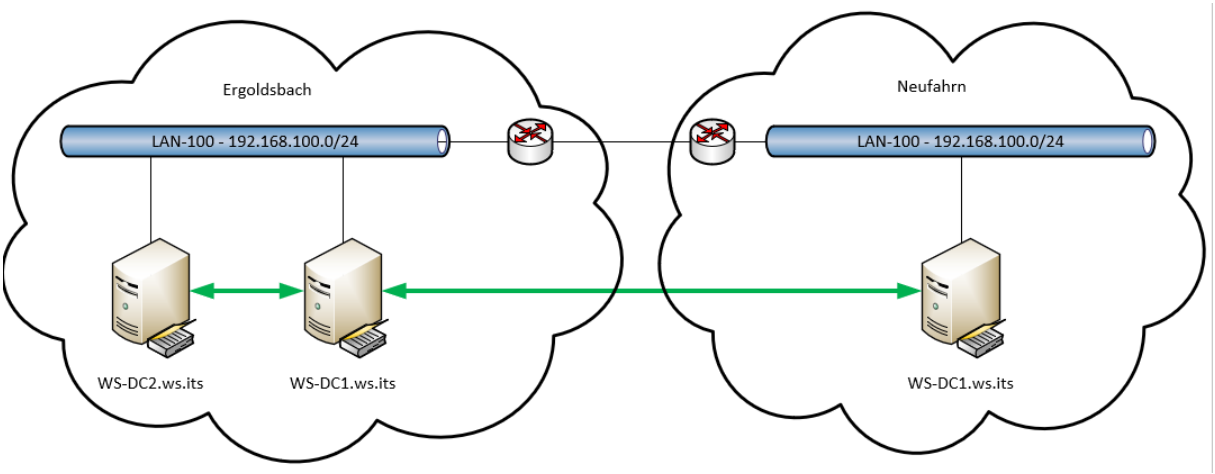
Inhalt

Zielsetzung

IST-Situation

Vor einigen Tagen habe ich meinen ersten Domain Controller auf Windows Server 2019 aktualisiert. Die beiden anderen DCs laufen noch mit Windows Server 2016.

Mein Active Directory arbeitet über zwei Standorte. Die Domain Controller haben dabei ein festes Replikations-Schema:



Die beiden DCs in Ergoldsbach haben eine grafische Oberfläche. Der WS-DC3 ist als Server Core installiert worden. Meine Gesamtstruktur arbeitet mit der Funktionsebene Windows Server 2016.

Im Hauptstandort Ergoldsbach sind alle Server und Services so konfiguriert, dass ich einen der beiden DCs ausschalten kann. Beide Server wurden also überall als DNS-Server angegeben. Der DHCP-Service ist über DHCP-Failover ausfallsicher. Der IPHelper in meiner PFSense spricht beide DHCP-Server an.

Alle Domain Controller laufen als virtuelle Maschine – jede hat dabei ihren eigenen Hyper-V-Host darunter.

Alle zusätzlichen Services wurden im Vorfeld entfernt: Beide DCs in Ergoldsbach stellten einmal eine ADFS-Farm bereit. Die beiden Server sind aber Teil meiner Privileged Access Management Lösung und stellen deren Kernfunktion durch ein Just-Enough-Administration-Enpunkt (JEA) zur Verfügung.

Soll-Situation

Heute soll der Domain Controller WS-DC2 auf Windows Server 2019 aktualisiert werden. Dabei müssen die Services Active Directory Domain Controller, DNS und DHCP migriert werden.

Die Namen und die IP-Adressen der Domain Controller möchte ich wiederverwenden. So spare ich mir den Aufwand, jeden (!) Service und jedes Gerät zu rekonfigurieren.

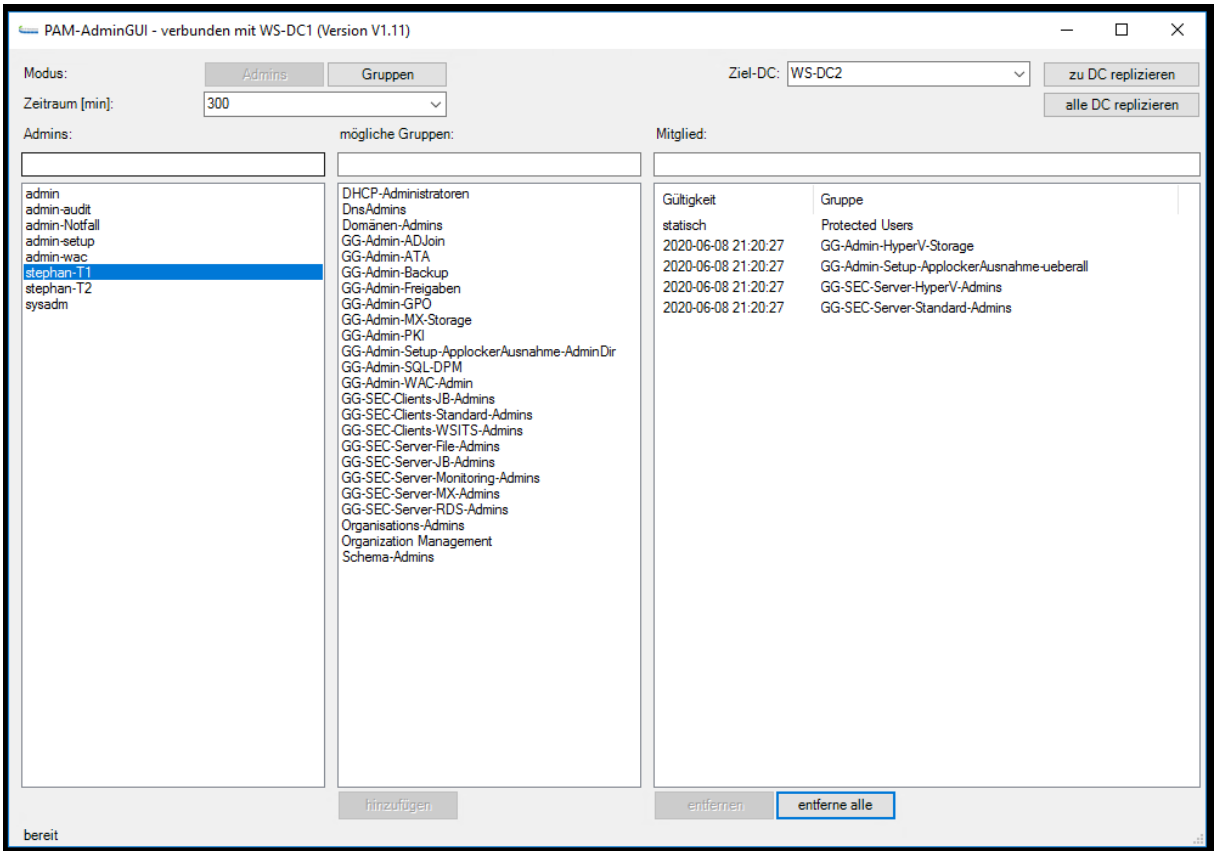
Migrationsplan

Wie beim ersten Server auch kommt hier ein Wipe & Load Szenario zur Anwendung: Zuerst entferne ich den alten Server aus meiner Infrastruktur. Anschließend installiere ich einen neuen Server mit den gleichen Namen und der gleichen IPv4-Konfiguration und richte die Services wieder ein.

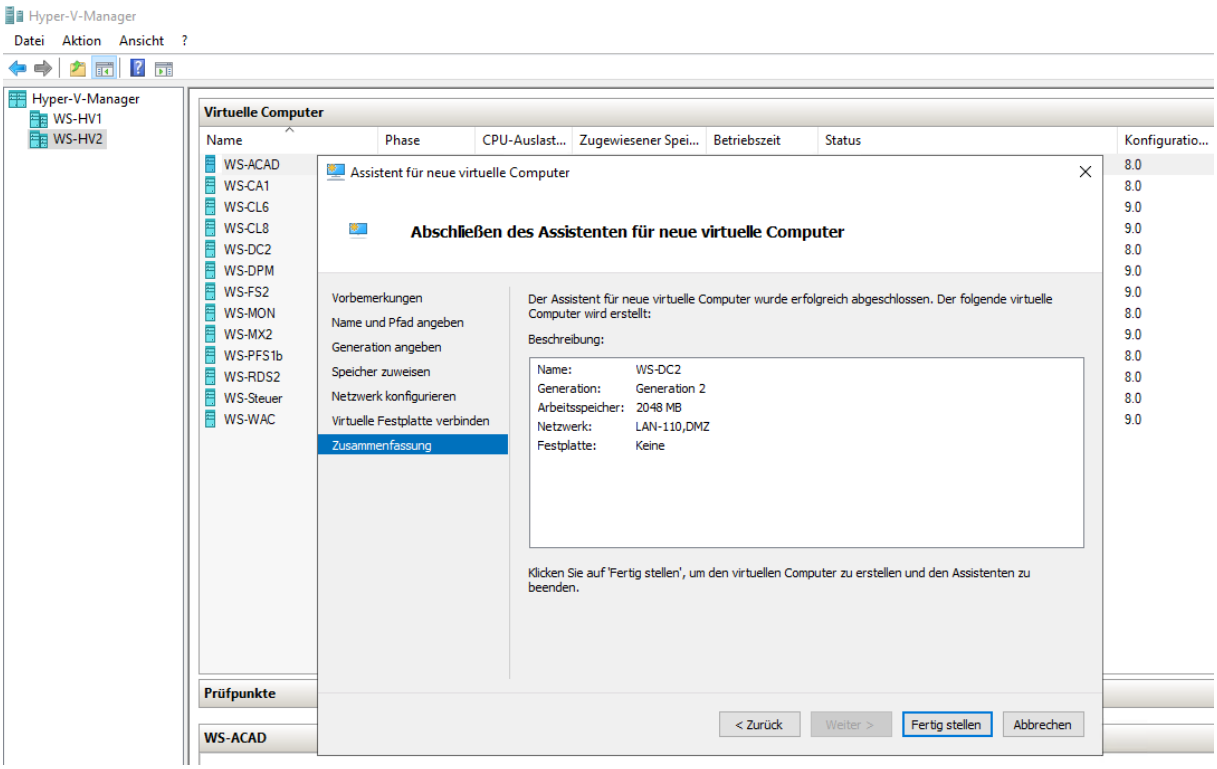
Vorbereitung

Aufbau der neuen VM

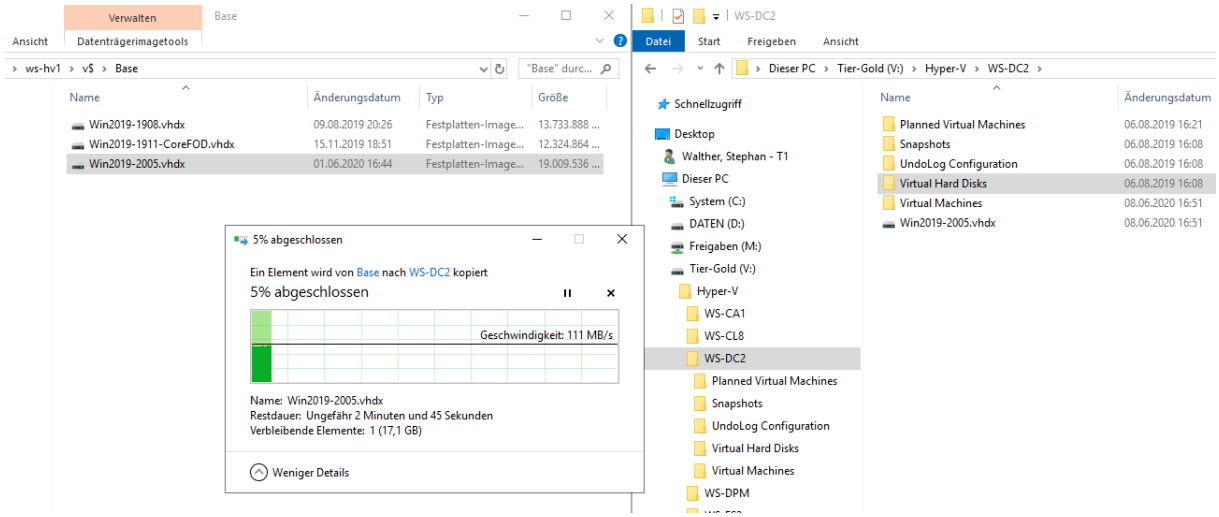
Es geht wieder mit der Auswahl der Berechtigungen für meinen Admin-Account los. Das regele ich mit meinem PowerShell-Script PAM-AdminGUI:



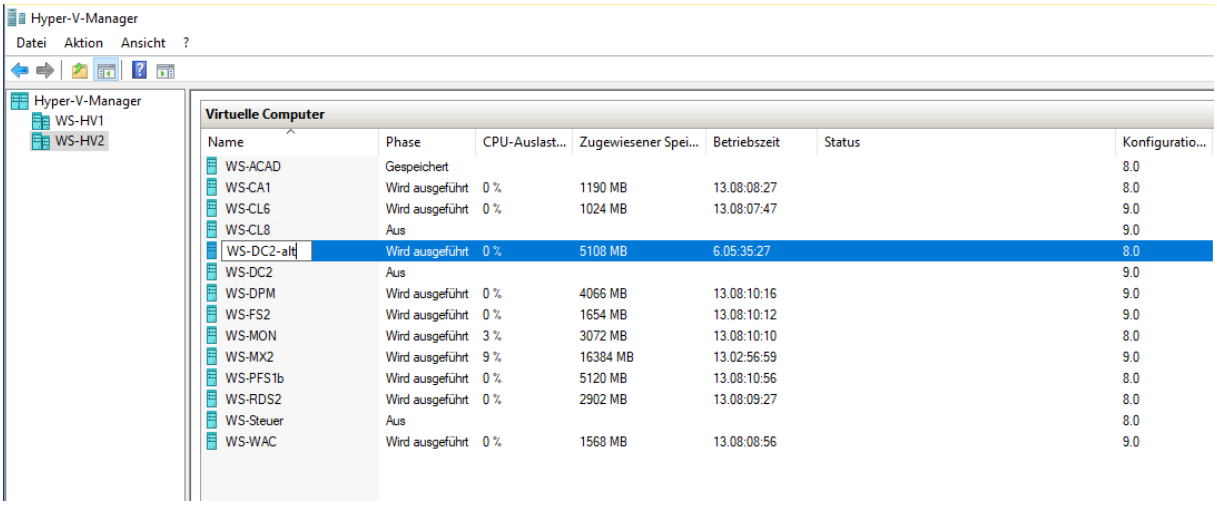
Mit Rechten ausgestattet melde ich mich am Hyper-V-Server an. Hier erstelle ich eine neue VM ohne große Besonderheiten: Sie läuft in der Generation 2, hängt im Client-Netzwerk LAN-110 und hat keine Festplattendatei. Der Anzeigename lautet schon WS-DC2:



Danach kopiere ich die Base-VHDX mit dem installierten Windows Server 2019 in das VM-Verzeichnis:

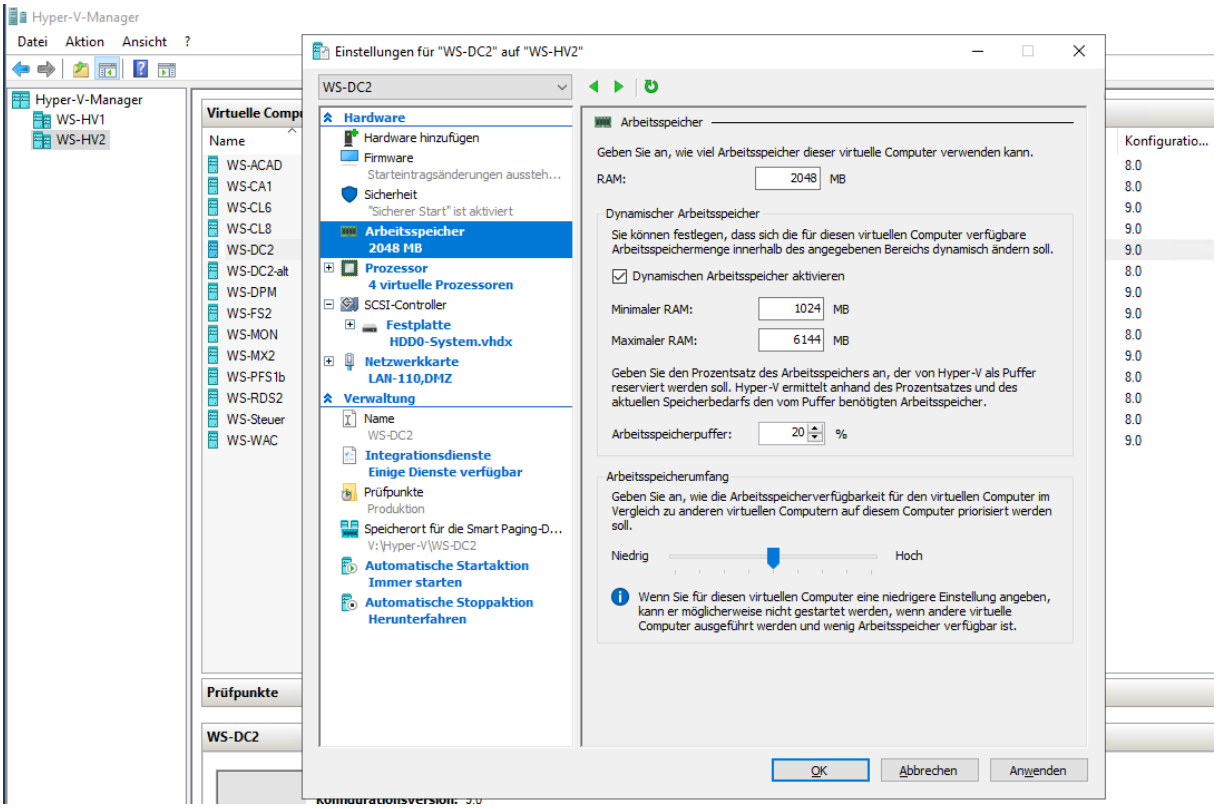


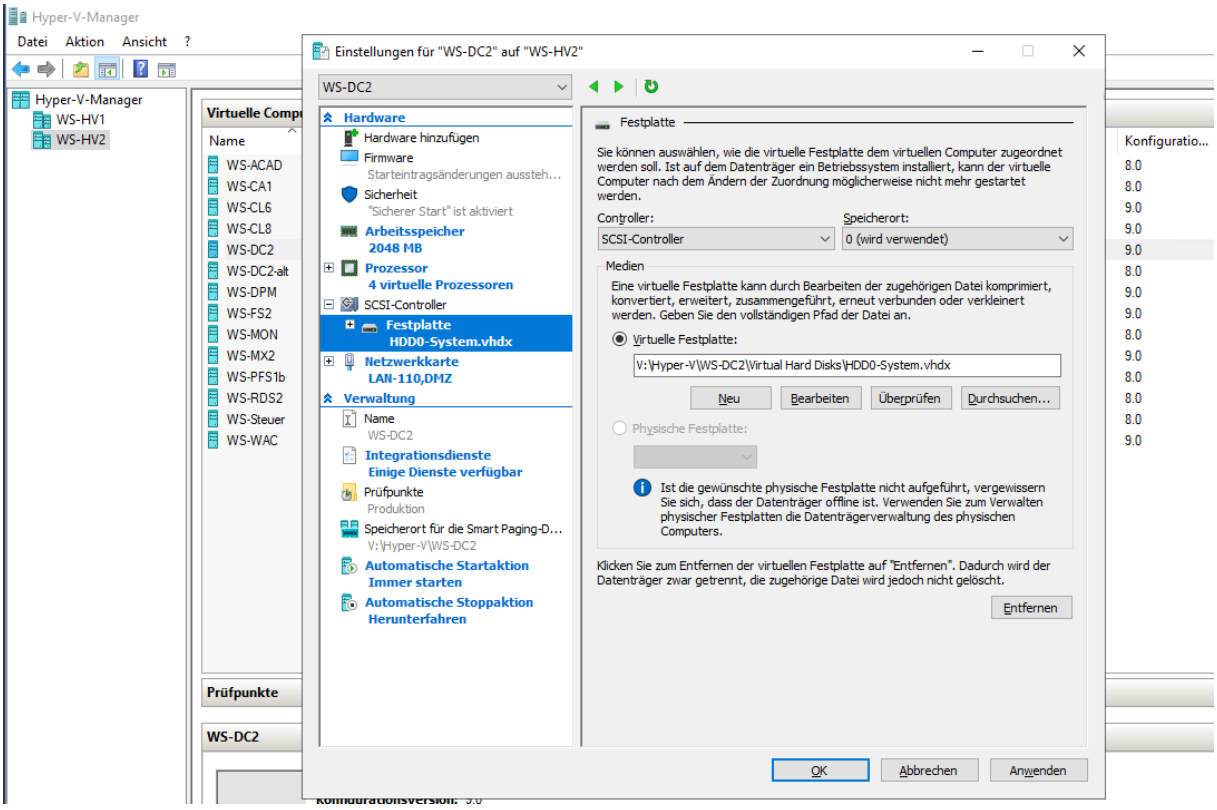
Dann benenne ich die alte VM um. So komme ich später nicht durcheinander. Der Anzeigename hat keinen Einfluss auf den Namen des Betriebssystems:

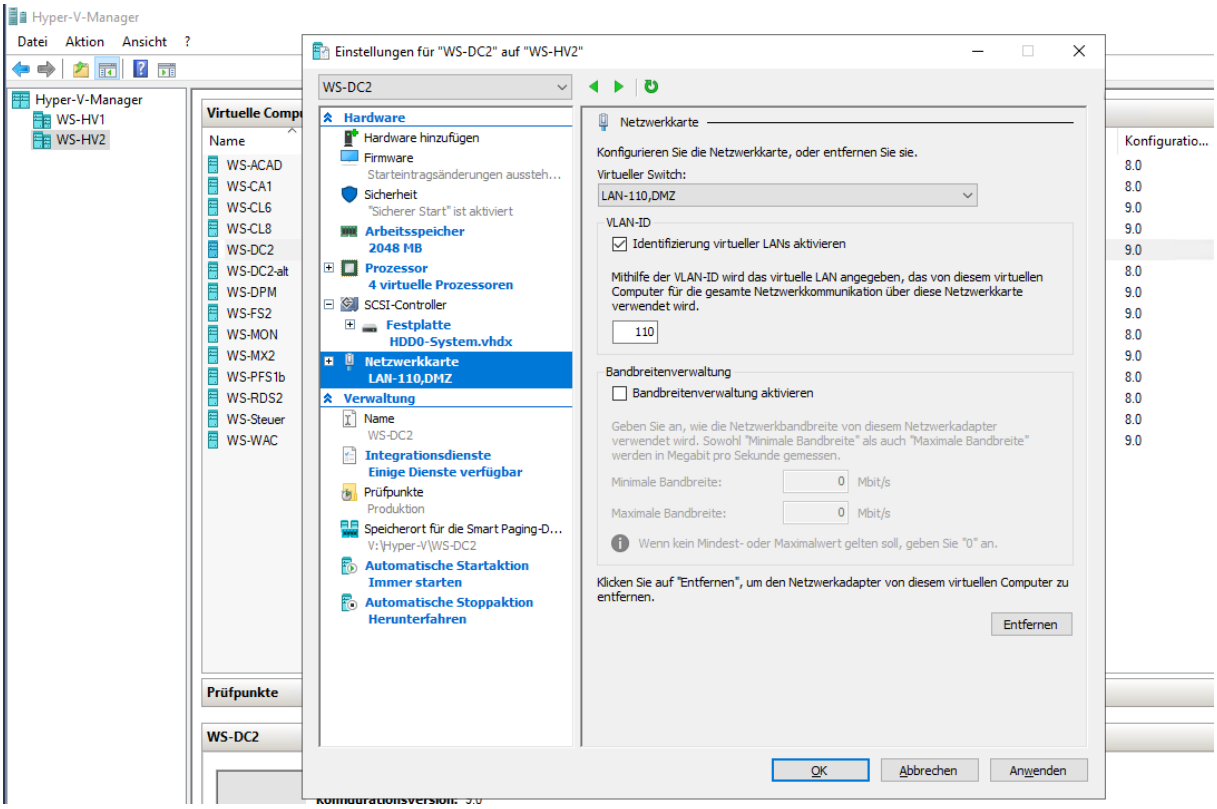


Weiter geht es mit dem Feintuning der VM. Hier nehme ich eine Reihe von Anpassungen vor:

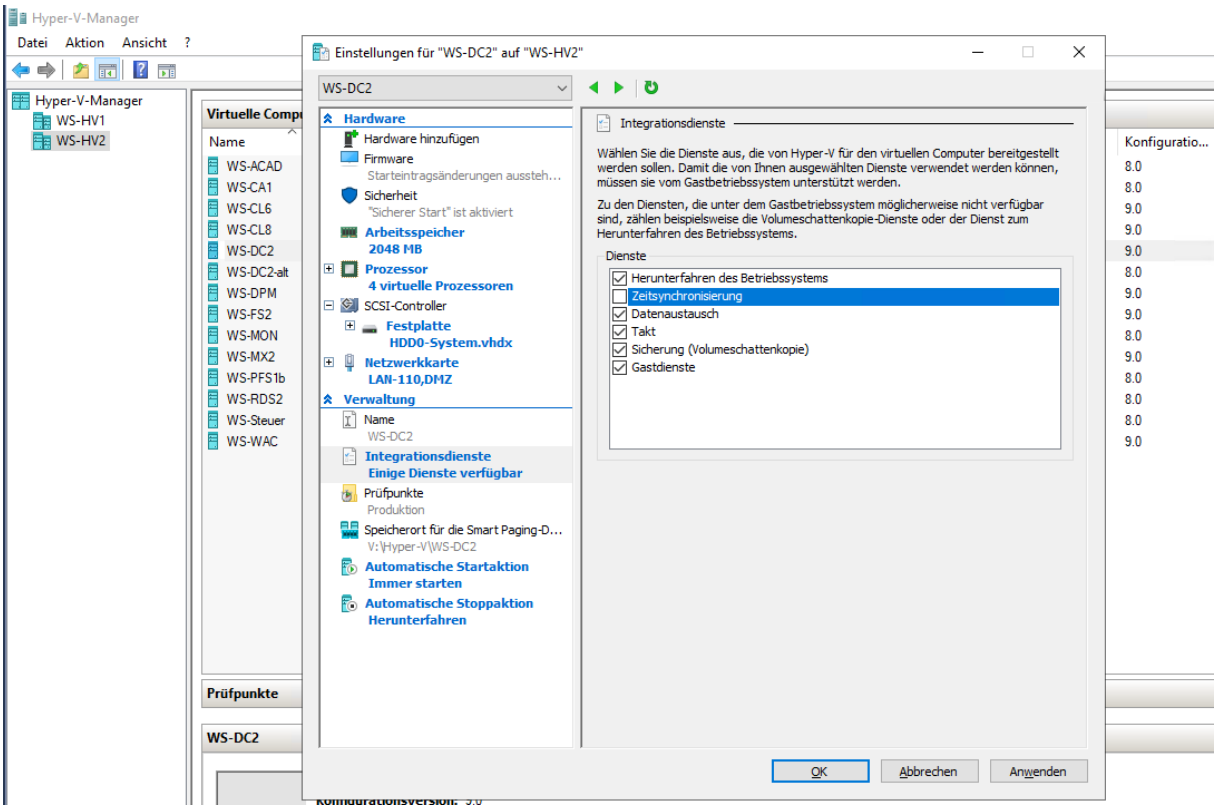
1. Die VM erhält bis zu 6GB Arbeitsspeicher. Das benötige ich wegen dem Microsoft ATA-Agenten.
2. Sie erhält Zugriff auf 4 vCPU.
3. Ich integriere die kopierte VHDX-Datei. Diese habe ich zuvor im Windows Explorer umbenannt.
4. Die Netzwerkkarte erhält eine VLAN-Konfiguration für den Zugriff zum Client-Netzwerksegment.
5. Ebenso stelle ich das Verhalten beim Ein- und Ausschalten des Hypervisors ein.


Hyper-V-Manager
Datei Aktion Ansicht ?
Hyper-V-Manager
WS-HV1
WS-HV2
Virtuelle Compu
Name
WS-ACAD
WS-CA1
WS-CL6
WS-CL8
WS-DC2
WS-DC2-alt
WS-DPM
WS-FS2
WS-MON
WS-MX2
WS-PFS1b
WS-RDS2
WS-Steuer
WS-WAC
Konfiguratio...
Prüfpunkte
WS-DC2
Einstellungen für "WS-DC2" auf "WS-HV2"
WS-DC2
Hardware
Hardware hinzufügen
Firmware
Starteintragsänderungen aussteh...
Sicherheit
"Sicherer Start" ist aktiviert
Arbeitsspeicher
2048 MB
Prozessor
4 virtuelle Prozessoren
SCSI-Controller
Festplatte
HDD0-System.vhdx
Netzwerkkarte
LAN-110,DMZ
Verwaltung
Name
WS-DC2
Integrationsdienste
Einige Dienste verfügbar
Prüfpunkte
Produktion
Speicherort für die Smart Paging-D...
V:\Hyper-V\WS-DC2
Automatische Startaktion
Immer starten
Automatische Stoppaktion
Herunterfahren
Arbeitsspeicher
Geben Sie an, wie viel Arbeitsspeicher dieser virtuelle Computer verwenden kann.
RAM: 2048 MB
Dynamischer Arbeitsspeicher
Sie können festlegen, dass sich die für diesen virtuellen Computer verfügbare Arbeitsspeichermenge innerhalb des angegebenen Bereichs dynamisch ändern soll.
Dynamischen Arbeitsspeicher aktivieren
Minimaler RAM: 1024 MB
Maximaler RAM: 6144 MB
Geben Sie den Prozentsatz des Arbeitsspeichers an, der von Hyper-V als Puffer reserviert werden soll. Hyper-V ermittelt anhand des Prozentsatzes und des aktuellen Speicherbedarfs den vom Puffer benötigten Arbeitsspeicher.
Arbeitsspeicherpuffer: 20 %
Arbeitsspeicherumfang
Geben Sie an, wie die Arbeitsspeicherverfügbarkeit für den virtuellen Computer im Vergleich zu anderen virtuellen Computern auf diesem Computer priorisiert werden soll.
Niedrig
Hoch
Wenn Sie für diesen virtuellen Computer eine niedrigere Einstellung angeben, kann er möglicherweise nicht gestartet werden, wenn andere virtuelle Computer ausgeführt werden und wenig Arbeitsspeicher verfügbar ist.
OK
Abbrechen
Anwenden

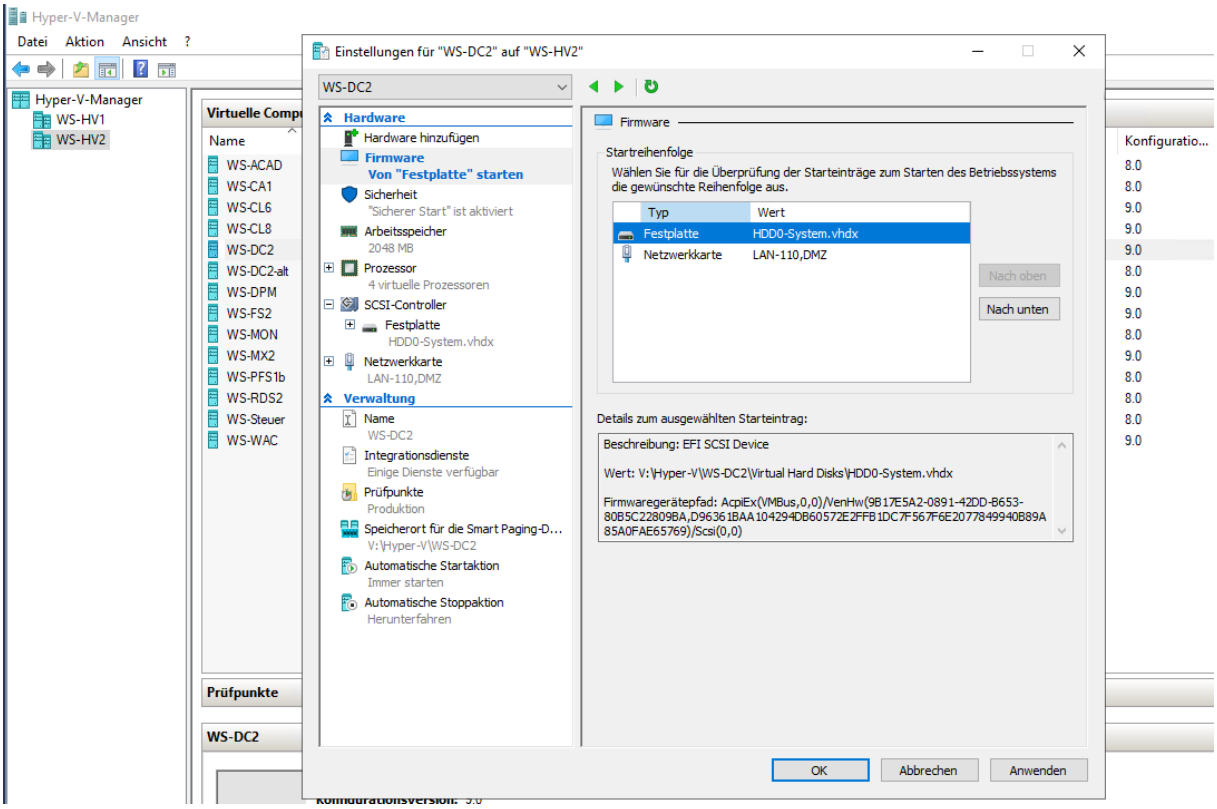

Hyper-V-Manager
Datei Aktion Ansicht ?
Hyper-V-Manager
WS-HV1
WS-HV2
Virtuelle Compu
Name
WS-ACAD
WS-CA1
WS-CL6
WS-CL8
WS-DC2
WS-DC2-alt
WS-DPM
WS-FS2
WS-MON
WS-MX2
WS-PFS1b
WS-RDS2
WS-Steuer
WS-WAC
Konfiguratio...
Prüfpunkte
WS-DC2
Einstellungen für "WS-DC2" auf "WS-HV2"
WS-DC2
Hardware
Hardware hinzufügen
Firmware
Starteintragsänderungen aussteh...
Sicherheit
"Sicherer Start" ist aktiviert
Arbeitsspeicher
2048 MB
Prozessor
4 virtuelle Prozessoren
SCSI-Controller
Festplatte
HDD0-System.vhdx
Netzwerkkarte
LAN-110,DMZ
Verwaltung
Name
WS-DC2
Integrationsdienste
Einige Dienste verfügbar
Prüfpunkte
Produktion
Speicherort für die Smart Paging-D...
V:\Hyper-V\WS-DC2
Automatische Startaktion
Immer starten
Automatische Stoppaktion
Herunterfahren
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-DC2\Virtual Hard Disks\HDD0-System.vhdx
Neu
Bearbeiten
Überprüfen
Durchsuchen...
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.
Entfernen
OK
Abbrechen
Anwenden



Damit es bei dieser VM nicht die gleichen Zeitprobleme gibt wie beim WS-DC1, deaktiviere ich die Zeitsynchronisierung mit dem Hyper-V-Host. Denn dieser holt sich seine Systemzeit als Domänenmitglied beim Domain Controller. Das wäre ein Henne-Ei-Problem:



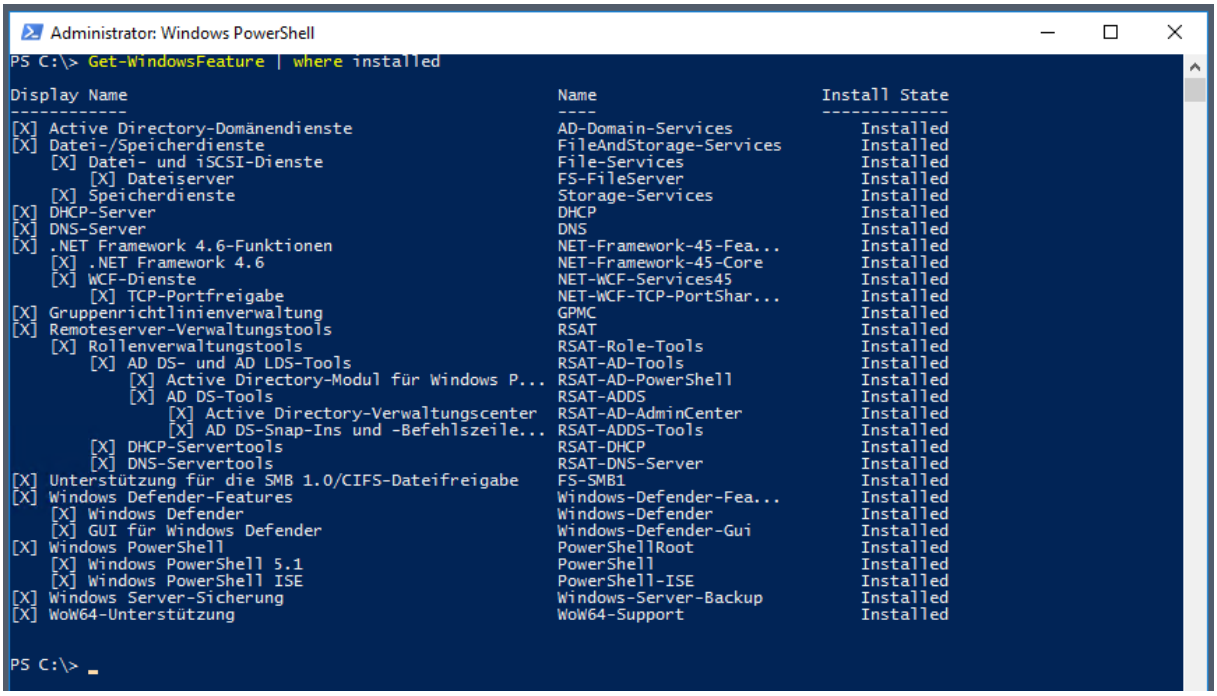
Nach einer Bestätigung verändere ich die Startreihenfolge. So wird immer von der VHDX gebootet:



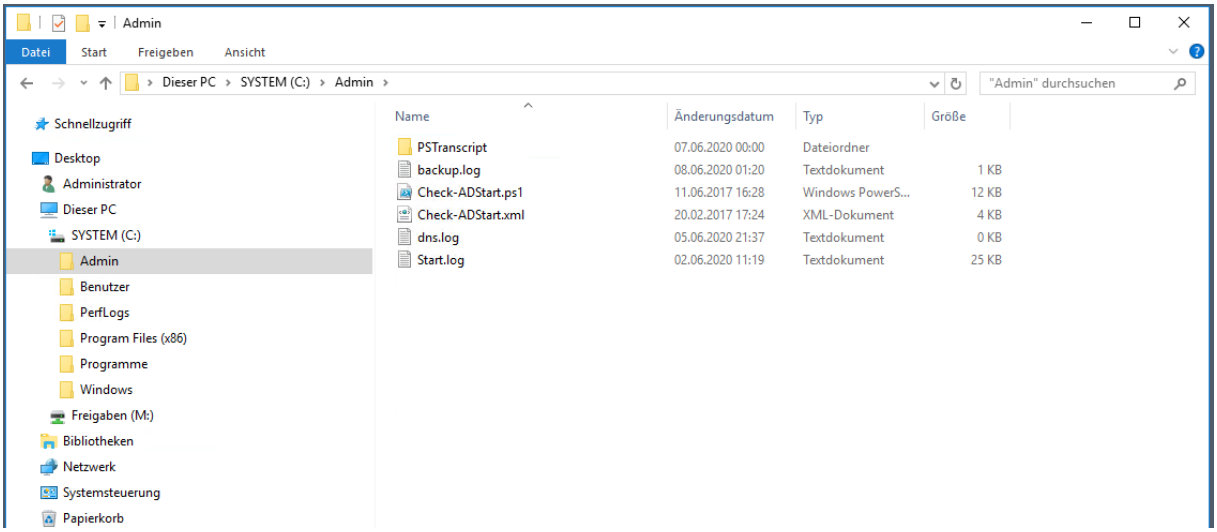
Die VM ist fertig. Ich lasse sie aber noch deaktiviert.

Sichtung von Informationen auf dem alten Server

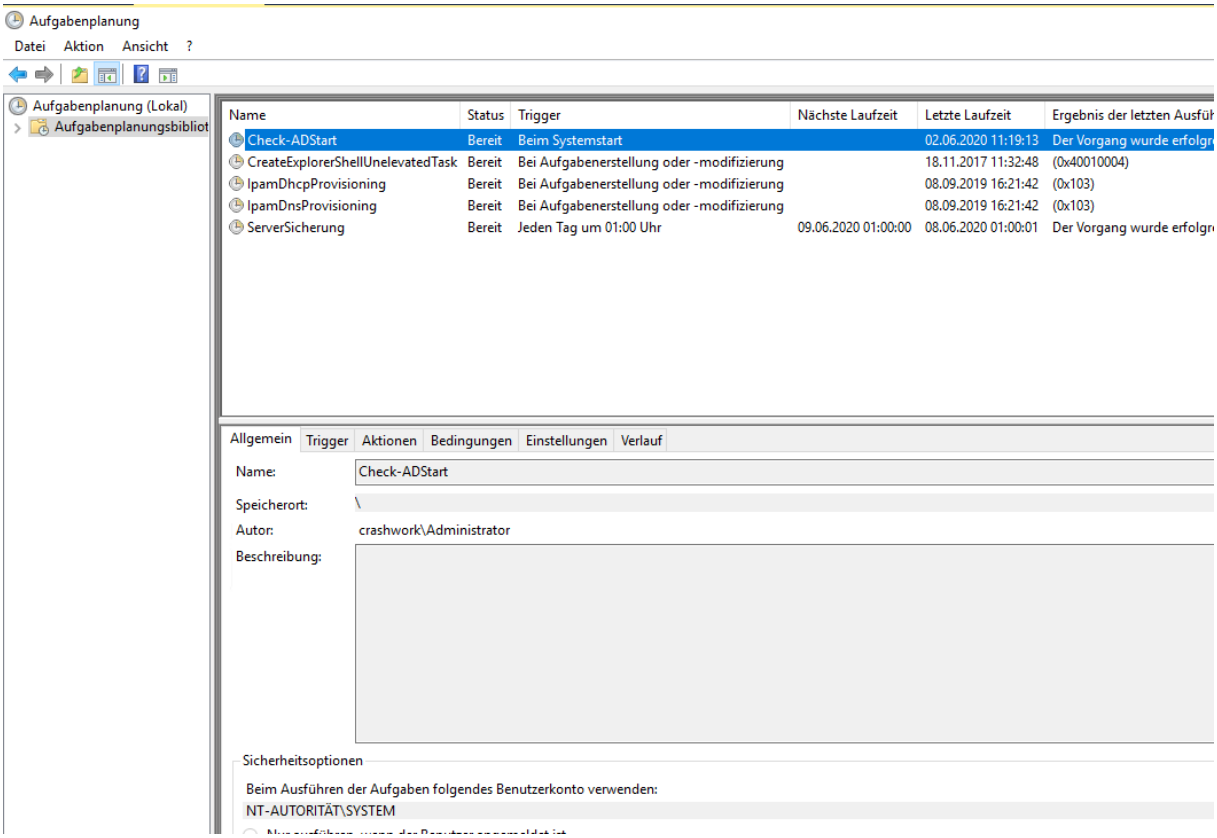
Bei jeder Migration sollte man sich das Altsystem genau ansehen. Man verbringt unter Umständen viele Stunden mit den Servern, aber einige Anpassungen liegen durchaus schon länger zurück. Aber spätestens beim Deaktivieren des alten Servers könnten die Probleme anfangen. Ich beginne mit der Auflistung der installierten Rollen und Features. Das sind alles Erwartete Werte:



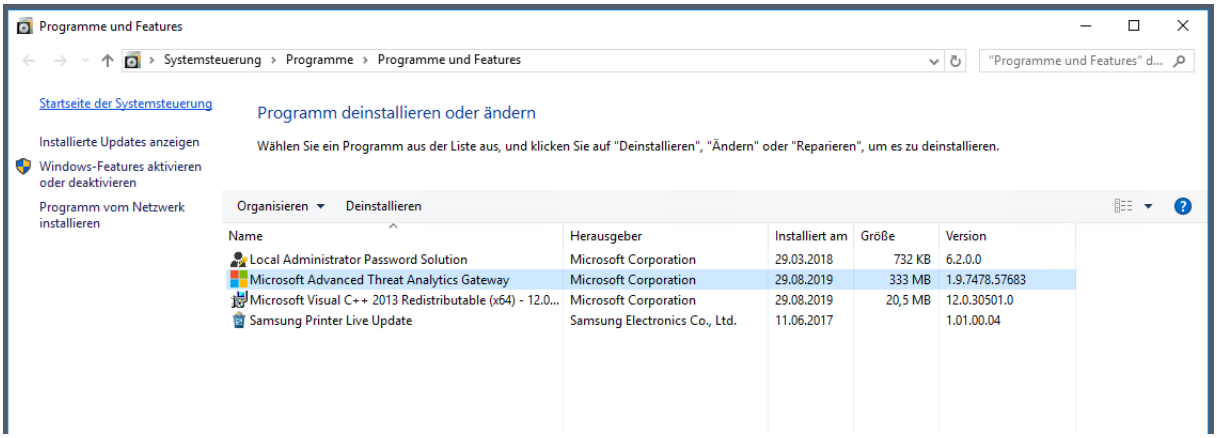
Im Adminverzeichnis c:\admin liegen keine Scripte. Der andere Server WS-DC1 war voll mit Dateien. Man erkennt hier einen Favoriten bei der Administration:



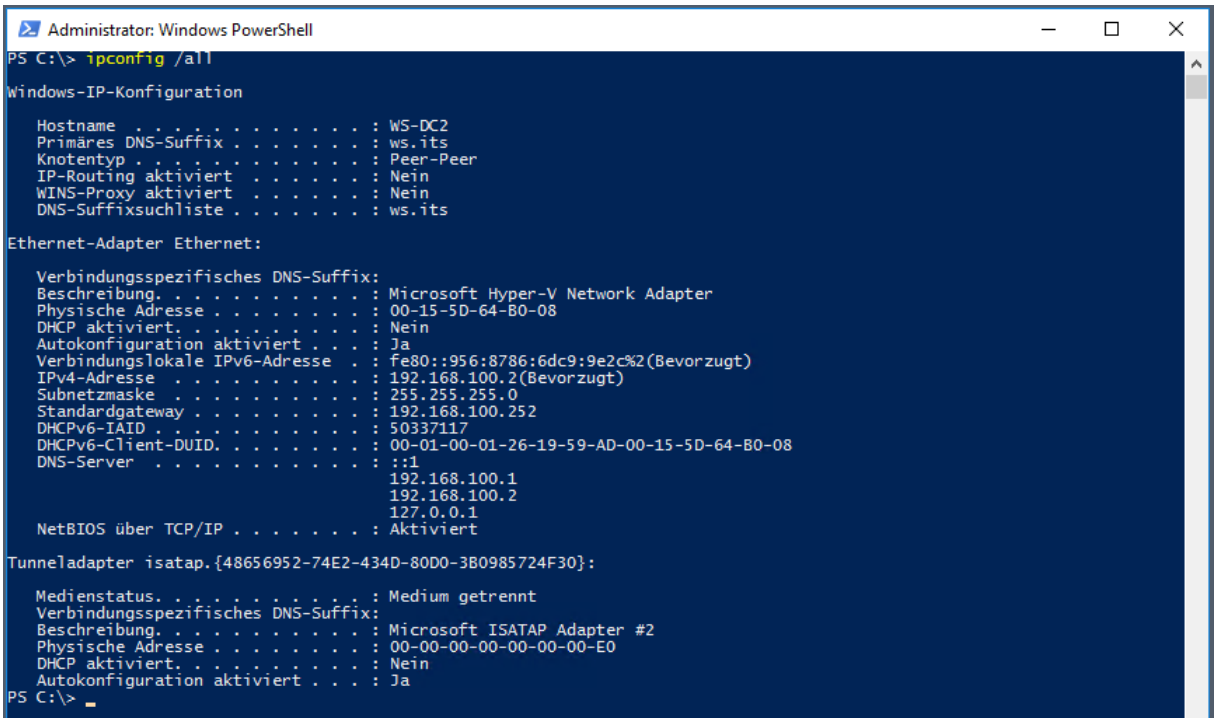
Ebenso liegen hier nur die Standard-Aufgaben. Diese muss ich nicht exportieren, da ich die passenden XML-Dateien bereits im AdminShare gespeichert habe:



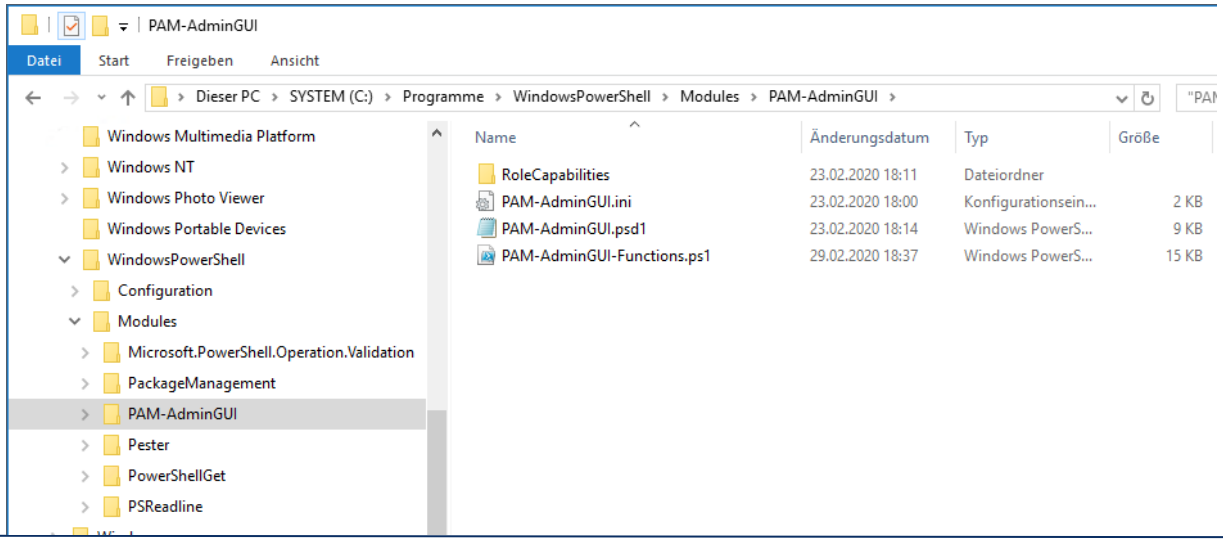
Zwei Anwendungen muss ich auf dem neuen Server nachinstallieren: LAPS für das Auslesen der lokalen Adminpassworte aus den AD-Computerkonten und den Microsoft ATA Agent. Der übermittelt an mein Microsoft Advanced Threat Analytics System sicherheitsrelevante Informationen, die ATA dann zentral analysieren und bewerten kann:

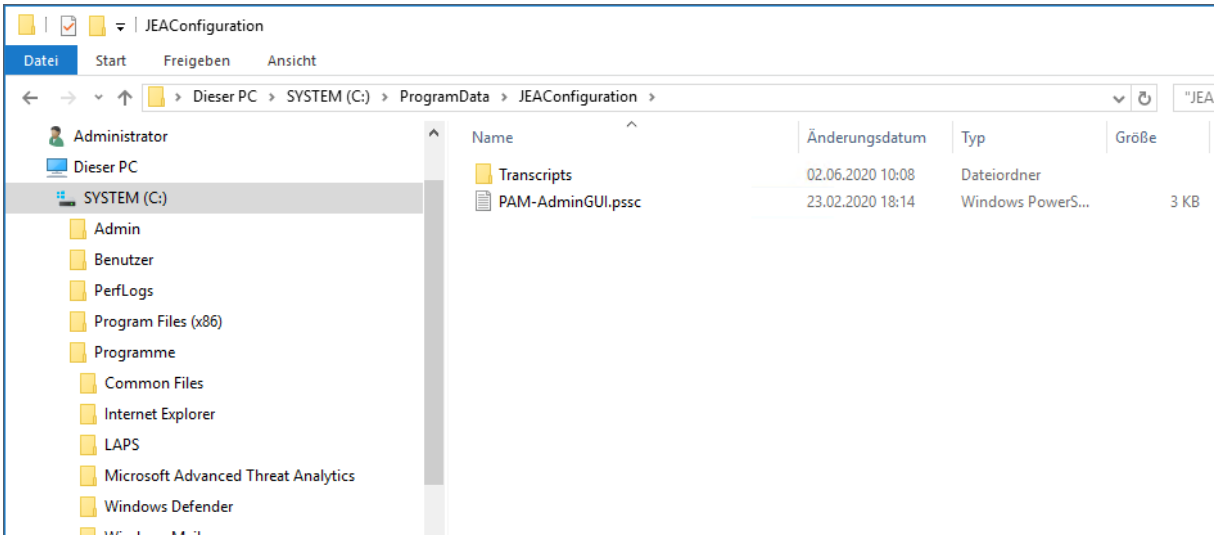


Die IP-Konfiguration muss ich ebenfalls auf dem neuen Server übernehmen. So spare ich mir eine Vielzahl von Anpassungen in meiner Infrastruktur:



Der WS-dC2 ist ebenfalls ein Endpunkt für mein PowerShell-Script PAM-AdminGUI. Auch diese Anpassung muss ich am neuen Server vornehmen:





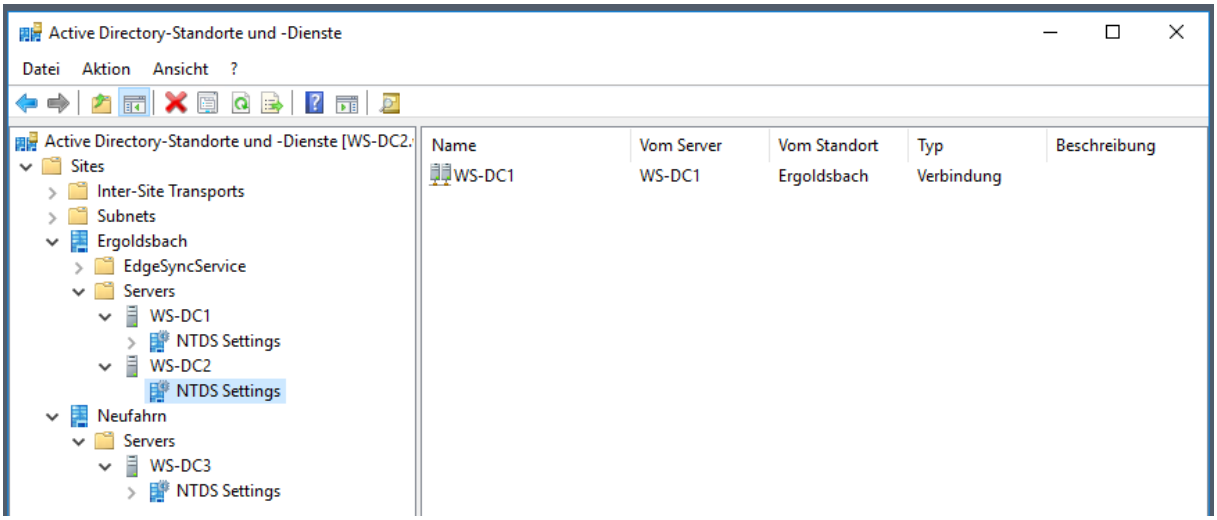
Der Server ist sauber. Es sind keine Altlasten mehr vorhanden. Das damals installierte ADFS hatte ich bereits vor Wochen entfernt. Und die IPAM-Integration gibt es seit Monaten nicht mehr.

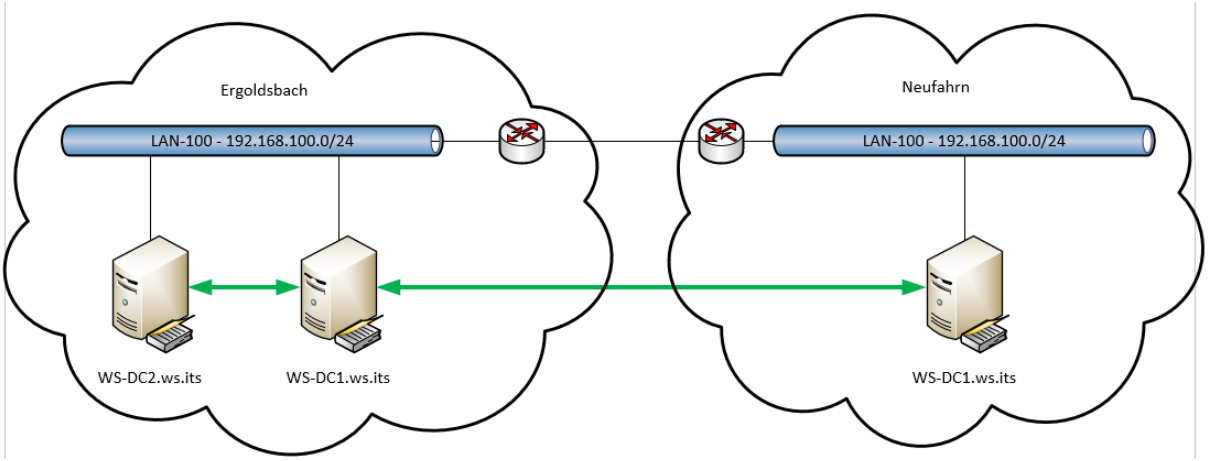
aktuelle Konfiguration des Active Directory

Auch wenn es nur ein paar Tage her ist, seit ich meinen Server WS-DC1 von Windows Server 2016 auf Windows Server 2019 neuinstalliert habe: Eine Kontrolle der Konfiguration lohnt sich vor jeder Migration.

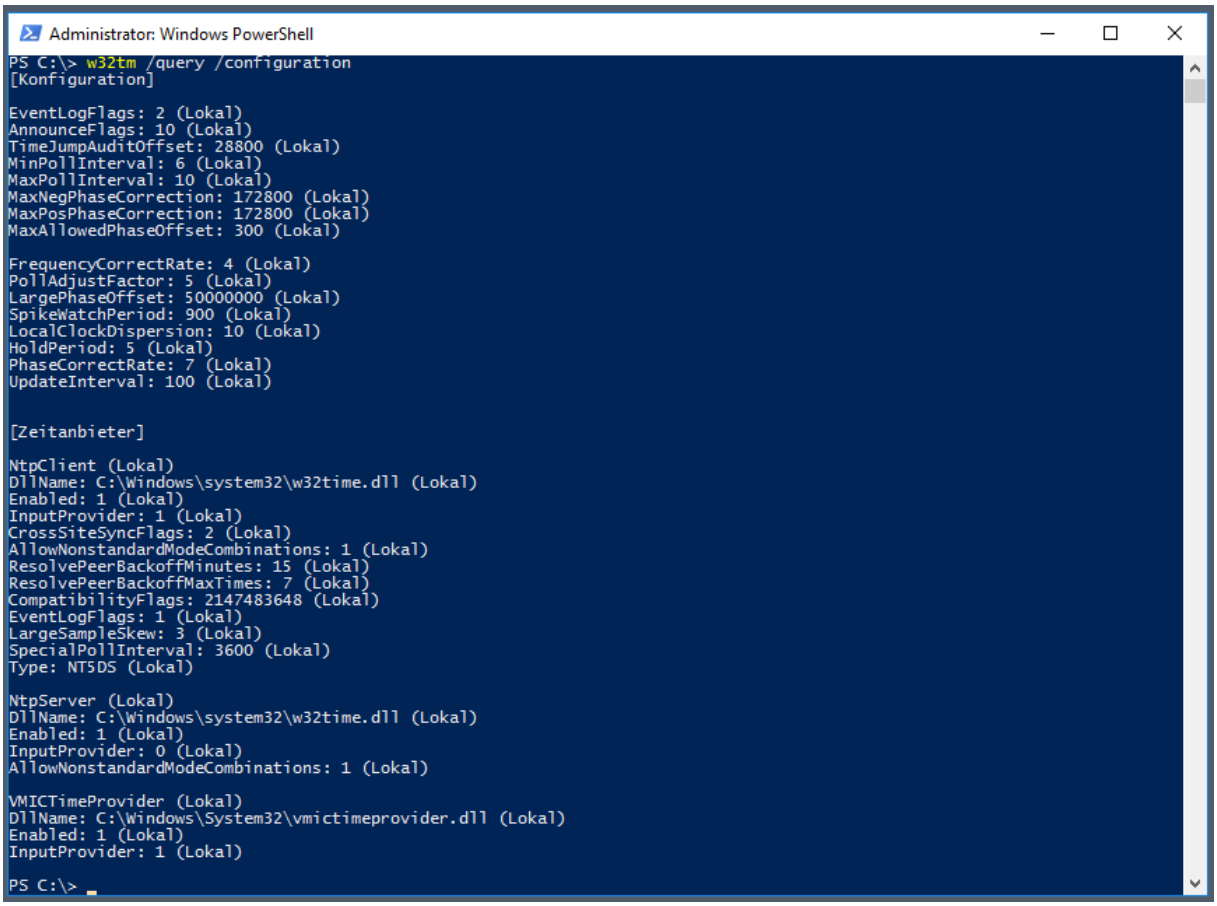
Die FSM liegen auf dem anderen DC:

Meine AD-Replikation verbindet den WS-DC2 bidirektional mit WS-DC1 und diesen wiederum bidirektional mit WS-DC3. Beim WS-DC1 musste ich hier eine Brücke zwischen WS-DC2 und WS-DC3 erstellen. Das ist hier aber nicht erforderlich:





Die Zeitkonfiguration ist Standard. Der Domain Controller holt sich seine Systemzeit automatisch vom PDC-Emulator. Und das ist der WS-DC1:



Die Domänenfunktionsebene und die Gesamtstrukturfunktionsebene habe ich bereits auf Windows Server 2016 angehoben. Das Active Directory Schema läuft mit der Version Windows Server 2019. Dafür hat der erste 2019er Domain Controller gesorgt.

Die AD-Replikation wird permanent durch mein Monitoring überwacht. Und auch die Eventlogs habe ich im Blick. Hier meldet mir ein PowerShell-Script täglich eine Zusammenfassung. Der Domain Controller WS-DC2 hatte in den letzten 24 Stunden keine Fehler und nur eine Warnung:

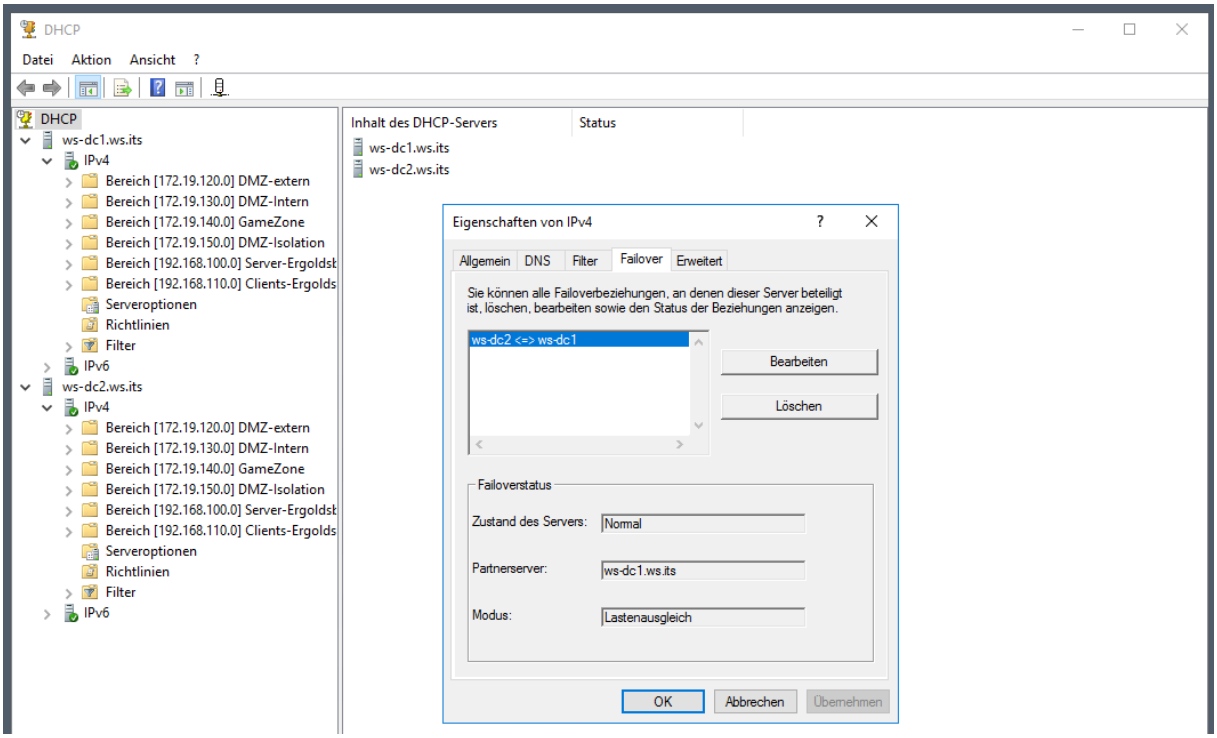
Zusammenfassung der Ereignisse (24h)

Server	Information	Warning	Error
WS-RDS1	15721	0	7
WS-PRINT1	15664	0	0
WS-FS1	15735	3	8
WS-DPM	15976	19	14
WS-HV2	17078	18	0
WS-HV3	16930	1	2
WS-MX2	26503	344	13
WS-FS3	15801	0	5
WS-ATA	15706	0	1
WS-NPS1	15673	0	7
WS-WAC	15747	0	7
WS-DC2	15803	1	0
WS-DC3	15754	1	0
WS-CM	15751	1	5
WS-RDS2	15723	4	0
WS-CA1	15672	0	0
WS-HV1	17031	15	2
WS-FS2	15810	0	0
WS-MON	10449	0	5
WS-DC1	15941	6	7
WS-MX1	26533	346	13

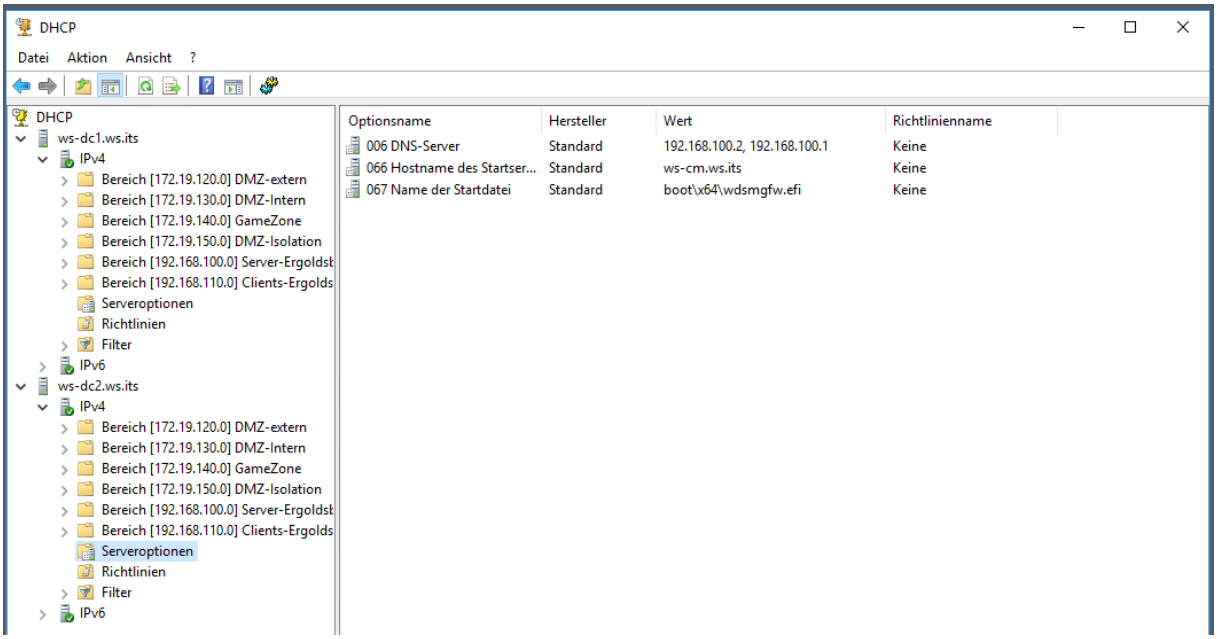
Eine Migration ist möglich.

aktuelle Konfiguration des DHCP

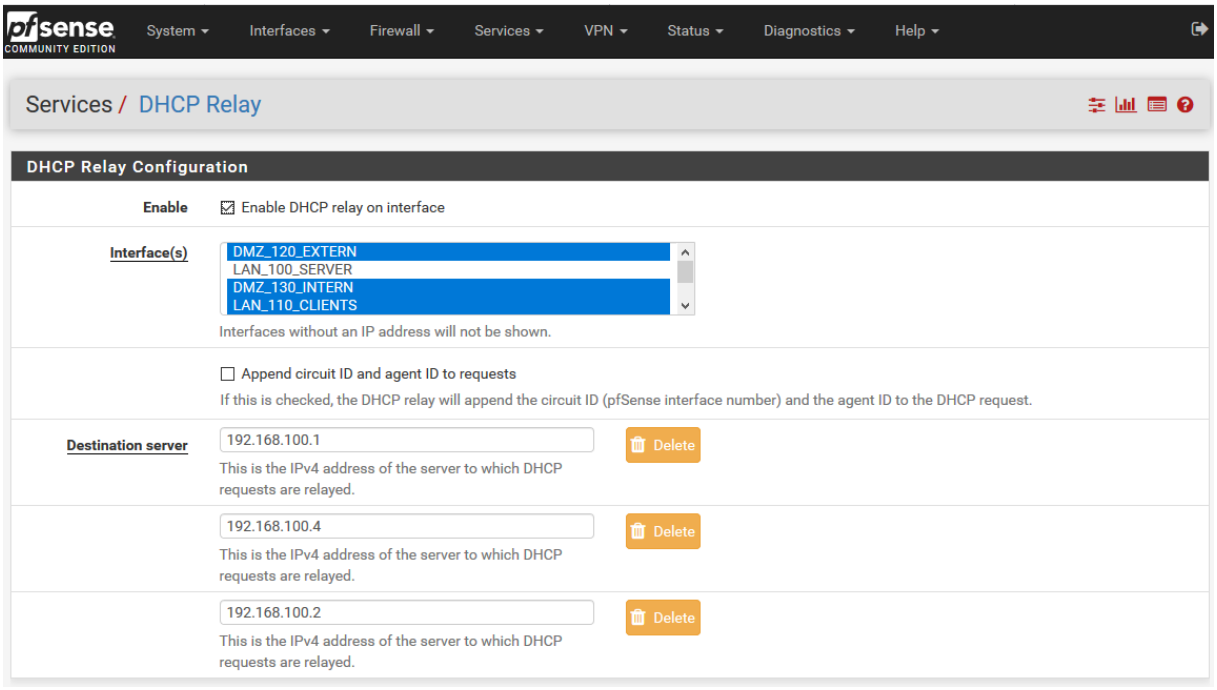
Auf dem Server läuft ein DHCP-Service. Dieser arbeitet mit WS-DC1 zusammen als DHCP-Failover:



Nur die lokalen Serveroptionen werden nicht synchronisiert:

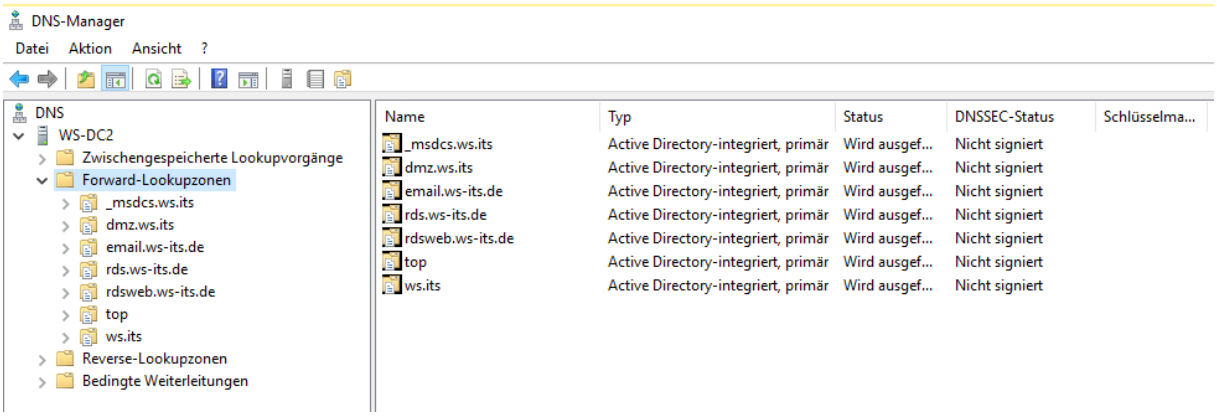


Beide DHCP werden von meiner PFSense als DHCP-Relayagent angesprochen. Ich kann also zu einer Zeit einen Server ausschalten, ohne dass der Service DHCP zum Erliegen kommt:

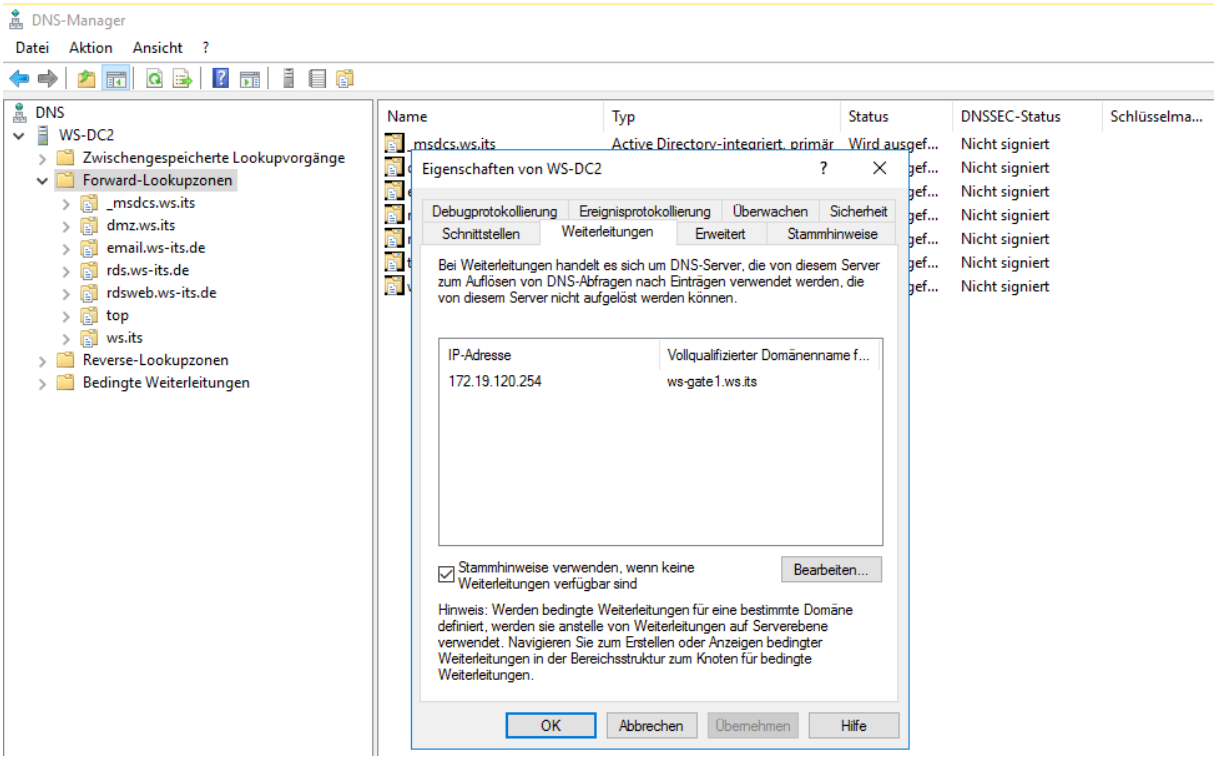


aktuelle Konfiguration des DNS

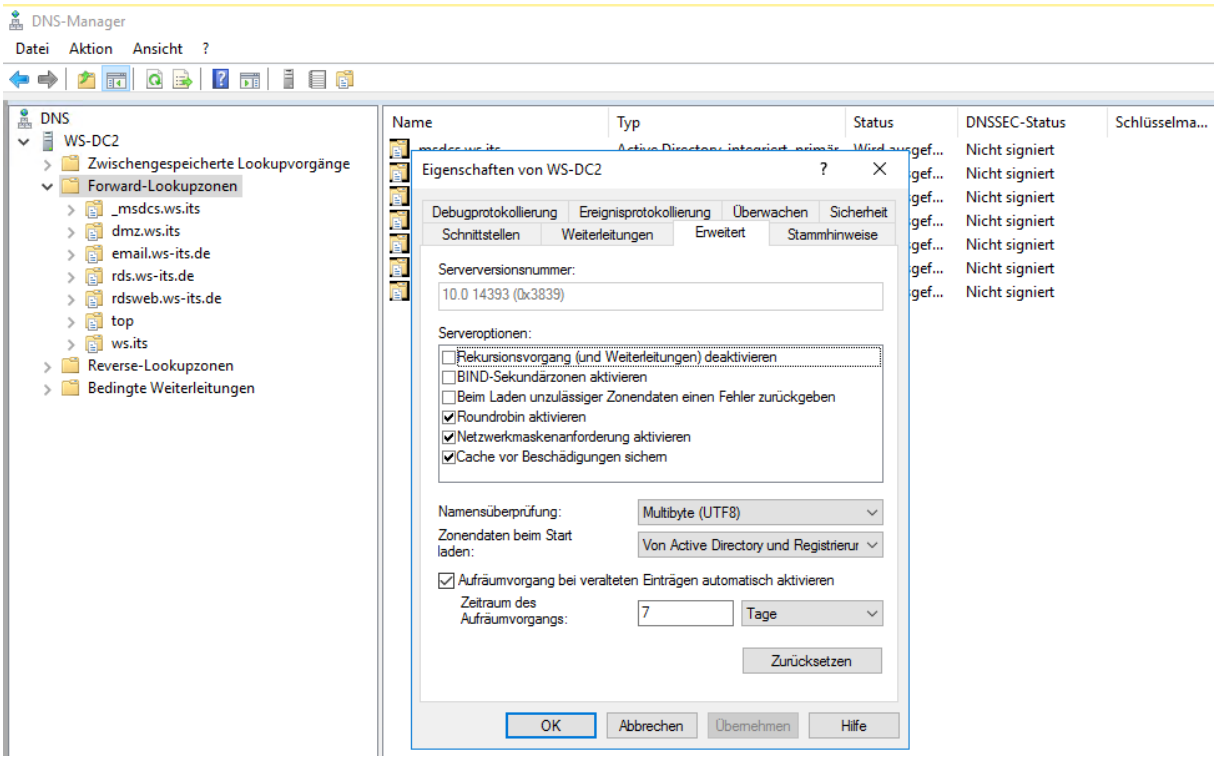
Auch der WS-DC2 hat nur Active Directory integrierte Zonen:



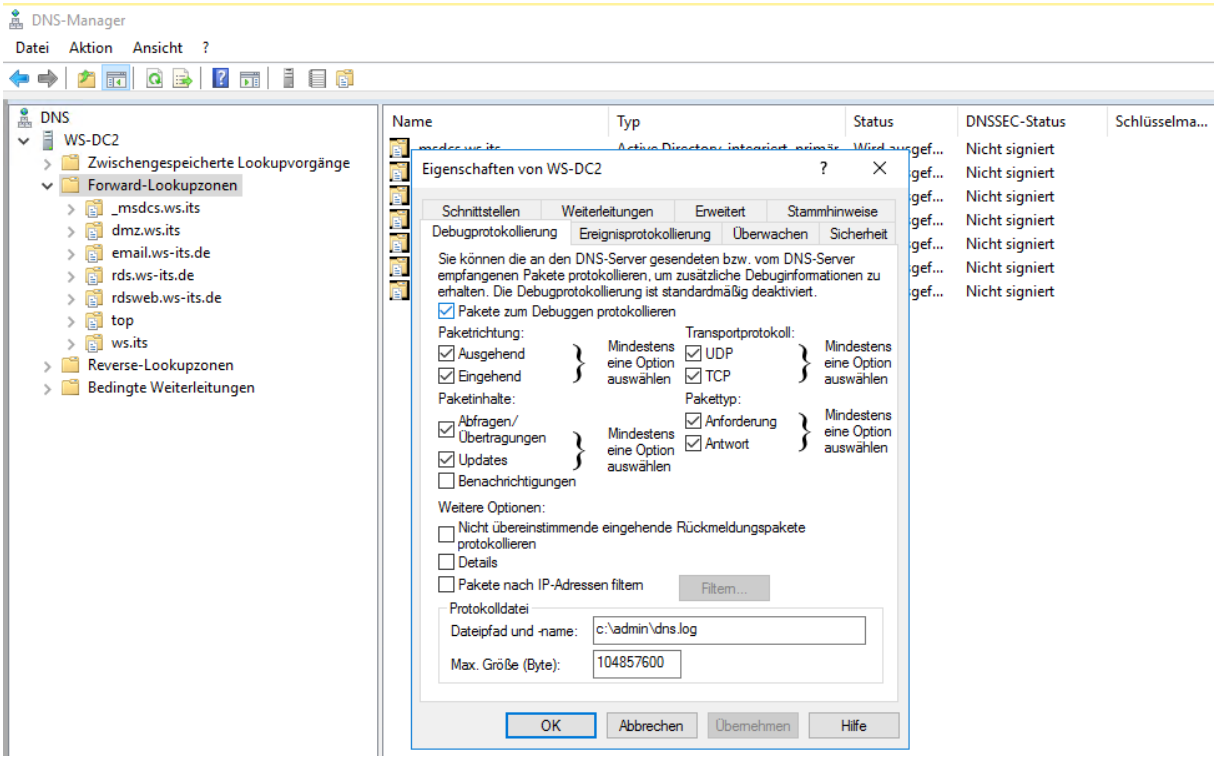
Der aktuelle Forwarder ist meine Fritzbox. Das muss ich anpassen, bevor ich den Domain Controller herunterstufe:

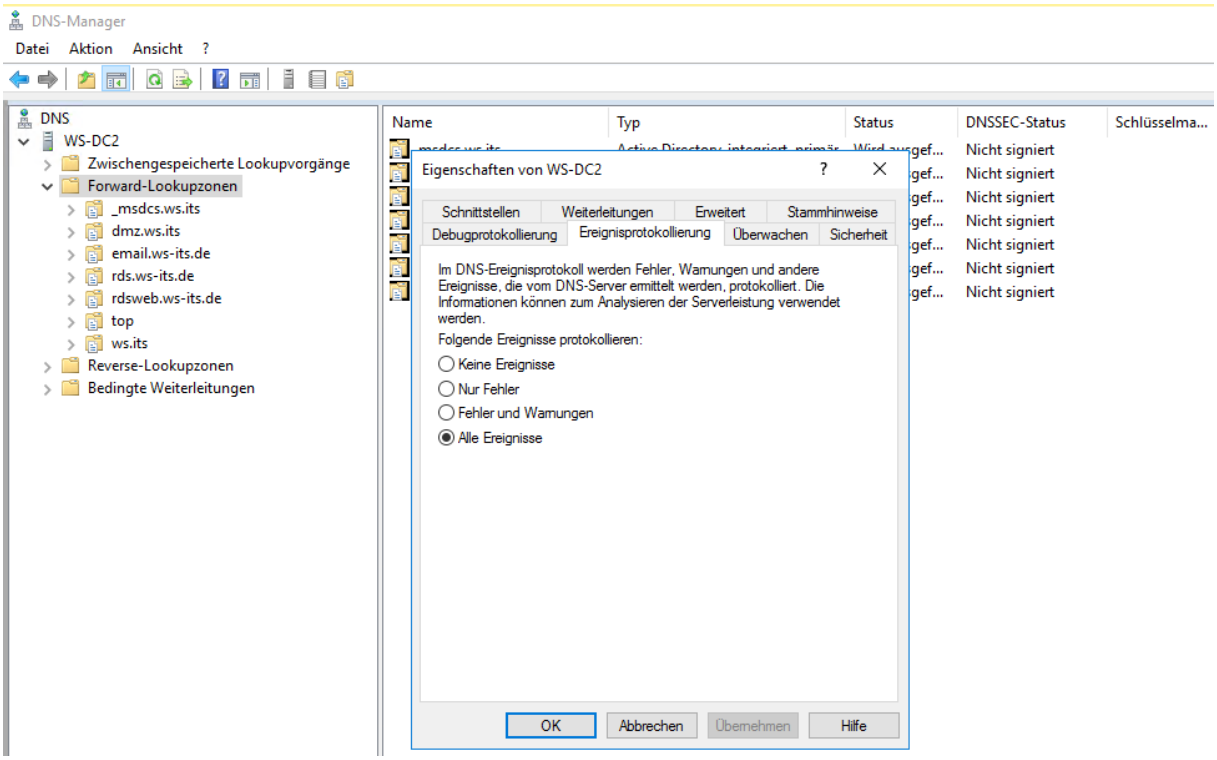


Die sonstigen Optionen sind schnell gesichtet:



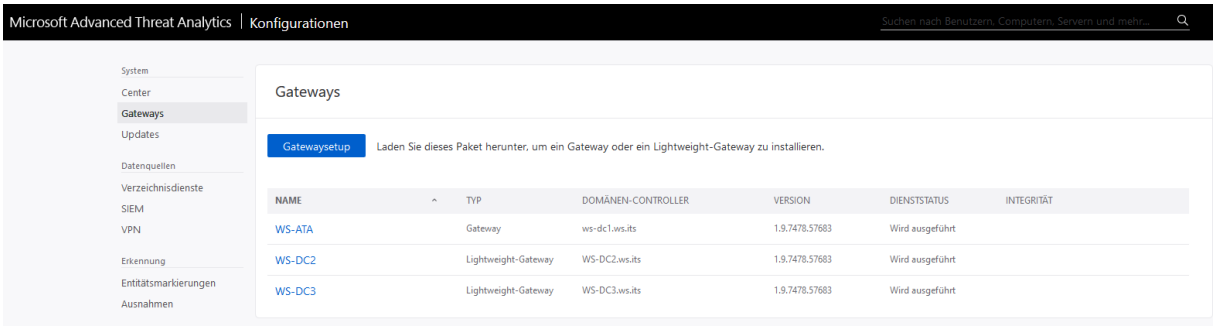
Auch dieser DNS protokolliert für Diagnosezwecke alle DNS-Anfragen in einer Textdatei:



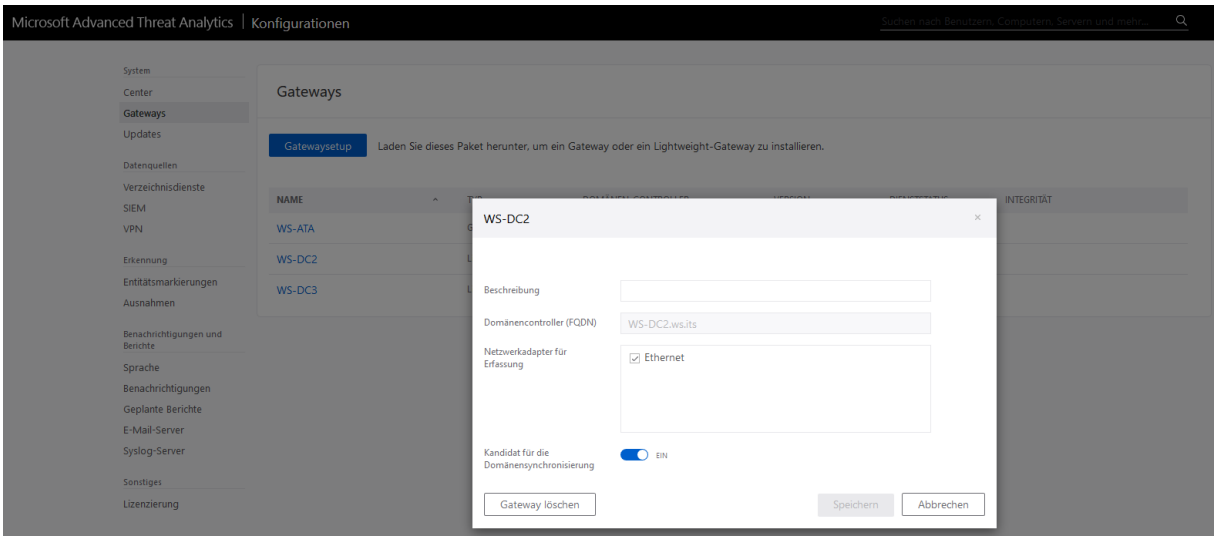


aktuelle ATA-Konfiguration

Vorhin habe ich schon den Microsoft ATA-Agent in der Programmliste der Systemsteuerung gesehen. Im ATA-Dashboard selber wird der Server WS-DC2 durch die Verbindung des Lightweight-Gateways gelistet. Das ist der Agent:

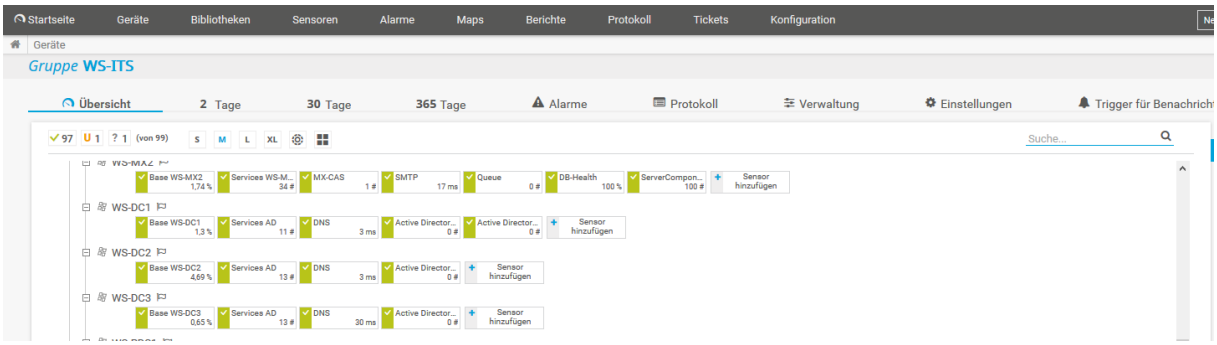


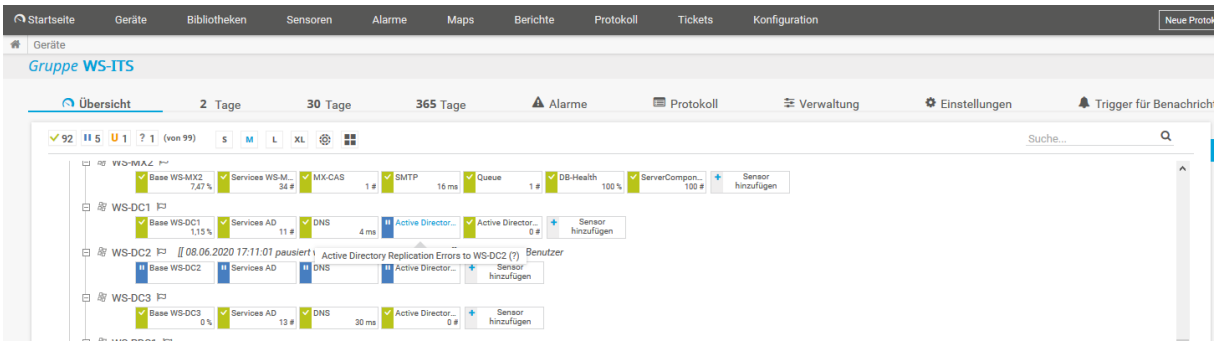
Zusätzlich holt sich mein ATA Informationen zum Active Directory vom Server WS-DC2:



Maintenance

Damit mein Monitoring bei dem Wipe & Load nicht ausflippt, deaktiviere ich einige Sensoren:

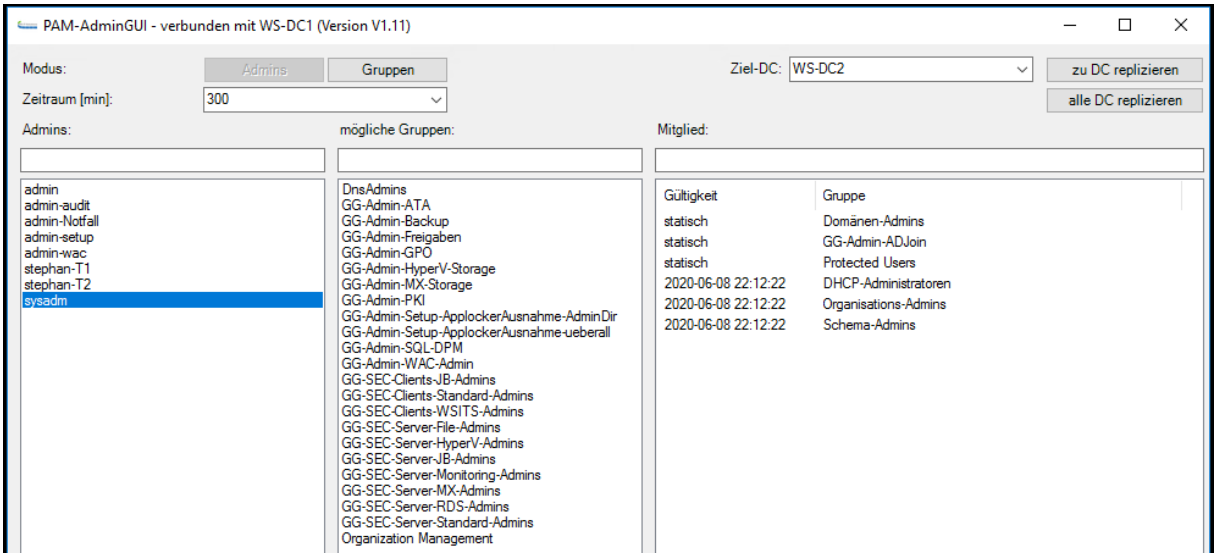




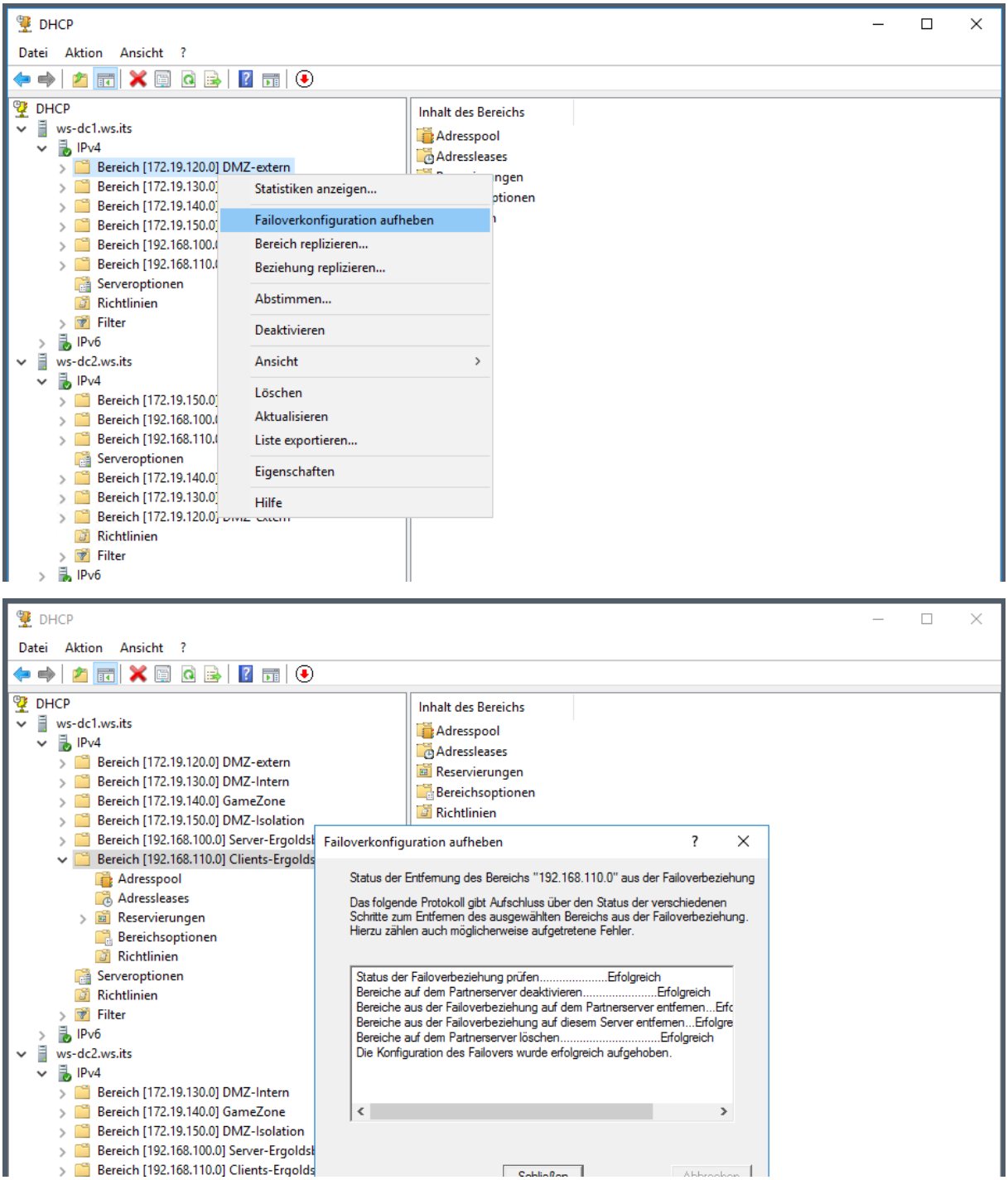
Deinstallation

Entfernen der Rolle DHCP

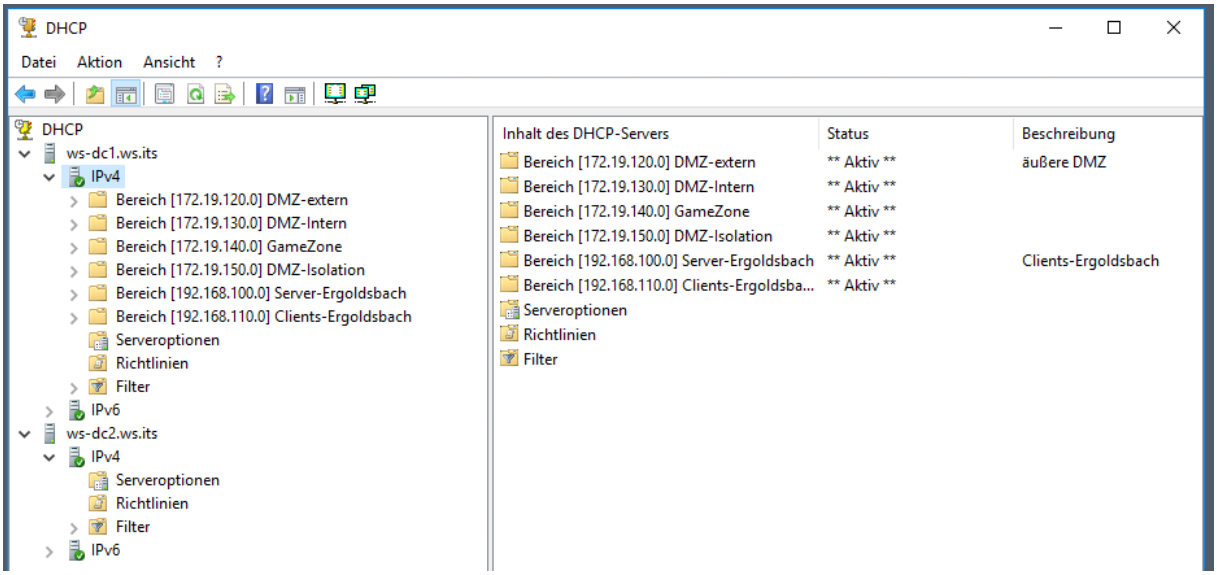
Die Vorarbeiten sind abgeschlossen. Ich beginne die Migration mit der Entfernung des DHCP-Failovers. Dazu statte ich meinen Admin-Account mit weiteren Rechten aus. Die werde ich auch für die AD-Migration benötigen:



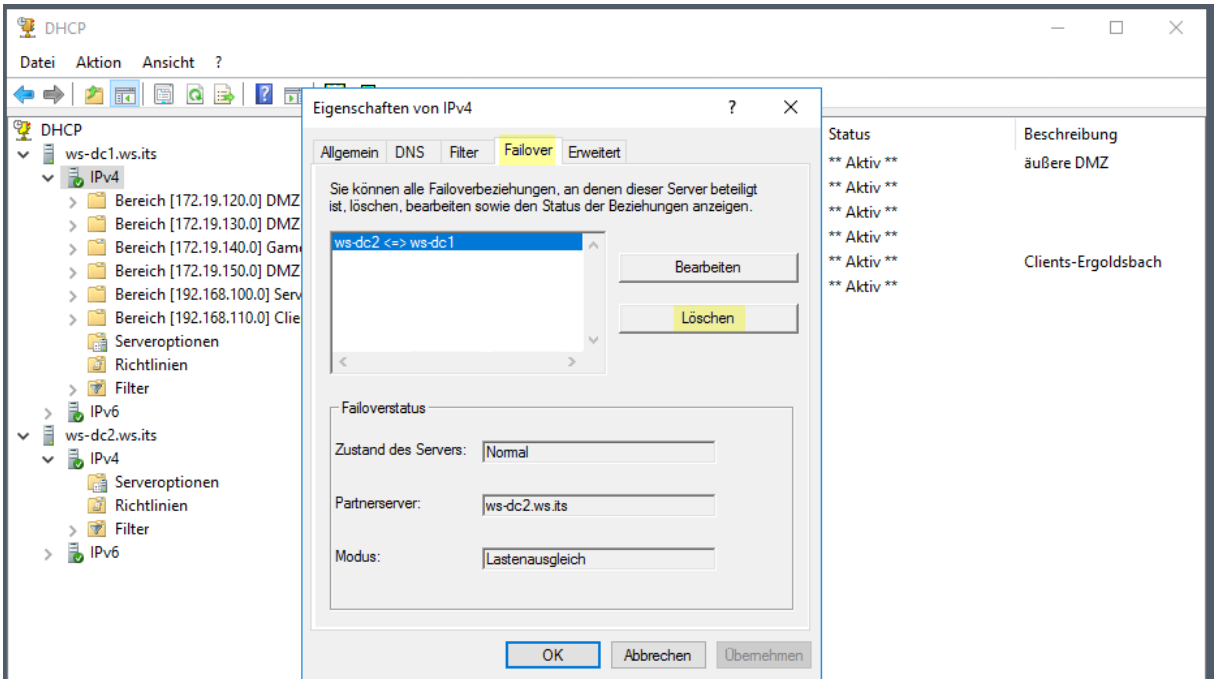
Nach einer Neuanmeldung entferne ich für jeden Scope vom anderen Server aus die Failover-Konfiguration:

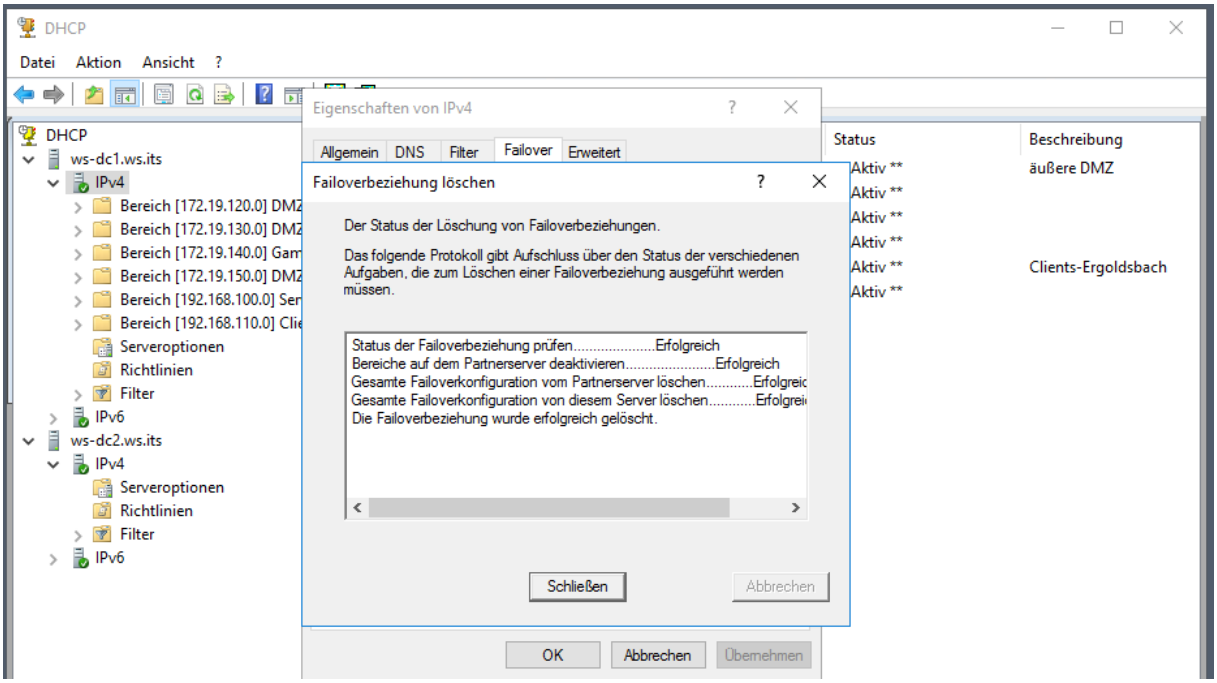


Dabei werden die Scopes auf dem Partnerserver – bei mir also auf WS-DC2 – entfernt:

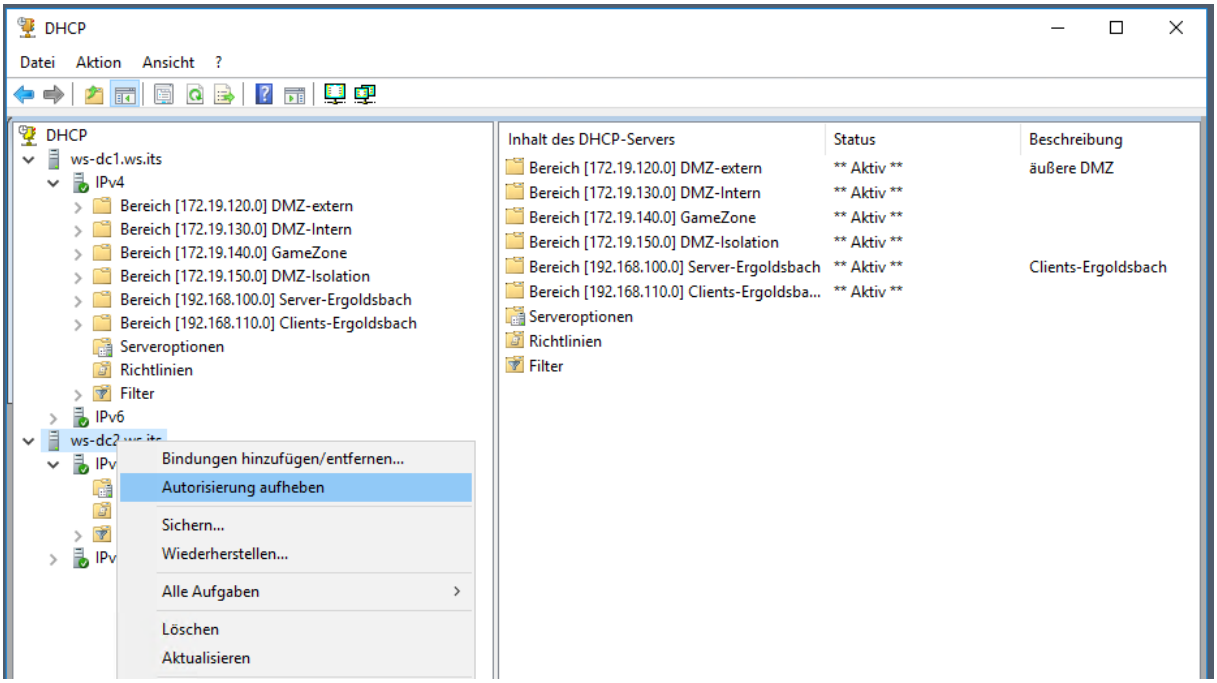


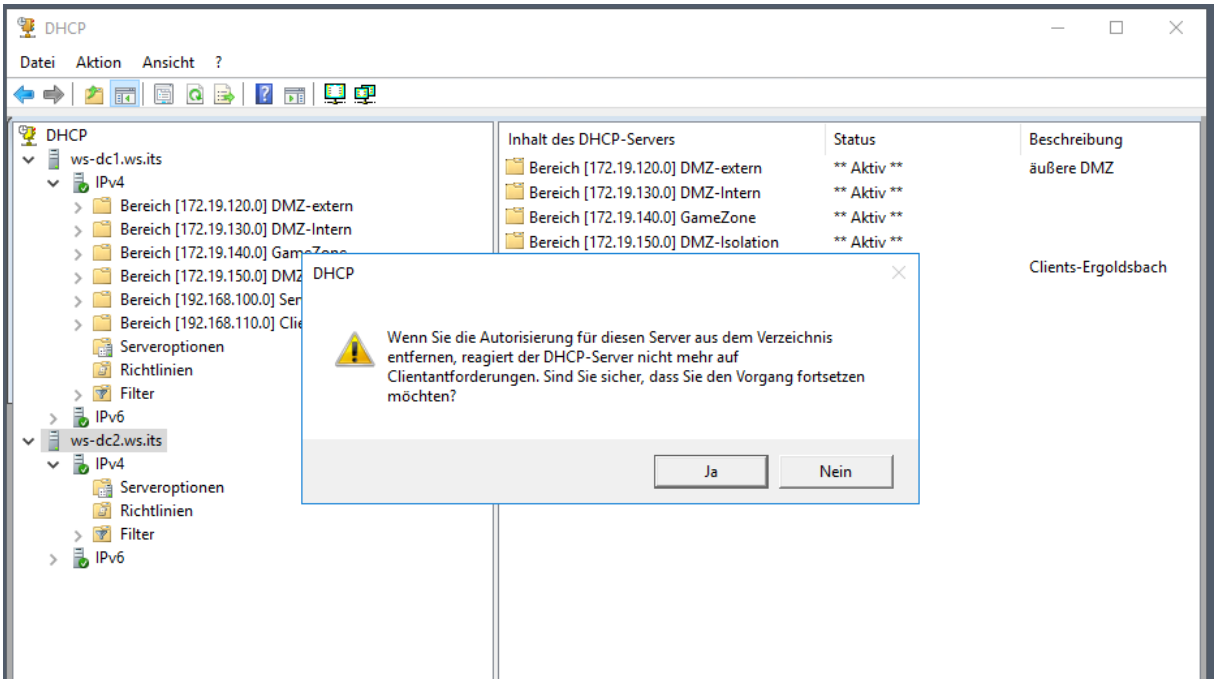
Zuletzt entferne ich noch das Failover selber:





Abschließend entferne ich die Autorisierung des DHCP-Service. So kann der Service nicht mehr starten:

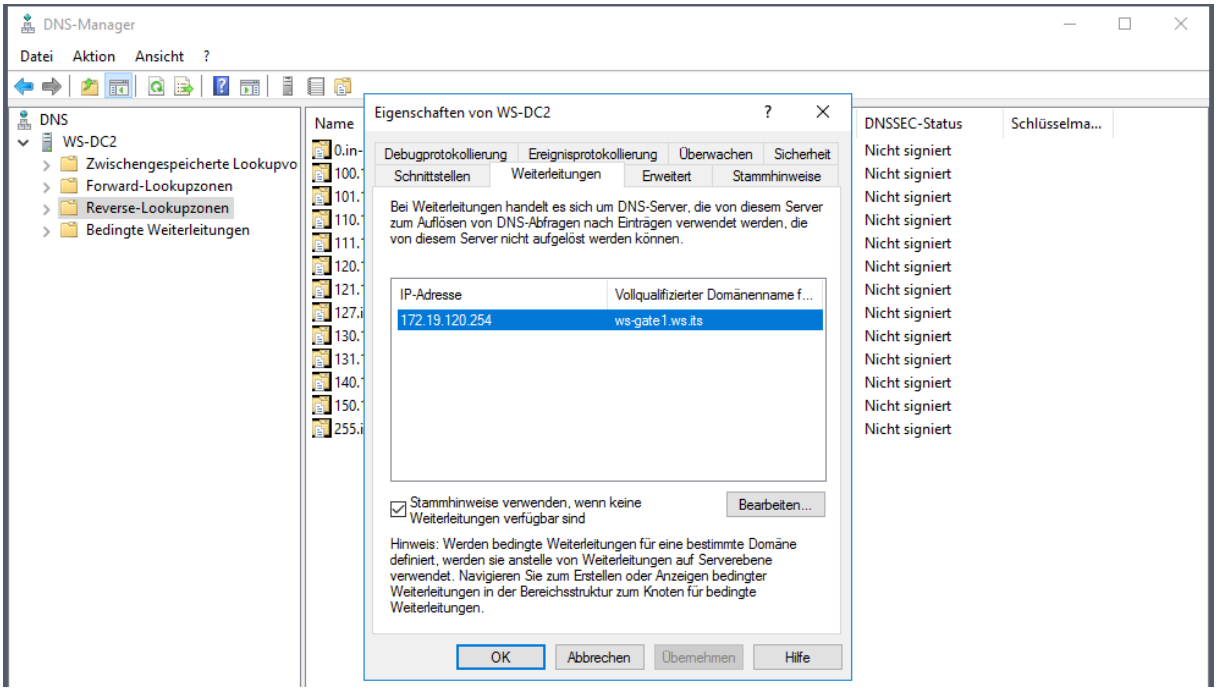




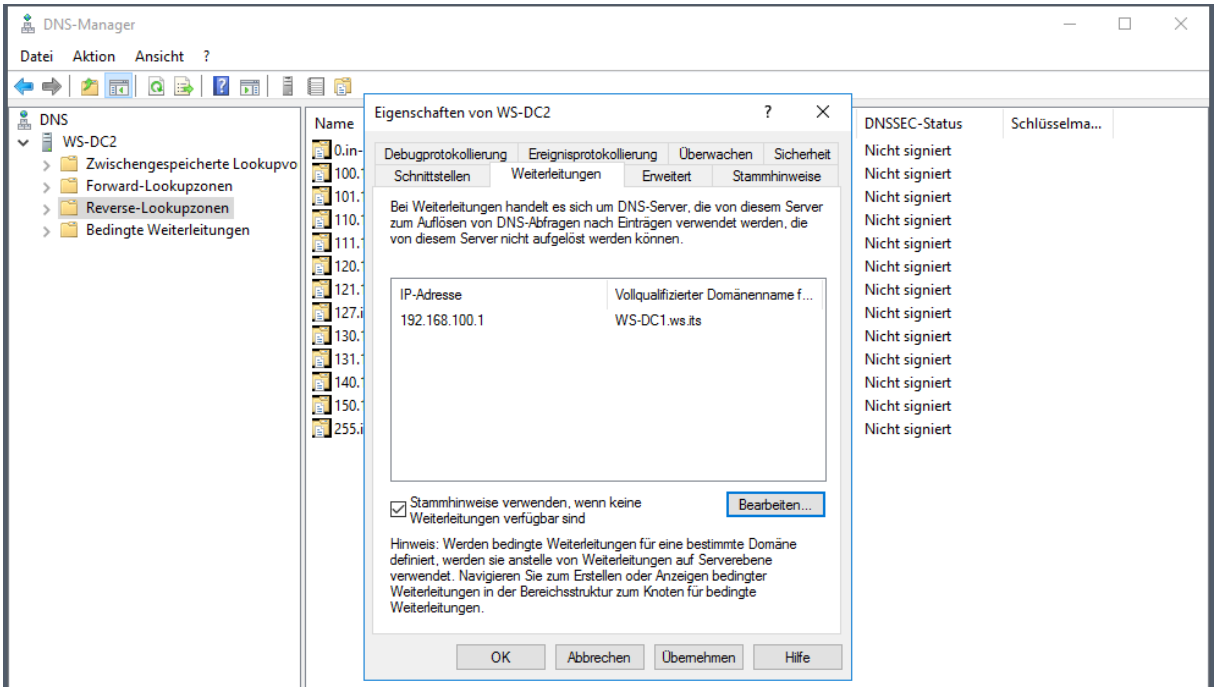
Die Rollen-Deinstallation im Server Manager erspare ich mir.

Vorbereiten der Rolle DNS

Bevor ich ein zweites Mal in das Problem mit dem zonenlosen DNS-Server laufe (Nachzulesen in der Dokumentation zur Migration des WS-DC1), verändere ich an dieser Stelle den globalen Forwarder. Aktuell ist das noch meine Fritzbox:



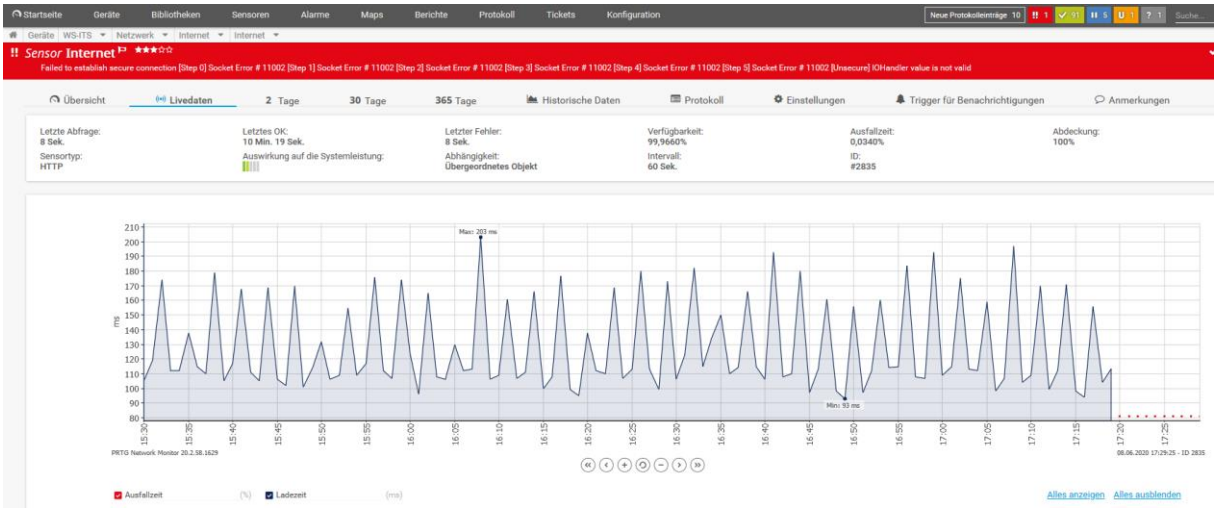
Wenn der Server WS-DC2 nachher keine Zonen mehr hat und Anfragen erhält, dann soll er sich an den WS-DC1 wenden:



Damit sollte ich DNS-Probleme vorbeugen.

TroubleShooting externe Namensauflösung

Oder auch nicht. Denn kurz nach der Veränderung des Forwarders meldete mein Monitoring Probleme mit dem Internet:

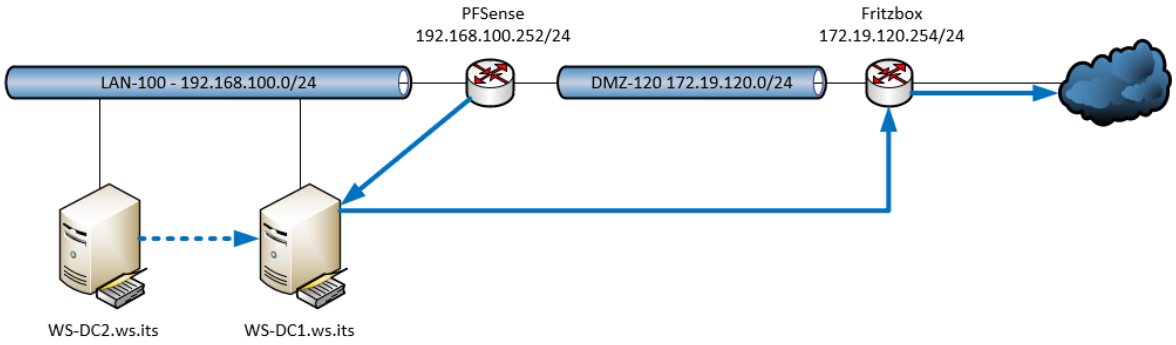


Meine Fritzbox ist aber verbunden und ein Ping auf z.B. 8.8.8.8 geht ohne Probleme durch. Wo kommt das Problem also her?

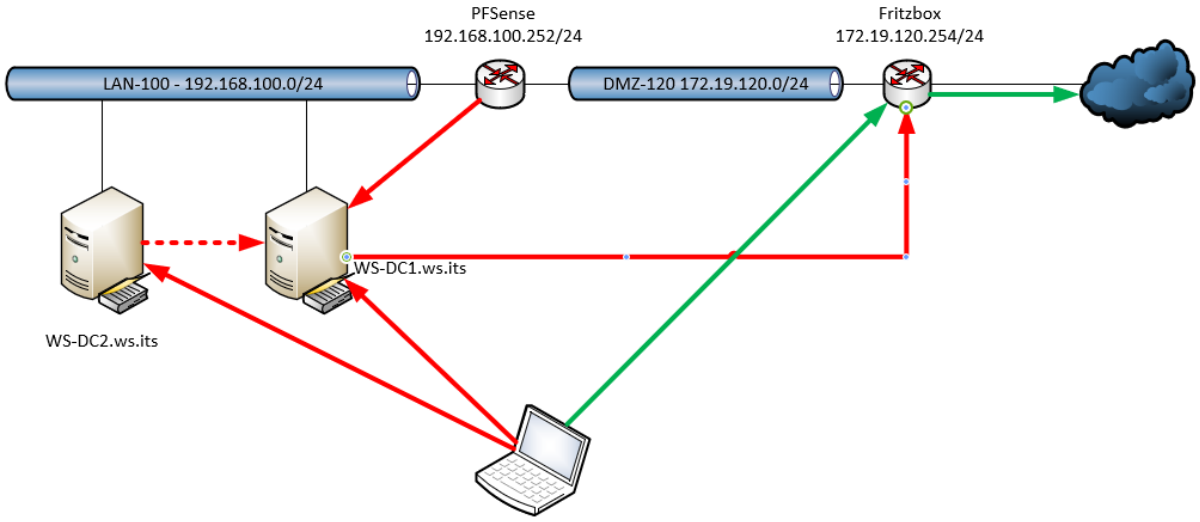
Ich versuche, mit nslookup einen Ansatz zu finden. Aber da hatte ich mal was ausprobiert. Seitdem funktioniert nslookup nicht mehr (alle Anfragen werden mit 0.0.0.0 beantwortet). Aber ein Ping benötigt ja auch eine Namensauflösung. Und die scheint nicht mehr zu funktionieren. Es liegt aber nicht an der externen Namensauflösung:

```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Users\sysadm> nslookup www.google.de
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:    www.google.de.ws.its
Address:  0.0.0.0

PS C:\Users\sysadm> ping www.google.de
Ping-Anforderung konnte Host "www.google.de" nicht finden. Überprüfen Sie den Namen, und versuchen Sie es erneut.
PS C:\Users\sysadm> nslookup www.google.de 192.168.100.252
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.100.252

DNS request timed out.
    timeout was 2 seconds.
PS C:\Users\sysadm> nslookup www.google.de 172.19.120.254
Server:  fritz.box
Address:  172.19.120.254

Nicht autorisierende Antwort:
Name:    www.google.de
Addresses:  2a00:1450:4001:81c::2003
          172.217.23.131

PS C:\Users\sysadm>
```

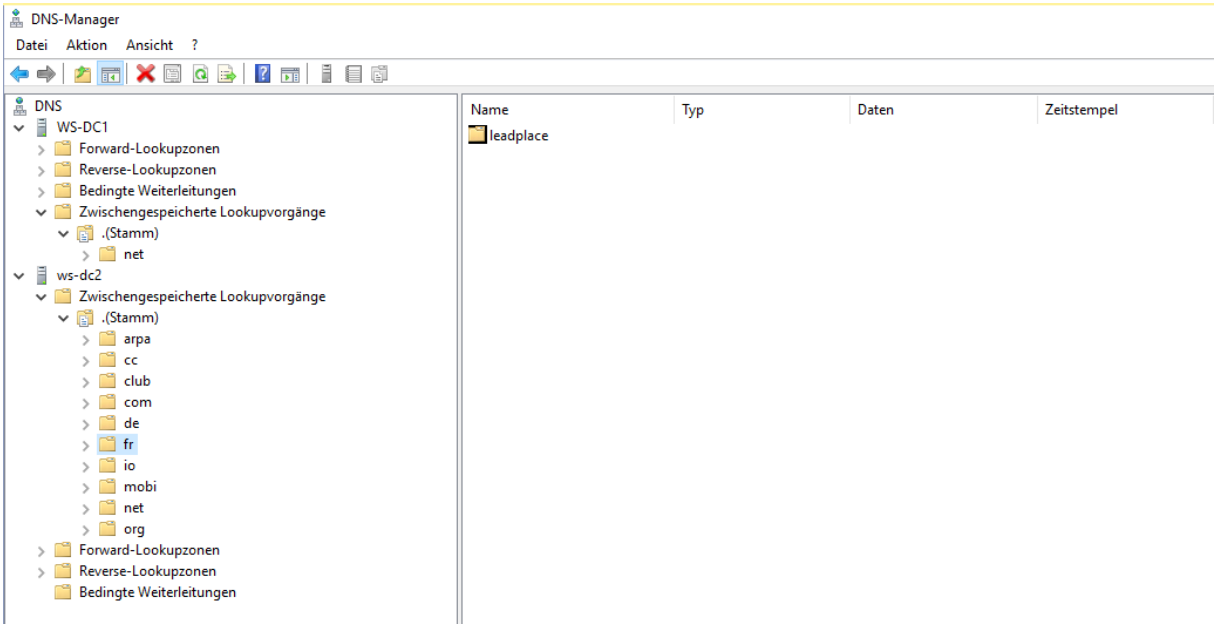
Dazu ist ein Schaubild hilfreich. Die blauen Pfeile zeigen die Forwarder an. WS-DC2 fragt aktuell beim WS-DC1 nach. Und dieser sollte an die Fritzbox weiterleiten:



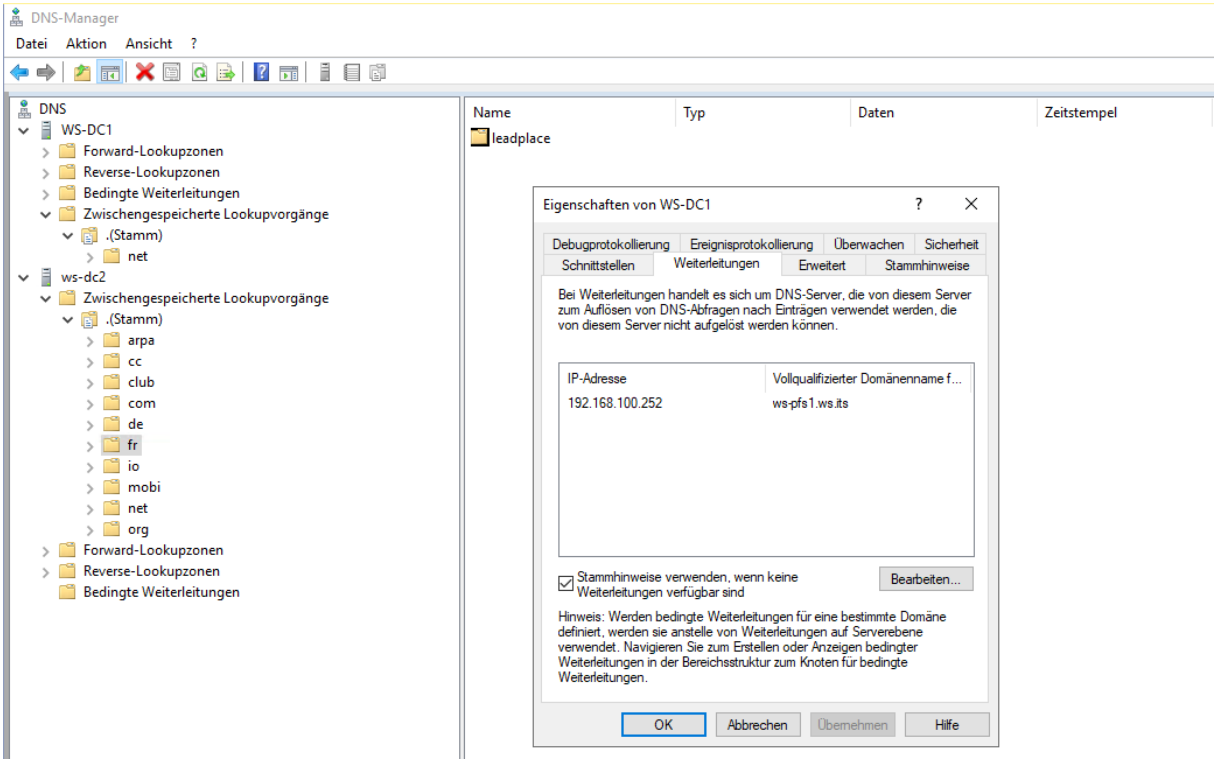
Wenn ich nun vom Client aus eine externe Namensauflösung über einen der beiden Domänen Controller versuche, dann schlägt diese fehl. Ebenso sind gerade alle Smartphones dem Problem beigetreten. Denn diese fragen die PFSense. Nur wenn ich die Fritzbox direkt befrage, erhalte ich eine Antwort:



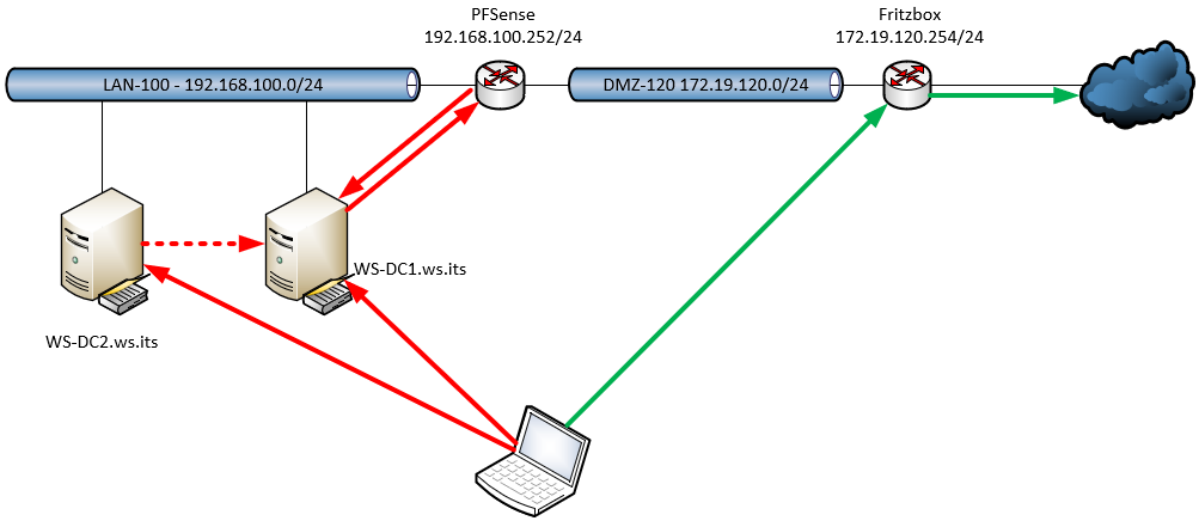
Ich kontrolliere mal den ServerCache beider DNS-Server. Der wird angezeigt, wenn man in der Management-Konsole die erweiterte Ansicht aktiviert. Das ist sehr interessant: Der Server WS-DC1 hat keine externen Namen im Cache! Nur der Server WS-DC2 ist noch versorgt:



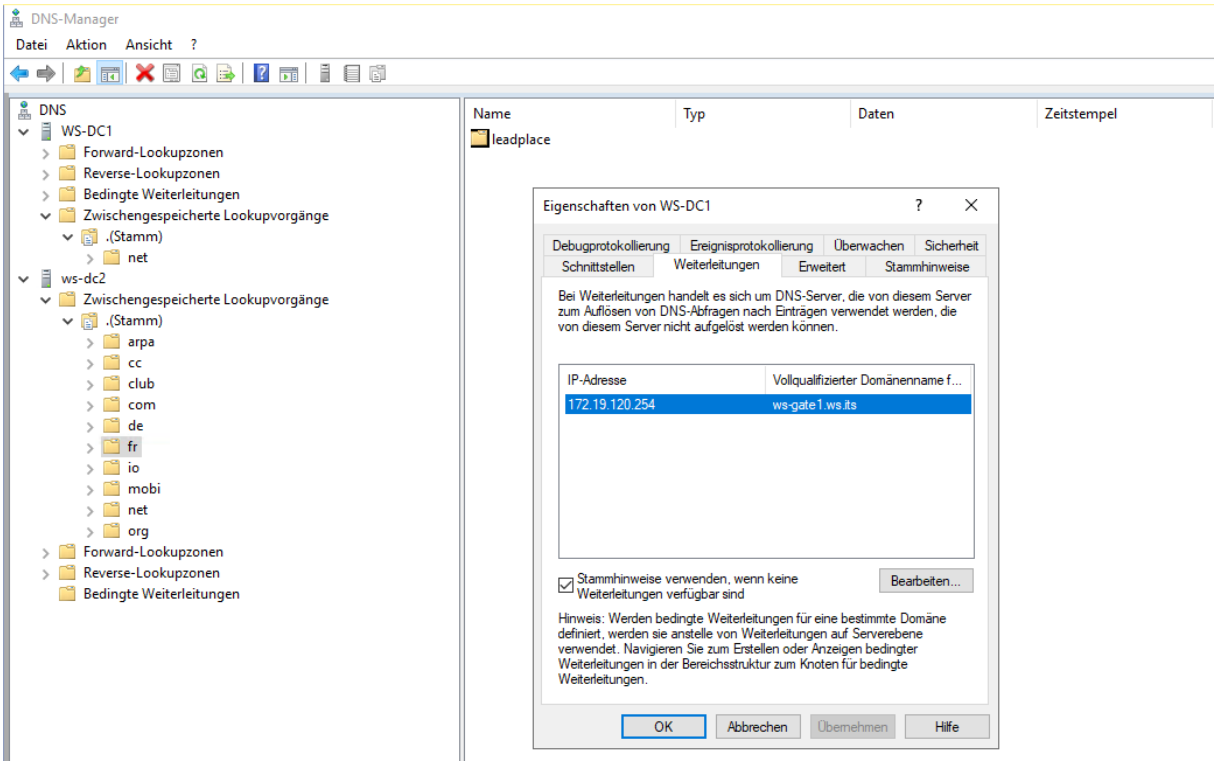
Das bedeutet, der Server WS-DC1 hatte die Störung schon vor der Umstellung am WS-DC2! Und da dieser nur für externe Auflösungen den Problemserver WS-DC1 befragt, weitet sich das Problem auf alle Clients aus. Offensichtlich ist der Server WS-DC1 nicht richtig konfiguriert. Das prüfe ich nach: Und Jackpot! Der Server hat einen falschen Forwarder:



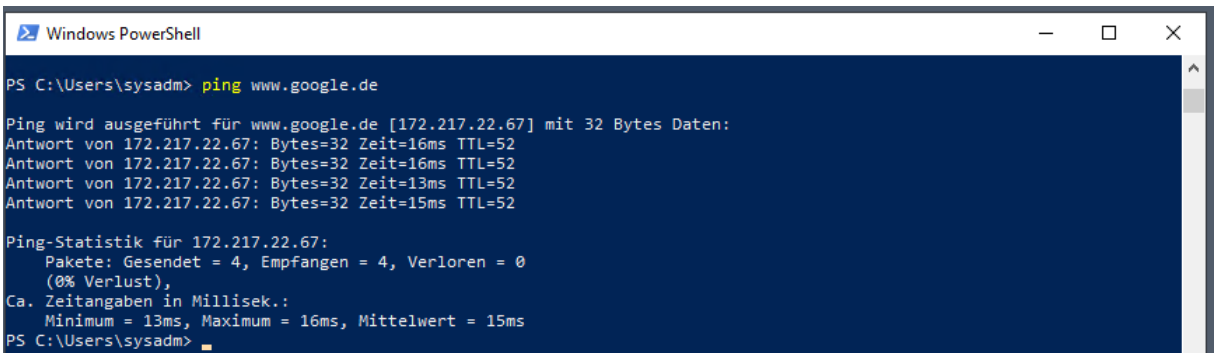
Das kann so nicht funktionieren. Im Schaubild erkennt man deutlich die Isolation:



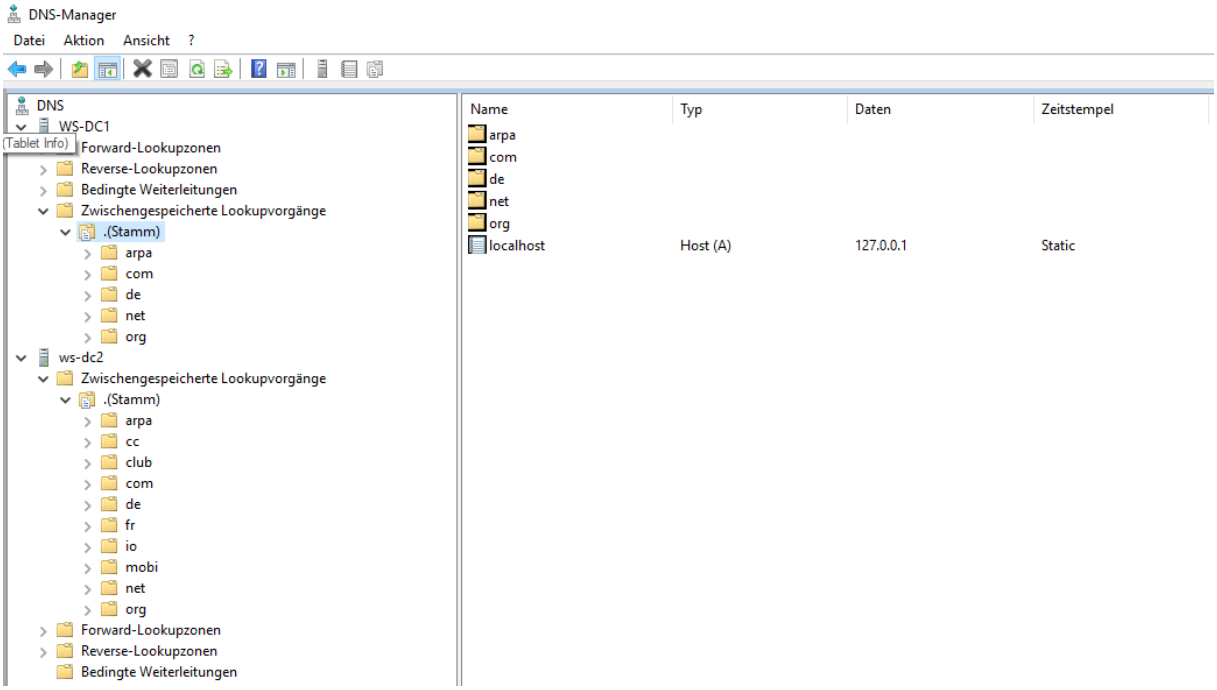
Ich stelle daher den richtigen Wert im Forwarder ein:



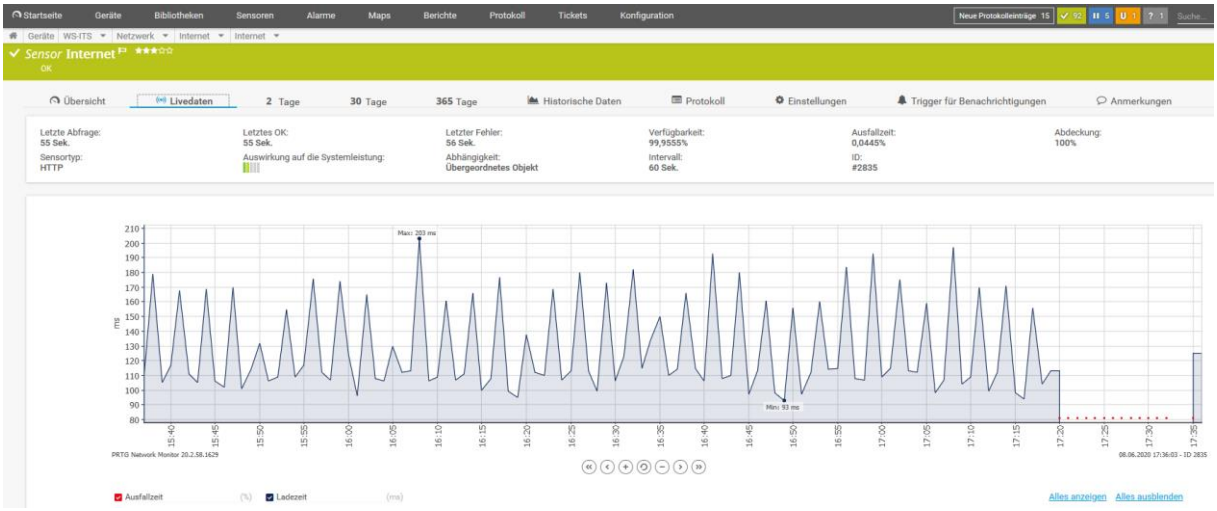
Und nahezu sofort kann ich die Namensauflösung erfolgreich testen:



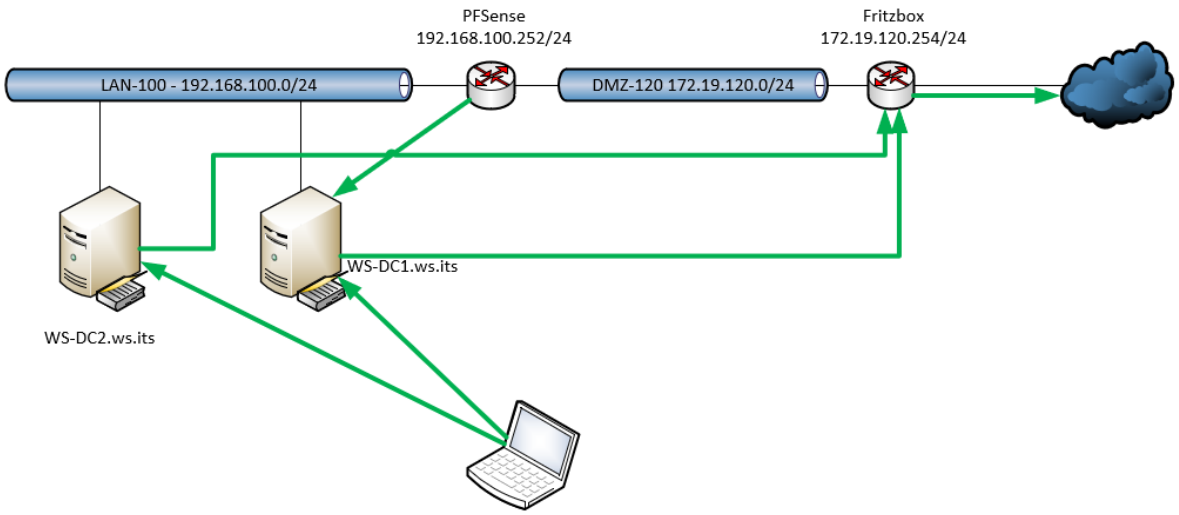
Im DNS-ServerCache tauchen die ersten Records auf:



Und auch mein Monitoring wird wieder grün:



Meine Namensauflösung funktioniert wieder einwandfrei nach dem geplanten Schema:



Erklärung:
Warum ist das Problem nicht schon vorher aufgefallen? Den anderen Domain Controller hatte ich vor 6 Tagen erneuert und dabei den Fehler konfiguriert. Etwa die Hälfte meiner Server und Clients verwendet WS-DC1 als primären DNS-Server. Aber fast alle Server kommen eh nicht in das Internet. So fällt bei denen natürlich auch ein Fehler bei der externen Namensauflösung nicht auf. Bleiben also noch die Clients über. Bei denen gibt es mehrere Erklärungen:

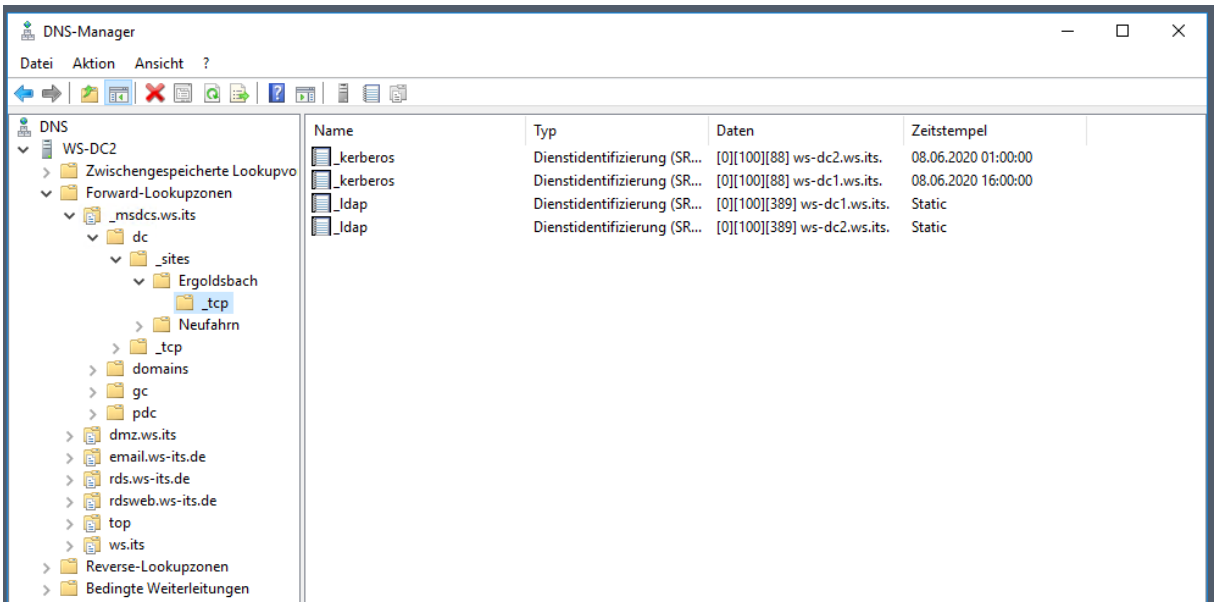
1. Jeder Client hat eine 50% Chance, durch das DHCP-Failover den WS-DC2 als primären DNS-Server zu erhalten. Da war wohl mein Notebook dabei.
2. Andere Clients bis auf einen waren ausgeschaltet. Ich habe gerade Urlaub.
3. Nur ein Client hatte Probleme. Und der Benutzer – mein Sohn – meldete mir Probleme mit dem Netzwerk erst heute…

Aber die Smartphones im Netzwerk müssten doch auffallen. Und das taten sie auch. Aber ich suchte an einer anderen Stelle. Ich habe zwei WLAN-AccessPoints verbaut. Diese habe ich am 01.06.2020 durch einen WLAN-Controller zusammengeschlossen, damit das Roaming besser funktioniert. Es wurde aber schlimmer. Aber ich hatte die Controller-Software im Verdacht. Es konnte ja keiner ahnen, dass die Namensauflösung teilweise nicht funktionierte. Smartphones sind für das Troubleshooting eben nur bedingt geeignet.

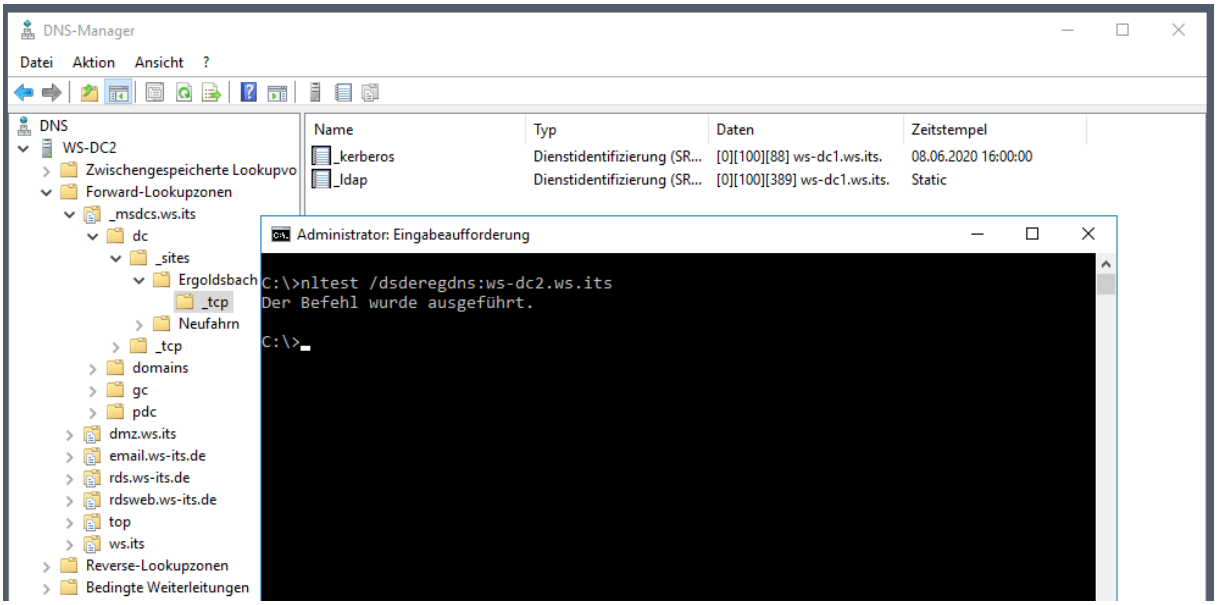
In größeren Netzwerken wäre ein solcher Fehler innerhalb der ersten Stunde aufgefallen.

Entfernen der Rolle Active Directory

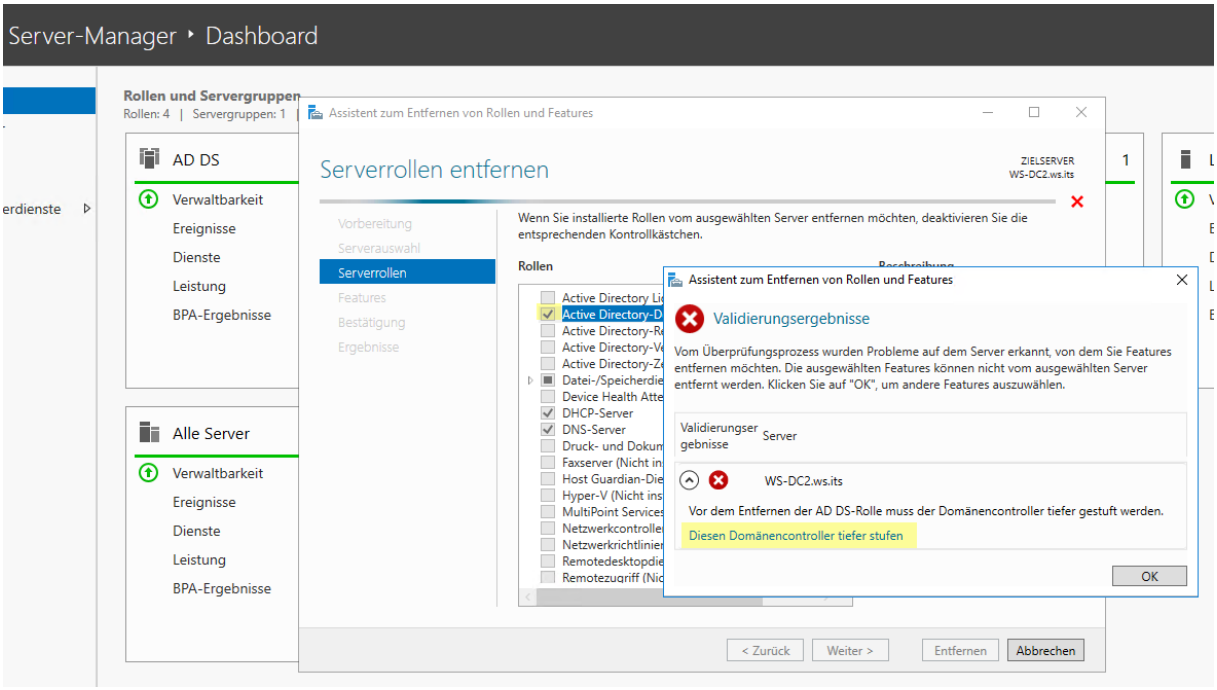
Nachdem meine Namensauflösung wieder funktioniert, kann es endlich mit der Migration weitergehen. Im DNS-Server stehen noch die vielen Records, mit denen die Clients meine Domain Controller und ihre Services finden:



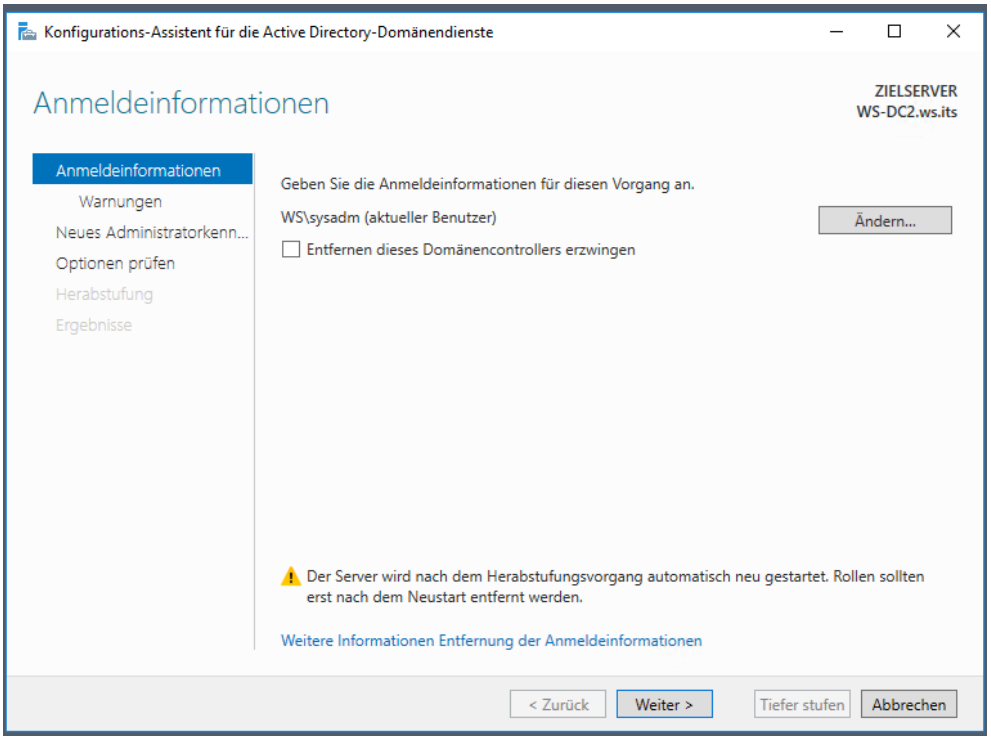
Ich leite die Maintenance ein, indem ich den Server WS-DC2 deregistriere:



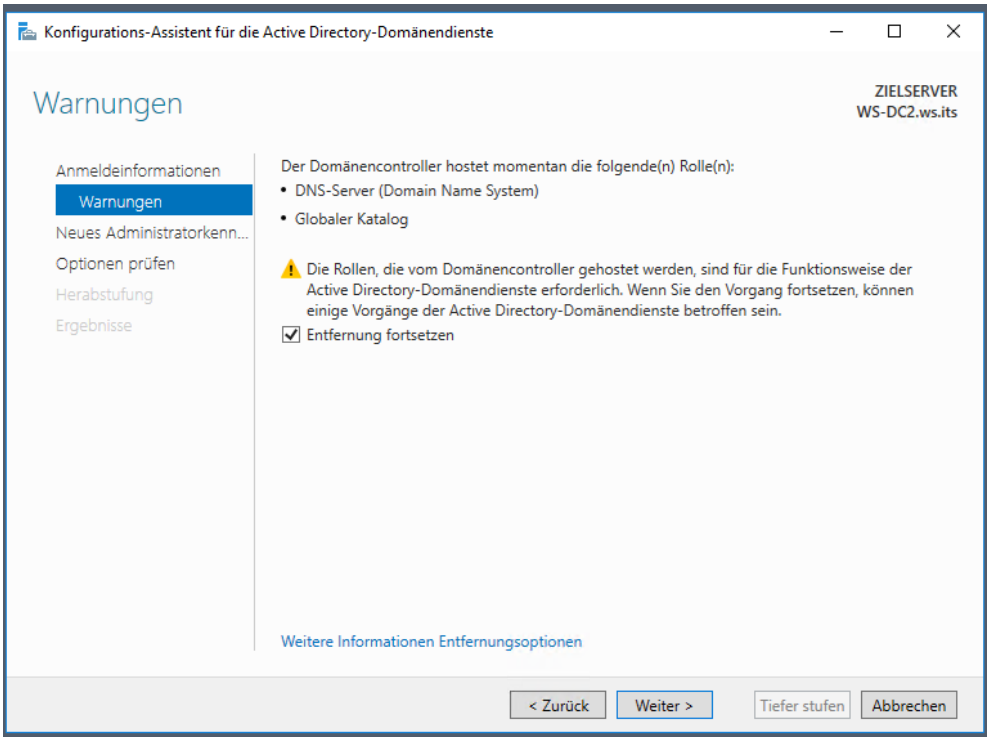
Dann starte ich die Rollen-Entfernung im Server Manager. Dabei kommt die bekannte Meldung, dass zuvor der Server als Domain Controller heruntergestuft werden muss. Das ist mein Einstiegspunkt:



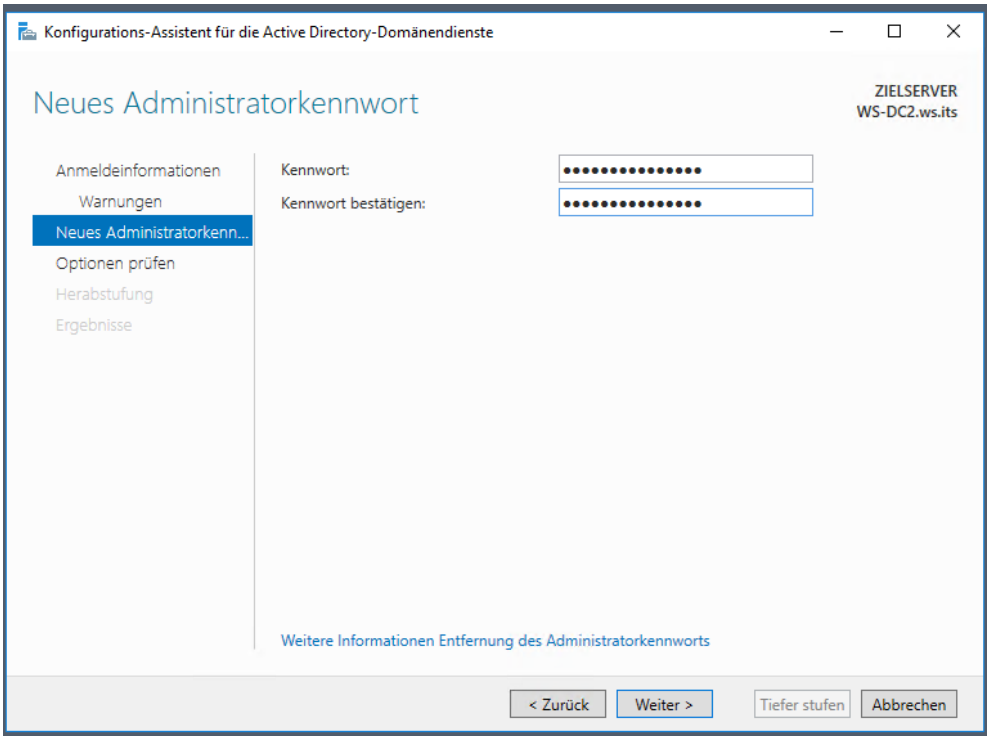
Der Assistent kann den aktuellen Benutzeraccount verwenden:



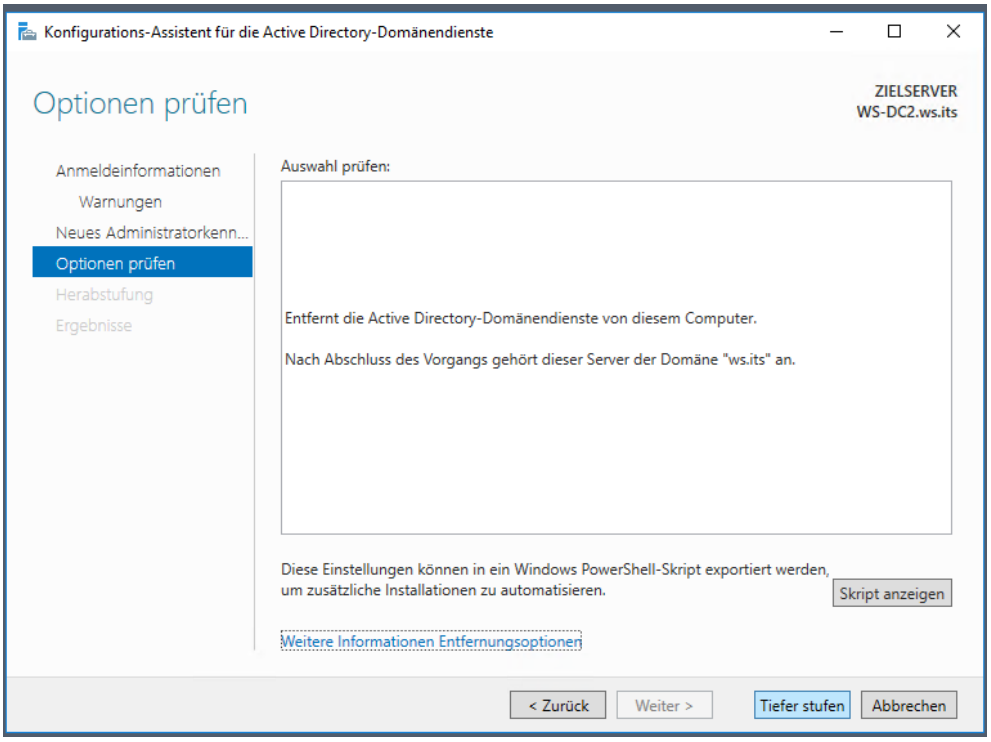
Hier muss nur der Haken zur Bestätigung gesetzt werden:



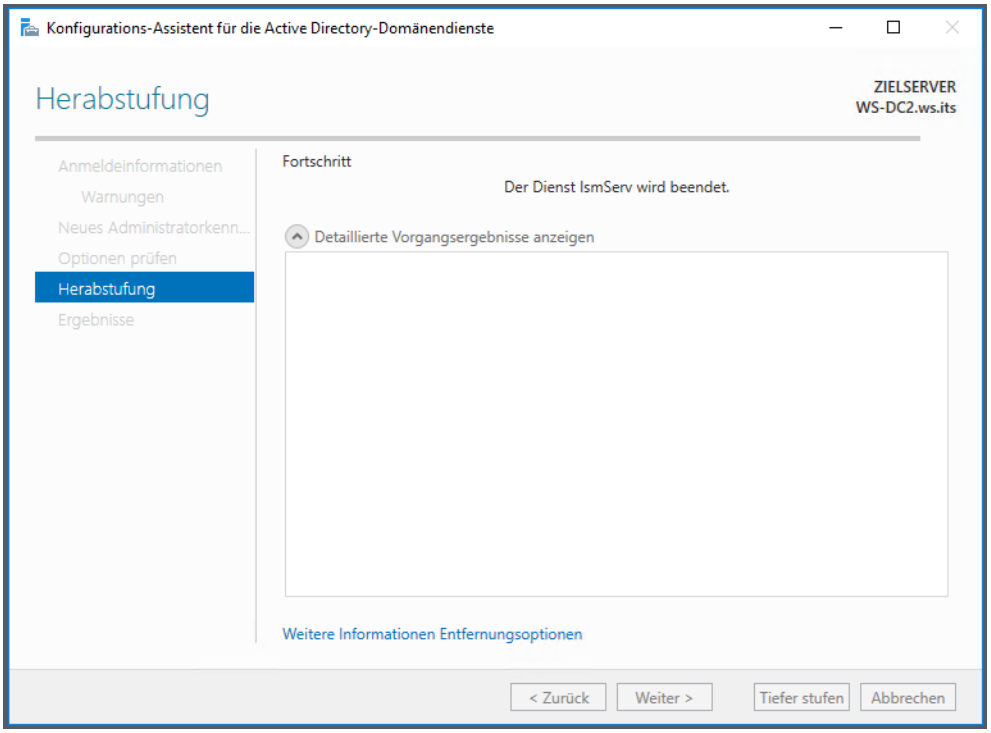
Nach Abschluss der Aktion hat der Server wieder einen lokalen Administrator-Account. Der braucht ein Passwort:



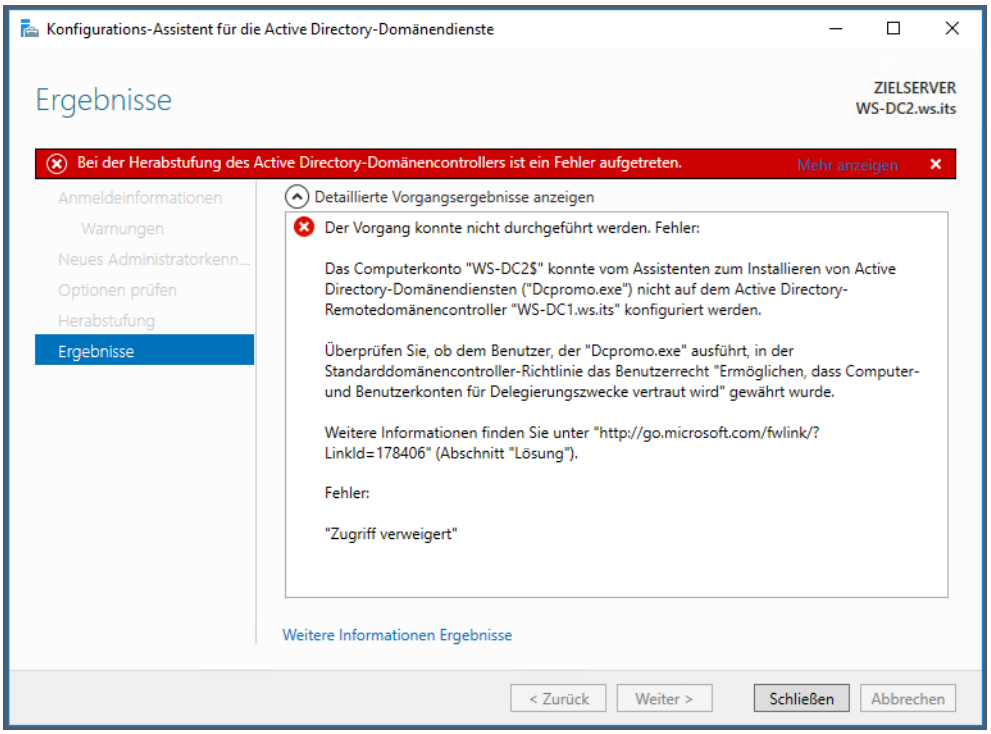
Und es kann losgehen:



Der Assistent startet:



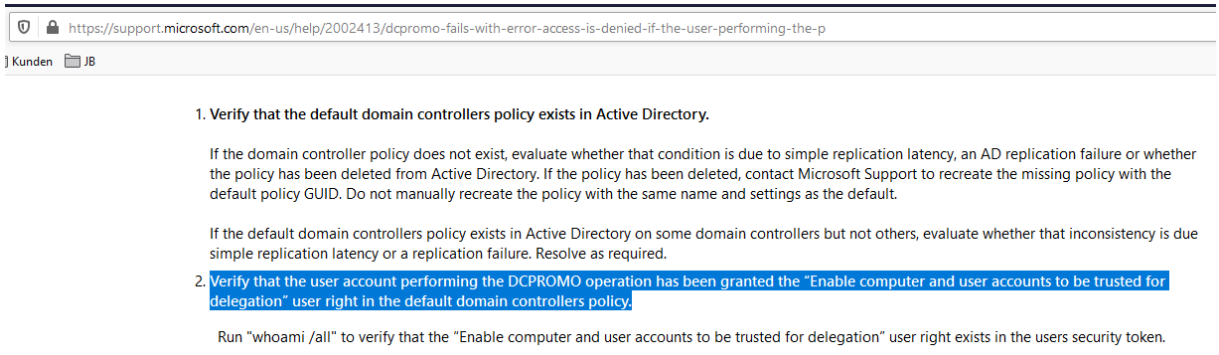
Aber leider bricht er nach einigen Sekunden mit dieser Fehlermeldung ab:



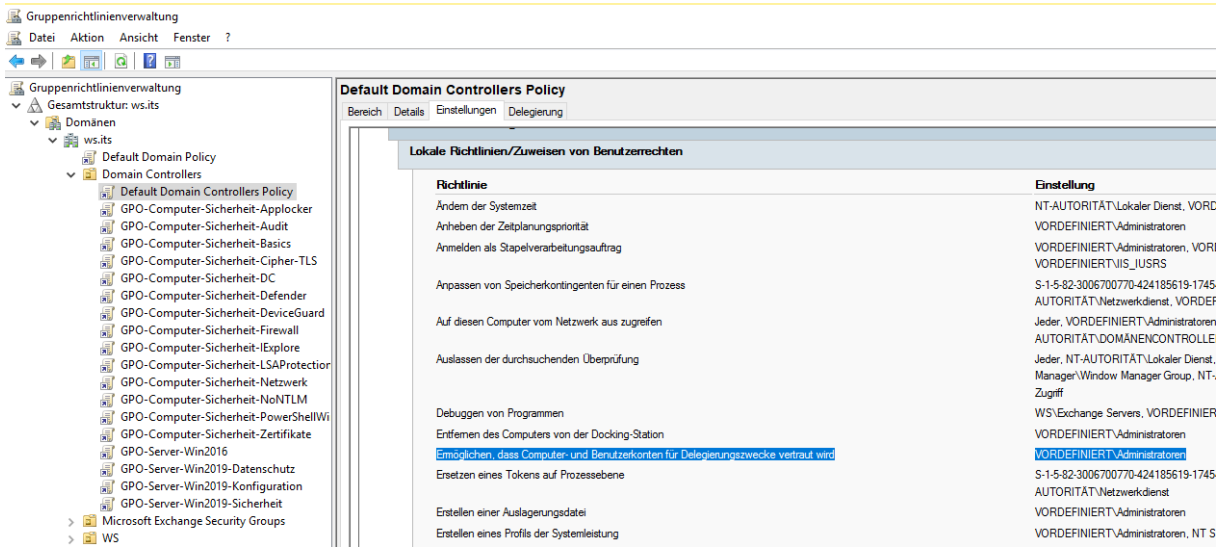
Das war nicht erfolgreich.

TroubleShooting beim Entfernen des Domain Controllers

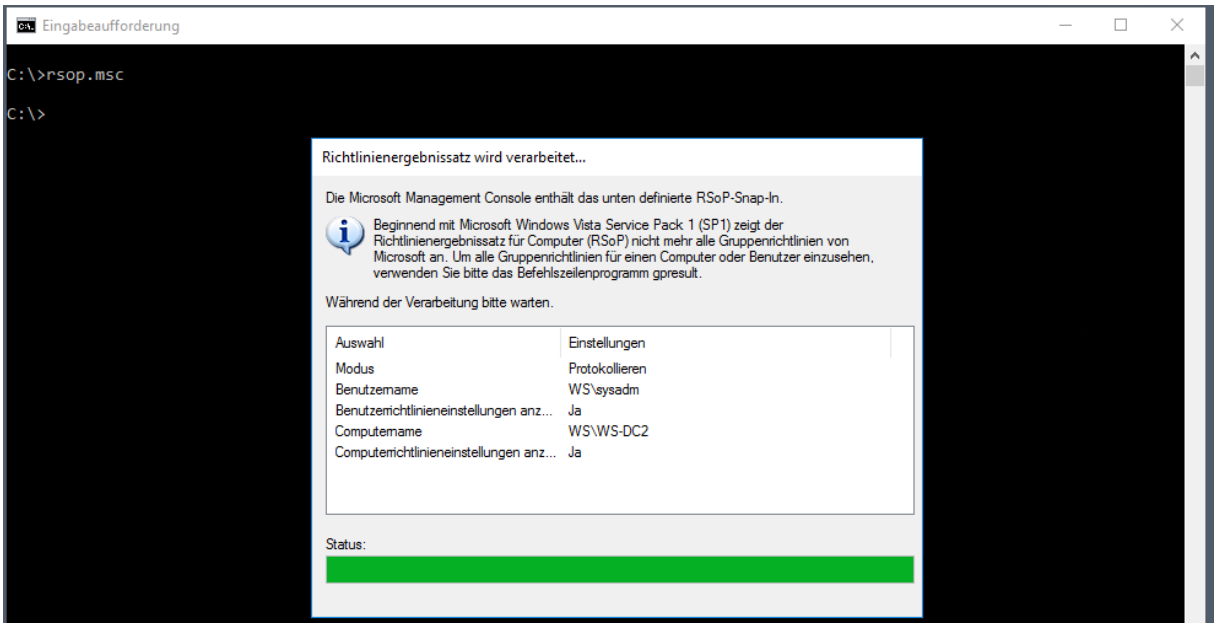
Also lege ich ein weiteres TroubleShooting ein. Der Link in der Fehlermeldung führt mich auf diese Webseite von Microsoft. Als Fehlerursache finde ich hier diesen Eintrag:



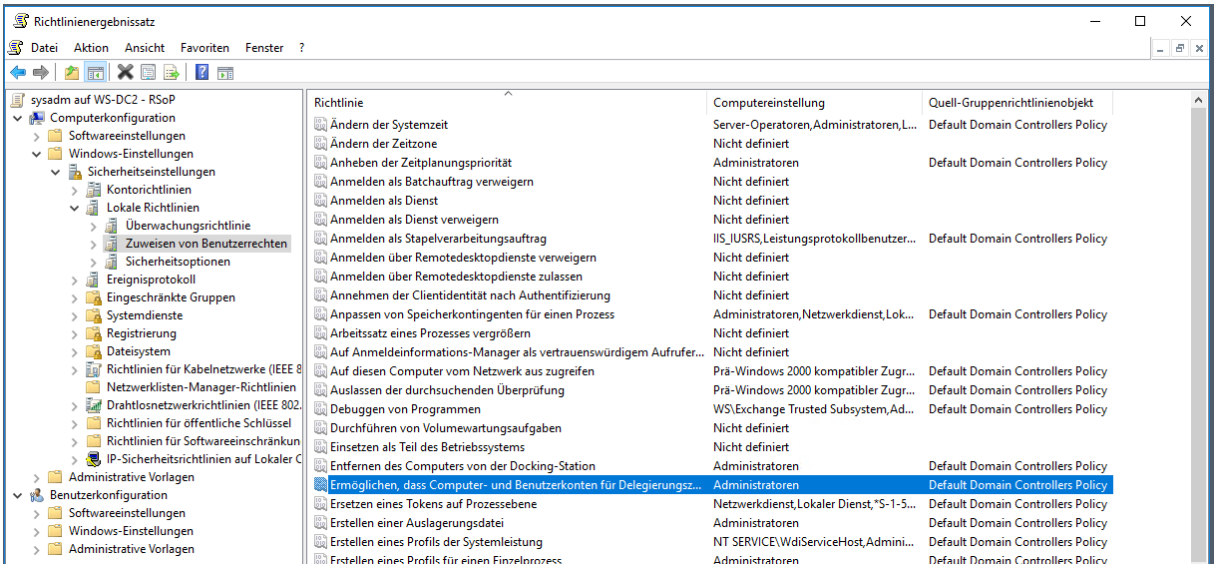
Die Einstellung wird normalerweise von der Default Domain Controller Policy gesetzt. Diese habe ich in meiner Infrastruktur nicht verändert:



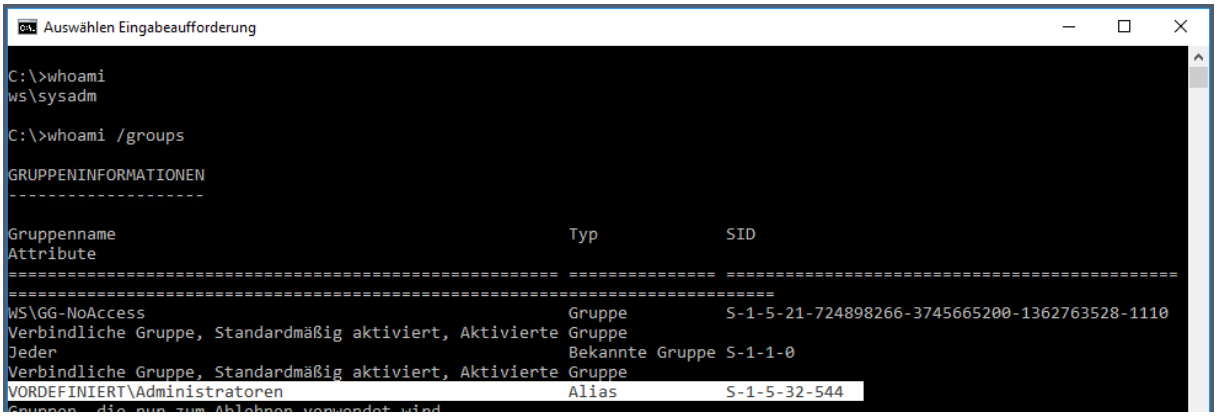
Ich erstelle mit RSOP eine Zusammenfassung der Gruppenrichtlinienverarbeitung. Vielleicht kommt diese Einstellung nicht an. Das könnte z.B. bei einer Überlagerung mit einer anderen GPO passieren:



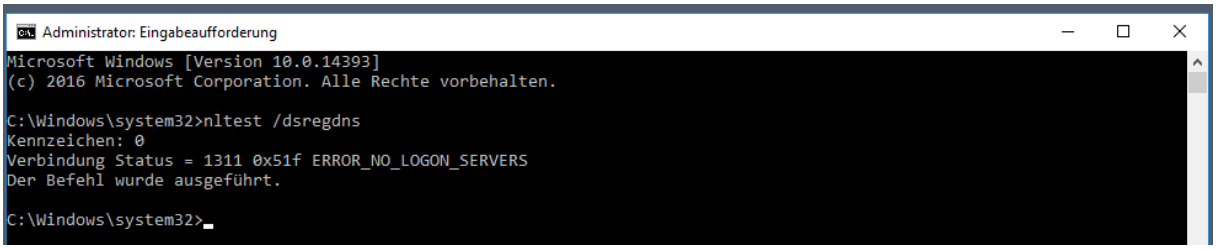
Im Ergebnis vom RSOP sehe ich aber die entsprechende Einstellung:



Das kann nicht mein Problem sein. Vielleich bin ich mit meinem Account nicht Mitglied in der Gruppe Administratoren? Ein einfaches whoami /groups zeigt die Mitgliedschaft an:

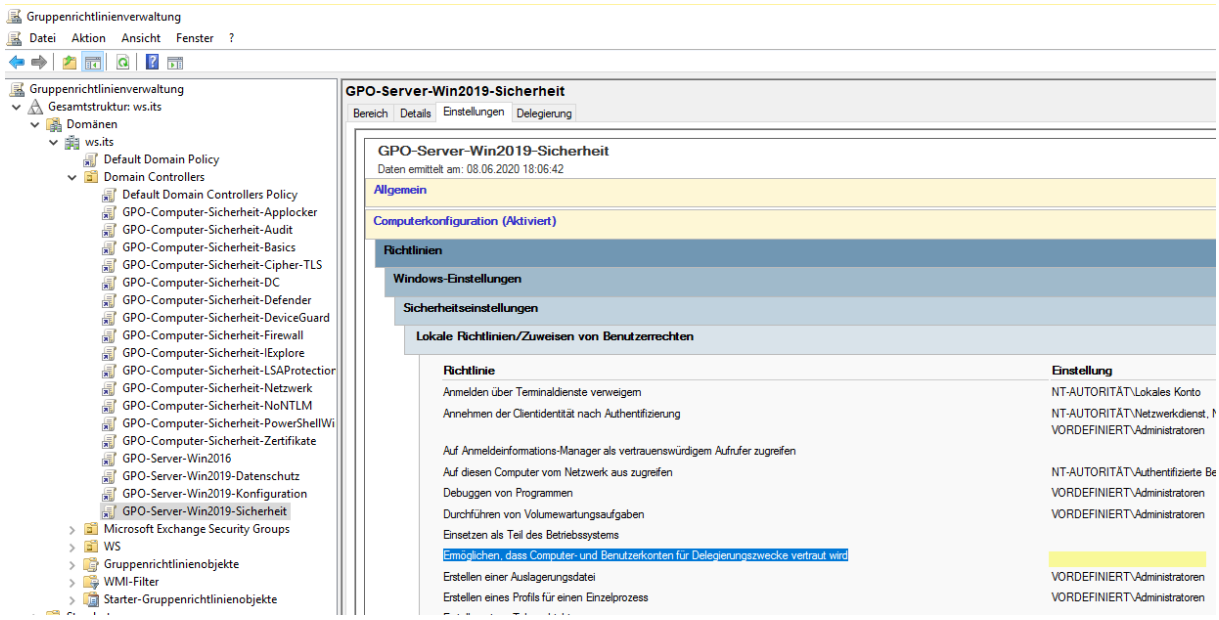


OK, dann beende ich mal die DNS-Maintenance, bis ich eine Lösung gefunden habe. Aber auch dieser Befehl schlägt jetzt fehl:

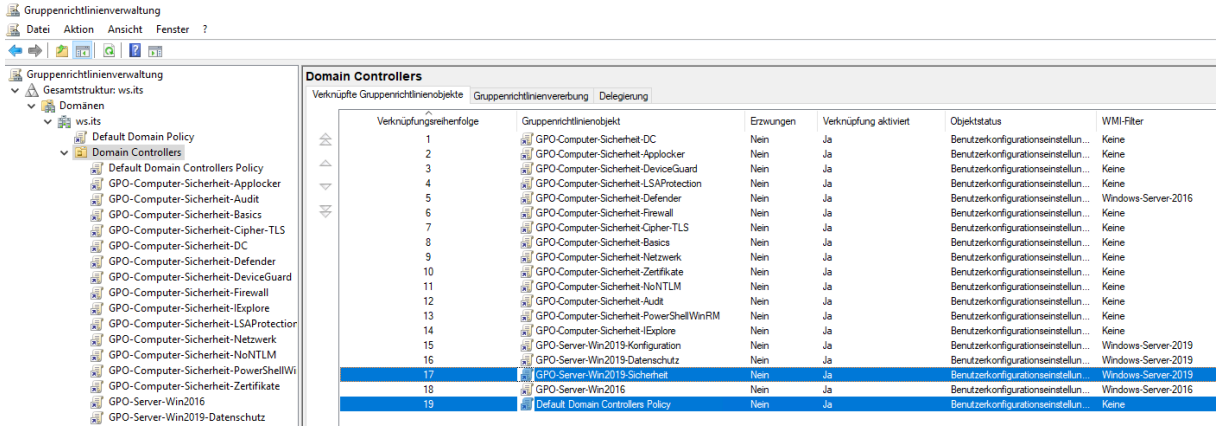


Da es absolut keine relevanten Einträge in den Eventlogs gibt, starte ich den Server mal neu. Dann versuche ich die Entfernung des Domain Controllers erneut. Der Fehler bleibt aber der gleiche.

Und dann kommt mir eine Idee: Was hat sich seit dem 02.06.2020 verändert, als ich erfolgreich den WS-DC1 herunterstufen konnte? Richtig: Seitdem habe ich einen Domain Controller mit Windows Server 2019, für den ich drei neue Gruppenrichtlinien auf der Organisationseinheit „Domain Controllers“ verknüpft habe. Vielleicht ist da eine Überlagerung enthalten? Und gleich die erste GPO ist ein Treffer! Hier wird das erforderliche Recht explizit niemandem gewährt:

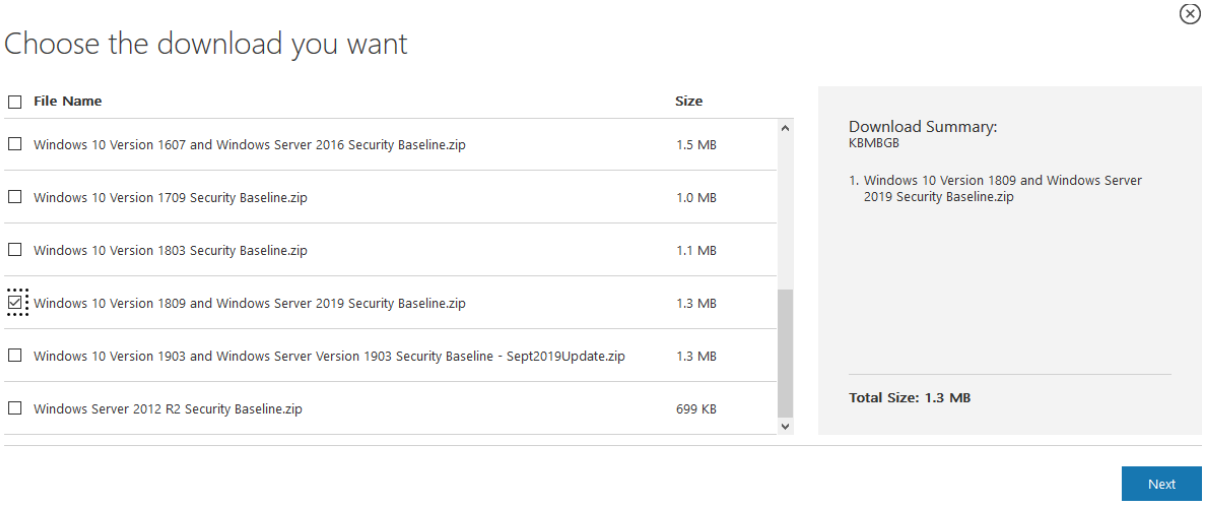


Und wie man deutlich sehen kann überlagert die GPO meine Default Domain Controller Policy:

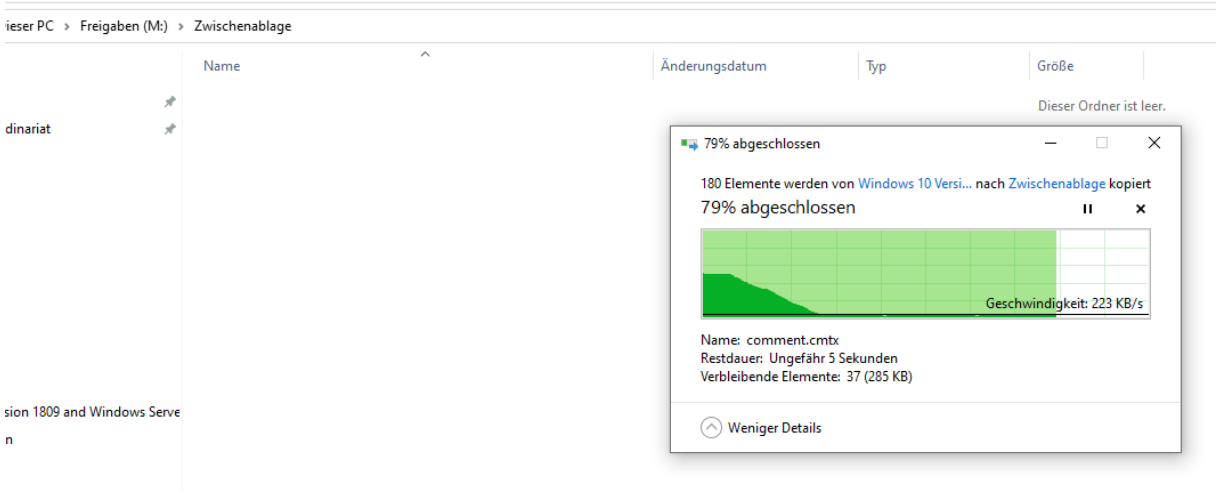


Was war denn an diesem Tag nur los? Vielleicht sollte ich im Urlaub keine Domain Controller mehr migrieren? Die Erklärung ist jetzt recht einfach: Die Gruppenrichtlinie „GPO-Server-Win2019-Sicherheit“ ist ein 1:1-Import der SecurityBaseline-GPO aus dem Security Compliance Toolkit von Microsoft. Nur ist diese GPO für Memberserver gedacht! Für Domain Controller gibt es eine eigene. Die hatte ich bisher aber nicht gebraucht. Für den Fall, dass es eine neuere Version gibt lade ich mir die Baselines direkt von Microsoft herunter:

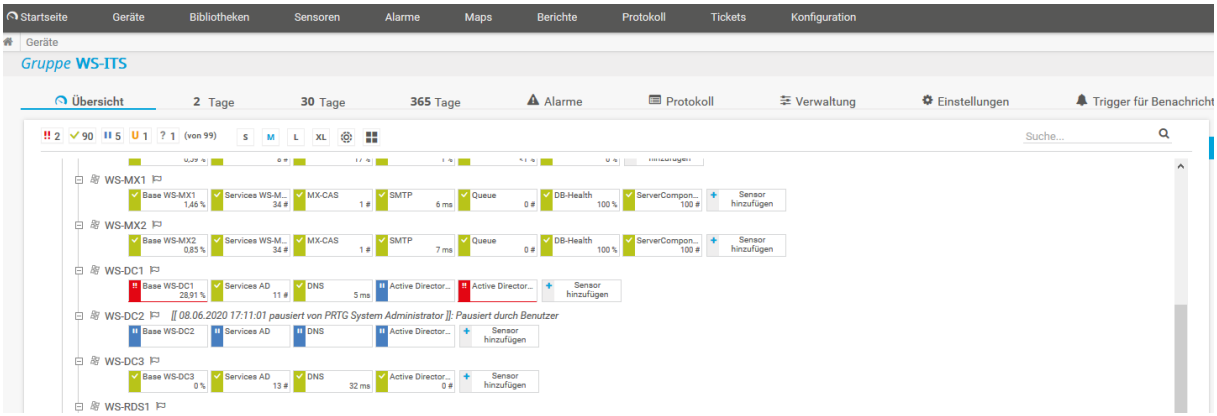
https://www.microsoft.com/en-us/download/details.aspx?id=55319



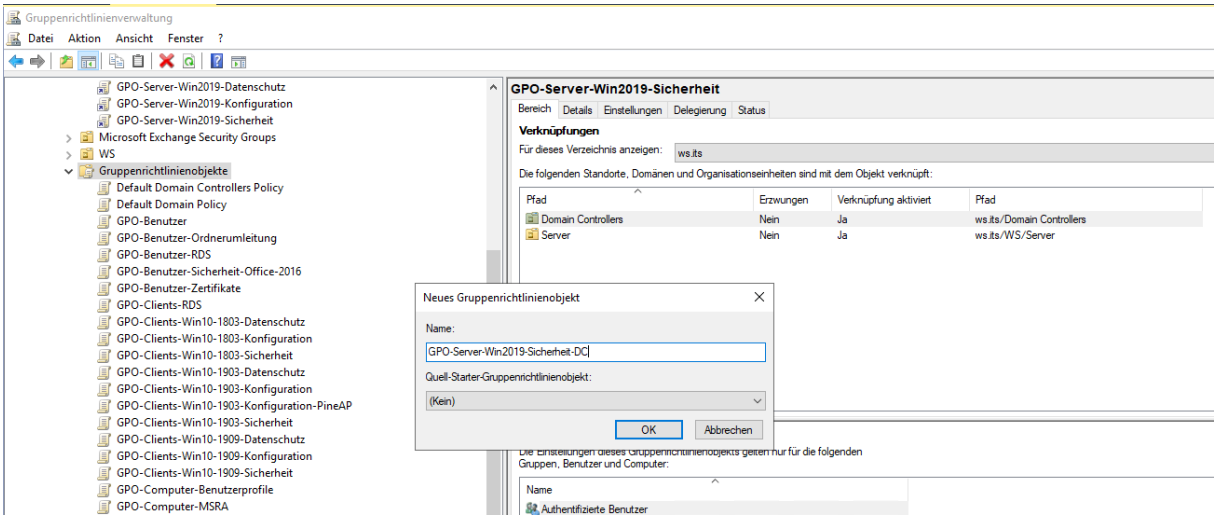
In der ZIP-Datei ist ein Ordner GPOs enthalten. Den kopiere ich in meine Zwischenablage-Freigabe:



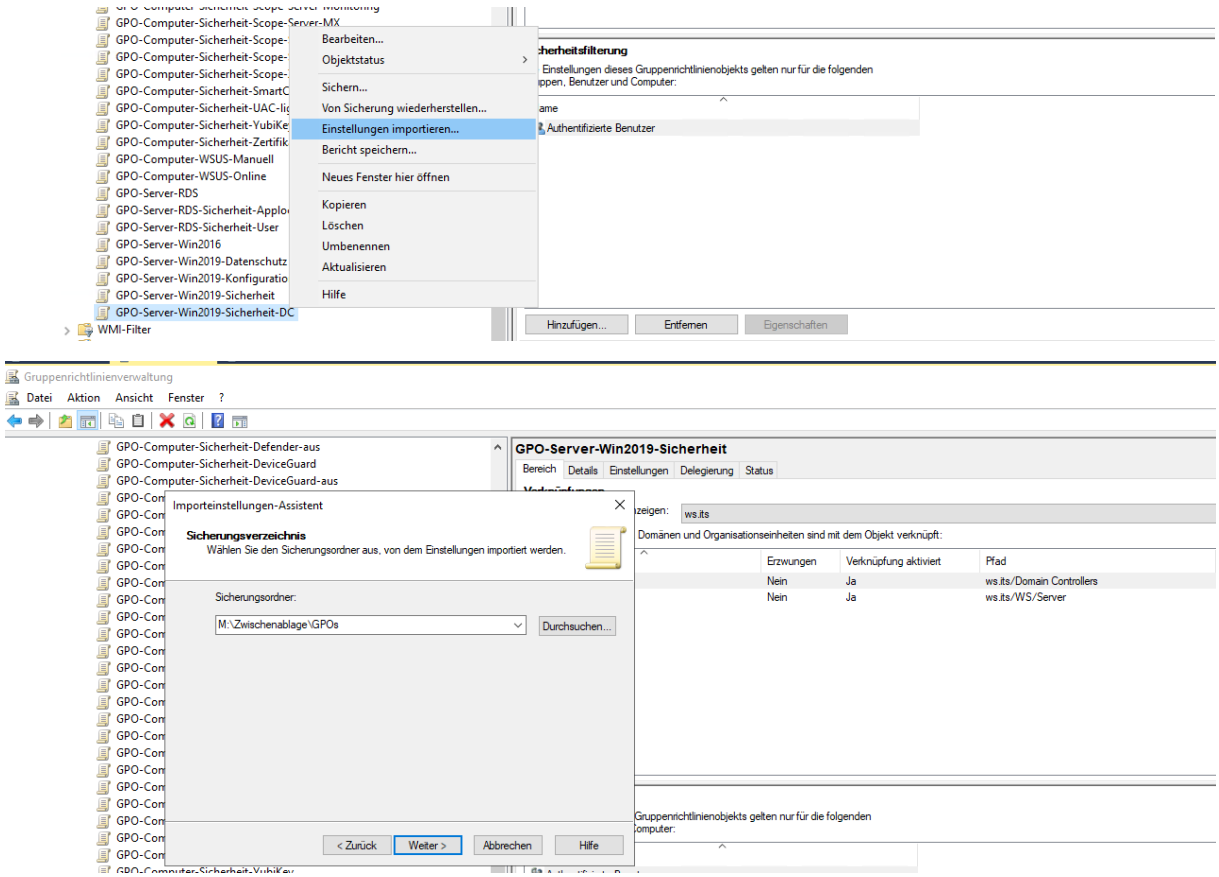
Mittlerweile hat mein Domain Controller weitere Probleme. Das könnten Folgeerscheinungen sein:



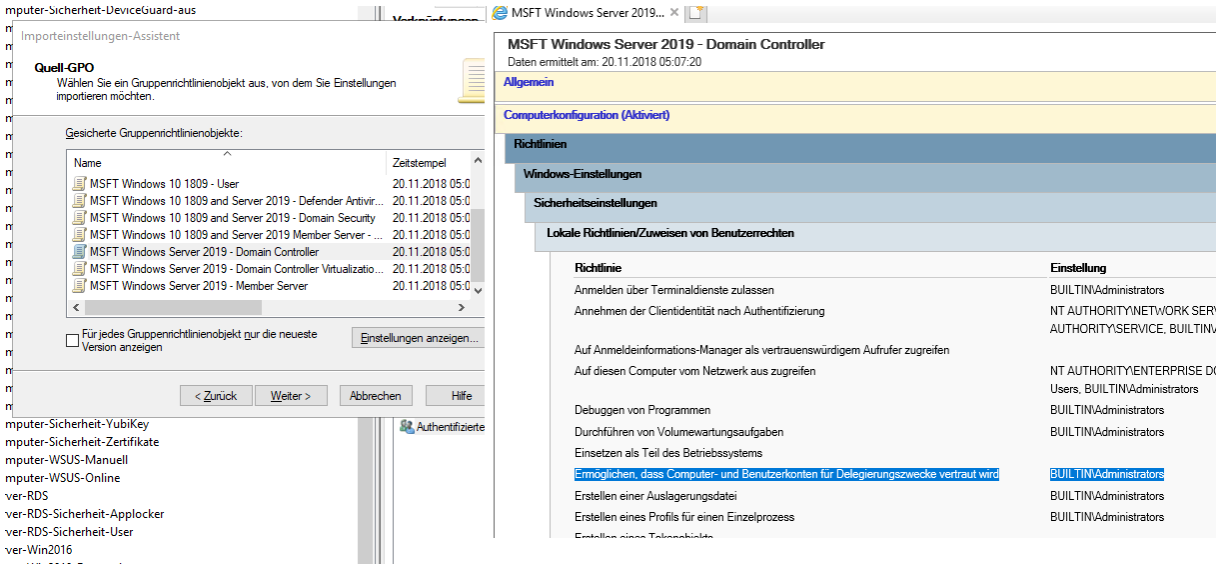
Nachdem die Baselines kopiert sind, erstelle ich eine neue Gruppenrichtlinie – speziell für die 2019er Domain Controller:



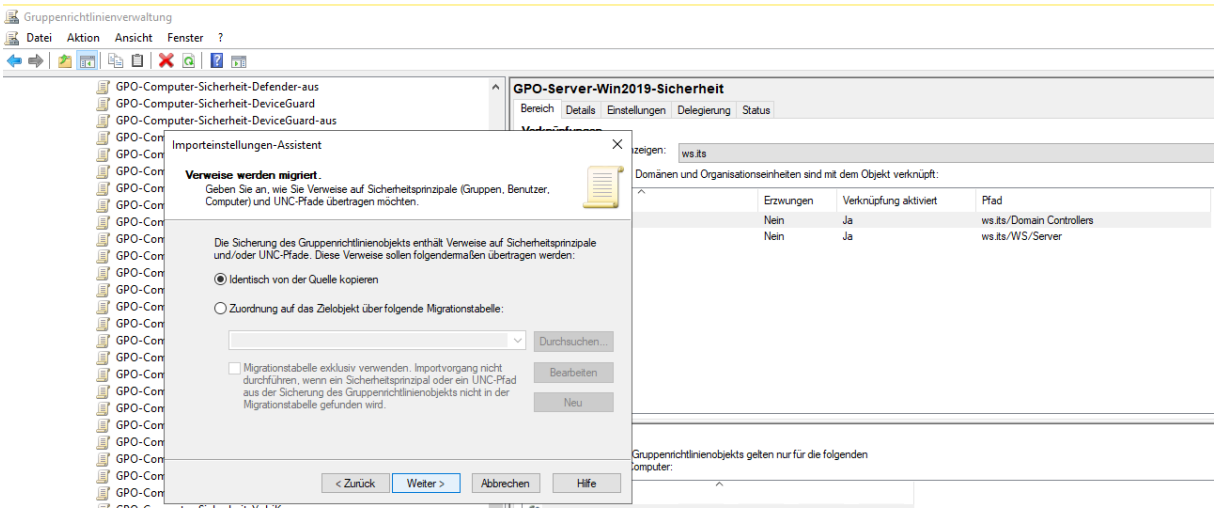
In die leere GPO importiere ich nun die Einstellungen der Baseline:



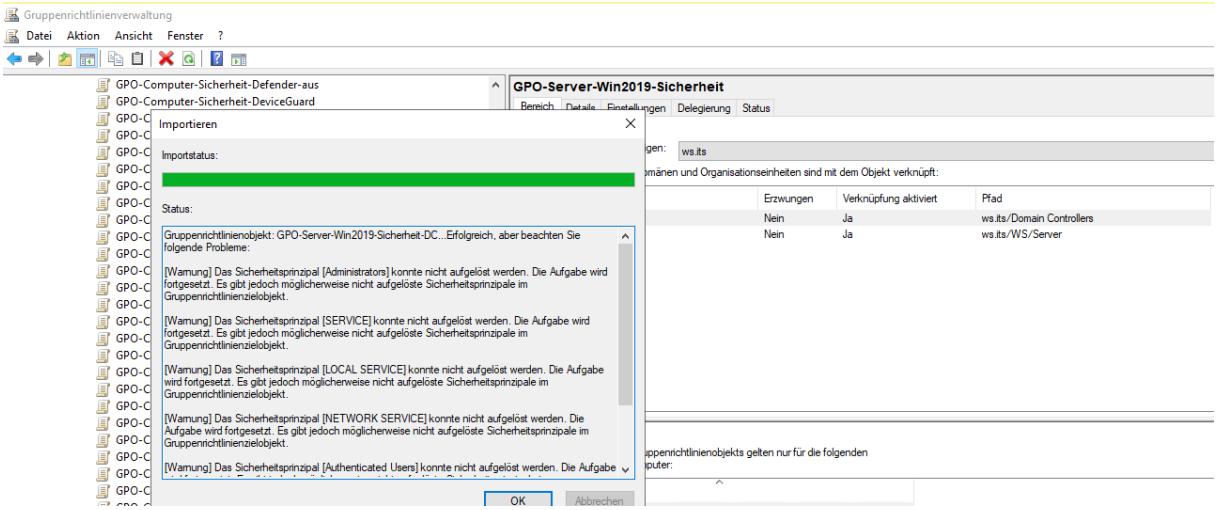
Die Unterordner im Verzeichnis GPOs sind kryptisch benannt. Aber der Import-Assistent kann die Namen sehr gut anzeigen. So finde ich die GPO zum Härten der Domain Controller. Ich schaue mir auch gleich mal den relevanten Teil in den Einstellungen an. Das sieht richtig aus:



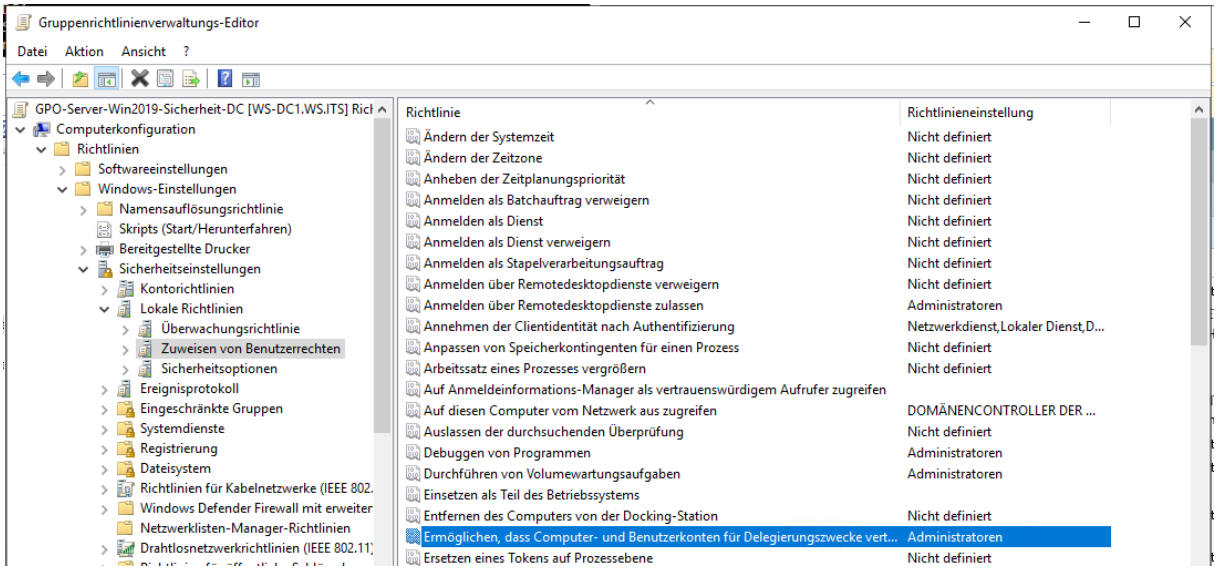
Die Sicherheitsprinzipale übernehme ich 1:1. Meist funktioniert das echt gut:



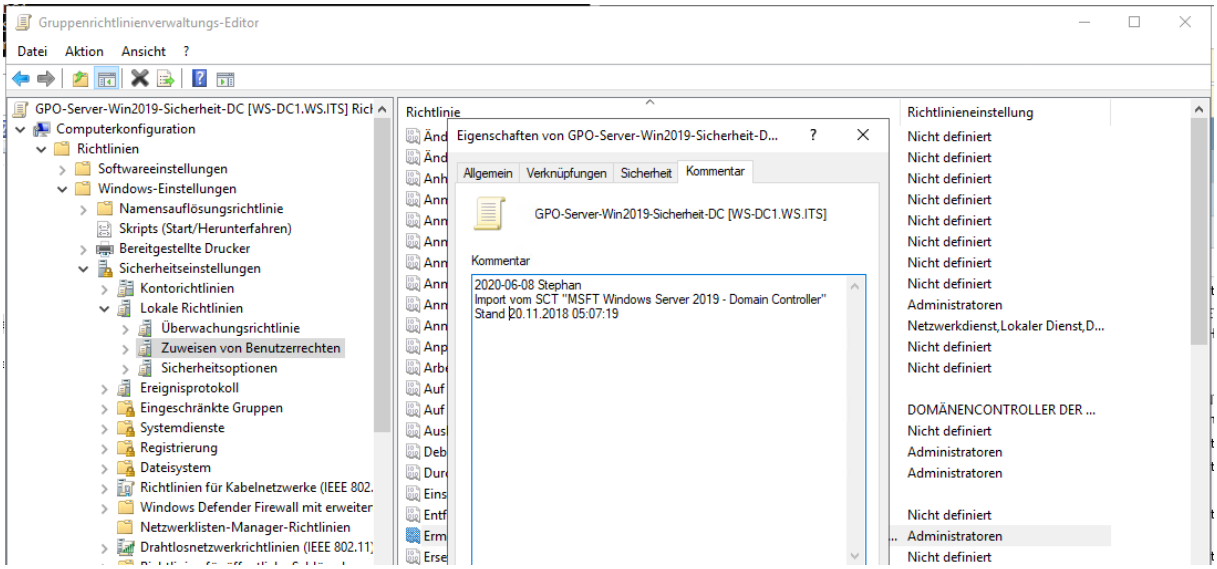
Es kommt beim Abschluss eine Warnmeldung:



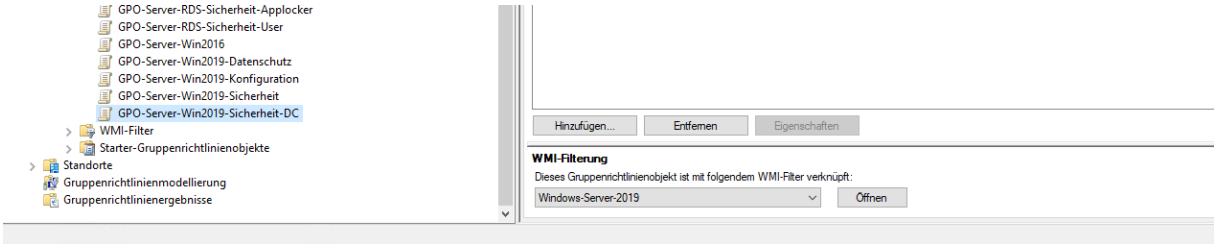
Aber ich kann alle Sicherheitsprinzipale übersetzt wiederfinden:



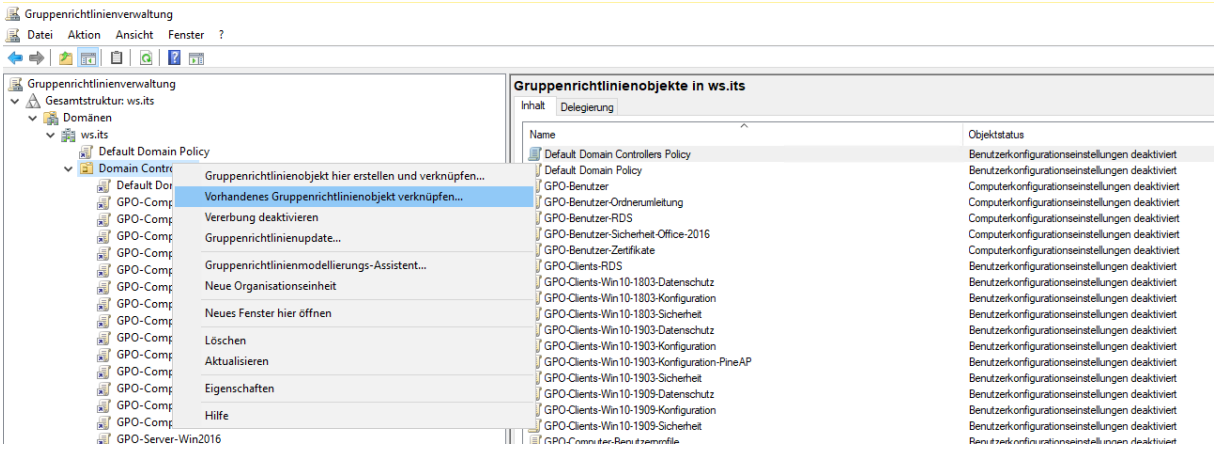
Zur Dokumentation editiere ich den Kommentar der neuen GPO:



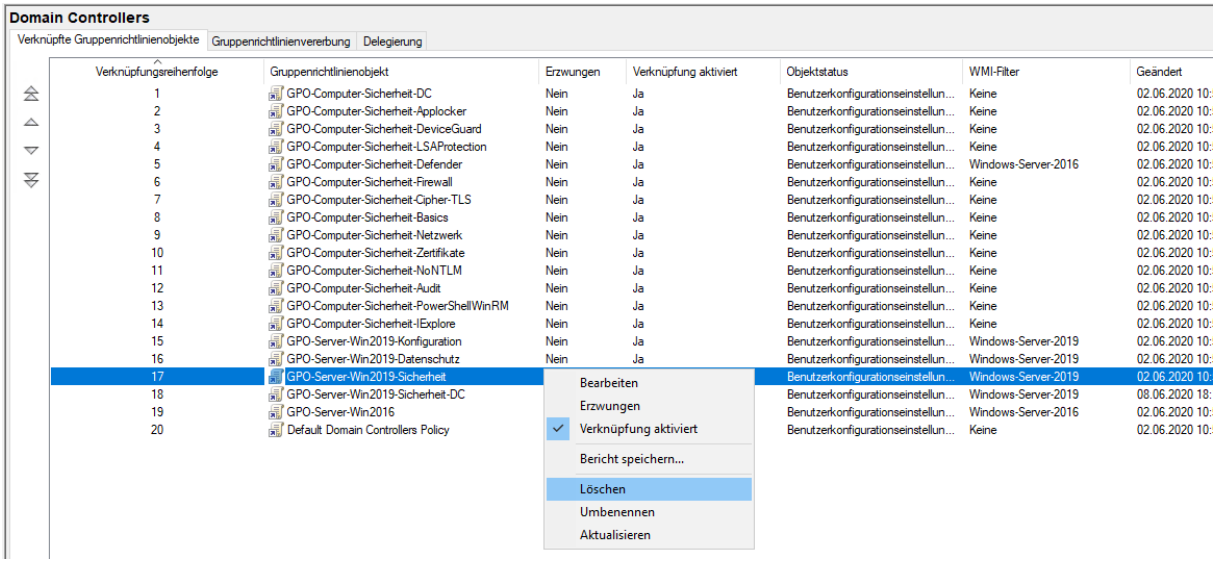
Jetzt platziere ich noch einen WMI-Filter. So wird diese Richtlinie nur von den neuen Domain Controllern verarbeitet:



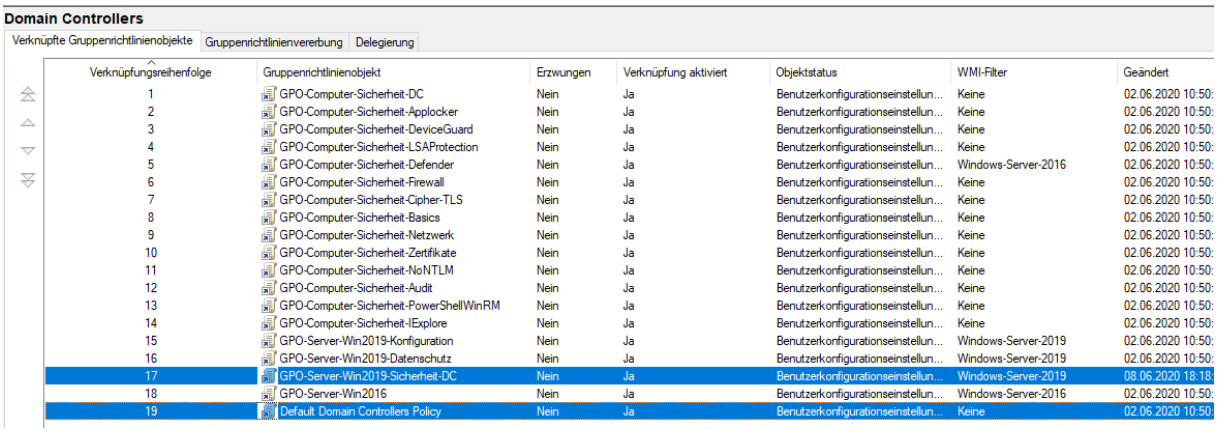
So ausgestattet kann ich die GPO auf die Organisationseinheit der Domain Controller verbinden:



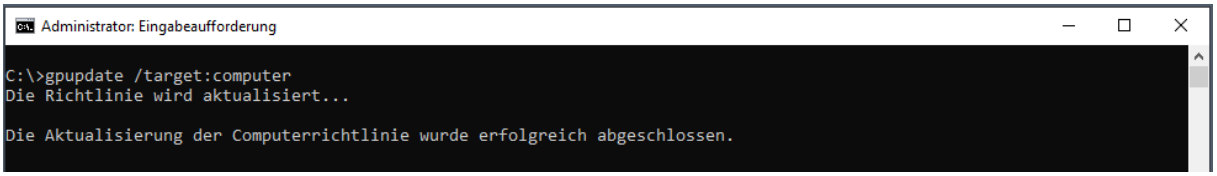
Die Memberserver-GPO ist hier nicht richtig. Daher lösche ich sie raus. Zusätzlich schiebe ich die neue GPO in der Verarbeitung weiter nach oben:



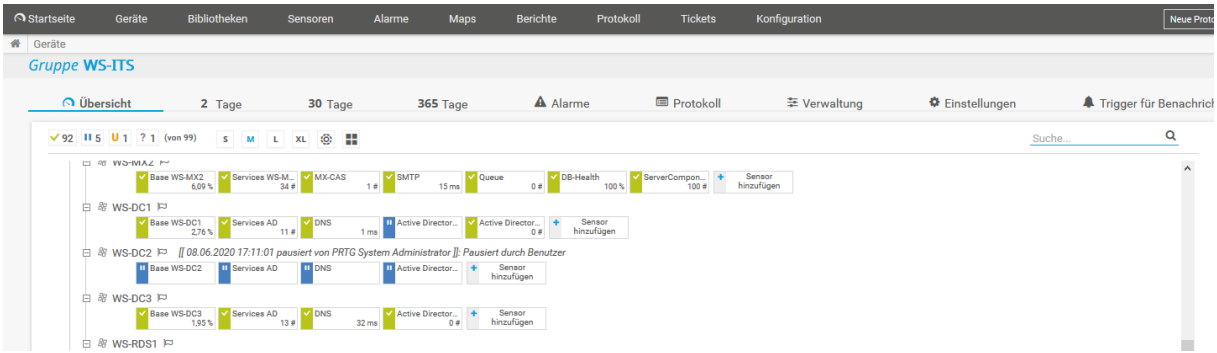
So überlagert die Härtungsrichtlinie die normale Default Domain Controller Policy:



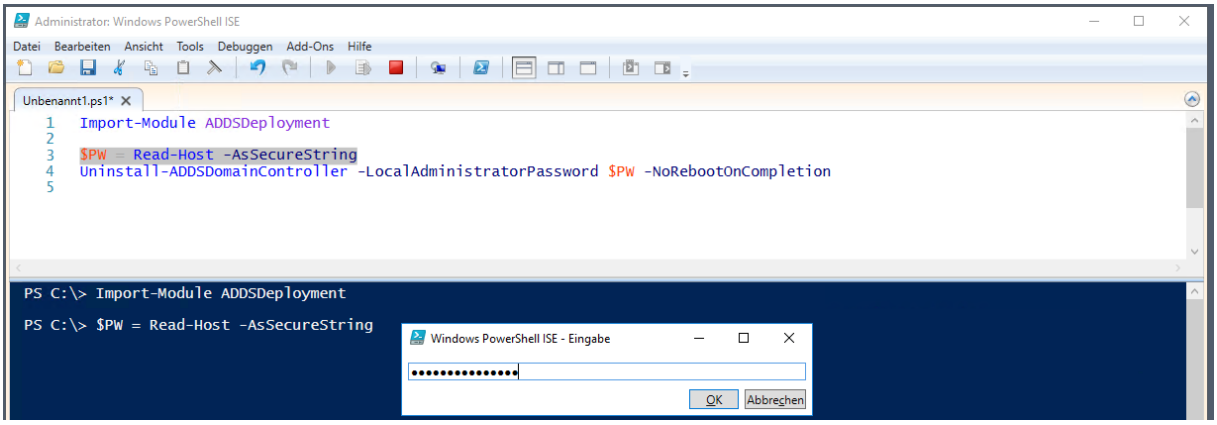
Jetzt aktualisiere ich die Gruppenrichtlinien auf dem WS-DC1, der ja schon mit Windows Server 2019 unterwegs ist:

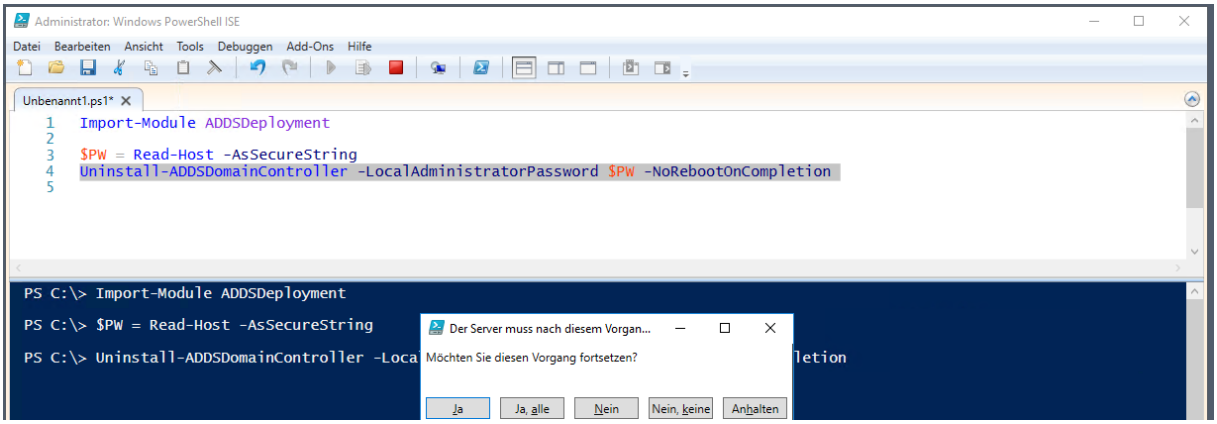


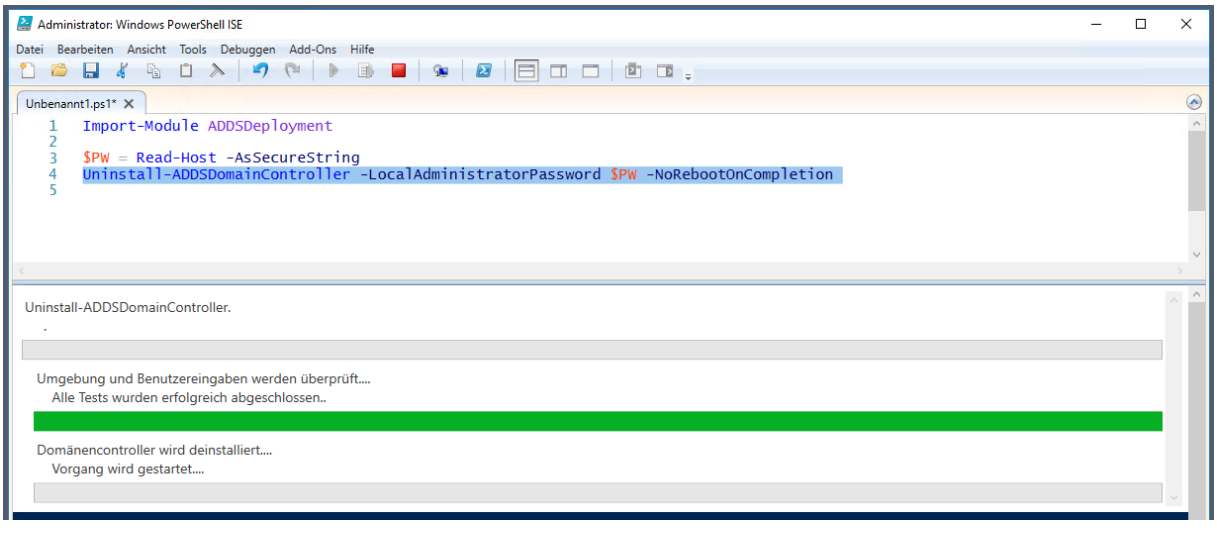
Kurz darauf wird das Monitoring wieder grün:

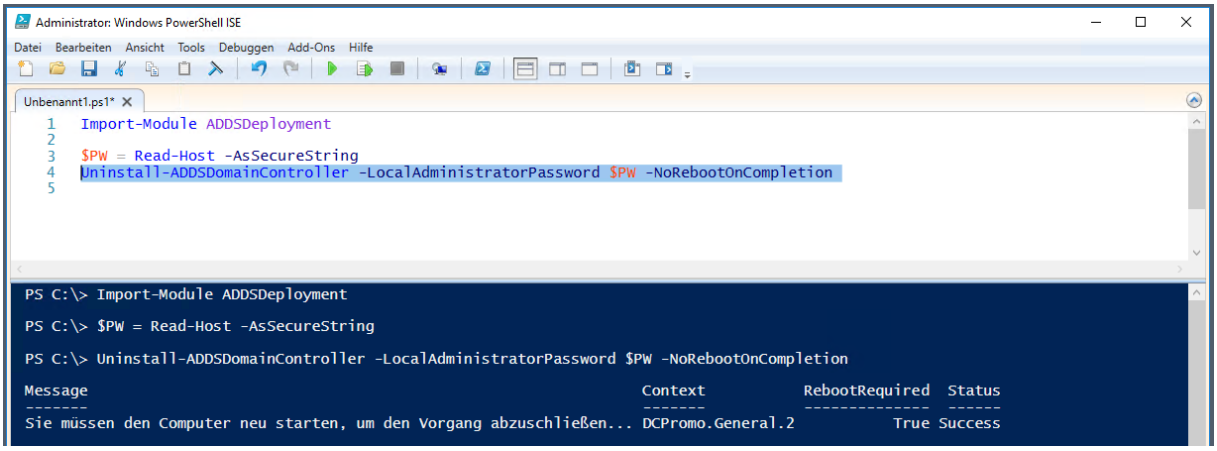


Scheinbar ist es jetzt die richtige Konfiguration. Also starte ich einen weiteren Versuch auf dem alten WS-DC2, um ihn als Domain Controller herunterzustufen. Dieses Mal nehme ich die PowerShell statt dem Server Manager:


Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
Unbenannt1.ps1*
1 Import-Module ADDSDeployment
2
3 $PW = Read-Host -AsSecureString
4 Uninstall-ADDSDomainController -LocalAdministratorPassword $PW -NoRebootOnCompletion
5
PS C:\> Import-Module ADDSDeployment
PS C:\> $PW = Read-Host -AsSecureString
Windows PowerShell ISE - Eingabe
OK
Abbrechen


Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
Unbenannt1.ps1*
1 Import-Module ADDSDeployment
2
3 $PW = Read-Host -AsSecureString
4 Uninstall-ADDSDomainController -LocalAdministratorPassword $PW -NoRebootOnCompletion
5
PS C:\> Import-Module ADDSDeployment
PS C:\> $PW = Read-Host -AsSecureString
PS C:\> Uninstall-ADDSDomainController -Loca
letion
Der Server muss nach diesem Vorgan...
Möchten Sie diesen Vorgang fortsetzen?
Ja
Ja, alle
Nein
Nein, keine
Anhalten

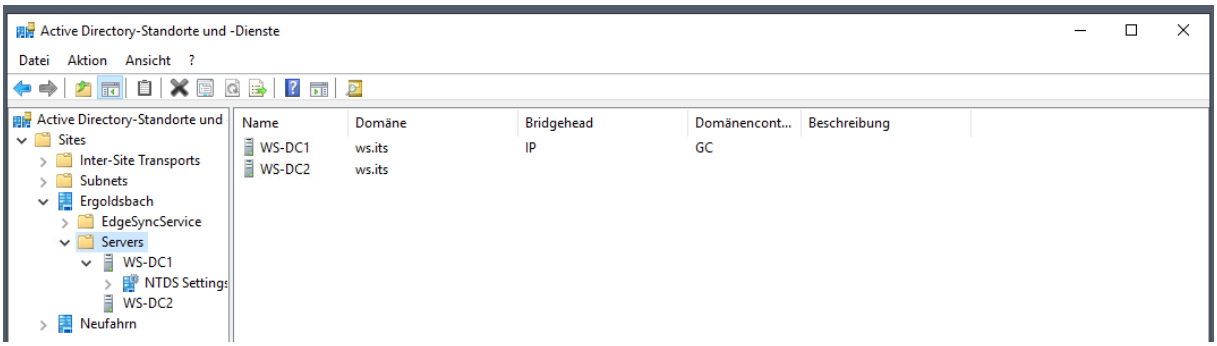

Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
Unbenannt1.ps1*
1 Import-Module ADDSDeployment
2
3 $PW = Read-Host -AsSecureString
4 Uninstall-ADDSDomainController -LocalAdministratorPassword $PW -NoRebootOnCompletion
5
Uninstall-ADDSDomainController.
Umgebung und Benutzereingaben werden überprüft....
Alle Tests wurden erfolgreich abgeschlossen..
Domänencontroller wird deinstalliert....
Vorgang wird gestartet....


Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
Unbenannt1.ps1*
1 Import-Module ADDSDeployment
2
3 $PW = Read-Host -AsSecureString
4 Uninstall-ADDSDomainController -LocalAdministratorPassword $PW -NoRebootOnCompletion
5
PS C:\> Import-Module ADDSDeployment
PS C:\> $PW = Read-Host -AsSecureString
PS C:\> Uninstall-ADDSDomainController -LocalAdministratorPassword $PW -NoRebootOnCompletion
Message Context RebootRequired Status
Sie müssen den Computer neu starten, um den Vorgang abzuschließen... DCPromo.General.2 True Success

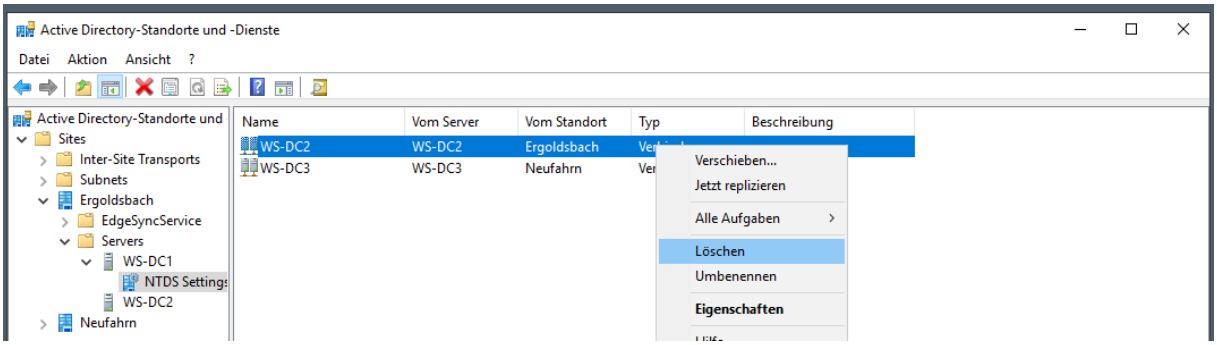
Na also. Auch dieses Problem wäre behoben. Zum Abschluss starte ich den Server neu.

Nacharbeiten im Active Directory

In der Management-Konsole „Active Directory Standorte und Dienste“ ist nur ein leerer Container vom WS-DC2 über geblieben:

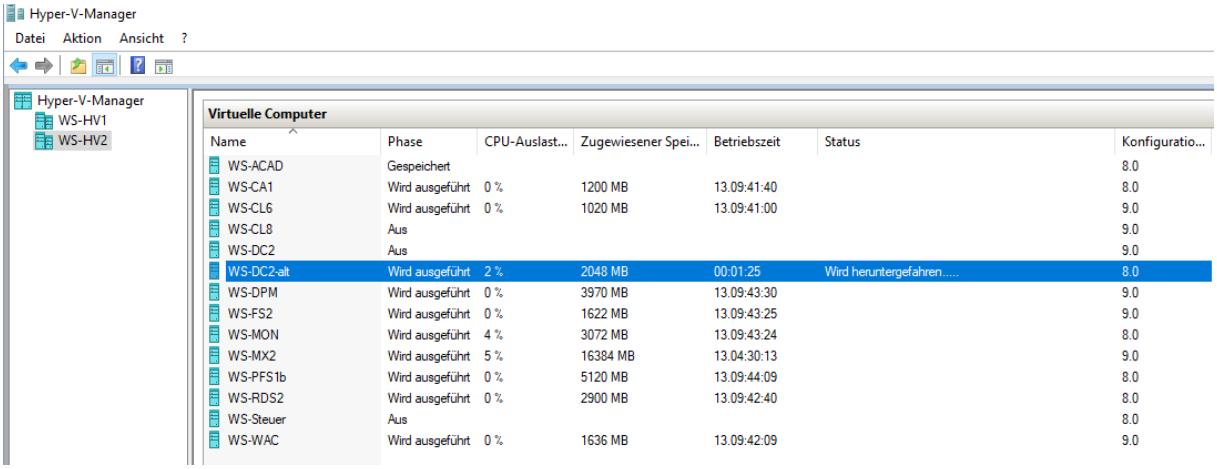


Und eine statische Replikationsverbindung. Die lösche ich manuell:

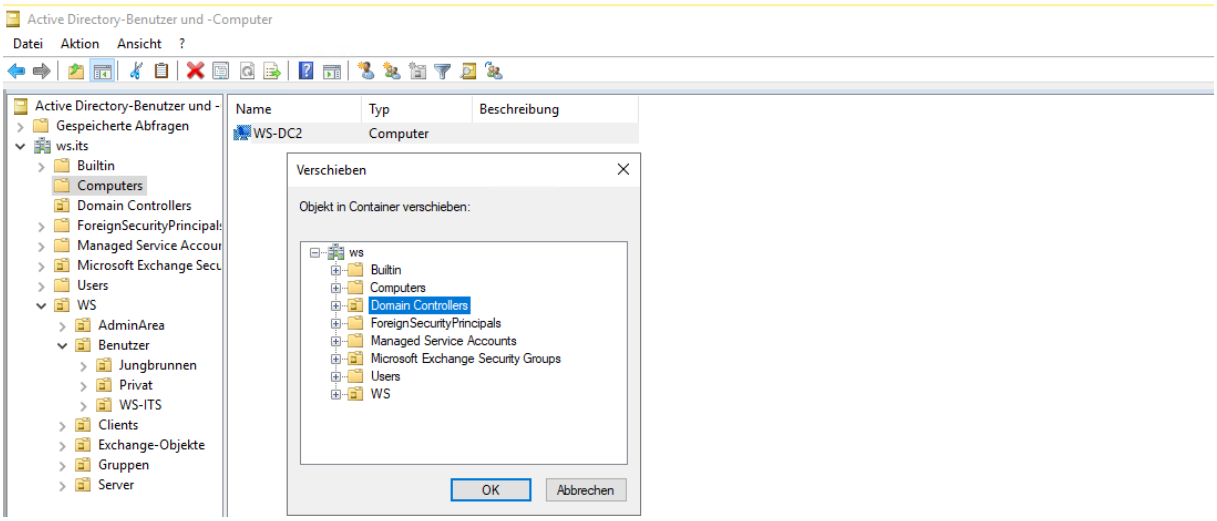


Entfernen des Servers

Weiter geht es mit dem Austausch. Ich fahre den alten Server im Hyper-V herunter. Der ist aktuell noch Mitglied im Active Directory, aber nur noch als Memberserver:



Danach verschiebe ich das AD-Computerkonto zurück in die OU „Domain Controllers“:

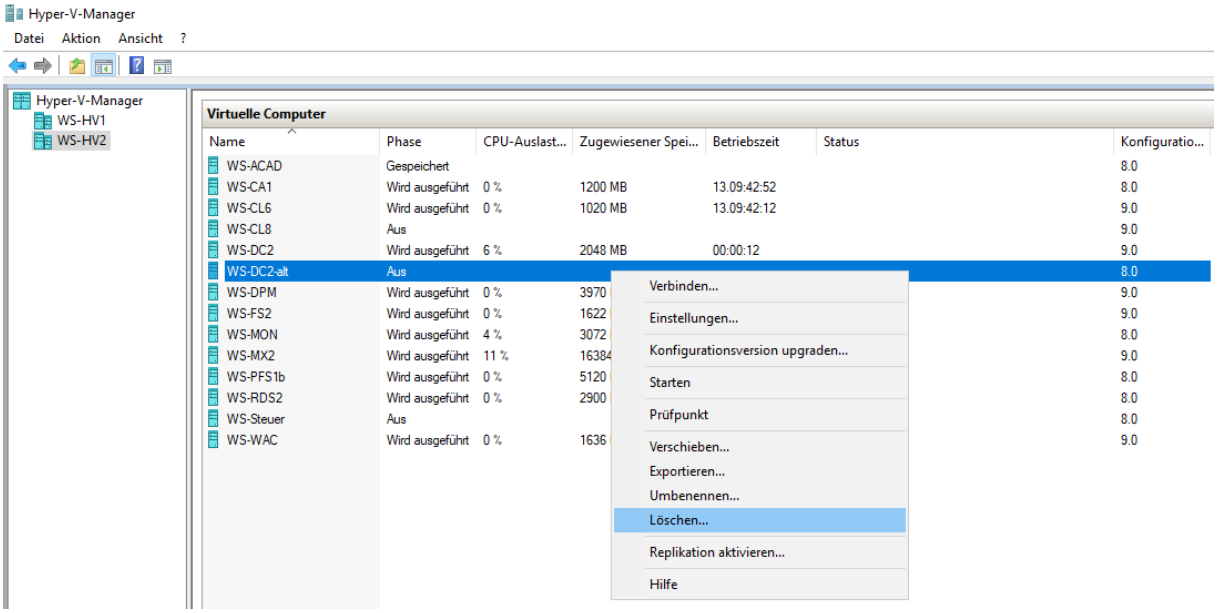


So kann der neue WS-DC2 ab dem ersten Moment im Active Directory gleich die richtigen Gruppenrichtlinien ziehen.

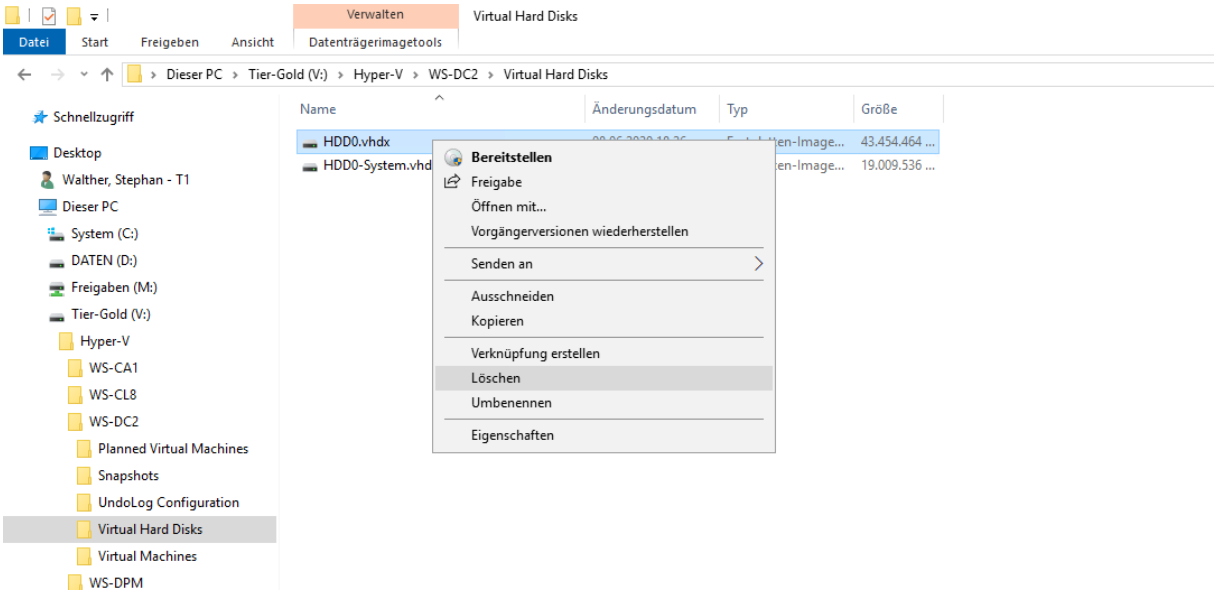
Bereitstellung des neuen Servers

Austausch der VM

Die alte virtuelle Maschine lösche ich im Hyper-V:



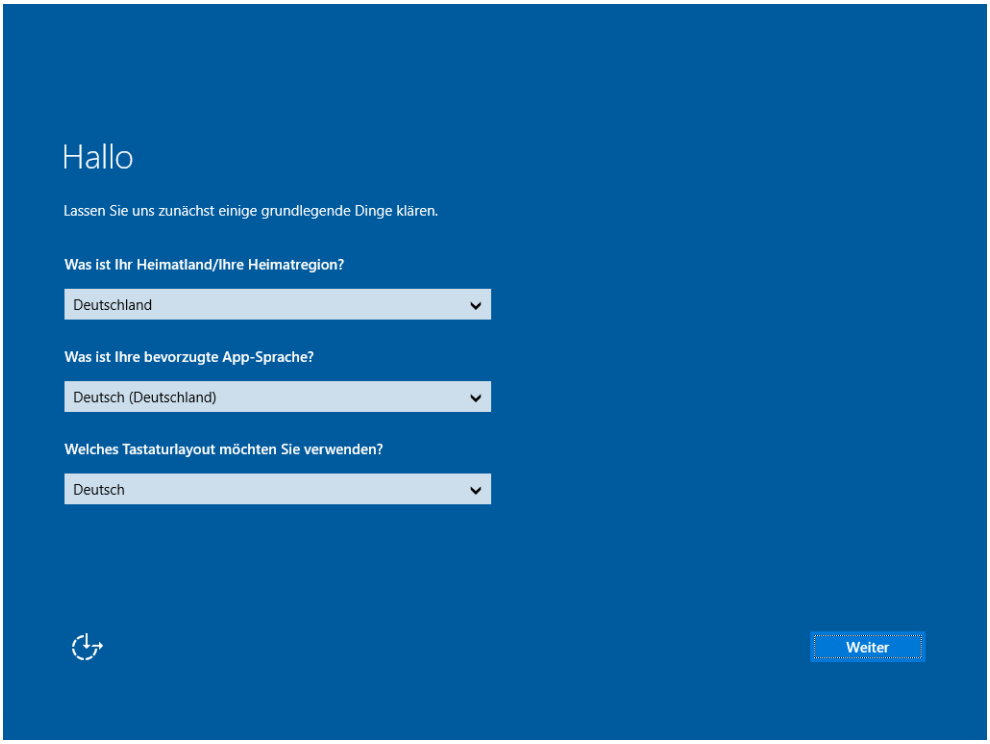
Dabei verbleibt nur die alte Festplattendatei im Speicher. Auch die wird entfernt:

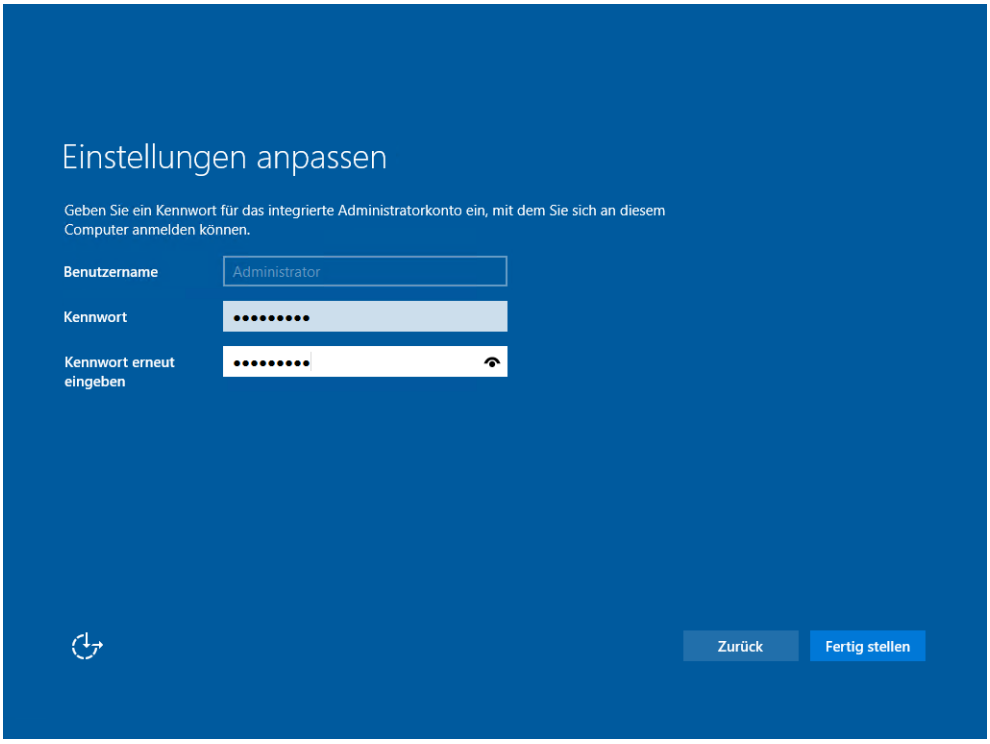


Damit ist der alte Server entfernt.

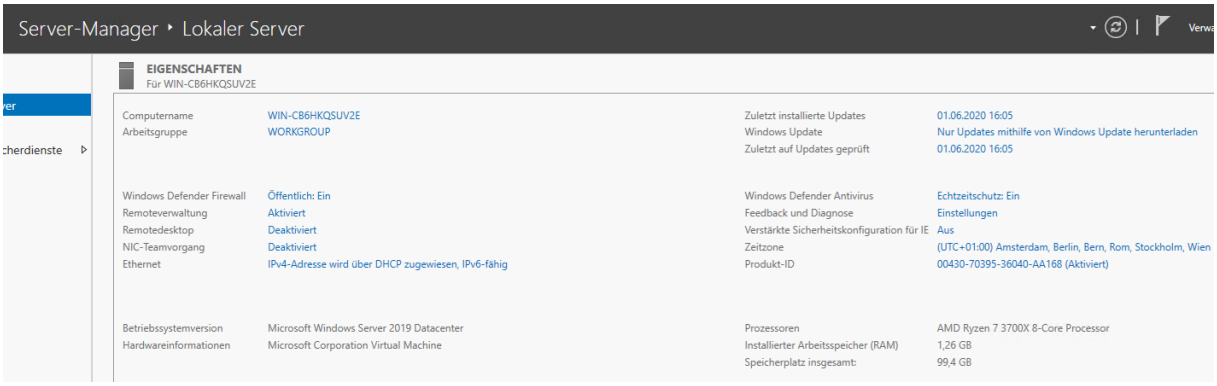
Betriebssystemvorbereitung

Jetzt schalte ich die neue VM ein und verbinde mich mit der Konsole. Der Server führt eine Hardwareerkennung aus und startet den Ersteinrichtungsassistenten:

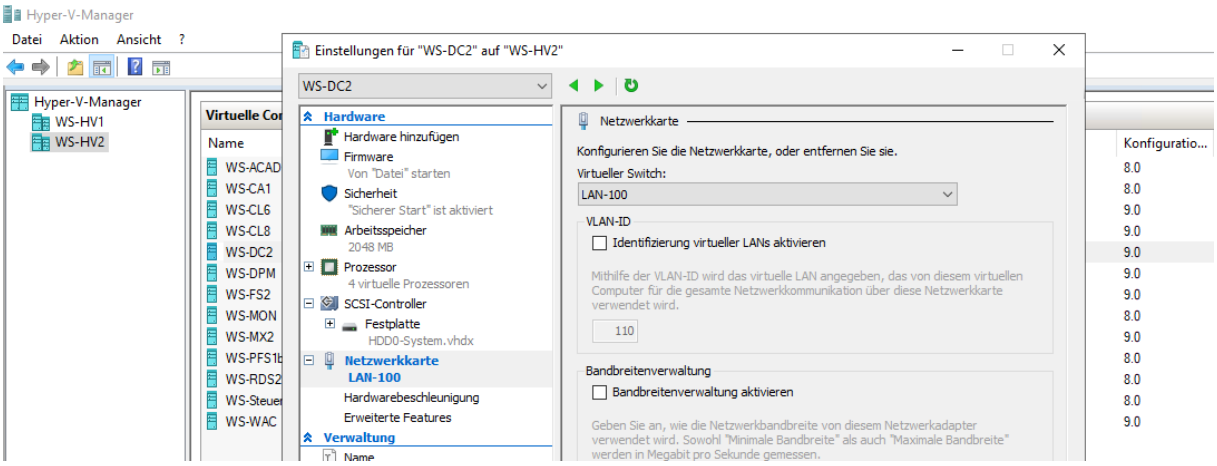




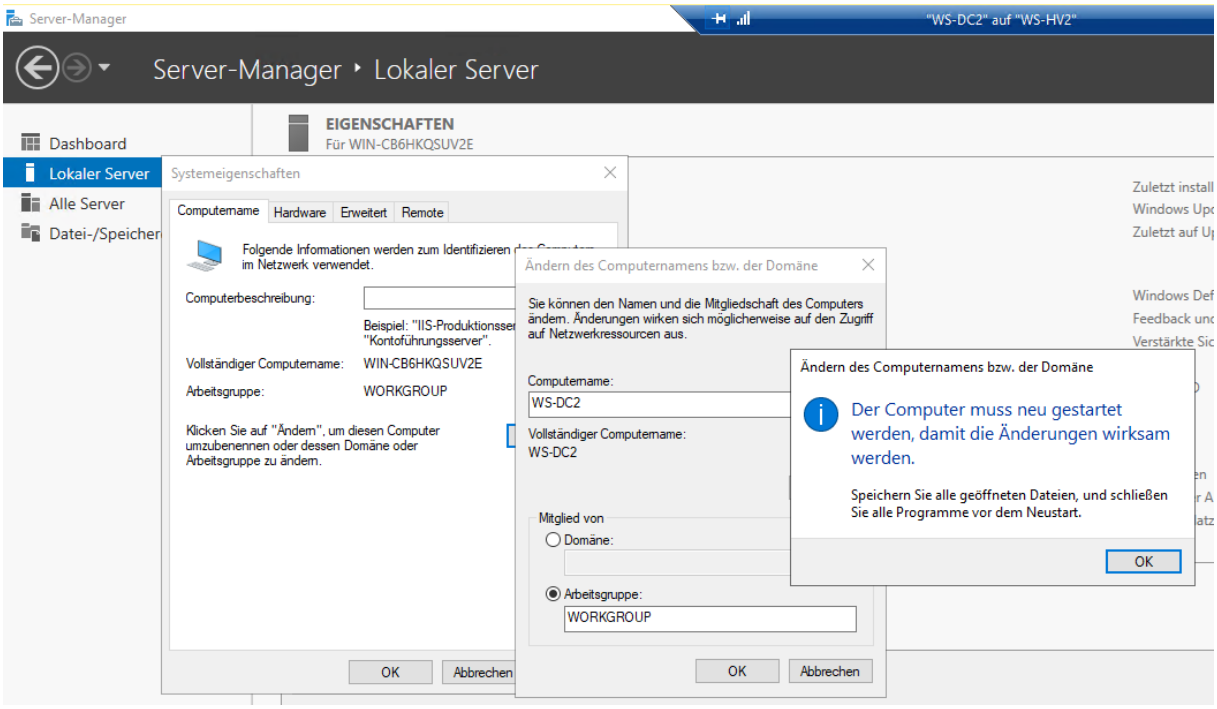
Nach wenigen Minuten bin ich auf dem Server lokal angemeldet. Da ich bei der Ersteinrichtung auch den Produkt-Key eingegeben habe und der Server aktuell im Client-Netzwerk gepatcht ist, hat er sich automatisch aktiviert. Das kann man im Server Manager erkennen:



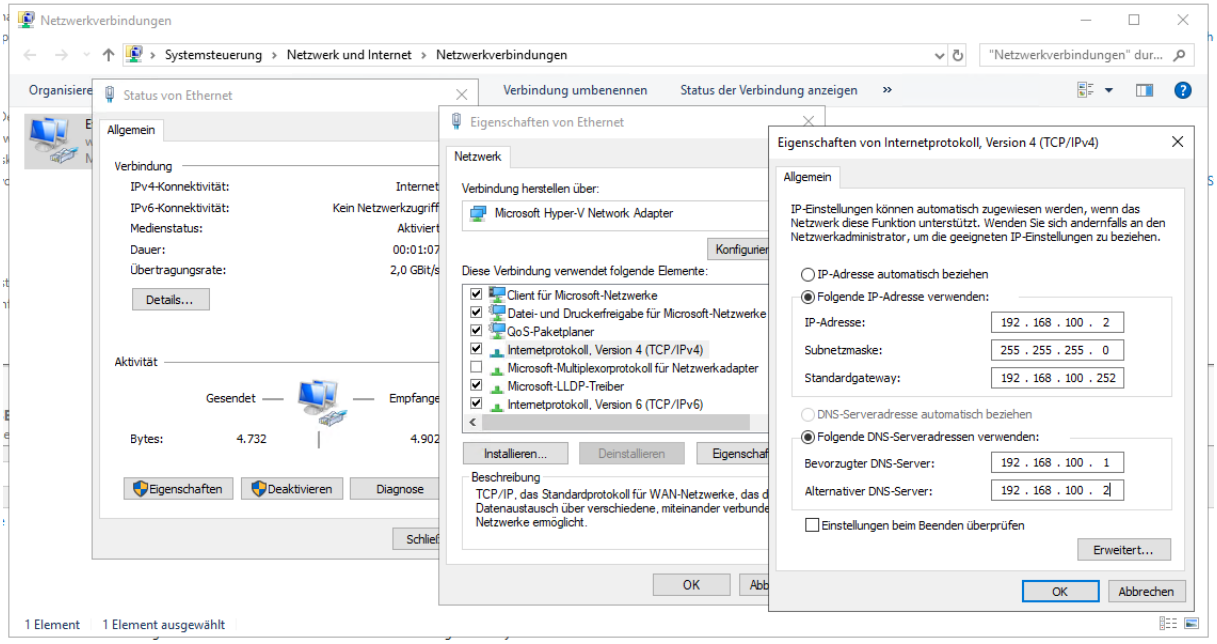
Mehr Internet-Zeit möchte ich nicht zugestehen. Daher patche ich die VM in mein Server-Netz LAN-100:



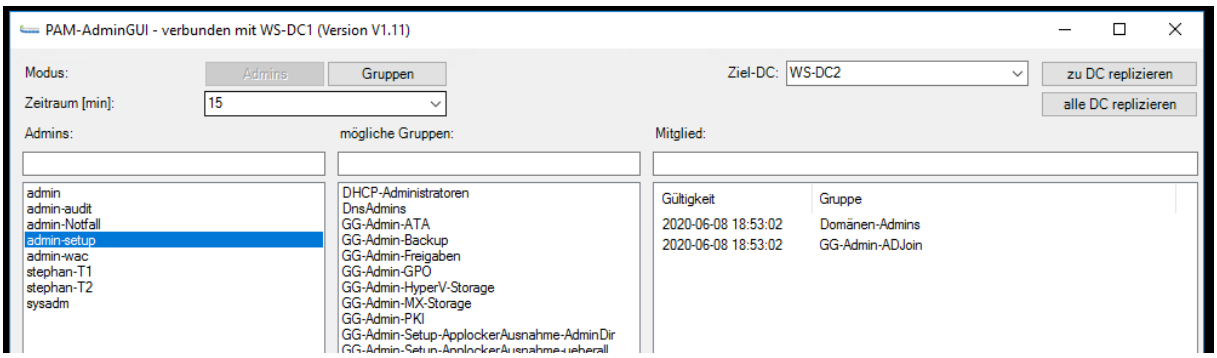
Der Server bekommt den alten Namen WS-DC2. Danach ist ein Neustart erforderlich:



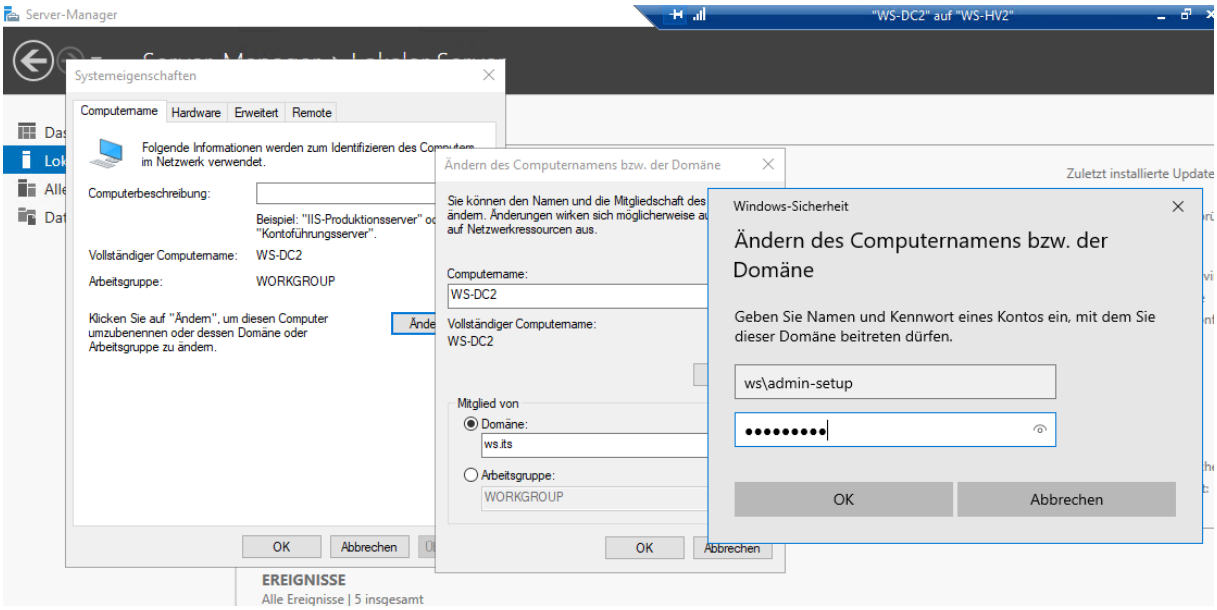
Nach der Anmeldung editiere ich die IP-Konfiguration. Hier trage ich die alte IP-Adresse ein:



Für den Domain Join brauche ich einen Admin-Account, der temporär Mitglied in diesen 2 Gruppen ist. 15 Minuten sollten locker ausreichen:

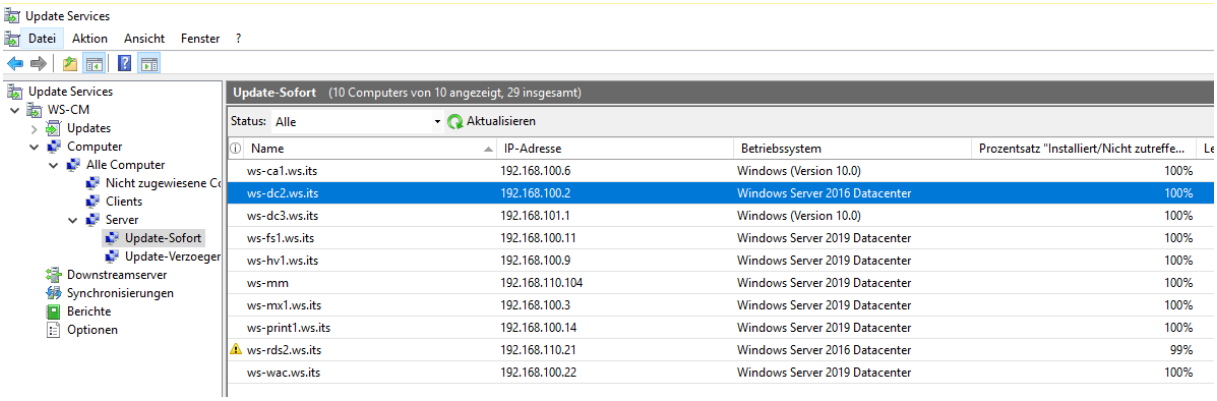


Jetzt nehme ich den Server in mein Active Directory auf:

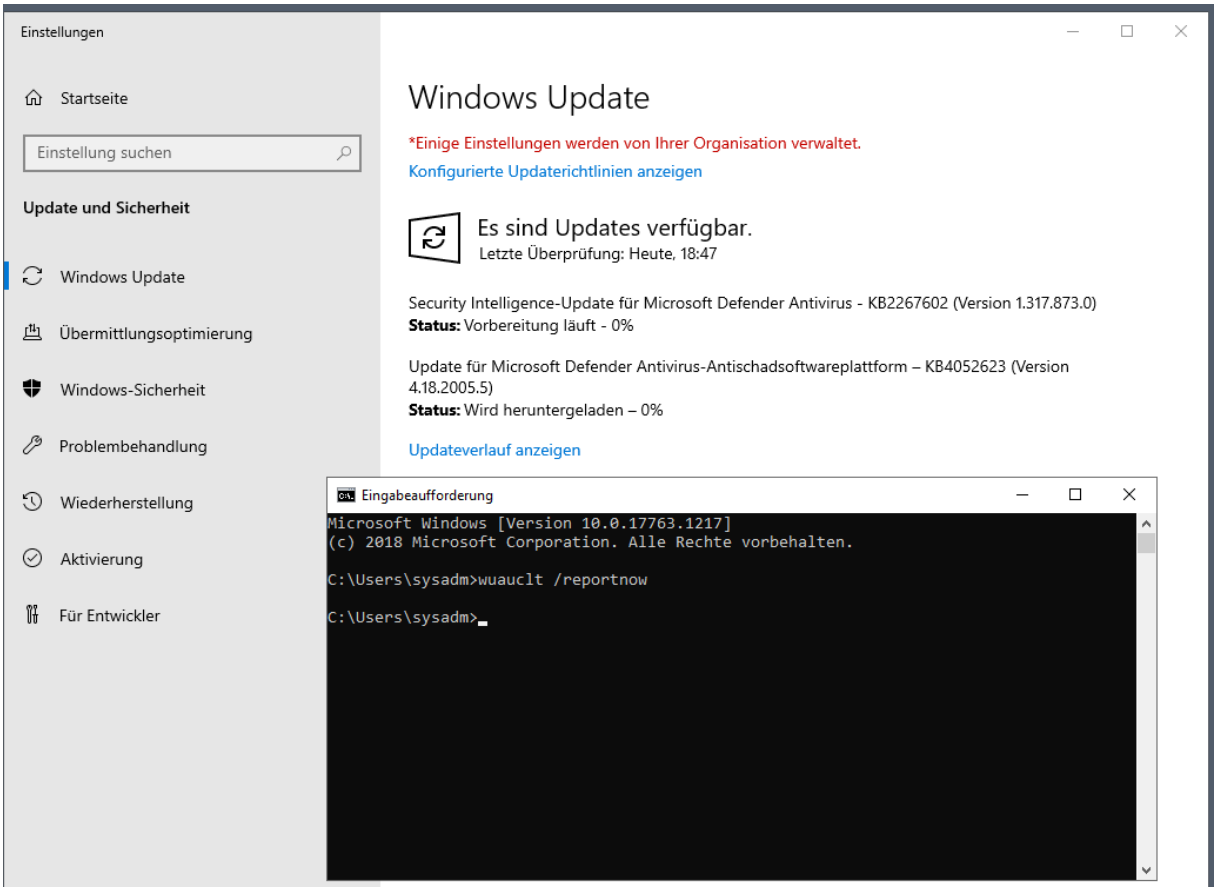


Auch hier wird ein Neustart fällig. Der neue WS-DC2 hat dabei das Computerkonto des alten Servers übernommen.

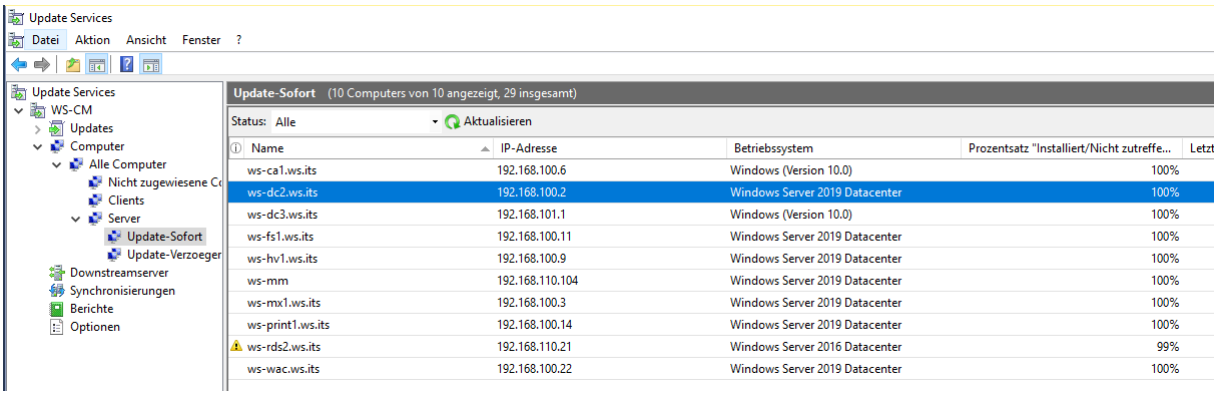
Zur Betriebssystemkonfiguration gehört auch die Aktualisierung des Windows Servers. Da ich das Installations-Image aber erst vor wenigen Tagen aktualisiert habe, sollte hier nicht viel fehlen. In meiner WSUS-Konsole wird noch der alte Server angezeigt:



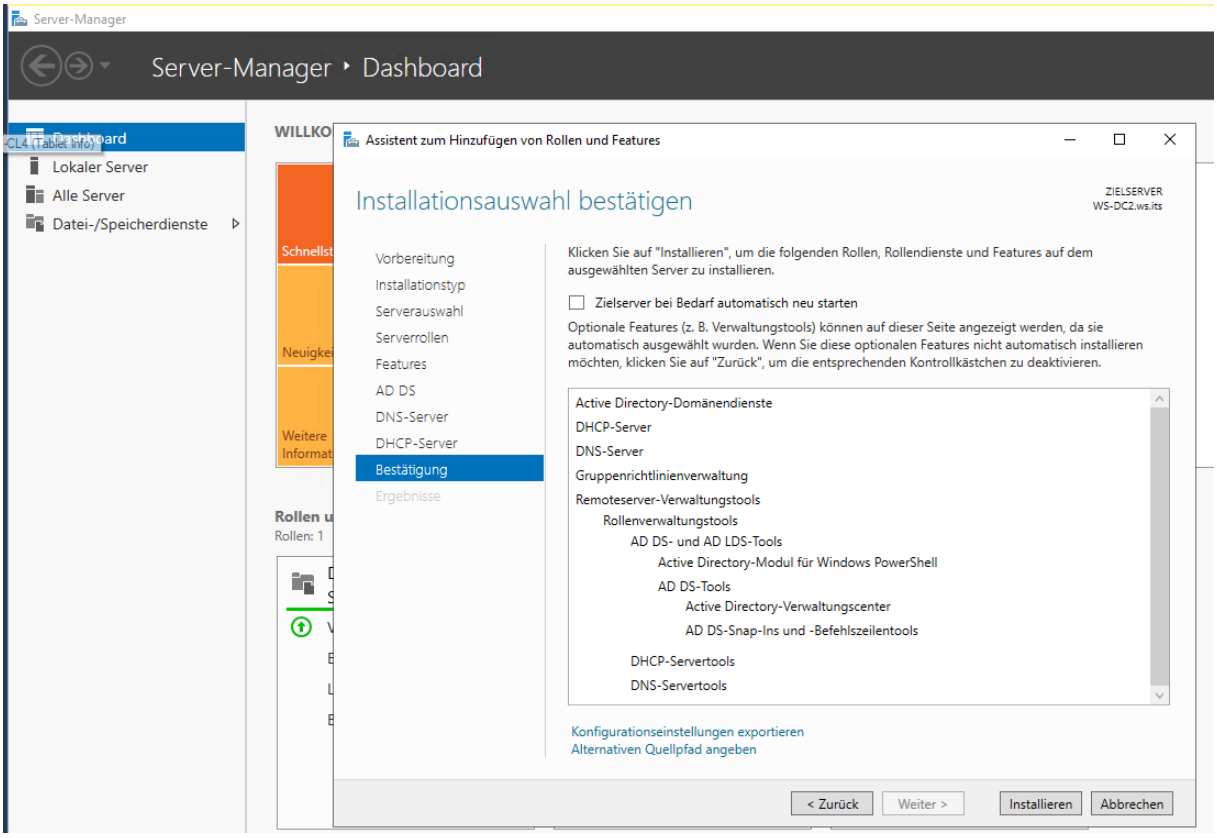
Jetzt suche ich nach Updates. Dabei lenkt eine Gruppenrichtlinie den Server auf meinen WSUS. Mit wuauclt /reportnow berichtet der Server sein Ergebnis direkt an den WSUS:



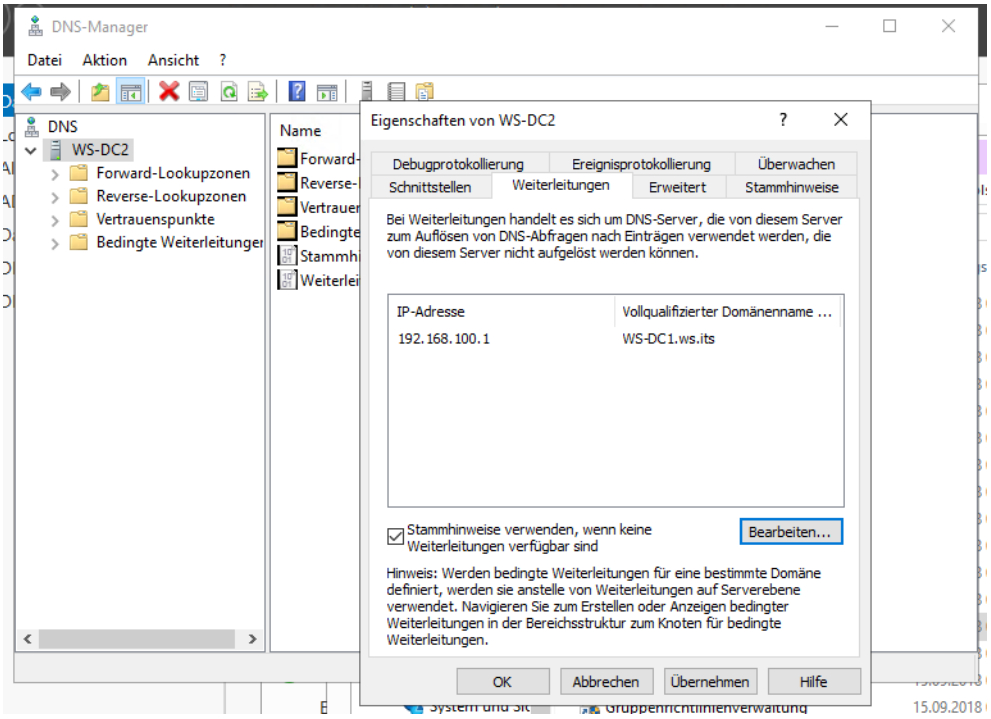
Und dieser aktualisiert den Eintrag:



Der Server ist nun grundsätzlich einsatzbereit. Daher installiere ich jetzt die Rollen und Features:

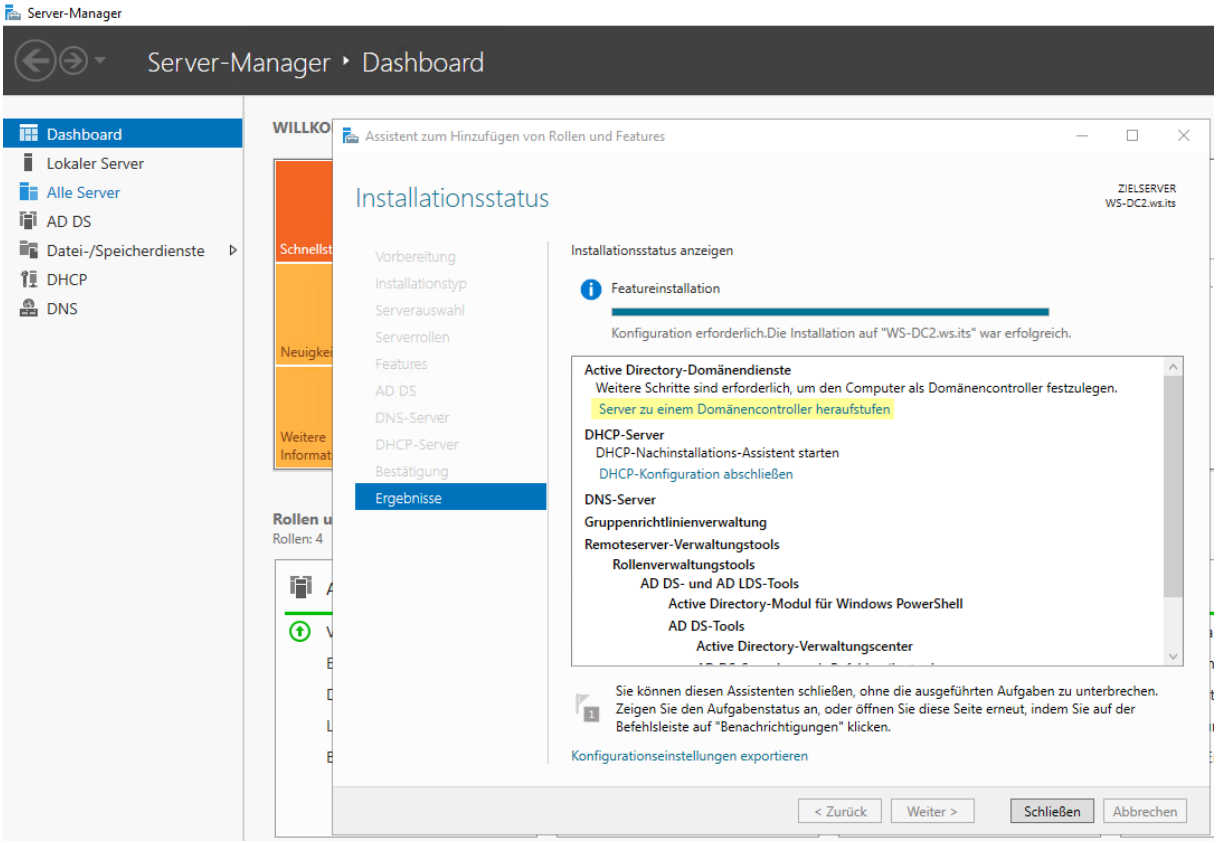


Zum Ende des Server Manager Vorgangs kann ich bereits auf die DNS-Konsole zugreifen. Hier editiere ich schnell den Forwarder auf den fertigen WS-DC1. So vermeide ich wieder die DNS-Probleme wegen den fehlenden Zonen:

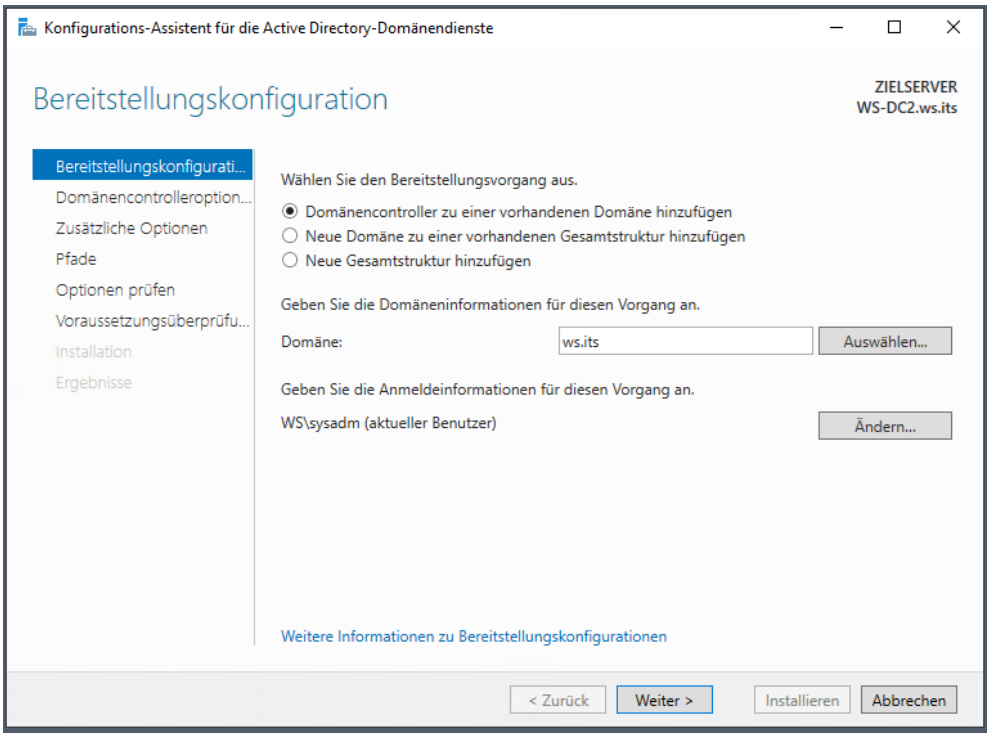


Installation der Rolle Active Directory

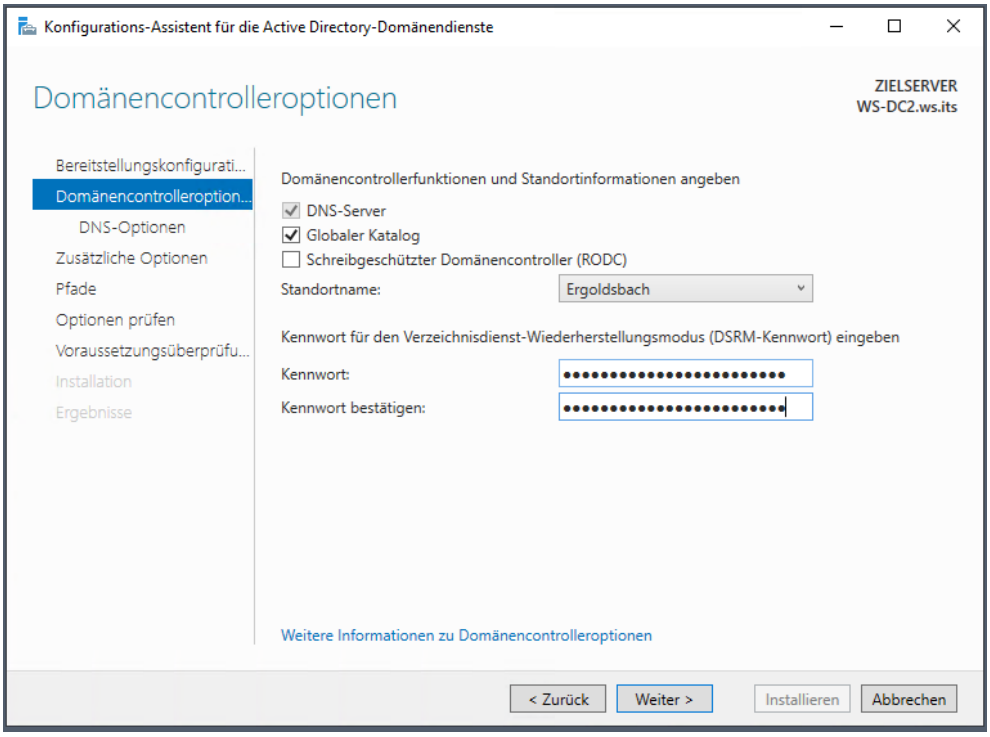
Der Server Manager hat die Rollen- und Feature-Installation abgeschlossen. Nun will er den Domain Controller heraufgestuft wissen. Ich starte den Assistenten direkt aus dem Abschlussfenster:



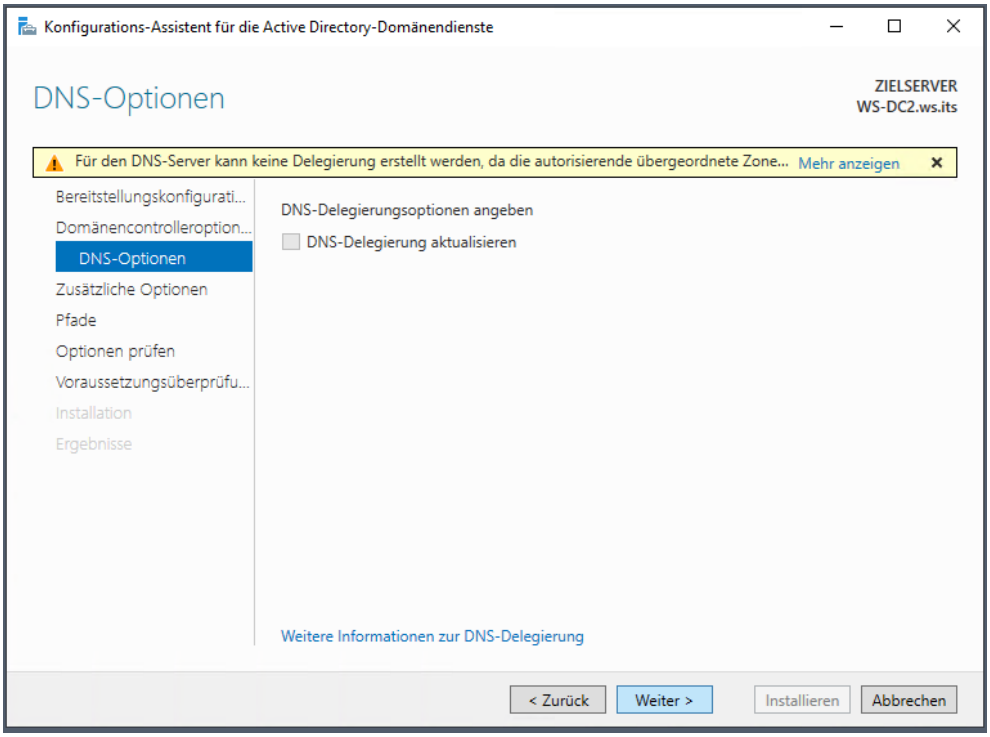
Der neue Server wird ein weiterer Domain Controller meiner Domäne:



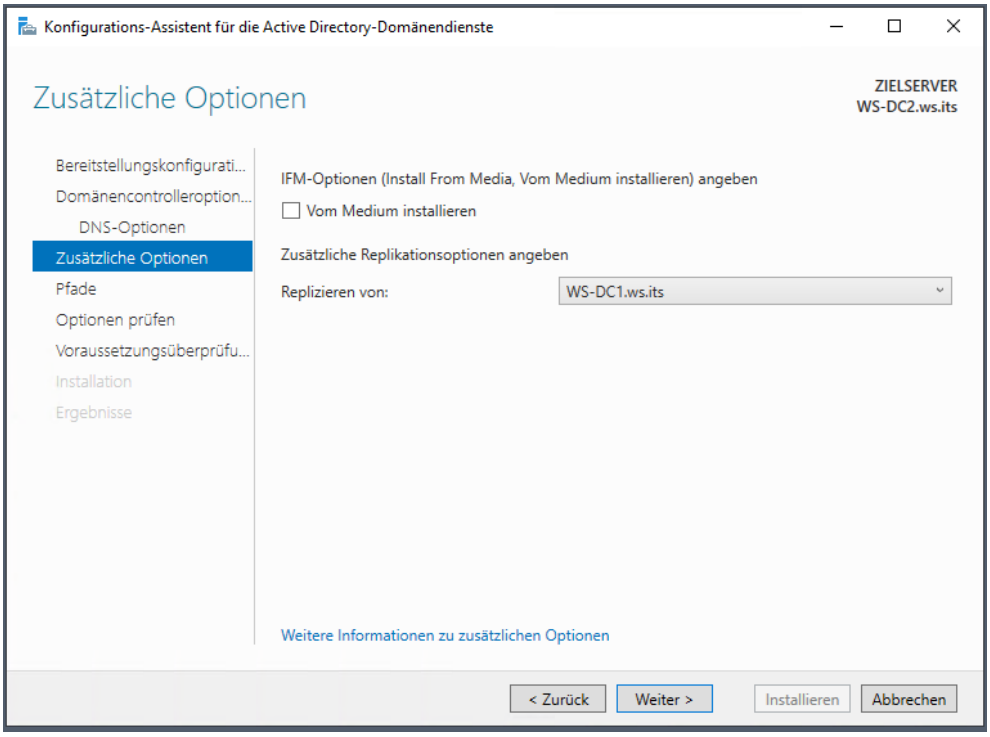
Die anderen Optionen erklären sich praktisch auch von allein. Ich definiere alle Domain Controller als globale Katalogserver. Die Belastung ist gering, dafür ist der Service aber verfügbarer. Und wenn alle DCs einer Gesamtstruktur als GC konfiguriert sind, dann spart man sich die FSMO Infrastruktur-Master. Vom RODC halte ich nichts mehr, daher lasse ich die Option weg. Das Wiederherstellungspasswort speichere ich wieder im Passwort-Safe:



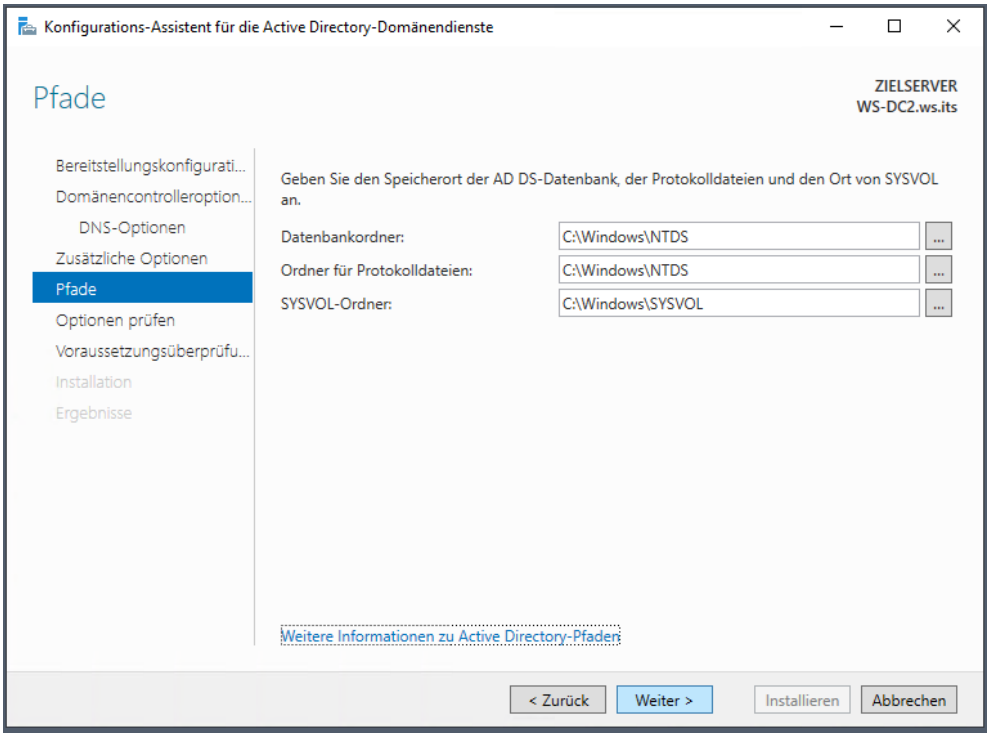
Eine DNS-Delegation ist nicht möglich, da es die übergeordnete Zone its. für meine Zone ws.its. nicht gibt:



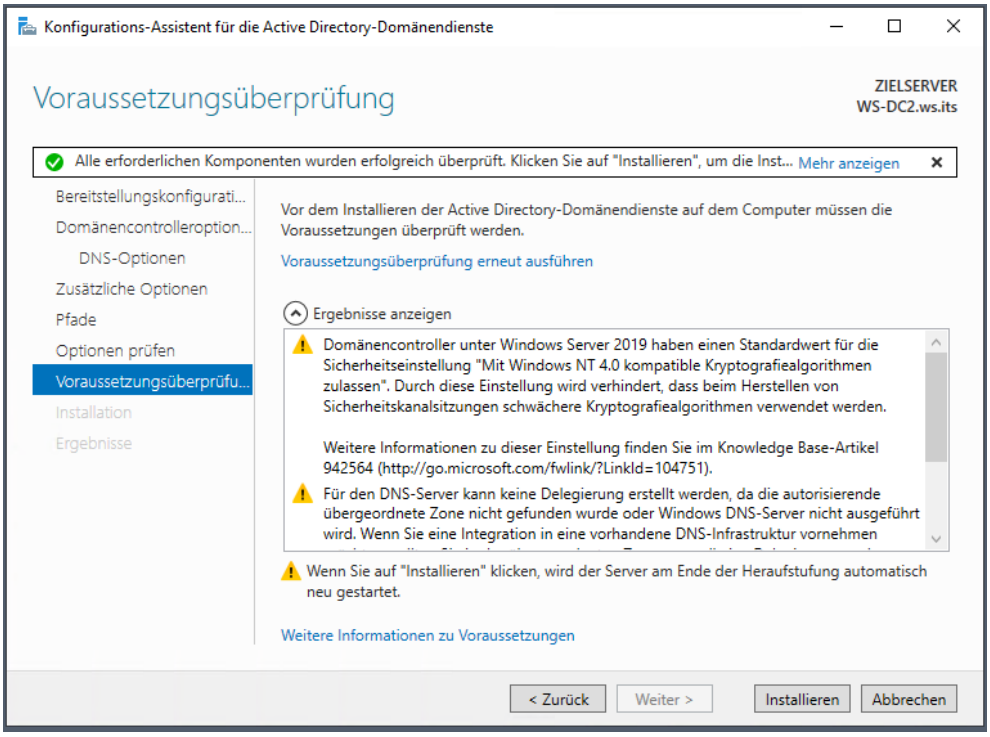
Die Erstreplikation soll sich der neue WS-DC2 vom WS-DC1 holen:



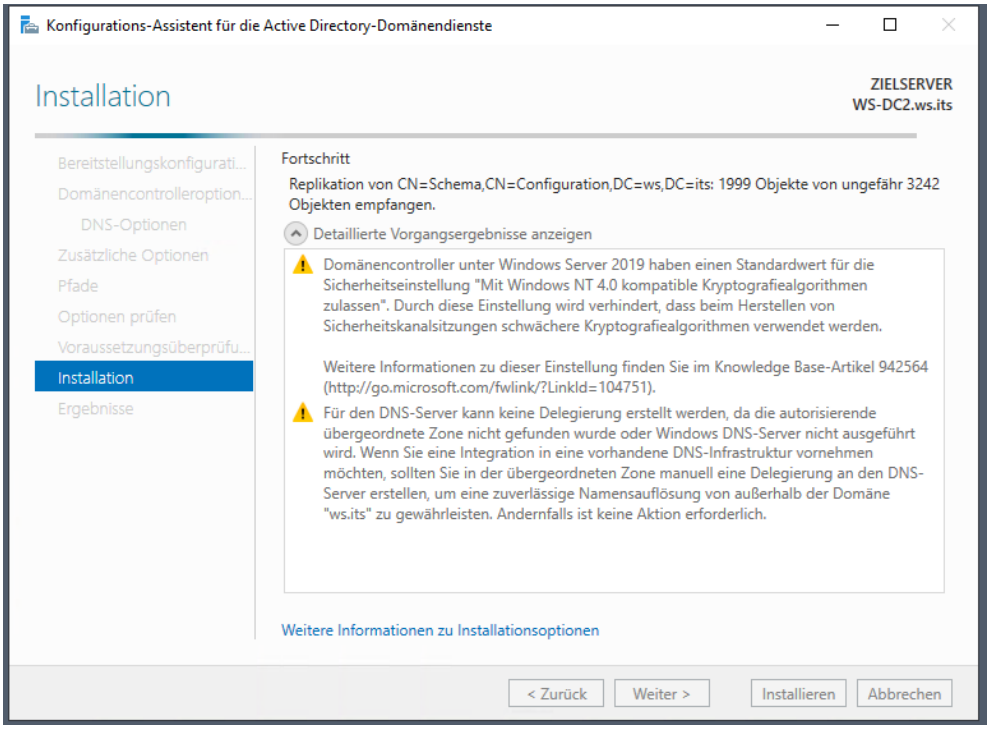
Die Pfade belasse ich beim Standard:



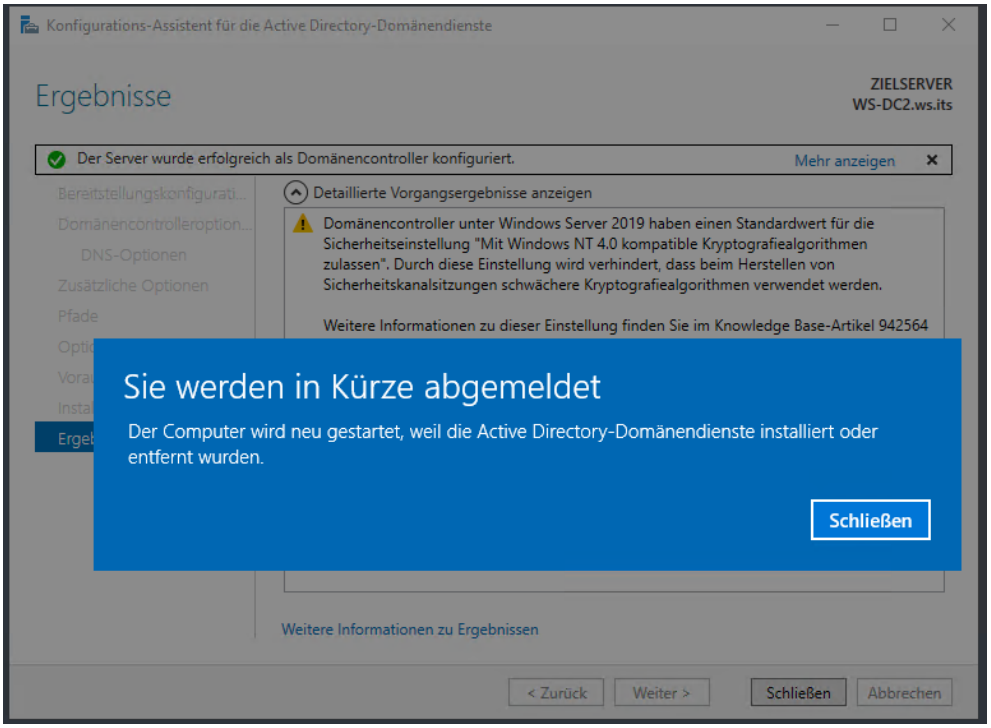
Die Vorprüfung zeigt keine Fehler:



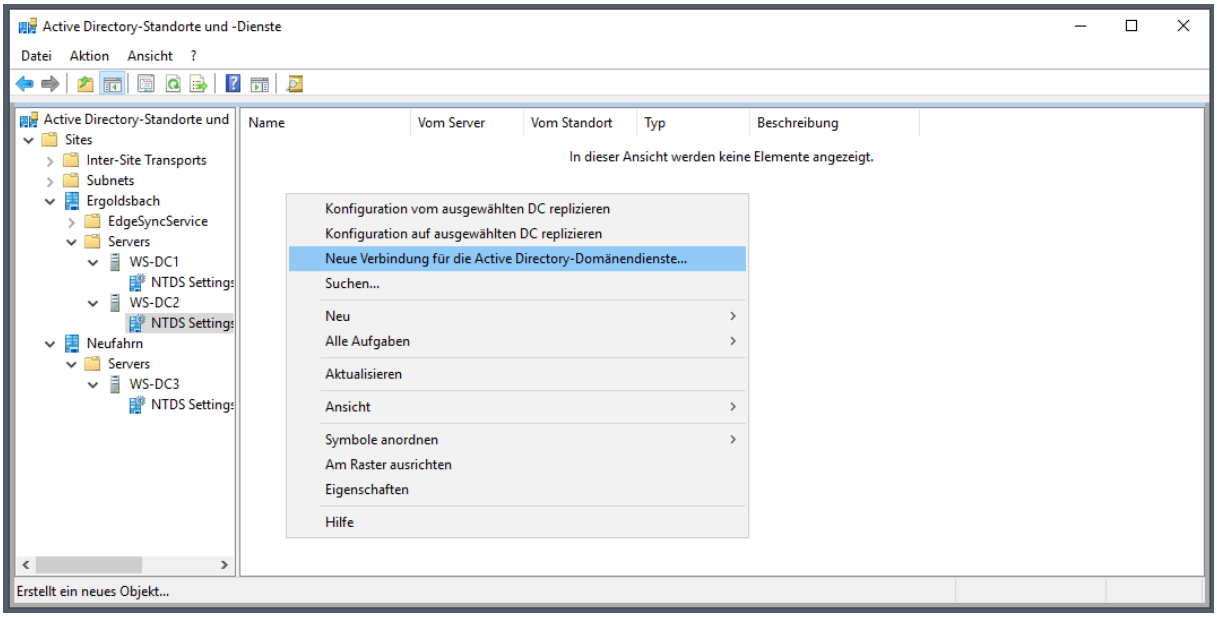
Also kann es losgehen. Der Server richtet sich als Domain Controller ein:

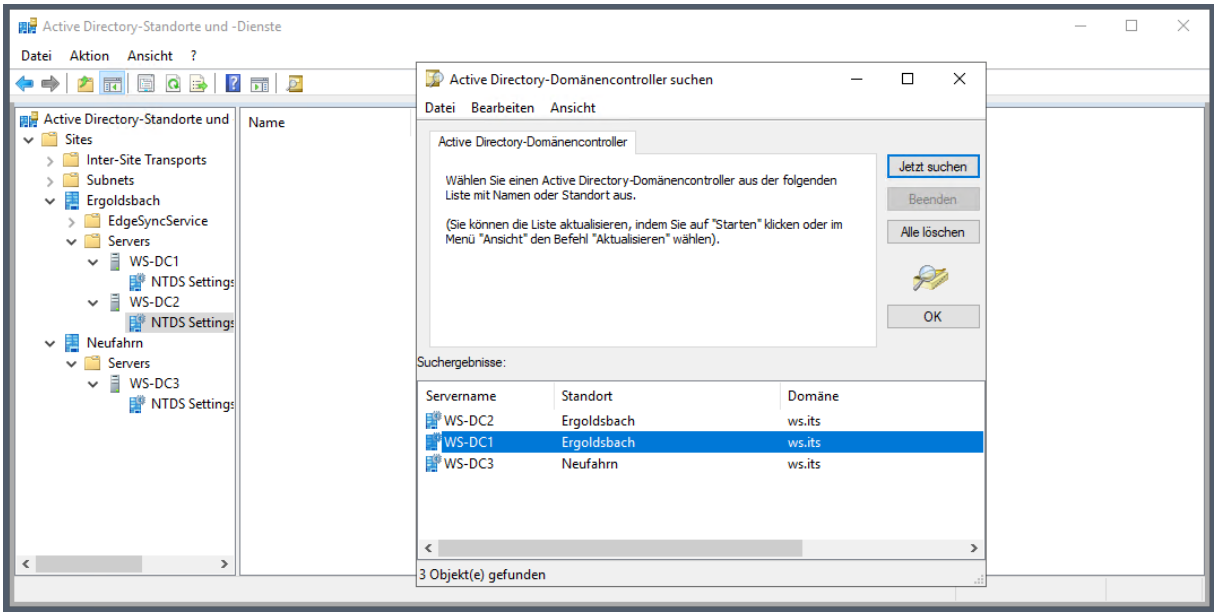


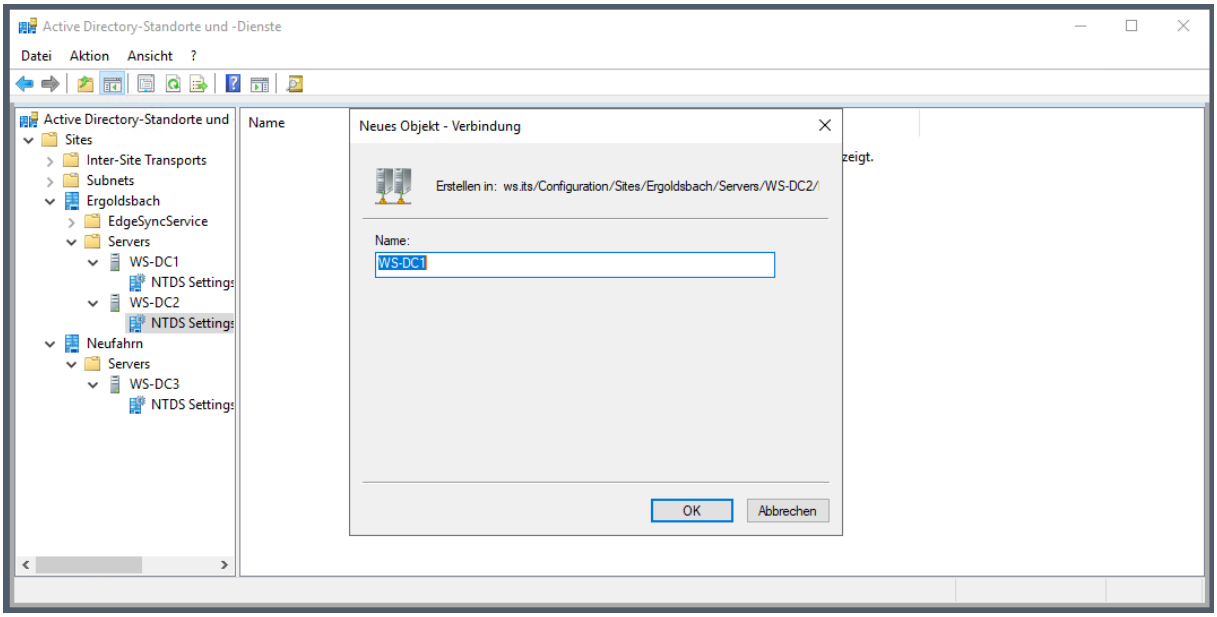
Der Prozess wird wieder mit einem Neustart abgeschlossen:



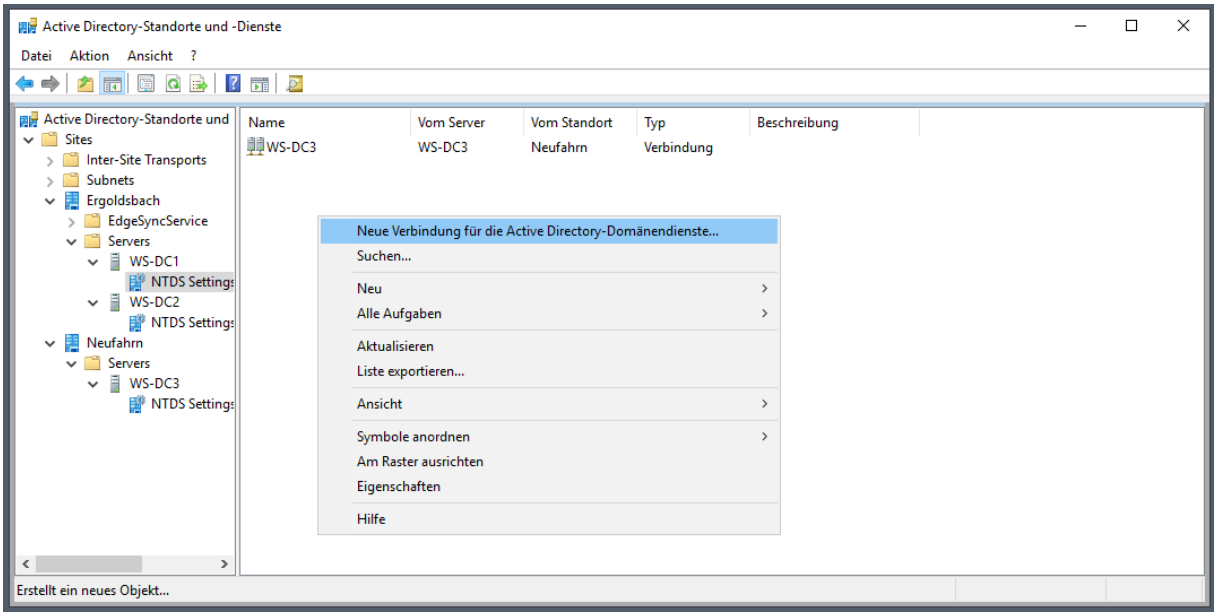
Auf dem anderen Domain Controller trage ich meine Wunsch-Konfiguration für die AD-Replikation ein. Dazu erstelle ich eine manuelle Verbindung zwischen WS-DC2 und WS-DC1:

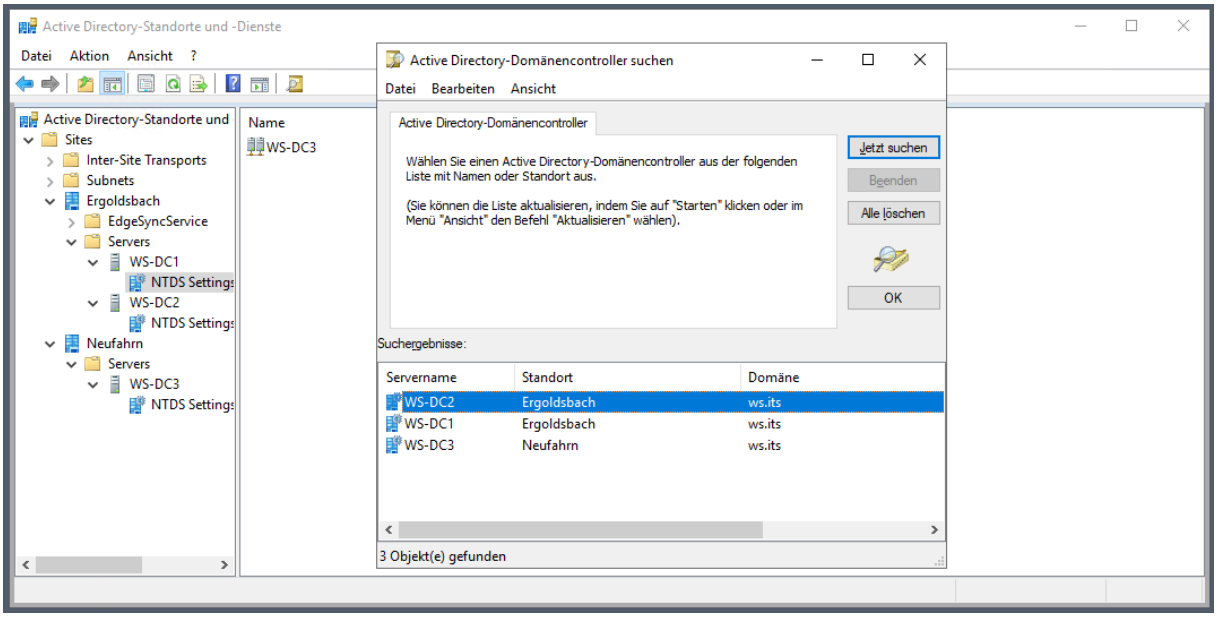


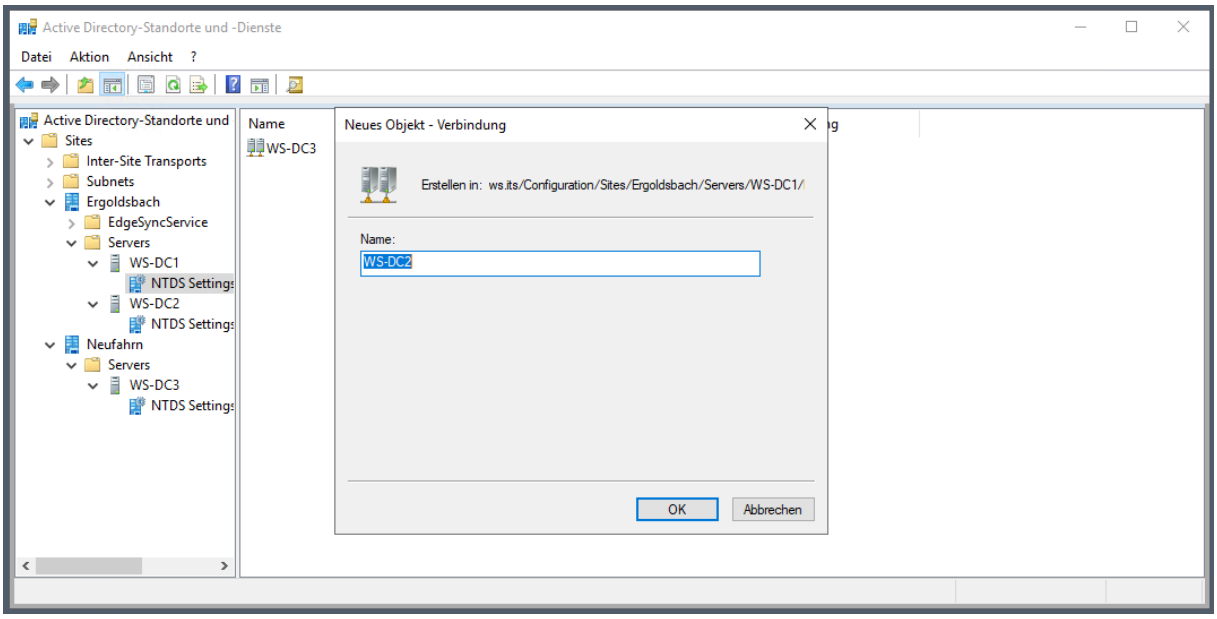




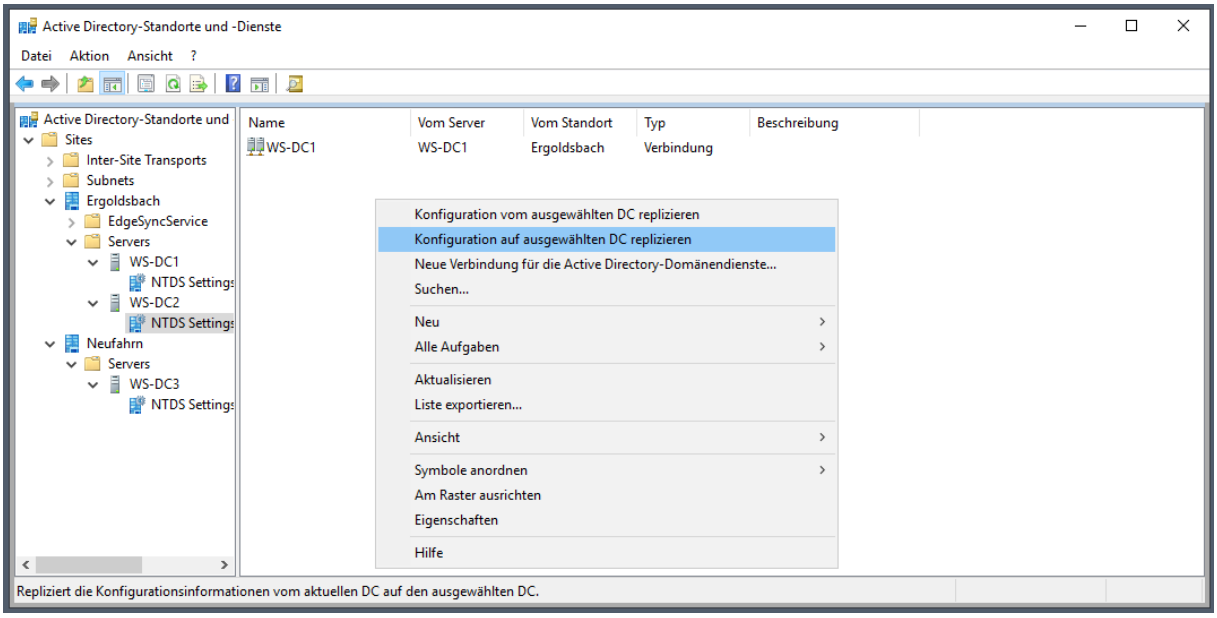
Die Verbindung soll bidirektional sein. Daher erstelle ich eine weitere Verbindung zwischen Server WS-DC1 und WS-DC2:


Active Directory-Standorte und -Dienste
Datei Aktion Ansicht ?
Active Directory-Standorte und
Sites
Inter-Site Transports
Subnets
Ergoldsbach
EdgeSyncService
Servers
WS-DC1
NTDS Settings
WS-DC2
NTDS Settings
Neufahrn
Servers
WS-DC3
NTDS Settings
Name
Vom Server
Vom Standort
Typ
Beschreibung
WS-DC3
WS-DC3
Neufahrn
Verbindung
Neue Verbindung für die Active Directory-Domänendienste...
Suchen...
Neu
Alle Aufgaben
Aktualisieren
Liste exportieren...
Ansicht
Symbole anordnen
Am Raster ausrichten
Eigenschaften
Hilfe
Erstellt ein neues Objekt...

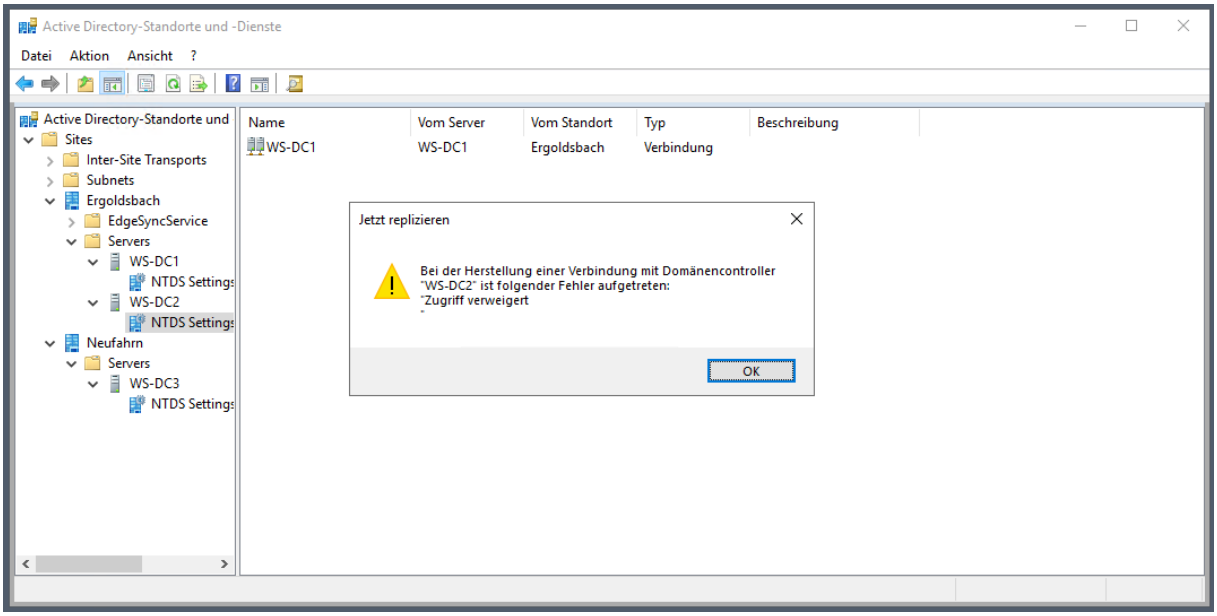

Active Directory-Standorte und -Dienste
Active Directory-Domänencontroller suchen
Datei Bearbeiten Ansicht
Active Directory-Domänencontroller
Wählen Sie einen Active Directory-Domänencontroller aus der folgenden Liste mit Namen oder Standort aus.
(Sie können die Liste aktualisieren, indem Sie auf "Starten" klicken oder im Menü "Ansicht" den Befehl "Aktualisieren" wählen).
Jetzt suchen
Beenden
Alle löschen
OK
Suchergebnisse:
Servername
Standort
Domäne
WS-DC2
Ergoldsbach
ws.its
WS-DC1
Ergoldsbach
ws.its
WS-DC3
Neufahrn
ws.its
3 Objekt(e) gefunden


Active Directory-Standorte und -Dienste
Neues Objekt - Verbindung
Erstellen in: ws.its/Configuration/Sites/Ergoldsbach/Servers/WS-DC1/
Name:
WS-DC2
OK
Abbrechen

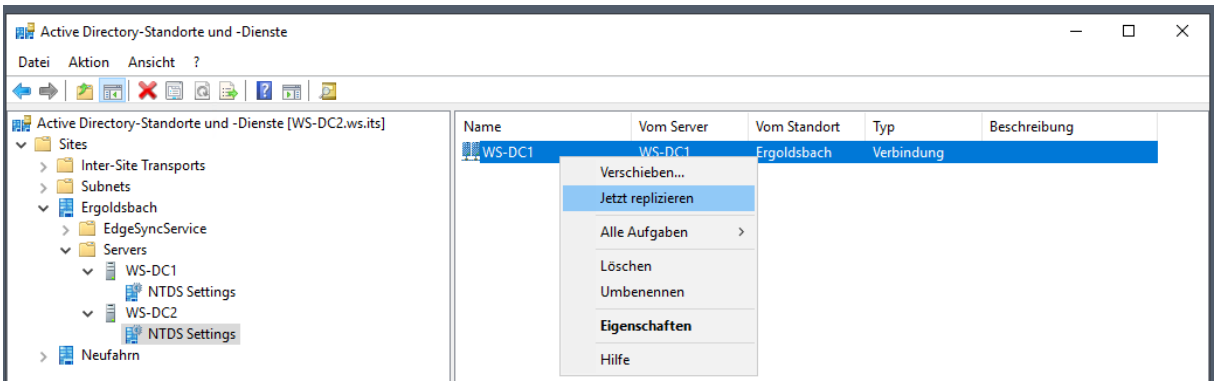
Jetzt übertrage ich meine Wunschkonfiguration vom Server WS-DC1 (mit dem hat sich die Konsole verbunden) auf den neuen Server WS-DC2. Ich könnte auch einfach warten, aber ich mag nicht warten:



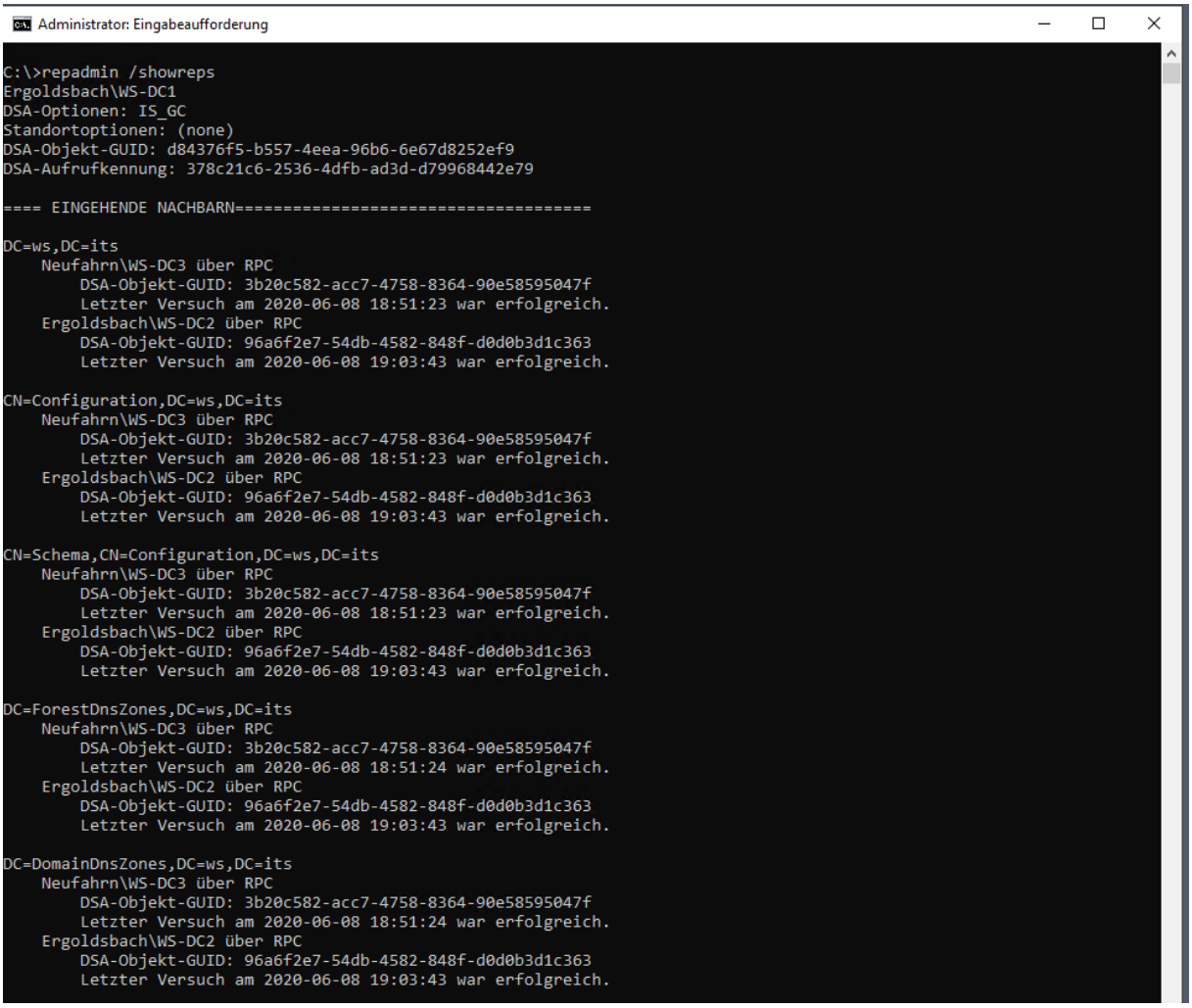
Aber ich soll wohl noch warten. Manchmal bin ich hier einfach zu ungeduldig:

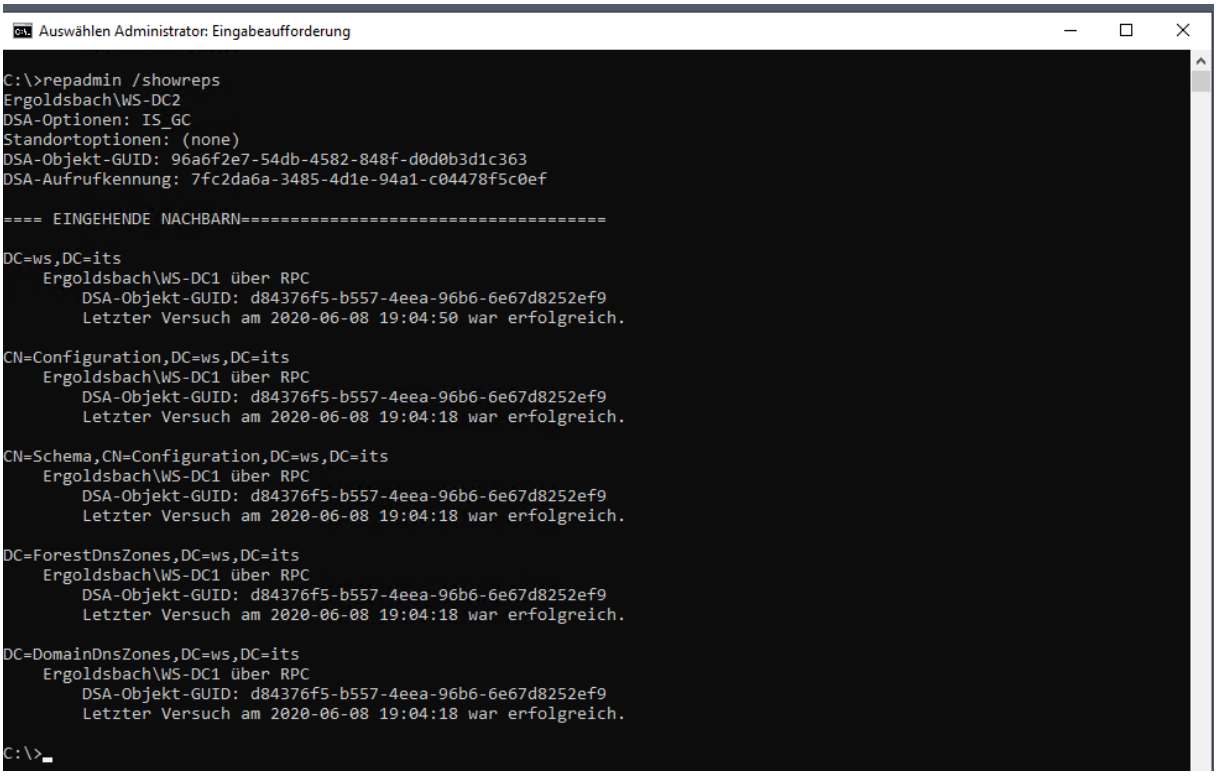


Der neue DC sieht die Verbindung bereits. Hier versuche ich die Rückreplikation zu starten:

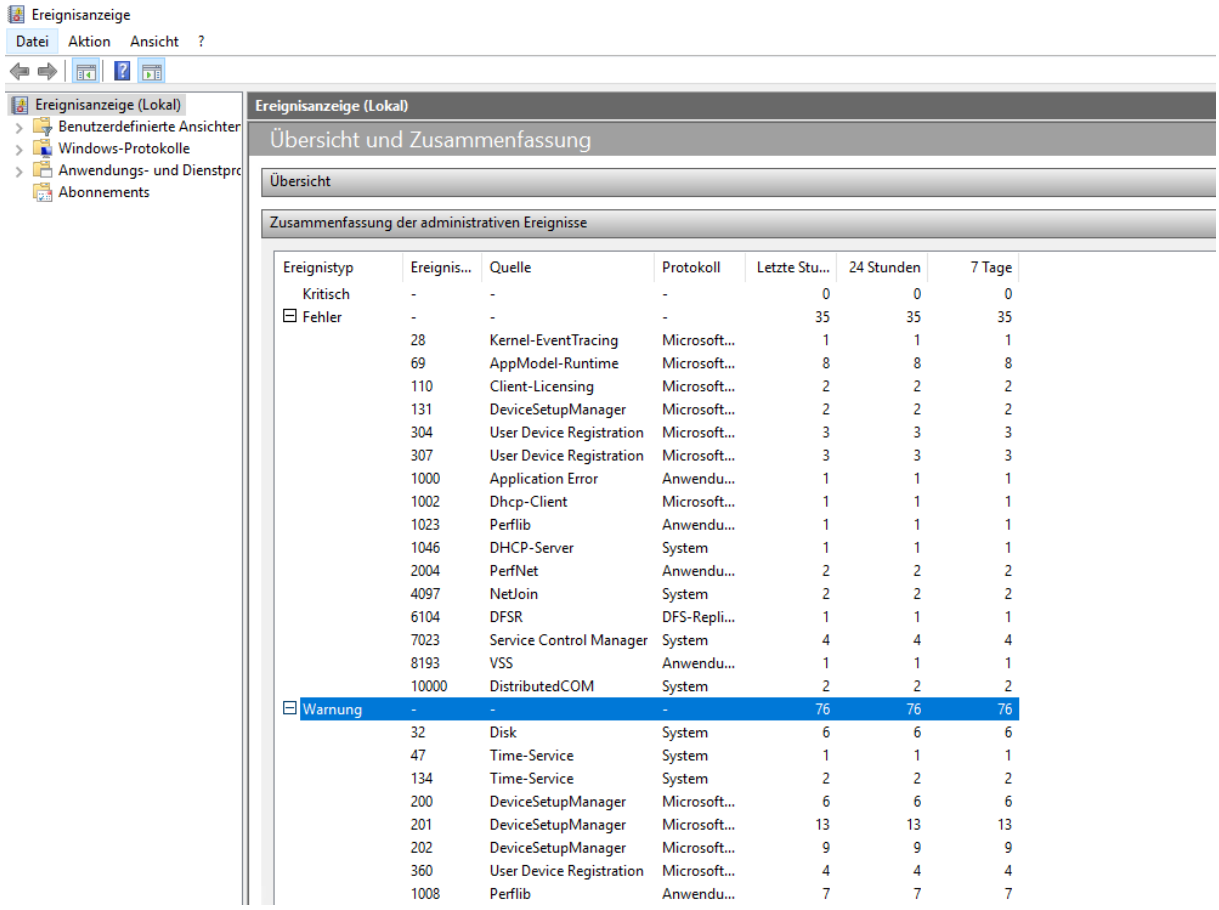


Nach wenigen Minuten sind beide Domain Controller synchron:





Dann ist es Zeit für einen Blick über die Eventlogs. Hier finde ich keine großen Probleme:

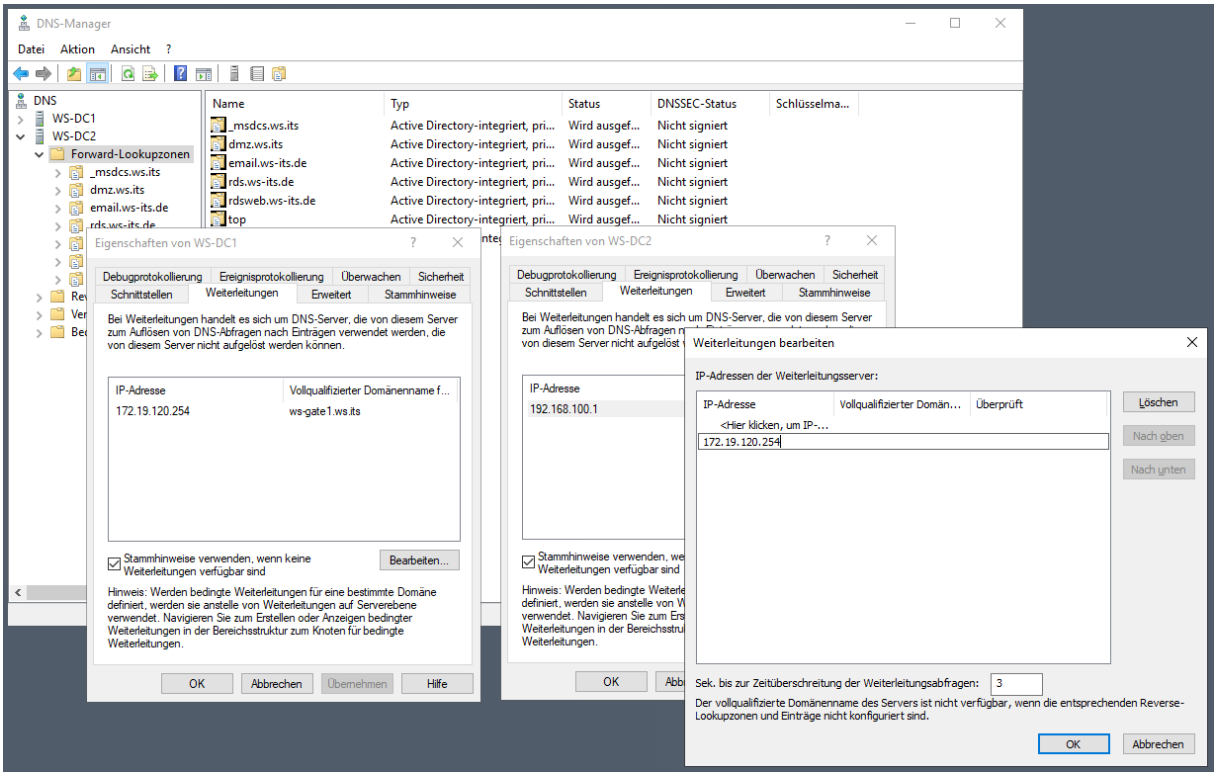


Ereignistyp	Ereignis...	Quelle	Protokoll	Letzte Stu...	24 Stunden	7 Tage
Kritisch	-	-	-	0	0	0
Fehler	-	-	-	35	35	35
	28	Kernel-EventTracing	Microsoft...	1	1	1
	69	AppModel-Runtime	Microsoft...	8	8	8
	110	Client-Licensing	Microsoft...	2	2	2
	131	DeviceSetupManager	Microsoft...	2	2	2
	304	User Device Registration	Microsoft...	3	3	3
	307	User Device Registration	Microsoft...	3	3	3
	1000	Application Error	Anwendu...	1	1	1
	1002	Dhcp-Client	Microsoft...	1	1	1
	1023	Perflib	Anwendu...	1	1	1
	1046	DHCP-Server	System	1	1	1
	2004	PerfNet	Anwendu...	2	2	2
	4097	NetJoin	System	2	2	2
	6104	DFSR	DFS-Repli...	1	1	1
	7023	Service Control Manager	System	4	4	4
	8193	VSS	Anwendu...	1	1	1
	10000	DistributedCOM	System	2	2	2
Warnung	-	-	-	76	76	76
	32	Disk	System	6	6	6
	47	Time-Service	System	1	1	1
	134	Time-Service	System	2	2	2
	200	DeviceSetupManager	Microsoft...	6	6	6
	201	DeviceSetupManager	Microsoft...	13	13	13
	202	DeviceSetupManager	Microsoft...	9	9	9
	360	User Device Registration	Microsoft...	4	4	4
	1008	Perflib	Anwendu...	7	7	7

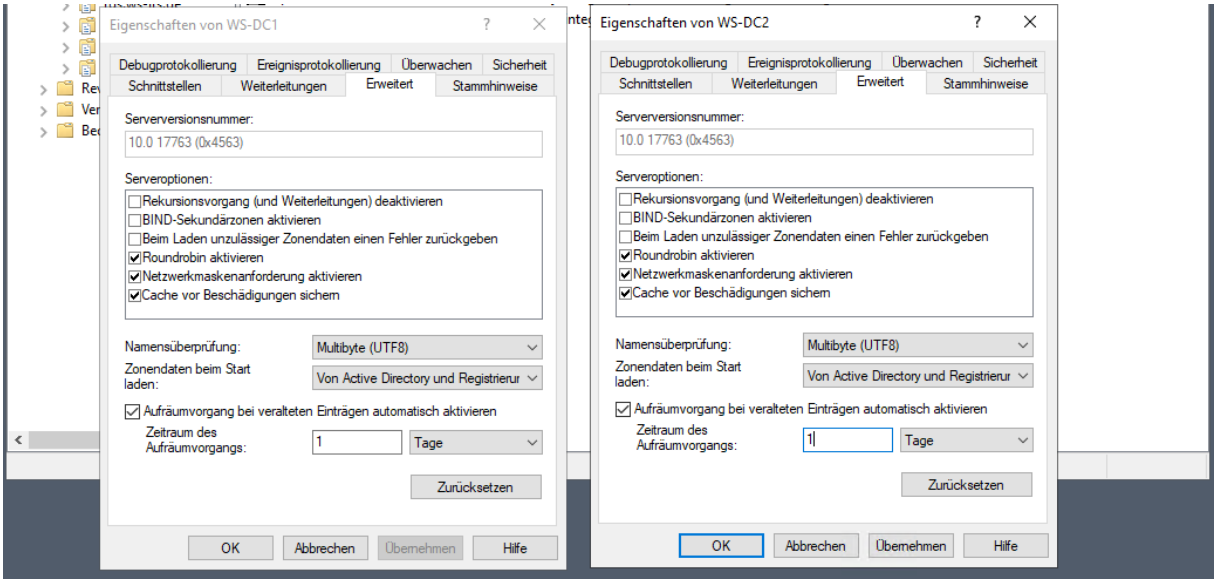
Damit ist die Rolle Active Directory migriert.

Installation der Rolle DNS

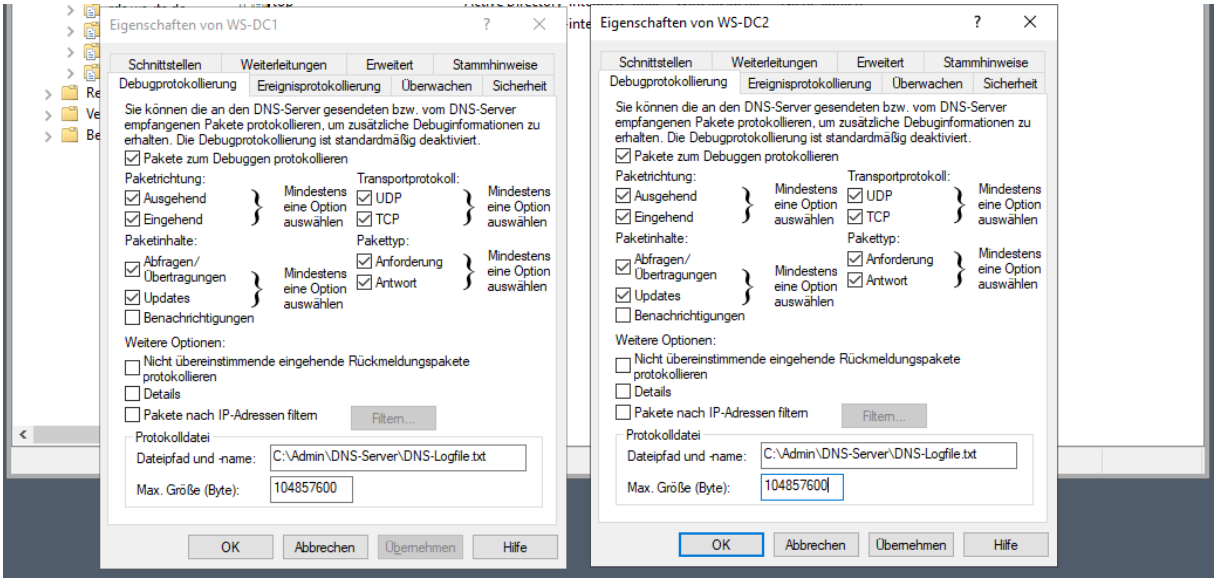
Mein DNS-Service ist in das Active Directory integriert. Daher hat der neue Server bereits alle Zonen geladen. Ich muss also nur noch ein paar Optionen anpassen. Zuerst verändere ich den Forwarder und trage hier meine Fritzbox WS-Gate1 ein. So kann der WS-DC2 auch externe Namen auflösen, wenn WS-DC1 nicht verfügbar ist:



Die Alterungseinstellungen übernehme ich vom WS-DC1:



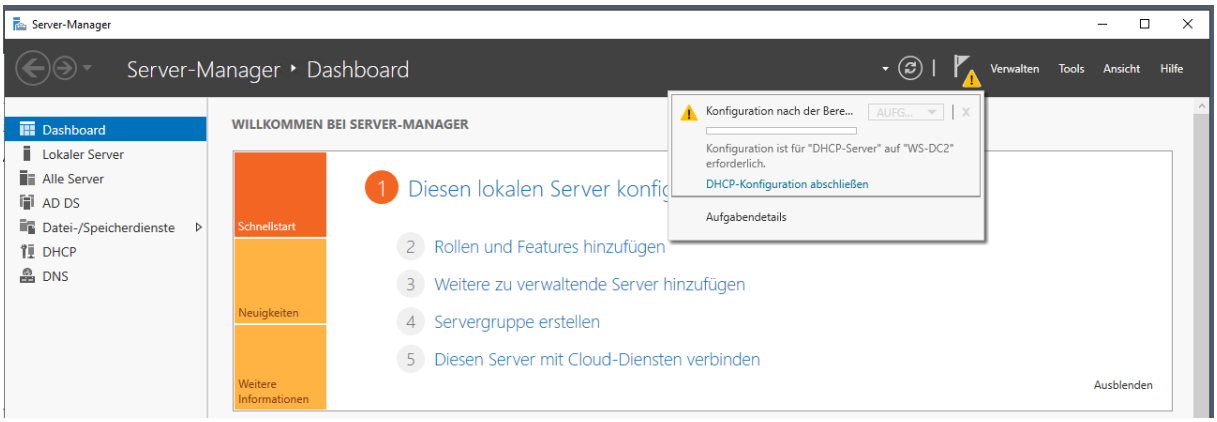
Ebenso die Konfiguration der DNS-Protokollierung. Hierfür habe ich unter c:\admin einen Ordner DNS-Server erstellt:

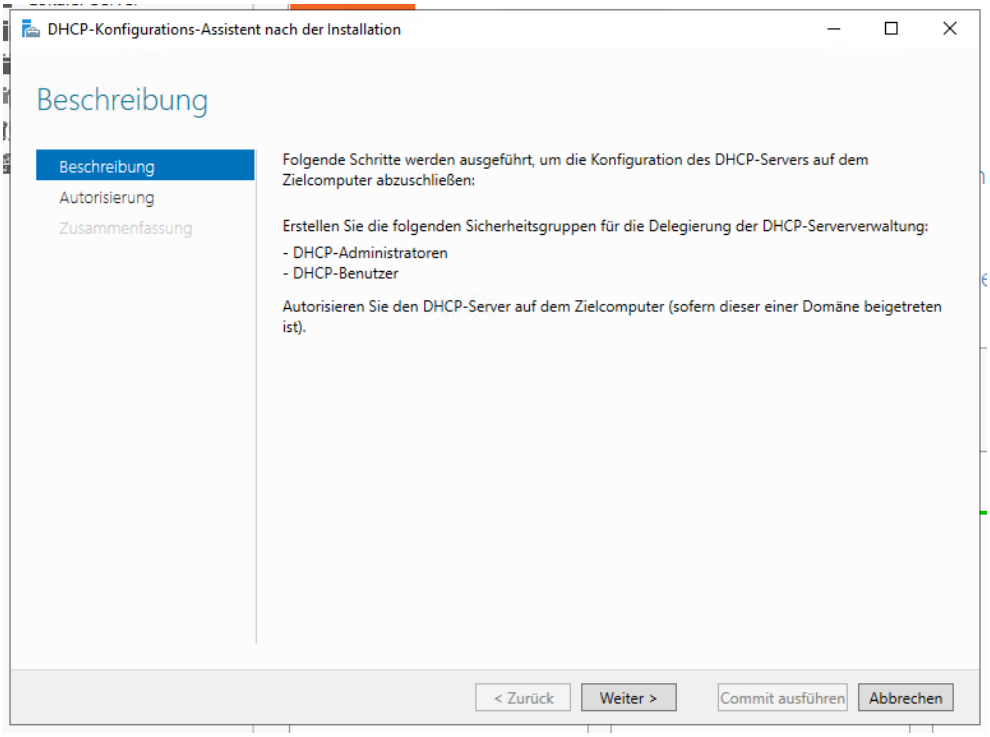


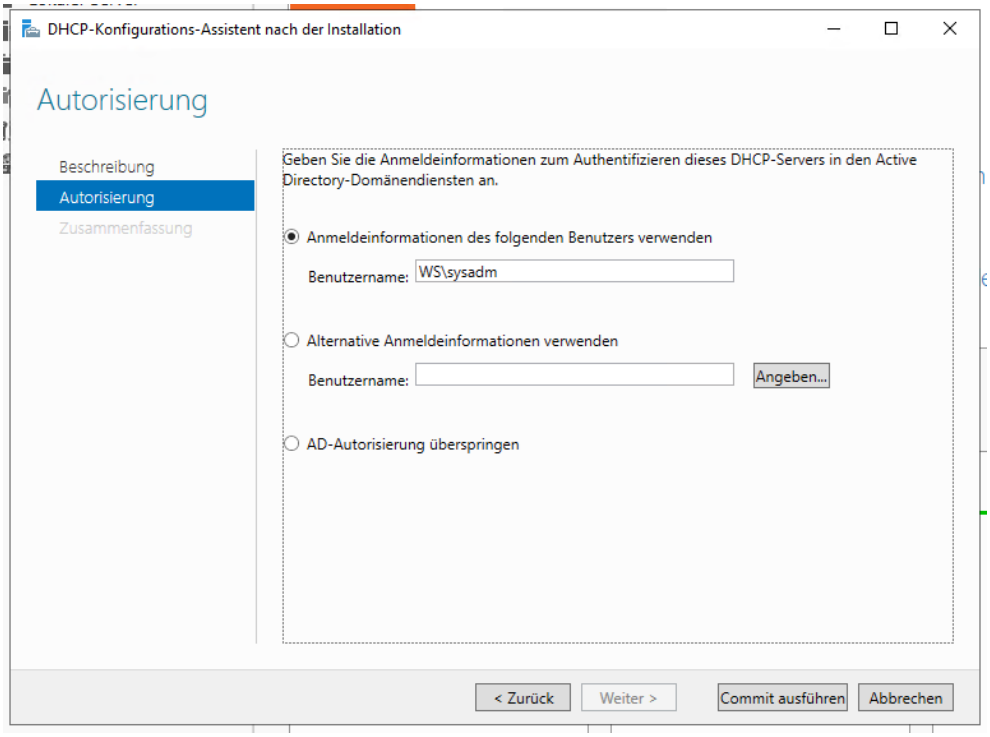
Das sollte alles gewesen sein. Der DNS-Server ist einsatzbereit.

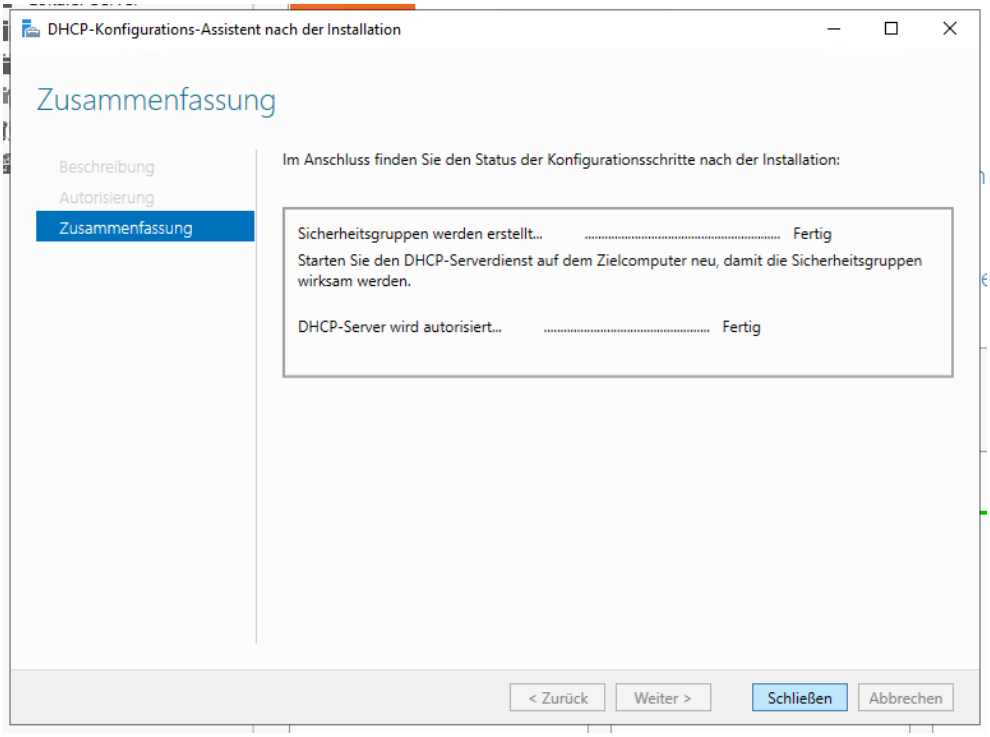
Installation der Rolle DHCP

Nun fehlt noch dir dritte Rolle: Der DHCP-Server. Im Server Manager kann ich die Autorisierung vornehmen:

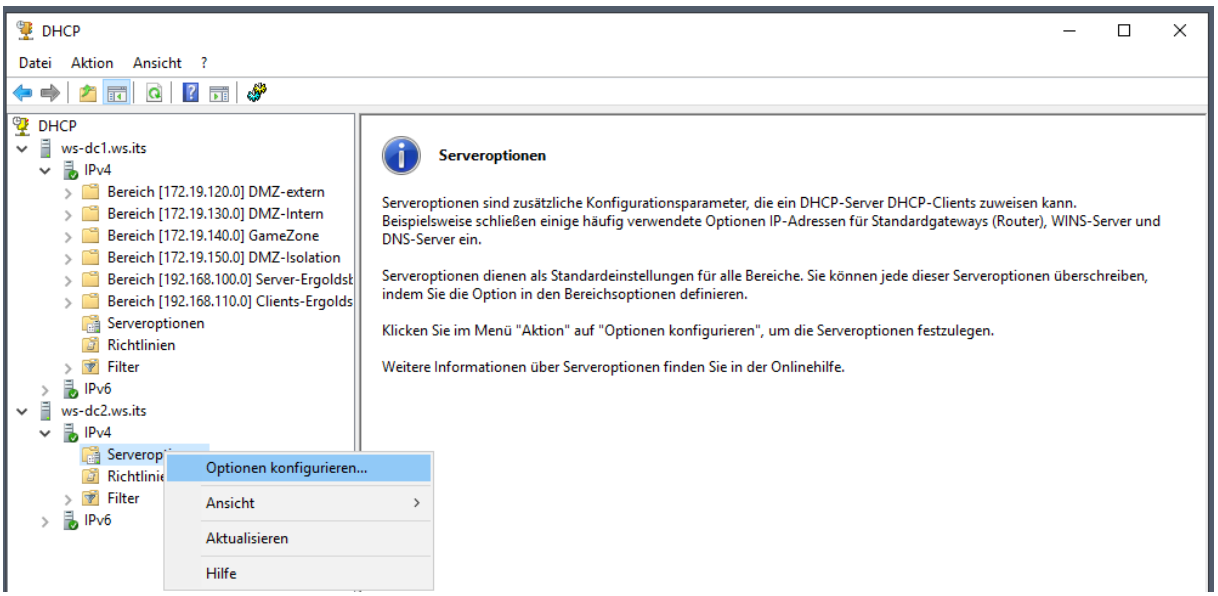



DHCP-Konfigurations-Assistent nach der Installation
Beschreibung
Beschreibung
Autorisierung
Zusammenfassung
Folgende Schritte werden ausgeführt, um die Konfiguration des DHCP-Servers auf dem Zielcomputer abzuschließen:
Erstellen Sie die folgenden Sicherheitsgruppen für die Delegierung der DHCP-Serververwaltung:
- DHCP-Administratoren
- DHCP-Benutzer
Autorisieren Sie den DHCP-Server auf dem Zielcomputer (sofern dieser einer Domäne beigetreten ist).
< Zurück
Weiter >
Commit ausführen
Abbrechen


DHCP-Konfigurations-Assistent nach der Installation
Autorisierung
Beschreibung
Autorisierung
Zusammenfassung
Geben Sie die Anmeldeinformationen zum Authentifizieren dieses DHCP-Servers in den Active Directory-Domänendiensten an.
Anmeldeinformationen des folgenden Benutzers verwenden
Benutzername: WS\sysadm
Alternative Anmeldeinformationen verwenden
Benutzername:
Angeben...
AD-Autorisierung überspringen
< Zurück
Weiter >
Commit ausführen
Abbrechen

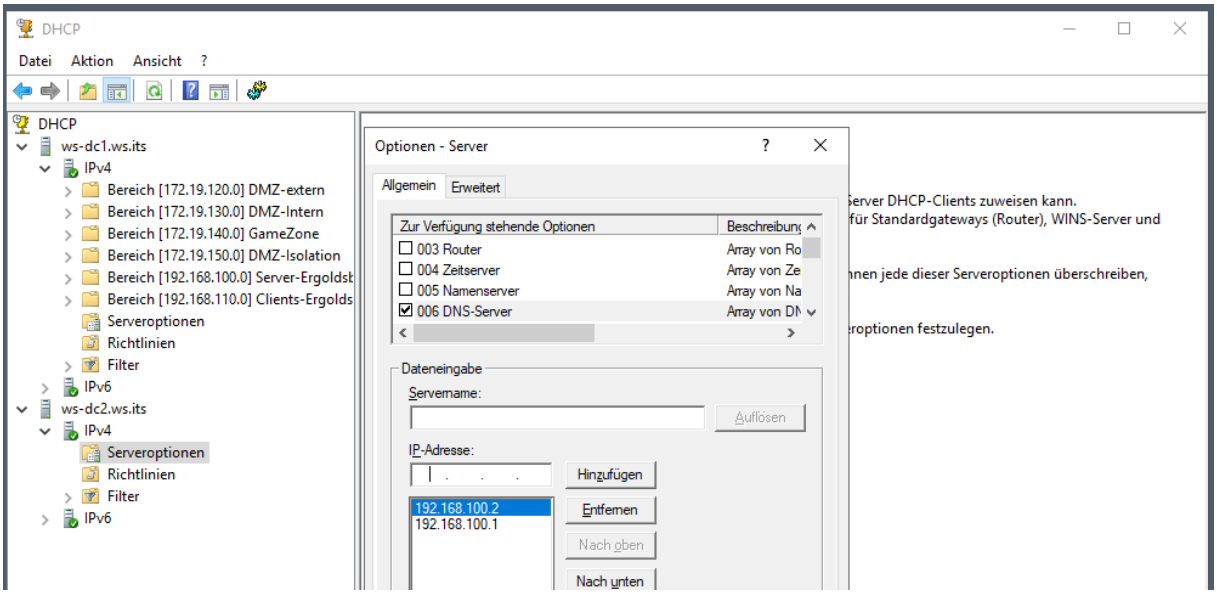


Danach wird der Service gestartet. Ich verbinde beide DHCP-Server in der Konsole. Zuerst trage ich im neuen Server die Server-Optionen ein:

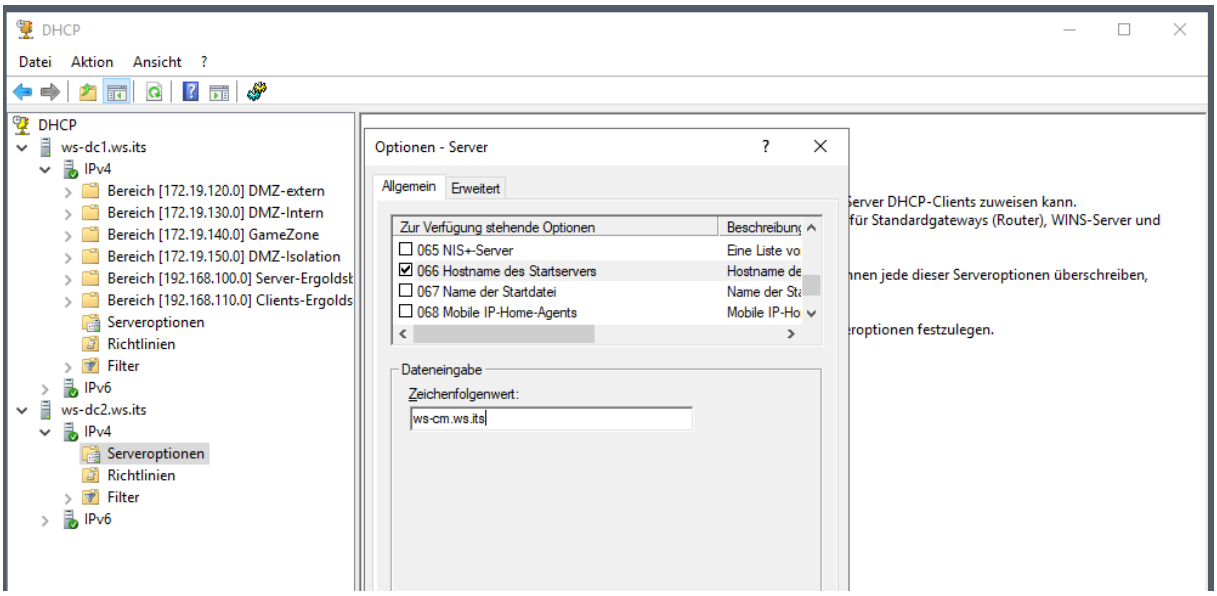


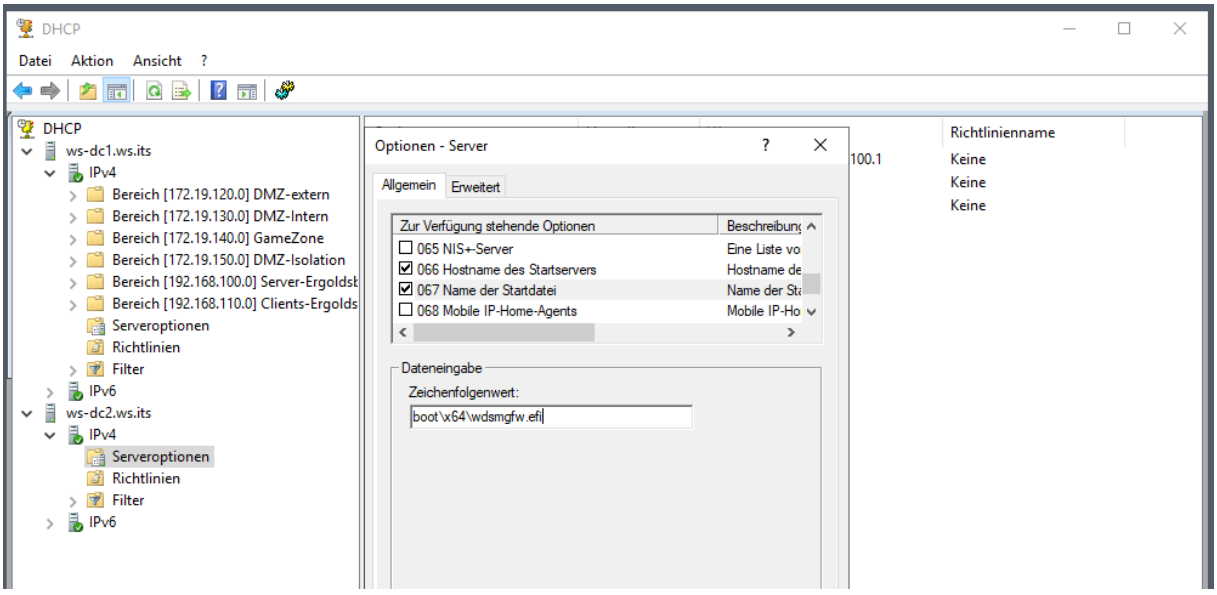
Die IP-Adressen der DNS-Server sind hier absteigend sortiert. So erhalte ich für DNS eine Art Lastverteilung:

1. Erhält ein Client seine IP-Adresse vom DHCP-Server WS-DC1, dann ist sein primärer DNS-Server der WS-DC1.
2. Erhält ein Client seine IP-Adresse vom DHCP-Server WS-DC2, dann ist sein primärer DNS-Server der WS-DC2.

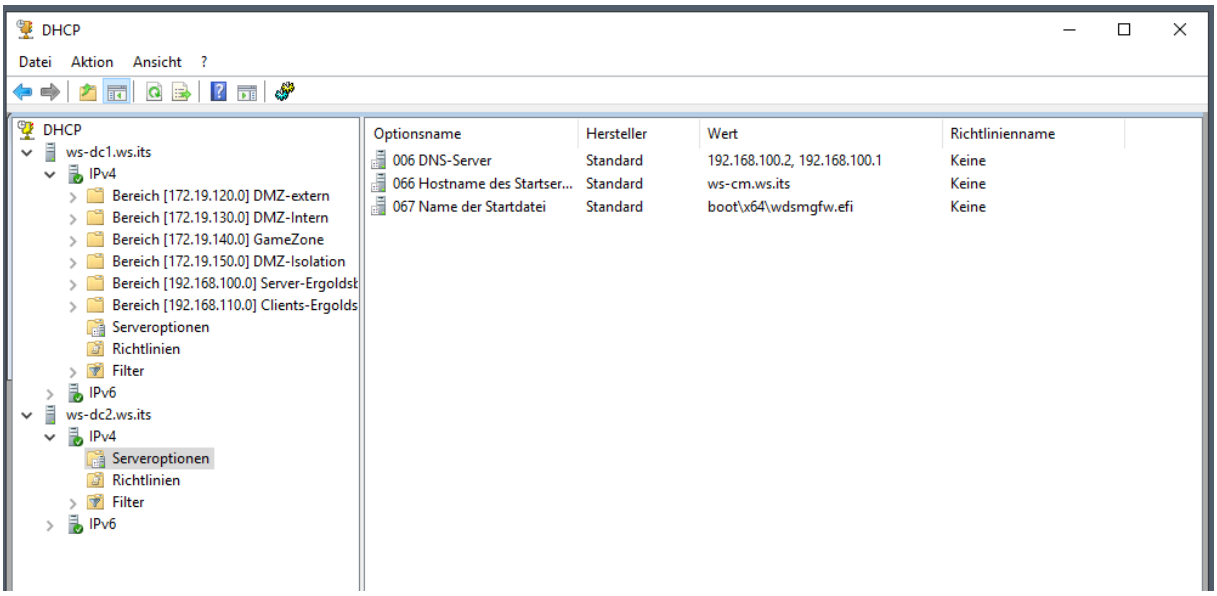


Und dann trage ich noch meinen Deployment-Server ein:

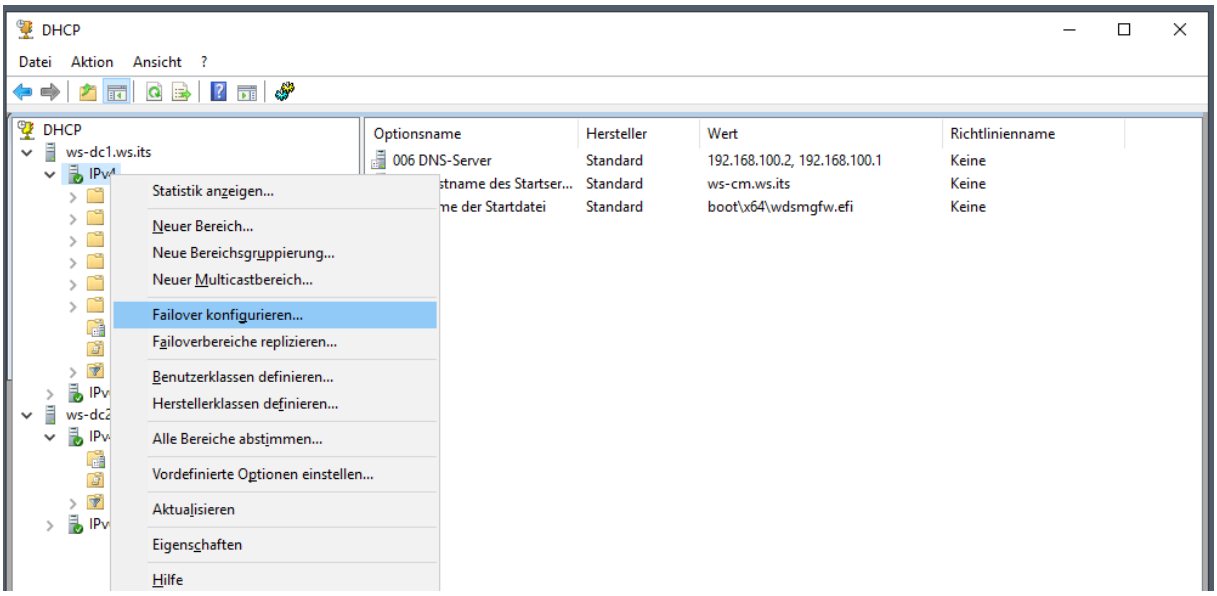




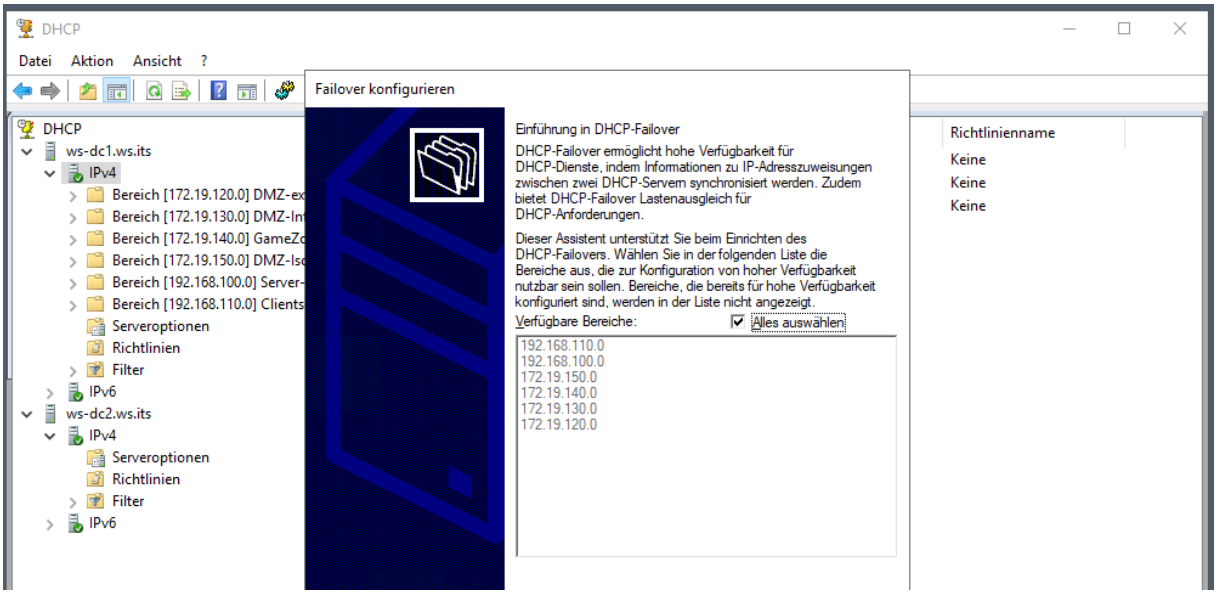
Die Server-Optionen werden in alle Scopes vererbt:



Die Scopes selber hole ich mir mit der Einrichtung des DHCP-Failovers auf den neuen Server. Den Prozess starte ich auf dem anderen Server WS-DC1:

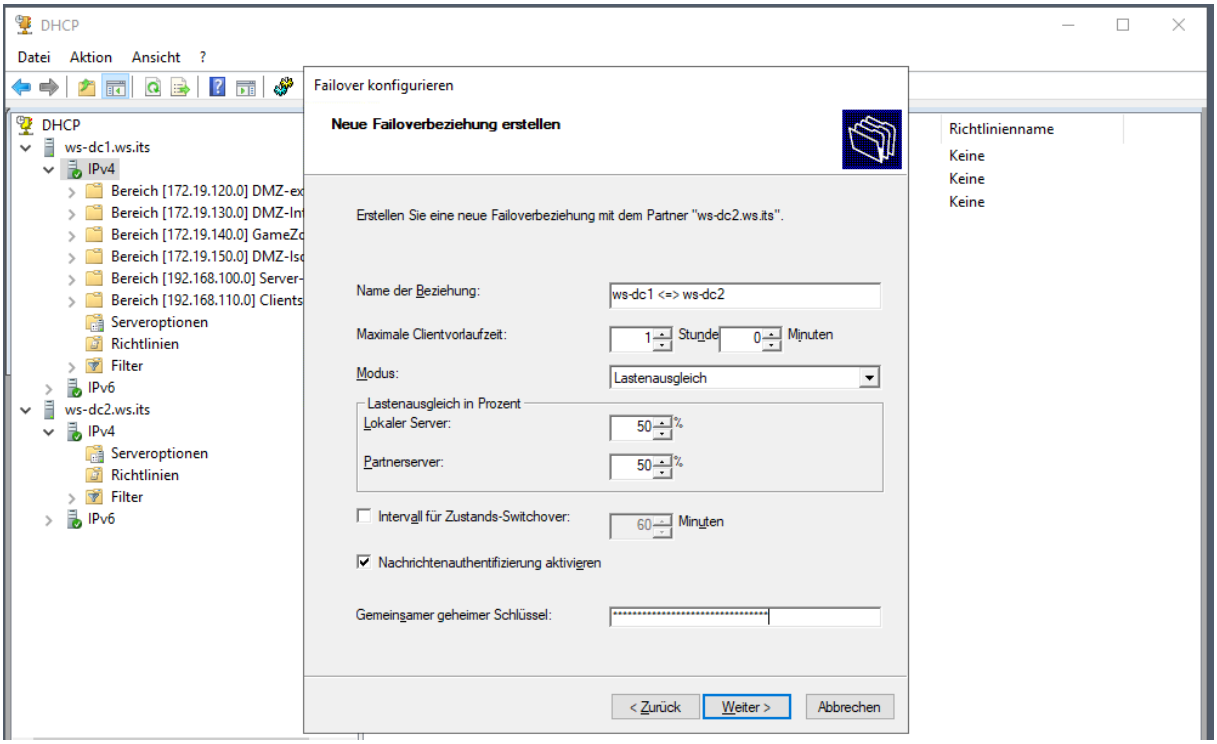


Ich werde gleich alle Scopes übernehmen:

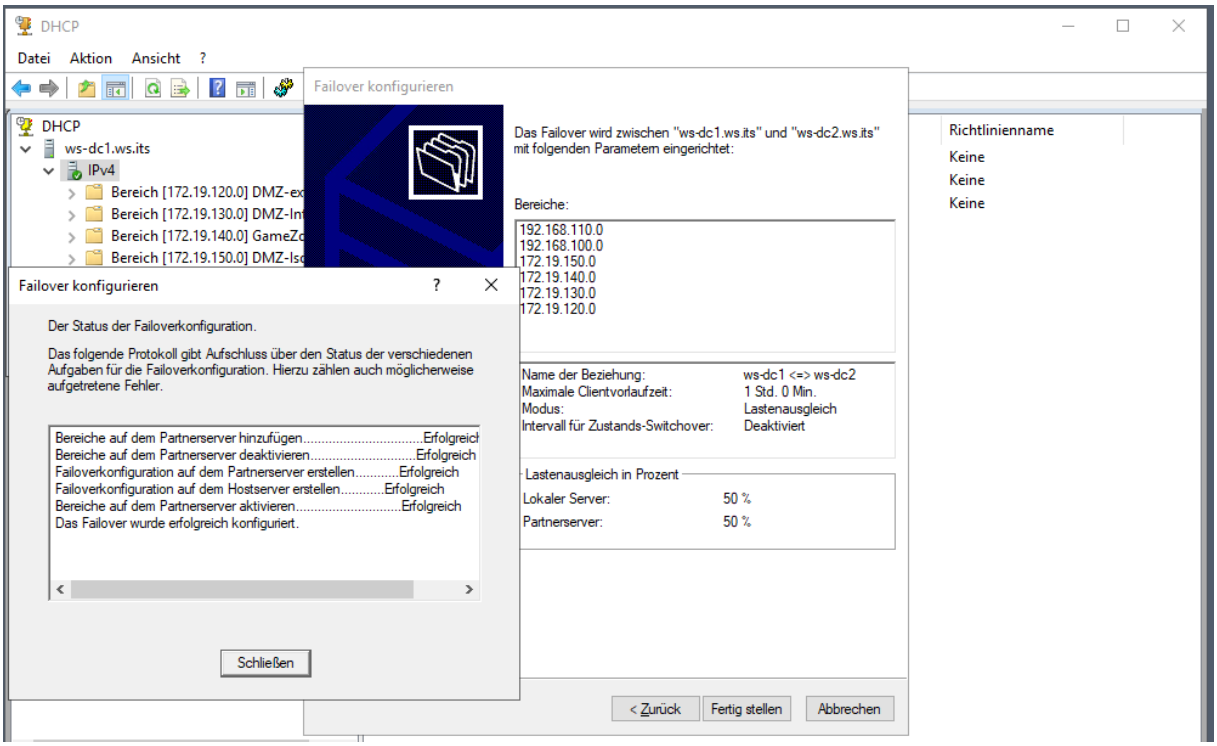


Der neue Partnerserver ist der neue WS-DC2:

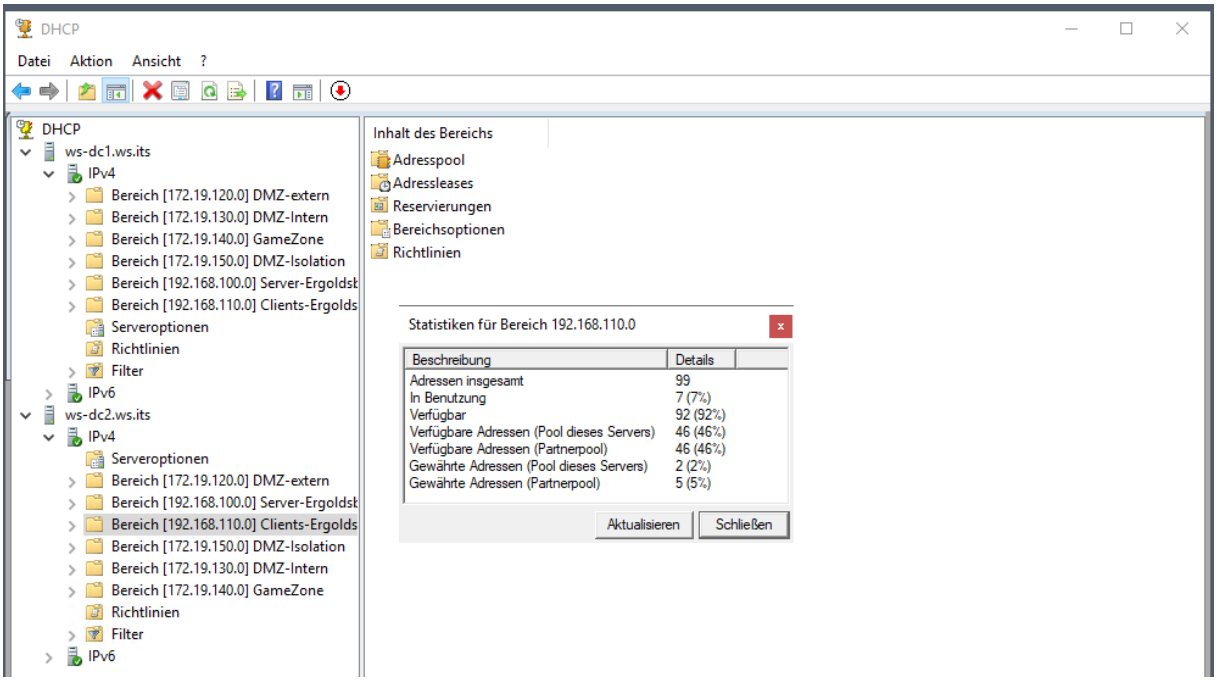
Die beiden Server arbeiten im Lastverteilungsmodus. Ich tippe ein beliebiges Passwort für die Absicherung ein:



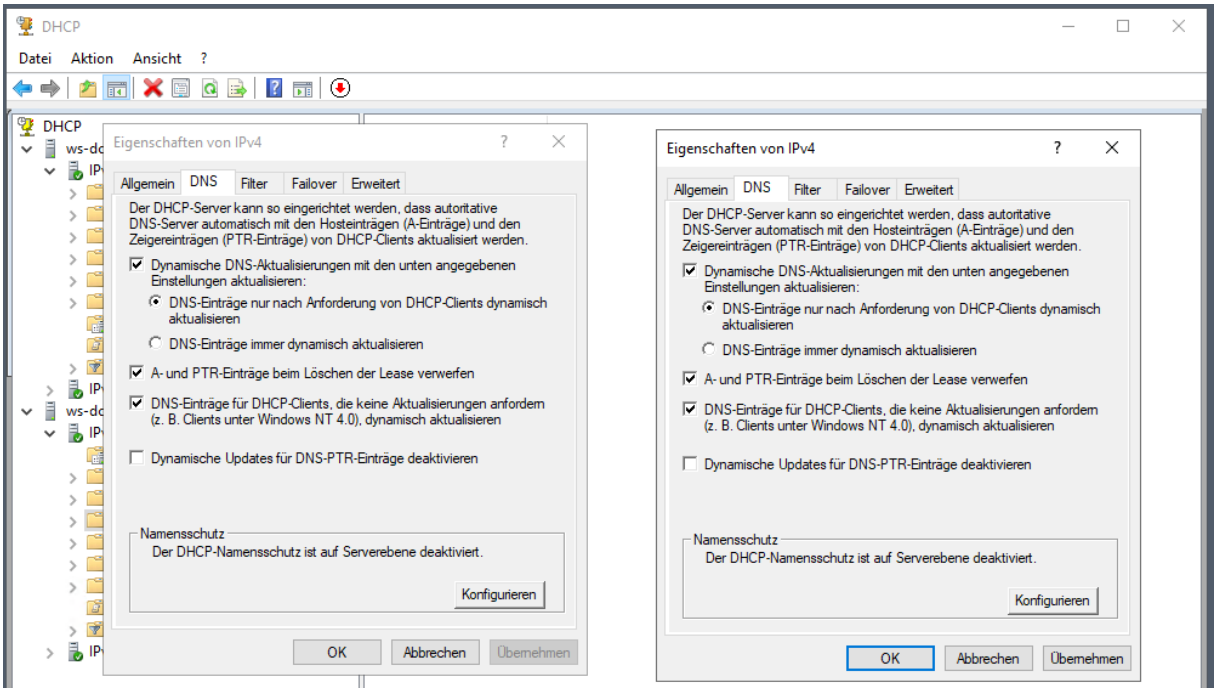
Der Abgleich dauert wenige Sekunden:



Und dann sind alle Scopes über das DHCP-Failover hochverfügbar. Selbst die Aufteilung der IP-Adressen wurde wieder hergestellt:



Zum Abschluss passe ich noch Optionen des DHCP-Services an:

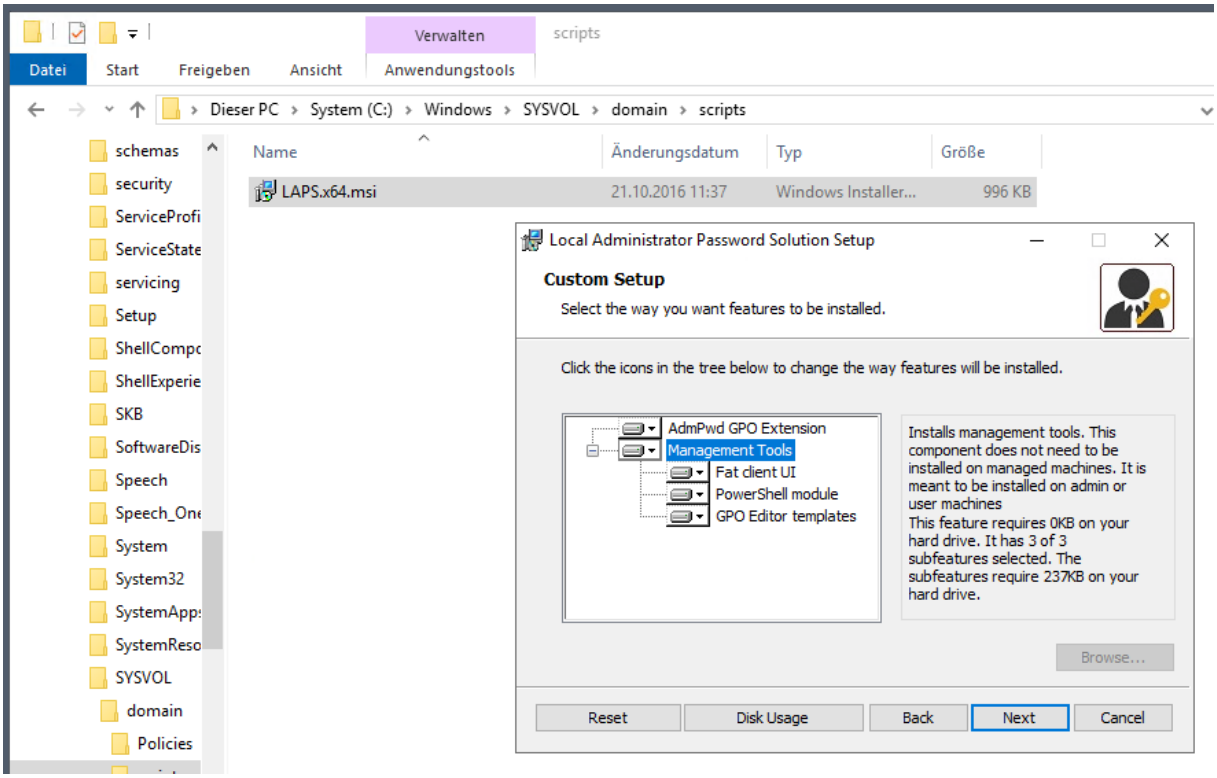


Damit sind die Funktionen des alten Servers auf den neuen übertragen.

Nacharbeiten

Installation LAPS

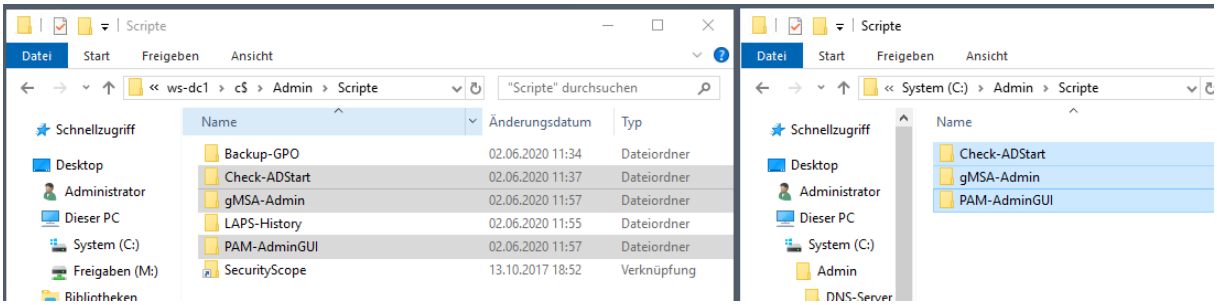
Ohne Nacharbeiten geht es aber nicht. Ich muss z.B. das LAPS (Local Administrator Password Solution) von Microsoft nachinstallieren. Die msi habe ich im netlogon-Verzeichnis abgelegt:



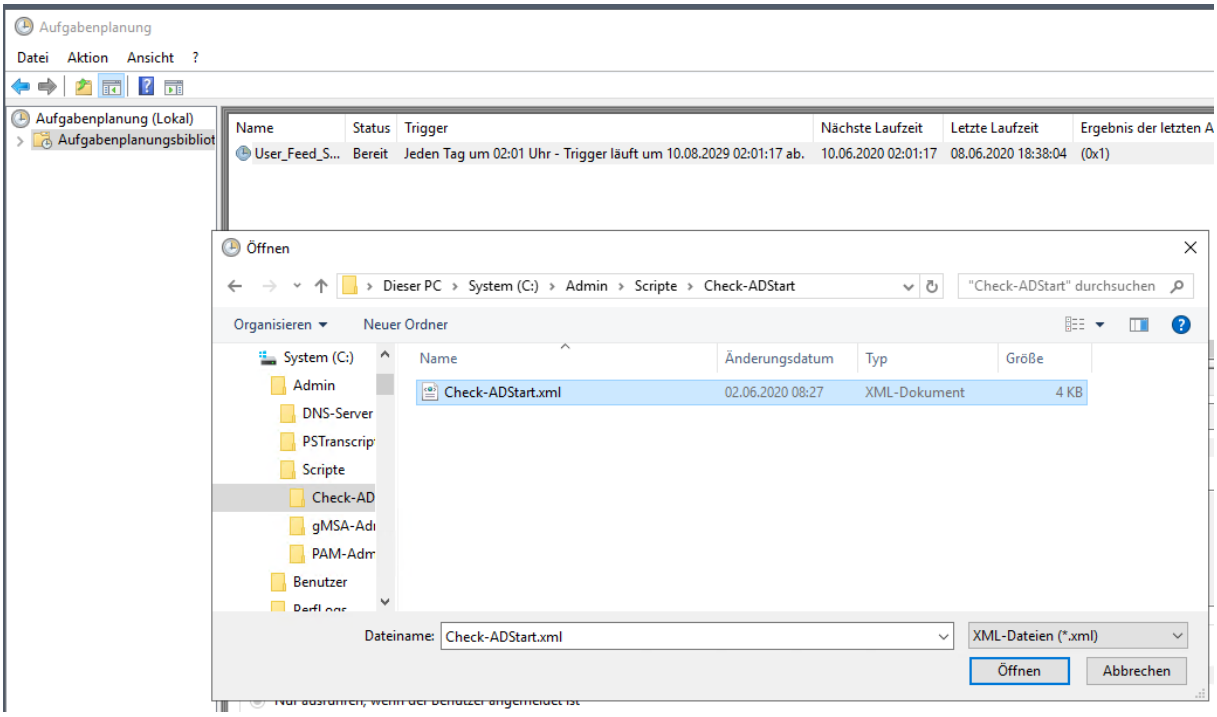
Die Konfiguration des LAPS hatte ich schon vor Jahren im Active Directory vorgenommen. Daher genügt hier die Installatin der Tools.

Adminverzeichnis & geplante Aufgaben

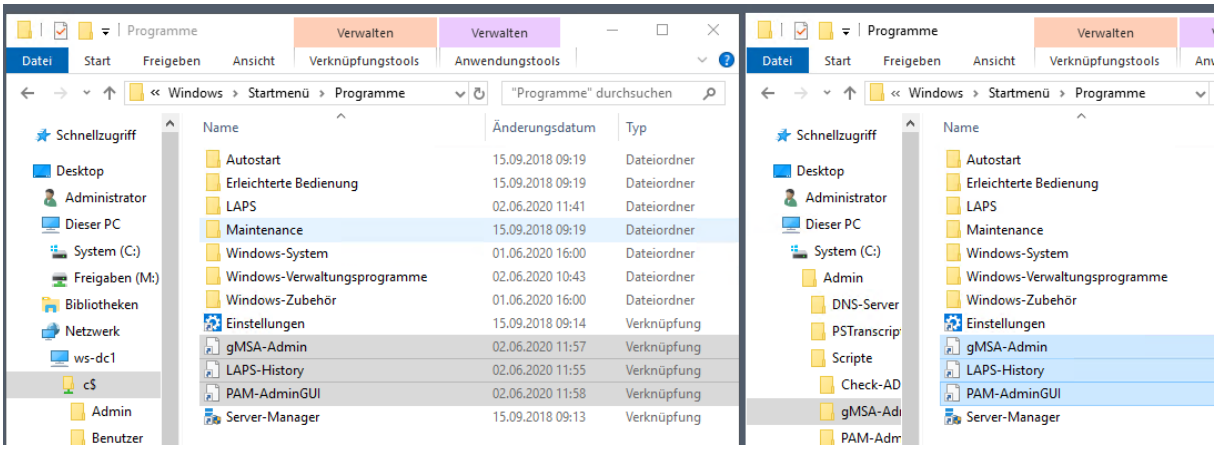
Weiter geht es mit der Einrichtung meines Admin-Verzeichnisses c:\admin. Hier kopiere ich mir einige Scripte vom anderen Domain Controller:



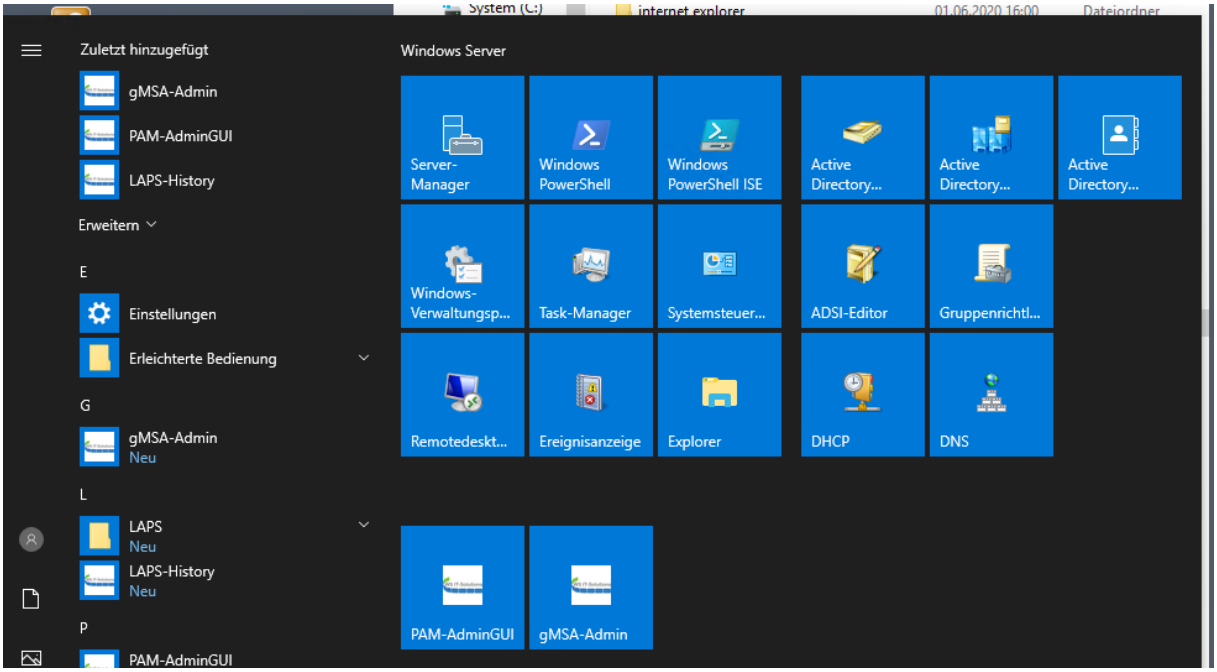
Das Script Check-ADStart hatte ich beim letzten Mal erläuftert. Auch auf diesem DC importiere ich es als geplante Aufgabe:



Dann kopiere ich mir noch ein paar Verknüpfungsdateien vom WS-DC1 in das Startmenü-Verzeichnis:

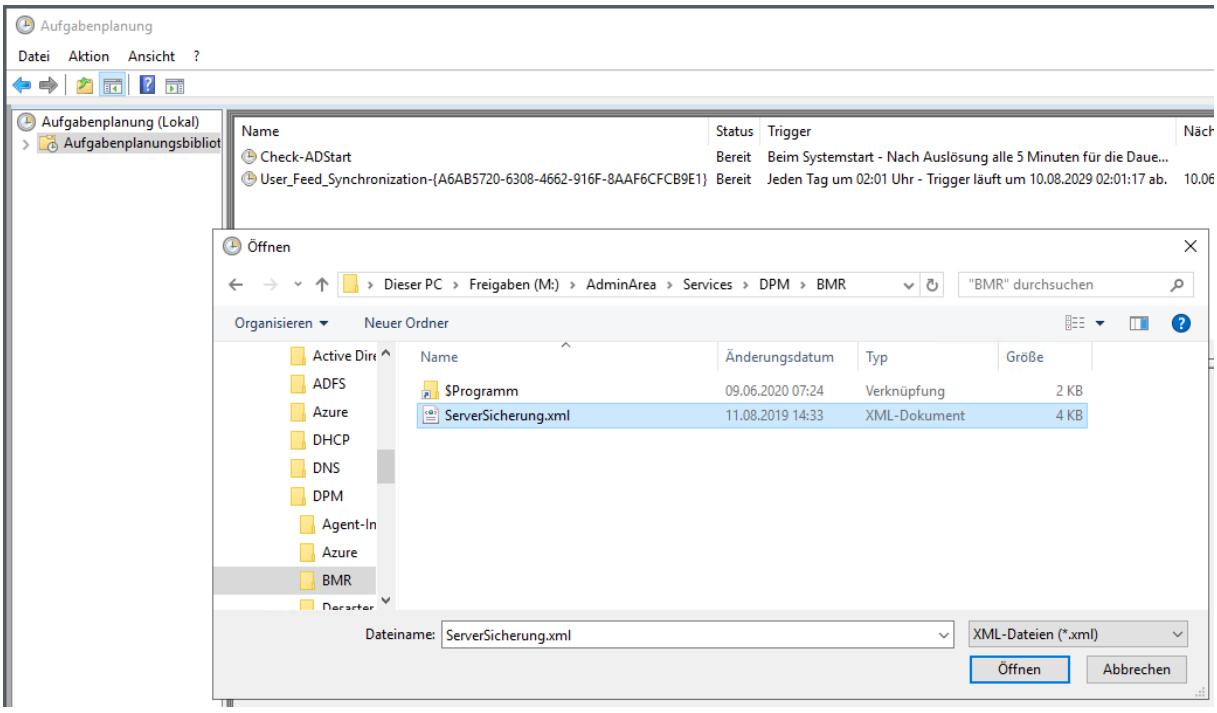


Damit kann ich meine eigenen Werkzeuge leicht ins Startmenü integrieren:

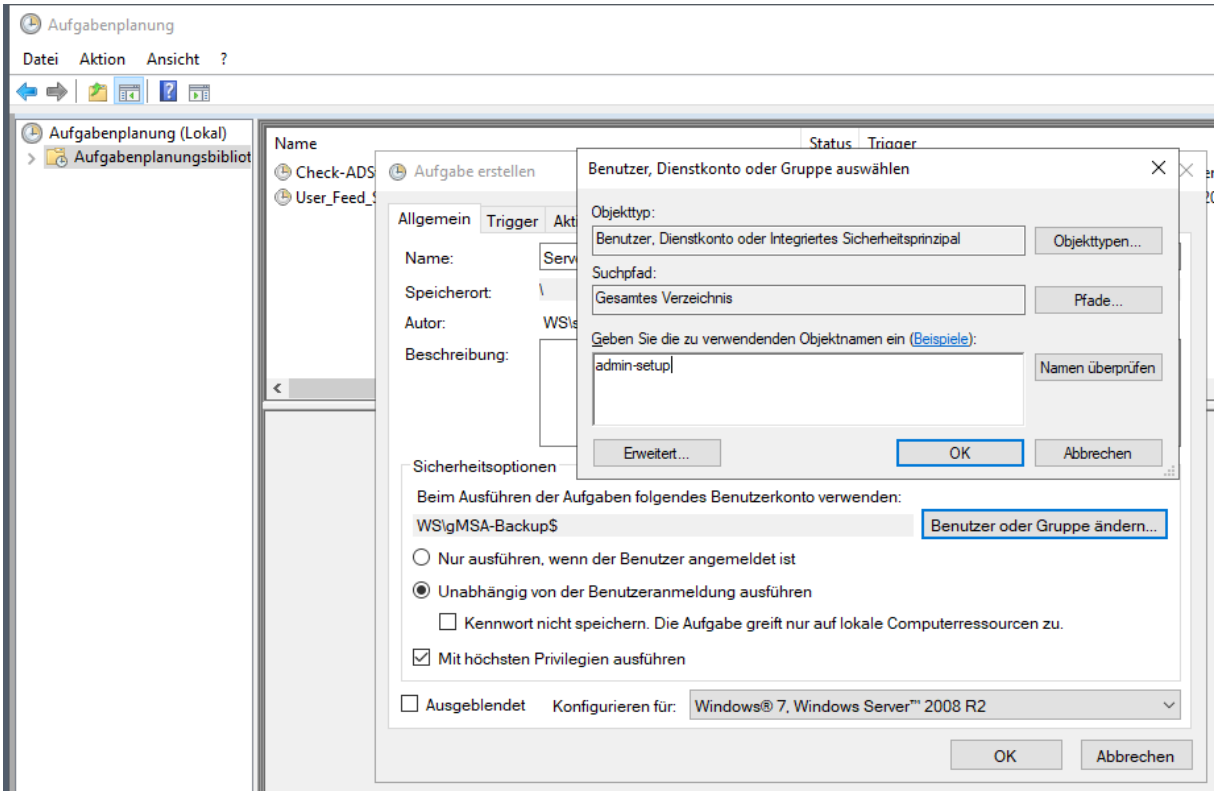


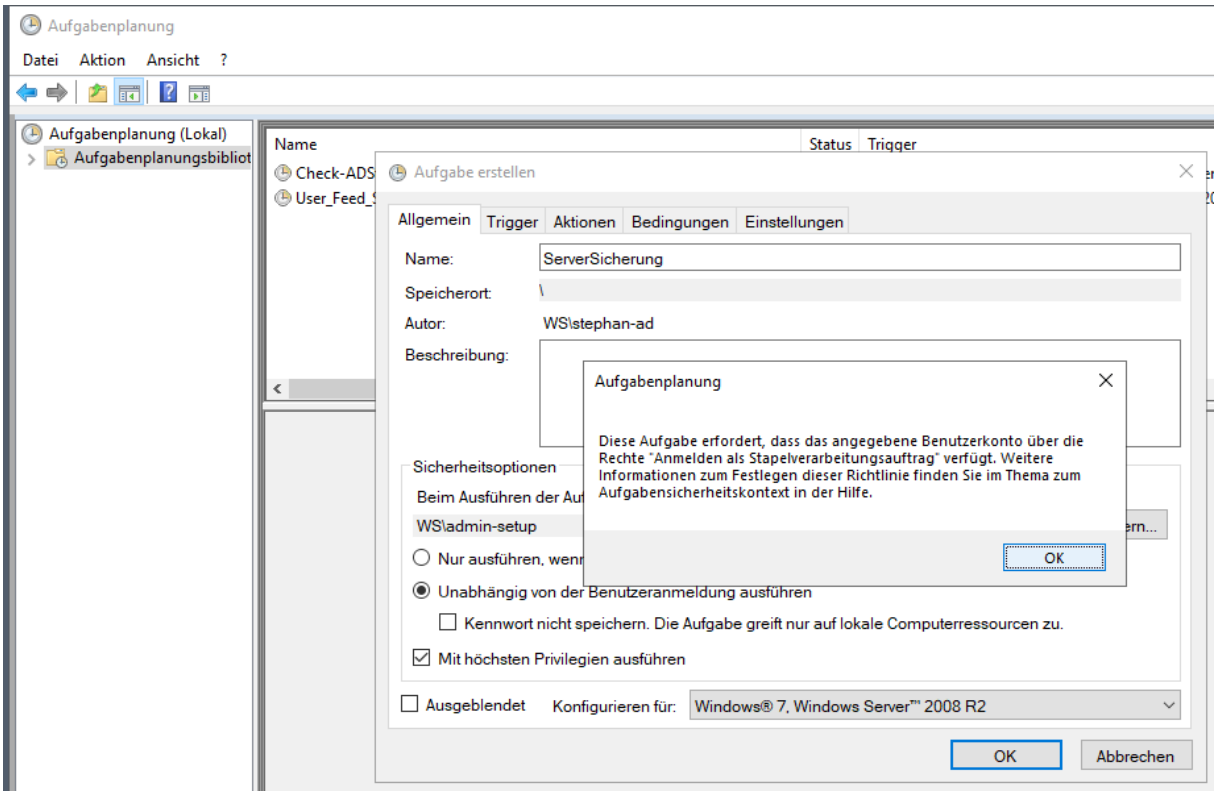
Datensicherung Windows Server

Die Datensicherung darf natürlich auch nicht fehlen. Ich importiere dazu wie immer meinen Sicherungs-Task als XML-Datei:

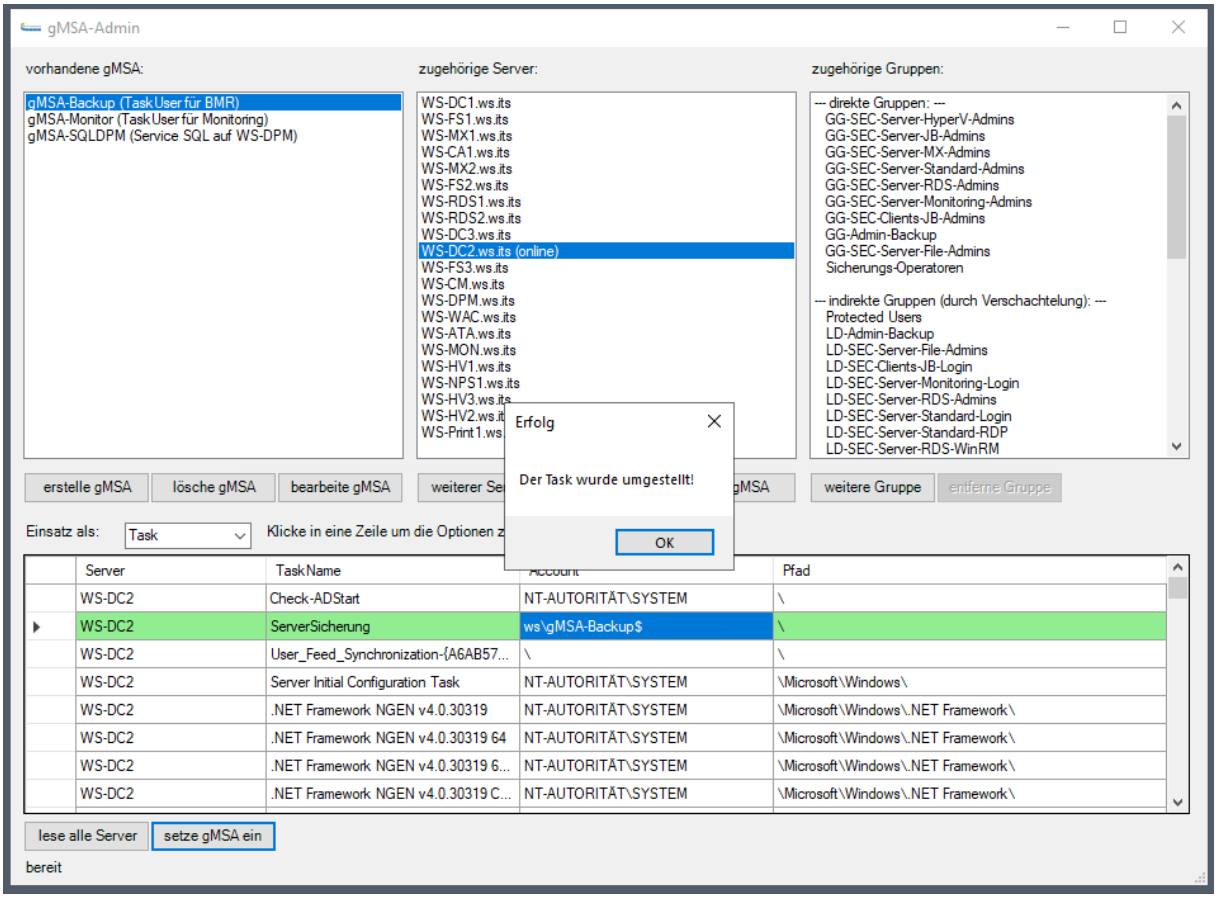


Dabei editiere ich den Task-Account und trage einen Dummy ein:





Der eigentliche Task-Account wird mit meinem PowerShell-Script „gMSA-Admin“ konfiguriert. Das habe ich mit meinem Adminverzeichnis bereitgestellt. So kann ich es auch gleich ausprobieren:



Heute wäre der Server eh mit einer Datensicherung an der Reihe gewesen. Das meldet mir zumindest die Mail mit der Zusammenfassung:

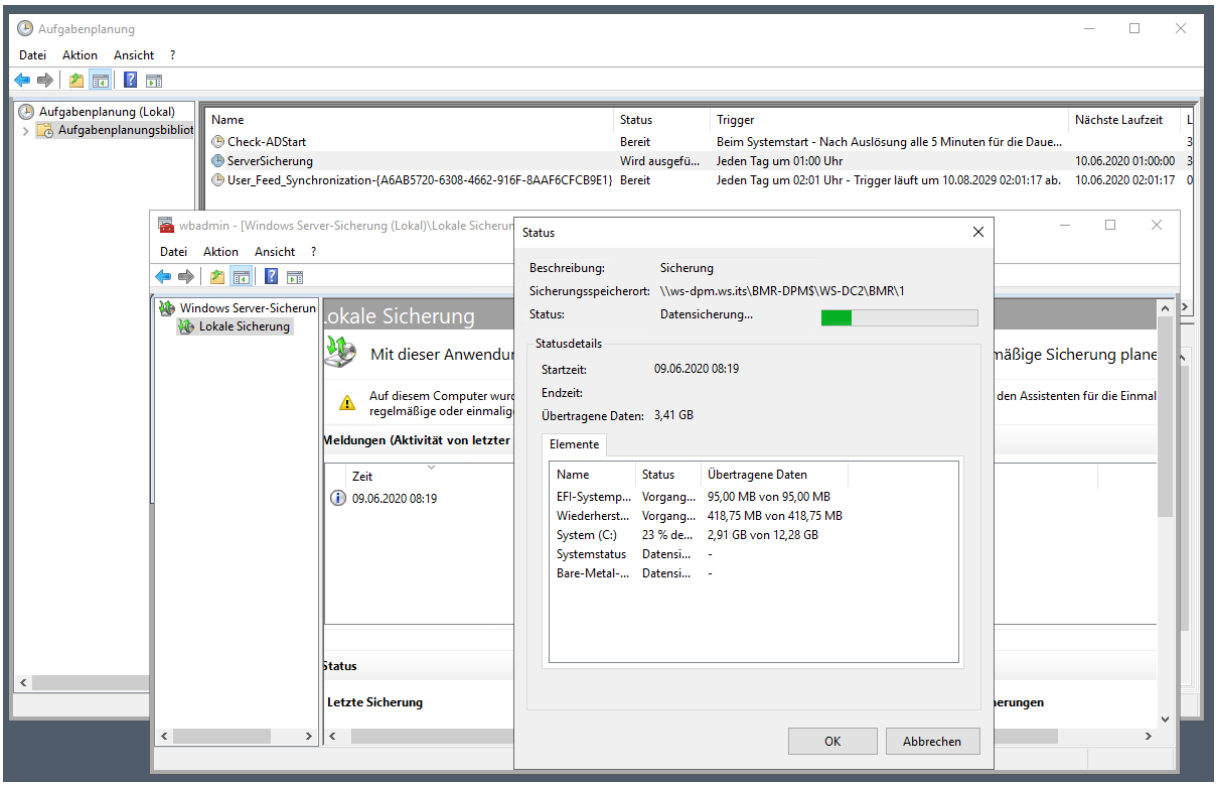
Serversicherung:

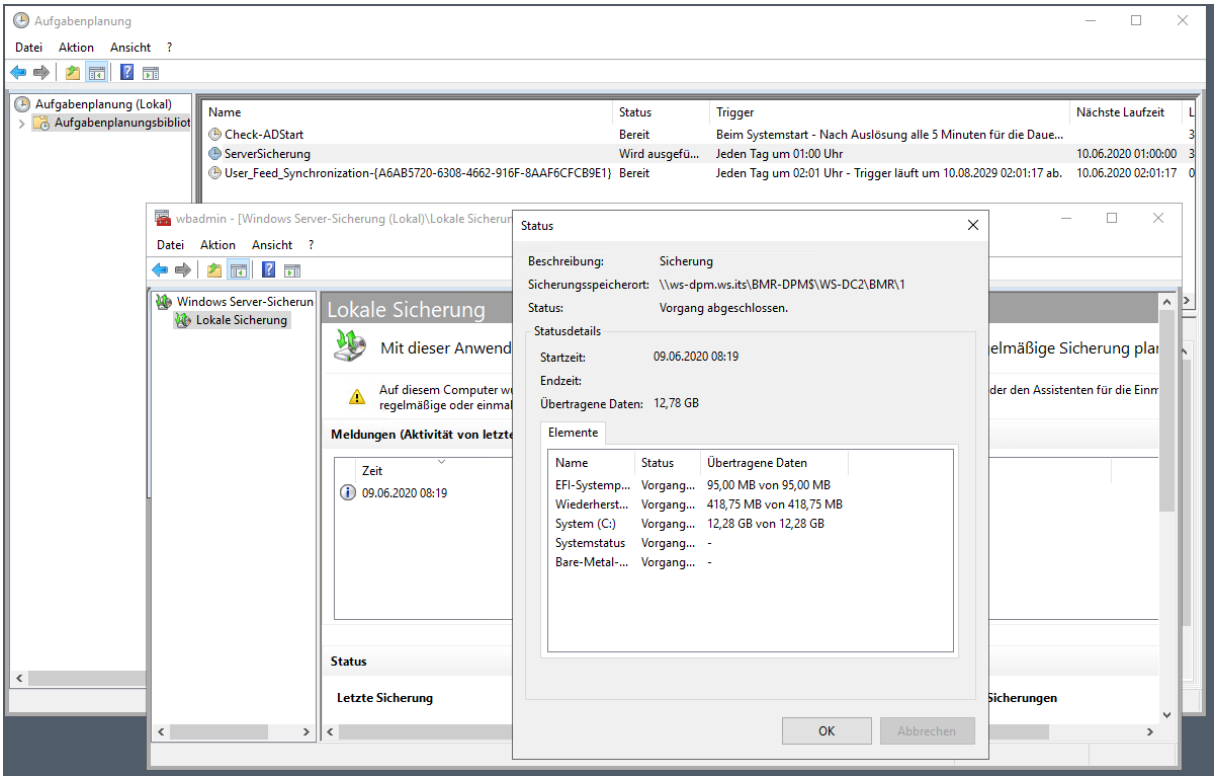
Server	JobName	StartZeit	EndZeit	Groesse	Status	Zeitplan	Slot
WS-WAC	BMR	--	--	0	OK	135	--
WS-RDS1	BMR	--	--	0	OK	135	--
WS-MX1	BMR	--	--	0	OK	135	--
WS-HV3	BMR	--	--	0	OK	135	--
WS-FS3	BMR	--	--	0	OK	135	--
WS-MON	BMR	--	--	0	OK	135	--
WS-CM	BMR	--	--	0	OK	135	--
WS-DC1	BMR	--	--	0	OK	135	--
WS-FS1	BMR	--	--	0	OK	135	--
WS-NPS1	BMR	--	--	0	OK	135	--
WS-HV1	BMR	--	--	0	OK	135	--
WS-DC2	BMR	??	??	0	Fehler	246	??
WS-HV2	BMR	01:00:01	01:05:02	27556	OK	246	4
WS-DC3	BMR	01:00:03	01:24:10	29394	OK	246	5
WS-FS2	BMR	01:40:02	01:48:15	22724	OK	246	1
WS-PRINT1	BMR	02:00:01	02:07:16	17937	OK	246	2
WS-RDS2	BMR	02:20:02	02:55:39	45216	Fehler -3	246	1
WS-DPM	BMR	02:50:02	02:58:02	33846	OK	246	5
WS-CA1	BMR	03:10:03	03:14:37	13798	OK	246	1
WS-ATA	BMR	03:30:01	03:45:23	43160	OK	246	3
WS-MX2	BMR	03:50:01	04:10:46	59134	OK	246	3

Statistik:

Sicherungsvolumen [MB]:	292765
Sicherungsdauer [min]:	191
Dauer effektiv [min]:	129
Geschwindigkeit [MB/min]:	2269

Daher starte ich sie nachträglich durch die Aufgabenplanung:

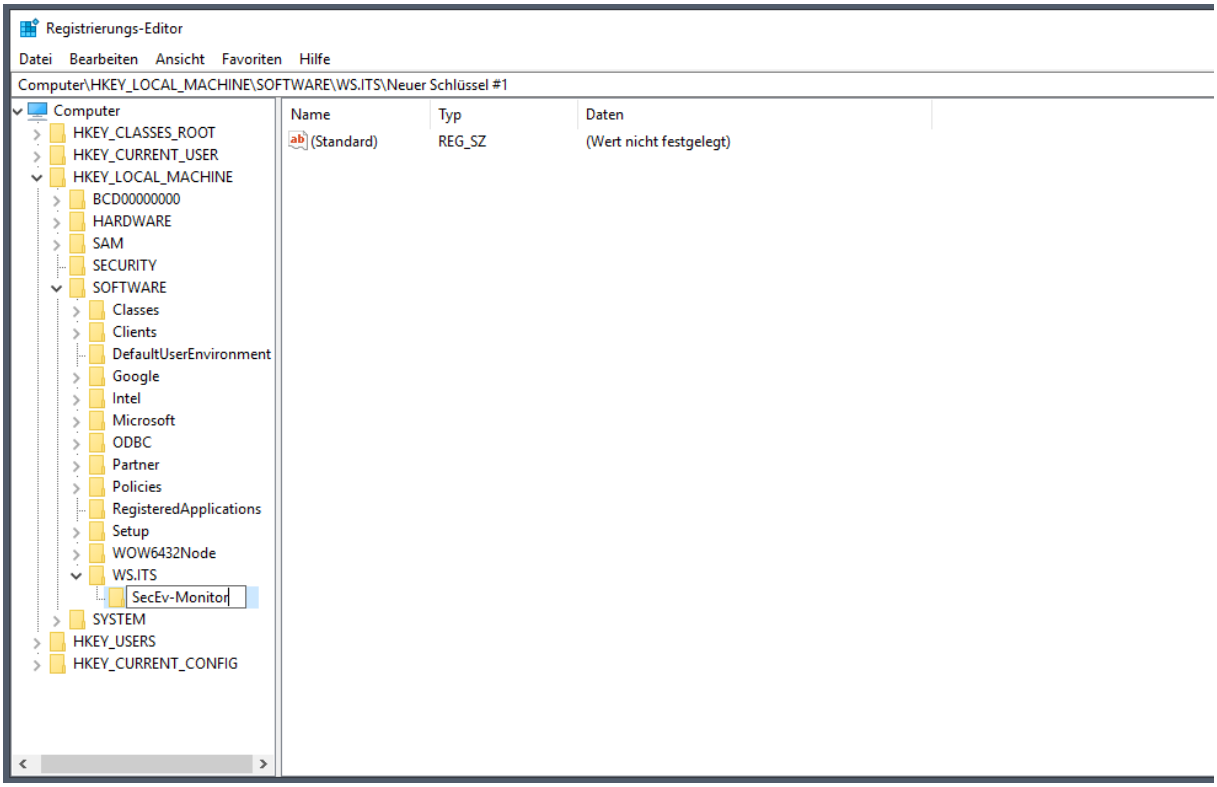




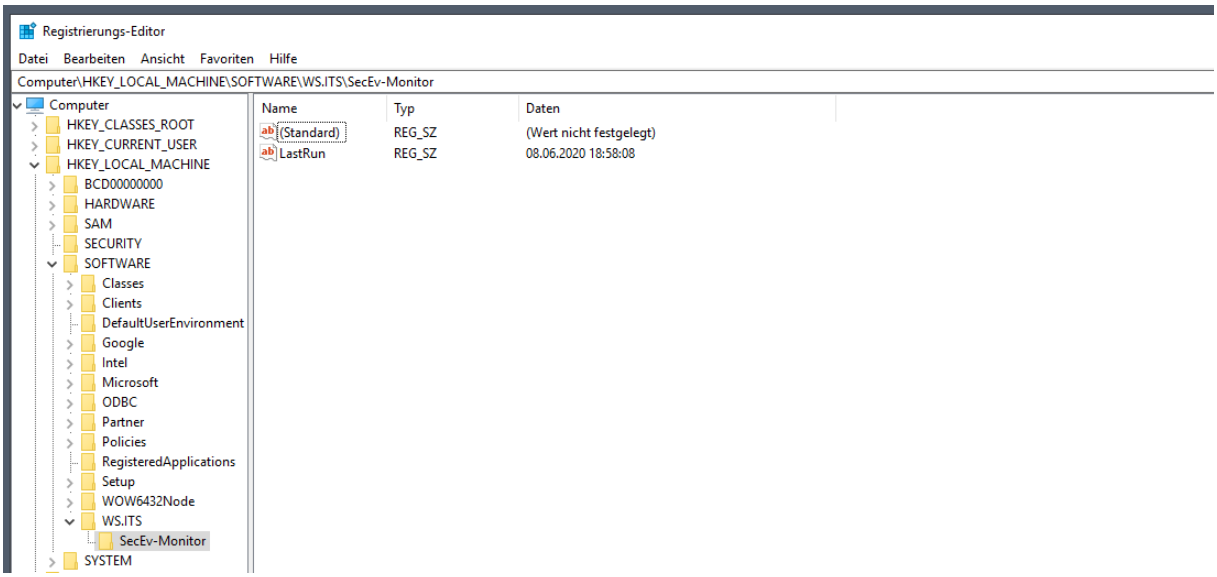
Der Vorgang dauert nur wenige Minuten. Mein neuer Domain Controller ist jetzt gesichert.

TroubleShooting des Monitorings

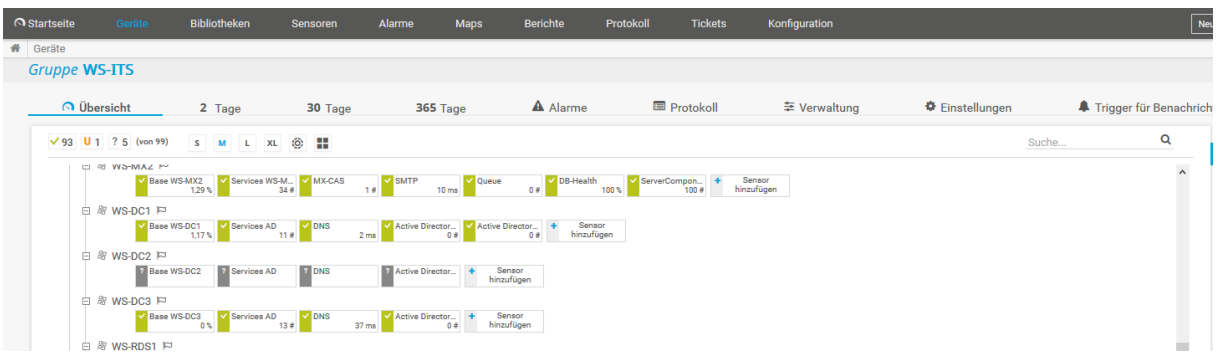
Mein PowerShell-Script „SecEv-Monitor“ soll fehlerhafte Anmeldeereignisse von allen Domain Controllern sammeln. Dabei merkt es sich den letzten Auslesezeitpunkt in der Registry. Das Script ist aber noch nicht fertig und die erforderlichen Schlüssel werden nicht automatisch erstellt. Das hole ich manuell nach:



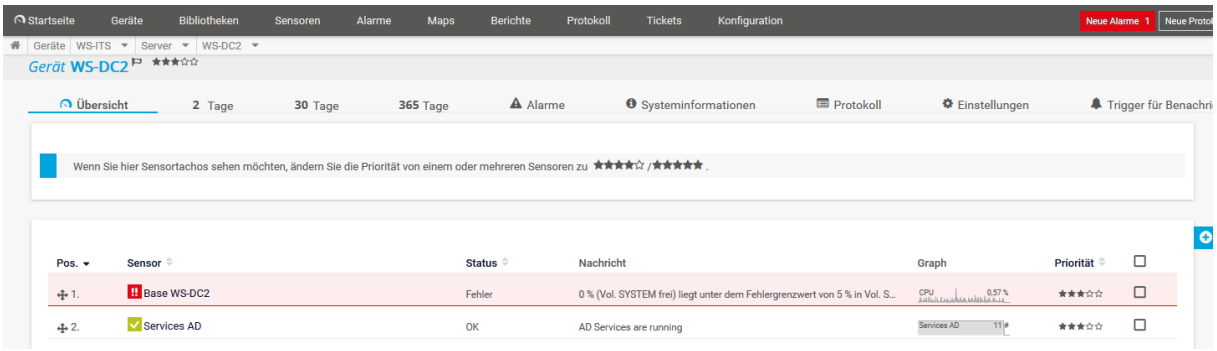
Nach einer Minute war das Script aktiv und hat erfolgreich die Zeit der Ausführung gespeichert:



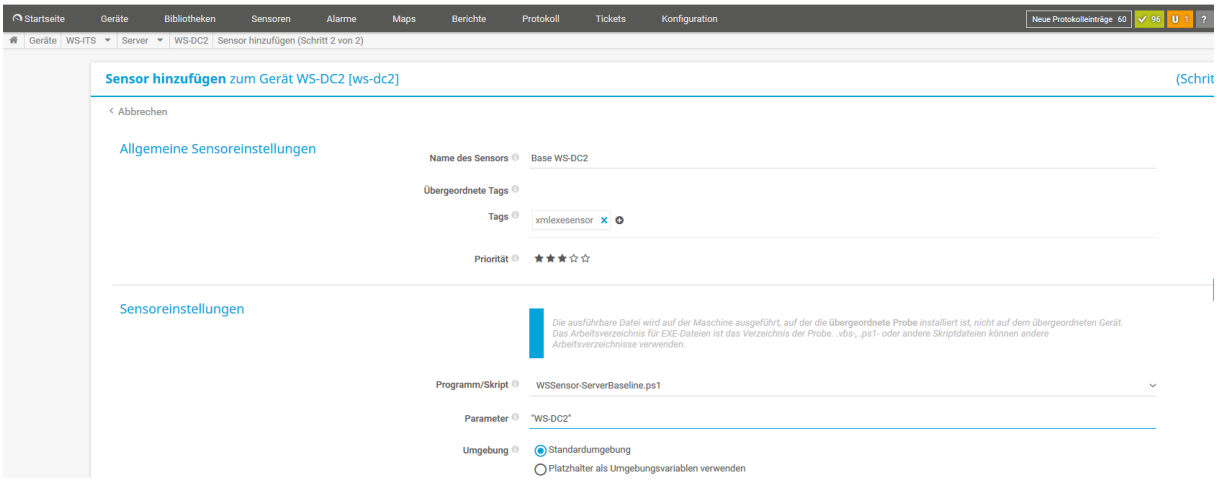
Im PRTG ist der Server immer noch pausiert. Ich beende die Pause. Dann dauert es etwas, bis die Sensoren gestartet werden:



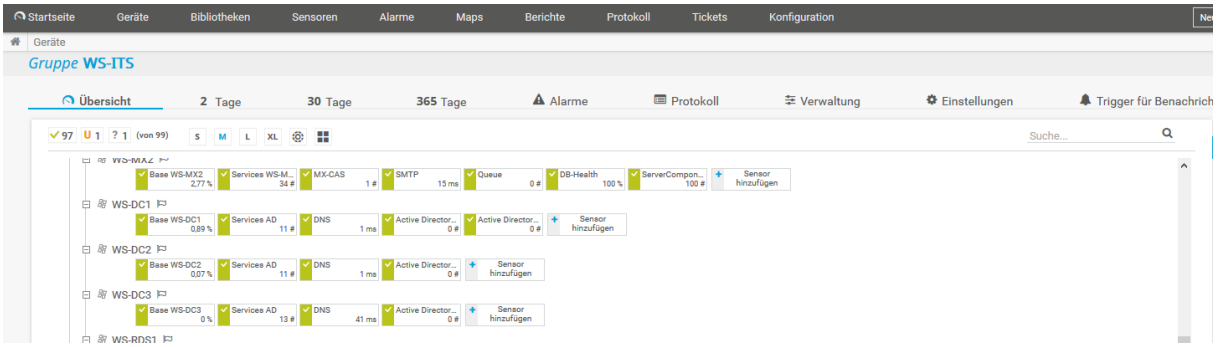
Wie beim anderen Server hängt mein selbstprogrammierter Sensor für die ServerBaseline:



Daher lösche ich den Sensor und erstelle ihn neu. Ich wähle den benutzerdefinierten Sensor „WSSensor-ServerBaseline.ps1“ und wende den Servernamen als Parameter an:

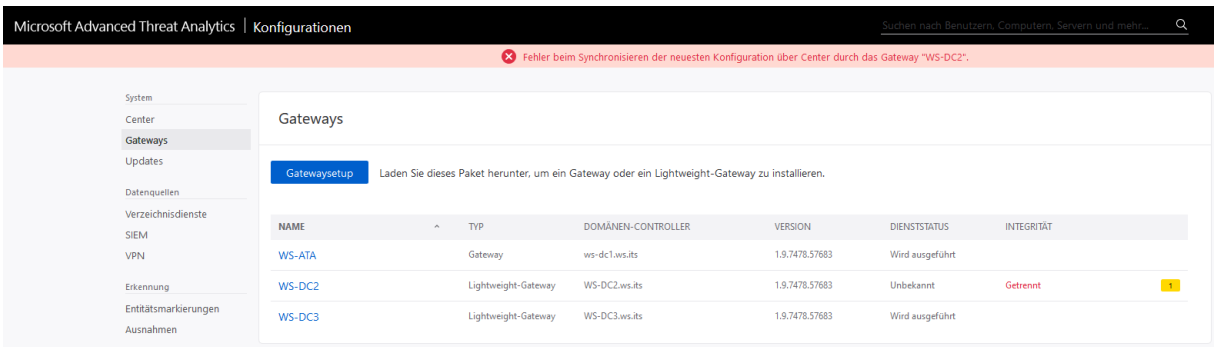


Nach einer Minute ist dann alles wieder grün:

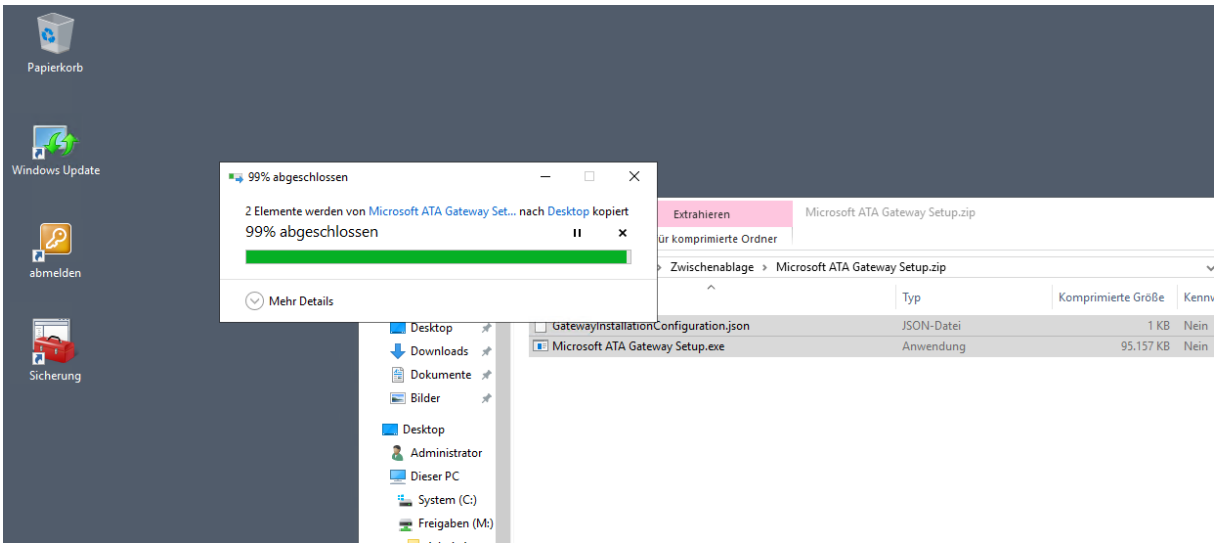


Integration ins ATA

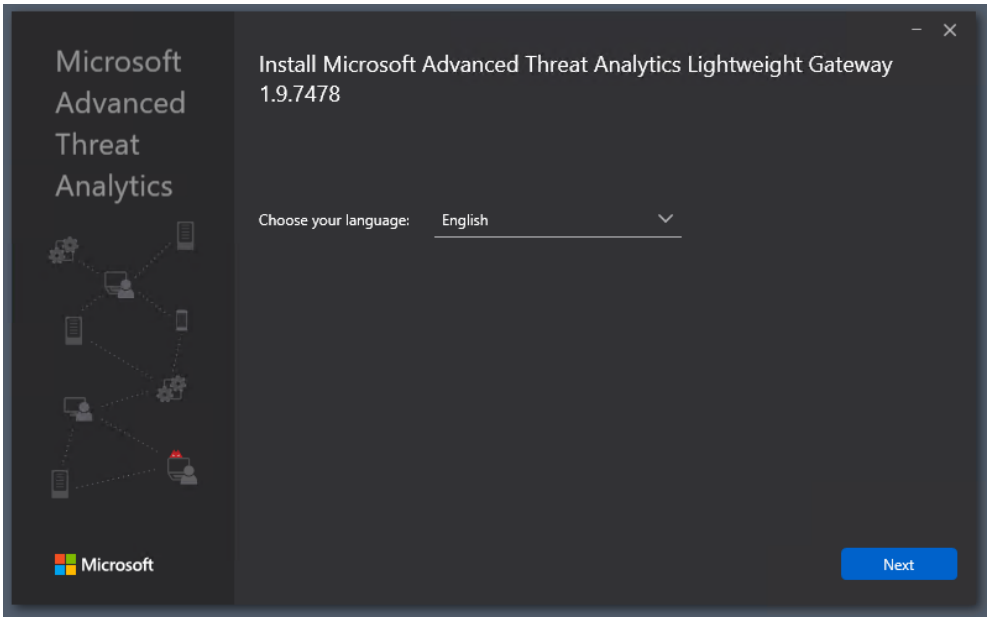
Nun fehlt noch der Wiederanschluss im Microsoft Advanced Threat Analytics Server. Das ATA vermisst den alten Server:



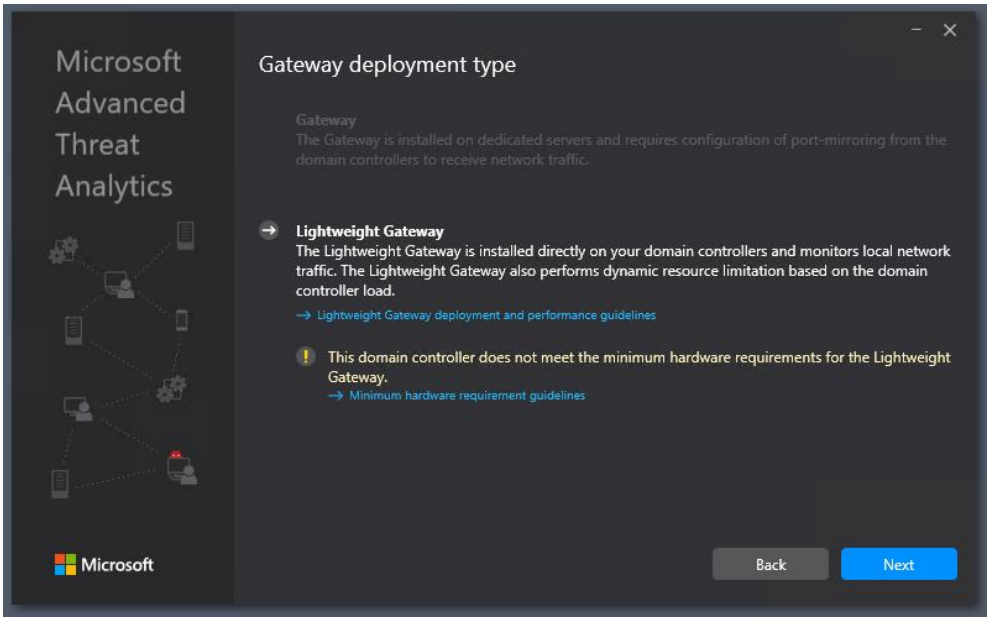
Ich lade mir aus der Konfigurationsseite das Gatewaysetup herunter und kopiere es auf den Server:



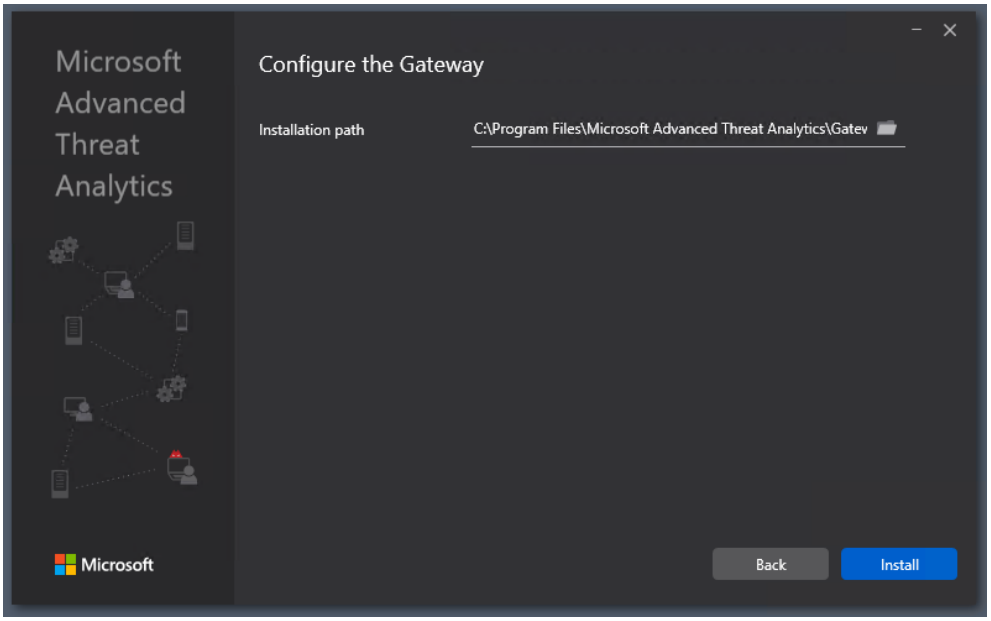
Die Ausführung ist recht einfach gehalten:



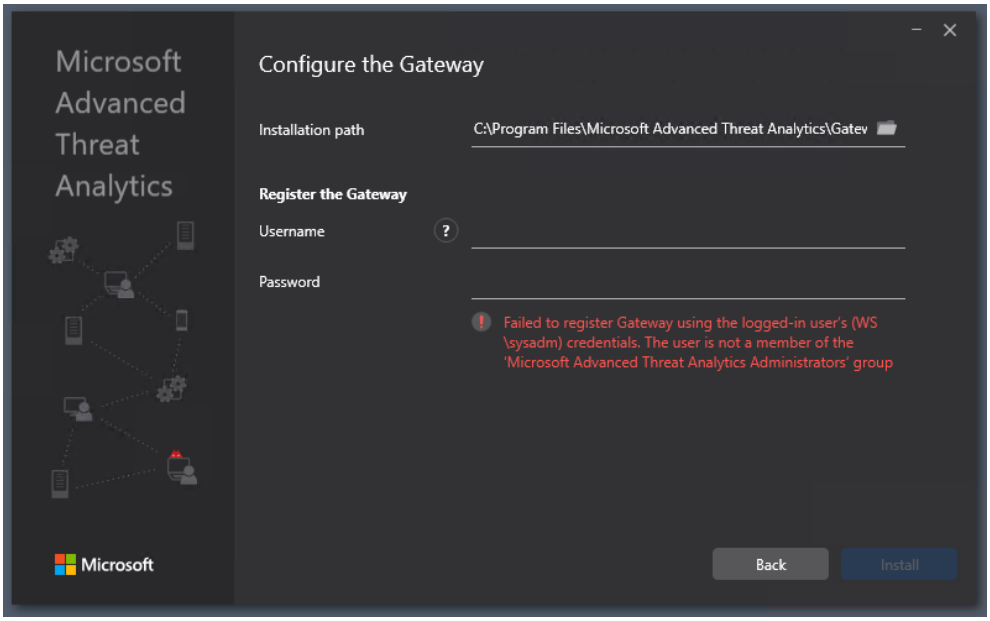
Der Server sollte mindestens 4GB Arbeitsspeicher haben. Ich habe den RAM im Hyper-V dynamisch zwischen 2GB und 6GB definiert. Das Setup liest aber nur den aktuellen Wert aus. Der scheint weniger als 4GB zu betragen:



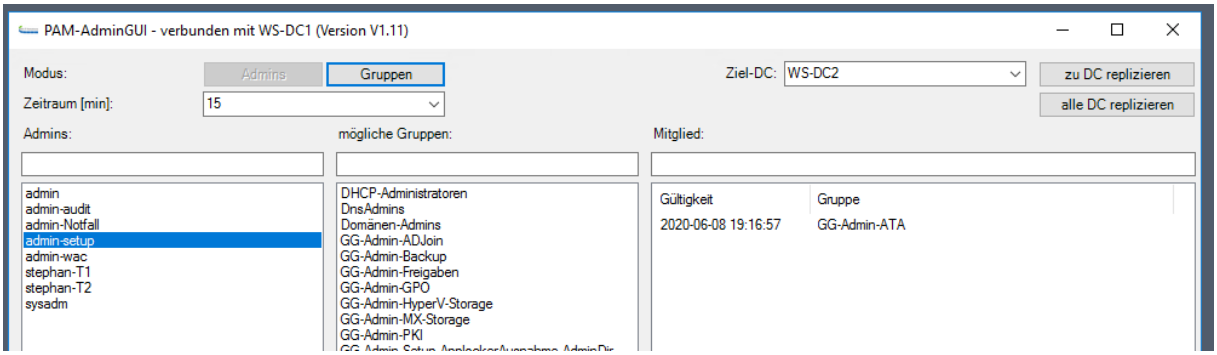
Ich bestätige die Warnung. Am Pfad verändere ich nichts:



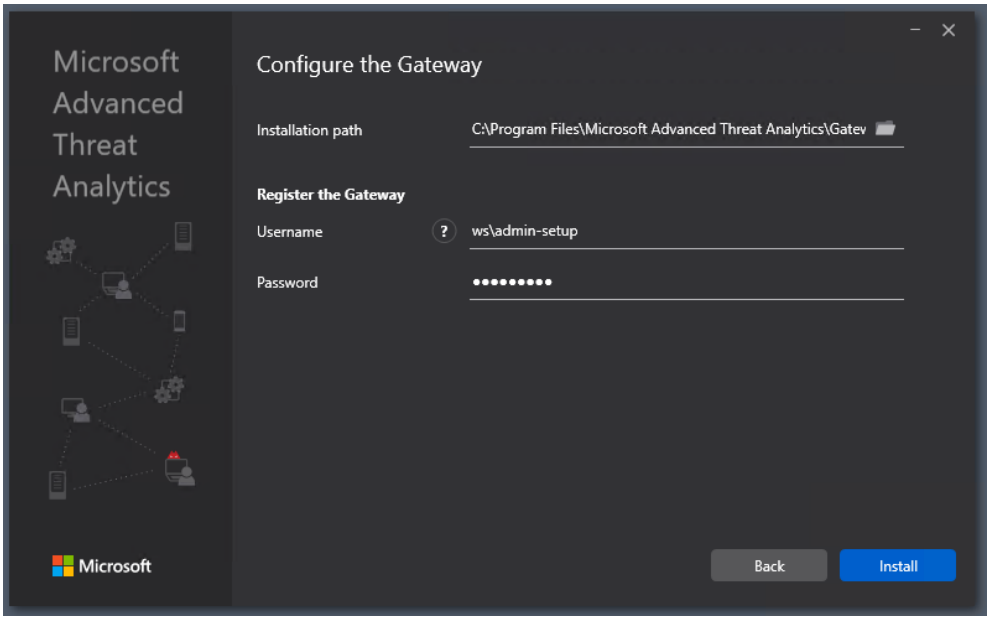
Beim Installieren wird der Domain Controller auch gleich im ATA registriert. Dabei muss der Benutzer in einer speziellen Sicherheitsgruppe Mitglied sein. Mein Account ist kein Mitglied:



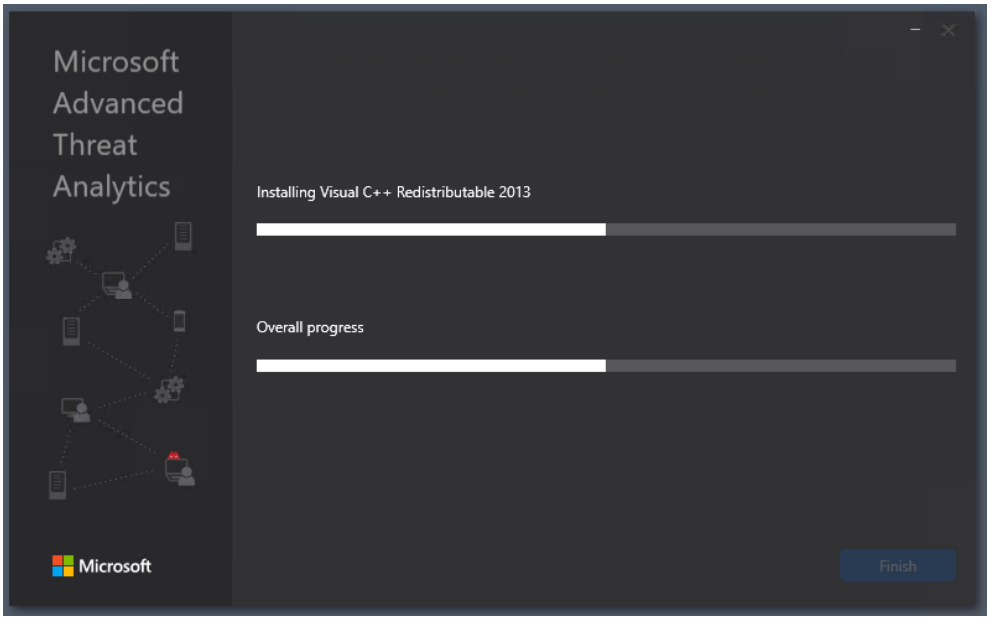
Aber mir wird eine alternative Anmeldung vom Setup angeboten. Daher richte ich einen Admin-Account temporär mit der entsprechenden Berechtigung aus. Die Active Directory Gruppe GG-Admin-ATA habe ich in die lokale Gruppe „Microsoft Advanced Threat Analytics Administrators“ auf meinem ATA-Server verschachtelt:

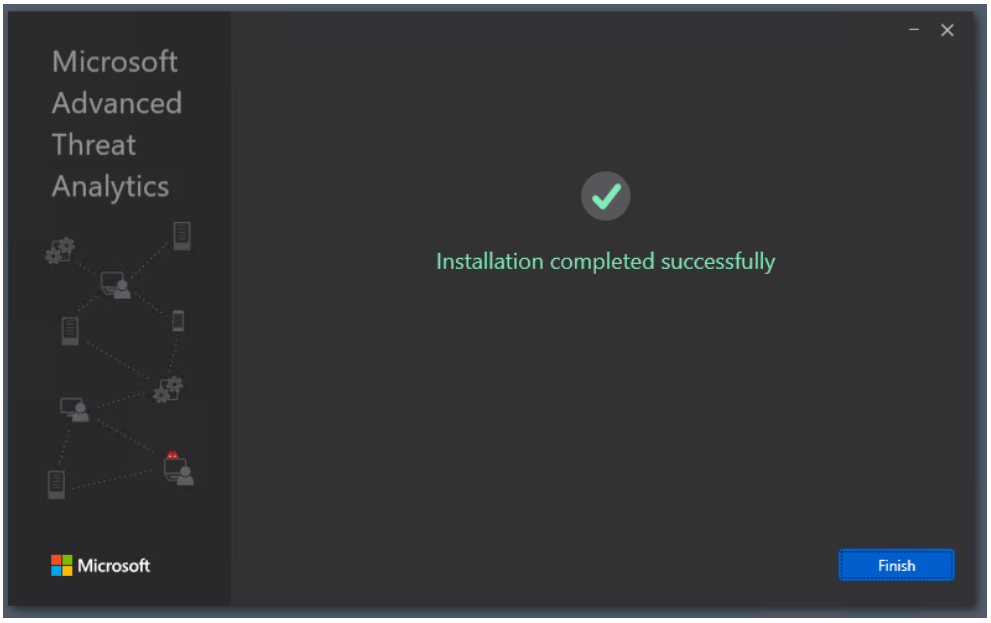


Mit dieser Anmeldung geht es weiter:

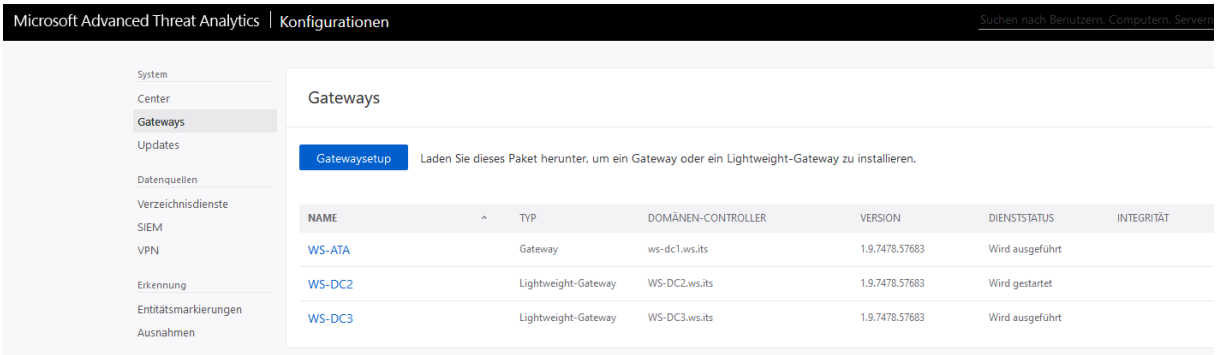


Das Setup braucht nur wenige Sekunden:

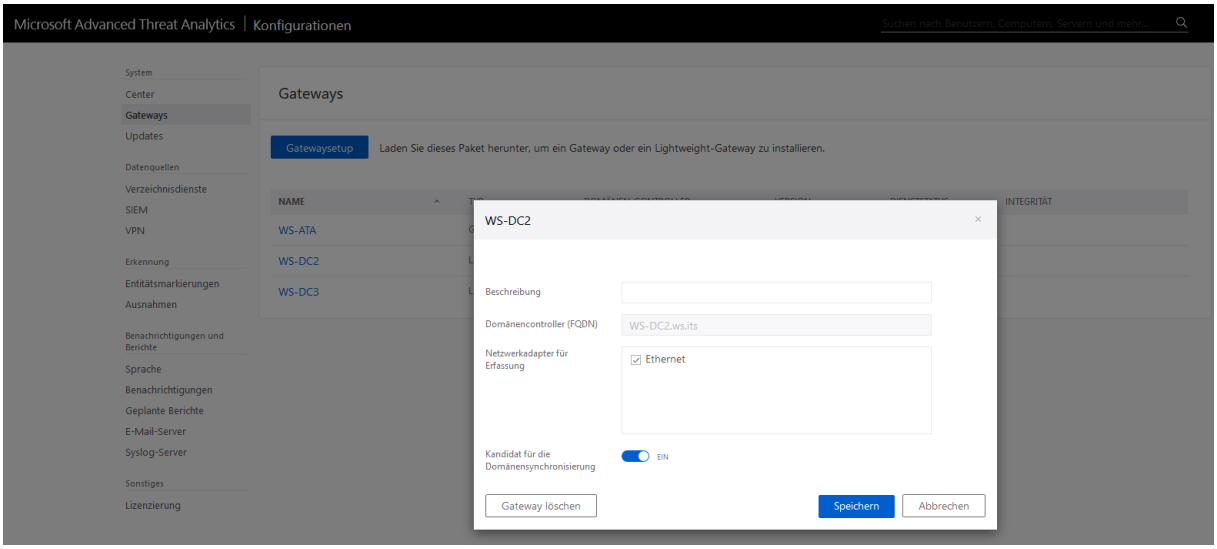




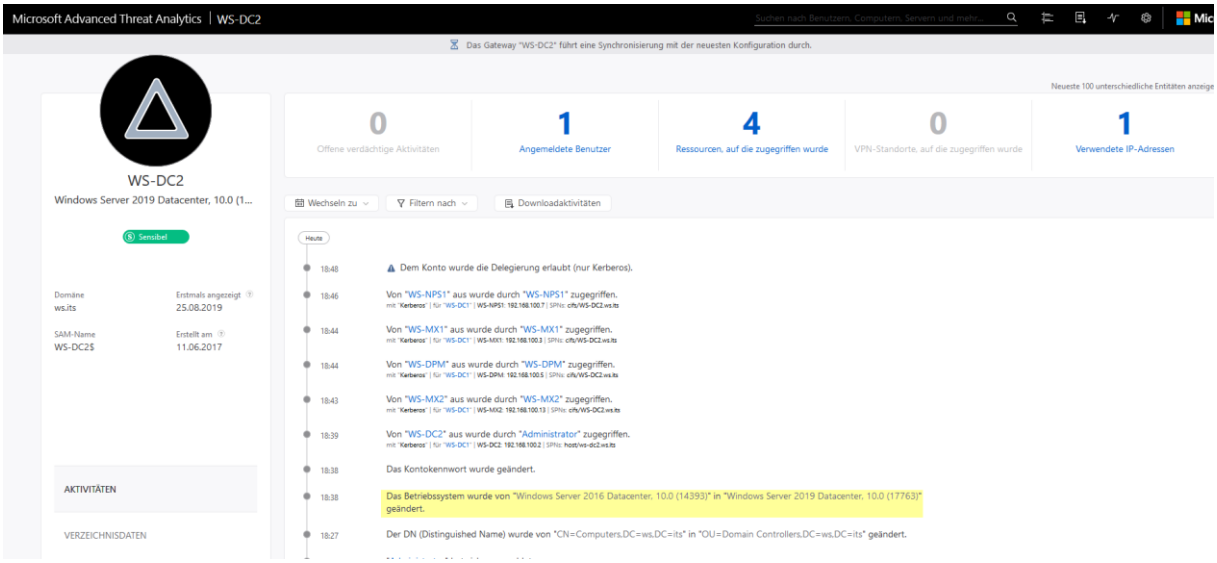
Danach meldet sich der Domain Controller im ATA. Die vorherige Identität wurde wiederverwendet:



Den neuen WS-DC2 aktiviere ich noch als „Kandidat für die Domänensynchronisierung“:



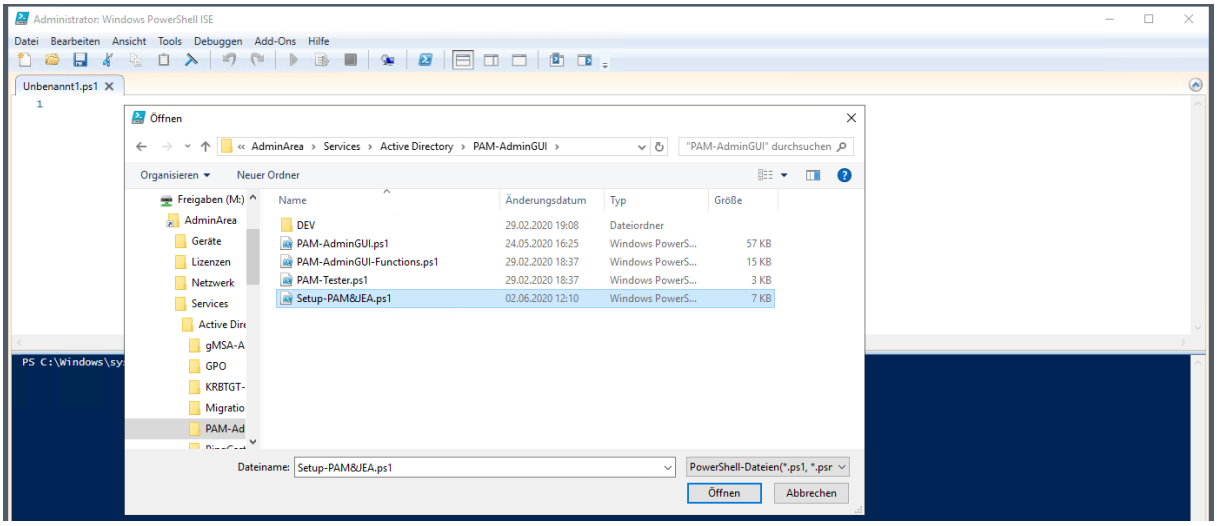
ATA hat den Wechsel des Betriebssystems mitbekommen und protokolliert:



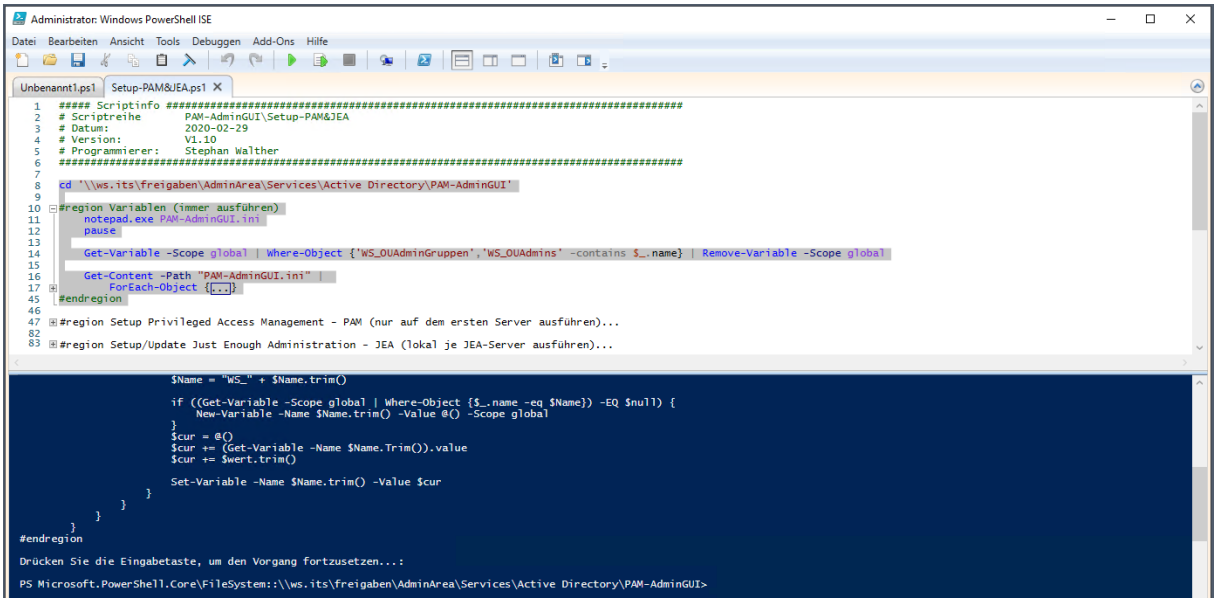
Jetzt erfasse ich wieder alle sicherheitsrelevanten Ereignisse.

PowerShell JEA-PAM-AdminGUI

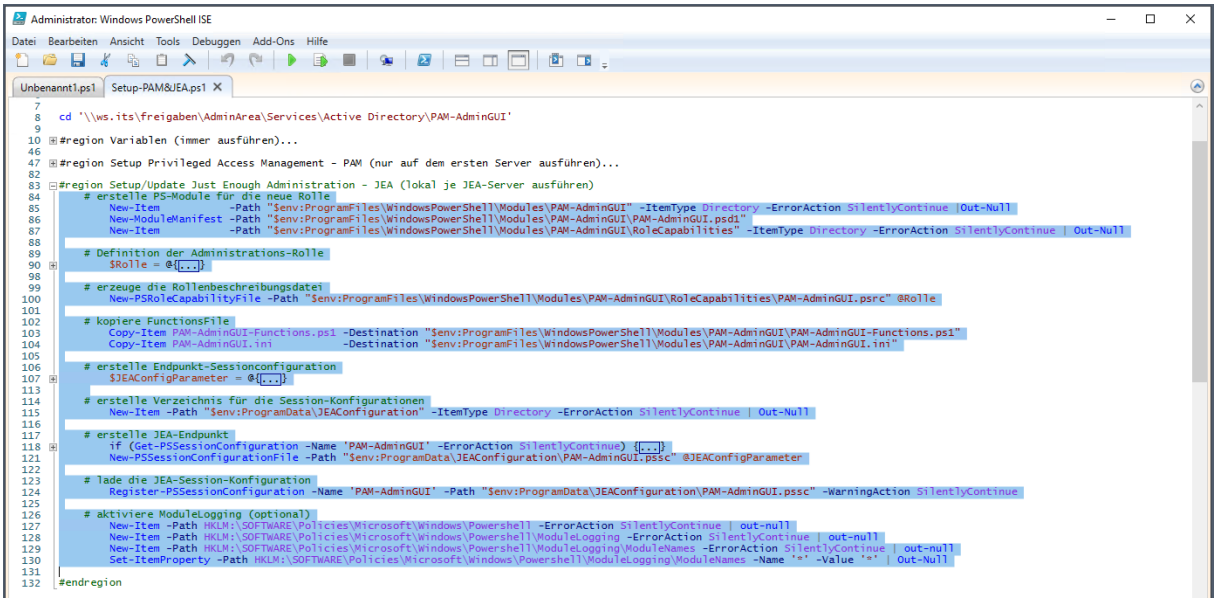
Mein PowerShell-Script „PAM-AdminGUI“ verwendet meine beiden Domain Controller WS-DC1 und WS-DC2 als JEA-Endpunkte für ein absolut minimales PowerShell-Remoting mit Just-Enough-Administration. Diesen Endpunkt muss ich aber zuvor konfigurieren. Dazu verwende ich mein PAM-AdminGUI-Setupscript:

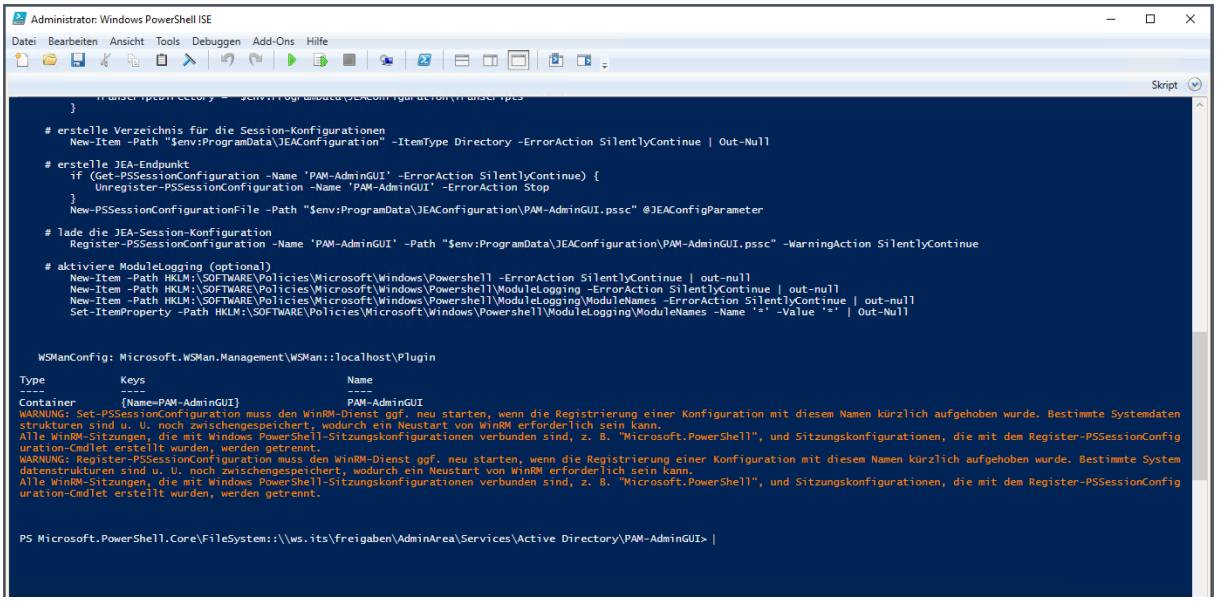


Zuerst lade ich den Regionsblock mit den Variablen:

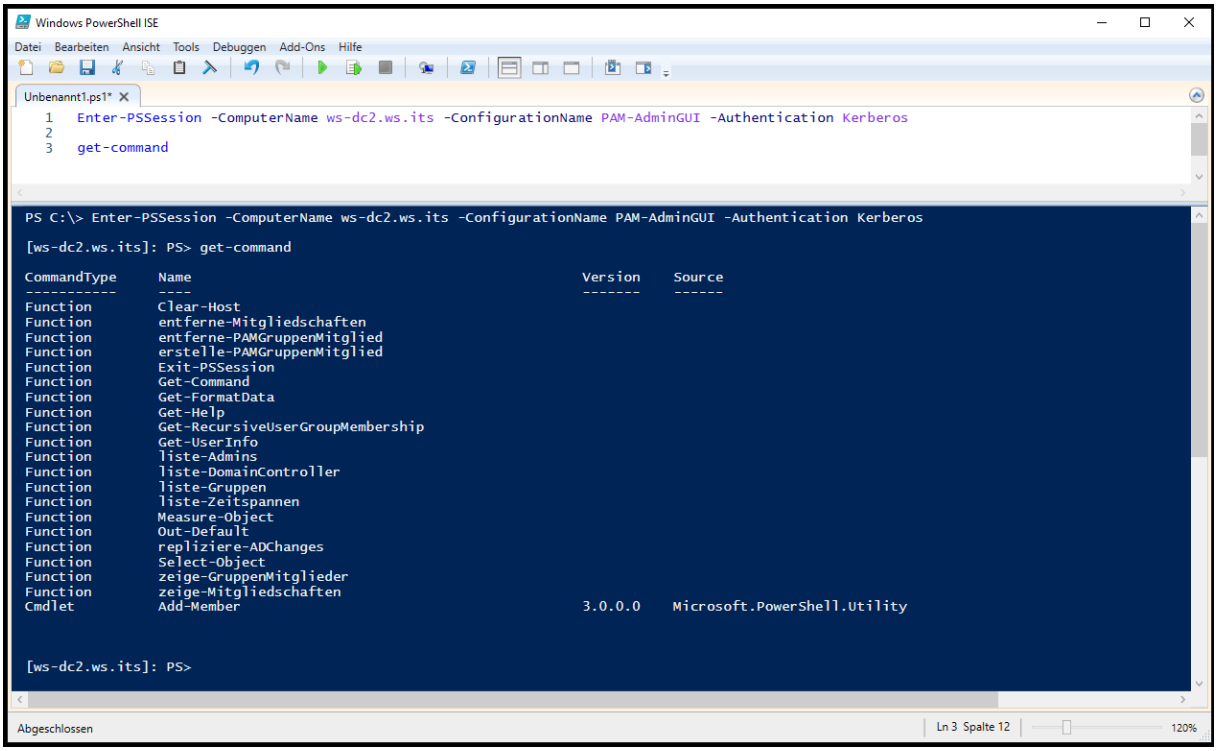


Und dann starte ich den Anweisungsblock, der den JEA-Endpunkt, die Konfiguration und die Proxyfunktionen erstellt:





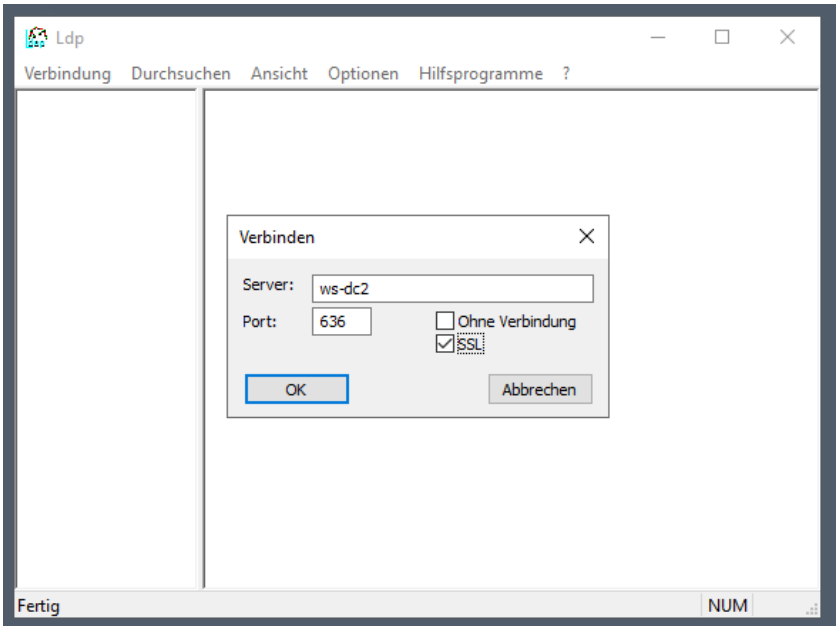
Vom Client aus rufe ich jetzt testhalber den Endpunkt auf. Mein Standardbenutzer hat das erforderliche Recht für den minimalen Verbindungsaufbau. Während der RemoteSession stehen mir nur die Proxyfunktionen zur Verfügung:



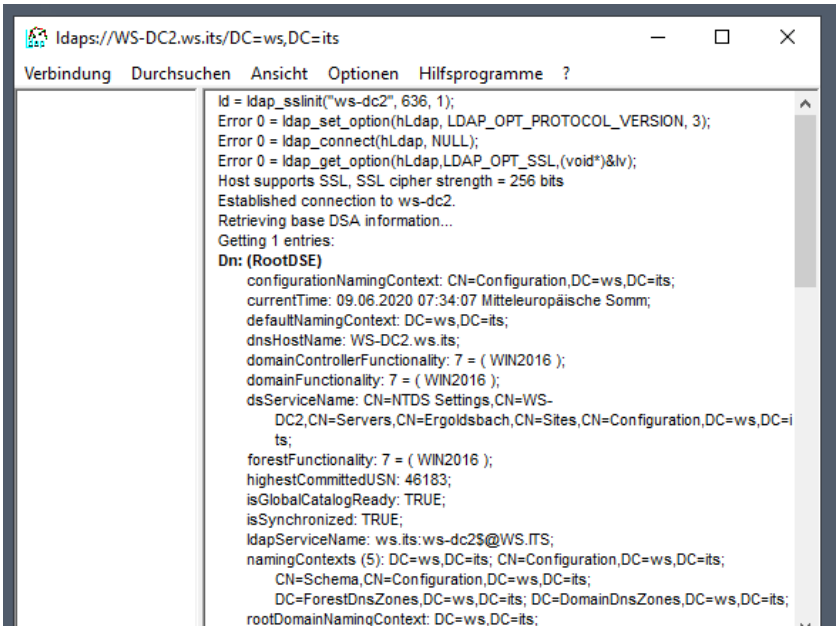
Auch das hat funktioniert.

Kontrolle LDAPS

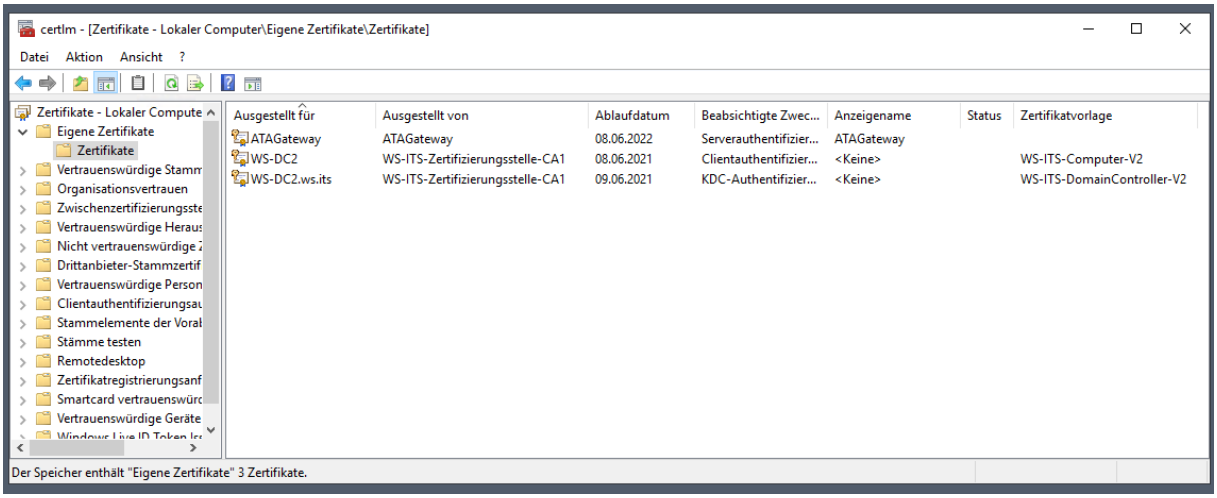
Alle Domain Controller sollten heute neben LDAP auch das sichere LDAPS anbieten. Das kann man recht einfach mit LDP.exe testen:



Der Server WS-DC2 kann via LDAPS angesprochen werden:



Denn er hat bereits über mein zentral konfiguriertes AutoEnrollment das dafür erforderliche Zertifikat von meiner Windows PKI erhalten:



Zusammenfassung

Nicht reibungslos, aber erfolgreich

Auch die zweite der drei Domain Controller Migrationen war nicht fehlerfrei. Aber jedes TroubleShooting ist auch ein Test der administrativen Fähigkeiten. Daher nehme ich solche Herausforderungen immer gerne mit.

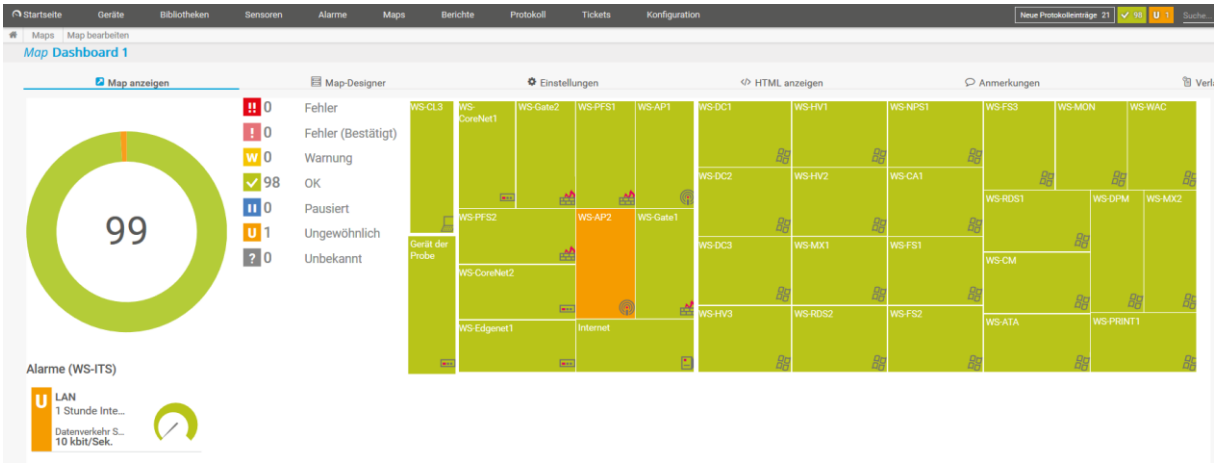
Einen Tag später erhalte ich wie gewohnt meine Mail des Server-Monitorings. Darin ist auch eine Sektion mit einer Zusammenfassung der Eventlogs enthalten. Die Anzahl der Fehler und Warnungen ist sehr überschaubar und liegt absolut im normalen Bereich. Die anderen Server haben den neuen Domain Controller angenommen und arbeiten friedlich weiter:

WS-DC2	WS-DC2.ws.its;ws.its	364	06/09/2021 02:39:19	WS-ITS-Zertifizierungsstelle-CA1
WS-DC2	WS-DC2.ws.its	364	06/08/2021 18:29:29	WS-ITS-Zertifizierungsstelle-CA1

Zusammenfassung der Ereignisse (24h)

Server	Information	Warning	Error
WS-HV1	17010	16	1
WS-ATA	15749	3	8
WS-HV2	17208	28	5
WS-FS1	15695	2	0
WS-RDS1	15696	0	0
WS-MX2	26529	355	30
WS-MX1	26577	374	45
WS-HV3	16912	1	0
WS-NPS1	15658	0	0
WS-FS3	15796	0	0
WS-DPM	15957	14	18
WS-DC3	15802	0	2
WS-DC2	16223	44	15
WS-CA1	15717	2	0
WS-RDS2	15784	9	6
WS-CM	15685	1	1
WS-WAC	15710	3	0
WS-FS2	15819	5	8
WS-MON	10429	0	0
WS-PRINT1	15670	0	7
WS-DC1	15975	8	2

Genauso sieht es auch mein Live-Monitoring PRTG:



Damit betrachte ich diese Migration als abgeschlossen.