

Inhalt

Zielsetzung	2
Bereitstellung von WS-HV4	2
Montage des neuen Servers	2
Installation des neuen Servers.....	3
Konfiguration des neuen Servers	5
Installation der Rollen und Features	8
Netzwerkconfiguration mit NIC-Teaming.....	9
Vorbereitung der Deaktivierung des alten Servers WS-HV1	15
PFSense-Maintenance	15
Monitoring	16
Entfernung einer defekten Festplatte	16
Herunterfahren der VMs auf dem alten Server.....	17
Auslesen von Informationen.....	18
Konfiguration von WS-HV4	18
Einbau des neuen Servers.....	18
Konfiguration des Storage	18
Konfiguration des Hyper-V	25
Import der VMs.....	27
Optimierung der VMs	29
Verschiebung einiger VMs	29
Verschiebung der großen VHDX der Fileserver	32
Maintenance beenden.....	38
Datensicherung einrichten	39
Einrichtung des Notfallzugangs.....	52
Vorgeschichte.....	52
Implementierung des Notfallplans	54
Zusammenfassung	58

Zielsetzung

Mein Hyper-V-Host „WS-HV1“ ist nun schon etliche Jahre im Dauereinsatz und seit einiger Zeit an seiner Belastungsgrenze angekommen. Daher soll er gegen eine neue Hardware ausgetauscht werden. Auf dieser wird das Betriebssystem im Rahmen meiner infrastrukturweiten Migration auf Windows Server 2019 umgestellt.

Durch die neue Hardware ist also ein Side-By-Side-Migrationsszenario möglich:

- Der neue Server wird als WS-HV4 eingerichtet
- Alle VMs von WS-HV1 werden auf WS-HV4 verschoben (ok, das ist ein Wipe-And-Load-Migrationsszenario)
- Die Hardware von WS-HV1 wird aus dem Serverschrank ausgebaut.
- Die neue Hardware von WS-HV4 wird in den Serverschrank integriert.

Wie üblich überlege ich mir vorab einige Ziele und Rahmenbedingungen, die ich erreichen bzw. einhalten möchte: Die Migration soll nach Möglichkeit ohne Service-Downtime während der üblichen Bürozeiten durchgeführt werden. Da aber ein Datenträger im alten Server noch recht jung ist (eine 500GB NVMe PCI-Gen3), möchte ich diese mit in den neuen Server einbauen. Darauf sind die meisten VMs gespeichert. Diese müssen für den Transfer ausgeschaltet werden. Mein Service-Design sieht aber für alle Produktionsdienste (Anmeldeservice, Mail, Dateisystem, Logging) eine Redundanz vor: Diese Services laufen also auf jeweils mindestens 2 Systemen. Und diese sind auf meine beiden Hyper-V-Hosts verteilt. Somit kann ich zu einer Zeit einen Hyper-V-Host herunterfahren, ohne dass die Dienste versagen.

Bereitstellung von WS-HV4

Montage des neuen Servers

Den neuen Server baue ich mir wieder aus meinen Wunschkomponenten zusammen. Wie die anderen Geräte ist die Basis ein Mix aus performanten Desktop-Komponenten. Die Gründe dafür sind recht einfach:

- Meine Server sollen sehr leise sein.
- Die produzierte Abwärme soll minimal sein.
- Der Stromverbrauch soll minimal sein.
- Die Leistungsklasse soll hoch sein.
- Ich benötige keine Hardware-Schutzkomponenten wie ECC-Memory oder teure RAID-Controller, da mein Ausfall-Szenario eines Hosts durch die Redundanz der Services kompensiert wird.
- Und bezahlbar darfs auch gerne sein.

CPU und Mainboard

Als Plattform habe ich mir einen AMD Ryzen 3700X ausgesucht. Mit AMD fahre ich seit Jahren sehr zufrieden und die neue Generation der Prozessoren unterstützt zudem PCI-Gen4. Daher habe ich ein passendes Mainboard mit 2 vollwertigen PCI-Gen4-Slots für NVMe-Speicher daruntergesetzt. Das Ganze soll schließlich ein paar Jahre Spass machen! Und mit 8 vCPU (16x logisch) freuen sich die vielen VMs. Zudem ist die Leistungsaufnahme extrem niedrig. Der ganze Server braucht 75W/h!

RAM

Dazu gibt es neue 2x32GB DDR4 PC3200 Module für den Arbeitsspeicher. Das Board kann davon nochmal so viel aufnehmen. Somit bleiben für den maximalen Ausbau 128GB auf dem Reißbrett stehen. Das sollte eine Weile genügen.

Storage

Für den Massenspeicher gönne ich dem System eine Gigabyte Aorus mit 1TB als TIER-GOLD Storage. Das Teil nutzt die PCI-Gen4-Schnittstelle recht gut aus. Und das beflügelt die VMs. Zusätzlich baue ich die „alte“ PCI-Gen3 NVMe mit 500GB um. Diese verwende ich als TIER-SILBER. Und für die großen Sachen verwende ich 2 neue WD Purple mit 4TB. Diese werden gespiegelt, da die abgelegten Nutzdaten keine Sicherung erfahren.

Netzwerk

Der Onboard-Adapter des Mainboards ist nicht brauchbar, da es für Windows Server 2019 keine passenden Treiber gibt. Und da ich eh mehrere Schnittstellen benötige, verbaue ich einen Intel Quadport Gbit-Adapter.

sonstige Hardware

Gekühlt wird das Ganze konventionell mit Lüftern. Deren Steuerung wird durch einen Controller mit 6 Sensoren optimiert. Das Board erhält einen TPM-Chip, damit ich einige Absicherungsoptionen nutzen kann. Eine Grafikkarte bekommt der Server nicht. Im Onlinebetrieb schalte ich mich mit einem USB-Grafikadapter auf. Und sollte wirklich mal ein Crash das System lahmlegen, dann baue ich die normale Grafikkarte eben ein. Den Kompromiss gehe ich der Umwelt zuliebe ein und spare den Strom und die Abwärme der GPU.

Montiert ist der kleine Server recht schnell. Und er kann sich doch sehen lassen, oder?



Wer jetzt denkt, das sei unprofessionell: Dieses System erfüllt alle meine Anforderungen an Leistung und Green-IT und ist zusammen mit dem nahezu baugleichen Server WS-HV3 in der Lage, eine hochverfügbare und sichere Infrastruktur zu betreiben. Die Vorgängersysteme lieferten dies seit 2013!

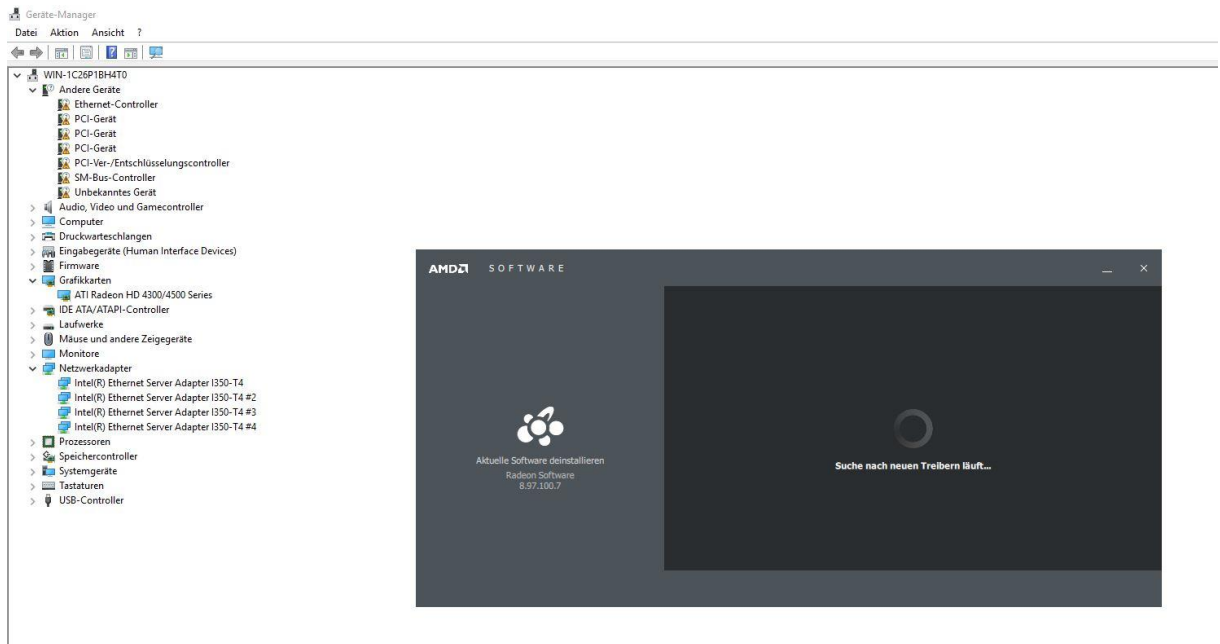
Und wegen dem Hersteller-Support und der nicht Windows Server 2019 zertifizierten Hardware: ich brauche keinen Support. Ich bin der Supporter! 😊

Installation des neuen Servers

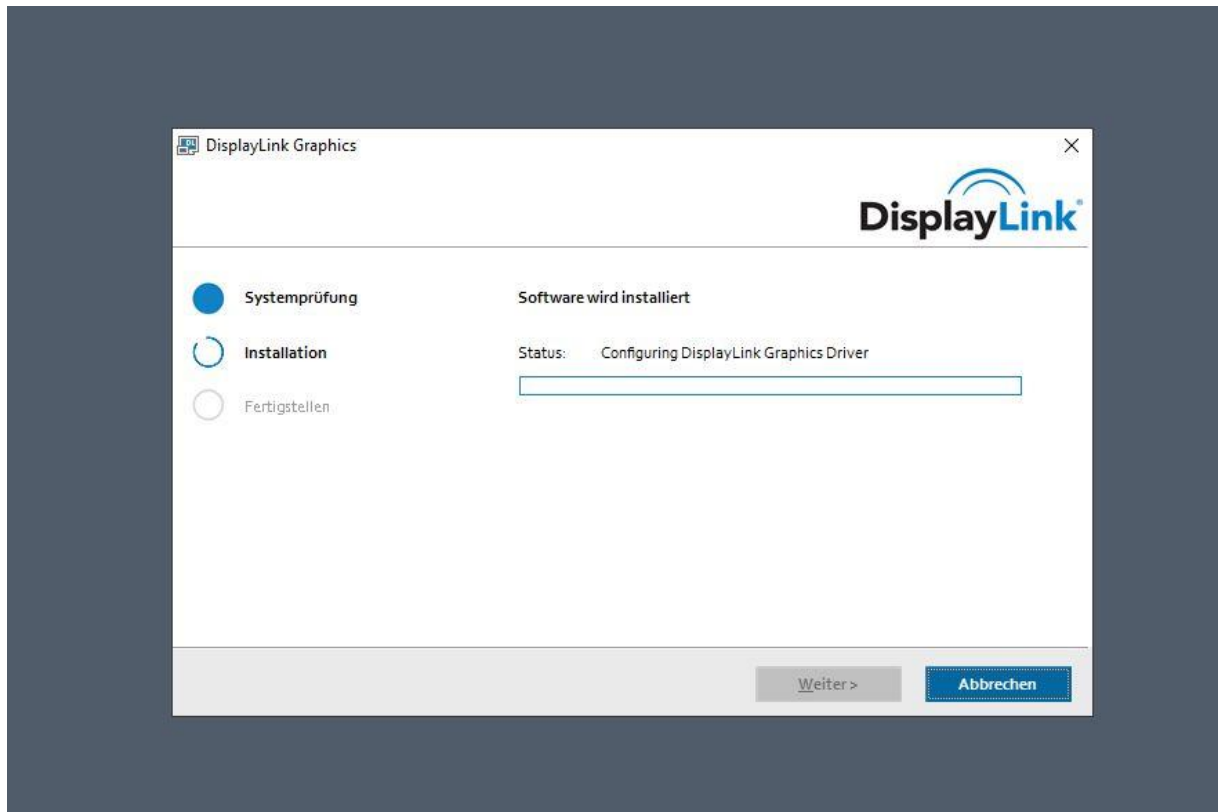
Nach der Montage konfigurierte ich noch einige Einstellungen in der UEFI-Umgebung. Dazu zählen UEFI-SecureBoot, der zusätzliche TPM-Chip und die Startreihenfolge beim Boot.

Da das System kein DVD-Laufwerk hat (und ich auch keine DVDs besitze), installiere ich das Betriebssystem über PXE von meinem Windows Deployment Server. Das Image hatte ich bereits vor einigen Wochen für meinen ersten Windows Server 2019 Hyper-V-Host bereitgestellt. Daher ging es hier etwas schneller.

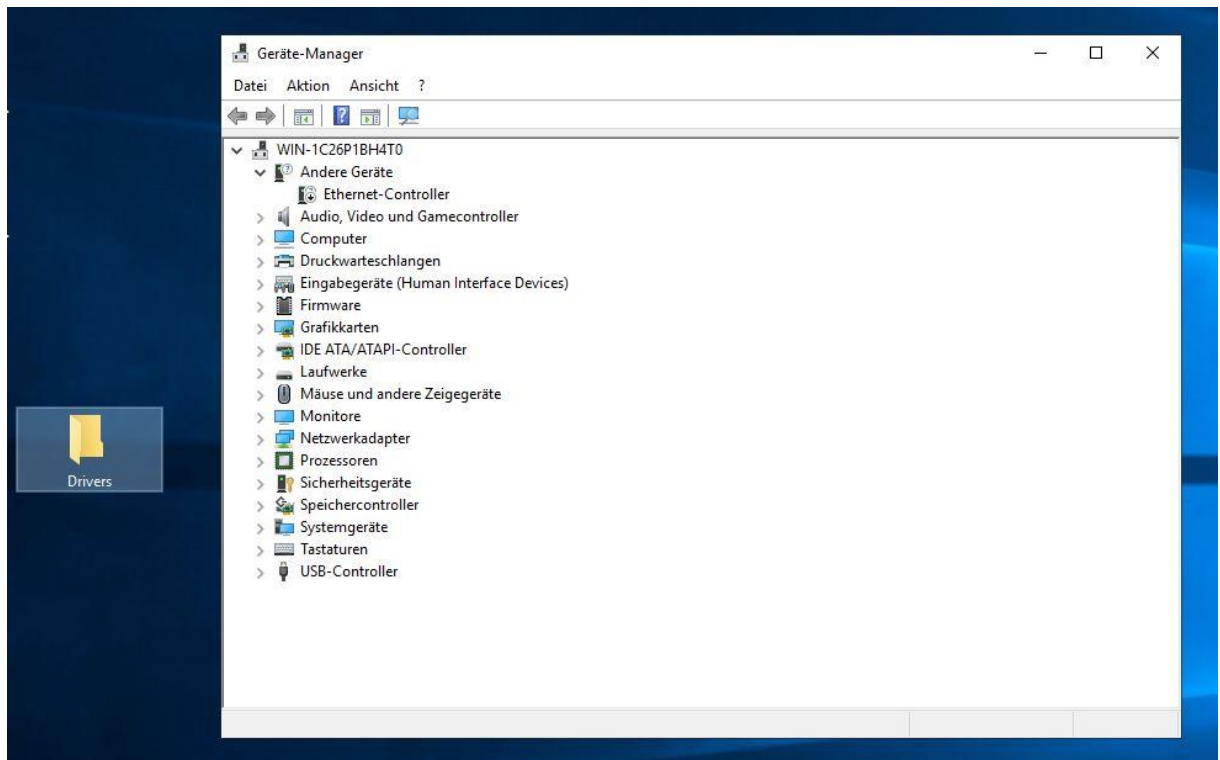
Nach dem Out-Of-Box-Experience-Mode installierte ich die notwendigen Treiber. Natürlich stellt der Hersteller des Mainboards keine für Windows Server zur Verfügung. Aber die Plattform entspricht im Wesentlichen der eines Windows 10 v1809. Also verwende ich Windows-10-Treiber. Und diese wurden ohne Meckern vom System installiert:



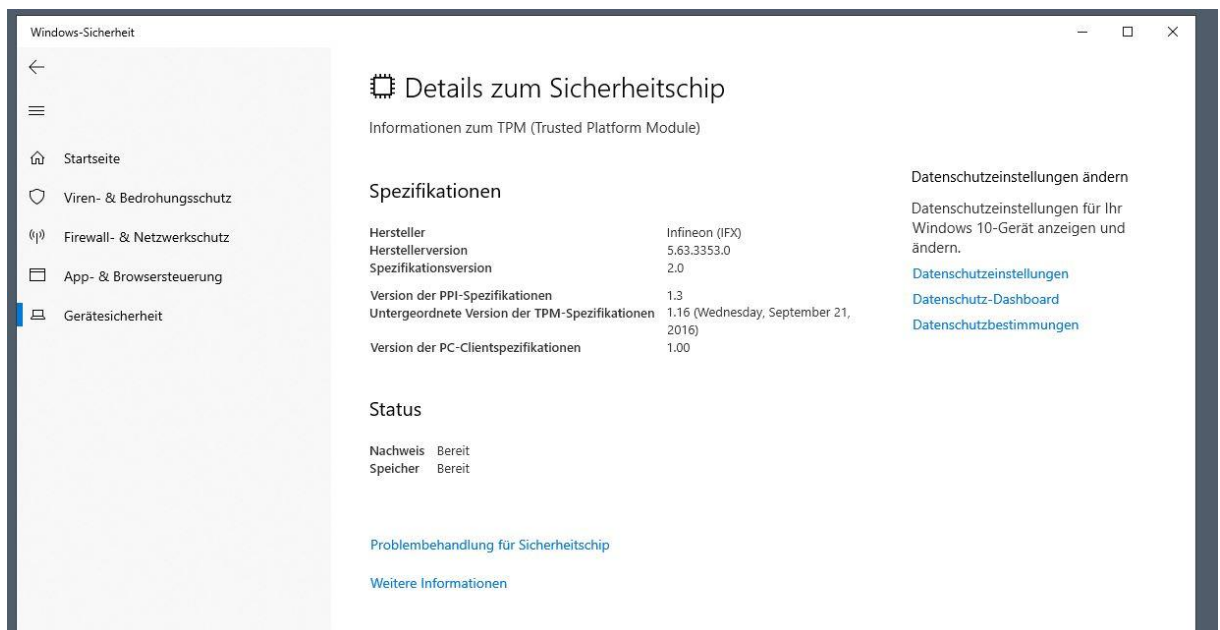
Meinen Monitor schlieÙe ich bei Bedarf über eine USB-Grafikkarte an. Der Treiber ist ebenfalls kompatibel:



Danach ist alles einsatzbereit:

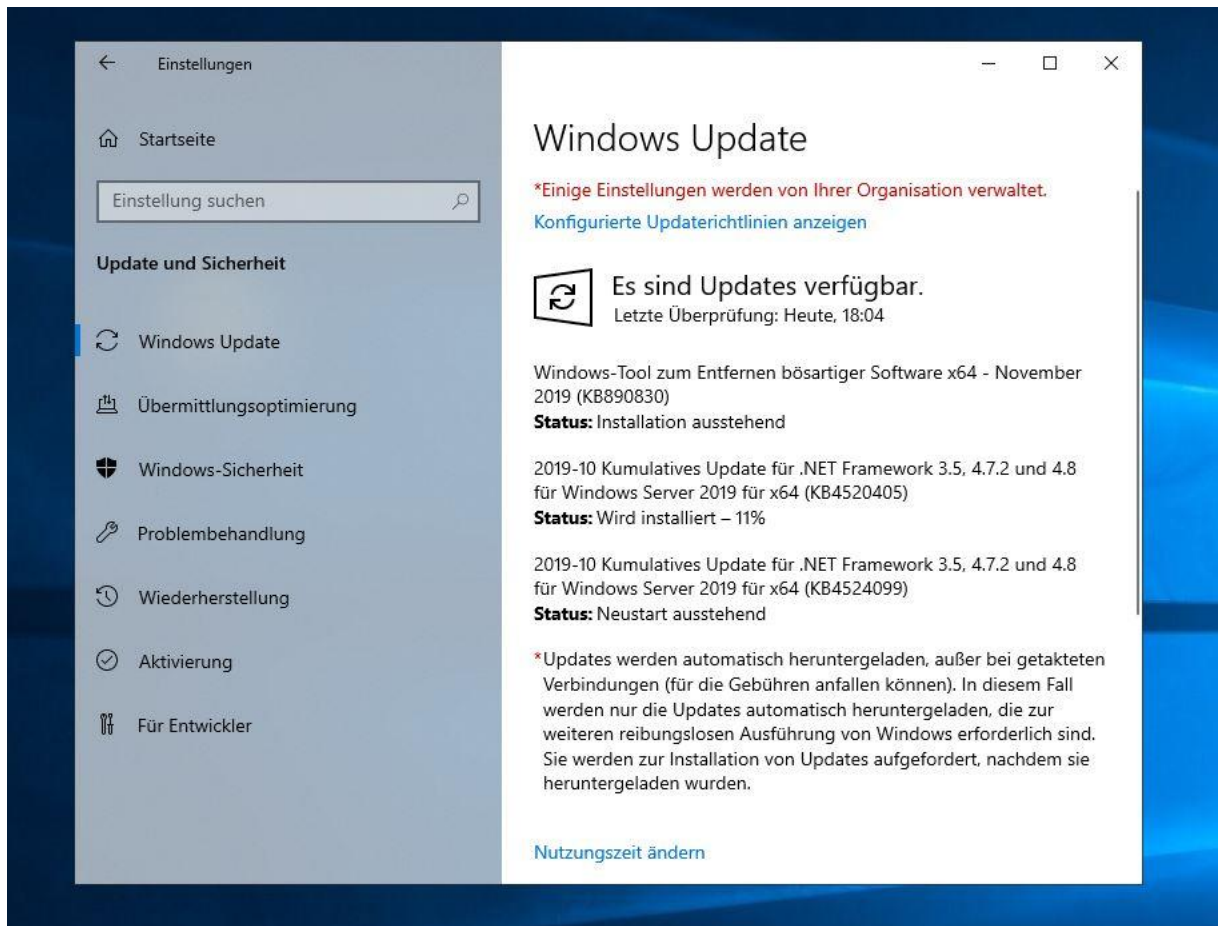


Nun kontrolliere ich noch fix den TPM-Chip. Dieser wird in den Einstellungen wie erwartet gelistet:

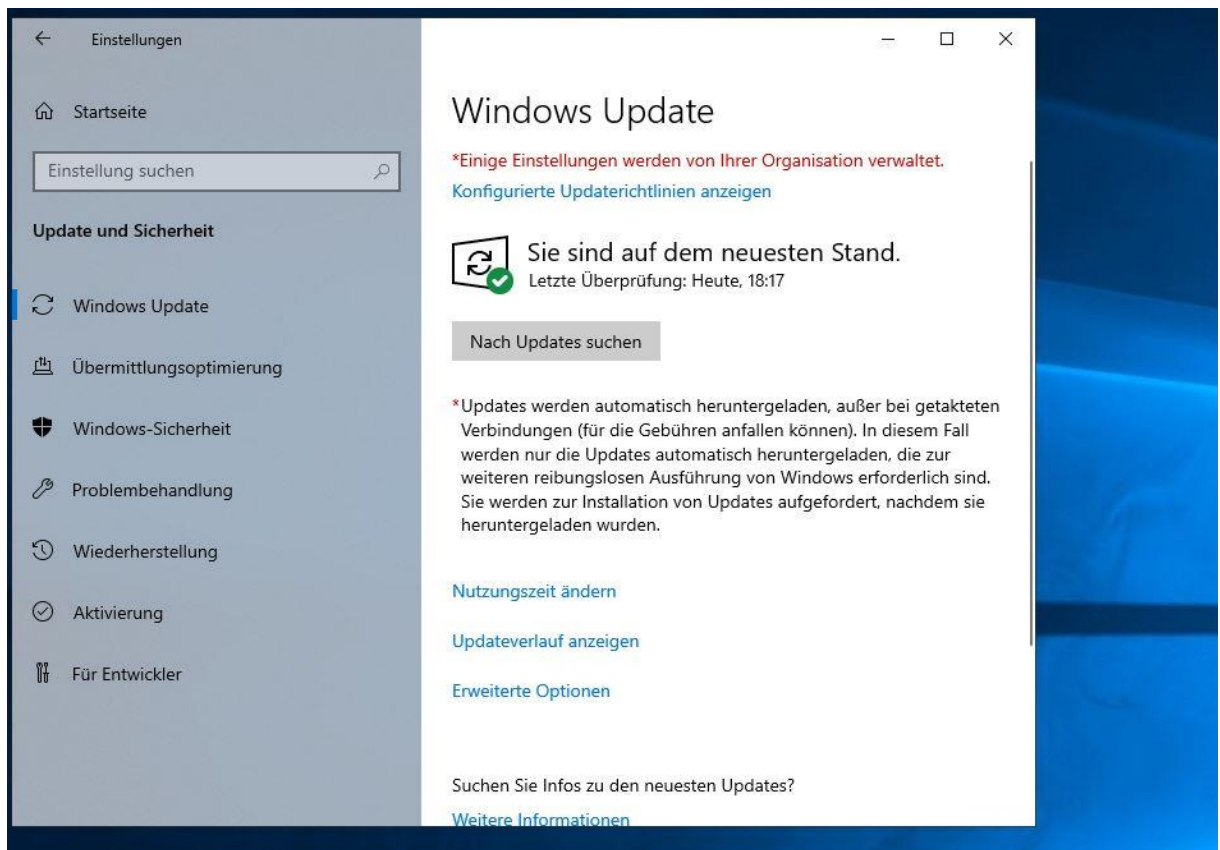


Konfiguration des neuen Servers

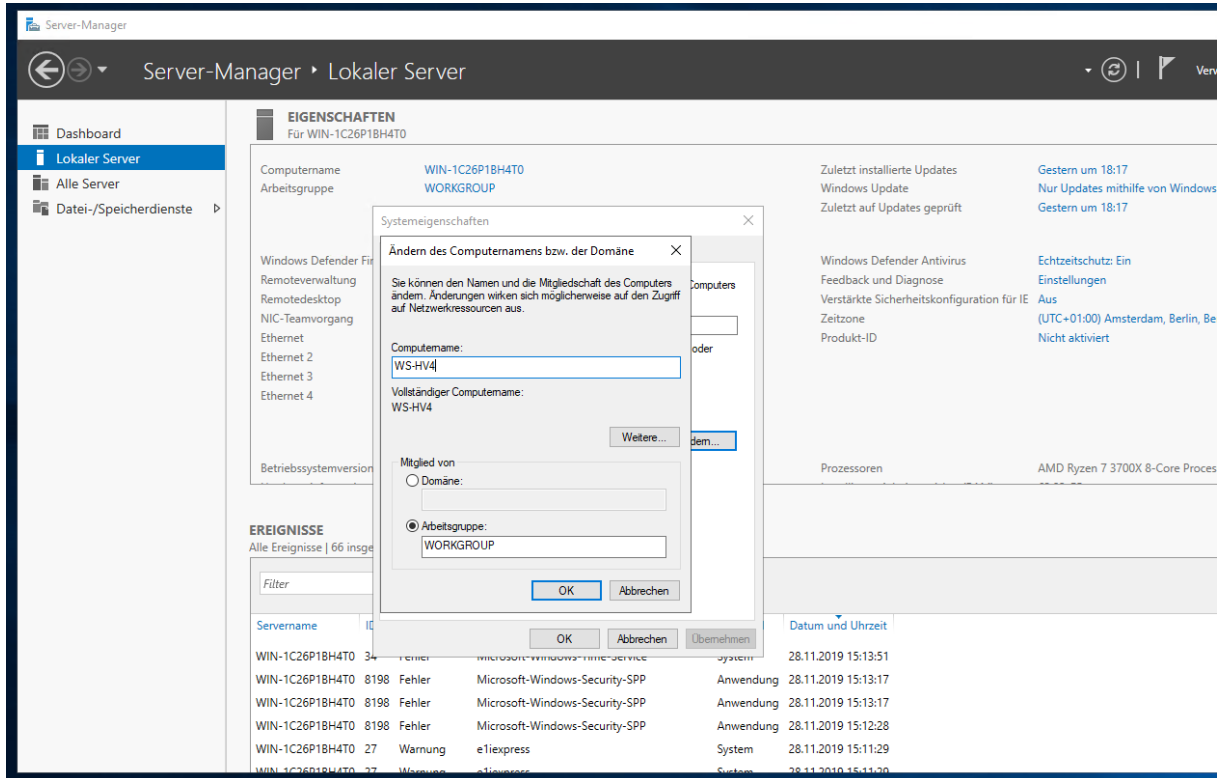
Der neue Server hängt aktuell im Client-Netzwerk. Dort kann er leicht eingeschränkt ins Internet. So kann ich das Betriebssystem erst einmal auf den aktuellen Stand aktualisieren:



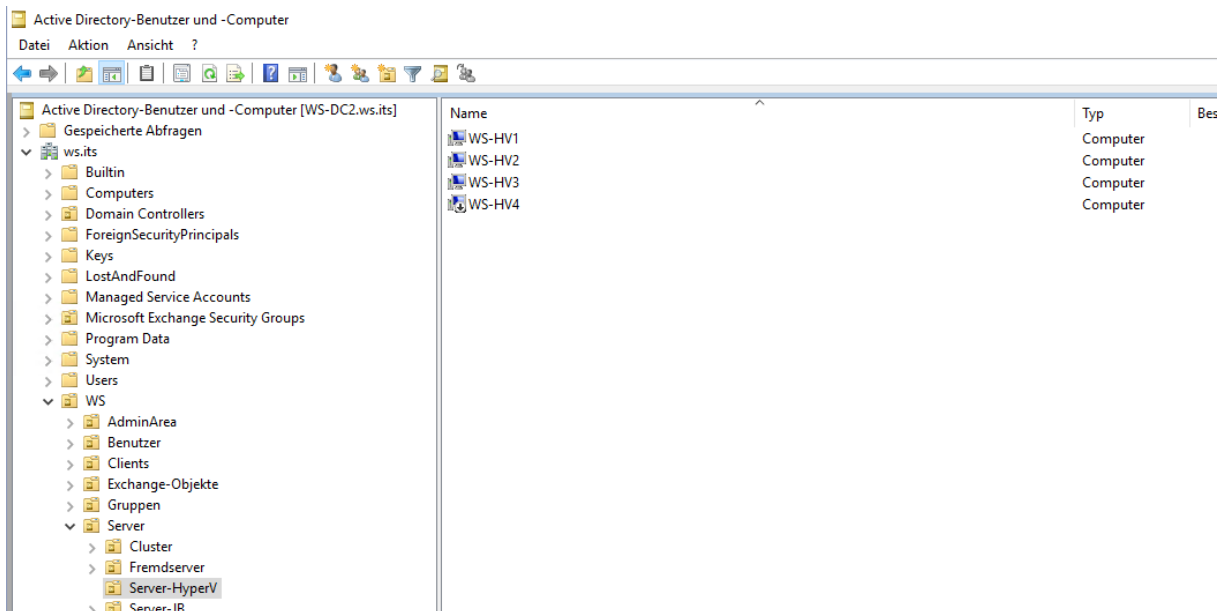
Die Updates werden wie gewohnt mit einem Neustart abgeschlossen. Danach passt die installierte Version:



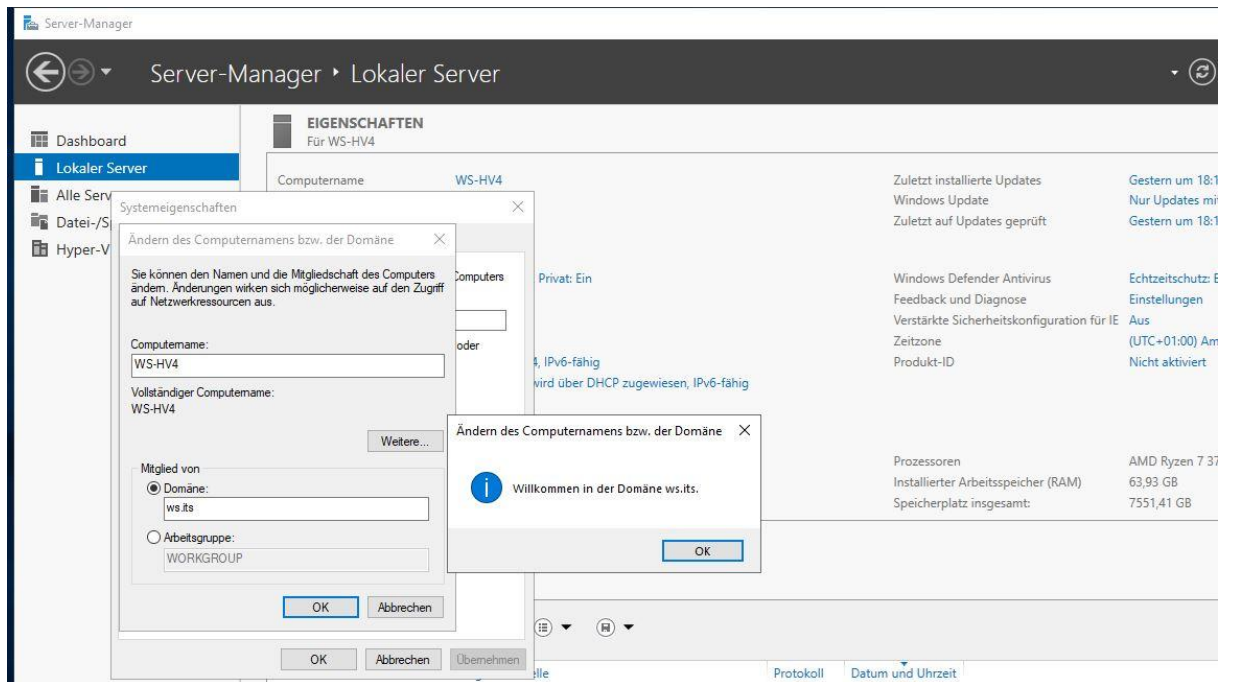
Nun bekommt das System seinen neuen Namen. Den Domain Join führe ich in einem zweiten Schritt aus:



Während der Server neustartet, erstelle ich im Active Directory ein neues Computerobjekt in der Organisationseinheit, in welcher meine Hyper-V-Hosts zu Hause sind:



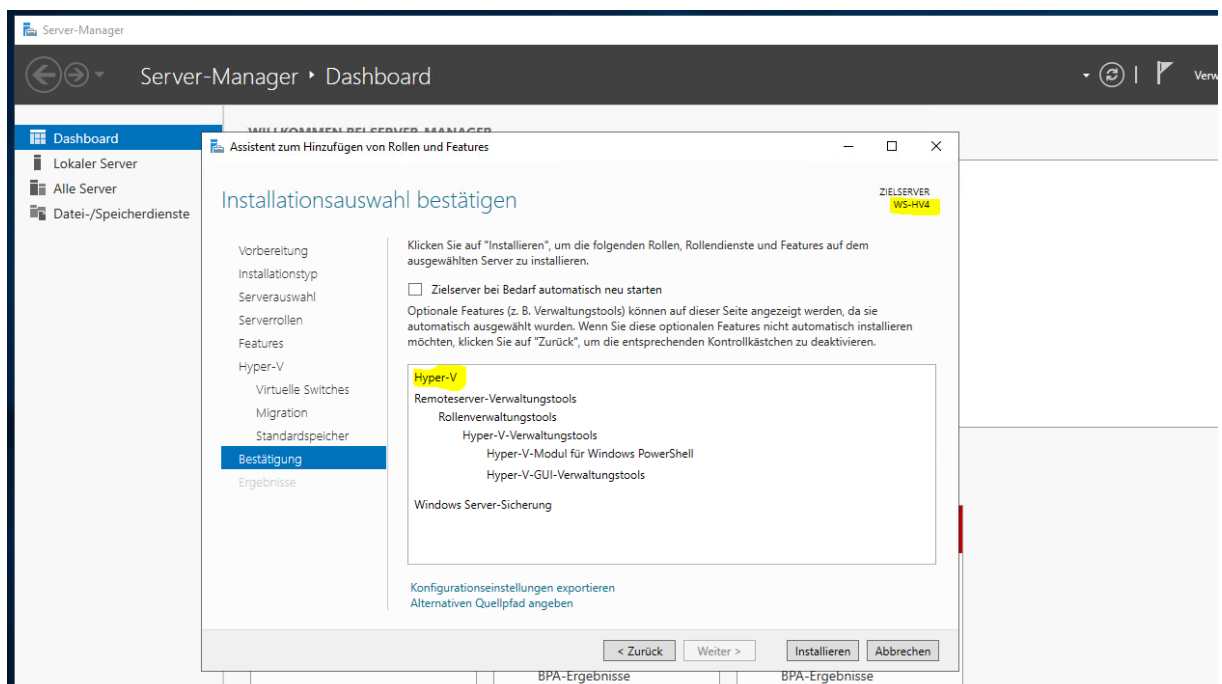
Nach der Anmeldung nehme ich das System in die Domäne auf:

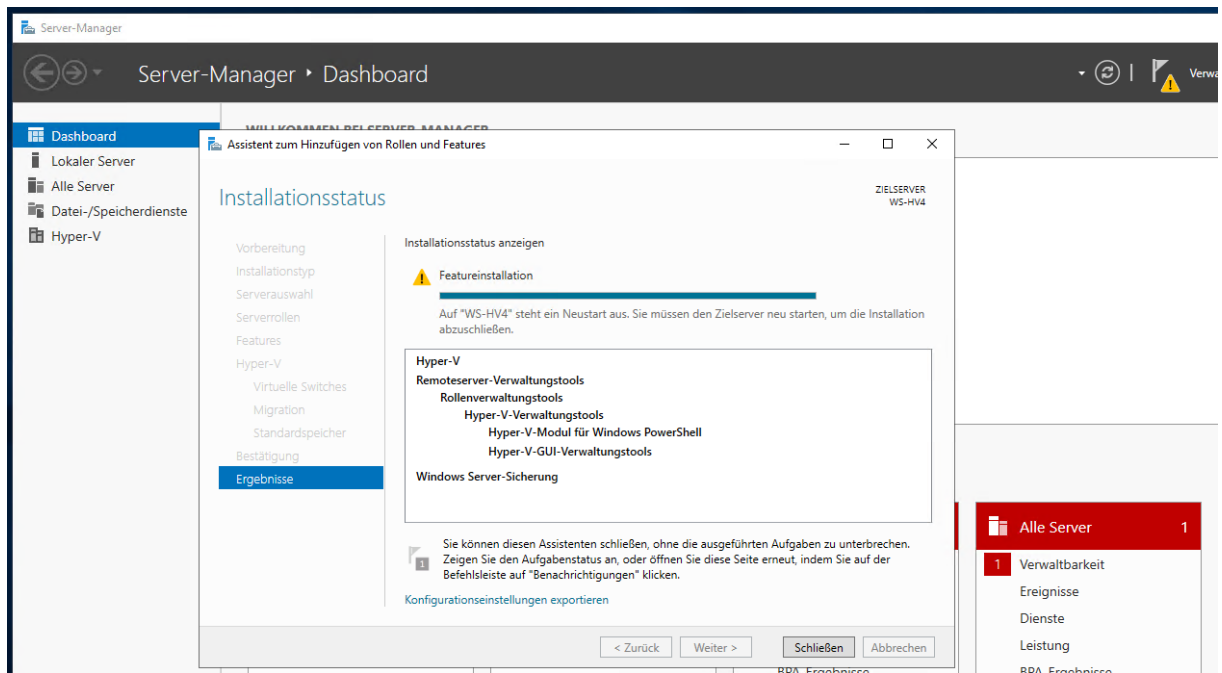


Nach dem Neustart ist das System Teil meiner Infrastruktur.

Installation der Rollen und Features

Nun installiere ich die Rolle Hyper-V und das Windows Server Backup Feature:





Da ist nichts dabei. Aber es ist erforderlich.

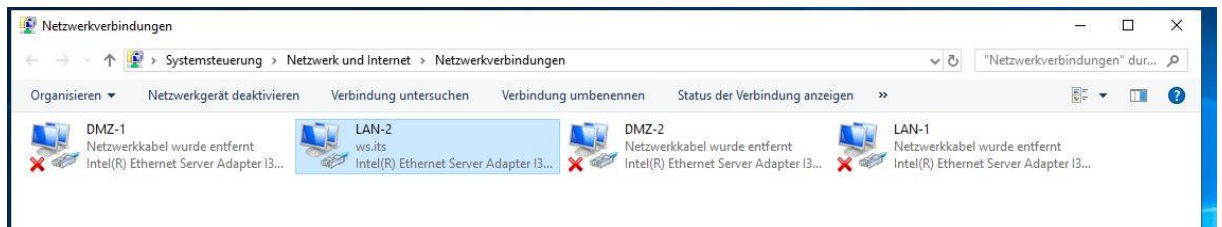
Netzwerkconfiguration mit NIC-Teaming

Viel spannender ist die Netzwerkkonfiguration. Der Server hat 4 Netzwerkkarten (Die Onboard-Nic habe ich wegen fehlender Treiber deaktiviert). Diese möchte so aufteilen:

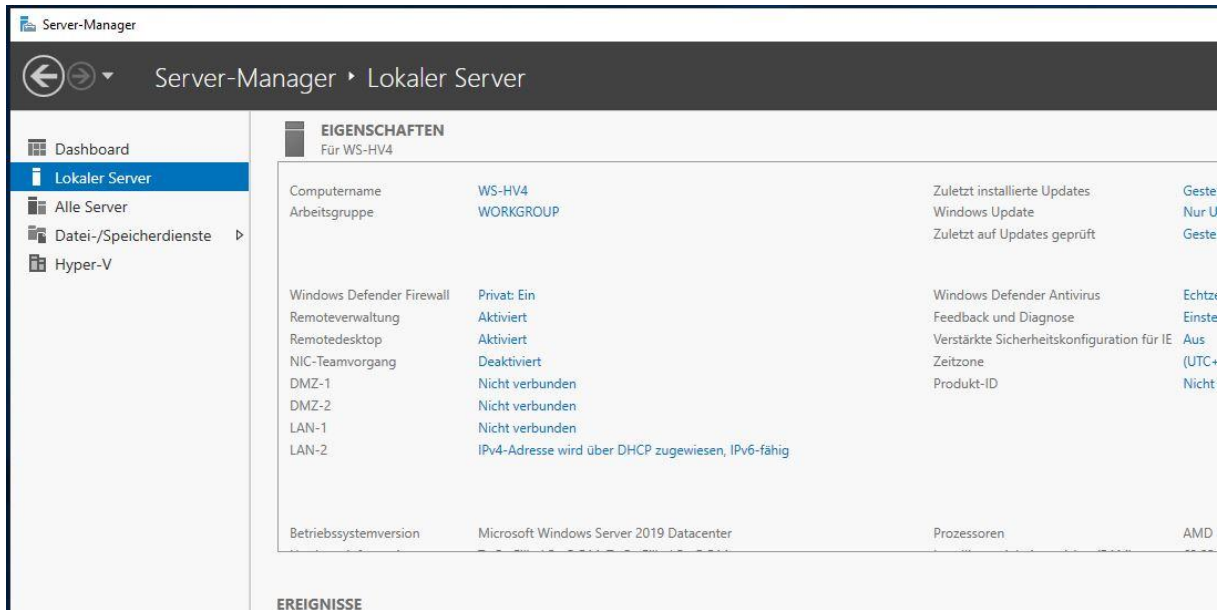
Anschluss	Team	VLAN	vSwitch	Verwendung
NIC1 → LAN-1	LAN-100	100	LAN-100	Servernetz
NIC2 → LAN-2	LAN-100	100	LAN-100	Servernetz
NIC3 → DMZ-1	DMZ	110,120,130,140,150	LAN-110,DMZ	Clientnetz, DMZ-Netze
NIC4 → DMZ-2	DMZ	110,120,130,140,150	LAN-110,DMZ	Clientnetz, DMZ-Netze

So kann ich immer 2 Adapter je Netzwerksegment an meine virtuellen Maschinen vergeben. Sollte ein Anschluss versagen, dann wird der Traffic auf dem anderen geroutet. So erhalte ich Lastverteilung und Verfügbarkeit.

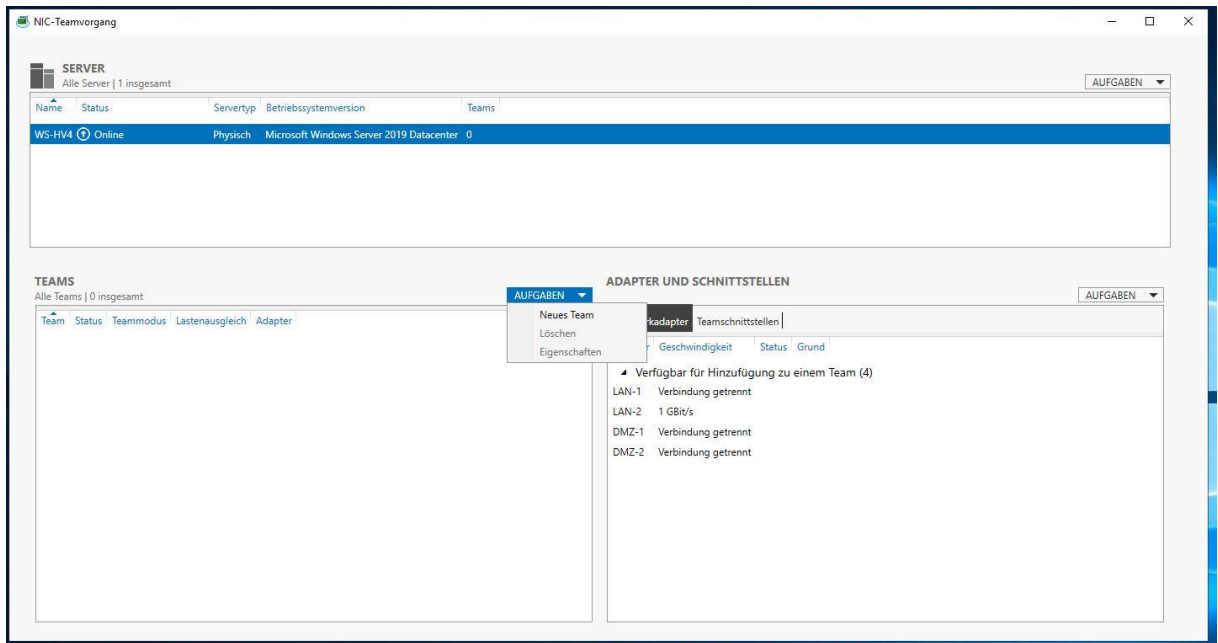
Dafür muss ich zunächst die physikalische Reihenfolge mit der logischen Reihenfolge abgleichen. Das geht recht einfach, indem ich ein Netzwerkkabel an einem Port herausziehe und prüfe, welcher Adapter als getrennt dargestellt wird. So kann ich die Zuweisung durch Umbenennen der Adapter vornehmen:



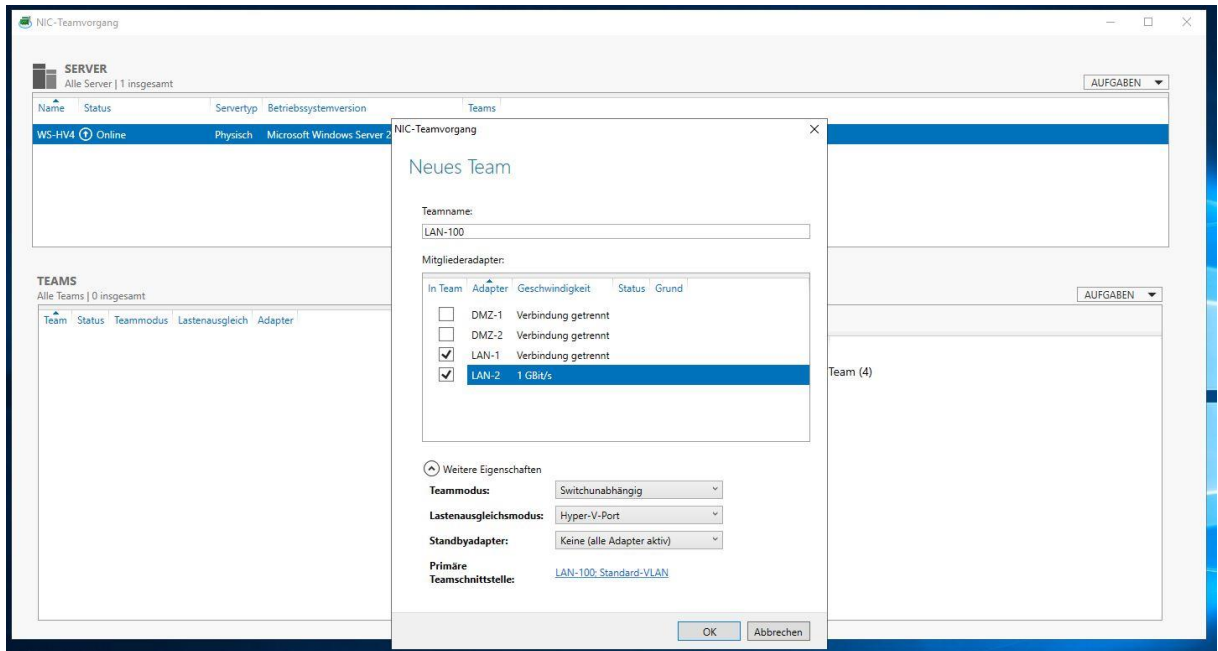
Jetzt kann ich die beiden Netzwerk-Teams bilden. Ich nutze dazu den Servermanager:



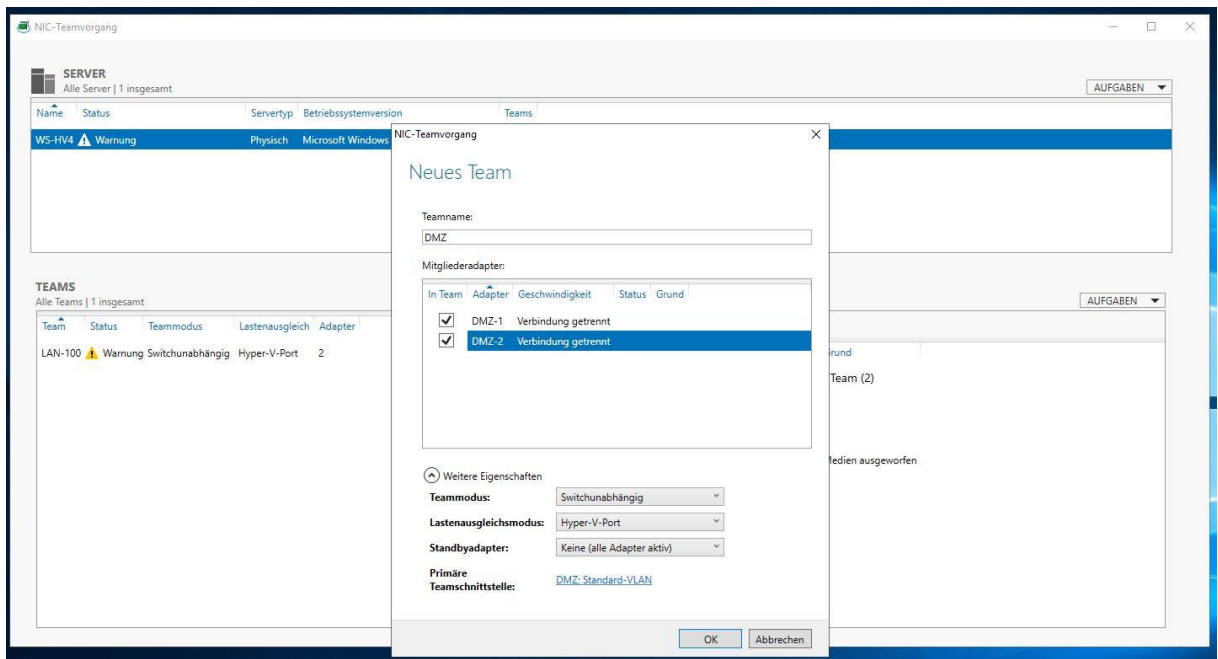
Der Prozess unterscheidet sich nicht von dem eines Windows Server 2016:



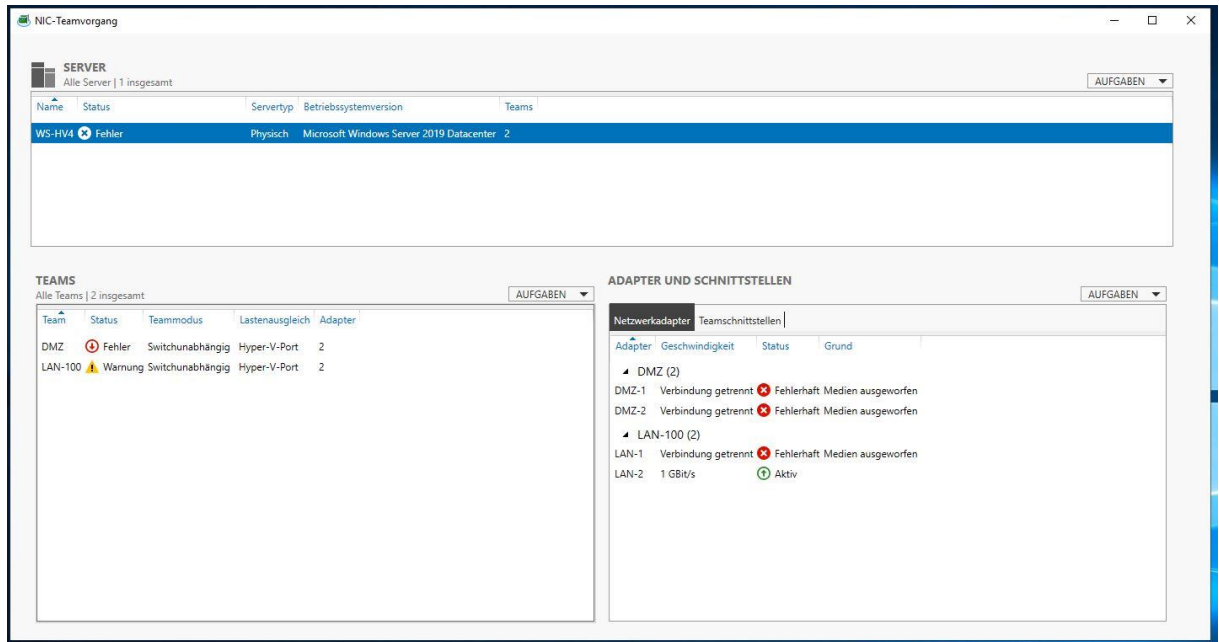
Ich wähle je Team die passenden Adapter aus und definiere den Anschluss als switchunabhängig. Mein Switch könnte LACP, aber dafür bin ich zu wenig Netzwerker. Und so passt es mir seit Windows Server 2012R2. Dazu optimiere ich das Team für die Verwendung vor einem Hyper-V-Switch:



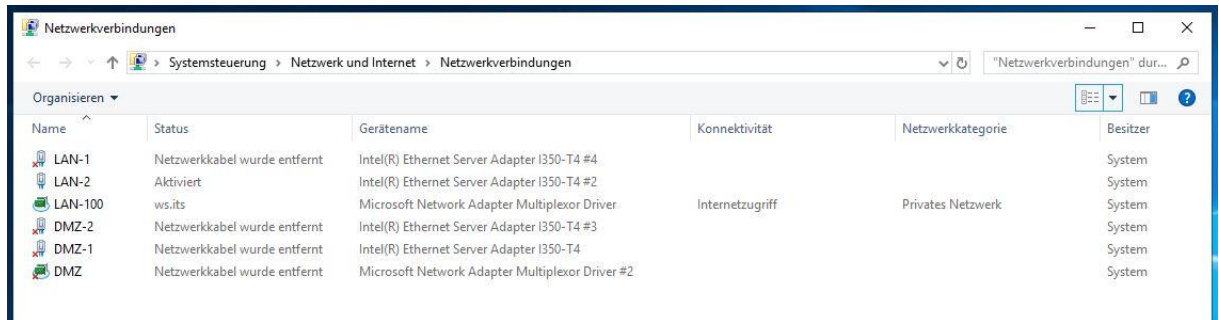
Das zweite Team bekommt die beiden verbleibenden Adapter zugewiesen:



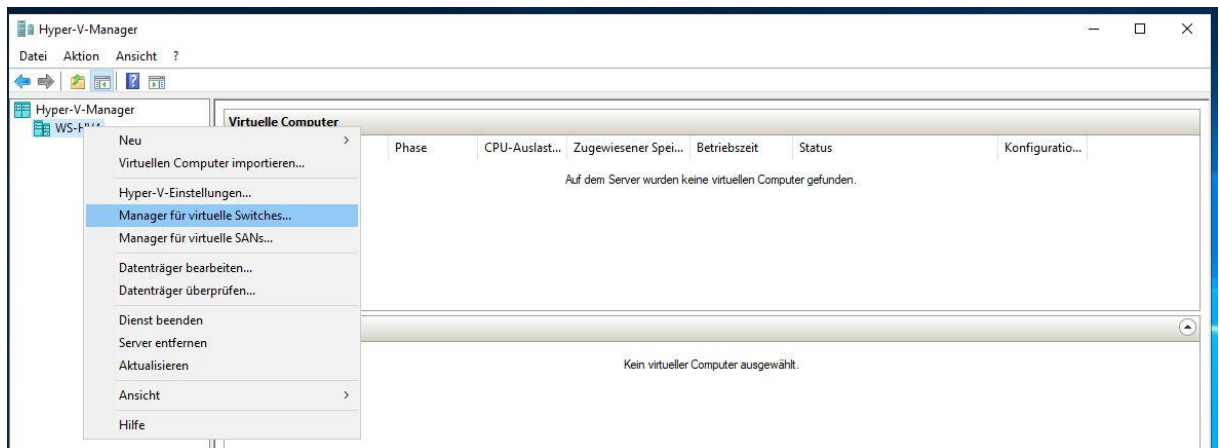
Da momentan nur ein Netzwerkkabel angeschlossen ist, meldet der Servermanager Verbindungsprobleme:



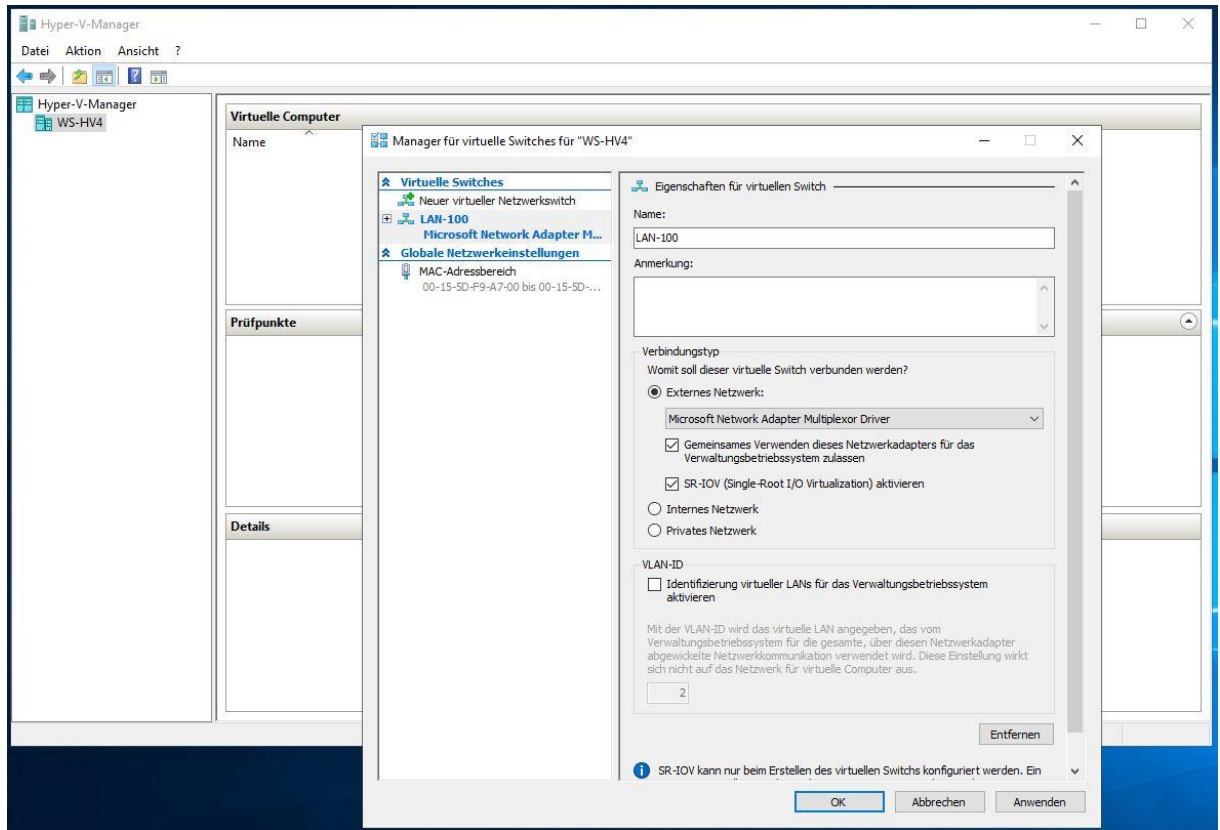
In der Netzwerkadapter-Ansicht der Systemsteuerung ergibt sich nun folgender Zwischenstand:



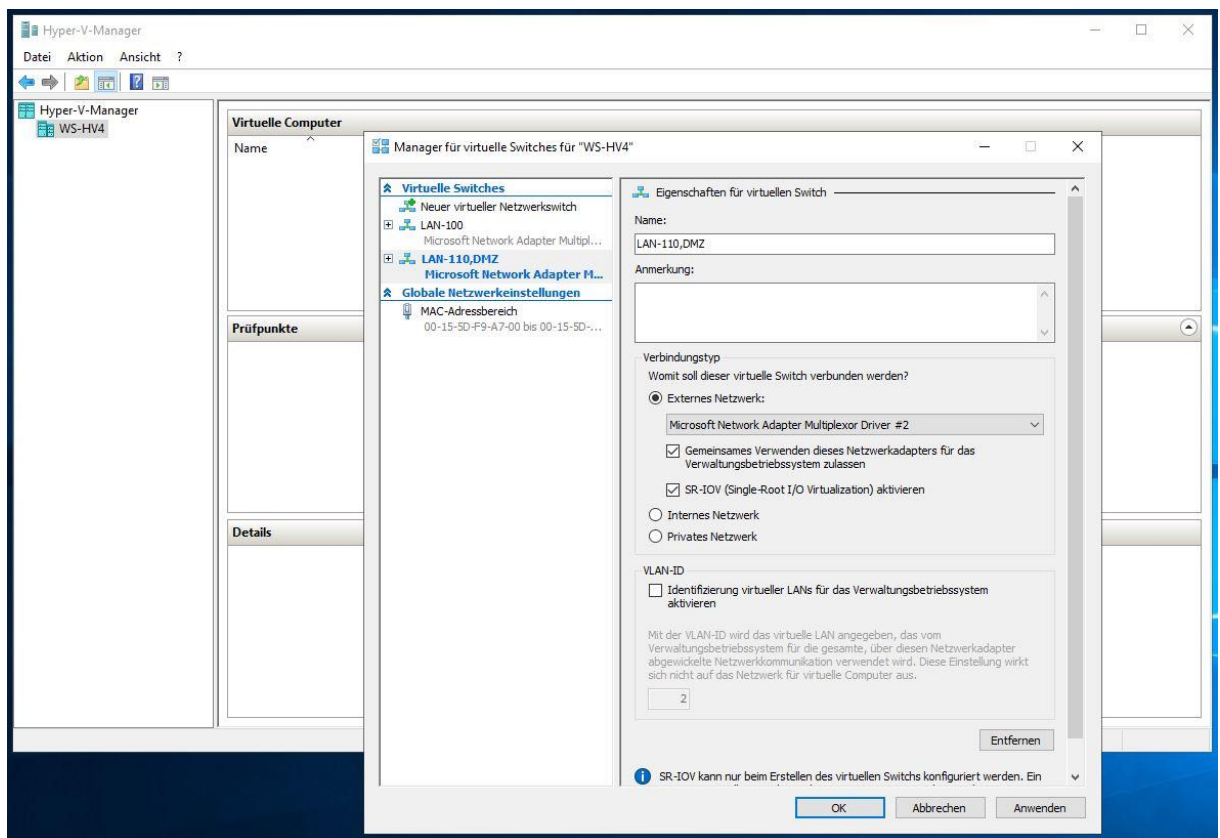
Der nächste Schritt führt mich in die Hyper-V-Managementkonsole. Dort erstelle ich nun 2 externe, virtuelle Switches, welche ich an die beiden Multiplexer-Teamadapter verweise:



Der erste Switch wird mein Servernetz abbilden. Das dazugehörige VLAN habe ich am realen Switch getaggt. Daher benötige ich hier keine Anpassung. Mein Hyper-V-Host soll das Netzwerk als Server ebenfalls verwenden. Daher aktiviere ich die Option „gemeinsame Verwendung“. Der physikalische Netzwerkadapter unterstützt SR-IOV. Diese Option kann ich also auch an den virtuellen Switch weiterreichen. Dies geht wie bei den vorherigen Hyper-V-Versionen nur bei der Erstellung des Switches:



Der zweite Switch wird analog aufgebaut. Die Zuweisung zum Team-Adapter kann über die dynamische Nummerierung korrekt vorgenommen werden. Dazu hilft es, die Netzwerkadapter in der Systemsteuerung zu suchen (ncpa.cpl):



Geschafft. Nun benötigt mein Server noch eine eigene, feste IPv4-Adresse in meinem Servernetz 192.168.100.0/24. Ich prüfe, welche laut DNS frei wäre. Dort wird die 192.168.100.14 nicht aufgeführt. Doch ist diese wirklich frei? Ausgehend

davon, dass alle Systeme online sind könnte man die IP einfach mal anpingen. Doch das dazugehörige ICMPv4-Protokoll wird gerne mal von den Firewalls geblockt. Valider finde ich daher die Sichtung des ARP-Caches unmittelbar nach einem Ping. Dieser speichert die Zuordnung zwischen IPv4 (OSI-Layer 3) und MAC-Adresse (OSI-Layer 2). Selbst mit aktiver Firewall muss ein System ARP-Requests beantworten. Wird also nach einem Ping die MAC-Adresse nicht im Cache gelistet, dann ist das System aus oder die IP ist nicht vergeben:

```

Auswählen C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\sysadm>nslookup 192.168.100.14
Server: UnKnown
Address: ::1

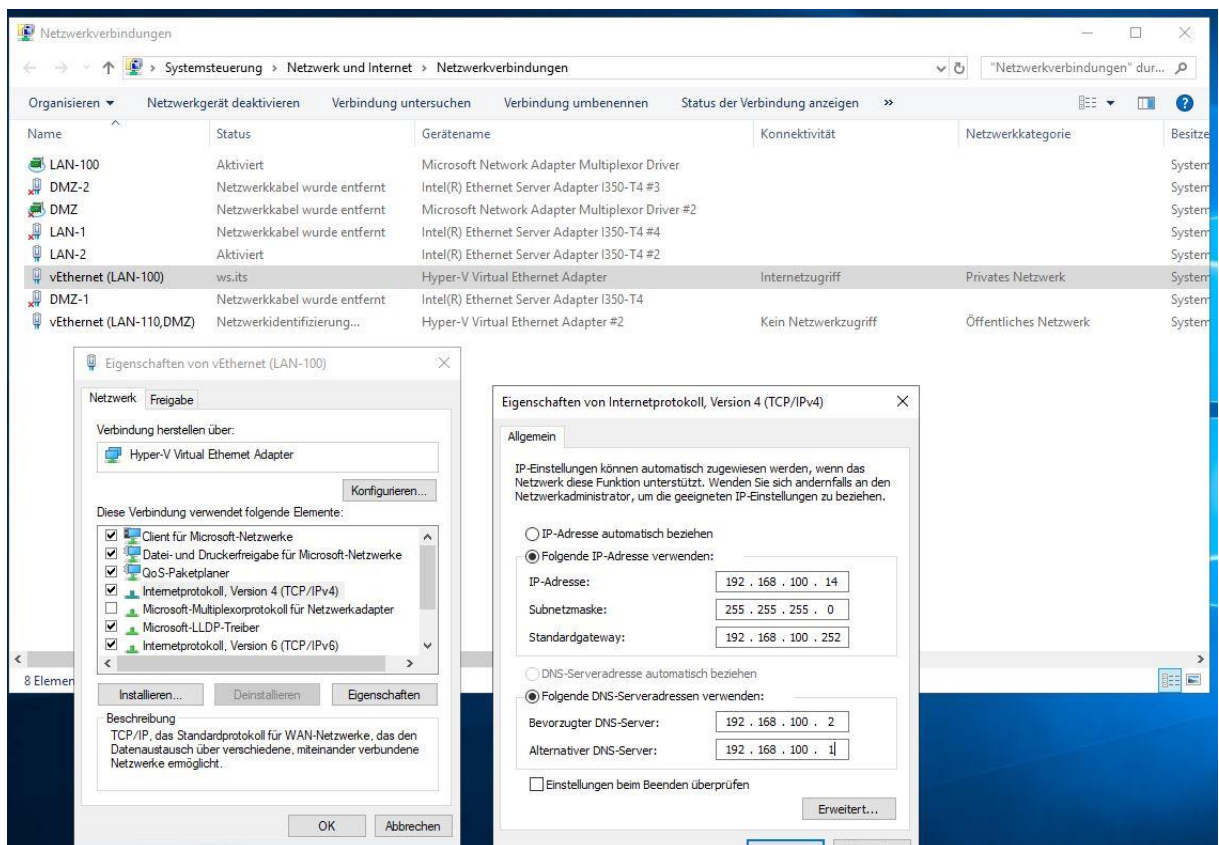
*** 192.168.100.14 wurde von UnKnown nicht gefunden: Non-existent domain.

C:\Users\sysadm>ping 192.168.100.14

Ping wird ausgeführt für 192.168.100.14 mit 32 Bytes Daten:
STRG-C
^C
C:\Users\sysadm>arp -a

Schnittstelle: 192.168.100.2 --- 0x2
Internetadresse      Physische Adresse      Typ
192.168.100.1        00-15-5d-64-bb-12      dynamisch
192.168.100.3        00-15-5d-64-bb-0f      dynamisch
192.168.100.4        00-15-5d-64-98-01      dynamisch
192.168.100.5        00-15-5d-64-b0-01      dynamisch
192.168.100.6        00-15-5d-64-98-00      dynamisch
192.168.100.7        00-15-5d-64-bb-13      dynamisch
192.168.100.9        00-13-3b-2f-97-d7      dynamisch
192.168.100.11       00-15-5d-64-bb-2e      dynamisch
192.168.100.12       00-15-5d-64-b0-04      dynamisch
192.168.100.13       00-15-5d-64-98-06      dynamisch
192.168.100.15       00-15-5d-64-bb-0f      dynamisch
192.168.100.17       00-15-5d-64-98-07      dynamisch
192.168.100.18       00-15-5d-64-b0-03      dynamisch
192.168.100.22       00-15-5d-64-b0-02      dynamisch
192.168.100.23       00-15-5d-64-bb-2c      dynamisch
192.168.100.41       a0-36-9f-8a-05-6d      dynamisch
192.168.100.152      a0-36-9f-8a-04-55      dynamisch
192.168.100.250      00-15-5d-64-bb-24      dynamisch
  
```

Laut meiner Dokumentation wurde die IP zuletzt von meinem WS-IPM (IPAM-Server) verwendet. Diesen habe ich bereits entfernt. Also besteht wenig Konfliktpotential bei der Wiederverwendung der IP-Adresse:



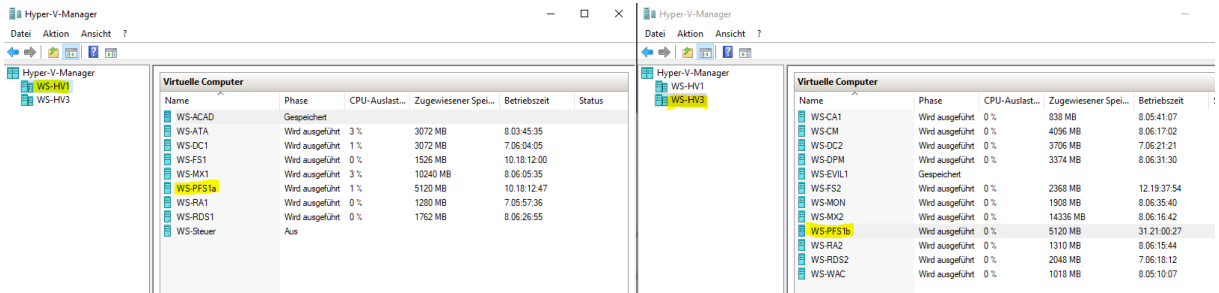
The screenshot shows the Windows Network Connections window. It lists several network adapters, including vEthernet adapters. The vEthernet (LAN-100) adapter is selected, and its properties are shown in a separate window. The properties window shows the network settings for the vEthernet adapter, including the IP address (192.168.100.14), subnet mask (255.255.255.0), and default gateway (192.168.100.252). The DNS server address is also set to 192.168.100.2.

Weiter geht es erst, nachdem der Storage im neuen Server bereitgestellt ist. Und da möchte ich eine NVMe aus dem alten Server weiterverwenden. Dazu muss ich also erst den alten Server abschalten.

Vorbereitung der Deaktivierung des alten Servers WS-HV1

PFSense-Maintenance

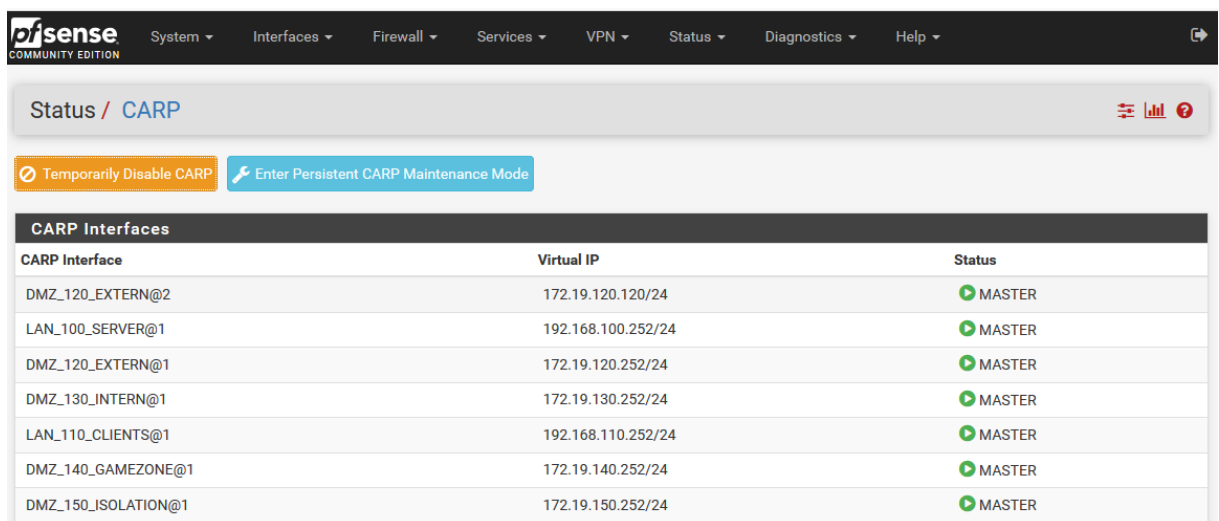
Noch läuft der alte Hyper-V-Host WS-HV1 im Hintergrund und seine VMs betreiben meine Infrastruktur. Darunter ist eine wichtige Backend-Komponente: meine zentrale Firewall-Lösung. Diese besteht aus 2 PFSense-Servern, die im Cluster meine virtuellen Netzwerke verbinden und schützen. Die WS-PFS1a auf dem alten Hyper-V-Host ist dabei der primäre Clusterknoten. Diese VM muss ich für den Transfer der „alten“ NVMe-Festplatte herunterfahren:



Name	Phase	CPU-Auslast...	Zugewiesener Spei...	Betriebszeit	Status
WS-ACAD	Gespeichert				
WS-ATA	Wird ausgeführt	3 %	3072 MB	8.03.45:35	
WS-DC1	Wird ausgeführt	1 %	3072 MB	7.06.04:05	
WS-FS1	Wird ausgeführt	0 %	1526 MB	10.18.12:00	
WS-MX1	Wird ausgeführt	3 %	10240 MB	8.06.05:35	
WS-PFS1a	Wird ausgeführt	1 %	5120 MB	10.18.12:47	
WS-RA1	Wird ausgeführt	0 %	1280 MB	7.05.57:36	
WS-RDS1	Wird ausgeführt	0 %	1762 MB	8.06.26:55	
WS-Steuer	Aus				

Name	Phase	CPU-Auslast...	Zugewiesener Spei...	Betriebszeit	Status
WS-CA1	Wird ausgeführt	0 %	838 MB	8.05.41:07	
WS-CM	Wird ausgeführt	0 %	4096 MB	8.06.17:02	
WS-DC2	Wird ausgeführt	0 %	3706 MB	7.06.21:21	
WS-DPM	Wird ausgeführt	0 %	3374 MB	8.06.31:30	
WS-EVIL1	Gespeichert				
WS-FS2	Wird ausgeführt	0 %	2368 MB	12.19.37:54	
WS-MON	Wird ausgeführt	0 %	1908 MB	8.06.25:40	
WS-MX2	Wird ausgeführt	0 %	14336 MB	8.06.16:42	
WS-PFS1b	Wird ausgeführt	0 %	5120 MB	31.21.00:27	
WS-RA2	Wird ausgeführt	0 %	1310 MB	8.06.15:44	
WS-RDS2	Wird ausgeführt	0 %	2048 MB	7.06.18:12	
WS-WAC	Wird ausgeführt	0 %	1018 MB	8.05.10:07	

In der PFSense gibt es einen Modus für die geplante Wartung. Dabei werden alle Funktionen auf das Backupsystem (WS-PFS1b auf dem anderen Hyper-V-Host) übertragen:



System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help

Status / CARP

Temporarily Disable CARP | Enter Persistent CARP Maintenance Mode

CARP Interface	Virtual IP	Status
DMZ_120_EXTERN@2	172.19.120.120/24	MASTER
LAN_100_SERVER@1	192.168.100.252/24	MASTER
DMZ_120_EXTERN@1	172.19.120.252/24	MASTER
DMZ_130_INTERN@1	172.19.130.252/24	MASTER
LAN_110_CLIENTS@1	192.168.110.252/24	MASTER
DMZ_140_GAMEZONE@1	172.19.140.252/24	MASTER
DMZ_150_ISOLATION@1	172.19.150.252/24	MASTER

Die Option ist einen Klick entfernt:

CARP Interface	Virtual IP	Status
DMZ_120_EXTERN@2	172.19.120.120/24	BACKUP
LAN_100_SERVER@1	192.168.100.252/24	BACKUP
DMZ_120_EXTERN@1	172.19.120.252/24	BACKUP
DMZ_130_INTERN@1	172.19.130.252/24	BACKUP
LAN_110_CLIENTS@1	192.168.110.252/24	BACKUP
DMZ_140_GAMEZONE@1	172.19.140.252/24	BACKUP
DMZ_150_ISOLATION@1	172.19.150.252/24	BACKUP

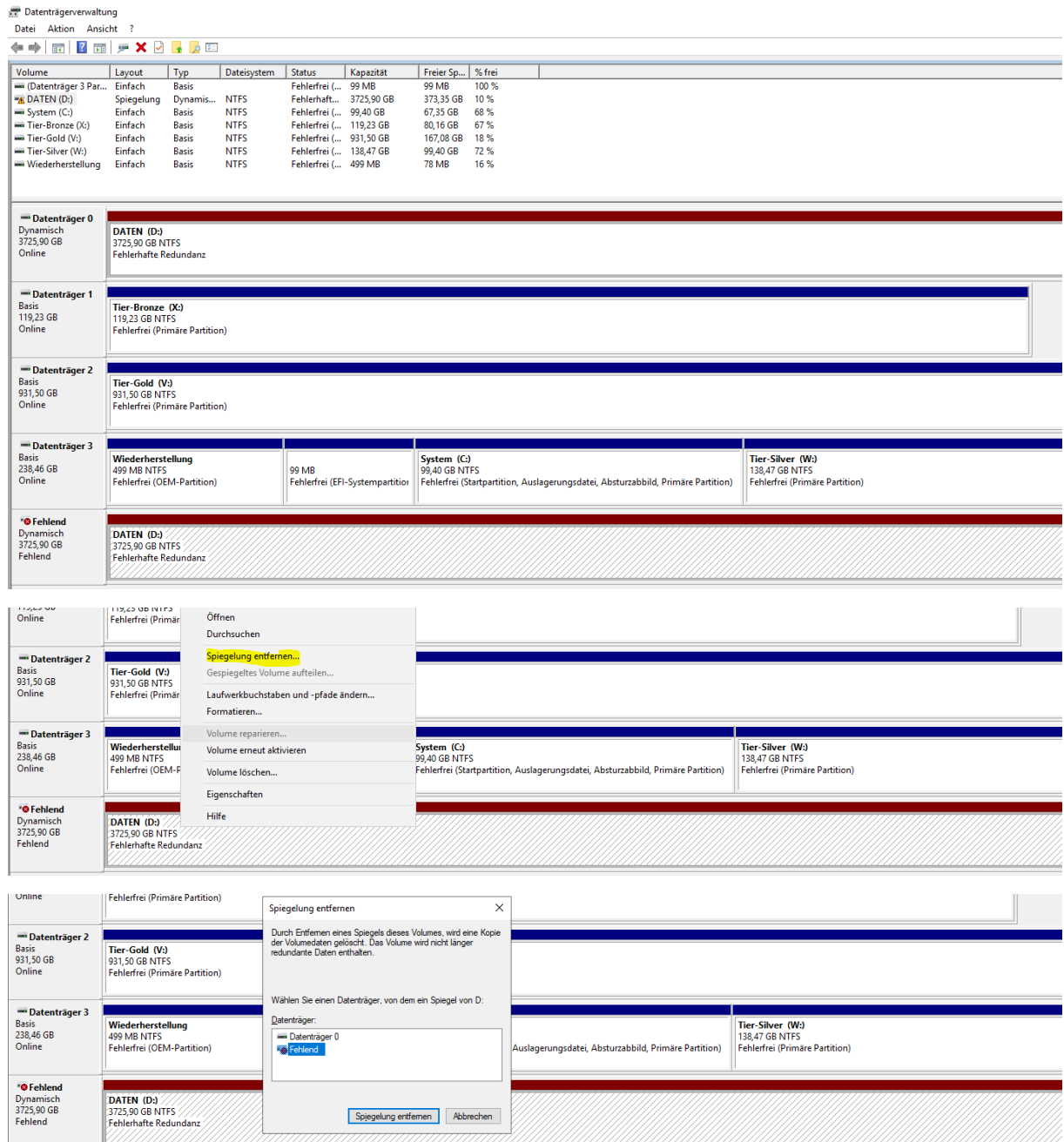
Nun kann ich die VM ohne Netzwerkprobleme einfach herunterfahren.

Monitoring

Mein Monitoring wird von einem PRTG-Server übernommen. Dieser hat natürlich etliche Sensoren auf meinem Hyper-V-Host konfiguriert bekommen. Damit es beim Abschalten des Servers keine Dauermeldungen gibt, pausiere ich alle Sensoren:

Entfernung einer defekten Festplatte

Im alten Server ist ein RAID1 aus 2x 2TB Festplatten verbaut. Vor einigen Tagen hat eine davon ihren Dienst quittiert. Da beide Platten die gleiche, lange Laufzeit hinter sich haben, möchte ich die noch intakten Dateien auf den neuen Server kopieren. Damit es beim Datentransfer keine Probleme gibt, entferne ich die defekte Platte aus dem Software-RAID1:



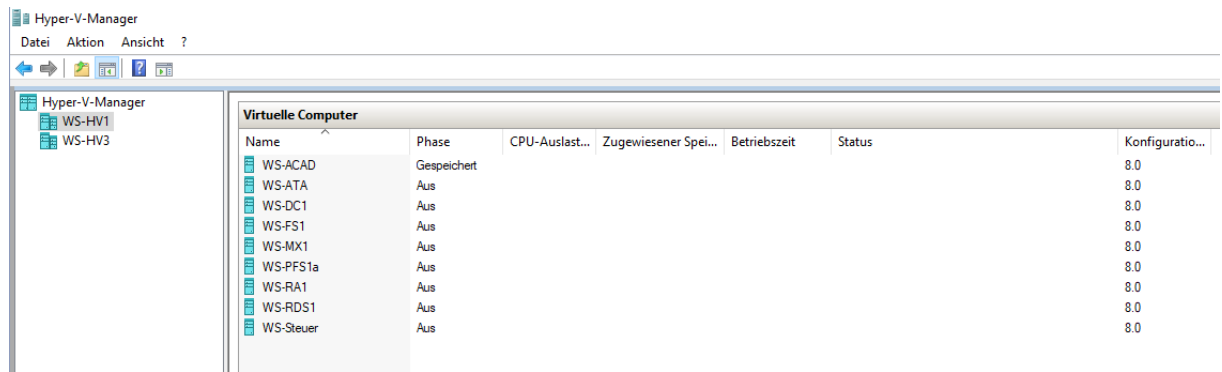
The screenshot shows the Windows Server 2019 Disk Management console. At the top, there is a table listing disks with columns for Volume, Layout, Typ, Dateisystem, Status, Kapazität, Freier Sp..., and % frei. Below the table, the disk configuration is shown in a graphical view with columns for Datenträger 0, 1, 2, 3, and Fehlend. A context menu is open over the 'Datenträger 2' (Tier-Gold (V)) disk, with the option 'Spiegelung entfernen...' highlighted. A dialog box titled 'Spiegelung entfernen' is displayed in the foreground, asking to select a mirror for the 'DATEN (D:)' volume. The 'Fehlend' disk is selected as the mirror.

Volume	Layout	Typ	Dateisystem	Status	Kapazität	Freier Sp...	% frei
(Datenträger 3 Par...	Einfach	Basis		Fehlerfrei (...)	99 MB	99 MB	100 %
DATEN (D:)	Spiegelung	Dynamis...	NTFS	Fehlerhaft...	3725,90 GB	373,35 GB	10 %
System (C:)	Einfach	Basis	NTFS	Fehlerfrei (...)	99,40 GB	67,35 GB	68 %
Tier-Bronze (X:)	Einfach	Basis	NTFS	Fehlerfrei (...)	119,23 GB	80,16 GB	67 %
Tier-Gold (V:)	Einfach	Basis	NTFS	Fehlerfrei (...)	931,50 GB	167,08 GB	18 %
Tier-Silver (W:)	Einfach	Basis	NTFS	Fehlerfrei (...)	138,47 GB	99,40 GB	72 %
Wiederherstellung	Einfach	Basis	NTFS	Fehlerfrei (...)	499 MB	78 MB	16 %

Herunterfahren der VMs auf dem alten Server

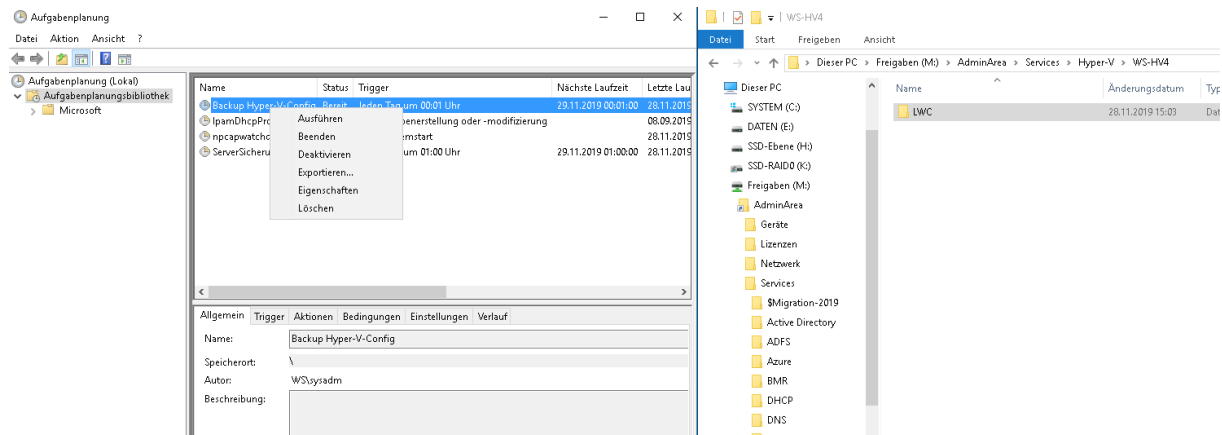
Die wichtigen Dienste in meiner Infrastruktur sind automatisch hochverfügbar. So habe ich auf beiden Hyper-V-Hosts je einen Domain Controller mit DNS und DHCP, einen Fileserver mit DFS-Namespaces und DFS-Replication, einen Exchange Server mit DAG und einen HA-Proxy in den PfSense. Die anderen Services, wie Microsoft ATA, Remote Desktop Services und Remote Access spielen hier keine Rolle. Die können auch mal nicht verfügbar sein.

Somit ist für meinen Betrieb alles gewährleistet. Ich schalte alle VMs auf dem alten Server aus. Nach einigen Minuten habe ich alle Dienste geprüft. Mein Mailsystem ist erreichbar. Ebenso die Dateidienste. Und anmelden kann ich mich auch.



Auslesen von Informationen

Auf dem alten Server sind noch 2 Aufgaben integriert. Diese kann ich hier exportieren und danach auf dem neuen Server importieren:



Auf dem Systemlaufwerk existieren noch einige Dateien und Ordner. Diese kopiere ich auf meinen Dateiserver. Es sind großteils nur Logfiles und einige Scripts. Vielleicht kann ich die noch einmal gebrauchen.

Mehr gibt es hier nicht. Den alten Server schalte ich jetzt aus.

Konfiguration von WS-HV4

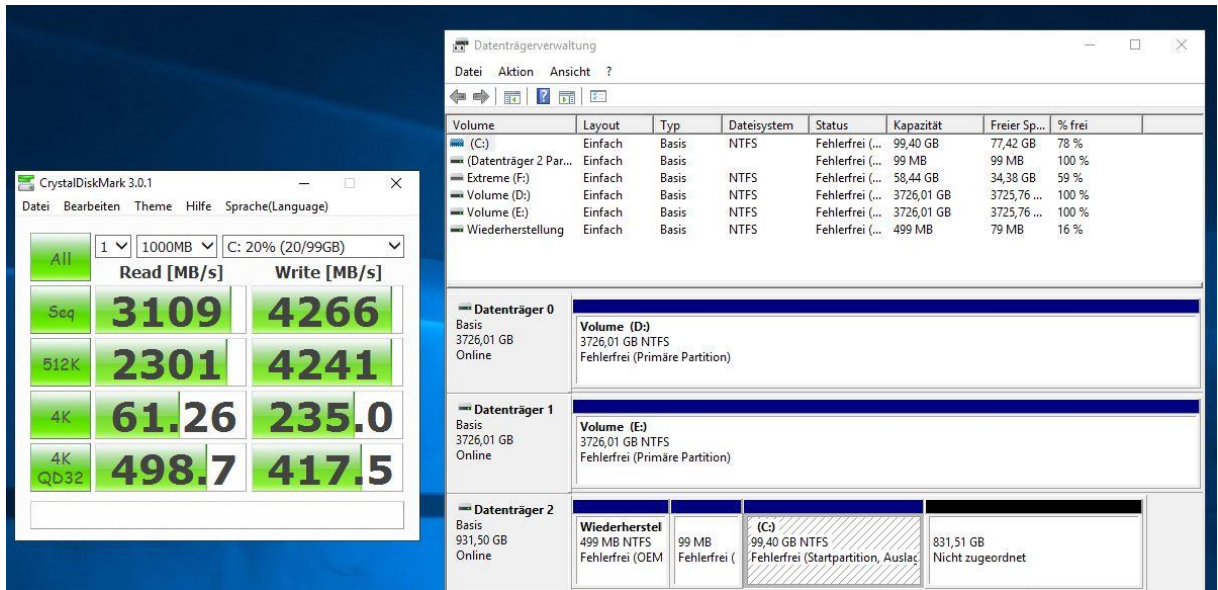
Einbau des neuen Servers

Die „alte“ NVMe-Platte entferne ich aus dem ausgeschalteten WS-HV1 und verbaue sie im neuen Server WS-HV4. Damit sind alle Hardware-Arbeiten abgeschlossen und der Server darf nun in seinen Slot in meinem Serverschrank einziehen. Hier kann ich alle 4 Netzwerkkarten anschließen.

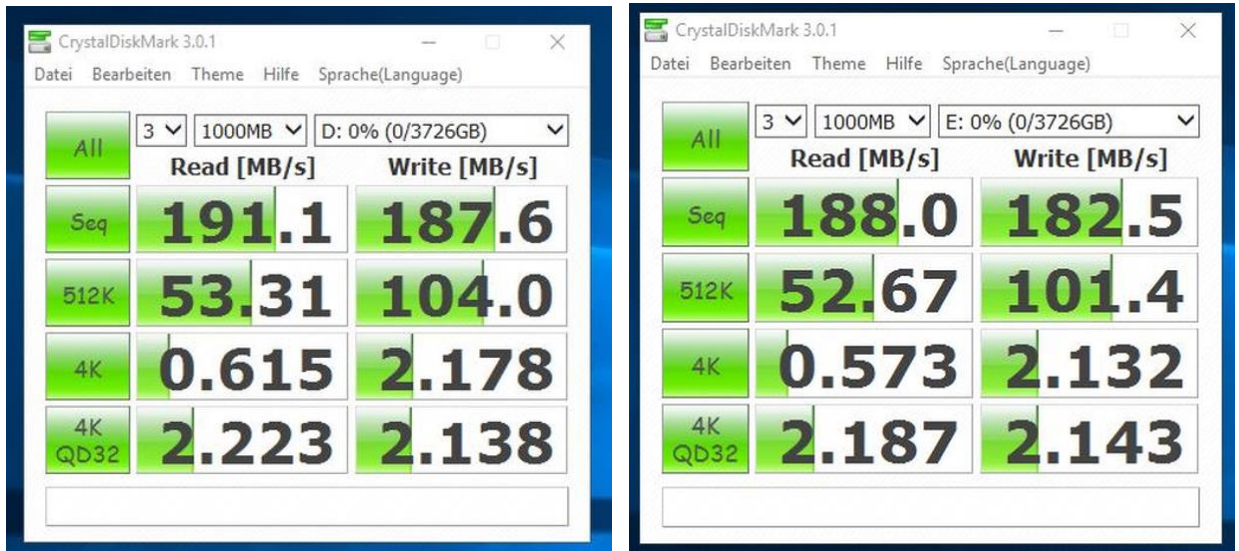
Die temporäre Grafikkarte, die mir den lokalen Zugriff z.B. für das UEFI ermöglichte, baue ich vorher noch aus. Damit spare ich Strom und Abwärme.

Konfiguration des Storage

Ich beginne mit einem Performance-Test der neuen PCI-Gen4-NVMe. Laut Hersteller sollen bis zu 5GB/s sequentiell erreicht werden:



Naja. Da wäre noch Luft nach oben. Aber für eine Handvoll VMs ist es bestimmt ausreichend. Und was liefern die neuen 4TB-Platten? Die sind laut Hersteller für 24/7-Betrieb von Videoüberwachungssystemen geeignet:



Eine Platte scheint etwas langsamer zu sein. Aber für meine statischen, großen Files reicht die Performance allemal.

Es wird Zeit, den Storage für meine Zielplattform einzurichten. Aktuell sind diese Festplatten und Volumes vorhanden:

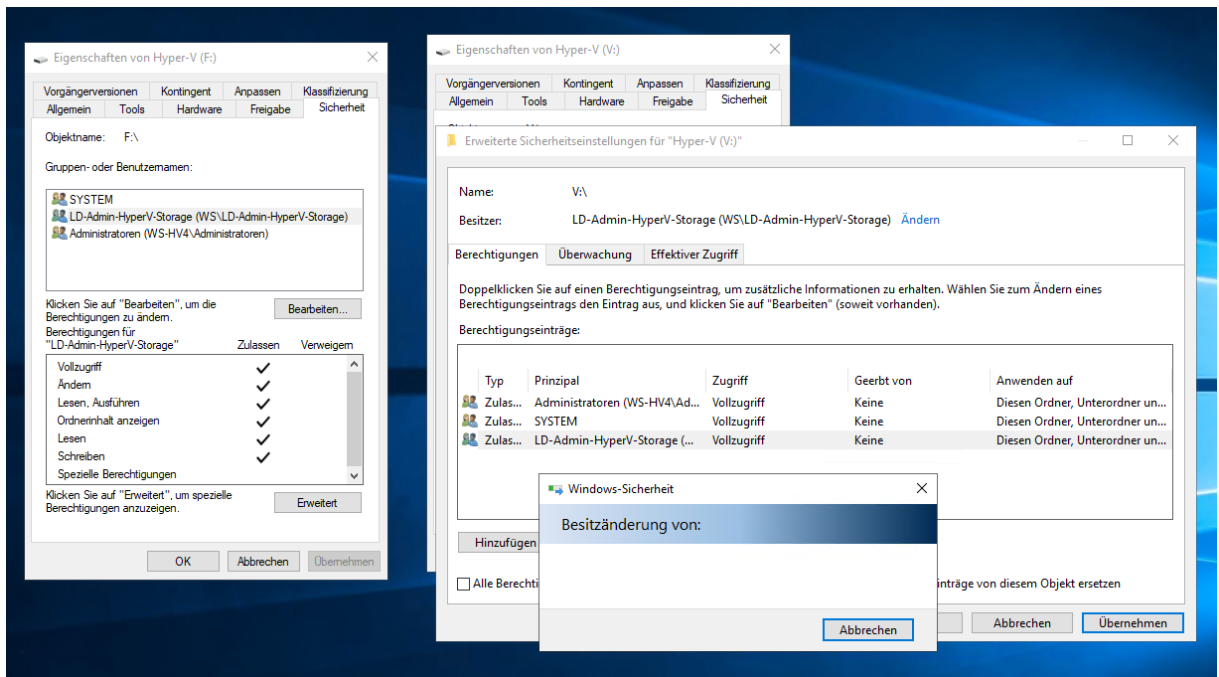
Volume	Layout	Typ	Dateisystem	Status	Kapazität	Freier Sp...	% frei
(C:)	Einfach	Basis	NTFS	Fehlerfrei (...)	99,40 GB	77,34 GB	78 %
(Datenträger 2 Par...)	Einfach	Basis	NTFS	Fehlerfrei (...)	99 MB	99 MB	100 %
Hyper-V (F:)	Einfach	Basis	NTFS	Fehlerfrei (...)	447,00 GB	156,34 GB	35 %
Hyper-V (V:)	Einfach	Basis	NTFS	Fehlerfrei (...)	831,51 GB	831,35 GB	100 %
Volume (D:)	Einfach	Basis	NTFS	Fehlerfrei (...)	3726,01 GB	3725,76 ...	100 %
Volume (E:)	Einfach	Basis	NTFS	Fehlerfrei (...)	3726,01 GB	3725,76 ...	100 %
Wiederherstellung	Einfach	Basis	NTFS	Fehlerfrei (...)	499 MB	79 MB	16 %

Datenträger	Speicher	Layout	Typ	Dateisystem	Status	Kapazität	Freier Sp...	% frei
Datenträger 0	Basis 3726,01 GB Online	Volume (D:)	Basis	NTFS	Fehlerfrei (Primäre Partition)	3726,01 GB	3725,76 ...	100 %
Datenträger 1	Basis 3726,01 GB Online	Volume (E:)	Basis	NTFS	Fehlerfrei (Primäre Partition)	3726,01 GB	3725,76 ...	100 %
Datenträger 2	Basis 931,50 GB Online	Wiederherstellung	Basis	NTFS	Fehlerfrei (OEM-Partition)	499 MB	79 MB	16 %
						99 MB	99 MB	100 %
						99,40 GB	77,34 GB	78 %
						447,00 GB	156,34 GB	35 %
						831,51 GB	831,35 GB	100 %
						3726,01 GB	3725,76 ...	100 %
						3726,01 GB	3725,76 ...	100 %
						499 MB	79 MB	16 %
Datenträger 3	Basis 447,01 GB Online	Hyper-V (F:)	Basis	NTFS	Fehlerfrei (Primäre Partition)	447,00 GB	156,34 GB	35 %

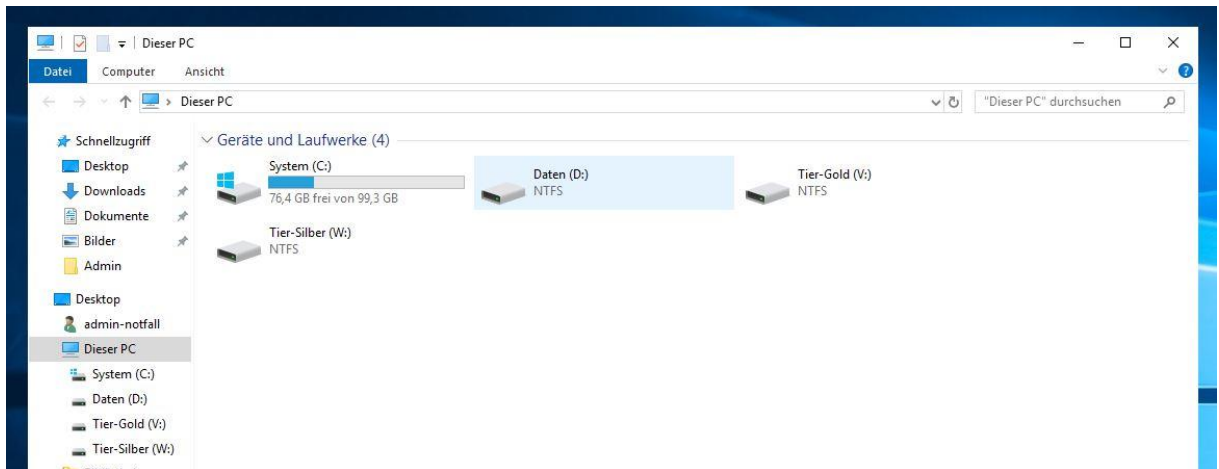
Also kann es nun an die Einrichtung der Speicher gehen. Folgendes Layout möchte ich abbilden:

Disk	Typ	Größe	Redundanz	Volumes
Disk 0	HDD	4TB	Mirror (Pool)	Daten (D:) → große VHDX
Disk 1	HDD	4TB	Mirror (Pool)	
Disk 2	NVMe PCI-Gen4	1TB	Single	System (C:) TIER-GOLD (V:) → VMs
Disk 3	NVMe PCI-Gen3	500GB	Single	TIER-SILBER (W:) → VMs

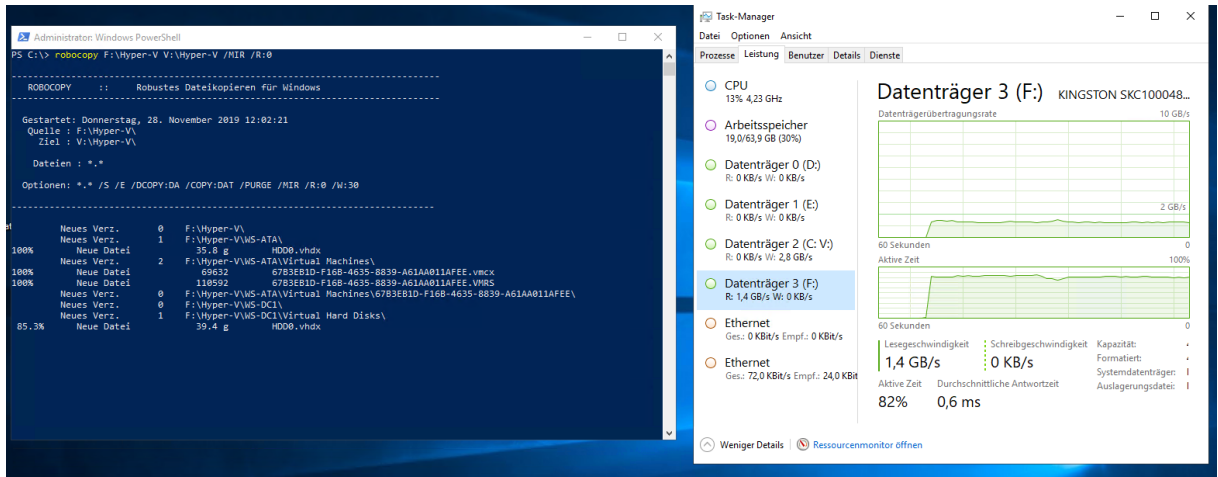
Die beiden großen Volumes D: und E: habe ich zum Testen der neuen Platten erstellt. Die Installation des neuen Servers habe ich auf die schnelle PCI-Gen4 Platte gelenkt. Hinter der Systempartition ist noch etlicher Speicher frei. Hier erstelle ich die neue Partition für meine VMs. Die zweite NVMe bringt schon ein Volume mit. Da liegen die alten VMs drauf. Ich beginne mit der neuen Partition auf der schnellen NVMe (Disk 2). Ich arbeite gerne mit Role-Based-Access-Control. Mein Ziel ist beim Hyper-V, dass ich auch als Administrator nicht ohne Weiteres auf die Datenspeicher der VMs zugreifen kann. Dieses Recht möchte ich bei Bedarf zusätzlich gewähren. Dafür editiere ich die Sicherheitsbeschreibungen meiner Daten-Partitionen. Die Gruppe „LD-Admin-HyperV-Storage“ hatte ich bereits im Active Directory für meine alten Server erstellt:



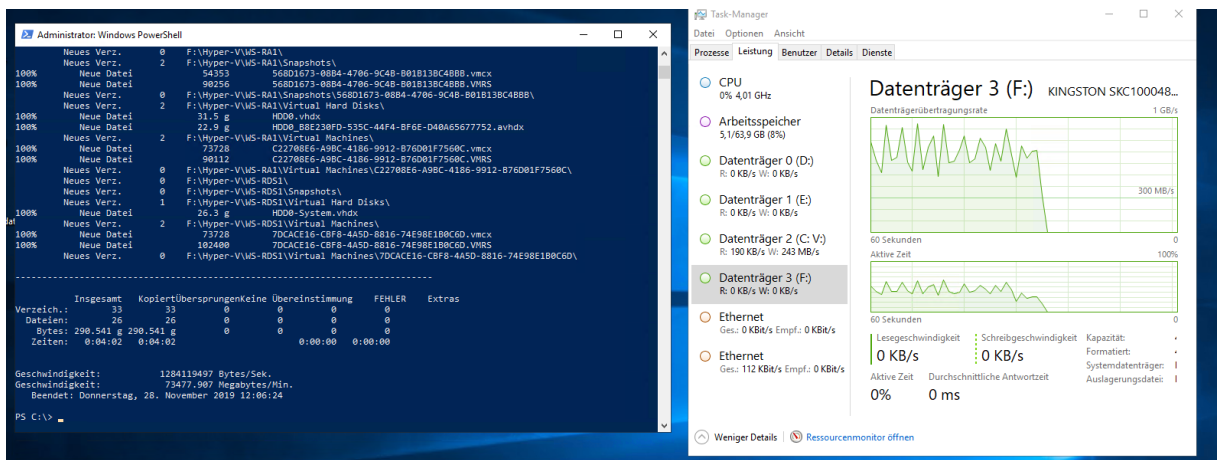
OK, ein User mit lokal administrativen Rechten kann einfach den Besitz übernehmen und sich so selber Zugriff verschaffen. Aber zum einen bin ICH der Administrator und es geht mir auch nicht um direkte administrative Tasks, sondern um z.B. eingeschleppte Schadsoftware. Diese könnte Daten, die direkt erreichbar sind einfach verschlüsseln. Ob die Aktion „Besitz übernehmen“ auch zum Portfolio des Schadcodes gehört? So schaut es nach der Einrichtung der Berechtigungen aus (Das Bild wurde später erstellt, aber hier passt es ganz gut rein):



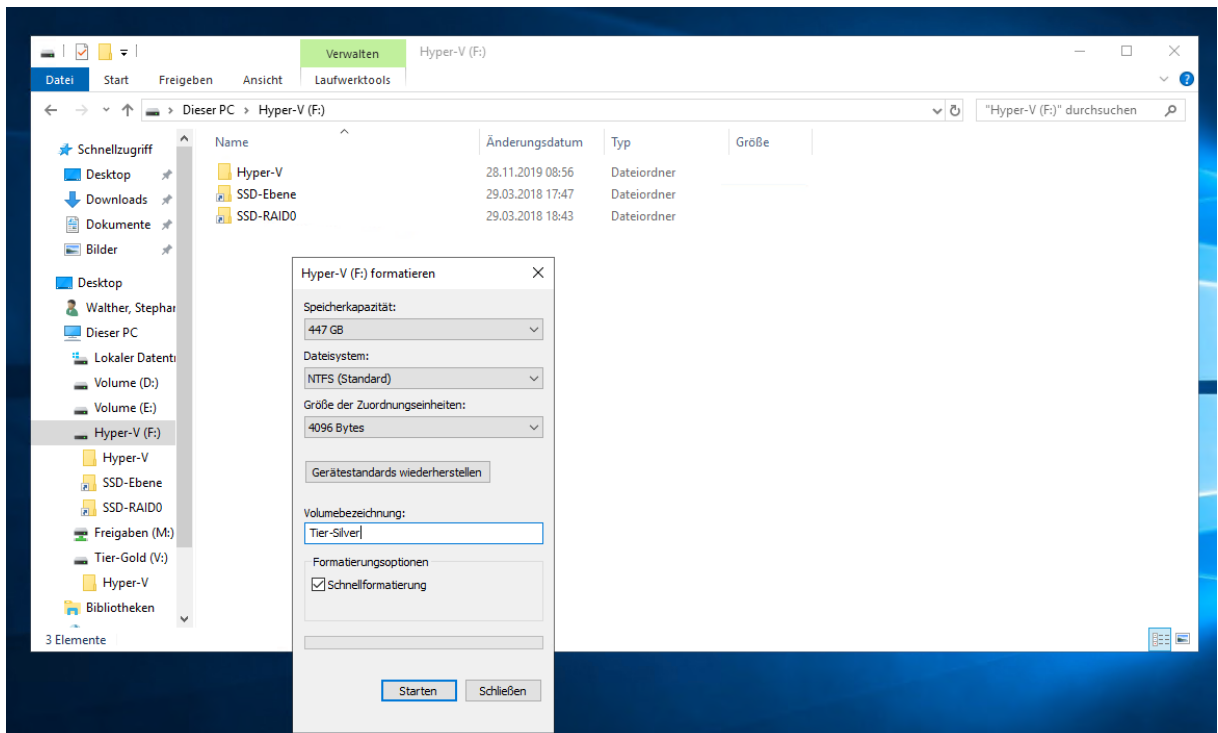
Nun kopiere ich die VMs von der alten auf die neue NVMe. Robocopy ist da immer noch ungeschlagen. Die Performance ist wie erwartet recht hoch. Leider bremst die alte NVMe den Transfer etwas aus:



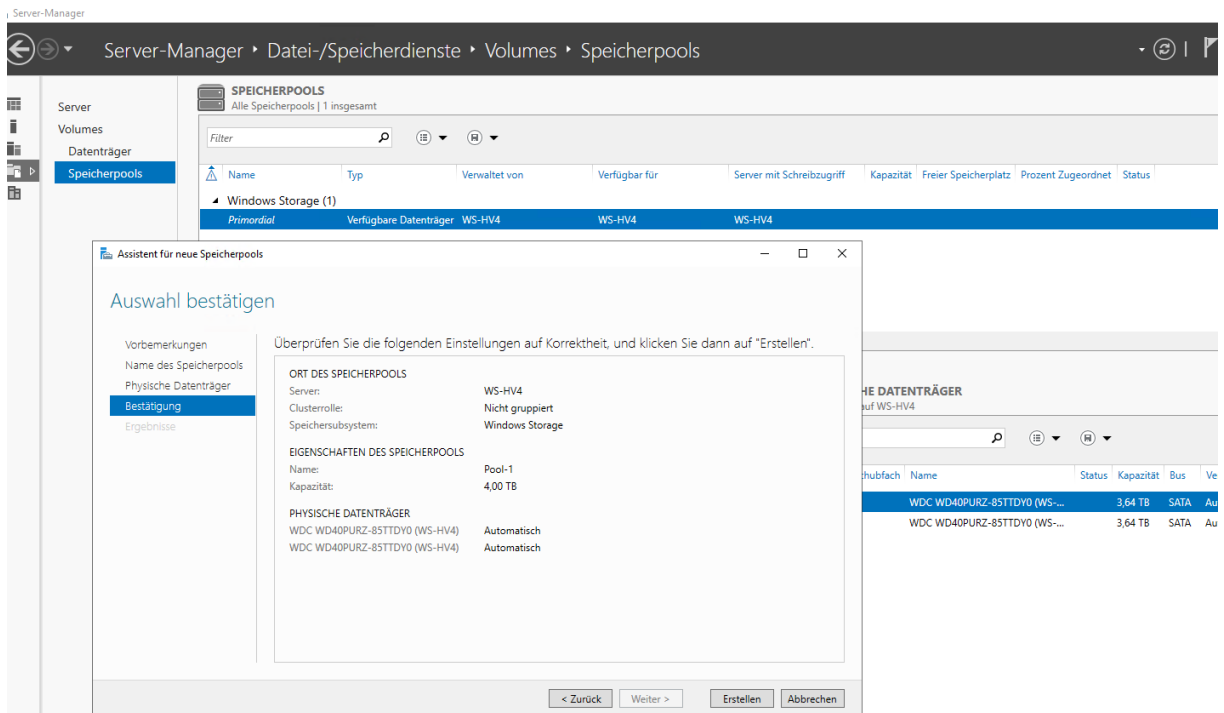
Aber im Schnitt 72GB/Min (1,2GB/S) ist doch nicht schlecht.



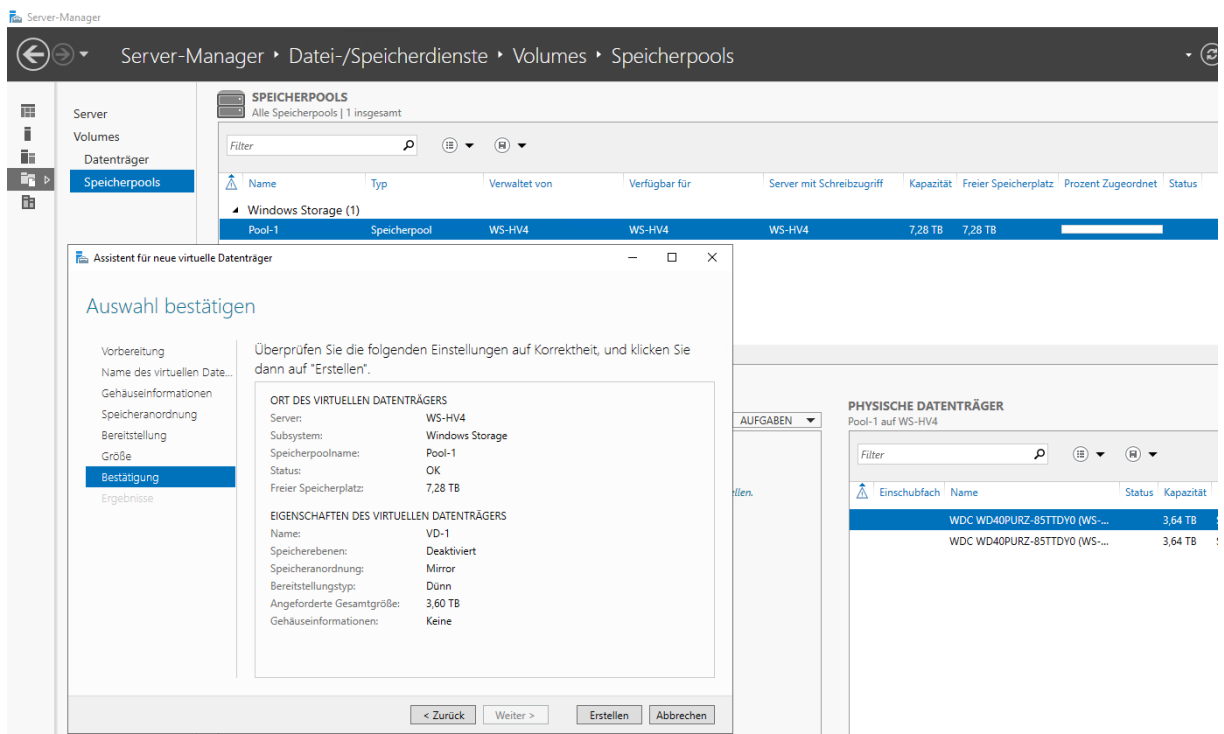
Die alte NVMe (Disk 3) ist nun frei. Für eine Bereinigung verwende ich eine Formatierung. Dabei passe ich auch gleich den Volume-Bezeichner an (TIER-SILBER):



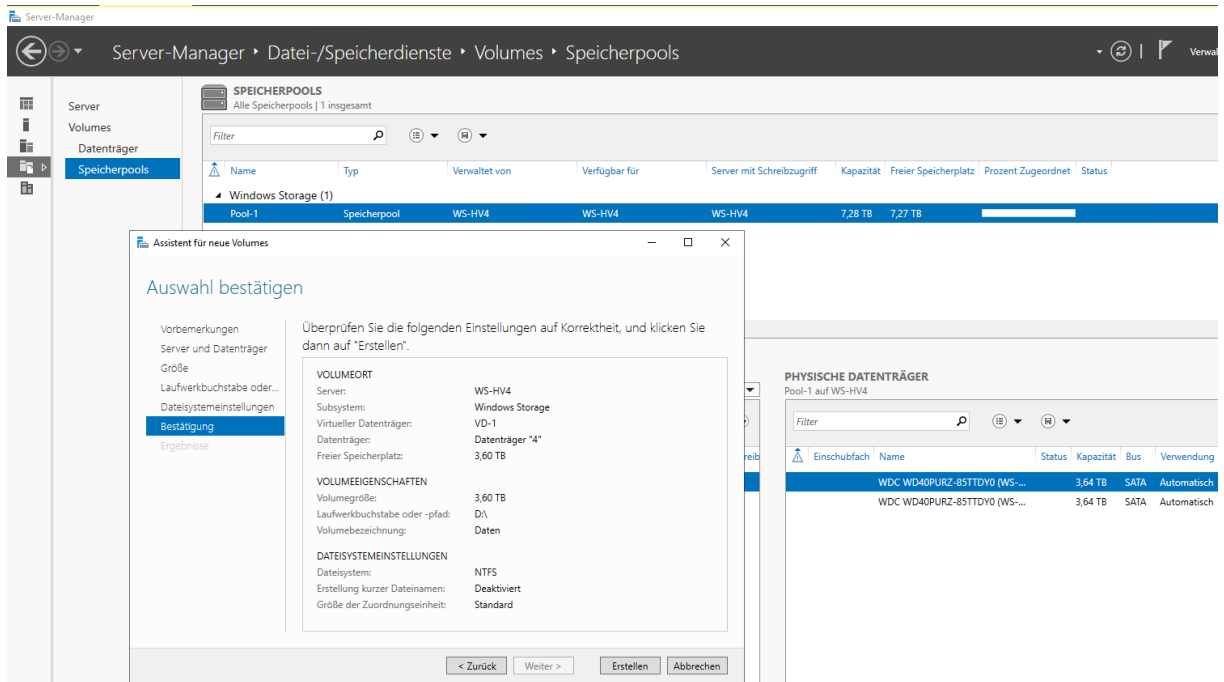
Nun entferne ich die beiden Test-Volumes auf den normalen 4TB-Platten (Disk 0 und 1). Damit werden sie frei für einen Speicherpool. Diesen erstelle ich im Servermanager:



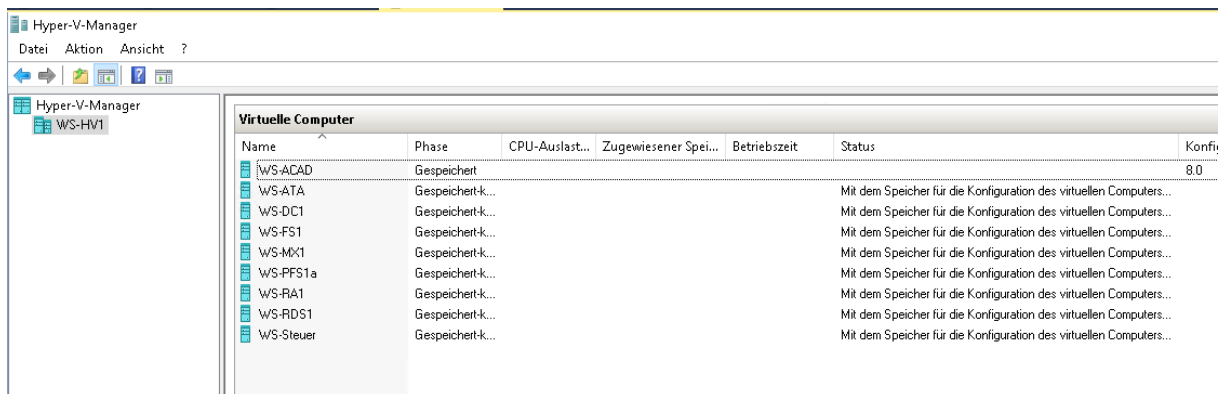
Der Pool umfasst beide 4TB-Platten. Darauf erstelle ich eine etwas kleinere, gespiegelte vDisk:



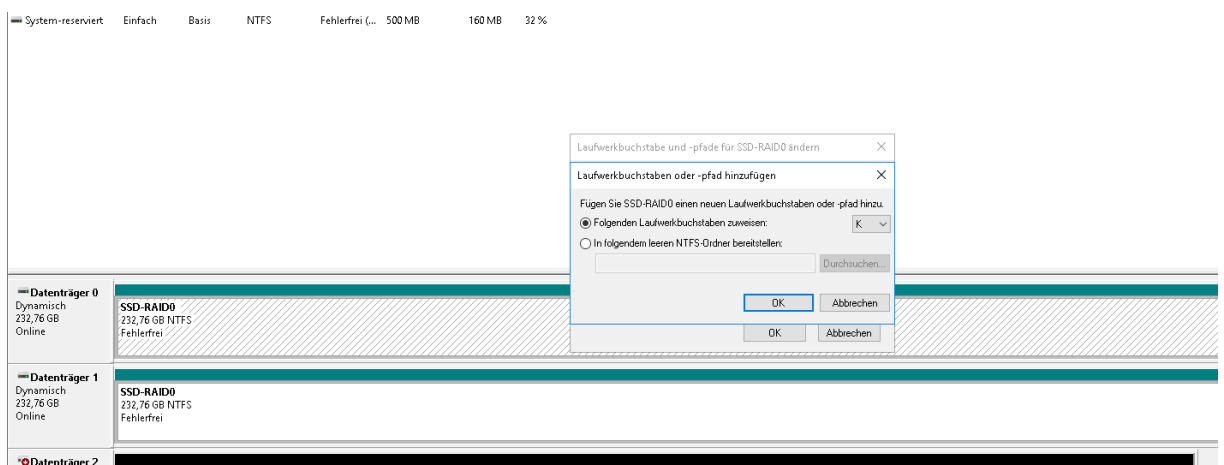
Und auf dieser vDisk formatiere ich ein Volume mit ausreichenden Speicher für meine großen Dateien:



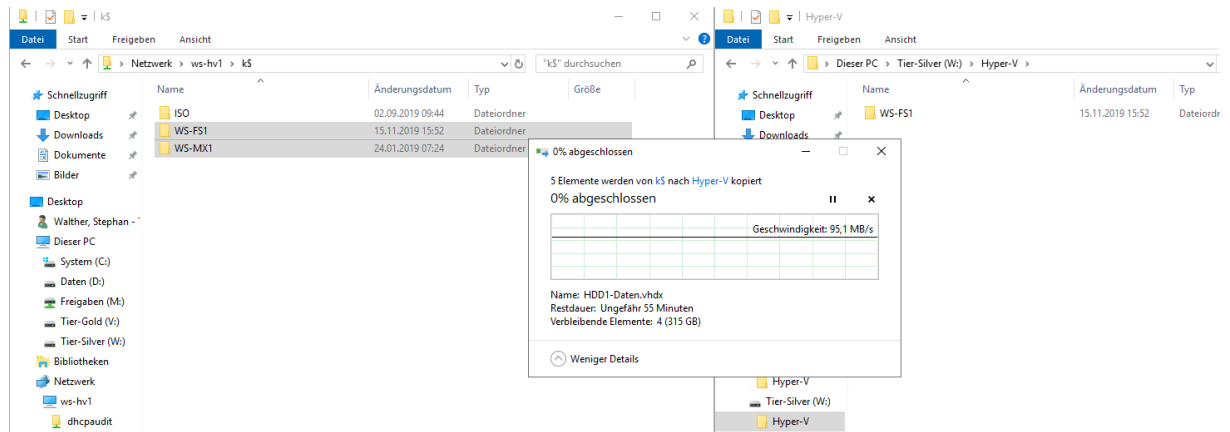
Da die alte NVMe aber damals schon zu klein wurde, lagerte ich einige VHDX-Dateien meiner VMs auf andere Datenträger aus. Diese Dateien möchte ich auf den neuen NVMe-Riegel kopieren. Dafür starte ich den alten Server wieder und stelle einen Zugriff zu den alten Datenträgern her. Im Hyper-V mault er, dass er die VMs nicht finden kann. Klar: Die VM-Dateien lagen auf der ausgebauten NVMe-Platte:



Die anderen Volumes hatte ich mit Mount-Points bereitgestellt. Da vergeb ich jetzt temporär Laufwerksbuchstaben:



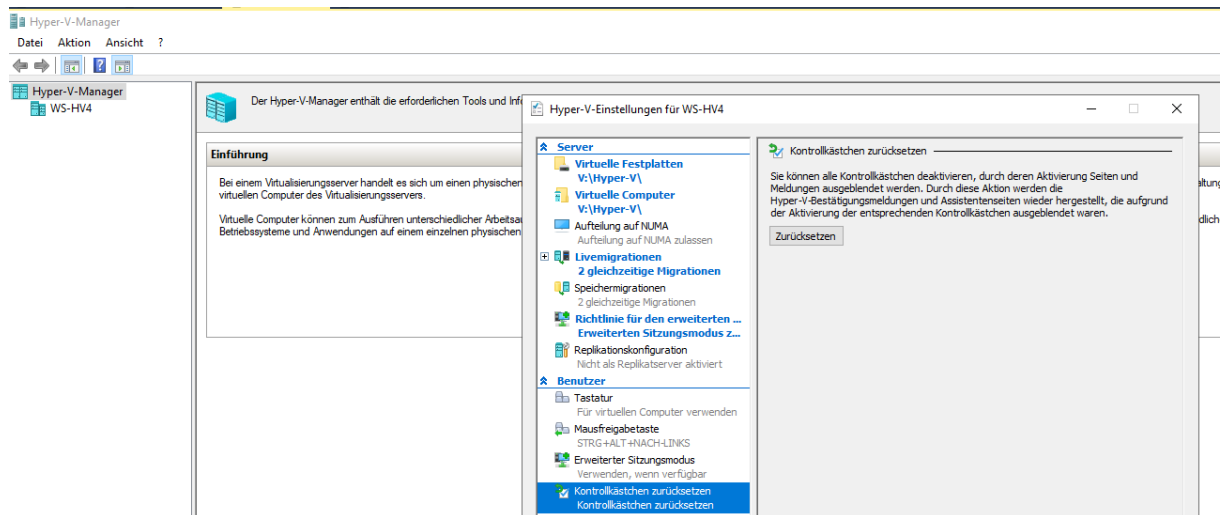
Und jetzt kann ich die fehlenden Dateien meiner VMs auf den neuen Server über das Netzwerk kopieren:



Nach einiger Zeit sind alle Dateien an ihren neuen Speicherplätzen. Bis dahin mach ich eine Pause.

Konfiguration des Hyper-V

Bevor die VMs in den neuen Hyper-V importiert werden können, muss ich diesen noch fertig einrichten. Dazu zählen einige generelle Settings:



Viel wichtiger für die Migration ist aber die Konfiguration im Active Directory. Ich möchte gerne virtuelle Maschinen ausgeschaltet von einem Hyper-V-Host zum anderen migrieren. Dafür stellt Microsoft die Option „LiveMigration“ zur Verfügung. Und diese verlangt eine Authentifizierung. Dabei kann CredSSP oder Kerberos verwendet werden. Da meine administrativen Konten aber Mitglieder in der Gruppe „Protected Users“ sind, muss ich Kerberos verwenden („Protected Users verhindert die Verwendung von CredSSP, WDigest und NTLM. Da bleibt nur Kerberos.) Für Kerberos muss aber vorher im Active Directory die Constrained Delegation eingerichtet werden:

Active Directory-Benutzer und -Computer

Active Directory-Benutzer und -Computer [WS-DC2.ws.its]

Name	Typ	Beschreibung
WS-HV1	Computer	
WS-HV2	Computer	
WS-HV3	Computer	
WS-HV4	Computer	

Eigenschaften von WS-HV3

Die Delegation sollte vorsichtig angewendet werden, da sie Diensten ermöglicht, Vorgänge im Namen anderer Benutzer auszuführen.

Computer bei Delegierungen nicht vertrauen
 Computer bei Delegierungen aller Dienste vertrauen (nur Kerberos)
 Computer bei Delegierungen angegebener Dienste vertrauen
 Nur Kerberos verwenden
 Beliebiges Authentifizierungsprotokoll verwenden

Dienste, für die dieses Konto delegierte Anmeldeinformationen verwenden kann:

Diensttyp	Benutzer oder Comp...	Port	Dienstname
cifs	WS-HV2.ws.its		
cifs	WS-HV1.ws.its		
Microsoft Virt...	WS-HV2.ws.its		
Microsoft Virt...	WS-HV1.ws.its		

Erweitert

Diese Einstellungen müssen je Server im Tab „Delegation“ definiert werden. Wichtig ist dabei, dass nicht „bedingungslos“ (unconstrained), sondern nur nach der Einhaltung von Bedingungen (constrained) die Anmeldeinformationen delegiert werden dürfen. Die Bedingungen sind die benannten Services CIFS und „Microsoft Virtual System Migration Service“ zum Zielsystem:

Active Directory-Benutzer und -Computer

Active Directory-Benutzer und -Computer [WS-DC2.ws.its]

Name	Typ	Beschreibung
WS-HV1	Computer	
WS-HV2	Computer	
WS-HV3	Computer	
WS-HV4	Computer	

Eigenschaften von WS-HV3

Die Delegation sollte vorsichtig angewendet werden, da sie Diensten ermöglicht, Vorgänge im Namen anderer Benutzer auszuführen.

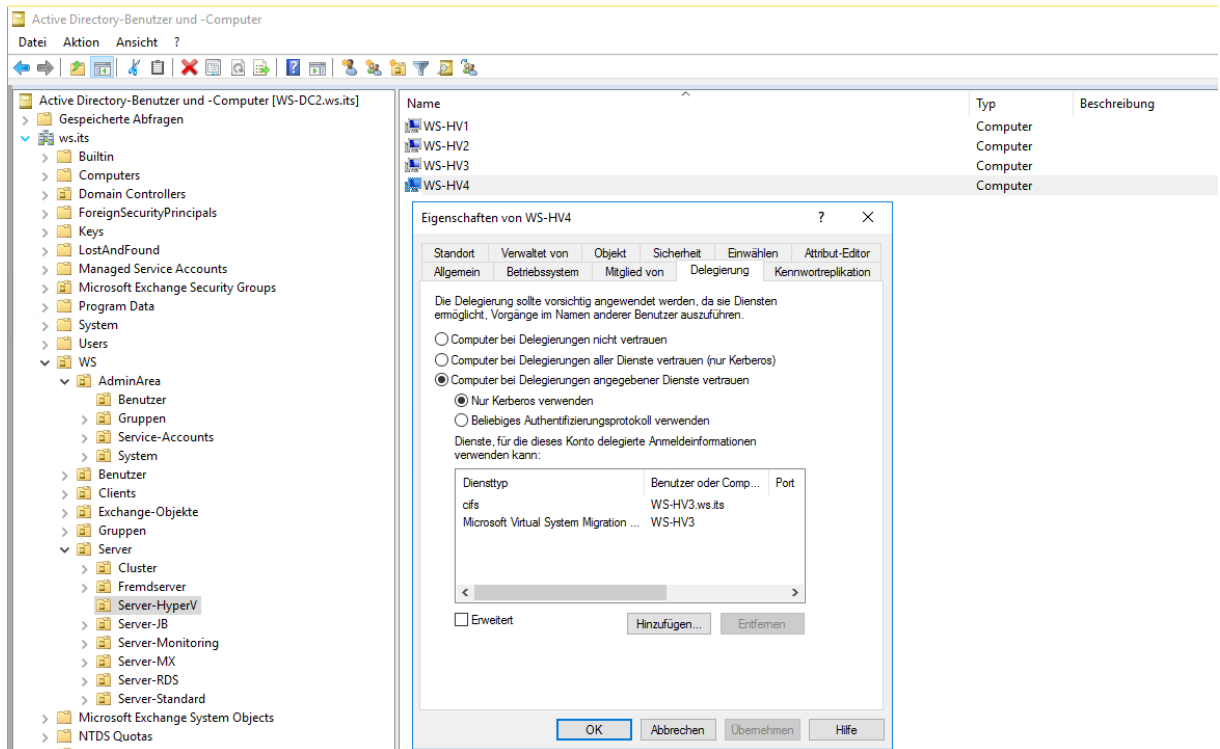
Computer bei Delegierungen nicht vertrauen
 Computer bei Delegierungen aller Dienste vertrauen (nur Kerberos)
 Computer bei Delegierungen angegebener Dienste vertrauen
 Nur Kerberos verwenden
 Beliebiges Authentifizierungsprotokoll verwenden

Dienste, für die dieses Konto delegierte Anmeldeinformationen verwenden kann:

Diensttyp	Benutzer oder Comp...
cifs	WS-HV4
Microsoft Virtual System Migration Service	WS-HV4

Erweitert

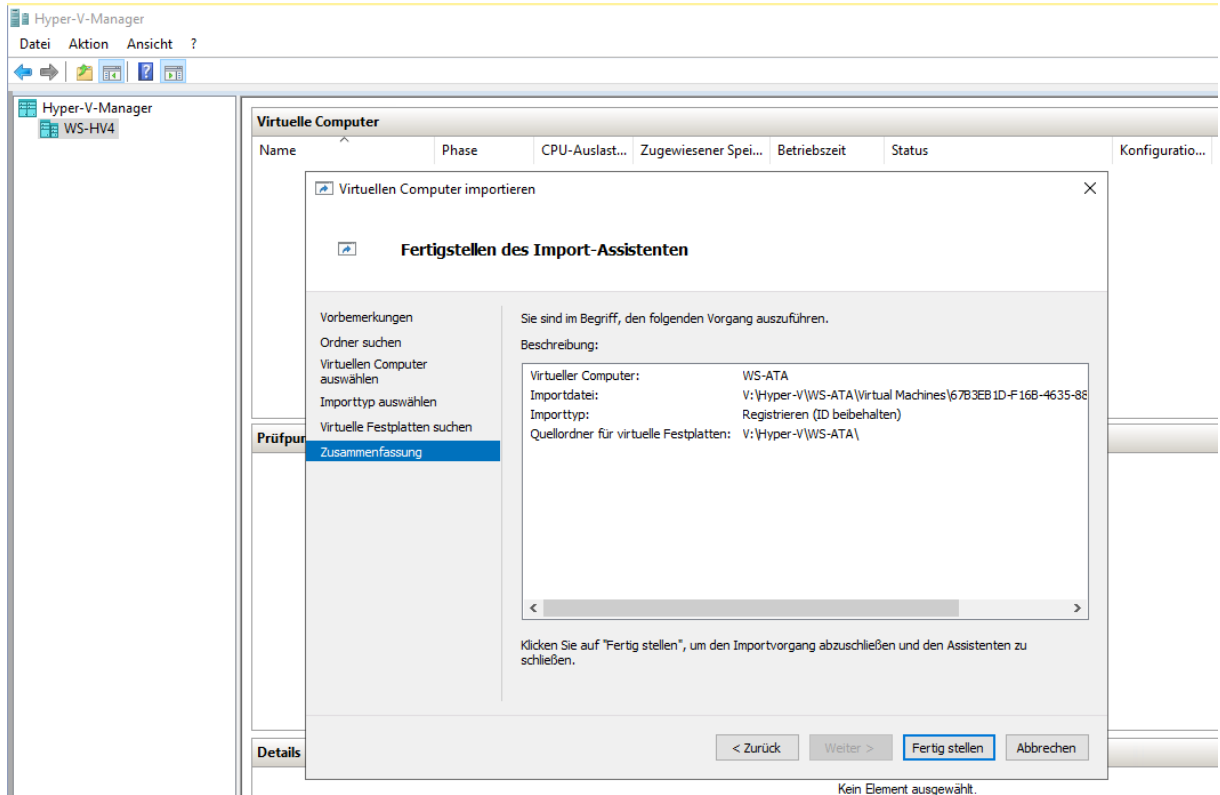
Und wie eben schon erwähnt, soll die Verschiebung auch in die Gegenrichtung möglich sein:



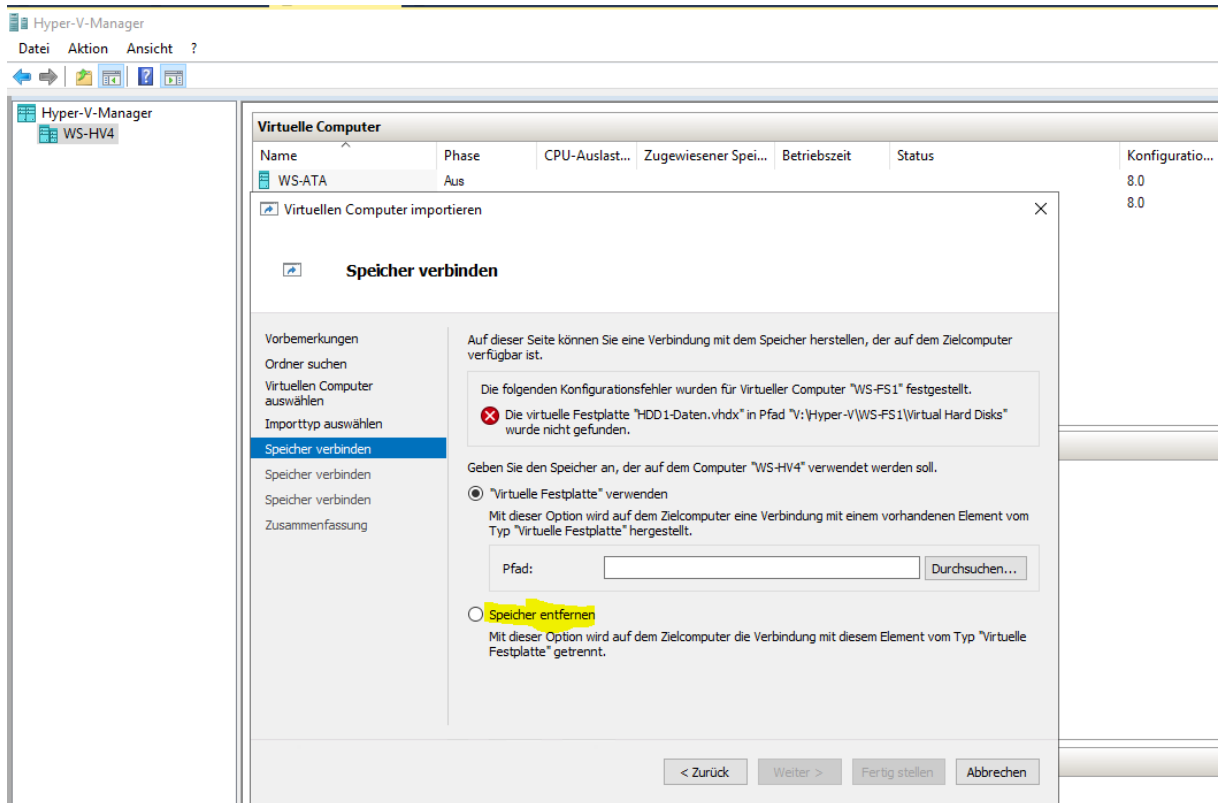
Das ist ein einmaliger Prozess. Mit der gegenseitigen Delegation kann ich VMs hin und wieder zurück verschieben.

Import der VMs

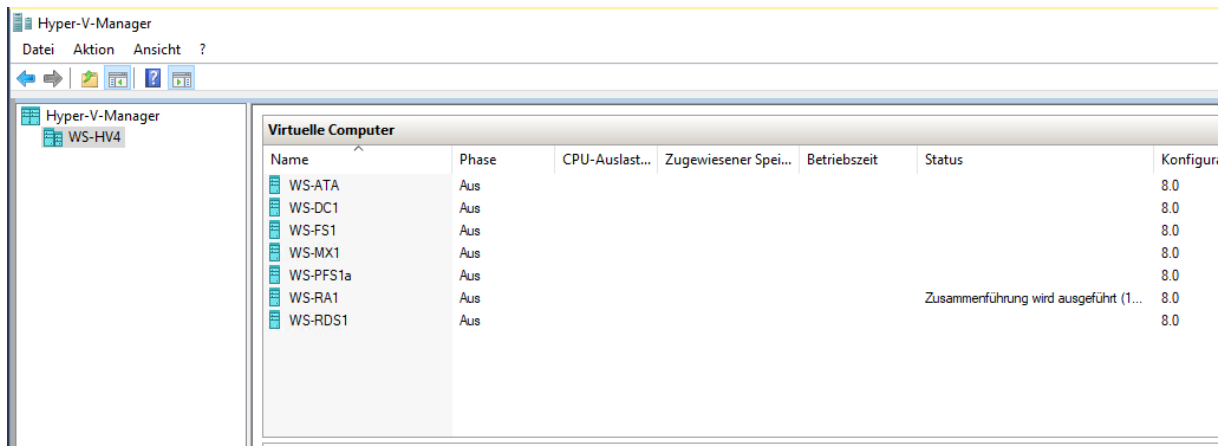
Die paar VMs importiere ich mit der MMC. Warum? Weil ich etliche Pfade für mein Redesign angepasst habe. Im GUI-Wizzard fragt das System einfach danach. In der PowerShell müsste ich jede Konfiguration manuell anpassen:



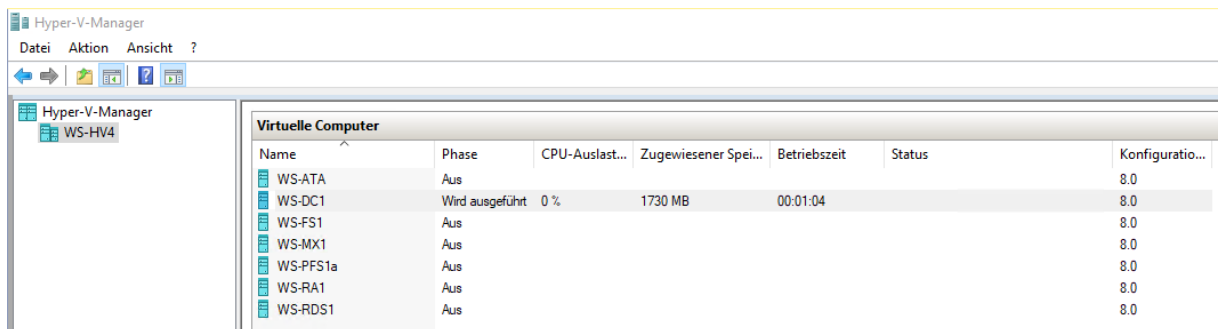
Der Speicher der VM lag vorher auf einem anderen Volume. Mit dem Wizzard kann ich ihn jetzt suchen oder die virtuelle Festplatte später zuweisen:



So kommt eine VM nach der anderen in den neuen Hyper-V-Host:



Ich starte die erste VM:

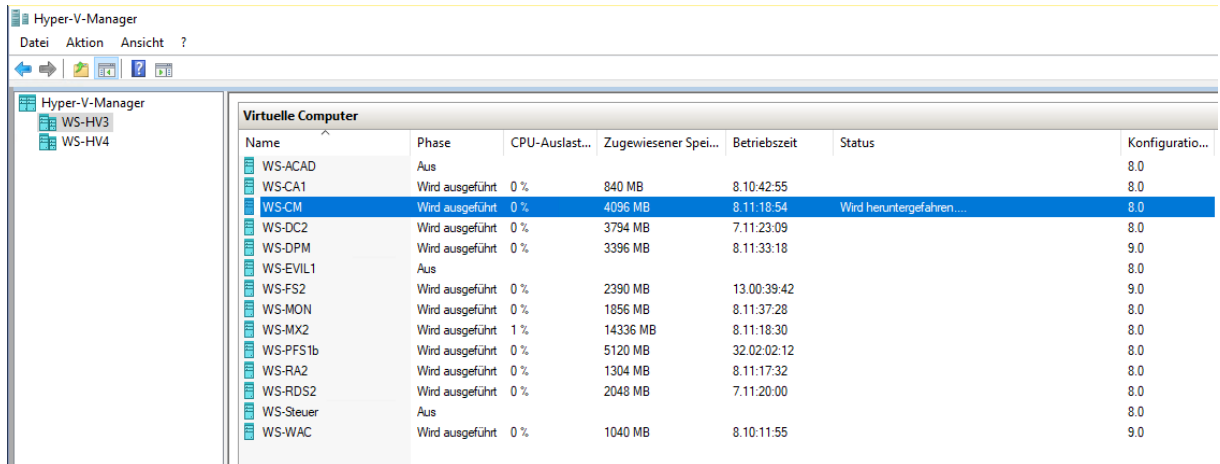


Und dann alle anderen. Bei einigen habe ich die Anzahl der vCPU und den Arbeitsspeicher an den größeren Hyper-V-Host angepasst.

Optimierung der VMs

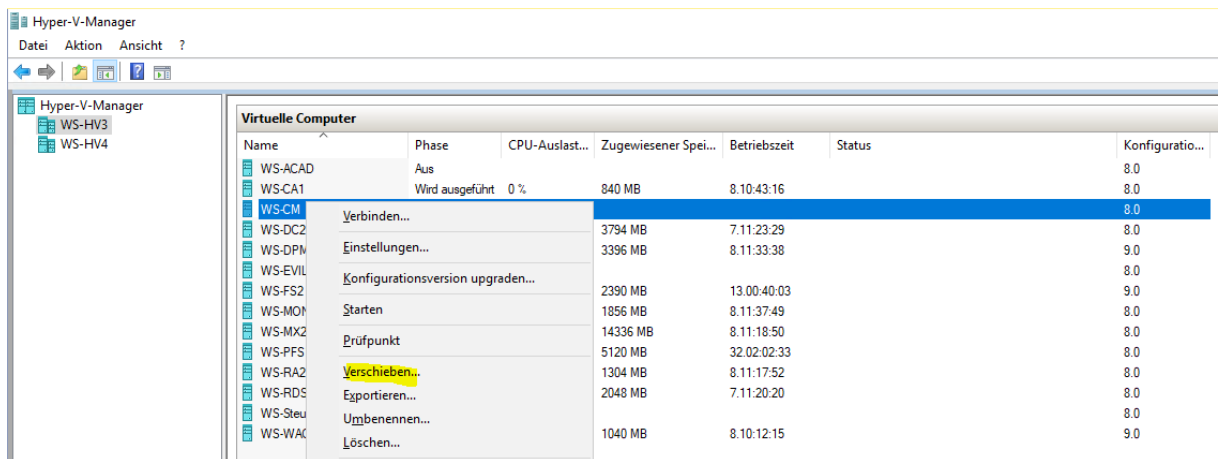
Verschiebung einiger VMs

Ich habe jetzt die Gelegenheit, meine VMs auf beiden neuen Hyper-V-Hosts neu zu verteilen und dabei die Belastung auszugleichen. Die VM „WS-CM“ enthält meinen WSUS und meinen WDS. Beide benötigen doch einigen Platz. Auf dem WS-HV4 ist davon jetzt ausreichend vorhanden. Daher verschiebe ich die gesamte VM auf den neuen Server. Der Service ist nicht produktionsrelevant. Daher fahre ich zuerst die VM herunter:



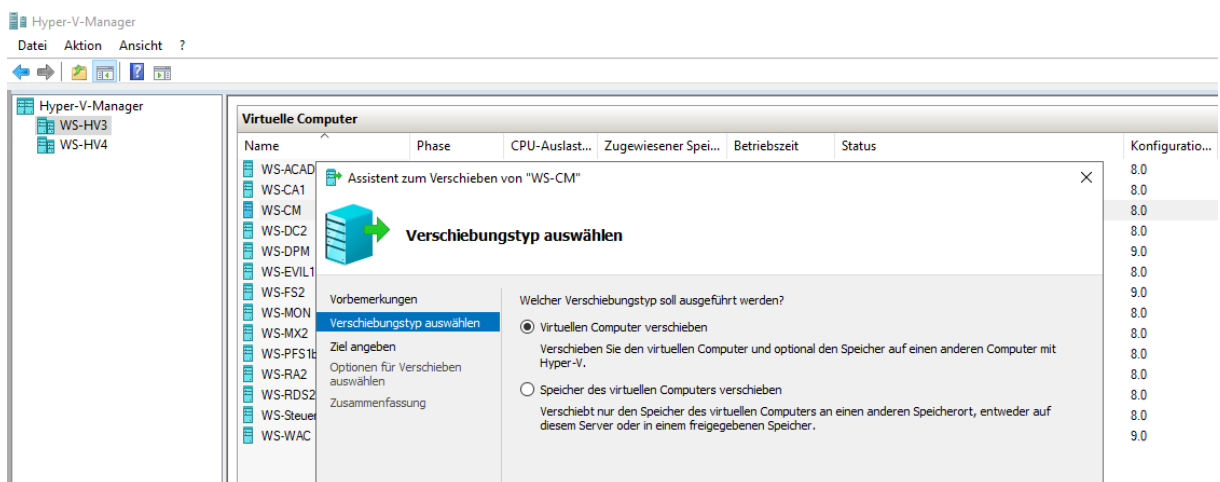
Name	Phase	CPU-Auslast...	Zugewiesener Spei...	Betriebszeit	Status	Konfiguratio...
WS-ACAD	Aus					8.0
WS-CA1	Wird ausgeführt	0 %	840 MB	8.10.42:55		8.0
WS-CM	Wird heruntergefahren...	0 %	4096 MB	8.11.18:54	Wird heruntergefahren...	8.0
WS-DC2	Wird ausgeführt	0 %	3794 MB	7.11.23:09		8.0
WS-DPM	Wird ausgeführt	0 %	3396 MB	8.11.33:18		9.0
WS-EVIL1	Aus					8.0
WS-FS2	Wird ausgeführt	0 %	2390 MB	13.00:39:42		9.0
WS-MON	Wird ausgeführt	0 %	1856 MB	8.11.37:28		8.0
WS-MX2	Wird ausgeführt	1 %	14336 MB	8.11.18:30		8.0
WS-PFS1b	Wird ausgeführt	0 %	5120 MB	32.02.02:12		8.0
WS-RA2	Wird ausgeführt	0 %	1304 MB	8.11.17:32		8.0
WS-RDS2	Wird ausgeführt	0 %	2048 MB	7.11.20:00		8.0
WS-Steuer	Aus					8.0
WS-WAC	Wird ausgeführt	0 %	1040 MB	8.10.11:55		9.0

Dann leite ich die Verschiebung über den Hyper-V-Manager ein:



Name	Phase	CPU-Auslast...	Zugewiesener Spei...	Betriebszeit	Status	Konfiguratio...
WS-ACAD	Aus					8.0
WS-CA1	Wird ausgeführt	0 %	840 MB	8.10.43:16		8.0
WS-CM	Verbinden...					8.0
WS-DC2	Einstellungen...	3794 MB		7.11.23:29		8.0
WS-DPM	Konfigurationsversion upgraden...	3396 MB		8.11.33:38		9.0
WS-EVIL1	Starten	2390 MB		13.00:40:03		9.0
WS-FS2	Stoppen	1856 MB		8.11.37:49		8.0
WS-MX2	Prüfpunkt	14336 MB		8.11.18:50		8.0
WS-PFS1b	Verschieben...	5120 MB		32.02.02:33		8.0
WS-RA2	Exportieren...	1304 MB		8.11.17:52		8.0
WS-RDS2	Umbenennen...	2048 MB		7.11.20:20		8.0
WS-Steuer	Löschen...					8.0
WS-WAC		1040 MB		8.10.12:15		9.0

Mit dem ersten Punkt wird die VM auf einen anderen Host verschoben:



Name	Phase	CPU-Auslast...	Zugewiesener Spei...	Betriebszeit	Status	Konfiguratio...
WS-ACAD						8.0
WS-CA1						8.0
WS-CM						8.0
WS-DC2						8.0
WS-DPM						9.0
WS-EVIL1						8.0
WS-FS2						9.0
WS-MON						8.0
WS-MX2						8.0
WS-PFS1b						8.0
WS-RA2						8.0
WS-RDS2						8.0
WS-Steuer						8.0
WS-WAC						9.0

Assistent zum Verschieben von "WS-CM"

Verschiebungstyp auswählen

Vorbemerkungen

Verschiebungstyp auswählen

Ziel angeben

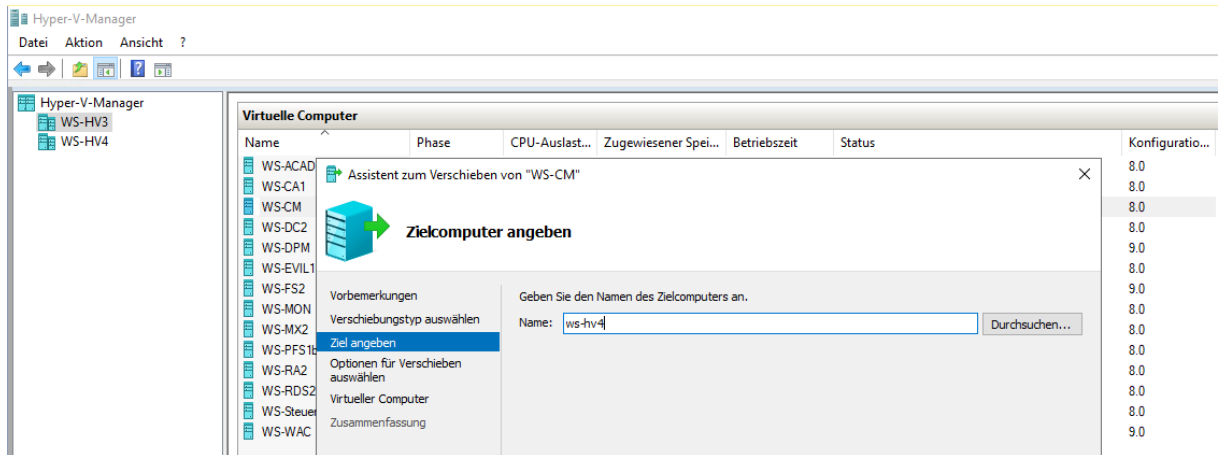
Optionen für Verschieben auswählen

Zusammenfassung

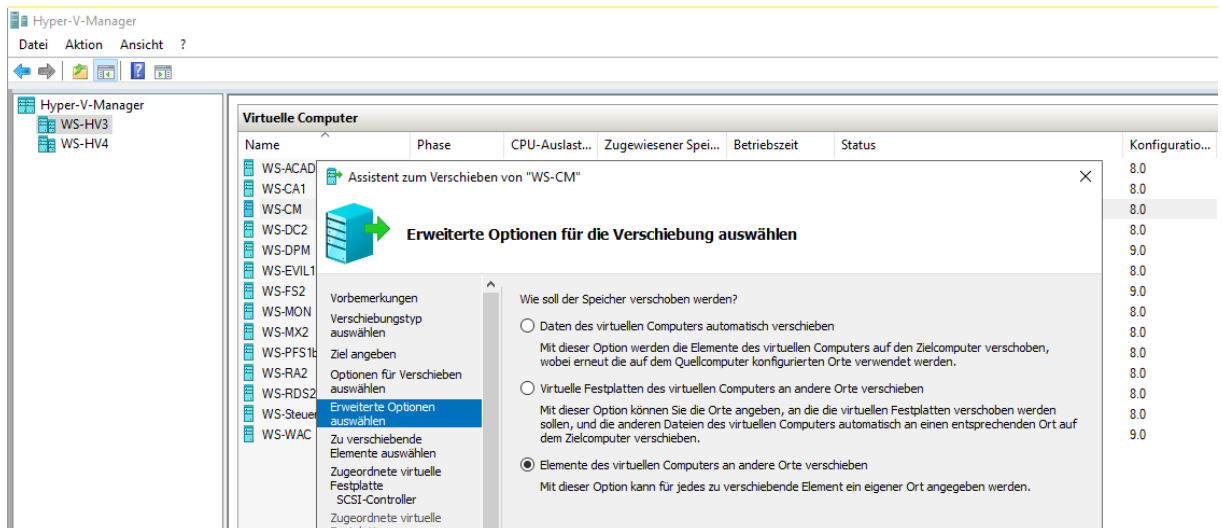
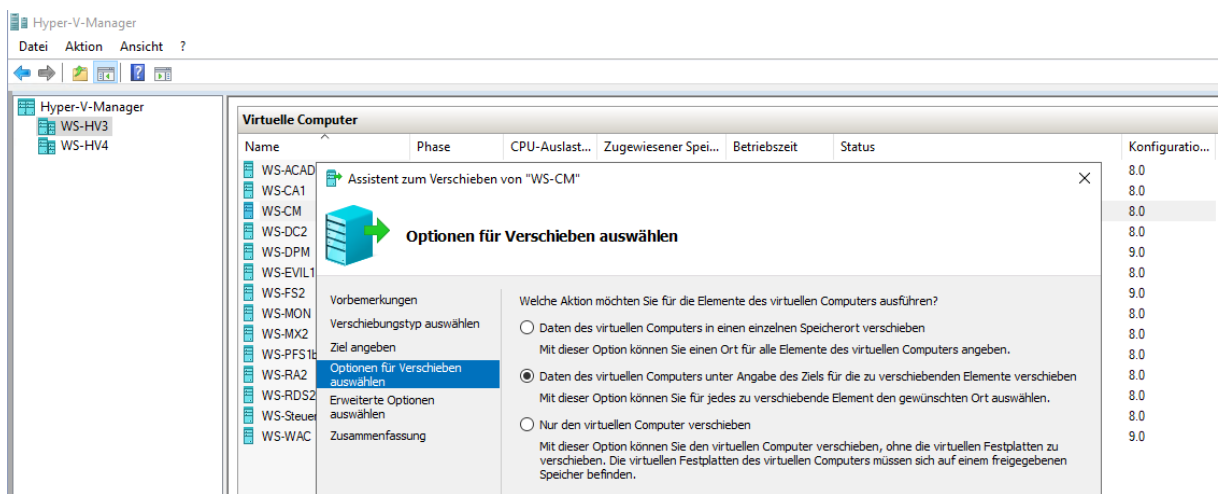
Welcher Verschiebungstyp soll ausgeführt werden?

Virtuellen Computer verschieben
Verschieben Sie den virtuellen Computer und optional den Speicher auf einen anderen Computer mit Hyper-V.

Speicher des virtuellen Computers verschieben
Verschiebt nur den Speicher des virtuellen Computers an einen anderen Speicherort, entweder auf diesem Server oder in einem freigegebenen Speicher.



Dort möchte ich die Dateien sinnvoll auf meine Volumes aufteilen. Dies kann mit der zweiten Option je VM-Bestandteil definiert werden:



Für jedes Element der VM wähle ich einen geeigneten Speicherplatz aus. Die VM selber und die System-VHDX kommen auf das TIER-GOLD (V:). Die beiden großen VHDX für den WSUS und den WDS lagere ich dagegen lieber auf dem langsameren RAID1 der normalen SATA-Platten:

Assistent zum Verschieben von "WS-CM"

Zu verschiebende Elemente auswählen

Vorbemerkungen
Verschiebungstyp auswählen
Ziel angeben
Optionen für Verschieben auswählen
Erweiterte Optionen auswählen
Zu verschiebende Elemente auswählen
Zugeordnete virtuelle Festplatte SCSI-Controller
Zugeordnete virtuelle Festplatte SCSI-Controller
Zugeordnete virtuelle Festplatte SCSI-Controller
Zugeordnete virtuelle Festplatte SCSI-Controller
Aktuelle Konfiguration

Wählen Sie die zu verschiebenden Elemente aus.

- HDD0.vhdx
- HDD1-WSUS.vhdx
- HDD2-WSUS.vhdx
- Aktuelle Konfiguration
- Prüfpunkte
- Smart Paging

Details

Name: HDD0.vhdx
Ordner: V:\Hyper-V\WS-CM\Virtual Hard Disks
Größe: 33,25 GB
Verfügbare Speicherplatz: 157 GB

Assistent zum Verschieben von "WS-CM"

Fertigstellen des Verschiebe-Assistenten

Vorbemerkungen
Verschiebungstyp auswählen
Ziel angeben
Optionen für Verschieben auswählen
Erweiterte Optionen auswählen
Zu verschiebende Elemente auswählen
Zugeordnete virtuelle Festplatte SCSI-Controller
Zugeordnete virtuelle Festplatte SCSI-Controller
Zugeordnete virtuelle Festplatte SCSI-Controller
Zugeordnete virtuelle Festplatte SCSI-Controller
Aktuelle Konfiguration
Prüfpunkte
Smart Paging

Sie sind im Begriff, den folgenden Vorgang auszuführen.

Beschreibung:

Virtueller Computer:	WS-CM
Verschiebungstyp:	Virtueller Computer und Speicher
Zielcomputer:	ws-hv4
Zu verschiebendes Element:	Zielspeicherort
Zugeordnete virtuelle Festplatte SCSI-Controller	V:\Hyper-v\WS-CM\Virtual Hard Disks\
Zugeordnete virtuelle Festplatte SCSI-Controller	D:\Hyper-v\WS-CM
Zugeordnete virtuelle Festplatte SCSI-Controller	D:\Hyper-v\WS-CM
Aktuelle Konfiguration	V:\Hyper-v\WS-CM
Prüfpunkte	V:\Hyper-v\WS-CM
Smart Paging	V:\Hyper-v\WS-CM

Klicken Sie auf "Fertig stellen", um die Verschiebung abzuschließen und den Assistenten zu beenden.

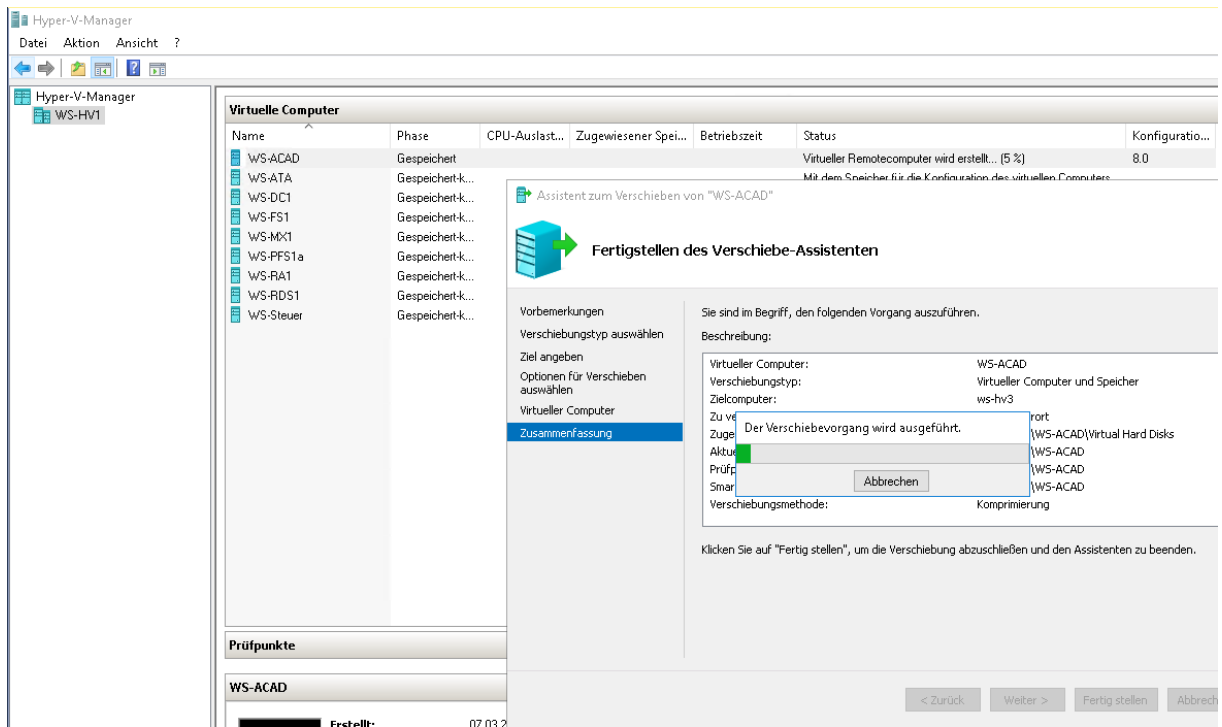
Zusammenfassung

< Zurück Weiter > **Fertig stellen** Abbrechen

Anschließend wird die VM verschoben:

Name	Phase	CPU-Auslast...	Zugewiesener Spei...	Betriebszeit	Status	Konfiguratio...
WS-ATA	Wird ausgeführt	0 %	3038 MB	01:18:39		8.0
WS-CM	Wird ausgeführt	0 %	2048 MB	00:00:00	Wird gestartet - Erfolgreich	8.0
WS-DC1	Wird ausgeführt	0 %	2778 MB	01:20:40		8.0
WS-FS1	Wird ausgeführt	0 %	762 MB	01:19:54		8.0
WS-MX1	Wird ausgeführt	0 %	14336 MB	01:19:19		8.0
WS-PFS1a	Wird ausgeführt	0 %	5120 MB	01:20:40		8.0
WS-RA1	Wird ausgeführt	0 %	1244 MB	01:19:59		8.0
WS-RDS1	Wird ausgeführt	0 %	1094 MB	01:19:24		8.0

Auf die gleiche Weise verschiebe ich eine andere VM vom WS-HV3 zum neuen WS-HV4:



Jetzt sind die VMs optimal auf beide Hosts verteilt.

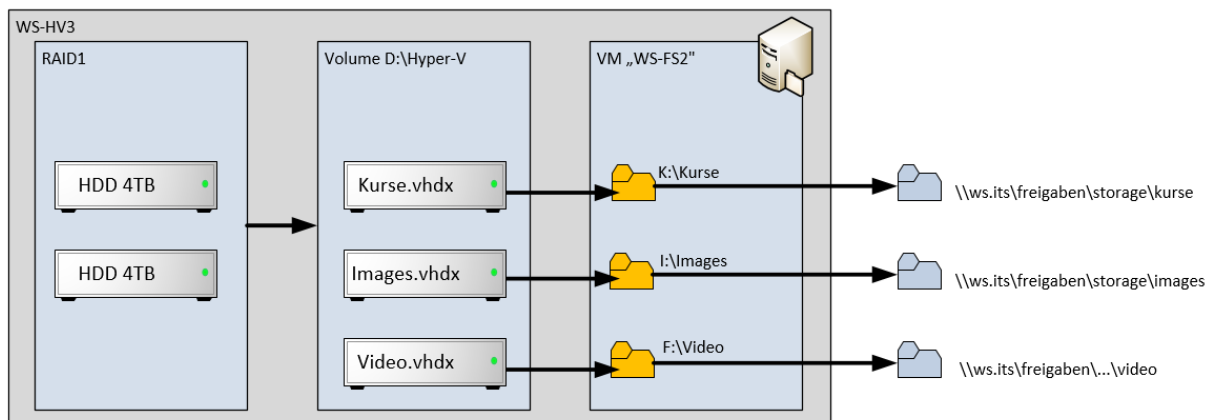
Verschiebung der großen VHDX der Fileserver

Beide Hosts haben zu den schnellen Flash-Speichern jeweils 2 langsamere und größere HDD, die gespiegelt sind. So kann ich auf beiden Servern große Dateien ablegen. Dennoch möchte ich eine Zweckbindung einführen:

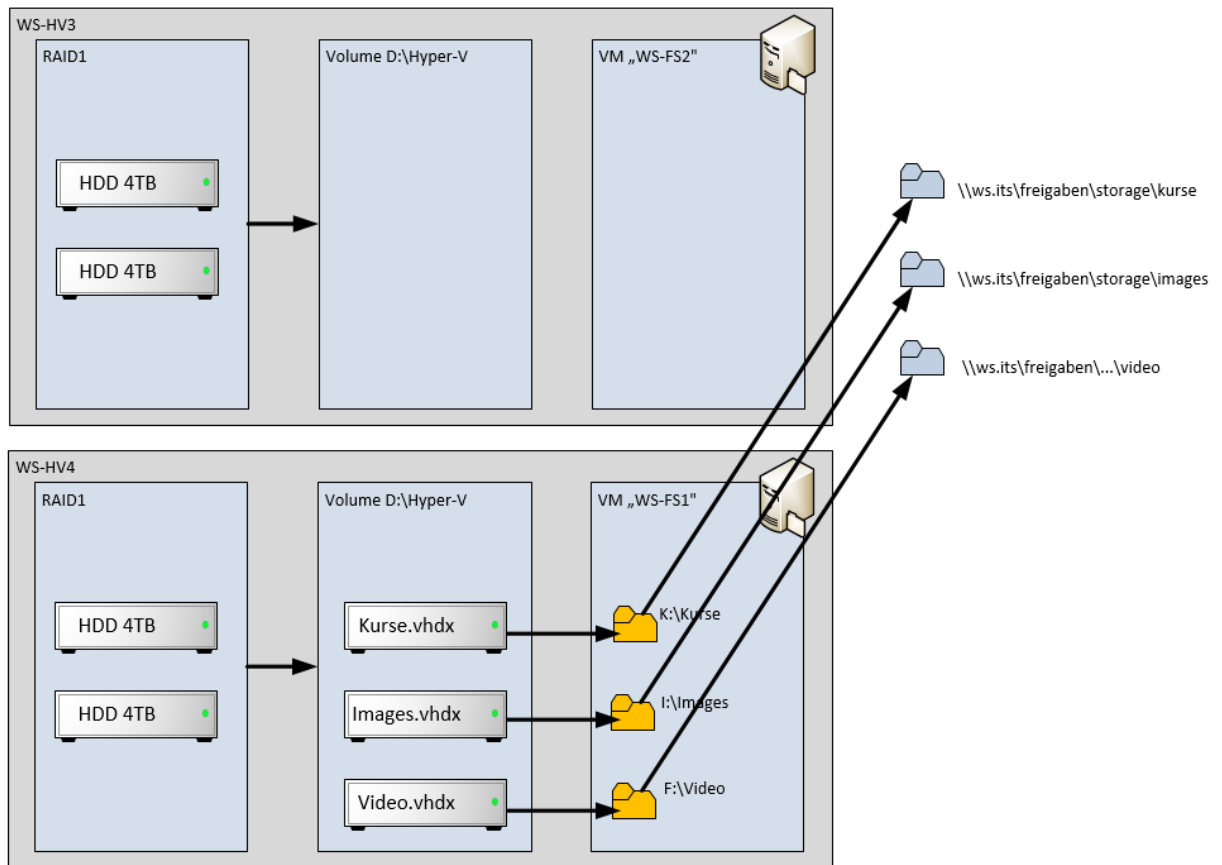
- Auf dem neuen Server WS-HV4 sollen Nutzdaten abgelegt werden
- Auf dem anderen Server WS-HV3 soll das RAID1 für lokale Datensicherungen genutzt werden.

Bisher speichert das RAID1 auf WS-HV3 aber Backups und große VHDX. Diese möchte ich jetzt auf WS-HV4 verschieben.

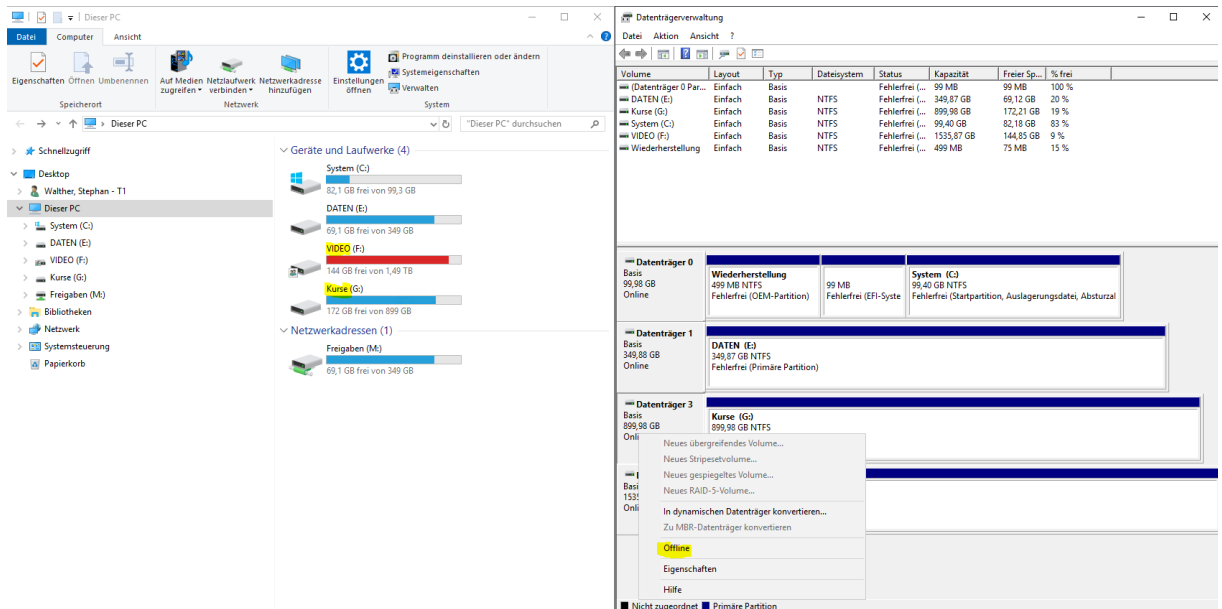
Was ist in den VHDX enthalten? Es gibt eine, in der meine Kurs-Umgebungen für Hyper-V abgelegt sind. Eine andere speichert Video-Dateien. Und in einer dritten befinden sich ISO-Dateien. Diese virtuellen Festplatten sind in dem virtuellen Fileserver eingebunden, der sich auf dem gleichen Hyper-V-Host befindet. Dieser Fileserver stellt die Ordner dann als Freigaben im Netzwerk bereit. Die Freigaben werden aber nicht direkt vom Client angesprochen, sondern über einen DFS-Namespace veröffentlicht. Alles klar? Kein Problem: So schaut das aktuell aus:



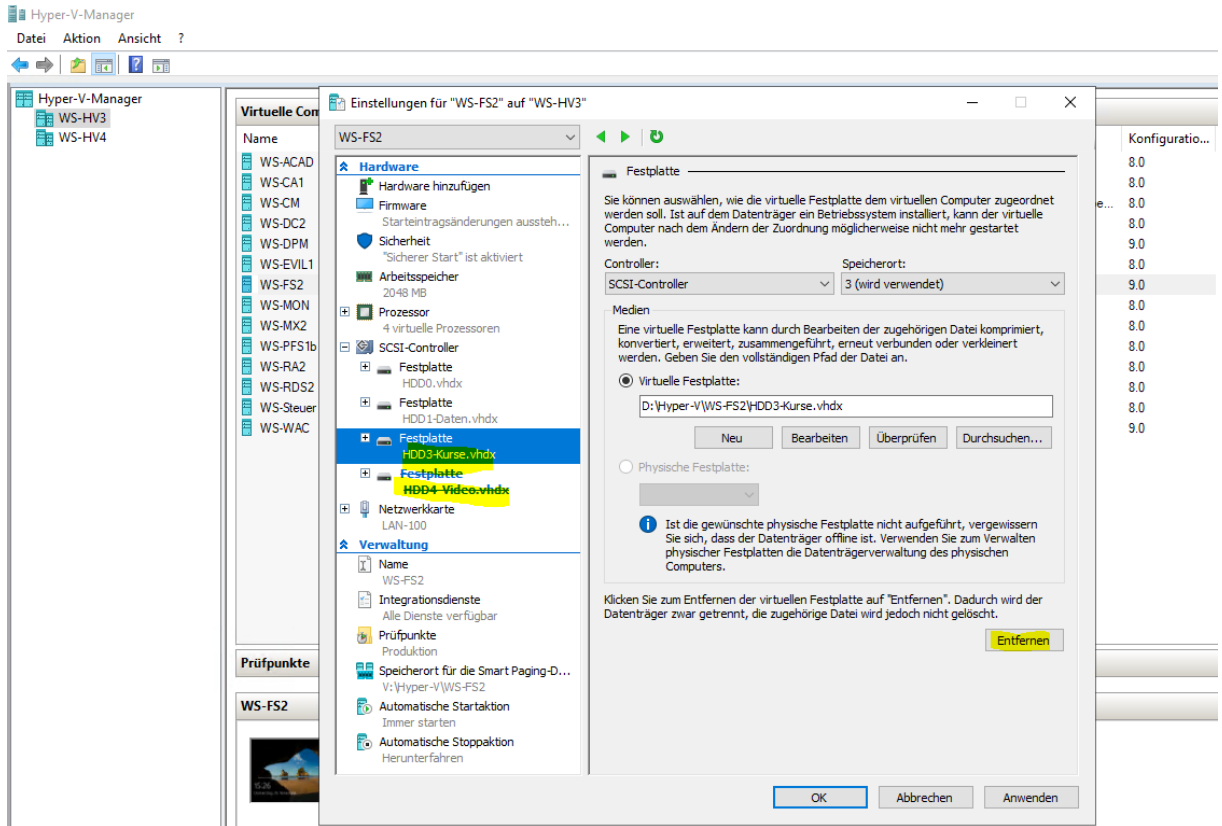
Ich verschiebe also nur die 3 VHDX-Dateien auf den neuen WS-HV4 und binde sie dort in den WS-FS1 ein. Danach erstelle ich dort die Freigaben und verändere die Links im DFS-Namespace. Für den Client ändert sich also nichts. Und im Backend hab ich die Dateien optimaler abgelegt:



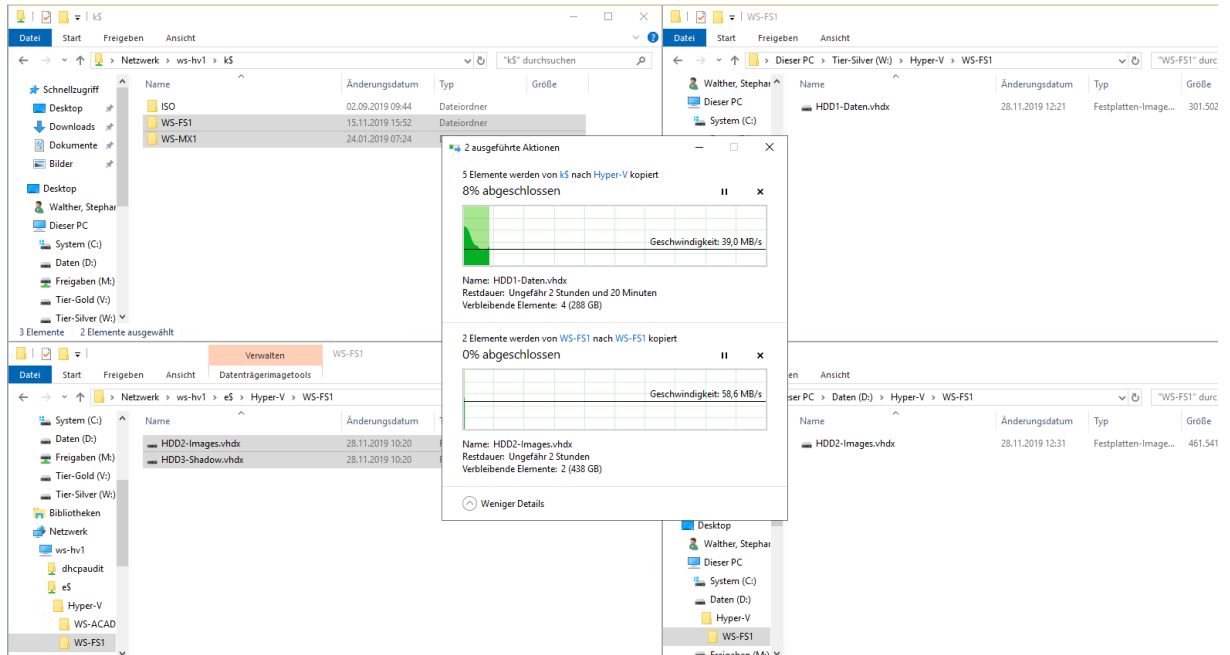
Dafür nehme ich die eingebundenen VHDX-Dateien im Fileserver WS-FS2 offline:



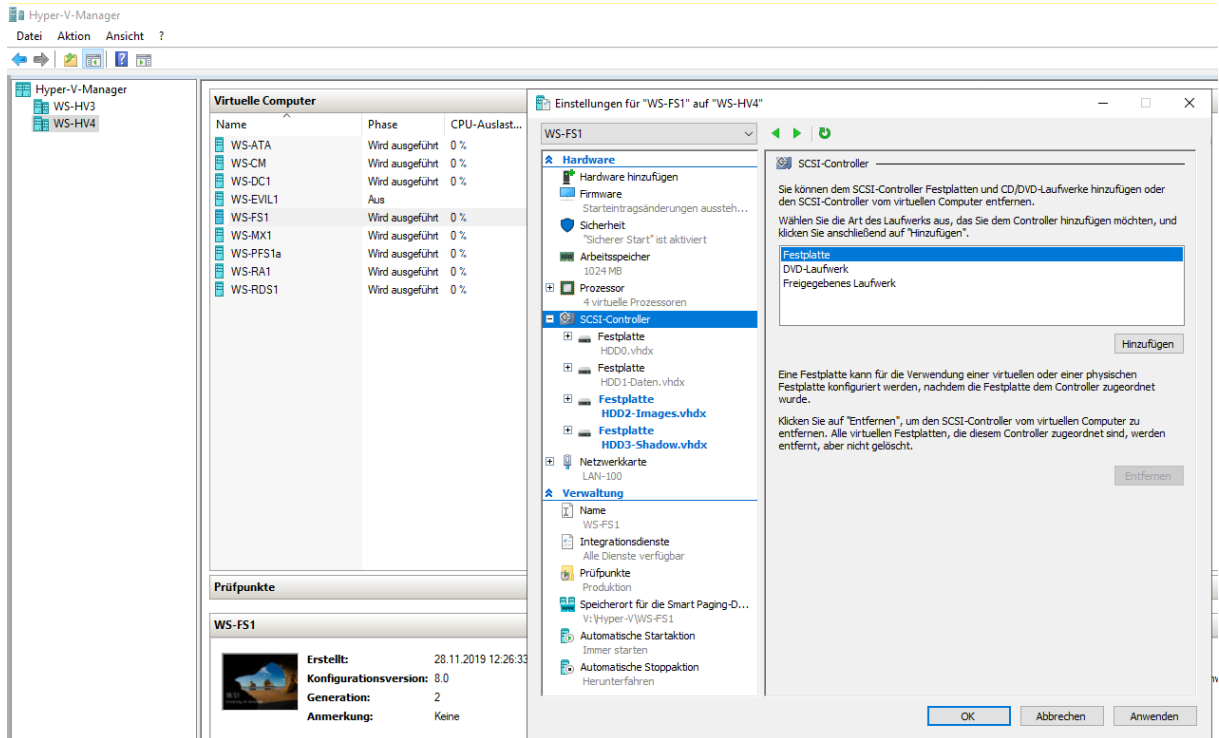
Nun kann ich sie aus der VM „ausbauen“:



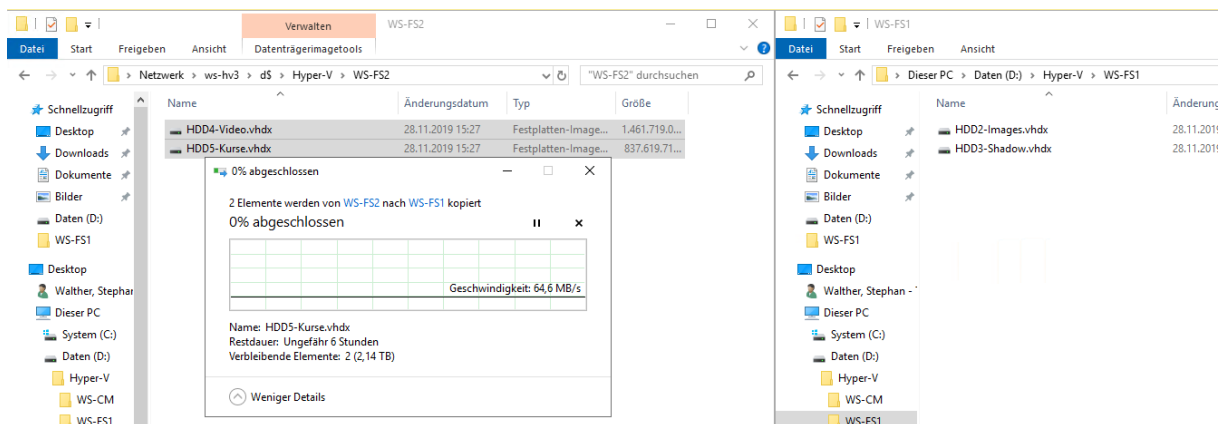
Die so freigewordenen Dateien kopiere ich vom WS-HV3 auf den neuen WS-HV4. Bei dieser Größe dauert das einige Zeit:



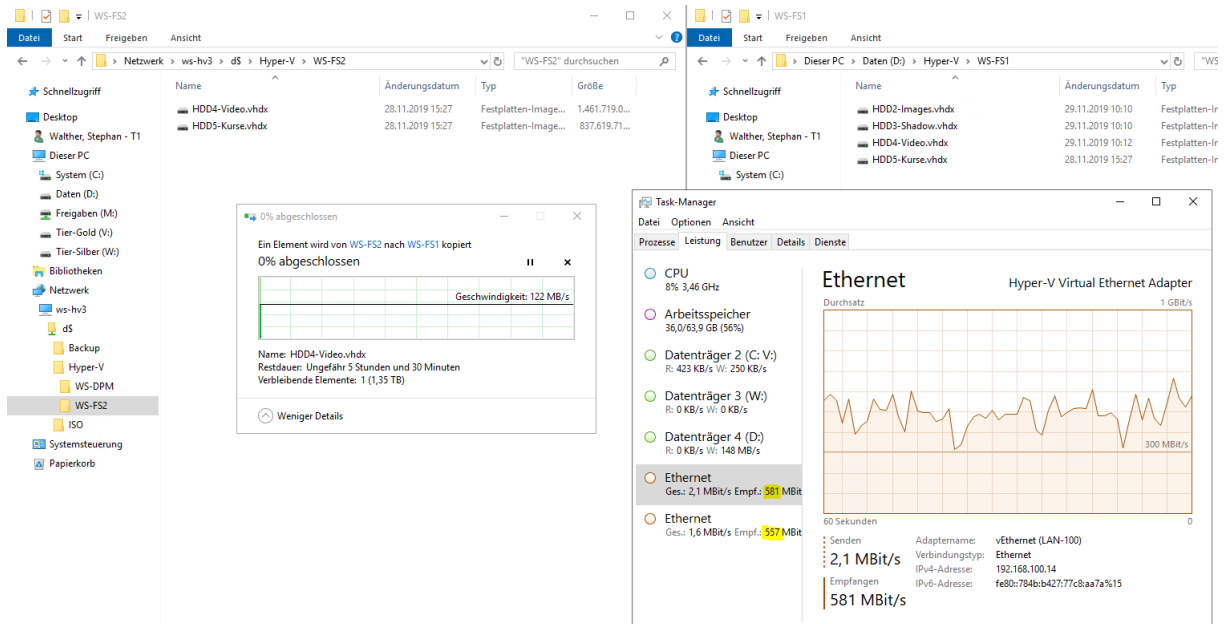
Die ersten VHDX sind übertragen. Daher binde ich sie in die VM ein:



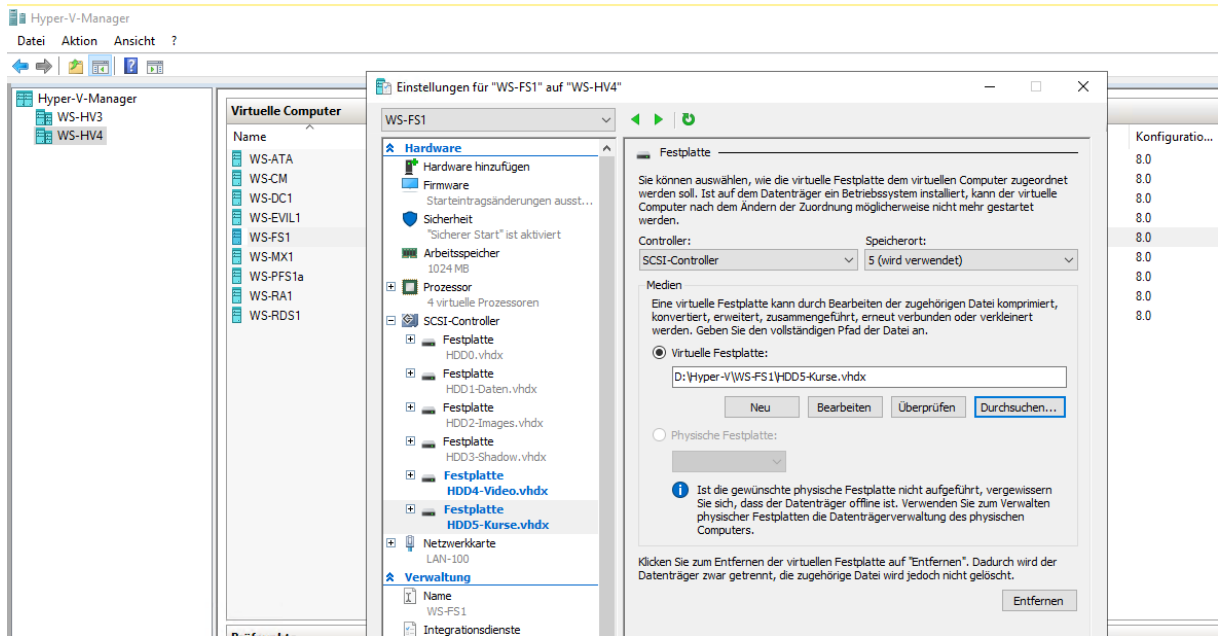
Jetzt kommt der nächste Schwung:



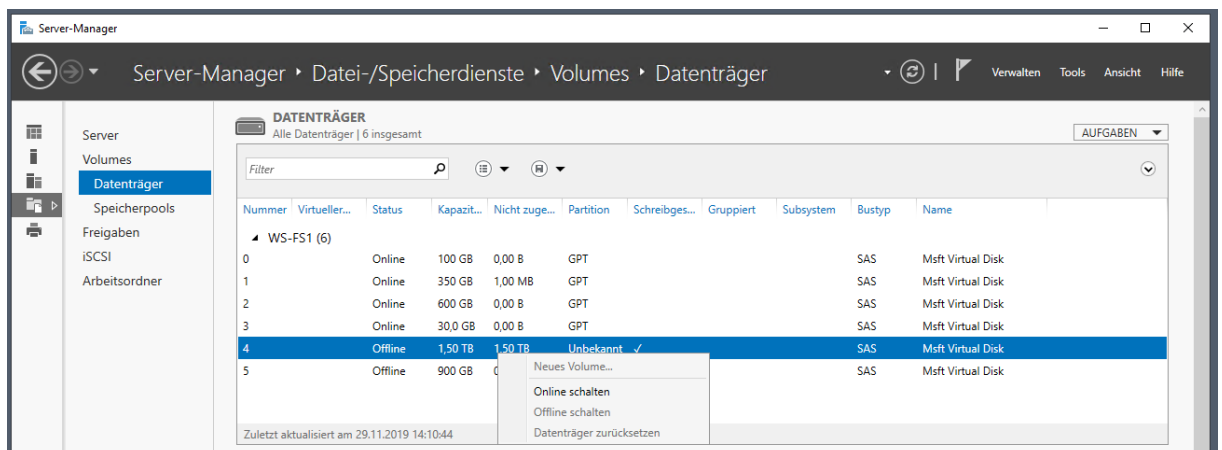
Interessant ist dieses Bild: beide Server haben 2 Netzwerkkarten und können sich über diese unterschiedlichen Netzwerke miteinander unterhalten. Die Kopieraktion wird dabei vom sendenden Server auf beide Adapter dynamisch aufgeteilt und der Empfänger setzt die Fragmente wieder zusammen:



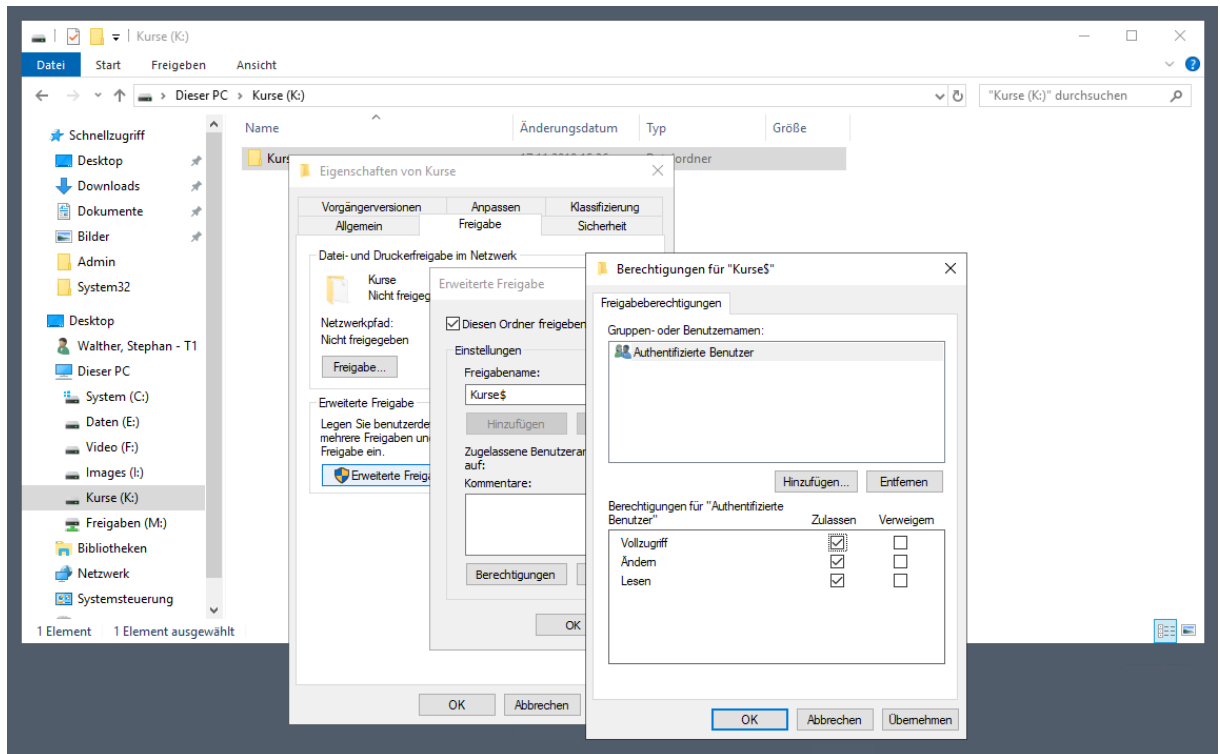
Nach einiger Zeit sind die Dateien endlich angekommen. Ich passe noch die Namen der VHDX an und binde sie endlich in meinen WS-FS1 ein:



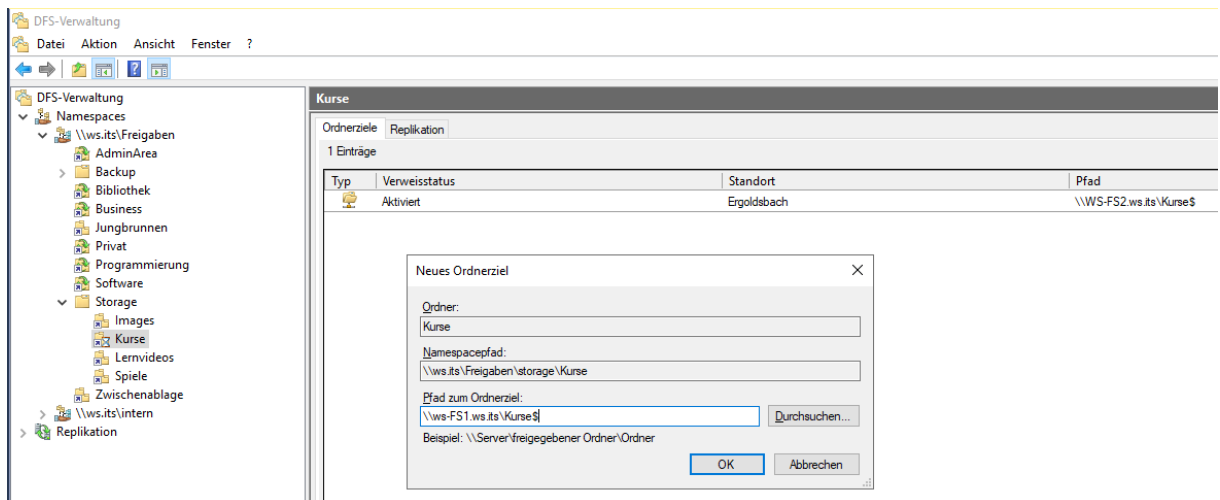
Die Datenträger müssen dann online geschaltet werden:



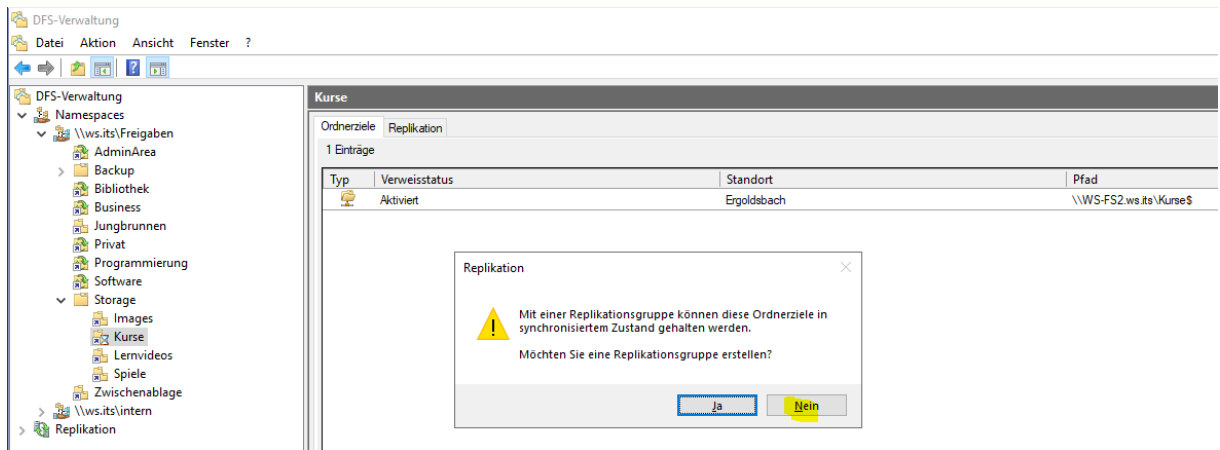
Als nächstes erstelle ich die versteckten Freigaben:



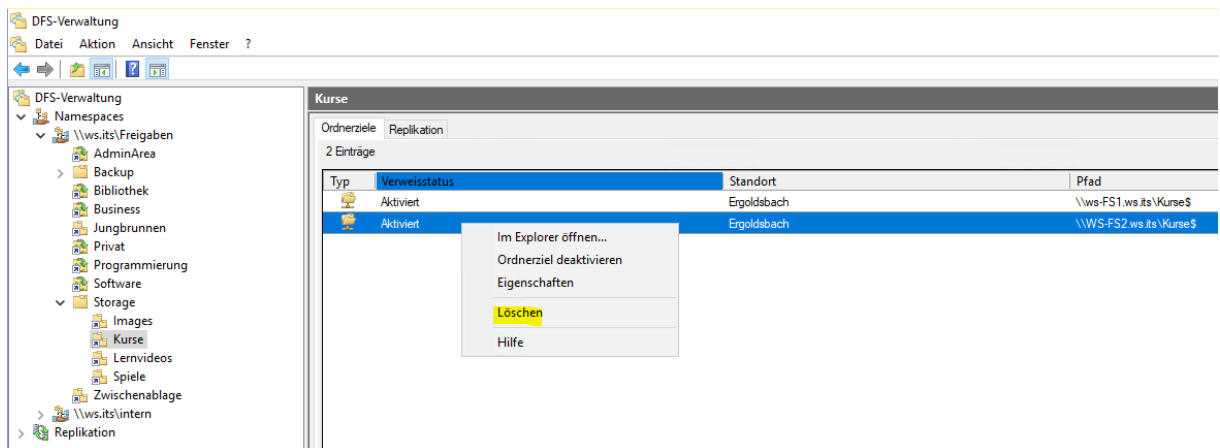
Und zuletzt trage ich die neuen Ziele im DFS-Namespace in den Links ein:



Ich will hier aber keine Replikation einrichten. Denn der alte Link ist ja nicht mehr erreichbar:

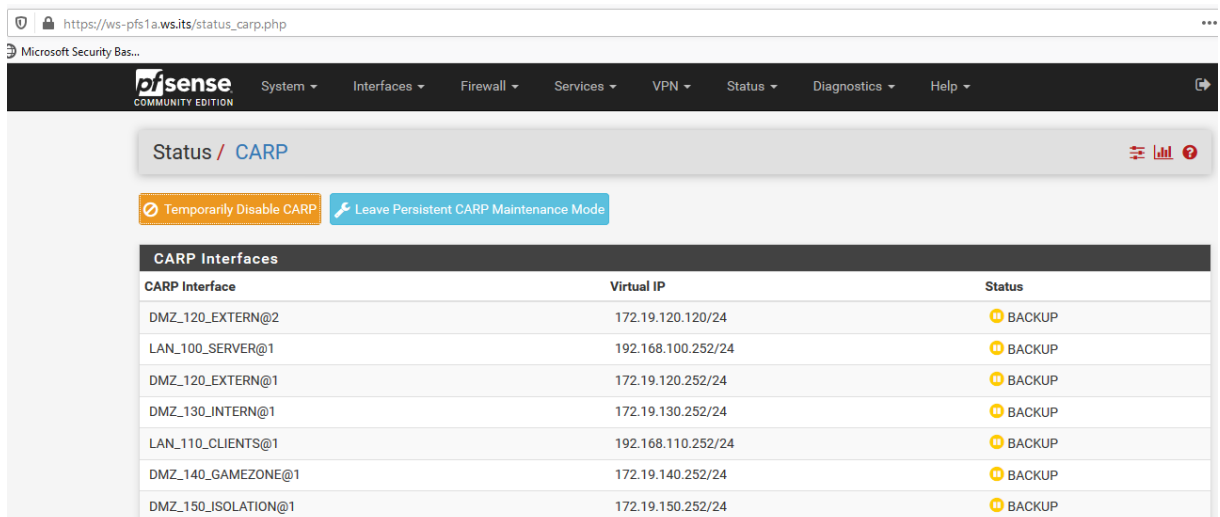


Den alten Link kann ich einfach löschen. Nun werden (nach Ablauf der Cache-Dauer – in meinem Fall 2 Minuten) die Clients auf die neue Location umgeleitet:



Maintenance beenden

In meinem PFSense-Cluster beende ich die Maintenance. Damit übernimmt die VM WS-PFS1a auf WS-HV4 wieder die primäre Rolle:



Im PRTG ändere ich den Server und muss einige Sensoren rekonfigurieren:

The screenshot shows the WS-ITS monitoring interface. The top navigation bar includes 'Startseite', 'Geräte', 'Bibliotheken', 'Sensoren', 'Alarme', 'Maps', 'Berichte', 'Protokoll', 'Tickets', and 'Konfiguration'. The main area displays a tree view under 'Gruppe WS-ITS' with sub-sections for 'Gerät der Probe', 'Netzwerk', and 'Server'. The 'Gerät der Probe' section shows three sensors: 'Serverzustand' (100%), 'Systemzustand' (100%), and 'Zustand der Pr...' (100%), all in green. The 'Netzwerk' section shows three sensors in green. The 'Server' section lists several Hyper-V VMs, each with multiple sensors. Some sensors are in red (warning), such as 'WS-DC1' (1%), 'WS-FS1' (<1%), 'WS-MX1' (21%), 'WS-PFS1a' (2%), 'WS-RA1' (30%), 'WS-ATA' (6%), 'WS-RDS1' (<1%), 'Volume IO C:' (77%), 'Volume IO V:' (64%), and 'Diak IO 0 D:' (0%).

Aber nach ein paar Klicks und einigen Minuten Wartezeit ist alles wieder grün:

This screenshot shows the same WS-ITS monitoring interface as above, but after a few clicks and some waiting time. The 'Gerät der Probe' section now shows three sensors: 'Serverzustand' (100%), 'Systemzustand' (100%), and 'Zustand der Pr...' (97%), all in green. The 'Netzwerk' section remains the same. The 'Server' section now shows all sensors in green, indicating that the previous warnings have been resolved. For example, 'WS-DC1' is now 1%, 'WS-FS1' is <1%, 'WS-MX1' is 21%, 'WS-PFS1a' is 2%, 'WS-RA1' is 30%, 'WS-ATA' is 6%, 'WS-RDS1' is <1%, 'Volume IO C:' is 77%, 'Volume IO V:' is 64%, and 'Diak IO 0 D:' is 0%.

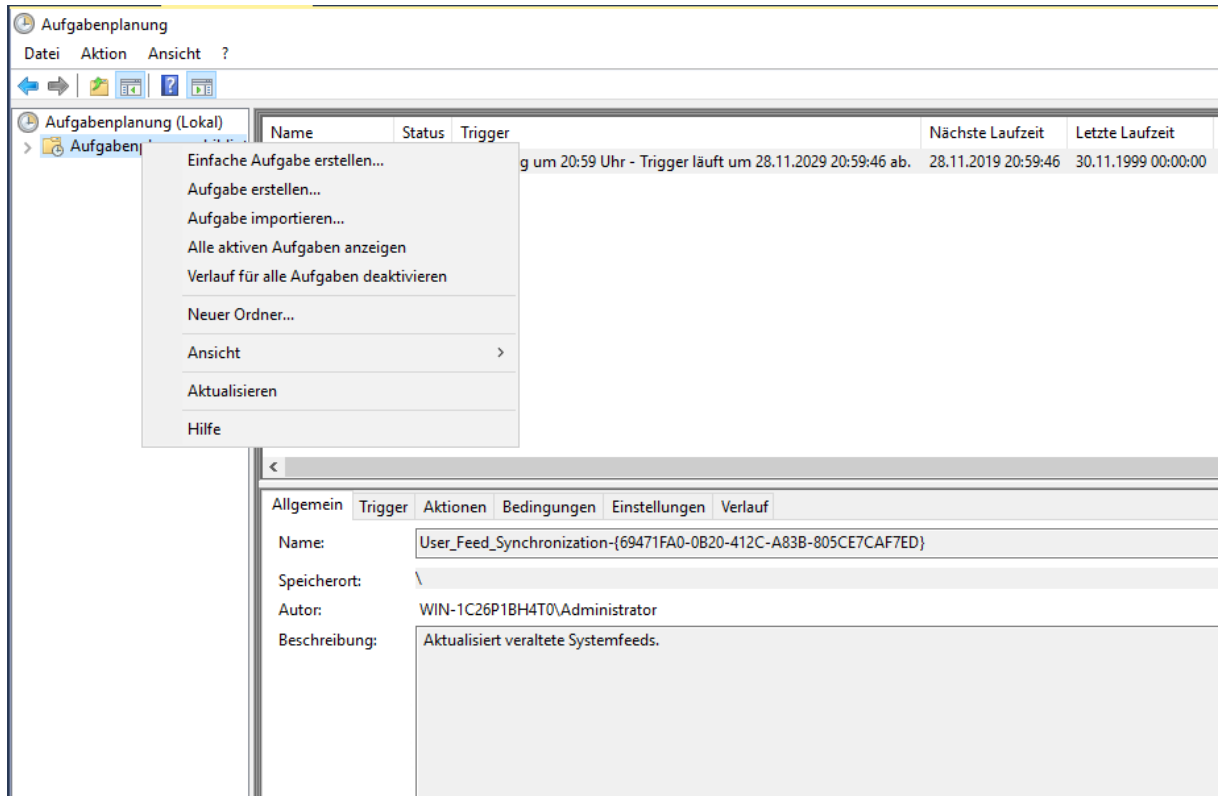
Datensicherung einrichten

Dann darf auch die Datensicherung nicht fehlen. Diese besteht bei mir aus 2 Sicherungsverfahren: einem Systemimage des Betriebssystems und einer Nutzdatensicherung. Im Falle eines Hyper-V-Hosts sind das die virtuellen Computer. Diese sichere ich aber zum großen Teil innerhalb der VM. Daher bleiben nicht viele VMs über.

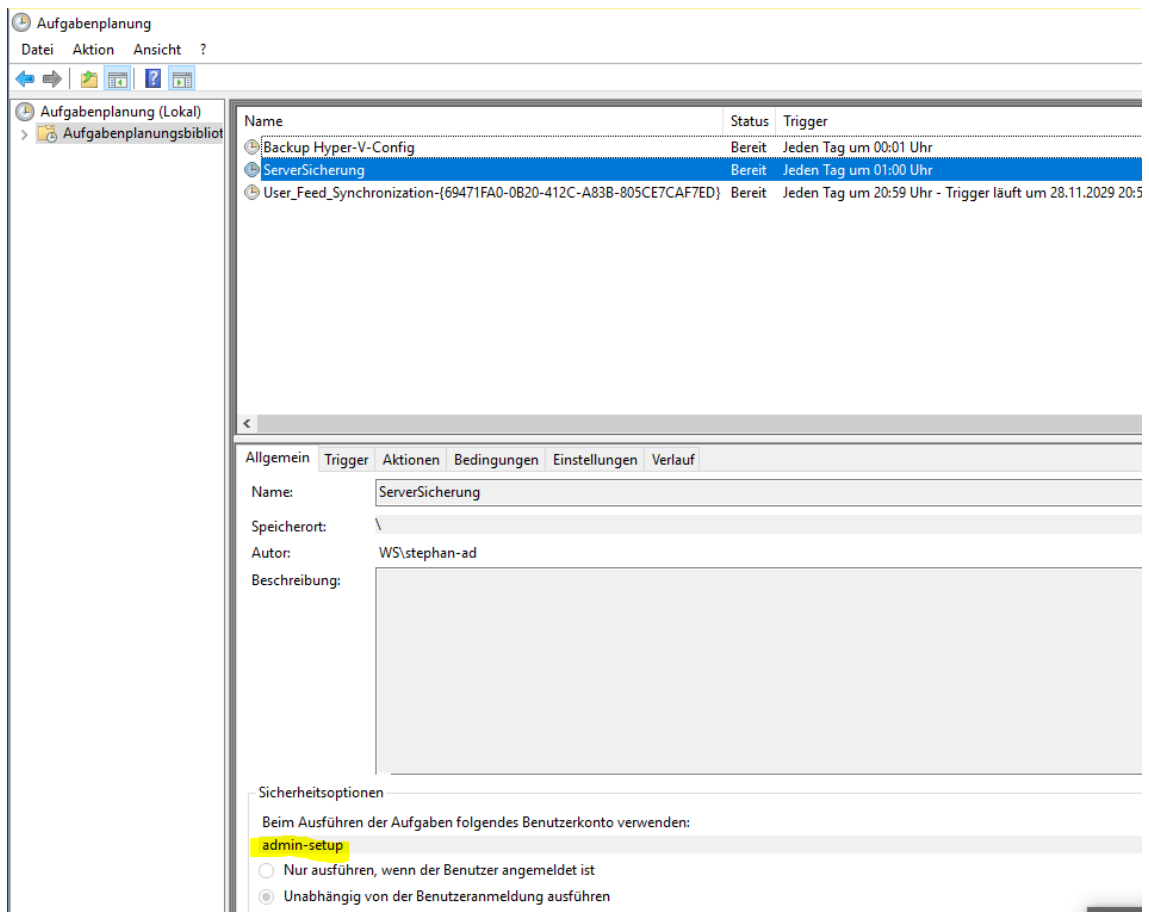
Vom alten Server hatte ich die Sicherungsaufgaben als XML-Dateien exportiert. Diese kopiere ich auf den neuen Server:

The screenshot shows two File Explorer windows side-by-side. The left window shows the 'Admin' folder on the old server, containing files like 'Hyper-V', 'PSTranscript', 'Backup Hyper-V-Config.xml', and 'ServerSicherung.xml'. The right window shows the 'WS-HV4' folder on the new server, containing files like 'LWC', 'Admin', 'iS', 'Kaspersky', 'Monitoring', 'PFSense', 'PrintServices', 'RDS', 'RemoteAccess', 'SCCM', and 'SCEP'. A yellow arrow points from the 'ServerSicherung.xml' file in the left window to the 'ServerSicherung.xml' file in the right window, indicating the transfer of the backup configuration.

Anschließend kann ich sie in der Aufgabenplanung wieder importieren:



Die erste Aufgabe erstellt eine Kopie der VM-Konfigurationsdateien auf dem Systemlaufwerk. So kann ich bei einem Ausfall die VMs einfach wieder generieren. Die zweite Aufgabe startet jeden morgen das SystemImageBackup. Diesr Task muss aber mit einem speziellen Sicherheitskonto ausgeführt werden: ein Group Managed Service Account. Diesen kann ich nicht direkt ansprechen. Daher importiere ich die Aufgabe mit einem Dummy-Konto:



Über eins meiner PowerShell-Skripts kann ich dann vom Domain Controller aus den gMSA eintragen:

The screenshot shows the 'gMSA-Admin' console. A dialog box titled 'neuer Server für gMSA' is open, prompting the user to enter the name of a server. The text 'WS-HV4' is entered in the input field. The background console shows a list of existing gMSAs and a list of servers to which they are assigned.

The screenshot shows the 'gMSA-Admin' console with the 'Server' tab selected. A table displays the configuration for the gMSA 'gMSA-Backup (TaskUser für BMR)' across various servers.

Server	TaskName	Account	Pfad
WS-HV4	Backup Hyper-V-Config	SYSTEM	\
WS-HV4	ServerSicherung	admin-setup	\
WS-HV4	User_Feed_Synchronizati...{69471FA...}	sysadm	\
WS-HV4	Server Initial Configuration Task	SYSTEM	\\Microsoft\Windows\
WS-HV4	.NET Framework NGEN v4.0.30319	SYSTEM	\\Microsoft\Windows\.NET Framework\
WS-HV4	.NET Framework NGEN v4.0.30319 64	SYSTEM	\\Microsoft\Windows\.NET Framework\
WS-HV4	.NET Framework NGEN v4.0.30319 6...	SYSTEM	\\Microsoft\Windows\.NET Framework\
WS-HV4	.NET Framework NGEN v4.0.30319 C...	SYSTEM	\\Microsoft\Windows\.NET Framework\

The screenshot shows the 'gMSA-Admin' console with the following configuration:

- vorhandene gMSA:** gMSA-ADFS (Service ADFS), gMSA-Backup (TaskUser für BMR), gMSA-Monitor (TaskUser für Monitoring), gMSA-SQLDPM (Service SQL auf WS-DPM)
- zugehörige Server:** WS-DC1.ws.its, WS-FS1.ws.its, WS-MX1.ws.its, WS-HV1.ws.its, WS-RA1.ws.its, WS-CA1.ws.its, WS-MX2.ws.its, WS-FS2.ws.its, WS-HV2.ws.its, WS-RA2.ws.its, WS-RDS1.ws.its, WS-RDS3.ws.its, WS-RDS2.ws.its, WS-DC2.ws.its, WS-CM.ws.its, WS-DPM.ws.its, WS-WAC.ws.its, WS-HV3.ws.its, WS-ATA.ws.its, WS-MON.ws.its, **WS-HV4.ws.its (online)**
- zugehörige Gruppen:**
 - direkte Gruppen: GG-SEC-Server-Monitoring-Admins, GG-SEC-Server-JB-Admins, GG-SEC-Server-RDS-Admins, GG-SEC-Server-Standard-Admins, GG-SEC-Server-MX-Admins, GG-SEC-Server-HyperV-Admins, GG-SEC-Clients-JB-Admins, GG-Admin-Backup, Sicherungs-Operatoren
 - indirekte Gruppen (durch Verschachtelung): LD-Admin-Backup, LD-Admin-SQL-DPM, LD-AD-AdminArea-R, LD-SEC-Clients-JB-Admins, LD-SEC-Clients-JB-Login, LD-SEC-Clients-JB-RDP, LD-SEC-Clients-JB-WinRM, LD-SEC-Server-HyperV-Admins, LD-SEC-Server-HyperV-Login, LD-SEC-Server-HyperV-RDP

Einsatz als: Task

Server	TaskName	Account	Pfad
WS-HV4	Backup Hyper-V-Config	SYSTEM	\
WS-HV4	ServerSicherung	ws\gMSA-Backup\$	\
WS-HV4	User_Feed_Synchronisation-{69471FA...}	sysadm	\
WS-HV4	Server Initial Configuration Task	SYSTEM	\Microsoft\Windows\
WS-HV4	.NET Framework NGEN v4.0.30319	SYSTEM	\Microsoft\Windows\.NET Framework\
WS-HV4	.NET Framework NGEN v4.0.30319 64	SYSTEM	\Microsoft\Windows\.NET Framework\
WS-HV4	.NET Framework NGEN v4.0.30319 6...	SYSTEM	\Microsoft\Windows\.NET Framework\
WS-HV4	.NET Framework NGEN v4.0.30319 C...	SYSTEM	\Microsoft\Windows\.NET Framework\

Buttons: erstelle gMSA, lösche gMSA, bearbeite gMSA, weiterer Server, entferne Server, teste gMSA, weitere Gruppe, entferne Gruppe

Buttons: lese alle Server, **setze gMSA ein**

Status: bereit

Den alten Server nehme ich dafür aus der Berechtigungsliste heraus:

The screenshot shows the 'gMSA-Admin' console after removing WS-HV1:

- vorhandene gMSA:** gMSA-ADFS (Service ADFS), gMSA-Backup (TaskUser für BMR), gMSA-Monitor (TaskUser für Monitoring), gMSA-SQLDPM (Service SQL auf WS-DPM)
- zugehörige Server:** WS-DC1.ws.its, WS-FS1.ws.its, WS-MX1.ws.its, **WS-HV1.ws.its (offline)**, WS-RA1.ws.its, WS-CA1.ws.its, WS-MX2.ws.its, WS-FS2.ws.its, WS-HV2.ws.its, WS-RA2.ws.its, WS-RDS1.ws.its, WS-RDS3.ws.its, WS-RDS2.ws.its, WS-DC2.ws.its, WS-CM.ws.its, WS-DPM.ws.its, WS-WAC.ws.its, WS-HV3.ws.its, WS-ATA.ws.its, WS-MON.ws.its, WS-HV4.ws.its (online)
- zugehörige Gruppen:** (Same as previous screenshot)

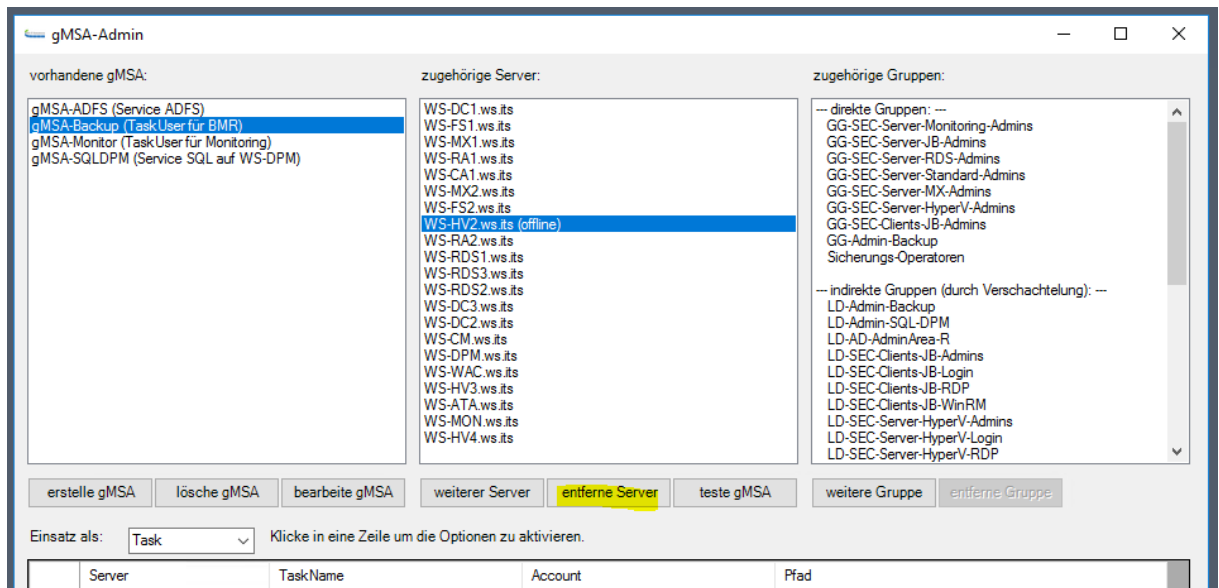
Einsatz als: Task

Server	TaskName	Account	Pfad
WS-HV4	Backup Hyper-V-Config	SYSTEM	\
WS-HV4	ServerSicherung	ws\gMSA-Backup\$	\
WS-HV4	User_Feed_Synchronisation-{69471FA...}	sysadm	\
WS-HV4	Server Initial Configuration Task	SYSTEM	\Microsoft\Windows\
WS-HV4	.NET Framework NGEN v4.0.30319	SYSTEM	\Microsoft\Windows\.NET Framework\
WS-HV4	.NET Framework NGEN v4.0.30319 64	SYSTEM	\Microsoft\Windows\.NET Framework\
WS-HV4	.NET Framework NGEN v4.0.30319 6...	SYSTEM	\Microsoft\Windows\.NET Framework\
WS-HV4	.NET Framework NGEN v4.0.30319 C...	SYSTEM	\Microsoft\Windows\.NET Framework\

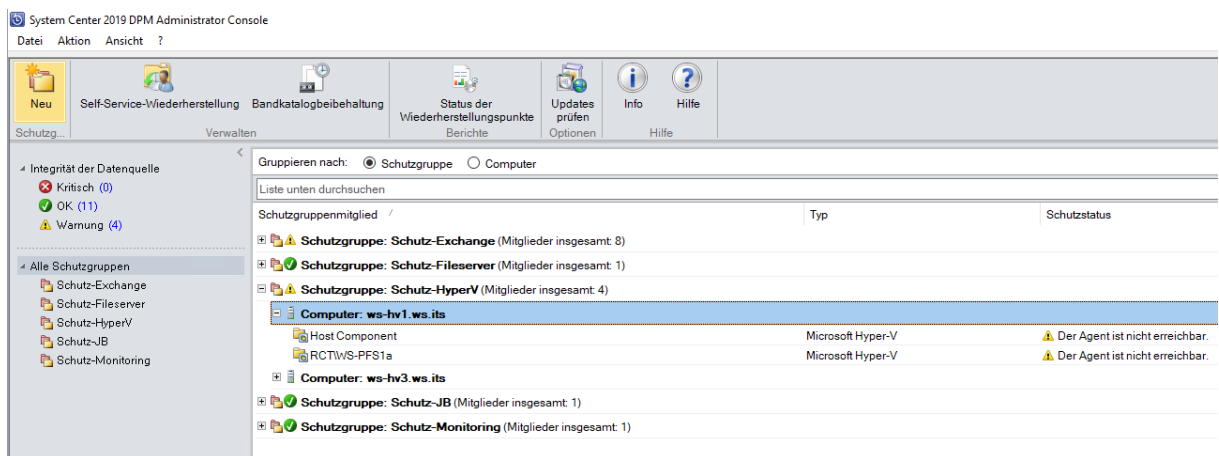
Buttons: erstelle gMSA, lösche gMSA, bearbeite gMSA, weiterer Server, **entferne Server**, teste gMSA, weitere Gruppe, entferne Gruppe

Status: bereit

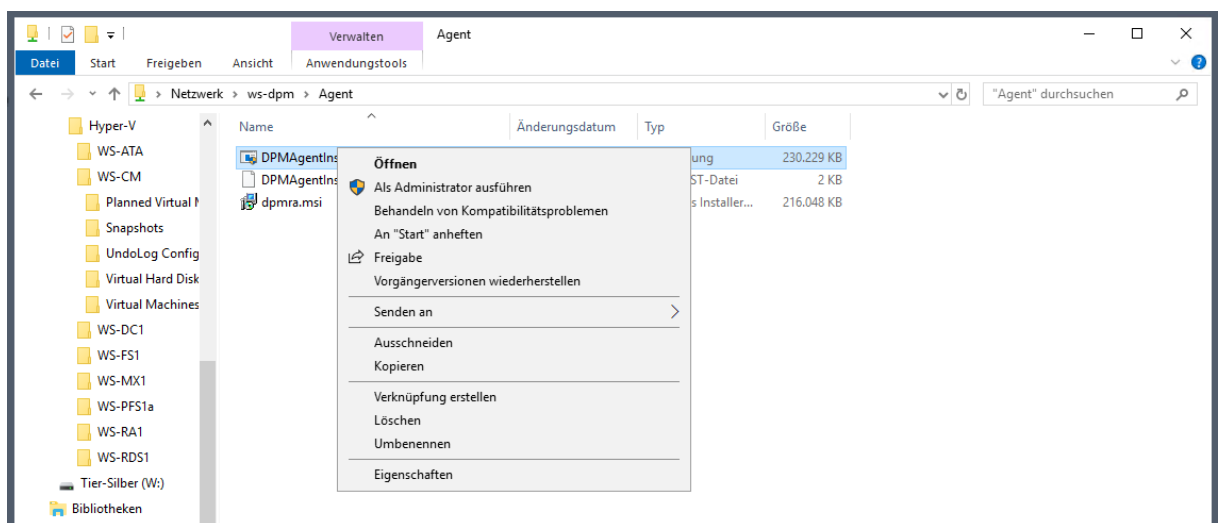
Na sowas: den alten WS-HV2 habe ich damals wohl vergessen. Dessen Entfernung hole ich gleich nach:

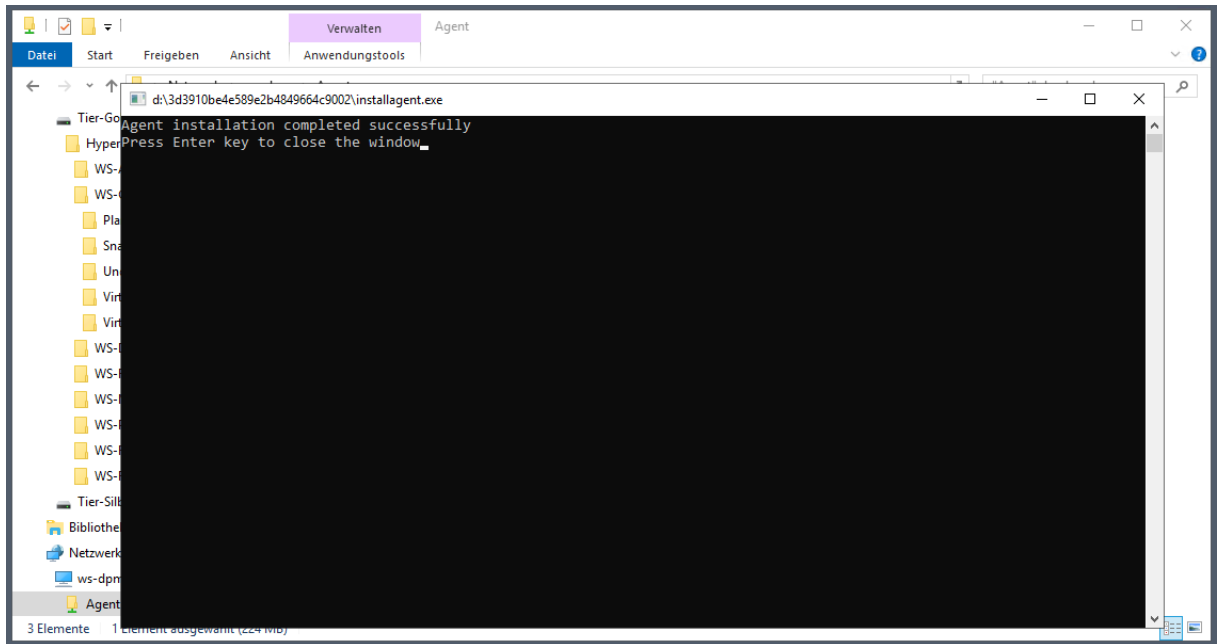


Damit ist die Datensicherung des Betriebssystems einsatzbereit. Fehlt noch die Sicherung der Nicht-Windows-VMs. Diese Aufgabe übernimmt mein System Center Data Protection Manager 2019. Dieser meldet bereits, dass der alte WS-HV1 nicht erreichbar ist:

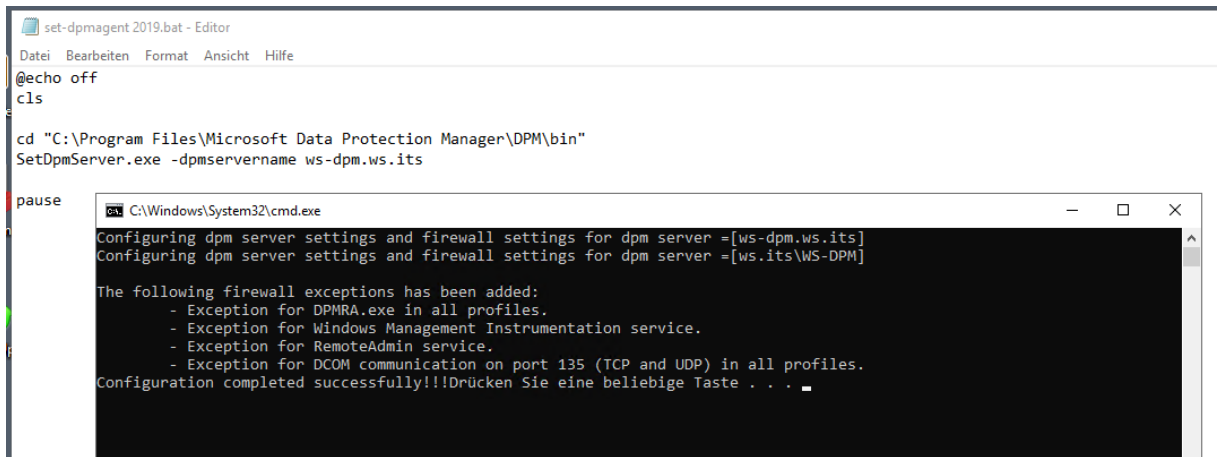


Damit der DPM die Sicherung ausführen kann, muss ich auf dem neuen Hyper-V-Host seinen Agent installieren:

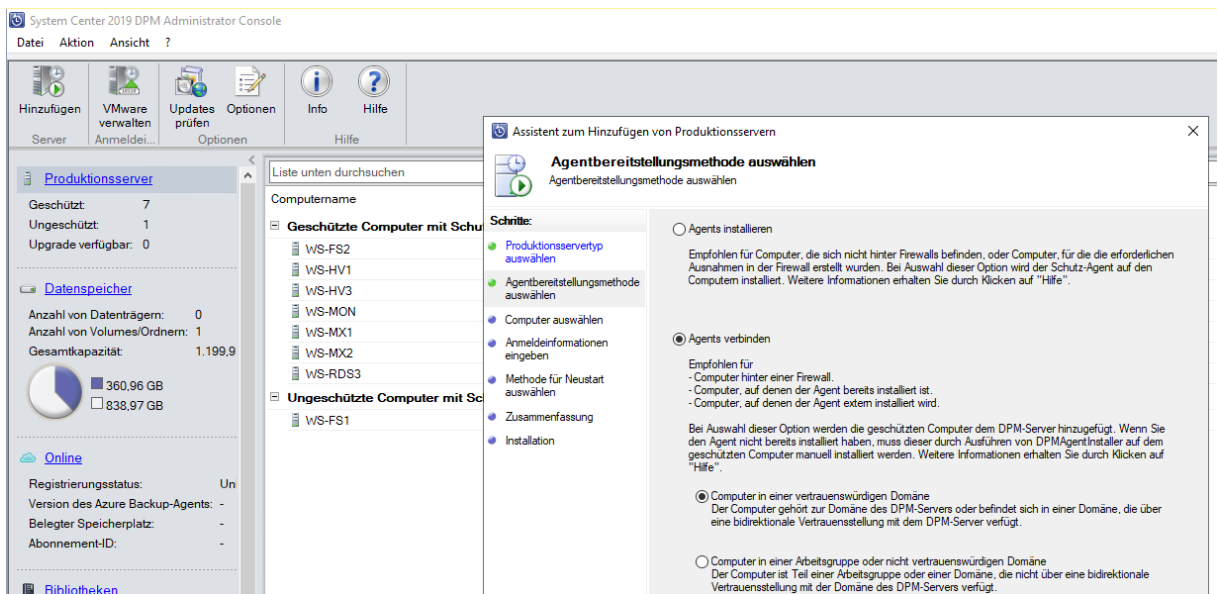




Der Agent selber wird mit einem Script auf seinen DPM geprägt. Das Script hatte ich vor einiger Zeit vorbereitet:



Nach der Konfiguration des Agent's kann ich ihn mit dem DPM verbinden:



System Center 2019 DPM Administrator Console

Assistent zum Hinzufügen von Produktionsservern

Computer auswählen
Dem DPM-Server anzufügende Computer auswählen

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-HV4/ws.its

Computer	Domäne
WS-CL5	ws.its
WS-CL7	ws.its
WS-CM	ws.its
WS-DC1	ws.its
WS-DC2	ws.its
WS-DC3	ws.its
WS-HV2	ws.its
WS-RA1	ws.its
WS-RA2	ws.its
WS-RDS1	ws.its
WS-RDS2	ws.its
WS-WAC	ws.its

System Center 2019 DPM Administrator Console

Assistent zum Hinzufügen von Produktionsservern

Anmeldeinformationen eingeben
Geben Sie die Anmeldeinformationen für ein Domänenkonto ein, das auf allen ausgewählten Computern Administratorrechte besitzt.

Geben Sie den Benutzernamen und die Domäne für ein Domänenkonto an, das über Administratorrechte auf den Computern verfügt, die Sie mit dem DPM-Server verbinden möchten.

DPM verwendet die Anmeldeinformationen zum Verbinden der Schutz-Agents.

Benutzername: admin-setup

Kenntwort: [masked]

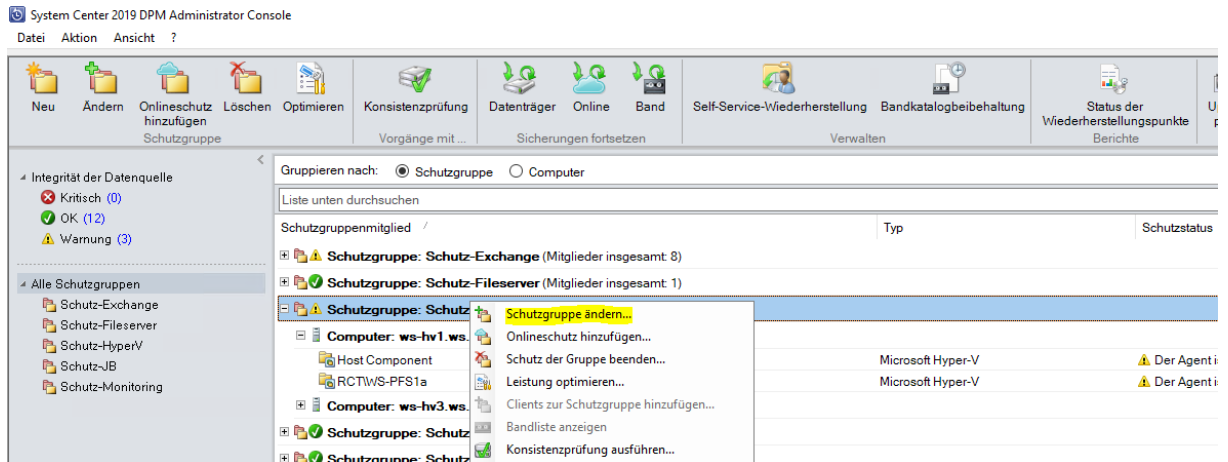
Domäne: ws.its

Danach kann der DPM auf die Speicher des Servers zugreifen:

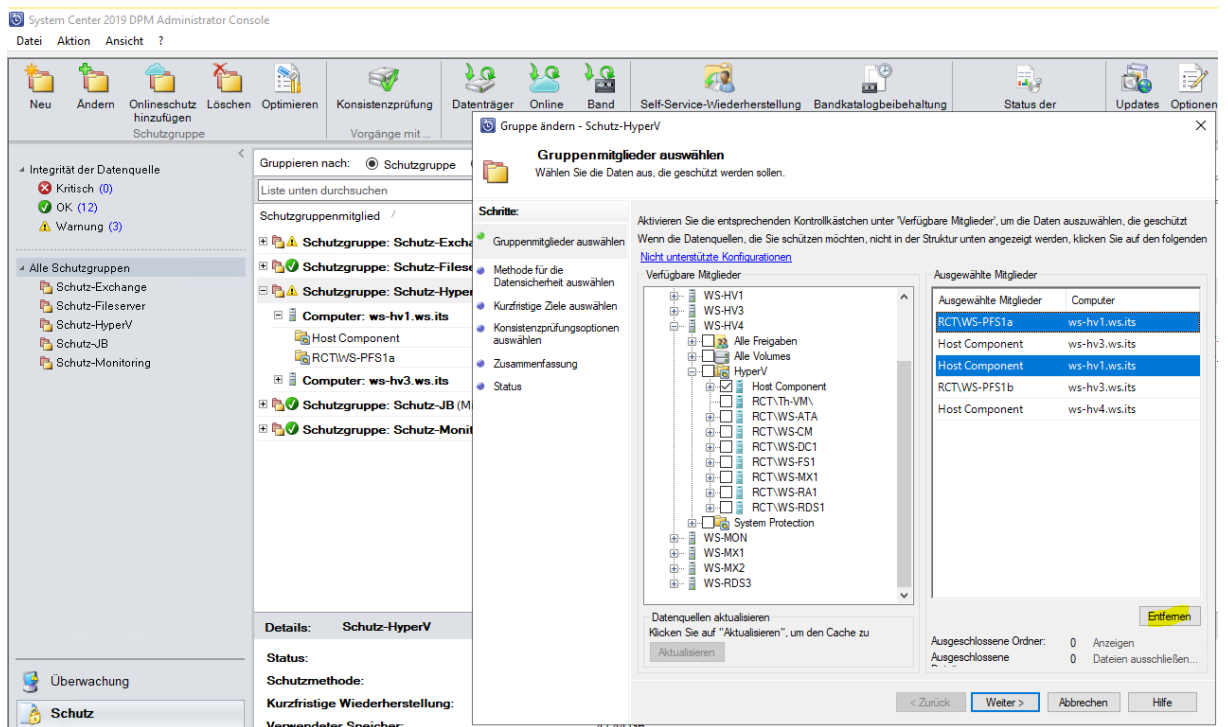
System Center 2019 DPM Administrator Console

Computername	Typ	Clustername	Domäne	Agent-Status
Geschützte Computer mit Schutz-Agent: (7 Computer)				
WS-FS2	Windows-Server	-	ws.its	Unbekannt
WS-HV1	Windows-Server	-	ws.its	Unbekannt
WS-HV3	Windows-Server	-	ws.its	Unbekannt
WS-MON	Windows-Server	-	ws.its	Unbekannt
WS-MX1	Windows-Server	DAG-1.ws.its	ws.its	Unbekannt
WS-MX2	Windows-Server	DAG-1.ws.its	ws.its	Unbekannt
WS-RDS3	Windows-Server	-	ws.its	Unbekannt
Ungeschützte Computer mit Schutz-Agent: (2 Computer)				
WS-FS1	Windows-Server	-	ws.its	Unbekannt
WS-HV4	Windows-Server	-	ws.its	OK

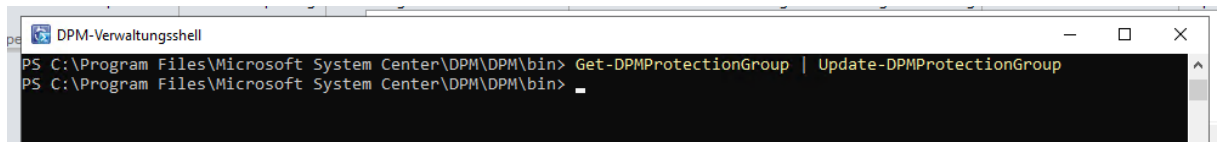
Für meine Hyper-V-Sicherung hatte ich bereits eine Schutzgruppe definiert. Aus dieser kann ich den alten Server entfernen und den neuen aufnehmen:



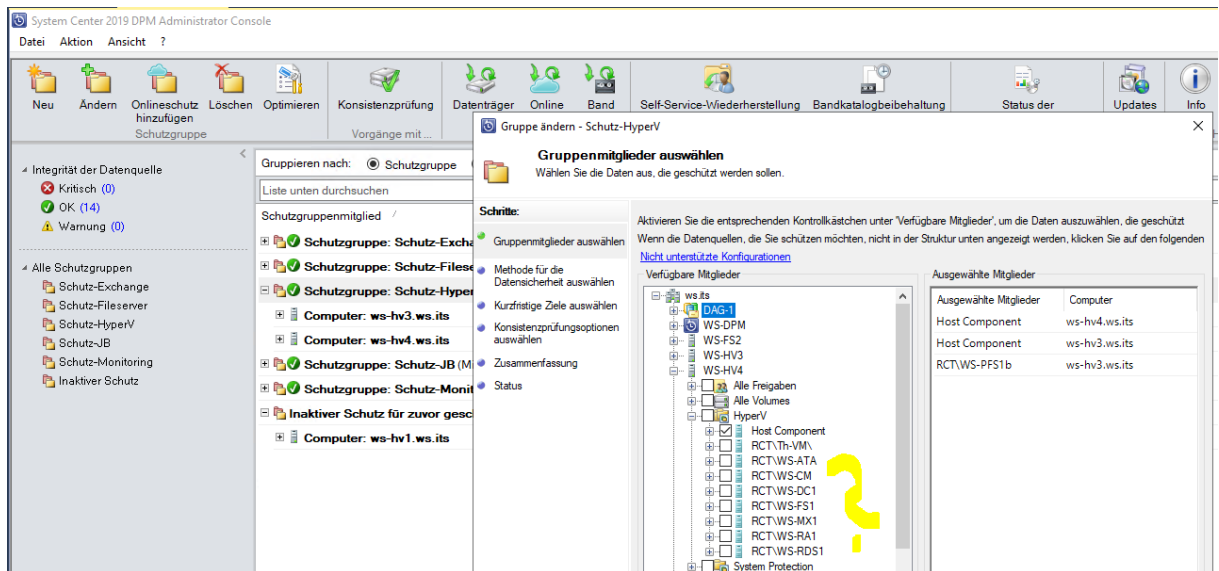
Vom alten Server hatte ich meine PFSense in die Sicherung integriert. Diese VM nehme ich heraus. Merkwürdig ist nur, dass die VM nicht im WS-HV4 angezeigt wird...



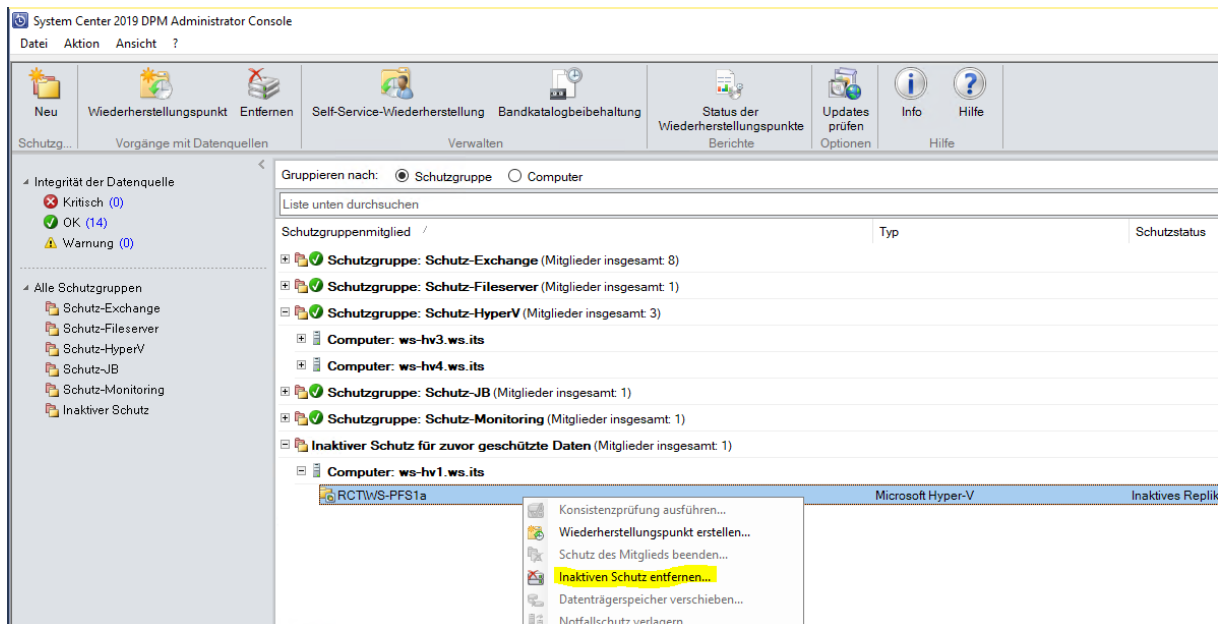
Auch der Schalter „aktualisieren“ ist nicht aktiv. Daher probiere ich es über die PowerShell auf dem DPM:



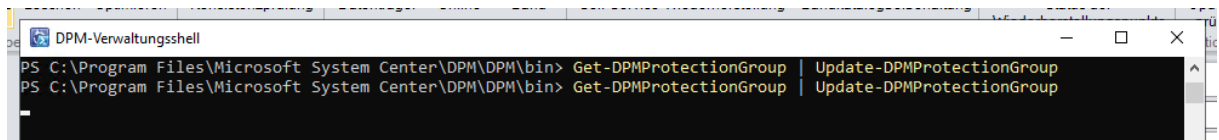
Doch die VM taucht nicht auf:



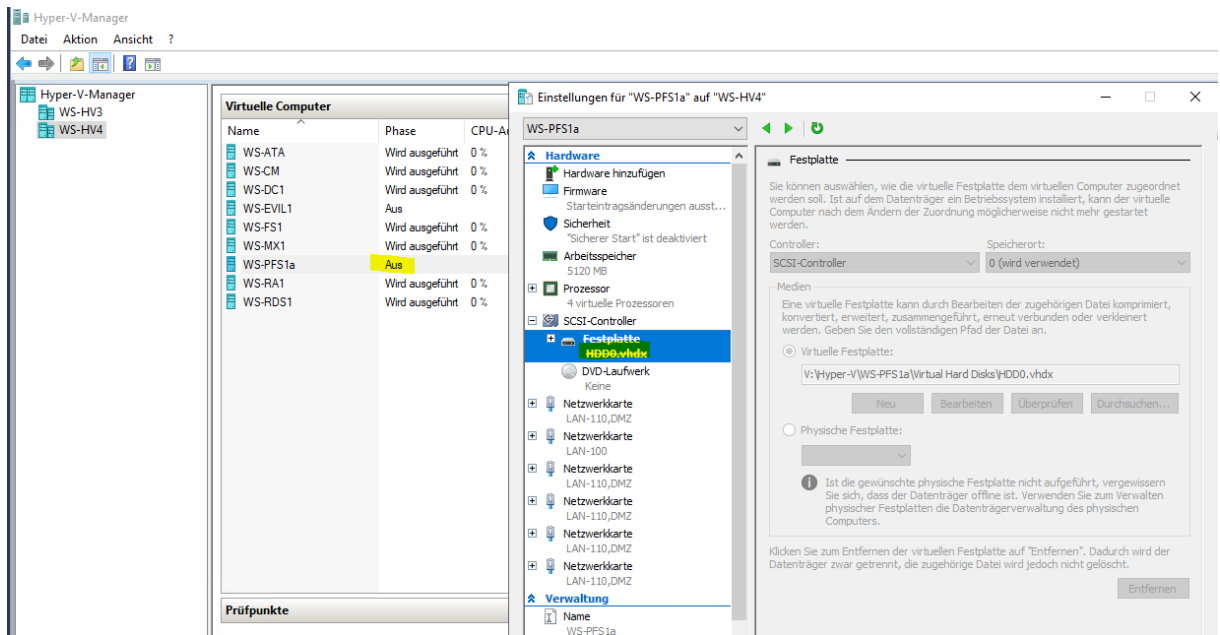
Vielleicht stört es den DPM, dass die gleiche VM jetzt auf einem anderen Host platziert ist? Ich entferne mal die jetzt getrennte Sicherung der VM:



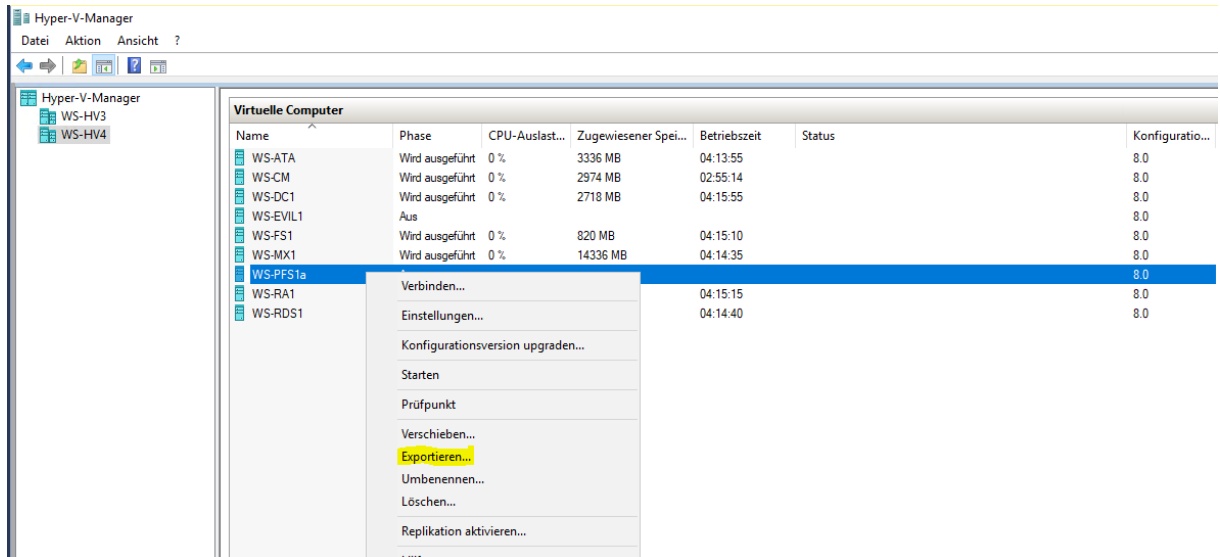
Und starte mehrere Aktualisierungen:



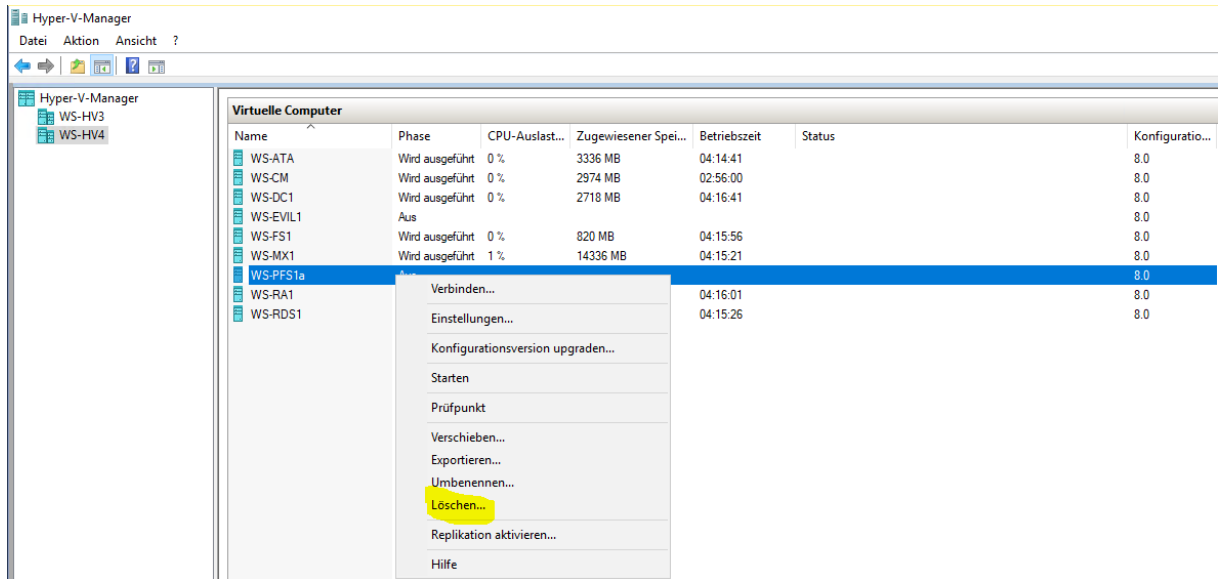
Aber die VM wird weiter nicht aufgelistet. Eine testweise erstellte, leere VM wird dagegen sofort in der Liste angezeigt. Im Netz finde ich Hinweise, dass der DPM die eindeutige VM-GUID wohl nur einmal listen kann. Und eben war sie noch dem WS-HV1 im Sicherungstask zugeordnet. Daher nehme ich die VM aus dem Hyper-V heraus und importiere sie mit einer neuen VM-GUID. Dazu starte ich in der PfSense wieder die Maintenance, fahre sie herunter und entferne die VHDX:



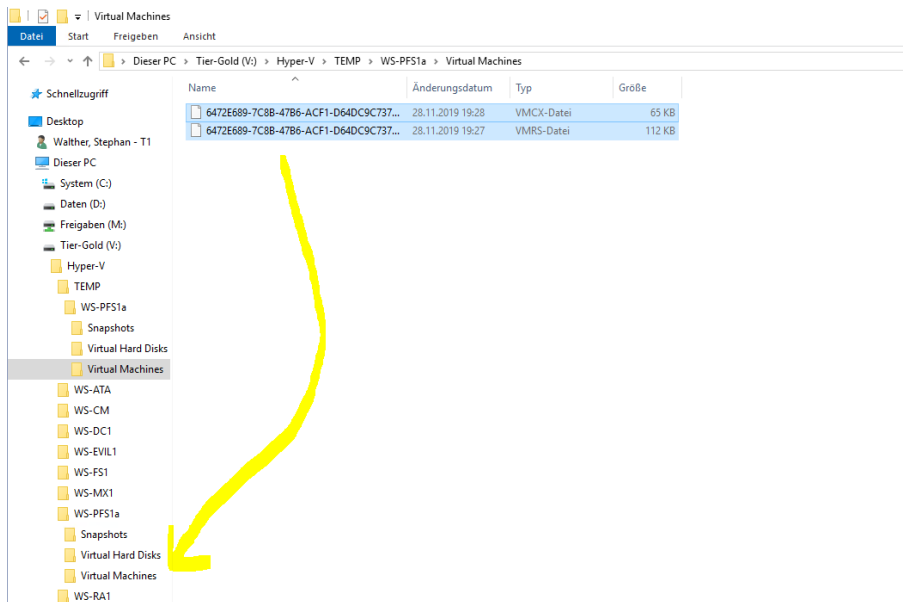
So kann ich die VM sehr schnell exportieren. Mit der eingebundenen VHDX würde er davon auch eine Kopie erstellen:



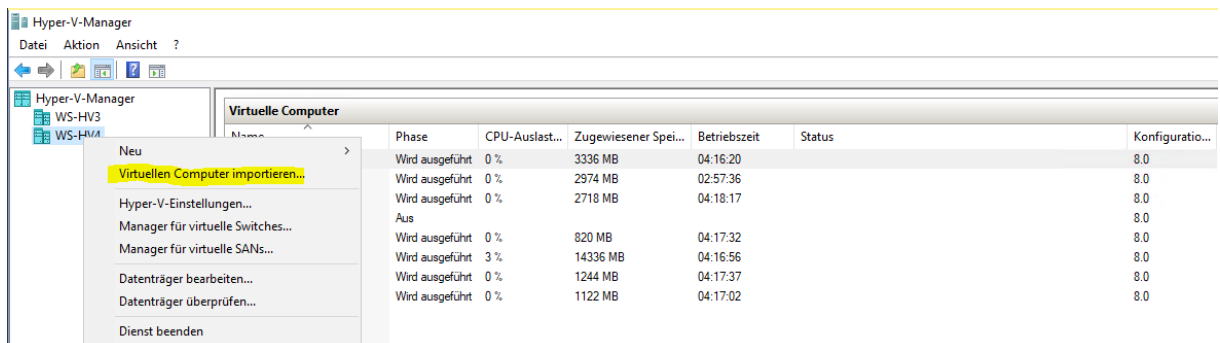
Jetzt lösche ich die aktuelle VM:



Dann verschiebe ich die Export-Dateien in das richtige Verzeichnis...



... und importiere die VM ohne ihre Festplatte. Die VM wird nun mit einer neuen VM-GUID integriert:



Hyper-V-Manager

Datei Aktion Ansicht ?

Virtuelle Computer

Name	Phase	CPU-Auslast...	Zugewiesener Spei...	Betriebszeit	Status	Konfiguratio...
WS-ATA	Wird ausgeführt	0 %	3336 MB	04:16:56		8.0
WS-CM	Wird ausgeführt	0 %	2974 MB	02:58:12		8.0
WS-DC1	Wird ausgeführt	0 %	2718 MB	04:18:53		8.0
WS-EVIL1	Aus					8.0
WS-FS1						8.0
WS-MX1						8.0
WS-RA1						8.0
WS-RDS1						8.0

Virtuellen Computer importieren

Importtyp auswählen

Vorbemerkungen

Ordner suchen

Virtuellen Computer auswählen

Importtyp auswählen

Zusammenfassung

Wählen Sie den auszuführenden Importtyp aus:

- Virtuellen Computer direkt registrieren (die vorhandene eindeutige ID verwenden)
- Virtuellen Computer wiederherstellen (die vorhandene eindeutige ID verwenden)
- Virtuellen Computer **kopieren** (neue eindeutige ID erstellen)

Hyper-V-Manager

Datei Aktion Ansicht ?

Virtuelle Computer

Name	Phase	CPU-Auslast...	Zugewiesener Spei...	Betriebszeit	Status	Konfiguratio...
WS-ATA	Wird ausgeführt	0 %	3336 MB	04:17:44		8.0
WS-CM	Wird ausgeführt	0 %	2974 MB	02:59:03		8.0
WS-DC1	Wird ausgeführt	0 %	2718 MB	04:19:44		8.0
WS-EVIL1	Aus					8.0
WS-FS1						8.0
WS-MX1						8.0
WS-RA1						8.0
WS-RDS1						8.0

Virtuellen Computer importieren

Ordner für die Dateien des virtuellen Computers auswählen

Vorbemerkungen

Ordner suchen

Virtuellen Computer auswählen

Importtyp auswählen

Ziel auswählen

Zusammenfassung

Sie können neue oder vorhandene Ordner angeben, um die Dateien des virtuellen Computers zu speichern. Andernfalls werden die Dateien in die Hyper-V-Standardordner auf diesem Computer oder in Ordner importiert, die in der Konfiguration des virtuellen Computers angegeben sind.

Virtuellen Computer an einem anderen Ort speichern

Ordner für die Konfiguration des virtuellen Computers:

V:\Hyper-V\WS-PFS1a [Durchsuchen...]

Prüfpunktspeicher:

V:\Hyper-V\WS-PFS1a [Durchsuchen...]

Ordner für Smart Paging:

V:\Hyper-V\WS-PFS1a [Durchsuchen...]

Abschließend baue ich die Festplatte wieder in die VM ein:

Hyper-V-Manager

Datei Aktion Ansicht ?

Virtuelle Computer

Name	Phase	CPU-Auslast...	Zugewiesener Spei...	Betriebszeit	Status	Konfiguratio...
WS-ATA	Wird ausgeführt	0 %	3336 MB	04:17:44		8.0
WS-CM	Wird ausgeführt	0 %	2974 MB	02:59:03		8.0
WS-DC1	Wird ausgeführt	0 %	2718 MB	04:19:44		8.0
WS-EVIL1	Aus					8.0
WS-FS1						8.0
WS-MX1						8.0
WS-PFS1a						8.0
WS-RA1						8.0
WS-RDS1						8.0

Einstellungen für "WS-PFS1a" auf "WS-HV4"

WS-PFS1a

Hardware

- Hardware hinzufügen
- Firmware
- Sicherheit
- Arbeitsspeicher
- Prozessor
- SCSI-Controller
- Festplatte**
- DVD-Laufwerk
- Netzwerkarte

Festplatte

Sie können auswählen, wie die virtuelle Festplatte dem virtuellen Computer zugeordnet werden soll. Ist auf dem Datenträger ein Betriebssystem installiert, kann der virtuelle Computer nach dem Ändern der Zuordnung möglicherweise nicht mehr gestartet werden.

Controller: SCSI-Controller Speicherort: 0 (wird verwendet)

Medien

Eine virtuelle Festplatte kann durch Bearbeiten der zugehörigen Datei komprimiert, konvertiert, erweitert, zusammengeführt, erneut verbunden oder verkleinert werden. Geben Sie den vollständigen Pfad der Datei an.

Virtuelle Festplatte:

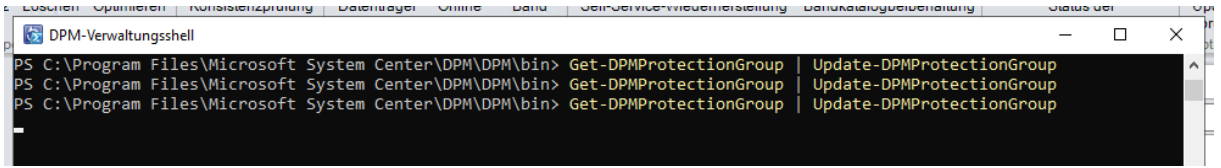
V:\Hyper-V\WS-PFS1a\Virtual Hard Disks\HDD0.vhdx

Physische Festplatte:

Ist die gewünschte physische Festplatte nicht aufgeführt, vergewissern Sie sich, dass der Datenträger offline ist. Verwenden Sie zum Verwalten physischer Festplatten die Datenträgerverwaltung des physischen Computers.

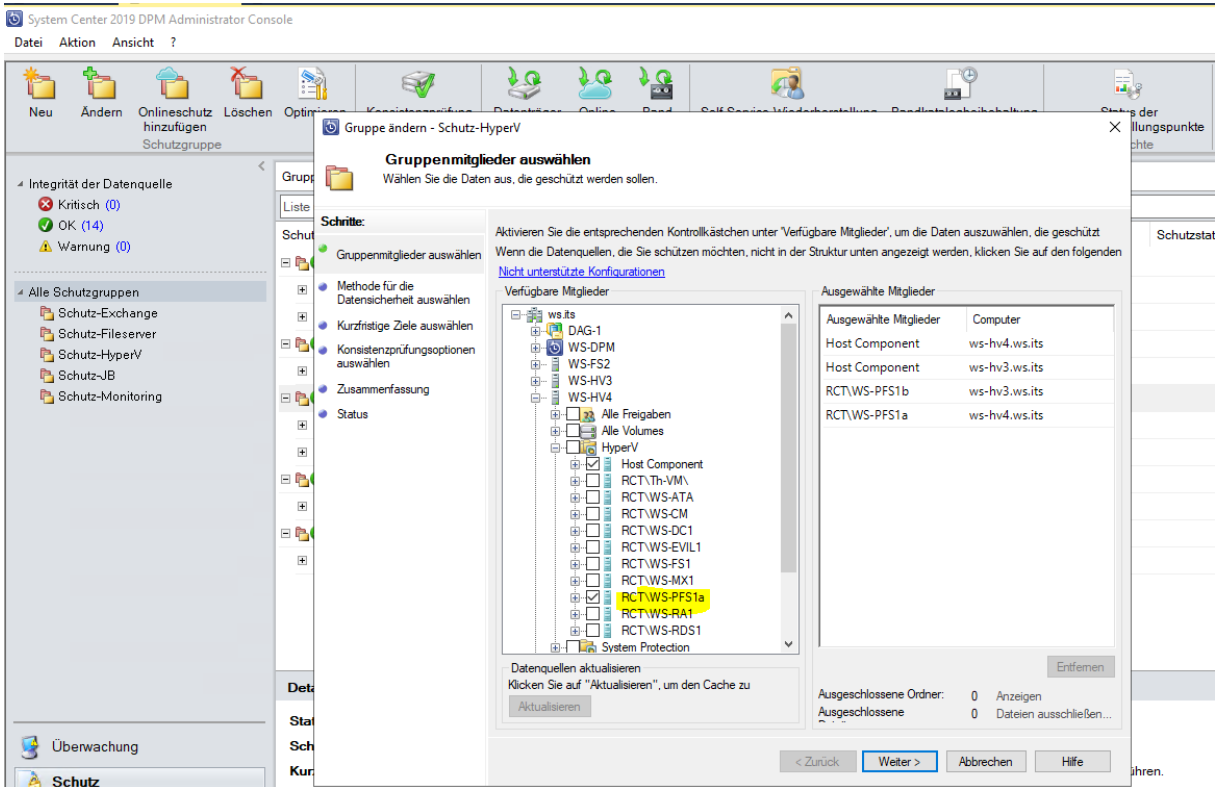
Klicken Sie zum Entfernen der virtuellen Festplatte auf "Entfernen". Dadurch wird der Datenträger zwar getrennt, die zugehörige Datei wird jedoch nicht gelöscht.

Jetzt bekommt der DPM noch einige Update-Aufgaben:

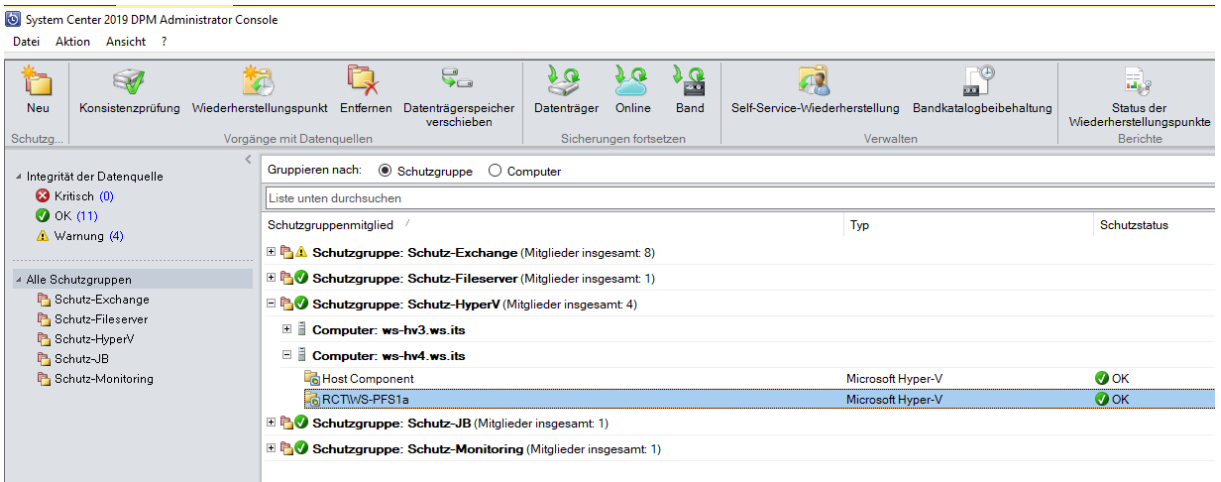


Aber nichts ändert sich: Die VM wird weiter nicht gelistet. OK, das muss für heute genügen.

Am nächsten Tag prüfe ich erneut: und die VM ist in der Liste. Ehrlich, ich hab keine Ahnung, was das war. Aber jetzt kann ich die Sicherung fertig konfigurieren:



Ein paar Minuten später ist die initiale Sicherung abgeschlossen:



Nun entferne ich noch die Agentverbindungen zu den nicht mehr vorhandenen Servern. Das geht auch in Version 2019 immer noch nicht in der grafischen Oberfläche:

Computername	Typ	Clustername	Domäne	Agent-Status
Geschützte Computer mit Schutz-Agent: (7 Computer)				
WS-FS2	Windows-Server	-	ws.its	OK
WS-HV3	Windows-Server	-	ws.its	OK
WS-HV4	Windows-Server	-	ws.its	OK
WS-MON	Windows-Server	-	ws.its	OK
WS-MX1	Windows-Server	DAG-1.ws.its	ws.its	OK
WS-MX2	Windows-Server	DAG-1.ws.its	ws.its	OK
WS-RDS3	Windows-Server	-	ws.its	OK
Ungeschützte Computer mit Schutz-Agent: (2 Computer)				
WS-FS1	Windows-Server	-	ws.its	Fehler
WS-HV1	Windows-Server	-	ws.its	Nicht verfügbar

Diese Aktion läuft nur in der PowerShell ohne Fehler durch:

```

PS C:\> cd -C:\Program Files\Microsoft System Center\DPM\bin\
PS C:\Program Files\Microsoft System Center\DPM\bin> .\dpmcliinitscript.ps1

Willkommen

Vollständige Cmdlets-Liste: Get-Command
Nur DPM-Cmdlets: Get-DPMCommand
Allgemeine Hilfe: help
Cmdlet-Hilfe: help <Cmdlet-Name> oder <Cmdlet-Name> -?
Cmdlet-Definition: Get-Command <Cmdlet-Name> -Syntax
DPM-Beispielskripts: Get-DPMsampleScript

PS C:\Program Files\Microsoft System Center\DPM\bin> cd\
PS C:\> Remove-ProductionServer.ps1 -DPMServerName ws-dpm.ws.its -PSName ws-fs1.ws.its
WARNUNG: Die Verbindung mit DPM-Server "ws-dpm.ws.its" wird hergestellt.
Removed ProductionServer successfully
PS C:\> Remove-ProductionServer.ps1 -DPMServerName ws-dpm.ws.its -PSName ws-hv1.ws.its
WARNUNG: Die Verbindung mit DPM-Server "ws-dpm.ws.its" wird hergestellt.
Removed ProductionServer successfully
PS C:\>
    
```

Jetzt sind nur noch aktive Server gelistet:

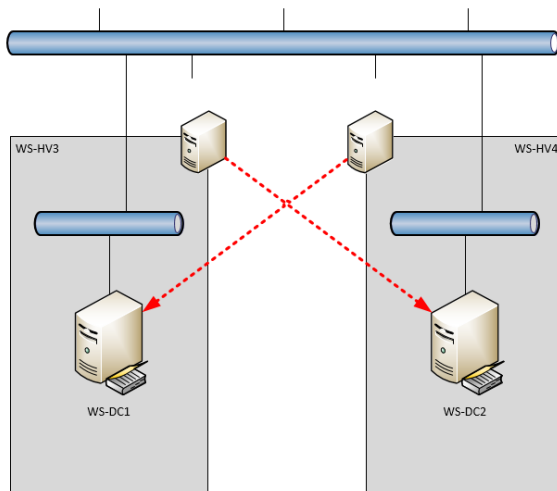
Computername	Typ	Clustername	Domäne	Agent-Status
Geschützte Computer mit Schutz-Agent: (7 Computer)				
WS-FS2	Windows-Server	-	ws.its	OK
WS-HV3	Windows-Server	-	ws.its	OK
WS-HV4	Windows-Server	-	ws.its	OK
WS-MON	Windows-Server	-	ws.its	OK
WS-MX1	Windows-Server	DAG-1.ws.its	ws.its	OK
WS-MX2	Windows-Server	DAG-1.ws.its	ws.its	OK
WS-RDS3	Windows-Server	-	ws.its	OK

Einrichtung des Noffallzugangs

Vorgeschichte

Ich hatte einmal ein Problem, dass durch meine Absicherungsmaßnahmen entstand: Meine Hyper-V-Hosts sind Mitglied in meiner Active Directory Domain. Jeder Host betreibt dabei einen Domain Controller in einer VM. Im Normalbetrieb ist das kein Problem. Auch beim Neustart eines Hosts kann dieser immer noch die Dienste des DC auf dem anderen Hosts ansprechen und sauber hochfahren. Sind aber beide Hosts ausgeschaltet (z.B. wegen einer geplanten, mehrstündigen Unterbrechung der Stromversorgung), dann wird es interessant.

So schaut das Abhängigkeitsschema beim Neustart aus:



Natürlich habe ich einen Wiederanlaufplan:

1. Ich starte einen Host und warte, bis dessen VMs (mit einem Domain Controller) gestartet sind. Der Host selber ist ohne Active Directory gestartet.
2. Dann starte ich den anderen Host. Dieser kann normal mit Active Directory hochfahren, da der DC auf dem anderen Host erreichbar ist. So kann auch der zweite Domain Controller als VM auf dem zweiten Host starten.
3. Dann fahre ich die VMs des ersten Hosts herunter und starte diesen neu.
4. Beim Neustart kann nun auch der erste Host eine Verbindung zum Active Directory über den Domain Controller des zweiten Hosts herstellen.
5. Dann werden die VMs des ersten Hosts gestartet und alles ist wieder im Normalbetrieb.

Das Problem

In der Theorie klingt das gut. Und auch in der Praxis hatte ich dieses Szenario schon mehrfach erfolgreich ausgeführt. Wo ist das Problem? Dieses begann mit der Ankündigung unseres Stromversorgers, dass die Versorgung mehrere Stunden aufgehoben wird. Das schaffen meine USV nicht. Also habe ich mich an dem Tag von außen aufgeschaltet und wollte beide Hosts mit allen VMs herunterfahren. Blöd war nur, dass ich versehentlich den Host zuerst herunterfuhr, über den ich von außen aufgeschaltet war. Somit konnte ich den anderen Host nicht mehr ansprechen.

Na gut, dann übernimmt das eben die USV, kurz bevor sie keine Ladung mehr hat. Das funktionierte auch. Leider kam dann der zweite unglückliche Umstand: der Versorger schaltete den Strom wieder ein und der Host startete wieder automatisch. Dann wurde die Versorgung aber wieder unterbrochen – während der Host startete. Die USV hatte keine Ladung mehr und so wurde der Host ohne Strom hart ausgeschaltet.

Danach startete er die VMs nicht mehr von allein. Der andere Host und dessen VMs wurde davon irgendwie durcheinandergebracht. Also ging nichts mehr.

Die Lösungsversuche

Na gut, dann wollte ich mich eben am Abend lokal anmelden und den VMs Starthilfe geben. Aber aus Sicherheitsgründen ist mein ServerAdmin-Account Mitglied in der Gruppe „Protected Users“. Für diese ist keine Zwischenspeicherung einer Anmeldung erlaubt. Ein Computer verhält sich daher so, als ob der Benutzer sich noch nie angemeldet hat: Er muss einen Domain Controller kontaktieren. Schade, denn diese waren ja nicht an...

OK, dann nimm ich den lokalen Administrator des Hosts für die Anmeldung. Der braucht kein Active Directory. Aber (mal wieder) aus Sicherheitsgründen verwende ich LAPS (Local Administrator Password Solution), um von allen lokalen Admins regelmäßig das Passwort automatisch zu ändern. Das jeweils gültige wird dabei – haltet euch fest – im Computerkonto im Active Directory gespeichert. Und die sind ja nicht erreichbar...

Meine letzte Option war mein 3. Domain Controller in meinem Außenstandort. Dieser ist über ein Site-To-Site-VPN erreichbar. Dazu musste ich aber mein Netzwerk überbrücken, denn meine virtuelle Firewall lief ja auch nicht. Über mehrere Hops bin ich endlich auf die Oberfläche meines Server Core gelangt. Dort konnte ich dann mit der PowerShell das aktuelle Passwort des lokalen Administrators auslesen. Mit diesem konnte ich mich endlich am Hyper-V-Host anmelden, das Problem beim VM-Start beheben, meine VMs starten und die Infrastruktur wieder in den Normalbetrieb überführen.

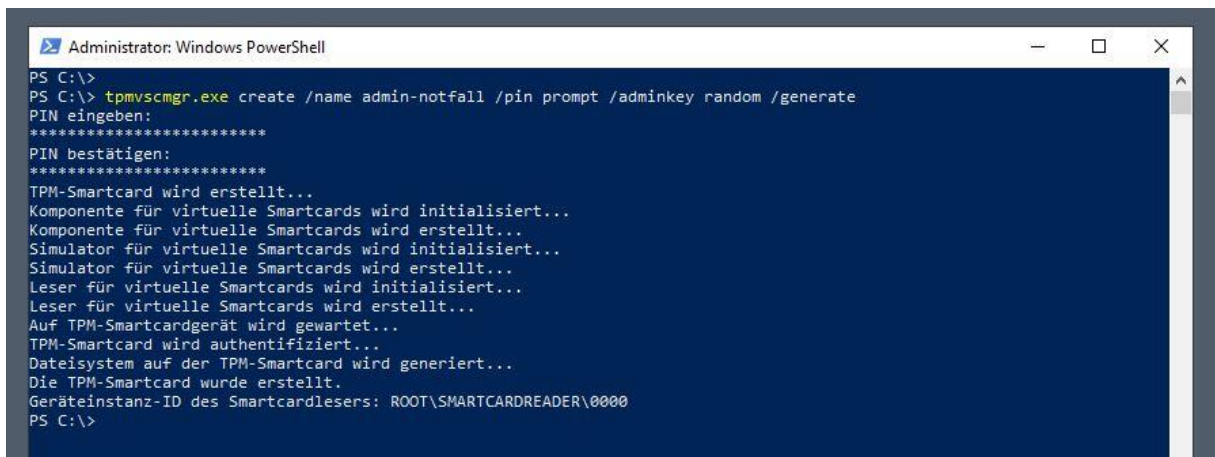
Aber es war schon recht knapp.

Implementierung des Notfallplans

Danach wollte ich eine Lösung für vergleichbare, zukünftige Ereignisse schaffen. Aber bitte ohne meine Sicherheitsmechanismen wieder zurückzubauen. Die Lösung besteht aus einem minimal berechtigten Account, der sich mit einer starken Authentifizierung OHNE Active Directory am Host lokal anmelden kann und die VMs wieder fit macht. Das Ziel erreiche ich mit einer virtuellen Smartcard.

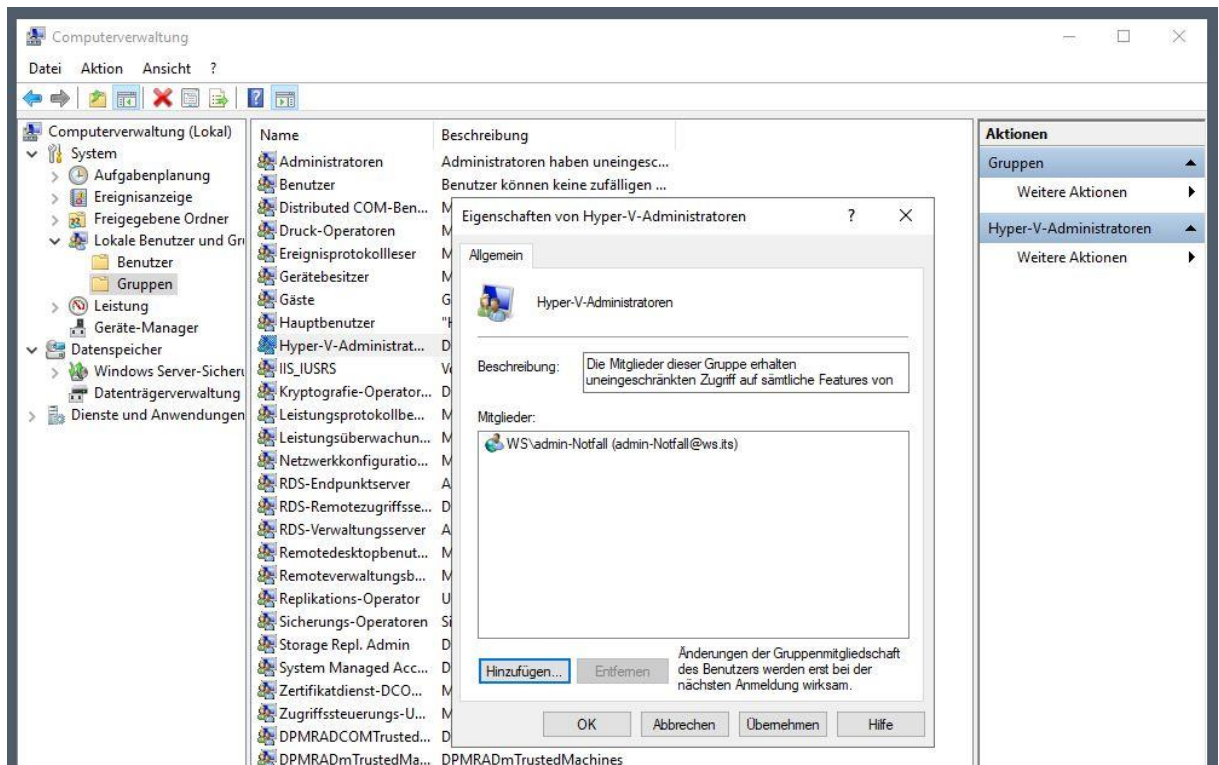
Auf meinem neuen Server möchte ich das gerne einbauen. Der TPM-Chip ist einsatzbereit. Auf diesem wird die virtuelle Smartcard sicher abgelegt.

Zuerst erstelle ich als Serveradministrator eine neue, virtuelle SmartCard. Dafür gibt es einen cmd-Befehl:

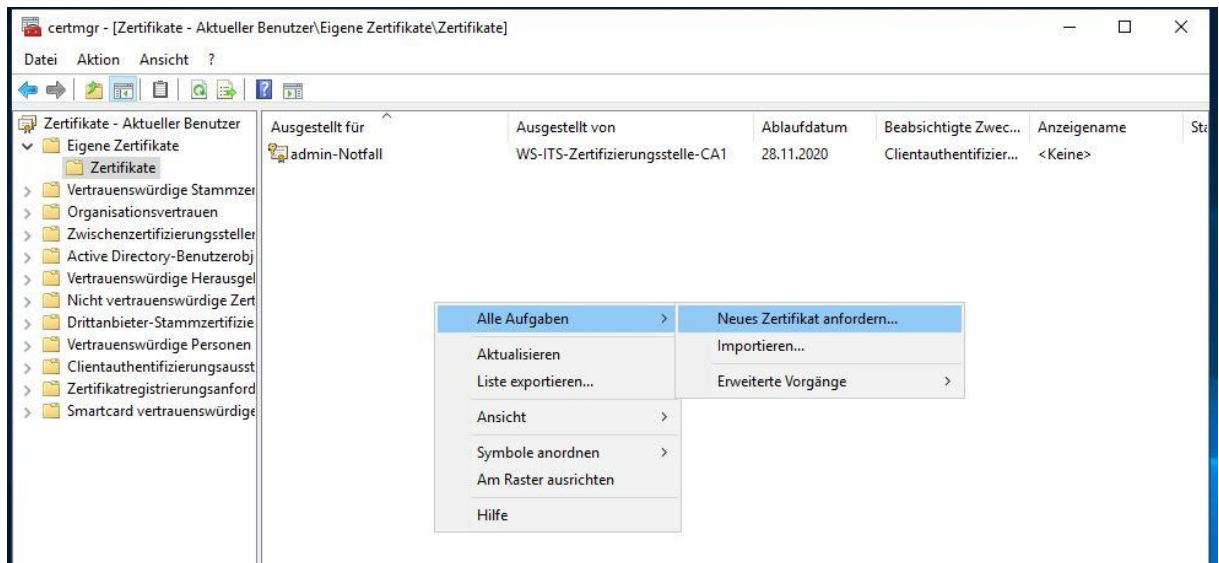


```
Administrator: Windows PowerShell
PS C:\>
PS C:\> tpmvscmgr.exe create /name admin-notfall /pin prompt /adminkey random /generate
PIN eingeben:
*****
PIN bestätigen:
*****
TPM-Smartcard wird erstellt...
Komponente für virtuelle Smartcards wird initialisiert...
Komponente für virtuelle Smartcards wird erstellt...
Simulator für virtuelle Smartcards wird initialisiert...
Simulator für virtuelle Smartcards wird erstellt...
Leser für virtuelle Smartcards wird initialisiert...
Leser für virtuelle Smartcards wird erstellt...
Auf TPM-Smartcardgerät wird gewartet...
TPM-Smartcard wird authentifiziert...
Dateisystem auf der TPM-Smartcard wird generiert...
Die TPM-Smartcard wurde erstellt.
Geräteinstanz-ID des Smartcardlesers: ROOT\SMARTCARDREADER\0000
PS C:\>
```

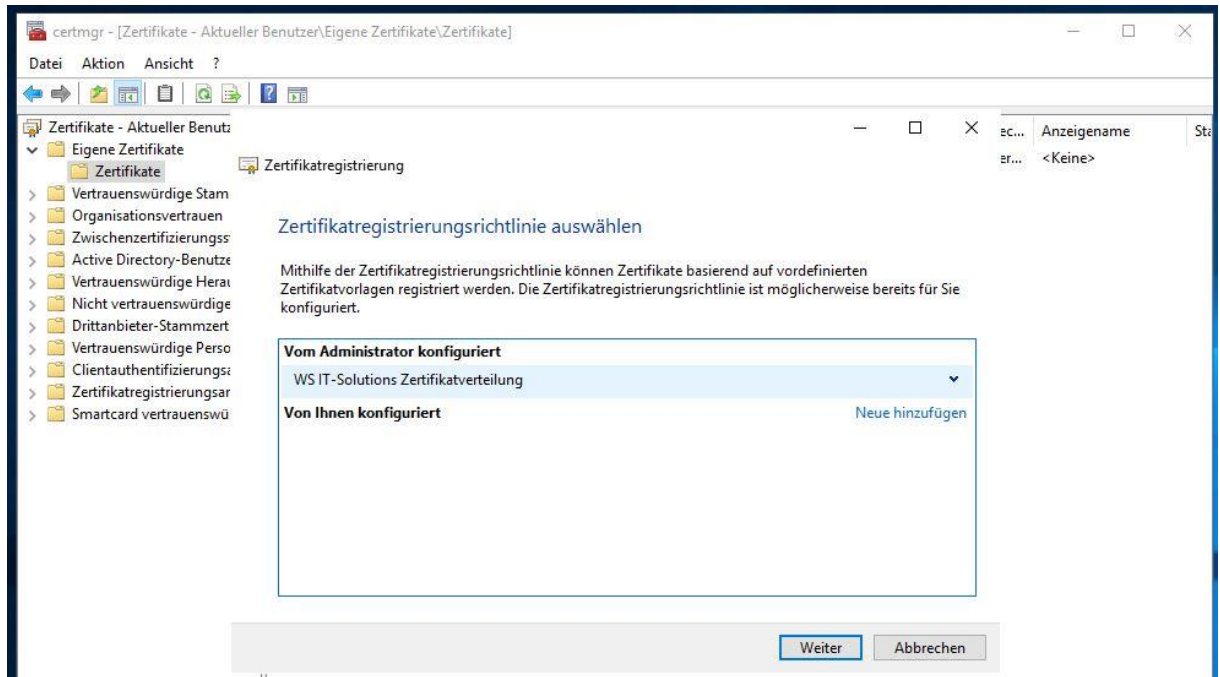
Bei diesem Prozess wird eine PIN abgefragt. Diese muss ich später als „Passwort“ bei der Notfallanmeldung eingeben. Mein Account heißt Admin-Notfall. Diesen trage ich als Mitglied in die Gruppe „Hyper-V-Administratoren“ ein. Damit kann ich mit dieser Kennung troubleshooten:



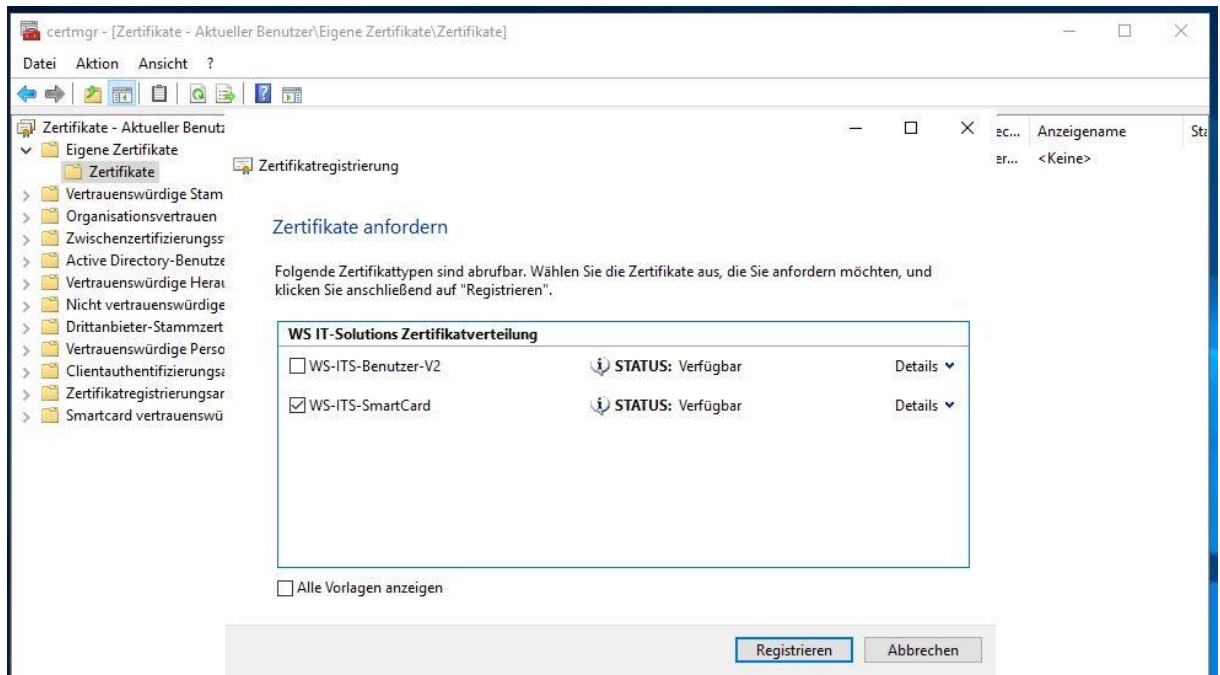
Jetzt melde ich mich mit der Kennung admin-notfall am Server an. Danach starte ich die certmgr.msc-Konsole, um ein persönliches Zertifikat bei meiner PKI anzufragen:



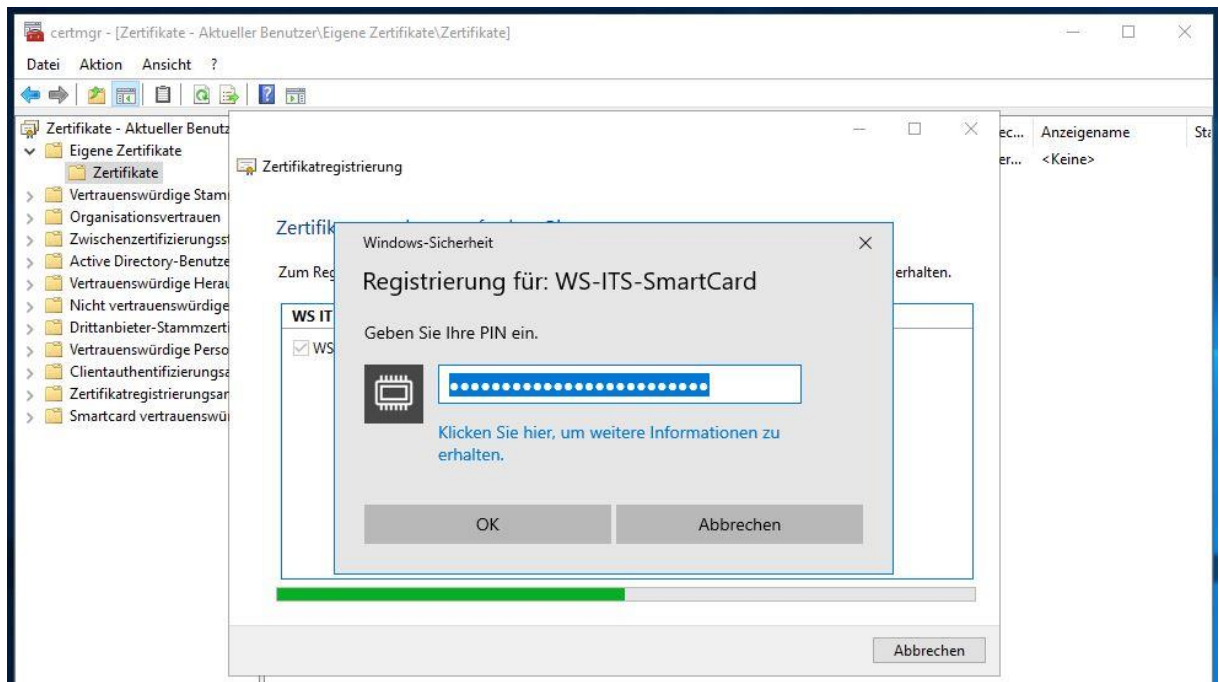
Der Request sucht über meine eigene Policy nach der PKI:



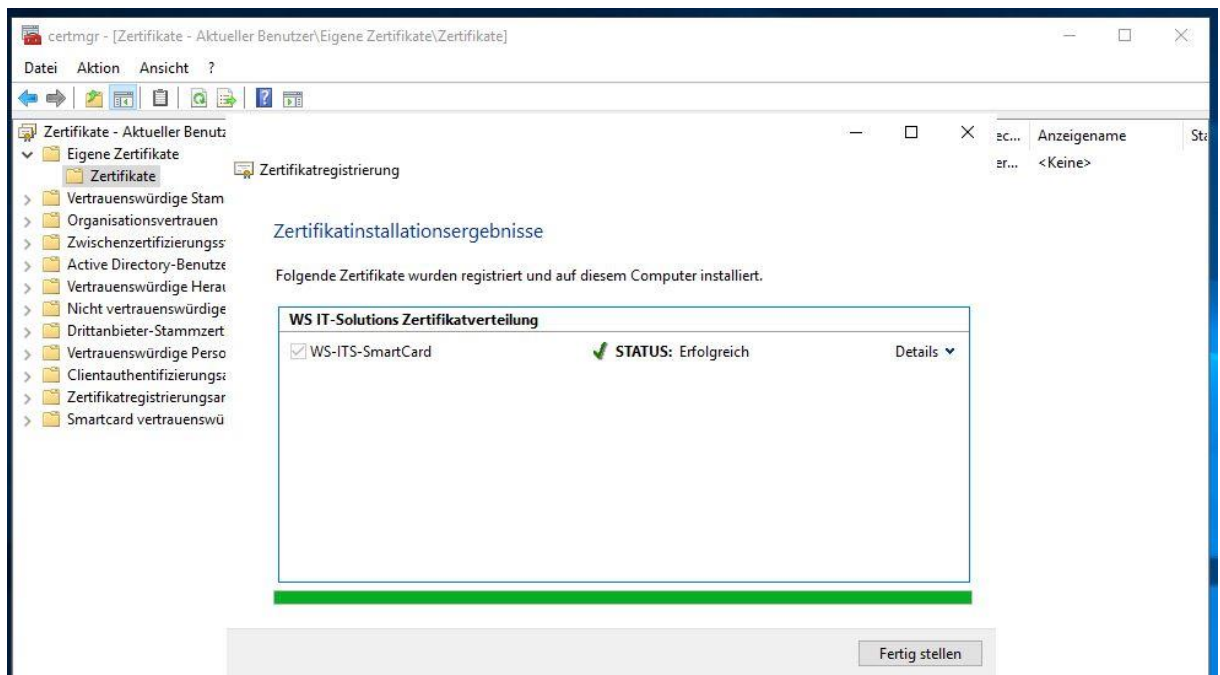
Die Vorlage ist bereits für diesen Account aktiviert. Daher kann ich sie einfach auswählen:



In der Vorlage ist hinterlegt, dass das Schlüsselmaterial des Zertifikates in einer Smartcard gespeichert werden muss. Der Wizzard sucht nach einer freien SC und findet die vorbereitete, virtuelle Instanz. Zur Verifizierung wird aber noch das zuvor festgelegte Passwort (die PIN) abgefragt:



Danach generiert die vSmartcard die Schlüssel, der Wizard sendet den Request an die PKI, diese signiert den Request und sendet das Ergebnis an den Wizard zurück. Dieser schließt dann den Vorgang ab:



Nun melde ich mich ab und über die Smartcard-PIN wieder an. Das funktioniert einwandfrei. Naja, der Domain Controller ist ja auch erreichbar... Das genügt aber nicht für einen Notfall! Dieser muss unter realen Bedingungen geprüft werden.

Realer Testlauf:

Es sind ein paar Vorbereitungsschritte erforderlich:

- Zuerst fahre ich die VMs des Hosts herunter.
- Dann rekonfiguriere ich den virtuellen Switch meines Servernetzwerkes als privaten Switch. So kommt der Host nicht mehr an die VMs heran.
- Als nächstes trenne ich die Netzwerkverbindungen zum Host. So kommt er auch nicht mehr an den anderen Domain Controller heran.

Jetzt gibt es keine Möglichkeit mehr für eine normale Anmeldung! Ich starte das System und entsperre mit der PIN die vSmartCard. Mit dieser lässt mich das System herein. Danach gehe ich in die Hyper-V-Konsole und rekonfiguriere den vSwitch (ein Standardbenutzer mit der Gruppenmitgliedschaft „Hyper-V-Admin“ darf das). Die VMs wurde bereits gestartet und sind jetzt auch wieder erreichbar.

Danach gibt es natürlich mein Procedere für einen sauberen Neustart mit realem Netzwerkanschluss.

Notfallkonzepte sind wichtig. Aber wichtiger als das Papier, auf dem sie beschrieben stehen ist ein erfolgreicher Testlauf unter realen Bedingungen!!!

Zusammenfassung

Auch wenn dieses Mal nicht so viele Seiten zusammengekommen sind: es war viel Arbeit. Aber es hat sich gelohnt:

- Ein weiterer Server läuft bei mir mit dem Betriebssystem Windows Server 2019
- Meine Hardware ist wieder UpToDate und fit für die nächsten Jahre.