

<u>Inhalt</u>

Zielsetzung	2
IST-Situation	2
Soll-Situation	2
Migrationsplan	2
Vorbereitung	2
Aufbau der neuen VM	2
Sichtung von Informationen auf dem alten Server	9
aktuelle Konfiguration des DHCP	11
aktuelle Konfiguration des DNS	12
aktuelle Konfiguration des Active Directory	14
aktuelle ATA-Konfiguration und Vorbereitung im ATA	16
Maintenance	17
Deinstallation	
Vorbereitung der Migration der Rolle DHCP	
Vorbereitung der Migration der Rolle DNS	19
Vorbereitung der neuen VM	20
Entfernen der Rolle Active Directory	23
Bereitstellung des neuen Servers	29
Austausch der VM	29
Bereitstellung des neuen Domain Controllers	30
Betriebssystemvorbereitung	31
Bereitstellung der Rolle Active Directory	32
Konfiguration Monitoring	36
Bereitstellung der Rolle DHCP	37
Bereitstellung der Rolle DNS	40
Integration ins ATA (mit TroubleShooting)	41
Nacharbeiten	47
Datensicherung des Windows Servers	47
Bereinigung im Hyper-V, Windows Update und Cleanup	49
PowerShell JEA-PAM-AdminGUI	51
Kontrolle LDAPS	51
Installation LAPS	52
Zusammenfassung	52

<u>Zielsetzung</u>

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

<u>Aufbau der neuen VM</u>

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:



🛥 PAM-AdminGUI - verbunden mit	WS-DC1.ws.its (Version V2.00)		
Zeitraum: 3 Stunden	~		
Ziel-DC:	✓ zu DC replizieren	zu allen DC replizieren Die automatische AD-Replikation	ion ist aktiv.
Security-Tiers:	Admins:	mögliche Gruppen:	aktive Mitgliedschaften:
x		(x
The 0 - Domain Administration The 1 - Server Administration Tre 2 - Oler Administration Tier 3 - Service Admin		GG-Admin-AD-Sion GG-Admin-DHCP GG-Admin-DNS GG-Admin-Setup-ApplockerAusnahme-AdminDir GG-Admin-Setup-ApplockerAusnahme-ueberall Schema-Admins	Gültigkeit Gruppe statisch Protected Users 2020-09-20 16:35:22 Domianer-Admins 2020-09-20 16:35:22 GG-SEC-DomainController-Admins 2020-09-20 16:35:22 Organisations-Admins
bereit - Wähle eine Gruppe zur Bearbeit PAM-AdminGUI - verbunden mit Zeitraum: 3 Stunden Ziel-DC: Security Tiers:	ung der Mitgliedschaft aus. WS-DC1.ws.its (Version V2.00) v zu DC replizieren	zu ellen DC replizieren zu ellen DC replizieren zoödliche Grupper	entfernen entferne alle
Security-Hers:	Admins:	moglicne Gruppen:	aktive mitgliedschaften:
alle Tier0 - Domain Administration Tier1 - Server Administration Tier3 - Service Admin	stephan-T1	GG-Admin-AD-GPO GG-Admin-AD-Join GG-Admin-AD-Join GG-Admin-AD-Join GG-Admin-AD-Solents GG-Admin-APS-Server GG-Admin-APS-Server GG-Admin-MX GG-Admin-MX GG-Admin-PKI GG-Admin-PKI GG-Admin-PKI GG-Admin-Setup-ApplockerAusnahme-ueberal GG-Admin-Setup-ApplockerAusnahme-ueberal GG-Admin-Setup-ApplockerAusnahme-ueberal GG-Admin-Setup-ApplockerAusnahme-ueberal GG-Admin-Setup-ApplockerAusnahme-ueberal GG-Admin-Setup-ApplockerAusnahme-ueberal GG-Admin-Setup-ApplockerAusnahme-ueberal GG-Admin-Setup-ApplockerAusnahme-ueberal GG-Admin-Setup-ApplockerAusnahme-ueberal GG-SEC-Server-HiP-Admins GG-SEC-Server-HiP-Admins GG-SEC-Server-RDS-Admins Organization Management	Image Gütigkeit Gruppe statisch Protected Users 2020-09-20 16:36:22 GG-Admin-DHCP 2020-09-20 16:36:22 GG-Admin-DNS 2020-09-20 16:36:23 GG-Admin-HyperV 2020-09-20 16:36:23 GG-Admin-HyperV 2020-09-20 16:36:23 GG-Admin-HyperV 2020-09-20 16:36:23 GG-Admin-HyperV-Storage 2020-09-20 16:36:23 GG-SEC-Server-Standard-Admins
bereit - Wähle eine Gruppe zur Bearbeit	tung der Mitgliedschaft aus.	hinzufügen	entfernen entferne alle

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:



Hyper-V-Manager WS-HV3	Virtuelle Computer	Abschließen	computer des Assistenten für neue virtuelle Computer	^
	Prüfpunkte WS-DC3 Erst Kon Ger	Vorbemerkungen Name und Pfad angeben Generation angeben Speicher zuweisen Netzwerk konfigurieren Virtuelle Festplatte verbinden Zusammenfassung	Der Assistent für neue virtuelle Computer wurde erfolgreich abgeschlossen. Der folgende virtuelle Computer wird erstellt: Beschreibung: Name: WS-DC3 Generation: Generation 2 Arbeitsspeicher: 2048 MB Netzwerk: VLANs Festplatte: Keine Klicken Sie auf 'Fertig stellen', um den virtuellen Computer zu erstellen und den Assistenten zu beenden.	

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

📙 🔁 🔜 🖛 Base	Verwalten		- 🗆	×		- - 1	WS-DC3		
Datei Start Freigeben Ansicht	Datenträgerimagetools			~ 🕐	Datei	Start	Freigeben	Ansicht	
← → × ↑ 📙 > Dieser PC → Hyp	er-V (V:) > Base	✓ Ö "Base" dur	chsuchen	P	$\leftarrow \rightarrow$	~ 个	- Hyper-	V (V:) > Hype	r-V > WS-DC3
📌 Schnellzugriff	Name		Änderungsdatum	Тур	📌 Sch	nellzugrif	f		Name
Deskton	- Win2019-1908.vhdx		09.08.2019 20:26	Festpl	Dec	kton			Snapshots
Walther Stephan - T1		/hdx	15.11.2019 18:51	Festpl	2 W	alther Ct	mhan T1		Virtual Hard Disks
					a "	aitrier, st	epilari - TT		Virtual Machines
Dieser PC						eser PC			
System (C:)		14% abgeschlosse	n		-		×		
DVD-RW-Laufwerk (D:)		Fin Element wird w	on Bace pach WS-Di	2 konier			D:)		
BACKUP-USB (E:)		14% aboeschi	oscen	us kopiei		iii.	v		
🛖 Freigaben (M:)		1470 abgeserie	033011				_		
Hyper-V (V:)									
Base				0	ieschwindig	keit: 288	MB/s		
Hyper-V									
ISO									
Bibliotheken		Restdauer: Ungefä	hr 30 Sekunden						
BACKUP-USB (E:)		Verbleibende Eleme	ente: 1 (10,0 GB)						
		🔿 Weniger Detail	ls						
Systemsteuerung					6 84		CD (5)		
A Pablerkorb					- BA	ACKUP-U	2B (E:)		

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

Hyper-V-Manager							
Datei Aktion Ansicht ?							
🗢 🤿 🙍 🖬 🚺 🖬							
Hyper-V-Manager	Virtuelle Computer						
	Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status	Konfiguratio
	WS-DC3	Wird ausgeführt	7 %	4096 MB	6.12:09:03		8.0
	WS-DC3-neu	Aus					9.0
	WS-FS3	Wird ausgeführt	2 %	1328 MB	6.12:08:39		8.0
	WS-PFS2	Wird ausgeführt	0 %	4096 MB	6.12:09:09		8.0

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:



Hyper-V-Manager		💼 Einstellungen für "WS-DC3-neu" auf "WS-HV3"	– 🗆 X
Datei Aktion Ansicht ?		WS-DC3-neu 🗸 🕨 🖏	
← Hyper-V-Manager WS-HV3	Virtuelle Computer Name P WS-DC3 V WS-DC3neu A WS-F53 V	Kardware Aradware hinzufügen Firmware Starteintragsänderungen aussteh Sicherheit Xcheltsspeicher 2048 MB	te
	WS-PFS2 V	B Prozessor 4 virtuelle Prozessoren 5 SCSI-Controler Computer für verwendet wir 111 B Netzwerkkarte VLNis X verwaltung Name	AN-ID wird das virtuelle LAN angegeben, das von diesem virtuellen die gesamte Netzwerkkommunikation über diese Netzwerkkarte d. waltung enverwaltung aktivieren wie die Netzwerkandprafie von diesem Netzwerkarlanter.
	Prüfpunkte WS-DC3-neu	WS-DC3-neu verwendet wi integrationsdienste Einige Dienste verfügbar Pröduktion Speicherort für die Smart Paging-D V: Hyper-VWS-DC3	rd, Sowohl "Minimale Bandbreite" als auch "Maximale Bandbreite" gabit pro Sekunde gemessen. breite: 0 Mbit/s doreite: 0 Mbit/s in Mindest- oder Maximalwert gelten soll, geben Sie "0" an.
	Erstellt: Konfiguratio Generation: Anmerkung:	Automatische Startaktion Neustart bei vorheriger Ausführung Automatische Stoppaktion Speichern	intfernen", um den Netzwerkadapter von diesem virtuellen Computer zu Entfernen
	Zusammenfassung Arbeitsspeich		OK Abbrechen Anwenden

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

C:\Windows\system32\LogonUI.exe	-	x
Administrator		
Das Benutzerkennwort muss vor der Anmeldung geändert werden.		
bbrechen		





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:

Administrator: C:\Windows\system32\cmd.exe - sconfi	g	-		x
14) Server herunterfahren 15) Zur Befehlszeile wechseln				^
Geben Sie eine Zahl ein, um eine Option	auszuwählen: 6			
Serverkonfigura	tion			
 Domäne/Arbeitsgruppe: Computername: Lokalen Administrator hinzufügen Remoteverwaltung konfigurieren Windows Update-Einstellungen: Updates herunterladen u. installieren Remotedesktop: 	Arbeitsgruppe: WORKGROUP WIN-VKGRADFF66F Aktiviert Nur Downloads Deaktiviert			
9) ም C:\Windows\System32\cscript.exe		- 1	. 1	o x
16 Microsoft (R) Windows Script Host, Ver 11 Copyright (C) Microsoft Corporation. J 12 Nach (a)llen oder nur nach (e)mpfohler 12 Alle geeigneten Updates werden gesuch 14 Ge	rsion 5.812 Alle Rechte vorbehalten. nen Updates suchen? a t			



Administrator: C:\Windows\system32\cmd.exe - se	config	_ 🗆 X
14) Server herunterfahren 15) Zur Befehlszeile wechseln		^
Geben Sie eine Zahl ein, um eine Onti	on auszuwählen: 6	
deben sie eine zunz ein, um eine oper		
Convertentia		
Serverkontig	uration	
1) Domäne/Arbeitsgruppe:	Arbeitsgruppe: WORKGROUP	
 Computername: Lokalen Administrator hinzufügen 	WIN-VKGKADFFOOF	
4) Remoteverwaltung konfigurieren	Aktiviert	
 Windows Update-Einstellungen: Updates herunterladen u. installie 	Nur Downloads rren	
7) Remotedesktop:	Deaktiviert	
 Motzworkoj sctali P C:\Windows\System32\cscript.exe 		X
10 11 Alle geeigneten Updates werden ges	ucht	
12 Liste geeigneter Elemente auf dem	Computer:	
12 12 1> 2020-05 Kumulatives Update für 22 2020-01 Update für Windows Serv	.NET Framework 3.5, 4.7.2 und 4.8 für Windows Server 2	2019 für x64 (KB4556441)
3> Security Intelligence-Update für	r Microsoft Defender Antivirus - KB2267602 (Version 1.	.317.390.0)
Ge 47 2020-05 Kumulatives opuate fur	windows Server 2019 (1009) fur X04-basierte Systeme (K	ND4351655)
(A)lle Updates, kei(n)e Updates od	er (b)estimmtes Update?	
Administrator: C:\Windows\system32\cmd.exe - si	config	_ 🗆 X
Administrator: C:\Windows\system32\cmd.exe - so 14) Server herunterfahren 15) Zur Befehlszeile wechseln	config	= • ×
Administrator C:\Windows\system32\cmd.exe -so 14) Server herunterfahren 15) Zur Befehlszeile wechseln Geben Sie eine Zahl ein, um eine Opti	config .on auszuwählen: 6	_ D X
Administrator C:\Windows\system32\cmd.exe-so 14) Server herunterfahren 15) Zur Befehlszeile wechseln Geben Sie eine Zahl ein, um eine Opti	config on auszuwählen: 6	– 🗆 X
Administrator C:\Windows\system32\cmd.exe-so 14) Server herunterfahren 15) Zur Befehlszeile wechseln Geben Sie eine Zahl ein, um eine Opti Serverkonfig	config .on auszuwählen: 6 .uration	_ D X
Administrator C:\Windows\system32\cmd.exe - so 14) Server herunterfahren 15) Zur Befehlszeile wechseln Geben Sie eine Zahl ein, um eine Opti Serverkonfig	config on auszuwählen: 6 uuration	
Administrator: C:\Windows\system32\cmd.exe - so 14) Server herunterfahren 15) Zur Befehlszeile wechseln Geben Sie eine Zahl ein, um eine Opti Serverkonfig 1) Domäne/Arbeitsgruppe: 2) Computername:	config on auszuwählen: 6 uration Arbeitsgruppe: WORKGROUP WIN-VKGRADFF66F	
Administrator. C:\Windows\system32\cmd.exe - so Administrator. C:\Windows\system32\cmd.exe - so Administrator. C:\Windows\system32\cmd.exe - so Server administrator ad	on auszuwählen: 6 uration Arbeitsgruppe: WORKGROUP WIN-VKGRADFF66F Aktiviert	
Administrator: C:\Windows\system32\cmd.exe - so 14) Server herunterfahren 15) Zur Befehlszeile wechseln Geben Sie eine Zahl ein, um eine Opti Serverkonfig 	config on auszuwählen: 6 guration Arbeitsgruppe: WORKGROUP WIN-VKGRADFF66F Aktiviert Nur Downloads	
Administrator. C:\Windows\system32\cmd.exe -su Administrator. C:\Windows\system32\cmd.exe -su Surverkell Geben Sie eine Zahl ein, um eine Opti Serverkonfig Computername: Lokalen Administrator hinzufügen Remoteverwaltung konfigurieren Windows Update-Einstellungen: Updates herunterladen u. installie Remotedesktop:	config con auszuwählen: 6 puration Arbeitsgruppe: WORKGROUP WIN-VKGRADFF66F Aktiviert Nur Downloads rren Deaktiviert	
Administrator: C:\Windows\system32\cmd.exe - so Administrator: C:\Windows\system32\cmd.exe - so Administrator: C:\Windows\system32\cmd.exe - so Administrator in a constraint Serverkonfig Domäne/Arbeitsgruppe: Computername: C	config on auszuwählen: 6 uration Arbeitsgruppe: WORKGROUP WIN-VKGRADFF66F Aktiviert Nur Downloads rren Deaktiviert Neustant erforderlich	
Administrator: C:\Windows\system32\cmd.exe - si 14) Server herunterfahren 15) Zur Befehlszeile wechseln Geben Sie eine Zahl ein, um eine Opti Serverkonfig 1) Domäne/Arbeitsgruppe: 2) Computername: 3) Lokalen Administrator hinzufügen 4) Remoteverwaltung konfigurieren 5) Windows Update-Einstellungen: 6) Updates herunterladen u. installie 7) Remotedesktop: 8) Notzuopkoisetall 9) Staupokoisetall 9) C:\Windows\System32\cscript.exe	config con auszuwählen: 6 puration Arbeitsgruppe: WORKGROUP WIN-VKGRADFF66F Aktiviert Nur Downloads pren Deaktiviert I Neustart erforderlich	
Administrator: C:\Windows\system32\cmd.exe - so Administrator: C:\Windows\system32\cmd.exe - so Administrator: C:\Windows\system32\cmd.exe - so Serverkonfig Demained Arbeitsgruppe: Computername: Lokalen Administrator hinzufügen Computername: Lokalen Administrator hinzufügen Windows Update-Einstellungen: Updates herunterladen u. installie Remotedesktop: Notzwonkoinstall C:\Windows\System32\cscript.exe C:\Windows\System32\cscript.exe Administrator Update für	config con auszuwählen: 6 uration Arbeitsgruppe: WORKGROUP WIN-VKGRADFF66F Aktiviert Nur Downloads rren Deaktiviert I Neustant erforderlich X Zum Abschließen von Windows Updates ist ein Neustant erforderlich.	– 🗆 X
Administrator: C:\Windows\system32\cmd.exe - si Administrator: C:\Windows\system32\cmd.exe - si Administrator: C:\Windows\system32\cmd.exe - si Ceben Sie eine Zahl ein, um eine Opti Serverkonfig Domäne/Arbeitsgruppe: Computername: Domäne/Arbeitsgruppe: Computername: Lokalen Administrator hinzufügen Remoteverwaltung konfigurieren Windows Update-Einstellungen: Updates herunterladen u. installie Remotedesktop: Mintownskoigetall C:\Windows\System32\cscript.exe C: C:\Windows\System32\cscript.exe C: Domaine/Arbeitsgruppe: Serverkonfigurieren S: WintowsSystem32\cscript.exe C: Serverkonfigurieren C: C: C: C: C: C: C: C: C: C:	config con auszuwählen: 6 guration Arbeitsgruppe: WORKGROUP WIN-VKGRADFF66F Aktiviert Nur Downloads pren Deaktiviert Nur Downloads tren Zum Abschließen von Windows Updates ist ein Neustart erforderlich. Jett neu starten?	_ □ × _ □ × 2019 für x64 (KB4556441): Erfolgr eich
Administrator: C:\Windows\system32\cmd.exe - si Administrator: C:\Windows\system32\cmd.exe - si Administrator: C:\Windows\system32\cmd.exe - si Administrator: Administrator: Administrator Domäne/Arbeitsgruppe: Computername: Lokalen Administrator hinzufügen Remoteverwaltung konfigurieren Windows Update-Einstellungen: Updates herunterladen u. installie Remotedesktop: Natzwonkoisctall C:\Windows\System32\cscript.exe C: Administrator binzufügen Administrator binzufügen C:\Windows\System32\cscript.exe C: Security Intelligence-Update für Advage-05 Kumulatives Update für C:\Windows Servi C:\Windows Serv	config con auszuwählen: 6 puration Arbeitsgruppe: WORKGROUP WIN-VKGRADFF66F Aktiviert Nur Downloads rren Deaktiviert Nur Downloads rren Deaktiviert Law Abschließen von Windows Updates ist ein Neustart erforderlich. Ja Nein	_ □ × _ □ × 2019 für x64 (KB4556441): Erfolgr eich x317.390.0): Erfolgreich KB4551853): Erfolgreich
Administrator: C:\Windows\system32\cmd.exe - si 14) Server herunterfahren 15) Zur Befehlszeile wechseln Geben Sie eine Zahl ein, um eine Opti Serverkonfig 1) Domäne/Arbeitsgruppe: 2) Computername: 3) Lokalen Administrator hinzufügen 4) Remoteverwaltung konfigurieren 5) Windows Update-Einstellungen: 6) Updates herunterladen u. installie 7) Remotedesktop: 8) Notzuopkoisctall 9) C:Windows\System32\cscript.exe 11 12 2020-05 Kumulatives Update für eich 12 2020-05 Kumulatives Update für 14 > 2020-05 Kumulatives Update für 15 2020-05 Kumulatives Update für 16 Installationsergebnis: Erfolgreich	config on auszuwählen: 6 puration Arbeitsgruppe: WORKGROUP WIN-VKGRADFF66F Aktiviert Nur Downloads tren Deaktiviert Nur Downloads tren Deaktiviert LumAbschließen von Windows Updates ist ein Neustart erforderlich. Ja Nein	X 2019 für x64 (KB4556441): Erfolgr eich .317.390.0): Erfolgreich KB4551853): Erfolgreich
<pre>Administrator: C:\Windows\system32\cmd.exe - si 4) Server herunterfahren 15) Zur Befehlszeile wechseln Geben Sie eine Zahl ein, um eine Opti Serverkonfig 1) Domäne/Arbeitsgruppe: 2) Computername: 3) Lokalen Administrator hinzufügen 4) Remoteverwaltung konfigurieren 5) Windows Update-Einstellungen: 6) Updates herunterladen u. installie 7) Remotedesktop: 8) Notzwopkoinstall 9) C.\Windows\System32\cscript.exe 11 1> 2020-05 Kumulatives Update für 12> 2020-01 Update für Windows Serv 13> Security Intelligence-Update für 14> 2020-05 Kumulatives Update für 15 Ge Installationsergebnis: Erfolgreich Neustart erforderlich: Wahr</pre>	config con auszuwählen: 6 puration Arbeitsgruppe: WORKGROUP WIN-VKGRADFF66F Aktiviert Nur Downloads men Deaktiviert I Neustart erforderlich. Ja Nein	ـــــــــــــــــــــــــــــــــــــ

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:

P C:\Windows\System32\cscript.exe	-	x
Microsoft (R) Windows Script Host, Version 5.812 Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.		
Nach (a)llen oder nur nach (e)mpfohlenen Updates suchen? a		
Alle geeigneten Updates werden gesucht		
Liste geeigneter Elemente auf dem Computer:		
1> 2020-09 Kumulatives Update für Windows Server 2019 (1809) für x64-basierte Systeme (KB4570333)		
Wählen Sie eine Option aus: (A)lle Updates, kei(n)e Updates oder (b)estimmtes Update? a		
Updates werden heruntergeladen		
Updates werden installiert	×	
Liste mit installierten Updates und individuellen Instal 1> 2020-09 Kumulatives Update für Windows Server 2019 (1 Jetzt neu starten?	ch	
Installationsergebnis: Erfolgreich Neustart erforderlich: Wahr Ja Nein]	
		~

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

VS IT-Solutions

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:

Aufgabenplanung								
Datei Aktion Ansicht ?								
🗢 🄿 🙍 🖬 🚺 🖬								
Aufgabenplanung (ws-dc3.w Aufgabenplanungshibligt)	Name	Status	Trigger		Näch	ste Laufzeit	Letzte Laufzeit	Ergebnis der le
	Check-ADStart	Bereit	Beim Systemstart				17.09.2020 03:55:57	Der Vorgang w
	IpamDhcpProvisioning	Bereit	Bei Aufgabenerstellur	Ausführen			08.09.2019 16:21:43	(0x103)
	IpamDnsProvisioning	Bereit	Bei Aufgabenerstellur	Beenden			08.09.2019 16:21:43	(0x103)
	ServerSicherung	Bereit	Jeden Tag um 01:00 U	Deaktivieren		2020 01:00:00	20.09.2020 01:00:01	Der Vorgang w
				Exportieren				
				Eigenschaften				
				Löschen				
	All	-						

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:

tei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe] 🙆 🔜 🔏 🐁 📋 ≽ 🖣 🍽 🕨 🗊 🔳 😪		D .					
Unbenannt1.ps1* X 1 Enter-PSSession -ComputerName ws-dc3							
1 Enter-PSSession -ComputerName ws-dc3							
2							
3 Get-WindowsFeature where installed							
$\frac{1}{100}$ and $\frac{1}{100}$ and $\frac{1}{100}$							
DISPIAY NAME	Name	Install State					
X] Active Directory-Domänendienste	AD-Domain-Services	Installed					
X] Datei-/Speicherdienste	FileAndStorage-Services	Installed					
[X] Datei- und iSCSI-Dienste	File-Services	Installed					
[X] Dateiserver	FS-FileServer	Installed					
[X] Speicherdienste	Storage-Services	Installed					
k] DHCP-Server	DHCP	Installed					
X] DNS-Server	DNS	Installed					
K] .NET Framework 4.6-Funktionen	NET-Framework-45-Fea	Installed					
[X] .NET Framework 4.6	NET-Framework-45-Core	Installed					
[X] WCF-Dienste	NET-WCF-Services45	Installed					
[X] TCP-Portfreigabe	NET-WCF-TCP-PortShar	Installed					
Gruppenrichtlinienverwaltung	GPMC	Installed					
x] Remoteserver-verwaltungstools	RSAI	Installed					
[X] ROITENVERWAITUNGSTOOTS	RSAI-ROIE-1001S	Installed					
[X] AD DS- UNU AD EDS-10015	RSAT-AD-1001S	Installed					
[X] ACLIVE DIRECLORY-MODULT LUR WINDOWS P	RSAT-AD-POWErShell	Installed					
() Windows Defender-Features	Windows-Defender-Fea	Installed					
kj wrhuows berender reacures	Windows-Defender	Installed					
[X] Windows Defender	PowerShellPoot	Installed					
[X] Windows Defender		Inscarried					
<pre>[X] Windows Defender X] Windows Powershell [X] Windows Powershell 5.1</pre>	PowerShell	Installed					
[X] Windows Defender X] Windows Powershell [X] Windows Powershell 5.1 X] Windows Server-Sicherung	PowerShell Windows-Server-Backup	Installed					

Es gibt auch bei den Freigaben keine Überraschungen:

Name	ScopeName	Path	Description
ADMIN\$	*	C:\Windows	Remoteverwaltung
c\$		c:\	Standardfreigabe
dhcpaudit		C:\Windows\svstem32\dhcp	
IPC\$			Remote-IPC
NETLOGON		C:\Windows\SYSVOL\sysvol\ws.its\SCRIPTS	Ressource für Anmeldeserver
SYSVOL		C:\Windows\SYSVOL\sysvol	Ressource für Anmeldeserver



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 Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005	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:

→ 👻 🛧 📙 > Dieser PC > System	(C:) > Admin > Backup-BMR > \$Programm				~ Ō	"\$Program	m" duro
Schnellzugriff	Name	Änderungsdatum	Тур	Größe			
	7zip	16.08.2019 10:27	Dateiordner				
Desktop	Datensicherung-Auswertung.xlsm	19.11.2015 11:45	XLSM-Datei	1.602 KB			
2 Walther, Stephan - T1	Log-Serversicherung.csv	19.09.2020 05:03	CSV-Datei	1.619 KB			
Dieser PC	Log-Sicherungsexport.csv	13.05.2015 16:16	CSV-Datei	1 KB			
System (C:)	Puntima lag	20.00 2020 00.00	Toutdaluumant	2 40			
System (C:)	Puntima lan	20.00.2020.00.00	Tartelalumant	סע כ	_		×
System (C:) Admin Rackup PMP PS C:\Admin\Bac	■ Durations for erShell kup-BMR\\$Programm> Import-Csv -Path .\	Log-Serversicherun	Tottlohumoot g.csv -Delimite	r ';' where se	rver -	□ EQ 'ws-dc3	×
Left System (C:) Admin Backup-BMR SC:\Admin\Bac Select -Last	■ Dusting to erShell kup-BMR\\$Programm> Import-Csv -Path .\ 10 Format-Table	20.00.2020.00.00 Log-Serversicherun	Tottlohumont g.csv -Delimite	میں د r ';' where se	- rver -	□ EQ 'ws-dc3	× ^
 System (C:) Admin Backup-BMR SProgramm Start-Tag Start 	☐ Durtimotion erShell kup-BMR\\$Programm> Import-Csv -Path .\ 10 Format-Table t-Zeit End-Tag End-Zeit Server Stat	Log-Serversicherun us Volumen JobN	Tatdebument g.csv -Delimite ame Slot	n ';' where se		□ EQ 'ws-dc3	×
 System (C:) Admin Backup-BMR Sprogramm PSTranscript 	Puters in the second s	Log-Serversicherun	g.csv -Delimite	אר ר';' where se		□ EQ 'ws-dc3	×
 System (C:) Admin Backup-BMR SProgramm PSTranscript 29.08.2020 01:0 SQL-Reporting 0.02 01:0 	Dusting Los rShell kup-BMR\\$Programm> Import-Csv -Path .\ 10 Format-Table t-Zeit End-Tag End-Zeit Server Stat 0:03 29.08.2020 01:24:41 WS-DC3 OK 0:03 29.08.2020 01:23:08 WS-DC3 OK	Log-Serversicherun us Volumen JobN 	g.csv -Delimite ame Slot 3 4	n';' where se	_	□ EQ 'ws-dc3	×
 System (C:) Admin Backup-BMR Sprogramm Sprogramm SqL-Reporting(1.09, 2020 01:0 09.2020 01:0 09.2020 01:0 	■ Dusting Los erShell Kup-BMR\\$Programm> Import-Csv -Path .\ 10 Format-Table t-Zeit End-Tag End-Zeit Server Stat 0:03 29.08.2020 01:24:41 WS-DC3 OK 0:03 01.09.2020 01:21:31 WS-DC3 OK 0:03 03.09.2020 01:21:31 WS-DC3 Feh	Log-Serversicherun us Volumen JobN 35784 BMR 35980 BMR er -3 35942 BMR	g.csv -Delimite ame Slot 	n';' where se		EQ 'ws-dc3	×
Leven (C:) Admin Backup-BMR SProgramm PS C:\Admin\Bac select -Last SProgramm Start-Tag Star 	■ Dusting Log erShell kup-BMR\\$Programm> Import-Csv -Path .\ 10 Format-Table t-Zeit End-Tag End-Zeit Server Stat 2:03 29.08.2020 01:22:4:41 WS-DC3 OK 2:03 01.09.2020 01:22:08 WS-DC3 OK 0:03 03.09.2020 01:21:31 WS-DC3 Fehl 2:03 05.09.2020 01:22:00 WS-DC3 OK	Log-Serversicherun us Volumen JobN 	g.csv -Delimite ame Slot 4 5 5	n ';' where se		EQ 'ws-dc3	×
System (C:) Admin PS C:\Admin\Bac Select - Last Short-Tag Star Scl-Reporting(1.09.2020 01:0 Benutzer PerfLogs 08.09.2020 01:0 Scl-Reporting(2.001.00)	Dusting Line Fshell Kup-BMR\\$Programm> Import-Csv -Path .\ 10 Format-Table t-Zeit End-Tag End-Zeit Server Stat 3:03 29.08.2020 01:24:41 WS-DC3 OK 3:03 01.09.2020 01:23:08 WS-DC3 OK 3:03 03.09.2020 01:21:31 WS-DC3 Fehl 3:03 05.09.2020 01:22:90 WS-DC3 OK 3:03 05.09.2020 01:22:90 WS-DC3 OK 3:03 05.09.2020 01:24:51 WS-DC3 OK 3:03 08.09.2020 01:24:51 WS-DC3 OK 3:04 08.09.2020 01:24:51 WS-DC3 OK 3:05 08.09.2020 01:24:51 WS-DC3 0K 3:05 08.09.2020 01:24:51 WS-DC3 0K	Log-Serversicherun us Volumen JobN 	g.csv -Delimite ame Slot 	n 'j' where se	_ rver -	EQ 'ws-dc3	×
 System (C:) Admin Backup-BMR SProgramm PSTranscript SQL-Reporting1.09.2020 01:0 Benutzer 03.09.2020 01:0 PerfLogs 69.2020 01:0 10.09.2020 01:0 	■ Dusting Loc erShell kup-BMR\\$Programm> Import-Csv -Path .\ 10 Format-Table t-Zeit End-Tag End-Zeit Server Stat 20:03 29:08.2020 01:24:41 WS-DC3 OK 0:03 01.09.2020 01:22:08 WS-DC3 OK 0:03 05.09.2020 01:22:09 WS-DC3 OK 0:03 05.09.2020 01:22:09 WS-DC3 OK 0:03 10.09.2020 01:22:41 WS-DC3 OK 0:03 10.09.2020 01:22:41 WS-DC3 OK	Log-Serversicherun US Volumen JobN 	g.csv -Delimite ame Slot 	n ';' where se	_	EQ 'ws-dc3	×
 System (C:) Admin Backup-BMR SProgramm PSTranscript SQL-Reportint SQL-Reportint Sol - 2020 01:0 Benutzer OS-92020 01:0 PerfLogs Neg-2020 01:0 Porgram Files (h12.09.2020 01:0 	■ Dusting Los erShell kup-BMR\\$Programm> Import-Csv -Path .\ 10 Format-Table t-Zeit End-Tag End-Zeit Server Stat 3:03 29.08.2020 01:24:41 WS-DC3 OK 3:03 01.09.2020 01:22:08 WS-DC3 OK 3:03 05.09.2020 01:22:08 WS-DC3 OK 3:03 05.09.2020 01:22:08 WS-DC3 OK 3:03 08.09.2020 01:22:08 WS-DC3 OK 3:03 08.09.2020 01:22:151 WS-DC3 OK 3:03 12.09.2020 01:22:130 WS-DC3 OK 3:03 12.09.2020 01:22:130 WS-DC3 OK	Log-Serversicherun us Volumen JobN 35784 BMR 35980 BMR 35960 BMR 36020 BMR 36020 BMR 36070 BMR 36070 BMR	g.csv -Delimite ame Slot 3 4 5 5 6 1 2	n ';' where se		EQ 'ws-dci	×
 System (C:) Admin Backup-BMR SProgramm SProgramm SQL-Reporting SQL-Reporting SQL-Reporting SQL-Reporting SQL-Reporting SQL-Reporting SQL-Reporting SQL-2020 01:0 05.092.0202 01:0 PerfLogs 08.09.2020 01:0 Porgram Files (N2.092.001:0 SQ2020 01:0 Program Files (N2.092.001:0 SQ2020 01:0 SQ2020 01:0 Program Files (N2.092.001:0 SQ2020 01:0 <li< td=""><td>Dusting Line Fshell Kup-BMR\\$Programm> Import-Csv -Path .\ 10 Format-Table t-Zeit End-Tag End-Zeit Server Stat sea 29.08.2020 01:24:41 WS-DC3 OK 8:03 01.09.2020 01:23:08 WS-DC3 OK 8:03 03.09.2020 01:21:31 WS-DC3 Fehl 8:03 05.09.2020 01:22:00 WS-DC3 OK 8:03 10.09.2020 01:22:41 WS-DC3 OK 8:03 10.09.2020 01:22:41 WS-DC3 OK 8:03 10.09.2020 01:22:41 WS-DC3 OK 8:03 15.09.2020 01:21:30 WS-DC3 OK 8:03 15.09.2020 01:21:30 WS-DC3 OK 8:03 15.09.2020 01:21:30 WS-DC3 OK 8:03 15.09.2020 01:21:90 WS-DC3 OK 8:04 15.09.2020 01:21:00 WS-DC3 OK</td><td>Log-Serversicherun us Volumen JobN </td><td>g.csv -Delimite ame Slot </td><td>n 'j' where se</td><td></td><td>C 'ws-dc3</td><td>×</td></li<>	Dusting Line Fshell Kup-BMR\\$Programm> Import-Csv -Path .\ 10 Format-Table t-Zeit End-Tag End-Zeit Server Stat sea 29.08.2020 01:24:41 WS-DC3 OK 8:03 01.09.2020 01:23:08 WS-DC3 OK 8:03 03.09.2020 01:21:31 WS-DC3 Fehl 8:03 05.09.2020 01:22:00 WS-DC3 OK 8:03 10.09.2020 01:22:41 WS-DC3 OK 8:03 10.09.2020 01:22:41 WS-DC3 OK 8:03 10.09.2020 01:22:41 WS-DC3 OK 8:03 15.09.2020 01:21:30 WS-DC3 OK 8:03 15.09.2020 01:21:30 WS-DC3 OK 8:03 15.09.2020 01:21:30 WS-DC3 OK 8:03 15.09.2020 01:21:90 WS-DC3 OK 8:04 15.09.2020 01:21:00 WS-DC3 OK	Log-Serversicherun us Volumen JobN 	g.csv -Delimite ame Slot 	n 'j' where se		C 'ws-dc3	×

aktuelle Konfiguration des DHCP

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

🚆 DHCP				
Datei Aktion Ans	iicht ?			
🗢 🔿 🖄 📰 🎾	🕻 🗐 🧟 🗟 🛛 🚺 📰 🖳			
PHCP → B ws-dc1.ws.its		Name IPv4 IPv6		
	Autorisierte Server verwalten		? ×	
	Autorisierte DHCP-Server:			
	Name IP-Adre	esse	Autorisieren	
	ws-dc1.ws.its 192.16	8.100.1	Aufheben	
	ws-dc3.ws.its 192.16	8.101.1	Aktualisieren	
	Wählen Sie einen Computer aus, und klicken Computer der DHCP-Konsole hinzuzufügen.	Sie dann auf "OK", ur	n einen	
		ОК	Schließen	

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



🏆 DHCP

Datei Aktion Ansicht ?

🗢 🔿 🔁 📰 🖻 📑 🛛				
DHCP ws-dc1.ws.its ws-dc3.ws.its ws-dc3.ws.its Bereich [172.19.121.0] DMZ-121 Adresspool Adressleases Sereichsoptionen Richtlinien Bereich [172.19.131.0] DMZ-131 Adresspool Adressleases Sereichsoptionen Richtlinien Bereich [192.168.111.0] LAN-101 Bereich [192.168.101.0] LAN-101 Adresspool Adresspool Richtlinien Bereich [192.168.111.0] LAN-101 Sereich [192.168.111.0] LAN-101 Bereich [192.168.111.0] LAN-101 Sereich [192.168.111.0] LAN-101 Richtlinien Bereichsoptionen Richtlinien Serveroptionen Richtlinien Richtlinien Serveroptionen Richtlinien Serveroptionen Richtlinien	^	Client-IP-Adresse	Name WS-CL3.ws.its WIN-VKGRADFF66F	Leaseablaufdatum Reservierung (aktiv) 21.09.2020 13:37:34

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:



Datei Aktion Ansicht ?					
🗢 🔿 🙇 📰 🙆 🖬 📋 🗐					
 DNS WS-DC1 ws-dc2 ws-dc3 Forward-Lookupzonen Reverse-Lookupzonen Vertrauenspunkte Bedingte Weiterleitungen 	Name 	Typ Active Directory-integriert, primär Active Directory-integriert, primär	Status Wird ausgef Wird ausgef Wird ausgef Wird ausgef Wird ausgef Wird ausgef Wird ausgef Wird ausgef	DNSSEC-Status Nicht signiert Nicht signiert Nicht signiert Nicht signiert Nicht signiert Nicht signiert Nicht signiert Nicht signiert Nicht signiert	Schlüsselma
La DNS-Manager Datei Aktion Ansicht ? ◆ → 2 000 Q Be 2 00 10 10 10 10 10 10 10 10 10 10 10 10]				
 ▲ DNS-Manager Datei Aktion Ansicht ? ◆ ● 2 □ 0 → 2 □ 1 0 0 → 2 □ 0 0 → 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	🔂	Τνρ	Status	DNSSEC-Status	Schlüsselma

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

🛔 DNS-Manager		
Datei Aktion Ansicht ?		
🔶 🔿 🙍 📰 📓 🔒 🛛 🖬 🛔	E1	
 DNS WS-DC1 ws-dc3 Forward-Lookupzonen Reverse-Lookupzonen Vertrauenspunkte Bedingte Weiterleitungen 	Name For Rev Bec Stat	Eigenschaften von ws-dc3 ? X Debugprotokollierung Ereignisprotokollierung Überwachen Sicherheit Schnittstellen Weterleitungen Erweitet Stammhinweise Bei Weterleitungen handelt es sich um DNS-Server, die von diesem Server zum Auflösen von DNS-Abfragen nach Einträgen verwendet werden, die von diesem Server nicht aufgelöst werden können. IP-Adresse Vollqualifizierter Domänenname f 172.19.121.254 ws-gate2.ws.its Weterleitungen verfügbar sind Bearbeiten Hinweis Weterleitungen für eine bestimmte Domäne definiert, werden sie anstelle von Weiterleitungen auf Serverebene verwendet. Navigieren Sie zum Erstellen oder Anzeigen bedingter OK Abbrechen Hilfe

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: WS IT-Solutions

WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC3) 2020-09-20 Migration auf Windows Server 2019

Administrator: Eingabeaufforderung

C:\>repadmin /showreps
Ergoldsbach\WS-DC1
DSA-Optionen: IS_GC
Standortoptionen: (none)
DSA-Objekt-GUID: d84376f5-b557-4eea-96b6-6e67d8252ef9
DSA-Aufrufkennung: 378c21c6-2536-4dfb-ad3d-d79968442e79
==== EINGEHENDE NACHBARN====================================
DC=ws.DC=its
Neufahrn\WS-DC3 über RPC
DSA-Objekt-GUID: 3b20c582-acc7-4758-8364-90e58595047f
Letzter Versuch am 2020-09-20 14:20:49 war erfolgreich.
Ergoldsbach\WS-DC2 über RPC
DSA-Objekt-GUID: 96a6f2e7-54db-4582-848f-d0d0b3d1c363
Letzter Versuch am 2020-09-20 14:23:47 war erfolgreich.
CN=Configuration.DC=ws.DC=its
Neufahrn\WS-DC3 über RPC
DSA-Objekt-GUID: 3b20c582-acc7-4758-8364-90e58595047f
Letzter Versuch am 2020-09-20 14:15:14 war erfolgreich.
Ergoldsbach\WS-DC2 über RPC
DSA-Objekt-GUID: 96a6f2e7-54db-4582-848f-d0d0b3d1c363
Letzter Versuch am 2020-09-20 14:21:59 war erfolgreich.
CN=Schema,CN=Configuration,DC=ws,DC=its
Ergoldsbach\WS-DC2 über RPC
DSA-Objekt-GUID: 96a6f2e7-54db-4582-848f-d0d0b3d1c363
Letzter Versuch am 2020-09-20 13:49:53 war erfolgreich.
Neufahrn\WS-DC3 über RPC
DSA-Objekt-GUID: 3b20c582-acc7-4758-8364-90e58595047f
Letzter Versuch am 2020-09-20 14:04:53 war erfolgreich.
DC=ForestDnsZones,DC=ws,DC=its
Ergoldsbach\WS-DC2 über RPC
DSA-Objekt-GUID: 96a6f2e7-54db-4582-848f-d0d0b3d1c363
Letzter Versuch am 2020-09-20 13:49:53 war erfolgreich.
Neufahrn\WS-DC3 über RPC
DSA-Objekt-GUID: 3b20c582-acc7-4758-8364-90e58595047f
Letzter Versuch am 2020-09-20 14:04:53 war erfolgreich.
DC=DomainDnsZones,DC=ws,DC=its
Ergoldsbach\WS-DC2 über RPC
DSA-Objekt-GUID: 96a6f2e7-54db-4582-848f-d0d0b3d1c363
Letzter Versuch am 2020-09-20 13:49:53 war erfolgreich.
Neufahrn\WS-DC3 über RPC
DSA-Objekt-GUID: 3b20c582-acc7-4758-8364-90e58595047f
Letzter Versuch am 2020-09-20 14:04:53 war erfolgreich.
C:\>

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.
ECN=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:

Microsoft Advanced Threat Analytic	s Konfigurationen						
System	-						
Center	Gateways						
Gateways							
Updates	Gatewaysetup	Ladon Sie diese	s Paket herunter um ein	Gateway oder ein Lightweight-I	Sateway zu installieren		
Datenquellen	Gutewaysetap	Educit Sic diese	s raket neranter, an en	Successive over ein Eightweight -	outeway za instancien.		
Verzeichnisdienste SIEM	NAME	^	ТҮР	DOMÄNEN-CONTROLLER	VERSION	DIENSTSTATUS	INTEGRITÄT
VPN	WS-ATA		Gateway	ws-dc1.ws.its	1.9.7478.57683	Wird ausgeführt	
Erkennung	WS-DC2		Lightweight-Gateway	WS-DC2.ws.its	1.9.7478.57683	Wird ausgeführt	
Entitätsmarkierungen Ausnahmen	WS-DC3		Lightweight-Gateway	WS-DC3.ws.its	1.9.7478.57683	Wird ausgeführt	
Benachrichtigungen und Berichte							



Gateways				
Gatewaysetup Laden Sie dieses Pak	et herunter, um ein Gateway	oder ein Lightweight-Gateway zu installie	eren.	
NAME ^ T	2014 ²			
WS-ATA G	WS-DC3			×
WS-DC2				
WS-DC3	Beschreibung			
	Domänencontroller (FQDN)	WS-DC3.ws.its		
	Netzwerkadapter für Erfassung	☑ Ethernet		
	Kandidat für die Domänensynchronisierung	DEAKTIVIERT		
	Gateway löschen		Speichern	Abbrechen
Microsoft Advanced Threat Analytics Konfigu	rationen			Suchen nach Benutzern, Con
System Center Gateways	ieways			
Updates Ga Datenquellen Verzeichnisdienste	Laden Sie dieses Paket	herunter, um ein Gateway oder ein Lightweight-Gatew	ay zu installieren.	

SIEM	NAME	^	ТҮР	DOMÄNEN-CONTROLLER	VERSION	DIENSTSTATUS	1
VPN	WS-ATA		Gateway	ws-dc1.ws.its	1.9.7478.57683	Wird ausgeführt	
Erkennung	WS-DC2		Lightweight-Gateway	WS-DC2.ws.its	1.9.7478.57683	Wird ausgeführt	
Entitätsmarkierungen							
Ausnahmen							

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

<u>Maintenance</u>

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:

WS IT-Solutions

WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC3) 2020-09-20 Migration auf Windows Server 2019

🔀 Windows PowerShell					
PS C:\> Resolve-DnsName -Name	www.ws-	its.de	e -Server w	s-dc3.ws.its	
Name www.ws-its.de	Type CNAME	TTL 137	Section Answer	NameHost ws-its.de	
Name : ws-its.de QueryType : AAAA TTL : 149 Section : Answer IP6Address : 2a01:238:20a:202:	:1086::				
Name : ws-its.de QueryType : A TTL : 146 Section : Answer IP4Address : 81.169.145.86					

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			x
Microsoft (R) Windows Script Host, Versi Copyright (C) Microsoft Corporation. All	on 5.812 e Rechte vorbehalten.		<u>^</u>
System wird überprüft			
Serverkonfigura	tion		
 Domäne/Arbeitsgruppe: Computername: Lokalen Administrator hinzufügen Remoteverwaltung konfigurieren 	Arbeitsgruppe: WORKGROUP WIN-VKGRADFF66F Aktiviert		
 5) Windows Update-Einstellungen: 6) Updates herunterladen u. installieren 7) Remotedesktop: 	Nur Downloads Deaktiviert		
8) Netzwerkeinstell. 9) Datum und Uhrzeit 10) Telemetrieeinstellungen 11) Windows-Aktivierung	Unbekannt		
12) Benutzer abmelden 13) Server neu starten 14) Server herunterfahren 15) Zur Befehlszeile wechseln			
Geben Sie eine Zahl ein, um eine Option	auszuwählen: 8		~

WS IT-Solutions

WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC3) 2020-09-20 Migration auf Windows Server 2019





Administrator: C:\Wind	ows\system32\cmd.exe - sconfig	-	×
Netzwerkkartene	instellungen		
NIC-Index Beschreibung IP-Adresse Subnetzmaske DHCP aktiviert Standardgateway Bevorzugter DNS-Ser Alternativer DNS-Se	1 Microsoft Hyper-V Network Adapter 192.168.101.1 fe80::2c7a:45b5:46b0:290f 255.255.255.0 Falsch 192.168.101.252 ver rver		
1) Adresse der Netz 2) DNS-Server festl 3) DNS-Servereinste 4) Zurück zum Haupt	werkkarte festlegen egen llungen löschen menü		
Gewünschte Option: DNS-Server			
Geben Sie den neuen Geben Sie den alter Der alternative DNS	bevorzugten DNS-Server ein (Leer = Abbrechen): 192.168.100.1 nativen DNS-Server ein (Leer = keiner): 192.168.101.1 -Server wurde festgelegt.		

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:

Serverkonfi	guration ====================================			
) Domäne/Arbeitsgruppe:) Computername:) Lokalen Administrator hinzufügen) Remoteverwaltung konfigurieren) Windows Update-Einstellungen:) Updates herunterladen u. installi	Arbeitsgruppe: W WIN-VKGRADFF66F Aktiviert Nur Downloads eren	ORKGROUP		
) Remotedesktop:) Netzwerkeinstell.) Datum und Uhrzeit 3) Telemetrieeinstellungen 1) Windows-Aktivierung 2) Renutzer ahmelden	Deaktiviert Unbekannt	Neu starten Der Computer muss neu gestartet werden, damit die Änderungen übernommen werden. Jetzt neu starten?	x	
5) Server neu starten 1) Server herunterfahren 5) Zur Befehlszeile wechseln		<u>Ja</u> Nein]	
eben Sie eine Zahl ein, um eine Opt	ion auszuwählen: 2			
omputername				

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:

WS IT-Solutions

WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC3) 2020-09-20 Migration auf Windows Server 2019



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:

ᡖ Server-Manager			
€ Server-Ma	nager • Alle Server		
Dashboard Lokaler Server Alle AD Datei-/Speicherdienste DHCP DNS	SERVER Alle Server 1 insgesamt Filter Servername IPv4-Adresse Verwaltbarkeit WS-DC1 192.168.100.1 Online - Leistungsindikatoren wurden nicht gestartet.	Letztes Update 20.09.2020 14:38:00	Windows-Aktivierung 00430-70395-36040-AA799 (Aktiviert)
📥 Server-Manager			
Server-Ma	nager • Alle Server		
 Dashboard Lokaler Server Alle Server AD DS Datei-/Speicherdienste DHCP DNS 	SERVER Alle Server 3 insgesamt Filter Servername IPv4-Adresse Verwaltbarkeit WS-DC1 192.168.100.1 Online - Leistungsindikatoren wurden nicht gestartet. WS-DC2 192.168.100.2 Online - Leistungsindikatoren wurden nicht gestartet. WS-DC3 192.168.101.1	Letztes Update 20.09.2020 14:38:00 20.09.2020 14:38:40 20.09.2020 14:38:47	Windows-Aktivierung 00430-70395-36040-AA799 (Aktiviert) 00430-70395-36040-AA168 (Aktiviert) 00377-90011-18116-AA655 (Aktiviert)

Über die Schalter oben rechts geht es weiter:

	– 0 ×
	- 🗭 🚩 Verwalten Tools Ansicht Hilfe
	Rollen und Features hinzufügen
	Rollen und Features entfernen
	Server hinzufügen
	Servergruppe erstellen
	Server-Manager-Eigenschaften
e Windows-Aktivierung	
:38:00 00430-70395-36040-AA799 (Aktiviert)	
:38:40 00430-70395-36040-AA168 (Aktiviert)	
38:47 00377-90011-18116-AA655 (Aktiviert)	

Für die Deinstallation selektiere ich den alten Server:

Vorbereitung	Wählen Sie einen Serv entfernt werden soller	er oder eine virtuelle Fe 1.	stplatte aus, von dem bzw. der Rollen und Fea	tures
Serverauswahl	 Einen Server aus d 	em Serverpool auswähl	en	
Serverrollen	O Virtuelle Festplatte	auswählen		
Features	Sonyorpool			
Bestätigung	Serverpoor			
Ergebnisse	Filter:			
	Name	IP-Adresse	Betriebssystem	
	WS-DC3.ws.its	192.168.101.1	Microsoft Windows Server 2016 Datacenter	r
	WS-DC1.ws.its	192.168.100.1	Microsoft Windows Server 2019 Datacenter	r
	WS-DC2.ws.its	192.168.100.2	Microsoft Windows Server 2019 Datacenter	r
	3 Computer gefunden	1		
	Auf dieser Seite werde von Windows Server a	en Server angezeigt, die Jusgeführt werden und i	unter Windows Server 2012 oder einer neuere mithilfe des Befehls "Server hinzufügen" im Se	en Versior rver-

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:

WS IT-Solutions

WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC3) 2020-09-20 Migration auf Windows Server 2019

🚗 Assistent zum Entfernen vo	on Rollen und Features		
Serverrollen er	itfernen		ZIELSERVER WS-DC3.ws.its
Vorbereitung Serverauswahl	Wenn Sie installierte Rollen vom ausgewählten Server entfernen möch entsprechenden Kontrollkästchen.	nten, deaktivieren Si	e die 🗙
Serverrollen	Rollen Be	schreibung	
Features Bestätigung	Active Directory Lightweight Directory Services (Ni △ Vo Active Directory-Domänendienste Active Directory-Rechteverwaltungsdienste (Nicht Do	n den Active Directo mänendiensten (Act main Services, AD D	ry- ive Directory S) werden
	📥 Assistent zum Entfernen von Rollen und Features	×	, en im e
	Validierungsergebnisse Vom Überprüfungsprozess wurden Probleme auf dem Server erkannt, von entfernen möchten. Die ausgewählten Features können nicht vom ausgew entfernt werden. Klicken Sie auf "OK", um andere Features auszuwählen.	dem Sie Features ählten Server	werden endet, um einer ugriff auf
	Validierungser gebnisse		m möglichen.
	WS-DC3.ws.its Vor dem Entfernen der AD DS-Rolle muss der Domänencontroller tiefer Diesen Domänencontroller tiefer stufen	gestuft werden.	
		OK	Abbrechen

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

📥 Konfigurations-Assistent für die	Active Directory-Domänendienste	_		×
Anmeldeinformat	ionen	W	ZIELSER VS-DC3.w	VER /s.its
Anmeldeinformationen Warnungen Neues Administratorkenn Optionen prüfen	Geben Sie die Anmeldeinformationen für diesen Vorgang an. <keine angegeben="" anmeldeinformationen=""> Entfernen dieses Domänencontrollers erzwingen</keine>	Ā	ndern	
Herabstufung Ergebnisse				
	 Der Server wird nach dem Herabstufungsvorgang automatisch neu gestarte erst nach dem Neustart entfernt werden. Weitere Informationen zu Anmeldeinformationen zum Entfernen 	et. Rolle	n sollten	
	< Zurück Weiter > Tiefer st	ufen	Abbrech	en

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:

ᡖ Konfigurations-Assistent für die	Active Directory-Domänendienste			-		×
Neues Administra	atorkennwort			١	ZIELSEF WS-DC3.v	RVER vs.its
Anmeldeinformationen	Kennwort:	•••••				
Warnungen	Kennwort bestätigen:	•••••				
Neues Administratorkenn						
Optionen prüfen						
Herabstufung						
Ergebnisse						
	Weitere Informationen zum Administ	ratorkennwort zum Entfernen				
		< Zurück Weiter >	Tiefer st	ufen	Abbreck	nen

So sollte es passen:

NS IT-Solutions

📥 Konfigurations-Assistent für die	Active Directory-Domänendienste	-		×
Optionen prüfen			ZIELSEF WS-DC3.v	RVER vs.its
Anmeldeinformationen Warnungen	Auswahl prüfen:			
Optionen prüfen Herabstufung	Entfernt die Active Directory-Domänendienste von diesem Computer,			
Ergebnisse	Nach Abschluss des Vorgangs gehört dieser Server der Domäne "ws.its" an.			
	Diese Einstellungen können in ein Windows PowerShell-Skript exportiert werde um zusätzliche Installationen zu automatisieren.	n, Sk	ript anzeig	jen
	Weitere Informationen zu Entfernungsoptionen	ufan	Abbreck	an

Oder doch nicht? Ich "liebe" ja diese äußerst detaillierten Fehlermeldungen...

VS IT-Solutions

Konfigurations-Assistent für die A	Active Directory-Domänendienste	– 🗆 X
Ergebnisse		ZIELSERVER WS-DC3.ws.its
() Bei der Herabstufung des Act	tive Directory-Domänencontrollers ist ein Fehler aufgetreten.	Mehr anzeigen 🛛 🗙
Anmeldeinformationen	O Detaillierte Vorgangsergebnisse anzeigen	
Warnungen	😣 Der Vorgang konnte nicht durchgeführt werden. Fehler:	
Neues Administratorkenn	Die SYSVOL-Replikation konnte nicht vorbereitet oder nicht e	ntfernt werden.
Optionen prüfen		
Herabstufung	"Das System kann das angegebene Gerät oder die angegeber	ne Datei nicht öffnen."
Ergebnisse		
	Ergebnisse	×
	Bei der Herabstufung des Active Directory-Domänencontrollers ist ein Fehle	er aufgetreten.
		ОК
	Weitere Informationen zu Ergebnissen	
	< Zurück Weiter >	Schließen Abbrechen

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: WS IT-Solutions

WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC3) 2020-09-20 Migration auf Windows Server 2019

C Administrator: C:\Windows\system32\cmd.exe - powershell			×
C:\Users\Stephan-T0>powershell			
Windows Powershell Copyright (C) 2016 Microsoft Corporation. Alle Rechte vorbehalten.			
<pre>PS C:\Users\Stephan-T0> Import-Module ADDSDeployment PS C:\Users\Stephan-T0> \$AdminPWD = Read-Host -AsSecureString ************************************</pre>			
<pre>PS C:\Users\Stephan-T0> Uninstall-ADDSDomainController -DemoteOper Password \$AdminPWD -NoRebootOnCompletion:\$true</pre>	ationMasterRole:\$tr	rue -Force:\$true -LocalAdm	inistrator
Administrator: C:\Windows\system32\cmd.exe - powershell			×
C:\Users\Stephan-T0>powershell			^
Uninstall-ADDSDomainController			
Umgebung und Benutzereingaben werden überprüft Alle Tests wurden erfolgreich abgeschlossen. [oooooooooooooooooooooooooooooooooooo	000000000000000000000000000000000000000		000]
Administrator: C:\Windows\system32\cmd.exe - powershell			×
C:\Users\Stephan-T0>powershell Windows PowerShell Converte (C) 2016 Wingersft Conservation Allo Boshto workshelter			^
copyright (C) 2016 Microsoft Corporation. Alle Rechte Vorbenalten.			
PS C:\Users\Stephan-T0> Import-Module ADDSDeployment PS C:\Users\Stephan-T0> \$AdminPWD = Read-Host -AsSecureString			
PS C:\Users\Stephan-T0> Uninstall-ADDSDomainController -DemoteOper Password \$AdminPWD -NoRebootOnCompletion:\$true	ationMasterRole: \$t r	rue -Force:\$true -LocalAdm	inistrator
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:

				and the second second	1000	and the second se	10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	100.0
🔀 Windows PowerShell							2 <u>—</u> 2	×
PS C:\> Resolve-DnsName -N	lame www.ws-	its.de	2					^
Name www.ws-its.de	Type CNAME	TTL 43	Section Answer	NameHost ws-its.de				
Name : ws-its.de QueryType : AAAA TTL : 74 Section : Answer IP6Address : 2a01:238:20a:	202:1086::							
Name : ws-its.de QueryType : A TTL : 43 Section : Answer IP4Address : 81.169.145.86								

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:

🔀 Windows PowerShell						_	×
PS C:\> Resolve-DnsName -Name	www.ws-	its.de	e -server 1	92.168.101.1			^
Name	Туре	TTL	Section	NameHost			
www.ws-its.de	CNAME	39	Answer	ws-its.de			
Name : ws-its.de QueryType : AAAA TTL : 148 Section : Answer IP6Address : 2a01:238:20a:202	:1086::						
Name : ws-its.de QueryType : A TTL : 39 Section : Answer IP4Address : 81.169.145.86 PS C:\>							

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:

Active Directory-Benutzer und -Computer			
Datei Aktion Ansicht ?			
🗢 🔿 🙍 📰 🤞 📋 🗙 🖾 🗟 🕞	1 🐍 🐮 🍸 🧕 🐍		
Active Directory-Benutzer und -Computer [WS-DC1	Name	Тур	Beschreibung
> Gespeicherte Abfragen	WS-DC3	Computer	
V III ws.its			
> Builtin			
Computers Demain Controllerr	Verschieben	×	
Domain Controllers EoreignSecurityPrincipals	verschieben	~	
Keve	Objekt in Container verschieben:		
> CostAndFound			
Managed Service Accounts		•	
Microsoft Exchange Security Groups	Builtin		
> 📔 Program Data	Computers		
> 📔 System	Domain Controllers		
> 📔 Users	Foreign SecurityPrincipals		
✓ 📓 WS			
> 📓 AdminArea			
> 🗐 Benutzer		ips III	
> 🖬 Clients	Microsoft Exchange System Object	ts	
> 🖬 Exchange-Objekte	NTDS Quotas		
V 🔄 Gruppen		×	
domainiokal		ALL 1	
> 🔤 giobai	OK	Abbrechen	
> enver			
> Server			

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

드 PAM-AdminGUI - verbunden	mit WS-DC1.ws.its (Version V2.00)			_
Zeitraum: 3 Stunden Ziel-DC:	✓ zu DC replizieren	zu allen DC replizieren Die automatische AD-F	Replikation ist aktiv.	
Security-Tiers:	Admins:	mögliche Gruppen:	aktive Mitgliedschaften:	
	x	x	x	
ale Terch - DomanAdministration Terch - ServerAdministration Terch - CiencrAdministration Terch - ServiceAdmin	dephan-T3	GG-Admin-AD-GPO GG-Admin-Backup GG-Admin-DHOP GG-Admin-DNS GG-Admin-MpanV GG-Admin-HyperV-Storage GG-Admin-HyperV-Storage GG-Admin-ADPS Server GG-Admin-MX GG-Admin-MX GG-Admin-MX	Gültigket Gruppe 2020-09-20 17:17:16 GG-Admin-ATA 2020-09-20 17:52:51 GG-Admin-AD-Join 2020-09-20 17:53:43 Domänen-Admins	

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

Cas Administrator: C:\Windows\system32\cmd.exe - powershell	-	х
PS C:\> Add-Computer -DomainName ws.its		^
Cmdlet Add-Computer an der Befehlspipelineposition 1 Geben Sie Werte für die folgenden Parameter an: Credential		
Bei Windows PowerShell anmelden ? 🗙		
Geben Sie Ihre Anmeldeinformationen ein.		
Benutzername: 🙍 ws\stephan-t3 🗸		
Kennwort:		
OK Abbrechen		



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:

📥 Konfigurations-Assistent für die	e Active Directory-Domänend	lienste			-	_		×
Bereitstellungskor	nfiguration					Z WS	IELSER -DC3.w	VER /s.its
Bereitstellungskonfigurati Domänencontrolleroption Zusätzliche Optionen Pfade Optionen prüfen Voraussetzungsüberprüfu Installation Ergebnisse	Wählen Sie den Bereitstel Domänencontroller zu Neue Domäne zu eine Neue Gesamtstruktur Geben Sie die Domänenin Domäne: Geben Sie die Anmeldein <keine anmeldeinformat<="" th=""><th>Ilungsvorgang a u einer vorhand er vorhandenen hinzufügen nformationen fü nformationen fü tionen angegeb</th><th>enen Domäne hinzu Gesamtstruktur hin: ir diesen Vorgang ar ws.its r diesen Vorgang an. en></th><th>fügen zufügen 1.</th><th></th><th>Ausw</th><th>ählen</th><th></th></keine>	Ilungsvorgang a u einer vorhand er vorhandenen hinzufügen nformationen fü nformationen fü tionen angegeb	enen Domäne hinzu Gesamtstruktur hin: ir diesen Vorgang ar ws.its r diesen Vorgang an. en>	fügen zufügen 1.		Ausw	ählen	
		< Zu	urück Weiter >		Installieren	A	bbrech	en

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

Konfigurations-Assistent für die	Active Directory-Domänendienste		_		×
Konfigurations-Assistent für die Bereitstellungskonfigurati Domänencontrolleroption Zusätzliche Optionen Pfade Optionen prüfen Voraussetzungsüberprüfu Installation Ergebnisse	Active Directory-Domänendienste figuration Wählen Sie den Bereitstellungsvorgang a © Domänencontroller zu einer vorhand O Neue Domäne zu einer vorhandenen O Neue Gesamtstruktur hinzufügen Geben Sie die Domäneninformationen fü Domäne: Geben Sie die Anmeldeinformationen fü ws\stephan-t0	us. enen Domäne hinzufügen Gesamtstruktur hinzufügen ir diesen Vorgang an. ws.its r diesen Vorgang an.		ZIELSE WS-DC3.1	X RVER ws.its
	Weitere Informationen zu Bereitstellung	konfigurationen			
	< Zu	ırück Weiter >	Installieren	Abbrec	hen

NS IT-Solutions

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:

📥 Konfigurations-Assistent für die	Active Directory-Domänendienste		-		×
Domänencontrolle	eroptionen			ZIELSEF WS-DC3.v	RVER vs.its
Bereitstellungskonfigurati Domänencontrolleroption DNS-Optionen Zusätzliche Optionen Pfade Optionen prüfen Voraussetzungsüberprüfu Installation Ergebnisse	Domänencontrollerfunktionen und Stand DNS-Server Globaler Katalog Schreibgeschützter Domänencontrol Standortname: Kennwort für den Verzeichnisdienst-Wied Kennwort: Kennwort bestätigen:	dortinformationen angeben ler (RODC) Neufahrn derherstellungsmodus (DSRM-Kennu •••••••••••	vort) ein	geben	3
	Weitere Informationen zu Domänencont	rolleroptionen			
	< Zu	rrück Weiter > Insta	llieren	Abbrech	nen

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:

📥 Konfigurations-A	ssistent für die	Active Directory-Domänendienste	_		×
DNS-Opti	onen			ZIELSI WS-DC3	ERVER .ws.its
Für den DNS	-Server kann k	eine Delegierung erstellt werden, da die autorisierende übergeordnete Zone	Mehr ar	nzeigen	×
Bereitstellungs Domänencontr DNS-Option	konfigurati rolleroption nen	DNS-Delegierungsoptionen angeben DNS-Delegierung aktualisieren			
Zusätzliche Op	tionen				
Pfade					
Optionen prüfe	en				
Voraussetzung	süberprüfu				
Installation					
Ergebnisse		Weitere Informationen zur DNS-Delegierung			
		< Zurück Weiter > Inst	tallieren	Abbre	then

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

📥 Konfigurations-Assistent für die	Active Directory-Domänendienste		-		×
Zusätzliche Optio	nen			ZIELSEI WS-DC3.v	RVER vs.its
Bereitstellungskonfigurati Domänencontrolleroption DNS-Optionen Zusätzliche Optionen	IFM-Optionen (Install From Media, Vom Vom Medium installieren Zusätzliche Replikationsoptionen angeb	Medium installieren) angeben en			
Pfade	Replizieren von:	WS-DC1.ws.its			~
Optionen prüfen					
Voraussetzungsüberprüfu					
Installation					
Ergebnisse					
	Weitere Informationen zu zusätzlichen C	ptionen			
	< 70	urück Weiter > Ins	tallieren	Abbreck	hen

Für einen Pfadwechsel gibt es keinen Grund:

WS IT-Solutions

🚡 Konfigurations-Assistent für die	Active Directory-Domänendienste		-		×
Pfade			١	ZIELSER WS-DC3.w	VER /s.its
Bereitstellungskonfigurati Domänencontrolleroption DNS-Optionen	Geben Sie den Speicherort der AD DS an.	-Datenbank, der Protokolldateien und d	den Ort v	ron SYSVC)L
Zusätzliche Optionen	Ordner für Protokolldateien:	C:\Windows\NTDS			
Pfade Optionen prüfen Voraussetzungsüberprüfu Installation Ergebnisse	Ordner für Protokolldateien: SYSVOL-Ordner:	C:\Windows\SYSVOL			
	Weitere Informationen zu Active Direc	zurück Weiter > Instal	lieren	Abbrech	ien

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

WS IT-Solutions

📥 Konfigurations-Assistent für die	Active Directory-Domänendienste – 🗆 🗙	
Voraussetzungsük	perprüfung ZIELSERVER WS-DC3.ws.its	
 Alle erforderlichen Kompor Bereitstellungskonfigurati Domänencontrolleroption DNS-Optionen Zusätzliche Optionen 	enten wurden erfolgreich überprüft. Klicken Sie auf "Installieren", um die Inst Mehr anzeigen X Vor dem Installieren der Active Directory-Domänendienste auf dem Computer müssen die Voraussetzungen überprüft werden. Voraussetzungsüberprüfung erneut ausführen	
Pfade Optionen prüfen Voraussetzungsüberprüfu Installation Ergebnisse	 Ergebnisse anzeigen 942564 (http://go.microsoft.com/fwlink/?Linkld=104751). Für den DNS-Server kann keine Delegierung erstellt werden, da die autorisierende übergeordnete Zone nicht gefunden wurde oder Windows DNS-Server nicht ausgeführt wird. Wenn Sie eine Integration in eine vorhandene DNS-Infrastruktur vornehmen möchten, sollten Sie in der übergeordneten Zone manuell eine Delegierung an den DNS-Server erstellen, um eine zuverlässige Namensauflösung von außerhalb der Domäne "ws.its" zu gewährleisten. Andernfalls ist keine Aktion erforderlich. Voraussetzungsüberprüfung abgeschlossen Alle erforderlichen Komponenten wurden erfolgreich überprüft. Klicken Sie auf "Installieren", um die Installation zu starten. 	
	Wenn Sie auf "Installieren" klicken, wird der Server am Ende der Heraufstufung automatisch neu gestartet. Weitere Informationen zu Voraussetzungen < Zurück	

nstallation	ZIELSERVE WS-DC3.ws.i
Bereitstellungskonfigurati Domänencontrolleroption DNS-Optionen	Fortschritt Replikation von CN=Schema,CN=Configuration,DC=ws,DC=its: 1000 Objekte von ungefähr 3273 Objekten empfangen.
Zusätzliche Optionen Pfade Optionen prüfen Voraussetzungsüberprüfu Installation Ergebnisse	 Domänencontroller unter Windows Server 2019 haben einen Standardwert für die Sicherheitseinstellung "Mit Windows NT 4.0 kompatible Kryptografiealgorithmen zulassen". Durch diese Einstellung wird verhindert, dass beim Herstellen von Sicherheitskanalsitzungen schwächere Kryptografiealgorithmen verwendet werden. Weitere Informationen zu dieser Einstellung finden Sie im Knowledge Base-Artikel 942564 (http://go.microsoft.com/fwlink/?Linkld=104751). Für den DNS-Server kann keine Delegierung erstellt werden, da die autorisierende übergeordnete Zone nicht gefunden wurde oder Windows DNS-Server nicht ausgeführt wird. Wenn Sie eine Integration in eine vorhandene DNS-Infrastruktur vornehmen möchten, sollten Sie in der übergeordneten Zone manuell eine Delegierung an den DNS-Server erstellen, um eine zuverlässige Namensauflösung von außerhalb der Domäne "ws.its" zu gewährleisten. Andernfalls ist keine Aktion erforderlich.
	Weitere Informationen zu Installationsoptionen

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

WS IT-Solutions

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:



WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC3) 2020-09-20 Migration auf Windows Server 2019

	Geräte	Bibliotheken	Sensoren	Alarme	Maps	Berichte	Protokoll	Tickets	Konfiguration Neue Alar
Geräte WS-IT	TS 🔻 Serv	ver 🔻 WS-DC3	Sensor hinzufüge	n (Schritt 2 vo	n 2)				
	Senso	or hinzufüge	en zum Gerät	t WS-DC3	[192.168	3.101.1]			
	< Abbr	rechen							
	Allg	gemeine Sen	soreinstellur	igen		Name de	es Sensors 💿	Base WS-DC3	
						Übergeor	dnete Tags 🕚		
							Tags 🕚	xmlexesensor	× 0
		Prioriti						★★★☆☆	
	Ser	nsoreinstellu	ngen					Die ausführl Das Arbeitsv Arbeitsverze	bare Datei wird auf der Maschine ausgeführt, auf der die übergeordnete Probe Insta verzeichnis für EXE-Dateien ist das Verzeichnis der Probevbs-, .ps1- oder andere Sk lichnisse verwenden.
						Progra	mm/Skript 🔍	WSSensor-Serve	erBaseline.ps1
							Parameter 🕚	"WS-DC3"	
							Umgebung 🖲	 Standardum Platzhalter a 	gebung Is Umgebungsvariablen verwenden
						Sicherh	eitskontext 🔍	 Sicherheitsko Die Zugangso 	ontext des Probe-Dienstes verwenden daten für Windows des übergeordneten Geräts verwenden

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:

Datei Start Freigeben Ansich	ıt			\sim
\leftarrow \rightarrow \checkmark \uparrow \blacksquare > Netzwerk > ws-	dc3 → c\$	ٽ ~	"c\$" durchsuchen	م
📌 Schnellzugriff	Name	Änderungsdatum	Тур	Größe
Dedter	Admin	20.09.2020 14:56	Dateiordner	
Desktop	Benutzer	20.09.2020 14:57	Dateiordner	
🥈 Walther, Stephan - T0	PerfLogs	01.06.2020 16:36	Dateiordner	
💻 Dieser PC	Program Files (x86)	15.09.2018 09:21	Dateiordner	
🏪 System (C:)		15.11.2019 17:49	Dateiordner	
🛖 Freigaben (M:)	Windows	20.09.2020 14:59	Dateiordner	
AdminArea	2020-09-20-DHCPExport-WS-DC3.cfg	20.09.2020 13:54	CFG-Datei	40 KB
- Zwischenablage		20.09.2020 15:06	Dateiordner	
	Microsoft ATA Gateway Setup.zip	20.09.2020 15:00	ZIP-komprimierte	95.157 KB
Bibliotheken				

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...

PS C	:\Win	ndows\sy	stem32>	Enter-P	SSession -ComputerName ws-dc3					
[ws- WARN WARN WARN WARN	[ws-dc3]: PS C:\Users\stephan-T0\Documents> Import-DhcpServer -File C:\2020-09-20-DHCPExport-WS-DC3.cfg -Leases -BackupPath C:\dhcp WARNUNG: Die Netzwerkverbindungsnit "ws-dc3" wurde unterbrochen. Es wurde für 4 Minuten versucht, die Verbindung wiederherzustellen WARNUNG: Versuch der Verbindungsaufnahme mit "ws-dc3" WARNUNG: Versuch der Verbindungsaufnahme mit "ws-dc3" WARNUNG: Versuch der Verbindungsaufnahme mit "ws-dc3"									
	2 \	Windows P	owerShell				-		×	
	Ping STRG- PS C: Route über 1	wird aus C \Users\S enverfolg maximal	geführt f tephan-T0 ung zu ws 30 Hops: *	Für ws-dc > tracer s-dc3.ws.	3.ws.its [192.168.101.1] mit 32 Bytes Daten: t -d ws-dc3 its [192.168.101.1] Zeitüberschreitung der Anforderung.				^	
	2 3	*	*	-	Zeitüberschreitung der Anforderung.					

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

Solut	ions	WSHow 2020-09	To – N -20 M	/ligrat ligratio	ion ein on auf	es Do Windo	main C ows Se	ontroll rver 20	ers auf 19	2019 (\	NS-D	C3
	NSE System	stem - Interi	faces -	Firewall 👻	Services -	VPN -	Status 🔻	Diagnostics 👻	Help 🗸			(
Serv	ices / Sn	ort / Block	ed Hosts									0
Snort I	Interfaces	Global Settings	Updates	a Alerts	Blocked	Pass Lists	Suppress	s IP Lists	SID Mgmt	Log Mgmt	Sync	
Block	ed Hosts a Blocked Ho	nd Log View S osts 🛃 Down	ettings _{oad}				Û	Clear				
		All blocke	d hosts will b	e saved			All b	locked hosts will	be removed			
Refr	esh and Log V	iew 🖪 Save			✓ Re	fresh		500			•	
		Save auto	-refresh and v	view settings	Defau	lt is ON		Numb Defau	er of blocked ent It is 500	ries to view.		
Last	500 Hosts I	Blocked by Sn	ort									
#	IP	Alert Des	criptions and	Event Times							Remove	
1	192.168.101. Q	1 ET SCAI ET SCAI	N Behavioral L N DCERPC rpc	Inusual Port 1 mgmt ifids Ur	35 traffic Poten authenticated E	tial Scan or Inf 3IND – 2020-09	ection – 2020-0)-20 15:13:40	9-18 07:41:02			×	
				11	nost IP address	is currently be	ing blocked Sno	rt.				

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:

😫 Bestätigen —		×
Die Konfiguration und Leases aus der Datei "c\2020-09-20-DHCPExport-WS-DC3.cfg" werden auf den Server "WS-DC3.Möchten Sie diese Aktion aus	ühren?" im	portiert.
Ja Nein		
P5 C:\Windows\system32> Enter-PSSession -ComputerName ws-dc3		
[ws-dc3]: PS C:\Users\stephan-TO\Documents> Import-DhcpServer -File c:\2020-09-20-DHCPExport-WS-DC3.cfg -Leases -Ba	kupPath o	c:\dhcp
[ws-dc3]: PS C:\Users\stephan-TO\Documents>		

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



Sechreibung Lotinitium Dammendisation Participations des Schritte werden ausgeführt um die Konfiguration des DHCP-Servers auf dem Zielosomung der DHCP-Servers	📥 DHCP-Konfigurations-Assistent	nach der Installation	- (×
Beschreibung Autorisierung Zusammerfasung Febreade Schriete werden ausgeführt, um die Konfiguration des DHCP-Servers auf dem Zeisomputer abzuschlieden: Bittelen Sie die folgenden Sicherheitsgruppen für die Delegierung der DHCP-Serverswaltung: DHCP-Abmittatoren DHCP-Abmittatoren Zusammerfasung Vordisierung DHCP-Server auf dem Ziekomputer (sofern dieser einer Domäne beigetreten attrisieren Sie den DHCP-Server auf dem Ziekomputer (sofern dieser einer Domäne beigetreten attrisieren Sie den DHCP-Server auf dem Ziekomputer (sofern dieser einer Domäne beigetreten attrisieren Sie die Anmeldeinformationen zum Authentifizieren dieses DHCP-Servers in den Active Director/Domänendiensten an. Beschreibung Zusammerfasung Geben Sie die Anmeldeinformationen zum Authentifizieren dieses DHCP-Servers in den Active Director/Domänendiensten an. Quantmerfasung Mentideinformationen des folgenden Benutzers verwenden Benutzername: WSISBephan-T0 Onterrative Anmeldeinformationen vervenden Benutzername: Angeben. On Ab-Autorisierung überspringen Ab-Autorisierung überspringen	Beschreibung				
Zusammerfasung Estellen Sie die folgenden Sicherheitsgruppen für die Delegierung der DHCP-Serverewaltung: - DHCP-Administratoren - DHCP-Server auf dem Zielcomputer (sofern dieser einer Domäne beigetreten is). Autorisieren Sie den DHCP-Server auf dem Zielcomputer (sofern dieser einer Domäne beigetreten is).	Beschreibung Autorisierung	Folgende Schritte werden ausgeführt, um die Konfiguration des DHCP-Servers au Zielcomputer abzuschließen:	f dem		
	Zusammenfassung	Erstellen Sie die folgenden Sicherheitsgruppen für die Delegierung der DHCP-Ser - DHCP-Administratoren - DHCP. Reputter	ververwa	altung:	
< Zurick		- DHCP-benutzer Autorisieren Sie den DHCP-Server auf dem Zielcomputer (sofern dieser einer Don ist).	näne bei	getrete	n
Zurück Weiter > Commit ausführen Abbrechen DHCP-Konfigurations-Assistent nach der Installation – I × Autorisierung Beschreibung Directory-Domänendiensten an. @ Anneldeinformationen zum Authentifizieren dieses DHCP-Servers in den Active Directory-Domänendiensten an. @ Anneldeinformationen des folgenden Benutzers verwenden Benutzername: WS\Stephan-T0 @ Alternative Anmeldeinformationen verwenden Benutzername: @ Alternative Anmeldeinformationen verwenden Benutzername: @ AD-Autorisierung überspringen @ AD-Autorisierung überspringen @ Atternative Anmeldeinformationen verwenden Benutzername: @ AD-Autorisierung überspringen					
Curick Weiter> Commit ausführen Abbrechen Abbrechen Abbrechen Curick Weiter> Commit ausführen Abbrechen Abbrechen Abtrechen Curick Weiter> Commit ausführen Abbrechen Abbrechen Curick Weiter> Commit ausführen Abbrechen Abbrechen Curick Weiter> Commit ausführen Abbrechen Curick Weiter> Commit ausführen Abbrechen Curick Weiter> Commit ausführen Abbrechen Commit ausführen Abbrechen Curick Weiter> Commit ausführen Abbrechen Commit ausführen Abbrechen Curick Weiter> Commit ausführen Abbrechen Curick Autorisierung					
< Zurick					
< Zurück					
DHCP-Konfigurations-Assistent nach der Installation × Autorisierung Beschreibung Autorisierung Ceben Sie die Anmeldeinformationen zum Authentifizieren dieses DHCP-Servers in den Active Directory-Domänendiensten an. @ Anmeldeinformationen des folgenden Benutzers verwenden Benutzername: WS\Stephan-T0 Alternative Anmeldeinformationen verwenden Benutzername: AD-Autorisierung überspringen AD-Autorisierung überspringen		< Zurück Weiter > Commit ausführ	en Ab	breche	n
Beschreibung Geben Sie die Anmeldeinformationen zum Authentifizieren dieses DHCP-Servers in den Active Directory-Domänendiensten an. Zusammenfassung	🔁 DHCP-Konfigurations-Assistent	nach der Installation	- (×
Beschreibung Geben Sie die Anmeldeinformationen zum Authentifizieren dieses DHCP-Servers in den Active Directory-Domänendiensten an. Zusammenfassung Anmeldeinformationen des folgenden Benutzers verwenden Benutzername: WS\Stephan-T0 Alternative Anmeldeinformationen verwenden Benutzername: Angeben AD-Autorisierung überspringen 	Autorisierung				
Zusammenfassung Anmeldeinformationen des folgenden Benutzers verwenden Benutzername: MS\Stephan-T0 Alternative Anmeldeinformationen verwenden Benutzername: Angeben AD-Autorisierung überspringen 	Beschreibung Autorisierung	Geben Sie die Anmeldeinformationen zum Authentifizieren dieses DHCP-Servers Directory-Domänendiensten an.	in den A	ctive	
Alternative Anmeldeinformationen verwenden Benutzername: Angeben AD-Autorisierung überspringen	Zusammenfassung	Anmeldeinformationen des folgenden Benutzers verwenden Benutzername: WS\Stephan-T0			
Angeben Angeben Angeben AD-Autorisierung überspringen		Alternative Anmeldeinformationen verwenden			
AD-Autorisierung überspringen		Benutzername: Angeben			
		O AD-Autorisierung überspringen			
< ZUPUCK Vielter > Commit austument Abbrechen		< Zurück Weiter > Commit ausführ	en Ab	obreche	en j

Oder auch nicht...

WS IT-Solutions

ᡖ DHCP-Konfigurations-Assiste	ent nach der Installation	_		×
Zusammenfassu	ng			
Beschreibung Autorisierung	Im Anschluss finden Sie den Status der Konfigurationsschritte nach der Inst	allation:		
Zusammenfassung	Sicherheitsgruppen werden erstellt Fehler beim Installieren der Sicherheitsgruppe "DHCP-Benutzer" oder "DH Administratoren". Fehlercode: 1722. Der RPC-Server ist nicht verfügbar. Diese Sicherheitsgruppen müssen für DHCP erstellt werden, da DHCP-Sei den Mitgliedern dieser Gruppen überwacht bzw. verwaltet werden könne DHCP-Server wird autorisiert Fehler Fehler beim Autorisiert des DHCP-Servers: 20079. Die angegebenen Ser Verzeichnisdienst vorhanden. Wenn der DHCP-Server nicht von den Active Directory-Domänendienster kann er nicht auf DHCP-Anforderungen reagieren.	Fehler HCP- ver aussch n. ver sind be n autorisier	nließlich v ereits im t wird,	von
	< Zurück Weiter > Sch	ıließen	Abbrec	hen

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:

🚆 DHCP					-	
Datei Aktion Ansicht ?						
🗢 🌩 🖄 📰 🗟 🖬						
🕎 DHCP	Client-IP-Adresse	Name	Leaseablaufdatum	Тур	Eindeutige ID	Be
> ws-dc1.ws.its	192.168.111.100	WS-CL3.ws.its	Reservierung (aktiv)	Keine	901b0e4e8726	
Bereich [172.19.121.0] DMZ-121						
> 📔 Bereich [172.19.131.0] DMZ-131						
> 🧮 Bereich [192.168.101.0] LAN-101						
✓ I Bereich [192.168.111.0] LAN-111						
Adresspool						
Adressleases						
Reserveringen						
Richtlinien						
📑 Serveroptionen						
📓 Richtlinien						
> 📝 Filter						
> 🔂 IPv6						

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:



臝 DNS-Manager			
Datei Aktion Ansicht ?			
🗢 🄿 者 📆 🖾 🔛 🕯 🖬	đ	Figenschaften von ws-dc3 ? X	
BNS	Name	e Weiterleitungen bearbeiten	\times
WS-DC1 ws-dc2 Image: Sonward-Lookupzonen Image: Sonward-Lookupzonen	Fon Rev Bed Star	IP-Adressen der Weiterleitungsserver: V IP-Adresse Vollqualifizierter Domän Überprüft Löschen IP-Adresse Vollqualifizierter Domän UP-Adresse Vollqualifizierter Domän Vollqualifizierter OK Vollqualifizierter Nach gben Vollqualifizierter OK Vollqualifizierter OK Vollqualifizierter OK Vollqualifizierter OK Vollqualifizierter OK Vollqualifizierter Nach gben Vollqualifizierter OK Vollqualifizierter OK Vollqualifizierter OK <	
		Sek. bis zur Zeitüberschreitung der Weiterleitungsabfragen: 3 Der vollqualifizierte Domänenname des Servers ist nicht verfügbar, wenn die entsprechenden Reverse- Lookupzonen und Einträge nicht konfiguriert sind.	
		OK Abbrechen	

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:



Microsoft Advance	ced Threat Analytics k	Configurationen					Suchen nach Benutze				
	System										
	Center	Gateways									
	Gateways										
	Updates	Gatewaysetu	Laden Sie die	ses Paket herunter, um e	in Gateway oder ein Lightweight-	Gateway zu installieren.					
	Datenquellen										
	Verzeichnisdienste										
	SIEM	NAME	^	ТҮР	DOMANEN-CONTROLLER	VERSION	DIENSTSTATUS				
	VPN	WS-ATA		Gateway	ws-dc1.ws.its	1.9.7478.57683	Wird ausgeführt				
	Erkennung	WS-DC2		Lightweight-Gateway	WS-DC2.ws.its	1.9.7478.57683	Wird ausgeführt				
	Entitätsmarkierungen										
	Ausnahmen		Öffnen von Microso	ft ATA Gateway Setup.zip	×						
	Benachrichtigungen und		Sie möchten folger	ide Datei öffnen:							
	Berichte		🦉 Microsoft AT	A Gateway Setup.zip							
	Sprache		Vom Typ: Con	mpressed (zipped) Folder (92,	9 MB)						
	Benachrichtigungen		von: https://a	ita.ws.its							
	Geplante Berichte		Wie soll Firefox m	it dieser Datei verfahren?							
	E-Mail-Server		○ <u>Ö</u> ffnen mit	Windows-Explorer (Standar	d) ~						
	Syslog-Server		Datei <u>s</u> peiche	rn							
	Sonstiges		Eür Dateien o	lieses Typs immer diese Aktio	on ausführen						
	Lizenzierung			C	OK Abbrechen						

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...

	$\leftarrow \rightarrow \checkmark \uparrow \blacksquare \rightarrow Die$	eser	PC > System (C:)			
	Organisieren 👻 Ausge	wäh	lten Ordner in Bibliothek einschließen 🔻	Zugriff gewähren auf 🔻	Neuer Ordner	
	🛃 Schnellzugriff	Ν	lame	Änderungsdatum	Тур	Größe
	Desktop *		Admin	20.09.2020 18:43	Dateiordner	
	🖆 Dokumente 💉	i	Benutzer	20.09.2020 14:57	Dateiordner	
	Develoads		DHCP	20.09.2020 16:28	Dateiordner	
- Download			PerfLogs	01.06.2020 16:36	Dateiordner	
	📰 Bilder 🛛 🖈		Program Files (x86)	15.09.2018 09:21	Dateiordner	
	📃 Desktop		Programme	15.11.2019 17:49	Dateiordner	
	🤱 Walther, Stephan	- [Windows	20.09.2020 14:59	Dateiordner	
	Dieser PC	[2020-09-20-DHCPExport-WS-DC3.cfg	20.09.2020 13:54	CFG-Datei	
	System (C)	[Microsoft ATA Gateway Setup.zip	20.09.2020 15:00	ZIP-Datei	95.1
	Ereigaben (Mt)					
	Diblication					
	Netzwerk					
	Systemsteuerung					

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

WS IT-Solutions WSHow 2020-09

WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC3) 2020-09-20 Migration auf Windows Server 2019

									 _
🖼 Administrator: C:\Windows\system32\cmd.exe - powershell								-	×
:\>power indows P opyright	oshell PowerShell : (C) Microsoft	Corpo	ration. Alle Rechte	vorbehalten.					
S C:\> E	xpand-Archive	-Path	'C:\Microsoft ATA Ga	teway Setup.	zip' -Destinatio	nPath c:\ATA			
S C:\>									
	🕳 System (C:)								
	$\leftarrow \rightarrow \checkmark \uparrow$	⇒ Die	ser PC > System (C;)						~ 7
_	Organisieren 🔻	Ausge	wählten Ordner in Bibliothek e	inschließen 🔻	Zugriff gewähren auf	 Neuer Ordner 			
	📌 Schnellzugriff	^	Name		Änderungsdatum	Тур	Größe		
	Desktop	*	Admin		20.09.2020 18:43	Dateiordner			
	Dokumente	*	Benutzer		20.09.2020 14:57	Dateiordner			
	Downloads	*	DHCP		20.09.2020 16:28	Dateiordner			
	- Pilder		PerfLogs		01.06.2020 16:36	Dateiordner			
	i bildei	~	Program Files (x86)		15.09.2018 09:21	Dateiordner			
	Desktop		Programme		15.11.2019 17:49	Dateiordner			
	🤱 Walther, Ste	phar	Windows		20.09.2020 14:59	Dateiordner			
	Dieser PC		2020-09-20-DHCPExpor	t-WS-DC3.cfg	20.09.2020 13:54	CFG-Datei	40 KB		
	System (Ci	,	Microsoft ATA Gateway	Setup.zip	20.09.2020 15:00	ZIP-Datei	95.157 KB		
	System (C:	/	ΑΤΑ		20.00.2020.19-40	Dateiordper			

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:

🛃 Ereignisanzeige							
Datei Aktion Ansicht ?							
🗢 🌩 🖄 📰 📓 🖬							
🛃 Ereignisanzeige (Lokal)	^	EXE and DLL Anzahl	von Ereignissen: 679 (!) N	leue Ereignisse sind verfü	gbar		
> 📑 Benutzerdefinierte Ansichten	li	Ebono	Datum und Ubrait	Quelle	Freignis-ID	Aufgabooka	
> 🙀 Windows-Protokolle		Informationon	20.00.2020.19:54:24	Applacker	2002	Keine	
Anwendungs- und Dienstprotokolle		() Informationen	20.09.2020 10.94.24	Appeocker	0002	Keine	
Active Directory-Webdienste	-	() informationen	20.09.2020 10:34:16	AppLocker	8002	Keine	
DFS-Replikation	-	Informationen	20.09.2020 18:54:15	AppLocker	8002	Keine	
Directory Service		Informationen	20.09.2020 18:54:15	AppLocker	8002	Keine	
DNS Server		1) Informationen	20.09.2020 18:54:08	AppLocker	8002	Keine	
Hardware-Ereignisse		1) Informationen	20.09.2020 18:53:58	AppLocker	8002	Keine	
📔 Internet Explorer		(1) Informationen	20.09.2020 18:53:20	AppLocker	8002	Keine	
V Microsoft	- 11	Informationen	20.09.2020 18:53:18	AppLocker	8002	Keine	
V Windows	10	(i) Informationen	20.09.2020 18:53:08	AppLocker	8002	Keine	
> All-User-Install-Agent	- 11	Freignis 8002, Appl.oc	ker				
> AllJoyn	- 11		-				
> AppID	- 11	Allgemein Details					
> Application Server-Applications	- 11						
V AppLocker	- 11	Die Ausführung v	on %OSDRIVE%\USERS\ST	EPHAN-TO\APPDATA\LO	DCAL\TEMP\3	ACDE58AD-FE7	2-4698-89F2-73CFB4B34271)\.CR\MICROSOFT ATA GATEWAY SETUP.EXE wurde zugelassen.
EXE and DLL	- 11						
MSI and Script	- 11						
Packaged app-Deployment	- 11						
Packaged app-Execution	- 11						
> AppModel-Runtime	- 11						
> Appreadiness	- 11						
> Apps-API	- 11						

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:



Temp									
$\leftarrow \rightarrow \lor \uparrow$ $\square \rightarrow$ Dieser PC \rightarrow System (Ci) \rightarrow Benutzer \rightarrow stephan-TO \rightarrow AppData \rightarrow Local \rightarrow Temp $\lor \heartsuit$								o" durc	
Administrator: C:\Windows\system32\cmd.exe - powe	Organisieren 👻 🧻 Öf	fnen 🔻 Zugriff gewähren au	f 🕶 Drucken Neuer	Ordner					
-a 01.04.2019 08:40	🗄 Dokumente 🖈 🛆	Name	*		Änderungsdatum	Тур	Größe		
-a 08.08.2017 10:07	🖊 Downloads 🖈	3			20.09.2020 18:55	Dateiordner			
-a 18.06.201/ 13:5/ -a 08.08.2017 19:19	📰 Bilder 🛛 🖈	Microsoft Advanced Threat	Analytics Gateway_202009201	85018.log	20.09.2020 18:50	Textdokument		7 KB	
-a 27.07.2017 14:18	Desktop	Microsoft Advanced Threat	Analytics Gateway_202009201	85106.log	20.09.2020 18:51	Textdokument		7 KB	
-a 25.03.2019 06:42 -a 28.01.2015 04:02	a Walther, Stephar	Microsoft Advanced Threat	Analytics Gateway_202009201	85134.log	20.09.2020 18:51	Textdokument		7 KB	
-a 01.05.2017 07:33	Dieser PC	Microsoft Advanced Threat	Analytics Gateway_202009201	85415.log	20.09.2020 18:54	Textdokument		7 KB	
-a 15.10.2015 23:57 -a 04.05.2017 23:33	System (C:)	MICrosoft Advanced Thread	Analytics Gateway_202009201	63333.log	20.09.2020 10.33	Textuokument		7 KD	
-a Microsoft Advanced Threat Analytics Gateway_2	0200920185555.log - Editor					_		x	
-a Datei Bearbeiten Format Ansicht Hilfe								_	
 1116:044AC [2220-09-20116:55:57]141 1116:044AC [2220-09-20118:55:57]141 1116:04AC [2220	c) Variable: KB304715 6) Variable: KB304715 6) Variable: NetFrame 6) Variable: NetFrame 6) Variable: WixBundl 6) Variable: WixBundl 7) Variable: WixBundl 7) Variable: WixBundl 7) Variable: WixBundl 7) Variable: WixBundl 7) Variable: WixBundl 7) Variable: WixBundl	Eloncomrigurationrier Atxists = 0 workCommandLineArgumen workRegistryValue = 46 ellevated = 1 elog = C:\Users\STEPHA eManufacturen = Microssoft Adva eDriginalSourceFolder = eOriginalSourceFolder = eSourceProcessFolder = SourceProcessFolt = C ellever = 4 eVersion = 1.9.748.57	<pre>str = C: \atd\\Gatewa ts = /passive /shown Hal4 /alue = 1 /\AppData\Local\Tem ff Corporation stred Threat Analytic ta\Microsoft ATA Gat = C:\ata\ Stata\ C:\ata\ \ata\Microsoft ATA 583</pre>	yinstallationconvigur mui s Gateway eway Setup.exe 36b4eac877} Gateway Setup.exe	ation.json	rs Gateway_2020	0920185	;5 =	
		5						v	
<	Ш		1		1			>	
			Windows (CRLF)	Zeile 55, Spalte 55	1	00%			
	6 Elemente 1 Element au	roewählt (6.17 KB)							

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:

👌 Ereignisanzeige			
Datei Aktion Ansicht ?			
🗢 🔿 📶 🖬			
🚦 Ereignisanzeige (Lokal)	Betriebsbereit A	Anzahl von Ereignissen: 0 (deaktiviert)	
> 🛱 Benutzerdefinierte Ansichten	Ehene	Datum und Ubrzeit	Quelle
> 🖺 Windows-Protokolle	Lbene	Datum und Unizeit	Quelle
Anwendungs- und Dienstprotokolle			
Active Directory-Webdienste			
DFS-Replikation			
Directory Service			
DNS Server			
Internet Explorer	1		
Microsoft			
✓	<		Ш
> 🧮 All-User-Install-Agent			
> 🛅 AllJoyn	II		
> 📫 AppID	Allgemein Deta	ails	
> Application Server-Applications			
> AppLocker	Angezeigte A	Ansicht O XML-Ansicht	
> AppModel-Runtime			
> AppReadiness			
> AppS-API		7	
Gespeicherte Protokolldatei	öffnen		
AppxPackaging Benutzerdefinierte Ansicht er	rstellen		
> 📫 ASN1 Benutzerdefinierte Ansicht in	mportieren		
> ATAPort Protokoll löschen			
> Audio			
> Authentication Actuents Protocol Internation			
> Authentication Eigenscharten			
Protokoll aktivieren			
Base-Filtering-F			
Alle Ereignisse speichern unt	ter		
Best Practices A Aufgabe an dieses Protokoll	anfügen		
> Bits-Client Ansicht	>		
Sluetooth-BthL Aktualisieren			
CAPI2	>		
Betriebsberen		1	
> CertificateServices-Deployment			

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



Betriebsbereit Anzahl von Ereignissen: 385 (!)	Neue Ereignisse sind verfügbar							
Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie				
🕕 Fehler	21.09.2020 16:30:09	CAPI2	30	Kettenrichtlinie überprüfen				
(i) Informationen	21.09.2020 16:30:09	CAPI2	30	Kettenrichtlinie überprüfen				
1 Informationen	21.09.2020 16:30:09	CAPI2	11	Kette erstellen				
Ereignis 30, CAPI2								
Allgemein Details								
Angezeigte Ansicht O XML-Ansich	ıt							
+ System								
- UserData								
- CertVerifyCertificateC	hainPolicy							
- Policy								
[type]	CERT_CHAIN_POLICY_SSL							
[constant]	4							
Certificate								
[filePof								
[subjectName								
Cartificate Chain	a danish s							
- CertificateChain								
[chainRef]	{5C314DA1-F94A-4B09-97A0-278CE220FDDD}							
- SSLAdditionalPol	icyInfo							
[authType]	server							
[serverName]	weataweite							
	ws dda.ws.its							
- ignoreriags								
[value]	0							
- Status								
[chainIndex]	0							
[elementinde	0 [x							
- EventAuxInfo								
[ProcessNam	e] ata.exe							
- CorrelationAuxIn	fo							
[Taskid]	{42E6C72C-44A4-4C4A-83CC-D5A93E12BF88}							
[SeqNumber]	1							
- Result	Der CN-Name des Zertifikats stimmt nicht mit dem	übergebenen Wert überein.						
[value]	800B010F	<u> </u>						

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:

드 PAM-AdminGUI - verbun	den mit WS-DC1.ws.its (Version V2.00)			-	\times
Zeitraum: 1 Stunde Ziel-DC:	✓✓ zu DC replizierer	n zu allen DC replizieren Die automatisc	1e AD-Replikation ist aktiv.		
Security-Tiers:	Admins:	mögliche Gruppen:	aktive Mitgliedschaften:		x
alle Tiero - Domain Administration Tier 1 - ServerAdministration Tier2 - ClientAdministration Tier3 - ServiceAdmin	stephan-T3	Domänen-Admins GG-Admin-AD-GPO GG-Admin-AD-Join GG-Admin-Backup GG-Admin-Plackup GG-Admin-Fingaben GG-Admin-Fingaben GG-Admin-Fingaben	 ▲ Goltigkeit Gri 2020-09-21 17:41:41 GG 2020-09-21 17:41:41 GG 2020-09-21 17:41:41 GG 	uppe 3-Admin-ATA 3-Admin-Setup-ApplockerAusnahme-ueberall 3-SEC-DomainController-Admins	

Mit dieser Kennung starte ich das Setup erneut:



Administrator: C:\Windows\sys	stem32\cmd.exe			×	
C:\Users\stephan-T3>cd_					
C:\>cd ATA	📙 Temp				
C:\ATAbata eye	\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow Die	ser PC > System (C:) > Benutzer > stephan-T3 > AppData > Local > Temp >			✓ Ö "Temp" dur
C:\ATA>explorer	Organisieren 👻 🧻 Öff	fnen 🔻 Zugriff gewähren auf 🔻 Drucken Neuer Ordner			
C+\ATA>	★ Schnellzugriff ■ Desktop ★ Dokumente	Name	Änderungsdatum	Тур	Größe
C. (A1A2		3	21.09.2020 16:43	Dateiordner	
		dd_vcredist_amd64_20200921164227.log	21.09.2020 16:42	Textdokument	9 KB
	L Downloads	dd_vcredist_amd64_20200921164227_0_vcRuntimeMinimum_x64.log	21.09.2020 16:42	Textdokument	168 KB
	Dilder A	dd_vcredist_amd64_20200921164227_1_vcRuntimeAdditional_x64.log	21.09.2020 16:42	Textdokument	189 KB
		Microsoft Advanced Threat Analytics Gateway_20200921164208.log	21.09.2020 16:43	Textdokument	18 KB
	Desktop	Microsoft Advanced Threat Analytics Gateway_20200921164208_001_BundleActio	21.09.2020 16:42	Textdokument	1 KB
	🤱 Walther, Stephar	Microsoft Advanced Threat Analytics Gateway_20200921164208_002_MsiPackage	21.09.2020 16:43	Textdokument	490 KB
	Dieser PC				
	System (C:)				

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

Microsoft Advan	ced Threat Analytics K	onfigurationen					Suchen nach Benutz	ern, Computern
	System Center Gateways	Gateways						
	Updates Datenquellen	Gatewaysetup	Laden Sie dieses	Paket herunter, um ein	Gateway oder ein Lightweight-G	ateway zu installieren.		
	SIEM	NAME	^	ТҮР	DOMÄNEN-CONTROLLER	VERSION	DIENSTSTATUS	INTEGRITÄT
	VPN	WS-ATA		Gateway	ws-dc1.ws.its	1.9.7478.57683	Wird ausgeführt	
	Erkennung	WS-DC2		Lightweight-Gateway	WS-DC2.ws.its	1.9.7478.57683	Wird ausgeführt	
	Entitätsmarkierungen Ausnahmen	WS-DC3		Lightweight-Gateway	WS-DC3.ws.its	1.9.7478.57683	Wird gestartet	

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:



Aurgabenplanung		
Datei Aktion Ansicht ?		
Aufgabenplanung (WS-DC3.) Aufgabenplanungsbibliot Name	Status Trigger Nächste Laufzeit Letzte Laufzeit Ergebnis der letzten Ausführung Autor	Erstellt
	Öffnen	×
	\leftarrow \rightarrow \checkmark \uparrow $_{\sim}$ « WS-DC3 \rightarrow LWC \checkmark $_{\circ}$ $^{\circ}$ "LWC" durchsuchen	Q
	Organisieren ▼ Neuer Ordner 🗄 🖛 [•
	Geräte ^ Name	Änder
	Lizenzen 🔮 Check-ADStart.xml	20.09.2
	Netzwerk	20.09.2
	Active Directory gMSA-Admin GPO KRBTGT-Reset Migration-2019 WS-DC1 WS-DC3	
		;
	Dateiname: ServerSicherung.xml V XML-Dateien (*.xml) Öffnen Abbr	~ rechen

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

Aufgabenplanung (WS-DC3A) Aufgabenplanungsbibliot	Name Status Trigger Nächste Laufzeit Letzte Laufzeit Ergebnis der letzten Ausführung Autor Erstell
	Aufgabe erstellen X
	Allgemein Trigger Aktionen Bedingungen Einstellungen
	Name: ServerSicherung
	Speicherort:
	Autor: WS\stephan-ad
	Beschreibung:
	Sicherheitsoptionen
	Beim Ausführen der Aufgaben folgendes Benutzerkonto verwenden:
	WS\stephan-T3 Benutzer oder Gruppe ändern
	O Nur ausführen, wenn der Benutzer angemeldet ist
	Nur ausführen, wenn der Benutzer angemeldet ist Unabhängig von der Benutzeranmeldung ausführen
	 Nur ausführen, wenn der Benutzer angemeldet ist Unabhängig von der Benutzeranmeldung ausführen Kennwort nicht speichern. Die Aufgabe greift nur auf lokale Computerressourcen zu.
	Nur ausführen, wenn der Benutzer angemeldet ist Unabhängig von der Benutzeranmeldung ausführen Kennwort nicht speichern. Die Aufgabe greift nur auf lokale Computerressourcen zu.
	Nur ausführen, wenn der Benutzer angemeldet ist Unabhängig von der Benutzeranmeldung ausführen Kennwort nicht speichern. Die Aufgabe greift nur auf lokale Computerressourcen zu. Mit höchsten Privilegien ausführen
	 Nur ausführen, wenn der Benutzer angemeldet ist Unabhängig von der Benutzeranmeldung ausführen

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



띀 gMSA-Admin		- 🗆 X
vorhandene gMSA:	zugehörige Server:	zugehörige Gruppen:
gMSA-Backup (Task User für MMR) gMSA-Monitor (Task User für Monitoring) gMSA-SQLDPM (Service SQL auf WS-DPM) erstelle gMSA Iösche gMSA bearbeite gMSA Iösche gMSA bearbeite gMSA Klicke in eine Zeile un	WS-DC1 ws its WS-FS1.ws its WS-CA1.ws its WS-CA1.ws its WS-RD51.ws its WS-RD51.ws its WS-RD51.ws its WS-RD52.ws its WS-DC2 ws its WS-DC2 ws its WS-DC2 ws its WS-DC4.ws its WS-CA2.ws its WS-WA2.ws its WS-HV1.ws.its WS-HV1.ws.its WS-HV1.ws.its WS-HV1.ws.its WS-HV2.ws.its WS-HV3.ws.it	direkte Gruppen: GG-SEC-Server-Monitoring-Admins GG-SEC-Server-Mantioring-Admins GG-SEC-Server-Standard-Admins GG-SEC-Server-MX-Admins GG-SEC-Server-MX-Admins GG-SEC-Server-MX-Admins GG-SEC-Server-MX-Admins GG-SEC-Server-MX-Admins GG-SEC-Server-MX-Admins GG-SEC-Server-MX-Admins GG-SEC-Server-MX-Admins GG-SEC-Server-File-Admins Sicherungs-Operatoren
Server Task Name	Account	Pfad
WS-DC3 ServerSicherung	ws\gMSA-Backup\$	X. In the second s
WS-DC3 .NET Framework NGE	N v4.0.30319 NT-AUTORITÄT\SYST	TEM \Microsoft\Windows\.NET Framework\
WS-DC3 .NET Framework NGE	N v4.0.30319 64 NT-AUTORITÄT\SYST	TEM \Microsoft\Windows\.NET Framework\
WS-DC3 .NET Framework NGE	N v4.0.30319 6 NT-AUTORITÄT\SYST	TEM \Microsoft\Windows\.NET Framework\
WS-DC3 .NET Framework NGE	N v4.0.30319 C NT-AUTORITÄT\SYST	TEM \Microsoft\Windows\.NET Framework\
WS-DC3 AD RMS Rights Policy	Template Mana	\Microsoft\Windows\Active Directory Rights Management Se
WS-DC3 AD RMS Rights Policy	Template Mana	\Microsoft\Windows\Active Directory Rights Management Se
WS-DC3 EDP Policy Manager	NT-AUTORITÄT\Loka	aler Dienst \Microsoft\Windows\AppID\
lese alle Server setze gMSA ein bereit		i

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:

Microsoft Advanced Threat Analytics Versuch der Remoteau	usführung erkannt				Suchen nach Benutzern, Computern, Servern
	Versuch der F	Remoteausführung e	rkannt	WS-DC3" ausoeführt-	Offen :
	• Versuch einer Rem 16:46 21.09:2020	ooteplanung von "Mindestens eine	Remoteausführung	vorbed ausgelant.	
	WS-DC1	KONTEN	ERSTELLT	ERGEBNIS	WS-DC3
	21.09.20 16:46	lubekannt	Unbekannter Task	Unbekannt	WS-DC3 waite

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:



Hyper-V-Manager							
Datei Aktion Ansicht ?							
🗢 🏟 📷 🚺 👔							
Hyper-V-Manager	Vietuelle Computer						
WS-HV1	Virtuelle Computer		1				
WS-HV2.WS.ITS	Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status	Konfiguratio
WS-HV3.WS.ITS	WS-DC3	Wird ausgeführt	1%	4096 MB	00:00:28		9.0
	WS-DC3-alt	Aus					8.0
	WS-FS3	Wird ausgeführt	0 %	1586 MB	27.13:02:49		8.0
	WS-PFS2	Wird ausgeführt	0 %	4096 MB	27.13:03:18		8.0

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

🖳 🏹 📙 🖛 cS				_		×
Datei Start Freigeben Ansicht						~ 🕐
$\leftarrow \rightarrow \checkmark \uparrow \mathbf{P}$ > Netzwerk > ws-dc3 > cS	>	ٽ ~	"c\$" c	durchsuchen		Q
📌 Schnellzugriff	Name	🖻 Freigabe			Größe	
Deckton	Admin	Senden an	>	Iner		
Wether Stanker TO	ATA	Ausschneiden		Iner		
Stephan - 10	Benutzer	Kopieren		Iner		
Dieser PC	DHCP	Varka ünfung anstallan		Iner		
System (C:)	PerfLogs Verknupfung erstellen			Iner		
🛖 Freigaben (M:)	Program Files (x86)	Löschen		Iner		
🐂 Bibliotheken	Programme	Umbenennen		Iner		
🔿 Netzwerk	Windows	Eigenschaften		Iner		
ws-dc3	2020-09-20-DHCPExport-WS-DC3.	cig 20.09.2020 15:34	сго-ра	itei	40	KB
	Microsoft ATA Gateway Setup.zip	20.09.2020 15:00	ZIP-kon	nprimierte	95.157	KB
SYSVOL						
🖭 Systemsteuerung						
Papierkorb						
10 Elemente 4 Elemente ausgewählt						

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:

Image: Services Image: Service	?	(1.0			
Vpdate Services	Nicht zugewiesene Co	omputer (I Computers von I angezeigt, 29 insgesamt)			
> 🛃 Updates	Status: Alle	- 📿 Aktualisieren			
✓ S Computer	① Name		IP-Adresse	Betriebssystem	Prozen
 Alle Computer Nicht zugewiesene Cr Clients Update-Sofont Update-Verzoeger Downstreamserver Synchronisierungen Berichte Optionen 	ws-dc3.ws.its	Gruppenmitgliedschaft für Computer festlegen Wählen Sie die Gruppe aus, denen dieser Co soll. Wenn Sie keine Gruppe auswählen, wird die Gruppe "Nicht zugewiesene Computer" vo Clients Server Update-Sofort Update-Verzoegent	192.168.101.1 X mputer angehören der Computer in erschoben. Abbrechen	Windows (Version 10.0)	

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:

Administrator: C:\Windows\system32\cmd.exe - powershell	-	x
PS C:\> cd "M:\AdminArea\Services\Active Directory\PAM-AdminGUI" PS M:\AdminArea\Services\Active Directory\PAM-AdminGUI> & '.\Setup-PAM&JEA.ps1' PS M:\AdminArea\Services\Active Directory\PAM-AdminGUI> & '.\Setup-PAM&JEA.ps1' -installiere_PAMAdminGUI Der PAMAdminGUI-JEAEndpunkt wurde installiert. PS M:\AdminArea\Services\Active Directory\PAM-AdminGUI> _		^

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:

rhindung Durcheur	hen Ansicht	Ontionen	Hilfsprogramme	2			
Verbinden	men Ansicht	Optionen	rinisprogramme				
Binden	Strg+B						
Trennen	,						
Neu	Street N						
Speichern	Sug+N						
Speichern unter							
Beenden							
bindung mit angegel	enen Server he	erstellen				NUM	
Ldp rbindung Durchsud	hen Ansicht	Optionen	Hilfsprogramme	?	-)
				Verbinden X			
				Port: 636 Ohne Yerbindung			





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:

Administrator: C:\Windows\system32\cmd.exe			-		x	
C:\Windows\SYSVOL\domain\scripts>LAPS.x64.msi			Ê			
C:\Windows\SYSVOL\domain\scripts>						
157 Local Administrator Pa	ssword Solution Setup	×				
Custom Setup Select the way you war	Custom Setup Select the way you want features to be installed.					
Click the icons in the tre	Click the icons in the tree below to change the way features will be installed.					
AdmPw B	d GPO Extension ment Tools Fat client UI PowerShell module GPO Editor templates	Installs management tools. This component does not need to be installed on managed machines. It is meant to be installed on admin or user machines This feature requires 0KB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 237KB on your hard drive.				
		Browse				
Reset	Disk Usage	Back Next Cancel				
					~	

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.