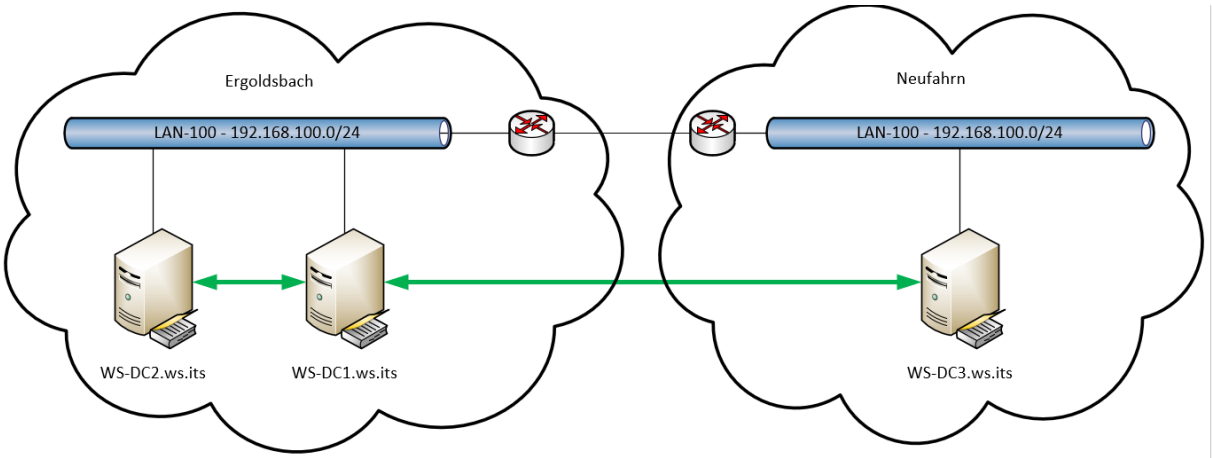
Inhalt

Zielsetzung

IST-Situation

Heute ist der letzte Domain Controller WS-DC3 an der Reihe und wird auf Windows Server 2019 aktualisiert. Die beiden anderen DCs laufen bereits mit diesem Betriebssystem.

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 Nebenstandort Neufahrn ist der Domain Controller alleine. Es gibt also keine Ausfallsicherheit. Alle Clients und Server verwenden daher den WS-DC1 im Standort Ergoldsbach als sekundären DNS-Server. Da auch der DHCP-Service auf dem WS-DC3 keine Verfügbarkeitsfunktion (DHCP-Failover) erhalten hat, sind die Lease-Zeiten entsprechend lang gewählt worden.

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

Alle Domain Controller sind 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-DC3 von Windows Server 2016 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.

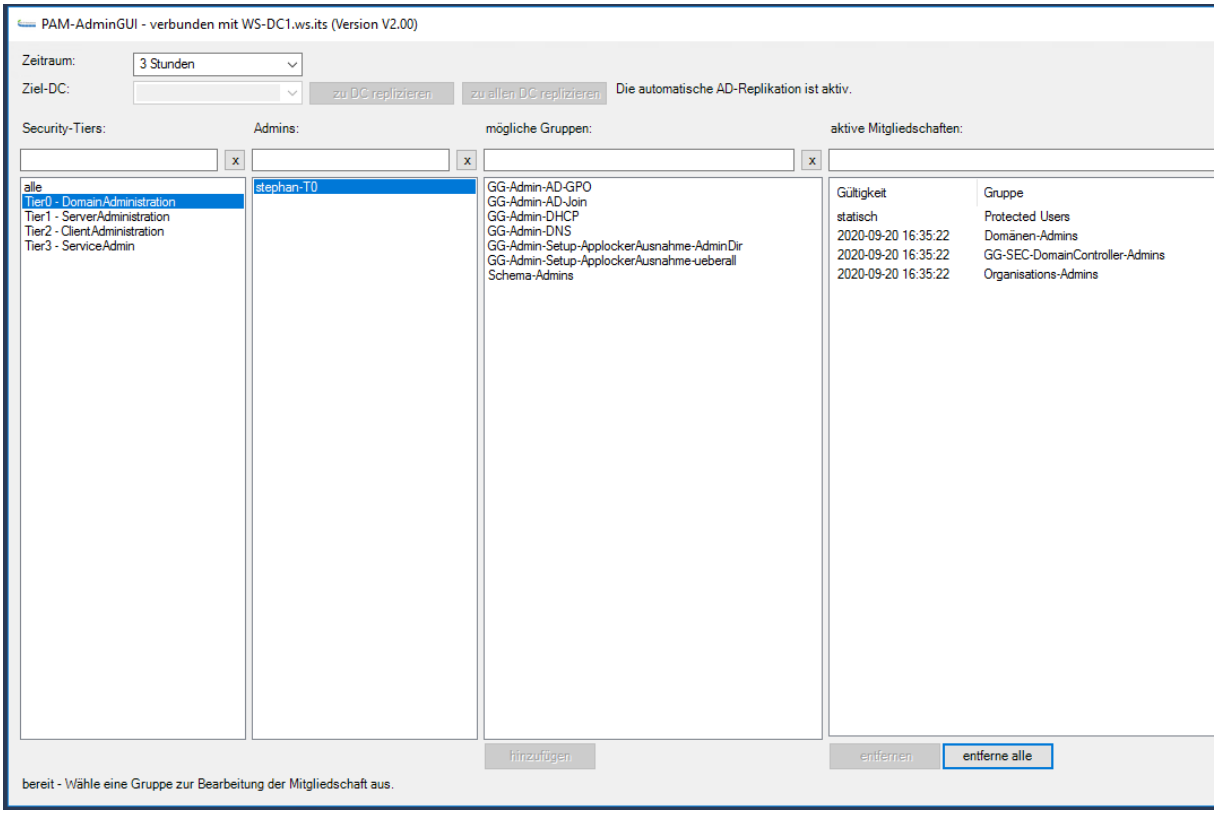
Migrationsplan

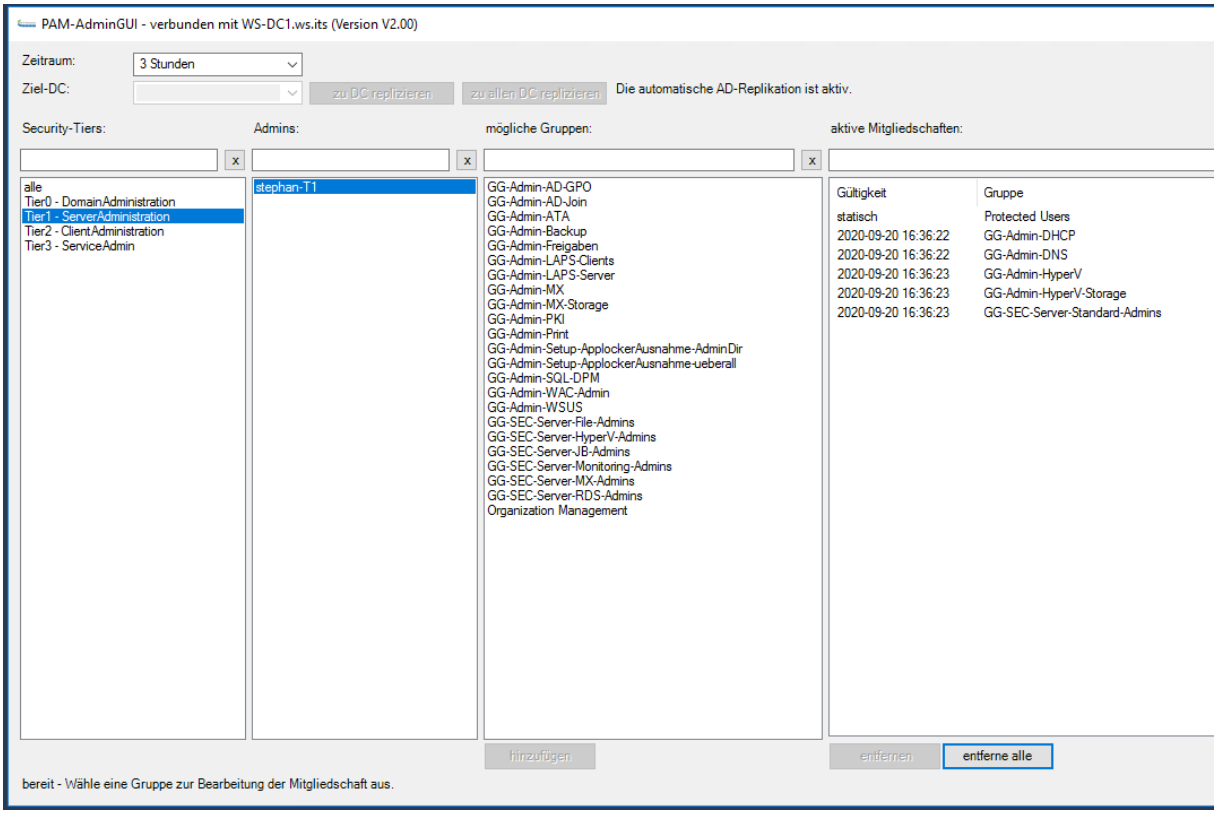
Wie bei den ersten Servern auch kommt hier ein Wipe & Load Szenario zur Anwendung: Zuerst entferne ich den alten Server aus meiner Infrastruktur. Anschließend installiere ich einen neuen Server mit den gleichen Namen und der gleichen IPv4-Konfiguration und richte die Services wieder ein.

Vorbereitung

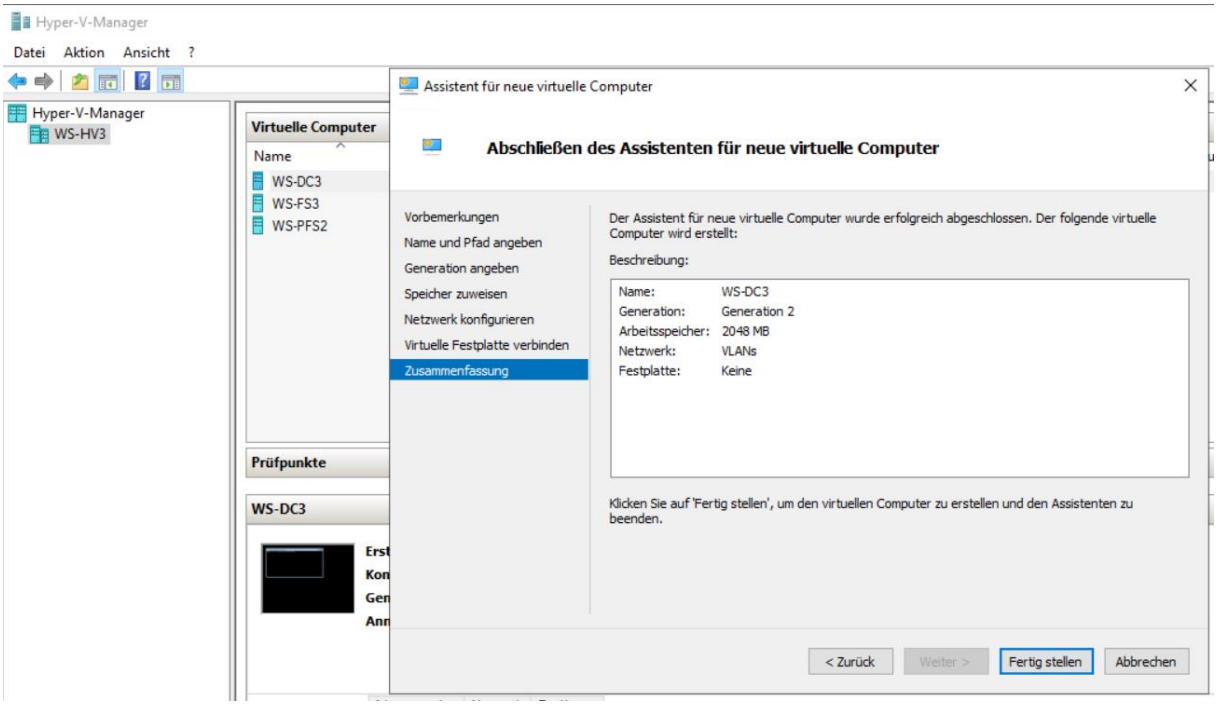
Aufbau der neuen VM

Ich beginne mit der Berechtigung meiner beiden Adminkennungen, da ich ein Zero-Privilege-Modell verwende: meine Adminkennungen haben 24/7 keine Berechtigungen. Diese werden durch mein PAM-Tool erst bei Bedarf und dabei auf Zeit vergeben:

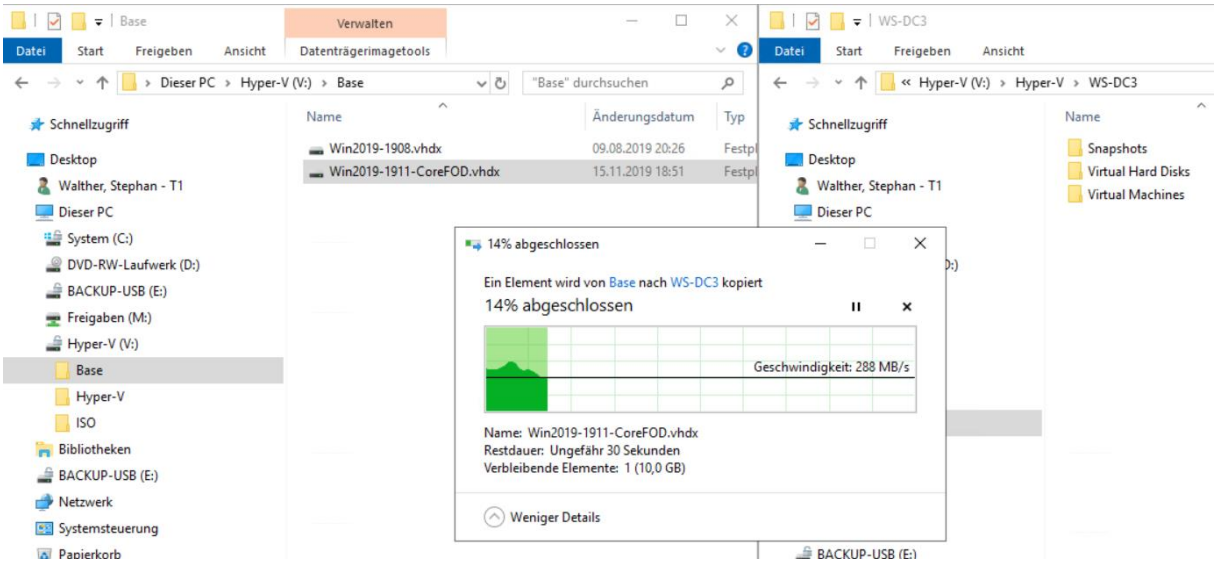




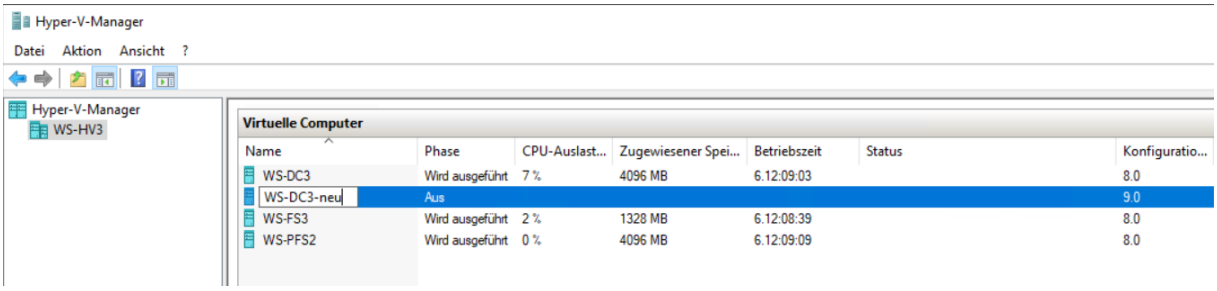
Um einen schnellen Austausch zu ermöglichen, stelle ich das neue Betriebssystem in einer neuen VM auf dem Hyper-V-Server WS-HV3 im Standort Neufahrn bereit:



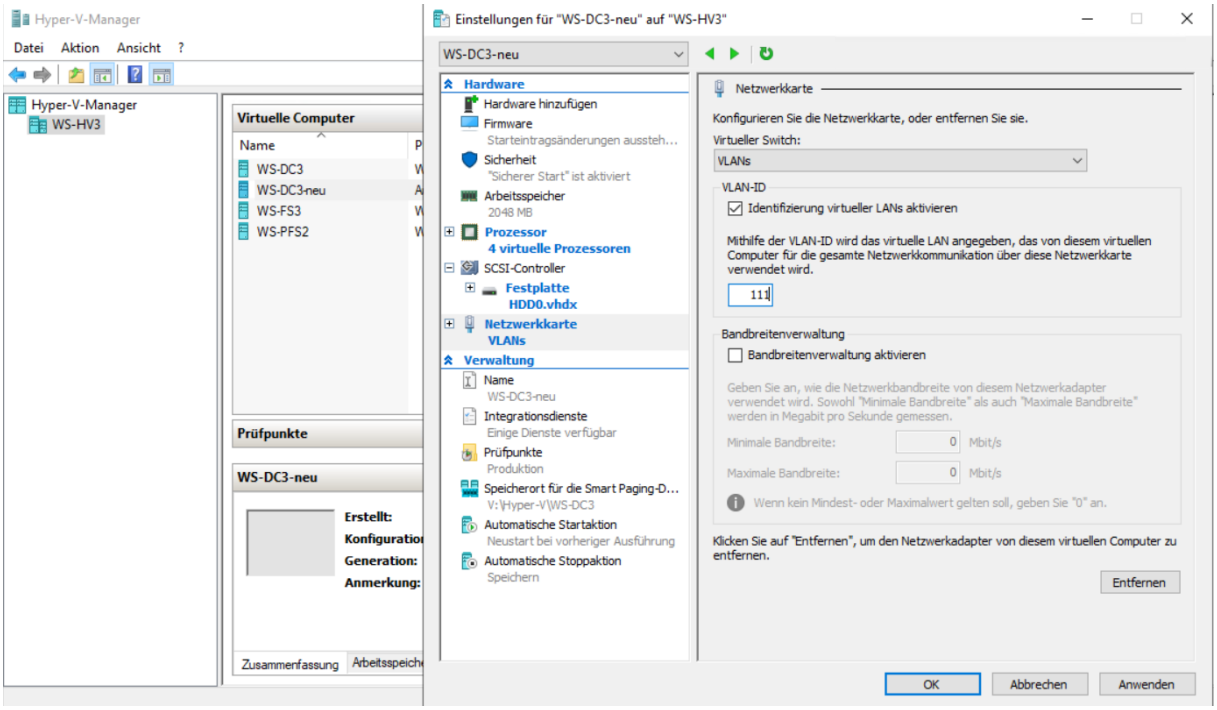
Vor einigen Wochen hatte ich bereits ein Betriebssystem-Image in einer VHDX-Datei vorbereitet. Ich kopiere die Datei in das Verzeichnis der virtuellen Maschine:



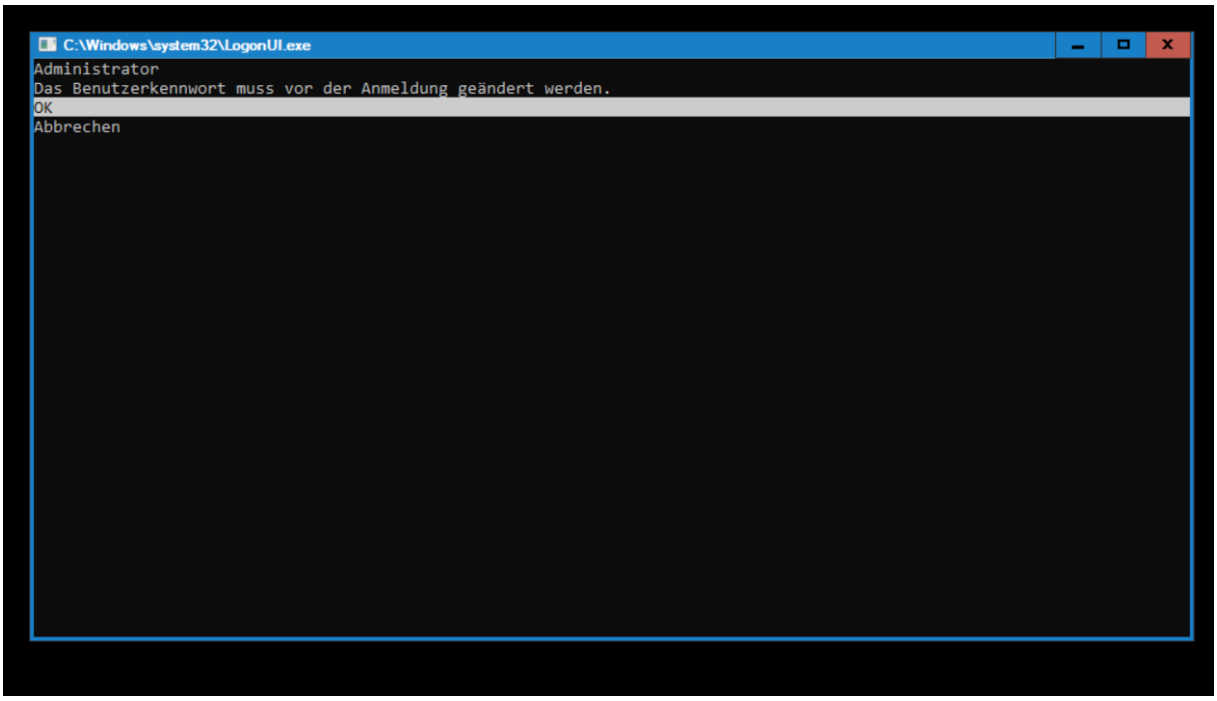
Der neue Servername entspricht dem alten. Damit ich nicht durcheinander komme, benenne ich die neue VM einfach um:

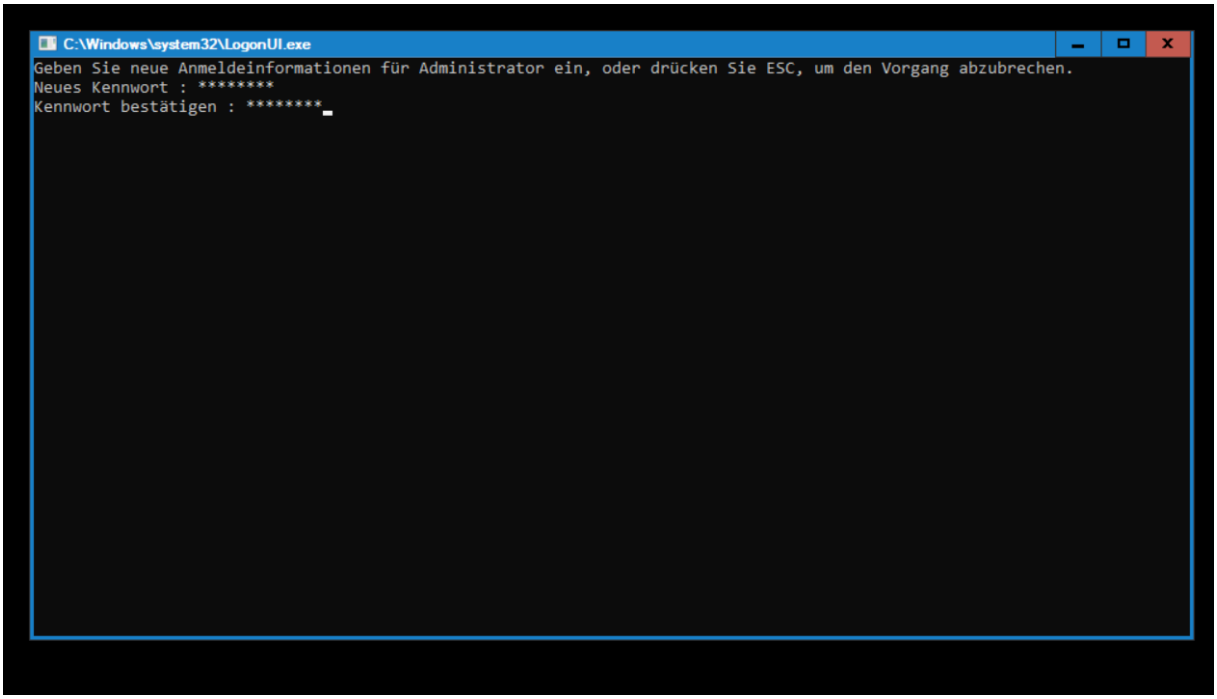


Die Server haben ein eigenes VLAN. Das ermöglicht mir eine gezielte Filterung und Überwachung der Netzwerkverbindungen. Da das Servernetz (VLAN 110) nicht ins Internet darf, patche ich den Server ins Client-VLAN 111:

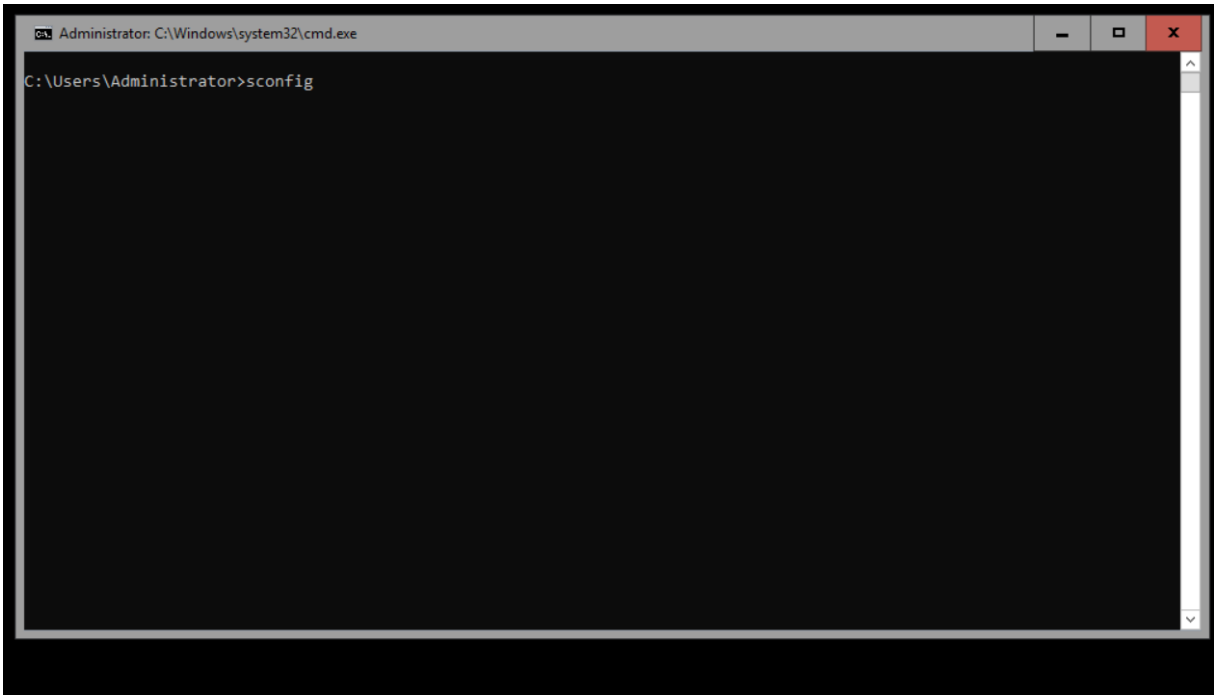


Nach dem Einschalten der VM läuft das Out-Of-Box-Experience-Setup durch. Abschließend muss ich das neue, lokale Administrator-Passwort eingeben:

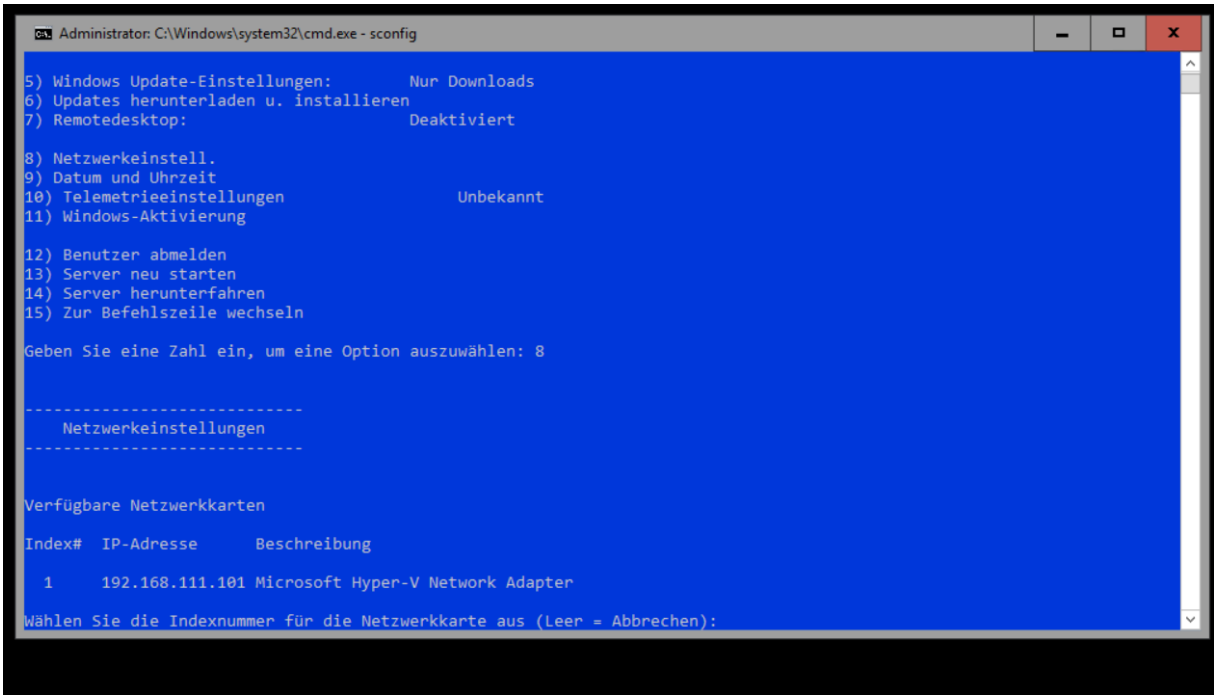




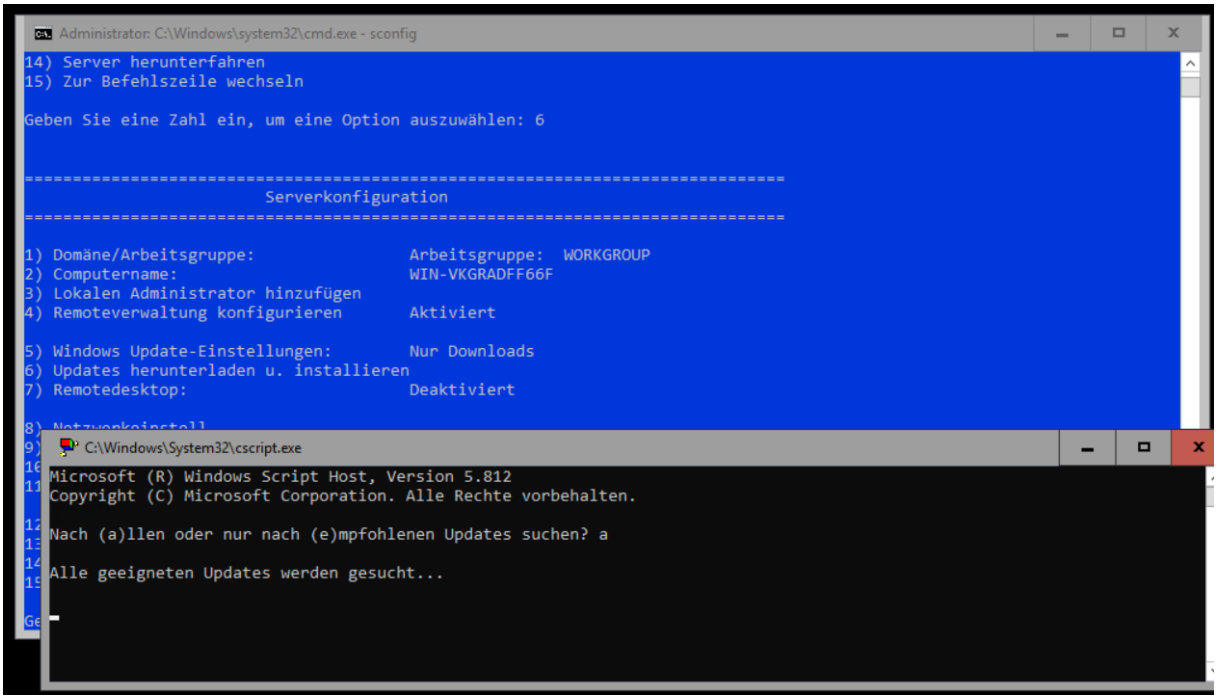
Das Betriebssystem habe ich als Server Core ohne grafische Oberfläche installiert. Daher geht es mit sconfig weiter:

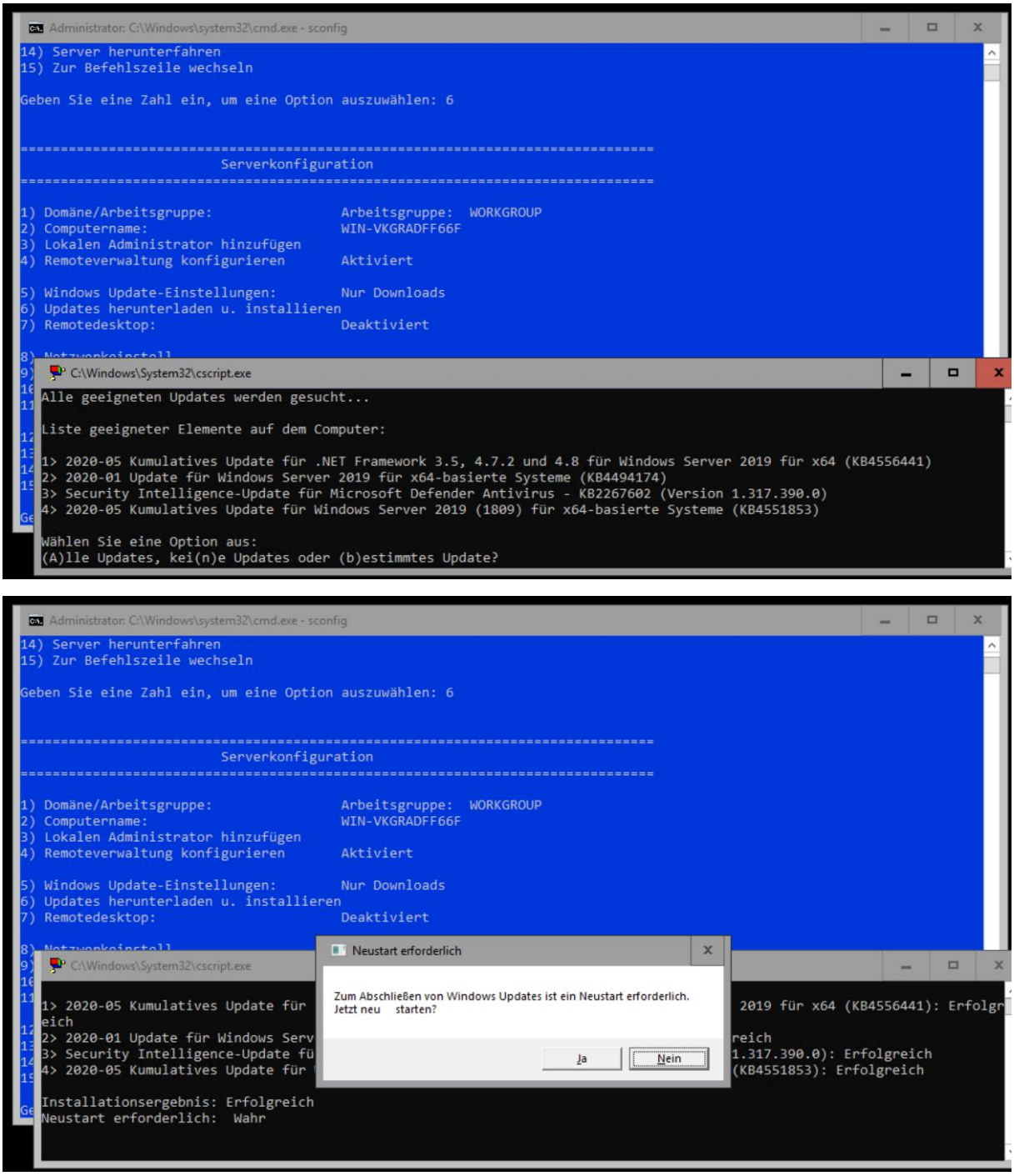


Zuerst kontrolliere ich die Netzwerk-Konfiguration. Der neue Server hat eine IPv4 vom DHCP-Server erhalten:

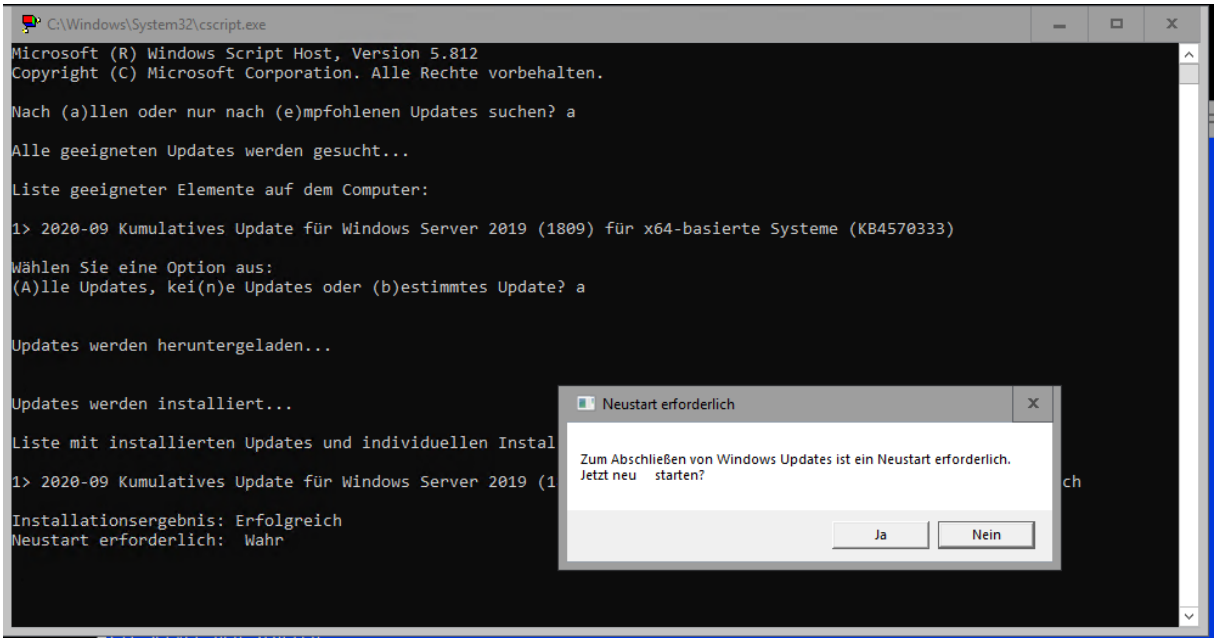


Damit kann das System das Internet erreichen. Ich starte die Aktualisierung des Betriebssystems:





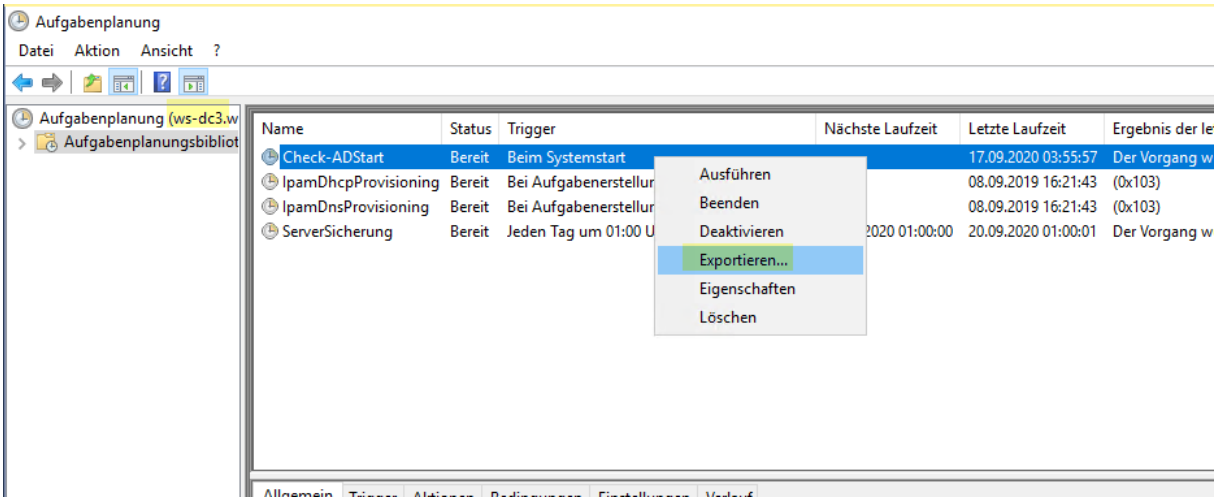
Auch wenn es nur eine Kommandozeile ist: Mit sconfig ist die Ersteinrichtung ein Kinderspiel! Das Patchlevel scheint mir aber mit der Version 2020-05 etwas alt zu sein. Daher starte ich nach dem Neustart einen weiteren Lauf:



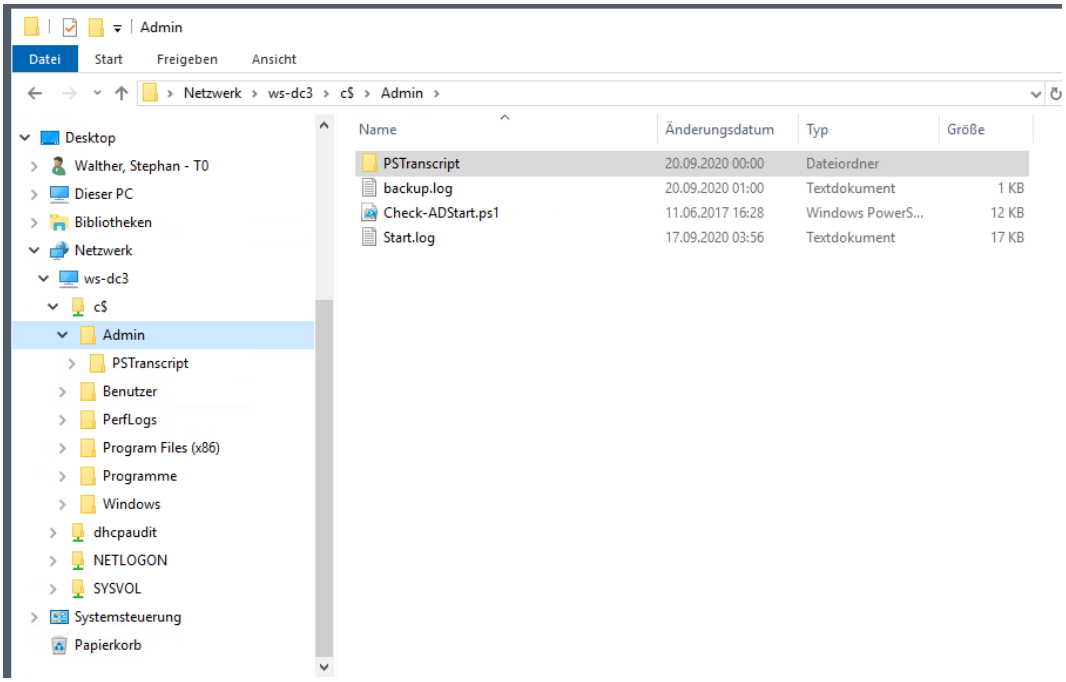
Das sieht schon besser aus. Da der Server eh gerade ins Internet kommt, aktiviere ich gleich noch das Betriebssystem.

Sichtung von Informationen auf dem alten Server

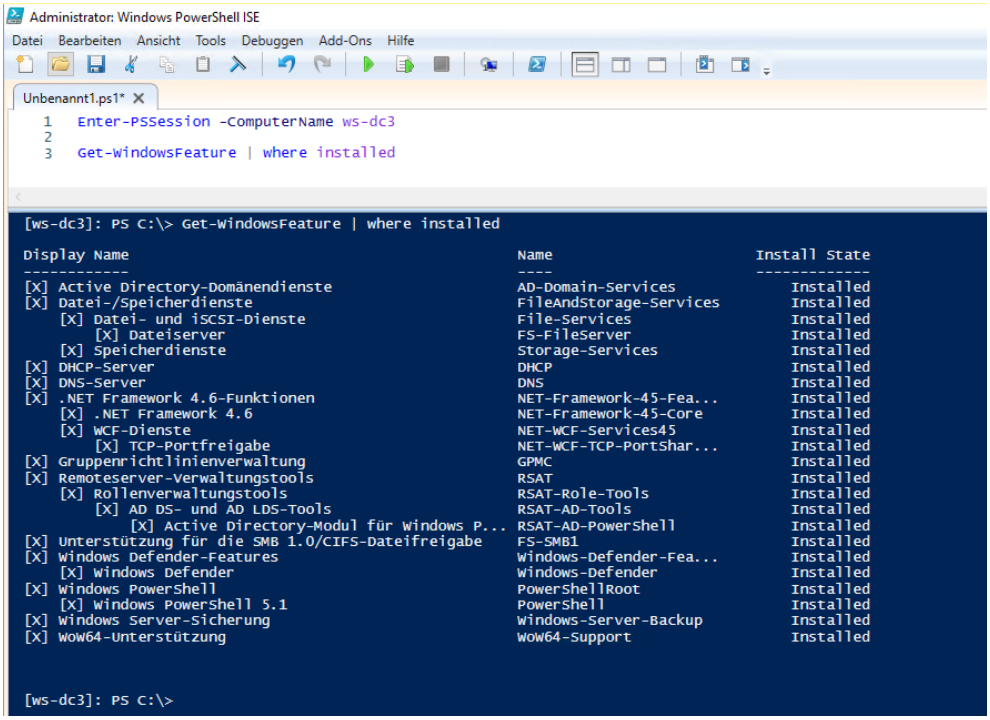
Wie bei allen Servern schaue ich mir die geplanten Aufgaben an. Die Aufgabe „Check-ADStart“ startet ein PowerShell-Script, dass den Start der Services nach einem Betriebssystem-Neustart verifiziert. Den Task exportiere ich in das Dateisystem:



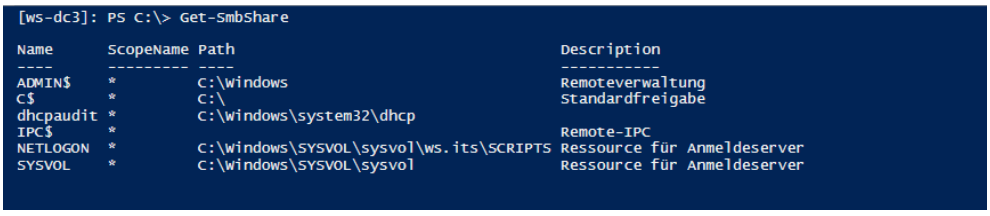
Auf dem Systemdatenträger selber ist nicht viel zu finden. Die relevanten Verzeichnisse und Dateien kopiere ich in mein zentrales Admin-Share:



Jetzt prüfe ich, welche Rollen und Features installiert sind. Das geht sehr einfach mit der PowerShell. Die ISE ist auf einem 2016er Server Core nicht verfügbar. Daher starte ich diese auf meinem WS-DC1 und verbinde mich remote mit dem WS-DC3. Installiert sind die erwarteten Features:



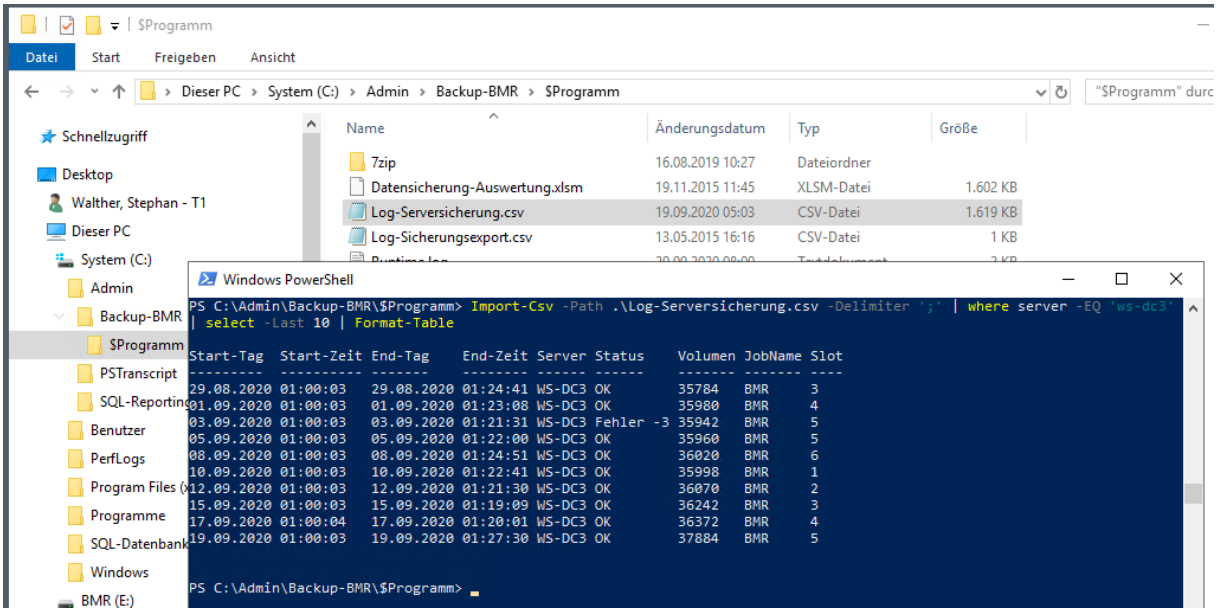
Es gibt auch bei den Freigaben keine Überraschungen:



Installierte Anwendungen lassen sich ebenfalls remote ermitteln. Der Domain Controller wird durch einen lokal bereitgestellten Microsoft Advanced Threat Analytics Agent (ATA) überwacht:

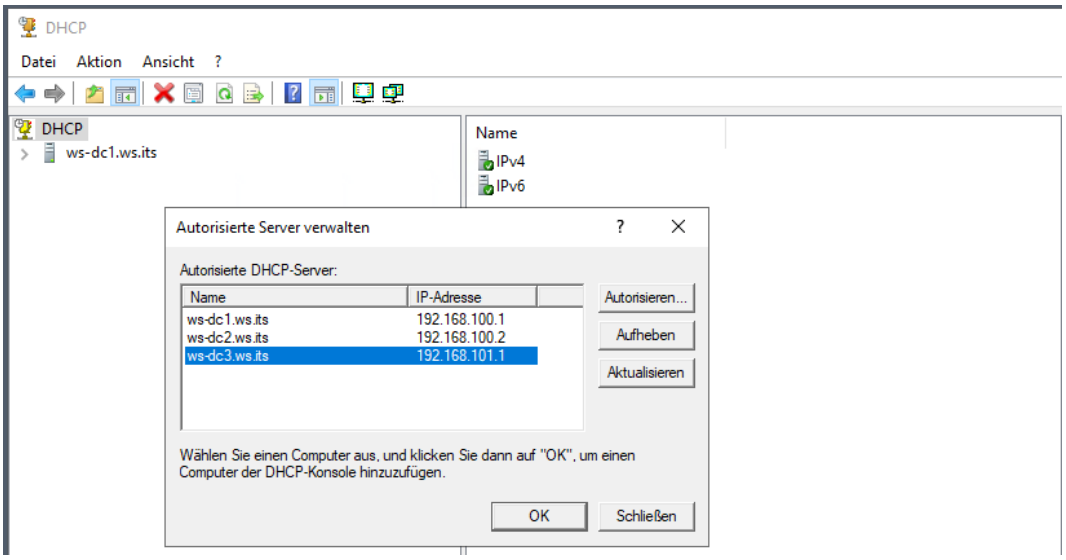
```
[ws-dc3]: PS C:\> Get-WmiObject -class win32_product | Format-Table -Property name,version

name                                                version
----                                                -------
Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 12.0.21005
Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005    12.0.21005
Microsoft Advanced Threat Analytics Gateway                   1.9.7478.57683


[ws-dc3]: PS C:\>
```

Die Datensicherung liegt auf meinem Backup-Server. Bis auf einen Job sind alle erfolgreich verlaufen. Ein Rollback wäre also denkbar:

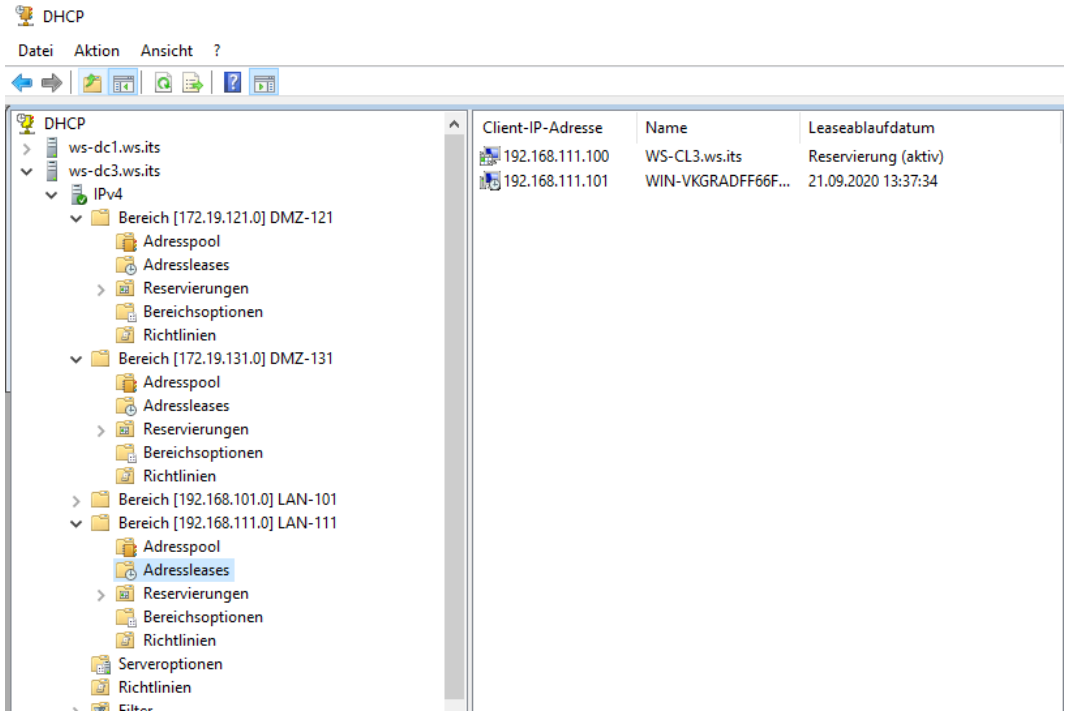


aktuelle Konfiguration des DHCP

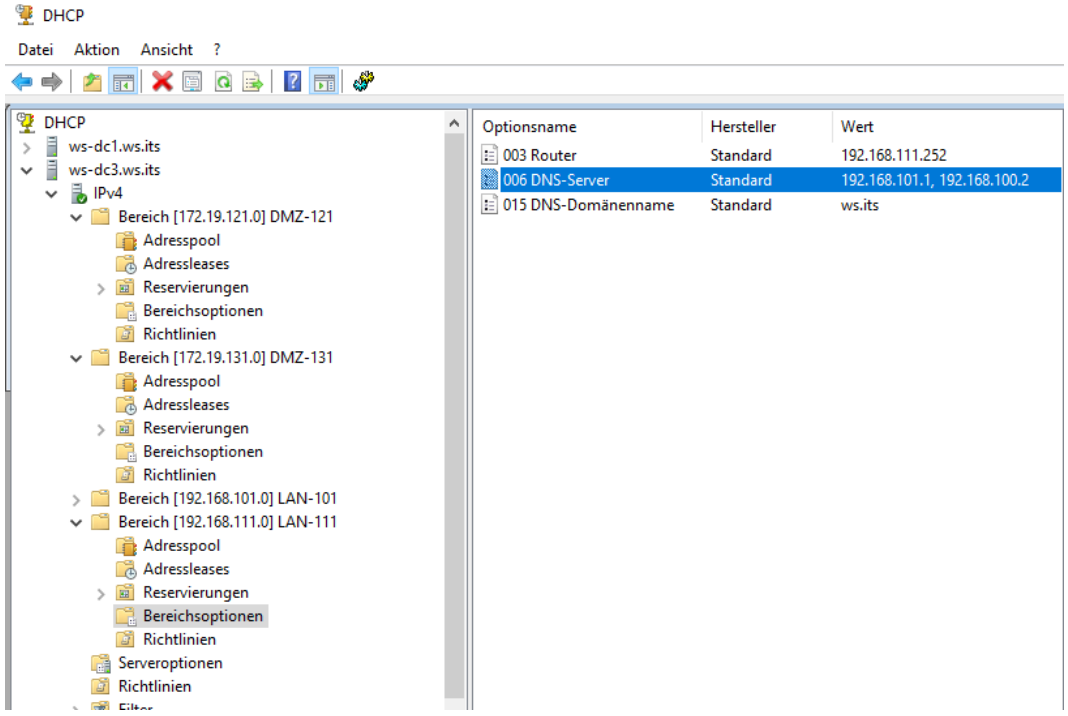
Wie sieht es im DHCP-Server aus? Dieser ist natürlich sauber im Active Directory registriert:



Da es sich in Neufahrn nur um einen kleinen Außenstandort handelt, sind die Scopes sehr übersichtlich befüllt:

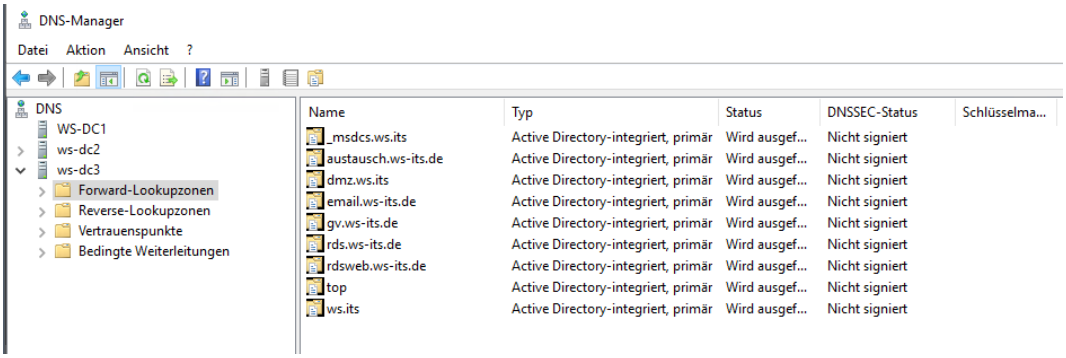


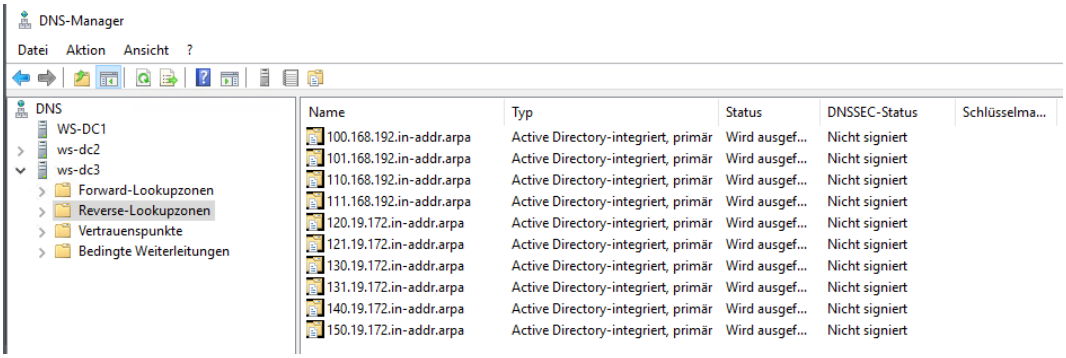
Wie bereits erwähnt ist der WS-DC3 alleine für den Standort zuständig. Fällt er aus, dann werden die Services DNS und Active Directory über das VPN aus dem Hauptstandort Ergoldsbach übernommen. Dazu müssen Clients und Server natürlich die richtigen Konfigurationen erhalten. In den DHCP-Serveroptions ist daher der WS-DC2 als sekundärer DNS hinterlegt – eigentlich sollte hier laut meiner Dokumentation der WS-DC1 mit der 192.168.100.1/24 stehen. Aber das kennt man ja …



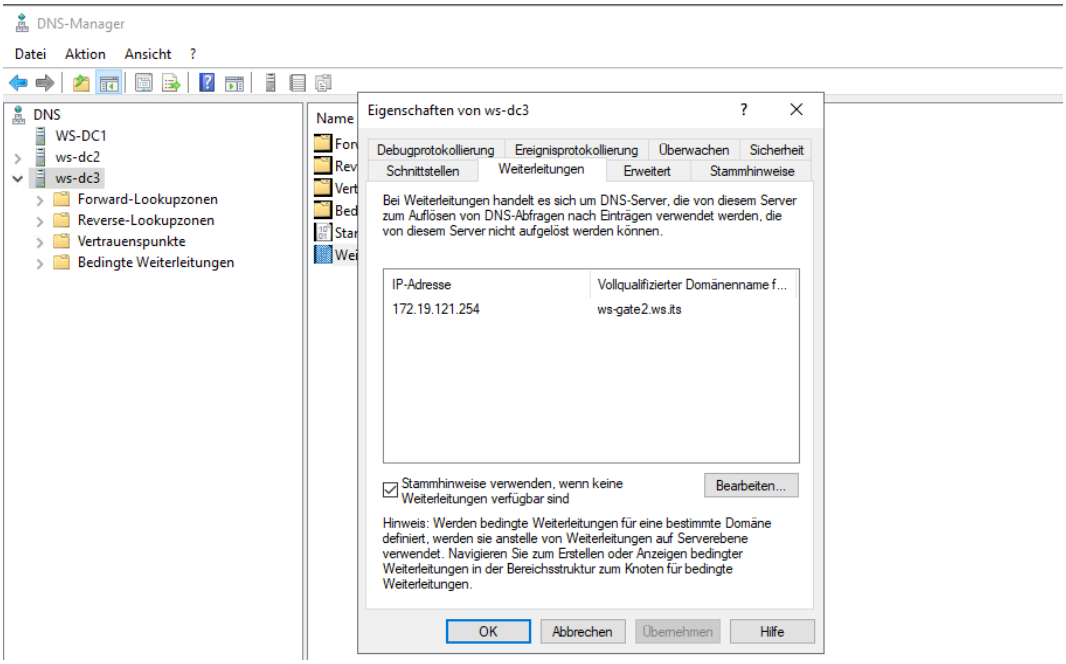
aktuelle Konfiguration des DNS

Alle meine Zonen sind AD-integriert. Daher hostet der WS-DC3 ein Replikat jeder Zone. Wichtig ist hierbei, dass keine lokal konfigurierten Zonen vergessen werden:

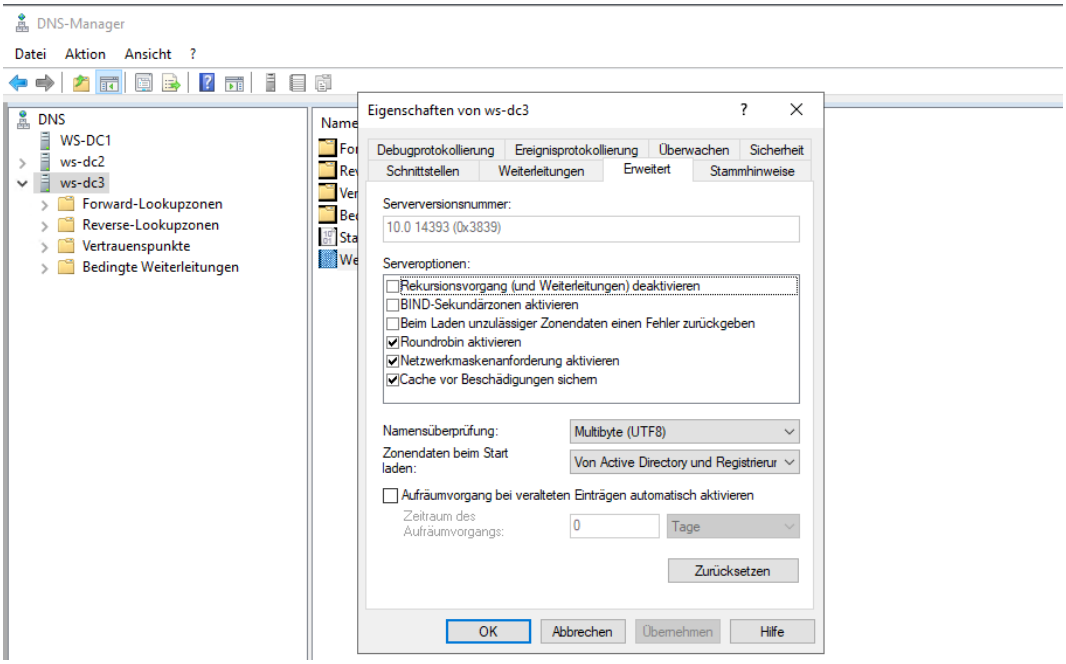




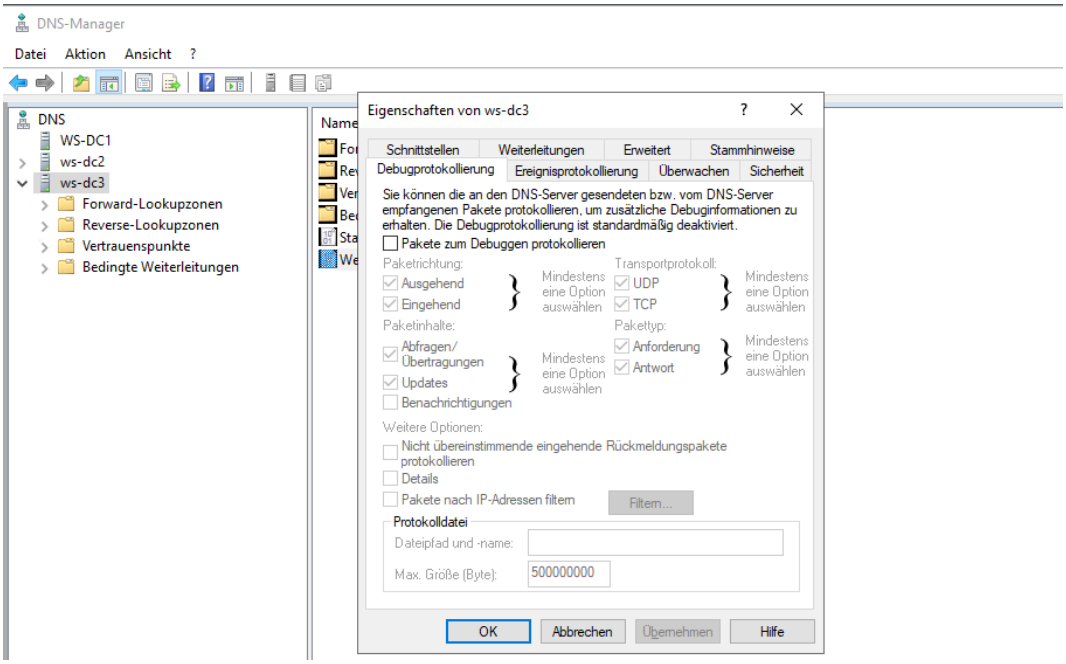
Als Forwarder verwendet der DNS-Server das Gateway im Außenstandort. Root-Hints sind als Fallback aktiv. Das sollte ich auf dem neuen Server ausschalten:



Sonst ist alles im Default konfiguriert:

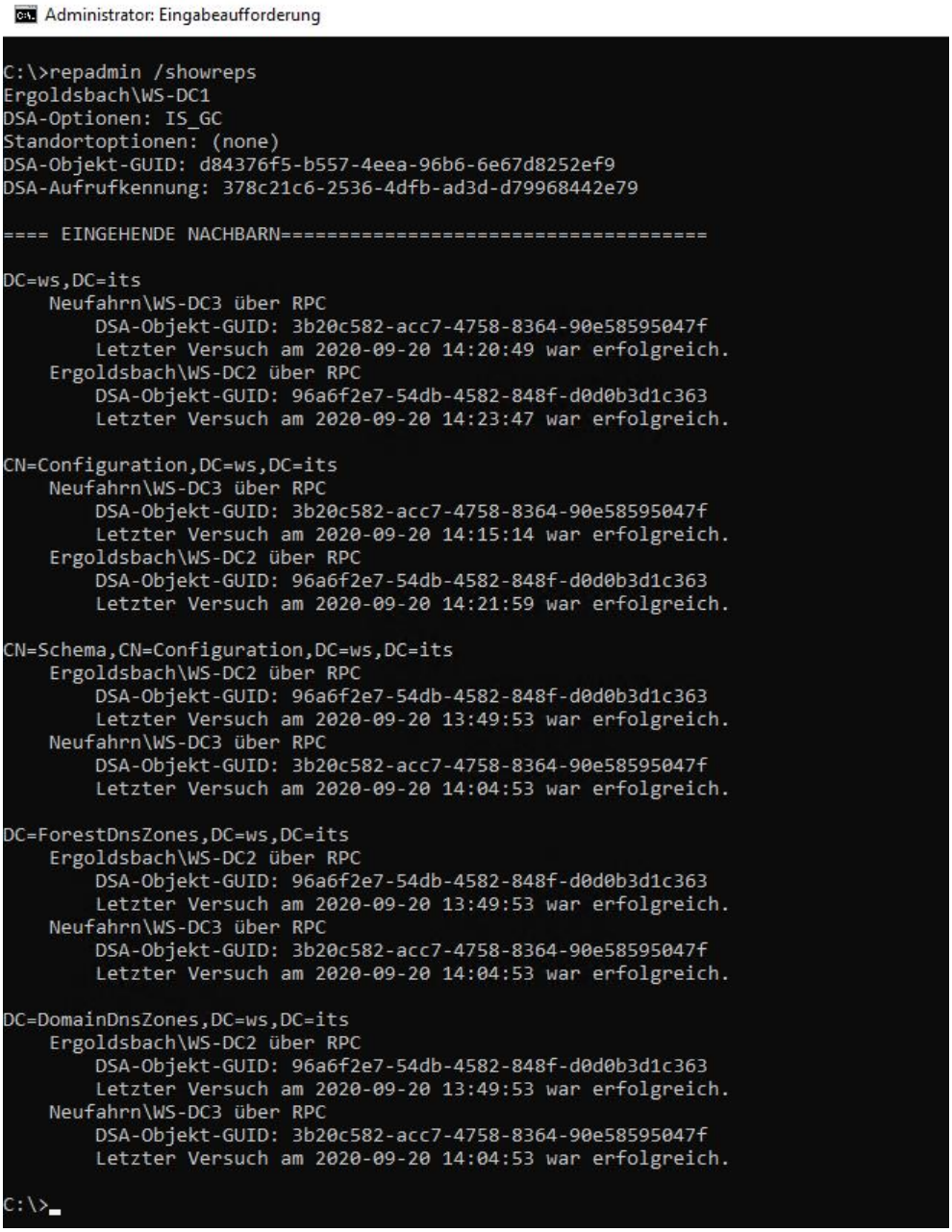


Auf meinen alten Servern hatte ich das DNS-Logging nicht aktiv. Auch das werde ich auf dem neuen Server anpassen:



aktuelle Konfiguration des Active Directory

Der Server ist ein vollständiger, schreibbarer Domain Controller mit der Zusatzfunktion Global Catalog. Die Replikationsverbindungen sind überschaubar und dank Bridgehead-Konfiguration vorhersehbar. Ein kurzer Blick auf das letzte Replikationsergebnis vom Server in Ergoldsbach gibt meiner Migration grünes Licht:

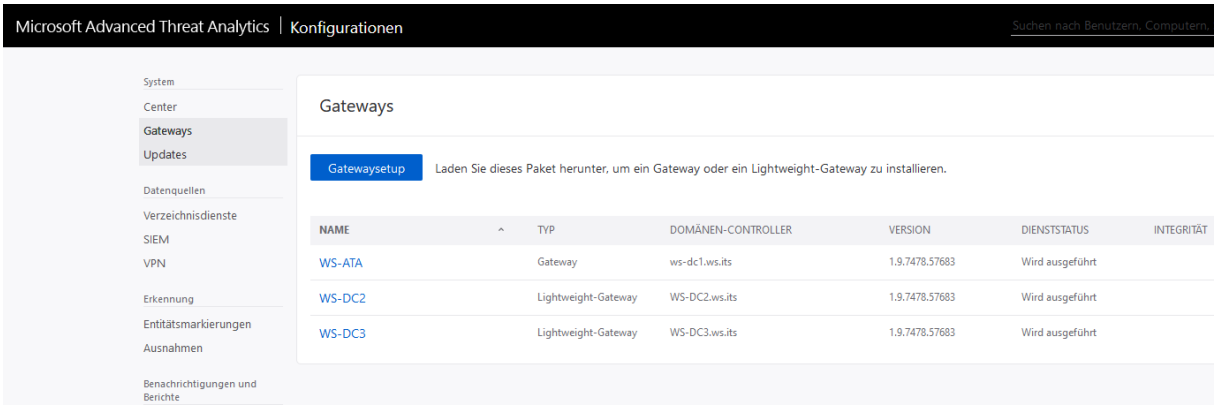


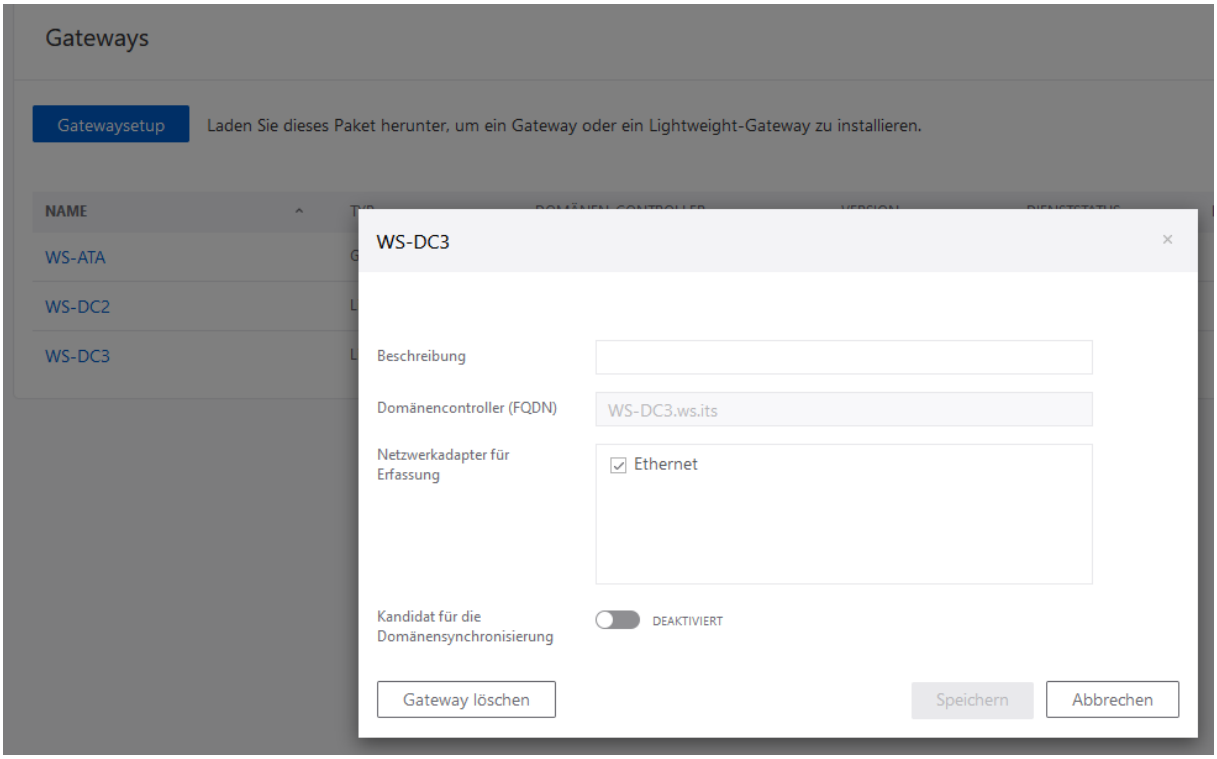
Und auch die Rückreplikation von Neufahrn nach Ergoldsbach ist erfolgreich:

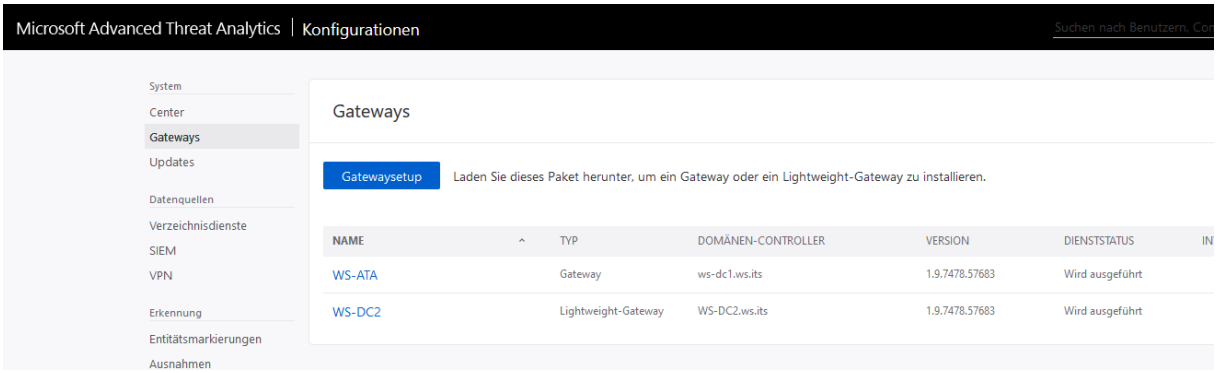
```
Administrator: Eingabeaufforderung - winrs -r:ws-dc3 cmd

C:\>winrs -r:ws-dc3 cmd
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Stephan-T0>repadmin /showreps
repadmin /showreps
Neufahrn\WS-DC3
DSA-Optionen: IS_GC
Standortoptionen: (none)
DSA-Objekt-GUID: 3b20c582-acc7-4758-8364-90e58595047f
DSA-Aufrufkennung: 272c97c6-29f6-4dab-a872-e5bb9f0d0379

==== EINGEHENDE NACHBARN====================================

DC=ws,DC=its
    Ergoldsbach\WS-DC1 über RPC
        DSA-Objekt-GUID: d84376f5-b557-4eea-96b6-6e67d8252ef9
        Letzter Versuch am 2020-09-20 14:25:16 war erfolgreich.

CN=Configuration,DC=ws,DC=its
    Ergoldsbach\WS-DC1 über RPC
        DSA-Objekt-GUID: d84376f5-b557-4eea-96b6-6e67d8252ef9
        Letzter Versuch am 2020-09-20 14:24:58 war erfolgreich.

CN=Schema,CN=Configuration,DC=ws,DC=its
    Ergoldsbach\WS-DC1 über RPC
        DSA-Objekt-GUID: d84376f5-b557-4eea-96b6-6e67d8252ef9
        Letzter Versuch am 2020-09-20 14:24:58 war erfolgreich.

DC=ForestDnsZones,DC=ws,DC=its
    Ergoldsbach\WS-DC1 über RPC
        DSA-Objekt-GUID: d84376f5-b557-4eea-96b6-6e67d8252ef9
        Letzter Versuch am 2020-09-20 14:24:58 war erfolgreich.

DC=DomainDnsZones,DC=ws,DC=its
    Ergoldsbach\WS-DC1 über RPC
        DSA-Objekt-GUID: d84376f5-b557-4eea-96b6-6e67d8252ef9
        Letzter Versuch am 2020-09-20 14:24:59 war erfolgreich.
```

aktuelle ATA-Konfiguration und Vorbereitung im ATA

Bei meiner letzten Migration stellte ich fest, das Microsoft ATA mit Wipe & Load Migrationen nicht so gut klarkommt. Daher deinstalliere ich den Server aus der ATA-Konsole:



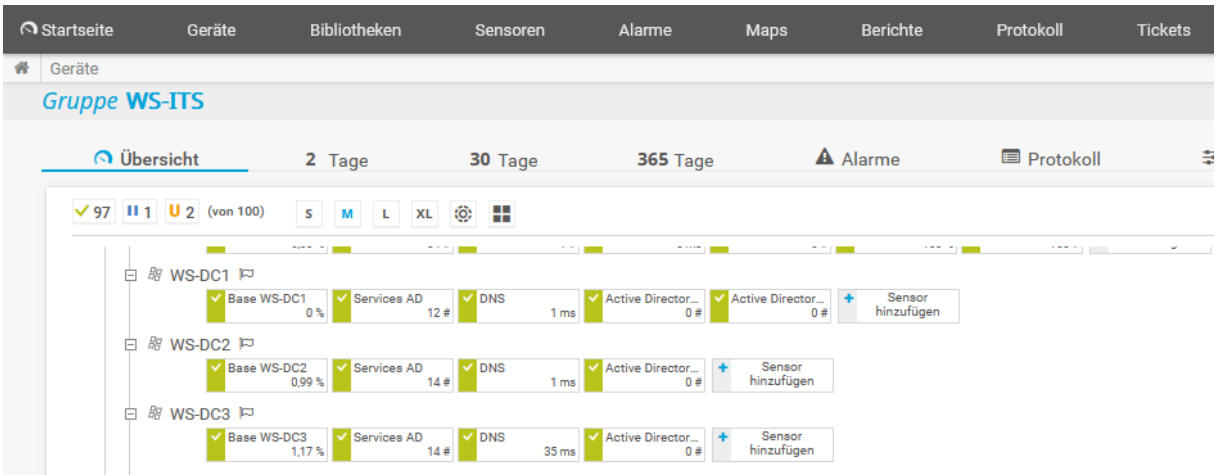




Ab jetzt kann ich ggf. nicht mehr alle Angriffsszenarien in Echtzeit verfolgen!

Maintenance

Mein Server wird zusätzlich vom PRTG-Monitoring überwacht. Hier pausiere ich die zuständigen Sensoren, damit ich Fehlalarme vermeide:

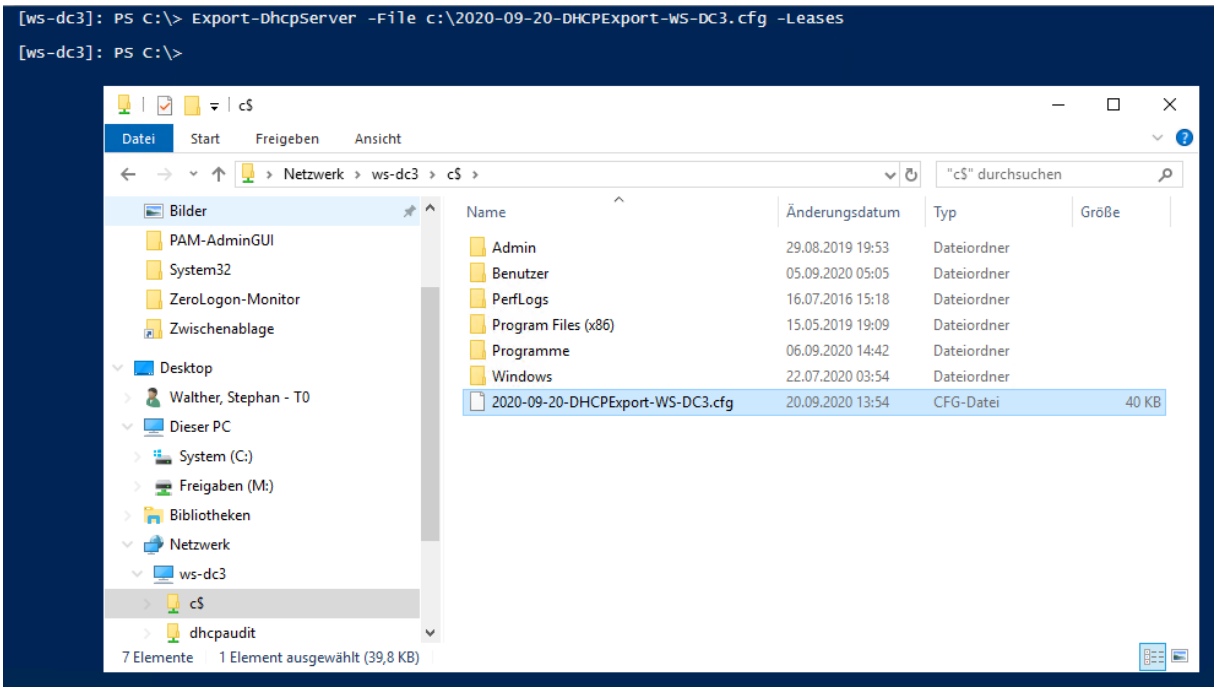


Deinstallation

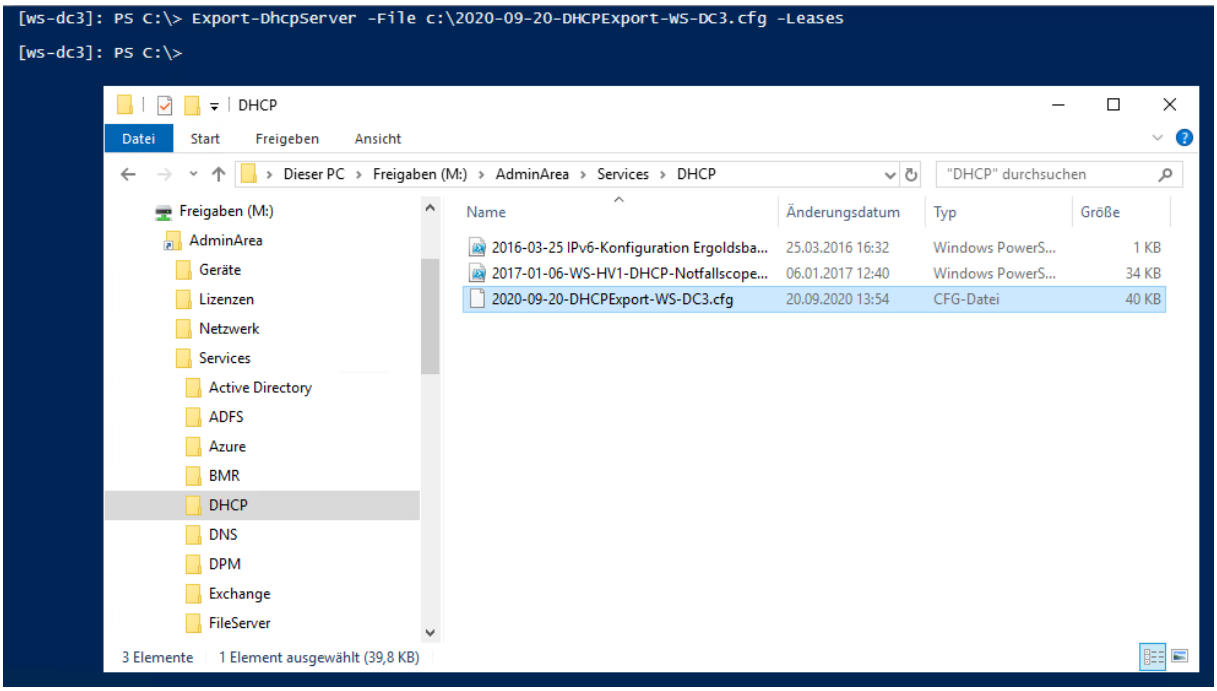
Vorbereitung der Migration der Rolle DHCP

Ich habe keine Show-Stopper gefunden. Daher beginne ich nun aktiv mit der Migration. Die Rolle DHCP ist zuerst an der Reihe. Hier erwarte ich keine Clientseitigen Probleme, denn zum einen sind alle Clients aktiv bereits mit einer Lease versorgt. Und zum anderen ist heute Sonntag – das ist ein prima Wartungszeitfenster!

Die Migration des DHCP ist denkbar einfach: Auf dem alten Server exportiere ich die Konfiguration und halte optional den Service an. Und auf dem neuen Server importiere ich die Konfiguration einfach wieder. Durch PowerShell-Remoting kann ich diese Arbeitsschritte von meinem WS-DC1 aus ausführen. Wichtig beim Export ist die Inklusion der bereits ausgestellten Leases. Das kann mit dem Parameter -Lease vorgenommen werden:



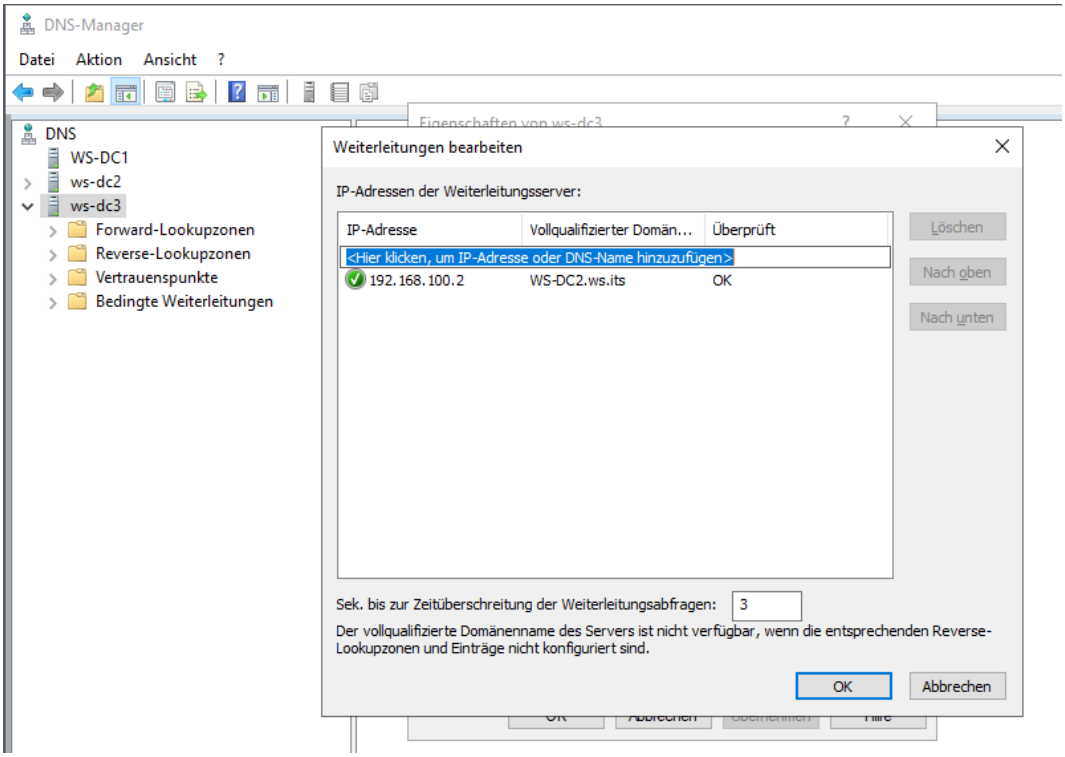
Die Konfigurationsdatei verschiebe ich in mein zentrales Adminverzeichnis:



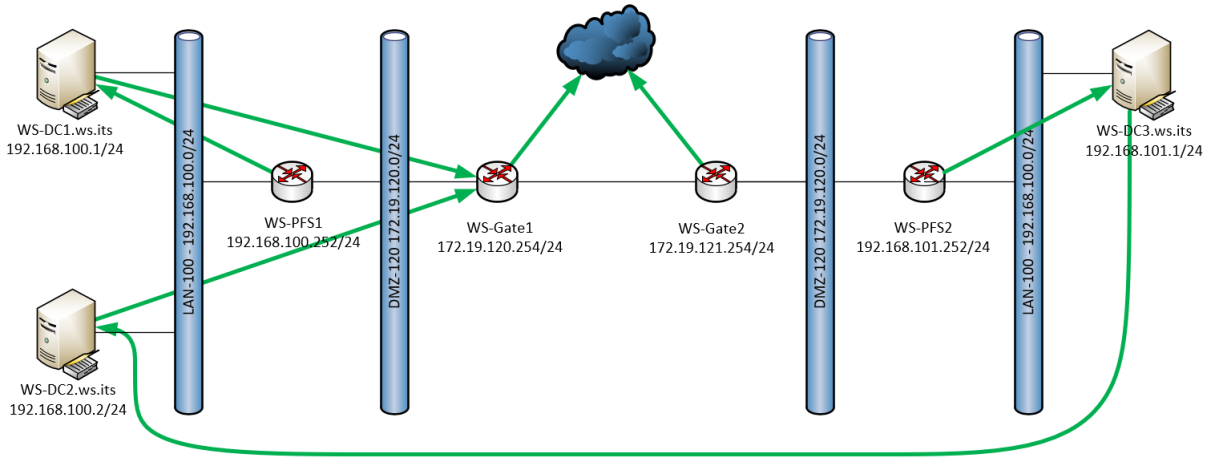
Den Service muss ich wegen meinem Wartungsfenster nicht anhalten.

Vorbereitung der Migration der Rolle DNS

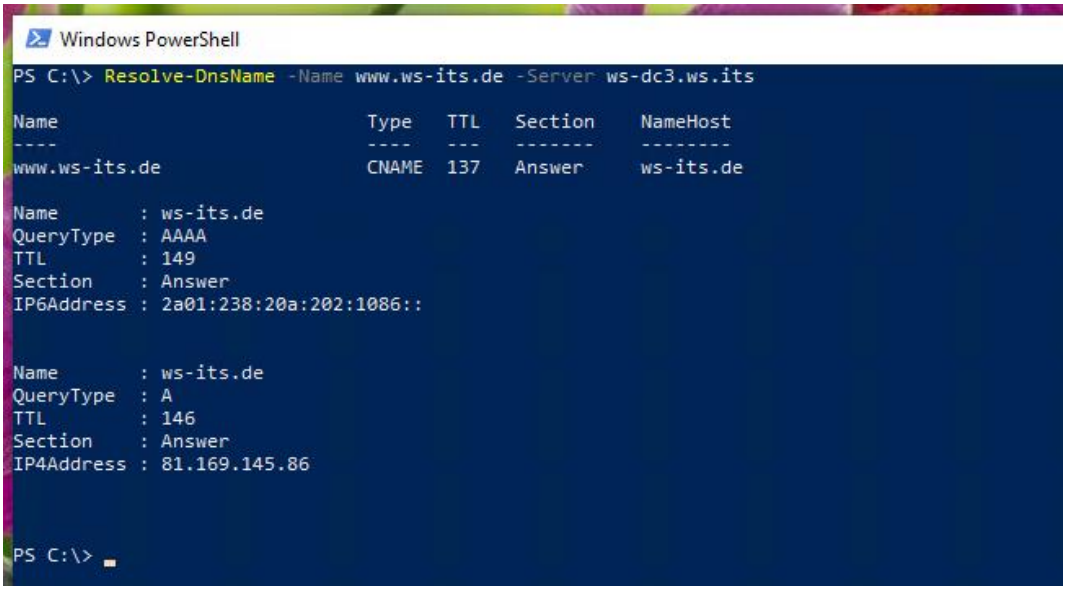
Weiter geht es im DNS. Eigentlich werden die Zonen ja bei der Neuinstallation über die AD-Replikation wieder eingespielt. Aber um diese Zonen geht es hier nicht. Viel wichtiger sind die Forwarder. Aktuell kann der Server auf Fragen zu meiner internen DNS-Zone ws.its direkt antworten, denn er ist ja als Domain Controller dazu autorisiert. Wenn ich aber gleich die Rolle Active Directory deinstalliere, dann verliert der DNS-Server den Zugriff auf die Zonen. Andere Server und Clients im Netzwerk werden ihn aber dennoch weiter befragen. Ohne eigene Zonen kann der DNS-Server aber nicht mehr antworten. Und dann bricht das Netzwerk zusammen. Daher rekonfiguriere ich den primären Forwarder um und zeige auf einen der anderen Domain Controller statt auf das Gateway:



Damit ergibt sich folgendes Layout für die Namensauflösung. Der WS-DC3 wird als DNS-Server ohne die Rolle Active Directory weiter funktional arbeiten. Nur erhält er die Antworten auf die Fragen der Clients selber vom WS-DC2 in Ergoldsbach. So sind meine internen DNS-Zonen weiter auflösbar. Und die externe Namensauflösung kann den gleichen Weg nehmen:

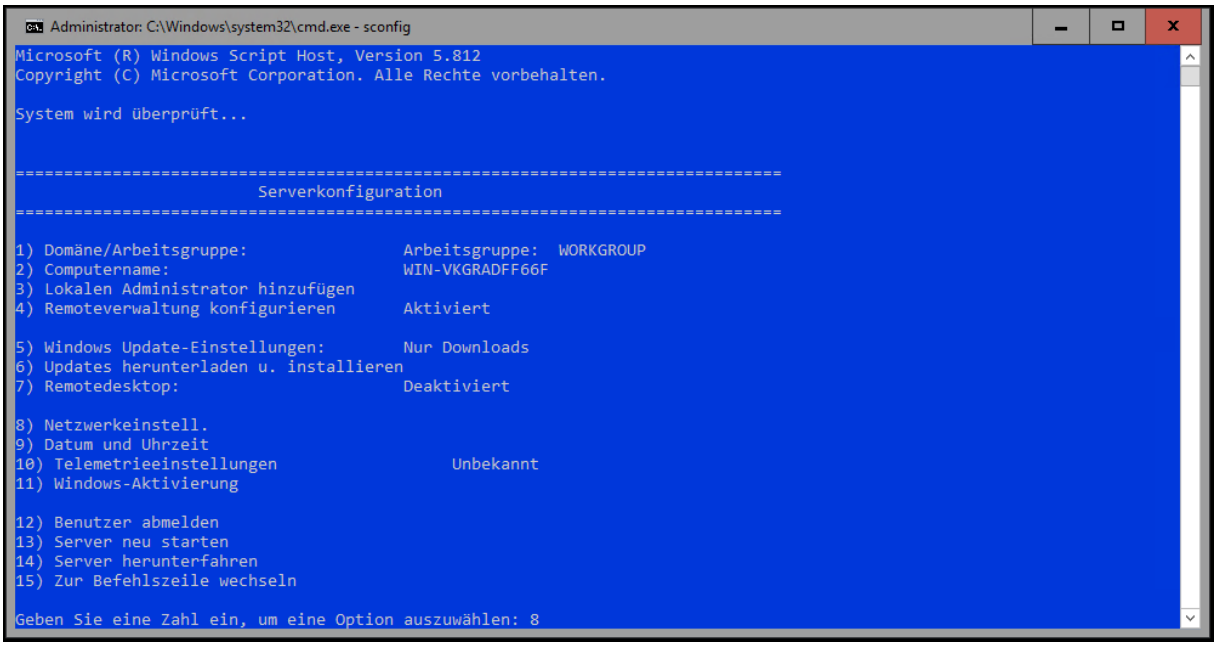


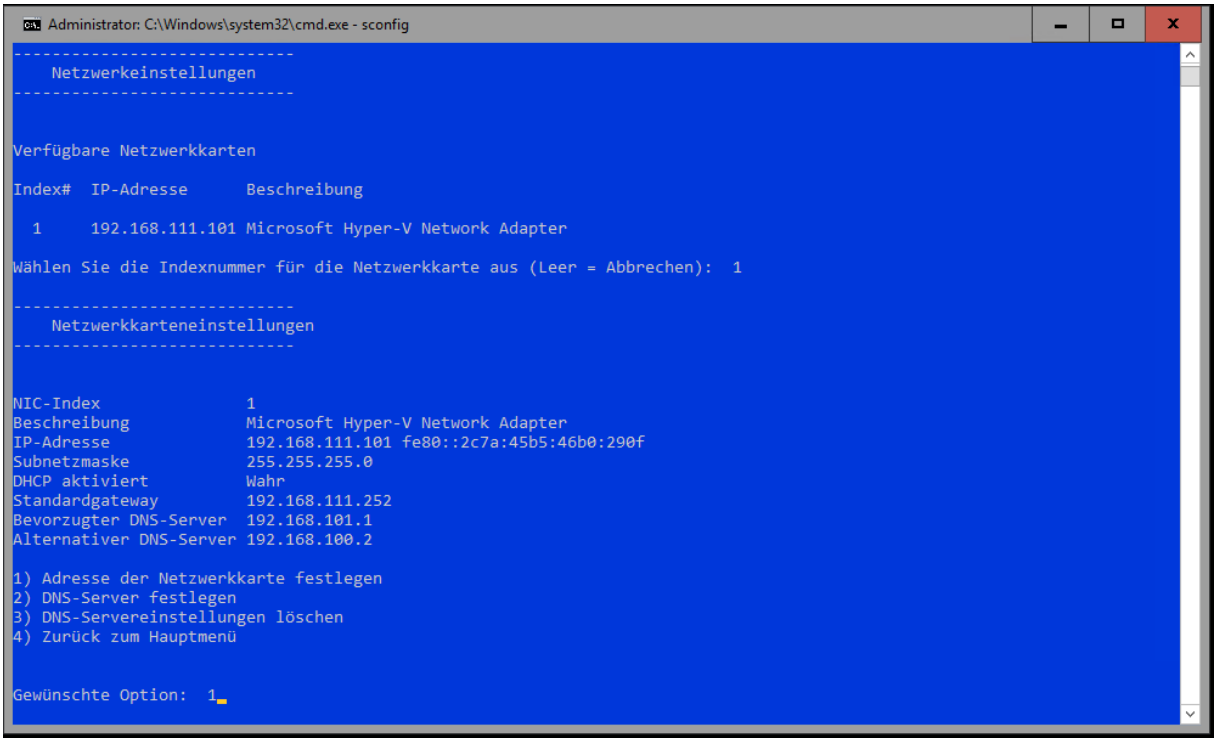
Ich teste das auf einem Client in Neufahrn. Das sieht gut aus:

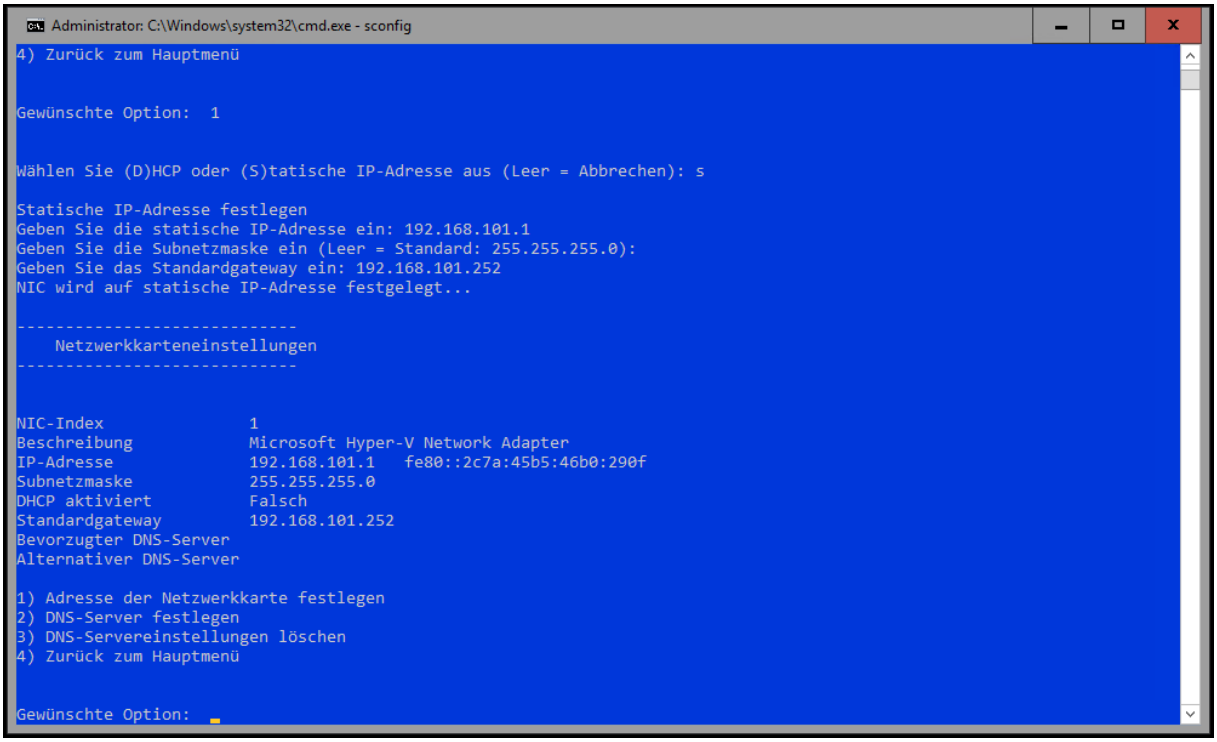


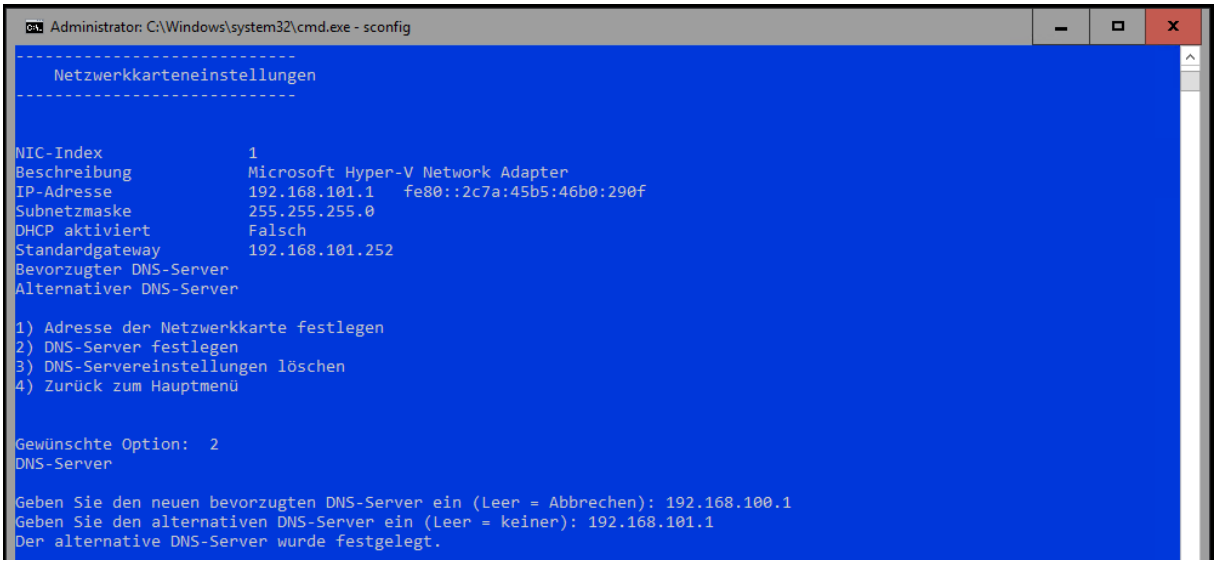
Vorbereitung der neuen VM

Jetzt bekommt die neue VM den finalen Schliff. So kann ich die Unterbrechung in der Namensauflösung so klein wie möglich halten. Zuerst deaktiviere ich den Netzwerkadapter der VM im Hyper-V-Manager. Danach kann ich in der VM die IPv4-Konfiguration des alten Servers eintragen:

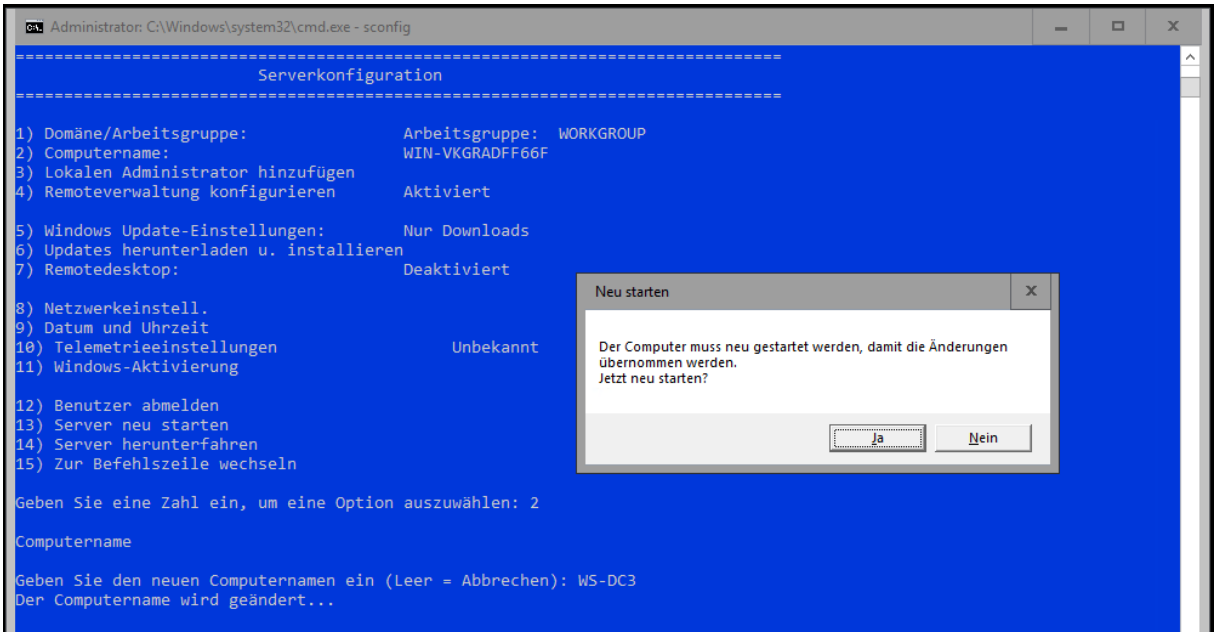



Administrator: C:\Windows\system32\cmd.exe - sconfig
Netzwerkeinstellungen
Verfügbare Netzwerkkarten
Index# IP-Adresse Beschreibung
1 192.168.111.101 Microsoft Hyper-V Network Adapter
Wählen Sie die Indexnummer für die Netzwerkkarte aus (Leer = Abbrechen): 1
Netzwerkkarteneinstellungen
NIC-Index 1
Beschreibung Microsoft Hyper-V Network Adapter
IP-Adresse 192.168.111.101 fe80::2c7a:45b5:46b0:290f
Subnetzmaske 255.255.255.0
DHCP aktiviert Wahr
Standardgateway 192.168.111.252
Bevorzugter DNS-Server 192.168.101.1
Alternativer DNS-Server 192.168.100.2
1) Adresse der Netzwerkkarte festlegen
2) DNS-Server festlegen
3) DNS-Servereinstellungen löschen
4) Zurück zum Hauptmenü
Gewünschte Option: 1

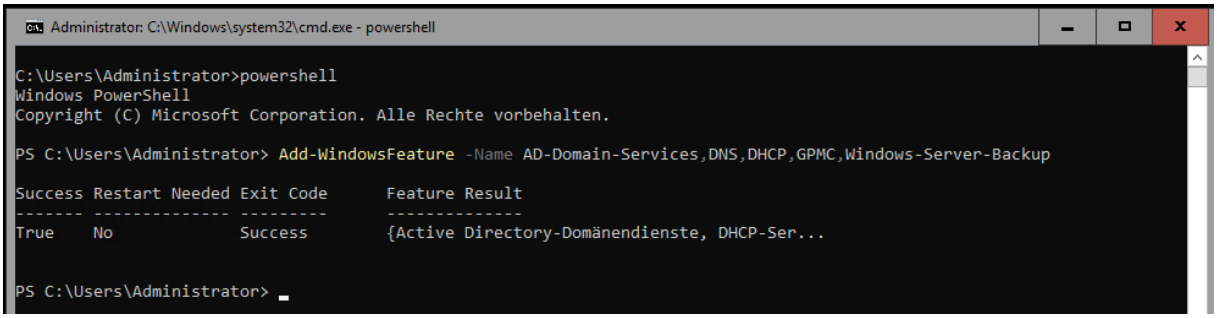

Administrator: C:\Windows\system32\cmd.exe - sconfig
4) Zurück zum Hauptmenü
Gewünschte Option: 1
Wählen Sie (D)HCP oder (S)tatische IP-Adresse aus (Leer = Abbrechen): s
Statische IP-Adresse festlegen
Geben Sie die statische IP-Adresse ein: 192.168.101.1
Geben Sie die Subnetzmaske ein (Leer = Standard: 255.255.255.0):
Geben Sie das Standardgateway ein: 192.168.101.252
NIC wird auf statische IP-Adresse festgelegt...
Netzwerkkarteneinstellungen
NIC-Index 1
Beschreibung Microsoft Hyper-V Network Adapter
IP-Adresse 192.168.101.1 fe80::2c7a:45b5:46b0:290f
Subnetzmaske 255.255.255.0
DHCP aktiviert Falsch
Standardgateway 192.168.101.252
Bevorzugter DNS-Server
Alternativer DNS-Server
1) Adresse der Netzwerkkarte festlegen
2) DNS-Server festlegen
3) DNS-Servereinstellungen löschen
4) Zurück zum Hauptmenü
Gewünschte Option:



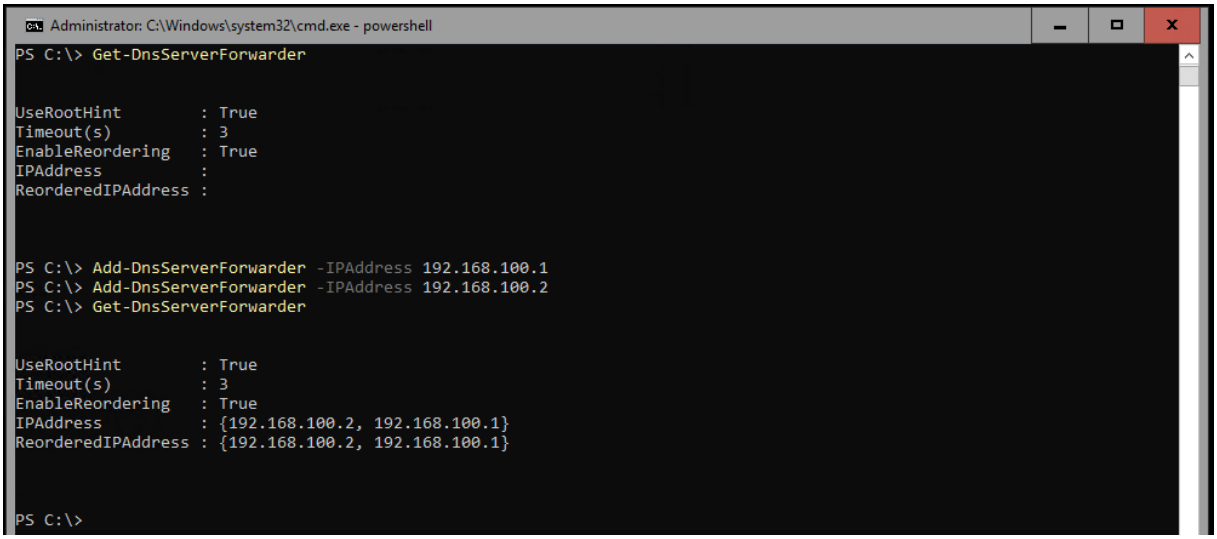
Danach kann ich das Betriebssystem umbenennen. Den Namen WS-DC3 kann ich auswählen, da der neue Server keine Netzwerkverbindung hat. Nun ist ein Neustart fällig:



Nach dem Neustart installiere ich die Rollen fürs Active Directory, DHCP und DNS. Das Feature Windows Backup brauche ich später auch:



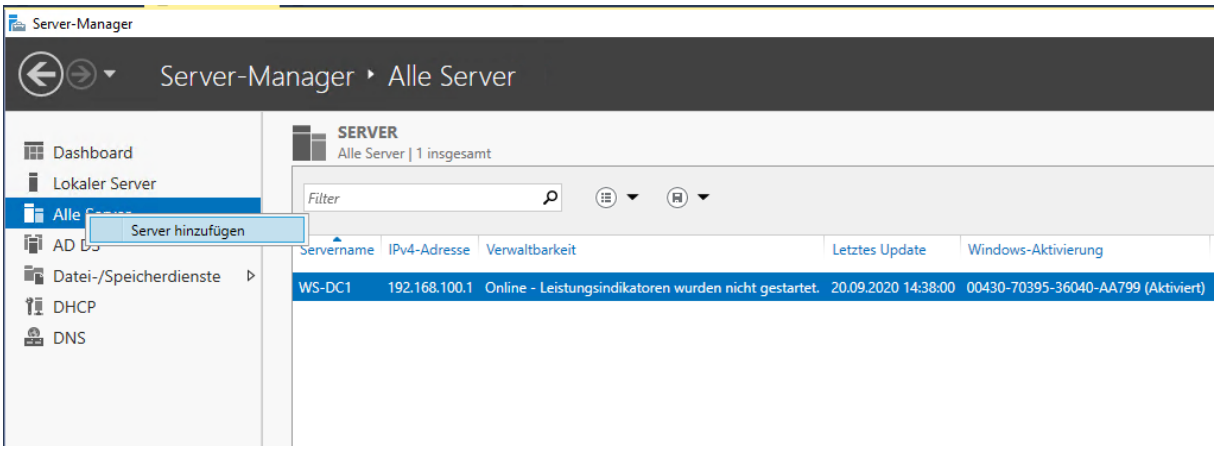
Immer noch ohne Netzwerkverbindung trage ich nun die Forwarder ein. Da der Server Core keine Verwaltungsoberfläche hat und ich kein Remoting ohne Netzwerk nutzen kann, muss hier die PowerShell aushelfen. Ich trage die beiden IPv4-Adressen der Domain Controller in Ergoldsbach ein:

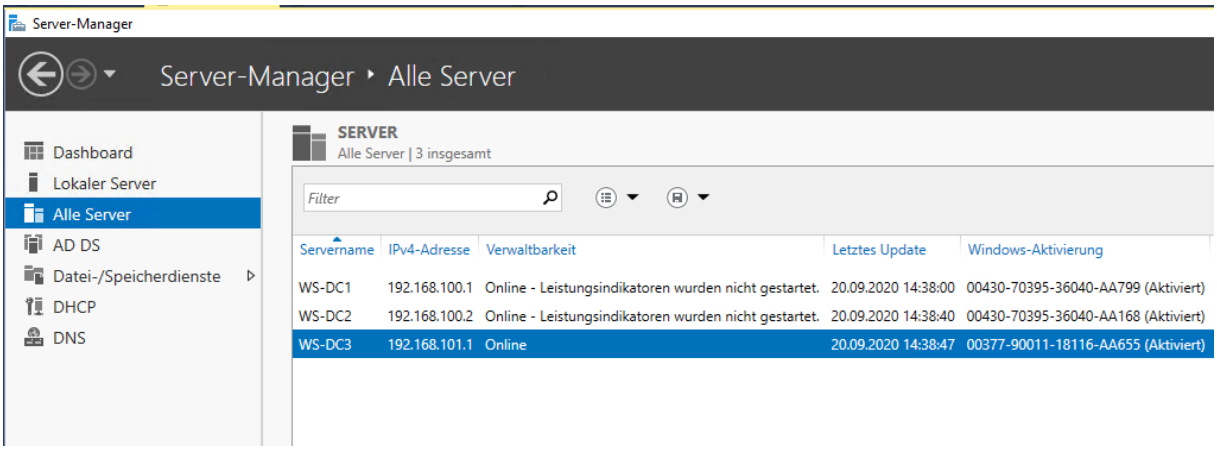


Wenn der neue WS-DC3 mit aktivem Netzwerk eine Frage via DNS erhält, dann holt er sich seine Antworten vom DNS in Ergoldsbach. Damit sind alle Rollen vorbereitet.

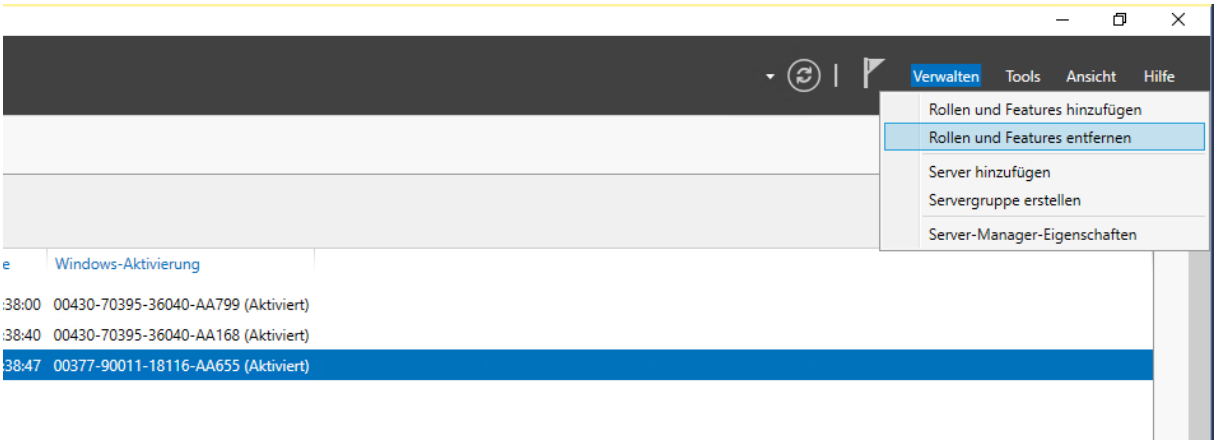
Entfernen der Rolle Active Directory

Als nächstes deinstalliere ich auf dem alten Server die Rolle Active Directory. Das geht mit einem Server Manager von einem GUI-Server sehr einfach. Ich verbinde den Server in die Konsole vom WS-DC1:

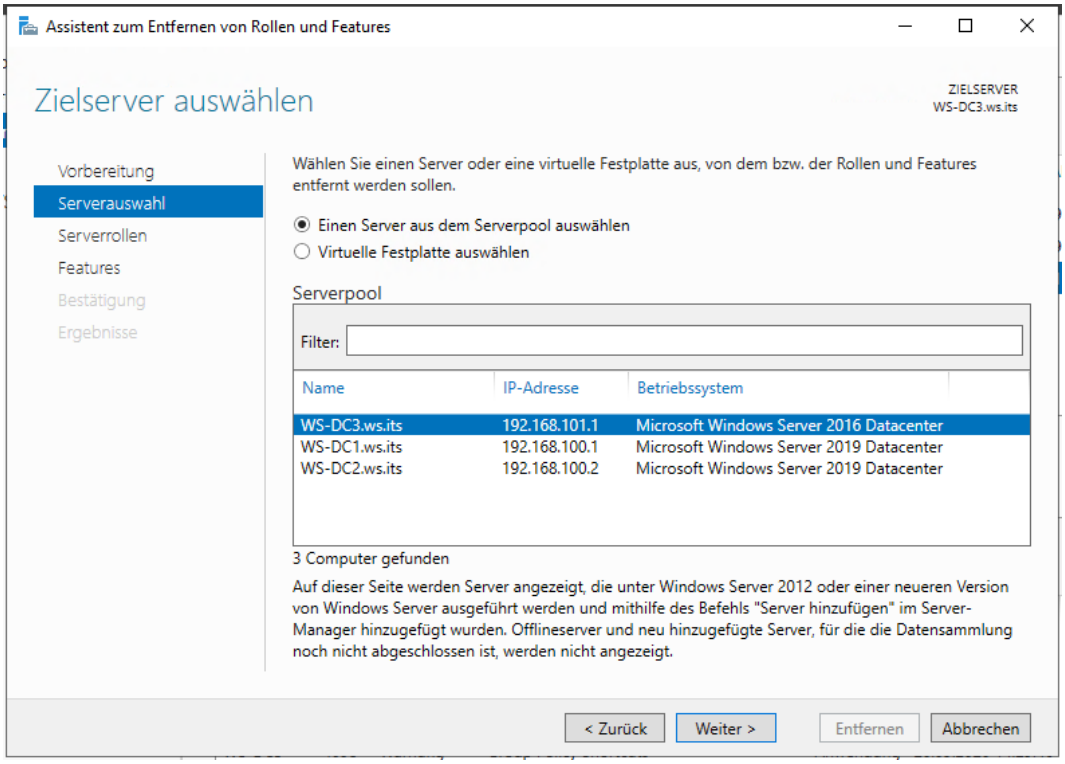




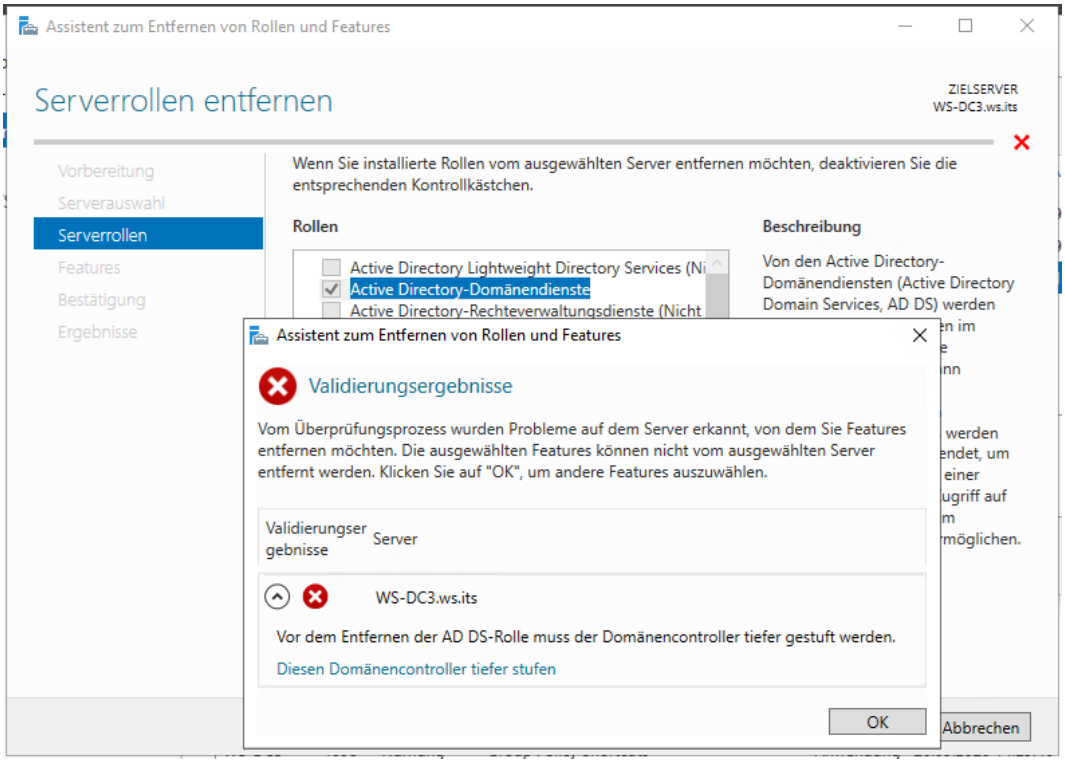
Über die Schalter oben rechts geht es weiter:



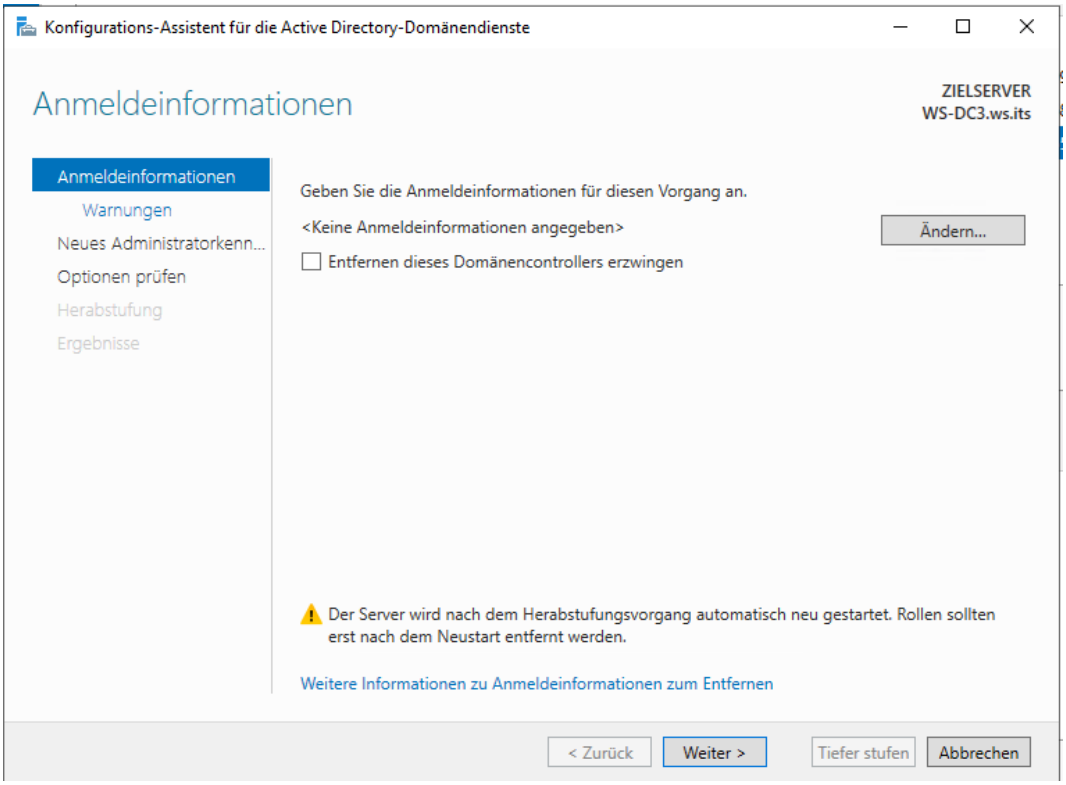
Für die Deinstallation selektiere ich den alten Server:



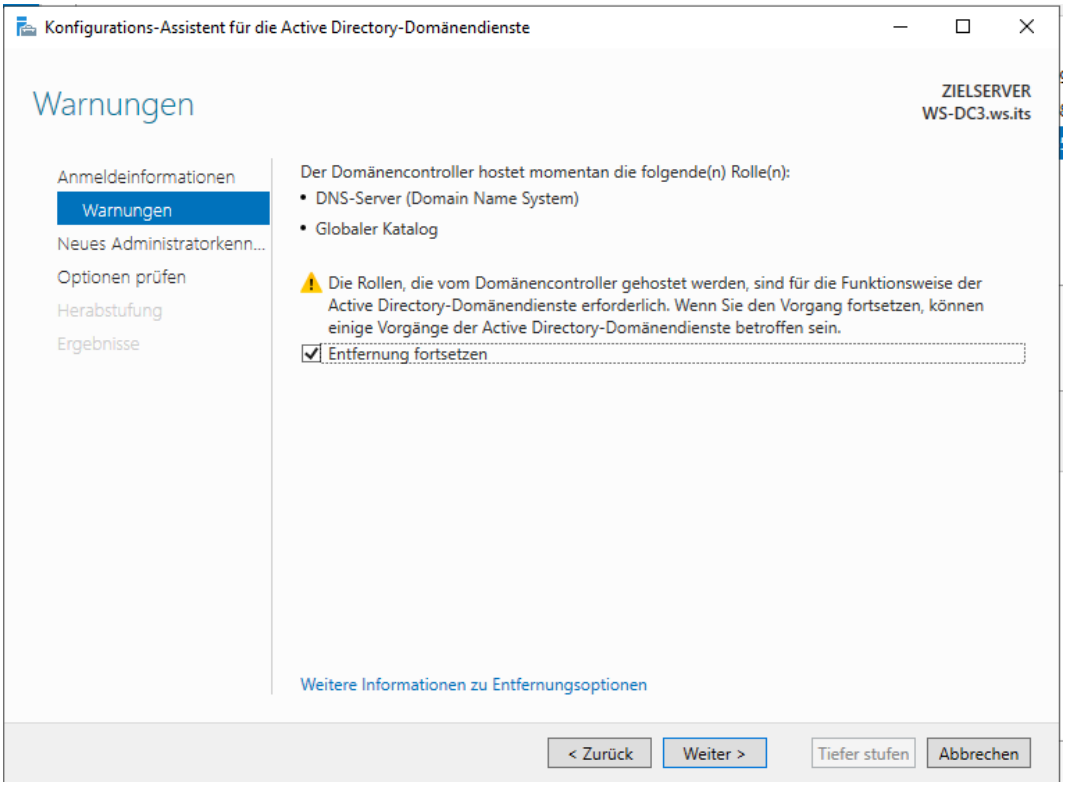
Bei der Vorabprüfung stellt der Server fest, dass die Rolle Active Directory aktiv verwendet wird. Beim Anzeigen dieser Fehlermeldung wird mir aber das Herabstufen angeboten. Da wollte ich hin:



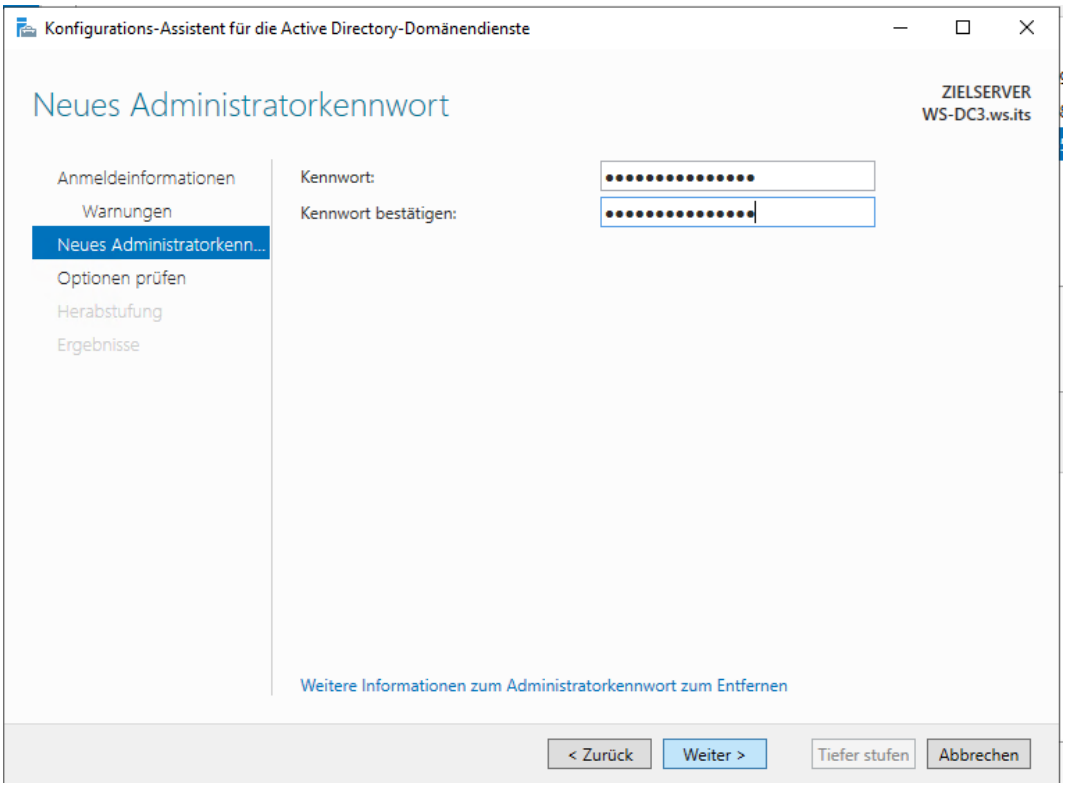
Mein aktueller Benutzer hat die dazu erforderlichen Rechte über mein PAM-Tool erhalten:



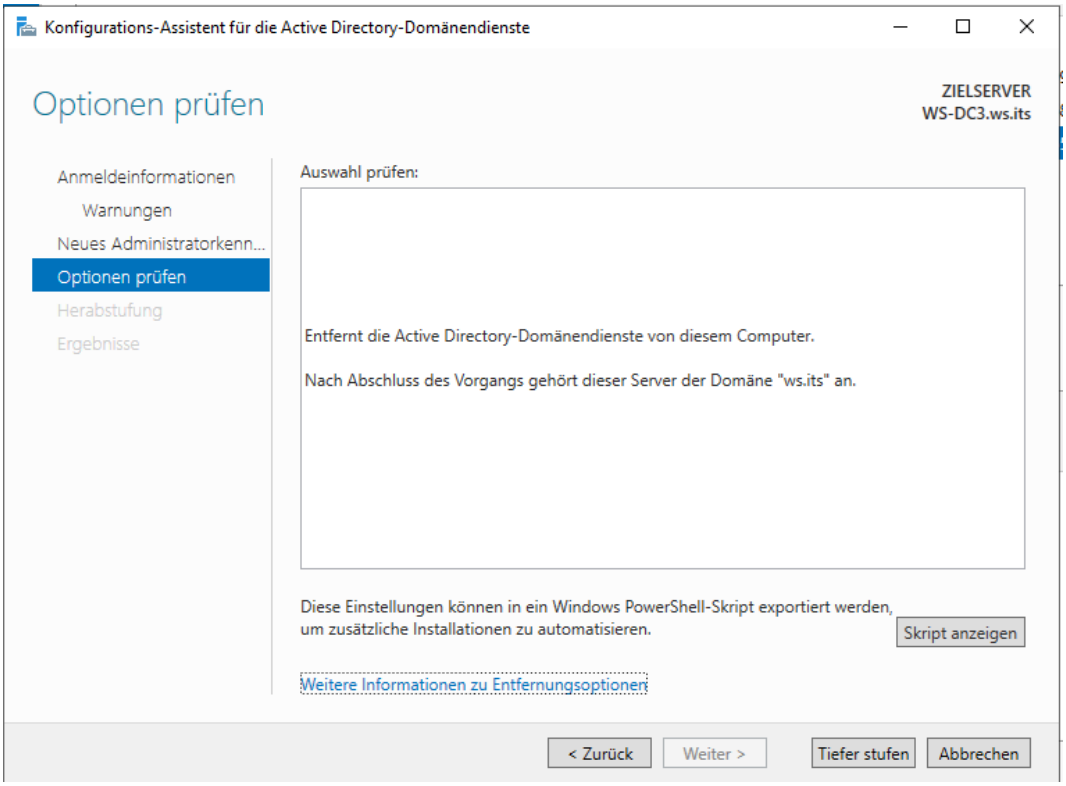
Die Bestätigungen sind fast eine Formsache, denn ohne geht es nicht weiter:



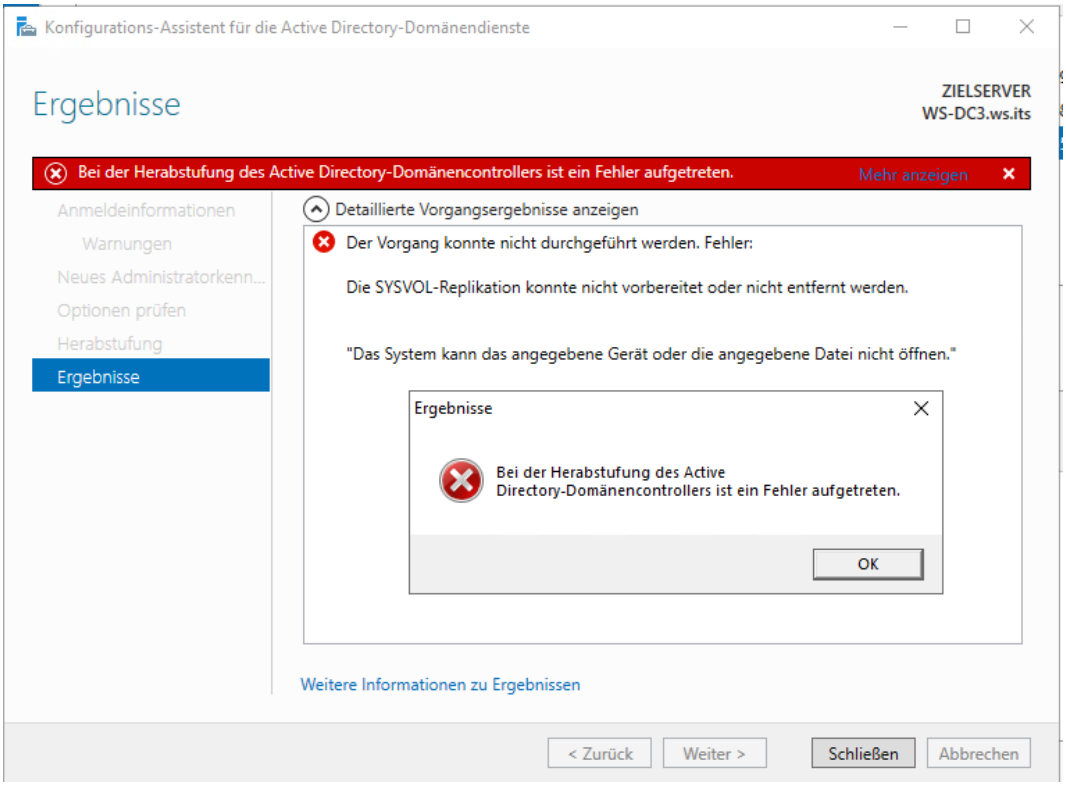
Nach dem Herabstufen ist der Server nur noch ein Memberserver. Dieser hat dann wieder einen lokalen Admin-Account. Und hier wird dessen Passwort definiert:



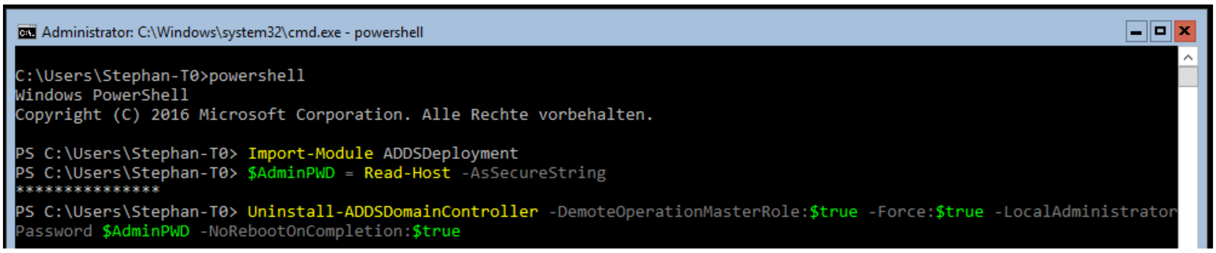
So sollte es passen:

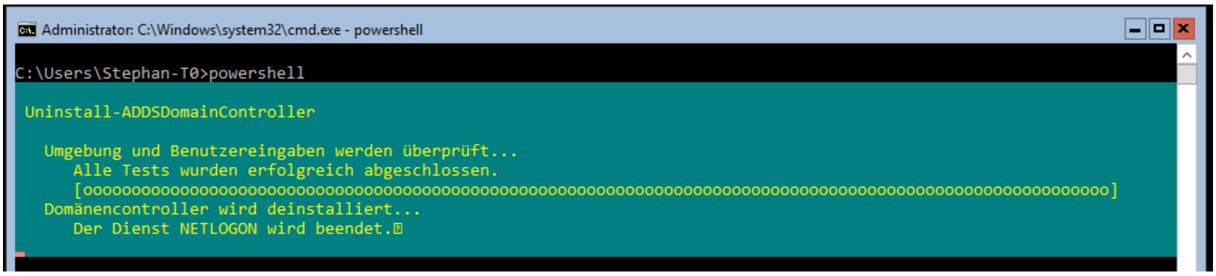


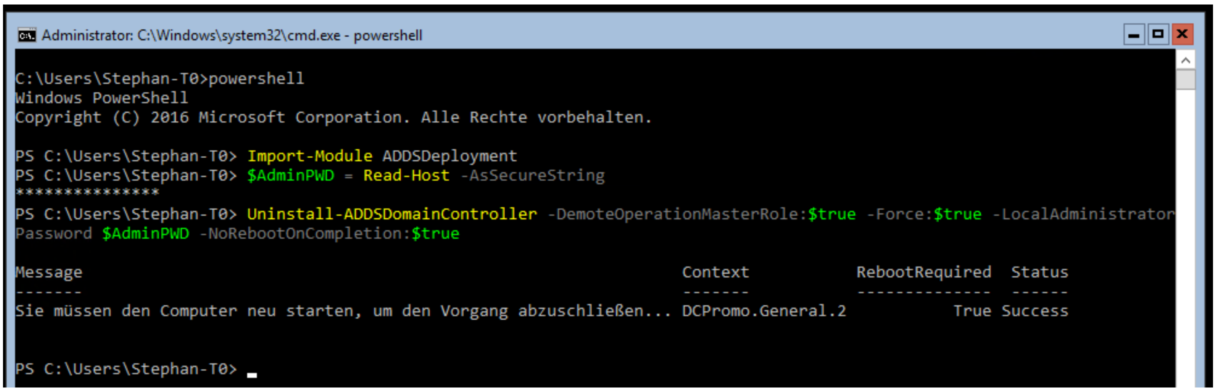
Oder doch nicht? Ich „liebe“ ja diese äußerst detaillierten Fehlermeldungen…



Aber ich habe da so eine Vermutung. Den Prozess habe ich remote angestoßen. Der Server Manager arbeitet mit PowerShell Remoting im Hintergrund. Und dieses Remoting gibt standardmäßig keine Credentials an das Zielsystem weiter. Wenn dann aber Befehle gegen ein drittes System im Hintergrund angestoßen werden sollen, dann entsteht nicht selten ein Doppel-Hop-Problem. Also versuche ich das Demoting (Herabstufen) einfach noch einmal lokal auf dem WS-DC3. Hier geht es nur mit der PowerShell:


Administrator: C:\Windows\system32\cmd.exe - powershell
C:\Users\Stephan-T0>powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Alle Rechte vorbehalten.
PS C:\Users\Stephan-T0> Import-Module ADDSDeployment
PS C:\Users\Stephan-T0> $AdminPWD = Read-Host -AsSecureString
****
PS C:\Users\Stephan-T0> Uninstall-ADDSDomainController -DemoteOperationMasterRole:$true -Force:$true -LocalAdministrator
Password $AdminPWD -NoRebootOnCompletion:$true


Administrator: C:\Windows\system32\cmd.exe - powershell
C:\Users\Stephan-T0>powershell
Uninstall-ADDSDomainController
Umgebung und Benutzereingaben werden überprüft...
Alle Tests wurden erfolgreich abgeschlossen.
[oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo]
Domänencontroller wird deinstalliert...
Der Dienst NETLOGON wird beendet.

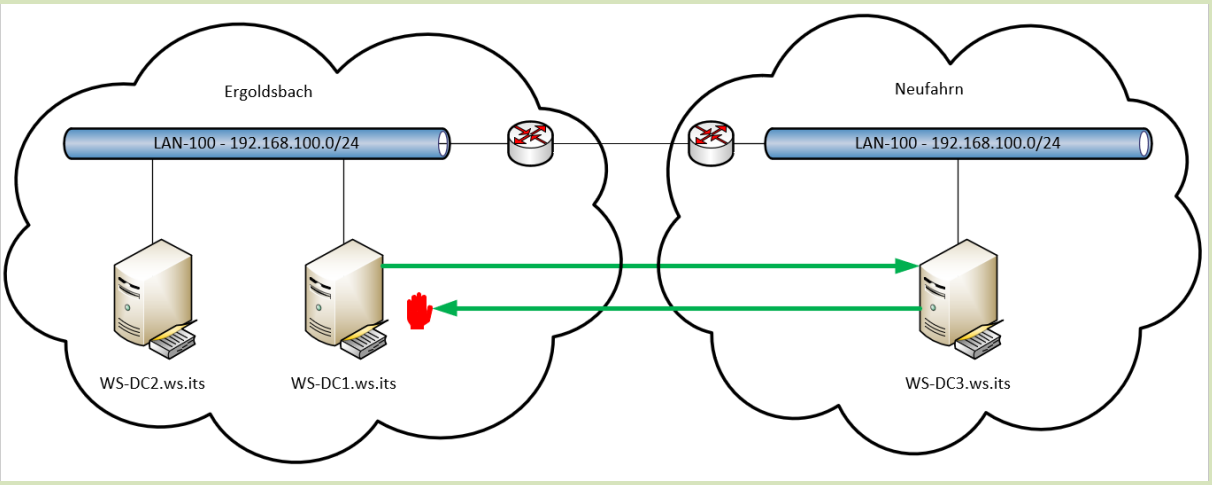

Administrator: C:\Windows\system32\cmd.exe - powershell
C:\Users\Stephan-T0>powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Alle Rechte vorbehalten.
PS C:\Users\Stephan-T0> Import-Module ADDSDeployment
PS C:\Users\Stephan-T0> $AdminPWD = Read-Host -AsSecureString
****
PS C:\Users\Stephan-T0> Uninstall-ADDSDomainController -DemoteOperationMasterRole:$true -Force:$true -LocalAdministrator
Password $AdminPWD -NoRebootOnCompletion:$true
Message Context RebootRequired Status
------- ------- -------------- ------
Sie müssen den Computer neu starten, um den Vorgang abzuschließen... DCPromo.General.2 True Success
PS C:\Users\Stephan-T0>

Na, das sah doch schon viel besser aus! Ich fahre den alten Server herunter. Offensichtlich war es ein Doppel-Hop…

Hintergrund:
Wo soll bei zwei Servern der doppelte Hop versteckt sein? Ganz einfach:

- Via PowerShell Remoting habe ich mich von WS-DC1 zum WS-DC3 verbunden (erster Hop).
- Dort hat das Demoting wohl eine finale Replikation des SYSVOL-Verzeichnisses anstoßen wollen – im Kontext meiner Anmeldung. Da kann es nur ein Ziel geben: Den PDC-Emulator der Domain. Und das ist mein WS-DC1. Also versuchte das Setup, eine Verbindung in meinem Anmeldekontext vom WS-DC3 zum WS-DC1 aufzubauen. Das ist der zweite Hop.
- Weil aber beim ersten Hop meine Credentials nicht auf den Zielserver übertragen werden (daher ist PowerShell-Remoting sehr viel sicherer als eine Remote Desktop Verbindung), konnte ich am Zielserver WS-DC1 nicht angemeldet werden

Das könnte dann so aussehen:

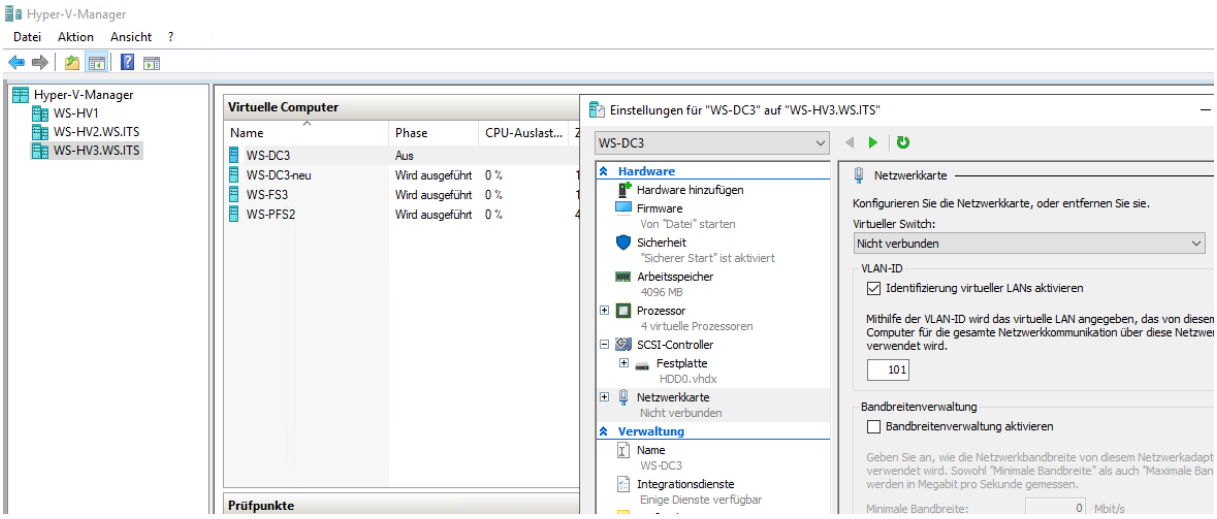


Bereitstellung des neuen Servers

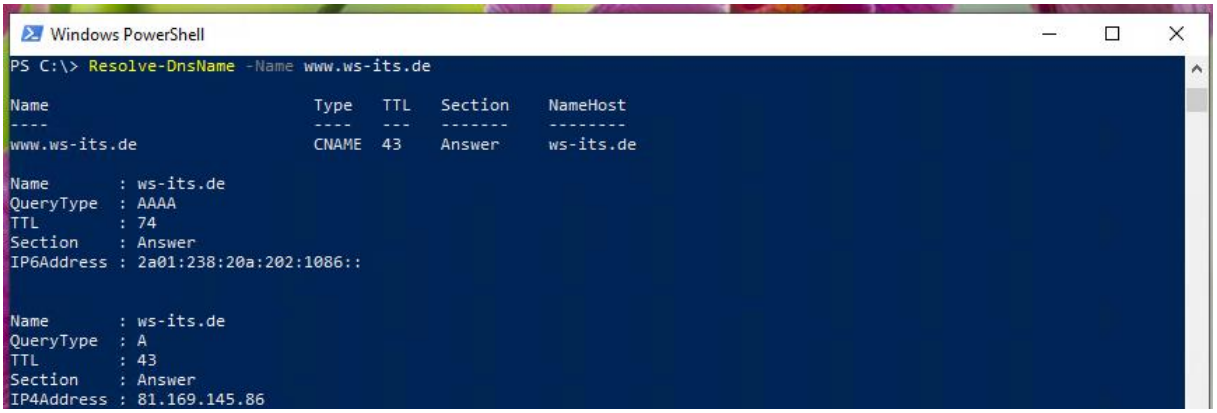
Austausch der VM

Jetzt bin ich eventuell in einer kritischen Übergangsphase. Das Fehlen des Domain Controllers gleichen die beiden anderen DCs aus. Aber das Fehlen des DNS-Servers kann durchaus Probleme verursachen. Daher gehe ich mal ein wenig Gas.

Ich patche den alten Server aus seinem Netzwerk heraus. So kann er mir beim versehentlichen Start nichts tun:



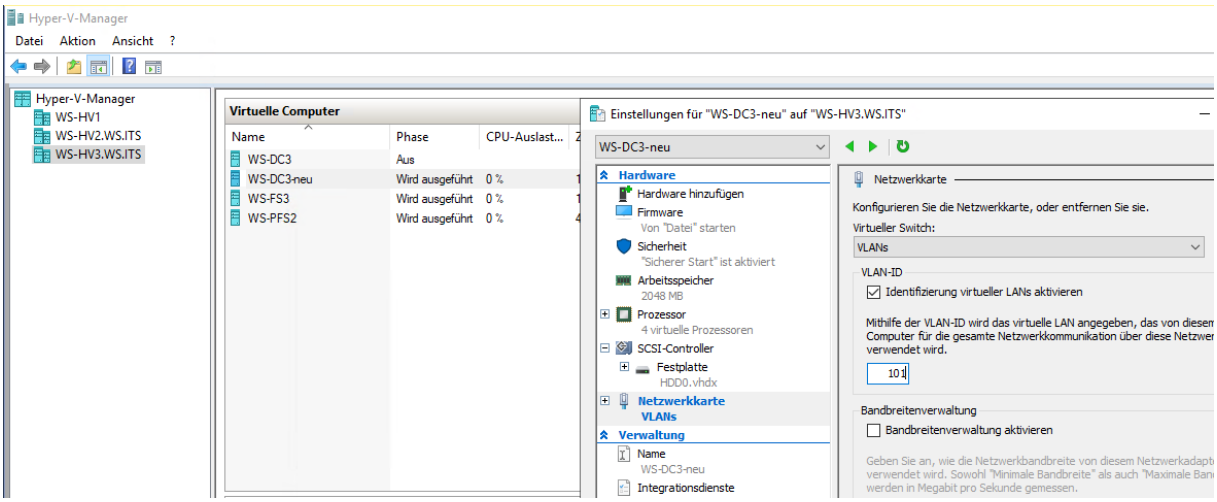
Die Namensauflösung auf meinem Testclient funktioniert weiter, denn dieser hat dank der DHCP-Optionen ja noch einen sekundären DNS-Server:



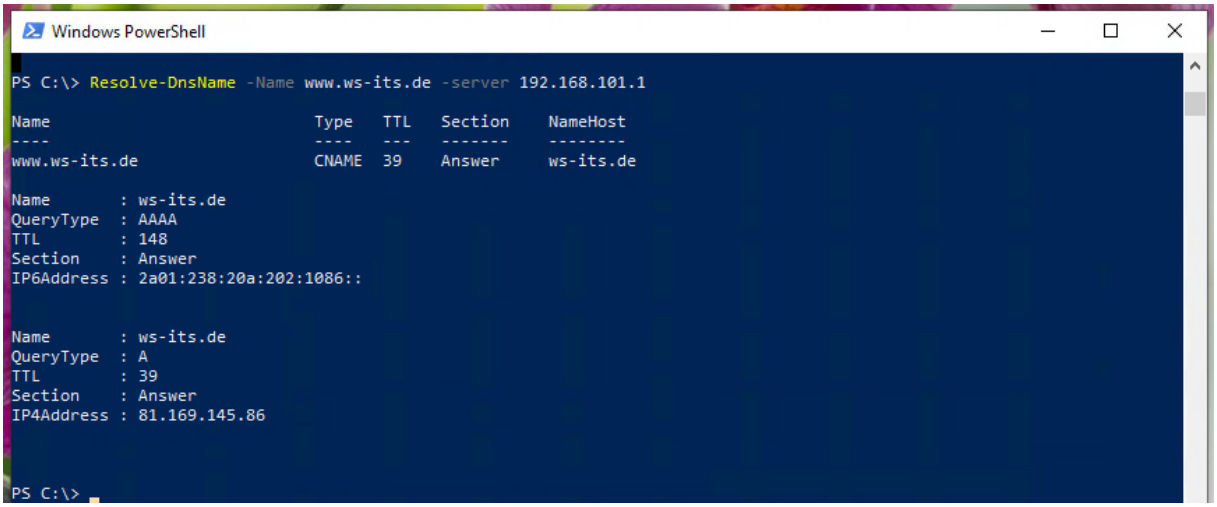
Aber andere Systeme haben vielleicht eine statische Konfiguration ohne zweiten DNS…

Bereitstellung des neuen Domain Controllers

Daher schließe ich nun den neuen Server an mein Server-Netzwerk an:



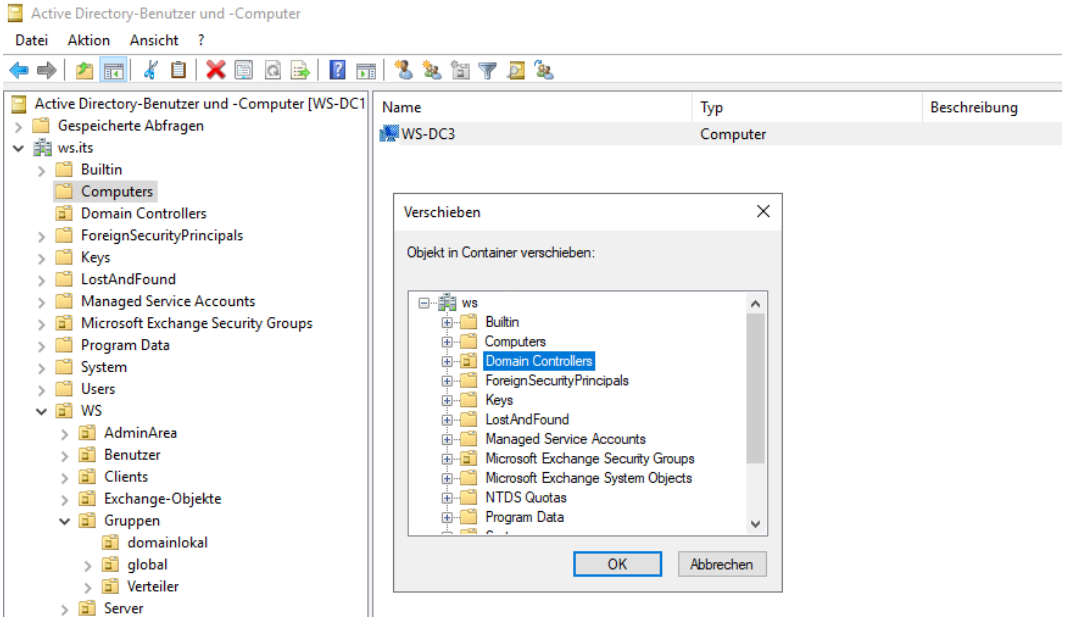
Jetzt werden die Fragen wieder lokal beantwortet. Da der neue Server die gleiche IPv4 wie der alte Server hat und als DNS-Server die Fragen zu einem der anderen DC forwarded, geht alles weiter wie bisher:



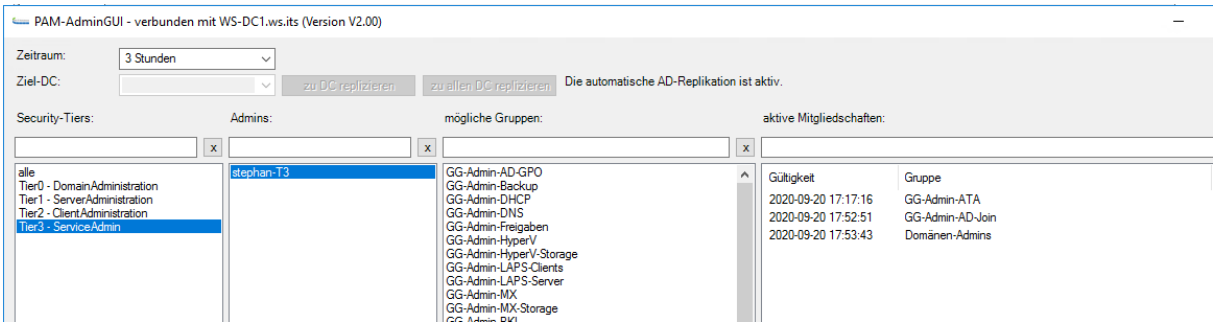
Der Schwenk hat nur wenige Sekunden gedauert.

Betriebssystemvorbereitung

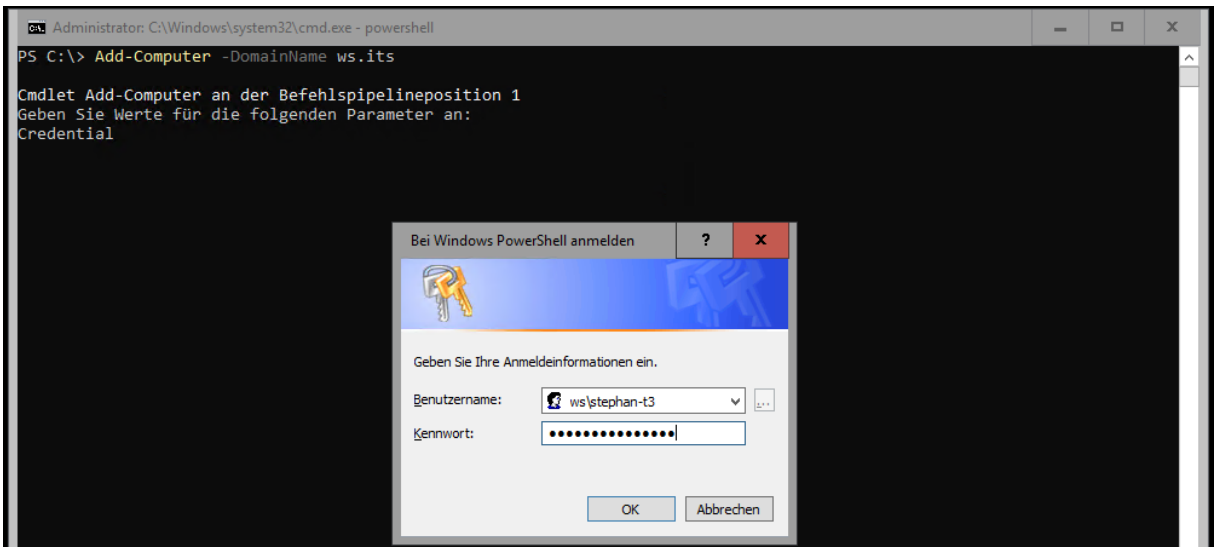
Nun kann ich in aller Ruhe die Rolle Active Directory vorbereiten. Das alte Computerkonto möchte ich wiederverwenden. Nach der Herabstufung liegt es jetzt im Container „Computers“. Ich verschiebe es in die Organisationseinheit „Domain Controllers“. Wenn ich anschließend den neuen Server in die Domain aufnehme, dann zieht er von seiner ersten Minute an nur die Gruppenrichtlinien der DCs:

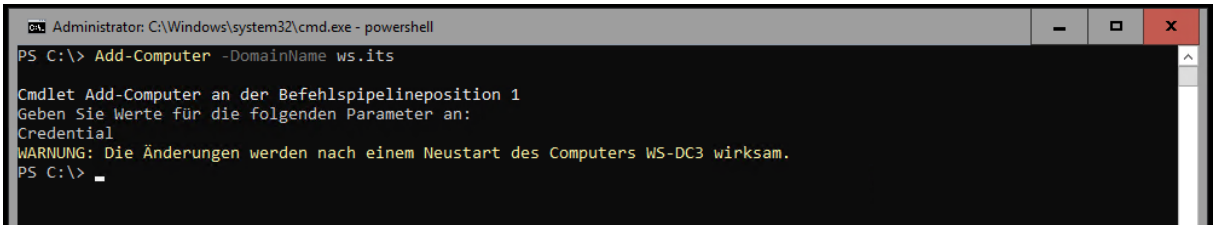


Den Domain-Join führe ich mit einer passenden Admin-Kennung aus. Diese bereite ich im PAM-Tool vor:



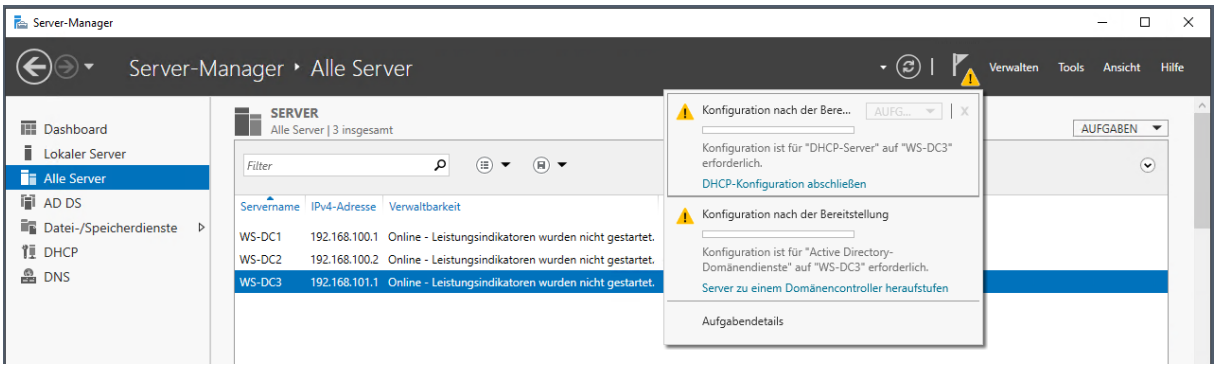
Und dann nehme ich den neuen Server mit der alten Kennung in das Active Directory auf:



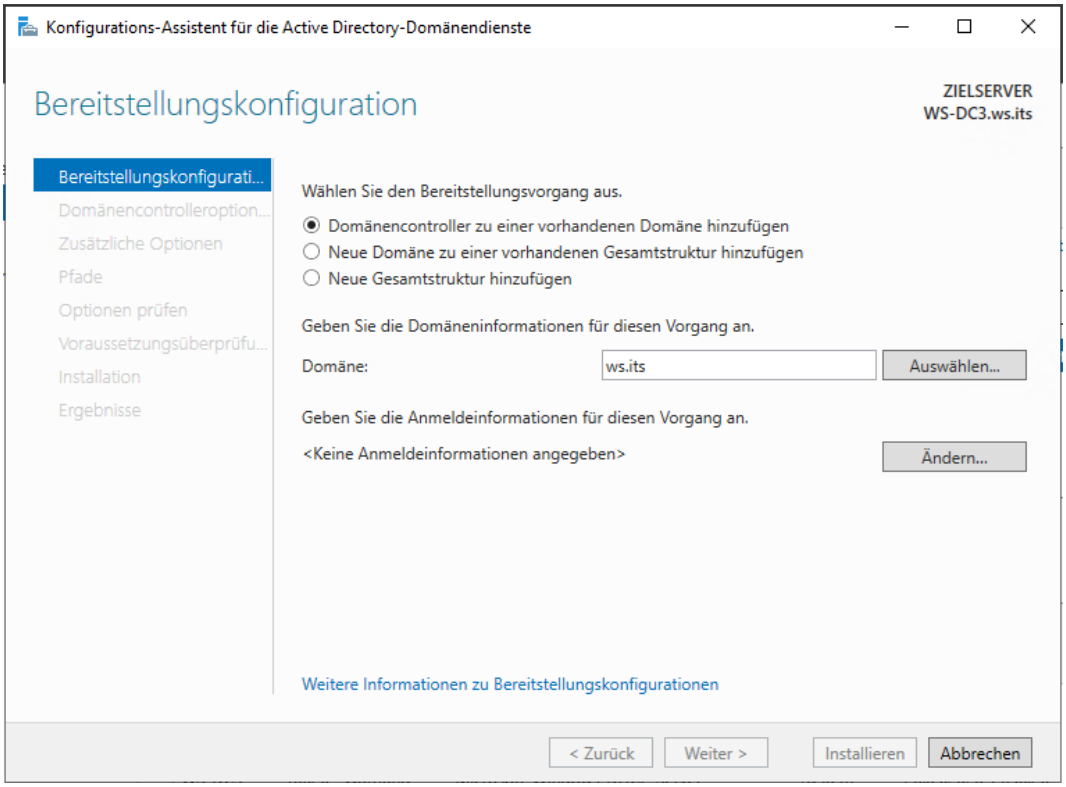


Bereitstellung der Rolle Active Directory

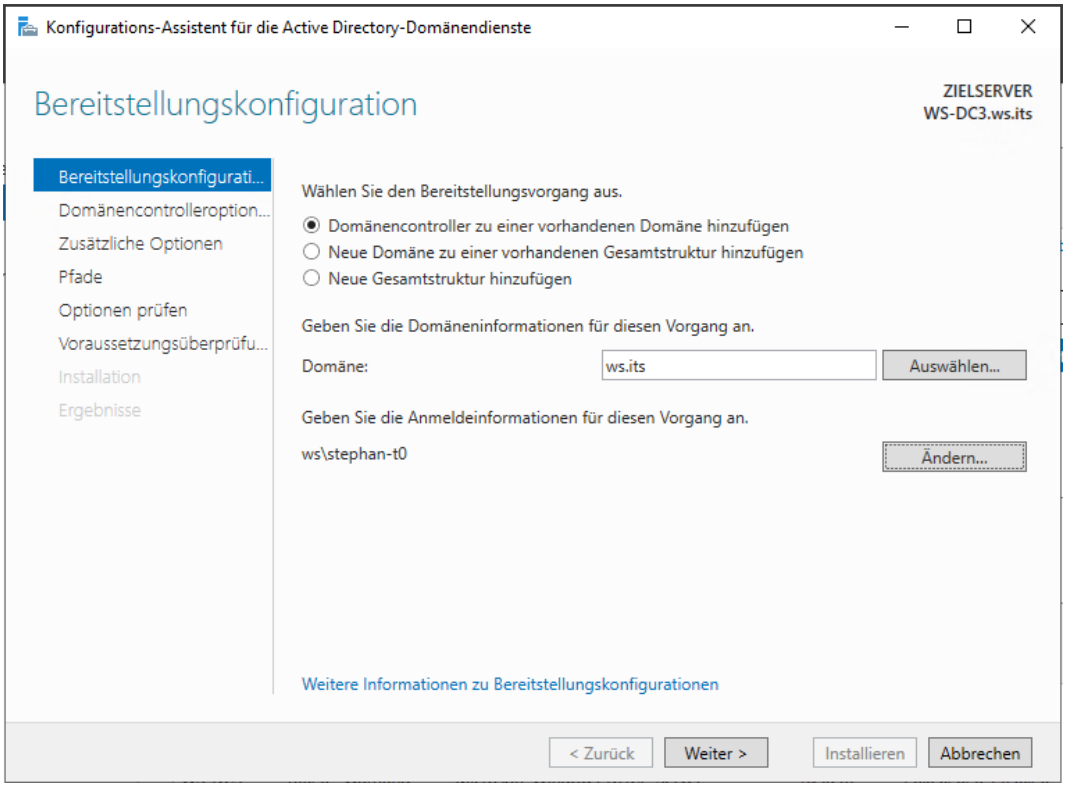
Nach dem Neustart verbinde ich den neuen Server in dem Server Manager von meinem WS-DC1. So kann ich die grafische Unterstützung für die Bereitstellung verwenden. Der Start lässt sich im Infobereich des Server Managers finden:



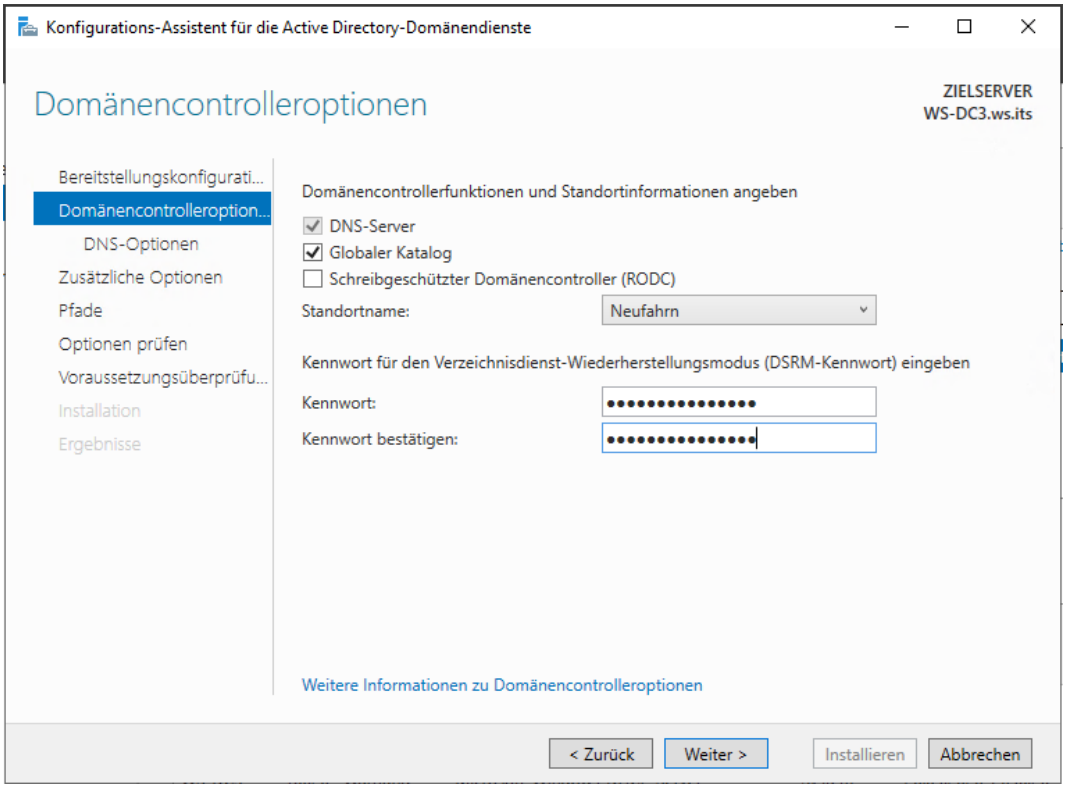
Ab hier ist der Weg wieder bekannt. Der neue Domain Controller soll wie die anderen auch meine Domain ws.its bereitstellen:



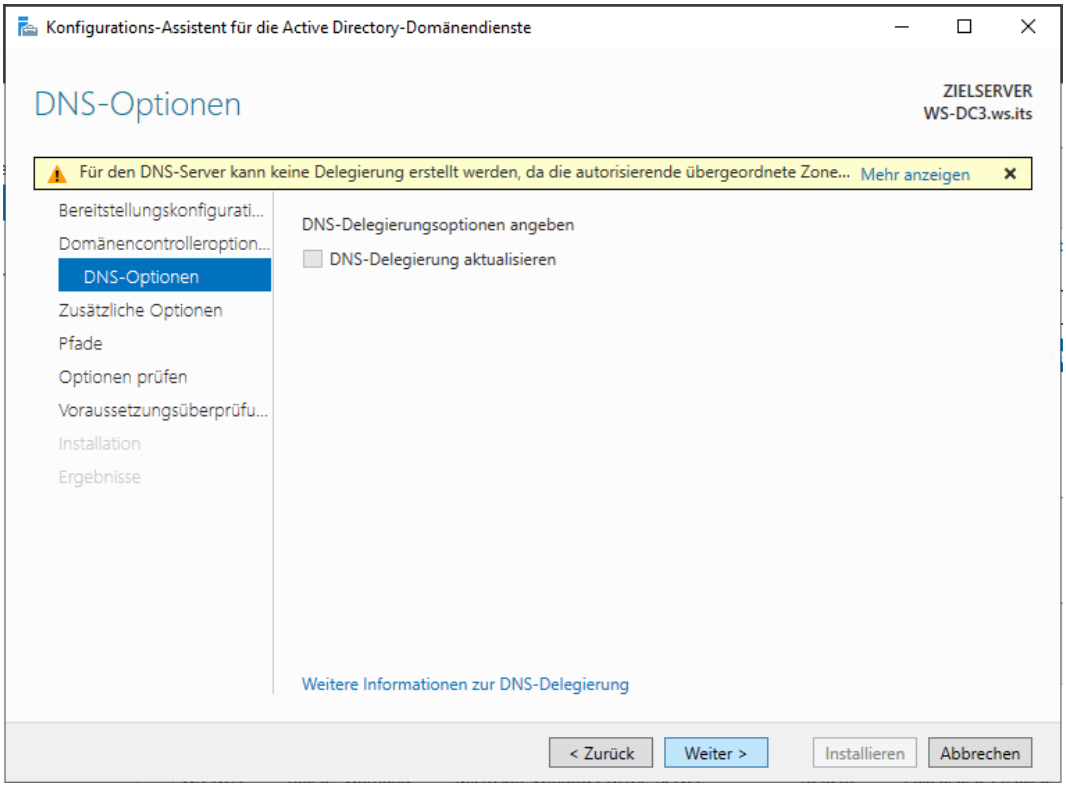
Die Anmeldung verändere ich und nutze meine freigeschaltete Kennung stephan-T0:



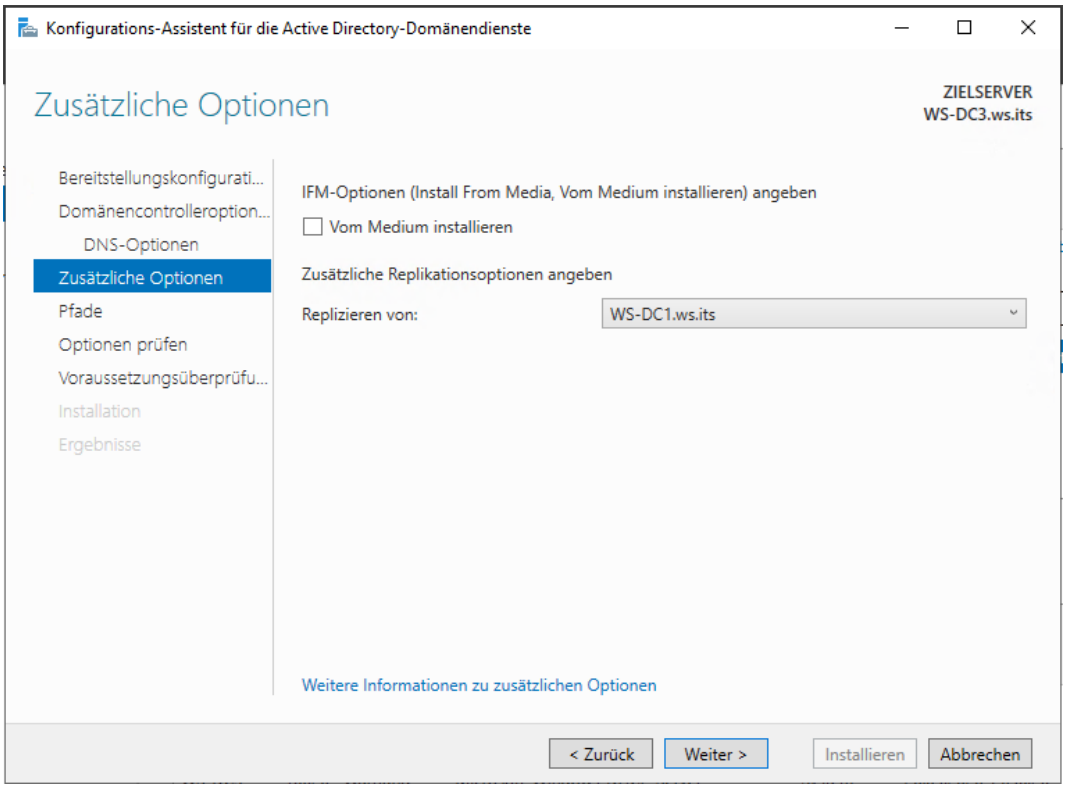
Alle Domain Controller führen bei mir einen globalen Katalog. Der Standort wurde basierend auf der statischen IPv4 richtig erkannt. Das Wiederherstellungspasswort speichere ich in meinem Passwort-Safe:



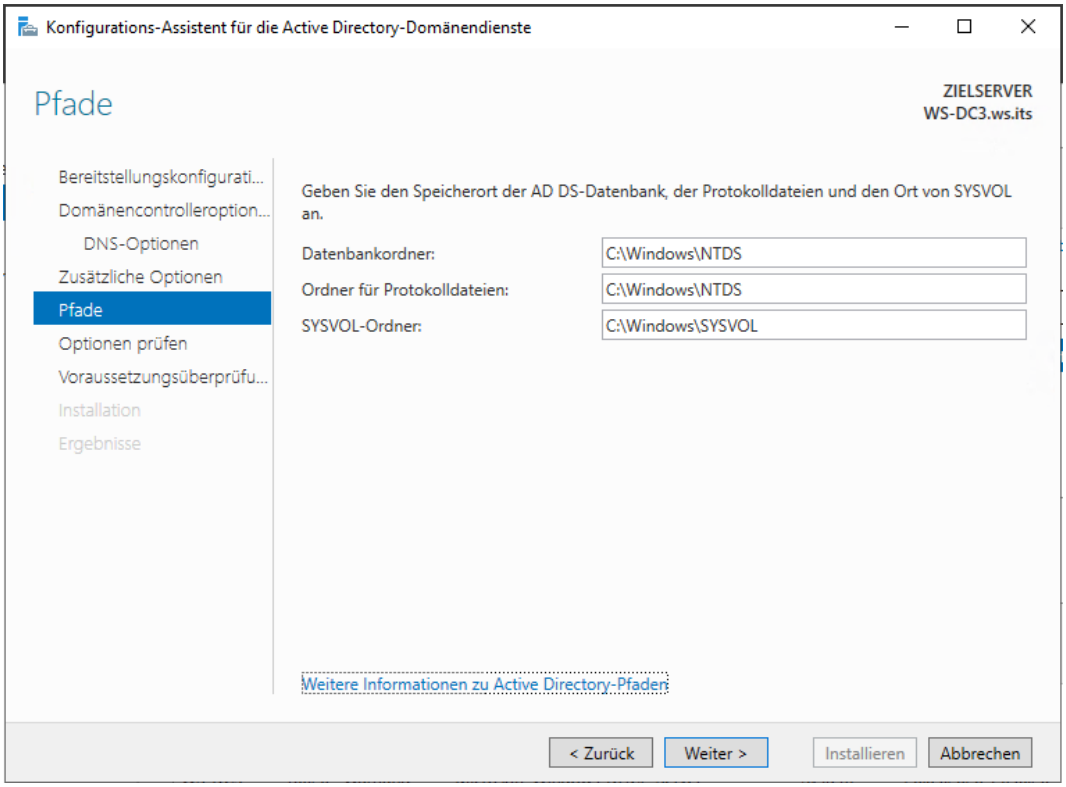
Diese Warnung kann ignoriert werden, denn die Toplevel-Domain *.its gibt es nicht. Also kann ich auch keinen übergeordneten DNS-Server um eine Delegation bitten:



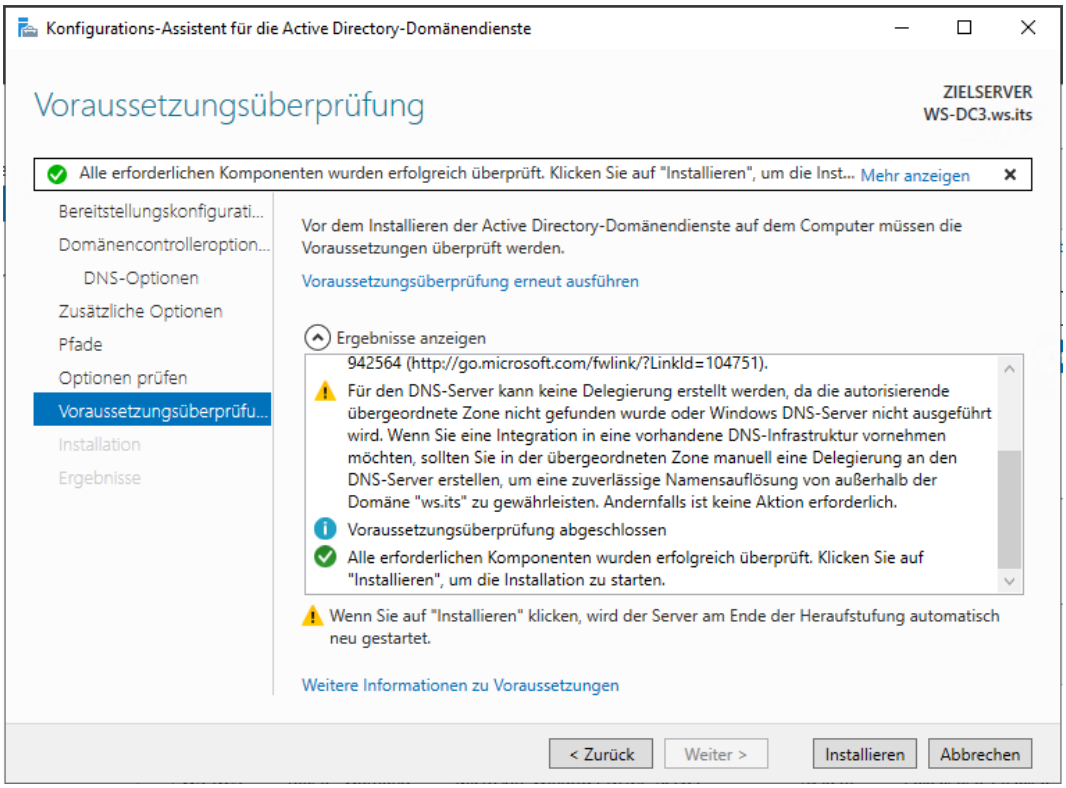
Mein Active Directory ist recht klein. Da kann ich die Replikation einfach über das VPN ausführen:

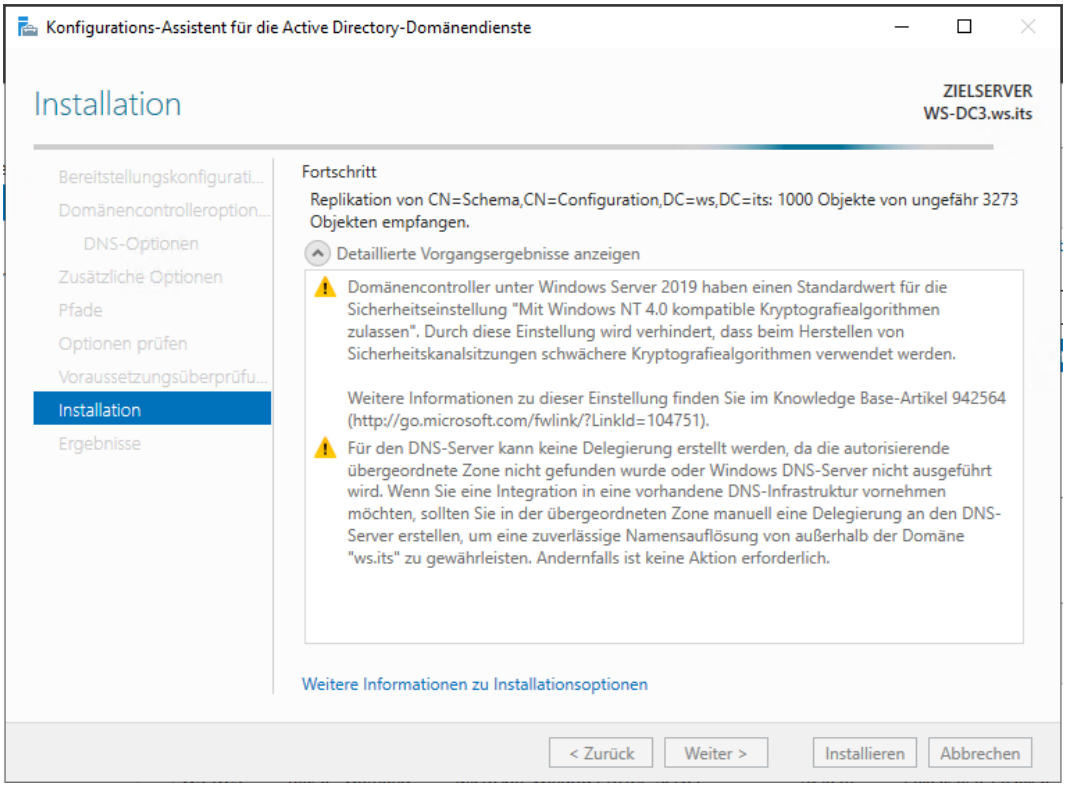


Für einen Pfadwechsel gibt es keinen Grund:



Der Assistent hat einige Vorprüfungen durchgeführt. Also kann es losgehen:

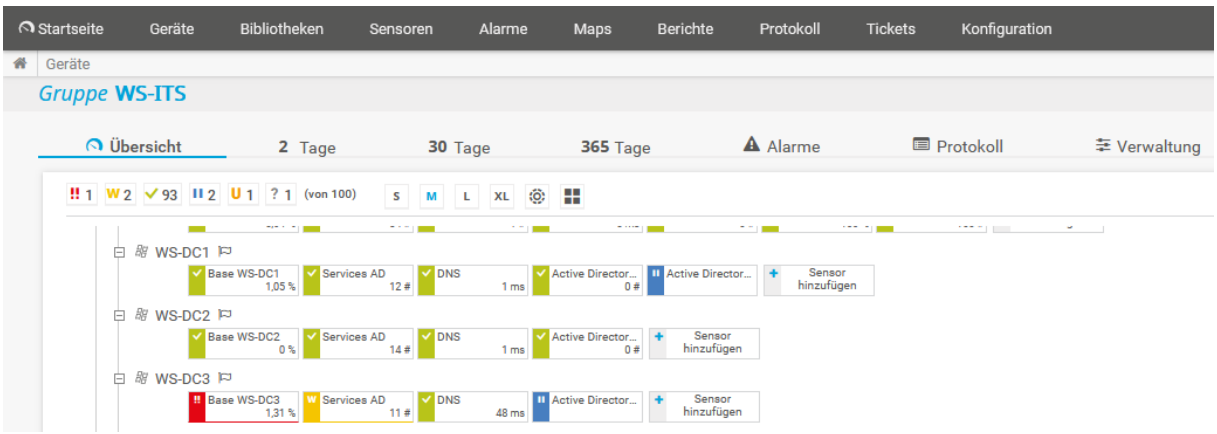




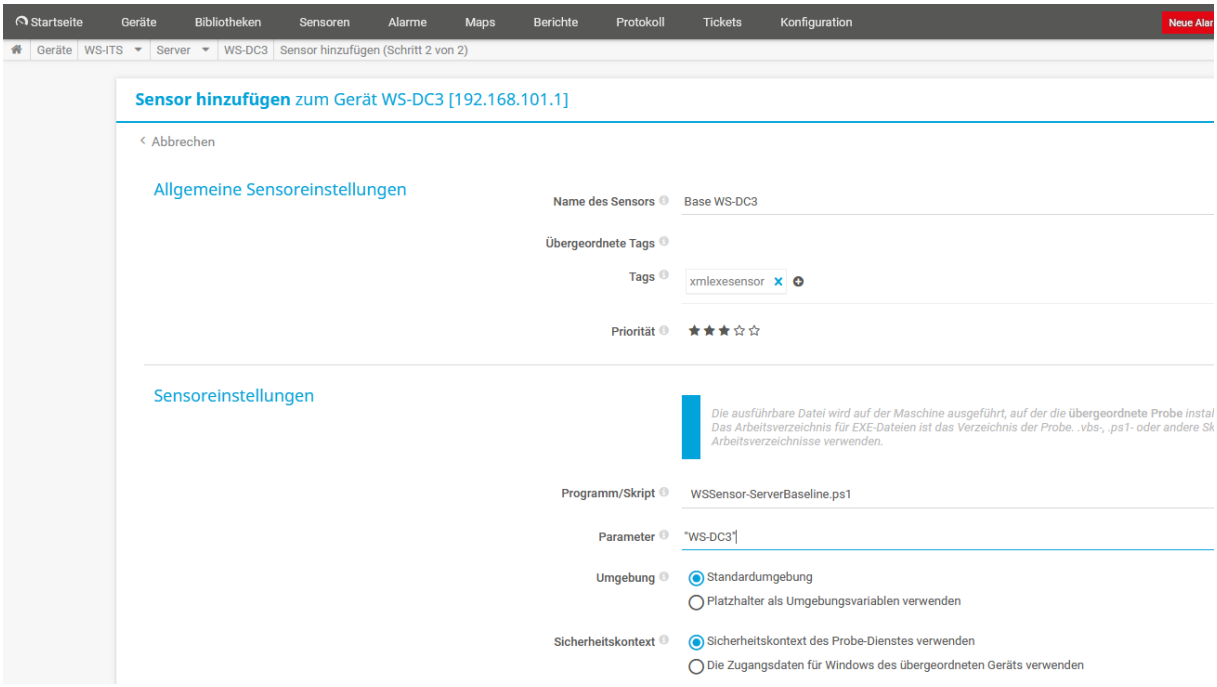
Nach einigen Minuten startet der Server WS-DC3 automatisch neu und kommt als Domain Controller hoch. Die AD-Replikation wird automatisch eingerichtet. Das Ergebnis schaue ich mir später im Monitoring an.

Konfiguration Monitoring

Und mit diesem geht es auch gleich weiter. Mein selbstprogrammierter Sensor „BASE“ findet die alten Festplatten des alten Servers nicht mehr (diese werden durch ihre GUID identifiziert):



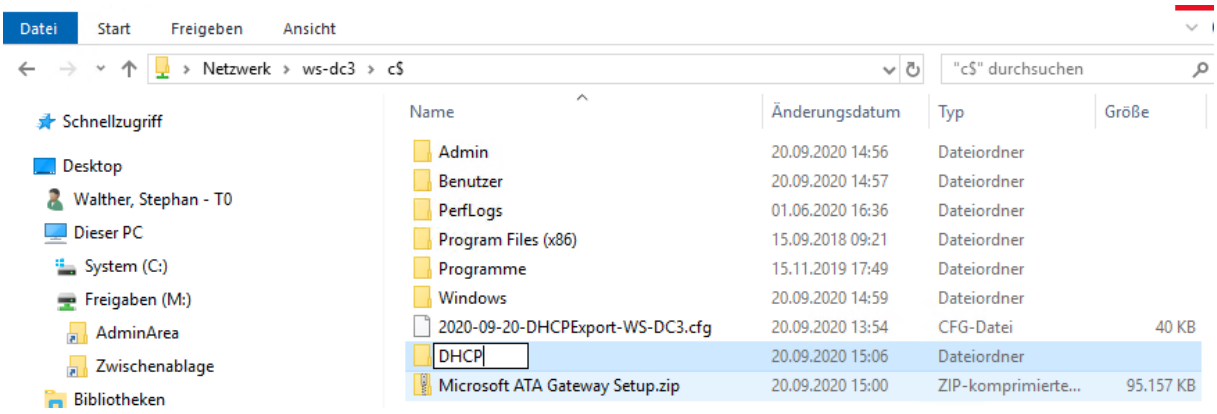
Daher lösche ich den Sensor und erstelle einen neuen:



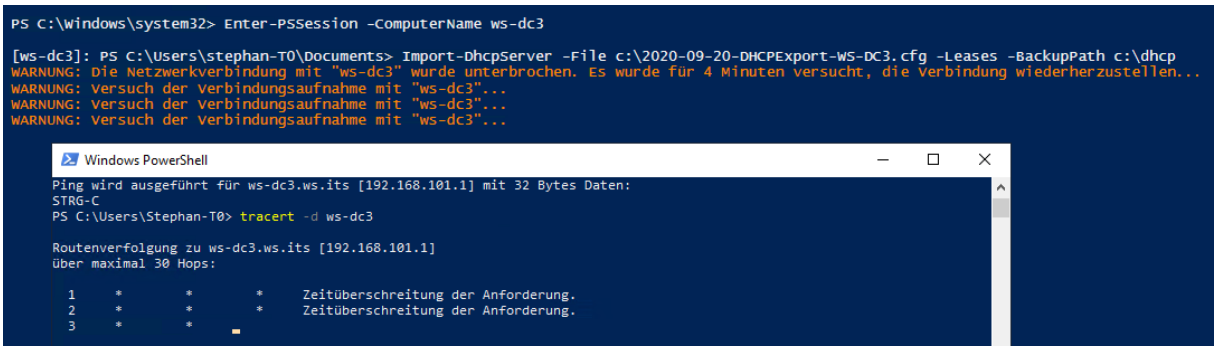
Der Rest passt automatisch.

Bereitstellung der Rolle DHCP

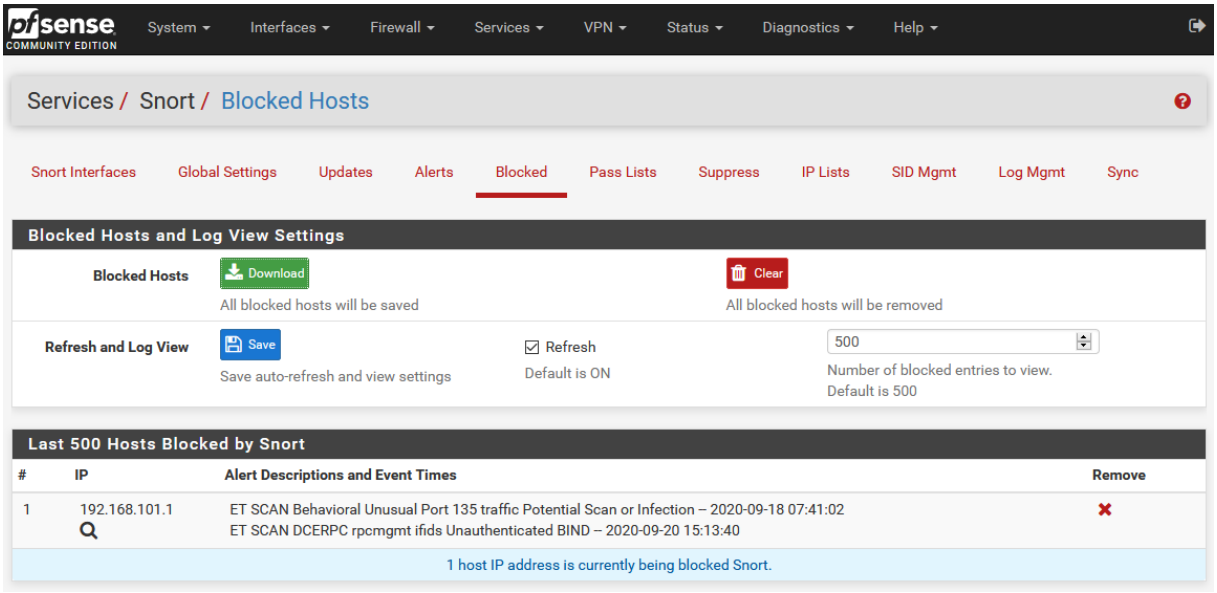
Also wird es Zeit für die anderen Rollen. Ich nehme mir zuerst den DHCP-Service vor. Die Konfiguration hatte ich auf dem alten WS-DC3 in eine Datei exportiert. Diese kopiere ich nun via SMB auf den neuen Server:



Danach importiere ich die Konfiguration in den bereits installierten, aber leeren DHCP-Service. Das soll die PowerShell erledigen. Mit einem PowerShell-Remoting verbinde ich mich mit WS-DC3 und starte den Import. Aber die Verbindung bricht ab! Ich starte zusätzlich ein ICMP-Echorequest (ping). Auch das bleibt unbeantwortet…



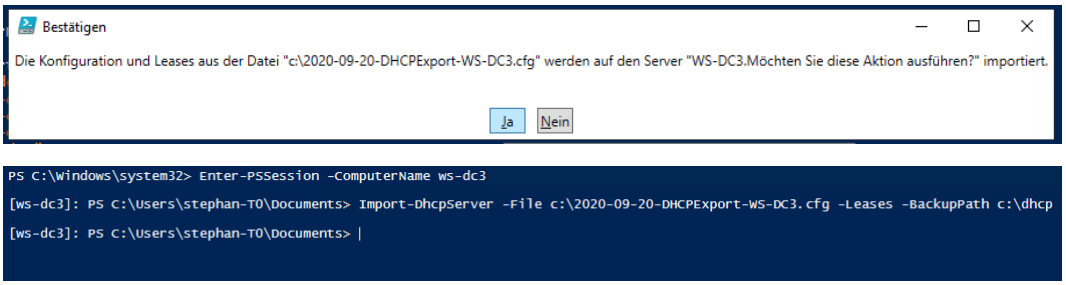
Die Ursache ist schnell gefunden: Mein IPS hat die Verbindung dynamisch blockiert:



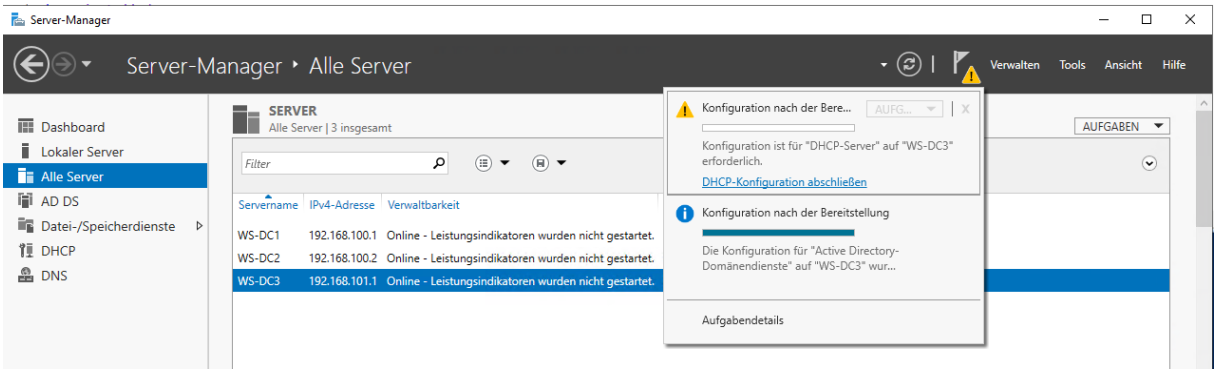
Vielleicht mag sich einer von euch die Frage stellen, wie ich darauf gekommen bin. Das ist einfach:

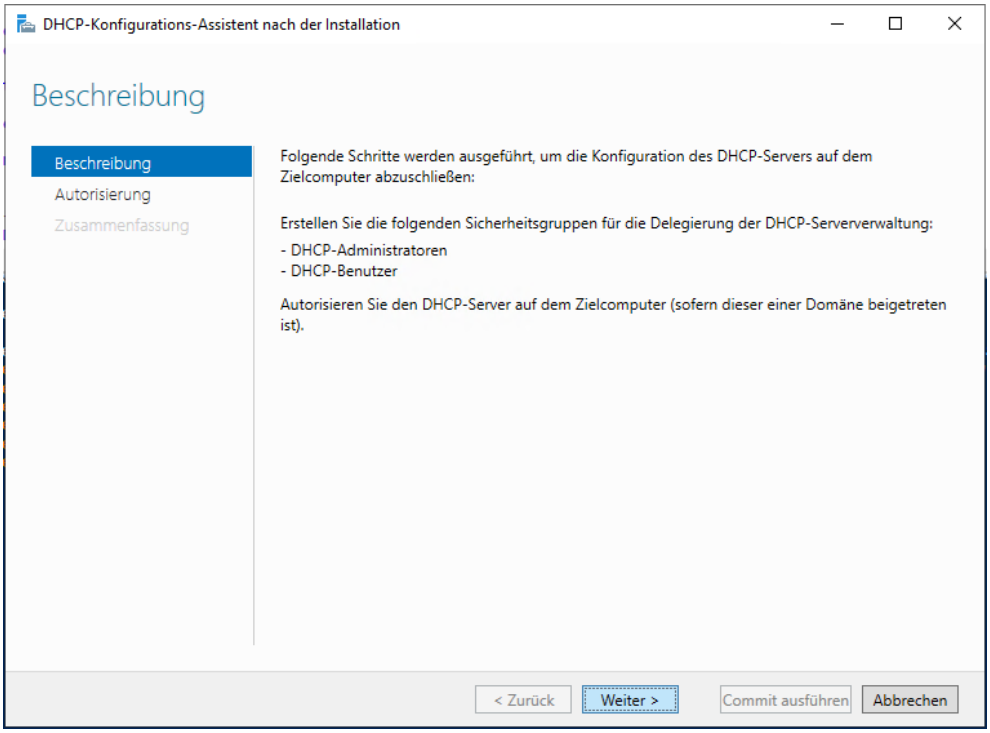
- Ich kenne mein Netzwerk und seine Services sehr genau.
- Und natürlich werde ich auch per Mail informiert, wenn das IPS eine Verbindung sperrt.

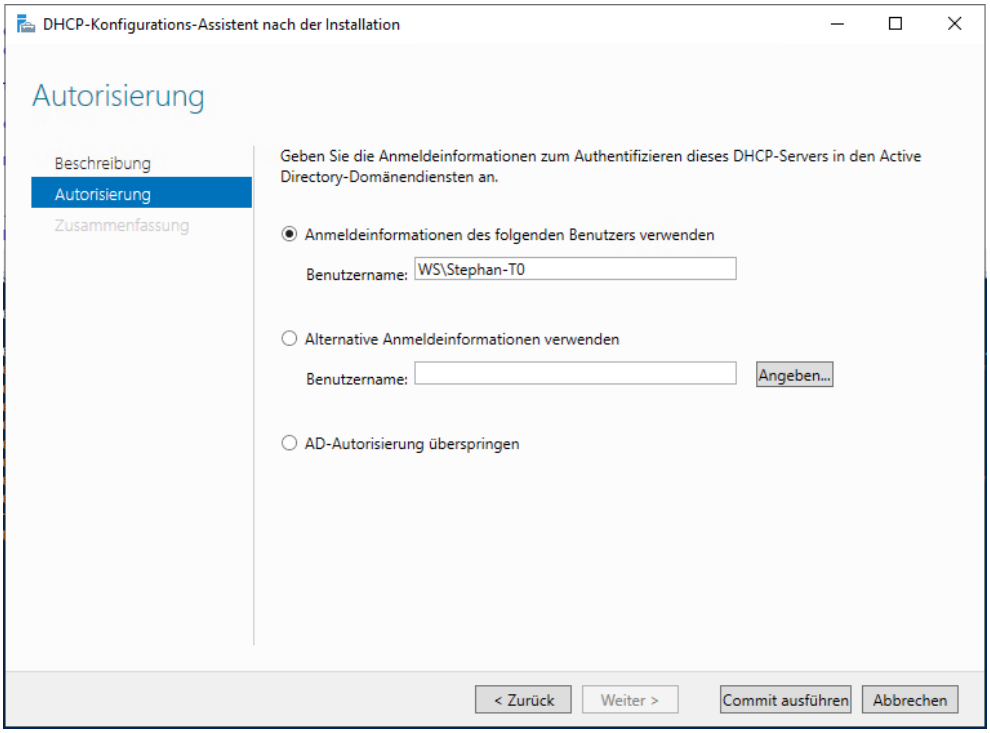
Nachdem ich die Blockierung aufgehoben habe, kann ich nun endlich den Import starten:



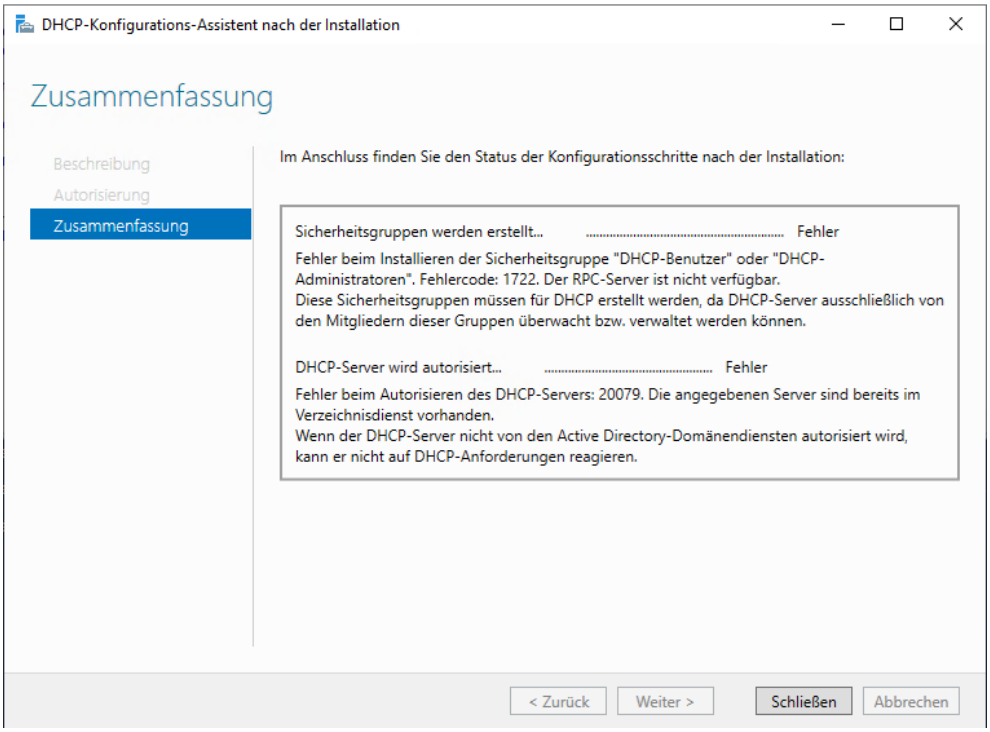
Danach registriere ich den DHCP-Server im Active Directory. Das geht über den immer noch verbundenen Server Manager recht einfach:



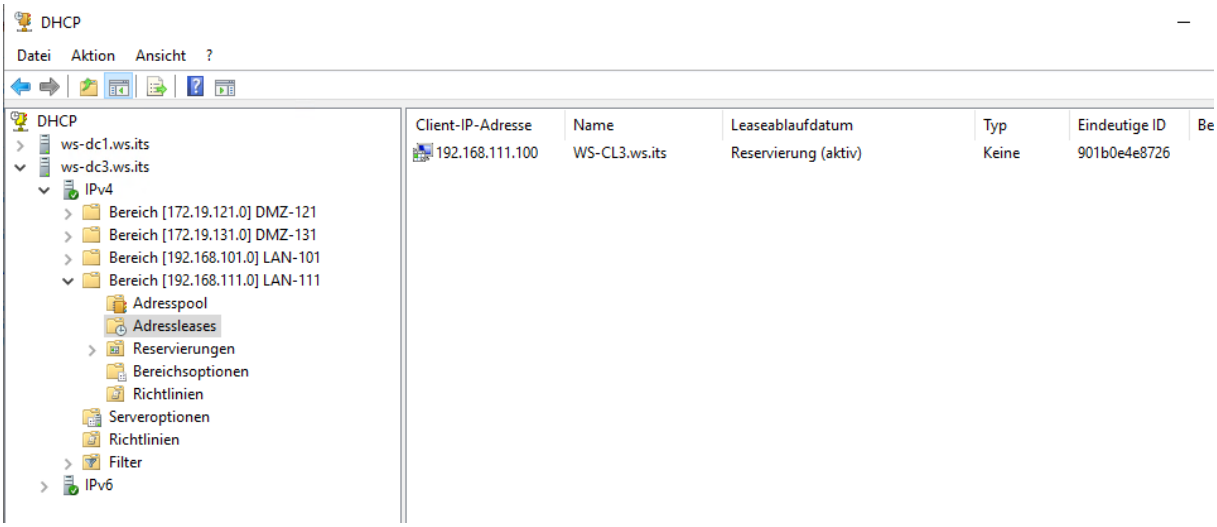




Oder auch nicht…



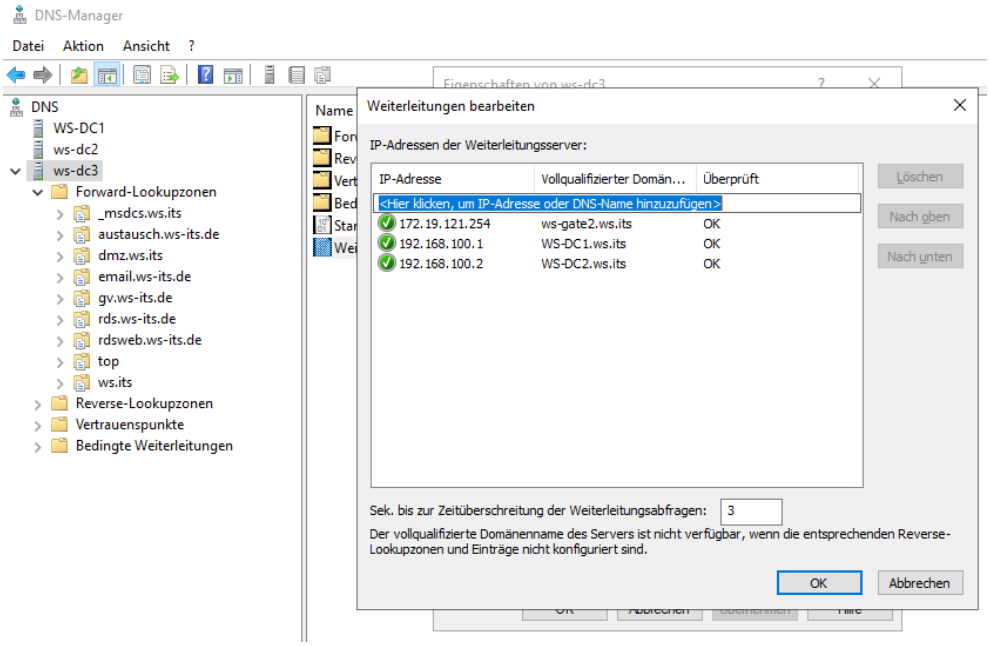
Egal: Die Sicherheitsgruppen gibt es bereits. Und die Autorisierung kann ich auch direkt in der DHCP-Managementkonsole vornehmen. Der Import vom alten Server hat funktioniert. Die Lease-Informationen wurden ebenfalls eingelesen:



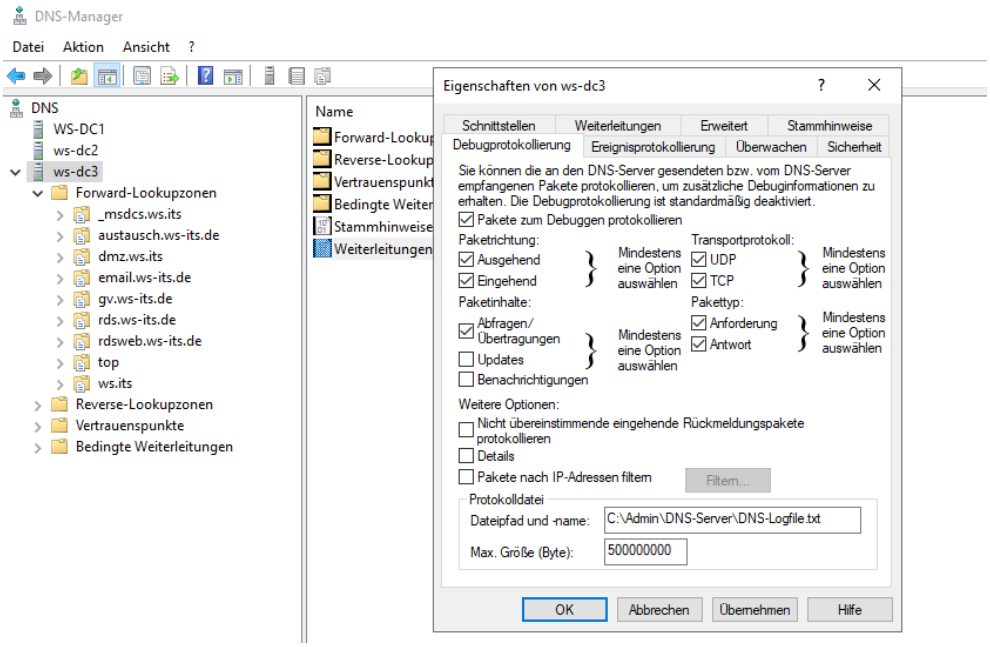
Damit ist diese Rolle wieder einsatzbereit.

Bereitstellung der Rolle DNS

Weiter geht es mit dem DNS-Service. Dieser ist durch seine AD-Integration ja eigentlich schon erreichbar. Aber es fehlt eben noch etwas Feintuning. Ich beginne mit den Forwardern. Primär soll das WS-Gate2 im Außenstandort befragt werden:



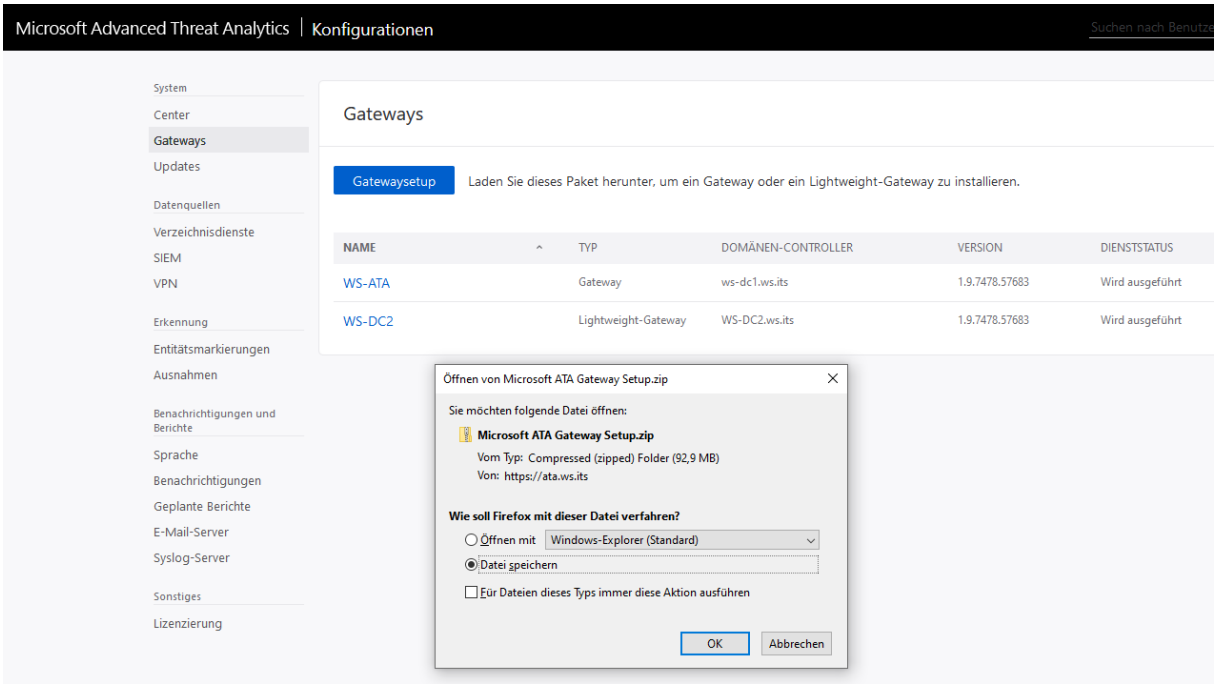
Dann bin ich ein Fan von Logging-Optionen. Daher aktiviere ich proaktiv das DNS-Debug-Log:



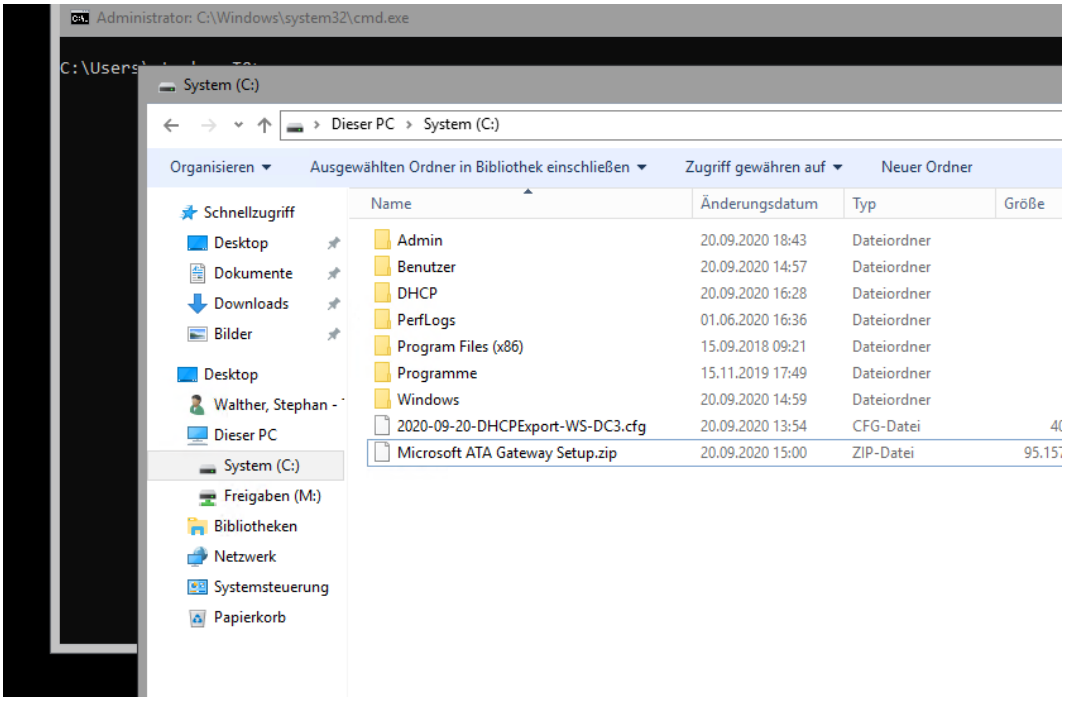
Der Rest soll für den Augenblick passen.

Integration ins ATA (mit TroubleShooting)

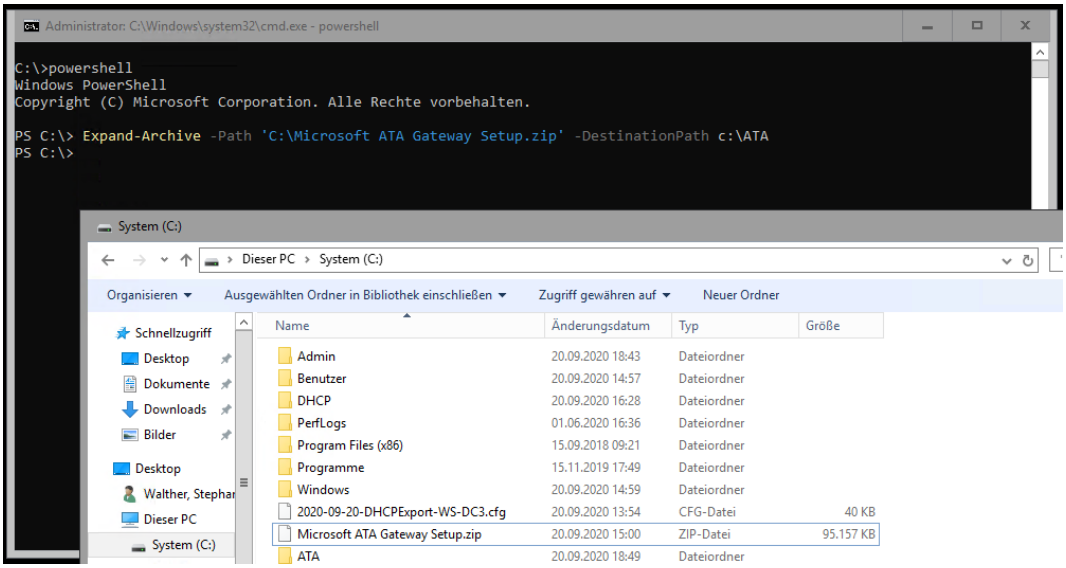
Danach geht es zum Sicherheits-Monitoring. Das übernimmt mein Microsoft Advanced Threat Analytics Service. Aus dem Webportal meines lokalen ATA-Servers hole ich mir das Gateway-Setup heraus:



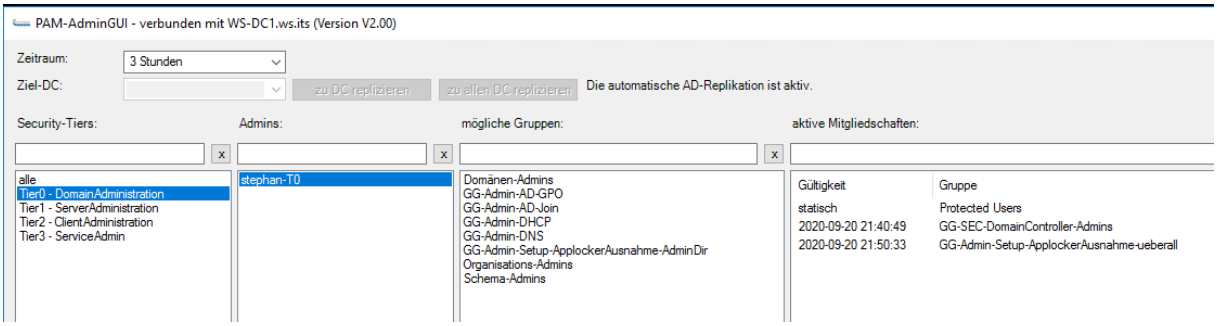
Dieses ZIP bringe ich auf meinen WS-DC3. Dort kann ich mit der cmd einen Windows Explorer starten, denn ich hatte ja mal diese Erweiterung installiert. Blöd nur, dass der Explorer nicht alle Funktionen wie im GUI-Server hat. Ein einfaches Öffnen von ZIP-Archiven ist nicht dabei…



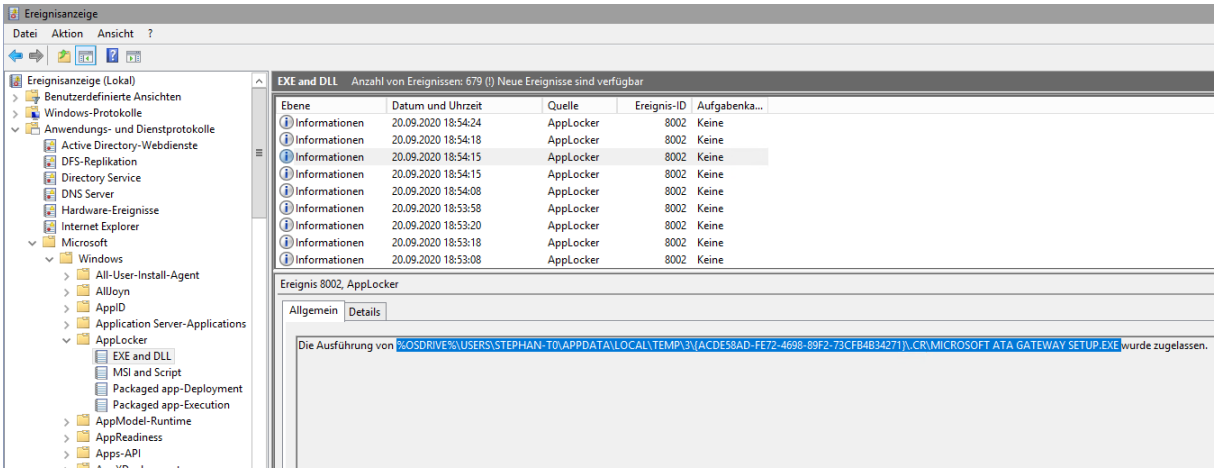
Also starte ich in der cmd die Powershell und entpacke so das Archiv:



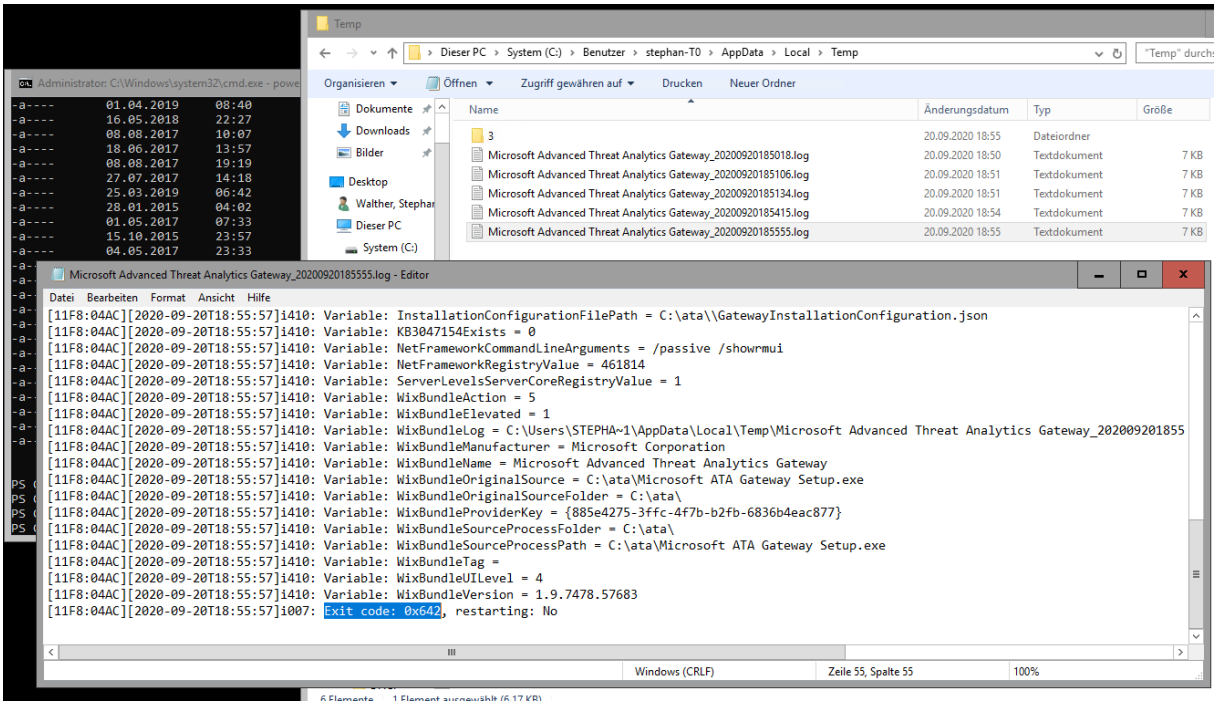
Nun fehlen noch die Installationsberechtigungen. Diese werden meinen Admin-Kennungen auch nur auf Zeit gegönnt und ansonsten 24/7 vom Applocker verwehrt:



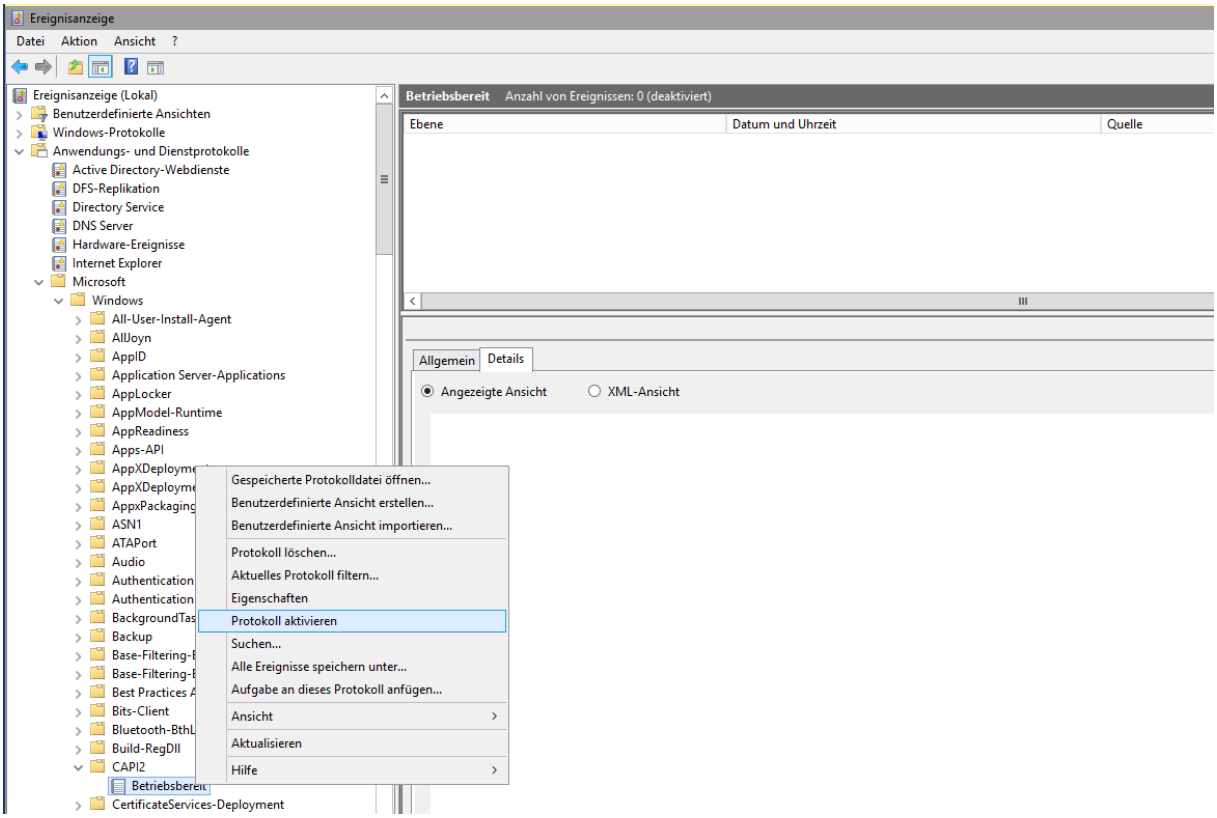
Über den Windows Explorer auf dem WS-DC3 starte ich das Setup. Aber nichts passiert. Das Setup wird nicht sichtbar ausgeführt und bricht anscheinend ab. Eventuell greift meine Applocker-Ausnahme nicht. Daher kontrolliere ich die dazugehörigen Eventlogs. Aber hier passt alles:



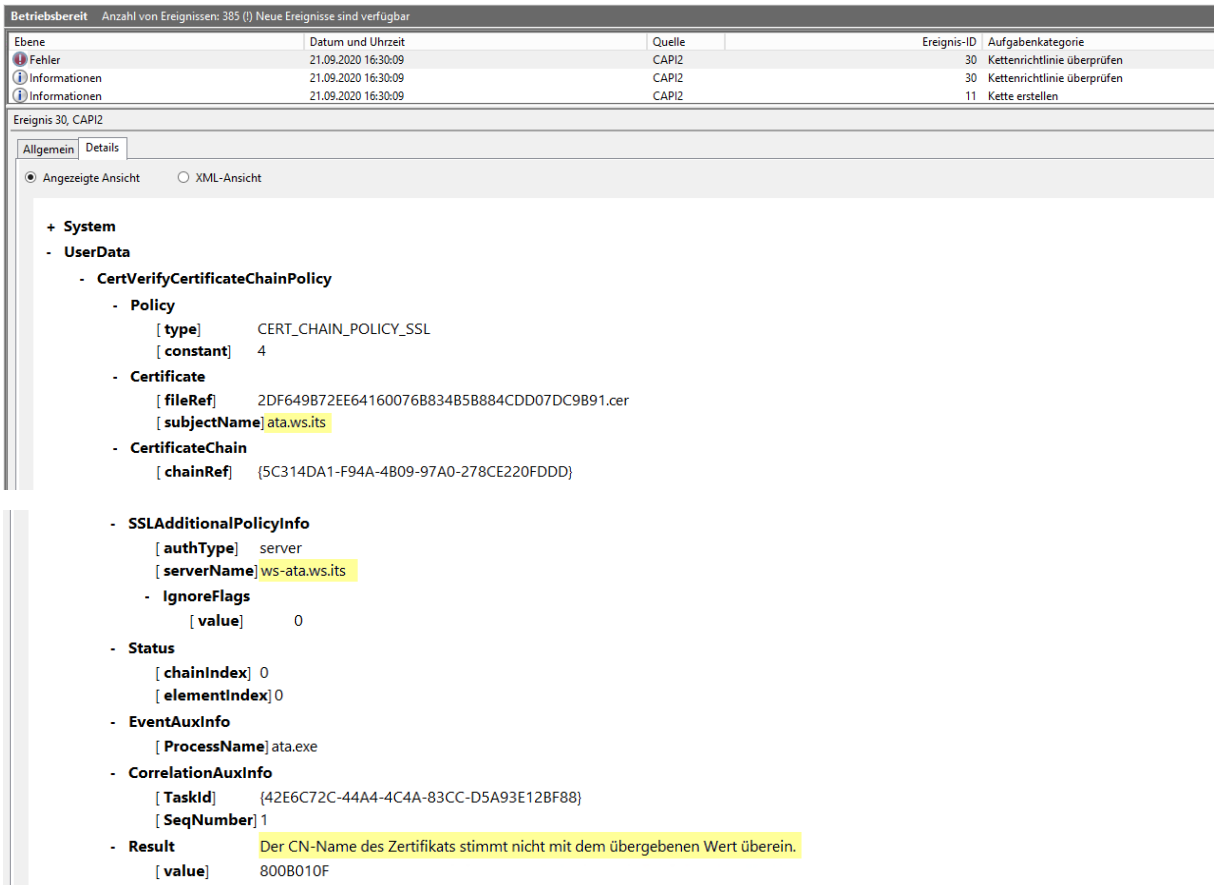
Also muss der Fehler im Setup liegen. Ich finde keine anderen, relevanten Eventlogs. Daher suche ich nach einem Setup-Logfile vom ATA-Gateway. Dieses ist nicht schwer zu finden, wenn man weiß, wo es liegt. Das Logfile selber ist gut lesbar. Je Setup-Versuch wird eine neue Logdatei generiert. Und der Fehlercode ist immer gleich:



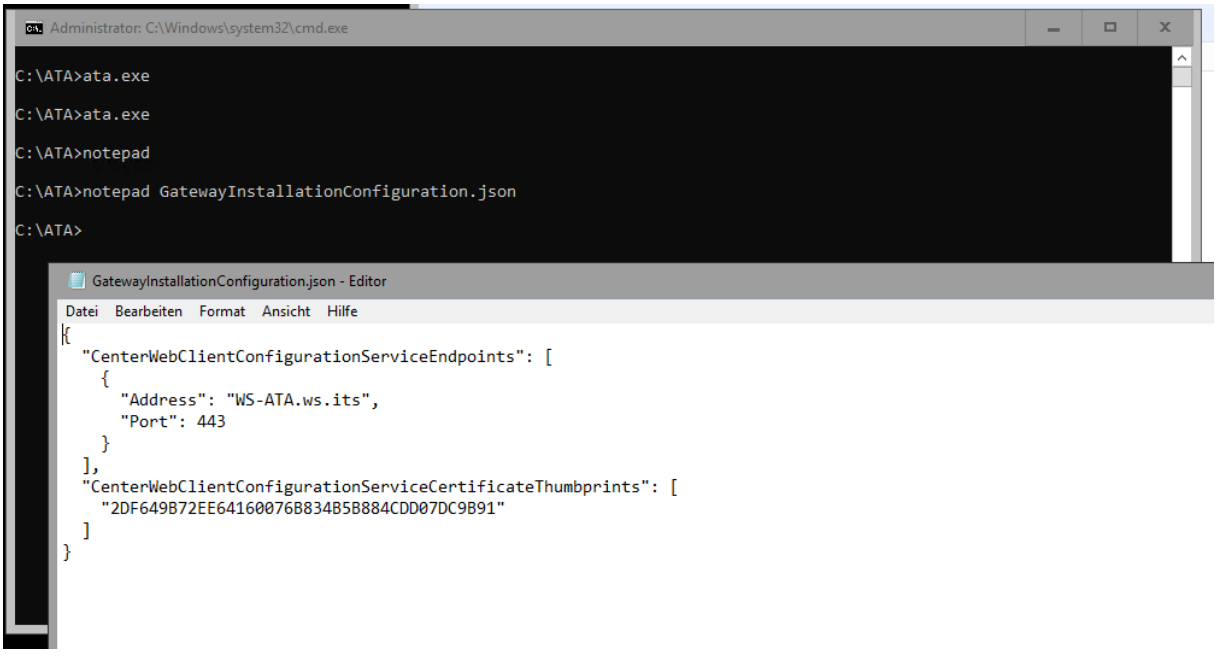
Ich durchsuche mit diesem Code das Internet, finde aber nur unpassende Artikel. Offensichtlich passt da was mit dem Zertifikat nicht. Daher aktiviere ich das CAPI-Eventlog auf dem Server. So kann dieser alle Ereignisse rund um Zertifikatthemen mitschreiben:



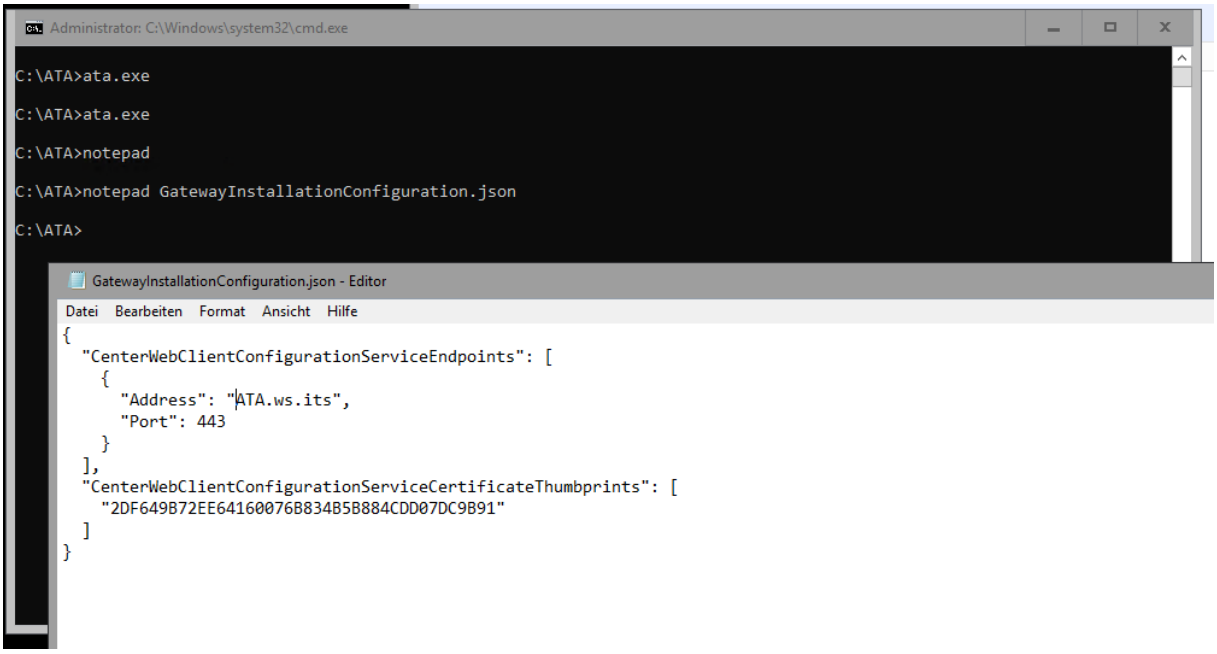
Anschließend starte ich ein neues Setup. Auch dieses wird still abgebrochen. Im CAPI-Log finde ich dann einen Treffer:



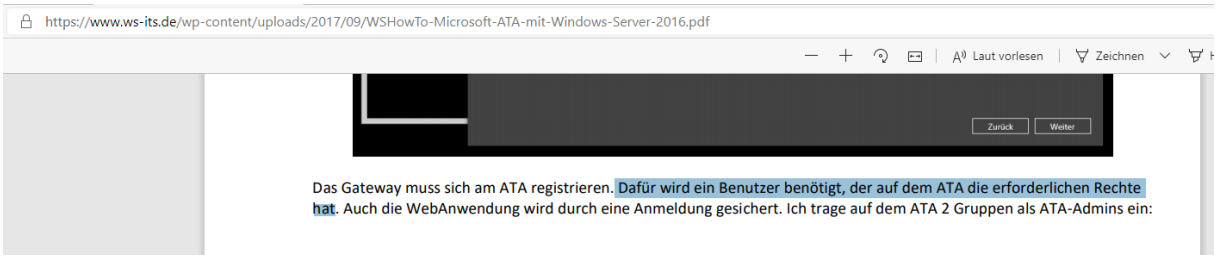
Das ist ja mal wieder klar: der Server meldet sich mit seinem CNAME „ata.ws.its“ (auf den auch das Zertifikat läuft), hat aber in der Config-Datei im Setup seinen FQDN „WS-ATA.ws.its“ mitgegeben. Und dann wird das Setup wegen einem CN-Mismatch abgebrochen. Die Config selber ist eine json-Datei, die im ZIP-Archiv lag. Diese öffne ich mit einem notepad auf WS-DC3:



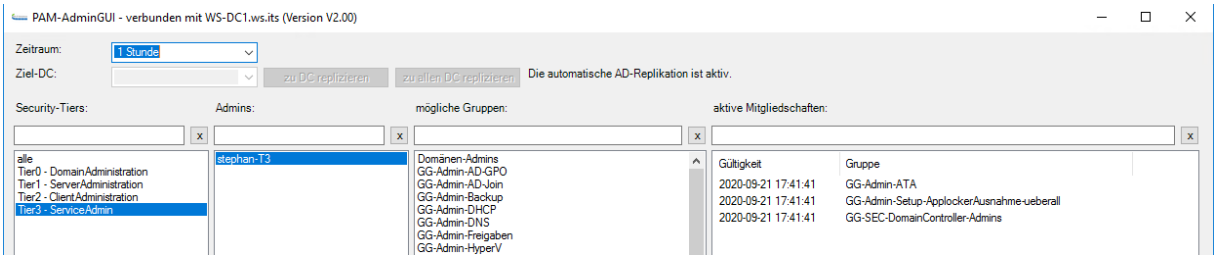
Eine Anpassung soll das Problem lösen. Ich tausche den Servernamen aus:



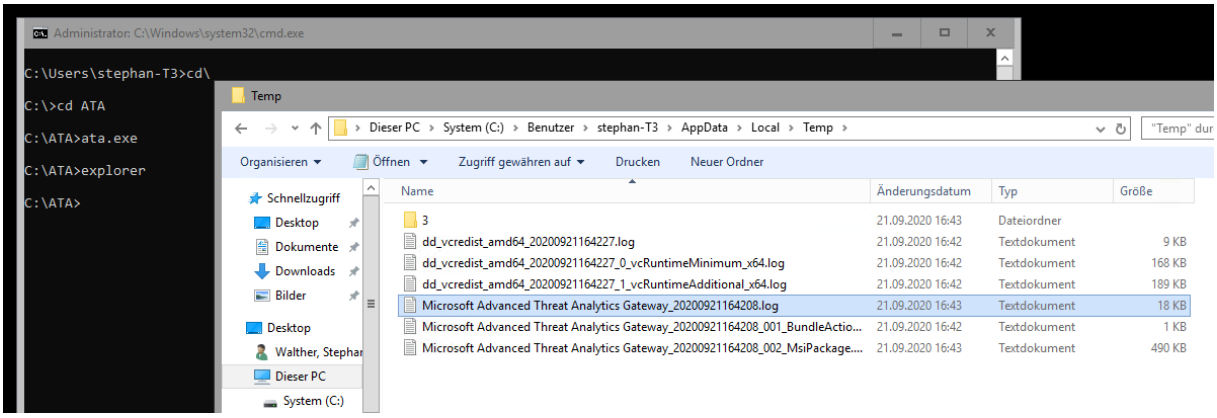
Und dann erinnere ich mich noch an ein anderes Problem bei der Installation des ATA-Gateways. Das hatte ich bei der Bereitstellung meines WS-DC2 (nachzulesen in diesem Artikel):



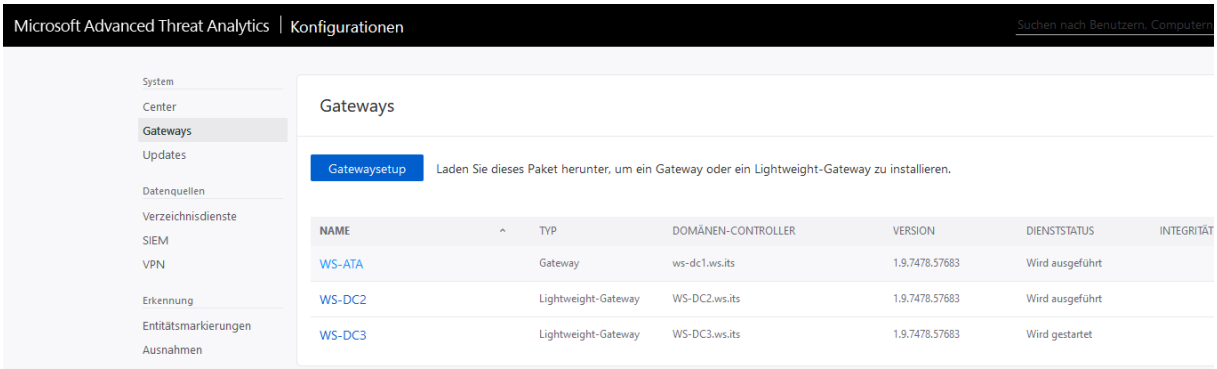
Meine Kennung stephan-T0 hat zwar auf dem Domain Controller die erforderlichen Rechte, ist aber auf dem Memberserver WS-ATA durch meine Security-Scopes mit Null Berechtigungen unterwegs. Also bereite ich eine Brücken-Kennung vor und nehme meinen Admin-Account stephan-T3 temporär in die Admingruppe für die Domain Controller und in die ATA-Sicherheitsgruppe auf:



Mit dieser Kennung starte ich das Setup erneut:



Das Setup selber ist immer noch silent. Aber in der ATA-Webkonsole registriert sich der neue WS-DC3:

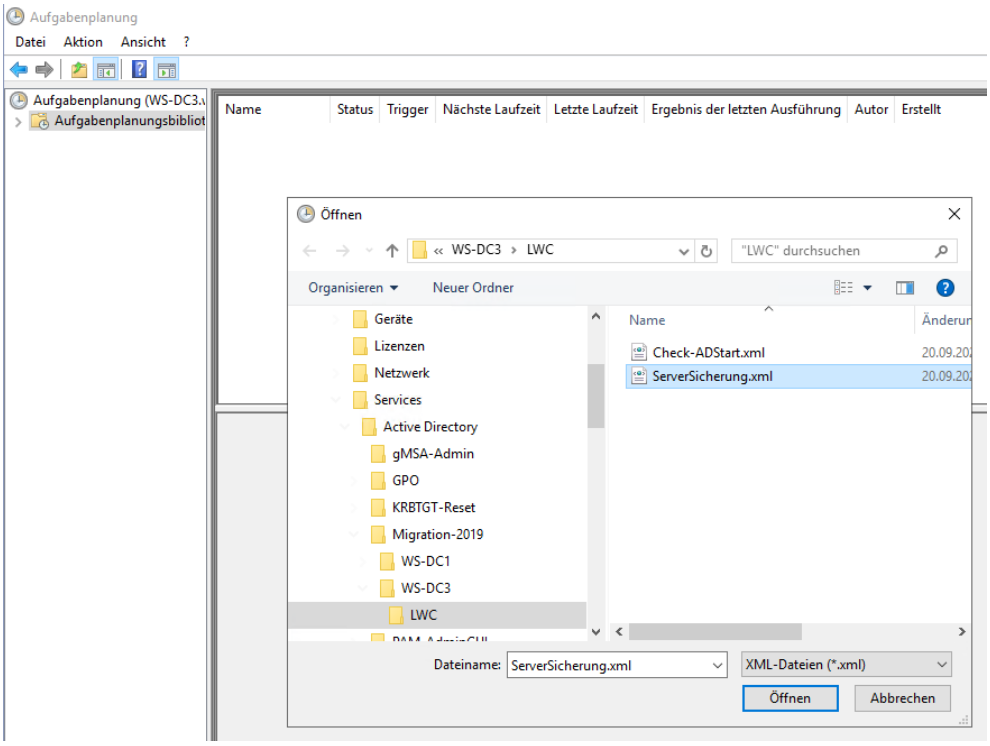


Damit habe ich wieder alle sicherheitsrelevanten Events auf den Domain Controllern im Blick.

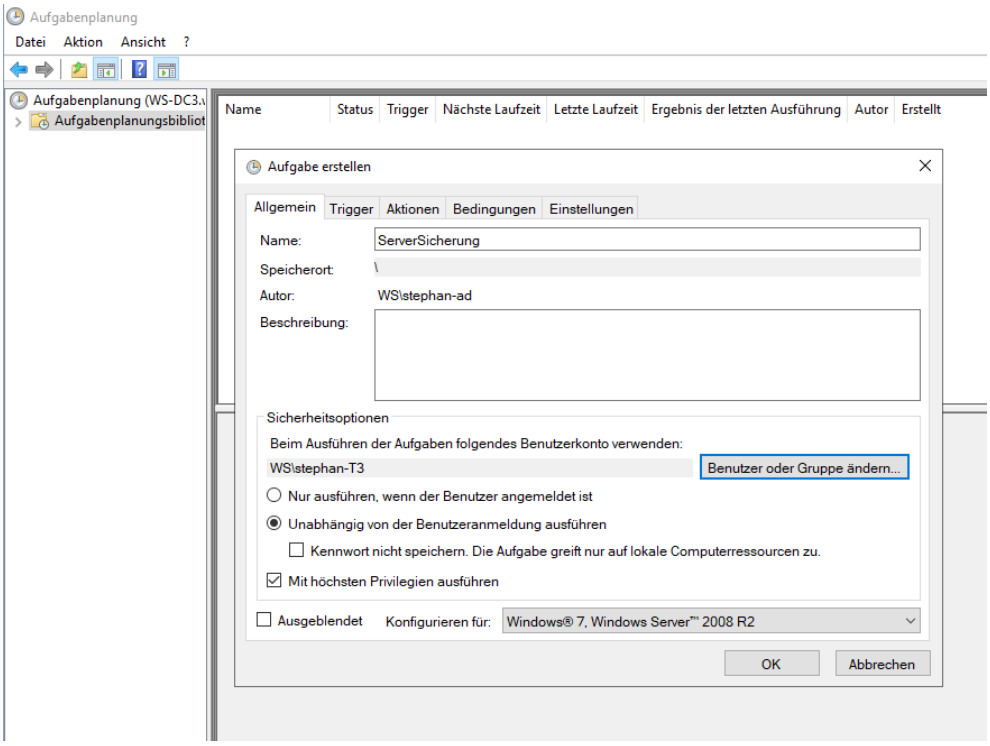
Nacharbeiten

Datensicherung des Windows Servers

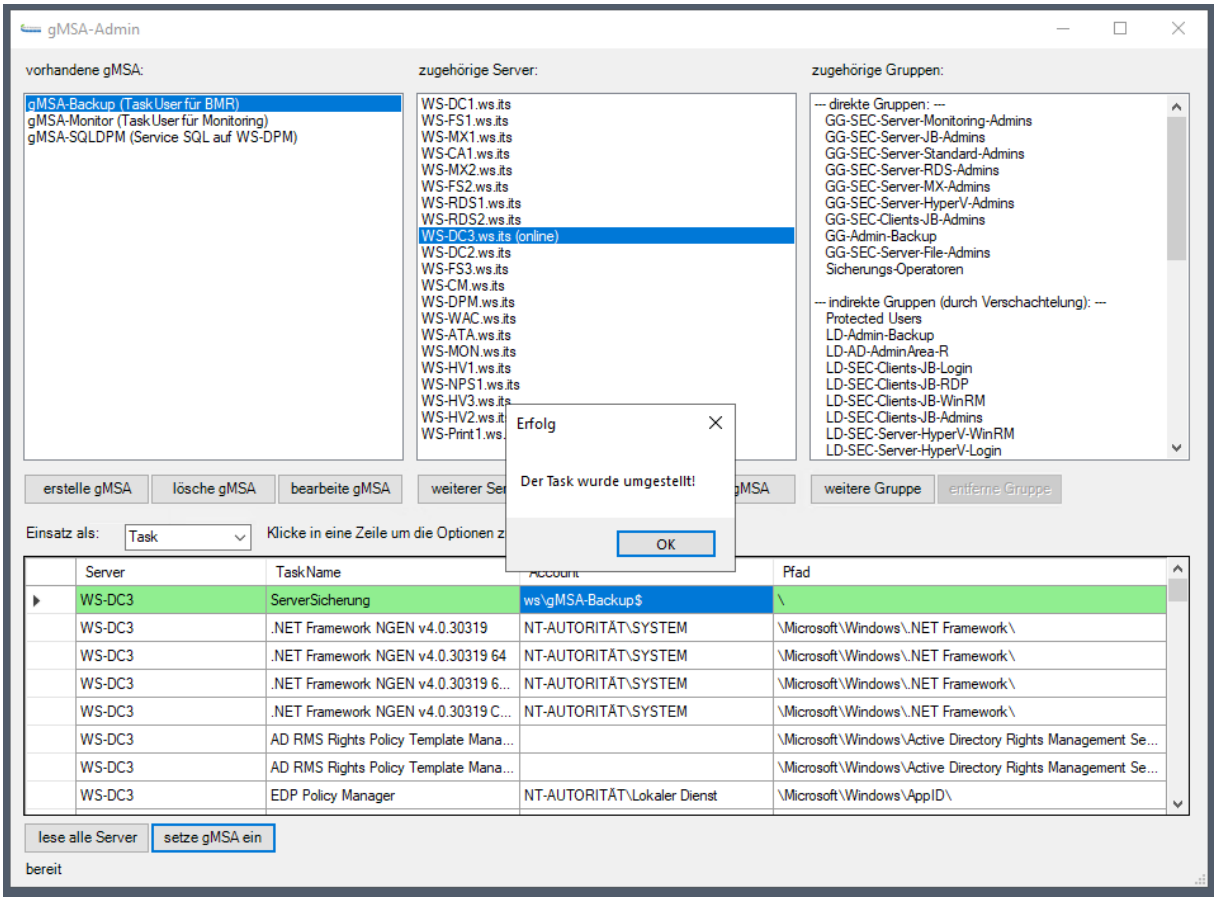
Nach der Aktivierung des Betriebssystems fehlen nun noch einige Nacharbeiten. Dazu gehört die Einrichtung der Datensicherung. Auf dem neuen Server verwende ich das Windows Backup Feature, dass ich über ein Script aufgabengesteuert laufen lasse. Die Aufgabe importiere ich als XML:



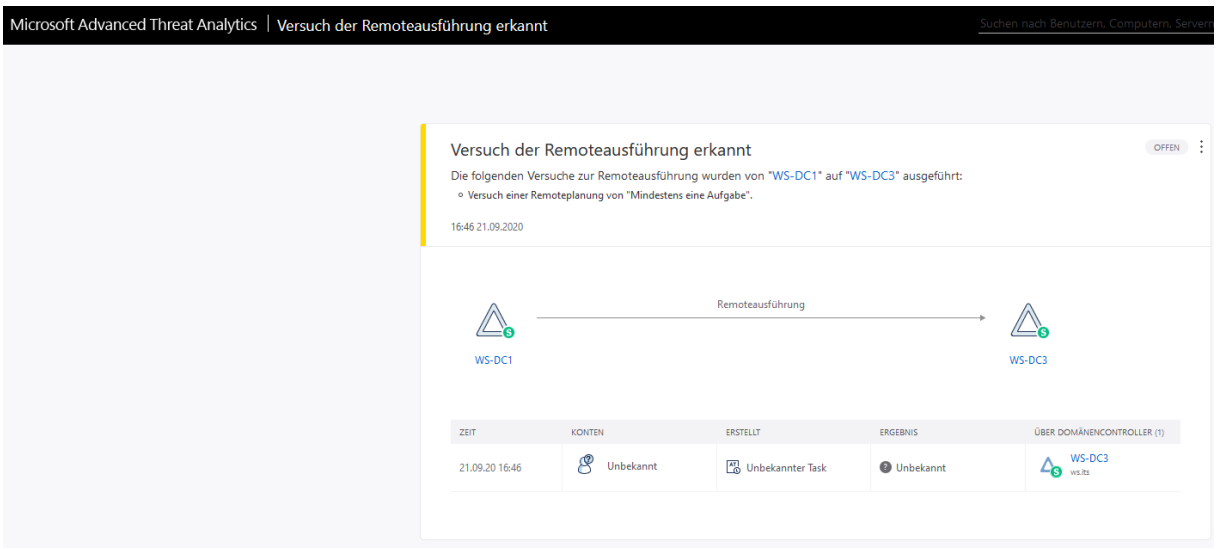
Temporär trage ich meine Admin-Kennung als Task-Account ein:



Mit meinem gMSA-Admin-Tool kann ich dann den richtigen Sicherungsaccount eintragen. Das ist dann ein Group Managed Service Account:



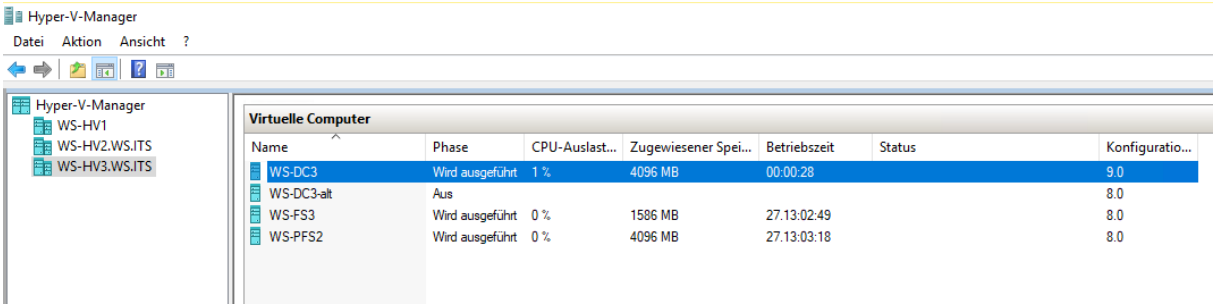
Direkt im Anschluss bekam ich eine Mail vom ATA-Service. Dieser hat eine unbekannte Aktion erkannt und eine Sicherheitswarnung ausgegeben. Das System ist also aktiv:



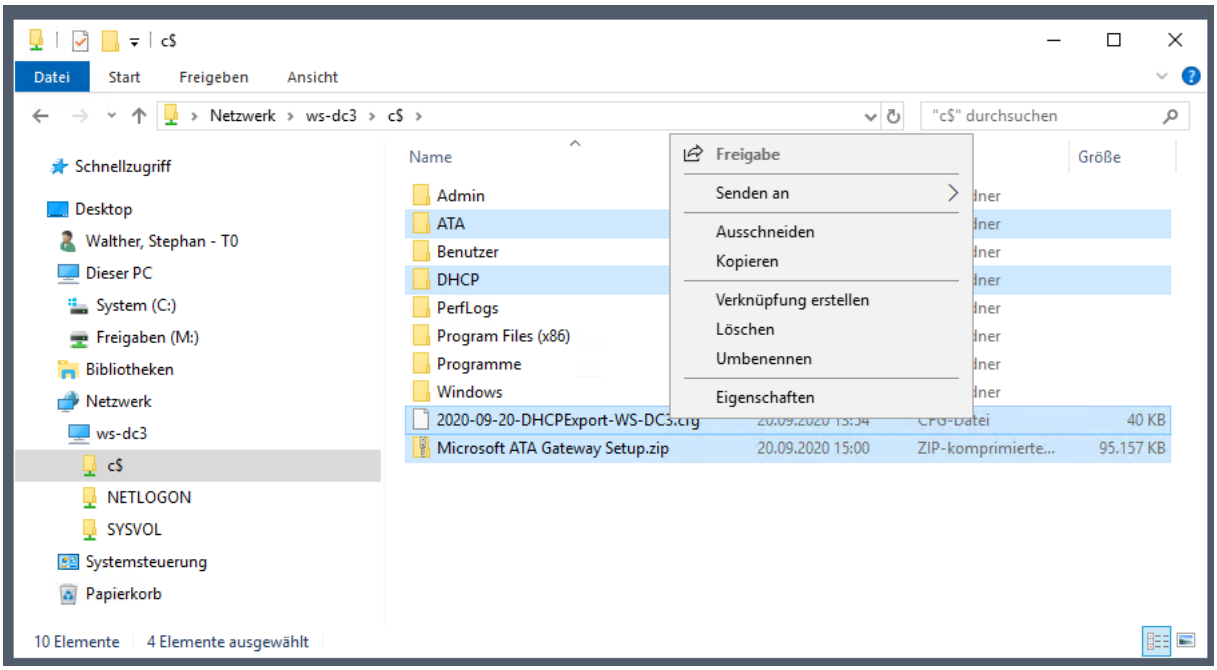
An dieser Stelle sei mir der Hinweis gestattet, dass mein PowerShell-Script „gMSA-Admin“ keinen Schadcode enthält. Vielmehr müssen wir uns auch bei der Anomalie-Erkennung an False-Positives gewöhnen.

Bereinigung im Hyper-V, Windows Update und Cleanup

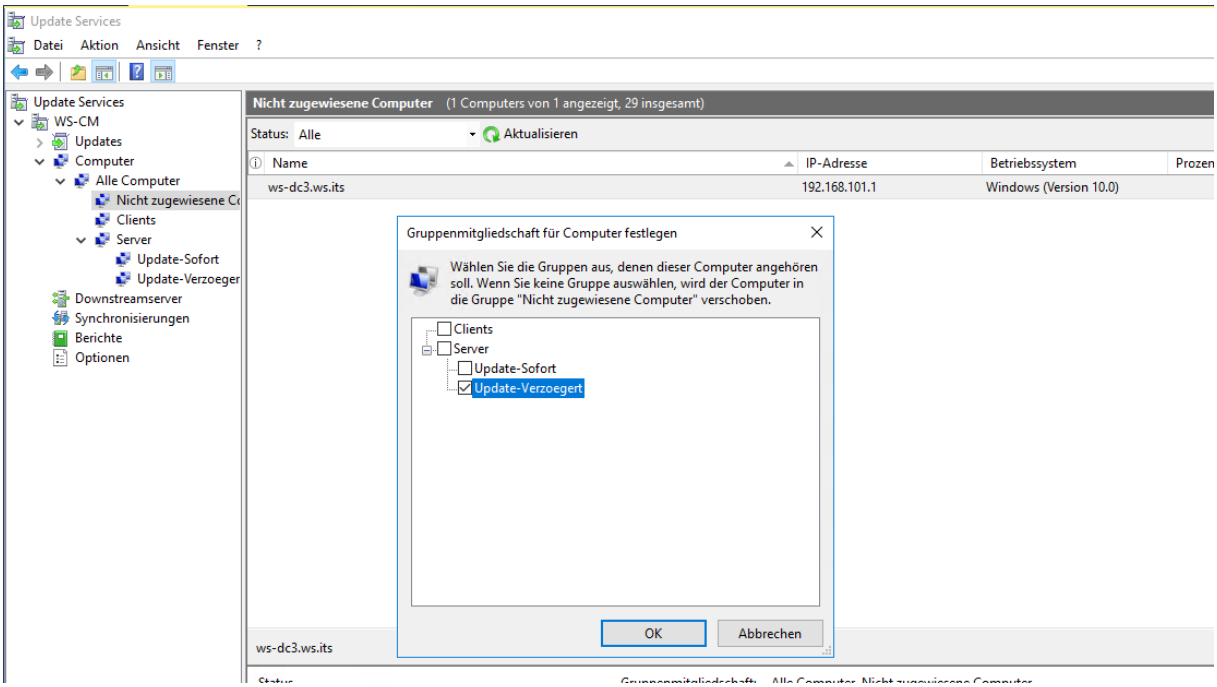
Im Hyper-V entferne ich den alten Server:



Alle für die Migration kopierten Dateien entferne ich auf dem neuen Server:

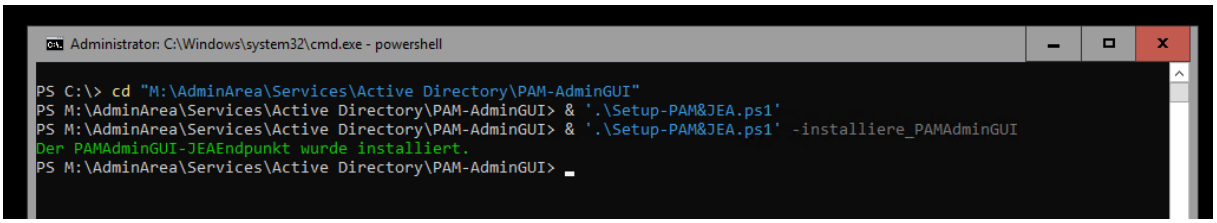


Natürlich soll der neue Server auch aktuell gehalten werden. Im WSUS hat er sich bereits registriert. Nun schiebe ich ihn in die richtige Update-Gruppe:



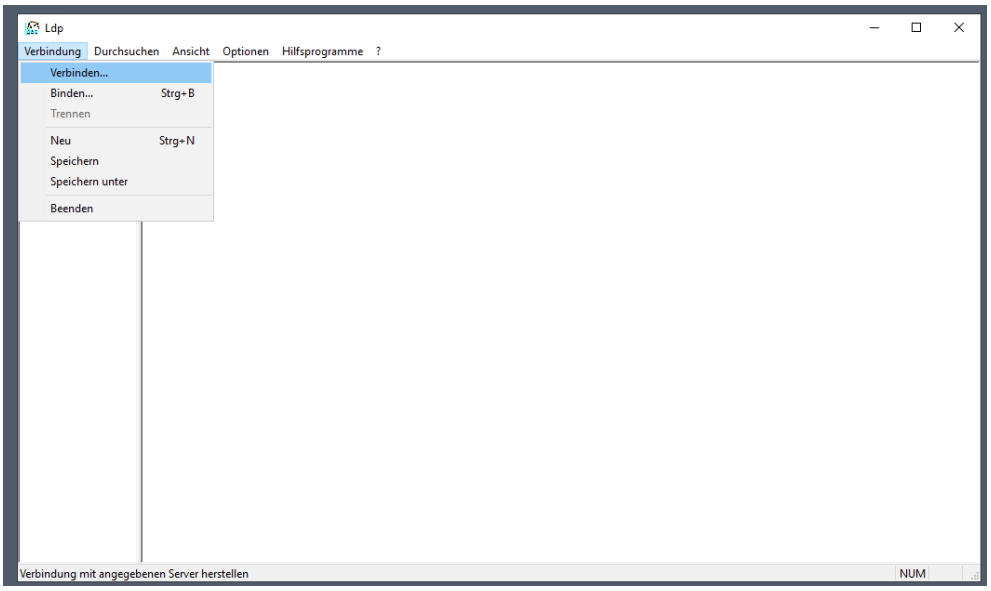
PowerShell JEA-PAM-AdminGUI

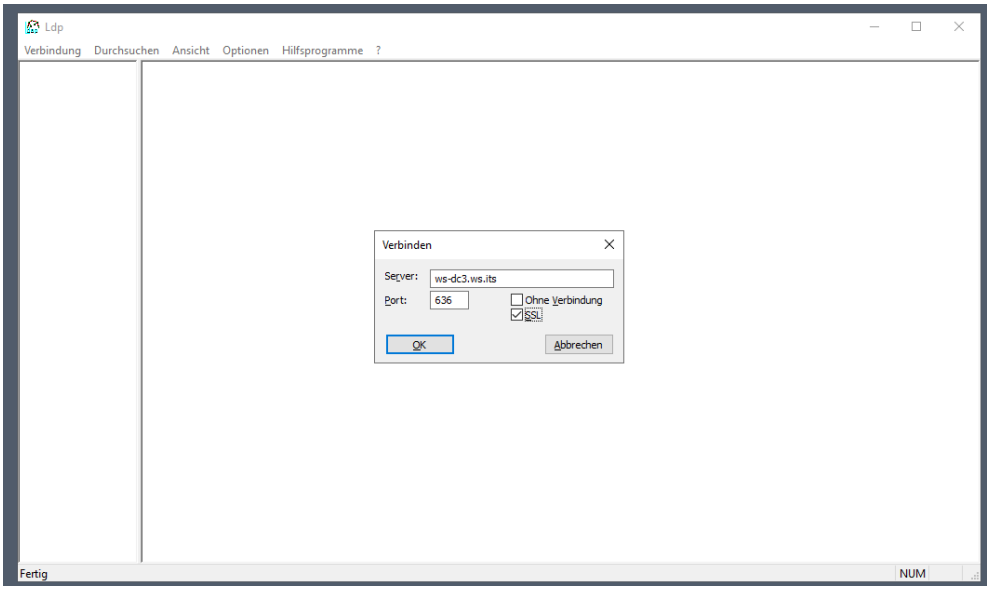
Meine PAM-Lösung habe ich hier schon etliche Male gezeigt. Im Backend verbindet sich das GUI-Script mit einem der Domain Controller. Auf diesem muss dazu ein JEA-Endpunkt für die Just-Enough-Administration-Lösung installiert sein. Das kann ich mit meinem Setup-Script erreichen:



Kontrolle LDAPS

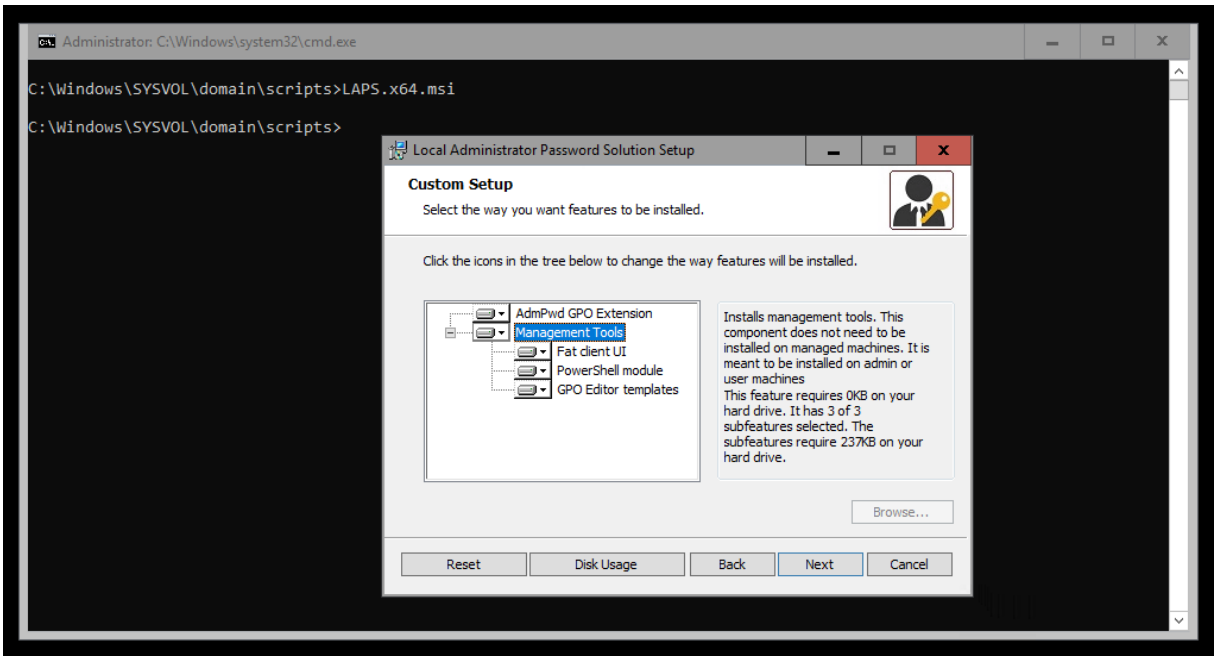
Durch meine interne PKI werden den Domain Controllern automatisch TLS-Zertifikate ausgestellt. Diese werden vollautomatisch für LDAPS verwendet. Eine Kontrolle der Bereitstellung kann nicht schaden. Dafür kann ldp.exe verwendet werden:





Installation LAPS

Meine lokalen Admin-Konten erhalten dank der Erweiterung LAPS (Local Administrator Password Solution) regelmäßig neue Kennwörter. Die Erweiterung zum Auslesen darf natürlich auf dem neuen DC nicht fehlen:



Zusammenfassung

Mit etwas Down-Time und ein wenig Schwierigkeiten beim Installieren des ATA-Gateways war es zusammenfassend eine einfache Aktualisierung. Mein Active Directory wird jetzt nativ von Windows Server 2019 bereitgestellt.