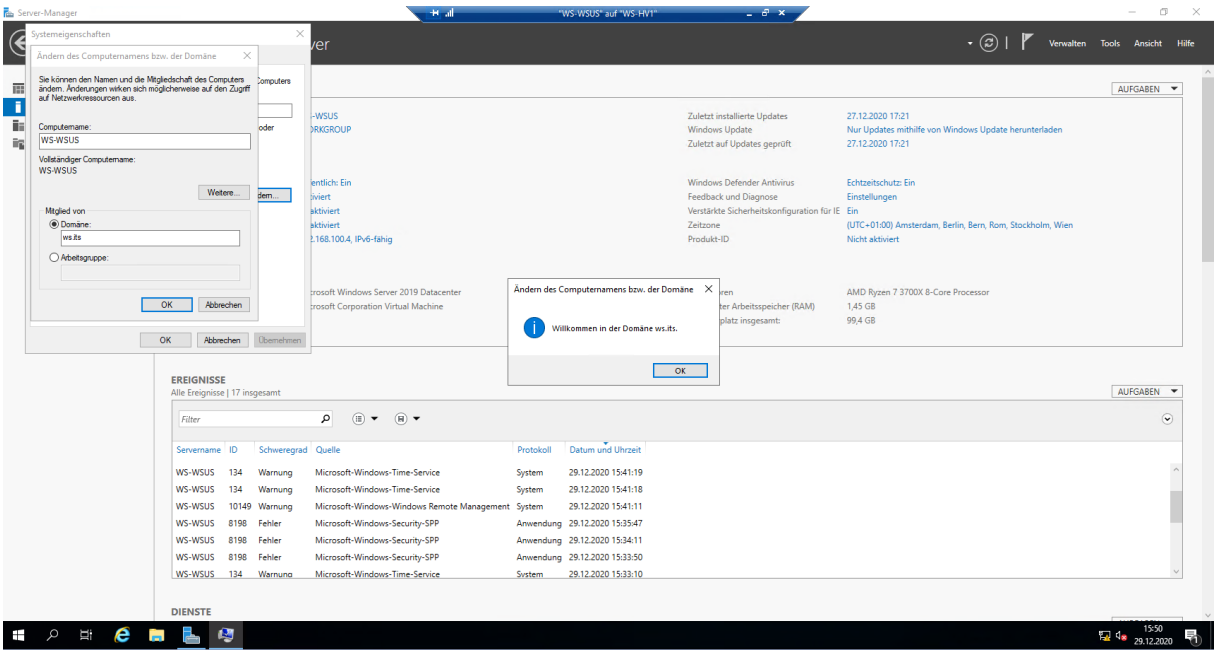
Nach einem Neustart melde ich mich wieder an und bereite den Domain Join vor. Mit meinem PAM-Tool delegiere ich die Berechtigung an meine T3-Kennung. Der Account hat sonst keine Rechte:



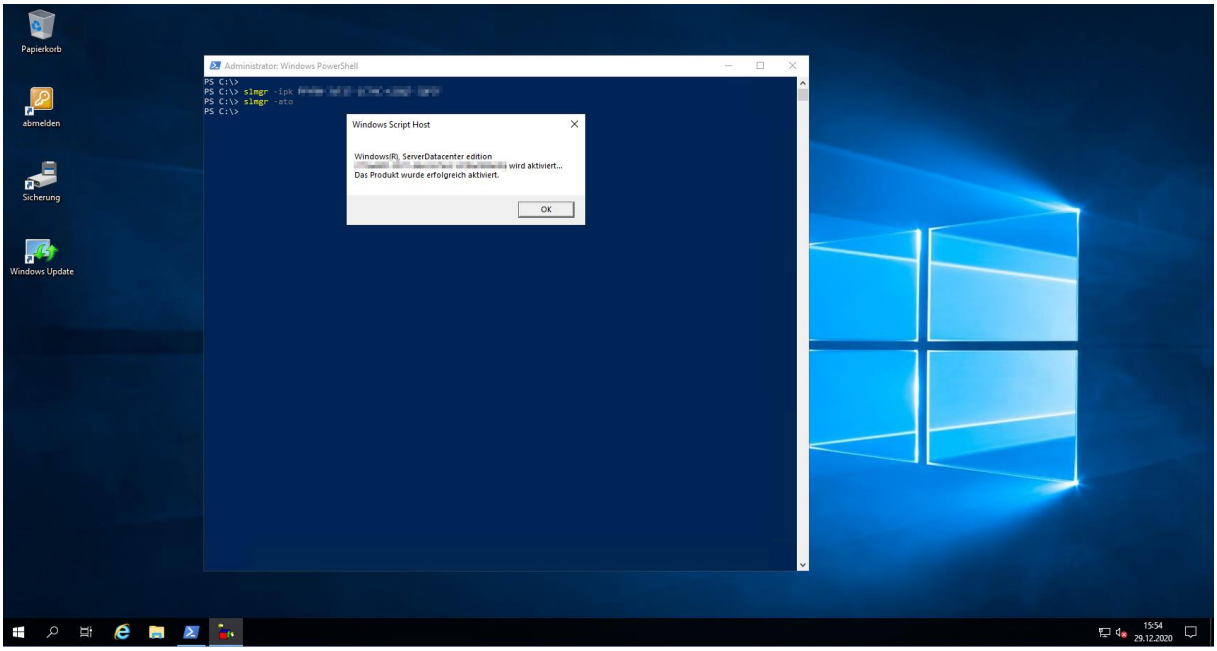
Und dann kann der Domain Join starten:



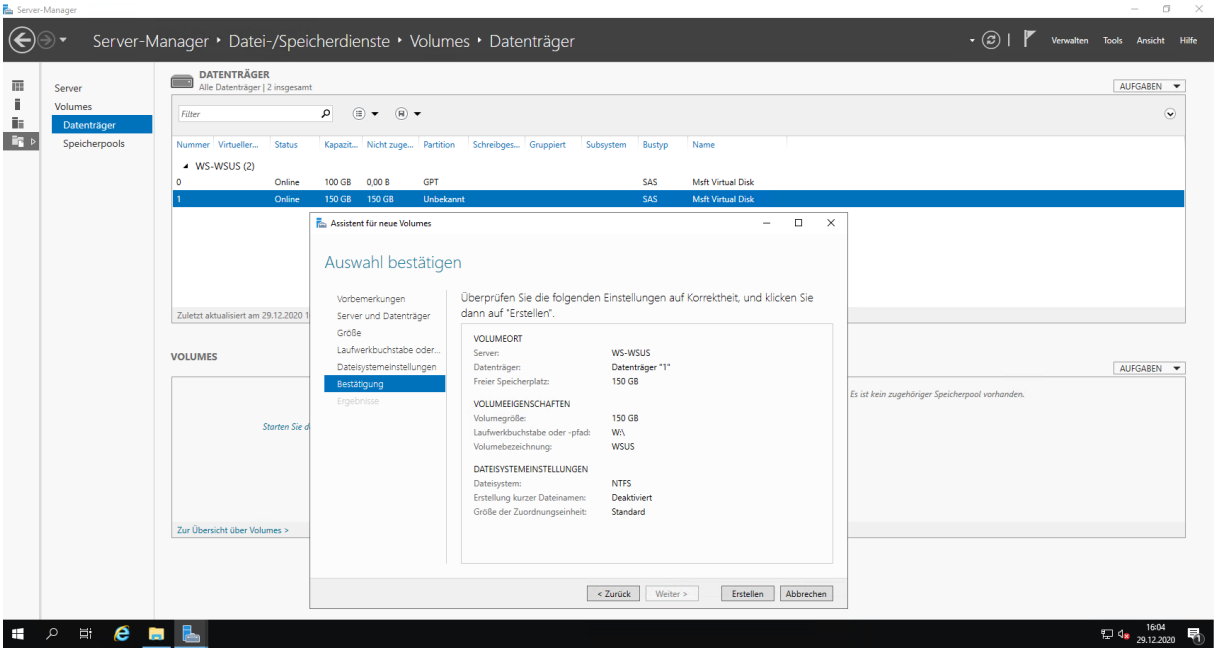
Das wäre dann auch erledigt:



Jetzt kommt noch die Aktivierung:

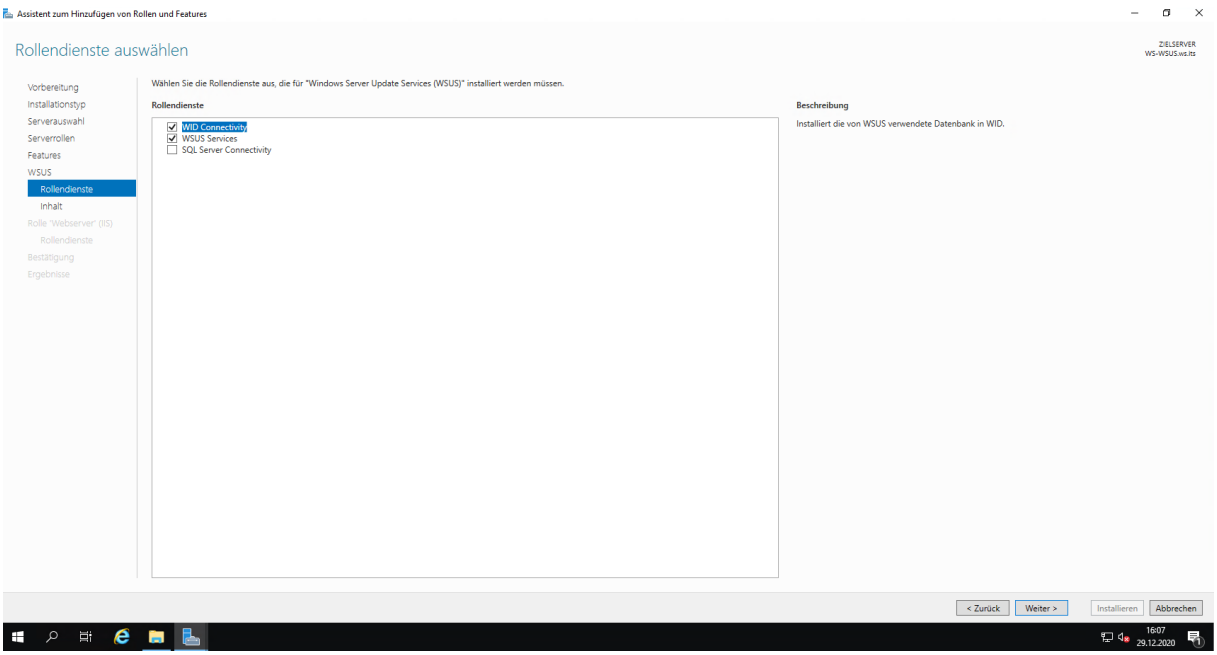


Und zuletzt wird auf dem zusätzlichen Datenträger eine Partition für die Ablage der WSUS-Updates erstellt:

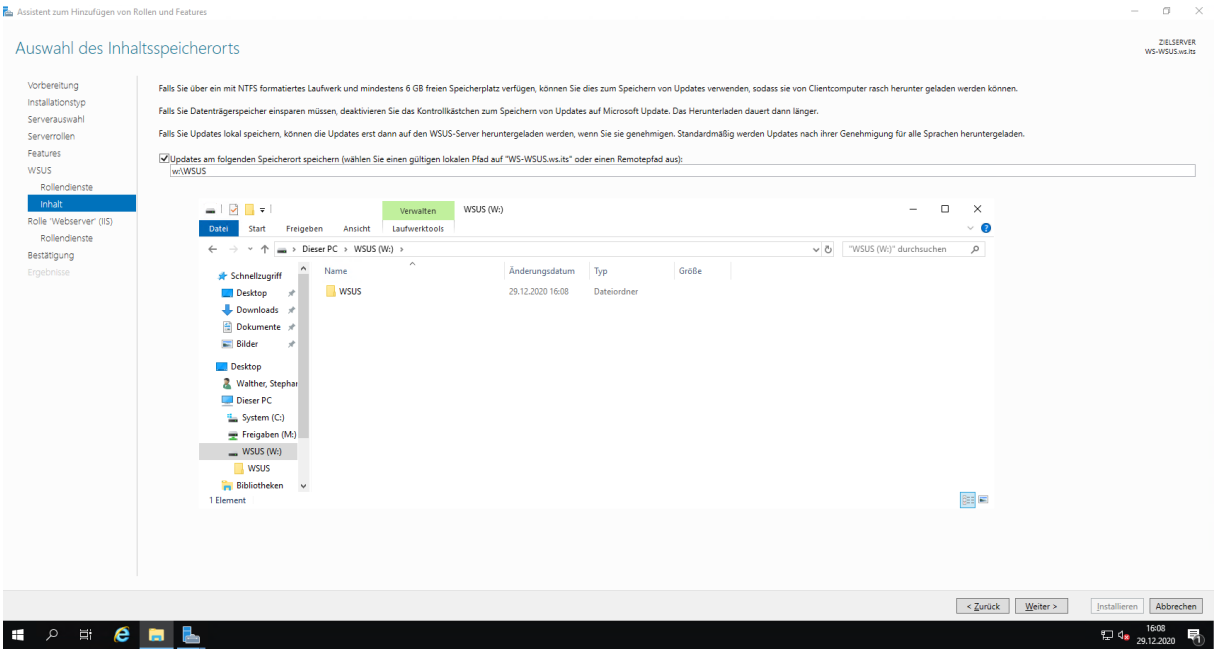


Rollen und Features

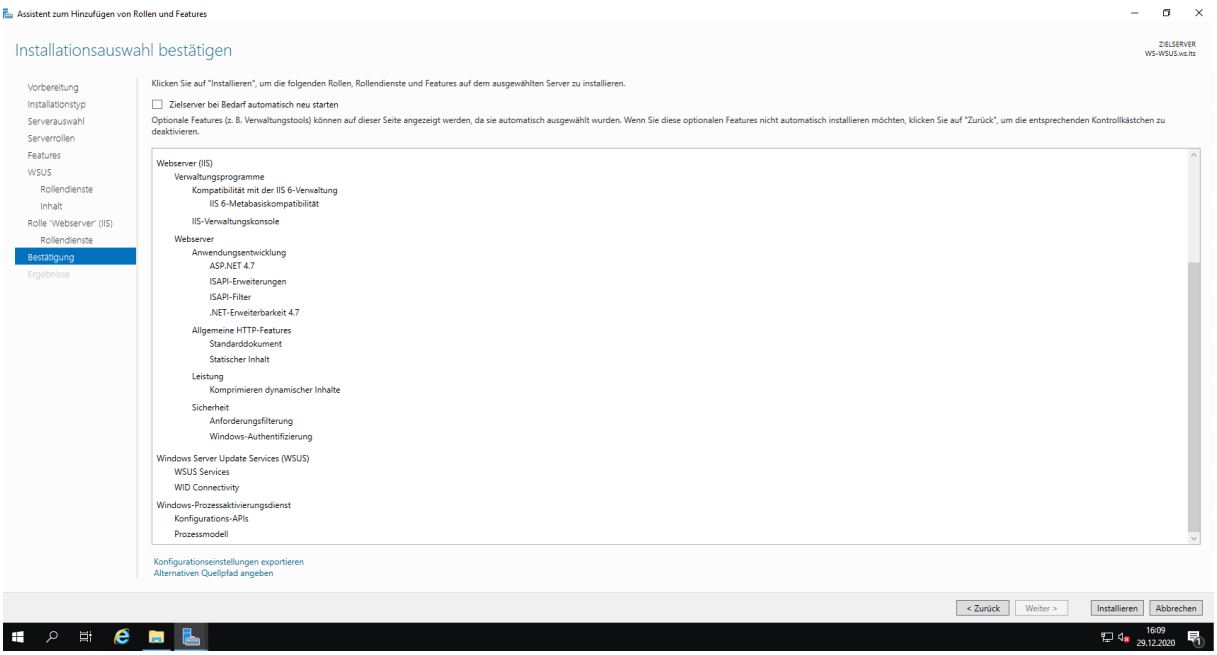
Im Server Manager starte ich die Rollen-Installation. Die Auswahl ist übersichtlich. In den Details wähle ich die Windows Internal Database aus. Diese reicht für meine Anforderungen locker aus:



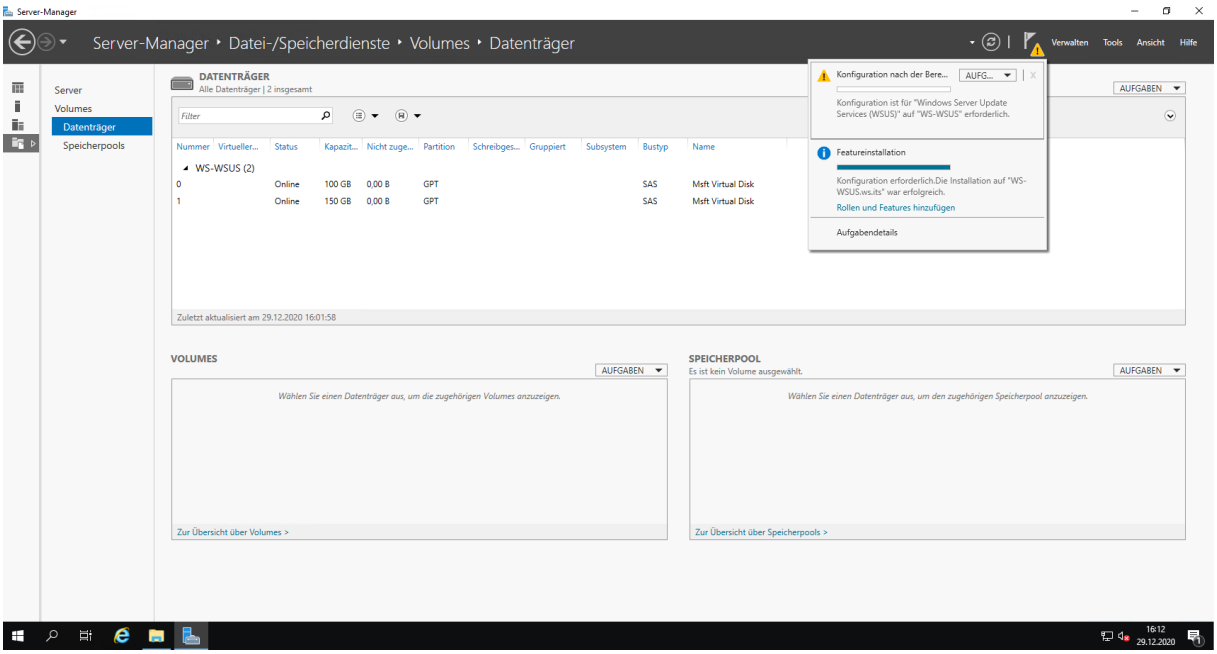
Die Rollen-Installation fragt nun den Speicherort der Updates ab. Auf der neuen Partition erstelle ich noch ein Verzeichnis in der Root. Diesen Pfad übergebe ich dann dem Server Manager:



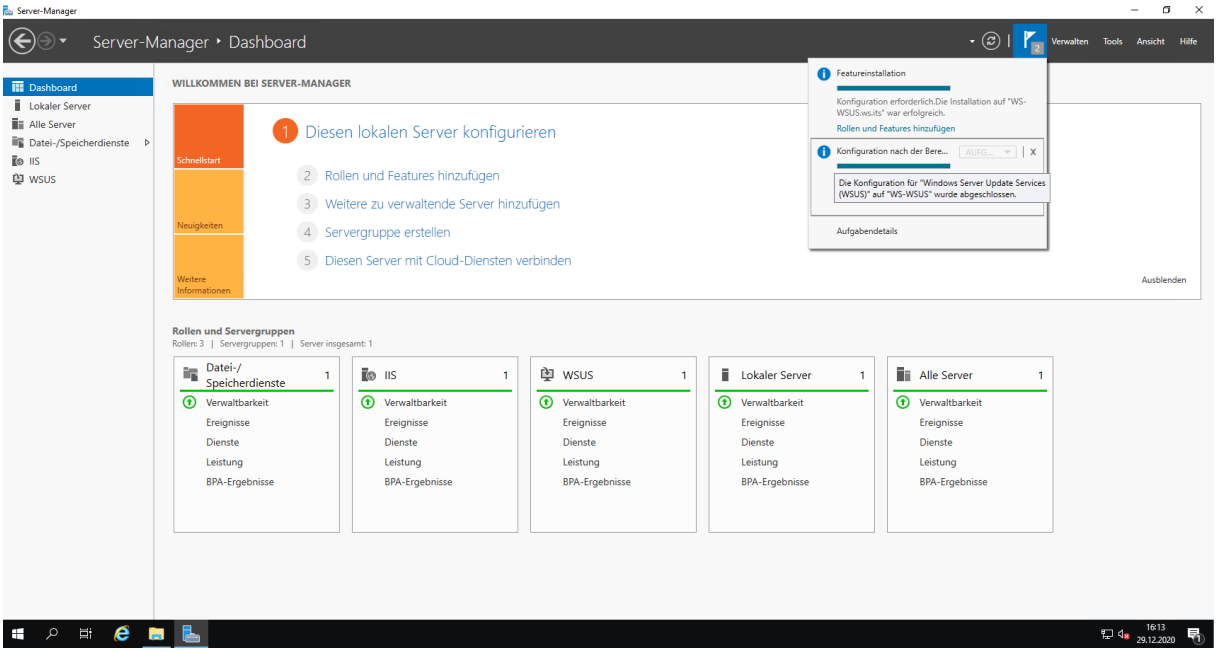
An der erforderlichen IIS-Auswahl verändere ich nichts:



Nach der Rollen-Installation starte ich das Post-Deployment:

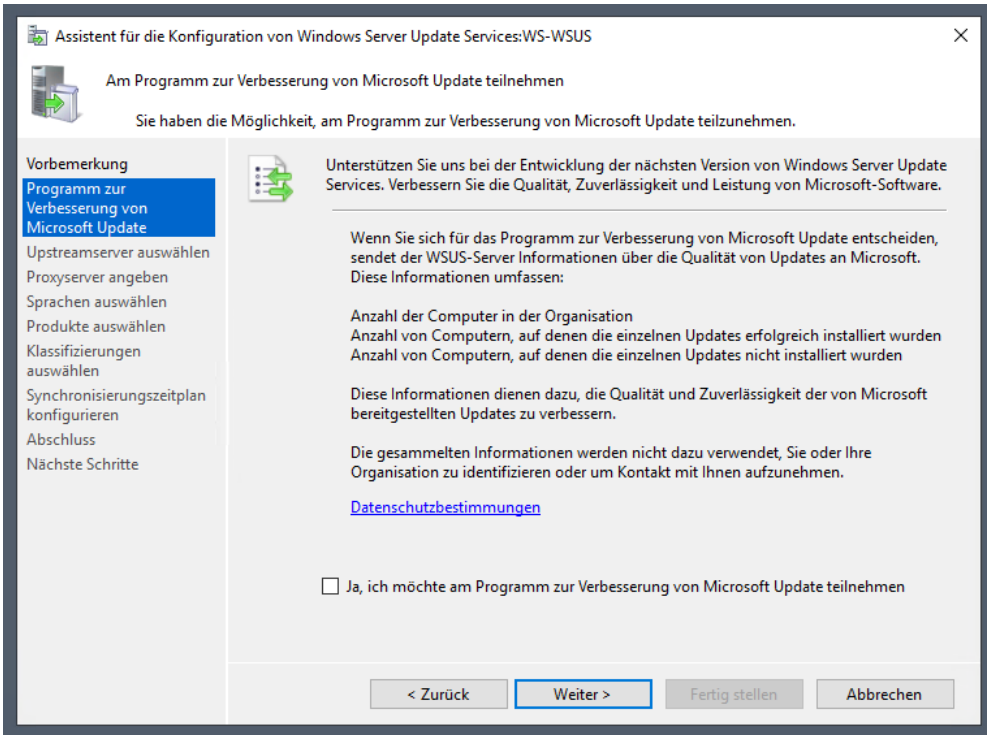


Das dauert nur wenige Sekunden:

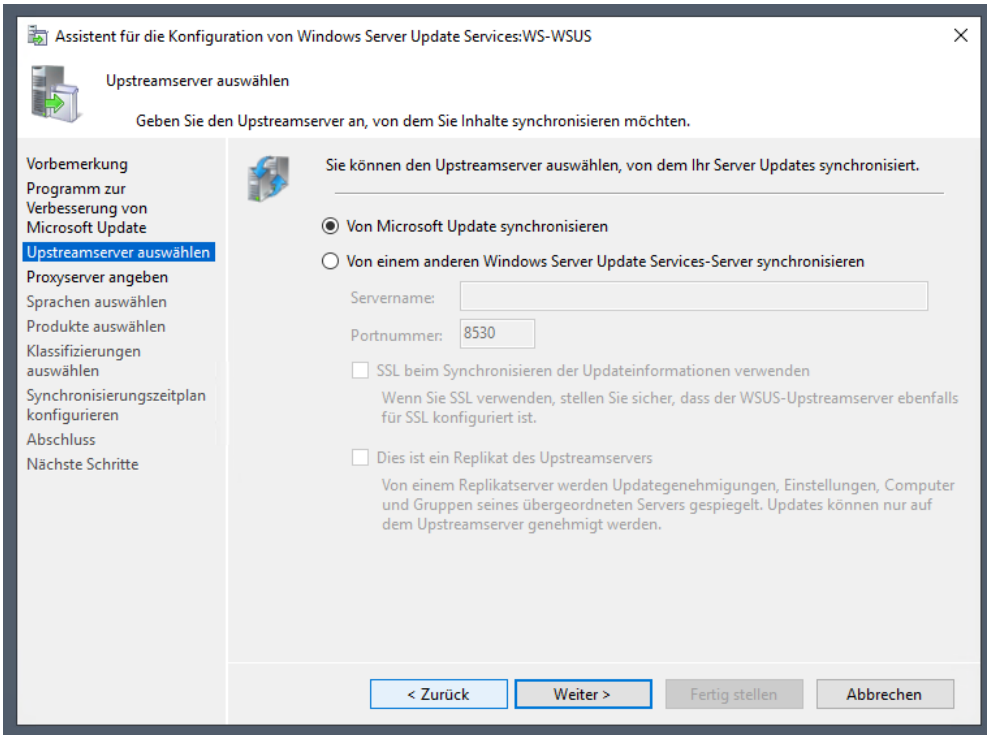


Konfiguration Rolle WSUS

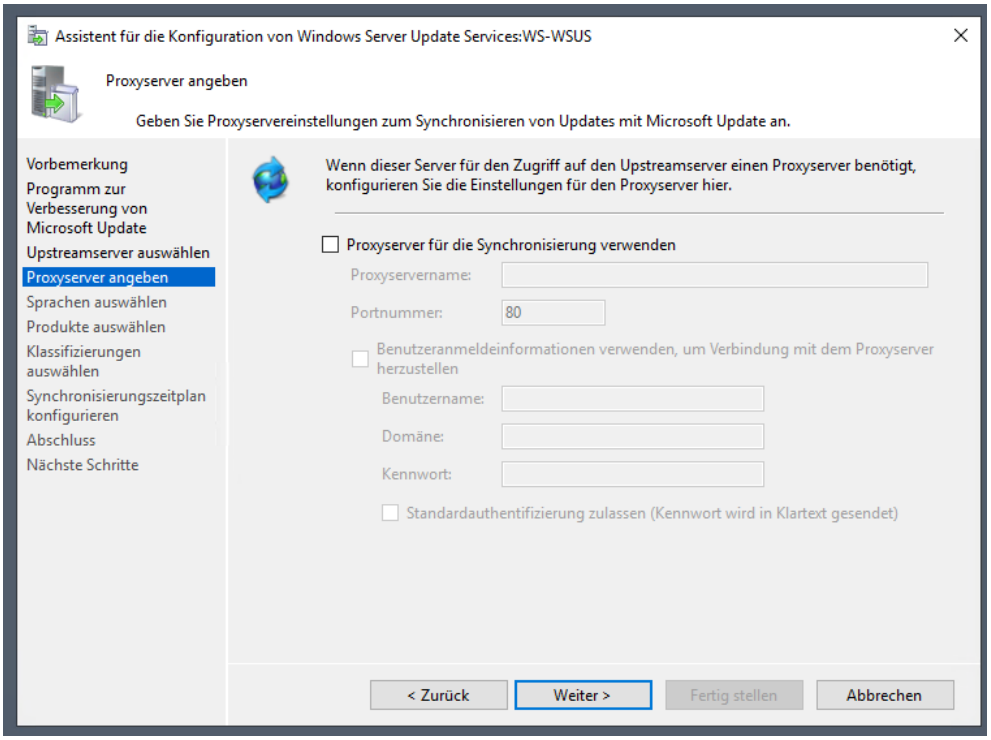
Weiter geht es mit der Feinkonfiguration des WSUS. Ich starte die Management-Konsole und mir wird der Einrichtungsassistent angezeigt:



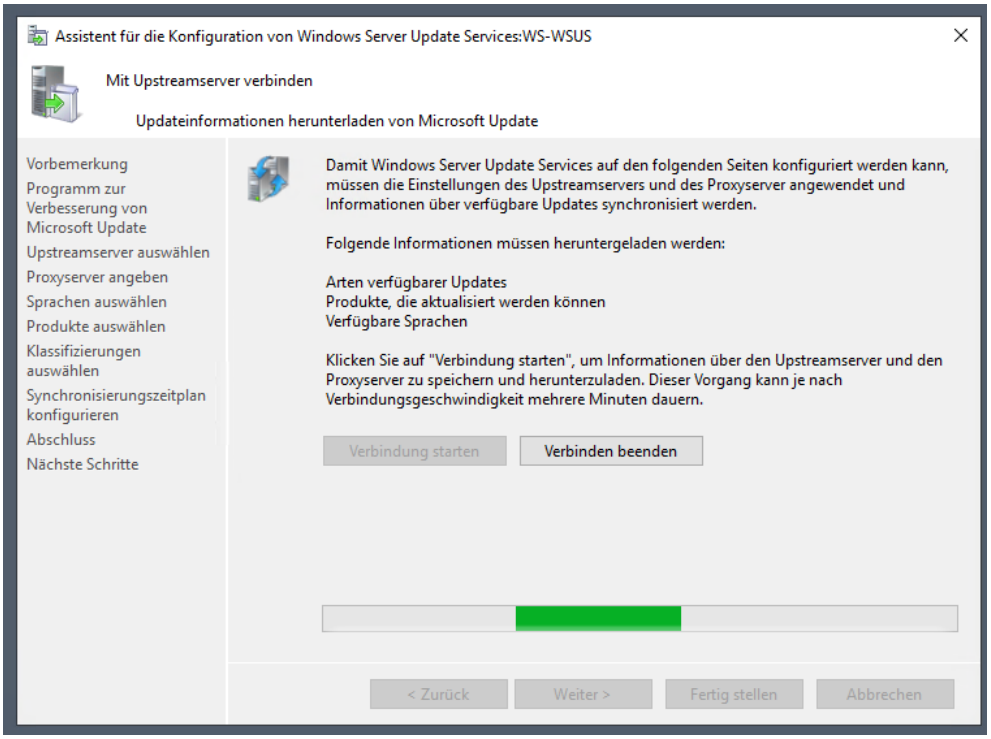
Meine flache Struktur besteht aus einem einzelnen WSUS. Dieser soll sich seine Updates direkt bei Microsoft holen:



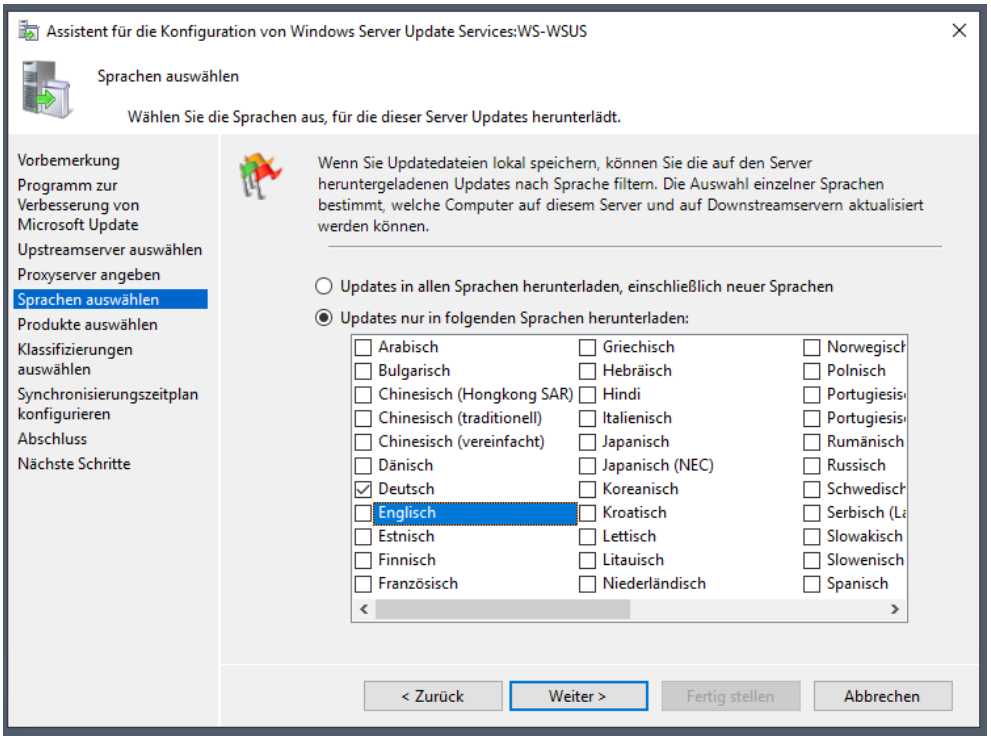
Dafür ist keine Proxy-Konfiguration erforderlich:



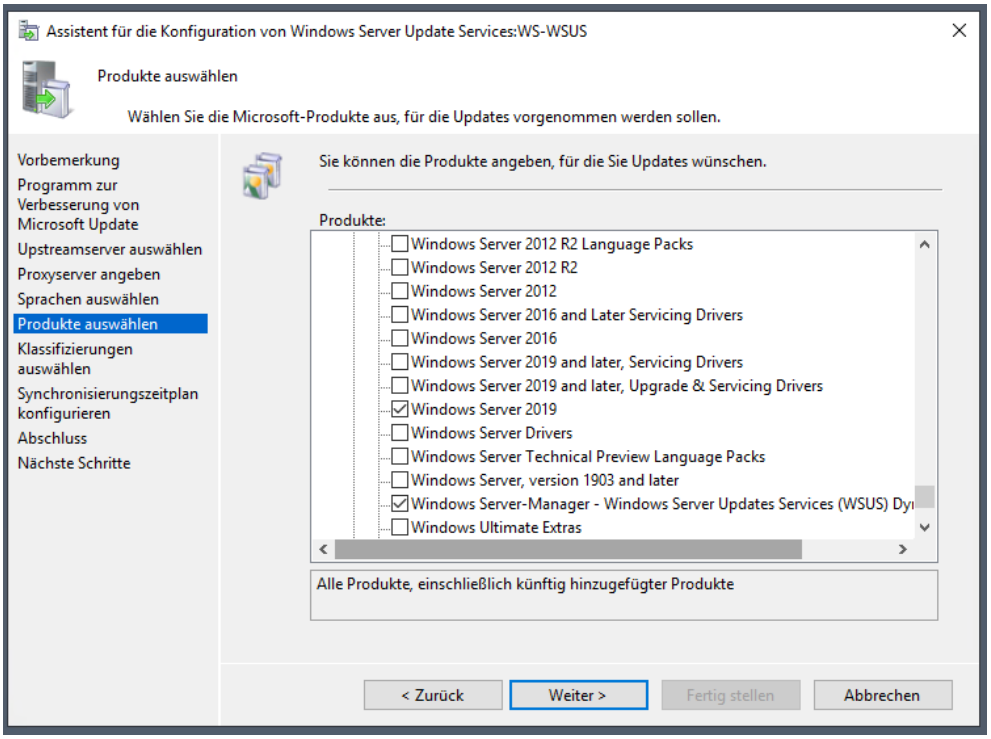
Danach vergeht eine kleine Ewigkeit, in der mein WSUS alle Informationen online abfragt und zusammenstellt:



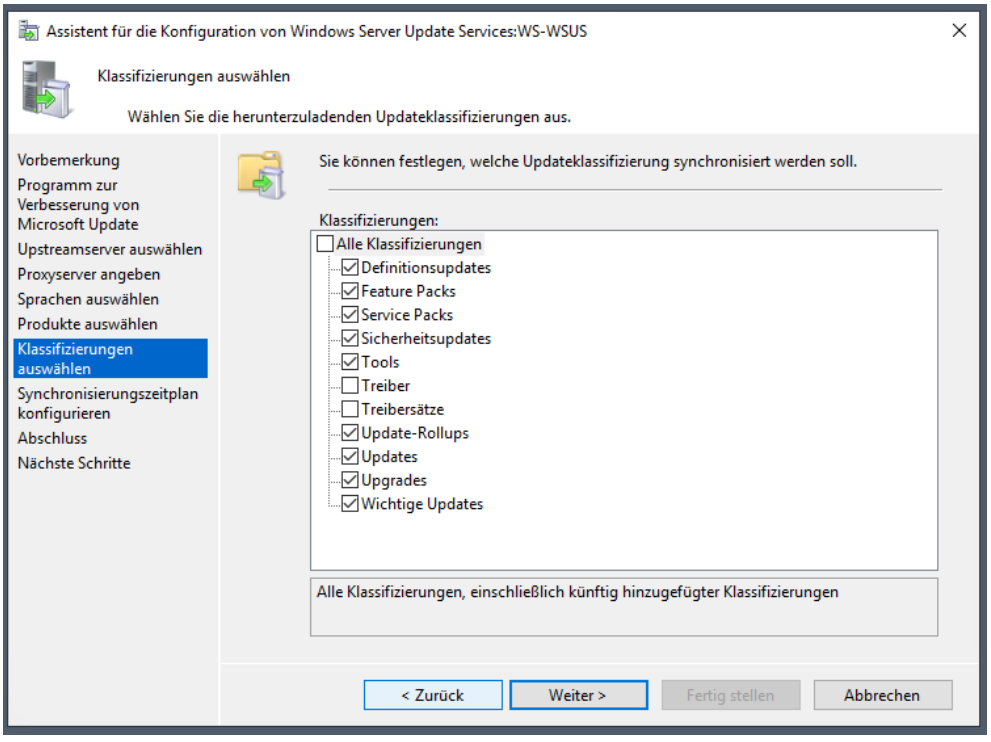
Danach kann ich die Sprachen auswählen. Wie beim alten WSUS benötige ich ausschließlich deutsche Updates:



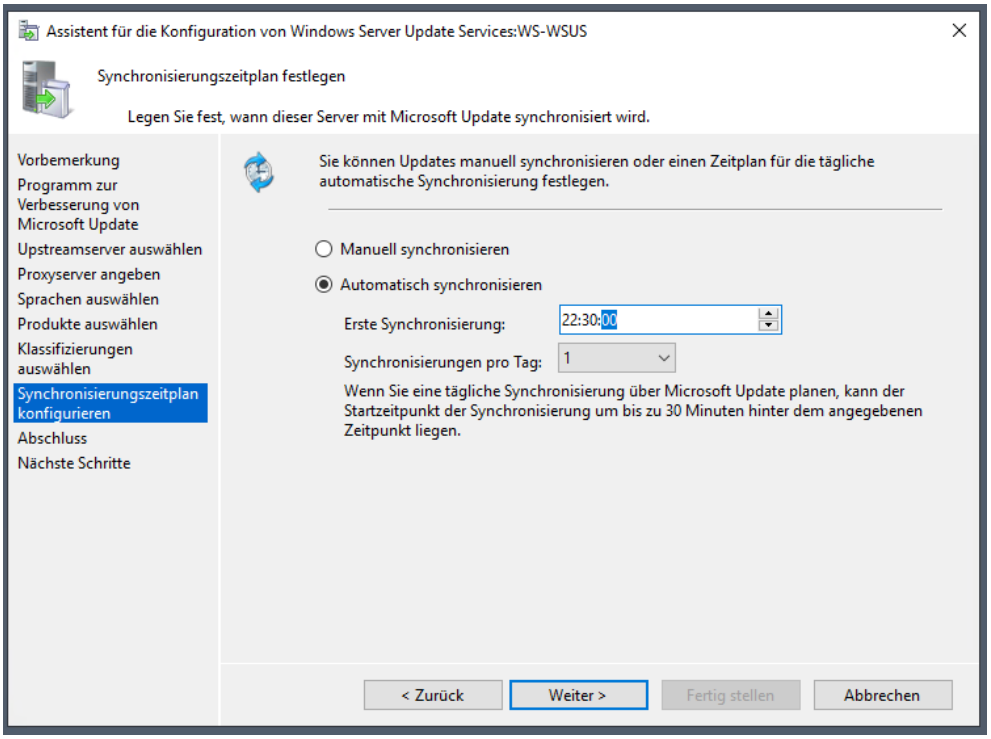
Weiter geht es mit der Auswahl der Produkte. Meine Infrastruktur ist durch meine Windows Server 2019 Migrationen sehr homogen geworden. Ich benötige nur noch Updates für dieses Server-Betriebssystem (mein letzter Server mit Windows Server 2016 wird morgen umgestellt). Windows 10 migriere ich in einigen Tagen auf 20H2. Daher lasse ich diese Werte noch außen vor:



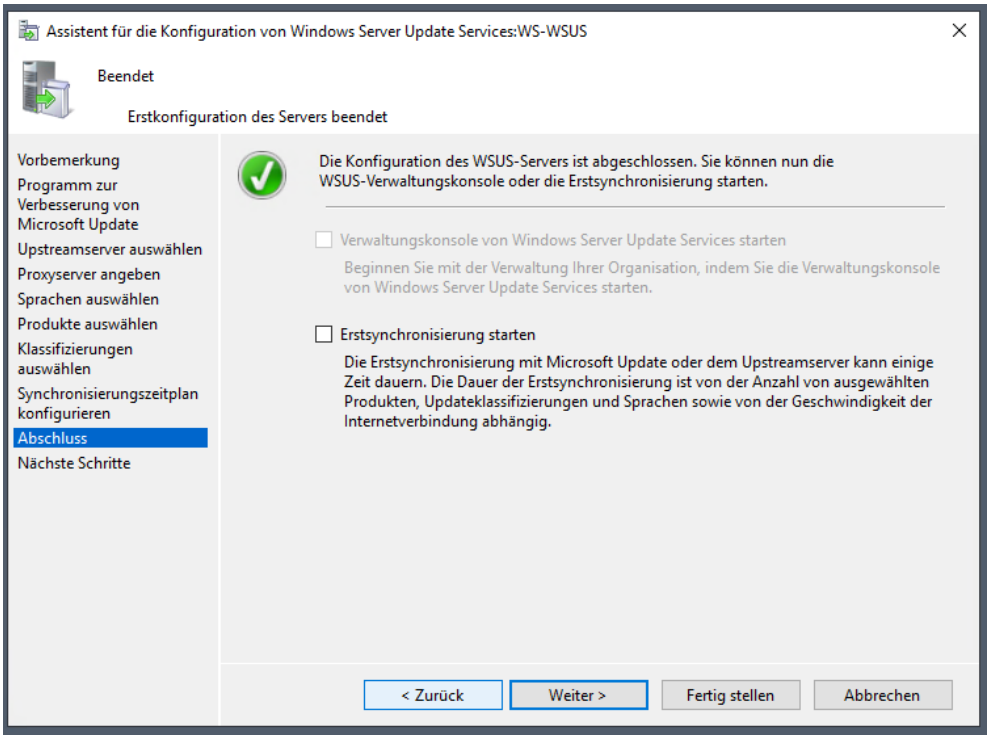
Die Klassifizierungsauswahl hat sich bewährt:



Die Synchronisierung soll wieder vor Mitternacht durchlaufen. Eine „geradere“ Zeitangabe als beim alten Server sieht aber irgendwie harmonischer aus:

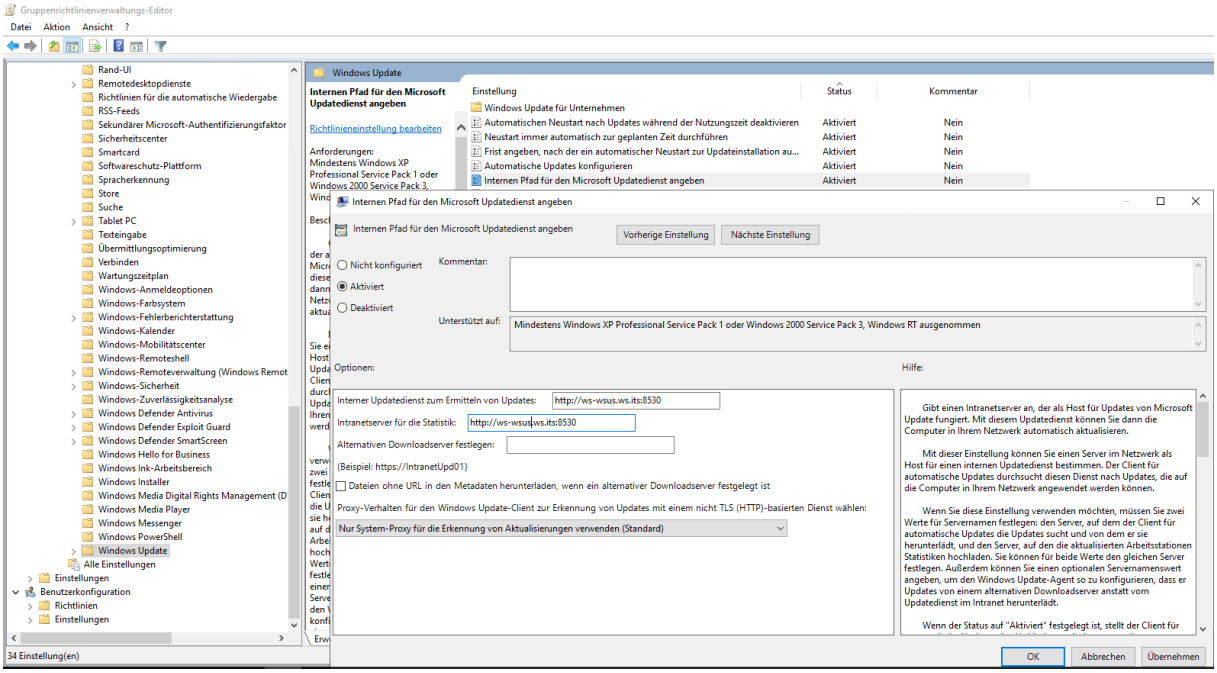


Die Erstsynchronisierung starte ich später. Die Einrichtung ist damit erst einmal abgeschlossen:

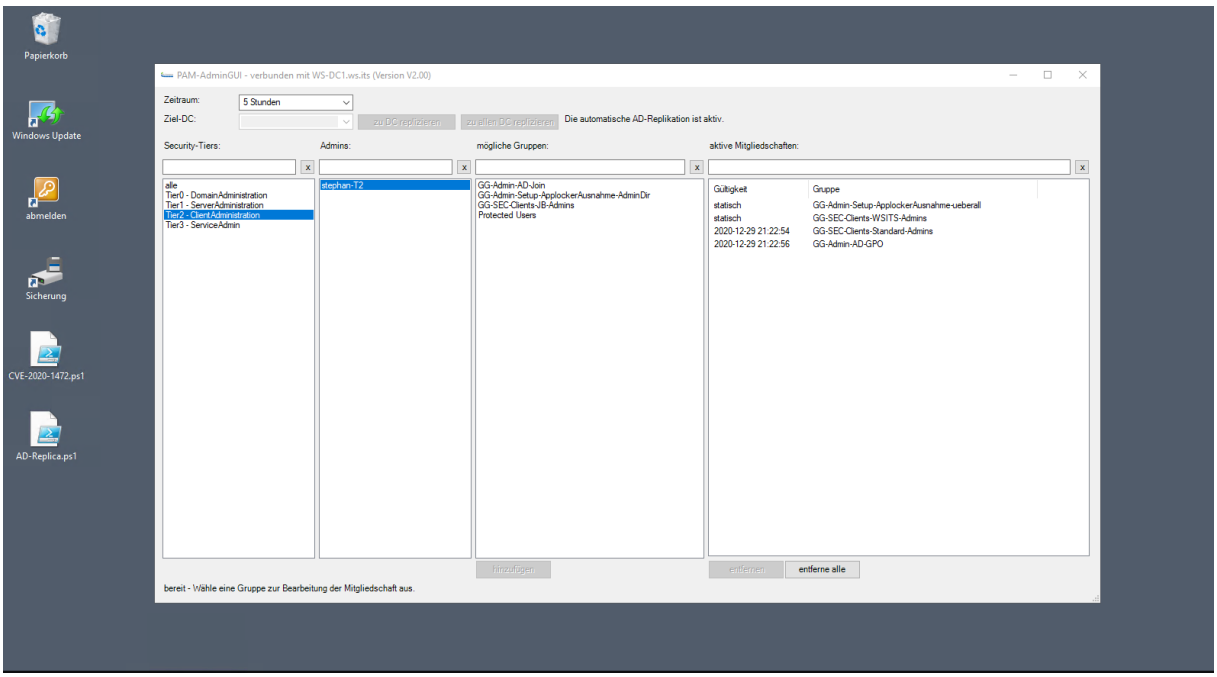


Anpassung Gruppenrichtlinie

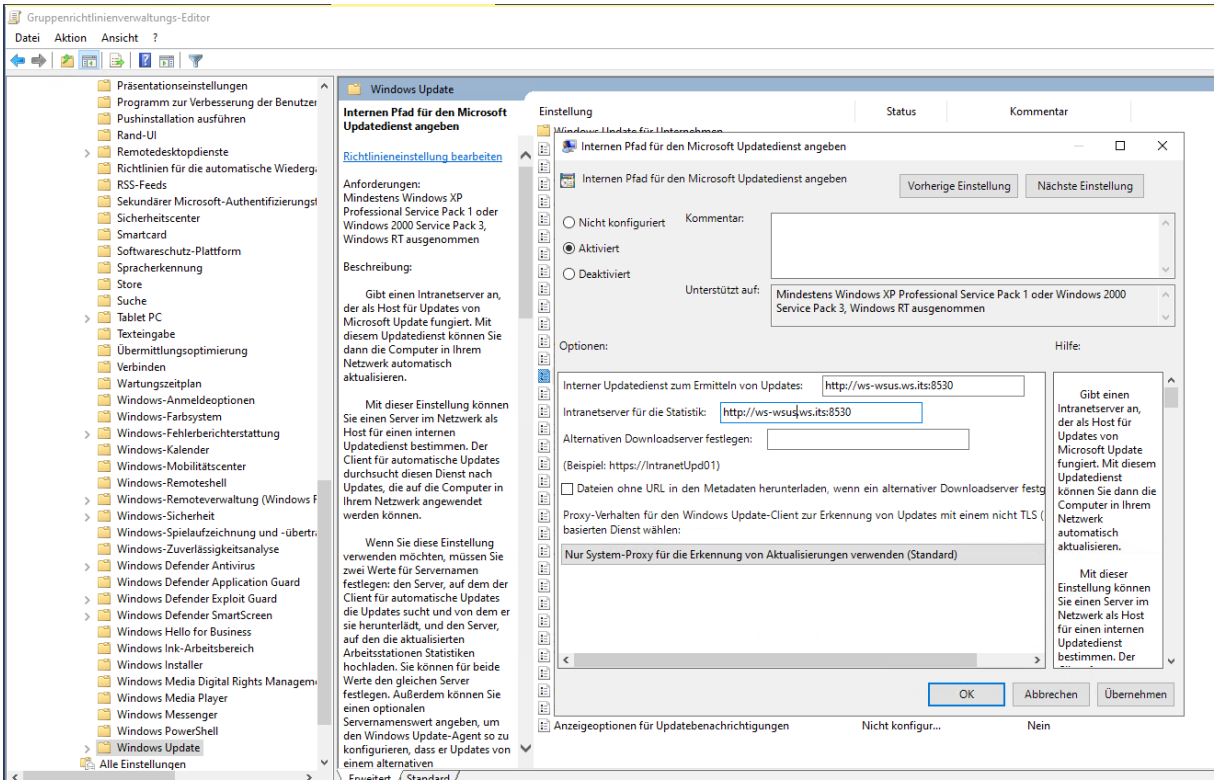
Dennoch wird der neue Server von meinen Systemen nicht gefunden, denn er hat einen anderen Namen. Auf meinem Domain Controller passe ich nun die entsprechenden Gruppenrichtlinien an. So lenke ich meine Clients und Server auf den neuen WSUS. Die Server-GPO editiere ich direkt auf dem Domain Controller:



Die Clients arbeiten aber nicht mit Windows Server 2019, sondern mit Windows 10 v1909. Dieses Betriebssystem unterscheidet sich vom Server. Demnach gibt es auch immer wieder Probleme mit der Verwendung der falschen Gruppenrichtlinien-Vorlagen (ADXM). Daher editiere ich die Client-GPO auf einem Windows 10 Rechner, den ich als GPO-Editorsystem eingerichtet habe. Meine T2-Kennung (Clientadmin) muss dafür temporär für die Editierung der Gruppenrichtlinien berechtigt werden. An die Gruppe GG-Admin-AD-GPO habe ich das Recht im AD delegiert:

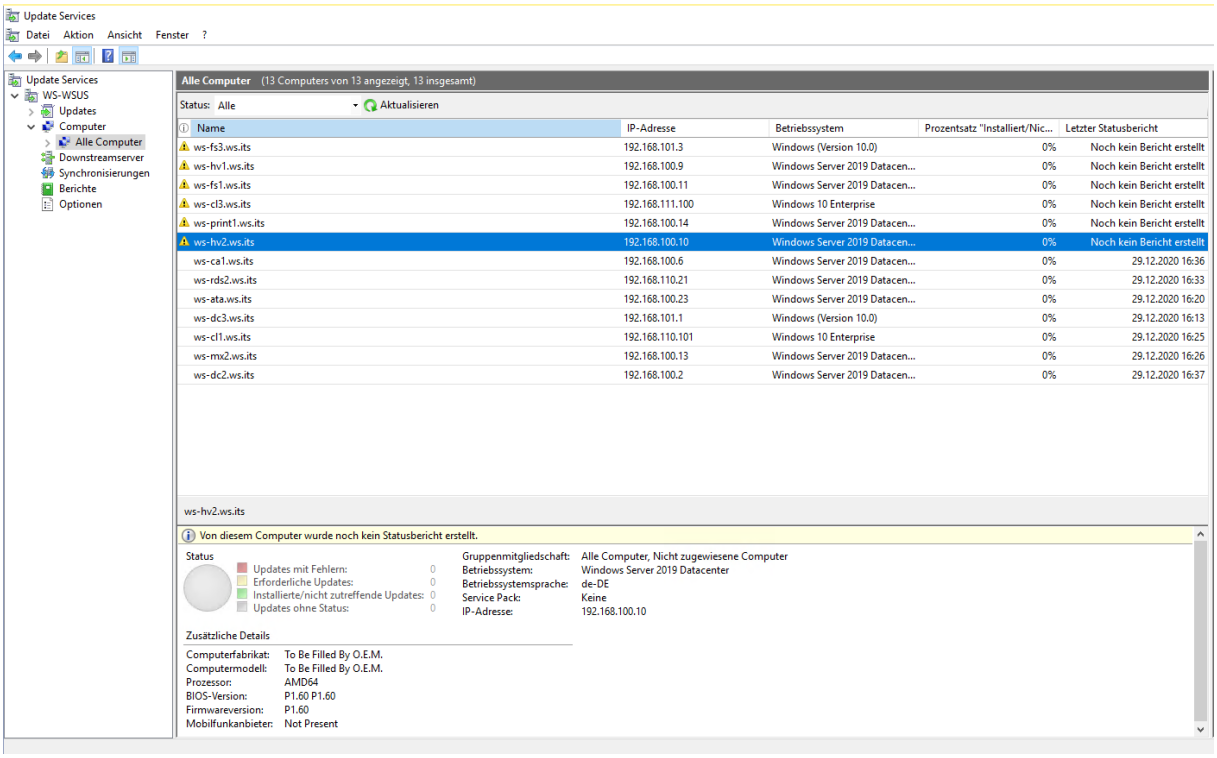


Dann suche ich die Client-GPO und passe den WSUS-Eintrag an:



Feintuning WSUS

Nach einem gpupdate oder einer passenden Wartezeit melden sich die Systeme meiner Infrastruktur nach und nach beim neuen WSUS. Dabei werden alle im Container „nicht zugewiesene Computer“ aufgenommen:

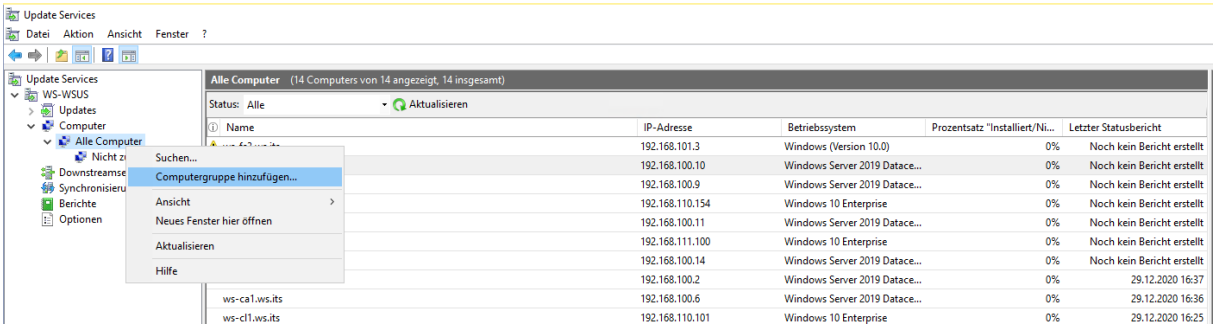


Meine Aktualisierungen möchte ich direkt mit der WSUS-Konsole kontrollieren können. Meine Gruppenrichtlinie weist alle Clients und Server an, Updates automatisch zu installieren (es gibt für meine Hyper-V-Hosts eine Ausnahme). Wenn nun aber alle Systeme im gleichen Container liegen und ich auf diesem die Updates genehmige, dann installieren alle zeitgleich die Updates und starten danach auch neu. Das würde einiges durcheinanderbringen. Daher werde ich ein anderes Verfahren konfigurieren:

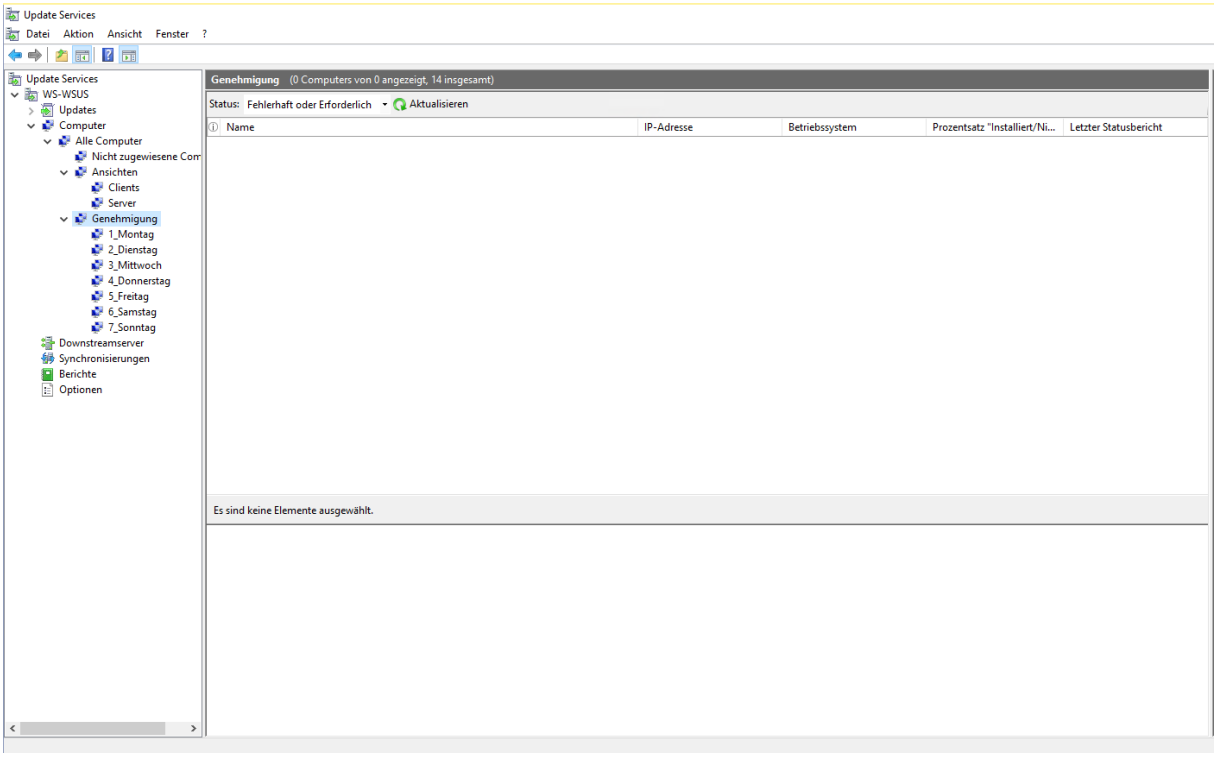
- Ich erstelle neue Container und verteile meine Server und Clients sinnvoll auf diese.
- Die Updates werden dann an unterschiedlichen Tageb auf den Containern genehmigt.
- So kommen zwar alle Systeme täglich zum WSUS, aber nur die Systeme im passenden Tages-Container erhalten ihre Updates und starten neu.

Das verteilt die Last und auch die Neustarts. Zudem kann ich so auch „schlechten“ Updates begegnen. Diese würden eben nur einen Teil meiner Server „versauen“ und ich könnte die Verteilung auf den anderen Containern rechtzeitig aufhalten.

Neue Container können einfach erstellt werden:

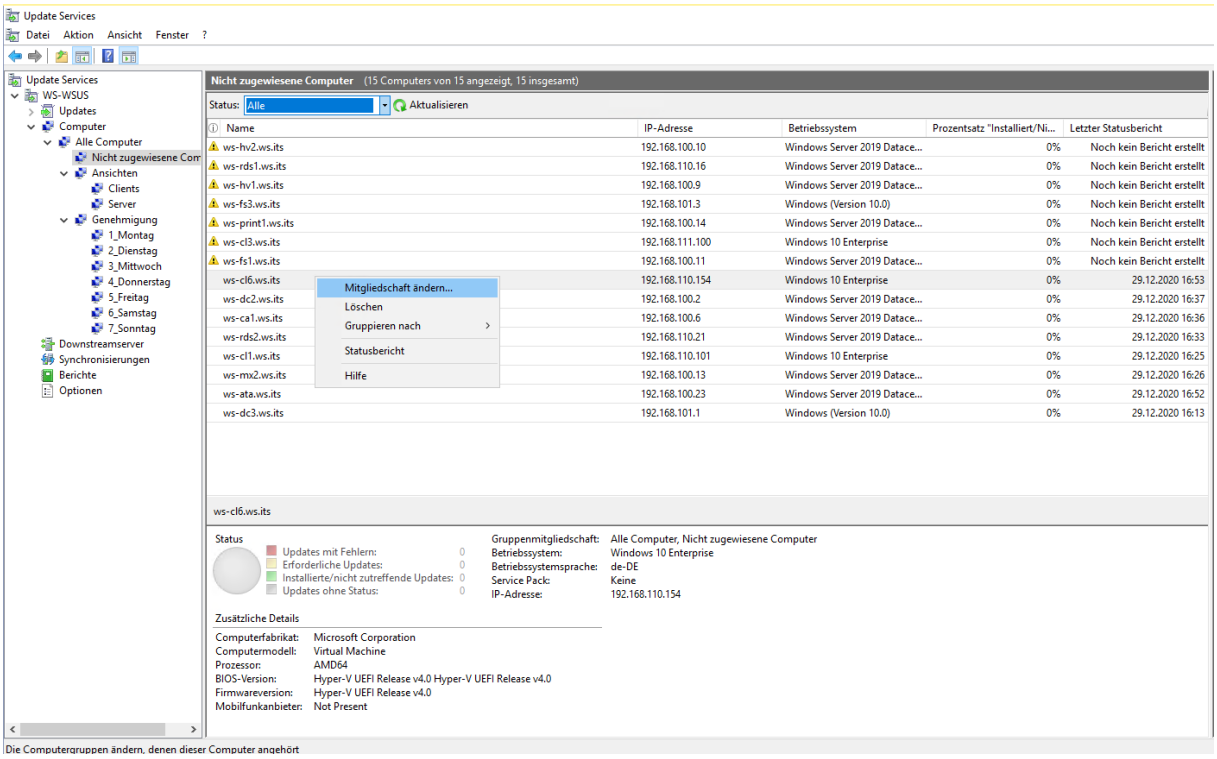


Ein paar Minuten später ist meine Wunsch-Struktur fertig. Der Haupt-Container „Genehmigung“ wird durch mein Genehmigungs-Script vollautomatisch bearbeitet. Hier muss jeder Server in genau einem Tages-Container platziert werden:

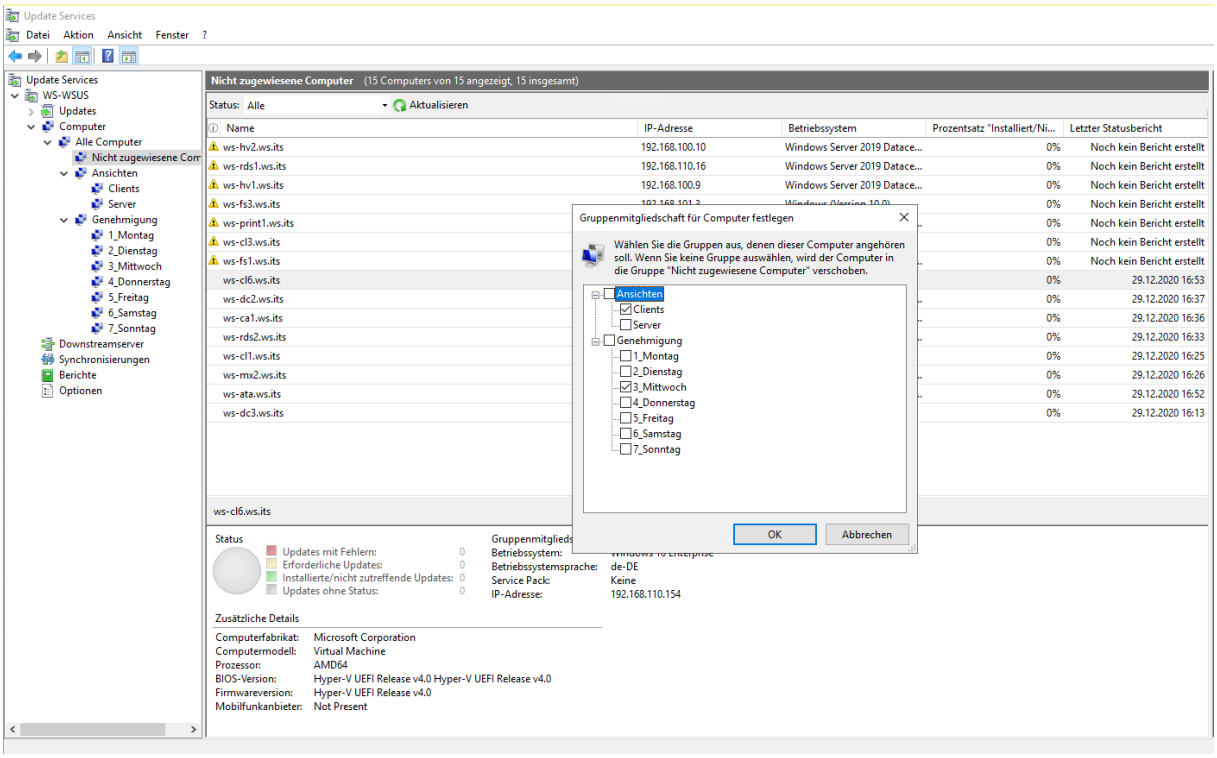


Der Haupt-Container „Ansichten“ ist für eine logische Gruppierung der Systeme gedacht. Hier setzt ein anderes Script an zud zeigt mir das Ergebnis der Updates gruppiert nach Clients und Server an – oder welche Gruppierung ich auch immer wünsche. Jedes System muss auch hier genau einer Ansicht zugeordnet werden.

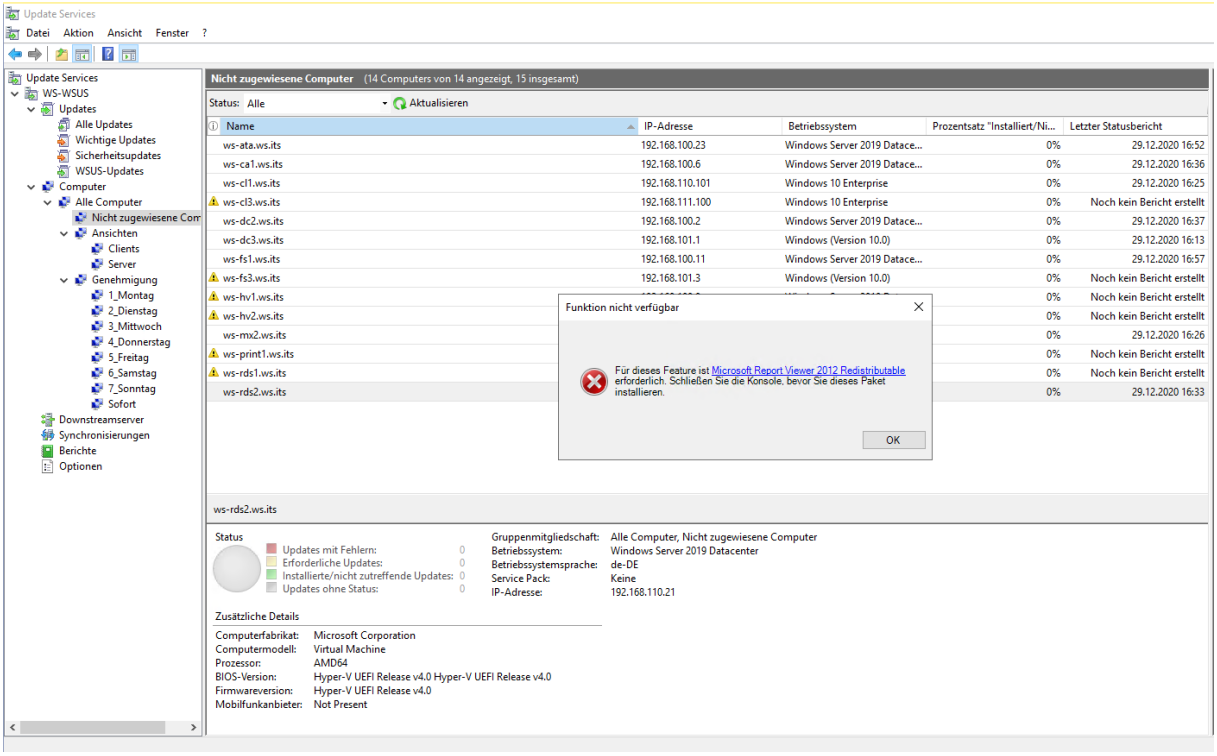
Das muss ich nun für jeden Computer konfigurieren:



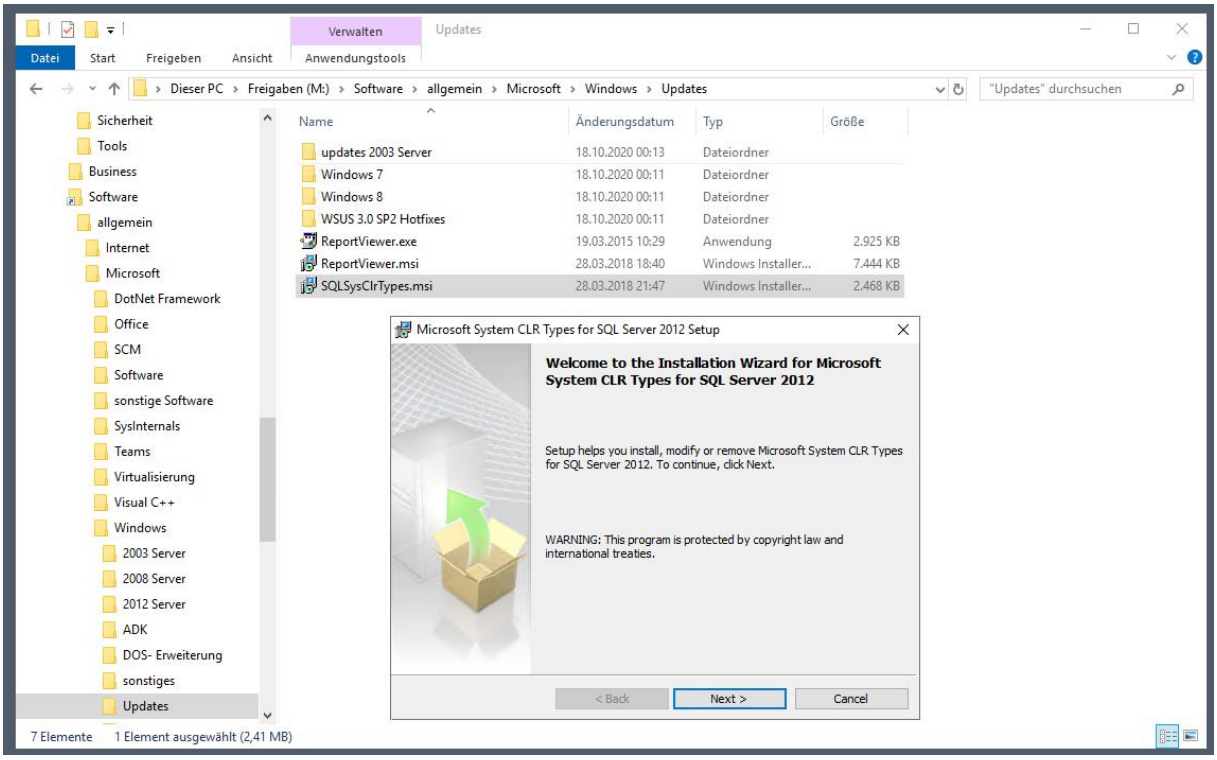
Ein Computer kann in mehreren Containern Mitglied sein. Und meine Regel lautet: genau eine Ansicht und genau ein Tages-Container muss ausgewählt werden:



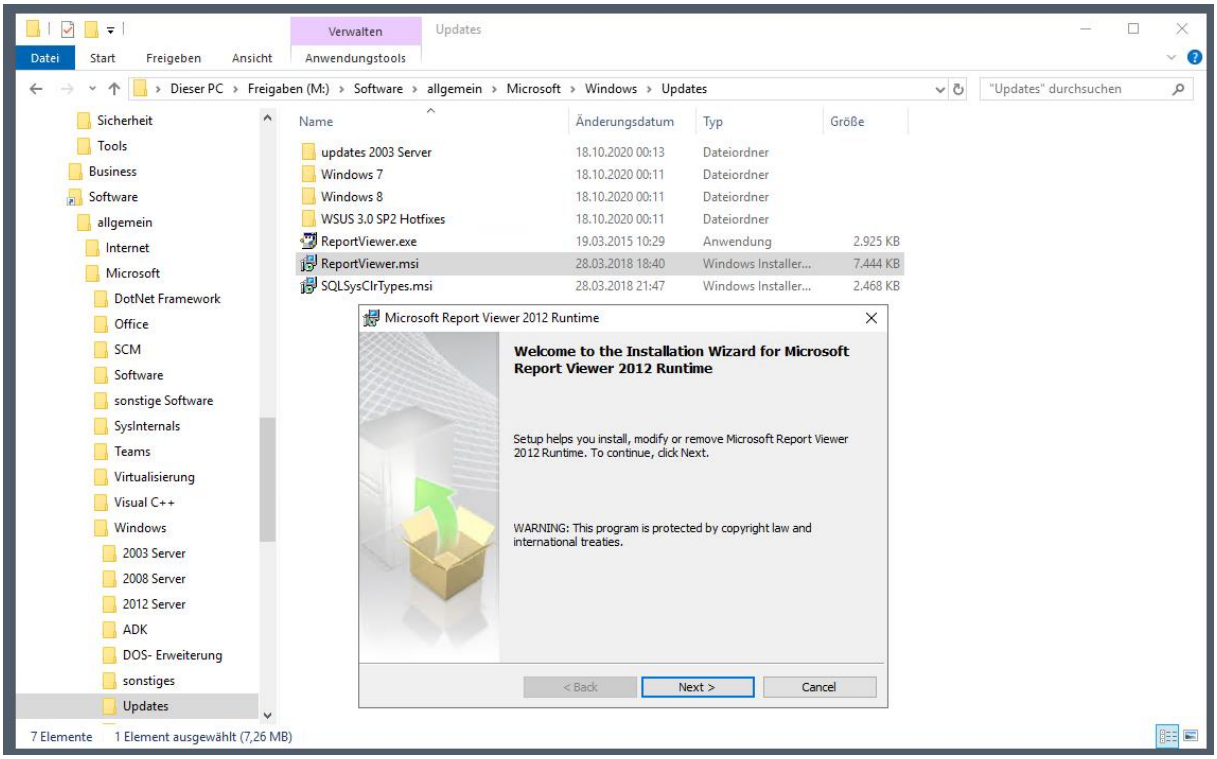
Nachdem ich mir hier ein neues Layout definiert habe geht es zu einer fehlenden Erweiterung. Die Details zu den Computern und Updates werden nur nach der Installation dieses Hilfstools angeteigt:



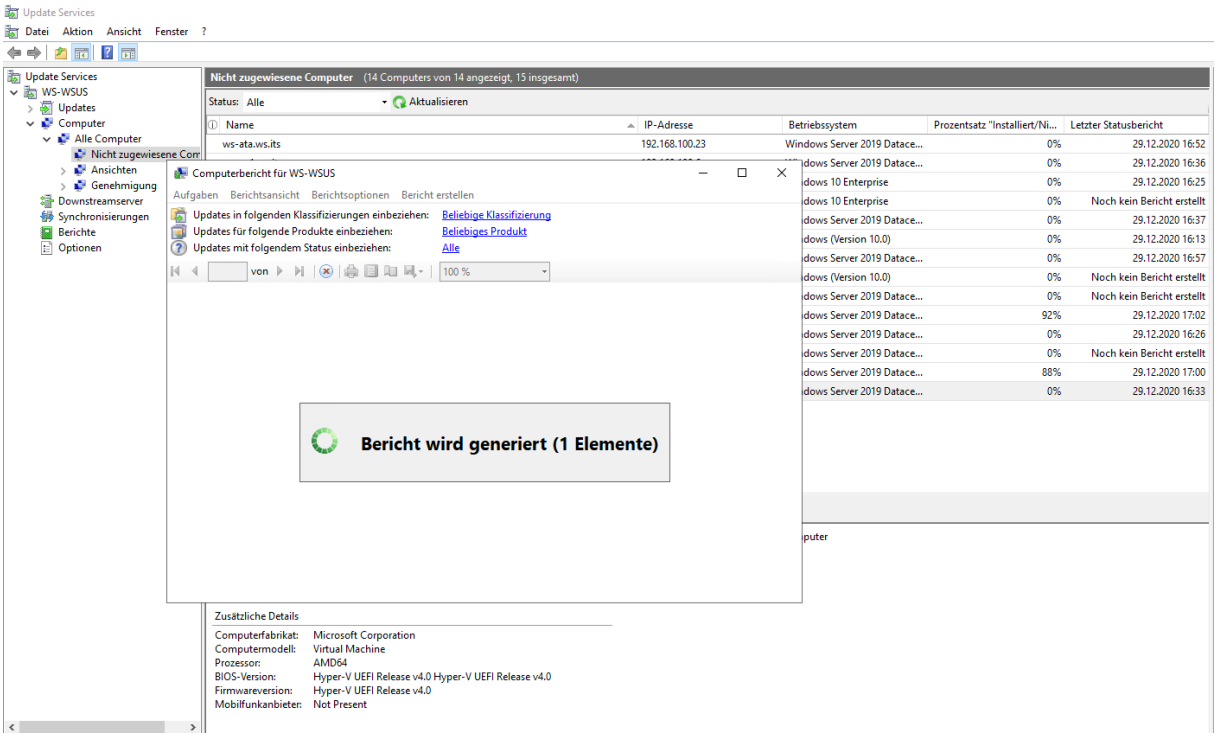
Das Setup habe ich bereits in der Schublade auf meinem Fileserver. Der Report Viewer braucht zusätzlich noch die CLR Types vom SQL Server:



Danach kann der Report Viewer installiert werden:

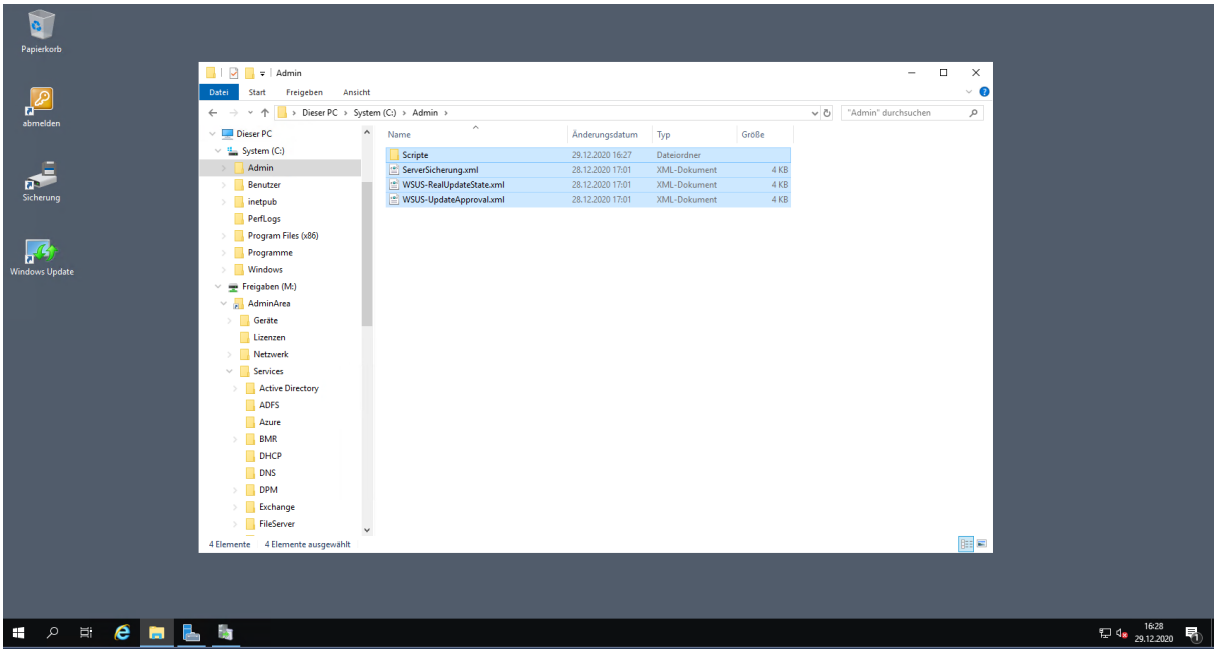


Nach einem Neustart der WSUS-Konsole wird ein Testbericht generiert:

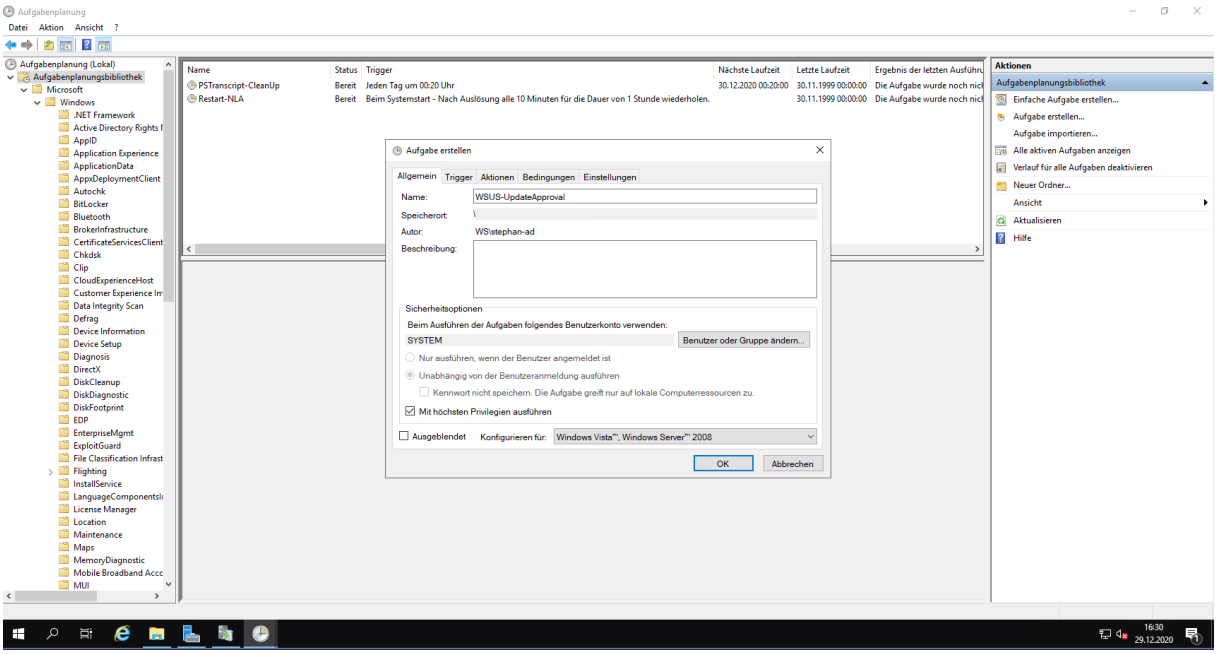


Script-Automation

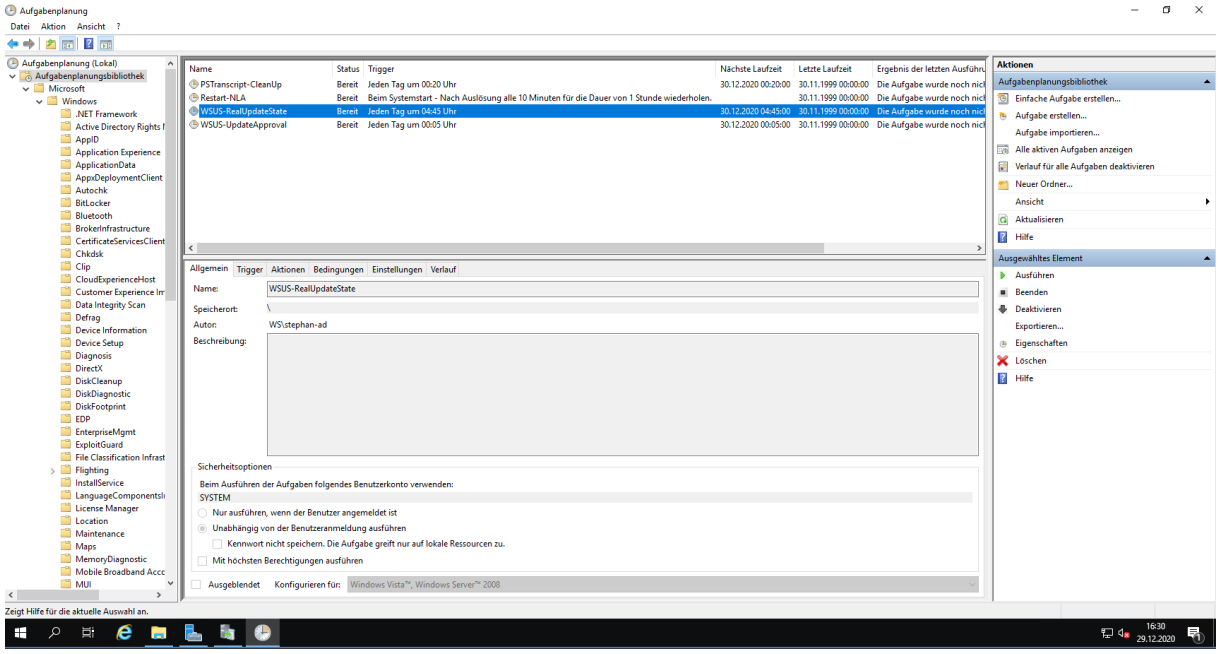
Im nächsten Schritt bringe ich meine Automationsscripte in den WSUS ein. Dabei handelt es sich um PowerShell-Scripte, die über geplante Aufgaben automatisch gestartet werden. Die Aufgaben hatte ich auf dem alten Server in XML-Dateien exportiert. Zuerst kopiere ich mir die Verzeichnisse und die XML-Dateien nach Laufwerk C:



Dann kann ich die Aufgaben importieren. Ich beginne mit dem Genehmigungsscript „WSUS-UpdateApproval.ps1“:



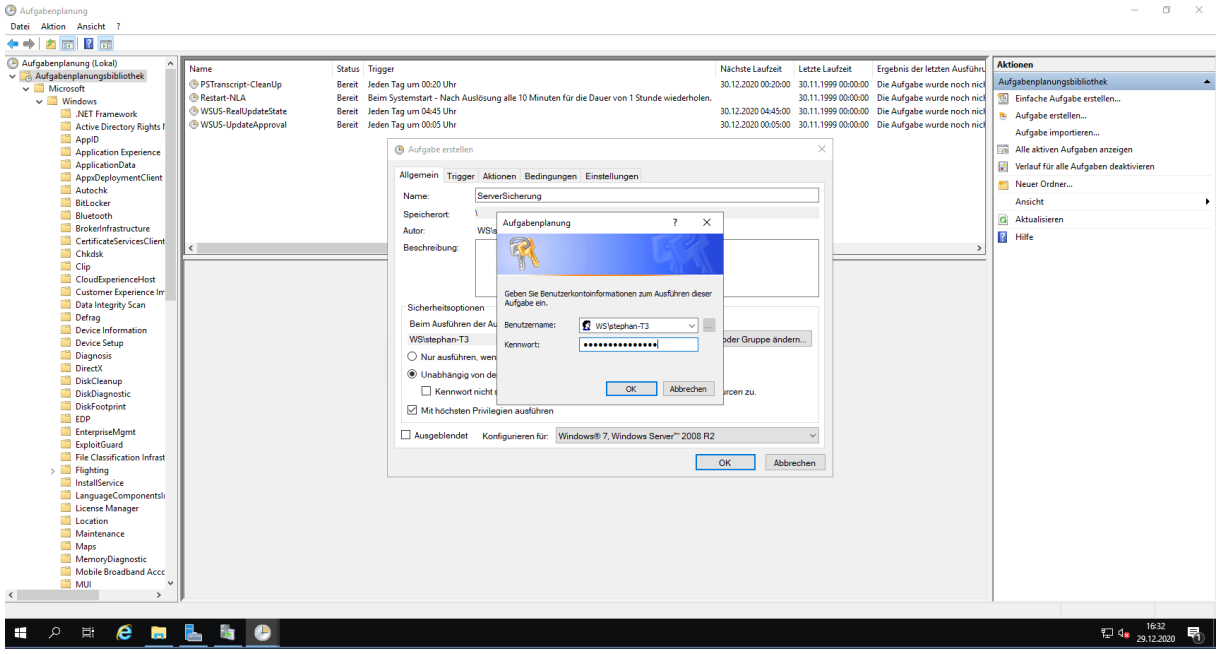
Auf die gleiche Weise hole ich das Script „WSUS-RealUpdateState.ps1“ als Aufgabe dazu:



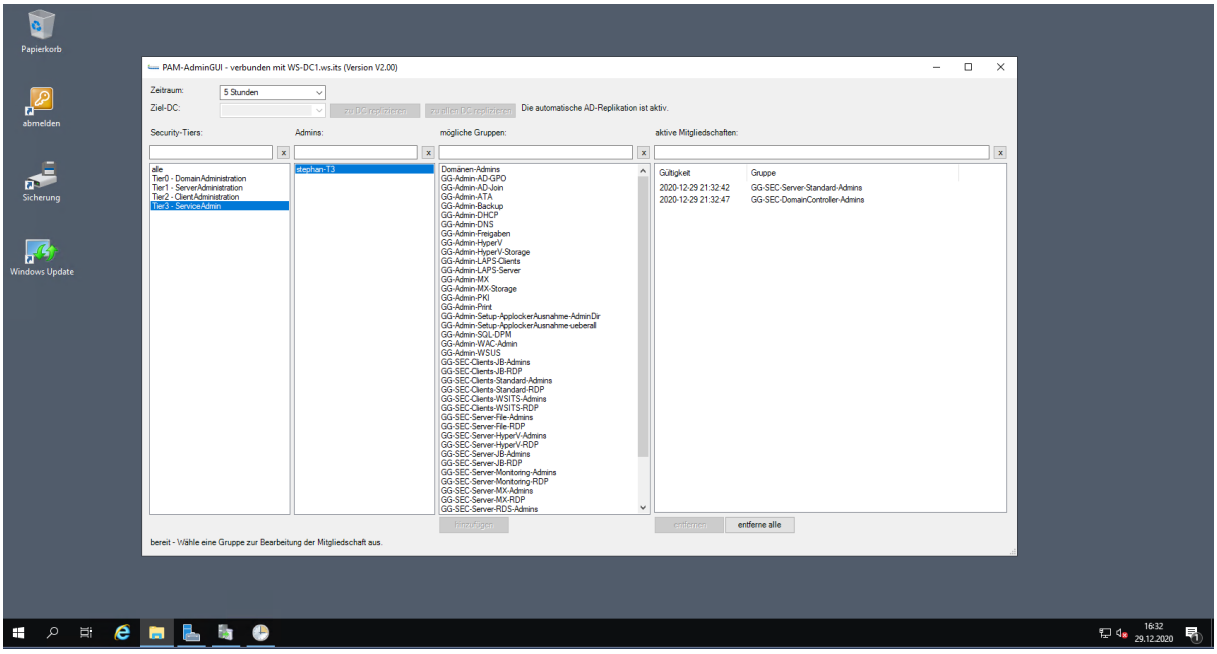
Das Feintuning nehme ich später vor.

Datensicherung

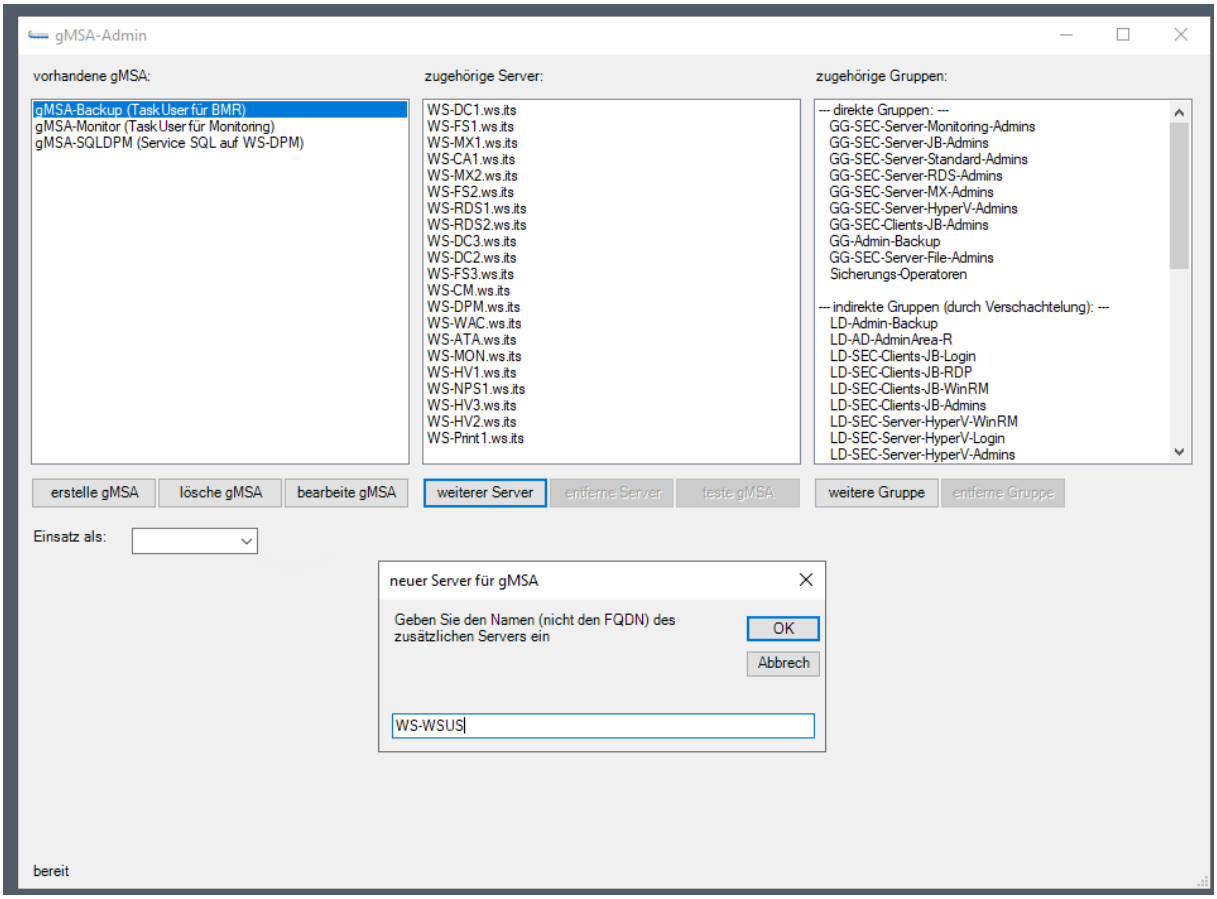
Denn eine Datensicherung ist bei den geplanten Aufgaben auch mit dabei. Auch hier importiere ich eine XML-Datei. Der Task soll über einen Group Managed Service Account laufen. Diesen kann ich aber nicht direkt eintragen. Also hinterlege ich temporär meine T3-Anmeldeinformationen:



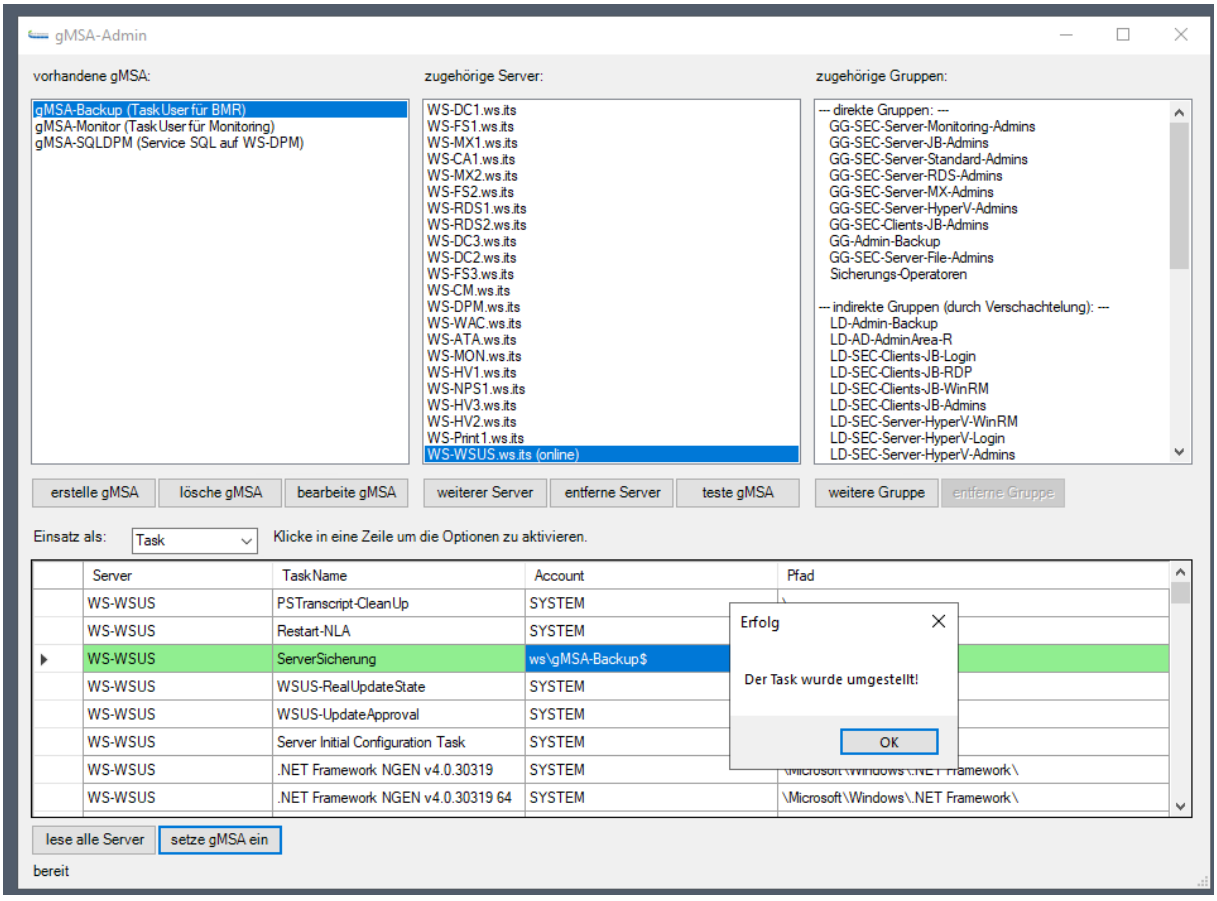
Für den gMSA-Delegierungsvorgang muss ich auf meinen Domain Controller wechseln. Dort benötigt meine T3-Kennung aber noch die administrativen Rechte auf Zeit delegiert:



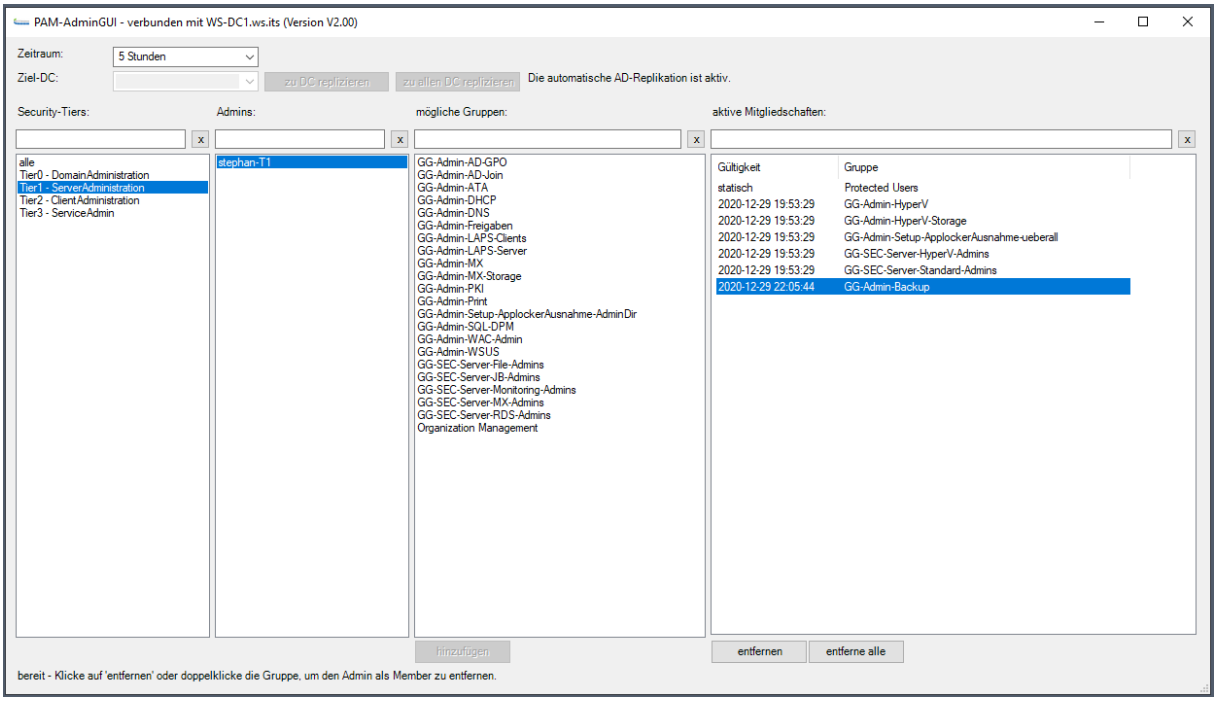
Danach ist die Anmeldung am Domain Controller als Stephan-T3 kein Problem. Hier starte ich mein PowerShell-Tool „gMSA-Admin“ und privilegiere den neuen WS-WSUS für den Abruf der aktuellen Anmeldeinformationen vom Backup-gMSA:



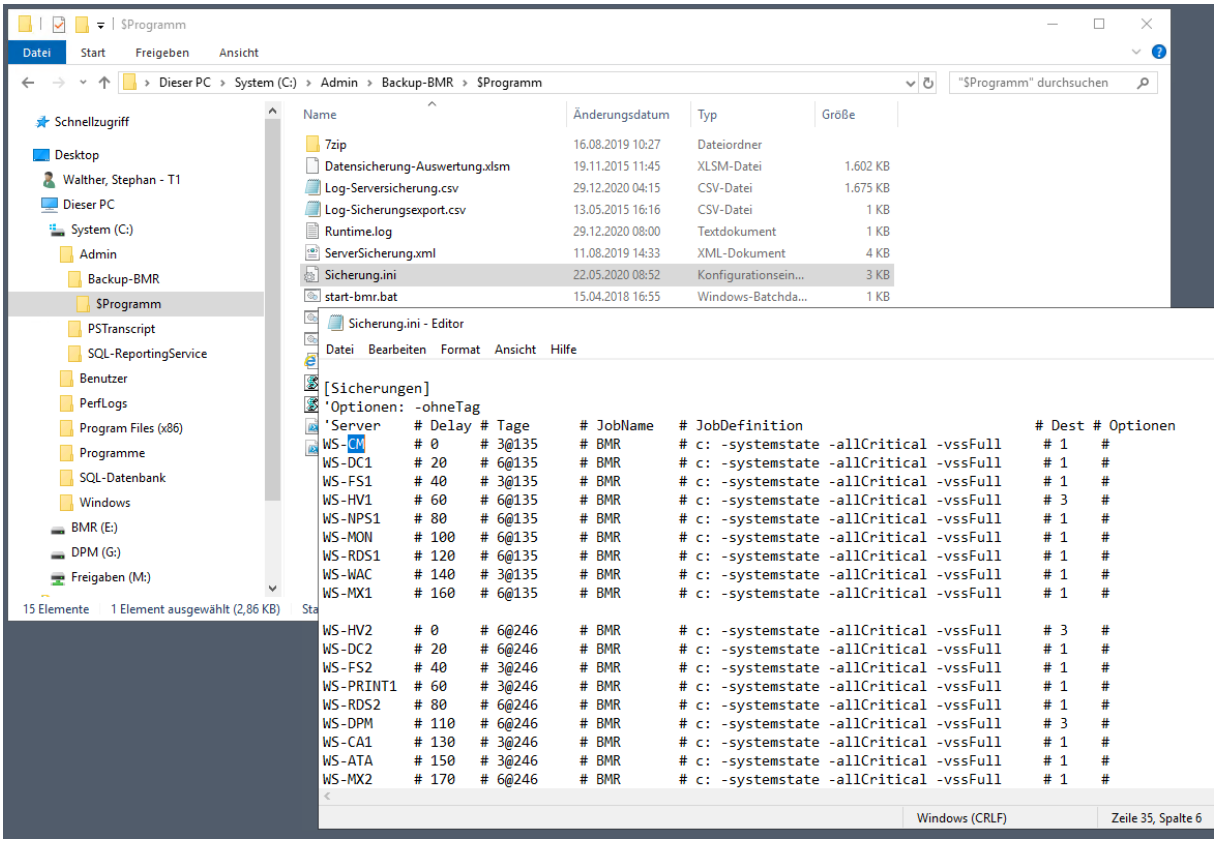
Direkt im Anschluss kann ich über mein Script den Task-Account austauschen:



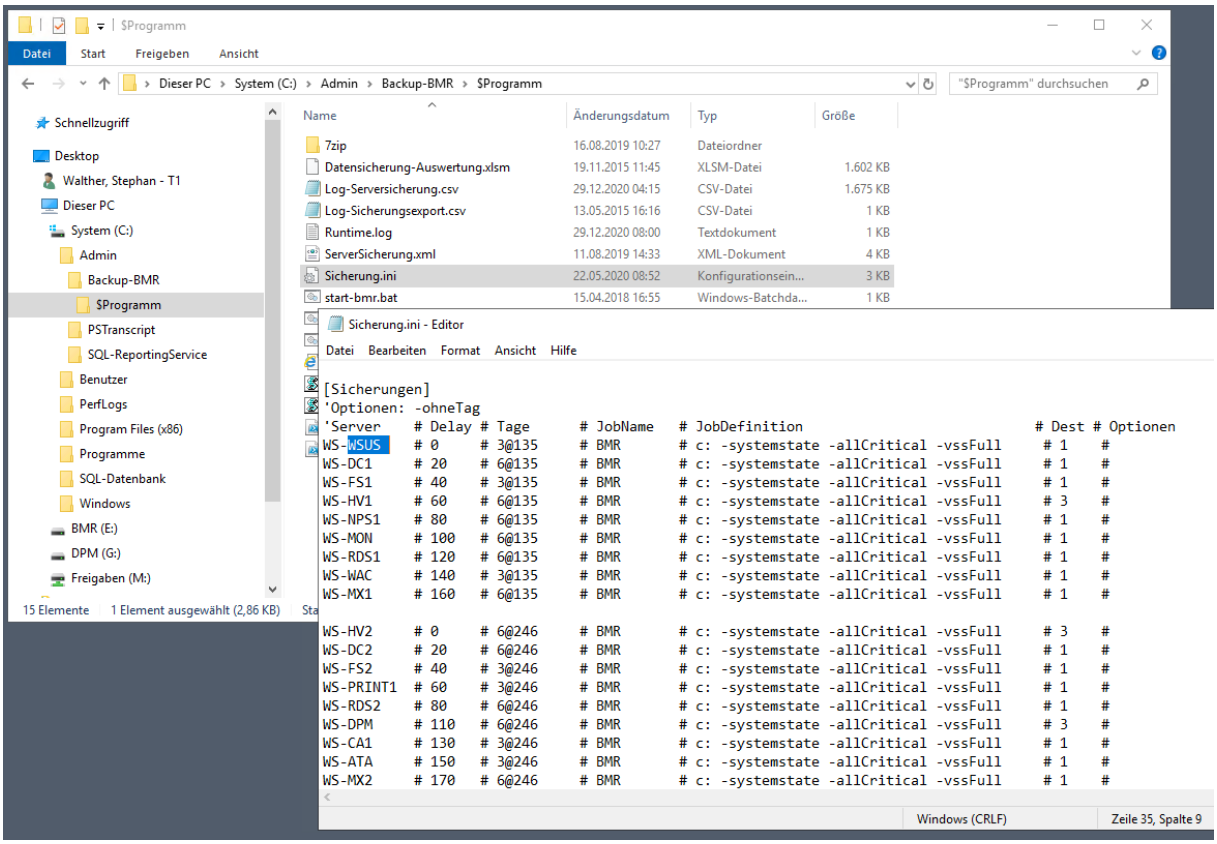
Der Server ist neu. Daher muss ich für den Sicherungsjob noch einen Auftrag auf meinem Backup-Server konfigurieren. Dafür nutze ich meine T1-Kennung und privilegiere sie für den Zugriff auf meinem Backup-Server:



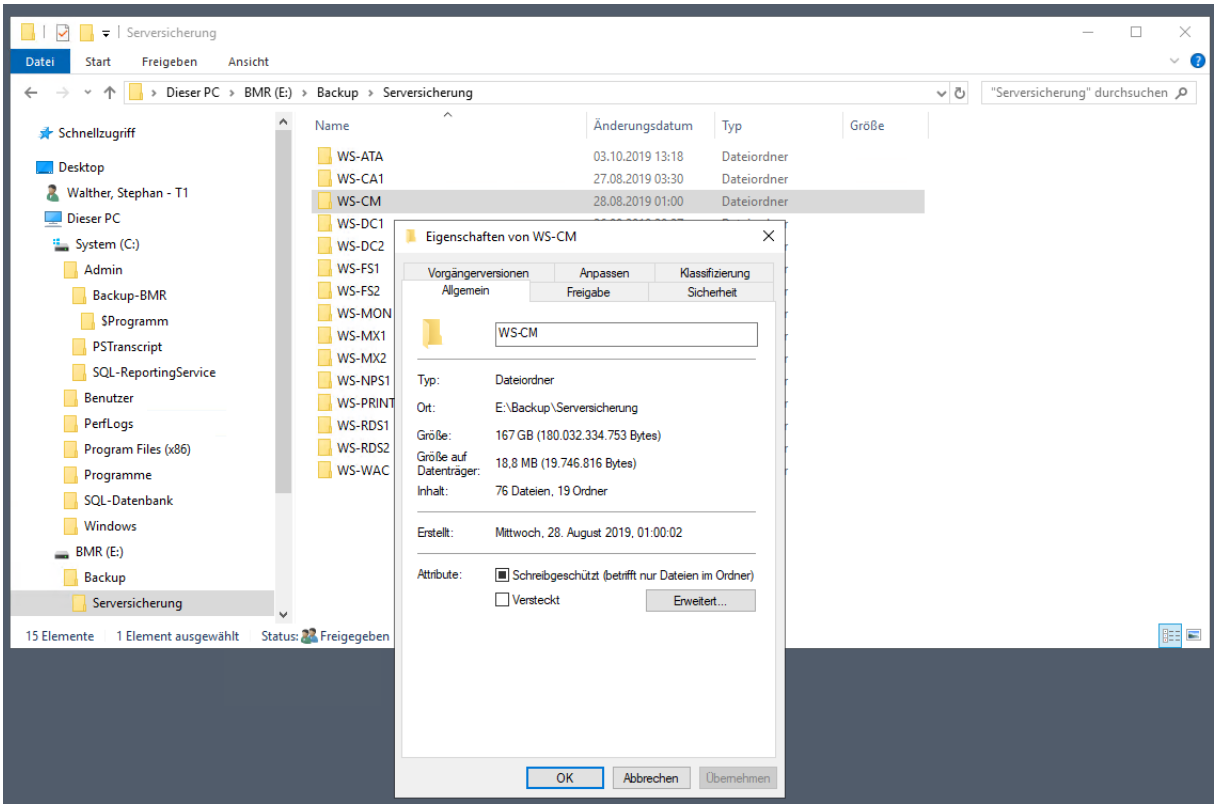
Meine ServerImage-Backup-Lösung basiert auf dem Windows Server Backup Feature, das über ein VB-Script zeitgesteuert ausgeführt wird. Die dazugehörige Konfiguration liegt zentral auf meinem Backup-Server und ist eigentlich auch nur eine ini-Datei. Hier steht noch der alte WS-CM drin:

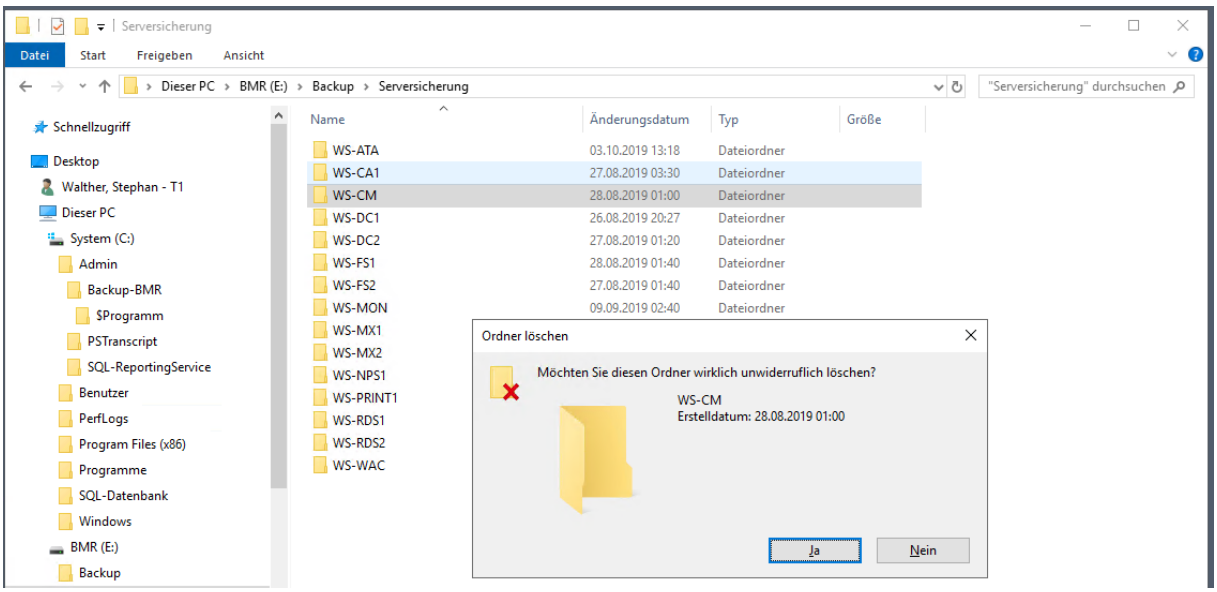


Den alten Servernamen passe ich einfach an:



Danach lösche ich noch die Sicherungen des alten Servers von der Backup-Festplatte:

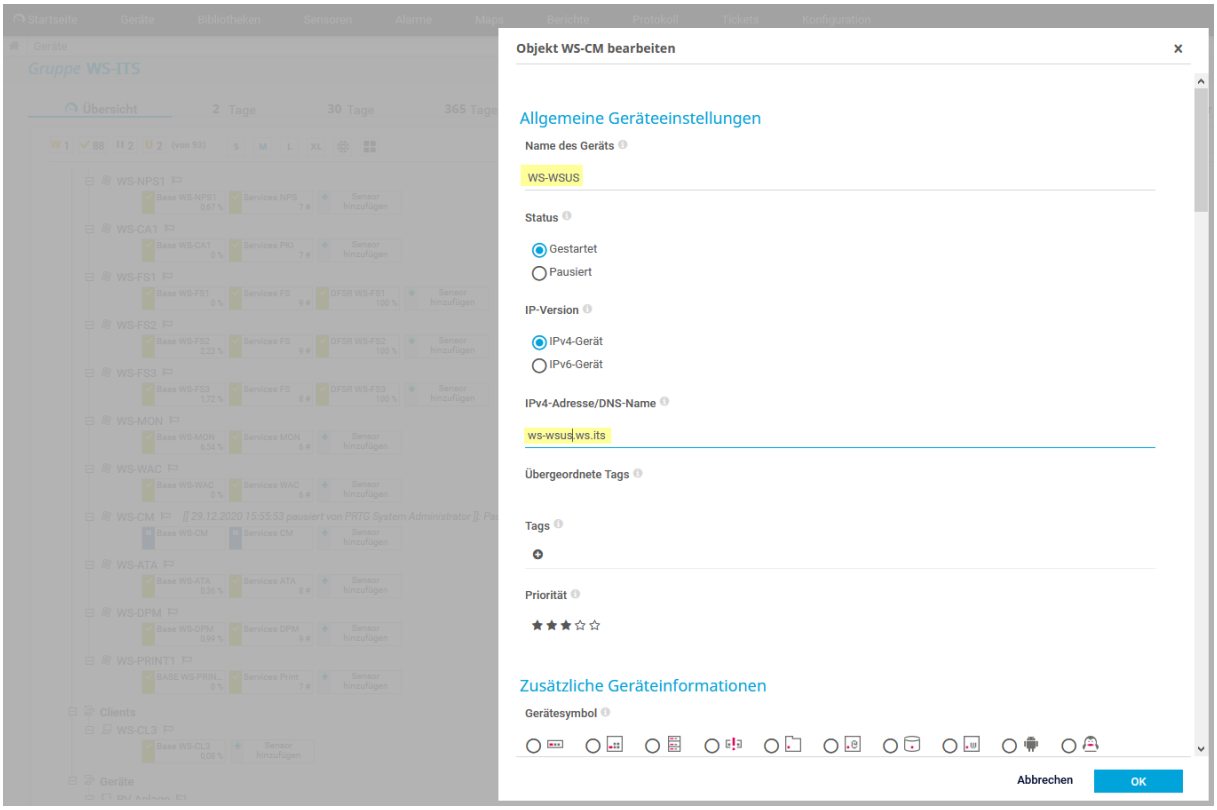




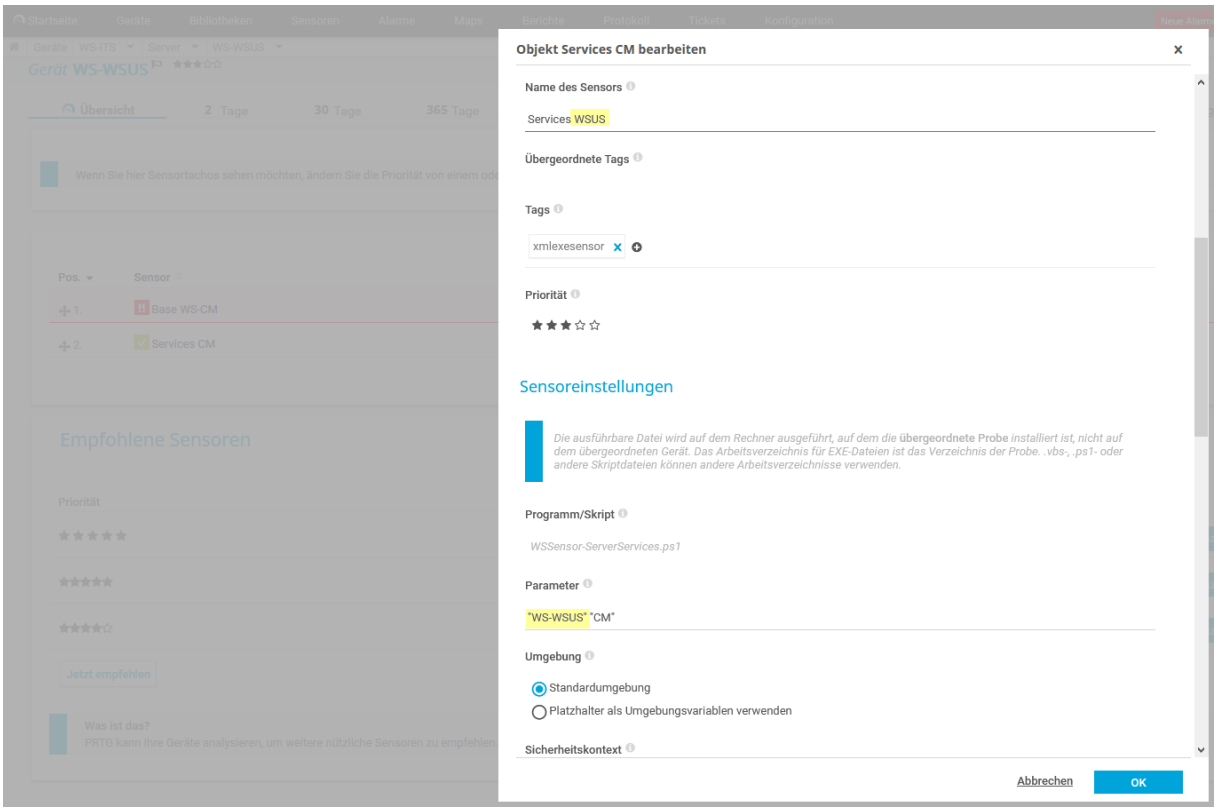
Damit sollte die nächste Sicherung fein durchlaufen.

Monitoring

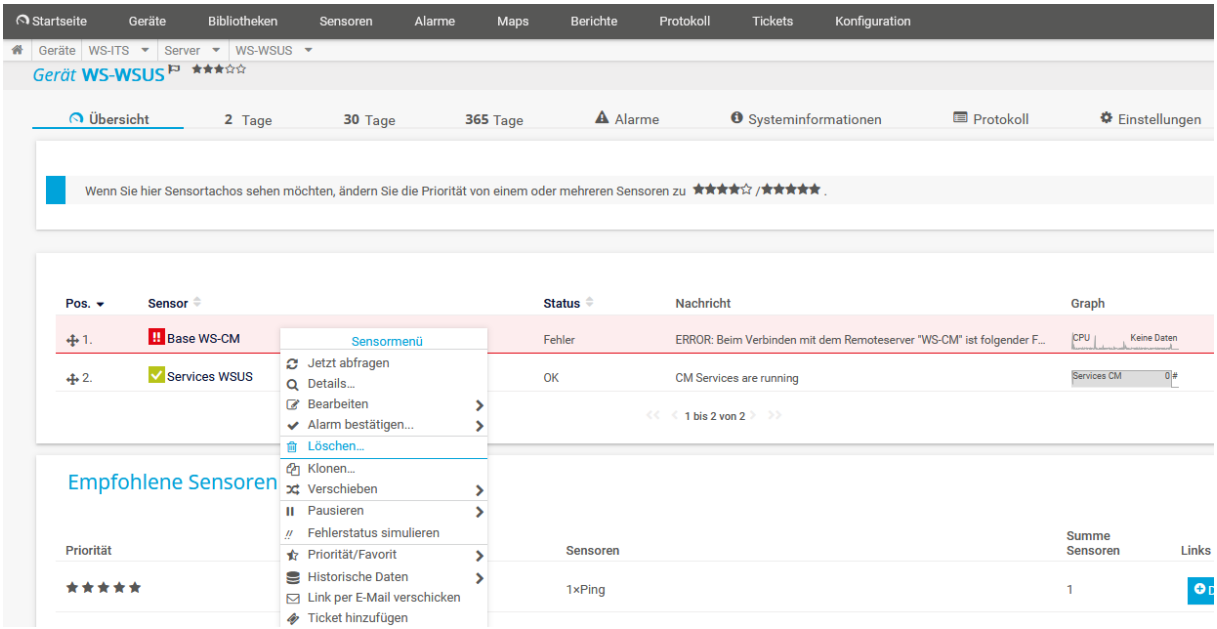
Eine Kleinigkeit für das Daily Business fehlt noch: Die Integration ins Monitoring. Bei mir werkelt dafür ein PRTG-Server, dem ich ein paar zusätzliche PowerShell-Scripte als Custom-Sensors programmiert habe. Einer davon erfasst die Basisdaten für meine Windows Server. Dafür modifiziere ich den alten Eintrag WS-CM:



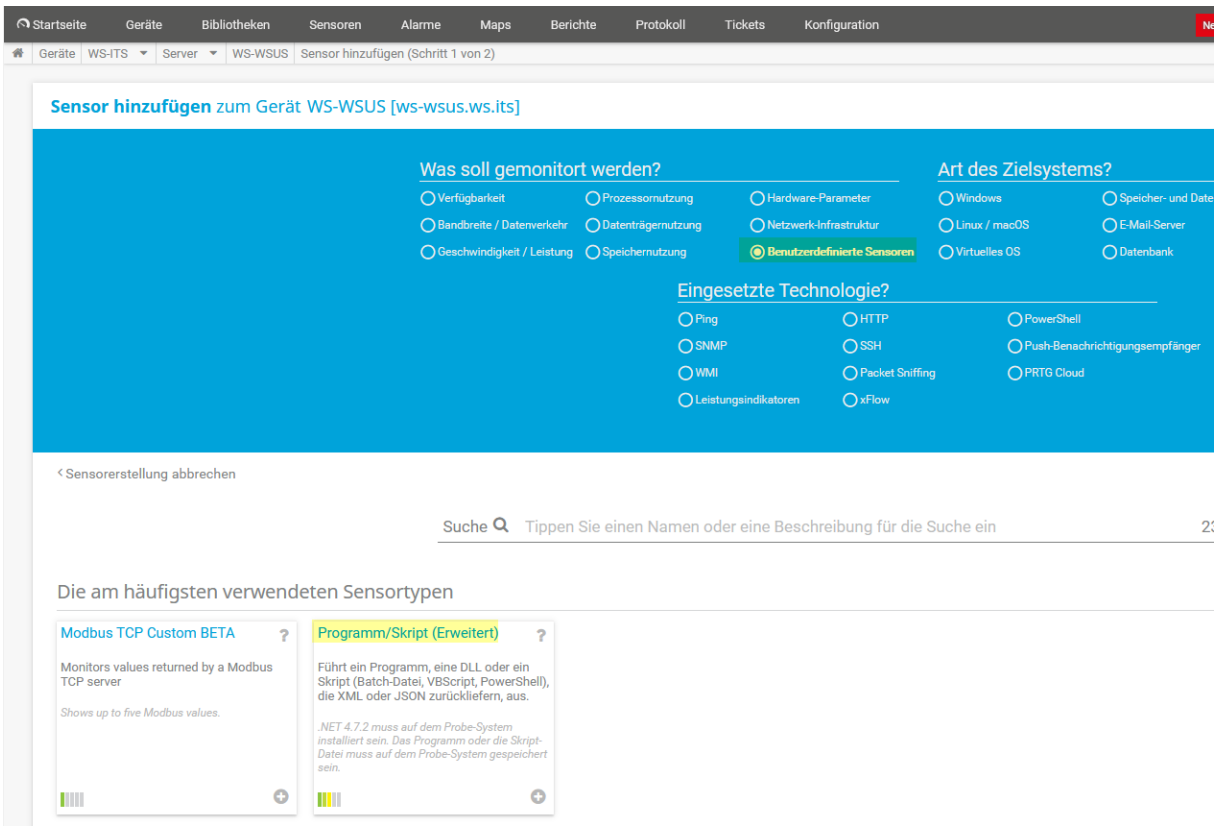
Den zweiten Sensor kann ich einfach durch eine Namensanpassung modifizieren:



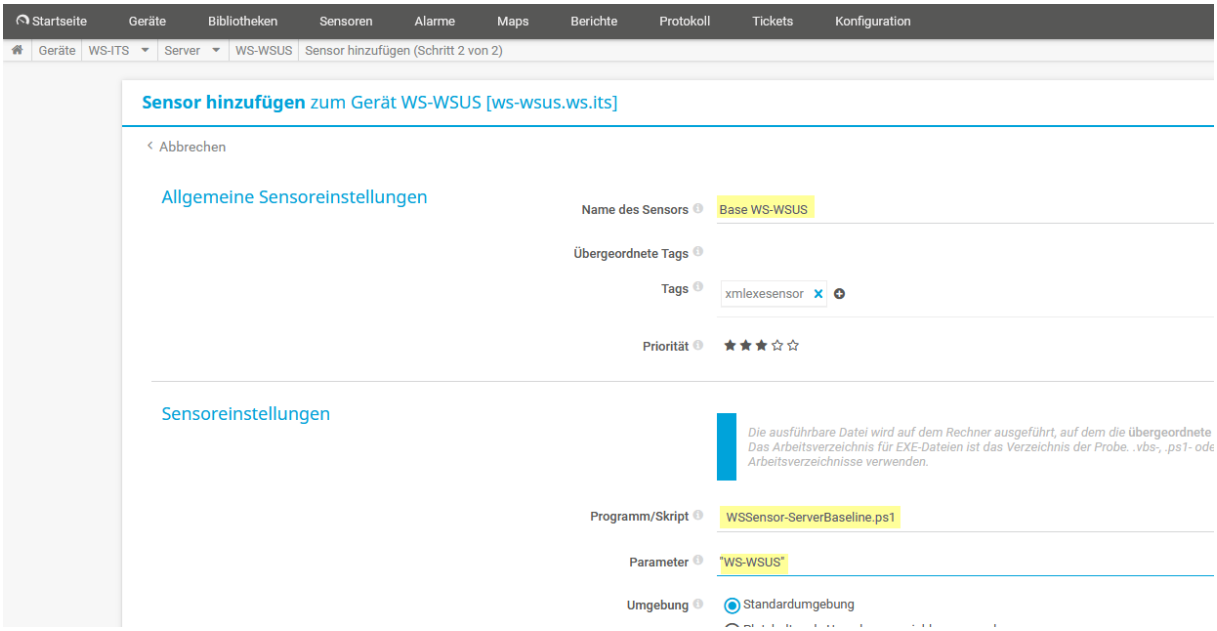
Aber der erste Sensor wird besser gelöscht und neu erstellt:



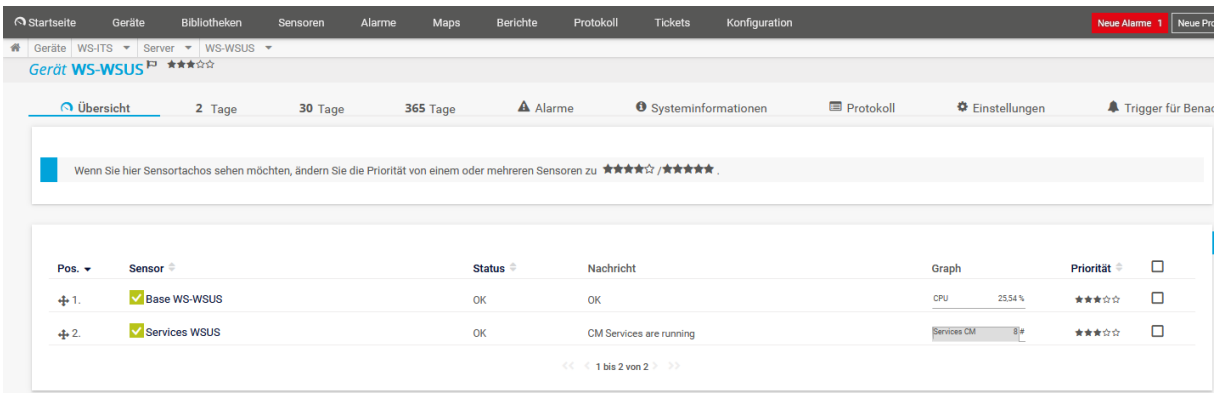
Für den neuen Sensor kann ich bequem den Dialog im Webportal vom PRTG verwenden:



Einige Eingaben später ist der Sensor eingerichtet:



Und einen weiteren Moment später ist der Sensor aktiv:

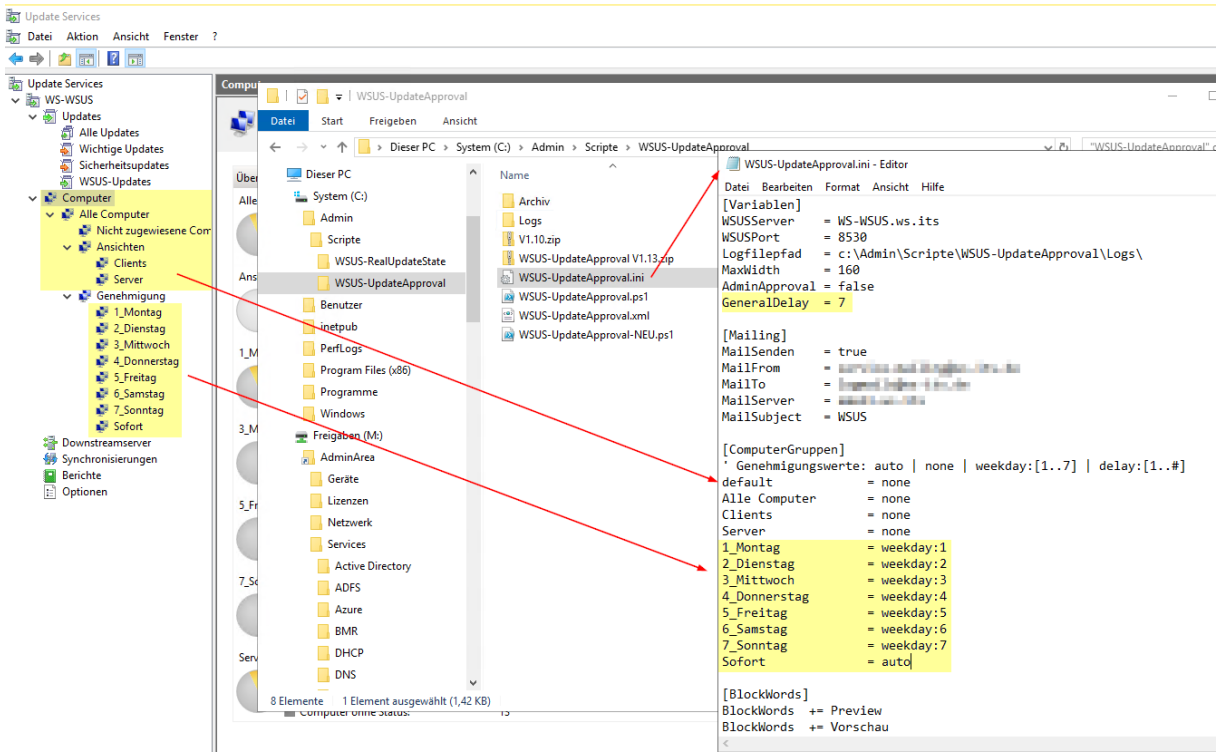


WSUS-UpdateApproval

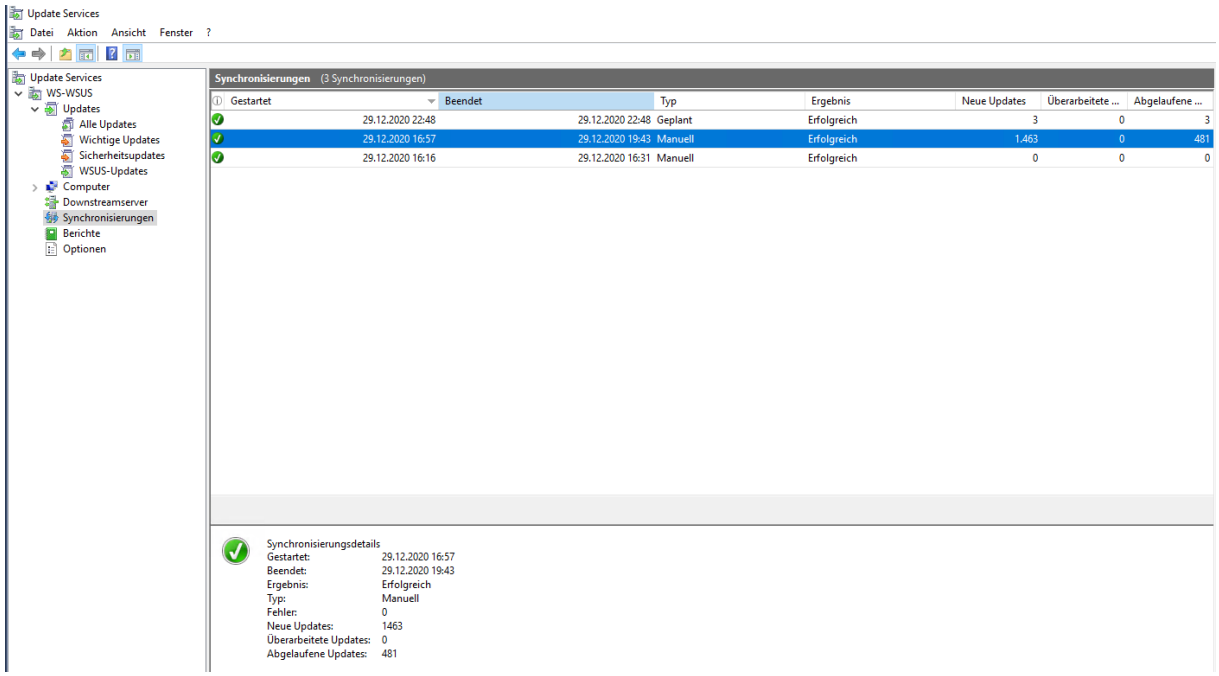
So. Nachdem die Basics erledigt sind, kann ich nun wieder an meine Automations-Scripte für den WSUS ran. Wie schon erwähnt, soll mein Script „WSUS-UpdateApproval“ einmal am Tag Updates auf vordefinierten WSUS-Containern genehmigen. Zusätzlich soll es nicht erwünschte Update ablehnen. Die Konfiguration basiert ebenfalls auf einer ini-Datei. Diese muss ich an die neue Struktur im WSUS anpassen. Wichtig ist dabei, dass es für jeden WSUS-Container einen passenden Eintrag für den Genehmigungsprozess gibt:

- Genehmigt werden Updates nur auf den Containern im Hauptordner „Genehmigung“. Die anderen Container unter „Ansichten“ erhalten keine Updates.
- Das GeneralDelay kennzeichnet die „Liegezeit“ von neu synchronisierten Updates: Wenn mein WSUS heute ein neues Update bei Microsoft erkennt, dann wird mein Script dieses Update beim nächsten Lauf erkennen und mir per Mail eine Info zukommen lassen. Dann wird das Update die nächsten 6 Tage ignoriert. Erst nach 7 Tagen wird das Update auf den an diesem Tag aktiven Containern genehmigt.

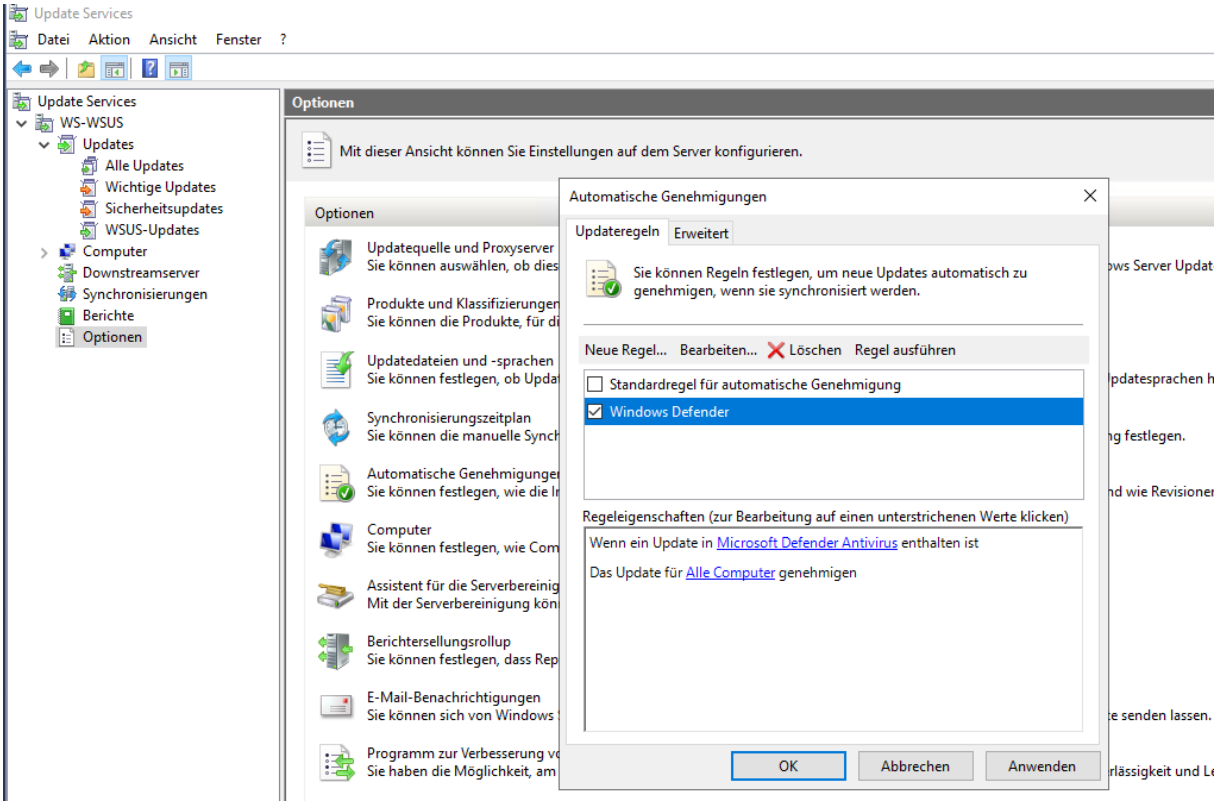
Aus der Grafik kann man die Zusammenhänge ableiten:



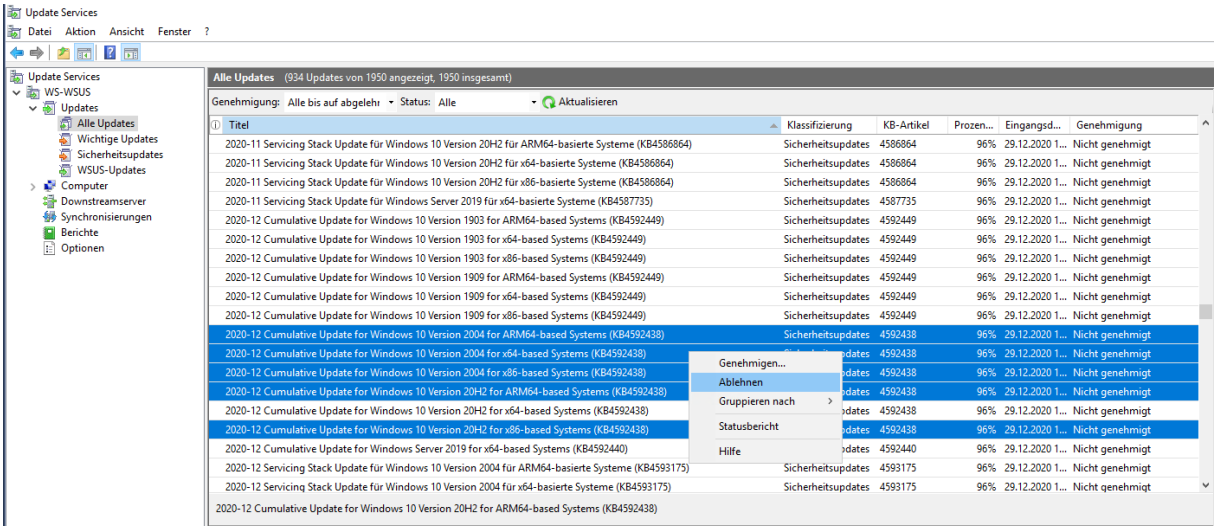
Der Server hat zwischenzeitlich die Synchronisierung neuer Updates vom Microsoft Update Server abgeschlossen. Bisher sind keine Updates genehmigt worden:



Denn ich habe die Standard-Genehmigungsregel NICHT aktiviert:



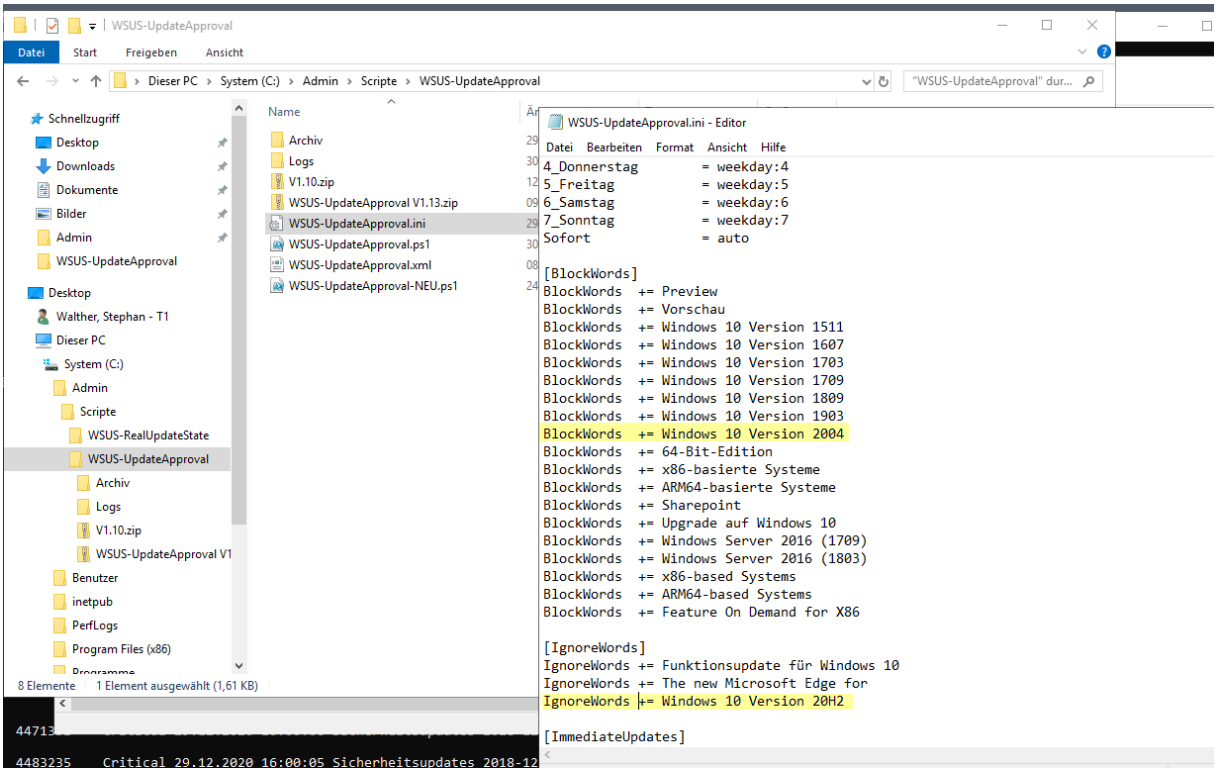
Jetzt müsste ich die Updates ablehnen, die synchronisiert wurden aber nicht gebraucht werden. Bei der Menge an Updates ist das extrem zeitraubend:



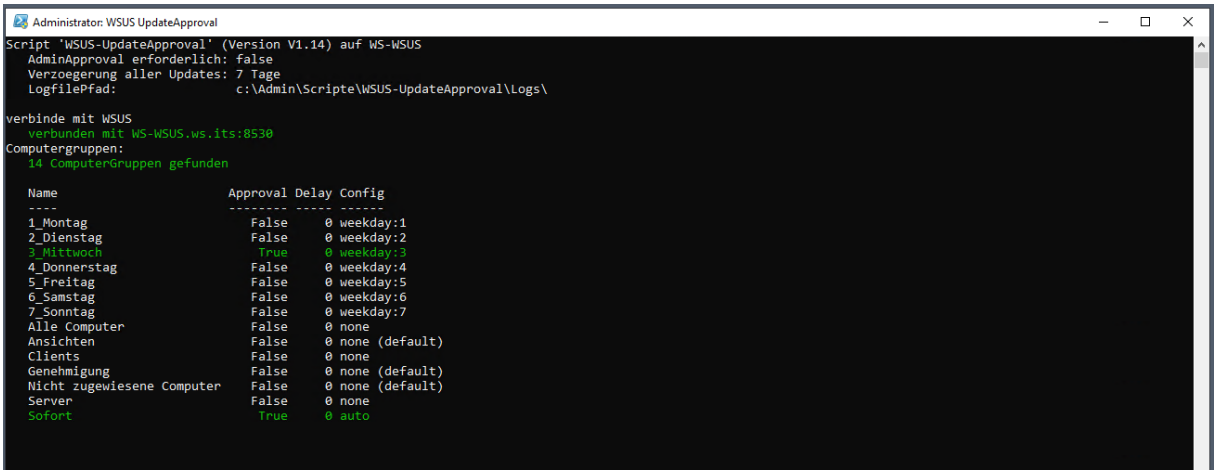
Aber auch das kann mein Script für mich automatisieren. Dafür habe ich die Sektion „BlockWords“ in der Konfiguration eingebaut. Hier kann ich die Textbausteine angeben, die ich in den Updates nicht haben möchte. Beim nächsten Lauf werden passende Update dann automatisch abgelehnt.

Das Muster dabei lässt sich gut in der Konfiguration erkennen. Ich benötige z.B. verschiedene Windows 10 Versionen nicht mehr. Warum soll ich die also pflegen, genehmigen und herunterladen? Gleiches gilt für x86-basierte Systeme oder ARM-Plattformen. Die verwende ich nicht. Also: raus damit.

Mit der Sektion „IgnoreWords“ kann ich mit den Texten übereinstimmende Updates ignorieren, statt sie abzulehnen oder zu genehmigen:



Es wird Zeit für einen Scriptlauf. Dann kann man die Logik in Aktion sehen. Das Script baut eine Verbindung zum WSUS auf, liest die Konfiguration ein und bestimmt, welcher WSUS-Container heute passende Updates genehmigt bekommt:



Dann werden die Updates im Datenbestand geladen. Aus der Gesamtmenge werden die bereits abgelehnten Updates ausgefiltert. Dann greifen meine Textfilter. Alle Updates mit einer Übereinstimmung in den Blockwords werden für die Ablehnung vorgemerkt:

```
lade Updateinformationen...
Updates im WSUS:

   Updates im Bestand:          1950
   ------------------------------------------------------------------------
   davon mit Status=expired:     484
   davon mit Status=declined:    532
   davon mit Blockword:            1 ('Preview')
   davon mit Blockword:            0 ('Vorschau')
   davon mit Blockword:            0 ('Windows 10 Version 1511')
   davon mit Blockword:            0 ('Windows 10 Version 1607')
   davon mit Blockword:            0 ('Windows 10 Version 1703')
   davon mit Blockword:            0 ('Windows 10 Version 1709')
   davon mit Blockword:            2 ('Windows 10 Version 1809')
   davon mit Blockword:          221 ('Windows 10 Version 1903')
   davon mit Blockword:            0 ('64-Bit-Edition')
   davon mit Blockword:           39 ('x86-basierte Systeme')
   davon mit Blockword:           40 ('ARM64-basierte Systeme')
   davon mit Blockword:            0 ('Sharepoint')
   davon mit Blockword:            0 ('Upgrade auf Windows 10')
   davon mit Blockword:            0 ('Windows Server 2016 (1709)')
   davon mit Blockword:            0 ('Windows Server 2016 (1803)')
   davon mit Blockword:           18 ('x86-based Systems')
   davon mit Blockword:           17 ('ARM64-based Systems')
   davon mit Blockword:            0 ('Feature On Demand for X86')
   davon mit Ignoreword:          45 ('Funktionsupdate für Windows 10')
   davon mit Ignoreword:           3 ('The new Microsoft Edge for')
   davon mit ImmediateWords:      13 ('Windows Defender')
   ------------------------------------------------------------------------
   aktuelle Updates:            548
   ------------------------------------------------------------------------
   sofort genehmigen:            13
   noch verzoegert:             535
   ohne Genehmigung:              0
   teilweise ohne Genehmigung:    0
   ohne Ablehnung:              338
```

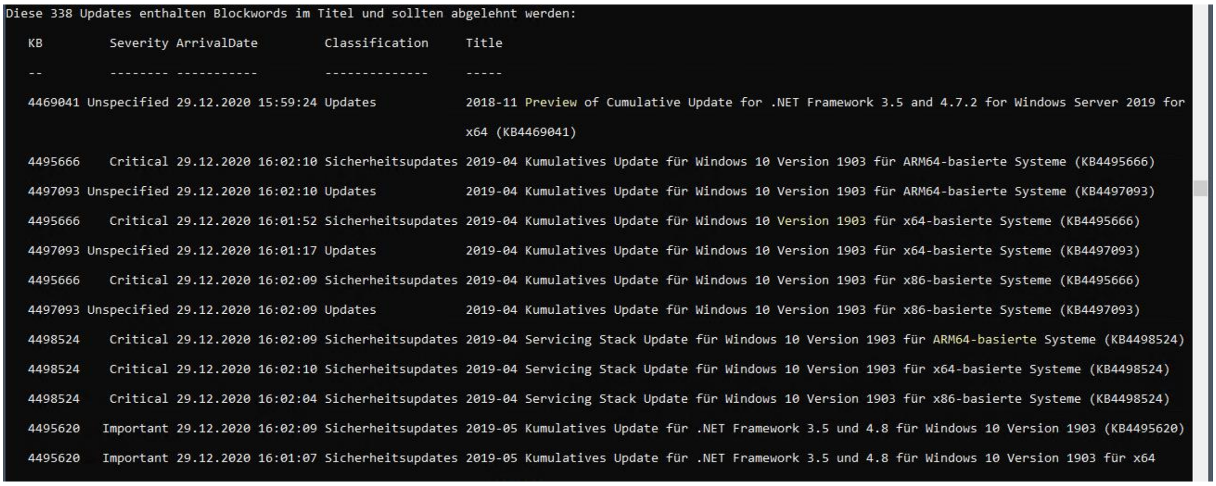
Das Script erkennt bei jedem Update den Tag der Synchronisierung. Dieses Datum wird für die Berechnung der Verzögerungsdauer verwendet:

```
Diese 535 Updates wurden neu geladen. Sie werden in 7 Tagen automatisch aktiviert:

   KB         Severity ArrivalDate         Classification     Title

   --         -------- -----------         --------------     -----

   4464330    Critical 29.12.2020 15:59:56 Sicherheitsupdates 2018-10 Kumulatives Update für Windows Server 2019 (1809) für x64-basierte Systeme (KB4464330)

   4465477    Critical 29.12.2020 16:00:04 Sicherheitsupdates 2018-10 Update für Windows Server 2019 (1809) für x64-basierte Systeme (KB4465477)

   4467708    Critical 29.12.2020 15:59:24 Sicherheitsupdates 2018-11 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4467708)

   4469342 Unspecified 29.12.2020 16:00:04 Updates            2018-11 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4469342)

   4465664    Critical 29.12.2020 15:59:51 Sicherheitsupdates 2018-11 Update für Windows Server 2019 für x64-basierte Systeme (KB4465664)

   4470788    Critical 29.12.2020 16:00:04 Sicherheitsupdates 2018-11 Update für Windows Server 2019 für x64-basierte Systeme (KB4470788)

   4470502   Important 29.12.2020 16:00:42 Sicherheitsupdates 2018-12 Kumulatives Update für .NET Framework 3.5 und 4.7.2 für Windows Server 2019 für x64
                                                              (KB4470502)

   4471332    Critical 29.12.2020 16:00:06 Sicherheitsupdates 2018-12 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4471332)

   4483235    Critical 29.12.2020 16:00:05 Sicherheitsupdates 2018-12 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4483235)

   4480056   Important 29.12.2020 16:00:51 Sicherheitsupdates 2019-01 Kumulatives Update für .NET Framework 3.5 und 4.7.2 für Windows Server 2019 für x64
                                                              (KB4480056)

   4481031 Unspecified 29.12.2020 16:00:05 Updates            2019-01 Kumulatives Update für .NET Framework 3.5 und 4.7.2 für Windows Server 2019 für x64
```

Eine Ausnahme kann aber auch definiert sein. Bei Signatur-Updates wäre eine Wartezeit von 7 Tagen eher fatal:

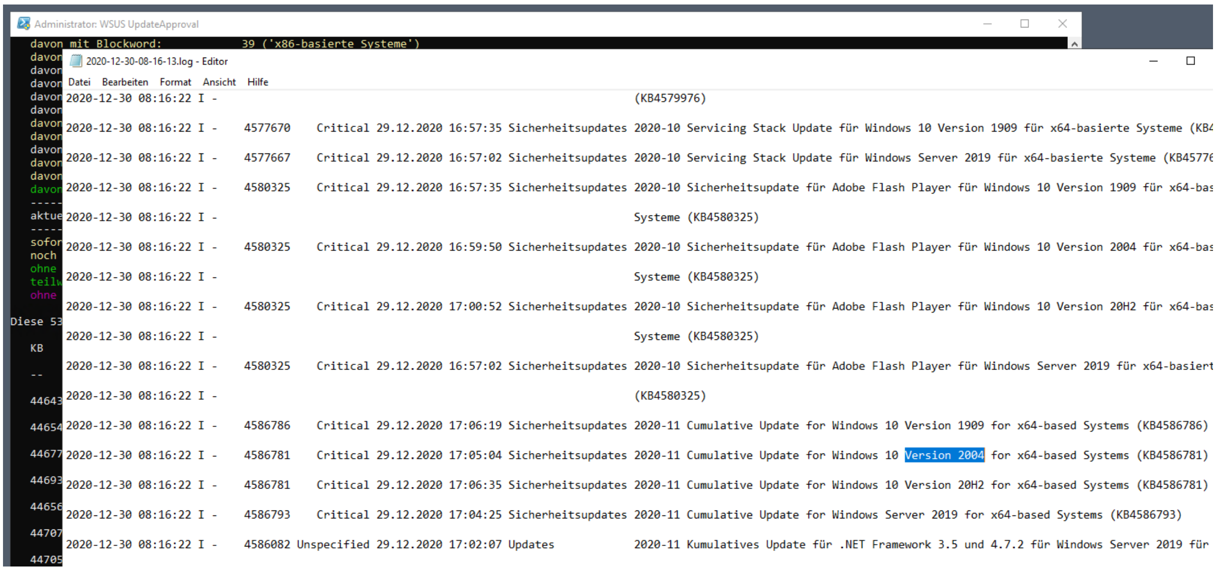
```
Diese 13 Updates benötigen eine sofortige Genehmigung:

   KB         Severity ArrivalDate         Classification     Title

   --         -------- -----------         --------------     -----

   915597  Unspecified 29.12.2020 18:38:13 Definitionsupdates Security Intelligence-Update für Windows Defender Antivirus - KB915597 (Version 1.329.1086.0)

   915597  Unspecified 29.12.2020 18:38:04 Definitionsupdates Security Intelligence-Update für Windows Defender Antivirus - KB915597 (Version 1.329.1274.0)

   915597  Unspecified 29.12.2020 18:38:06 Definitionsupdates Security Intelligence-Update für Windows Defender Antivirus - KB915597 (Version 1.329.477.0)

   915597  Unspecified 29.12.2020 18:38:07 Definitionsupdates Security Intelligence-Update für Windows Defender Antivirus - KB915597 (Version 1.329.510.0)

   915597  Unspecified 29.12.2020 18:38:09 Definitionsupdates Security Intelligence-Update für Windows Defender Antivirus - KB915597 (Version 1.329.689.0)

   915597  Unspecified 29.12.2020 18:38:11 Definitionsupdates Security Intelligence-Update für Windows Defender Antivirus - KB915597 (Version 1.329.885.0)

   4052623 Unspecified 29.12.2020 16:27:28 Updates            Update für Windows Defender Antivirus-Antischadsoftwareplattform – KB4052623 (Version 4.18.2001.10
)
   4052623 Unspecified 29.12.2020 16:28:04 Updates            Update für Windows Defender Antivirus-Antischadsoftwareplattform – KB4052623 (Version 4.18.2001.10
)
```

Alle für die Ablehnung vorgemerkten Updates können noch einmal kontrolliert werden. Die Blockwords sind im Text mal teilweise farbig dargestellt:



```
Diese 338 Updates enthalten Blockwords im Titel und sollten abgelehnt werden:

  KB        Severity ArrivalDate         Classification     Title
  --        -------- -----------         --------------     -----
  4469041 Unspecified 29.12.2020 15:59:24 Updates           2018-11 Preview of Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows Server 2019 for
                                                            x64 (KB4469041)
  4495666    Critical 29.12.2020 16:02:10 Sicherheitsupdates 2019-04 Kumulatives Update für Windows 10 Version 1903 für ARM64-basierte Systeme (KB4495666)
  4497093 Unspecified 29.12.2020 16:02:10 Updates           2019-04 Kumulatives Update für Windows 10 Version 1903 für ARM64-basierte Systeme (KB4497093)
  4495666    Critical 29.12.2020 16:01:52 Sicherheitsupdates 2019-04 Kumulatives Update für Windows 10 Version 1903 für x64-basierte Systeme (KB4495666)
  4497093 Unspecified 29.12.2020 16:01:17 Updates           2019-04 Kumulatives Update für Windows 10 Version 1903 für x64-basierte Systeme (KB4497093)
  4495666    Critical 29.12.2020 16:02:09 Sicherheitsupdates 2019-04 Kumulatives Update für Windows 10 Version 1903 für x86-basierte Systeme (KB4495666)
  4497093 Unspecified 29.12.2020 16:02:09 Updates           2019-04 Kumulatives Update für Windows 10 Version 1903 für x86-basierte Systeme (KB4497093)
  4498524    Critical 29.12.2020 16:02:09 Sicherheitsupdates 2019-04 Servicing Stack Update für Windows 10 Version 1903 für ARM64-basierte Systeme (KB4498524)
  4498524    Critical 29.12.2020 16:02:10 Sicherheitsupdates 2019-04 Servicing Stack Update für Windows 10 Version 1903 für x64-basierte Systeme (KB4498524)
  4498524    Critical 29.12.2020 16:02:04 Sicherheitsupdates 2019-04 Servicing Stack Update für Windows 10 Version 1903 für x86-basierte Systeme (KB4498524)
  4495620   Important 29.12.2020 16:02:09 Sicherheitsupdates 2019-05 Kumulatives Update für .NET Framework 3.5 und 4.8 für Windows 10 Version 1903 (KB4495620)
  4495620   Important 29.12.2020 16:01:07 Sicherheitsupdates 2019-05 Kumulatives Update für .NET Framework 3.5 und 4.8 für Windows 10 Version 1903 für x64
```

Das Script kennt einen Admin- und einen Task-Modus. Im Admin-Modus muss die Genehmigung und die Ablehnung manuell bestätigt werden. Im Task-Modus wird automatisch gearbeitet. Im Admin-Modus kann ich also die vielen abzulehnenden Updates noch einmal validieren. Ich will ja nicht zu viel löschen. Jeder Scriptlauf erstellt eine Logdatei. Diese nutze ich nun für eine Anpassung der Konfiguration. Hier finde ich z.B. Updates für Windows 10 v2004:



```
Administrator: WSUS UpdateApproval
davon mit Blockword:            39 ('x86-basierte Systeme')
2020-12-30-08-16-13.log - Editor
Datei  Bearbeiten  Format  Ansicht  Hilfe
2020-12-30 08:16:22 I -                                                            (KB4579976)
2020-12-30 08:16:22 I -    4577670    Critical 29.12.2020 16:57:35 Sicherheitsupdates 2020-10 Servicing Stack Update für Windows 10 Version 1909 für x64-basierte Systeme (KB4
2020-12-30 08:16:22 I -    4577667    Critical 29.12.2020 16:57:02 Sicherheitsupdates 2020-10 Servicing Stack Update für Windows Server 2019 für x64-basierte Systeme (KB4577
2020-12-30 08:16:22 I -    4580325    Critical 29.12.2020 16:57:35 Sicherheitsupdates 2020-10 Sicherheitsupdate für Adobe Flash Player für Windows 10 Version 1909 für x64-bas
2020-12-30 08:16:22 I -                                                            Systeme (KB4580325)
2020-12-30 08:16:22 I -    4580325    Critical 29.12.2020 16:59:50 Sicherheitsupdates 2020-10 Sicherheitsupdate für Adobe Flash Player für Windows 10 Version 2004 für x64-bas
2020-12-30 08:16:22 I -                                                            Systeme (KB4580325)
2020-12-30 08:16:22 I -    4580325    Critical 29.12.2020 17:00:52 Sicherheitsupdates 2020-10 Sicherheitsupdate für Adobe Flash Player für Windows 10 Version 20H2 für x64-bas
2020-12-30 08:16:22 I -                                                            Systeme (KB4580325)
2020-12-30 08:16:22 I -    4580325    Critical 29.12.2020 16:57:02 Sicherheitsupdates 2020-10 Sicherheitsupdate für Adobe Flash Player für Windows Server 2019 für x64-basiert
2020-12-30 08:16:22 I -                                                            (KB4580325)
2020-12-30 08:16:22 I -    4586786    Critical 29.12.2020 17:06:19 Sicherheitsupdates 2020-11 Cumulative Update for Windows 10 Version 1909 for x64-based Systems (KB4586786)
2020-12-30 08:16:22 I -    4586781    Critical 29.12.2020 17:05:04 Sicherheitsupdates 2020-11 Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB4586781)
2020-12-30 08:16:22 I -    4586781    Critical 29.12.2020 17:06:35 Sicherheitsupdates 2020-11 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB4586781)
2020-12-30 08:16:22 I -    4586793    Critical 29.12.2020 17:04:25 Sicherheitsupdates 2020-11 Cumulative Update for Windows Server 2019 for x64-based Systems (KB4586793)
2020-12-30 08:16:22 I -    4586082 Unspecified 29.12.2020 17:02:07 Updates            2020-11 Kumulatives Update für .NET Framework 3.5 und 4.7.2 für Windows Server 2019 für
```

Diese Betriebssystemversion verwende ich nicht. Daher werde ich sie in die Blockwords aufnehmen. Zusätzlich interessieren mich weitere Patterns nicht. Meine Konfigurationsdatei wird daher erweitert:

WSUS-UpdateApproval.ini - Editor

Datei Bearbeiten Format Ansicht Hilfe

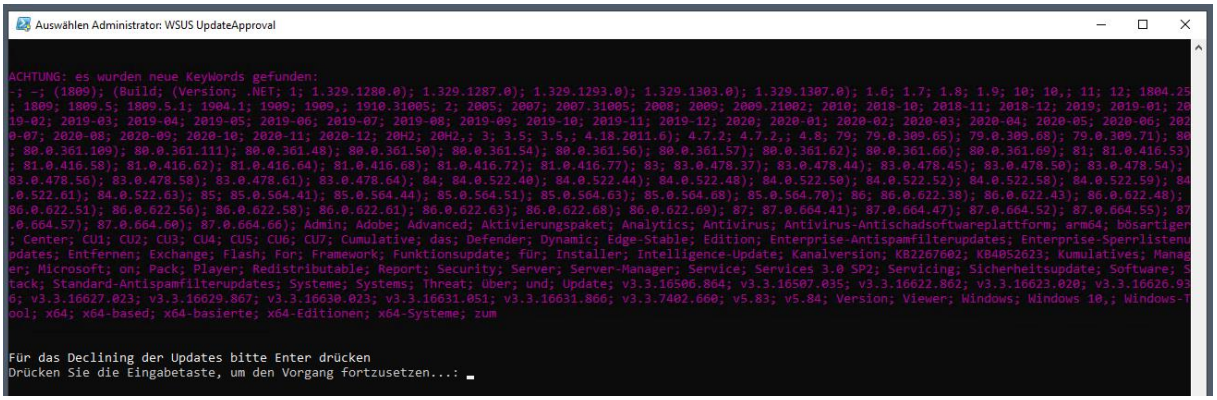
```
Clients             = none
Server              = none
1_Montag            = weekday:1
2_Dienstag          = weekday:2
3_Mittwoch          = weekday:3
4_Donnerstag        = weekday:4
5_Freitag           = weekday:5
6_Samstag           = weekday:6
7_Sonntag           = weekday:7
Sofort              = auto

[BlockWords]
BlockWords  += Preview
BlockWords  += Vorschau
BlockWords  += Windows 10 Version 1511
BlockWords  += Windows 10 Version 1607
BlockWords  += Windows 10 Version 1703
BlockWords  += Windows 10 Version 1709
BlockWords  += Windows 10 Version 1809
BlockWords  += Windows 10 Version 1903
BlockWords  += Windows 10 Version 2004
BlockWords  += 64-Bit-Edition
BlockWords  += x86-basierte Systeme
BlockWords  += ARM64-basierte Systeme
BlockWords  += Sharepoint
BlockWords  += Upgrade auf Windows 10
BlockWords  += Windows Server 2016 (1709)
BlockWords  += Windows Server 2016 (1803)
BlockWords  += x86-based Systems
BlockWords  += ARM64-based Systems
BlockWords  += Feature On Demand for X86
BlockWords  += für ARM64-Editionen
BlockWords  += für x86-Editionen
BlockWords  += Microsoft Edge-Beta
BlockWords  += Microsoft Edge-Dev

[IgnoreWords]
IgnoreWords += Funktionsupdate für Windows 10
IgnoreWords += The new Microsoft Edge for
IgnoreWords += Windows 10 Version 20H2

[ImmediateUpdates]
ImmediateWords += Windows Defender
```

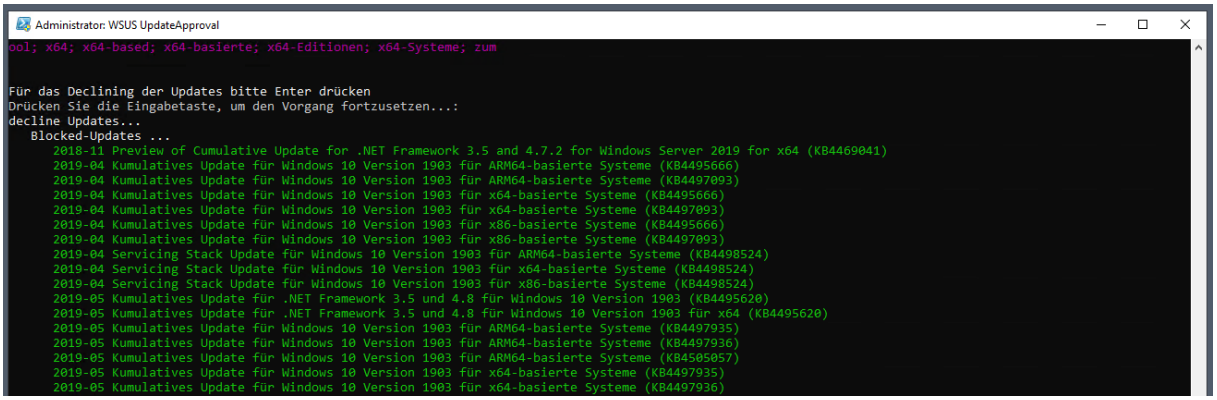
Ich beende das Script ohne eine Genehmigung oder Ablehnung und starte es mit der aktualisierten Konfiguration erneut. Von den 535 Updates sind jetzt nur noch 289 über. Und das nur durch die Ausblendung einer Windows 10 Version und den beiden Architekturen (ARM64 und x86). Nicht schlecht, oder?

Administrator: WSUS UpdateApproval

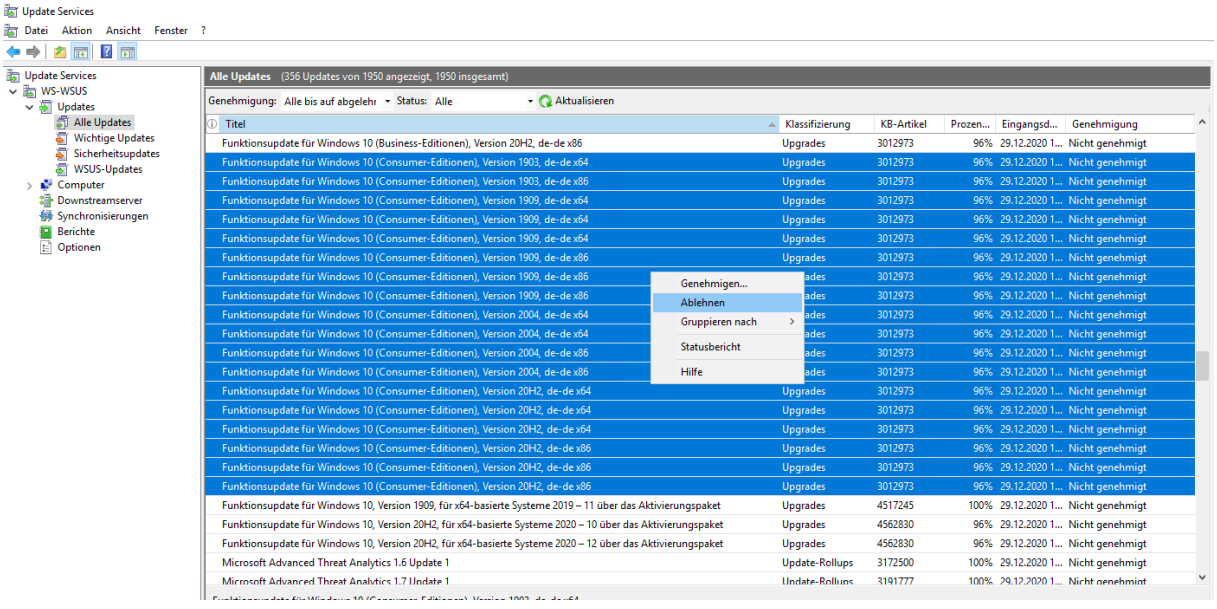
```
lade Updateinformationen...
Updates im WSUS:

   Updates im Bestand:          1950
   ------------------------------------------------------------------------
   davon mit Status=expired:     484
   davon mit Status=declined:    532
   davon mit Blockword:            1 ('Preview')
   davon mit Blockword:            0 ('Vorschau')
   davon mit Blockword:            0 ('Windows 10 Version 1511')
   davon mit Blockword:            0 ('Windows 10 Version 1607')
   davon mit Blockword:            0 ('Windows 10 Version 1703')
   davon mit Blockword:            0 ('Windows 10 Version 1709')
   davon mit Blockword:            2 ('Windows 10 Version 1809')
   davon mit Blockword:          221 ('Windows 10 Version 1903')
   davon mit Blockword:           63 ('Windows 10 Version 2004')
   davon mit Blockword:            0 ('64-Bit-Edition')
   davon mit Blockword:           31 ('x86-basierte Systeme')
   davon mit Blockword:           32 ('ARM64-basierte Systeme')
   davon mit Blockword:            0 ('Sharepoint')
   davon mit Blockword:            0 ('Upgrade auf Windows 10')
   davon mit Blockword:            0 ('Windows Server 2016 (1709)')
   davon mit Blockword:            0 ('Windows Server 2016 (1803)')
   davon mit Blockword:           11 ('x86-based Systems')
   davon mit Blockword:           10 ('ARM64-based Systems')
   davon mit Blockword:            0 ('Feature On Demand for X86')
   davon mit Blockword:           74 ('für ARM64-Editionen')
   davon mit Blockword:           97 ('für x86-Editionen')
   davon mit Blockword:           21 ('Microsoft Edge-Beta')
   davon mit Blockword:           15 ('Microsoft Edge-Dev')
   davon mit Ignoreword:          45 ('Funktionsupdate für Windows 10')
   davon mit Ignoreword:           2 ('The new Microsoft Edge for')
   davon mit Ignoreword:           7 ('Windows 10 Version 20H2')
   davon mit ImmediateWords:      13 ('Windows Defender')
   ------------------------------------------------------------------------
   aktuelle Updates:            302
   ------------------------------------------------------------------------
   sofort genehmigen:            13
   noch verzoegert:             289
   ohne Genehmigung:              0
   teilweise ohne Genehmigung:    0
   ohne Ablehnung:              578

Diese 289 Updates wurden neu geladen. Sie werden in 7 Tagen automatisch aktiviert:
```

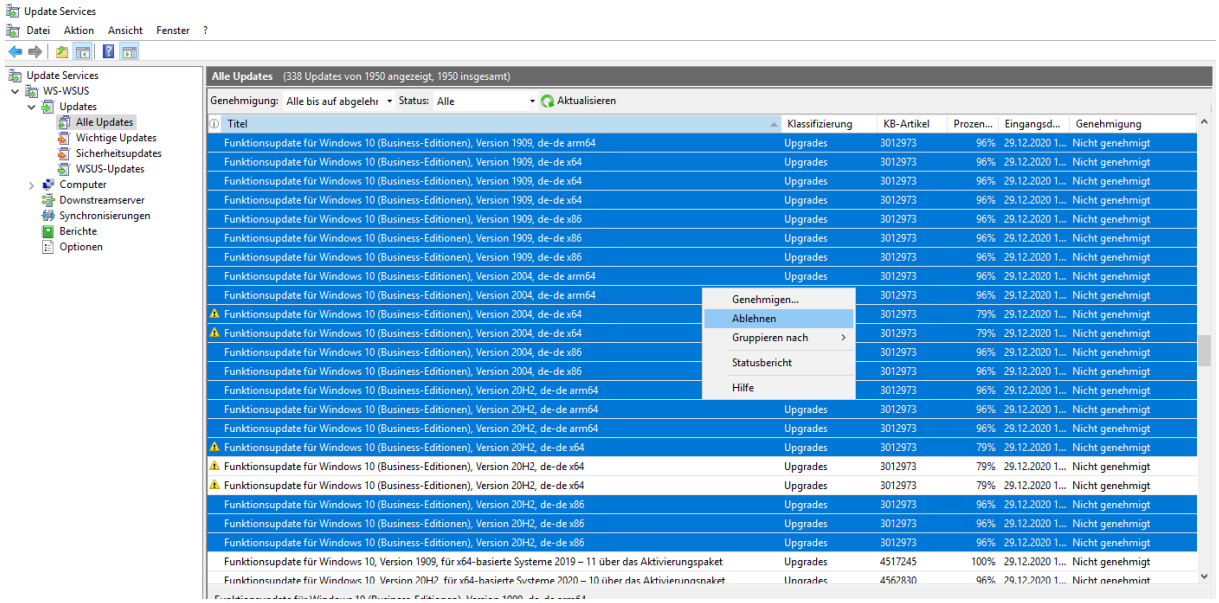
Jeder Lauf schlägt mir potentielle neue KeyWords für die Blocklist vor. Beim „ersten“ Lauf kommt da natürlich einiges zusammen. Danach starte ich die Ablehnung der nicht erforderlichen Updates:



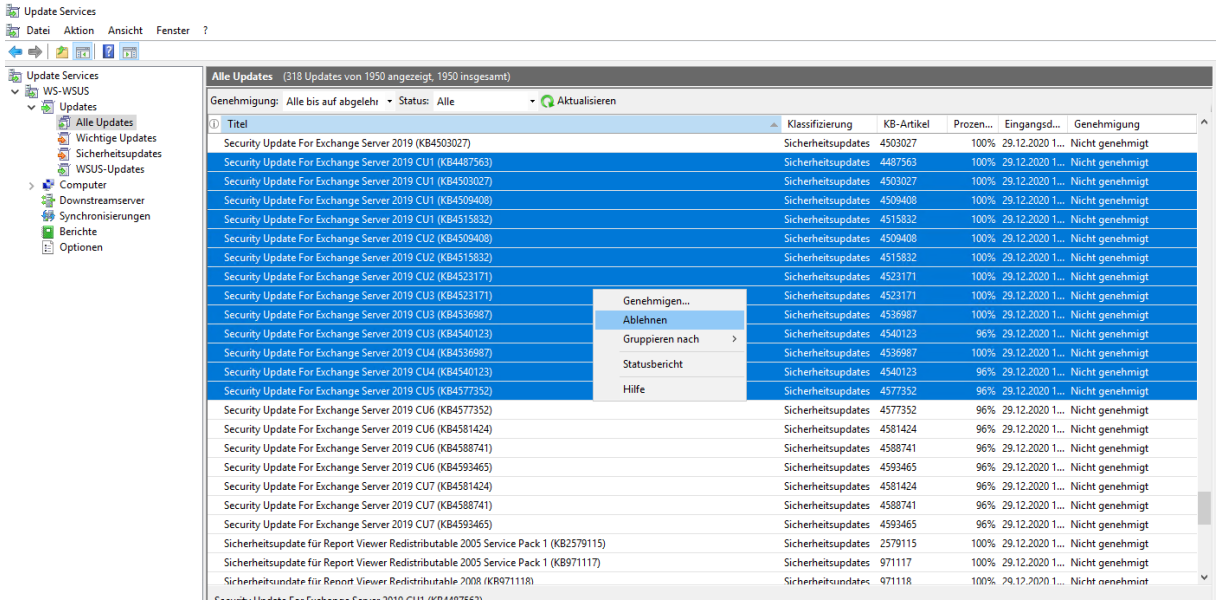


Funktionsupdates habe ich in meinem Script ausgeschlossen. Dies entferne ich in der Management-Konsole:

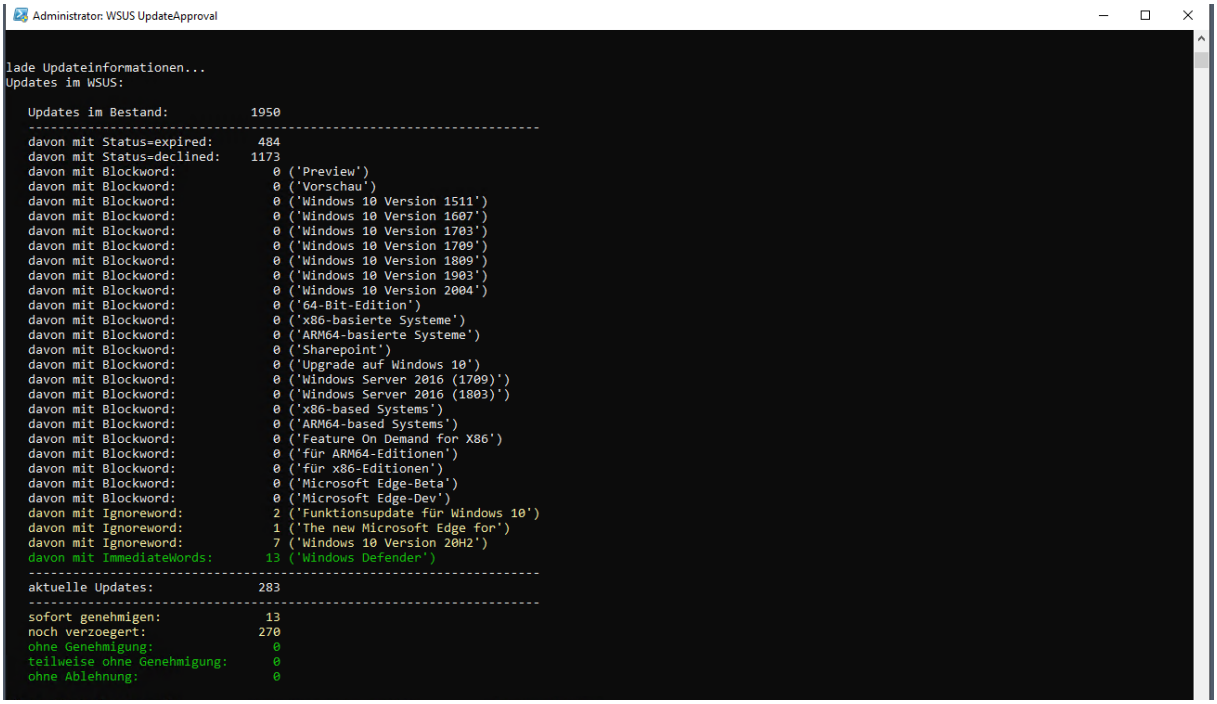




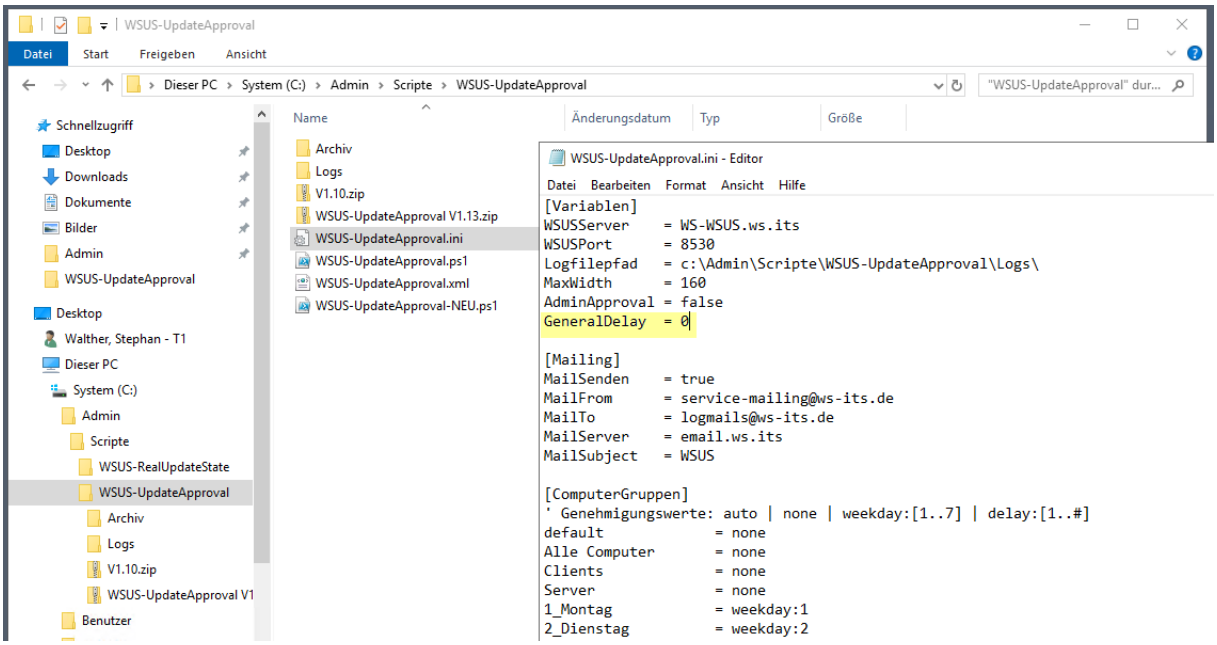
Ebenso sind etliche Exchange Updates enthalten, die ich durch meinen CU-Stand nicht mehr benötige. Auch diese lösche ich manuell:



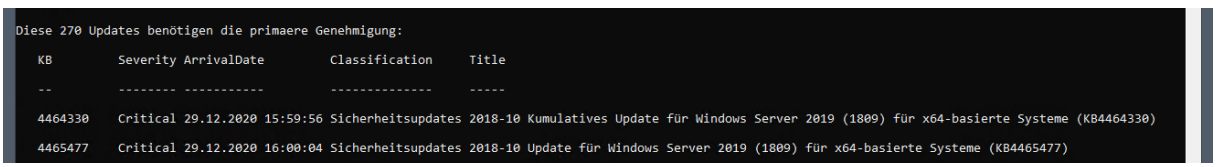
Nach diesen manuellen Bereinigungen starte ich mein Script erneut:



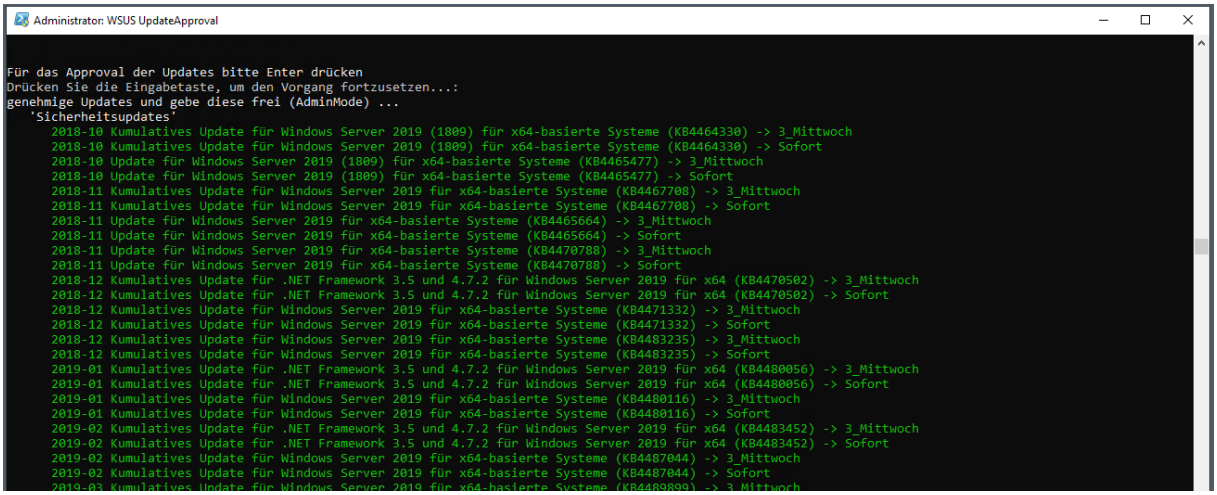
So sieht das schon viel angenehmer aus. Für einen ersten Lauf des WSUS deaktiviere ich in der Konfiguration des Scriptes das Delay:



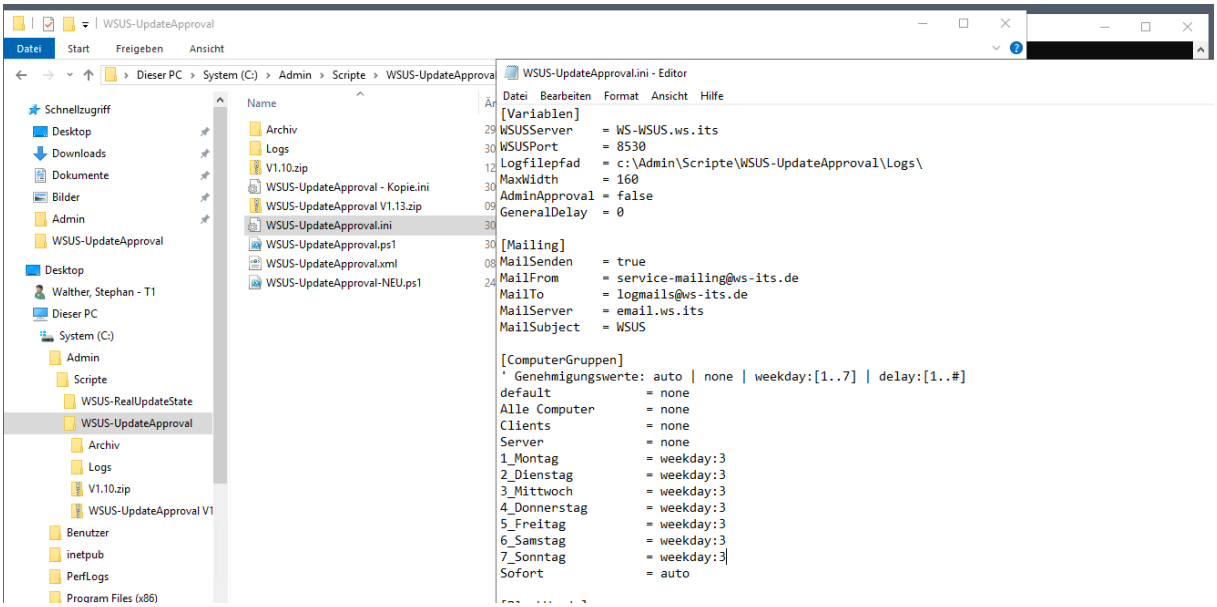
Mit einem neuen Scriptlauf werden die 270 Updates für die primäre Genehmigung erkannt. Primär bedeutet dabei, dass die Updates noch nie genehmigt und daher auch noch nicht heruntergeladen wurden. Die Genehmigung wird auf den WSUS-Containern vorgenommen, die „heute“ an der Reihe sind. Nach einer primären Genehmigung wird an jedem Folgetag eine Genehmigung auf ausstehenden Containern ermittelt und durchgeführt, bis alle Container und damit alle Computer versorgt werden:



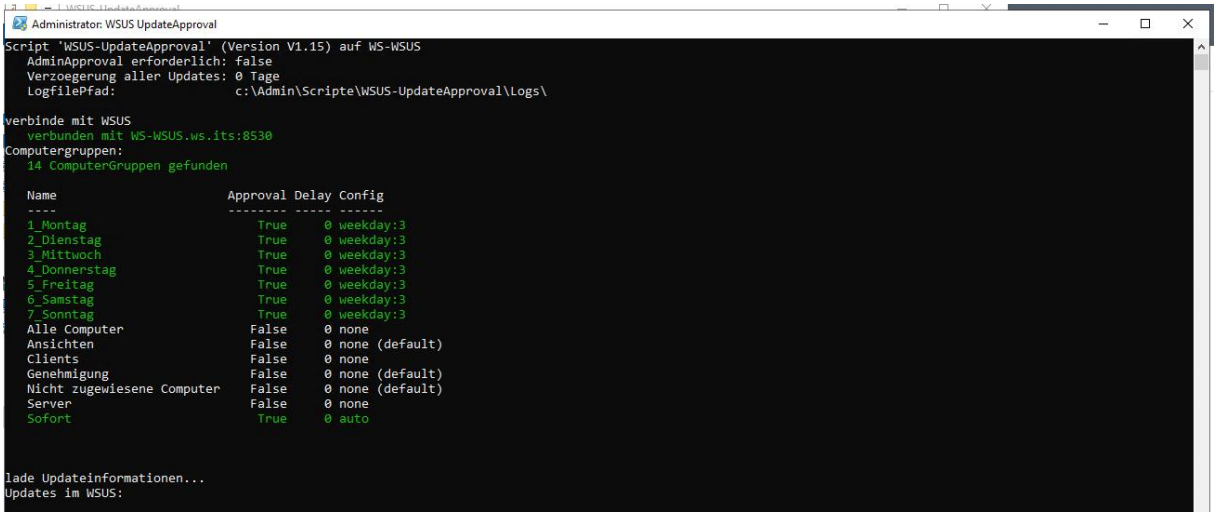
Ich bestätige mit Enter die Genehmigung. Heute ist Mittwoch. Daher werden die Updates für diesen Container und den Container „sofort“ freigeschaltet:



Diese Updates sind bei mir in der Infrastruktur schon installiert. Daher hole ich die Genehmigung mit meinem Script für alle anderen Container jetzt nach. Dafür ändere ich einfach in der Konfiguration den weekday:



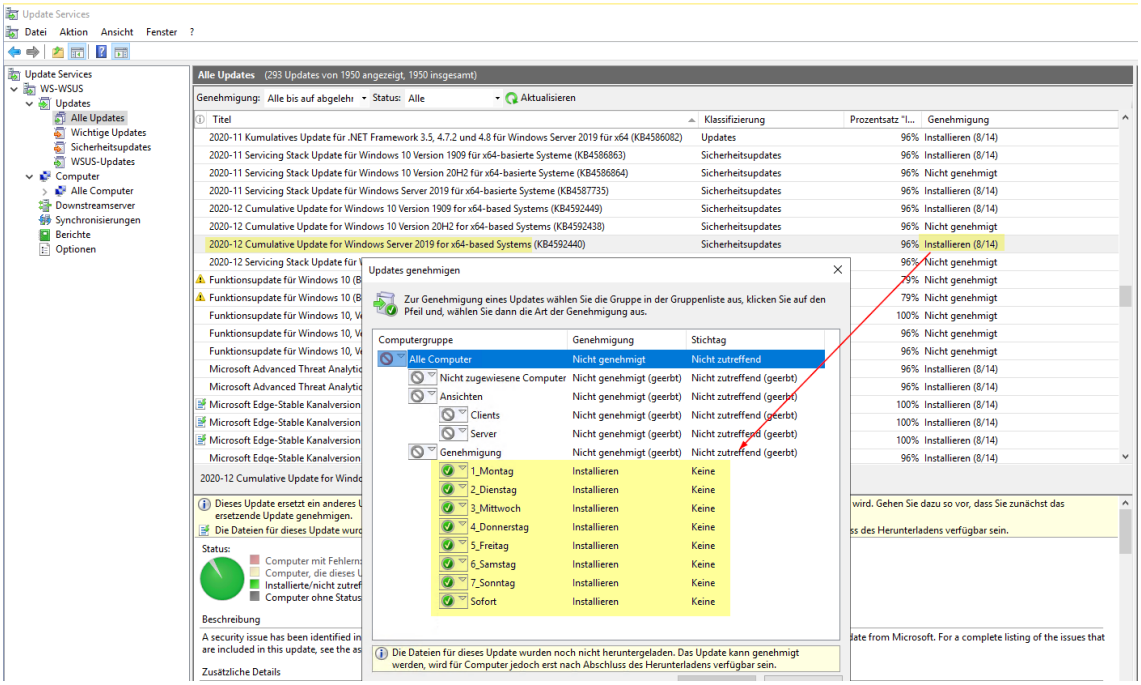
Der nächste Scriptlauf erkennt, dass „heute“ alle Container an der Reihe sind:



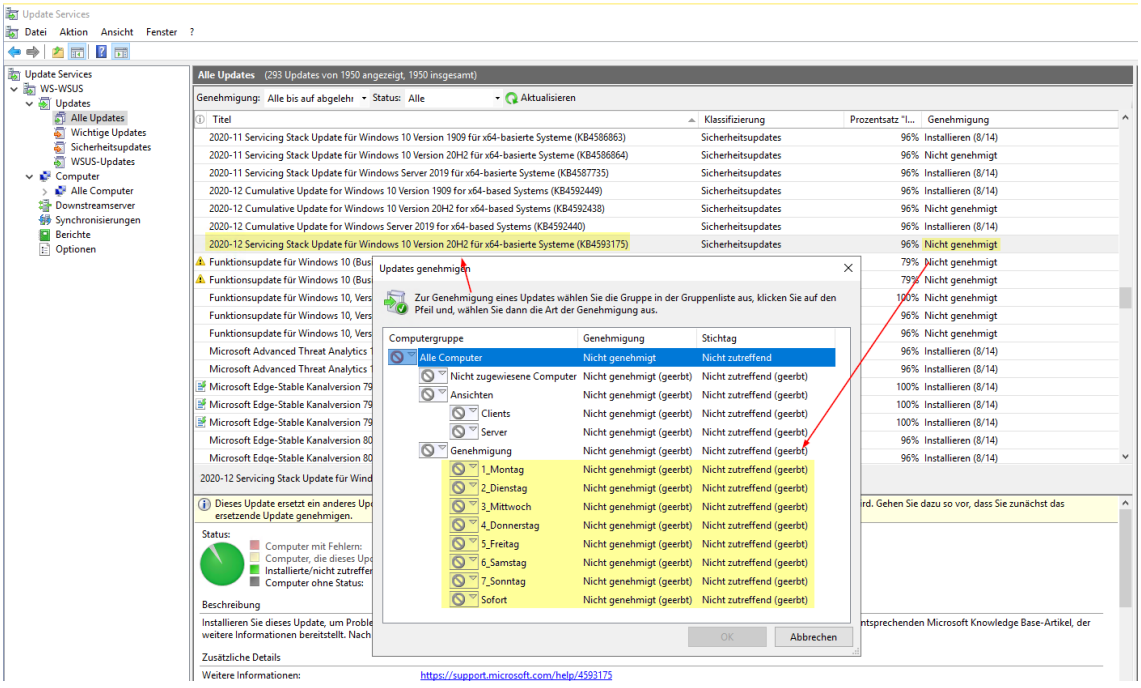
Dann wird die Genehmigung durchgeführt:

```
2019-05 Kumulatives Update für .NET Framework 3.5, 4.7.2 und 4.8 für Windows Server 2019 für x64 (KB4499405) -> 2_Dienstag
2019-05 Kumulatives Update für .NET Framework 3.5, 4.7.2 und 4.8 für Windows Server 2019 für x64 (KB4499405) -> 4_Donnerstag
2019-05 Kumulatives Update für .NET Framework 3.5, 4.7.2 und 4.8 für Windows Server 2019 für x64 (KB4499405) -> 5_Freitag
2019-05 Kumulatives Update für .NET Framework 3.5, 4.7.2 und 4.8 für Windows Server 2019 für x64 (KB4499405) -> 6_Samstag
2019-05 Kumulatives Update für .NET Framework 3.5, 4.7.2 und 4.8 für Windows Server 2019 für x64 (KB4499405) -> 7_Sonntag
2019-05 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4494441) -> 1_Montag
2019-05 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4494441) -> 2_Dienstag
2019-05 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4494441) -> 4_Donnerstag
2019-05 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4494441) -> 5_Freitag
2019-05 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4494441) -> 6_Samstag
2019-05 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4494441) -> 7_Sonntag
2019-05 Servicing Stack Update für Windows Server 2019 für x64-basierte Systeme (KB4499728) -> 1_Montag
2019-05 Servicing Stack Update für Windows Server 2019 für x64-basierte Systeme (KB4499728) -> 2_Dienstag
2019-05 Servicing Stack Update für Windows Server 2019 für x64-basierte Systeme (KB4499728) -> 4_Donnerstag
2019-05 Servicing Stack Update für Windows Server 2019 für x64-basierte Systeme (KB4499728) -> 5_Freitag
2019-05 Servicing Stack Update für Windows Server 2019 für x64-basierte Systeme (KB4499728) -> 6_Samstag
2019-05 Servicing Stack Update für Windows Server 2019 für x64-basierte Systeme (KB4499728) -> 7_Sonntag
2019-06 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4503327) -> 1_Montag
2019-06 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4503327) -> 2_Dienstag
2019-06 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4503327) -> 4_Donnerstag
2019-06 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4503327) -> 5_Freitag
```

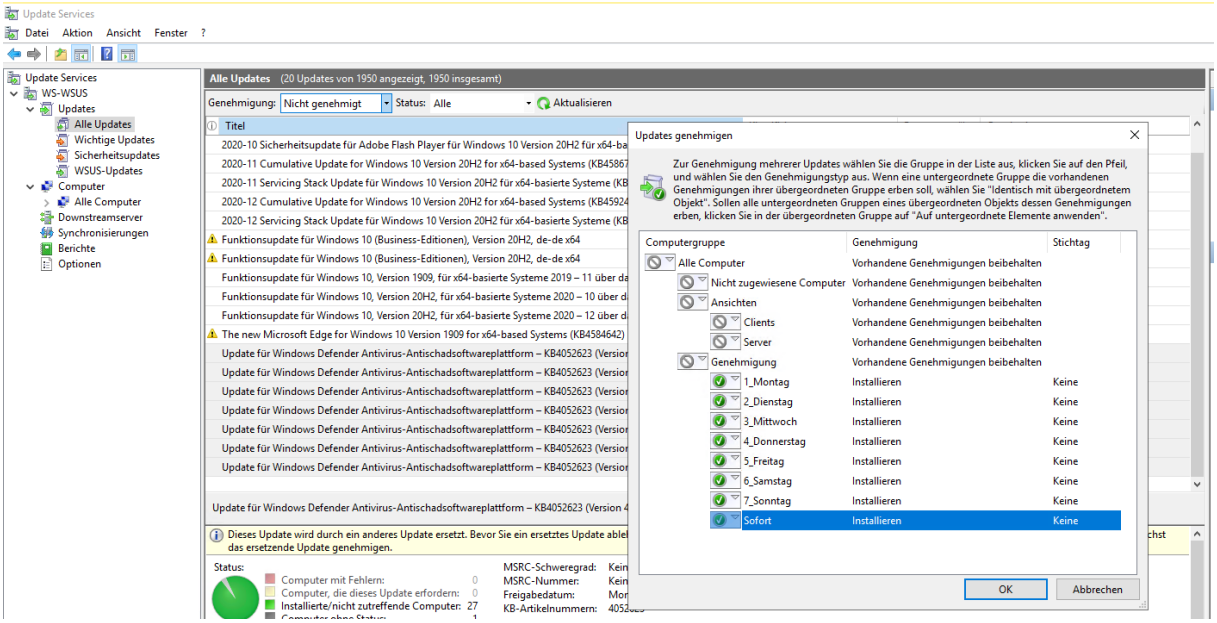
Ich teste das Ergebnis mit der WSUS-Konsole. Dieses Update ist auf allen erforderlichen Containern aktiv:



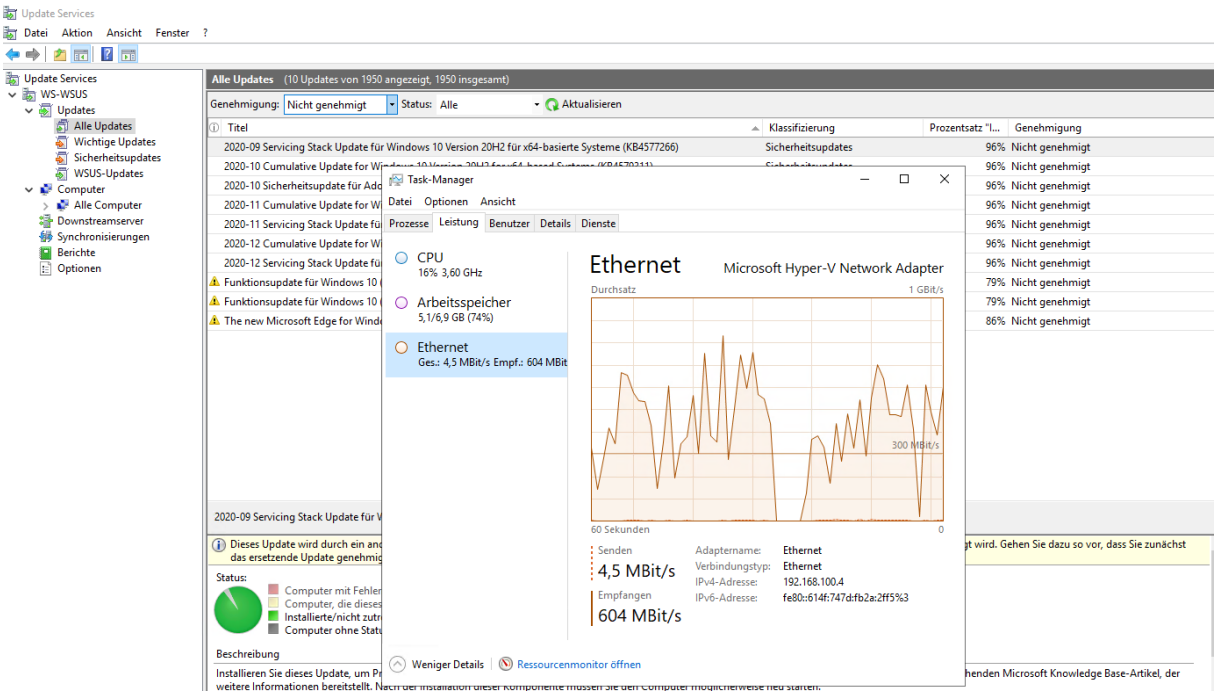
Alle Updates für Windows 10 20H2 werden derzeit noch durch das Script ignoriert. Das kann ich in der Konsole ebenfalls bestätigen:



Jetzt schaue ich mir noch die Updates an, die nicht genehmigt und nicht abgelehnt wurden. Die 20H2er sind irrelevant. Aber die Signatur-Updates brauchen noch eine Starthilfe (diese werden von meinem Script ignoriert und sollen über eine Default-Genehmigung vom WSUS bereitgestellt werden. Diese läuft aber erst beim nächsten Sync.). Also genehmige ich manuell:



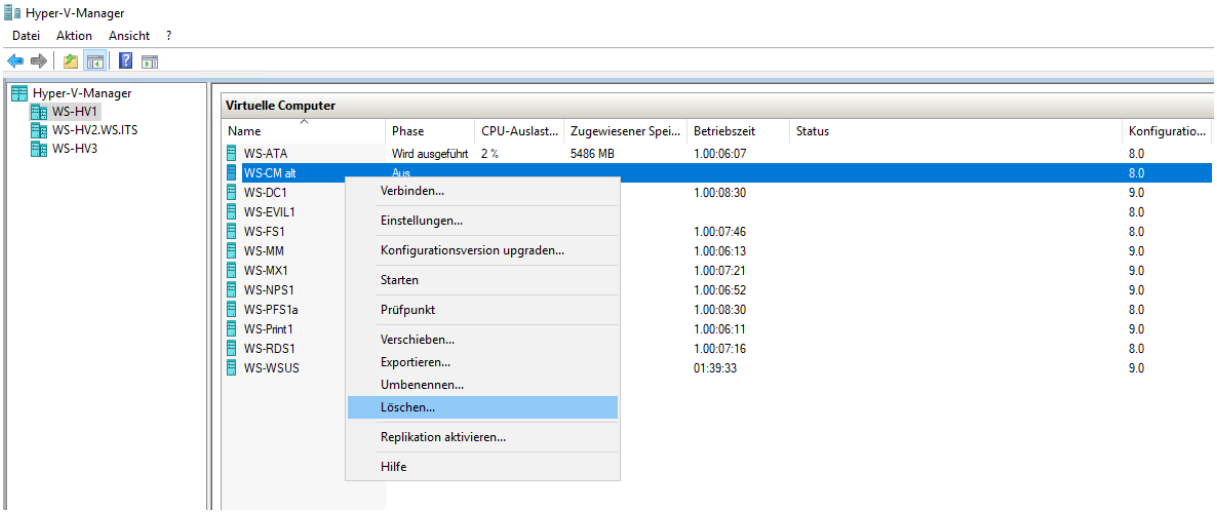
Nach einer Genehmigung wird der WSUS die Updates von den Microsoft Servern herunterladen. Das kann einen Moment dauern:



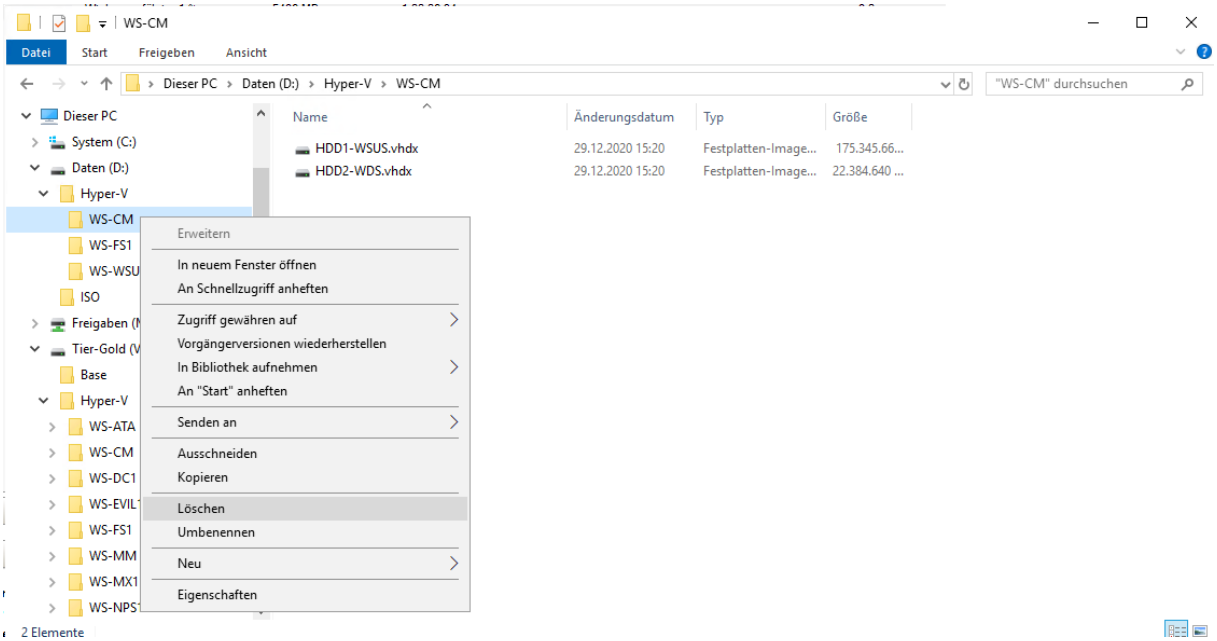
Danach passe ich meine Script-Konfiguration wieder auf die einzelnen Wochentage an und aktiviere das Delay von 7 Tagen.

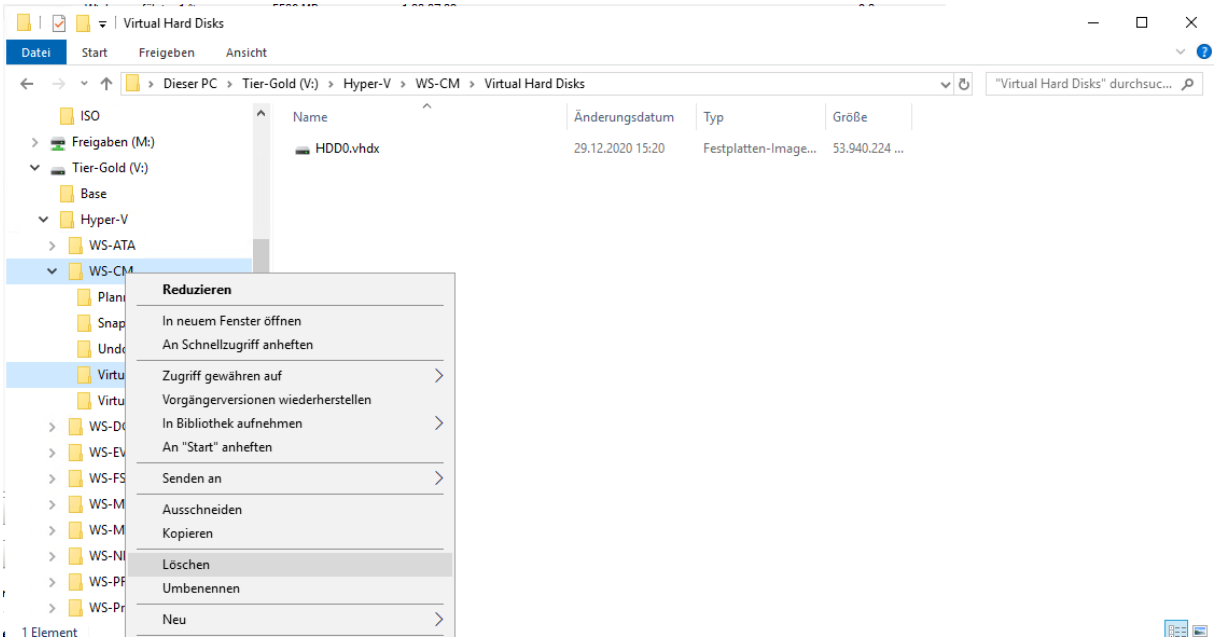
Cleanup

Der alte Server wird nun nicht mehr benötigt und kann gelöscht werden:

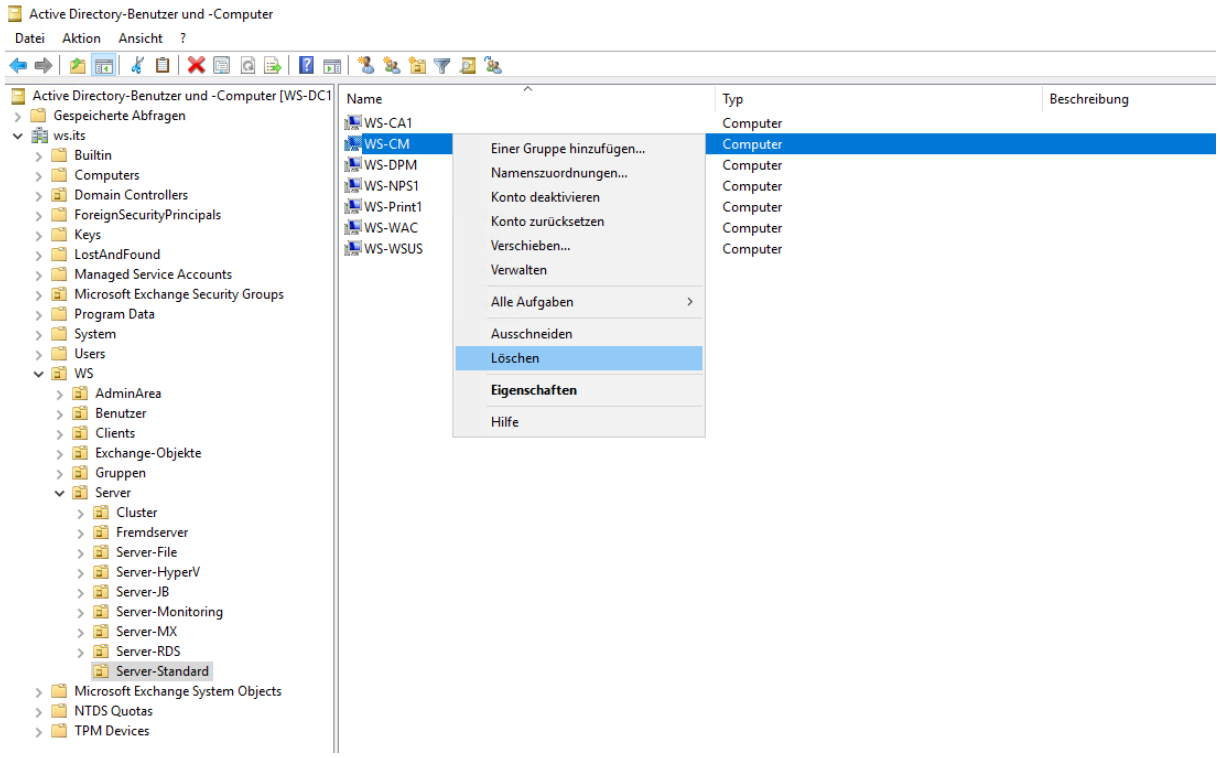


Die Festplattendateien werden dabei nicht vergessen:



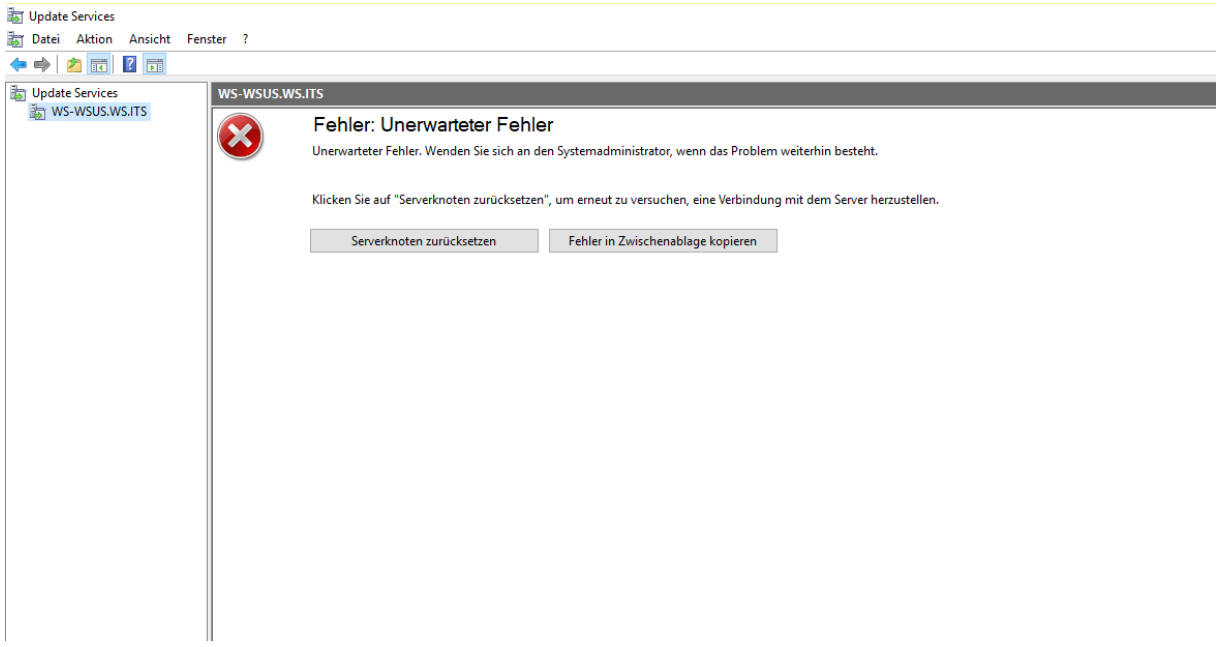


Ebenso wird das alte Computerkonto im Active Directory nicht mehr benötigt und kann gelöscht werden:

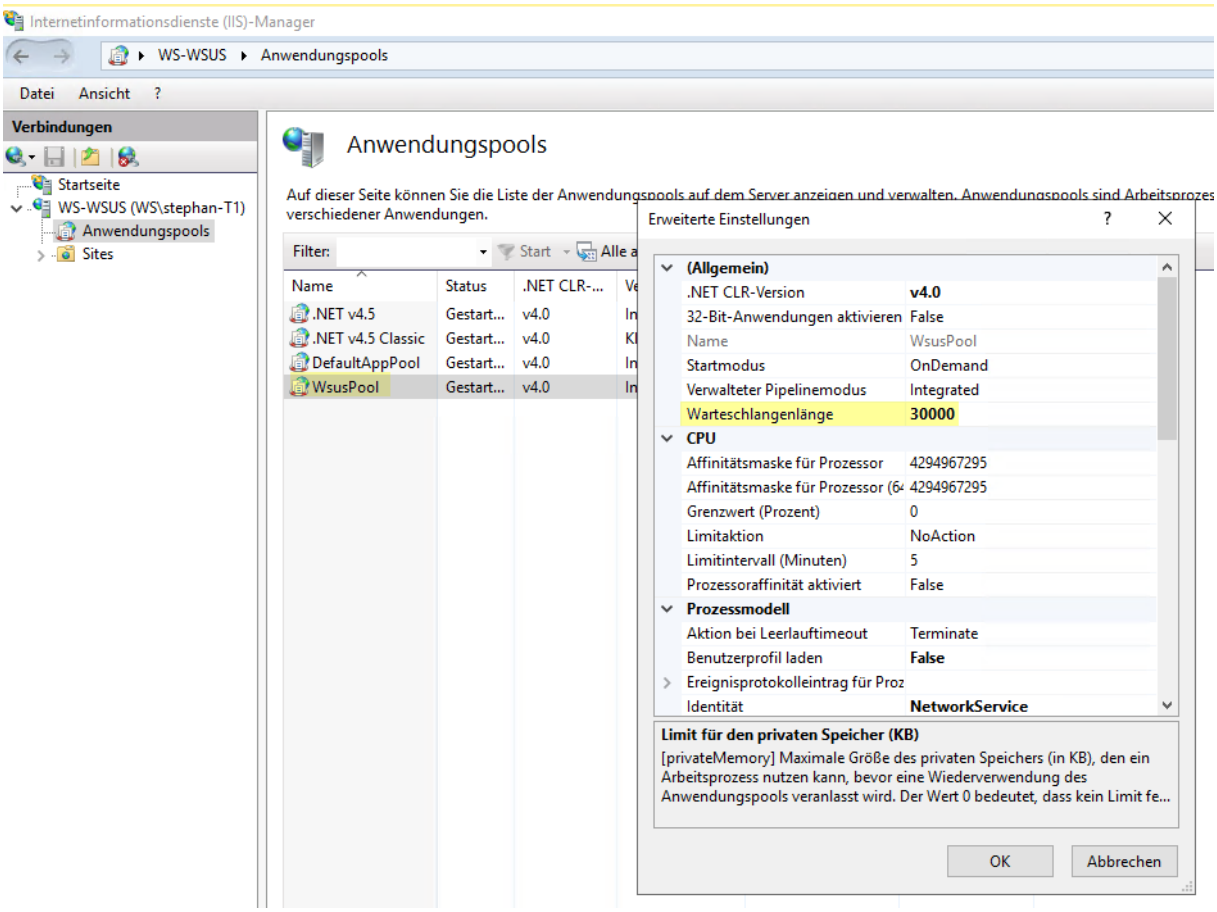


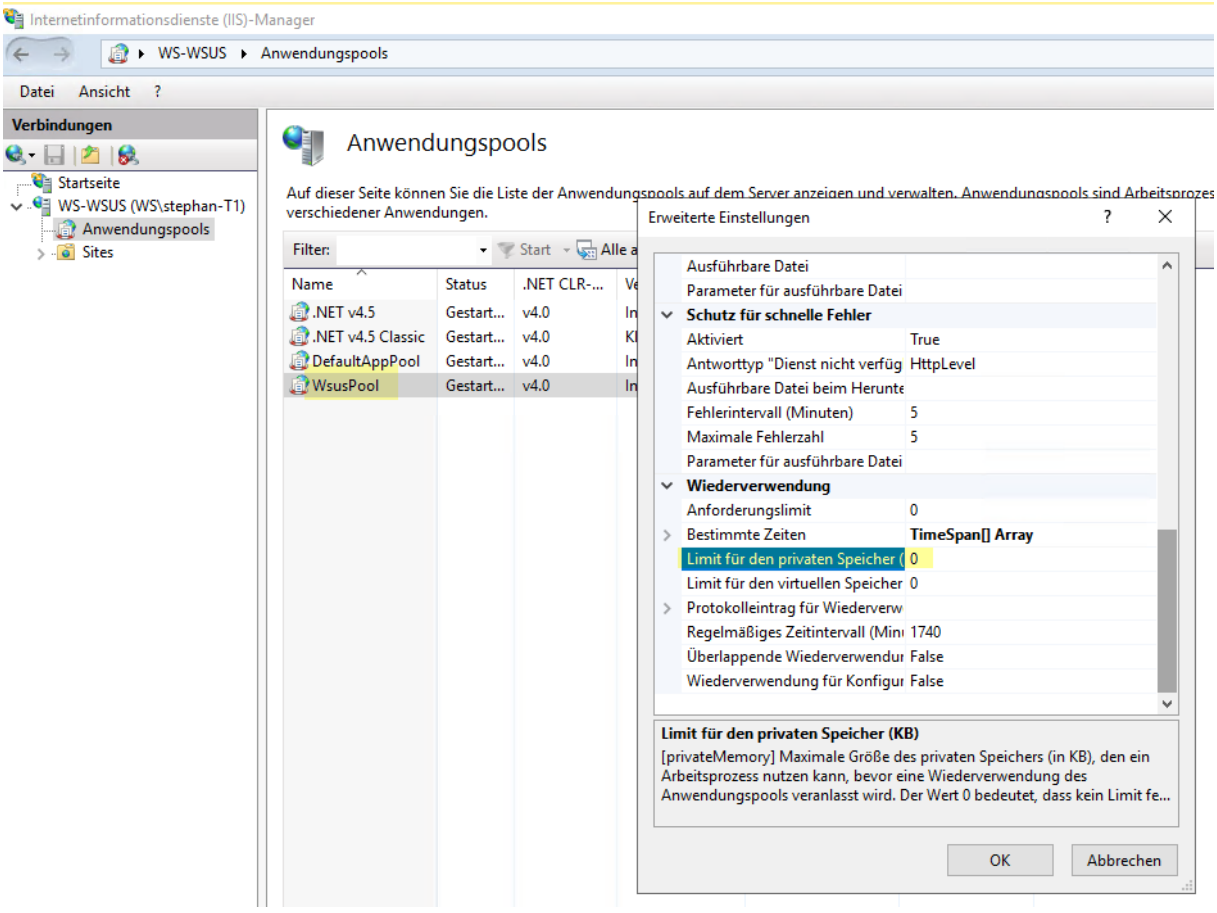
TroubleShooting Performance

Durch die vielen Scriptläufe und den Download der vielen Updates kommt es zu einem Problem in der WSUS-Konsole. Die Ursache ist mir durchaus bekannt und kann auf zu wenig System-Ressourcen zurückgeführt werden:

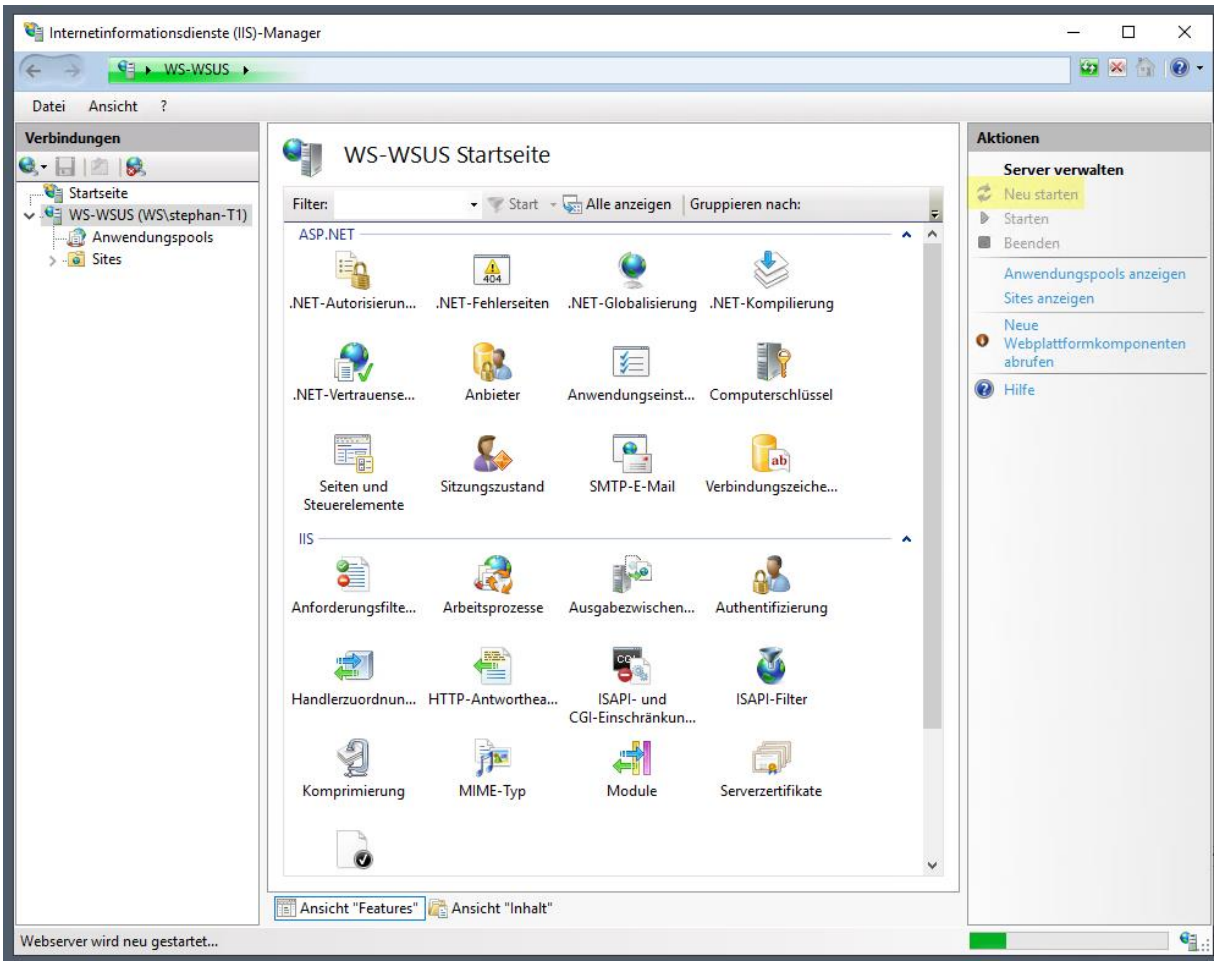


Der WSUS stellt seine Anwendung im IIS bereit. Dabei genügen die Standardeinstellungen für den Application-Pool sehr selten. Ich passe die Werte entsprechend an:


Internetinformationsdienste (IIS)-Manager
WS-WSUS ▸ Anwendungspools
Datei Ansicht ?
Verbindungen
Startseite
WS-WSUS (WS\stephan-T1)
Anwendungspools
Sites
Anwendungspools
Auf dieser Seite können Sie die Liste der Anwendungspools auf dem Server anzeigen und verwalten. Anwendungspools sind Arbeitsprozes
verschiedener Anwendungen.
Filter:
Start
Alle a
Name
Status
.NET CLR-...
.NET v4.5
Gestart...
v4.0
.NET v4.5 Classic
Gestart...
v4.0
DefaultAppPool
Gestart...
v4.0
WsusPool
Gestart...
v4.0
Erweiterte Einstellungen
(Allgemein)
.NET CLR-Version
v4.0
32-Bit-Anwendungen aktivieren
False
Name
WsusPool
Startmodus
OnDemand
Verwalteter Pipelinemodus
Integrated
Warteschlangenlänge
30000
CPU
Affinitätsmaske für Prozessor
4294967295
Affinitätsmaske für Prozessor (6
4294967295
Grenzwert (Prozent)
0
Limitaktion
NoAction
Limitintervall (Minuten)
5
Prozessoraffinität aktiviert
False
Prozessmodell
Aktion bei Leerlauftimeout
Terminate
Benutzerprofil laden
False
Ereignisprotokolleintrag für Proz
Identität
NetworkService
Limit für den privaten Speicher (KB)
[privateMemory] Maximale Größe des privaten Speichers (in KB), den ein Arbeitsprozess nutzen kann, bevor eine Wiederverwendung des Anwendungspools veranlasst wird. Der Wert 0 bedeutet, dass kein Limit fe...
OK
Abbrechen


Internetinformationsdienste (IIS)-Manager
WS-WSUS ▸ Anwendungspools
Datei Ansicht ?
Verbindungen
Startseite
WS-WSUS (WS\stephan-T1)
Anwendungspools
Sites
Anwendungspools
Auf dieser Seite können Sie die Liste der Anwendungspools auf dem Server anzeigen und verwalten. Anwendungspools sind Arbeitsprozes
verschiedener Anwendungen.
Filter:
Start
Alle a
Name
Status
.NET CLR-...
.NET v4.5
Gestart...
v4.0
.NET v4.5 Classic
Gestart...
v4.0
DefaultAppPool
Gestart...
v4.0
WsusPool
Gestart...
v4.0
Erweiterte Einstellungen
Ausführbare Datei
Parameter für ausführbare Datei
Schutz für schnelle Fehler
Aktiviert
True
Antworttyp "Dienst nicht verfüg
HttpLevel
Ausführbare Datei beim Herunte
Fehlerintervall (Minuten)
5
Maximale Fehlerzahl
5
Parameter für ausführbare Datei
Wiederverwendung
Anforderungslimit
0
Bestimmte Zeiten
TimeSpan[] Array
Limit für den privaten Speicher (
0
Limit für den virtuellen Speicher
0
Protokolleintrag für Wiederverw
Regelmäßiges Zeitintervall (Mini
1740
Überlappende Wiederverwendur
False
Wiederverwendung für Konfigur
False
Limit für den privaten Speicher (KB)
[privateMemory] Maximale Größe des privaten Speichers (in KB), den ein Arbeitsprozess nutzen kann, bevor eine Wiederverwendung des Anwendungspools veranlasst wird. Der Wert 0 bedeutet, dass kein Limit fe...
OK
Abbrechen

Nach den beiden Modifikationen starte ich den IIS einmal durch:

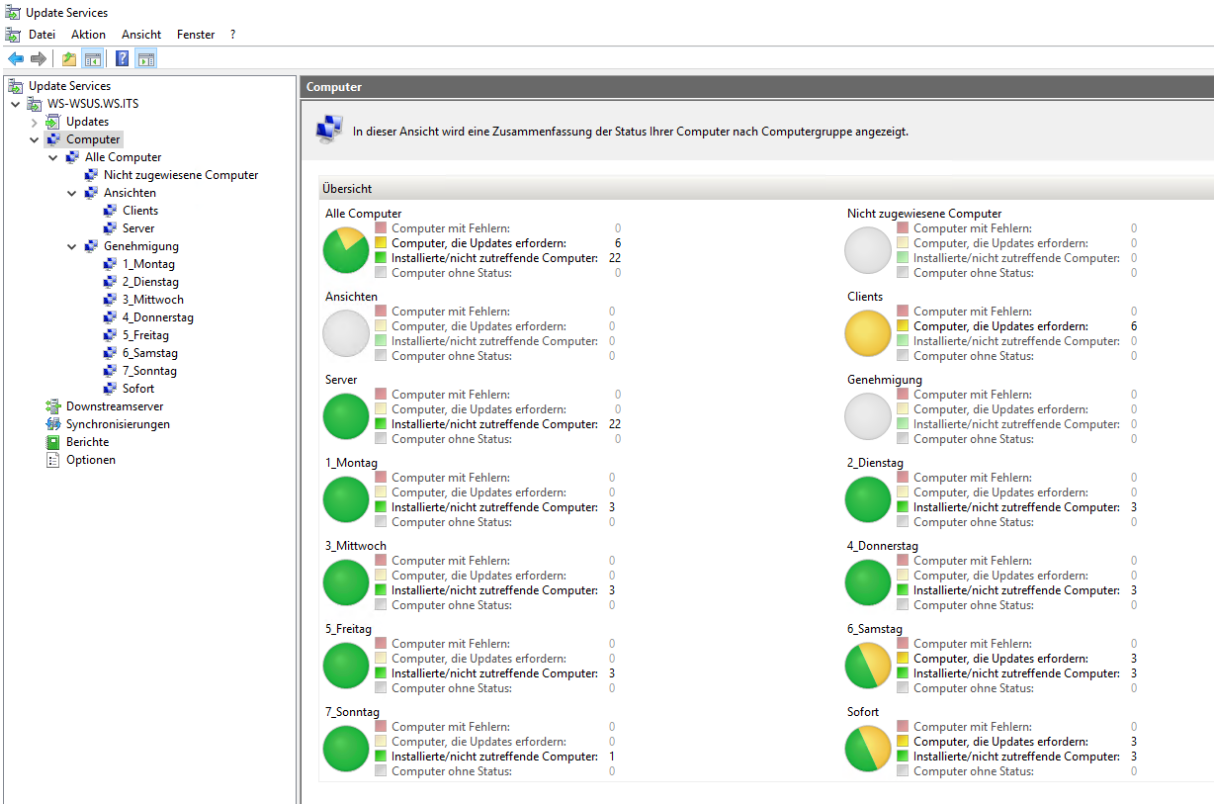


Danach funktioniert die Verbindung zwischen WSUS und Konsole wieder.

Zusammenfassung

Ergebnis

Meine Clients und Server haben sich mittlerweile alle beim WSUS gemeldet und wurden in ihre neuen Container eingruppiert. Auch die Updates sind alle geladen. So konnten meine Computer ihr Patchlevel an den WSUS melden. Und in der WSUS-Console kann ich das Ergebnis überprüfen. Man erkennt viel Grün. Ebenso kann man sehen, dass ich meine Systeme auf die 7 Wochentage aufgeteilt habe:



Mein Script „WSUS-RealUpdateState“ hat mir auch schon die erste Mail zukommen lassen. Darin werden die Computer mit ihrem echten Update-Level gezeigt (Updates, die nicht genehmigt wurden, werden nicht gewertet). Auch hier ist alles Grün. Zusätzlich kann man jetzt recht gut erkennen, wofür ich die „Ansichten“-Container verwende:

Zusammenfassung

count	name	Proz
28	OK	100%

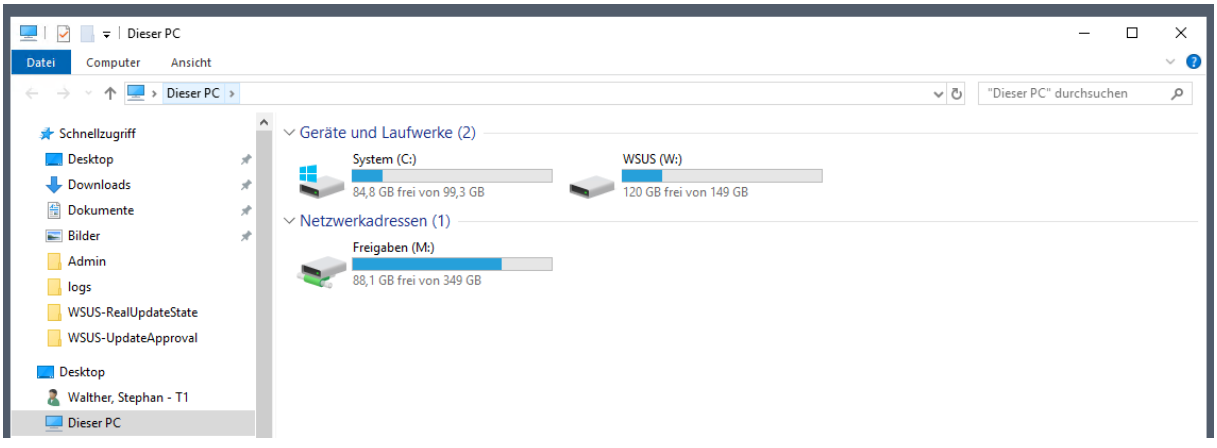
Clients

FullDomainName	IPAddress	Groups	ODDescription	LastReport	NotInstalled	Downloaded	Failed	other
ws-cl1.ws.its	192.168.110.101	6_Samstag		2020-12-30 12:45	0	0	0	0
ws-cl3.ws.its	192.168.111.100	6_Samstag		2020-12-30 12:51	0	0	0	0
ws-cl4	172.19.130.101	Sofort		2020-12-30 01:10	0	0	0	0
ws-cl5.ws.its	192.168.110.106	Sofort		2020-12-30 12:36	0	0	0	0
ws-cl6.ws.its	192.168.110.154	Sofort		2020-12-30 12:52	0	0	0	0
ws-cl7.ws.its	192.168.110.152	6_Samstag		2020-12-30 05:53	0	0	0	0

Server

FullDomainName	IPAddress	Groups	ODDescription	LastReport	NotInstalled	Downloaded	Failed	other
ws-ata.ws.its	192.168.100.23	2_Dienstag		2020-12-30 01:06	0	0	0	0
ws-ca1.ws.its	192.168.100.6	2_Dienstag		2020-12-30 12:11	0	0	0	0
ws-dc1.ws.its	192.168.100.1	5_Freitag		2020-12-30 11:43	0	0	0	0
ws-dc2.ws.its	192.168.100.2	3_Mittwoch		2020-12-30 12:08	0	0	0	0
ws-dc3.ws.its	192.168.101.1	4_Donnerstag		2020-12-30 12:41	0	0	0	0
ws-dpm.ws.its	192.168.100.5	1_Montag		2020-12-30 11:31	0	0	0	0
ws-fs1.ws.its	192.168.100.11	5_Freitag		2020-12-30 11:32	0	0	0	0
ws-fs2.ws.its	192.168.100.12	3_Mittwoch		2020-12-30 12:49	0	0	0	0
ws-fs3.ws.its	192.168.101.3	1_Montag		2020-12-30 12:49	0	0	0	0
ws-hv1.ws.its	192.168.100.9	Sofort		2020-12-30 12:40	0	0	0	0
ws-hv2.ws.its	192.168.100.10	Sofort		2020-12-30 12:40	0	0	0	0
ws-hv3.ws.its	192.168.101.2	7_Sonntag		2020-12-30 12:41	0	0	0	0
ws-mm	192.168.110.104	Sofort		2020-12-30 12:37	0	0	0	0
ws-mon.ws.its	192.168.100.18	6_Samstag		2020-12-30 12:46	0	0	0	0
ws-mx1.ws.its	192.168.100.3	1_Montag		2020-12-30 11:00	0	0	0	0
ws-mx2.ws.its	192.168.100.13	5_Freitag		2020-12-30 10:02	0	0	0	0
ws-nps1.ws.its	192.168.100.7	4_Donnerstag		2020-12-30 11:29	0	0	0	0
ws-print1.ws.its	192.168.100.14	4_Donnerstag		2020-12-30 12:48	0	0	0	0
ws-rds1.ws.its	192.168.110.16	3_Mittwoch		2020-12-30 10:30	0	0	0	0
ws-rds2.ws.its	192.168.110.21	2_Dienstag		2020-12-30 10:43	0	0	0	0
ws-wac.ws.its	192.168.100.22	6_Samstag		2020-12-30 12:29	0	0	0	0
ws-wsus.ws.its	fe80::614f:747d:fb2a:2ff5%3	6_Samstag		2020-12-30 11:17	0	0	0	0

Durch die gezielte Auswahl der erforderlichen Updates habe ich auf meinem Datenträger E: enorm viel Speicherplatz einsparen können:



Insgesamt ist der Server besser als vorher aufgestellt. Die Migration kann damit als abgeschlossen betrachtet werden.