Inhalt

Zielsetzung

Im Vorfeld dieser Aktionen hatte ich zu meinen beiden alten Hyper-V-Servern WS-HV1 und WS-HV2 zwei neue Server gekauft und als WS-HV3 und WS-HV4 installiert. So war mir eine Side-by-Side-Migration meiner virtuellen Maschinen möglich:

- alle VMs von **WS-HV2** wurden auf **WS-HV3** verschoben
- alle VMs von **WS-HV1** wurden auf **WS-HV4** verschoben

Nach der Migration habe ich die beiden alten Server zurückgebaut und entfernt. Eigentlich war jetzt alles gut. Aber ihr kennt das vielleicht: die Namen der Maschinen passen jetzt nicht mehr. Das ist wie ein schief hängendes Bild!

Und ich hatte ein Muster bei der Benennung meiner Server

- **WS-HV1** betreibt u.A. WS-DC1, WS-FS1, WS-MX1, WS-RDS1
- **WS-HV2** betreibt u.A. WS-DC2, WS-FS2, WS-MX2, WS-RDS2

Im Rahmen meiner Migration auf Windows Server 2019 möchte ich auch den 3. Hyper-V-Server in meinem Außenstandort neu installieren. Dieser soll dem Muster im Hauptstandort folgen:

- **WS-HV3** soll u.A WS-DC3 und WS-FS3 betreiben

Und hier wird das Problem deutlich: der Name **WS-HV3** ist bereits vergeben. Also muss ich die Namen der beiden ersten Server vorab anpassen. Das sollte doch kein Problem sein, oder?

Aber wer schon etwas Zeit mit Windows Servern verbracht hat, der weiß: Das wird nicht einfach. Vor einigen Tagen hatte ich mit einem Kunden eine kleine Diskussion zur Umbenennung von etlichen Servern. Ich vertrete den Standpunkt, dass Server nicht umbenannt werden sollten. Und dieser Artikel wird beweisen, dass der Aufwand und die Gefahren nicht zu unterschätzen sind!

Meine Zielsetzung sieht so aus:

- **WS-HV3** soll in **WS-HV2** umbenannt werden
- **WS-HV4** soll in **WS-HV1** umbenannt werden

Dazu möchte ich die alten IPv4-Adressen der Server wiederverwenden. Also steht auch ein Austausch der IP-Konfiguration an.

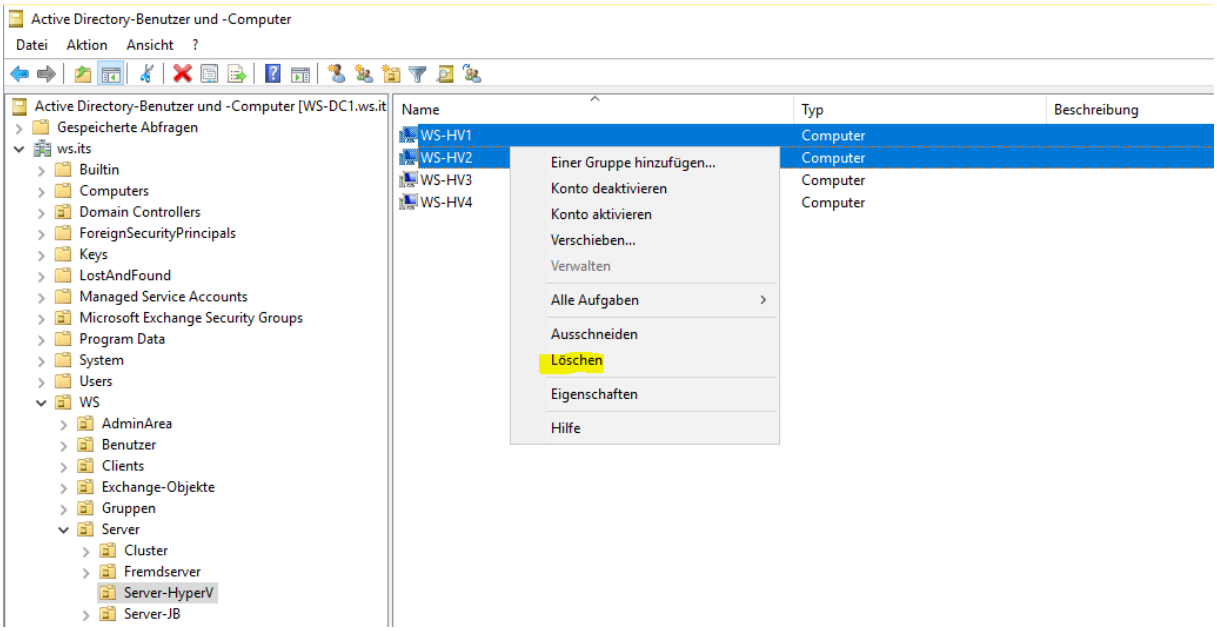
Vorarbeiten

Bedenkt immer:
Nicht jeder Server lässt sich einfach mit einem neuen Namen versehen. Für einige Services existieren aktive Blockierungen (z.B. bei PKI-Servern). Andere Services wie z.B. Active Directory oder Exchange Server haben ihre bekannten Probleme damit. Und bei anderen Servern könnten die installierten Anwendungen oder Funktionen wie z.B. das Failover Clustering Schwierigkeiten mit einem einfachen Umbenennen haben.

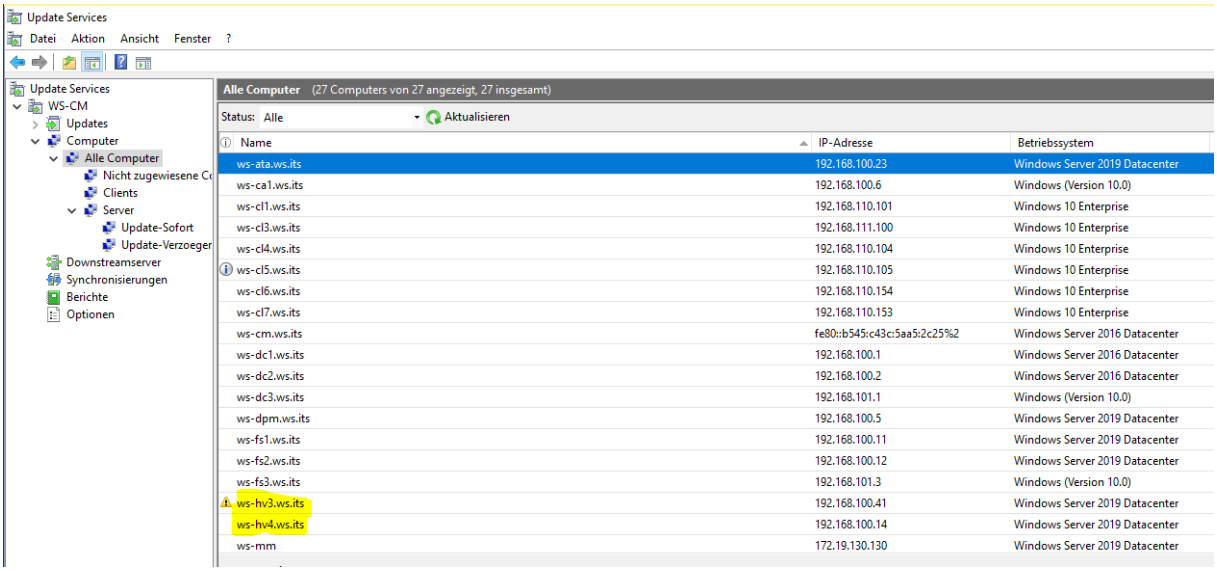
Empfehlung:
Prüft genau, ob es Einschränkungen und bekannte Probleme gibt, bevor ihr eure Server umbenennt. Nur weil das Betriebssystem euch nicht daran hindert, ist euch ein gelingen auch garantiert.

Für Hyper-V sind mir außerhalb eines Failover-Clusters und ohne Integration in einen Verwaltungsservice wie System Center Virtual Machine Manager keine Abhängigkeiten und Einschränkungen bekannt. Daher wage ich den Schritt.

Zuerst müssen die zuvor verwendeten Namen an allen Stellen entfernt werden! Ein wichtiger Speicher ist das Active Directory. Hier finde ich noch die beiden Computerkonten der alten Server. Diese lösche ich, damit deren Namen frei werden:



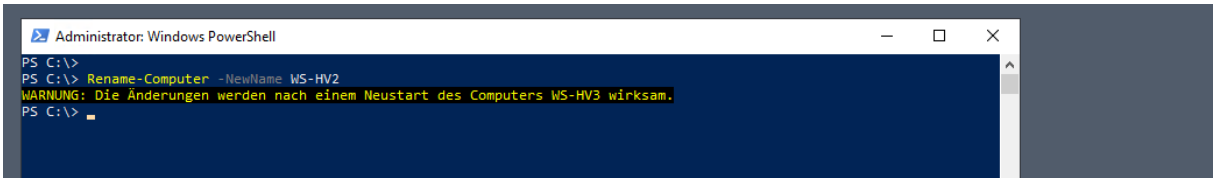
Im WSUS entferne ich ebenfalls die beiden alten Server. So bleiben nur die neuen Namen gelistet:



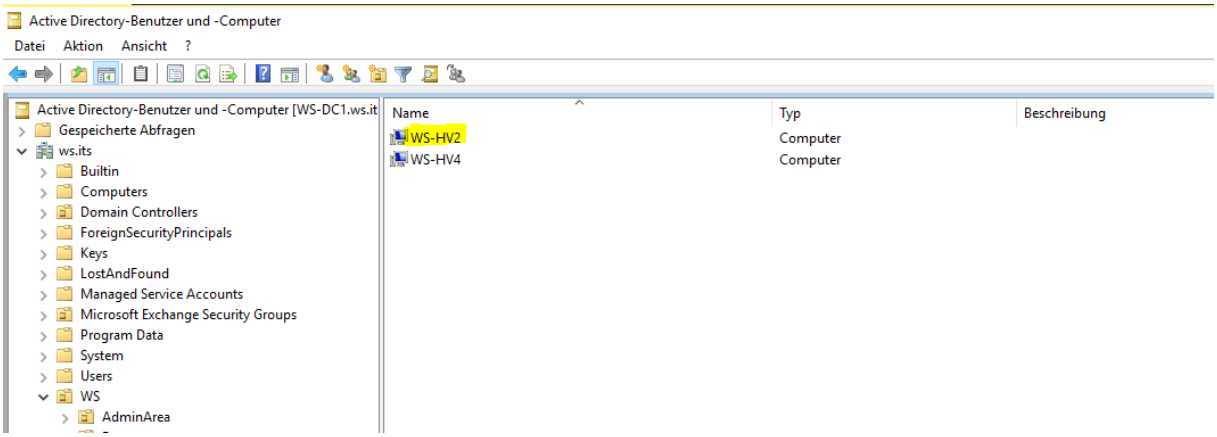
Umbenennen der Server

WS-HV3 wird zu WS-HV2

Das eigentliche Umbenennen ist wirklich einfach. Ich habe mich für den PowerShell-Befehl entschieden:

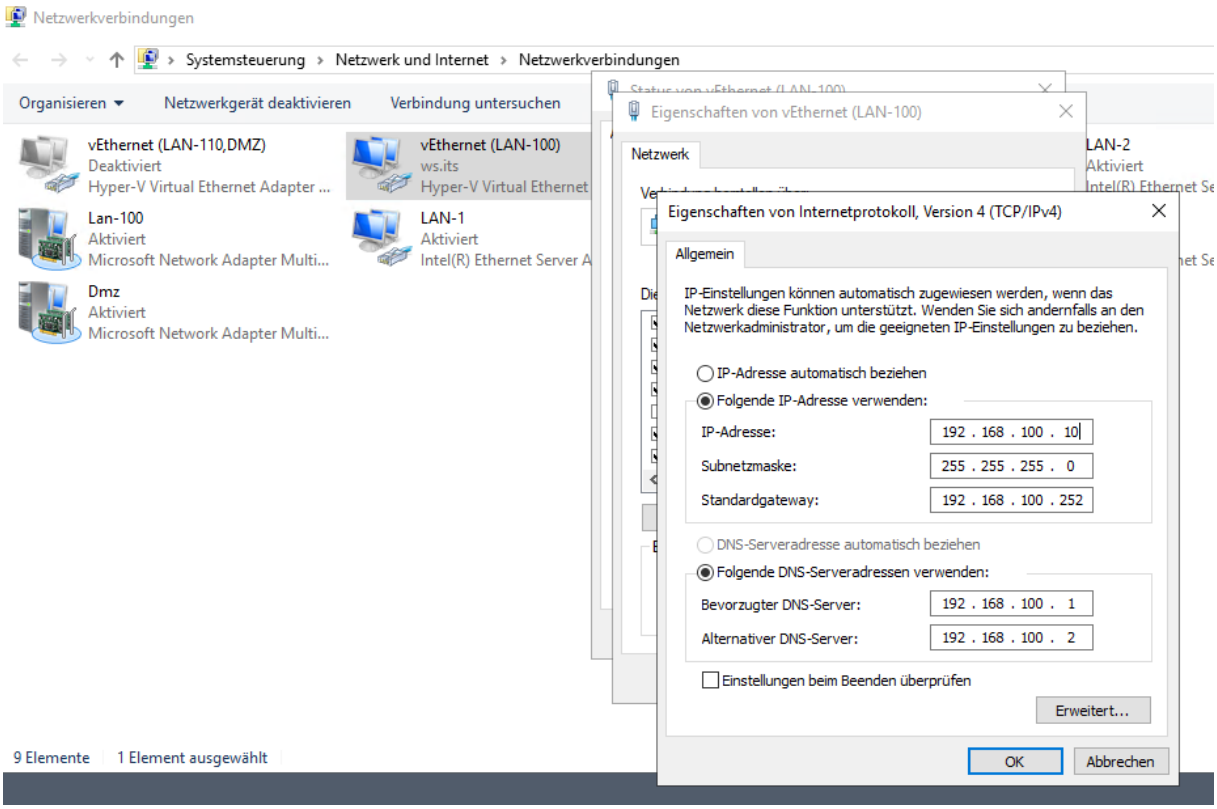


Der Computer benennt sein eigenes AD-Konto selber um:



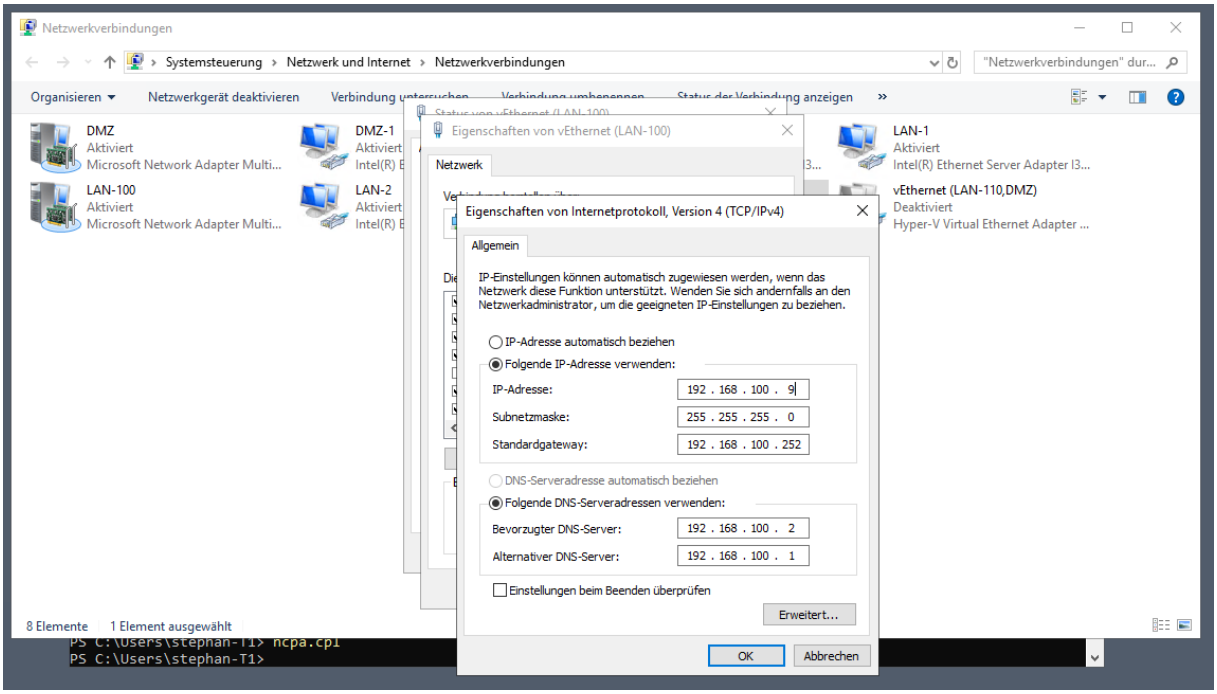
Diese Information sollte auf alle Domain Controller repliziert werden, bevor es weiter gehen kann. Ich hole mir also einen Kaffee. Danach darf der Server WS-HV2 neustarten.

Nun bekommt der Server noch seine IPv4-Adresse angepasst:

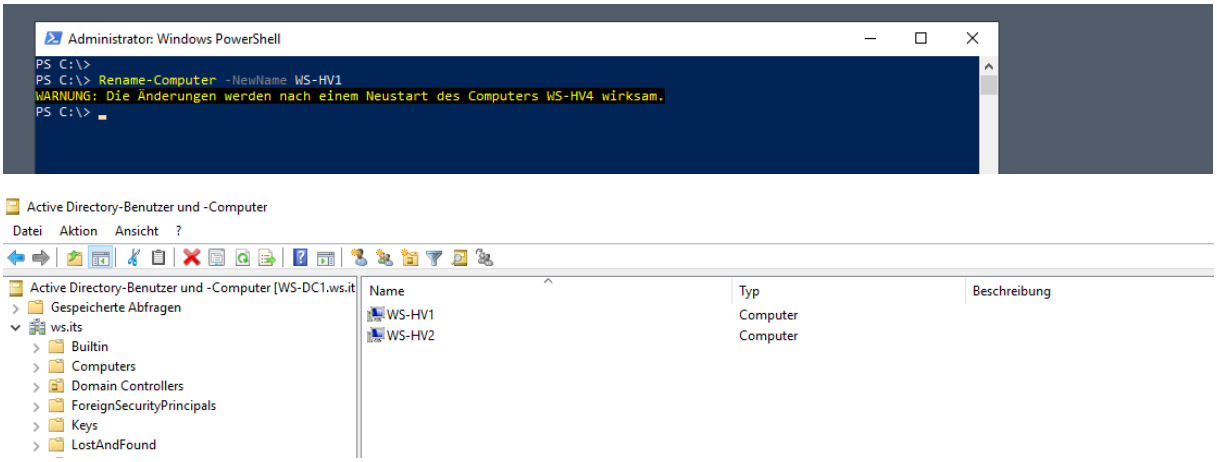


WS-HV4 wird zu WS-HV1

Beim 2. Server führe ich die gleichen Aktionen aus. Ich ändere die IP-Adresse:



Und anschließend erhält der Server seinen neuen Namen:



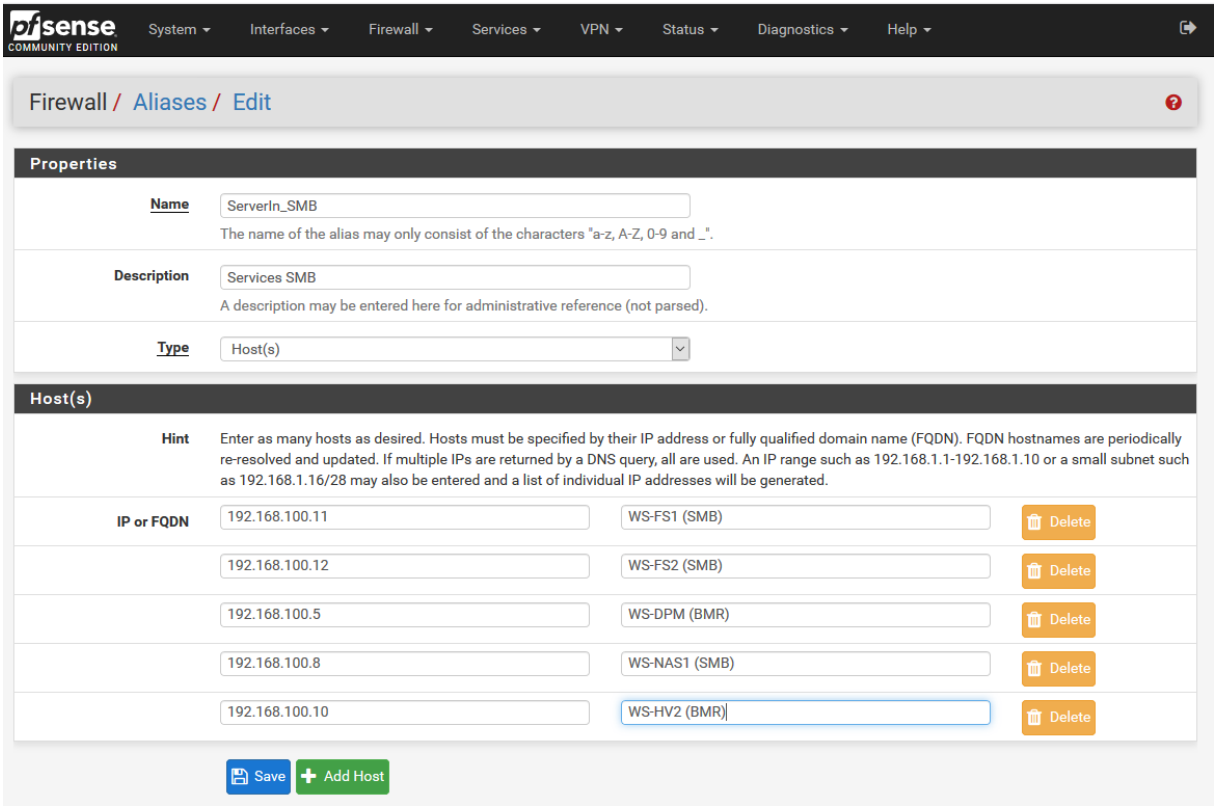
Einen Neustart (und einen weiteren Kaffee) später ist auch diese Aktion abgeschlossen.

Damit wäre das Offensichtliche erledigt. Nun folgen die vielen Anpassungen und Korrekturen…

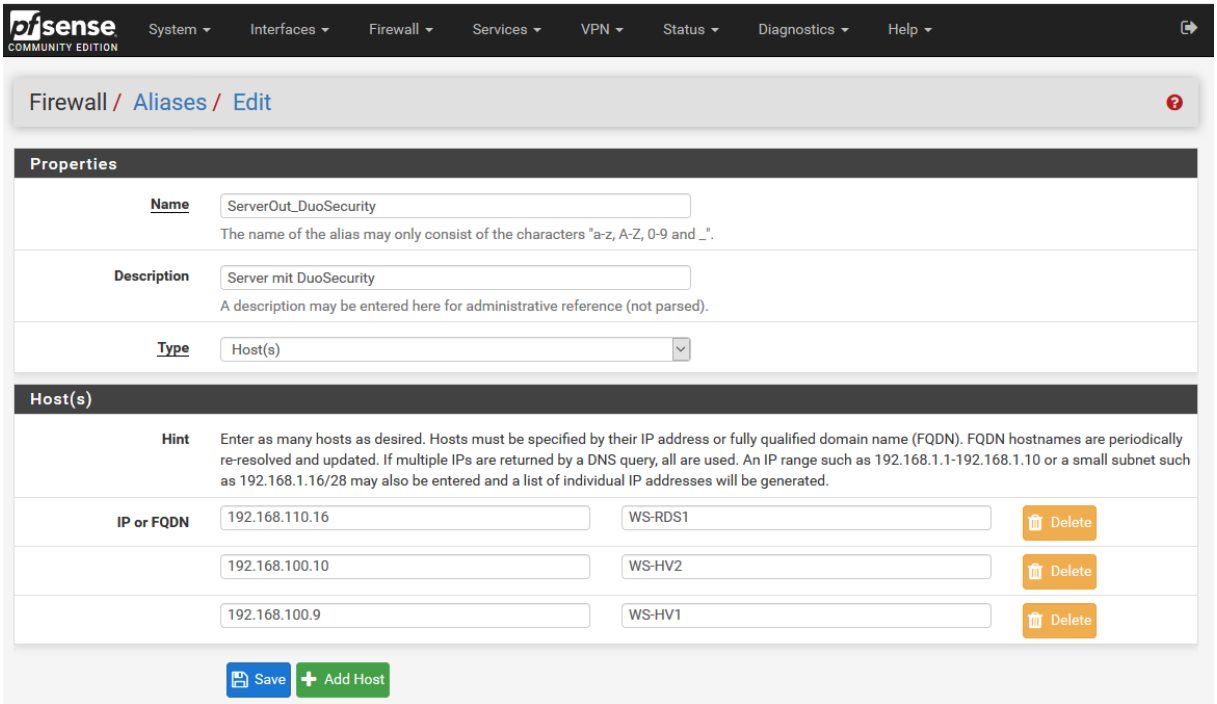
Nacharbeiten

Firewall

Im ersten Schritt passe ich die Aliase für meine Firewall-Ausnahmen an. Mein Server WS-HV2 stellt eine Freigabe bereit. Diese muss erreichbar sein:



Beide Server müssen eine URL im Internet für die 2FA erreichen können:

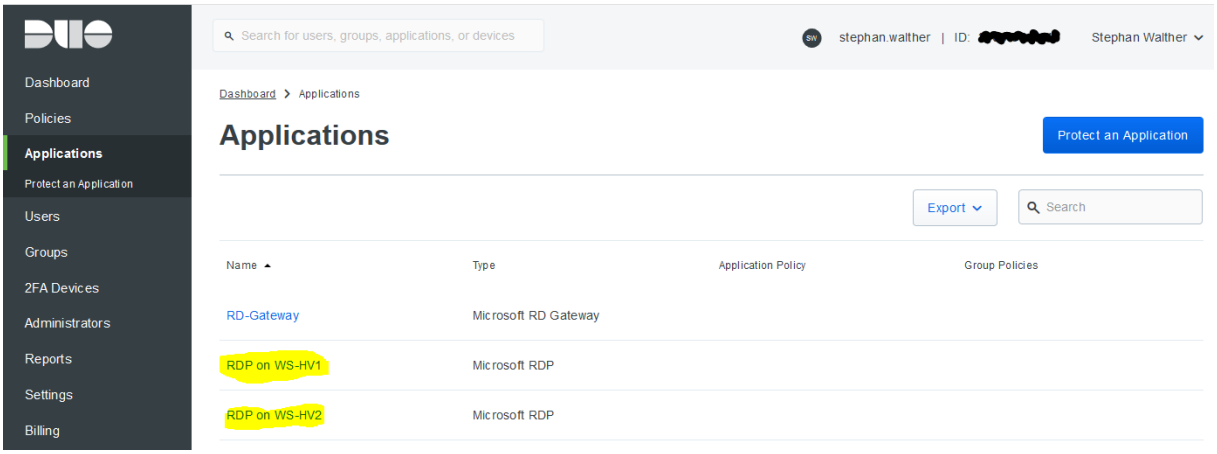


Mehr Ausnahmen sind für die beiden Server nicht vorhanden. Bei Servern mit anderen Services kann das natürlich mehr ausarten.

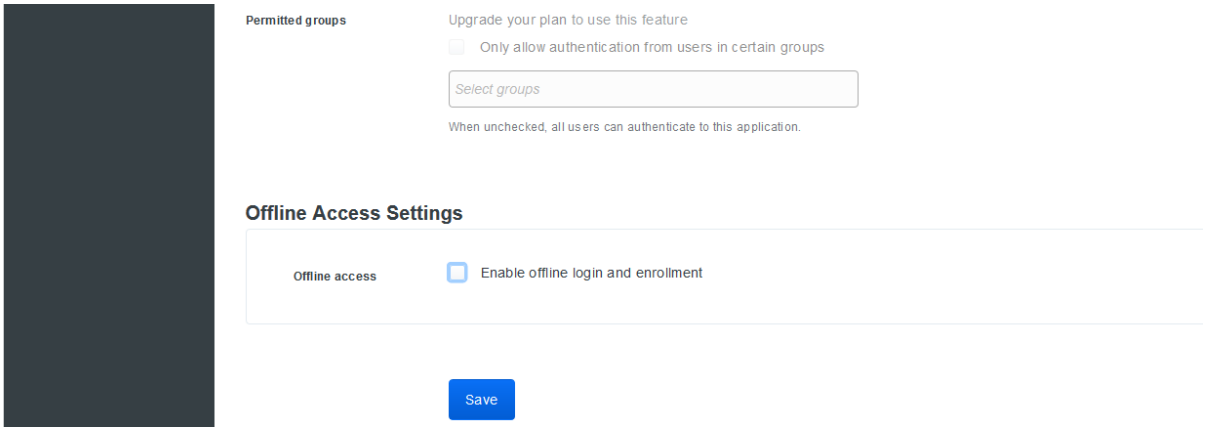
DUO-2FA

Beide Server sind mit einer Zweifaktor-Authentifizierung abgesichert. Bei einer Anmeldung via RDP oder bei einer lokalen Anmeldung muss eine Push-Bestätigung über mein Smartphone erfolgen. Als Anbieter nutze ich DUO.

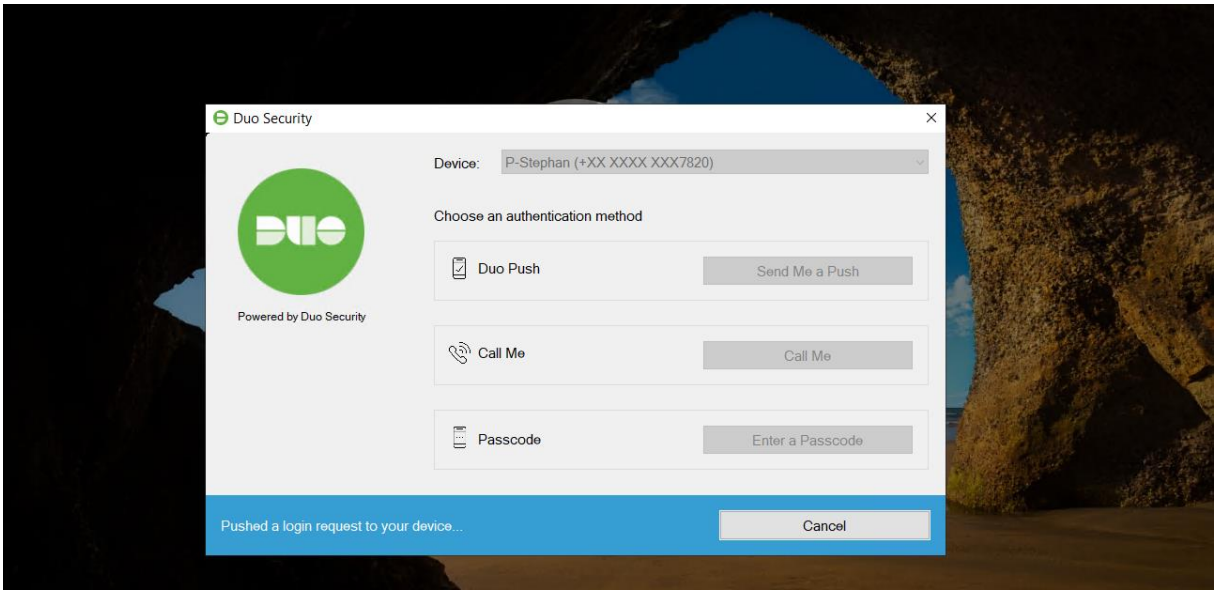
Im DUO-Adminportal sind meine geschützten Applikationen gelistet – natürlich mit den alten Namen. Diese sind aber nur Anzeigenamen, die sich leicht verändern lassen:



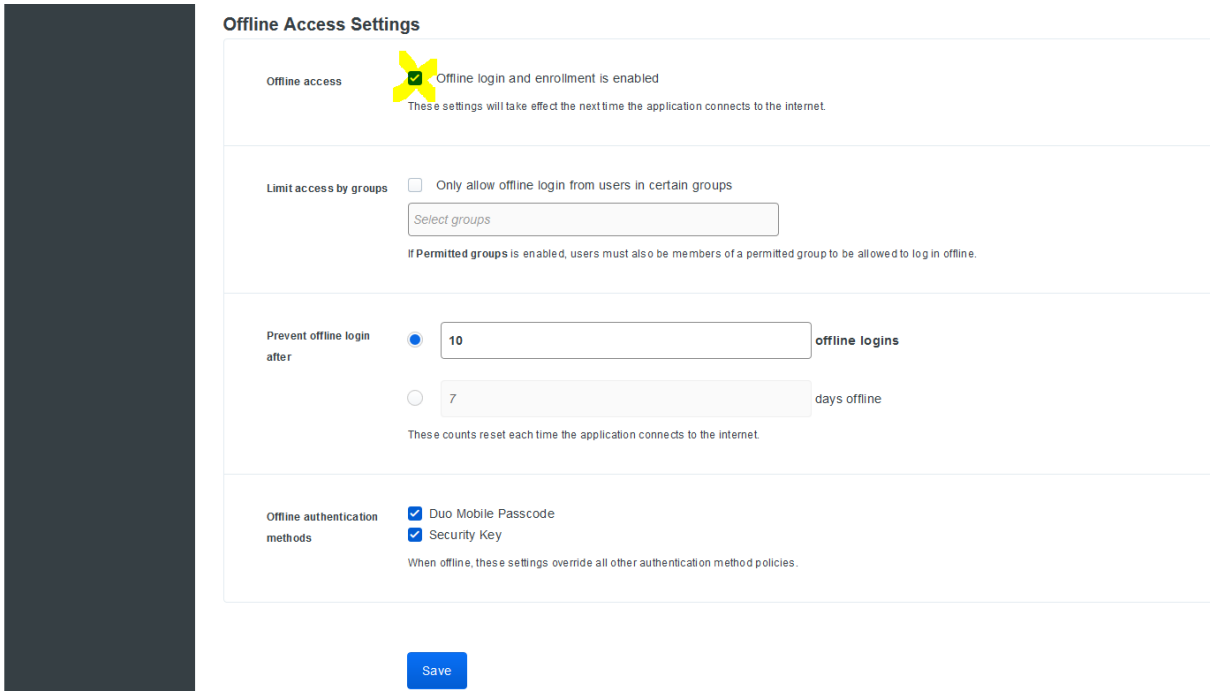
Die Namen werden in der Push-Benachrichtigung angezeigt. Ich habe aber auch für den Fall einer ausgefallenen Internetleitung in meinem Smartphone den Offline Access konfiguriert. In diesem Fall fragt der Server nach einem Token, den mein Smartphone generieren kann. Leider kann ich die Namen im Smartphone nicht nachträglich anpassen. Daher entferne ich die Konfiguration im Smartphone und nehme den Offline Access für beide Applications in DUO raus:



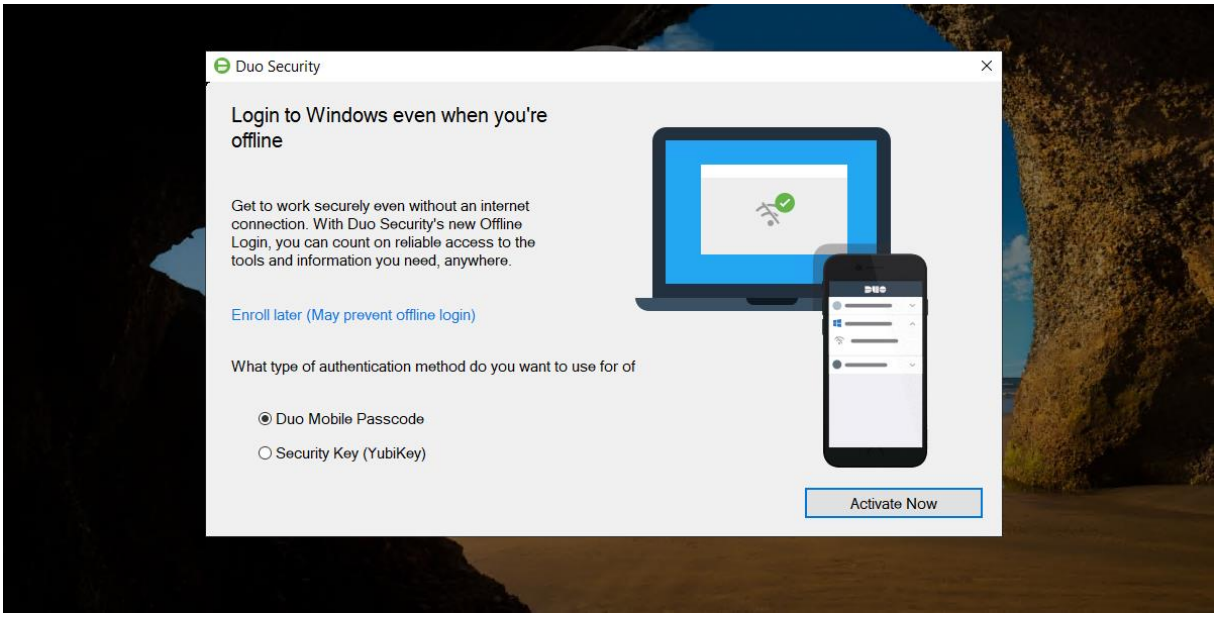
Danach ist eine neue Anmeldung an den Servern erforderlich. Dabei „lernt“ der Client, dass jetzt kein Offline Access mehr gewünscht ist:



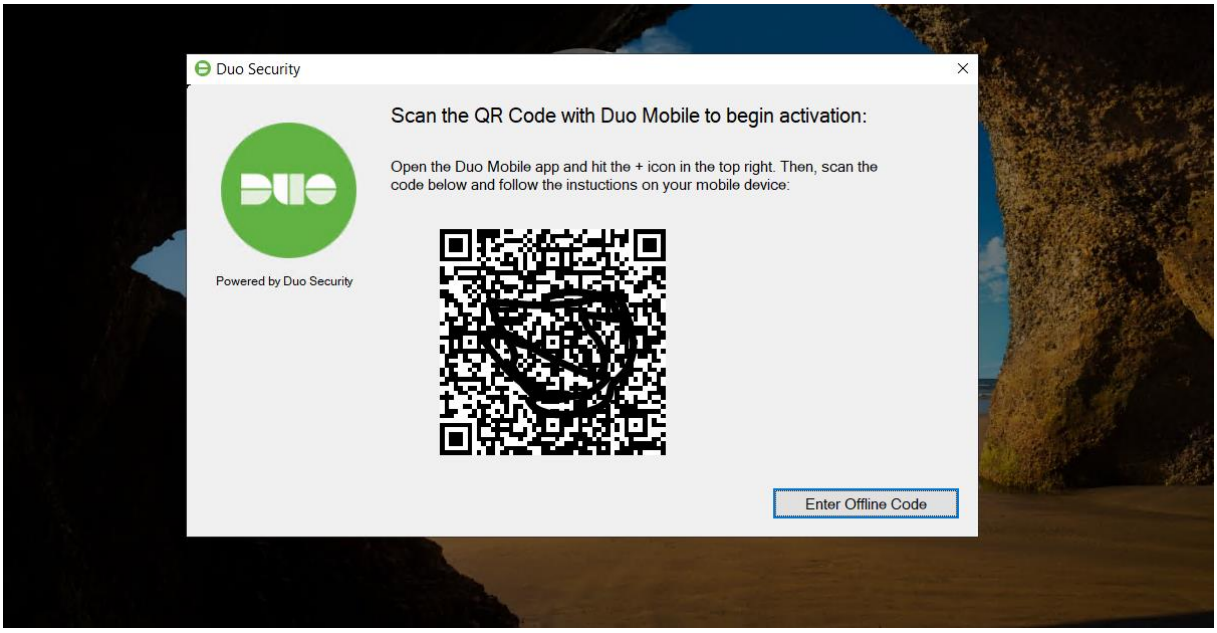
Nun aktiviere ich den Offline Access wieder im DUO-Adminportal:



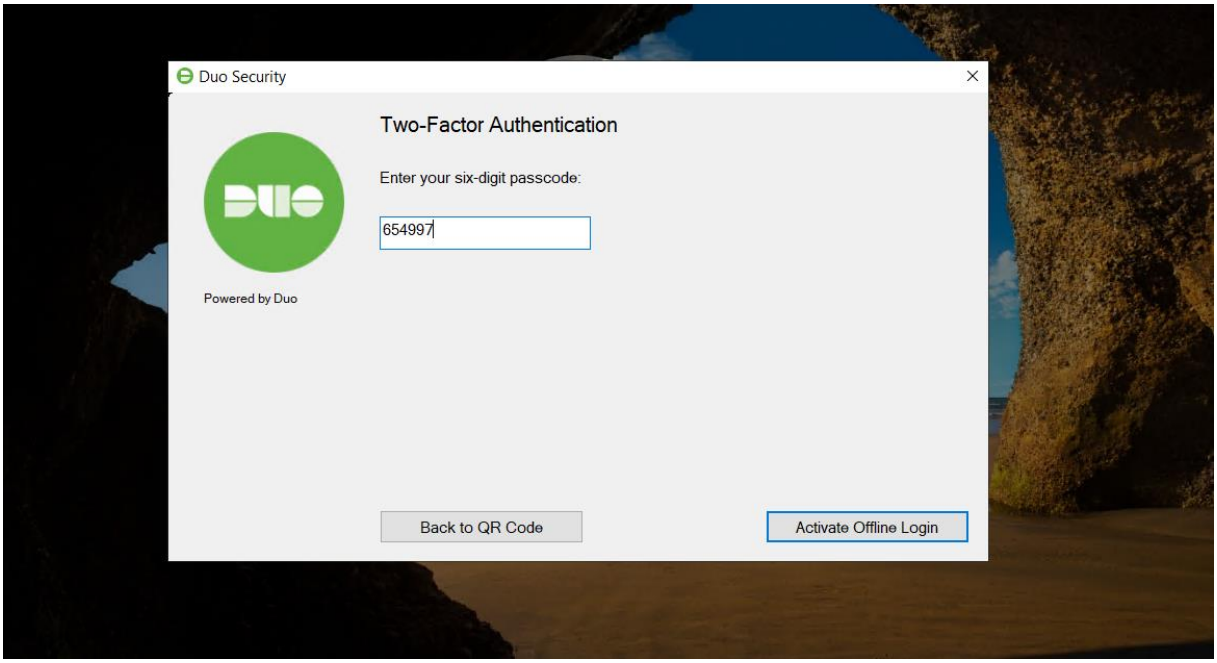
Dann melde mich erneut an den Servern an. Diese „lernen“ nun, dass ich auch offline zugreifen möchte – und starten die Konfiguration



Dazu muss ich in der DUO-App den QR-Code abscannen. Dabei kann ich der Anwendung in der App den neuen Servernamen vergeben. Die App im Smartphone lässt keine Screenshots zu. Daher sieht man hier nur die Bilder des Servers:



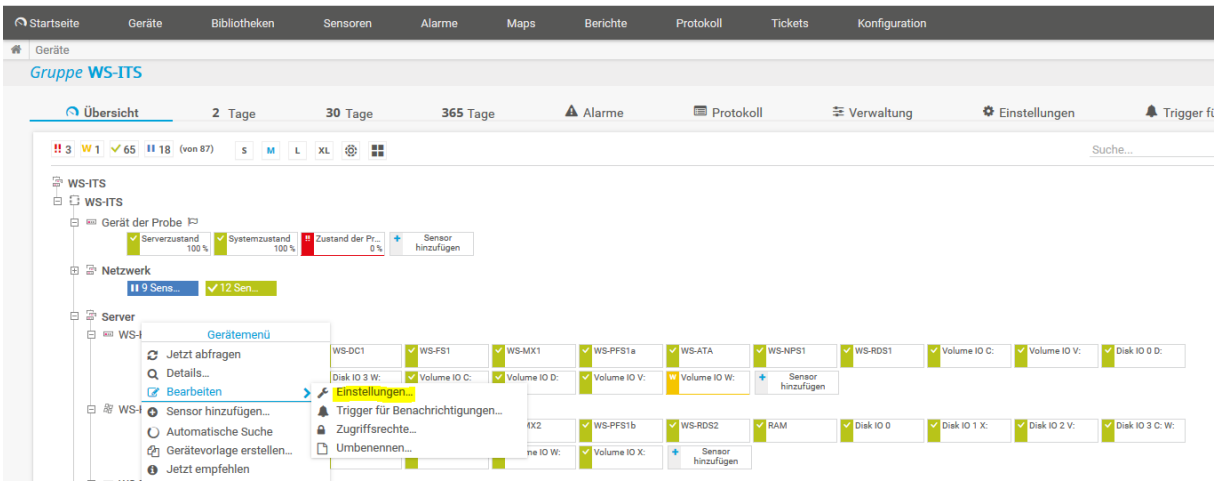
Die Rückbestätigung erfolgt mit einem passcode, den die App generiert. Diesen gebe ich in das Konfigurationsfenster ein:

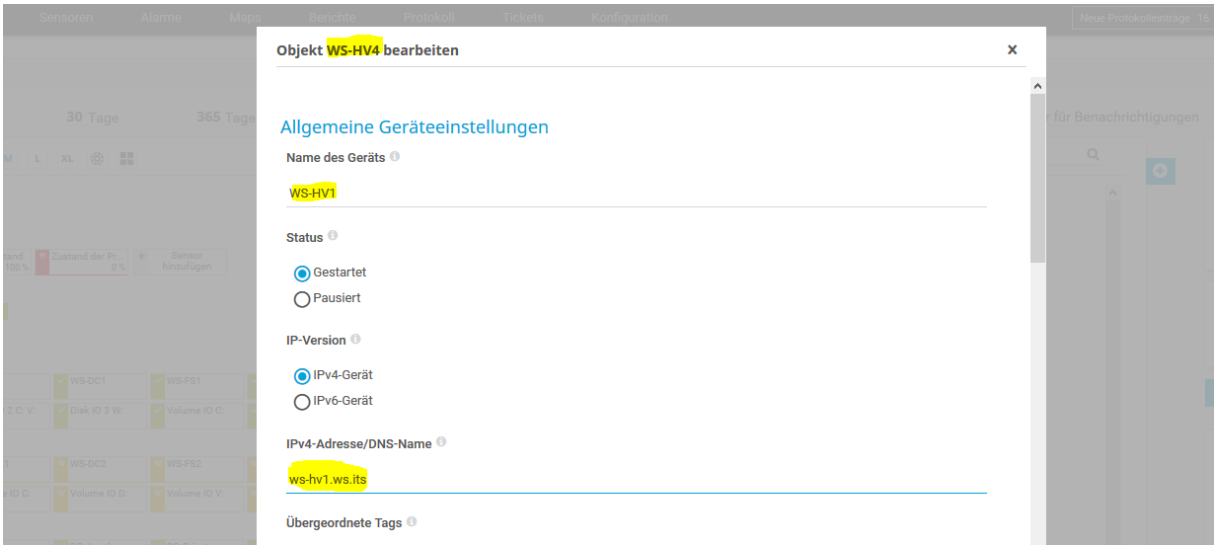


Der Aufwand war durchaus vertretbar.

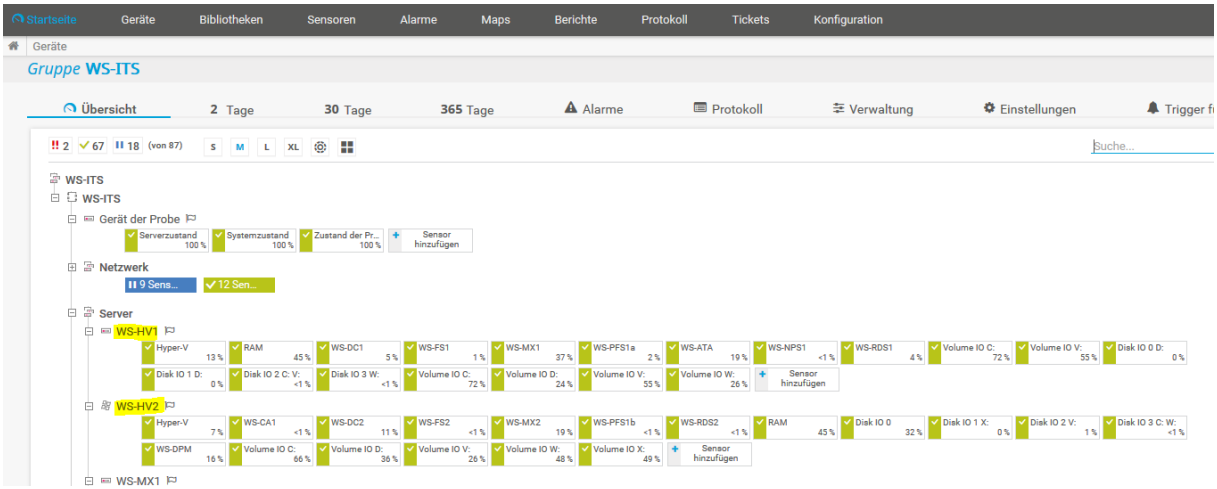
PRTG-Monitoring

Für mein Echtzeitmonitoring verwende ich PRTG. Dieses kann Agent-frei mit den hinterlegten Servern kommunizieren und so die erforderlichen Daten abfragen. Die Server habe ich mit deren FQDN hinterlegt. Diesen und den Anzeigenamen muss ich verändern. Beides erreiche ich über die Einstellungen des Zielservers:



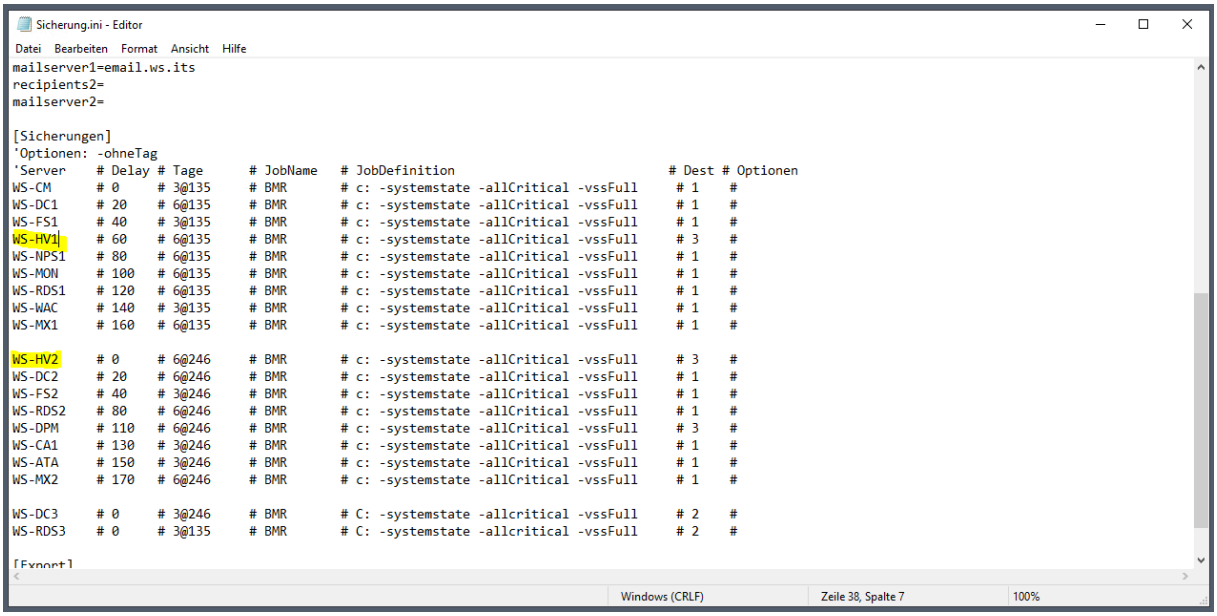


Da die Sensoren und die Serverkennung unverändert sind, läuft das Monitoring einfach weiter:

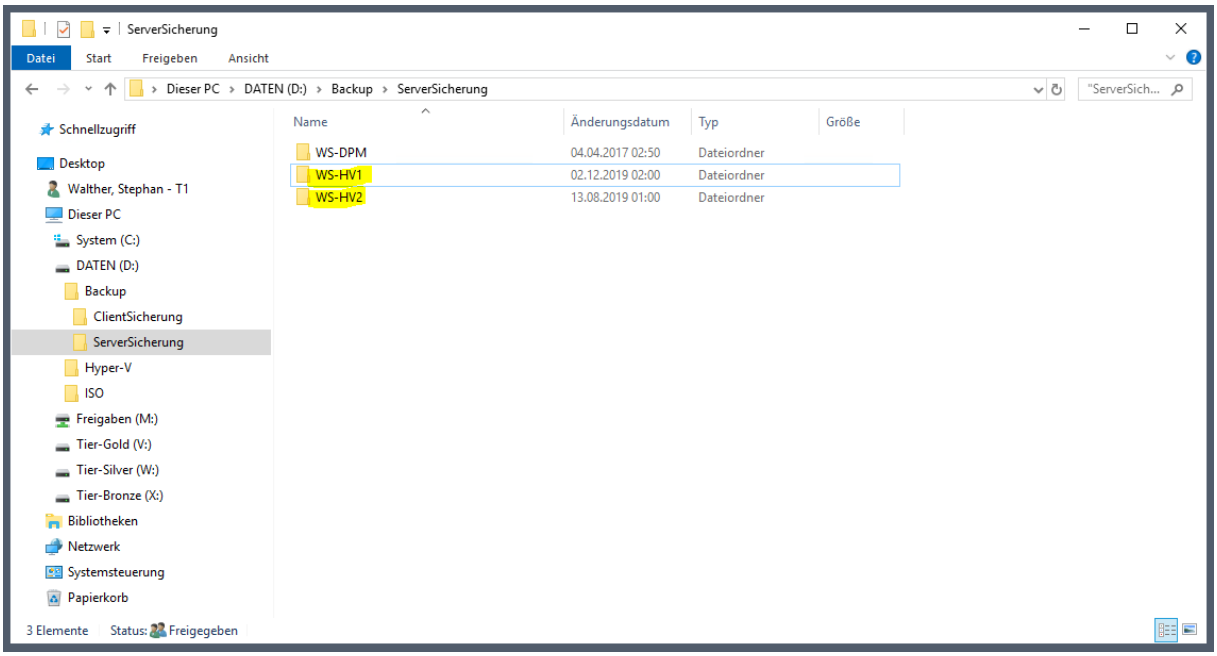


Datensicherung BMR

Meine Datensicherung besteht aus 2 Komponenten. Eine davon sichert die Betriebssysteme mit einem SystemStateImage. Dieses kann ich im Rahmen einer Bare Metal Recovery (BMR) wiederherstellen. Die Images erstelle ich mit der Windows Server Sicherung, welche von einem zentralen Script und dessen Konfiguration angetrieben wird. In der Konfigurationsdatei müssen die richtigen Servernamen vorhanden sein. Also ändere ich hier die Namen entsprechend ab:



Die Windows Server Sicherung sichert die Images in ein Verzeichnis mit dem Namen des Servers. Damit es hier einfach nahtlos weitergeht, passe ich die Namen der Verzeichnisse an:

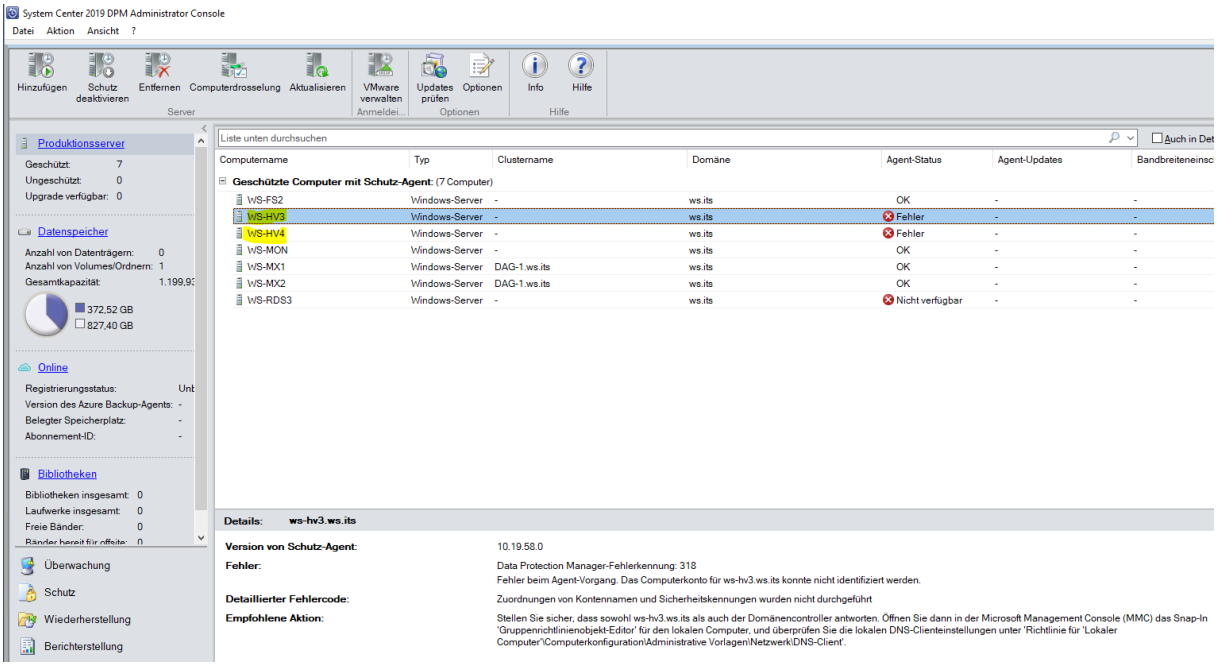


Meine Scriptlösung erstellt immer eine neue Vollsicherung. Daher sind keine weiteren Anpassungen erforderlich.

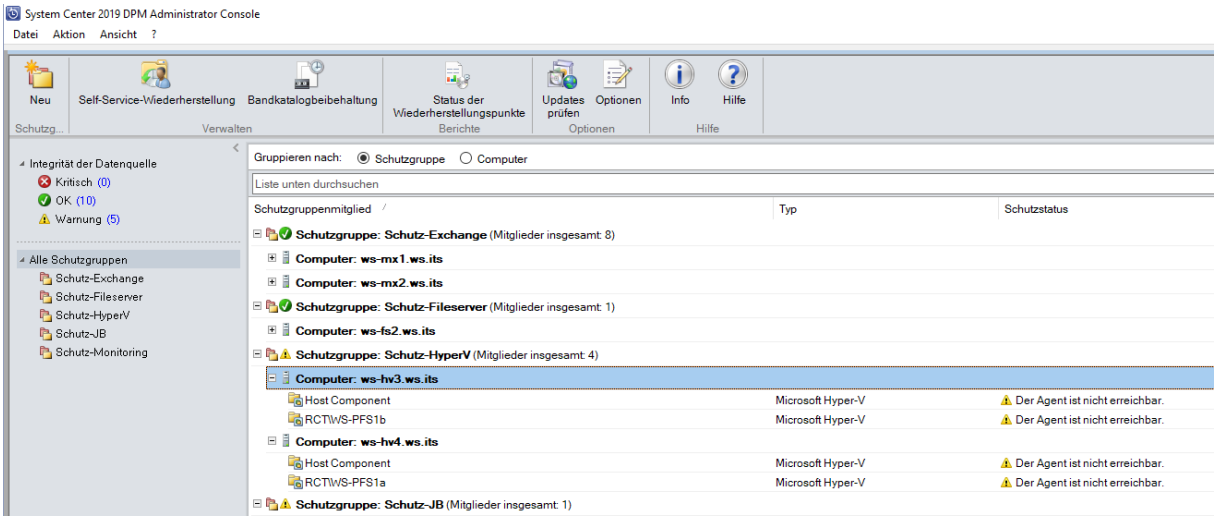
Datensicherung mit DPM

Meine zweite Komponente in der Datensicherung ist die Sicherung der Nutzdaten. Diese führe ich mit Microsoft System Center Data Protection Manager (DPM) 2019 aus. Der DPM-Server kommuniziert mit seinen Sicherungszielen über einen dort installierten und verbundenen Agent. Meine Hyper-V-Server haben beide diesen Agent installiert. Darüber sichere ich meine virtuellen Linux-Server.

Doch die Verbindung wird im DPM als fehlerhaft dargestellt:

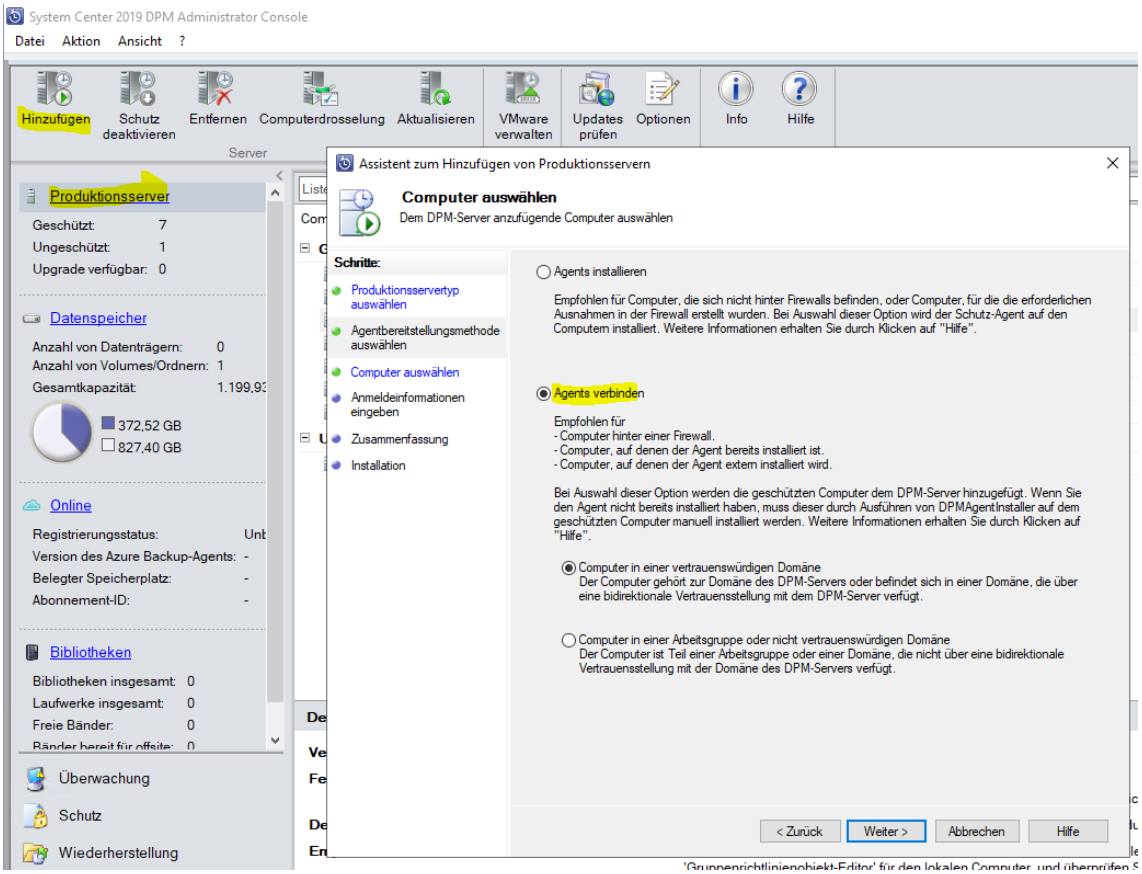


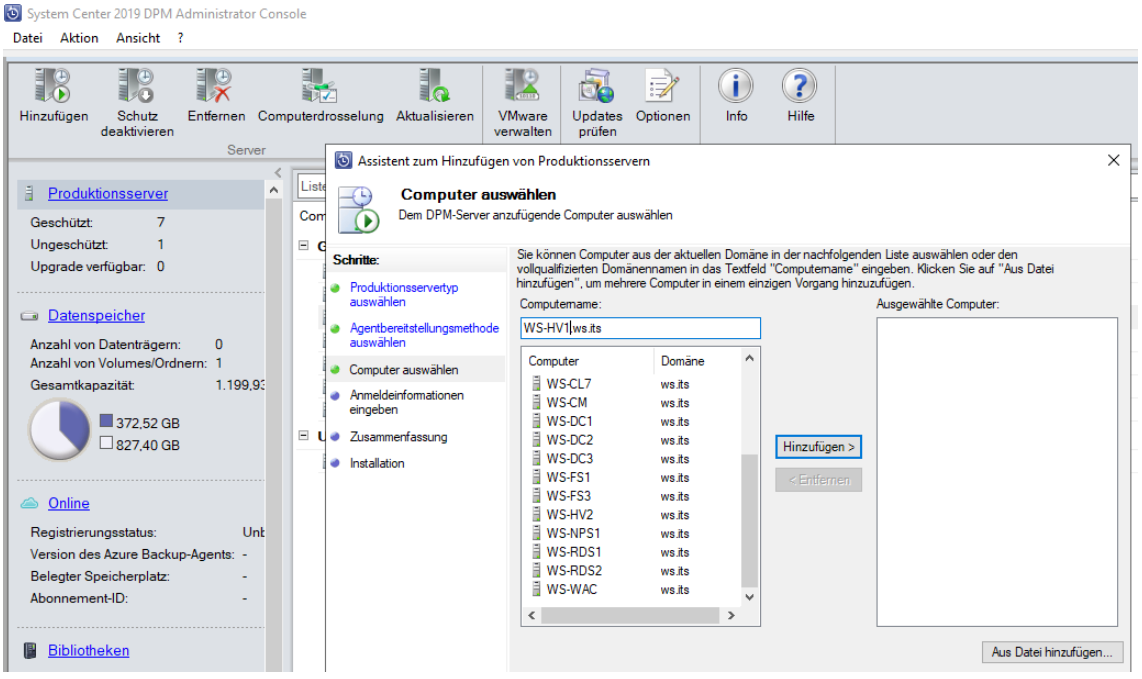
Und daher sind auch die hinterlegten Sicherungsaufgaben im entsprechenden Zustand:

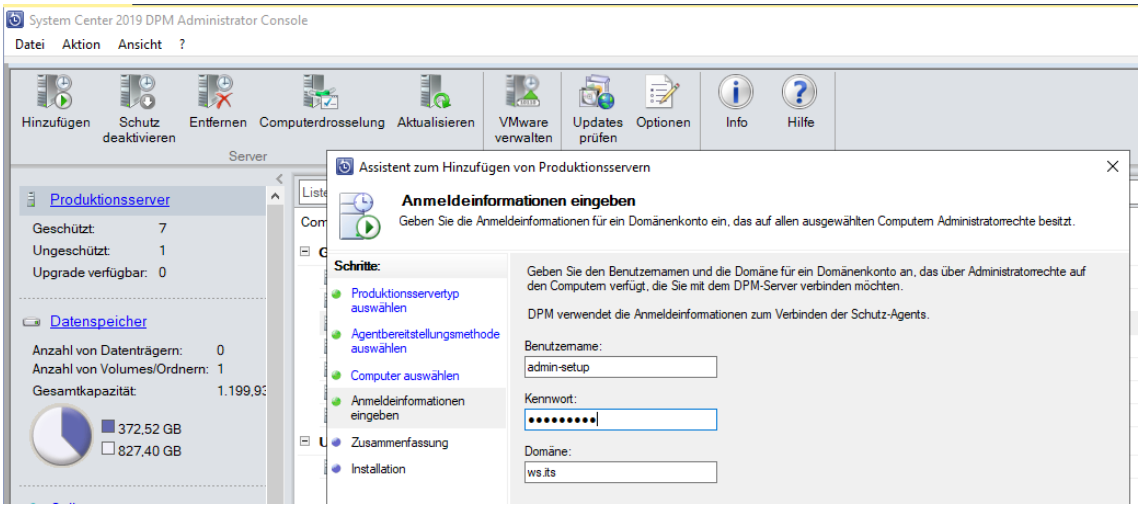


Leider gibt es in der GUI keine Option für „benenne eine Sicherungsquelle um“. Da der DPM aber auch mit der PowerShell konfiguriert werden kann, suche ich dort nach einem passenden cmdlet. Aber auch hier wurde diese Funktion nicht vorgesehen… Leider finde ich auch in der „Produktdokumentation“ des DPM keine Hinweise. Also muss ich selber eine Lösung suchen.

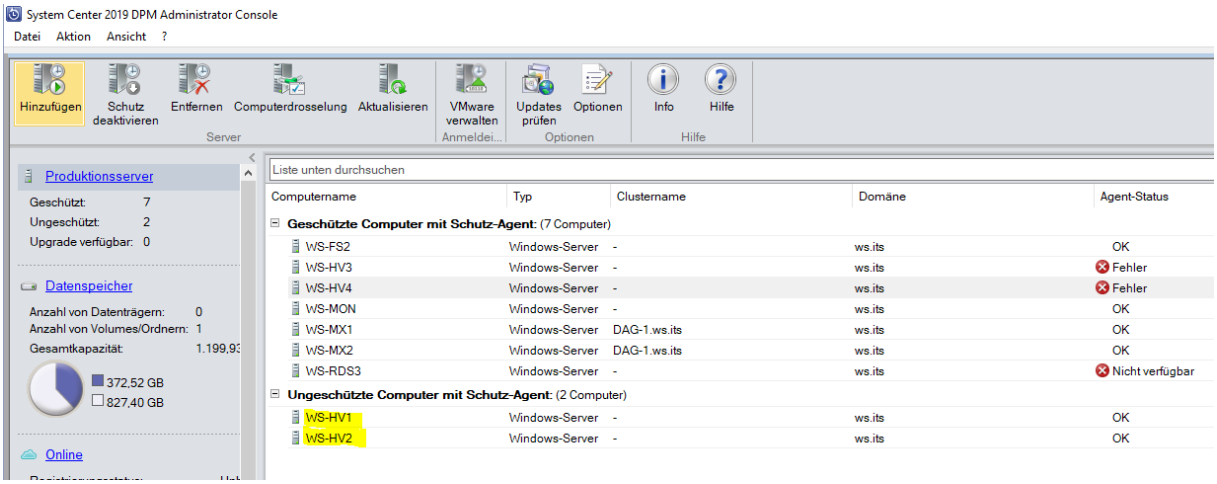
Vielleicht erkennt der DPM beim erneuten Verbinden der Agents, dass es die gleichen Server sind und korrigiert die Einstellungen? Ich starte die entsprechende Aktion in der DPM-Konsole:


System Center 2019 DPM Administrator Console
Datei Aktion Ansicht ?
Hinzufügen
Schutz deaktivieren
Entfernen
Computerdrosselung
Aktualisieren
VMware verwalten
Updates prüfen
Optionen
Info
Hilfe
Server
Produktionsserver
Geschützt: 7
Ungeschützt: 1
Upgrade verfügbar: 0
Datenspeicher
Anzahl von Datenträgern: 0
Anzahl von Volumes/Ordnern: 1
Gesamtkapazität: 1.199,93
372,52 GB
827,40 GB
Online
Registrierungsstatus:
Version des Azure Backup-Agents: -
Belegter Speicherplatz: -
Abonnement-ID: -
Bibliotheken
Bibliotheken insgesamt: 0
Laufwerke insgesamt: 0
Freie Bänder: 0
Überwachung
Schutz
Wiederherstellung
Assistent zum Hinzufügen von Produktionsservern
Computer auswählen
Dem DPM-Server anzufügende Computer auswählen
Schritte:
Produktionsservertyp auswählen
Agentbereitstellungsmethode auswählen
Computer auswählen
Anmeldeinformationen eingeben
Zusammenfassung
Installation
Agents installieren
Empfohlen für Computer, die sich nicht hinter Firewalls befinden, oder Computer, für die die erforderlichen Ausnahmen in der Firewall erstellt wurden. Bei Auswahl dieser Option wird der Schutz-Agent auf den Computern installiert. Weitere Informationen erhalten Sie durch Klicken auf "Hilfe".
Agents verbinden
Empfohlen für
- Computer hinter einer Firewall.
- Computer, auf denen der Agent bereits installiert ist.
- Computer, auf denen der Agent extern installiert wird.
Bei Auswahl dieser Option werden die geschützten Computer dem DPM-Server hinzugefügt. Wenn Sie den Agent nicht bereits installiert haben, muss dieser durch Ausführen von DPMAgentInstaller auf dem geschützten Computer manuell installiert werden. Weitere Informationen erhalten Sie durch Klicken auf "Hilfe".
Computer in einer vertrauenswürdigen Domäne
Der Computer gehört zur Domäne des DPM-Servers oder befindet sich in einer Domäne, die über eine bidirektionale Vertrauensstellung mit dem DPM-Server verfügt.
Computer in einer Arbeitsgruppe oder nicht vertrauenswürdigen Domäne
Der Computer ist Teil einer Arbeitsgruppe oder einer Domäne, die nicht über eine bidirektionale Vertrauensstellung mit der Domäne des DPM-Servers verfügt.
< Zurück
Weiter >
Abbrechen
Hilfe


System Center 2019 DPM Administrator Console
Datei Aktion Ansicht ?
Hinzufügen
Schutz deaktivieren
Entfernen
Computerdrosselung
Aktualisieren
VMware verwalten
Updates prüfen
Optionen
Info
Hilfe
Server
Produktionsserver
Geschützt: 7
Ungeschützt: 1
Upgrade verfügbar: 0
Datenspeicher
Anzahl von Datenträgern: 0
Anzahl von Volumes/Ordnern: 1
Gesamtkapazität: 1.199,93
372,52 GB
827,40 GB
Online
Registrierungsstatus:
Version des Azure Backup-Agents: -
Belegter Speicherplatz: -
Abonnement-ID: -
Bibliotheken
Assistent zum Hinzufügen von Produktionsservern
Computer auswählen
Dem DPM-Server anzufügende Computer auswählen
Schritte:
Produktionsservertyp auswählen
Agentbereitstellungsmethode auswählen
Computer auswählen
Anmeldeinformationen eingeben
Zusammenfassung
Installation
Sie können Computer aus der aktuellen Domäne in der nachfolgenden Liste auswählen oder den vollqualifizierten Domänennamen in das Textfeld "Computername" eingeben. Klicken Sie auf "Aus Datei hinzufügen", um mehrere Computer in einem einzigen Vorgang hinzuzufügen.
Computername:
WS-HV1|ws.its
Computer
Domäne
WS-CL7 ws.its
WS-CM ws.its
WS-DC1 ws.its
WS-DC2 ws.its
WS-DC3 ws.its
WS-FS1 ws.its
WS-FS3 ws.its
WS-HV2 ws.its
WS-NPS1 ws.its
WS-RDS1 ws.its
WS-RDS2 ws.its
WS-WAC ws.its
Hinzufügen >
< Entfernen
Ausgewählte Computer:
Aus Datei hinzufügen...



Doch die beiden Server werden nun jeweils doppelt angezeigt: einmal mit dem alten Namen (und leider mit den dazugehörigen Sicherungsjobs) und einmal als „nicht geschützte“ Server mit den neuen Namen:

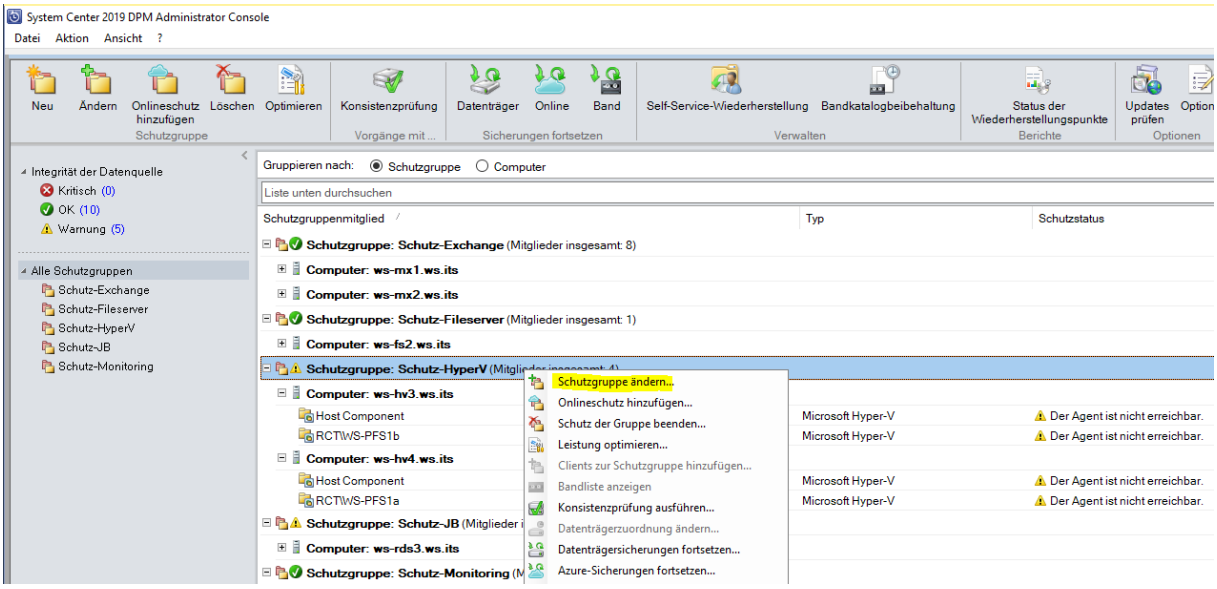


Ggf. gäbe es noch die Option, in der SQL-Datenbank die Anpassung vorzunehmen. Aber dazu fehlt mir der Überblick über die Abhängigkeiten und die Struktur der Daten. Das ist keine Option für ein systemkritisches Backup.

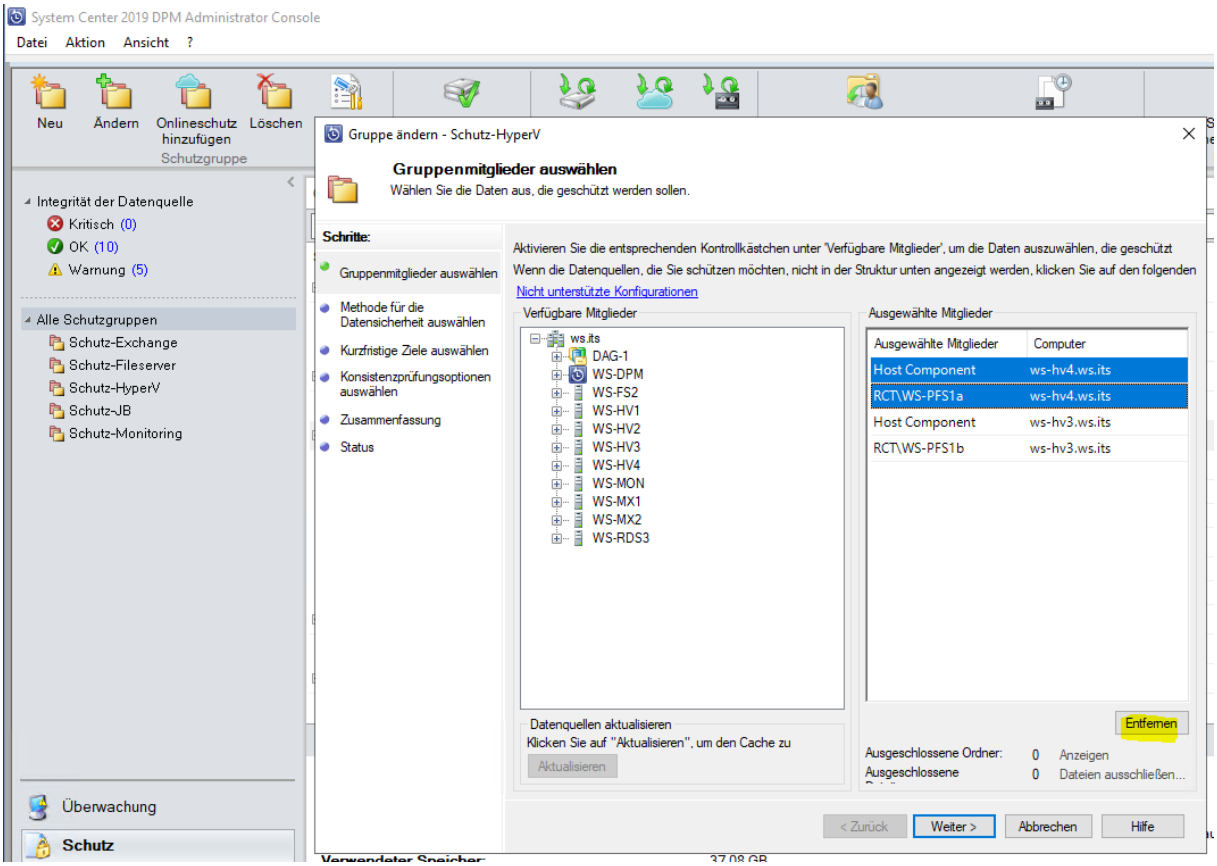
Also bleibt mir wohl nichts anderes über, als die bereits vorhandenen Sicherungen aufzugeben und neu zu implementieren. In meinem Fall ist der Verlust nicht dramatisch, da es nur die beiden VMs mit meiner Linux-Firewall betrifft. An den virtuellen Servern habe ich in letzter Zeit keine relevanten Veränderungen vorgenommen, die ich mit einer SystemState—Recovery wiederherstellen müsste. Aber bei anderen Servern oder unter anderen Umständen wäre der Verlust der Historie der Datensicherung durchaus ein Problem.

Ich versuche nicht, die neue Sicherung parallel zur alten (nicht mehr funktionalen) Sicherung aufzubauen. Der DPM würde durch die ID der VMs die Dopplung erkennen. Und im Worst Case kann ich dann vielleicht weder die alte noch die neue Sicherung wiederherstellen. Das ist mir zu heiß.

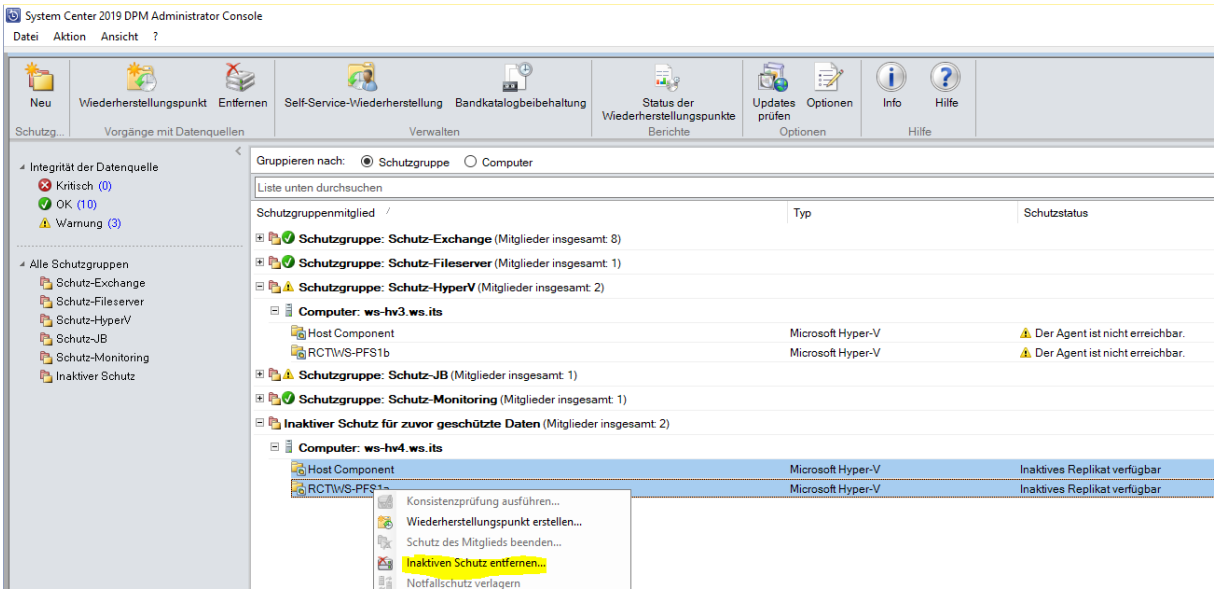
Ich ändere also die Schutzgruppe und entferne dort die „alten“ Sicherungsdefinitionen:



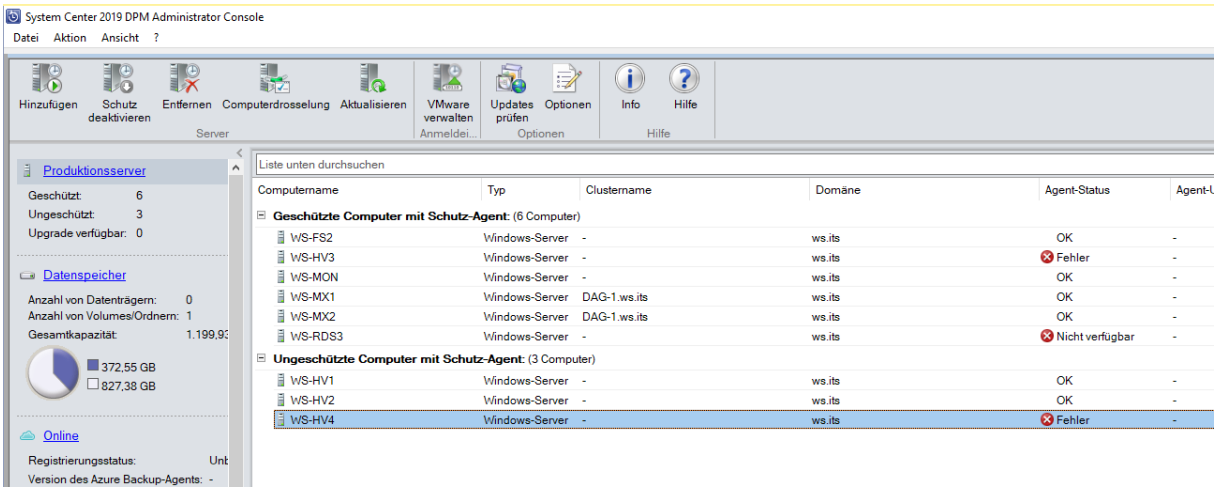
Bei der Auswahl der Gruppenmitglieder entferne ich testweise die Teile des alten WS-HV4:



Da die Schutzgruppe noch über Sicherungsquellen verfügt, bleibt sie weiter bestehen. Die beiden Teile werden als inaktiver Schutz weitergeführt. Diesen kann bzw. muss ich entfernen, damit ich die Sicherung neu aufbauen kann:



Nun wird der alte Servername in der Agent-Übersicht frei. In der GUI kann man den Eintrag aber nicht bereinigen:

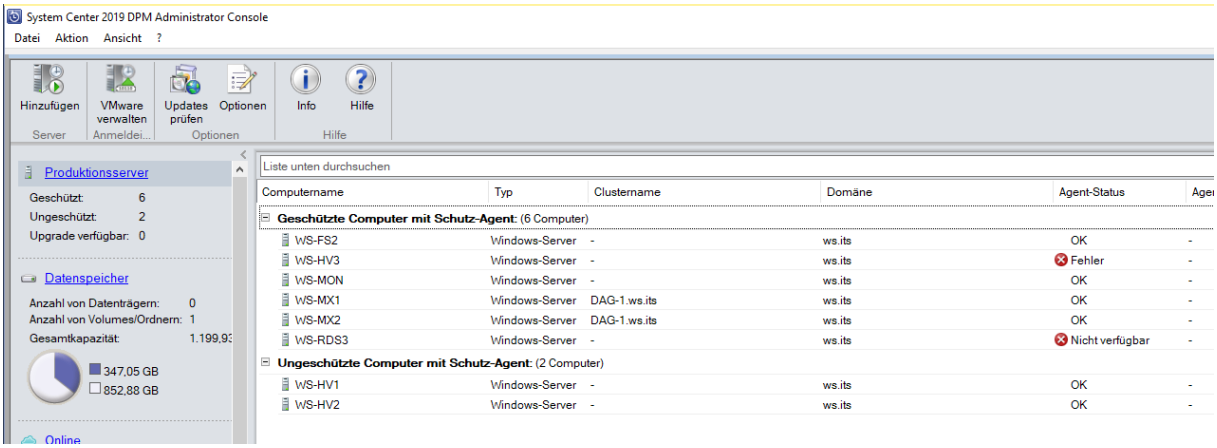


Das geht nur mit der PowerShell – wenn auch nicht ohne Warnungen. Diese haben das „nicht existierende“ Konto des Servers als Ursache. Klar, denn er heißt ja jetzt anders…

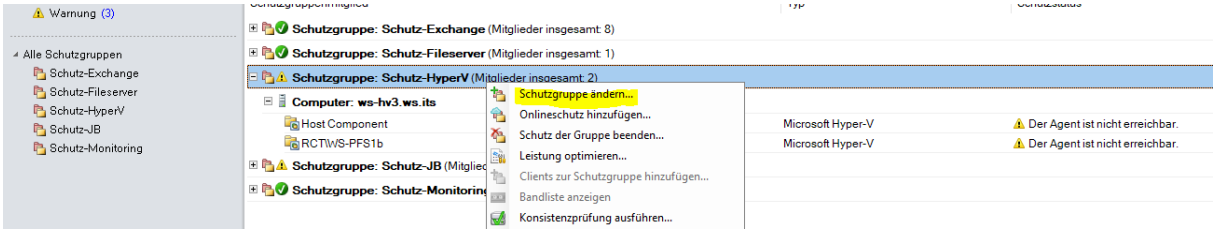
```
$curdir = Get-Location
cd "C:\Program Files\Microsoft System Center 2019\DPM\DPM\bin\"
.\dpmcliinitscript.ps1
cd $curdir
cls

Remove-ProductionServer.ps1 -DPMServerName ws-dpm.ws.its -PSName WS-HV4.ws.its
```

```
PS C:\> Remove-ProductionServer.ps1 -DPMServerName ws-dpm.ws.its -PSName WS-HV4.ws.its
There is failure while removing production server
C:\Program Files\Microsoft System Center\DPM\DPM\bin\Remove-ProductionServer.ps1 : Der geschützte Computer WS-HV4 konnte nicht aus einer der folgenden Gruppen entfernt werden.
1. Verteilte COM-Benutzer
2. DPMRADmTrustedMachines
3. MSDPMTrustedMachines
In Zeile:1 Zeichen:1
+ Remove-ProductionServer.ps1 -DPMServerName ws-dpm.ws.its -PSName WS-H ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,Remove-ProductionServer.ps1

Entfernen Sie WS-HV4 aus den oben aufgeführten Gruppen.

PS C:\> Remove-ProductionServer.ps1 -DPMServerName ws-dpm.ws.its -PSName WS-HV4.ws.its
WARNUNG: Die Verbindung mit DPM-Server "ws-dpm.ws.its" wird hergestellt.
There is failure while removing production server
C:\Program Files\Microsoft System Center\DPM\DPM\bin\Remove-ProductionServer.ps1 : Der geschützte Computer ws-hv4.ws.its konnte nicht entfernt werden.
In Zeile:1 Zeichen:1
+ Remove-ProductionServer.ps1 -DPMServerName ws-dpm.ws.its -PSName WS-H ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,Remove-ProductionServer.ps1

Stellen Sie sicher, dass der geschützte Computer mit dem DPM-Server verbunden ist. Wenn sich der geschützte Computer in der Active Directory-Domäne befindet, stellen Sie sicher, dass Sie den rich
tigen FQDN des geschützten Computers angegeben haben. Wenn ws-hv4.ws.its ein für NetBIOS konfigurierter Arbeitsgruppencomputer ist, geben Sie den NetBIOS-Namen an. Geben Sie andernfalls den DNS-N
amen des Arbeitsgruppencomputers an.

PS C:\>
```

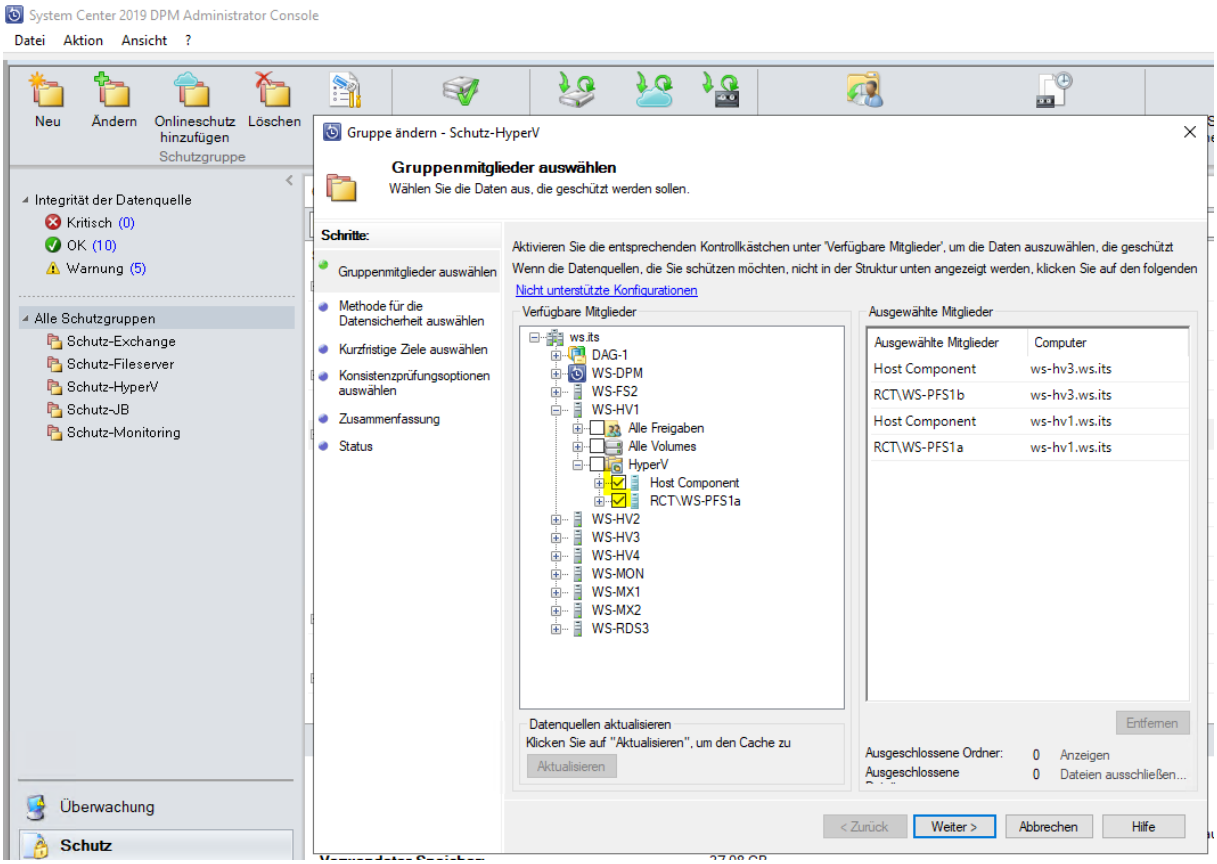
Aber der Eintrag ist verschwunden:



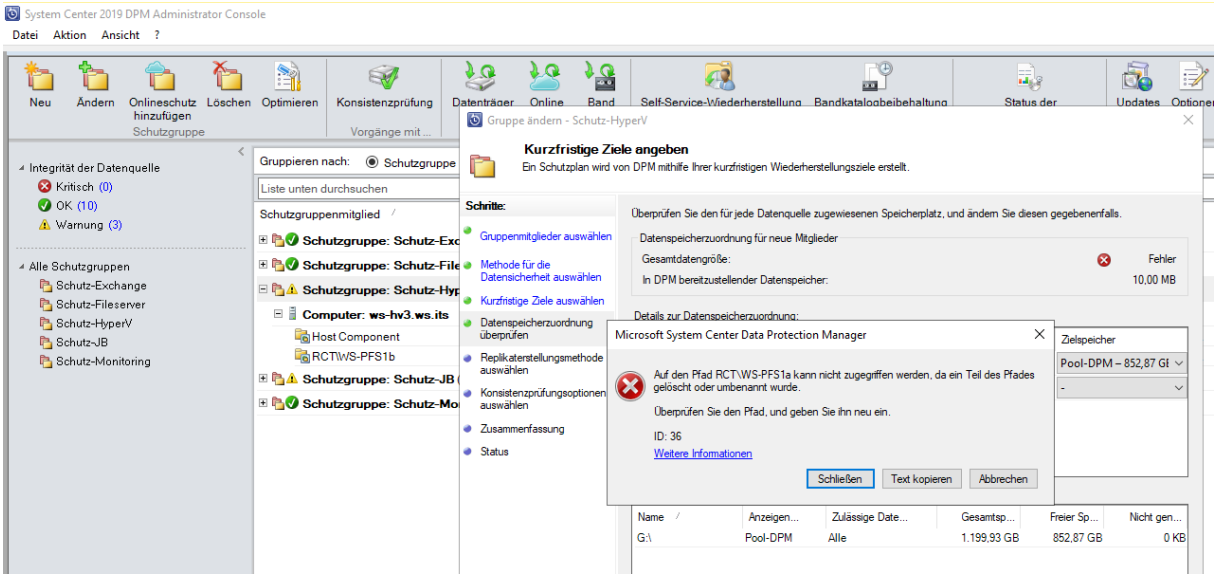
Nun kann ich die Schutzgruppe um den gelöschten Eintrag erweitern und meine VM wieder in die Sicherung aufnehmen:



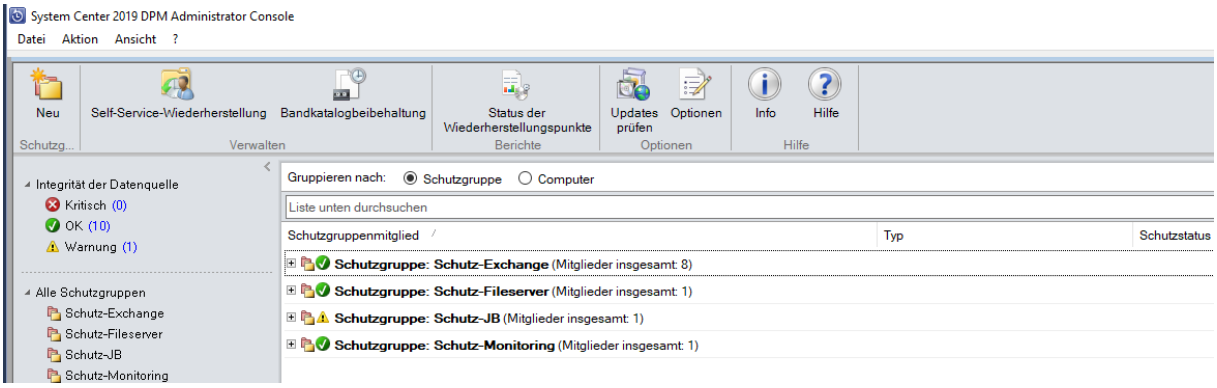
Interessanterweise zeigt die Konsole nur die eine VM an. Auf dem Hyper-V-Host laufen aber viel mehr VMs. Und der Aktualisieren-Schalter funktioniert nicht (er ist einfach ausgegraut). Aber egal, denn ich möchte ja nur genau diese VM sichern:



Aber im nächsten Schritt zeigt sich, dass der DPM mit der Manipulation nicht klarkommt:



Ich entferne nun die komplette Schutzgruppe für meine VMs. Vielleicht liegt es ja daran:

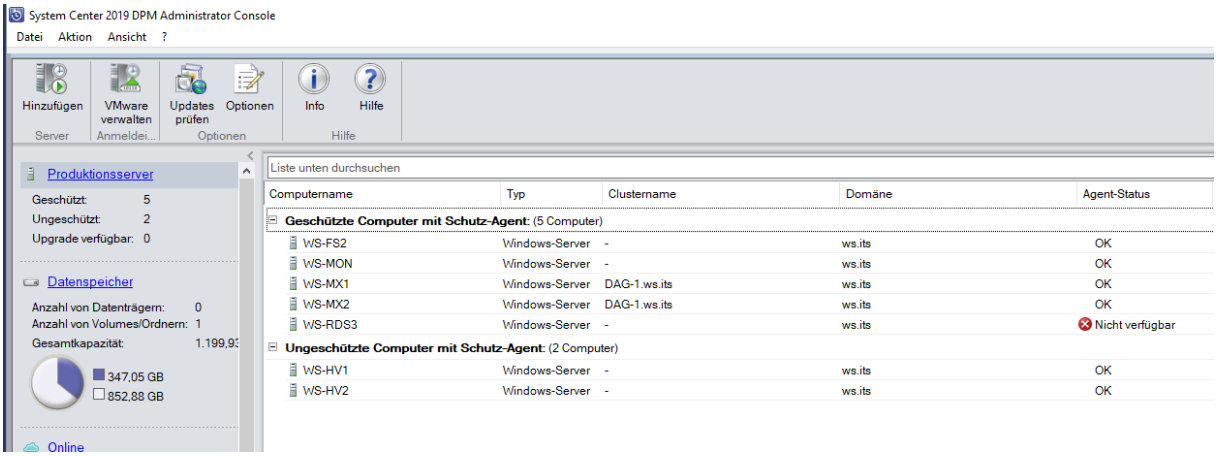


Zudem entferne ich den zweiten verwaisten Agent-Eintrag:

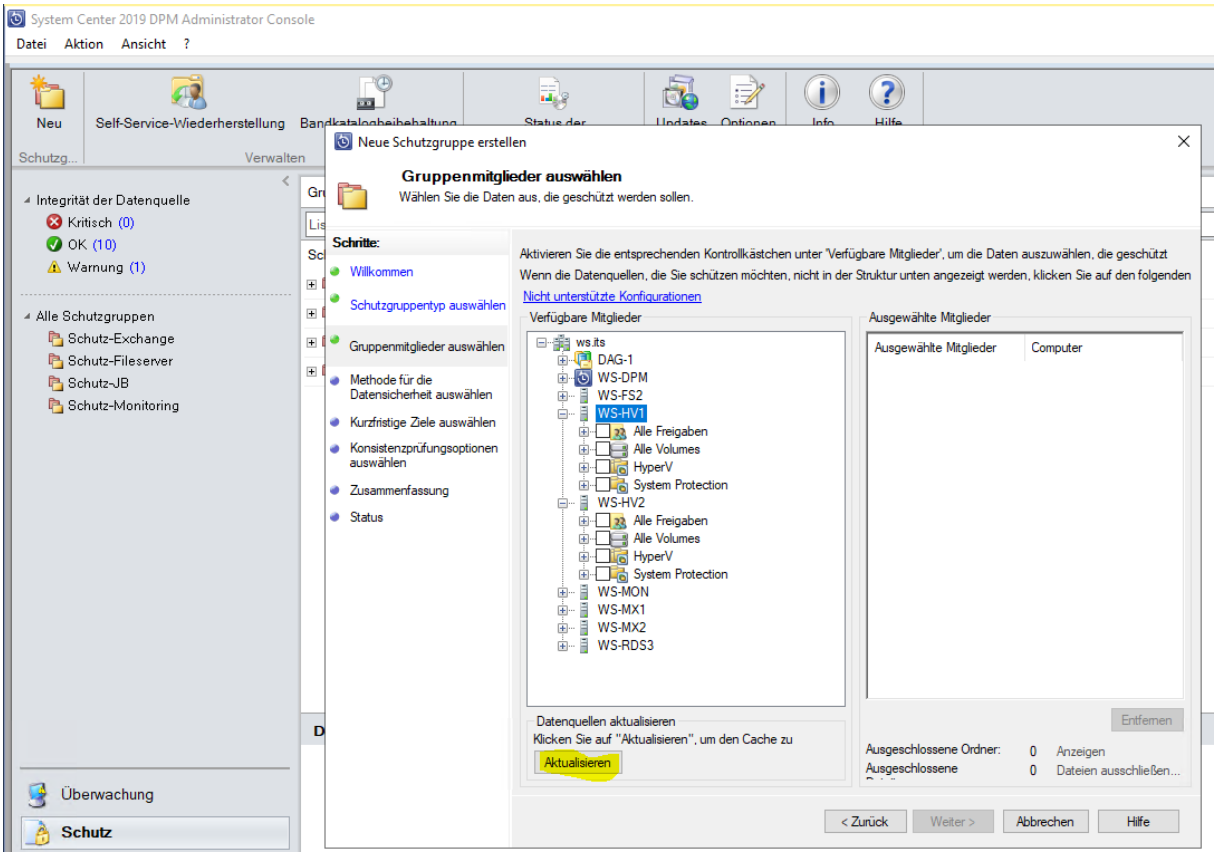
```
$curdir = Get-Location
cd "C:\Program Files\Microsoft System Center 2019\DPM\DPM\bin\"
.\dpmcliinitscript.ps1
cd $curdir
cls

Remove-ProductionServer.ps1 -DPMServerName ws-dpm.ws.its -PSName WS-HV3.ws.its

```

```
PS C:\> Remove-ProductionServer.ps1 -DPMServerName ws-dpm.ws.its -PSName WS-HV3.ws.its
WARNUNG: Die Verbindung mit DPM-Server "ws-dpm.ws.its" wird hergestellt.
There is failure while removing production server
C:\Program Files\Microsoft System Center\DPM\DPM\bin\Remove-ProductionServer.ps1 : Der geschützte Computer WS-HV3 konnte nicht aus einer der folgenden Gruppen entfernt werden.
1. Verteilte COM-Benutzer
2. DPMRADmTrustedMachines
3. MSDPMTrustedMachines
In Zeile:1 Zeichen:1
+ Remove-ProductionServer.ps1 -DPMServerName ws-dpm.ws.its -PSName WS-H ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,Remove-ProductionServer.ps1

Entfernen Sie WS-HV3 aus den oben aufgeführten Gruppen.

PS C:\>
```

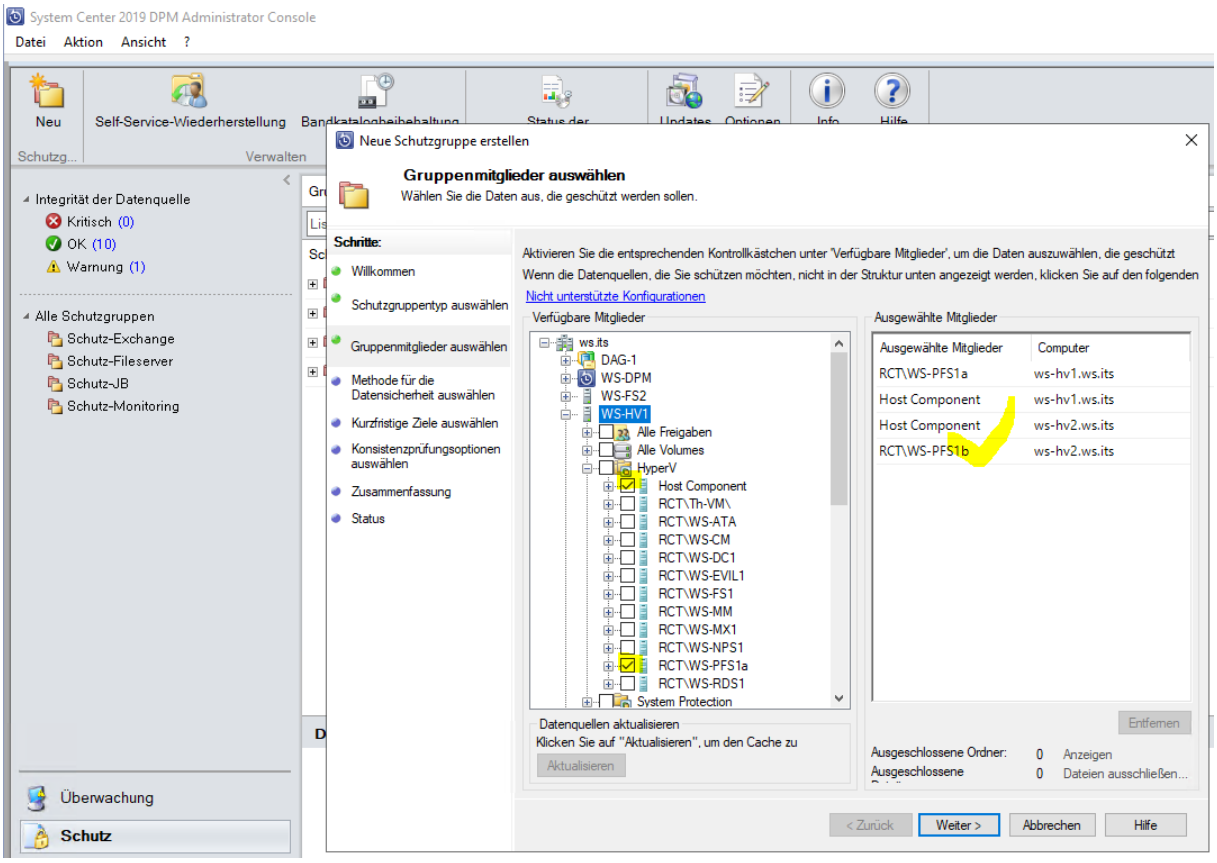
So erhalte ich ein sauberes System – ohne Hyper-V-Sicherung:



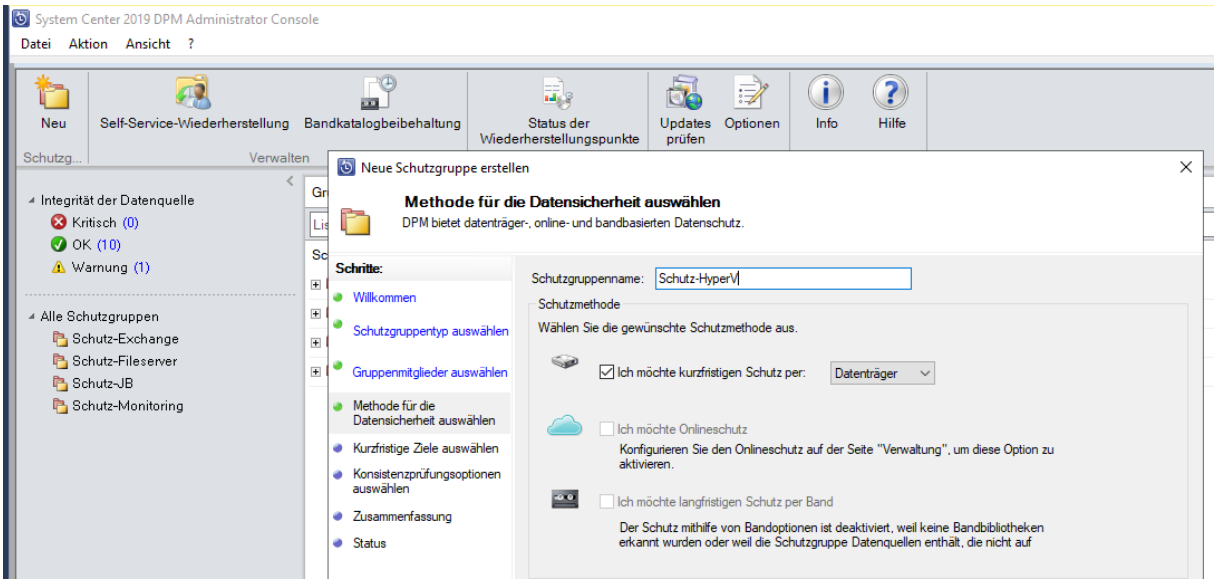
Danach erstelle ich die Schutzgruppe komplett neu. Jetzt ist auch der „Aktualisieren“-Schalter aktiv. Ich lasse den DPM also noch nach neuen VMs suchen:



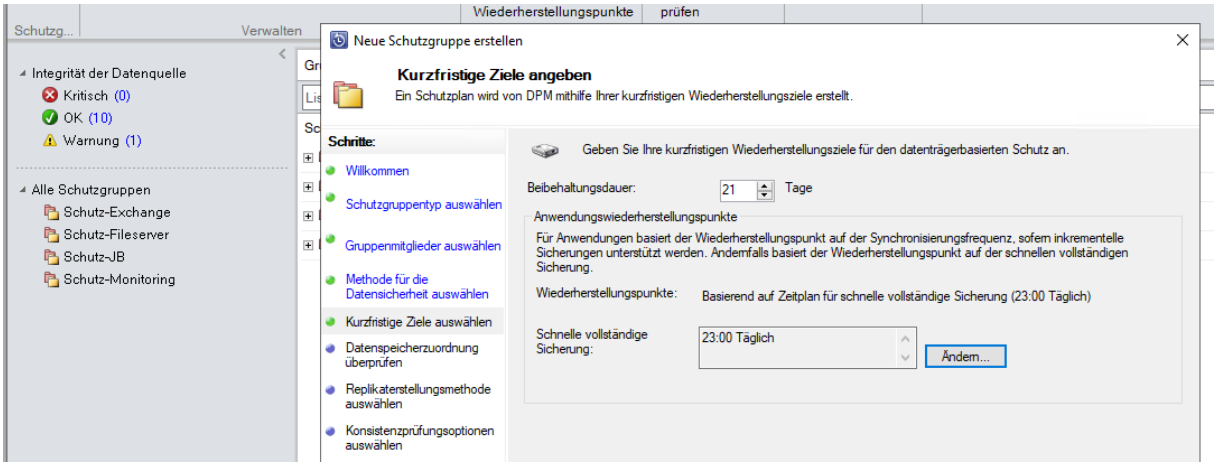
Und jetzt passt die Anzeige zum IST-Stand. Ich wähle die gewünschten Linux-VMs aus:



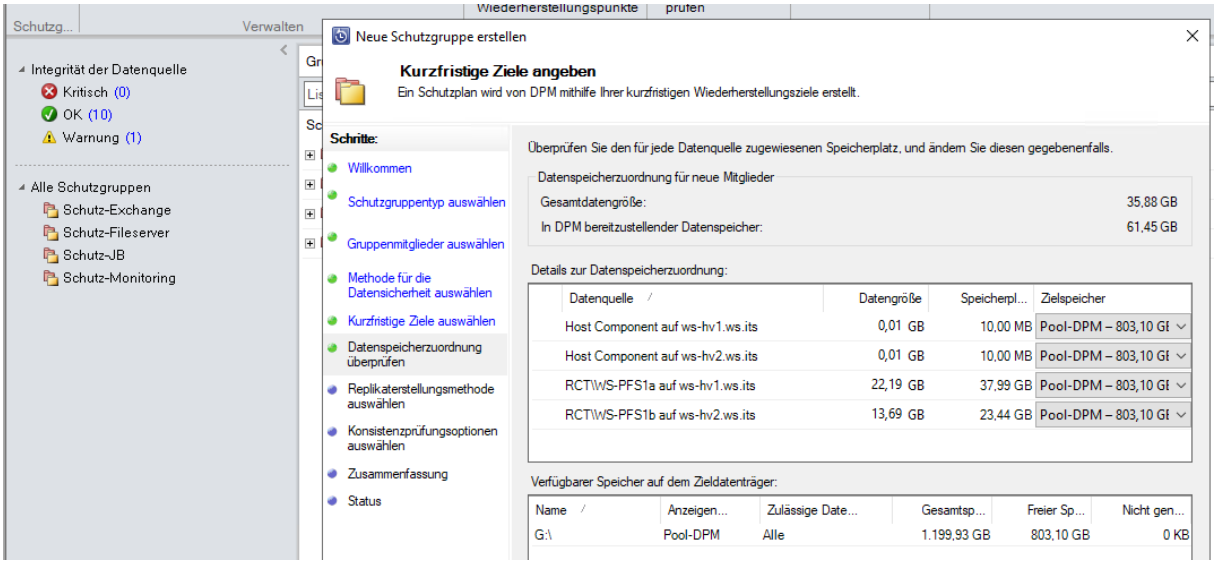
Die weiteren Optionen betreffen die Einstellungen der Datensicherung. Zum einen gehört ein sprechender Anzeigename dazu:



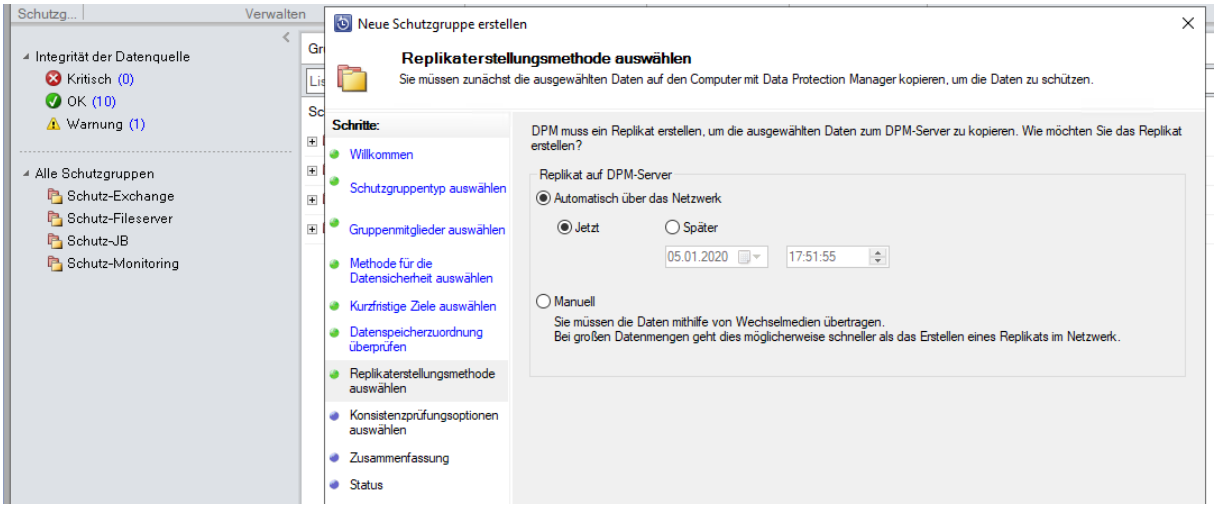
Aber auch die Aufbewahrungsdauer der Sicherungen und der Sicherungszeitpunkt sind wichtig:

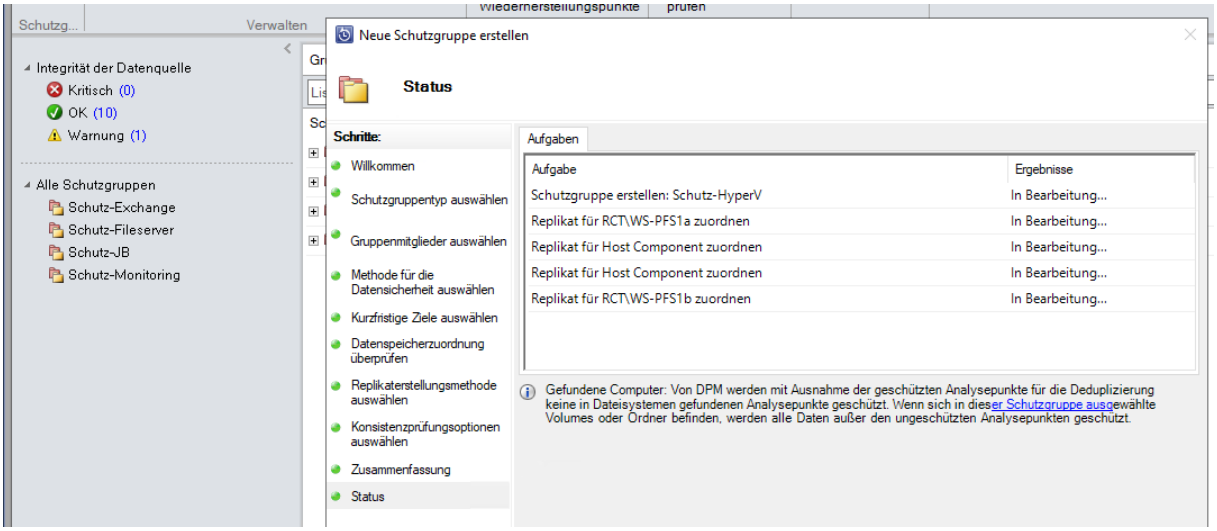


Das Sicherungsziel ist ein VHDX-Pool:

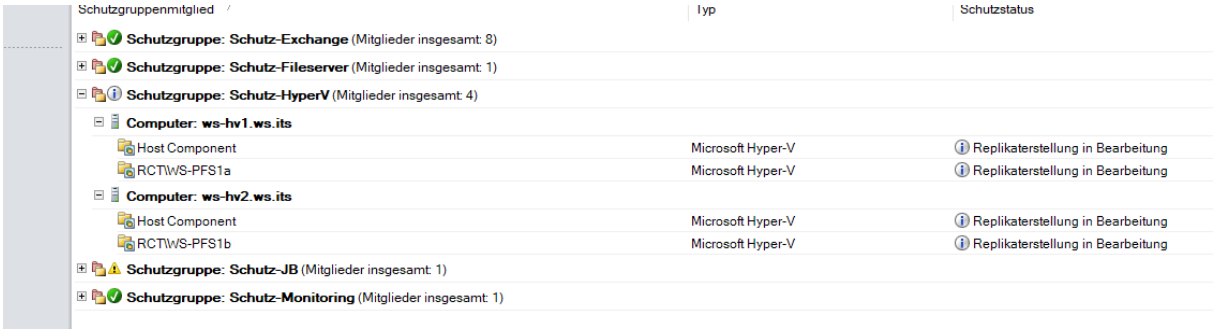


Die VMs sind nicht sehr groß. Und zudem habe ich keine Sicherung mehr im Bestand. Daher starte ich die Datensicherung sofort:

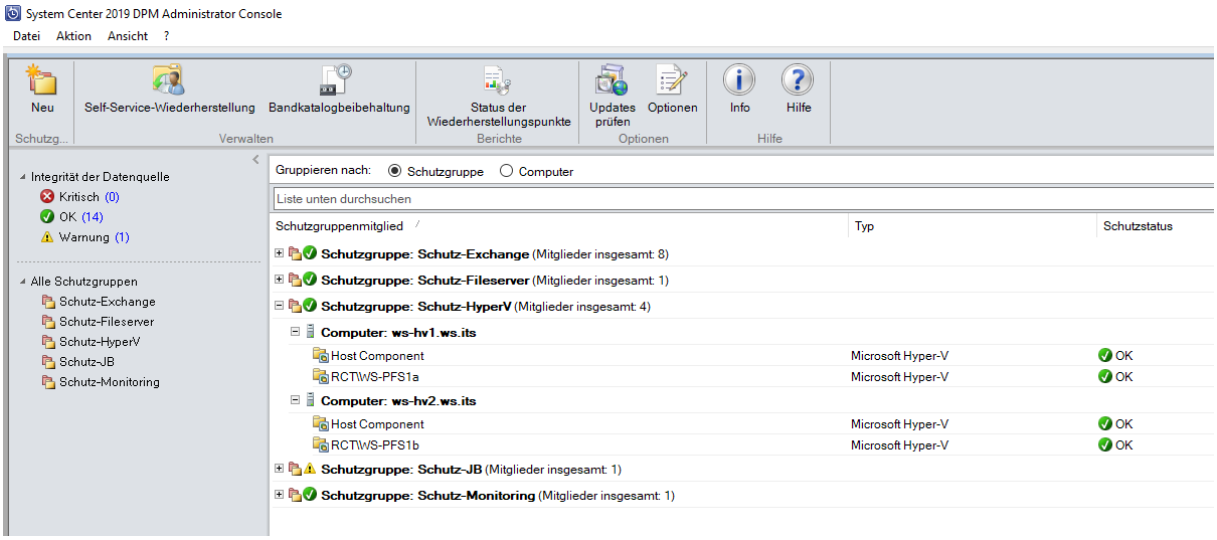




Nach Abschluss des Assistenten werden die VMs wie gewünscht gesichert:



Und nach wenigen Minuten ist die Sicherung abgeschlossen:

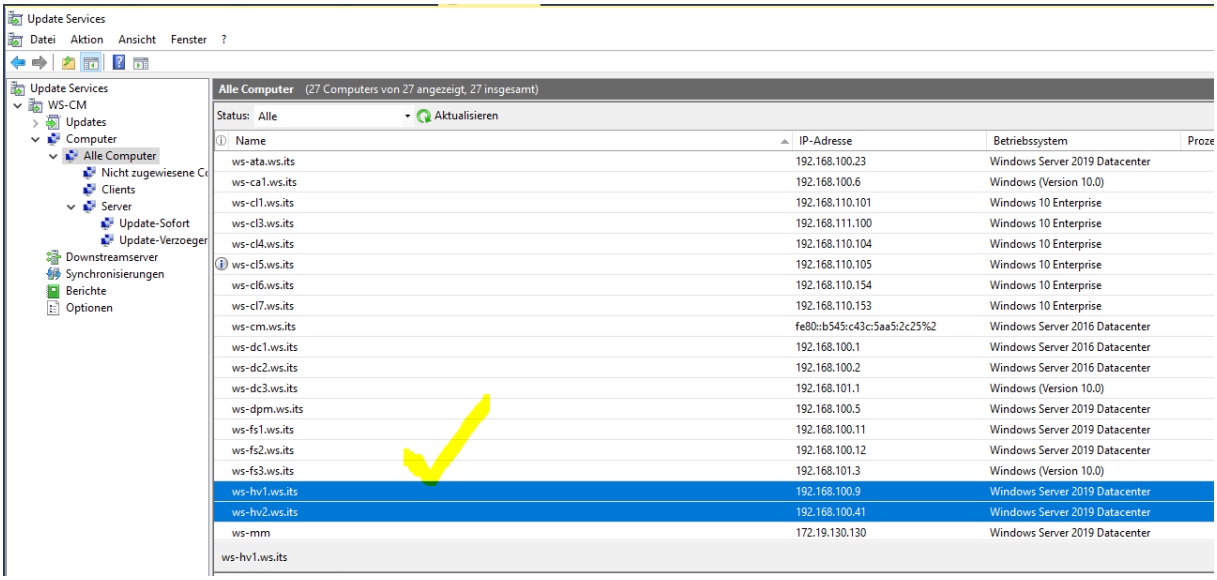


Würde ich alle VMs auf diese Weise sichern, dann wäre der Impact durch das „einfache“ Umbenennen enorm! Und das betrifft wahrscheinlich auch andere Sicherungsprogramme!

Microsoft hat das wohl selber nicht vorgesehen…

WSUS

Im WSUS tragen die Server ihre Meta-Informationen selber ein. Die Zuordnung gelingt über eindeutige SUS-IDs, die beim ersten Kontakt mit dem WSUS generiert werden. Durch das Umbenennen der Server wurde die ID nicht verändert. So wird im WSUS der alte Name einfach durch den neuen ersetzt:

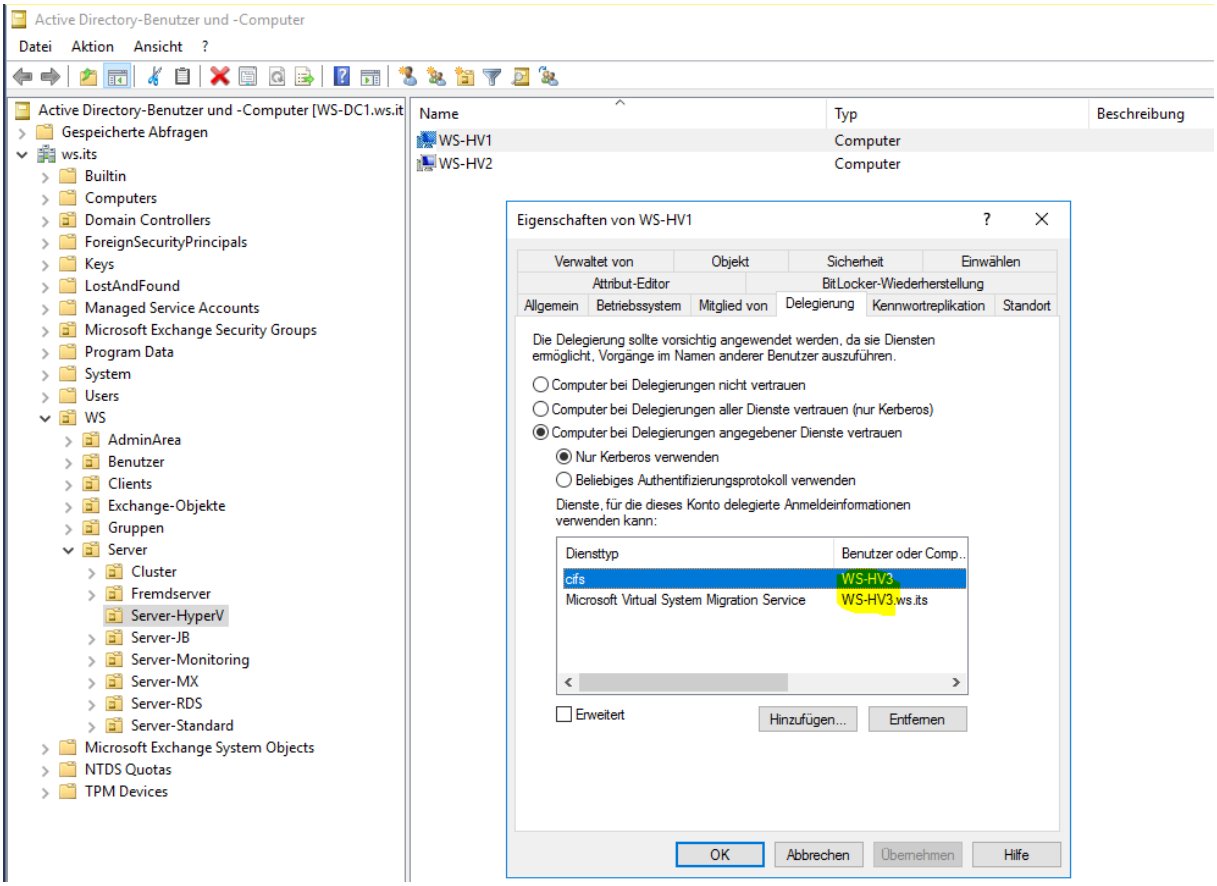


Dies funktioniert aber nur, wenn der neue Name noch nicht verwendet wurde. Aber die Bereinigung führte ich ja bereits zu Beginn durch.

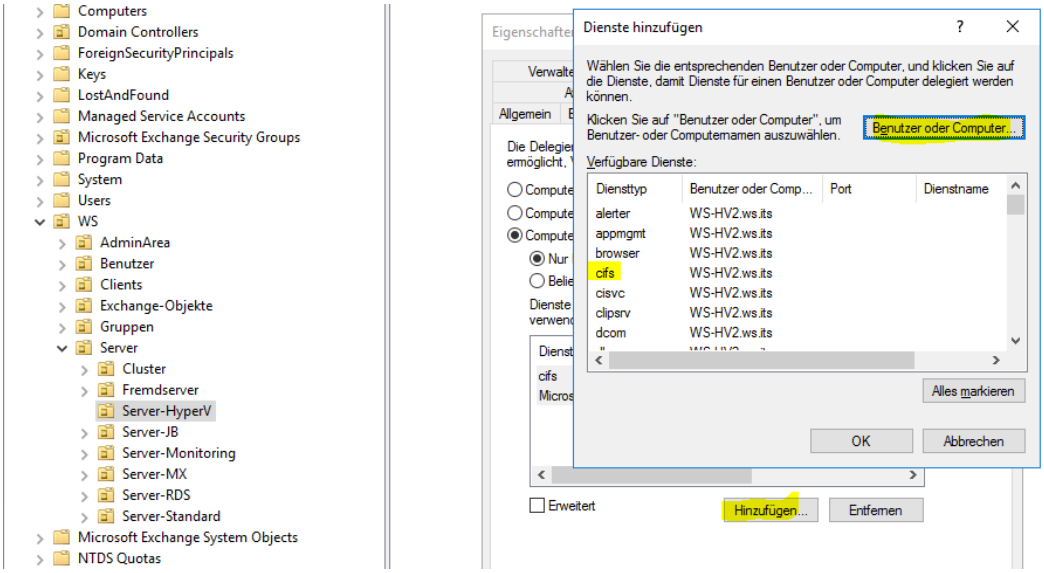
Active Directory

Im Active Directory gibt es doch nichts mehr zu korrigieren… oder? In meinem Fall schon, denn ich habe im Hyper-V die VM-LiveMigration-Konfiguration mit Kerberos abgesichert. Dafür muss in den Computerkonten der Hyper-V-Hosts die Constrained Delegation eingerichtet werden. Das hatte ich bidirektional zwischen Server WS-HV3 und WS-HV4 vorgenommen.

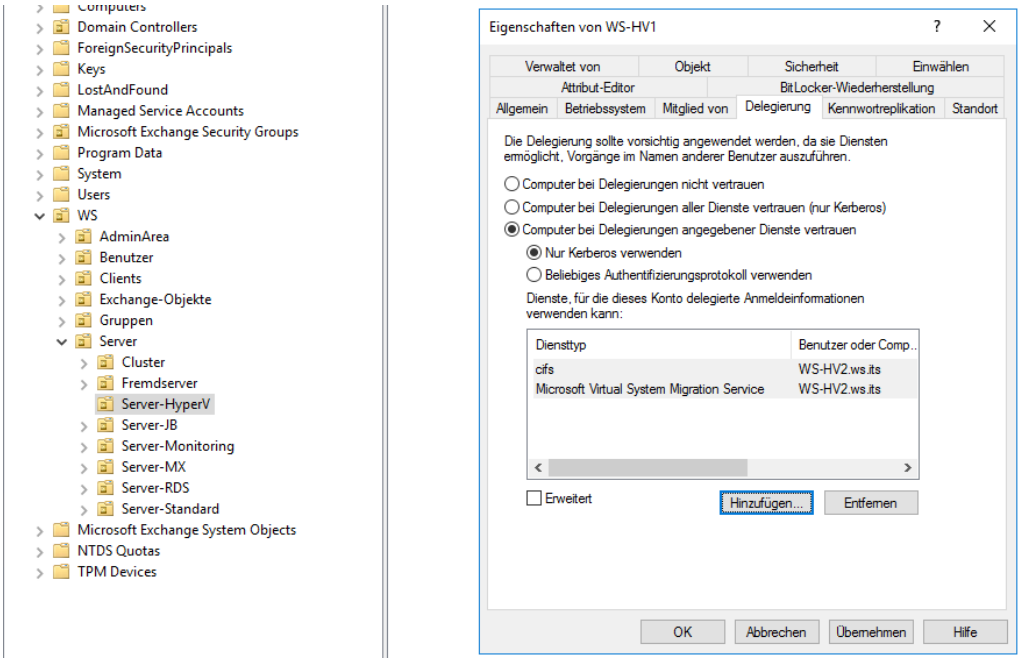
Eine Kontrolle der Delegationen ergibt aber, dass hier immer noch die alten Werte drinstehen:



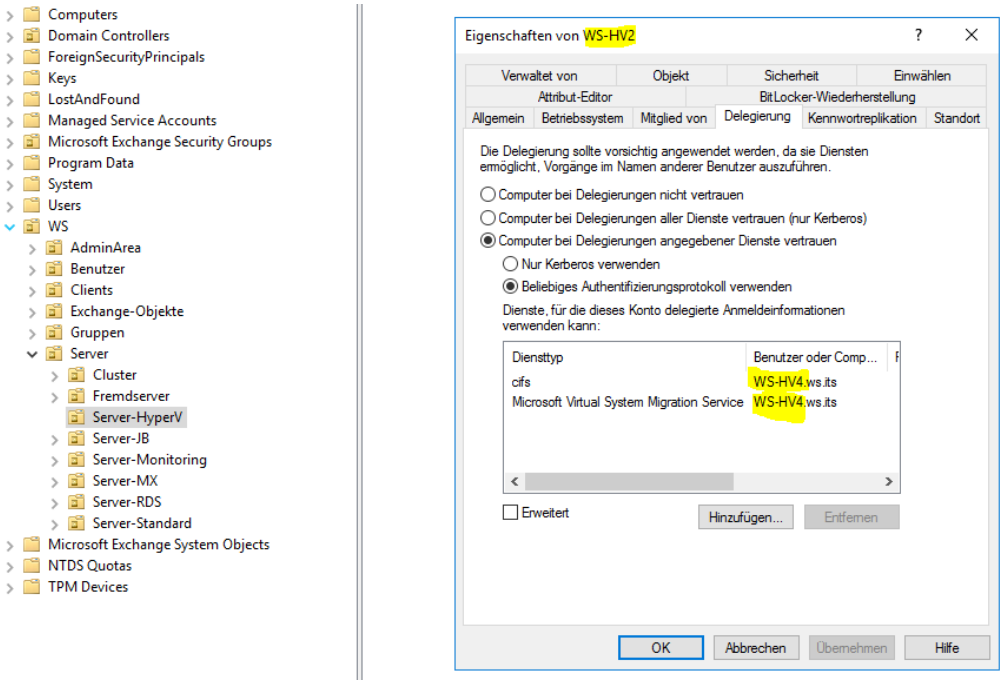
Naja, bei der nächsten Verschiebung einer VM wär's bestimmt aufgefallen… Ich trage jetzt den neuen Servernamen ein, da es in der GUI keine Option zum Editieren vorhandener Werte gibt:



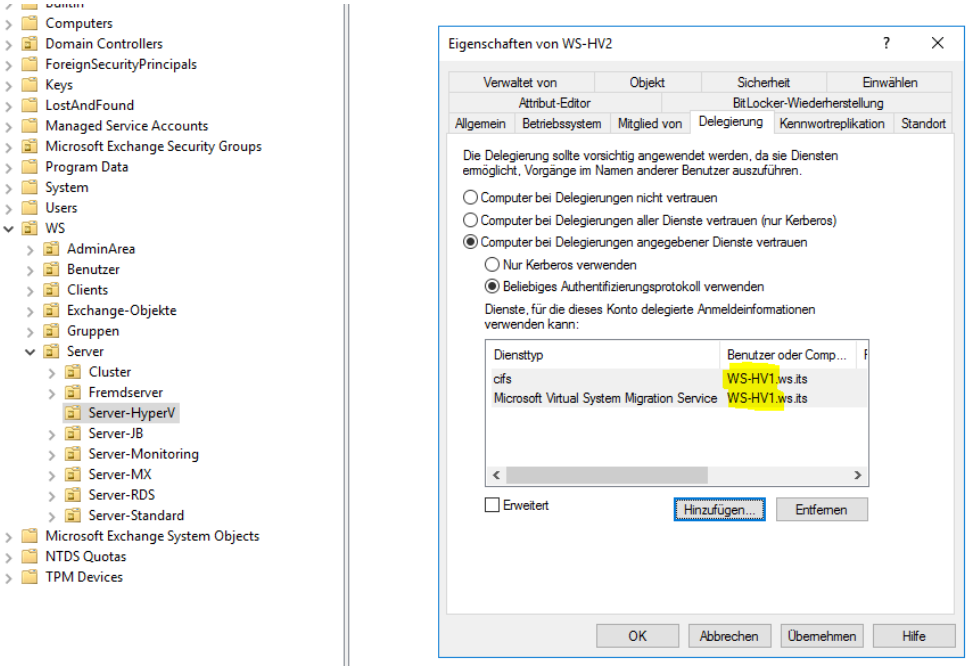
Und nachdem ich die verwaisten Werte entfernt habe, passt wieder alles:



Aber auch der andere Server hat die alten Werte behalten:



Also füge ich die neuen Werte ein und lösche die alten:

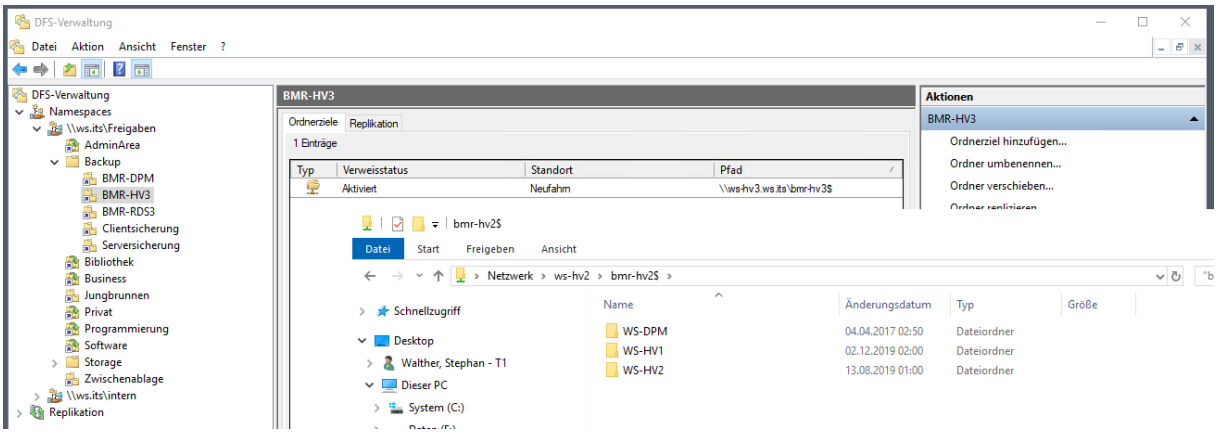


Jetzt funktionieren auch die Live-Migrationen meiner VMs wieder.

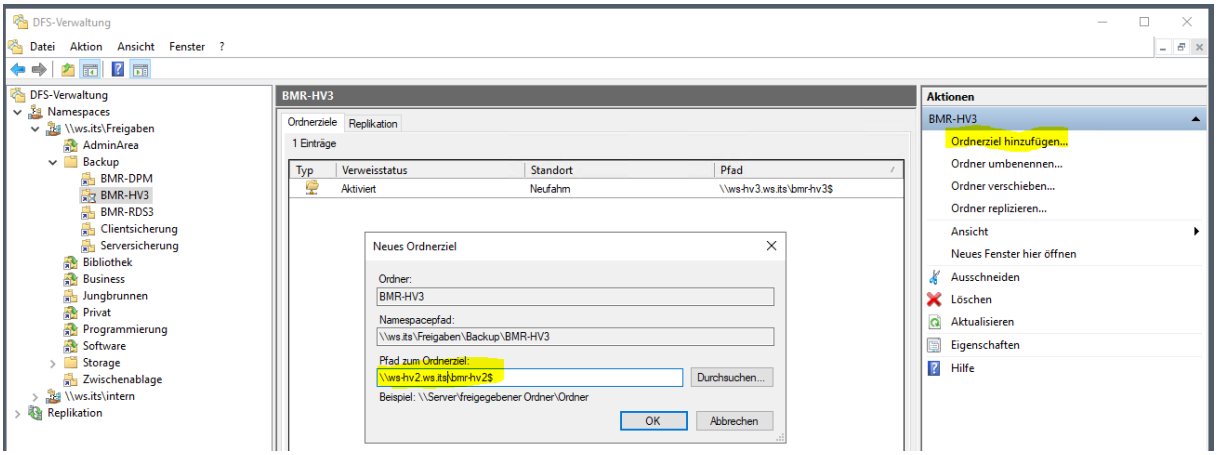
DFS-Namespace

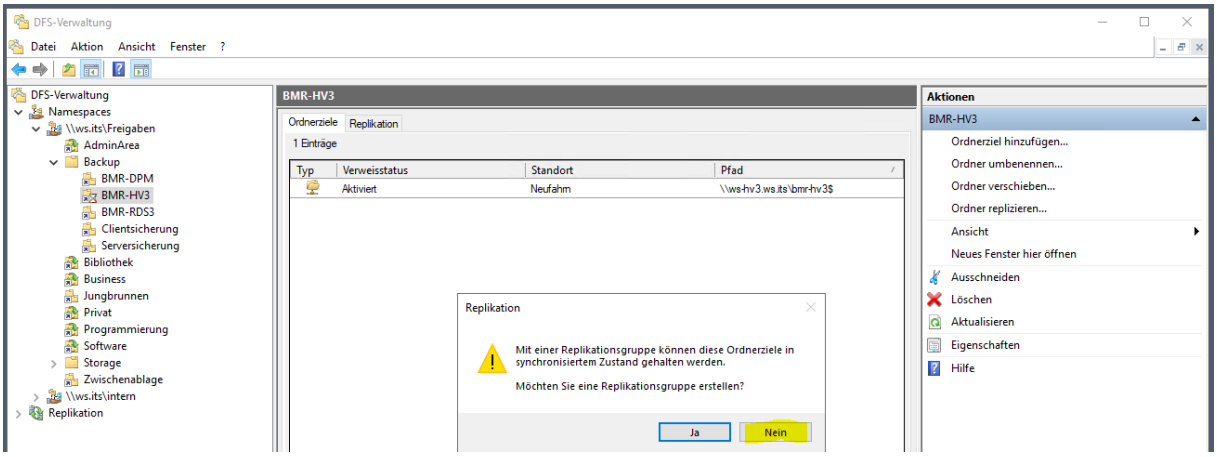
Was haben zwei Hyper-V-Server mit dem verteilten Dateisystem (DFS) zu tun? Richtig: Eigentlich nichts. Aber bei mir habe ich aus Kapazitätsgründen auf einem der beiden Server eine Freigabe eingerichtet, in welcher beide Hyper-V-Server und auch der DPM-Server ihre Datensicherung speichern können. Es geht mir dabei nur um das Recovery-Szenario „Betriebssystem- oder Hardwareausfall“. Die Sicherung landet auf einer separaten Festplatte im WS-HV3. Fällt dessen Systemfestplatte aus, dann kann ich einfach wiederherstellen. Das gilt für beide Hyper-V-Server. Der DPM übernimmt meine Nutzdatensicherung (Fileservice, Mailservice, …), kann sich aber nicht selber sichern. Daher hat er hier auch einen Slot für seine Betriebssystemsicherung erhalten.

Die Freigabe für die Sicherung habe ich auch in meinen DFS-Namespace aufgenommen. Dies vereinfacht die Administration erheblich. Da noch einige andere Zugriffspunkte für die Datensicherung existieren, habe ich diese in einem Unterordner im DFS-N organisiert. Die Bezeichner folgen den Servernamen. Also muss ich hier auch aktiv werden:

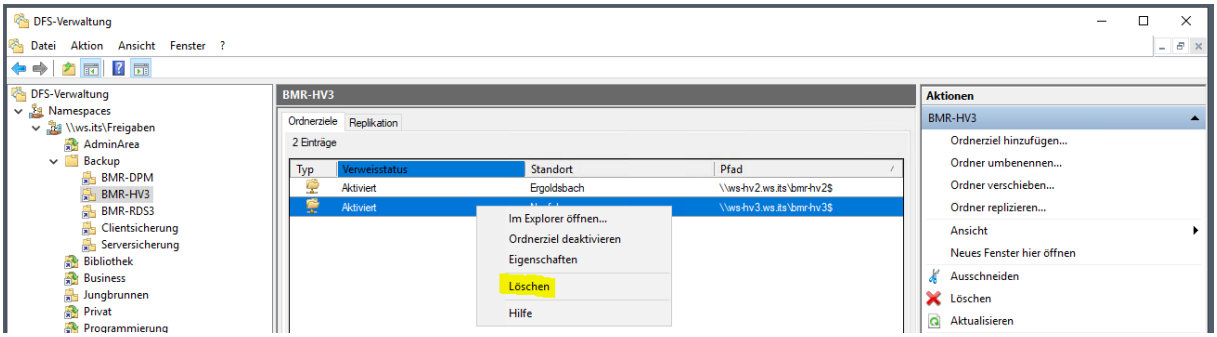


Die Umstellung ist einfach: Ich füge das neue Ziel zum neuen Servernamen als Link hinzu – ohne dabei eine Replikationsgruppe zu erstellen (die Quelle und das Ziel sind der gleiche Server!):

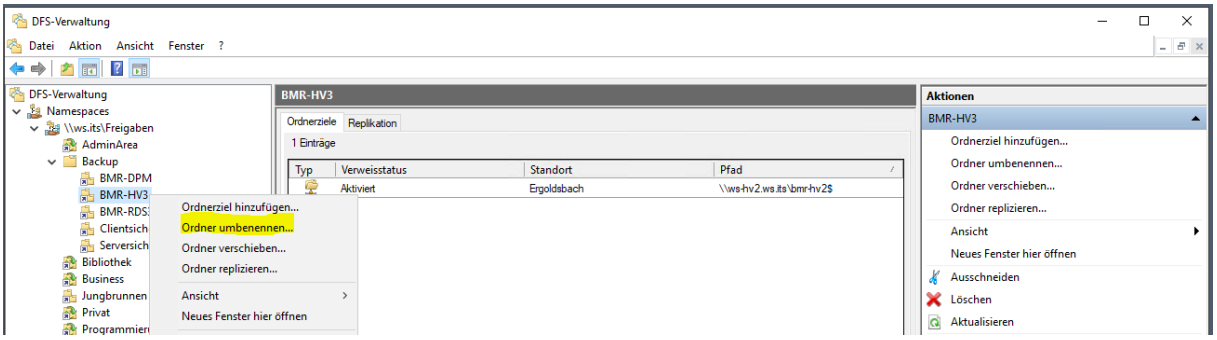


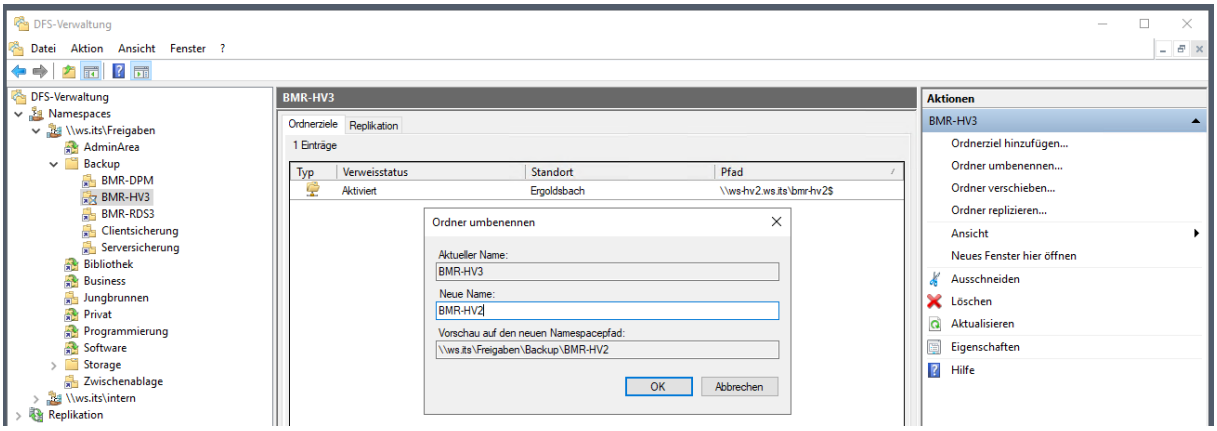


Dann entferne ich den Link zum alten Servernamen. Hierbei ist wieder darauf zu achten, dass nur der Link zum Ziel und nicht der gesamte Ordner gelöscht wird:



Den Ordner selber kann ich einfach umbenennen:

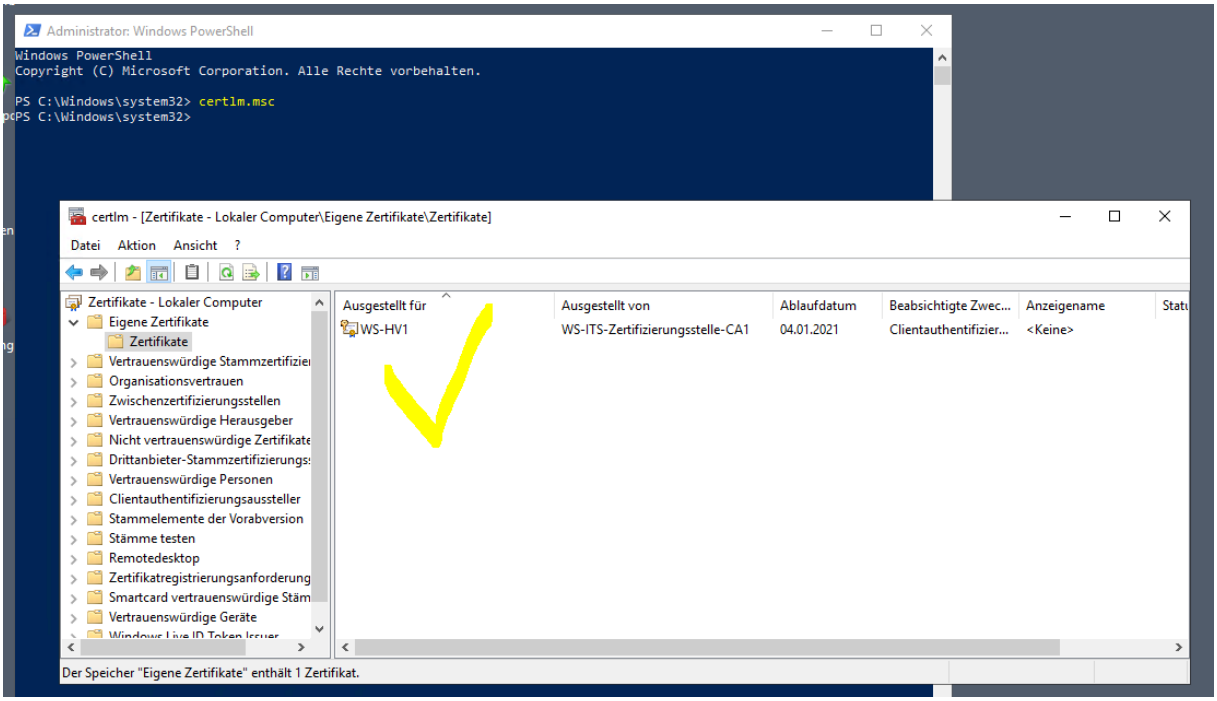




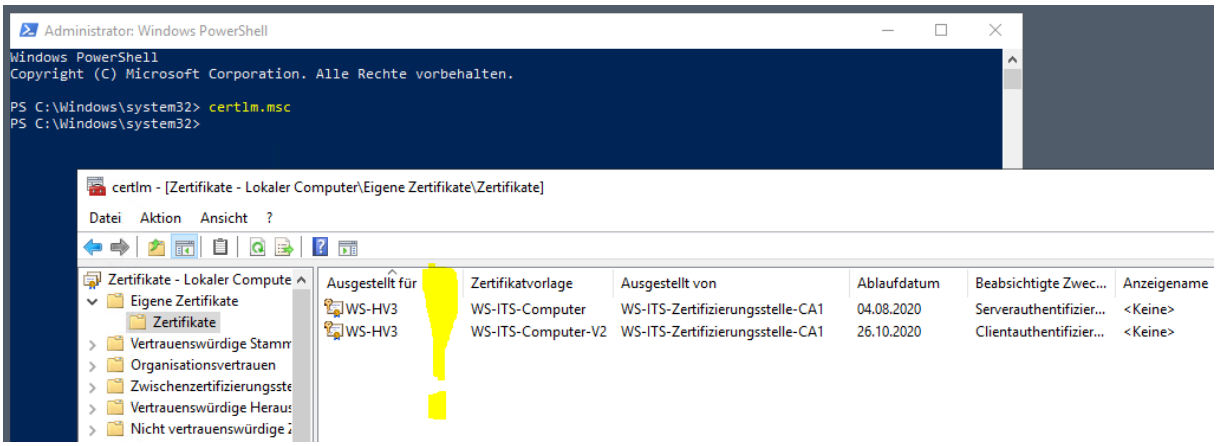
Nach wenigen Minuten wird diese Information dann auch auf den Clients ankommen. Den Link im DFS habe ich in keinem Script oder dergleichen verwendet. Es ist nur ein Zugriffspunkt, wenn ich administrativ die Sicherung sichten oder z.B. bereinigen muss. Daher gibt es nach der Umstellung des Pfades keine weiteren Anpassungen.

Zertifikate

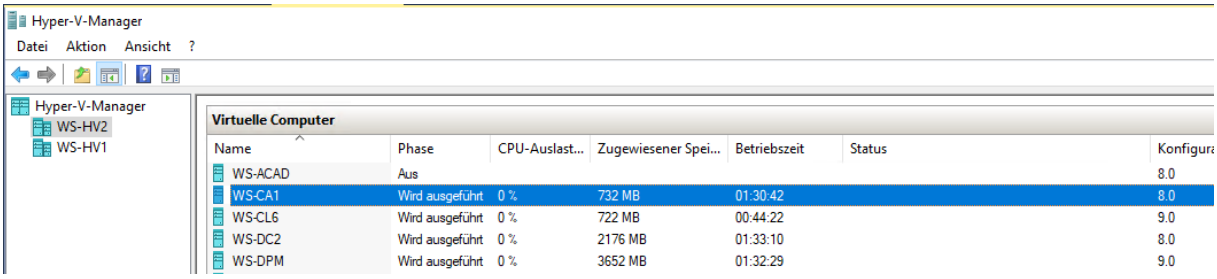
Dank meiner internen Active Directory integrierten PKI und einer GPO erhalten alle Systeme vollautomatisch ihre Computerzertifikate. Diese werden üblicherweise auf den CN der Server ausgestellt. Diesen habe ich aber durch das Umbenennen verändert. Wurden die Zertifikate automatisch korrigiert (erneuert)?



Der Server WS-HV1 hat bereits ein neues Zertifikat bekommen und damit das alte überschrieben. Aber der andere Server ist noch nicht so weit:

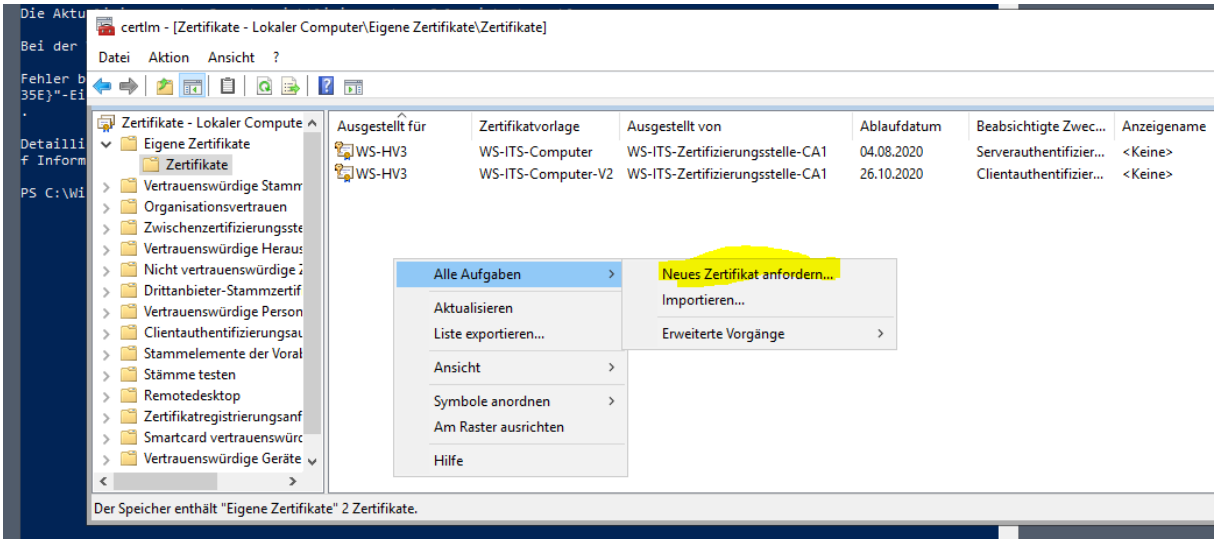


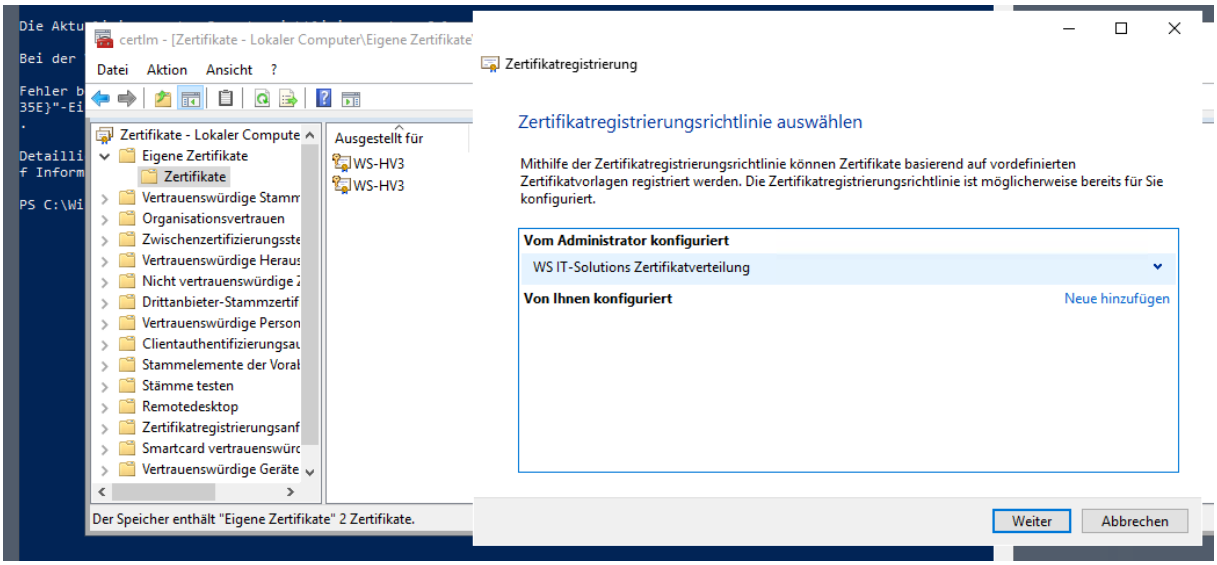
Die Ursache dafür ist einfach: die Zertifikat-Automatik läuft ab dem Systemstart in einem 8-Stunden-Intervall. WS-HV1 hat bei seinem Neustart die PKI kontaktiert und die Neuausstellung vorgenommen. Die PKI läuft in einer VM auf WS-HV2 und war daher problemlos erreichbar:

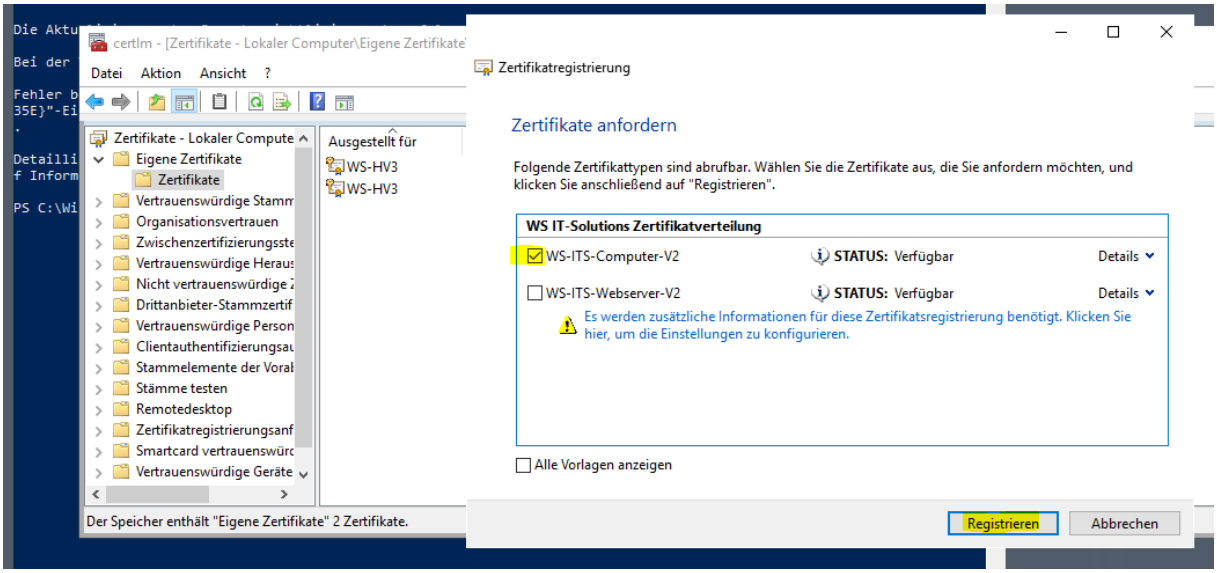


Beim Neustart nach der Umbenennung von WS-HV2 war die VM mit der PKI aber ausgeschaltet. Der Server konnte nach seinem Start also keine Verbindung aufbauen. Und er wird es erst in knapp 8 Stunden wieder probieren.

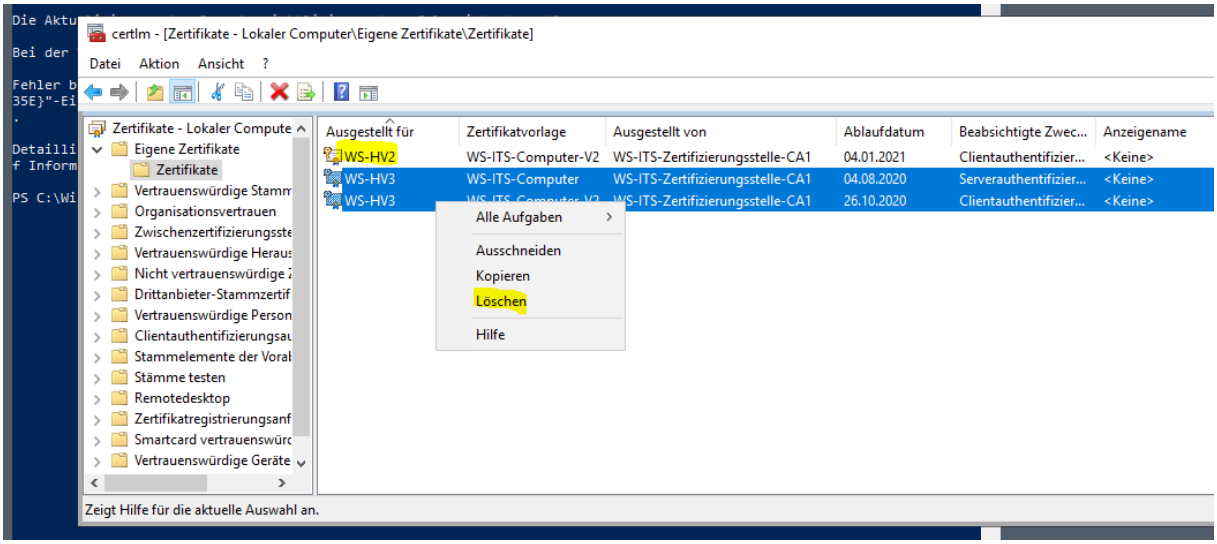
So lange möchte ich nicht warten. Daher frage ich das Zertifikat manuell an:







Dabei werden die alten Zertifikate aber nicht überschrieben. Diese muss ich selber löschen:



Mit etwas Geduld bereinigen sich die Abhängigkeiten von allein. Aber eine Kontrolle ist immer besser.

weitere Abhängigkeiten

Scripte sind eine beliebte Location für feste Servernamen. In meinem Fall war es nur das Backup-Script. Da könnte aber noch viel mehr vorhanden sein.

Auch Anwendungen nehmen gerne den Servernamen in ihre Konfiguration auf. Ein Beispiel war mein DPM. Je nach Server können da auch etliche andere Anwendungen bereitstehen.

Zusammenfassung

Die Anpassung der beiden Servernamen habe ich erfolgreich durchgeführt. Man sieht aber, wie viele Komponenten und Dienste da hinten dranhängen können. Ein Umbenennen würde ich niemanden für produktive Umgebungen empfehlen!

Überlegt euch eine Namenskonvention zusammen mit euren Kollegen. Es wird nie eine optimale Lösung für alle Bereiche und alle Zeiten geben. Weder das stumpfe Durchnummerieren, noch die Verwendung von Servicenamen scheint ideal zu sein.

Daher möchte ich an dieser Stelle mein Namensschema mit seinen Eigenheiten und den Vor- und Nachteilen einmal darstellen. Ich hatte es damals so designed:

WS-xy(z)#

- **WS** … ist ein Präfix, der meine Systeme kurz einleitet. Ein Name wie DC1 war mir einfach zu „einfach“. Denkbar wären hier auch DEV- oder PROD- ➔ ich könnte also in einer Testumgebung einen Klon des WS-DC1 als DEV-DC1 herstellen.
- **xy(z)** … ist ein Kürzel für den Hauptservice des Servers. Das Kürzel sollte zwischen 2 und 3 Zeichen lang sein. Aktuell verwende ich DC (DomainController), MX (Microsoft Exchange), RDS (Remote Desktop Service), FS (File Service), MON (Monitor: PRTG, Syslog, WEF), …
- **#** … dies soll eine laufende Nummer sein, damit ich von einem Service mehrere Instanzen bzw. Server bereitstellen kann. Die Nummer soll dabei auch im Idealfall der Position der VM zu einem Hyper-V-Host darstellen. So wird die VM WS-FS2 auf WS-HV2 platziert sein. Die Nummer kann bei Services, die definitiv nur auf einem Server laufen werden entfallen.

Es gibt bei meinem Schema aber auch Nachteile:

- Heute verwende ich z.B. für mein Monitoring den Server WS-MON. Geplant ist also kein zweiter Server. Was würde aber passieren, wenn ich morgen ein hochverfügbares Monitoring benötige? Sollte ich immer eine Laufnummer verwenden?
- Die Nummerierung sieht nur eine Stelle vor. Bei den Servern sollte dies auch je Service genügen, aber bei den Clients wäre es denkbar: WS-CL1 … WS-CL9, WS-CL10 Bei einer Sortierung kommt die 10 leider immer zwischen der 1 und der 2. Also doch lieber 2 Ziffern mit führender Null?
- Mit 3 Buchstaben kann ich nicht jeden Service exakt beschreiben: vor einigen Tagen habe ich einen Media-Server benötigt. Ein möglicher Name war: WS-Med. Nur was soll das sein? Klingt irgendwie medizinisch… Genannt hab ich ihn jetzt WS-MM (MultiMedia). Aber intuitiv ist doch irgendwie anders…
- Zur Zeit von Windows Server 2012R2 hatte ich einen IPAM-Server mit dem Namen WS-IPM. Auf diesem habe ich später testweise das PRTG-Monitoring installiert. Dieser Fall ist namenstechnisch leicht abzufangen: Ein Server bekommt einfach nicht mehrere Rollen bzw. Funktionen konfiguriert. Wird eine neue Anwendung bereitgestellt, dann erhält diese ihren eigenen Server. Aber was passiert, wenn die zusätzlichen Server zusätzliche Lizenzkosten verursachen und daher nicht möglich sind?
- Ich habe 2 Jahre nach dem Erstellen meiner Infrastruktur einen zweiten Standort dazu bekommen. Leider hatte ich im Namensschema keinen Marker für die geografische Position eingeplant. Bisher war es möglich, alle Server mit der Laufnummer 3 in dem Außenstandort zu platzieren. Aber dies stellt durchaus eine Einschränkung dar, ist nicht intuitiv und schränkt mich im Hauptstandort auf 2 Server je Service ein.

Es lohnt sich also, im Vorfeld über die Bezeichner nachzudenken. Und sollte wirklich ein Umbenennen erforderlich werden, dann überlegt ganz genau, wo sich diese Veränderung überall auswirken wird.

Und noch ein Tipp:
CNAMEs im DNS sind keine gute Idee! Ich habe das schon öfter auch nach Migrationen gesehen: Der neue Server hat einen anderen Namen und im DNS existiert ein Alias mit dem alten Namen, der auf den neuen Server zeigt. Netzwerktechnisch funktioniert das durchaus. Aber für die Authentifizierung kann so kein Kerberos verwendet werden. Zudem belegt dann ein Server 2 Namen.