

## <u>Inhalt</u>

Zielsetzung	2
IST-Situation	2
Soll-Situation	2
Migrationsplan	2
Vorbereitung	3
Aufbau der neuen VM	3
Sichtung von Informationen auf dem alten Server	5
aktuelle Konfiguration des Active Directory	10
aktuelle Konfiguration des DHCP	11
aktuelle Konfiguration des DNS	13
Verschiebung des SecEv-Monitors auf WS-MON	15
aktuelle ATA-Konfiguration	20
Prüfung der Gruppenrichtlinien	21
Maintenance	22
Deinstallation	23
Entfernen der Rolle DHCP	23
Entfernen der Rolle Active Directory	26
Troubleshooting nach dem Herabstufen	35
Nacharbeiten im Active Directory	37
Entfernen des Servers	
Bereitstellung des neuen Servers	40
Austausch der VM	40
Betriebssystemvorbereitung	41
Installation der Rolle Active Directory	
Installation der Rolle DNS	64
Installation der Rolle DHCP	65
Nacharbeiten	70
Installation LAPS	70
Adminverzeichnis	71
Datensicherung der GPO	74
Datensicherung LAPS (Script LAPS-History)	75
Datensicherung Windows Server	77
TroubleShooting Monitoring	78
Integration ins ATA	83
PowerShell JEA-PAM-AdminGUI	84
TroubleShooting des Zeitservers	85
TroubleShooting LDAPS	91
Zusammenfassung	93

## <u>Zielsetzung</u>

## IST-Situation

Ich aktualisiere meine gesamte Infrastruktur auf Windows Server 2019. Heute beginne ich mit dem ersten von drei Domain Controllern. Diese stellen die Infrastruktur mit der Active Directory Domain ws.its bereit. Sie arbeiten zusätzlich als DNS-Server und als DHCP-Server.

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



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

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

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

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

### Soll-Situation

Alle Domain Controller sollen mit Windows Server 2019 laufen. Die aktuelle Konfiguration hat sich bestens bewährt. Daher möchte ich am Modell meines Active Directory nichts verändern.

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. Mal ehrlich: wo geben wir überall die speziellen IPs der Domain Controller an und wo ist der FQDN hinterlegt?

### **Migrationsplan**

Ein Inplace-Upgrade schließe ich aus. Da gibt es einfach zu viele Probleme. Daher kommt für das Recycling der Namen und IPs nur ein Wipe & Load infrage. Bei den Domain Controllern WS-DC1 und WS-DC2 sollte eine Verfügbarkeit der Services AD, DNS und DHCP gegeben sein. Während der Migration kann auf die höhere Verfügbarkeit verzichtet werden. Die Umstellung wird während der normalen Betriebszeit durchgeführt.

# <u>Vorbereitung</u>

## Aufbau der neuen VM

Zuerst erstelle ich mir eine neue virtuelle Maschine. Dazu bereite ich meinen Server-Account mit den passenden, temporären Gruppenmitgliedschaften vor:

PAM-AdminGUI -	verbunden mit WS-DC1	Version V1.11)			- 🗆 X
Modus: Zeitraum [min]:	Admins 1440	Gruppen	Ziel-DC: W	'S-DC2 v	zu DC replizieren alle DC replizieren
Admins:		mögliche Gruppen:	Mitglied:		
admin- admin-audit admin-Notfall admin-wac stephan-T1 stephan-T2 sysadm		DHCP-Administratoren Dns.Admins Domänen-Admins GG-Admin-ADJoin GG-Admin-ADJoin GG-Admin-ADJoin GG-Admin-Freigaben GG-Admin-Freigaben GG-Admin-Setup-ApplockerAusnahme-AdminDir 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-Cients-Standard-Admins GG-SEC-Cients-Standard-Admins GG-SEC-Cients-Standard-Admins GG-SEC-Server-M-Admins GG-SEC-Server-M-Admins GG-SEC-Server-MS-Admins GG-SEC-Server-RDS-Admins Organization-Admins Organization Management Schema-Admins	Gültigkeit statisch 2020-06-03 08:02:38 2020-06-03 08:02:39 2020-06-03 08:02:39	Gruppe Protected Users GG-Admin-HyperV-Storage GG-SEC-Server-HyperV-Admins GG-SEC-Server-Standard-Admins	
		hinzufügen	entfernen e	entferne alle	

Die VM selber erstelle ich ohne große Besonderheiten. Der Name entspricht im Hyper-V schon dem der alten VM:

Virtuelle Compu	ıter						
Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status		Konfigurati
🗧 WS-ATA	Wird ausgeführt	1%	6144 MB	7.04:22:56			8.0
WS-CM	Wird ausgeführt	0 %	4096 MB	7.04:15:47			8.0
WS-DC1	Wird ausgeführt	0 %	2160 MB	7.04:11:14			8.0
WS-EVIL1           WS-FS1           WS-MM           WS-MX1           WS-NPS1           WS-PFS1a           WS-Print1           WS-RDS1	Assistent für neue vir	tuelle Compute	er sistenten für neue	virtuelle Com	nputer	×	8.0 8.0 9.0 9.0
	Vorbemerkungen Name und Pfad angeben Generation angeben Speicher zuweisen Netzwerk konfigurieren Virtuelle Festplatte verbin Zusammenfassung	Der Ar Compi Besch Nam Gen Arbe Netz Fest	ssistent für neue virtuelle ( ter wird erstellt: rebung: e: WS-DC1 eration: Generation: tisspeicher: 2048 MB werk: LAN-100 platte: Keine	Computer wurde e	rfolgreich abgeschlossen. Der folgende virtuelle		9.0 8.0
Prüfpunkte	_	Klicker beend	n Sie auf 'Fertig stellen', un en.	n den virtuellen Co	mputer zu erstellen und den Assistenten zu	ne Prü	fpunkte vorhanden.

Damit ich zwischenzeitlich nicht durcheinander komme, benenne ich die neue VM um:

Hyper-V-Manager							
Datei Aktion Ansicht ?							
🗢 🔿 🙍 🖬 👔							
Hyper-V-Manager WS-HV1	Virtuelle Computer						
WS-HV2	Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status	Konfiguratio
WS-HV3	WS-ATA	Wird ausgeführt	1 %	6144 MB	7.04:23:22		8.0
	🗧 WS-CM	Wird ausgeführt	0 %	4096 MB	7.04:16:13		8.0
	WS-DC1	Wird ausgeführt	0 %	2160 MB	7.04:11:37		8.0
	WS-DC1-neu	Aus					9.0
	WS-EVIL1	Gespeichert					8.0
	WS-FS1	Wird ausgeführt	0 %	3176 MB	11.01:21:09		8.0
	🗧 WS-MM	Wird ausgeführt	0 %	994 MB	11.01:17:44		9.0

Jetzt kopiere ich mir meine neue Basefile in das Verzeichnis der VM. Darin ist ein vollwertiger Windows Server 2019 mit grafischer Oberfläche enthalten:

📕   🛃 📕 🖛	Verwalten	Base — 🗆 🗙	🛄 I 📝 🛄 ╤ I WS-DC1
Datei Start Freigeben	Ansicht Datenträgerimagetools	~	2 Datei Start Freigeben Ansicht
← → · ↑ 📙 → Dieser PC	> Tier-Gold (V:) > Base	v Ö "Base" durchsuchen 🔎	← → × ↑ 🕞 > Dieser PC > Tier-Gold (V:) > Hyper-V > WS-DC
📌 Schnellzugriff	Name	Änderungsdatum Typ Größe	★ Schnellzugriff
Desktop	<ul> <li>Win2019-1908.vhdx</li> <li>Win2019-1911-CoreFOD.vhdx</li> </ul>	09.08.2019 20:26 Festplatten-Image 13.733.888 15.11.2019 18:51 Festplatten-Image 12.324.864	Desktop Virtual Hard Disks
🍇 Walther, Stephan - T1 💻 Dieser PC	Win2019-2005.vhdx	01.06.2020 16:44 Festplatten-Image 19.009.536	💰 Walther, Stephan - T1 💻 Dieser PC
🏪 System (C:)			System (C:)
🔜 Daten (D:)		27% abgeschlossen	- 🗆 X
🛖 Freigaben (M:)			(M:)
👝 Tier-Gold (V:)		Ein Element wird von Base nach WS-DC1 kopiert	(V:)
Base		27% abgeschlossen	н х
Hyper-V			
👝 Tier-Silber (W:)		Geschwi	ndigkeit: 1,88 GB/s A
🀂 Bibliotheken			n
i Netzwerk			1
📴 Systemsteuerung		Name: Win2019-2005.vhdx Restdauer: Berechnung	L1
Papierkorb		Verbleibende Elemente: 1 (13,2 GB)	•
		( Weniger Details	и
			K1

Jetzt kann ich die VM fertig konfigurieren. Mehr RAM, mehr CPU und die neue VHDX werden "eingebaut". Zudem passe ich einige Optionen an:

	Einstellungen f ür "WS-DC1-neu" auf "WS	-HV1" — 🗆 X	
	WS-DC1-neu 🗸	€   0	
Hyper-V-Manager WS-HV1 WS-HV2 WS-HV3 WS-HV3 WS-KV1 WS-C1 W	WS-DC1-neu       V         A Hardware       Fardware hinzofigen         Finware       Startenitragsinderungen aussteh         Sicheres Start'ist aktiviert       Sicheres Start'ist aktiviert         Arbeitsspeicher       2048 HB         Image: Start ist aktiviert       Prozessor         4 virtuelle Prozessoren       Image: Start ist aktiviert         Image: Start ist aktiviert       Prozessor         Image: Start ist aktiviert       Prozessoren         Image: St	Festplatte     Festplatte     Festplatte     Festplatte     Festplatte     Festplatte     Festplatte     Festplatte dem virtuelle Festplatte dem virtuellen Computer zugeordnet     orguter nauswählen, wie die virtuelle Festplatte dem virtuellen Computer zugeordnet     orguter nauswählen, wie die virtuelle Festplatte dem virtuellen Computer zugeordnet     orguter nauswählen, wie die virtuelle Festplatte dem virtuellen Computer zugeordnet     orguter nauswählen, wie die virtuelle Festplatte dem virtuellen Computer zugeordnet     orguter setzetzetze          (virdi verwendet)         (virdi Verson Coll virtuelle Austingten Pfad der Datei an.         (virdi Verson Coll virtuelle Austingten Pfad der Datei an.         (virdi Verson Coll virtuelle Austingten Pfad der Datei an.         (virdi Verson Coll virtuelle Austingten Detson virdienet         (virdi Verson Coll virtuelle Austingten Detson virdienet         (virdi Verson Coll virtuelle Austingten Doorsystem.virdien         (virdi Verson Coll virtuelle Austingten Doorsystem.virdien         (virdi Verson Coll virtuelle Austingten Doorsystem.virdien         (virdi Verson Coll virtuelle Austingten Coll virtuellen         (virdi Verson Coll virtuelle Austingten Coll virtuellen         (virdi Verson Coll virtuellen Dissis/PDDo-System.virdix         (virdi Verson Coll virtuellen         (virdi Verson Coll virtuellen         (virdi Verson Coll virtuellen         (virdi Verson Coll virtuellen Coll virtuellen         (virdi Verson Coll virtuellen Coll virtuellen         (virdi Verson Coll virtuellen	<ul> <li>Konfiguratio.</li> <li>8.0</li> <li>8.0</li> <li>9.0</li> <li>8.0</li> <li>9.0</li> <li>9.0</li> <li>9.0</li> <li>9.0</li> <li>9.0</li> <li>8.0</li> <li>9.0</li> <li>8.0</li> <li>9.0</li> <li>8.0</li> <li>9.0</li> <li>8.0</li> <li>9.0</li> <li>8.0</li> <li>9.0</li> <li>8.0</li> <li>9.0</li> <li>9.0</li> <li>8.0</li> <li>9.0</li> <li>9.0</li> <li>8.0</li> <li>9.0</li> <li></li></ul>
WS-DC1-neu			

Abschließend passe ich die Startreihenfolge des UEFI-Boots an:



Die neue VM ist fertig. Aber bevor ich weitermachen kann, muss ich mich um den alten Server kümmern.

#### Sichtung von Informationen auf dem alten Server

Wie bei jeder Migration sollte das alte System genau untersucht werden. Wenn man etwas übersieht, kann das nach dem Abschalten übel ausgehen. Diese Rollen und Features sind noch aktiv. Das alles gehört irgendwie zum Domain Controller:

Display 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
[X] DHCP-Server	DHCP	Installed
[X] DNS-Server	DNS	Installed
[X] .NET Framework 4.6-Funktionen	NET-Framework-45-Fea	Installed
[X] .NET Framework 4.6	NET-Framework-45-Core	Installed
[X] WCE-Dienste	NET-WCE-Services45	Installed
[X] TCP-Portfreigabe	NET-WCE-TCP-PortShar	Installed
[X] Gruppenrichtlinienverwaltung	GPMC	Installed
[X] Remoteserver-Verwaltungstools	RSAT	Installed
[X] Featureverwaltungstools	RSAT-Feature-Tools	Installed
[X] Verwaltungshilfsprogram	ne für die BitLoc RSAT-Feature-Tools-B	Installed
[X] BitLocker-Wiederhers	tellungskennwort RSAT-Feature-Tools-B	Installed
[X] Rollenverwaltungstools	RSAT-Role-Tools	Installed
[X] AD DS- und AD LDS-Tools	RSAT-AD-Tools	Installed
[X] Active Directory-Mod	dul für windows P RSAT-AD-PowerShell	Installed
ÎXÎ AD DS-TOOIS	RSAT-ADDS	Installed
[X] Active Directory	/-Verwaltungscenter RSAT-AD-AdminCenter	Installed
X AD DS-Snap-Ins i	ind -Befehlszeile RSAT-ADDS-Tools	Installed
[X] DHCP-Servertools	RSAT-DHCP	Installed
[X] DNS-Servertools	RSAT-DNS-Server	Installed
[X] Tools für Dateidienste	RSAT-File-Services	Installed
[X] DES-Verwaltungstools	RSAT-DES-Mamt-Con	Installed
[X] Unterstützung für die SMB 1.0/CI	FS-Dateifreigabe FS-SMB1	Installed
[X] Windows Defender-Features	Windows-Defender-Fea	Installed
[X] Windows Defender	Windows-Defender	Installed
[X] GUT für Windows Defender	Windows-Defender-Gui	Installed
[X] Windows PowerShell	PowerShellRoot	Installed
[X] Windows Powershell 5.1	PowerShell	Installed
[X] Windows PowerShell TSE	Powershell_TSE	Installed
[x] Windows Server-Sicherung	Windows-Server-Backup	Installed
[x] wow64-Unterstützung	Wow64_Support	Installed

Der Server hat nur eine sichtbare Partition. Wie bei meinen anderen Servern habe ich hier meine Ablage im Verzeichnis C:\Admin aufgebaut.

#### Praxistipp:

Die Administratoren einer Infrastruktur sollten auf allen Servern eine gleichartige Form der Datenablage aufbauen. So kann man sich einfacher zurechtfinden und auch Migrationen wie diese hier werden vereinfacht.

In diesem Verzeichnis sind einige Scripte und Logfiles vorhanden. Da muss ich vorab aufräumen:

WS IT-Solutions

WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019

I     Image: Imag	t			- 0	× ^ (?
An Schnellzugriff Kopieren Einfügen anhetten Zwischenablage	sschneiden Id kopieren kknüpfung einfügen Verschieben Kopieren nach * nach * Organisieren	Neuer Ordner Neu Neu Offnen Neuer Offnen Offnen Offnen Offnen Offnen Offnen Offnen Offnen Offnen Offnen Offnen	Alles auswählen	n en	
← → · ↑ → Dieser PC → SYS1	TEM (C:) > Admin >			dmin" durchsuchen	P
> 📌 Schnellzugriff	Name	Änderungsdatum Typ	Größe		^
<ul> <li>Administrator</li> <li>Dieser PC</li> <li>SYSTEM (C:)</li> <li>Admin</li> <li>Benutzer</li> <li>PerfLogs</li> <li>Program Files (x86)</li> <li>Programme</li> <li>Windows</li> </ul>	gMSA-Admin GPO GPO-Analyse KABTGT-Reset LAPS-History PAM-AdminGUI PingCastle PSTranscript SceEv-Monitor AdmPwd.adml	13.04.2018 17:01         Dateordner           23.04.2020 14:34         Dateordner           15.11.2018 11:39         Dateordner           11.05.2020 08:13         Dateordner           26.09.2018 06:17         Dateordner           0.60.2018 18:58         Dateordner           0.106.2020 00:00         Dateordner           0.106.2020 00:00         Dateordner           0.206.2020 00:14         Dateordner           0.206.2020 00:14         Dateordner           0.206.2020 00:14         Dateordner           0.206.2020 00:14         Dateordner           2.206.2015 20:15         ADML-Datei	4 KB		
<ul> <li>Treigaben (M:)</li> <li>Bibliotheken</li> <li>Metzwerk</li> <li>Systemsteuerung</li> <li>Papierkorb</li> </ul>	AdmPwd.admx backup.log Check-ADStart.ps1 Check-ADStart.xml dns.log dns1.log MSS-legacy.adm1 MSS-legacy.adm1 MSS-legacy.admx pfirewall.log.old SecGuide.adm1 SecGuide.adm1 SecCuityScope Start.lon	22.06.2015 20:15         ADMX-Datei           02.06.2020 01:20         Textdokument           11.06.2017 16:28         Windows PowerS           20.02.2017 17:24         XML-Dokument           02.06.2020 05:40         Textdokument           25.01.2020 17:46         Textdokument           24.09.2015 04:11         ADMX-Datei           13.10.2017 19:05         Verknüpfung           29.12.2019 18:10         CUD-Datei           27.03.2019 17:56         ADML-Datei           13.10.2017 19:75         ADMX-Datei           13.10.2017 19:75         Verknüpfung           29.12.2019 18:10         CUD-Datei           27.03.2019 17:50         ADML-Datei           13.10.2017 19:75         Verknüpfung           27.03.2019 17:50         ADML-Datei           13.10.2017 19:75         Verknüpfung           27.03.2019 17:40         ADMX-Datei           13.10.2017 18:52         Verknüpfung           26.05.200 04:15         Textdokument	4 KB 1 KB 1 KB 4 KB 0 KB 88.846 KB 17 KB 2 KB 0 KB 0 KB 14 KB 30 KB 2 KB 74 KR		Ŭ

Ich verschiebe etliche Scripte auf mein zentrales Admin-Share auf den Fileservern. Die anderen Scripte verschiebe ich in einen neuen Ordner C:\Admin\Scripte:

Datei Start Freigeben Ansi	rht		- 0	×	Datei Start Freigeben Ansi	cht
An Schnellzugriff Kopieren Einfügen	Verschleben nach * Klöschen •	Neuer Ordner Neu Öffnen	Alles auswählen Nichts auswählen		An Schnellzugriff Kopieren Einfügen	Verschieben nach
← → × ↑ → Dieser PC → SY	(STEM (C:) > Admin	ٽ ٽ ۲	'Admin" durchsuchen	p	← → · ↑ • « Freigaben (M:)	AdminArea > Services > Active Directory >
Schnellzugriff      Desktop     Administrator      Dieser PC     SvSTEM (C:)      Admin     PSTranscript     Scripte     Backup-GPO     Check-ADStart     LAPS-History     SecEv-Monitor     Benutzer     Pendl oze	Name PStranscript Scripte Sectv-Monitor dns.log		Admin durchsizchen Änderungsdatum 02.06.2020 00:00 02.06.2020 00:22 02.06.2020 00:21 02.06.2020 05:40	Typ Dateio Dateio Dateio Textdo	<ul> <li>Schnelizugriff</li> <li>Desktop</li> <li>Administrator</li> <li>Dieser PC</li> <li>SYSTEM (C)</li> <li>Freigaben (Mk)</li> <li>AdminiAreas</li> <li>Geräte</li> <li>Lizenzen</li> <li>Netzwerk</li> <li>Services</li> <li>SMigration-2019</li> <li>Active Directory</li> </ul>	Administed 5 Services 7 Active Directory 5 Name Mane Marka Admin GPO KRBTGT-Reset PAM-AdminGUI PringCastle SecurityScope 2016-03-25 Set-ADComputers NoMonitor.ps1 2016-03-25 enable Kecheros-Delegation.ps1 2016-03-28 Win2015ServiceDirable.reg 2017-03-28 Win2015ServiceDirable.rml 2017-04-05 Win2015ServiceDirable.rml 2017-04-05 gMSA-Monter (rm VS-RDS1 ps1
Program Files (x86) Programme Windows Freigaben (M:)					GPO KRBTGT-Reset PAM-AdminGUI PingCastle	2017-04-25 gMSA-Backup und SchedTask Serversicherun     2017-05-17 gMSA-Backup und SchedTask Serversicherun     2017-05-22 gMSA-Backup für Copy-CRMDB.ps1     2017-06-11 CodeSigning.docx     2017-06-11 gMSA-ADFS.ps1

Diese lokalen Scripte werden automatisch durch geplante Aufgaben gestartet. Eine davon ist mein SecEv-Monitor:



Aufgabenplanung						- 0	×
Datei Aktion Ansicht ?							
🗢 🔿 🙇 📰 🚺							
Aufgabenplanung (Lokal)	Name		Status	Trigger	Nächste Laufzeit	Letzte Laufze	eit
	Check-ADStart		Bereit	Beim Systemstart - Nach Auslösung alle 5 Minuten für die Dauer von 15 Minuten wiederholen.		26.05.2020 04	4:15:00
	CreateExplorerShe	llUnelevatedTask	Bereit	Bei Aufgabenerstellung oder -modifizierung		24.11.2017 19	9:16:55
	🕒 lpamDhcpProvisi	oning	Bereit	Bei Aufgabenerstellung oder -modifizierung		08.09.2019 16	5:22:06
	IpamDnsProvision	ning	Bereit	Bei Aufgabenerstellung oder -modifizierung		08.09.2019 16	5:22:06
	LAPS-History		Bereit	Jeden Tag um 22:30 Uhr	02.06.2020 22:30:00	26.09.2018 06	5:17:26
	SecEv-Monitor		Wird ausgeführt	Jeden Tag um 13:00 Uhr - Nach Auslösung alle 1 Stunde für die Dauer von 1 Tag wiederholen.	02.06.2020 09:00:00	02.06.2020 08	8:00:02
	ServerSicherung		Bereit	Jeden Tag um 01:00 Uhr	03.06.2020 01:00:00	02.06.2020 0	1:00:01
	G Sicherung-GPO		Bereit	Jeden Tag um 04:45 Uhr	03.06.2020 04:45:00	02.06.2020 04	4:45:01
	<						>
	Allgemein Trigger	Aktionen Bedi	ngungen Einstelli	ungen Verlauf			
	Name:	SecEv-Monitor					
	Speicherort:	١					
	Autor:	WS\sysadm					
	Beschreibung:						
	Sicherheitsoptione	n					
	Beim Ausführen d	er Aufgaben folg	endes Benutzerkon	to verwenden:			
	WS\gMSA-Monit	or\$					
	<ul> <li>Nur ausführen</li> </ul>	, wenn der Benut:	zer angemeldet ist				
	💿 Unabhängig v	on der Benutzerar	nmeldung ausführe	n			
	Kennwort	nicht speichern. D	)ie Aufgabe greift r	ur auf lokale Ressourcen zu.			
	Mit höchsten	Berechtigungen a	usführen				
	Ausgeblendet	Konfigurieren f	ür: Windows® 7,	Windows Server™ 2008 R2			$\sim$
< >		,					

SecEv ist dabei meine Abkürzung für SecurityEvent. Das Script analysiert die Sicherheits-Eventlogs aller Domain Controller und filtert dabei interessante, sicherheitsrelevante Events heraus. Diese werden protokolliert und analysiert. Bei Bedarf kann das Script Warnmeldungen ausgeben:



Das Script muss ich vom Server exportieren. Das mache ich nach der Datensichtung. An dieser Stelle kann ich aber die vielen Aufgaben als XML-Datei exportieren:

WS IT-Solutions

## WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019

④ Aufgabenplanung								- 0	×
Datei Aktion Ansicht ?									
🗢 🔿 🙍 💽 🚺 🖬									
Aufgabenplanung (Lokal)	Name	Status		Trigger			Nächste Laufzeit	Letzte Laufzei	it
>Aurgabenpianungsbioliot	ufgabenplanungsbibliot ♥ Check-ADStart ♥ Check-ADStart ♥ JapanDhcpProvisi ♥ JapanDhcpProvisi ♥ JapanDhcpProvisi ♥ JapanDhcpProvisi ♥ JapanDhcpProvisi ♥ JapanDhcpProvisi ♥ JapanDhcpProvisi ♥ JapanDhcpProvisi ♥ JapanDhcpProvisi ♥ Secky-Monitor ♥ Secky-Monitor ♥ Sicherung -GPO ↓ Øschen		⊧führt	Beim Systemstart - Nach Auslösung alle 5 Minuten für die D Bei Aufgabenerstellung oder -modifizierung Bei Aufgabenetstellung oder -modifizierung Bei Aufgabenetstellung oder -modifizierung Jeden Tag um 22:30 Uhr Jeden Tag um 3:00 Uhr - Nach Auslösung alle 1 Stunde für Jeden Tag um 04:45 Uhr	iederholen. ederholen.	02.06.2020 22:30:00 02.06.2020 09:00:00 03.06.2020 01:00:00 03.06.2020 04:45:00	26.05.2020 043 24.11.2017 19: 08.09.2019 16: 08.09.2019 16: 26.09.2018 06: 02.06.2020 08: 02.06.2020 01: 02.06.2020 04:	:15:00 :16:55 :22:06 :22:06 :17:26 :00:02 :00:01 :45:01	
⊘ Aufgabenplanung         Datei       Aktion       Ansicht       ?         ⇐ ➡ 2       ๔       👔       👔       🗊									×
Aufgabenplanung (Lokal)	Name Check-ADStart Check-ADSta	<ul> <li>Speichern unter</li> <li>Schnellzugriff</li> <li>Desktop</li> <li>Administrato</li> <li>Desktop</li> <li>Administrato</li> <li>System (C:</li> <li>Admin</li> <li>System (C:</li> <li>Scripte</li> <li>Sectored</li> <li>Benutzer</li> <li>Dateiname:</li> <li>Dateiname:</li> </ul>	> Dir Neuer or :) Cript Monitor XML-	ser PC > SYSTEM (C.) > Admin > v v v v v v v v v v v v v v v v v v	dmin" durchsuchen	X P Typ Dateiord Dateiord Dateiord	Nächste Laufzeit 02.06.2020 22:30:00 03.06.2020 04:45:00 03.06.2020 04:45:00 03.06.2020 04:45:00	Letzte Laufze 26.05.2020 04 24.11.2071 9 08.09.2019 16 08.09.2019 16 26.09.2018 06 02.06.2020 01 02.06.2020 04	iit 4:15:00 1:16:55 5:22:06 5:22:06 5:17:26 1:00:01 1:445:01

Diese Dateien kann ich dann auf dem neuen Server wieder importieren. Das spart viel Zeit:

📙   🛃 🚽 Admin					- 0	×
Datei Start Freigeben Ansicht						~ 🕜
An Schnelizugriff Kopieren Einfügen anhetten	Verschieben Kopieren nach * nach *	Neuer Element •	Eigenschaften	Alles auswäh Nichts ausw Auswahl um	hlen ählen ikehren	
Zwischenablage	Organisieren	Neu	Öffnen	Auswähle	n	
← → → ↑ 🔒 → Dieser PC → SYSTEM (C:) → Admin				5 V	"Admin" durchsuchen	Q
✤ Schnellzugriff	^	Änderungsdat	tum Typ	Größe		
PSTranscript		02.06.2020 00:0	00 Dateiordner			
Administrator		02.06.2020 08:2	22 Dateiordner			
SecEv-Monitor		02.06.2020 08:2	28 Dateiordner			
Check-ADStart.	ml	02.06.2020 08:2	27 XML-Dokument	4 KB		
SYSTEM (C:)		02.06.2020 05:4	40 Textdokument	2.583 KB		
🔄 Admin 🏼 🗁 gMSA-Admin		17.06.2019 18:3	38 Verknüpfung	2 KB		
PSTranscript 🖅 LAPS-History		13.05.2019 11:	35 Verknüpfung	2 KB		
Scripte	nl	02.06.2020 08:2	28 XML-Dokument	4 KB		
Backup-GPO		25.10.2019 13:2	28 Verknüpfung	2 KB		
Check ADStart	ml	02.06.2020 08:2	28 XML-Dokument	5 KB		
Sicherung-GPO	xml	02.06.2020 08:2	28 XML-Dokument	4 KB		

Dann durchsuche ich die lokal installierten Anwendungen. Hier ist ein Microsoft ATA Gateway installiert. Damit kann mein Monitor-Server weitere Analysen durchführen. Auf diesem Server ist das aber nicht mehr erforderlich. Dann sehe ich noch LAPS, mit dem ich die lokalen Adminkennwörter meiner Memberserver und Clients aus der AD-Datenbank auslesen kann. Und ein html-to-pdf-Converter ist vorhanden. Der gehört zu meinem SecEv-Monitor:





Die IP-Konfiguration ist sehr wichtig. Die muss ich später 1:1 übertragen:



Wie bereits erwähnt, ist mein WS-DC1 für mein PAM-Script das Remote-Ziel. Das dazugehörige Script mit den Proxyfunktionen finde ich im Programmverzeichnis:



Der JEA-Endpunkt ist unter C:\Programdata registriert:



Ich kopiere alle Scripte und Aufgaben-Exporte auf meinen Fileserver:

WS IT-Solutions

📙   🛃 🚽   Admin				- 0	×	📙   🛃 📃 🔻   Admin			
Datei Start Freigeben Ansio	ht				^ 🕐	Datei Start Freigeben Ar	isicht		
An Schnellzugriff Kopieren Finfügen	Verschieben nach - X Löschen -	Neuer Eig	Penschaften	Alles auswählen		An Schnellzugriff Kopieren Einfügen	Verschieben nach	X Löschen -	Neuer
anheften	Contraction and the contraction of the contraction	Ordner	•	🔡 Auswahl umkehren		anheften	Nopieren nach	- P Oniberteritien	Ordner •
Zwischenablage	Organisieren	Neu	Öffnen	Auswählen		Zwischenablage	Organis	ieren	Neu Öf
← → ∽ ↑ 📙 > Dieser PC > SY	'STEM (C:) → Admin		~ Ö ~	dmin" durchsuchen	P	← → ~ ↑ 📙 « Active Direct	ory > Migration-2019 >	WS-DC1 → LWC →	Admin ,
🖈 Schnellzugriff	Name	^		Änderungsdatum	Тур	🖈 Schnellzugriff	<ul> <li>Name</li> </ul>	^	Änderungsdatum
Desktop	PSTranscript			02.06.2020 00:00	Dateio	Desktop			Dieser Ordner ist leer.
2 Administrator	Scripte			02.06.2020 08:22	Dateio	2 Administrator			
Dieser PC	Check-ADStart.xml			02.06.2020 08:27	XML-I	Dieser PC			
SVSTEM (C·)	ans.log			02.06.2020 05:40	Textor	2	×		
Admin	- gMax-Admin			14% abgeschlossen			^		
DETransmint	LAPS-History.ml			7.582 Elemente werder	n von Adr	nin nach Admin kopiert			
Contraction Contraction	PAM-AdminGUI			14% abgeschloss	en		¢		
Benutzer	Sicherung-GPO.xml						-		
PerfLogs						Geschwindigkeit: 412 KB/:	-		
Program Files (x86)							-		
Programme				News, encodered			-		
Windows				Restdauer: Ungefähr 2	Minuten				
🛖 Freigaben (M:)				Verbleibende Elemente	: 6.469 (3	5,3 MB)			
Bibliotheken				-					
Netzwerk				O Weniger Details					
Sustemstellerung			l			Migration-2019			

### aktuelle Konfiguration des Active Directory

Der Server stellt einen zentralen Teil meiner Infrastruktur dar. Damit ich bei der Migration ohne Probleme durchkomme, analysiere ich nun mein Active Directory. Der Server WS-DC1 ist aktuell mein Flexible Single Master Operator für alle 5 Rollen:

PS C:\> netdom /query f	smo		
Schemamaster	WS-DC1.WS.its		
Dom,,nennamen-Master	WS-DC1.WS.its		
PDC	WS-DC1.ws.its		
RID-Pool-Manager	WS-DC1.ws.its		
Infrastrukturmaster	WS-DC1.WS.its		
Der Befehl wurde ausgef	hrt.		

Dazu agiert er als IP-Bridgehead-Server. Mit dieser Funktion ist er der primäre Replikationspartner für standortübergreifende Replikationen:

문문 Active Directory-Standorte und -Dienste					- 0	×
Datei Aktion Ansicht ?						
🗢 🔿 🙋 📷 📋 🗶 🖾 🧟 🕞 🛛 🖬 💆						
Active Directory-Standorte und -Dienste [WS-DC1.ws.its	Name	Domäne	Bridgehead	Domänencont	Beschreibung	
V 🔛 Sites	WS-DC1	ws.its	IP	GC		
> Subnets	WS-DC2	ws.its		GC		
🗸 📔 Ergoldsbach						
> EdgeSyncService						
V C Servers						
WS-DC1						
✓ ■ WS-DC2						
> I NTDS Settings						
🗸 🚪 Neufahrn						
✓ <sup>™</sup> Servers						
VS-DC3						

Das bedeutet aber auch, dass dieser Server die Relikation aller Domain Controller ausführt. Wenn er fehlt, dann sind die beiden anderen DCs zumindest für eine Zeit isoliert:





Der Server WS-DC1 ist als PDC-Emulator auch der primäre Zeitserver meiner Infrastruktur. Er selber kann sich seine Zeit von einem öffentlichen NTP-Server holen:



Die Domänenfunktionsebene und die Gesamtstrukturfunktionsebene habe ich bereits auf Windows Server 2016 angehoben. Das Active Directory Schema läuft mit der Version Windows Server 2016. Das sollte für eine Koexistenz mit Windows Server 2019 genügen.

#### aktuelle Konfiguration des DHCP

Der Server WS-DC1 ist ebenfalls als DHCP-Server aktiv. Seine Scopes synchronisiert er mit dem WS-DC2 über ein DHCP-Failover:



🐏 DHCP					_	
Datei Aktion Ansicht ?						
🗢 🌩 🙋 📰 📓 🙆 📑 🗍 🖳 💷						
W	Inhalt des DHCP-Servers Bereich [172.19.120.0] Bereich [172.19.130.0] Bereich [172.19.140.0] Bereich [172.19.150.0] Bereich [192.168.110.0] Bereich [192.168.110.0] Richtlinien Filter	DMZ-extern DMZ-Intern GameZone DMZ-Isolation ] Server-Ergoldsbach ] Clients-Ergoldsba Eigenschaften von IP Allgemein DNS f Sie können alle Faild ist, löschen, bearbeit ws-dc1 ws-dc2 < Failoverstatus Zustand des Server Partnerserver: Modus:	Status ** Aktiv ** Pv4 Filter Failover poverbeziehungen ten sowie den St rs: Normal ws-dc2.ws. Lastenausg	Beschreibung äußere DMZ Clients-Ergoldsbach Erweitert an denen dieser Server b atus der Beziehungen anze Bearbei Lösch	Failoverbezi ws-dc1 ws- ws-dc1 ws- ws-dc1 ws- ws-dc1 ws- ws-dc1 ws- reteiligt eteiligt eteiligt en	ehung -dc2 -dc2 -dc2 -dc2 -dc2 -dc2 -dc2
			0	K Abbrechen	Übernehmen	

Die Konfiguration ist Standard:

DHCP			_	
<ul> <li>DHCP</li> <li>Ws-dc1.ws.its</li> <li>Bereich [172.19.120.0] DMZ-extern</li> <li>Bereich [172.19.130.0] DMZ-Intern</li> <li>Bereich [172.19.140.0] GameZone</li> <li>Bereich [172.19.150.0] DMZ-Isolation</li> <li>Bereich [192.168.100.0] Server-Ergoldsbach</li> <li>Bereich [192.168.110.0] Clients-Ergoldsbach</li> <li>Serveroptionen</li> <li>Richtlinien</li> <li>Filter</li> <li>IPv6</li> </ul>	Inhalt Bei Bei Bei Bei Ser Ric Filt	Failoverbeziehung anzeigen/bearbeiten       ?         Parameter in Verbindung mit der Failoverbeziehung bearbeiten:       Name der Beziehung:       ws.dc1 ws.dc2         Zustand dieses Servers:       Normal       Zustand ändern         Zustand des Partnerservers:       Normal         Zustand des Partnerservers:       Normal         Image: Machnichtenauthentifizierung aktivieren       Gemeingamer geheimer Schlüssel:         Image: Inglervall für Zustands-Switchover:       60 - Minuten         Maximale Clientvorlaufzeit:       1 - Stunden       0 - Minuten	×	ziehung s-dc2 s-dc2 s-dc2 s-dc2 s-dc2 s-dc2
	<	Image: Constructed construction       Image: Construction       I	]	>

Meine PFSense verbindet alle internen Netzwerke miteinander. Sie fungiert daher als DHCP-Relay (IPHelper) und leitet Anfragen an beide DHCP-Server weiter:

COMMUNITY EDITION	✓ Interfaces ✓	Firewall 👻	Services 🗸	VPN 🗸	Status 🕶	Diagnostics 🗸	Help 🗸	€
Services / DHCP	Relay							≆ Ш 🗖 9
DHCP Relay Configu	ration							
Enable	Enable DHCP rela	ay on interface						
Interface(s)	DMZ_120_EXTERN LAN_100_SERVER DMZ_130_INTERN LAN_110_CLIENTS Interfaces without an	N I S n IP address will r	not be shown.		~			
	Append circuit ID If this is checked, the	and agent ID to r e DHCP relay will	requests append the circu	iit ID (pfSens	se interface nu	mber) and the agent	ID to the DHCP re	equest.
Destination server	192.168.100.1 This is the IPv4 addr requests are relayed	ess of the server	to which DHCP	Î	Delete			
	192.168.100.4 This is the IPv4 addr requests are relayed	ess of the server	to which DHCP	Î	Delete			
	192.168.100.2 This is the IPv4 addr requests are relayed	ess of the server	to which DHCP		Delete			

Damit sollte ich die DHCP-Funktion vom alten WS-DC1 herunternehmen können, ohne dass es zum Service-Ausfall kommt.

### aktuelle Konfiguration des DNS

Jeder Domain Controller ist auch als schreibbarer Namensserver unterwegs. Ich sichte nun die lokale Konfiguration des DNS-Services. Der Forwarder ist meine Fritzbox in der äußeren DMZ:

🚊 DNS-Manager		- 🗆 X
Datei Aktion Ansicht ?		
ᆃ 🔶  📷 🖸 🧟 👘		
<ul> <li>DNS</li> <li>WS-DC1</li> <li>Toivard-Lookupzonen</li> <li>Reverse-Lookupzonen</li> <li>Bedingte Weiterleitungen</li> <li>ws-dc2</li> <li>ws-dc3</li> </ul>	Name     Typ     Status       Imsdcs.ws.its     Active Directory-integriert, primär     Wird aus       Idmz.ws.its     Active Directory-integriert, primär     Wird aus       Irds.ws-its.de     Active Directory-integriert, primär     Wird aus       Itop     Active Directory-integriert, primär     Wird aus       Ivs     Active Directory-integriert, primär     Wird aus       Vista     Active Directory-integriert, primär     Wird aus       Valualifizienter     Nonachista     Schristalien       Veterfeitungen handelt es sich	DNSSEC-Status Schlüsselma sgeführt Nicht signiert sgeführt Nicht signiert sgeführt Nicht signiert sgeführt Nicht signiert sgeführt Nicht signiert sgeführt Nicht signiert

WS IT-Solutions

WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019

#### Der Server darf aufräumen:

	Debugprotokollierung Ereignisprotokollierung Überwachen Sicherheit
	Schnittstellen Weiterleitungen Erweitert Stammhinweise
	Serverversionsnummer:
	10.0 14393 (0x3839)
	Serveroptionen:
	Rekursionsvorgang (und Weiterleitungen) deaktivieren  RiND-Sekundärzonen aktivieren
	Beim Laden unzulässiger Zonendaten einen Fehler zurückgeben
	Roundrobin aktivieren
	✓Netzwerkmaskenanforderung aktivieren
	I Cache vor Beschädigungen sichem
	Namensüberprüfung: Multibyte (UTF8) V
	Zonendaten beim Start laden: Von Active Directory und Registrierur V
	Aufräumvorgang bei veralteten Einträgen automatisch aktivieren
	Zeitraum des Aufräumvorgangs: 1 Tage
	Zurücksetzen
	OK Abbrechen Übernehmen Hilfe
>	

Ebenso habe ich das Logging aktiv. So kann ich im Nachgang verdächtige Namensanfragen an die Clients zuweisen:

Schnittstellen       Wetterleitungen       Erweitert       Stammhinweise         Debugprotokollierung       Ereignisprotokollierung       Überwachen       Sicherheit         Sie können die an den DNS-Server empfangenen Pakete protokollierun, ist standardmaßig desktiviert.       Pakete zum Debuggen protokollierun Paketinchtung:       Image and and and a desktiviert.         Ø Pakete zum Debuggen protokollierun Paketinchtung:       Mindestens eine Option auswählen       Transportprotokolli: Ø UDP Beine Option auswählen       Mindestens eine Option auswählen         Ø Ausgehend       Mindestens eine Option auswählen       Ø UDP Ø Akordenung Ø Afrörderung Ø Antwort       Mindestens eine Option auswählen         Ø Lipdates       Mindestens eine Option auswählen       Ø Antwort       Benachrichtigungen         Wettere Optionen:       Ø Artwort       Ø Antwort       eine Option auswählen         Ø Neht überenistimmende eingehende Rückmeldungspakete ortokolleren       Fitem         Pakete nach IP-Adressen filten       Fitem         Protokollatei       O Detais       Max. Größe (Byte):       104857600		Eigenschaften von WS-DC1	? ×	
Debugrotokollierung       Ereignisprotokollierung       Überwachen       Sicherheit         Sie können die an den DNS-Server empfrangenen Pakete protokollierung ist standardmäßig deaktiviert.       Pakete zum Debuggen protokollieren         Pakete zum Debuggen protokollieren       Paketer zum Debuggen protokollieren       Mindestens         Pakete zum Debuggen protokollieren       Paketrichtung:       Mindestens       UDP         Paketer zum Debuggen protokollieren       Paketrichtung:       Mindestens       UDP         Paketrichtung:       Mindestens       UDP       eine Option auswählen       Mindestens         Paketrichtung:       Mindestens       UDP       eine Option auswählen       eine Option auswählen         Paketrigen/       Mindestens       ZArtwort       eine Option auswählen         Updates       waiswählen       Artwort       eine Option auswählen         Benachrichtigungen       Weitere Optionen:       Artwort       eine Option auswählen         Nicht übereinstimmende eingehende Rückmeldungspakete protokollieren       protokollieren       protokollieren         Paketer nach IP-Adressen filter       Filterm       Protokollieren       mas         Max. Größe (Byte):       104857600       filters       Filterm		Schnittstellen Weiterleitungen Erweiter	t Stammhinweise	
Sie können die an den DNS-Server gesendeten bzw. vom DNS-Server empfangenen Pakete protokollieren, um zusätzliche Debugginformationen zu erhalten. Die Debuggrotokollieren Paketichtung:		Debugprotokollierung Ereignisprotokollierung Ü	berwachen Sicherheit	
		Debugprotokolierung       Ereignisprotokolierung       U         Sie können die an den DNS-Server gesendeten bzwempfangenen Pakete protokolieren       muziažizliche         Paketz zum Debugprotokolierung ist standardmäßig       Paketz zum Debugpen protokolierun         Paketz zum Debugpen protokolierung ist standardmäßig       Paketz zum Debugpen protokolieren         Paketz zum Debugpen protokolierung ist standardmäßig       Paketz zum Debugpen protokolierung ist standardmäßig         Paketz zum Debugpen protokolieren       Mindestens       U UDP         Paketzinhalte:       Mindestens       Mindestens         Obertragungen       Mindestens       Pakettypic         Updates       Mindestens       Antwoi         Detraigungen       Mindestens       Antwoi         Weitere Optionen:       Nicht übereinstimmende eingehende Rückmeldu       Paketten ach IP-Adressen fittem         Pakete nach IP-Adressen fittem       Eitem       Patem         Pateigfad und name:       c:\admin\dns.log       Max. Größe (Byte):       104857600	berwachen Sicherheit v. vom DNS-Server Debuginformationen zu g deaktiviert. protokoll: Mindestens eine Option auswählen lerung ht Bindestens eine Option auswählen uswählen	
	>		Time	

Das Eventlogging ist default:

Eigenschaften von WS-DC1 ? ×	
Schnittstellen       Weiterfeltungen       Erwetert       Stammhinweise         Debugprotokollierung       Ereignisprotokollierung       Überwachen       Sicherheit         Im DNS-Ereignisprotokoll werden Fehler, Wamungen und andere Ereignisse, die vom DNS-Server ermittet werden, protokolliert. Die Informationen können zum Analysieren der Serverleistung verwendet werden.       Folgende Ereignisse         Folgende Ereignisse       Nur Fehler         O Nur Fehler       Fehler und Wamungen         @ Alle Ereignisse	

Diese Rolle sollte nicht schwer zu migrieren sein.

#### Verschiebung des SecEv-Monitors auf WS-MON

Dieses Script kann auf meinen Domain Controllern nach fehlerhaften Anmeldungen suchen und mit per Mail darüber berichten. Das Script läuft 24/7 auf meinem WS-DC1. Es würde aber besser auf meinem Monitoring-Server WS-MON platziert sein. Daher verschiebe ich diese Funktion.

Zuerst bereite ich meinen AdminAccount mit meinem PAM-Tool vor, damit ich mich mit dem WS-MON verbinden kann. Zusätzlich muss ich dort noch eine Anwendung installieren. Das würde mein Applocker auch für den Admin verhindern – wenn er nicht in der Whitelist-Gruppe Mitglied ist:

드 PAM-AdminGUI - verb	bunden mit WS-DC1 (	Version V1.11)			-		×
Modus: Zeitraum (min):	Admins	Gruppen	Ziel-DC: W	/S-DC2 ~	zu [ alle	)C replizie	eren
Admins:		mögliche Gruppen:	Mitglied:		une	DC TOPIIZI	
admin admin-audit admin-Notfall admin-setup admin-wac stephan-T1 stephan-T2 sysadm		DHCP-Administratoren Dns.Admins Domänen-Admins GG-Admin-ADJoin GG-Admin-ADJoin GG-Admin-ATA GG-Admin-Backup GG-Admin-Backup GG-Admin-Setu-PoplockerAusnahme-AdminDir GG-Admin-Stup-OplockerAusnahme-AdminDir GG-Admin-Setu-DPM GG-Admin-Setu-DPM GG-Admin-Setu-DPM GG-SEC-Clients-JB-Admins GG-SEC-Clients-VBT-Admins GG-SEC-Clients-VBT-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins Organizations-Admins Organization Management Schema-Admins	Gültigkeit statisch 2020-06-03 08:02:38 2020-06-03 08:02:39 2020-06-03 08:02:39 2020-06-03 08:25:14 2020-06-03 08:55:24	Gruppe Protected Users GG-3dmin-HyperV-Storage GG-SEC-Server-HyperV-Admins GG-SEC-Server-Standard-Admins GG-4dmin-Setup-ApplockerAusnahme GG-SEC-Server-Monitoring-Admins	eueberali		

Ich beende den Task auf dem Server. Das Script ist beim Wiederanlauf so clever und holt auf den Domain Controllern die verpassten Events einfach nach, solange diese nicht durch die Umlaufprotokollierung der Eventlogs gelöscht wurden:



Aufgabenplanung							-		×
Datei Aktion Ansicht ?									
🗢 🔿 🗾 🖬 🖬									
Aufgabenplanung (Lokal)	Name		Status	Tr	igger	Nächste Laufzeit	Letzte	Laufzei	t
	() Check-ADStart		Bereit	Be	eim Systemstart - Nach Auslösung alle 5 Minuten für die Dauer von 15 Minuten wiederholen.		26.05.2	020 04:	15:00
	CreateExplorerShellUnelevated     B IpamDhcpProvisioning     B IpamDnsProvisioning			Be	ei Aufgabenerstellung oder -modifizierung		24.11.2	017 19:	16:55
				Be	ei Aufgabenerstellung oder -modifizierung		08.09.2	019 16:	22:06
				Be	ei Aufgabenerstellung oder -modifizierung		08.09.2	019 16:	22:06
	LAPS-History		Bereit	Je	den Tag um 22:30 Uhr	02.06.2020 22:30:00	26.09.2	018 06:	17:26
	BecEv-Monitor	Ausföhren	führt Je	den Tag um 13:00 Uhr - Nach Auslösung alle 1 Stunde für die Dauer von 1 Tag wiederholen.	02.06.2020 09:00:00	02.06.2	020 08:	00:02	
	BerverSicherung	Austunren		Je	den Tag um 01:00 Uhr	03.06.2020 01:00:00	02.06.2	020 01:	00:01
	④ Sicherung-GPO	Beenden		Je	den Tag um 04:45 Uhr	03.06.2020 04:45:00	02.06.2	020 04:	45:01
		Deaktivieren							
	Exportieren. Keigenschaft		eren						
			n						>
	Allgemein Trigger	Löschen		instellung	jen Verlauf				

Jetzt verschiebe ich das Scriptverzeichnis in meine Zwischenablage. Mein Domain Controller kann den Server WS-MON nicht direkt erreichen:



Da hat sich schon einiges an Dateien angesammelt. Währende der Verschiebung installiere ich auf dem Server WS-MON einen HTML-to-PDF-Converter:



Dann verschiebe ich die Scriptdateien und die alten Logfiles von der Zwischenablage auf den Monitor-Server:





Die exportiere Aufgabe kann ich im Server WS-MON einfach importieren:



Der ausführende Account ist ein Group-Managed-Service-Account. Den kann ich nicht direkt angeben, da ich sein Passwort nicht kenne. Ich verwende stattdessen einen Dummy-Account:



Vom alten DC aus möchte ich nun mit meinem PowerShell-Script gGMSA-Admin den Task auf den gMSA-Account umstellen. Aber meine Rechte reichen nicht aus:

드 gMSA-Admin			- 🗆 X
vorhandene gMSA:		zugehörige Server:	zugehörige Gruppen:
gMSA-Backup (TaskUser für BMR) (gMSA-Monitor (TaskUser für Monitoring) gMSA-SQLDPM (Service SQL auf WS-DPM)		WS-DC1.ws.its WS-MON.ws.its	
erstelle gMSA lösche gMSA bea Einsatz als:	Fehler Der Compu Verbinden aufgetreter "about_Rer	ter WS-MON.ws.its konnte nicht mit WinRM ausgelesen v nit dem Remoteserver "WS-MON.ws.its" ist folgender Fehl : Zugriff verweigert Weitere Informationen finden Sie im H note_Troubleshooting".	
			ОК

Die Ursache ist einfach – wenn auch leider noch sehr unüblich in den meisten Infrastrukturen: meine Domain Admins haben auf den Memberservern und auf den Clients keine (!) Rechte mehr. Die meiste Zeit sind diese auch nicht erforderlich. Aber jetzt benötige ich eine kurze Brücke. Da hilft mir wieder mein Script PAM-AdminGUI. Ich gebe meinem Domain Admin die Adminrechte auf dem Monitoring-Server durch eine zeitlich begrenzte Gruppenmitgliedschaft:



드 PAM-AdminGUI - verb	unden mit WS-DC1 (Version \	V1.11)			-		×
Modus: Zeitraum [min]:	Admins Gr 1440	ruppen V	Ziel-DC: WS	6-DC2 ~	zu [ alle	DC repliz DC repliz	ieren zieren
Admins: admin-audit admin-Nutfall admin-setup admin-wac stephan-T1 stephan-T2 sysadm	mögli DHCF DnsA GG-A GG-A GG-A GG-A GG-A GG-A GG-A GG	che Gruppen: 	Mitglied: Gültigkeit statisch statisch 2020-06-03 09:03:05	Gruppe Domänen-Admins GG-Admin-ADJoin Protected Users GG-SEC-Server-Monitoring-Admins			

Nach einer Neuanmeldung am Domain Controller ist die Gruppenmitgliedschaft aktiv. Jetzt kann ich den gMSA in den Script-Task eintragen:

📟 gMSA-Admin				- 🗆	$\times$
vorhandene gMSA:	zugehörige Ser	ver:	zugehörige Gruppen:		
gMSA-Backup (Task User für BMR) gMSA-Monitor (Task User für Monitorins) gMSA-SQLDPM (Service SQL auf WS-DF	PM)	s (online) Erfolg X		ins ng-Admins ns d-Admins Admins Admins ns h Verschachtelung): wortreplikationsgruppe ns	
		Der Task wurde umgestellt!	LD-SEC-Server-HyperV- LD-SEC-Server-HyperV-	Admins Login	~
erstelle gMSA lösche gMSA Einsatz als: Task V	bearbeite gMSA weiterer Se licke in eine Zeile um die Optionen	ок	SA weitere Gruppe ent	erne Gruppe	
Server	TaskName		Pfad		^
WS-MON P	PrivilegedADUser-Analyse	WS\gMSA-Monitor\$	X		
WS-MON S	ServerMonitor	WS\gMSA-Monitor\$	N		
WS-MON C	Cleanup-PSTranscripts	NT-AUTORITÄT\SYSTEM	N		
WS-MON n	npcapwatchdog	NT-AUTORITÄT\SYSTEM	X		
► WS-MON S	SecEv-Monitor	ws\gMSA-Monitor\$	X		
WS-MON S	ServerSicherung	WS\gMSA-Backup\$	N		
WS-MON S	SnortMonitor	NT-AUTORITÄT\SYSTEM	N		
WS-MON U	Jser_Feed_Synchronization-{A6AB57	WS-MON\sysadm	Λ		~
lese alle Server setze gMSA ein bereit					

Das Script erstellt ein Runtime-Logfile. So kann ich den Laufzeitstatus überprüfen. Ich starte den Script-Task. Der gMSA wird korrekt verwendet und die Events werden analysiert:



🔜   🖸 📑 🖛   SecEv-Monitor		– 🗆 X
Datei Start Freigeben Ansicht		× <b>0</b>
← → × ↑ → Dieser PC → System (C:)	> Admin > SecEv-Monitor	
	A News	RunTime.log - Editor
> 📌 Schnellzugriff	Name	Datei Bearbeiten Format Ansicht Hilfe
∽ 🛄 Desktop	CSV	Benutzername: WS\gMSA-Monitor\$ RunAs-Benutzer: WS\gMSA-Monitor\$
> 🤱 Walther, Stephan - T1	Statistik	Konfigurationsname:
🗸 🛄 Dieser PC	RunTime log	Computer: WS-MON (Microsoft Windows NT 10.0.17763.0)
V 🏪 System (C:)	SecEy-Monitor.ini	Hostanwendung: C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe C:\Admin\SecEv-Monitor'
× Admin	SecEv-Monitor.ps	Prozess-10: 7000 PSVersion: 5.1.17763.1007
PrivilegedADUser-Analyse	SecEv-Monitor.xn	PSEdition: Desktop
		PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17763.1007
		BuildVersion: 10.0.17763.1007
> Secev-Monitor		ULRVerSion: 4.0.30319.42000 WSManStackVersion: 3.0
ServerMonitor		PSRemotingProtocolVersion: 2.3
SnortMon		SerializationVersion: 1.1.0.1
> Benutzer		************
		starte RemoteJobs
> 📙 Program Files (x86)		INFO: WS-0C1 - less Security-Eventing ab 2020-00-02 05:00:05
> Programme		INFO: WS-DC3 - lese Security-Eventlog ab 2020-06-02 09:00:06
> Windows		INFO: WS-DC2 - lese NTLM-Eventlog ab 2020-06-02 09:00:05
> Monitoring (E:)		INFO: WS-DC2 - durchsuche 14 Events
Freigaben (Mt)		INFU: WS-DUZ - 10 moegliche Tretter INFU: WS-DUZ - 10 moegliche Tretter INFU: WS-DUZ - lese NTLM_Eventlog ab 2020-06-02 09:00:06
		INFO: WS-DC3 - keine Events gefunden
> AdminArea	<b>~</b>	INFO: WS-DC1 - lese NTLM-Eventlog ab 2020-06-02 09:00:05
7 Elemente 1 Element ausgewählt (1,67 KB)		INFO: WS-DC1 - durchsuche 1 Events
		INFO: WS-DC1 - 1 moeglicher Treffer
		analysiere und protokolliere das Ergebnis 11 Events werden veranheitet:
		ermittle Zeitgrenzen
		erstelle die Arbeitstabelle
		fuelle die Arbeitstabelle
		speichere Zusammenfassung in Datei 'C:\Admin\SecEv-Monitor\Statistik\Zusammenfassung.csv'
		speichere Details in Datei (:\Admin\Sectv-Monitor\CSV\2020-06-02.csv)
		Statistik veraltet ==> aktualisiere Statistik

Damit ist diese Funktion erfolgreich verschoben.

### aktuelle ATA-Konfiguration

Meine Sicherheitsanalyse stützt sich auch auf einen Microsoft ATA – ein Advanced Threat Analytics System, das Anomalien erkennt und danach alarmieren kann. Dieser Service klinkt sich in alle Domain Controller ein. Dabei kann entweder ein lokaler Agent installiert werden oder man arbeitet mit einer Netzwerk-Traffic-Weiterleitung.

Der Domain Controller WS-DC1 kommt ohne einen Agent aus:

👫 Microsoft Advanced Threat Ana 🗙	+							- 🗆 ×
← → ♂ ☆ 0	https://ata.ws.its/	configuration?tab=gateways				⊘ ☆		III\ 🗊 🚯 💾 🔻 🗏
🜔 DuckDuckGo 🗎 ws.its 🗎 Links 🗎 Kun	nden 🗎 JB 🔘 NPS Serv	rer: A certifica 💮 Open Sourc	e Passwor					
Microsoft Advanced Threat Analy	vtics   Konfiguratio	onen					Q	Microsoft
System							٥	
Center	Gateways							Keine Benachrichtigungen
Gateways								
Updates	Gatewaysetup	Laden Sie dieses Paket heru	inter, um ein Gateway ode	er ein Lightweight-Gate	way zu installieren.			
Datenquellen								
Verzeichnisdienste SIEM	NAME	түр	DOMÄNEN-CONTRO	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 gestartet			
Entitätsmarkierungen Ausnahmen	WS-DC3	Lightweight-Gateway	WS-DC3.ws.its	1.9.7478.57683	Wird ausgeführt			
Benachrichtigungen und Berichte								

Das funktioniert, weil mein Server WS-ATA als virtuelle Maschine auf dem gleichen Hyper-V-Host läuft, wie der virtuelle Server WS-DC1. Dessen Netzwerk-Traffic lasse ich mit Hyper-V-Mitten spiegeln. Das Interface wird als Quelle angezapft:





Das Ziel ist die Netzwerkkarte des Servers WS-ATA. Diese Funktion darf beim neuen DC nicht fehlen. Daher stelle ich sie in seiner Netzwerkkarte mit ein:



Damit ist im ATA keine weitere Aktion erforderlich.

#### Prüfung der Gruppenrichtlinien

Das wird gerne vergessen: Auch die Domain Controller verarbeiten Gruppenrichtlinien. Und diese müssen auf deren Betriebssysteme abgestimmt sein. Ich habe natürlich schon fertige GPO für Windows Server 2019 im Einsatz – aber diese sind noch nicht auf der OU "Domain Controllers" verbunden!



Das habe ich bisher nicht benötigt. Aber der neue Server soll vom ersten Moment an gut abgesichert sein. Daher verbinde ich die drei Gruppenrichtlinien:

📓 Gruppenrichtlinierverwaltung									
🚠 Datei Aktion Ansicht Fenster ?									
🗢 🔿 🙍 📰 📋 🗙 🖾 🧕	? 🖬								
Gruppenrichtlinierverwaltung Domain Controllers									
✓ ▲ Gesamtstruktur: ws.its	V A Gesamtstruktur: ws.its								
🗸 🕌 Domānen	V 🔒 Domänen								
V 🙀 ws.its Verknüpfungsreihenfolge Gruppenrichtlinienobjekt Erzwungen Verknüpfung aktiviert Objektstatus WMI-Filter							WMI-Filter		
🛒 Default Domain Policy			1	GPO-Computer-Sicherheit-DC	Nein	Ja	Benutzerkonfigurations	Keine	
<ul> <li>Domain Controllers</li> </ul>			2	GPO-Computer-Sicherheit-Applocker	Nein	Ja	Benutzerkonfigurations	Keine	
🛒 Default Domain	Gruppenrichtlinienobjekt hie	r erstelle	en und verknüpfen	GPO-Computer-Sicherheit-DeviceGuard	Nein	Ja	Benutzerkonfigurations	Keine	
🛒 GPO-Computer	Vorhandenes Gruppenrichtlin	ienobje	kt verknüpfen	GPO-Computer-Sicherheit-LSAProtection	Nein	Ja	Benutzerkonfigurations	Keine	
GPO-Computer	Vererbung deaktivieren	-		GPO-Computer-Sicherheit-Defender	Nein	Ja	Benutzerkonfigurations	Windows-Server-2016	
GPO-Computer	vereibung deaktivieren			GPO-Computer-Sicherheit-Firewall	Nein	Ja	Benutzerkonfigurations	Keine	
GPO-Computer	Gruppenrichtlinienupdate			GPO-Computer-Sicherheit-Cipher-TLS	Nein	Ja	Benutzerkonfigurations	Keine	
GPO-Computer	Gruppoprichtlinionmodellier		ristant	GPO-Computer-Sicherheit-Basics	Nein	Ja	Benutzerkonfigurations	Keine	
gruppenrichtlinienmodellierungs-Assistent		GPO-Computer-Sicherheit-Netzwerk	Nein	Ja	Reputzerkonfigurations	Keine			

Wichtig ist die Verarbeitungsreihenfolge. Der WMI-Filter sorgt dafür, dass sich die Richtlinien der unterschiedlichen Betriebssysteme nicht in die Quere kommen:



#### **Maintenance**

Mein Monitoring hat einige Sensoren, die mein Active Directory überwachen. Mit der Deinstallation würde es hier einige Alarme geben. Daher pausiere ich die entsprechenden Sensoren:

WS IT-Solutions

## WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019

							Neue Protoko
Startseite	Geräte	Bibliotheken Sen:	soren	Alarme	Maps	Berichte	
Geräte WS-ITS	<ul> <li>Server</li> <li>WS-I</li> </ul>	Gerätemenü					
Gerät WS-DO		Jetzt abfragen					
		Q Details					
🔿 Übersicht	2 Tage	Bearbeiten	>	Systeminformationen	Protokoll	🌣 Einstellungen	🐥 Tri
		Sensor hinzufügen					
		O Automatische Suche	>				
Wenn Sie	e hier Sensortachos sel	Cerätevorlage erstellen		der mehreren Sensoren zu *****	\$\ <b>****</b>		
_		<ul> <li>Jetzt empfehlen</li> </ul>					
		↓ <sup>A</sup> <sub>Z</sub> Alphabetisch sortieren					
		面 Löschen					
		Contraction Klonen					
Pos -	Sensor 🚔	X Verschieben	>	,	Creah	Priorität 🌲	
105. 0		II Pausieren	Ш	Beliebig lang pausieren		i nontat	
<b>4</b> 1.	✓ Base WS-DC1	<ul> <li>Fortsetzen</li> </ul>	Ō	Für 5 Minuten	a mandata a landa a sa landa a sa landa a sa landa a sa	0% ★★★☆☆	
	_	<ul> <li>(Pausiert durch übergeordnetes Objekt</li> </ul>	t) Ō	Für 15 Minuten			_
<b>.</b>	Services AD	riorität/Favorit	Ō	Für 1 Stunde	ces AD	13 # ★★★☆☆	
		🛢 Historische Daten	0	Für 3 Stunden			
<b>4</b> • 3.	V DNS	Geräte-Werkzeuge	0	Fur 1 lag	ortzeit		
<b>-t</b> - 4	Active Directory Re	Q Duplikate finden	0	BIS	Sync Res	0# ***	
	, tour o bir colory no	Link per E-Mail verschicken	49	Einmaliges Zeittenster für wartung			
<b>4</b> 5.	Active Directory Re	Ticket hinzufügen			Last Sync Res	0# ★★★☆☆	
			his 5	von 5 > >>			

## **Deinstallation**

## Entfernen der Rolle DHCP

Jetzt kann der Rückbau des alten Servers starten. Nur so kann ich den Namen und die IP-Adresse freibekommen. Ich statte meinen AdminAccount mit weiteren Rechten aus. Die Mitgliedschaft als Enterprise-Admin und als Schema-Admin wird die Neuinstallation ermöglichen:

드 PAM-AdminGUI - ver	rbunden mit WS-DC1 (	Version V1.11)				_		×
Modus: Zeitraum [min]:	Admins	Gruppen	Ziel-DC: W	/S-DC2	~	zu D alle D	C replizie )C replizi	eren eren
Admins:		mögliche Gruppen:	Mitglied:					
admin admin-audit admin-Vatfall admin-wetup admin-wac stephan-T1 stephan-T2 sysadm		DrsAdmins GG-Admin-ATA GG-Admin-Backup GG-Admin-Backup GG-Admin-Freigaben GG-Admin-Freigaben GG-Admin-HyperV-Storage GG-Admin-MyerV-Storage GG-Admin-Setup-ApplockerAusnahme-AdminDir GG-Admin-Setup-ApplockerAusnahme-ueberal GG-Admin-Setup-ApplockerAusnahme-ueberal GG-Admin-SQL-DPM GG-Admin-SQL-DPM GG-Admin-SQL-DPM GG-SEC-Clients-B-Admins GG-SEC-Clients-B-Admins GG-SEC-Server-File-Admins GG-SEC-Server-File-Admins GG-SEC-Server-File-Admins GG-SEC-Server-File-Admins GG-SEC-Server-File-Admins GG-SEC-Server-File-Admins GG-SEC-Server-RDS-Admins GG-SEC-Server-RDS-Admins GG-SEC-Server-RDS-Admins GG-SEC-Server-RDS-Admins GG-SEC-Server-RDS-Admins GG-SEC-Server-RDS-Admins	Gültigkeit statisch statisch 2020-06-03 09:23:50 2020-06-03 09:23:50 2020-06-03 09:23:50	Gruppe Domänen-Admins GG-Admin-ADJoin Protected Users DHCP-Administratoren Organisations-Admins Schema-Admins				

Nach der Neuanmeldung möchte ich den Server aus dem DHCP-Failover entfernen. Dann übernimmt diese Funktion mein Server WS-DC2:

WS IT-Solutions

WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019

Aber Achtung: Die Meldung besagt, dass ich vom WS-DC1 aus die Entfernung des WS-DC2 einleite! Das ist genau das Gegenteil meines Plans:



Also starte ich den Assistenten vom WS-DC2 aus:





Jetzt ist es richtig. Ich wiederhole die Aktion für jeden einzelnen Scope:



Nach einer Aktualisierung sind alle Scopes des alten Servers entfernt. Nur die Serveroptionen bleiben über:



Jetzt entferne ich noch die Einstellung des DHCP-Failovers:

WS IT-Solutions

WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019

1			
🖞 DHCP		- 0	$\times$
Datei Aktion Ansicht ?			
🗢 🌩 🖄 📰 🖾 🔒 🛛 🖬 🛄 🛱			
Y       DHCP         ✓       Ws-dc1.ws.its         ✓       FPv4         〇       Serveroptionen         ◇       Richtlinien         >       Filter         >       Bereich [172.19.120.0] DMZ-extern         >       Bereich [172.19.130.0] DMZ-lotern         >       Bereich [172.19.130.0] DMZ-lotern         >       Bereich [172.19.130.0] DMZ-lotern         >       Bereich [172.19.130.0] DMZ-lotern         >       Bereich [172.19.10.0] DMZ-lotern         >       Bereich [172.19.10.0] DMZ-lotern         >       Bereich [172.19.10.0] DMZ-lotern         >       Bereich [172.19.10.0] DMZ-lotern         >       Bereich [192.168.110.0] Clients-Ergold         >       Bereich [192.168.110.0] Clients-Ergold         >       Bereich [192.168.110.0] Clients-Ergold         >       Bereich [192.168.110.0] Clients-Ergold         >       Filter         >       Filter         >       Filter         >       Pv6	Inhalt des DHCP-Servers       Status       Beschreiblung         Bereich [172.19.120.0] DMZ-extern       ** Aktiv **       äußere DMZ         Bereich [172.19.130.0] DMZ-Intern       ** Aktiv **       Beschreiblung         Bereich [172.19.130.0] DMZ-Intern       ** Aktiv **       Beschreiblung         Bereich [172.19.130.0] DMZ-Intern       ** Aktiv **       Beschreiblung         Bereich [172.19.130.0] DMZ-Intern       ** Aktiv **       Ergoldsbach         Bereich [Stektmen on IPv4       ? ×       Figleschaften von IPv4         Bereich [Stektmen]       Serving Enveltent       Ergoldsbach         Bereich [Stektmen]       Serving Enveltent       Bescheiten         Bereich [Stektmen]       Serving Enveltent       Bescheiten         Bereich [Stektmen]       Serving Enveltent       Bescheiten         Bereich [Stektmen]       Bescheiten       Bescheiten         Bereich [Stektmen]       Bescheiten       Bescheiten         Filter       Falloverstatus       Bescheiten       Löschen         Zustand des Servers: [Normal       Partnerserver: [ws.dol.1.ws.its]       Modus:       Lastenausgleich         OK       Abbrechen       Übernehmen       Ergoldsbach	Failoverbeziehung	

Der Server ist im Active Directoy autorisiert. Das hebe ich für die bevorstehende Deinstallation auf:

🕎 DHCP			-	×
Datei Aktion Ansio	ht ?			
🗢 🔿 🖄 📆 🗙	🗐 🙆 🛃 🚺 📰 🛄	<u>.</u>		
<b>9</b> DHCP		Name		
v ws-dc1.ws.its	Bindungen hinzufügen/ent	fernen		
😭 Server	Autorisierung aufheben			
ji Richtl > ♥ Filter > ₩ IPv6	Sichern Wiederherstellen			
> 📋 ws-dc2.ws.its	Alle Aufgaben	>		
	Ansicht	>		
	Löschen Aktualisieren Liste exportieren			
	Eigenschaften			
	Hilfe			
	П			
🖞 DHCP			_	×
Datei Aktion Ansi	cht ?			
(+ +) 🖄 📰 🗙	🔲 🗟 🔒 🔽 🧊 🛄	<b>9</b>		
👰 рнср		Name		 _
v ws-dc1.ws.its		₿IPv4		
V D IPv4	otionen	iPv6		
🔯 Richtlin	ien			
> 📝 Filter > 🛼 IPv6		DHCP	×	
>		Â	Wenn Sie die Autorisierung für diesen Server aus dem Verzeichnis entfernen, reagiert der DHCP-Server nicht mehr auf Clientantforderungen. Sind Sie sicher, dass Sie den Vorgang fortsetzen möchten?	
			Ja Nein	

Danach habe ich nur noch einen aktiven DHCP-Server. Mit dem DHCP-Failover ist ein Wechsel so einfach.

#### Entfernen der Rolle Active Directory

Weiter geht es mit dem Active Directory. Hier baue ich temporär eine alternative Replikationstopologie auf. Der Server WS-DC2 soll sich direkt mit WS-DC3 austauschen können:





Die Verbindungen können leicht im Active Directory Sites and Services erstellt werden:









Active Directory-Standorte und -Dienste						_	×
Datei Aktion Ansicht ?							
🗢 🔿   🙇 📰 🖾 🕰 📑   🗕							 
<ul> <li>Active Directory-Standorte und -Dienste [WS-DC1.ws.it</li> <li>Sites</li> <li>Inter-Site Transports</li> <li>IP</li> <li>SMTP</li> <li>Subnets</li> <li>Ergoldsbach</li> <li>EdgeSyncService</li> <li>Servers</li> <li>WS-DC1</li> <li>WS-DC1</li> <li>WS-DC2</li> <li>NTDS Settings</li> <li>Reufahm</li> <li>Servers</li> <li>WS-DC3</li> <li>NTDS Settings</li> </ul>	Name WS-DC1 Active Datei Bu Active C Wähle Usate m (Sie kä Menü <sup>1</sup>	Vom Server WS-DC1 e Directory-Domänencon earbeiten Ansicht lirectory-Domänencontroller n Sie einen Active Directory it Namen oder Standort aus nnen die Liste aktualisieren, Ansicht" den Befehl "Aktual	Vom Standort Ergoldsbach troller suchen Domänencontroller au indem Sie auf "Starte sieren" wählen).	Typ Verbindung 	Beschreibung		
	Suchergebr	isse:					
	Servernar	ne Standort		Domäne			
	📲 WS-D	C3 Neufahrn		ws.its			
	WS-D	2 Ergoldsback	1	ws.its			
	₩ WS-D	C1 Ergoldsback	1	ws.its			
	<				>		
	3 Objekt(e	gefunden					

Danach entferne ich die IP-Bridgehead-Funktion vom Server WS-DC1:

Lotter Aktion:       1         Image: Aktion:       Image: I	Active Directory-Standorte und -Dienste						×
Active Directory-Standorte und -Dienste [WS-DC1.ws.itt]       Name       Domăne       Bridgehead       Domănencont       Beschreibung         ✓       Sites       ✓       Inter-Site Transports       Ø       GC         ✓       Sites       ✓       Sites       GC         ✓       Sites       ✓       GC         ✓       Sites       GC         ✓       EdgeSyncService       ✓         ✓       Servers       ✓       WS-DC1         ✓       Servers       ✓       WS-DC1         ✓       Servers       ✓       WS-DC1         ✓       WS-DC3       ✓       WS-DC1         ✓       NTDS Settings       Omänencontrolletype:       Globaler Kdalog         Domänencontrolletype:       Globaler Kdalog       Beschreibung:         Transporte für de det andotübergrefende Deterviblemtitung:       Server ist ein bevorzugter Bröghende Transporte:         SMTP       ✓       Handingen Server       Findende Transporte:							 
OK Abbrechen Übernehmen Hilfe	<ul> <li>Active Directory-Standorte und -Dienste [WS-DC1.ws.it:</li> <li>Sites</li> <li>Inter-Site Transports</li> <li>P</li> <li>SWDP</li> <li>Subnets</li> <li>Ergoldsbach</li> <li>Ergoldsbach</li> <li>EdgeSyncService</li> <li>WS-DC1</li> <li>WS-DC2</li> <li>Neufahm</li> <li>Servers</li> <li>WS-DC3</li> <li>WS-DC3</li> </ul>	Name Domän WS-DC1 ws.its WS-DC2 ws.its Eigenschaften von WS-I Allgemein Objekt Sick WS-DC1 Computer: Domänen: Domänencontrollertyp: Beschreibung: Transpote für die standortübergreifende Datenübermittlung: SMTP	e DC1 US-DC1 WS-DC1 Ws.its Globaler Katalog Hinzufügen >> <<	Bridgehead IP ? ×	Domänencont GC GC	Beschreibung	

Die Anpassung der Replikation wird ein paar Minuten dauern. Währendessen verschiebe ich die FSMO-Rollen. Da hilft die PowerShell. Der neue Träger wird mein Server WS-DC2:



		_
Administrator: Windows PowerShell ISE	_	$\times$
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe		
2020-06-02 Move-FSMO.ps1* X		
1 Import-Module ActiveDirectory		^
2         Move-ADDirectoryServerOperationMasterRole         -Identity         WS-DC2         -OperationMasterRole         DomainNamingMaster           4         Move-ADDirectoryServerOperationMasterRole         -Identity         WS-DC2         -OperationMasterRole         InfrastructureMaster           5         Move-ADDirectoryServerOperationMasterRole         -Identity         WS-DC2         -OperationMasterRole         InfrastructureMaster           6         Move-ADDirectoryServerOperationMasterRole         -Identity         WS-DC2         -OperationMasterRole         RIDMaster           7         Move-ADDirectoryServerOperationMasterRole         -Identity         WS-DC2         -OperationMasterRole         SchemaMaster           8         Move-ADDirectoryServerOperationMasterRole         -Identity         WS-DC2         -OperationMasterRole         SchemaMaster		
9 netdom /query tsmo		~
PS C:\> Import-Module ActiveDirectory		^
P5 C:\> Move-ADDirectoryserverOperationMasterRole -Identity W5-DC2 -OperationMasterRole DomainNamingMaster		
📓 Betriebsmasterrolle verschieben — 🗆 🗙		
Möchten Sie die Rolle "DomainNamingMaster" zum Server "WS-DC2.ws.its" verschieben?		
Ja Ja, alle <u>N</u> ein Nein, <u>k</u> eine An <u>h</u> alten		

Die Rollen werden live verschoben. Eine Kontrolle bestätigt den neuen Owner:

Administrator: Windows PowerShell ISE	- C	1	×
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe			
2020-06-02 Move-F5MO.ps1* ×			
1 Import-Module ActiveDirectory			^
2       Move-ADDirectoryServerOperationMasterRole -Identity WS-DC2 -OperationMasterRole DomainNamingMaster         4       Move-ADDirectoryServerOperationMasterRole -Identity WS-DC2 -OperationMasterRole InfrastructureMaster         5       Move-ADDirectoryServerOperationMasterRole -Identity WS-DC2 -OperationMasterRole PDEtmulator         6       Move-ADDirectoryServerOperationMasterRole -Identity WS-DC2 -OperationMasterRole RIDMaster         7       Move-ADDirectoryServerOperationMasterRole -Identity WS-DC2 -OperationMasterRole RIDMaster         8       netdom /query fsmo			
<pre>&gt; Import-Module ActiveDirectory</pre>			>
PS C:\> Move-ADDirectoryServerOperationMasterRole -Identity WS-DC2 -OperationMasterRole DomainNamingMaster			
PS C:\> Move-ADDirectoryServerOperationMasterRole -Identity WS-DC2 -OperationMasterRole InfrastructureMaster			
PS C:\> Move-ADDirectoryServerOperationMasterRole -Identity WS-DC2 -OperationMasterRole PDCEmulator			
PS C:\> Move-ADDirectoryServerOperationMasterRole -Identity WS-DC2 -OperationMasterRole RIDMaster			
PS C:\> Move-ADDirectoryServerOperationMasterRole -Identity WS-DC2 -OperationMasterRole SchemaMaster			
PS C:\> netdom /query fsmo Schemanaster WS-DC2.ws.its Dom,nennamen-Master WS-DC2.ws.its PDC WS-DC2.ws.its RID-Pool-Manager WS-DC2.ws.its Infrastrukturmaster WS-DC2.ws.its			

Auch nach einer solchen Aktion sollte man sich einen Kaffee holen. Die DCs benötigen unter Umständen einige Minuten für die Anpassung.

#### Praxistipp:

Der PDC-Emulator ist immer noch der primäre Zeitserver unter den Domain Controllern. Wird dieser für eine längere Zeit auf einen anderen DC verschoben, dann sollte dort auch die NTP-Konfiguration angepasst werden.

Ich verzichte auf eine Zeitkonfiguration. Der neue Server ist in knapp einer Stunde einsatzbereit. Ich starte die Herabstufung des Domain Controllers durch die Deinstallation der Rolle Active Directory:

ᡖ Server-Manager					- 🗆 ×
Server-N	Manager 🕨 Lokale	r Server	-	• 🕄   🚩 Verwalter	Tools Ansicht Hilfe
	_			Rollen und Features hinzufügen	
	EIGENSCHAFTER	4		Rollen und Features entfernen	
Dashboard	Für WS-DC1			Server hinzufügen	AUFGABEN V
Lokaler Server	Computername	WS-DC1	Zuletzt installierte Undate	Servergruppe erstellen	
Alle Server	Domäne	ws.its	Windows Update	Server-Manager-Eigenschaften	on ein verwalteter Dienst f
AD DS			Zuletzt auf Updates geprüft	t Heute um 08:05	
Datei-/Speicherdienste					
TI DHCP	Windows-Firewall	Domäne: Ein	Windows Defender	Echtzeitschutz: Ein	
C DNS	Remoteverwaltung	Aktiviert	Feedback und Diagnose	Einstellungen	
	Remotedesktop	Aktiviert	Verstärkte Sicherheitskonfig	guration für IE Aus	
	NIC-Teamvorgang	Deaktiviert	Zeitzone	(UTC+01:00) Amsterdam, Berlin	n, Bern, Rom, Stockholm, W
	Ethernet	192.168.100.1, IPv6-fähig	Produkt-ID	00377-90011-18116-AA847 (A	ktiviert)



Bei diesem Vorgang hält mich der Server Manager auf. So kann ich das Demoting einleiten:



Das Entfernen eines Domain Controllers ist recht einfach:

ᡖ Konfigurations-Assistent für die	:	×	
Anmeldeinformat	ionen	ZIELSERVE WS-DC1.ws.it	:R ts
Warnungen Neues Administratorkenn Optionen prüfen	Geben Sie die Anmeldeinformationen für diesen Vorgang an. WS\sysadm (aktueller Benutzer)	Ändern	]
Herabstufung Ergebnisse			
	Der Server wird nach dem Herabstufungsvorgang automatisch neu gesta erst nach dem Neustart entfernt werden. Weitere Informationen Entfermung der Apmeldeinformationen	rtet. Rollen sollten	
	< Zurück Weiter > Tiefer	stufen Abbrechen	

ᡖ Konfigurations-Assistent für die	Active Directory-Domänendienste —		×
Warnungen		ZIELSEI WS-DC1.v	RVER vs.its
Anmeldeinformationen Warnungen Neues Administratorkenn Optionen prüfen Herabstufung Ergebnisse	<ul> <li>Der Domänencontroller hostet momentan die folgende(n) Rolle(n):</li> <li>DNS-Server (Domain Name System)</li> <li>Globaler Katalog</li> <li>▲ Die Rollen, die vom Domänencontroller gehostet werden, sind für die Funktion: Active Directory-Domänendienste erforderlich. Wenn Sie den Vorgang fortsetze einige Vorgänge der Active Directory-Domänendienste betroffen sein.</li> <li>✓ Entfernung fortsetzen</li> </ul>	sweise der n, können	
	Weitere Informationen Entfernungsoptionen		
	< Zurück Weiter > Tiefer stufen	Abbreck	hen

WS IT-Solutions

Das Passwort wird für den nach Abschluss wieder aktiven, lokalen Administrator benötigt:

📥 Konfigurations-Assistent für die	-		×		
Neues Administra		ZIELSEF WS-DC1.v	RVER vs.its		
Anmeldeinformationen	Kennwort:	•••••	]		
Warnungen	Kennwort bestätigen:	•••••			
Neues Administratorkenn					
Optionen prüfen					
Herabstufung					
Ergebnisse					
	Weitere Informationen Entfernung des A	dministratorkennworts			
	< Z	urück Weiter > Tiefer s	tufen	Abbrech	ien

Die Aktion lässt sich auch scripten, aber mit ein paar Mausklicks geht es dann doch schneller:

📥 Konfigurations-Assistent für die	Active Directory-Domänendienste	- 🗆 X		
Optionen prüfen		ZIELSERVER WS-DC1.ws.its		
Anmeldeinformationen	Auswahl prüfen:			
Warnungen		🔳 tmp7349.tmp	- Editor	– 🗆 X
Neues Administratorkenn		Datei Bearbeiten	Format Ansicht ?	
Herabstufung Ergebnisse	Entfernt die Active Directory-Domänendienste von diesem Computer.	# # Windows Pow #	werShell-Skript für AD DS	-Bereitstellung
	Nach Abschluss des Vorgangs gehört dieser Server der Domäne "ws.its" an.	Import-Modulo Uninstall-AD -DemoteOpera -Force:\$true	e ADDSDeployment DSDomainController ` tionMasterRole:\$true `	
		<		×
	Diese Einstellungen können in ein Windows PowerShell-Skript exportiert werder um zusätzliche Installationen zu automatisieren. Weitere Informationen Entfernungsoptionen	, Skript anzeigen		
	< Zurück Weiter > Tiefer stu	fen Abbrechen		

VS IT-Solutions

Bevor ich den Prozess starte, leite ich eine Art Active Directory Maintenance ein, indem ich seine DNS-Records aus den DNS-Servern entferne. Der Domain Controller wird üblicherweise über DNS gefunden. Ohne seine Records werden die Clients auf andere DCs gelenkt. Die Records haben eine TTL von 10 Minuten. Diese sollte man dazu noch abwarten. Danach kennt den DC kein Client mehr:

🖾 Administrator: Eingabeaufforderung	-	×
C:\>nltest /dsderegdns:ws-dc1.ws.its Der Befehl wurde ausgeführt.		î
C:\>_		

Hier sieht man das Ergebnis in einem Container im DNS. Da stand bis eben auch der WS-DC2 als Kerberos- und LDAP-Server:

🛓 DNS-Manager					
Datei Aktion Ansicht ?					
🗢 🔿 🔁 📷 🗙 🖾 🍳 🕞 🛙 🖬 🕴	i i				
DNS WS-DC2 > Zwischengespeicherte Lookupvorgänge V Forward-Lookupzonen V J msdcs.ws.its V dc V Sites V Ergoldsbach V tep > tep > tep > domains > gc > gc	Name 	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][88] ws-dc2.ws.its. [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 19:00:00 Static	
> 🛐 dmz.ws.its					

Die Wartezeit nutze ich zur Kontrolle im DNS. Nltest kann nicht alle Records entfernen. Die überzähligen lösche ich manuell:



DNS-Manager					
Datei Aktion Ansicht ?					
2 🖬 🗙 🖻 Q 😖 🛛 🖬	1				
Vischengespeicherte Lookupvorgänge	Name	Turn	Datas	Zaitstampal	
<ul> <li>Forward-Lookupzonen</li> </ul>	Name	тур	Daten	Zeitstempei	
✓ ☐ _msdcs.ws.its	sites				
🗸 🚞 dc	(identisch mit übergeordne	Host (A)	102 168 100 1	01.06.2020.10:00:00	
✓ <sup>™</sup> _sites		Host (A)	192.168.100.2	01.06.2020 15:00:00	
V 📔 Ergoldsbach	(identisch mit übergeordne	Host (A)	192.168.101.1	01.06.2020 18:00:00	
tcp	(deniser nie usergestanen)	11050 (11)	1321100110111	0110012020 10100100	
V Neufahrn					
tcp					
v C domains					
domains db9320e4-a7ef-441a-a232-e0					
🗸 🚞 gc					
✓ iii _sites					
V 📔 Ergoldsbach					
tcp					
V Neutahrn					
tcp					
v <sup>a</sup> pdc					
tcp					
👔 dmz.ws.its					
👔 email.ws-its.de					
rds.ws-its.de					
👔 rdsweb.ws-its.de					
top					
V ws.its					
✓sites					
V C Neufahrn					
tcp					
🚞 _tcp					
_udp					
DomainDnsZones					
> 📫 _sites					
DNS-Manager					
Datei Aktion Ansicht ?					
Datel Aktion Ansient :					
	96				
			1	1	
<ul> <li>→ 2 m × 0 × 0 × 0 × 0 × 0 × 0 × 0 × 0 × 0 ×</li></ul>	Name	Тур	Daten	Zeitstempel	
→     2     Image: Non-State in the state in th	Name	Typ Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark>	Zeitstempel 01.06.2020 15:00:00	
<ul> <li>Autor analytic - Autor anal</li></ul>	Name	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<ul> <li>Autor austria - Autor aut</li></ul>	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<ul> <li>Autority analytic and a state of the state o</li></ul>	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<ul> <li>Action and the second se</li></ul>	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
Autor Allahar Allah	Name Jdap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<ul> <li>Autor Alarkit .</li> <li>Aut</li></ul>	Name _Idap _Idap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<ul> <li>Action analytic i</li> <li>Action analytic i&lt;</li></ul>	Name _ldap _ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
Autor Anarchi Anarc	Name _Idap _Idap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<ul> <li>Autor Anarchi - A</li></ul>	Name _Idap _Idap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
Autor Alarkit . Autor Alarkit . Autor Alarkit . Zwischengespeicherte Lookupvorgänge ^ Zwischengespeicherte Lookupvorgänge ^ Forward-Lookupzonen	Name _Idap _Idap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
Autor Alarchi Alarc	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
Action analytic is a second	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
Action Analytic 1 Action Analytic 1<	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
Autor Analytic .          Image: Autor Analytic .         Image: Autor Analyt	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<pre>&gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; S Zwischengespeicherte Lookupvorgänge / &gt; S Zwischengespeicherte Lookupvorgängespeicherte / &gt; S Zwischengespeicherte Lookupvorgängespeicherte / &gt; S Zwischengespeicherte Lookupvorgängespeicherte Lookupvorgängespeicherte Lookupvorgängespeicherte / &gt; S Zwischengespeicherte / &gt; S Zwischengespeicherte / &gt; S Zwischengespeicherte / &gt; S Zwischengespeicherte / </pre>	Name _Idap _Idap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
Autor Analytic Ana	Name _Idap _Idap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
Autor Alarkit . Zwischengespeicherte Lookupvorgänge ^ Forward-Lookupzonen Siles Ltcp Siles Ltcp Siles Siles Ltcp Siles Siles Ltcp Siles Siles Siles Ltcp Siles Siles<	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
Autor Analytic 1 Forward-Lookupzonen Forward-Lookupz	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
Action Analytic 1 Action Analytic 1<	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
Actor Analytic 1 Forward-Lookupzonen Forward-Lookupz	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
Autor Analytic 1 Forward-Lookupzonen	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
Autor Analytic 1 Autor Analytic 1 Autor Alarchic 1 Zwischengespeicherte Lookupvorgänge ^ Zwischengespeicherte Lookupvorgänge ^ Forward-Lookupzonen Imades.ws.its Imades.ws.its.de Imades.ws.its.de Imades.ws.its.de Imades.ws.its.de Imades.ws.its.de Imades.ws.its.de Imades.ws.its.de Imades.ws.its.de	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] <mark>ws-dc1.ws.its.</mark> [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<pre>&gt; Aktor Alarkit . &gt; Aktor Alarkit . &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; Source Forward-Lookupzonen &gt; Source</pre>	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] ws-dc1.ws.its. [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<pre>&gt; Aktor Alarkit .</pre>	Name ldap ldap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] ws-dc1.ws.its. [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<pre>&gt; Actor analytic</pre>	Name Jdap Jdap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] ws-dc1.ws.its. [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<pre>&gt;def Pakton Paintin</pre>	Name Jdap Jdap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] ws-dc1.ws.its. [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<pre>&gt;dec Pactor Particle 1 &gt; dec Pactor Particle 1 &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; dc &gt; forward-Lookupzonen &gt; dc &gt; forward-Lookupzonen &gt; dc &gt; forward-Lookupzonen &gt; forwa</pre>	Name Jdap Jdap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] ws-dc1.ws.its. [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<pre>&gt; Actor analytic : &gt; Actor analytic : &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Swischengespeicherte Lookupvorgänge &gt; Swischengespeicherte</pre>	Name Jdap Jdap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] ws-dc1.ws.its. [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<pre>&gt; Aktor Alarkit : &gt; Aktor Alarkit : &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; Swischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; Swischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; Swischengespeicherte Lookupvorgänge ^ &gt; Swischengespeicherte Lookupvorgänge &gt; Swischengespeicherete Lookupvorgänge &gt; Swischengespeicherte Lookupvorgäng</pre>	Name Jdap Jdap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] ws-dc1.ws.its. [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<pre>&gt; Aktor Alarkit : &gt; Aktor Alarkit : &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; Swischwisse &gt; Itep &gt; Meufahrn </pre>	Name Jdap Jdap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] ws-dc1.ws.its. [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<pre>&gt;det = Aktor = Alarche : . &gt; det = Aktor = Alarche : . &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt;</pre>	Name Jdap Jdap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] ws-dc1.ws.its. [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<pre>&gt;def Pakton Alarkit . &gt; 2 Auton Alarkit . &gt; 2 Zwischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; 3 Zwischengespeicherte Lookupvorgänge ^ &gt; 6 Forward-Lookupzonen &gt; 3 Zwischengespeicherte Lookupvorgänge ^ &gt; 6 Forward-Lookupzonen &gt; 6 Lookupzonen &gt; 1 Ergoldsbach 1 Ctp &gt; 1 domains &gt; 1 dob320e4-a7ef-441a-a232-e0 1 Ctp &gt; 1 ctp 2 Jtp 2 dob320e4-a7ef-441a-a232-e0 1 Ctp &gt; 1 dob320e4-a7ef-441a-a232-e0 1 Ctp &gt; 1 ctp 2 Jtp &gt; 1 dob320e4-a7ef-441a-a232-e0 1 Ctp &gt; 1 ctp &gt; 2 Meufahrn 1 ctp &gt; 2 Meufahrn 1 ctp &gt; 2 Meufahrn 1 ctp 2 Jtp &gt; 2 Meufahrn 1 ctp 2 Jup &gt; 2 Neufahrn 1 ctp 2 Jup &gt; 2 Neufahrn 1 ctp 2 Jup &gt; 2 DomainDnsZones &gt; 1 Jup &gt; 1 dob &gt; 2 Jup &gt; 2 DomainDnsZones &gt; 1 Jup &gt; 2 Jup</pre>	Name Jdap Jdap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] ws-dc1.ws.its. [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<pre>&gt;def Pactor Paristric : &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; Swischerter Lookupvorgänge ^ &gt; Swischerter Lookupvorgänge ^</pre>	Name Jdap Jdap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] ws-dc1.ws.its. [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	
<pre>&gt; Aktor Alarkit : &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Zwischengespeicherte Lookupvorgänge ^ &gt; Swischengespeicherte Lookupvorgänge ^ &gt; Forward-Lookupzonen &gt; Swischengespeicherte Lookupvorgänge ^ &gt; Swischengespeicherte Lookupvorgängespeicherte Looku</pre>	Name Jdap Jdap	Typ Dienstidentifizierung (SR Dienstidentifizierung (SR	Daten [0][100][389] ws-dc1.ws.its. [0][100][389] ws-dc2.ws.its.	Zeitstempel 01.06.2020 15:00:00 01.06.2020 19:00:00	

Das Entfernen des Domain Controllers läuft fehlerfrei. Anschließend startet der Server als Memberserver neu.

#### Troubleshooting nach dem Herabstufen

Aber jetzt habe ich ein Problem. Ich kann auf keinen meiner Server mehr zugreifen. Mein Remoting-Tool zeigt dieses Fenster für jeden Server:



Das kann eigentlich nur an der Namensauflösung liegen. Diese teste ich am Client:



Die Ursache ist einfach – wenn zugleich auch fatal: Der Server WS-DC1 ist für etwa die Hälfte meiner Clients und Server der primäre DNS-Server gewesen. Zusätzlich habe ich in meiner Infrastruktur alle anderen Namensauflösungs-Methoden (NBNS, LLMNR) deaktiviert. Eigentlich sollten jetzt alle Systeme den einsatzbereiten WS-DC2 für die DNS-Namensauflösung verwenden:



Aber ein DNS-Client mit mehreren konfigurierten DNS-Servern hat eine feste Arbeitsweise:

- 1. Alle DNS-Server werden gemäß ihrer konfigurierten Reihenfolge kontaktiert.
- 2. Reagiert ein DNS-Server nicht auf eine Anfrage, dann wird er aus der Liste temporär entfernt und der Client befragt den nächsten Server der Liste. Der Timeout eines DNS-Servers liegt dabei bei etwa 20 Sekunden.
- 3. Sind alle DNS-Server der Liste temporär entfernt, dann schlägt die DNS-Anfrage fehl.

Aber der WS-DC1 ist doch kein DNS-Server mehr und so sollten doch alle Systeme den funktionalen Server WS-DC2 befragen. Oder? Eben nicht: der Server WS-DC1 ist immer noch ein DNS-Server. Nur hat er eben keinen Zugriff mehr auf die Active Direcory integrierten Zonen! Er bekommt also eine Anfrage für z.B. ws-hv1.ws.its, hat aber keine Zone, in welcher er nachsehen könnte. Also antwortet er mit "non existent". Und genau das ist mein Problem: **er antwortet**! Damit ist er als DNS-Server vom Client bestätigt. Warum sollte der Client also einen sekundären DNS-Server konaktieren? Nur, weil ihm die Antwort nicht gefällt?

Jetzt habe ich mehrere Optionen:

**NS IT-Solutions** 

- 1. Ich muss mich mit dem Server WS-DC1 verbinden, um den Service DNS zu beenden. Dann kann ich ihn deinstallieren und alles ist gut.
- 2. Ich könnte mich auch mit dem Hyper-V-Host verbinden, die Netzwerkkarte des virtuellen DCs deaktivieren und dann die Rolle DNS über die Konsole deinstallieren.

Eigentlich ist das auch kein Problem. Man verbindet sich einfach mit mstsc und der IPv4-Adresse mit dem Zielserver. Aber auch hier grätscht mir meine sichere Infrastruktur rein: Alle meine administrativen Accounts sind Mitglied der Gruppe "Protected Users". Diese dürfen nur Kerberos für die Authentifizierung verwenden. Und Kerberos kann nur mit dem Namen bei der Verbindung verwendet werden. Die IP-Adresse hat ja keine ServicePrincipalName. Für die IPv4-Verbindung kommt nur NTLM infrage. Dieses Protokoll habe ich aber zusätzlich domänenweit deaktiviert.

Ich kann mich also weder via IPv4 mit dem Server WS-DC1 verbinden, noch kann ich eine Verbindung zum Hyper-V-Host aufbauen. Also bleiben 2 weitere Optionen:

- Ich verwende einen Notfall-Account f
  ür die lokale Anmeldung am Hyper-V-Server und deaktiviere so den alten WS-DC1
- 2. Oder ich verwende die noch offene Verbindung zum WS-DC2.

Ha, die habe ich ganz übersehen. Eigentlich würde das auch keinen Sinn ergeben, da mein Domain Admin auf Memberservern ja eh keine Rechte hat. Aber der "neue" Memberserver WS-DC1 ist in CN=Computers,DC=ws,DC=its gelandet. Da greifen meine Gruppenrichtlinien für das Tiermanagement nicht. Also hat der Server in seiner lokalen Gruppe "Administratoren" die Gruppe "Domain Admins" aufgenommen. Der Default eben. Also kann ich eine Verbindung über die PowerShell aufbauen. Auf dem WS-DC2 funktioniert die Namensauflösung lokal sehr gut, da er ::1 an der ersten Stelle der


DNS-Serverliste verwendet – das ist seine Loopback-IPv6. Die Verbindung kommt also zustande. So kann ich die Rolle DNS deinstallieren:



Nach einigen Cache-Bereinigungen schwenkt mein Client nach etwa 20 Sekunden auf den WS-DC2 für die Namensauflösung. Klar, denn ohne die Rolle DNS kann der Server WS-DC1 nicht länger auf Anfragen reagieren und darauf antworten. Er wird also vom Client verworfen:



Die Aktion hat etwa 5 Minuten Zeit gekostet und einen Teil meiner Infrastruktur gestört. Nach weiteren 5 Minuten war im Monitoring wieder alles grün. Das zeigt, dass man seine Infrastruktur kennen sollte! Und auch ein wenig Hintergrundwissen ist von Vorteil. Probleme können bei Migrationen entstehen. Man muss nur gezielt darauf reagieren können!

### Nacharbeiten im Active Directory

Weiter geht es im Active Directory. Ich muss kontrollieren, ob sich der Server korrekt ausgetragen hat. Dazu kontrolliere ich die Replikationsverbindungen. Der Server WS-DC2 hat den WS-DC1 bereits vergessen:

R Active Directory-Standorte und -Dienste						-		×
Datei Aktion Ansicht ?								
🗢 🔿 🔁 📰 🖾 🐼 🛃								
Active Directory-Standorte und -Dienste [WS-	Name	Vom Server	Vom Standort	Тур	Beschreibung			
V Sites	WS-DC3	WS-DC3	Neufahrn	Verbindung				
Subnets								
V Ergoldsbach								
> 📔 EdgeSyncService								
✓								
WS-DC1								
VS-DC2								
P NTDS Settings								
WS-DC3								
If NTDS Settings								

WS-DC1 hat noch eine Verbindung gespeichert. Diese entferne ich manuell. Damit beschleunige ich den Prozess:

Active Directory-Standorte und -Dienste								-	×
Datei Aktion Ansicht ?									
← →   2   🗙 🖾 🙆 🗟   2									
Active Directory-Standorte und -Dienste [WS-	Name	Vom Serve		Vom Standort	Т	Гур	Beschreibung		
V Sites	WS-DC1	WS-DC1				rbindung			
Inter-Site Transports	WS-DC2	WS-DC2	Ve	rschieben		rbindung			
> Subnets			Jet	zt replizieren					
Elgolosbach			All	e Aufgaben	>				
<ul> <li>Gervers</li> </ul>									
WS-DC1			Lö	schen					
VS-DC2			Un	nbenennen					
📑 NTDS Settings			Eig	jenschaften					
V 📔 Neufahrn			1.0	16 -					
V Servers			HI	те					
WS-DC3									
INTDS Settings									

**NS IT-Solutions** 

Achtung: Das Entfernen habe ich in der Konfigurationspartition vom Server WS-DC2 vorgenommen. Der aktuelle Server kann in der Verbindung oben links im Fenster angezeigt werden. Jetzt muss ich die Veränderung aber noch auf den WS-DC3 replizieren. Natürlich kann ich auch warten. Aber ich will fertig werden:

Active Directory-Standorte und -Dienste							-	-	×
Datei Aktion Ansicht ?									
🗢 🔿 🔁 📰 🖾 😣 🖬 🚨									
Active Directory-Standorte und -Dienste [WS-	Name WS-DC2	Vom WS-	n Server -DC2	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibun	g		
V Servers		Konfigura	ation vom auso	jewählten DC repl	izieren				
✓ ■ WS-DC2		Konfigura	ation auf ausge	wählten DC repliz	ieren				
Provide the settings of the settings of the settings of the setting of the set		Neue Verl Suchen	bindung für di	e Active Directory-	Domänendienste				
✓ Servers ✓ ∰ WS-DC3 ∰ NTDS Settings		Neu Alle Aufg	aben			>			

Im Monitoring werden einige Replikationen als ausgefallen gezeigt. Und auch einer meiner Exchange Server ist noch wegen dem DNS-Problem beleidigt:





Aber insgesamt ist der alte Domain Controller erfolgreich entfernt worden.

### Entfernen des Servers

Ich verschiebe das Computerkonto im Active Directory in eine andere OU:



Aber das war die Falsche. Der Server gehört nachher natürlich in die OU Domain Controllers:





Wenn ich also gleich den neuen Windows Server 2019 in das Active Directory aufnehme, dann wird er von der ersten Sekunde an die Gruppenrichtlinien der Domain Controller verarbeiten.

# Bereitstellung des neuen Servers

## Austausch der VM

Ich schalte die alte VM aus. Dann ändere ich ihren Namen in "WS-DC1-alt". Damit ist der Name "WS-DC1" frei für das neue System:

Hyper-V-Manager							
Datel Aktion Ansicht ?							
Hyper-V-Manager	Virtuelle Computer						
WS-HV2	Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status	Konfiguratio
WS-HV3	🗧 WS-ATA	Wird ausgeführt	0 %	6144 MB	7.06:11:28		8.0
	🖥 WS-CM	Wird ausgeführt	0 %	4096 MB	7.06:04:19		8.0
	WS-DC1	Aus					9.0
	WS-DC1-alt	Aus					8.0
	WS-EVIL1	Gespeichert					8.0
	WS-FS1	Wird ausgeführt	0 %	3330 MB	11.03:09:15		8.0
	🗧 WS-MM	Wird ausgeführt	0 %	994 MB	11.03:05:50		9.0

Den alten Server benötige ich nicht mehr:

• 🔿 🖄 📷 🛛 🖬							
Hyper-V-Manager	Virtuelle Compute	er					
WS-HV2	Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status	Konfigurati
WS-HV3	WS-ATA	Wird ausgeführt	0 %	6144 MB	7.06:12:14		8.0
	🗧 WS-CM	Wird ausgeführt	0 %	4096 MB	7.06:05:06		8.0
	WS-DC1	Wird ausgeführt	12 %	2048 MB	00:00:29		9.0
	WS-DC1-alt	Ане					8.0
	WS-EVIL1	Verbinden					8.0
	WS-FS1	Einstellungen		30 MB	11.03:10:01		8.0
	WS-MM	Konfigurationsversion	ungraden	4 MB	11.03:06:36		9.0
		WS-MX1 Konfigurationsversion u	pyrauenili	336 MB	10.18:22:42		9.0
	WC DEC1	Starten		10 MB	11.02-10-46		5.0
	WS-Print 1	Prüfpunkt		20 MB	11.00:53:37		9.0
	WS-RDS1			30 MB	7.06:13:39		8.0
		Verschieben					
		Exportieren					
		Umbenennen					
		Löschen					
		Replikation aktivieren					



Ebenso lösche ich die alte VHDX-Festplattendatei:

📙   🛃 📕 🖛	Verwalten	Virtual Hard Disks						
Datei Start Freigeben	Ansicht Datenträgerimaget	tools						
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\square$ $\rightarrow$ Dieser PC	← → × ↑ 📙 > Dieser PC > Tier-Gold (V:) > Hyper-V > WS-DC1 > Virtual Hard Disks							
📌 Schnellzugriff	Name	Änderungsdatum	Тур	Größe				
Deckton	HDD0.vh	02.06.2020.00:52	Festplatten-Image	46.731.264				
Walther Stenhan - T1	HDD0-Sy 🞯 Bereitstel	llen	Festplatten-Image	19.009.536				
Dieser PC	Öffnen mi	·+						
System (C:)	Vorgängen	versionen wiederherstellen						
🔜 Daten (D:)	Senden an	· >						
🛖 Freigaben (M:)	Ausschnei	iden						
Tier-Gold (V:)	Kopieren							
Base	Verknünfu	ing erstellen						
Hyper-V	Löschen							
WS-ATA	Umbenenr	nen						
WS-CM	Figenechal	ftan						
WS-DC1	Eigenschaf	nen						
📙 Virtual Hard Disks								
Virtual Machines								

### **Betriebssystemvorbereitung**

Der neue Server kann gestartet werden. Er durchläuft den Einrichtungsprozess:

Hallo			
Lassen Sie uns zunächst einige grundlege	ende Dinge klären.		
Was ist Ihr Heimatland/Ihre Heimatregi	on?		
Deutschland	~	<ul> <li>Image: A second sec second second sec</li></ul>	
Was ist Ihre bevorzugte App-Sprache?			
Deutsch (Deutschland)	~	•	
Deutsch (Deutschland) Welches Tastaturlayout möchten Sie ver	vrwenden?		
Deutsch (Deutschland) Welches Tastaturlayout möchten Sie ver Deutsch	rwenden?	· ·	
Deutsch (Deutschland) Welches Tastaturlayout möchten Sie ver Deutsch	rwenden?	· ·	

Nach wenigen Eingaben kann ich mich anmelden:





Für die Aktivierung trage ich den Produkt Key ein. Die Online-Aktivierung gelingt aber nur im Client-Netzwerk. Daher patche ich den Server fix um:

Einstellungen		– 🗆 X
යි Startseite	Aktivierung	
Einstellung suchen	Windows Edition Windows Server 2019 Datacenter Aktivierung Windows-Aktivierungsserver sind nicht ei	rreichbar
C Windows Update	Weitere Informationen	ellungen für "WS-DC1" auf "WS-HV1" – 🗆 X
曲 Übermittlungsoptimierung	Wenn Sie Probleme mit der Aktivierung haben, w "Problembehandlung" aus, um das Problem mög	Hardware hinzufügen Konfigurieren Sie die Netzwerkkarte, oder entfernen Sie sie. Firmware Von Datei Starten Witzuller Starten
Windows-Sicherheit	Problembehandlung	Sicherist LAN-110,DMZ   Sicherist Statistication of the second statisticat
Problembehandlung	Windows jetzt aktivieren	Avis no     Processor     Mithilfs der VLAN-ID wird das virtuelle LAN angegeben, das von desen virtuelen     4 virtuelle Processoren     Computer für die gesamte Netzwerkkommunikaton über dese Netzwerkkarte     werwende twird
S Wiederherstellung	Wählen Sie "Product Key ändern" aus, um einen r installieren.	Festplate     HODO-System.vhdx     Ind
Aktivierung     Für Entwickler	C Product Key ändern	Bandbreitemerwaltung         Bandbreitemerwaltung           urwaltung         Bandbreitemerwaltung aktivieren           Name         Geben Sie an, wie die Netzwerkbandbreite von diesem Netzwerkadapter werwerde twei. Sowohl "Winder Bandbreite" als auch "Navinala Raundwata"
		Integrationdenste         werden in Megabit pro Sekunde gemessen.         Mathies behade bit.           Alle Dienste verflügbar         Minimale Bandbreite:         0         Mathies           Prüfunkte         Produktion         Maximale Bandbreite:         0         Mathies           Soecherst für die Smart Pagna-D         Maximale Bandbreite:         0         Mathies         Mathies

WS IT-Solutions

# WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019



Damit ist das System dauerhaft aktiviert. Er kann zurück in das abgesicherte Servernetzwerk:

Einstellungen	
<ul> <li>Definition of the state of the</li></ul>	"
Wit     Image: Control of the second s	Identifizierung virtueller LANs aktivieren Mithilfe der VLAN-ID wird das virtuelle LAN angegeben, das von diesem virtuellen Computer für die gesamte Netzwerkkommunikation über diese Netzwerkkarte verwendet wird. 110
₩ Wi     ₩ Wi     ¥     Wi     ¥     Verwaltung	Bandbreitenverwaltung Bandbreitenverwaltung aktivieren
	Geben Sie an, wie die Netzwerkbandbreite von diesem Netzwerkadapter verwendet wird. Sowohl "Minimale Bandbreite" werden in Megabit pro Sekunde gemessen.
Wi Brüfpunkte Produktion Speicherort für die Smart Paging-D	Minimale Bandbreite: U Mbit/s Maximale Bandbreite: 0 Mbit/s Minimale Bandbreite: 0 Mbit/s
V: Hyper-V/WS-DC1 W Automatische Startaktion Immer starten Automatische Stoppaktion Herunterfahren	Verin ken Mindest- oder Maximaiwert gelten sol, geben Sie U an. Klicken Sie auf "Entfernen", um den Netzwerkadapter von diesem virtuellen Computer zu entfernen. Entfernen 105

Hier bekommt er jetzt die statische Konfiguration mit der alten IPv4-Adresse:



👰 Netzwerkverbindungen			_	
$\leftarrow$ $\rightarrow$ $\checkmark$ $\bigstar$ $\blacksquare$ Systemsteuerung > Net	tzwerk und Internet > Netzwerkverbindungen	v" ق	etzwerkverbindung	gen" dur 🔎
Organisieren 🔻 Netzwerkgerät deaktivieren	Verbindung untersuchen Verbindung umbenennen	Status der Verbindung anzeigen »		- 🔳 😮
Ethernet ws.its Microsoft Hyper-V Network Adap Ve Di Ethernet 1 Element ausgewählt	Eigenschaften von Ethernet	Eigenschaften von Internetprotokoll, Version 4 (TCP/IPv4         Allgemein         IP-Einstellungen können automatisch zugewiesen werden, Netzwerk diese Funktion unterstützt. Vienden Sie sich ande Netzwerk denser turg, um die geigeneten IP-Einstellungen         IP-Adresse utomatisch beziehen         IP-Adresse utomatisch beziehen         IP-Adresse:         192. 168. 100.         Subnetzmaske:         255. 255. 255.         Standardgateway:         192. 168. 100.         DNS-Serveradresse automatisch beziehen         IB-Serveradresse automatisch beziehen         IB-Serveradresse automatisch beziehen         IB-Serveradresse automatisch beziehen         IB-Serveradresse automatisch beziehen         IB-Serveradressen verwenden:         Bevorzugter DNS-Server:       192. 168. 100.         Alternativer DNS-Server:       192. 168. 100.         Einstellungen beim Beenden überprüfen	i) X wenn das ernfalls an den zu beziehen.	
		OK	Abbrechen	

Für den Domain Join muss ich einen NTLM-fähigen AdminAccount in eine spezielle Gruppe aufnehmen. Aber mein PAM-Tool kann keine Verbindung zum Domain Controller WS-DC1 herstellen:

📟 PAM-AdminGUI - nicht v	verbunden (Version V1.11)		- 🗆 X
Modus: Zeitraum [min]:	Admins Gruppen	Ziel-DC: [	<ul> <li>zu DC replizieren</li> <li>alle DC replizieren</li> </ul>
Gruppen:	mögliche Admins:	Mitglieder:	
	FEHLER Es konnte kei aufgebaut we	ne Verbindung zum JEA-Endpunkt WS-DC1\PAM-Adn rden!	X ninGUI
			ОК
	hinzufügen	entfernen	entferne alle

Klar, denn den gibt es aktuell nicht. Aber dafür habe ich in der letzten Version eine hochverfügbare JEA-Konfiguration eingebaut. Das Script verbindet sich einfach mit einem anderen DC:



📟 PAM-AdminGUI - ve	rbunden mit WS-DC2 (	Version V1.11)			- 🗆 X
Modus: Zeitraum (min):	Admins	Gruppen	Ziel-DC:		<ul> <li>zu DC replizieren</li> <li>alle DC replizieren</li> </ul>
Admins:	L	mögliche Gruppen:	Mitglied:		
admin admin-audit admin-Notfall admin-wac stephan-T1 stephan-T2 sysadm		DHCP-Administratoren DrsAdmins GG-Admin-Backup GG-Admin-Backup GG-Admin-Freigaben GG-Admin-Freigaben GG-Admin-Fyely-Storage GG-Admin-Kye-V-Storage GG-Admin-Setu-Applocker-Ausnahme-Admin Dir GG-Admin-Setu-Applocker-Ausnahme-ueberall GG-Admin-Setu-Applocker-Ausnahme-ueberall GG-Admin-Setu-Applocker-Ausnahme-ueberall GG-Admin-Setu-Applocker-Ausnahme-ueberall GG-Admin-Setu-Applocker-Ausnahme-ueberall GG-SEC-Clients-JB-Admins GG-SEC-Clients-VBT-Admins GG-SEC-Clients-VBT-Admins GG-SEC-Clients-WBT-Admins GG-SEC-Server-Hile-Admins GG-SEC-Server-Mort-Admins GG-SEC-Server-Mort-Admins GG-SEC-Server-Mort-Admins GG-SEC-Server-Mort-Admins GG-SEC-Server-Mort-Admins GG-SEC-Server-Mort-Admins Organisations-Admins Organisation-Admins Organisation Management Protected Users Schema-Admins	Gültişkeit 2020-06-03 09:07:05 2020-06-03 10:09:45	Gruppe GG-Admin-ATA Domänen-Admins	
bereit		hinzufügen	entfernen e	entferne alle	

Auf dem neuen Server passe ich den Namen an und starte einmal neu. So kann der Server nachher die Identität des alten DCs übernehmen:

🔁 Server-Manager		- D X
<b>E</b> .	Server-Manager • Lokaler Server	🛛 í 🖉 Verwalten Tools Ansicht Hilfe
Dashboard     Lokaler Server     Alle Server     Datei-/Speiche	Systemeigenschafte  Systemeigenschafte  Systemeigenschafte  Subart Concretent Remote  Subart Co	Zuletzt installierte Update       Gestern um 16:05         Nindows Update       Caruf Updates mithile von Mindows Update herunterladen         Andern des Computernamens bzw. der Domäne       Echtzeitschutz: Ein         Breidenungen wich no möglohenveise auf der Zuger       Echtzeitschutz: Ein         Orgutername:       (UTC-01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien         Andern des Computernamens:       (UTC-01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien         Mögled von       Oer Computer muss neu gestartet         Wetter       Wetter         Wetter       Orgutername: vor dem Neustart.         WorkGROUP       OK         OK       Abbrechen

Es folgt der Domain Join:





Der Server ist nach dem Neustart als Domain Member aktiv. Normalerweise würde ich jetzt die Windows Updates nachinstallieren. Das Image ist aber erst einen Tag alt. Der Server ist also Up-to-date. Mit wuauclt initialissiere ich den Kontakt zum WSUS-Server:

WS IT-Solutions

# WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019

Einstellungen		_	×
<ul> <li>ŵ Startseite</li> <li>Einstellung suchen</li> <li>✓</li> <li>✓</li> <li>Windows Update</li> <li>(<sup>th</sup>)</li> <li>(<sup>th</sup>)</li> <li>(<sup>th</sup>)</li> </ul>	Windows Update *Einige Einstellungen werden von Ihrer Organisation verwaltet. Konfigurierte Updaterichtlinien anzeigen Sie sind auf dem neuesten Stand. Letzte Überprüfung: Heute, 10:16 Nach Updates suchen		
	Suchen Sie online nach Updates von Microsoft Update.		
Windows-Sicherheit  Windows PowerShell		_	×
Problembehandl Windows PowerShell Copyright (C) Microsoft	Corporation. Alle Rechte vorbehalten.		^
Wiederherstellun         PS C:\Users\sysadm> wuau           S C:\Users\sysadm> _	clt /reportnow		
⊘ Aktivierung			
🖁 Für Entwickler			
			~

Wuauclt war erfolgreich. Der Server hat sein WSUS-Computerobjekt übernommen:

🐻 Update Services				
📷 Datei Aktion Ansicht Fenster	?			
🗢 🄿 🙍 🖬 🚺 🖬				
by Update Services	Update-Verzoegert	(12 Computers von 12 angezeigt, 29 insgesamt)		
-CC3 (Desktop ()B)	Status: Alle	🗸 📿 Aktualisieren		
🗸 💕 Computer	<ol> <li>Name</li> </ol>	IP-Adresse	Betriebssystem	Prozentsatz "Installiert/Nicht zutreffend" Le
V Ne Computer	ws-ata.ws.its	192.168.100.23	Windows Server 2019 Datacenter	100%
Clients	ws-cm.ws.its	fe80::a86a:6300:131b:a28e%2	Windows Server 2016 Datacenter	100%
v Server	🔺 ws-dc1.ws.its	192.168.100.1	Windows Server 2019 Datacenter	99%
💕 Update-Sofort	ws-dpm.ws.its	192.168.100.5	Windows Server 2019 Datacenter	100%
💕 Update-Verzoeger	ws-fs2.ws.its	192.168.100.12	Windows Server 2019 Datacenter	100%
Downstreamserver	ws-fs3.ws.its	192.168.101.3	Windows (Version 10.0)	100%
Berichte	ws-hv2.ws.its	192.168.100.10	Windows Server 2019 Datacenter	100%
Optionen	ws-hv3.ws.its	192.168.101.2	Windows Server 2019 Datacenter	100%
	<li>ws-mon.ws.its</li>	192.168.100.18	Windows Server 2019 Datacenter	97%
	ws-mx2.ws.its	192.168.100.13	Windows Server 2019 Datacenter	100%
	ws-nps1.ws.its	192.168.100.7	Windows Server 2019 Datacenter	100%
	ws-rds1.ws.its	192.168.110.16	Windows Server 2019 Datacenter	100%

Ich installiere die Rollen und Features für den neuen Domain Controller. Da sind keine Überraschungen dabei:





Ab jetzt würde ich wieder in die gleiche DNS-Problematik reinrutschen wie nach der Entfernung des alten DCs. Daher konfiguriere ich jetzt einen DNS-Forwarder: den WS-DC2. Alle Anfragen werden also an den funktionalen DC weitergeleitet. Die Clients können den WS-DC1 dadurch erfolgreich befragen:





### Installation der Rolle Active Directory

Ich starte die Heraufstufung zu einem Domain Controller im Server Manager:

	🚘 Assistent zum Hinzufügen von R	ollen und Features — 🗌	×	
Dashbo				
Lokaler	Installationsstatus	ZIELSERVE WS-DC1.ws.i	ERits	
Alle Ser				
I AD DS		Installationsstatus anzeigen		
Datei-/		1 Featureinstallation		
DHCP				
DNS		Konfiguration erforderlich.Die Installation auf "WS-DC1.ws.its" war erfolgreich.		
		Active Directory-Domänendienste	^	
		Weitere Schritte sind erforderlich, um den Computer als Domänencontroller festzulegen.		
		DHCD Server		
		DHCP-Server DHCP-Nachinstallations-Assistent starten		
	Bestätigung	DHCP-Konfiguration abschließen		
	Ergebnisse	DNS-Server		
		Gruppenrichtlinienverwaltung		
		Remoteserver-verwaltungstools		
		AD DS- und AD LDS-Tools		
		Active Directory-Modul für Windows PowerShell		1
		AD DS- IOOIS Active Directory-Verwaltungscenter		
		AD DS-Snap-Ins und -Befehlszeilentools	✓ ≥it	•
		Sie können diesen Assistenten schließen, ohne die ausgeführten Aufgaben zu unterbrechen.		
		Zeigen Sie den Aufgabenstatus an, oder öffnen Sie diese Seite erneut, indem Sie auf der		1
		berenisielste auf "Benächrichtigungen" klicken.		



Der Prozess ist recht einfach. Der neue WS-DC1 soll ein weiterer Domain Controller meiner bestehenden Domain werden:

🚡 Konfigurations-Assistent für die	Active Directory-Domänendienste		-		×
Bereitstellungskon	figuration			ZIELSEF WS-DC1.w	VER /s.its
Bereitstellungskonfigurati Domänencontrolleroption Zusätzliche Optionen Pfade Optionen prüfen Voraussetzungsüberprüfu Installation Ergebnisse	Wählen Sie den Bereitstellungsvorgang a © Domänencontroller zu einer vorhand O Neue Domäne zu einer vorhandenen O Neue Gesamtstruktur hinzufügen Geben Sie die Domäneninformationen für Domäne: Geben Sie die Anmeldeinformationen für WS\sysadm (aktueller Benutzer)	us. enen Domäne hinzufügen Gesamtstruktur hinzufügen r diesen Vorgang an. ws.its r diesen Vorgang an.	A	ıswählen	
	Weitere Informationen zu Bereitstellungs	konfigurationen			
	< Zu	rück Weiter >	Installieren	Abbrech	ien

Vom RODC halte ich nicht (mehr) so viel. Das Wiederherstellungspasswort hinterlege ich in meinem Passwortsafe:

ᡖ Konfigurations-Assistent für die	Active Directory-Domänendienste		-		х
Domänencontrolle	eroptionen		W	ZIELSER\ S-DC1.ws	/ER s.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-Wie Kennwort: Kennwort:	dortinformationen angeben ler (RODC) Ergoldsbach v derherstellungsmodus (DSRM-Kennwo	ort) eingel	ben	
	Weitere Informationen zu Domänencont	rolleroptionen			
	< Z0	urück Weiter > Installie	eren /	Abbreche	en

Die Warnmeldung vom DNS kann ignoriert werden. Die DNS-Zone its. gibt es nicht. Also kann ich darin keinen DNS-Server für die Delegierung der Subzone ws.its. bitten:

🚡 Konfigurations-Assistent für die Active Directory-Domänendienste	- 0	×
DNS-Optionen	ZIELSERV WS-DC1.ws	/ER .its
▲ Für den DNS-Server kann keine Delegierung erstellt werden, da die autorisierende überg	geordnete Zone Mehr anzeigen	<
Bereitstellungskonfigurati Domänencontrolleroption DNS-Optionen Zusätzliche Optionen Pfade Optionen prüfen Voraussetzungsüberprüfu Installation Ergebnisse		
Weitere Informationen zur DNS-Delegierung < Zurück Weiter	er > Installieren Abbreche	n

Die Replikation der AD-Objekte starte ich mit meinem WS-DC2 im gleichen Standort:

📥 Konfigurations-Assistent für die	Active Directory-Domänendienste		-		×
Zusätzliche Optio	nen		v	ZIELSEF VS-DC1.w	VER /s.its
Bereitstellungskonfigurati Domänencontrolleroption DNS-Optionen	IFM-Optionen (Install From Media, Vom	Medium installieren) angeben			
Zusätzliche Optionen	Zusatzliche Replikationsoptionen angeb	en			
Vorbereitungsoptionen	Replizieren von:	WS-DC2.ws.its			Ŷ
Optionen prüfen					
Voraussetzungsüberprüfu					
Installation					
Ergebnisse					
	Weitere Informationen zu zusätzlichen C	ptionen			
	< Z0	urück Weiter > Instal	lieren	Abbrech	ien

Die Pfade belasse ich im Default:

WS IT-Solutions

🛓 Konfigurations-Assistent für die	Active Directory-Domänendienste		-		×
Pfade			,	ZIELSEF WS-DC1.v	RVER vs.its
Bereitstellungskonfigurati Domänencontrolleroption	Geben Sie den Speicherort der AD [ an.	DS-Datenbank, der Protokolldateien u	nd den Ort v	on SYSV0	DL
DNS-Optionen	Datenbankordner:	C:\Windows\NTDS			
Zusätzliche Optionen	Ordner für Protokolldateien:	C:\Windows\NTDS			
Pfade	SYSVOL-Ordner:	C:\Windows\SYSVOL			
Vorbereitungsoptionen					
Optionen prüfen					
Voraussetzungsüberprüfu					
Installation					
Ergebnisse					
	Weitere Informationen zu Active Dir	ectory-Pfaden			
		< Zurück Weiter > In	stallieren	Abbreck	nen

Diesen Schritt kann und sollte man auslagern, wenn man eine große und gewachsene Struktur mit vielen Domain Controllern hat. Windows Server 2019 bringt aber kaum Neuerungen mit. Daher gehe ich bei mir das Risiko ein und starte die Aktualisierung auf einem von 2 Domain Controllern:

🚘 Konfigurations-Assistent für die	Active Directory-Domänendienste	-		×
Vorbereitungsopti	ionen		ZIELSEF WS-DC1.w	VER vs.its
Bereitstellungskonfigurati Domänencontrolleroption DNS-Optionen Zusätzliche Optionen Pfade Vorbereitungsoptionen Optionen prüfen Voraussetzungsüberprüfu Installation Ergebnisse	Zum Installieren dieses Domänencontrollers muss der Assistent die folgenden \ • Gesamtstruktur- und Schemavorbereitung • Domänenvorbereitung	/orgār	ıge ausfüh	iren:
	Weitere Informationen zu Vorbereitungsoptionen			
	< Zurück Weiter > Installie	ren	Abbrech	nen

Die Zusammenfassung sieht richtig aus:

WS IT-Solutions

🚡 Konfigurations-Assistent für die A	Active Directory-Domänendienste	-		×
Optionen prüfen		١	ZIELSEI WS-DC1.v	RVER vs.its
Bereitstellungskonfigurati Domänencontrolleroption DNS-Optionen Zusätzliche Optionen Pfade Vorbereitungsoptionen Optionen prüfen Voraussetzungsüberprüfu Installation Ergebnisse	Auswahl prüfen: Konfiguriert diesen Server als zusätzlichen Active Directory-Domänencontroller Domäne "wsits". Standortname: Ergoldsbach Zusätzliche Optionen: Schreibgeschützter Domänencontroller: Nein Globaler Katalog: Ja DNS-Server: Ja DNS-Delegierung aktualisieren: Nein Quelldomänencontroller: WS-DC2.ws.its Diese Einstellungen können in ein Windows PowerShell-Skript exportiert werde um zusätzliche Installationen zu automatisieren.	n, Skri	e ipt anzeig	∽ yen
	< Zurück Weiter > Installie	ren	Abbreck	hen

#### Die Prüfungen sind eher oberflächlich:

WS IT-Solutions



Und dann geht es auch schon los:

	Fortschritt
	Replikation von CN=Schema,CN=Configuration,DC=ws,DC=its: 1999 Objekte von ungefähr 3485 Objekten ompfangen
	Detailliarte Vorgangrangehriste anzeigen
	Detaillette volgangsergebrisse anzeigen
	Sicherheitseinstellung "Mit Windows NT 4.0 kompatible Kryptografiealgorithmen
	zulassen". Durch diese Einstellung wird verhindert, dass beim Herstellen von
onen prüfen	Sicherneitskanaisitzungen schwachere Kryptografiealgorithmen verwendet werden.
ssetzungsüberprüfu	Weitere Informationen zu dieser Einstellung finden Sie im Knowledge Base-Artikel 942564
tion	(http://go.microsofi.com/iwink/scinkid=104731).
bnisse	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 Sekunden startet der Server neu:

WS IT-Solutions



Und mein Domain Controller WS-DC1 ist installiert.

Ich kontrolliere zuerst wieder die AD-Replikation. Der neue Server wird wieder als IP-Bridgehead konfiguriert:

WS IT-Solutions

Active Directory-Standorte und -Dienste							_	×
Datei Aktion Ansicht ?								
Active Directory-Standorte und -Dienste [WS-DC1.]	Name	Vom Server	Vom Standort	Тур		Beschreibung		
Sites		1	n dieser Ansicht w	erden keir	e Elemer	nte angezeigt.		
> 📋 Subnets								
🗸 📙 Ergoldsbach								
> 📔 EdgeSyncService	Eigenschaften von \	WS-DC1		?	×			
V Servers	Allgemein Objekt	Sicherheit Attribut	Editor					
If NTDS Settings	-							
VS-DC2	WS-	DC1						
If NTDS Settings					_			
V Neufahrn	Computer	WS-DC1						
✓	computer.	WS-Del						
📲 NTDS Settings	Domäne:	ws.its						
	Domänencontrollert	typ: Globaler Kat	alog					
	Beschreibung:							
	Transporte für die standortübergreifen	de	Server ist ei Bridgebeads	n bevorzug	ter			
	Datenübermittlung:		folgende Tra	ansporte:				
	IP							
< >>	SMIP	Hinzufüg	en >>					
		<< Entfe	men				_	
	0	K Abbrech	Übernehmen	Hit	e			

Es wurde bereits eine automatische Replikationsverbindung eingerichtet. Ich erstelle aber lieber meine eigenen:

R Active Directory-Standorte und -Dienste							-	×
Datei Aktion Ansicht ?								
🗢 🌩 🛛 🚈 🖾 🖾 🖾 🔤								
Active Directory-Standorte und -Dienste [WS-DC1.	Name		Vom Server	Vom Standort	Typ	Beschreibung		
> 🖆 Inter-Site Transports > 📫 Subnets ✔ 📜 Ergoldsbach	77 Cautomatis	in genener.>	W3-DC2	Ergolusbach	verbindung			
EdgeSyncService     Servere		Neue Verbi	indung für die Act	tive Directory-Domä	nendienste			
✓ I WS-DC1		Suchen						
WS-DC2		Neu				>		
IN Steel In Steel		Alle Aufga	ben			>		
V 📙 Neufahrn		Aktualisier	en					
VI WS-DC3		Liste expor	tieren					
I NTDS Settings		Ansicht				>		
		Symbole a	nordnen			>		
		Am Raster	ausrichten					
		Ligensena	iten					
		Hilfe						

Der Server soll wieder zwischen den beiden anderen Servern vermitteln. Die automatische Verbindung entferne ich:



Real Active Directory-Standorte und -Dienste						-	×
Datei Aktion Ansicht ?							
🗢 🔿 🙋 📰 🖾 🖉 📷 💆							
<ul> <li>Active Directory-Standorte und -Dienste [WS-DC1.//</li> <li>Sites</li> <li>Sites</li> <li>Inter-Site Transports</li> <li>Subnets</li> <li>Ergoldsbach</li> <li>EdgeSyncService</li> <li>Servers</li> <li>WS-DC1</li> <li>WS-DC2</li> <li>NTDS Settings</li> <li>Servers</li> <li>NEMATAR</li> <li>Servers</li> <li>WS-DC3</li> <li>NTDS Settings</li> </ul>	Name ĐWS-DC2 ĐĐWS-DC3	Vom Server WS-DC2 WS-DC3	Vom Standort Ergoldsbach Neufahrn	Typ Verbindung Verbindung	Beschreibung		

Den Vorgang wiederhole ich für jeden Domain Controller:

						-	×
Datei Aktion Ansicht ?							
← ⇒ 2 ☶ 🗙 🖾 Q 🕞 🛛 ☶ 🛛							
Real Active Directory-Standorte und -Dienste [WS-DC1.)	Name	Vom Server	Vom Standort	Тур	Beschreibung		
✓ Sites	🛄 <automatisch ge<="" td=""><td>neriert&gt; WS-DC1</td><td>Ergoldsbach</td><td>Verbindung</td><td></td><td></td><td></td></automatisch>	neriert> WS-DC1	Ergoldsbach	Verbindung			
> Subnets		Verschieben					
🗸 📙 Ergoldsbach		Jetzt replizieren					
EdgeSyncService     Gervers		Alle Aufgaben >					
VS-DC1		Löschen					
₩ NTDS Settings		Umbenennen					
NTDS Settings		Eigenschaften					
V Rufahrn		Hilfe					
✓		,					
MTDS Settings							
Active Directory-Standorte und -Dienste							
· ·						_	×
Datei Aktion Ansicht ?						_	×
Datei Aktion Ansicht ?						_	×
Datei Aktion Ansicht ?	Name	Vom Server	Vom Standort	Тур	Beschreibung	-	×
Datei Aktion Ansicht ? Aktion Ansicht ?	Name WS-DC1	Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung	-	×
Datei Aktion Ansicht ? Aktion Ansicht ? Active Directory-Standorte und -Dienste [WS-DC1., Sites Sites Subnets	Name 111 WS-DC1	Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung	_	×
Datei Aktion Ansicht ? Aktion Ansicht ? Active Directory-Standorte und -Dienste [WS-DC1., Sites Sites Subnets Ergoldsbach	Name 11 WS-DC1	Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung	_	×
Datei Aktion Ansicht ? Aktion Ansicht ? Active Directory-Standorte und -Dienste [WS-DC1./ Sites Subnets Ergoldsbach Ergoldsbach Sentre	Name 101 WS-DC1	Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung	-	×
Datei Aktion Ansicht ? Aktion Ansicht ? Active Directory-Standorte und -Dienste [WS-DC1.v Sites Subnets Ergoldsbach GregeSyncService Conservers Subnets Might Ergoldsbach Subnets Might Ergoldsbach Might Ergoldsb	Name 聊WS-DC1	Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung		×
Datei Aktion Ansicht ? Aktion Ansicht ? Active Directory-Standorte und -Dienste [WS-DC1.v Sites Inter-Site Transports Subnets Ergoldsbach Servers Servers Servers Servers Servers Servers Sites Servers Serv	Name WS-DC1	Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung		×
Datei Aktion Ansicht ? Aktion Ansicht ? Active Directory-Standorte und -Dienste [WS-DC1.v Sites Inter-Site Transports Subnets Ergoldsbach Servers Servers WS-DC1 WS-DC1 WS-DC1 WS-DC1 WS-DC1 WS-DC1 WS-DC2 WS-DC2 WS-DC2 WS-DC2 WS-DC3	Name WS-DC1	Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung		×
Datei Aktion Ansicht ? Aktion Ansicht ? Active Directory-Standorte und -Dienste [WS-DC1.v Sites Subnets Ergoldsbach Servers Server	Name WS-DC1	Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung		×
Datei Aktion Ansicht ? Aktion Ansicht ? Active Directory-Standorte und -Dienste [WS-DC1.v Sites Subnets Ergoldsbach Servers WS-DC1 WS-DC1 WS-DC1 WS-DC1 WS-DC1 WS-DC1 WS-DC2 WS-DC2 WS-DC2 WS-DC2 WS-DC2 WS-DC2 WS-DC2 WS-DC2	Name WS-DC1	Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung		×
Datei Aktion Ansicht ? Aktion Ansicht ? Active Directory-Standorte und -Dienste [WS-DC1.v Sites Subnets Ergoldsbach BedgeSyncService Bervers Bervers WS-DC1 WS-DC1 WS-DC1 WS-DC1 NTDS Settings NTDS Settings Servers Servers Servers Servers WS-DC2 WS-DC2 WS-DC2 WS-DC3 WS-DC3 WS-DC3 WS-DC3 WS-DC3 WS-DC3 WS-DC3	Name	Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung		×
Datei Aktion Ansicht ? Aktion Directory-Standorte und -Dienste [WS-DC1.v Sites Subnets Ergoldsbach Servers Servers WS-DC1 WS-DC1 WS-DC2 WS-DC2 WS-DC2 WS-DC2 WS-DC2 WS-DC3 Servers Servers Servers Servers WS-DC3 WS-DC3 WS-DC3	Name WS-DC1	Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung		×
Datei Aktion Ansicht ?	Name	Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung		×
Datei Aktion Ansicht ?	Name	Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung		×
Datei Aktion Ansicht ?	Name	Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung		×





Jetzt kennt der Server WS-DC1 meinen Replikationsplan. Diesen muss ich noch auf die beiden anderen DCs übertragen:

R Active Directory-Standorte und -Dienste							-	×
Datei Aktion Ansicht ?								
🗢 🌩 🖄 📰 🖾 🧟 🖬 🖉								
<ul> <li>Active Directory-Standorte und -Dienste [WS-DC1.)</li> <li>Sites</li> <li>Inter-Site Transports</li> </ul>	Name		Vom Server WS-DC1	Vom Standort Ergoldsbach	Typ Verbindung	Beschreibung		
> 🧰 Subnets 🗸 🚆 Ergoldsbach								
EdgeSyncService		Konfiguration	vom ausgewählte	n DC replizieren				
✓ ■ Servers		Konfiguration auf ausgewählten DC replizieren						
₩ NTDS Settings WS-DC2		Neue Verbindung für die Active Directory-Domänendienste Suchen						
NTDS Settings Neufahrn Servers		Neu Alle Aufgaber	ı		>			
✓ joervers ✓ j WS-DC3 ﷺ NTDS Settings		Aktualisieren Liste exportier	ren					
		Ansicht			>			
		Symbole anor Am Raster au Eigenschafter	rdnen srichten		>			



Jetzt prüfe ich, ob sich der neue WS-DC1 korrekt im DNS registriert hat. Das geht mit nltest sehr einfach. Aber auch eine Stichprobe im DNS kann nicht schaden:



Fein: Der neue DC kann von den Clients gefunden werden.

WS IT-Solutions

Spätestens jetzt sollten auch die Eventlogs untersucht werden. Gab es Probleme?



🛃 Ereignisanzeige								
Datei Aktion Ansicht ?								
🧼 🔿 📊 🛛 🖬								
Ereignisanzeige (Lokal)	Freignisanzeige (Lok	al)						
> 📑 Benutzerdefinierte Ansichter	i'u tu		r					
> 📫 Windows-Protokolle	Ubersicht und	d Zusami	mentassung					
> 💾 Anwendungs- und Dienstpro	Übersicht							
Abonnements								
	Zusammenfassung	der administ	rativen Ereignisse					
	Ereignistyp	Ereignis	Quelle	Protokoll	Letzte Stu	24 Stunden	7 Tage	
	Kritisch	- 1	-	-	0	0	0	
	E Fehler	-		-	26	52	52	
		28	Kernel-EventTracing	Microsoft	1	1	1	
		69	AppModel-Runtime	Microsoft	4	12	12	
		110	Client-Licensing	Microsoft	0	4	4	
		131	DeviceSetupManager	Microsoft	0	2	2	
		304	User Device Registration	Microsoft	3	3	3	
		307	User Device Registration	Microsoft	3	3	3	
		1002	Dhcp-Client	Microsoft	2	2	2	
		1014	Security-SPP	Anwendu	2	2	2	
		1023	Perflib	Anwendu	1	1	1	
		1046	DHCP-Server	System	1	1	1	
		6104	DFSR	DFS-Repli	1	1	1	
		7023	Service Control Manager	System	0	1	1	
		8193	VSS	Anwendu	1	1	1	
		8198	Security-SPP	Anwendu	3	3	3	
		8200	Security-SPP	Anwendu	2	2	2	
		10000	DistributedCOM	System	2	2	2	
		10010	DistributedCOM	System	0	1	1	
		10317	NDIS	System	0	10	10	
	🖯 Warnung	-	-	-	68	75	75	
		32	Disk	System	6	6	6	
		47	Time-Service	System	1	1	1	
		104	Client-Licensing	Microsoft	0	1	1	
		134	Time-Service	System	4	6	6	
		200	DeviceSetupManager	Microsoft	5	5	5	
		201	DeviceSetupManager	Microsoft	16	16	16	

Das sieht eigentlich ganz gut aus. Die Replikationsverbindungen sollten inzwischen genug Zeit zur Angleichung haben. Also kontrolliere ich die Ergebnisse:

🔀 Administrator: Windows PowerShell	_	×
PS 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 Ergoldsbach\WS-DC2 über RPC DSA-Objekt-GUID: d11ed1cf-4a9f-4b89-b826-c43bfe5ace21 Letzter Versuch am 2020-06-02 11:02:38 war erfolgreich.		
CN=Configuration,DC=ws,DC=its Ergoldsbach\WS-DC2 über RPC DSA-Objekt-GUID: d1led1cf-4a9f-4b89-b826-c43bfe5ace21 Letzter Versuch am 2020-06-02 10:59:25 war erfolgreich. Neufahrn\WS-DC3 über RPC DSA-Objekt-GUID: 3b20c582-acc7-4758-8364-90e58595047f Letzter Versuch am 2020-06-02 10:59:51 war erfolgreich.		
CN=Schema,CN=Configuration,DC=ws,DC=its Ergoldsbach\WS-DC2 über RPC DSA-Objekt-GUID: d11ed1cf-4a9f-4b89-b826-c43bfe5ace21 Letzter Versuch am 2020-06-02 10:51:51 war erfolgreich.		
DC=ForestDnsZones,DC=ws,DC=its Ergoldsbach\WS-DC2 über RPC DSA-Objekt-GUID: d11ed1cf-4a9f-4b89-b826-c43bfe5ace21 Letzter Versuch am 2020-06-02 10:58:13 war erfolgreich.		
DC=DomainDnsZones,DC=ws,DC=its Ergoldsbach\WS-DC2 über RPC DSA-Objekt-GUID: d11ed1cf-4a9f-4b89-b826-c43bfe5ace21 Letzter Versuch am 2020-06-02 10:58:16 war erfolgreich. PS C:\> ■		

Mmh, da fehlen einige Verbindungen: Eigentlich sollte jede der 2 Partitionen über 2 eingehende Verbindungen verfügen – so wie die Configuration-Partition... WS-DC3 macht irgendwie noch nicht richtig mit.

Wichtig ist auch, das repadmin nur eingehende Verbindungen anzeigt. Die Replikation ist aber bidirektional. Also kontrolliere ich auch die beiden anderen DCs. Das hier ist das Ergebnis vom WS-DC3 in Neufahrn:

Administrator: C:\Windows\system32\cmd.exe	- <b>-</b> ×
C:\Users\sysadm>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 (never) war erfolgreich.	
CN=Configuration,DC=ws,DC=its Ergoldsbach\WS-DC1 über RPC DSA-Objekt-GUID: d84376f5-b557-4eea-96b6-6e67d8252ef9 Letzter Versuch am 2020-06-02 10:59:36 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 (never) war erfolgreich.	
DC=ForestDnsZones,DC=ws,DC=its Ergoldsbach\WS-DC1 über RPC DSA-Objekt-GUID: d84376f5-b557-4eea-96b6-6e67d8252ef9 Letzter Versuch am (never) war erfolgreich.	
DC=DomainDnsZones,DC=ws,DC=its Ergoldsbach\WS-DC1 über RPC DSA-Objekt-GUID: d84376f5-b557-4eea-96b6-6e67d8252ef9 Letzter Versuch am (never) war erfolgreich.	
C:\Users\sysadm>	~

Die Verbindungen waren noch nie erfolgreich. Das kann kurz nach der Einigung auf eine Replikationstopologie durchaus so sein. Aber ich helfe mal nach:



Nach wenigen Sekunden ist der WS-DC3 versorgt:





#### Nun ist noch der Rückweg dran:

📲 Active Directory-Standorte und -Dienste					- 🗆	$\times$
Datei Aktion Ansicht ? $\leftarrow \Rightarrow   \ge \boxed{10} \times \boxed{10} @ \Rightarrow   \boxed{2} \boxed{10} = 2$						
<ul> <li></li></ul>	Name WS-DC2		Vom Server WS-DC2	Vom Standort Ergoldsbach Neufahrn	Typ Verbindung	В
<ul> <li>Subnets</li> <li>Ergoldsbach</li> <li>EdgeSyncService</li> <li>Servers</li> <li>WS-DC1</li> <li>WTDS Settings</li> </ul>		Verschieben Jetzt replizierer Alle Aufgaben Löschen	>	<b>ACCOUNT</b>	terbindeng	
<ul> <li>♥ WS-DC2</li> <li>♥ NTDS Settings</li> <li>♥ Meufahm</li> <li>♥ Orvers</li> <li>♥ WS-DC3</li> <li>♥ NTDS Settings</li> </ul>		Umbenennen Eigenschaften Hilfe				

Der Server WS-DC1 hatte aber noch einige Lücken im repadmin. Die machen sich hier bemerkbar. Er weigert sich, weil die Replikationsverbindung noch nicht vollständig eingetragen wurde:

🗱 Active Directory-Standorte und -Dienste				—	$\times$
Datei Aktion Ansicht ? ← ➡ 2 〒 × □ 0 ⊡ 12 □ 12 □ 2					
<ul> <li>Active Directory-Standorte und -Dienste [WS-DC1.ws.its]</li> <li>Sites</li> <li>Inter-Site Transports</li> <li>Subnets</li> <li>Ergoldsbach</li> <li>EdgeSyncService</li> <li>Servers</li> <li>WS-DC1</li> <li>WS-DC2</li> <li>WS-DC2</li> <li>NTDS Settings</li> <li>Servers</li> <li>Servers</li> <li>WS-DC3</li> <li>WS-DC3</li> <li>NTDS Settings</li> </ul>	Name WS-DC2 WS-DC3 Jetzt replizieren Beim Versuch of Domänencont "WS-DC1" zu s aufgetreten: "Der Namensk wird nicht von - Dieser Vorgan	Vom Server WS-DC2 WS-DC3 den Namenskontext ' troller 'WS-DC3' nach synchronisieren, ist fo ontext wird entwede n angegebenen Serve g wird nicht fortgese	Vom Standort Ergoldsbach Neufahrn Domänencontroller Igender Fehler r gerade entfernt oder r repliziert. tzt.	Typ Verbindung Verbindung	В

Das machen die Domain Controller alleine aus. Da hilft also ein weiterer Kaffee. Na also, es geht doch:

WS IT-Solutions



WS IT-Solutions

WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019



Die AD-Replikation ist vollständig aktiv und arbeitet nach dem vorgesehenen Plan.

Weiter geht es mit den FSMO-Rollen. Die verschiebe ich wieder auf den WS-DC1 zurück:

<pre>Import-Module ActiveDirectory Move-ADDirectoryServerOperationMasterRole -Identity WS-DC1 -OperationMasterRole DomainNamingMaster Move-ADDirectoryServerOperationMasterRole -Identity WS-DC1 -OperationMasterRole InfrastructureMaster Move-ADDirectoryServerOperationMasterRole -Identity WS-DC1 -OperationMasterRole PDCEmulator Move-ADDirectoryServerOperationMasterRole -Identity WS-DC1 -OperationMasterRole RIDMaster Move-ADDirectoryServerOperationMasterRole -Identity WS-DC1 -OperationMasterRole -Identity</pre>
PS C:\> netdom /query fsmo Schemamaster WS-DC2.ws.its Dom_nennamen-Master WS-DC2.ws.its PDC WS-DC2.vs.its RID-Pool-Manager WS-DC2.vs.its Infrastrukturmaster WS-DC2.ws.its Der Befehl wurde ausgefhrt.
PS C:\> Import-Module ActiveDirectory
PS C:\> Move-ADDirectoryServerOperationMasterRole -Identity WS-DC1 -OperationMasterRole DomainNamingMaster
PS C:\> Move-ADDirectoryServerOperationMasterRole -Identity WS-DC1 -OperationMasterRole InfrastructureMaster
PS C:\> Move-ADDirectoryServerOperationMasterRole -Identity WS-DC1 -OperationMasterRole PDCEmulator
PS C:\> Move-ADDirectoryServerOperationMasterRole -Identity WS-DC1 -OperationMasterRole RIDMaster
PS C:\> Move-ADDirectoryServerOperationMasterRole -Identity WS-DC1 -OperationMasterRole SchemaMaster
PS C:\> netdom /query fsmo Schemamaster WS-DC1.ws.its Dom,nennamen-Master WS-DC1.ws.its PDC WS-DC1.ws.its RID-Pool-Manager WS-DC1.ws.its Infrastrukturmaster WS-DC1.ws.its Der Befehl wurde ausgefhrt.



Der Domain Controller ist einsatzbereit.

### Installation der Rolle DNS

Die Rolle DNS wurde im Setup des Active Directory mit konfiguriert. Hier fehlt nur etwas Feintuning. Zuerst stelle ich den Forwarder auf meine Fritzbox um. Hier stand bis eben noch die IP-Adresse des Domain Controllers WS-DC2:

🍰 DNS-Manager			$\square$ $\times$
Datei Aktion Ansicht ?	Eigenschaften von WS	S-DC1 ? X	
🗢 🔿 🙍 📆 🙆 🕞 👔	Debugprotokollierung	Ereignisprotokollierung Überwachen Sicherheit	
🚊 DNS 🛛 Name	Schnittstellen	Weiterleitungen bearbeiten	×
WS-DC1  Forward-Lookupzonen  Reverse-Lookupzonen	Bei Weiterleitungen h zum Auflösen von DN von diesem Server nic	IP-Adressen der Weiterleitungsserver:	1 Kashas
<ul> <li>Vertrauenspunkte</li> <li>Bedingte Weiterleitunger</li> </ul>	IP-Adresse	IP-Adresse Vollqualifizierter Domän Uberprüft <hier ip<="" klicken,="" td="" um=""><td>Loscnen Nach <u>o</u>ben</td></hier>	Loscnen Nach <u>o</u> ben
i rosv	192.168.100.2		Nach <u>u</u> nten
191 WS-			
	Stammhinweise ve Weiterleitungen ve		
	Hinweis: Werden bed definiert, werden sie a verwendet. Navigiere Weiterleitungen in de Weiterleitungen.	Sek. bis zur Zeitüberschreitung der Weiterleitungsabfragen: 3 Der vollqualifizierte Domänenname des Servers ist nicht verfügbar, wenn die entsprechend	len Reverse-
< >>	ок	Lookupzonen und Einträge nicht konfiguriert sind.	Abbrechen

Dann passe ich die Zeiten für das Aufräumen an:

Datei       Aktion       Ansicht       ?       Eigenschaften von WS-DC1       ?       ?         Image: Second Secon		
Image: Serverversionsnummer;     Image: Serverversionsnummer;		
<ul> <li>Forward-Lookupzonen</li> <li>Reverse-Lookupzonen</li> <li>Vertrauenspunkte</li> <li>Vertrauenspunkte</li> <li>Redingte Weiterleitunger</li> </ul> <li>Indextrement in the state of the sta</li>	DINSEC-Status Schlusself Nicht signiert Nicht signiert Nicht signiert Nicht signiert Nicht signiert Nicht signiert	na

Das Logging aktiviere ich ebenfalls. Die Logdatei lenke ich aber in ein anderes Verzeichnis um:

WS IT-Solutions

WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019

🚔 DNS-Manager		– – X
Datei Aktion Ansicht ?	Eigenschaften von WS-DC1 ? X	
<ul> <li>DNS</li> <li>WS-DC1</li> <li>Forward-Lookupzonen</li> <li>Reverse-Lookupzonen</li> <li>Vertrauenspunkte</li> <li>Bedingte Weiterleitunger</li> <li>rds.</li> <li>top</li> <li>ws.</li> </ul>	Schnittstellen       Weiterleitungen       Erweitert       Stammhinweise         Debugprotokollierung       Ereignisprotokollierung       Überwachen       Sicherheit         Sie können die an den DNS-Server gesendeten bzw. vom DNS-Server empfangenen Pakete protokollierung ist standardmäßig deaktiviet.       Debugprotokollierung ist standardmäßig deaktiviet.         Pakete zum Debuggen protokollierun       Transportprotokoll:       Mindestens eine Option       Mindestens eine Option         Paketinchtung:       Mindestens eine Option       Mindestens eine Option       Mindestens eine Option       Mindestens eine Option         Abfragen/       Mindestens eine Option auswählen       Mindestens eine Option       Mindestens eine Option       Mindestens eine Option         Wetere Optionen:       Mindestens       Antwort       Mindestens eine Option       Mindestens eine Option         Nicht übereinstimmende eingehende Rückmeldungspakete protokollieren       Fitem.       Mindestens         Details       Pakete nach IP-Adressen filtem       Fitem.         Protokolldatei       C:\Admin\DNS-Server\DNS-Logfile txt         Max. Größe (Byte):       104857600       Mindestens	DNSSEC-Status Schlüsselma Nicht signiert Nicht signiert Nicht signiert Nicht signiert Nicht signiert Nicht signiert

Das war auch schon alles. Der ganze Rest kam über die Active Directory Integration.

## Installation der Rolle DHCP

Die Rolle DHCP habe ich vorhin mitinstalliert. Deren Konfiguration starte ich im Server Manager:

Dashboard	EIGENSCHAFTEN Für WS-DC1		1 Konfi	guration nach der Ber	re AUFG ▼ X
Lokaler Server Alle Server AD DS Datei-/Speicherdienste	Computername Domäne	WS-DC1 ws.its	Zuletzt Konfig Windo Zuletzt Aufga	guration ist für "DHCF derlich. 2 <mark>-Konfiguration absch</mark> abendetails	P-Server" auf "WS-DC1" <u>lließen</u> E von ein verwalteter Dienst für Upda
DHCP DNS	Windows Defender Firewall Remoteverwaltung Remotedesktop NIC-Teamvorgang Ethernet	Domäne: Ein Aktiviert Aktiviert Deaktiviert 192.168.100.1, IPv6-fahig	Windows Defender Feedback und Diagr Verstärkte Sicherheit Zeitzone Produkt-ID	Antivirus nose tskonfiguration für IE	Echtzeitschutz: Ein Einstellungen Aus (UTC-01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien 00430-70395-36040-AA799 (Aktiviert)
erver-Manager DHCP-Konfigurations-Assisten Autorisierung	Betriebssystemversion	Microsoft Windows Server 2019 Datacenter	Prozessoren		AMD Ryzen 7 3700X 8-Core Processor -  -  -
Server-Manager DHCP-Konfigurations-Assisten Autorisierung Beschreibung Autorisierung	Betriebssystemversion t nach der Installation Geben Sie die Anmeldeinforma Directory-Domänendiensten ar	Microsoft Windows Server 2019 Datacenter	Prozessoren	dates	AMD Ryzen 7 3700X 8-Core Processor   AMD Ryzen 7 3700X 8-Core Processor
Server-Manager	Betriebssystemversion t nach der Installation Geben Sie die Anmeldeinforma Directory-Domänendiensten ar ( Anmeldeinformationen des Benutzername: WS\sysadm	Microsoft Windows Server 2019 Datacenter tionen zum Authentifizieren dieses DHCP-Server 5. folgenden Benutzers verwenden n	Prozessoren X	dates eprüft ntivirus	AMD Ryzen 7 3700X 8-Core Processor
Server-Manager  DHCP-Konfigurations-Assisten  Autorisierung  Beschreibung  Autorisierung Zusammenfassung	Betriebssystemversion t nach der Installation Geben Sie die Anmeldeinforma Directory-Domänendiensten an      Anmeldeinformationen des Benutzername: WS\sysadn     Alternative Anmeldeinformu Benutzername:     AD-Autorisierung übersprin	Microsoft Windows Server 2019 Datacenter	rs in den Active	dates eprüft ntivirus se konfiguration für IE	AMD Ryzen 7 3700X 8-Core Processor



Server-Manager				X
🔁 DHCP-Konfigurations-Assiste	nt nach der Installation —		×	🕶 🧭   🚩 Verwalten Tools Ansicht Hilfe
Zusammenfassu Beschreibung Autonsierung Zusammenfassung	Im Anschluss finden Sie den Status der Konfigurationsschritte nach der Installation: Sicherheitsgruppen werden erstellt Fertig Starten Sie den DHCP-Serverdienst auf dem Zielcomputer neu, damit die Sicherheit wirksam werden. DHCP-Server wird autorisiert Fertig	sgruppen		AUFGABEN   Jates Heute um 10:17 Updates automatisch mithilfe von ein verwalteter Dienst für Upda eprüft Heute um 10:16  tivirus Echtzeitschutz: Ein se Einstellungen konfiguration für IE Aus (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien 00430-70395-36040-AA799 (Aktiviert)  AMD Ryzen 7 3700X 8-Core Processor
				zicher (RAM) 2,37 GB mt: 99,4 G8
	< Zurück Weiter > Schließen	Abbreche	en	AUFGABEN 👻

Die Autorisierung wurde erfolgreich vorgenommen.

Im nächsten Schritt konfiguriere ich die Serveroptionen:



Die DNS-Server und ihre Reihenfolge werden in alle Scopes übernommen. WS-DC1 nennt seine IPv4 als primären DNS. Der WS-DC2 dagegen veröffentlich seine eigene IP als primär. So erreiche ich eine Lastverteilung, da ja auch die Clientanfragen auf beide DHCP-Server verteilt werden:

👮 DHCP	Ortigen (	2 ×	×
Datei Aktion Ansicht ?	Optionen - Server	· ^	
🗢 🔿 🚾 🙆 📓 🖬 🦑	Allgemein Erweitert		
<ul> <li>DHCP</li> <li>ws-dc1.ws.its</li> <li>IPv4</li> <li>Serveroptionen</li> <li>Richtlinien</li> <li>Filter</li> <li>IPv6</li> <li>Ws-dc2.ws.its</li> <li>IPv6</li> <li>Bereich [172.19.120.0] DMZ-extern</li> <li>Bereich [172.19.140.0] GameZone</li> <li>Bereich [172.19.140.0] GameZone</li> <li>Bereich [172.19.150.0] DMZ-Isolation</li> <li>Bereich [192.168.100.0] Server-Ergoldsbach</li> <li>Serveroptionen</li> <li>Richtlinien</li> <li>Filter</li> <li>IPv6</li> </ul>	Zur Verfügung stehende Optionen         003 Router         004 Zeitserver         005 Namenserver         006 DNS-Server            Dateneingabe         Servername:         Image: Imag	Beschreibun; ∧ Aray von Ro Aray von Ze Aray von Na Aray von DN ↓ > Auflösen	) DHCP-Server DHCP-Clients zuweisen kann. kdressen für Standardgateways (Router), e. Sie können jede dieser Serveroptionen finieren. die Serveroptionen festzulegen. inehilfe.



Mein Deployment-Server wird ebenfalls zentral im DHCP veröffentlicht:



Mehr Optionen habe ich vorher auch nicht verwendet. Ich starte nun die Konfiguration des DHCP-Failovers auf dem noch aktiven DHCP-Server WS-DC2:



Ich möchte alle Scopes höher verfügbar gestalten:



<ul> <li>Processing of the second sec</li></ul>	Datei Aktion Ansicht ?	Failover konfigurieren			
	<ul> <li> Image: Severoptionen <ul> <li>Image: Severoptionen</li> <li>Image: Severoptione</li></ul></li></ul>		Ehrführung in DHCP-Falover DHCP-Falover emröglicht hohe Verfügbarket für DHCP-Dienste, indem Informationen zu IP-Adresszuweisungen zwischen zwie DHCP-Servern synchronisiet werden. Zudem bietet DHCP-Falover Lastenausgleich für DHCP-Arforderungen. Dieser Assistent urterstützt Sie beim Einrichten des DHCP-Falovers. Wählen Sie in der folgenden Liste die Bereiche aus, die zur Konfiguration von hoher Verfügbarket konfiguriert sind, werden in der Liste nicht angezeigt. Verfügbare Bereiche: 192.168.110.0 192.181.00.0 172.19.150.0 172.19.120.0	58.100.2 .efi	Richtlinienname Keine Keine

Der neue Partnerserver ist der neue Windows Server 2019:

🖞 DHCP		7	- 0	$\times$
Datei Aktion Ansicht ?	Failover konfigurieren			
	Den Partnerserver angeben, der für Failover verwendet werden soll			
<ul> <li>DHCP</li> <li>Ws-dc1.ws.its</li> <li>IPv4</li> <li>Serveroptionen</li> <li>Richtlinien</li> <li>Filter</li> <li>IPv6</li> <li>Ws-dc2.ws.its</li> <li>Ereich [172.19.120.0] DMZ-texter</li> <li>Bereich [172.19.130.0] DMZ-texter</li> <li>Bereich [172.19.140.0] GameZone</li> <li>Bereich [172.19.150.0] DMZ-tsola</li> <li>Bereich [192.168.110.0] Clients-Ei</li> <li>Serveroptionen</li> <li>Richtlinien</li> <li>Filter</li> <li>IPv6</li> </ul>	Geben Sie den Hostnamen oder die IP-Adresse des DHCP-Pattnerservers an, mit dem das Fallover konfiguriett werden soll.         Sie Können einen Server in der Liste der Server mit einer vorhandenen Falloverkonfiguration auswählen, oder Sie können die Liste der autorisierten DHCP-Server durchsuchen und in dieser Liste einen Server auswählen.         Attenzierver:       ws.dc1.ws.its         Vorhandene Falloverbeziehungen, die mit diesem Server konfiguriert sind, wiederverwenden         Vorhandene Falloverbeziehungen, die mit diesem Server konfiguriert sind.	- 68.100.2 ν.efi	Richtlinienname Keine Keine Keine	

Die Konfiguration des Failovers belasse ich weitestgehend im Standard. Das Passwort ist eine zufällige Zeichenfolge auf der Tastatur:



👮 DHCP				- 🗆 X
Datei Aktion Ansicht ?	Failover konfigurieren			
	Neue Failoverbeziehung erstellen	La como da como da Como da como da com		,
We -dc1.ws.its             ✓ ■ IPv4             We -dc1.ws.its             We -dc1.ws.its	Erstellen Sie eine neue Failoverbeziehung m	nit dem Partner "ws-dc1.ws.its".	68.100.2 v.efi	Richtlinienname Keine Keine Keine
<ul> <li>Bereich [172.19.120.0] DMZ-exterr</li> <li>Bereich [172.19.130.0] DMZ-exterr</li> <li>Bereich [172.19.130.0] DMZ-Interr</li> <li>Bereich [172.19.140.0] GmZ-Interr</li> <li>Bereich [172.19.150.0] DMZ-Isolat</li> <li>Bereich [192.168.100.0] Server-Erg</li> <li>Bereich [192.168.110.0] Clients-Erg</li> <li>Serveroptionen</li> </ul>	Name der <u>B</u> eziehung: Maximale Clientvorlaufzeit: Modus: Lastenausgleich in Prozent Lokaler Server: <u>P</u> artnerserver:	ws-dc2 <=> ws-dc1 1 → Stunde 0 → Minuten Lastenausgleich ▼ 50 → ½ 50 → ½		
ii Kichtiinien > i Filter > iii IPv6	<ul> <li>Intervall für Zustands-Switchover:</li> <li>Nachrichtenauthentifizierung aktivigren</li> <li>Gemeingamer geheimer Schlüssel:</li> </ul>	60 Min <u>u</u> ten		

Die Angleichung dauert wenige Sekunden:

9 DHCP			_	- 🗆 X
Datei Aktion Ansicht ?	ailover konfigurieren			
<ul> <li>← ➡) 2</li> <li>□</li> <li>□&lt;</li></ul>		Das Failover wird zwischen "ws-dc2.ws.its" und "ws-dc1.ws.its" mit folgenden Parametern eingerichtet: _Bereiche:	68.100.2	Richtlinienname Keine Keine
Failover konfigurieren Der Status der Failoverkonfiguration. Das folgende Protokoll gibt Aufschluss über den : Aufgaben für die Failoverkonfiguration. Hierzu zäl aufgetretene Fehler. Bereiche auf dem Partnerserver hinzufügen Failoverkonfiguration auf dem Partnerserver erstell Bereiche auf dem Partnerserver stelle Bereiche auf dem Partnerserver stelle	? × Status der verschiedenen Ien auch möglicherweise Erfolgreich Erfolgreich ellenErfolgreich enErfolgreich Erfolgreich	192.168.110.0           192.168.100.0           172.19.150.0           172.19.150.0           172.19.130.0           172.19.130.0           172.19.120.0           Maximale Clientvorlaufzeit:           1 Skd.0 Min.           Modus:           Lastenausgleich           Intervall für Zustands-Switchover:	v.efi	Keine
Das Failover wurde erfolgreich konfiguriert. <	>	Lastenausgleich in Prozent       Lokaler Server:     50 %       Partnerserver:     50 % </td <td></td> <td></td>		

Nach einer Aktualisierung sind die Scopes sichtbar. Und auch die Aufteilung der IP-Adressen hat automatisch funktioniert. Clients werden bei einem DHCP-Renew keine Probleme haben:



PHCP		_	$\times$
Datei Aktion Ansicht ?			
• 🔿   🚈 📰 🗮 🖬 🤉 🔛 🖉 📷   📀			
<ul> <li>DHCP</li> <li>Ws-dc1.ws.its</li> <li>Bereich (172.19.120.0) DMZ-extern</li> <li>Bereich (172.19.130.0) DMZ-Intern</li> <li>Bereich (172.19.140.0) GameZone</li> <li>Bereich (192.168.110.0) Clients-Ergoldsbach</li> <li>Bereich (192.168.100.0) Server-Ergoldsbach</li> <li>Filter</li> <li>Bereich (172.19.120.0) DMZ-extern</li> <li>Bereich (172.19.130.0) DMZ-Intern</li> <li>Bereich (172.19.130.0) DMZ-Isolation</li> <li>Bereich (172.19.130.0) DMZ-isolation</li> <li>Bereich (172.19.150.0) DMZ-isolation</li> <li>Bereich (192.168.110.0) Clients-Ergoldsbach</li> <li>Bereich (192.168.110.0) Clients-Ergoldsbach</li> <li>Bereich (192.168.110.0) Clients-Ergoldsbach</li> <li>Bereich (192.168.110.0) DMZ-isolation</li> <li>Bereich (192.68.110.0) DMZ-isolation</li> <li>Bereich (192.68.110.0) DMZ-isolation</li> </ul>	Inhalt des Bereichs         ▲ Adresspool         ▲ Adressleases         ■ Reservierungen         ● Bereichsoptionen         ■ Richtlinien         Statistiken für Bereich 192.168.110.0         ■ Beschreibung         Details         Adressen insgesamt         99         In Benutzung         7(7%)         Verfügbare Adressen (Pool dieses Servers)         22(32%)         Verfügbare Adressen (Partnerpool)         46(45%)         Gewährte Adressen (Partnerpool)         5(5%)         Aktualisieren		

Jetzt gleiche ich noch die DHCP-Konfiguration beider Server an:

Eigenschaften von IPv4 ?	×	Eigenschaf	ten von	IPv4				?	×
Allgemein DNS Filter Failover Erweitert		Allgemein	DNS	Filter	Failover	Erweitert	t		
Der DHCP-Server kann so eingerichtet werden, dass autoritative DNS-Server automatisch mit den Hosteinträgen (A-Einträge) und de Zeigereinträgen (PTR-Einträge) von DHCP-Clients aktualisiert werde	en en.	Der DHC DNS-Sen Zeigerein	P-Server ver autor trägen (F	r kann so matisch r PTR-Eint	o eingerichte mit den Hos räge) von D	et werden, teinträgen )HCP-Clier	, dass autorita (A-Einträge) nts aktualisier	ative und den t werden.	
Dynamische DNS-Aktualisierungen mit den unten angegebener Einstellungen aktualisieren:	n	Dynar Einste	mische [ ellungen	ONS-Akti aktualisi	ualisierunge eren:	n mit den	unten angeg	ebenen	
C DNS-Einträge nur nach Anforderung von DHCP-Clients dyna aktualisieren	amisch	DI     ak	NS-Einträ tualisiere	äge nur r en	nach Anford	lerung vor	n DHCP-Clien	ts dynamiso	ch
ONS-Einträge immer dynamisch aktualisieren		0 DI	NS-Einträ	äge imme	er dynamiscl	h aktualisi	eren		
A- und PTR-Einträge beim Löschen der Lease verwerfen		🔽 A- un	d PTR-E	inträge b	oeim Lösche	en der Lea	ise verwerfen	I.	
DNS-Einträge für DHCP-Clients, die keine Aktualisierungen anfo (z. B. Clients unter Windows NT 4.0), dynamisch aktualisieren	ordem	DNS-Einträge für DHCP-Clients, die keine Aktualisierungen anfordem (z. B. Clients unter Windows NT 4.0), dynamisch aktualisieren					m		
Dynamische Updates für DNS-PTR-Einträge deaktivieren		🗌 Dyna	mische l	Jpdates	für DNS-PT	R-Einträge	e deaktivierer	n	
Namensschutz Der DHCP-Namensschutz ist auf Serverebene deaktiviert. Konfigurie	ieren	Namensschutz Der DHCP-Namensschutz ist auf Serverebene deaktiviert. Konfigurieren							
OK Abbrechen Ob	pemehmen				Oł	(	Abbrechen	Überne	ehmen

Das war sehr einfach.

# **Nacharbeiten**

### Installation LAPS

Es folgt die Installation des LAPS. Damit kann ich die Passworte der lokalen Admins mit einer GUI aus dem AD heraus auslesen:

WS IT-Solutions

WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019



### **Adminverzeichnis**

Auch das Adminverzeichnis c:\admin wird wieder befüllt:

📙   🖸 📑 🖛   Admin			_ □	$\times$	📕 I 📝 📑 🖛 l Admin	
Datei Start Freigeben Ansicht				~ ?	Datei Start Freigeben Ansicht	
← → · · ↑ 🦲 « Active Directory > Migration-2	019 > WS-DC1 > LWC > Admin	∨ Ö "Admin" d	lurchsuchen	Q	← → · ↑ 🛄 > Dieser PC > System (	C:) > Admin
📌 Schnellzugriff	Name	Änderungsdatum	Тур	Grö	🖈 Schnellzugriff	Name
System32	Scripte	02.06.2020 09:37	Dateiordner		System32	DNS-Server
Dealter	Check-ADStart.xml	02.06.2020 08:27	XML-Dokument		Desister	PSTranscript
Desktop	gMSA-Admin	17.06.2019 18:38	Verknüpfung		Desktop	
Administrator	LAPS-History	13.05.2019 11:35	Verknüpfung		Administrator	
Dieser PC	LAPS-History.xml	02.06.2020 08:28	XML-Dokument		Dieser PC	
System (C:)	PAM-AdminGUI	25.10.2019 13:28	Verknüpfung		System (C:)	
🛖 Freigaben (M:)	Sicherung-GPO.xml	02.06.2020 08:28	XML-Dokument		Admin	
AdminArea					DNS-Server	
Geräte					PSTranscript	
Lizenzen					Benutzer	
Netzwerk					PerfLogs	
Services	• 5.556 Elemente (3	30,8 MB) wurden gefunden	. –		× Program Files (x86)	
\$Migration-2019					Programme	
Active Directory	Kopieren von Adr	min nach Admin wird vorber	eitet		Windows	
gMSA-Admin	5.556 Elemen	te (30,8 MB) wurden	gefunden II	×	🛫 Freigaben (M:)	
GPO					🐂 Bibliotheken	
KRBTGT-Reset					🔿 Netzwerk	
Migration-2019	Wiehr Details				Systemsteuerung	
WS-DC1					Papierkorb	
LWC						
Admin						
Scripte						
PAM-AdminGUI						

Darin sind auch die xml-Dateien der Aufgabenplaung enthalten. Diese importiere ich im Anschluss:



A forkersterrer								~
Aufgabenplanung						-	Ц	^
Datel Aktion Ansicht ?								
							_	
Aufgabenplanung (Lokal) > Aufgabenplanungsbibliot	Status Trigger		Nächste Laufzeit	Letzte Laufzeit	Ergebnis der letzten Au	usführung Au	ıtor	
1	Einfache Aufgabe ers'	tellen						
	Neue Aufgabe erstelle	en						
	Aufgabe importieren.							
<	Aktualisieren							>
r p								
Aufgabenplanung								×
Datei Aktion Ansicht ?	- 🕑 Öffnen					×		
	📕 🔶 👻 🛧 🔚 > Dieser P	C → System (C:) → Admin →		√ Ū	"Admin" durchsuchen	م		
<ul> <li>Aufgabenplanung (Lokal)</li> <li>Aufgabenplanungsbibliot</li> </ul>	Organisieren 🔻 Neuer Ordn	her					tor	
	System (C:) ^ Na	ame	Änderungsdatum	Тур	Größe			
	Admin	DNS-Server	02.06.2020 11:12	Dateiordner				
1	Benutzer	PSTranscript	02.06.2020 10:13	Dateiordner				
	PerfLogs	Scripte	02.06.2020 11:34	Dateiordner	4 KD			
<	Program Files	Check-ADStart.xml	02.06.2020 08:27	XML-Dokument XMI -Dokument	4 KB			>
	Programme	Sicherung-GPO.xml	02.06.2020 08:28	XML-Dokument	4 KB			
	Windows							
	ADES							
	ADWS							
	apprompat							
	AppReadine							
	Datei <u>n</u> ame:	Check-ADStart.xml		~	XML-Dateien (*.xml)	~		
					Ö <u>f</u> fnen Ab	obrechen		
						.d		
< >								

### Der Import schlägt fehl:

Aufgabenplanung			- 🗆 X
Datei Aktion Ansicht ?	Aufgabe erstellen		
Aufgabenplanung (Lokal)  Aufgabenplanungsbibliot	Allgemein       Trigger       Aktionen       Bedingungen       Einstellung         Name:       Check-ADStart       Auf         Speicherort:       Image: Check-ADStart       Auf         Autor:       crashwork/Administrator       Fe         Beschreibung:       Image: Check-ADStart       Auf         Sicherheitsoptionen       Eeim Ausführen der Aufgaben folgendes Benutzerkonton       NT-AUTORITATISYSTEM         Nur ausführen, wenn der Benutzer angemeldet ist       Unabhängig von der Benutzeranmeldung ausführen         Mit höchsten Privilegien ausführen       Imageblendet       Konfigurieren für:       Windows Vista", 1	gen fgabenplanung thier für Aufgabe "Check-ADStart". Fehlermeldung: Der fr hier wurde geneldet: Die Aufgaben-XML enthält einen V twoeder falsch formatiert ist oder sich außerhalb des Bere findet. verwenden: Benutzer oder Gruppe ändern auf lokale Computerressourcen zu. Windows Server" 2008 v	Ergebnis der letzten Ausführung Autor

Die Ursache liegt wahrscheinlich beim hinterlegten Konto. Ich trage versuchshalber meinen Dummy-Admin ein:


(*) Aufgabenplanung		- 🗆 X
Datei Aktion Ansicht ?	×	
Aufgabenplanung (Loka)     Aufgabenplanungsbibliot     Allgermein Trigger Aktionen Bedringursaan Einestallunnaan.     Benutzer, Dienstkonto oder Gruppe auswählen     Objekttyp:     Benutzer, Dienstkonto oder Integrietes Sicherhetsprinzpal     Suchpfad:     Geben Se de zu verwendenden Objektnamen ein (Respelle):     admin setupl     Sicherheitsoptionen     Beim Aufgaben folgend     Nrt-AUTORITATSYSTEM     Nur ausführen, wenn der Benutzer anmeldung ausführen     Nur ausführen der Aufgaben nicht speichern. Die Aufgabe greift nur auf lokale Computerressourcen zu.     Mit höchsten Privilegien ausführen     Ausgeblendet Konfigurieren für: Windows Vista"; Windows Server" 2008     OK Abb	Objekttyper	× etzten Ausführung Autor

#### Das hat funktioniert. Jetzt stelle ich den System-Account wieder ein:

Aufgabenplanung			– 🗆 X
Datei Aktion Ansicht ?			
🗢 🔿 🙍 📰			
Aufgabenplanung (Loka)	Name     Status     Trigger <ul> <li>Check-ADStart</li> <li>Berint</li> <li>Beim Systemstart - Na</li> </ul> <ul> <li>Allgemein</li> <li>Trigger</li> <li>Aktionen</li> <li>Bedingungen</li> <li>Name:</li> <li>Check-ADStart</li> <li>Speicherort:</li> <li>Autor:</li> <li>crashwork\Administrator</li> <li>Beschreibung:</li> <li>Sicherheitsoptionen</li> <li>Beim Ausführen der Aufgaben folgendes Benu</li> <li>WS\admini-setup</li> <li>Nura usführen, wenn der Benutzeranmeldung a</li> <li>Kennwort nicht speichern. Die Aufgabe</li> <li>Mit höchsten Berechtigungen ausführen</li> </ul>	Figenschaften von Check-ADStart (Lokaler Computer)   Allgemein Trigger   Attor: Check-ADStart   Speicherort: Image: Check-ADStart   Autor: crashwork/Administrator   Beschreibung: Image: Check-ADStart   Sicherheitsoptionen Image: Check-ADStart   Beim Ausführen der Aufgaben folgendes Benutzerkonto verwenden:   SYSTEM   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   Ausgeblendet   Konfigurieren für:   Windows Vista <sup>m</sup> , Windows Server <sup>m</sup> 2008	< Autor crashwork\Adminis

Auch das hat funktioniert...



Aufgabenplanung					-	- 0	×		
Datei Aktion Ansicht ?									
🗢 🔿 🙍 📰									
Aufgabenplanung (Lokal)	Name	Status Trigger	Nächste Laufzeit	Letzte Laufzeit	Ergebnis der letzten Ausführung	Autor			
	Check-ADStart	Bereit Beim Systemstart - Nach Auslösung alle 5 Minuten für die Daue		30.11.1999 00:00:00	Die Aufgabe wurde noch nich	crashwork\	Adminis		
	<						>		
	Allgemein Trigge	r Aktionen Bedingungen Einstellungen Verlauf							
	Name:	Check-ADStart					^		
	Speicherort:	I							
	Autor:	crashwork\Administrator					_		
	Beschreibung:								
	- Sicherheitsontio	nen							
	Beim Ausführer	) der Aufgaben folgendes Benutzerkonto verwenden:							
	NT-AUTORITÄT\SYSTEM								
	<ul> <li>Nur ausführ</li> </ul>	en, wenn der Benutzer angemeldet ist							
	Unabhängig Kennwo	von der Benutzeranmeldung ausführen it nicht sneichern. Die Aufgabe greift nur auf lokale Ressourcen zu							
	Mit höchste	n Berechtigungen ausführen							
							¥		

Diese erste Aufgabe wird nach jedem Start ausgeführt. Das aufgerufene PowerShell-Script prüft, ob alle relevanten Dienste des Domain Controllers gestartet wurden und ob die erwarteten Eventlogs protokolliert worden. Wenn da etwas nicht stimmt, dann wird eine Korrektur gestartet. Der gesamte Vorgang wird dann in einer Textdatei protokolliert. Der letzte Start war erfolgreich:



#### Datensicherung der GPO

Ich habe ein weiteres Script, das über einen Task gestartet wird. Dieses sichert mir in einem Rotationsverfahren alle Gruppenrichtlinien. Ich importiere den Task:



Aufgabenplanung							- 0	×
Datei Aktion Ansicht ?								
🗢 🔿 🙍 📰 🚺								
<ul> <li>Aufgabenplanung (Lokal)</li> <li>Aufgabenplanungsbibliot</li> </ul>	Name Status () Check-ADStart Wird ausgeführt	Trigger Beim Systemstart - Nach Auslösung alle 5 M	Nä /inuten für die Daue	chste Laufzeit	Letzte Laufzeit 02.06.2020 11:37:19	Ergebnis der Die Aufgabe	letzten Ausführun wird momentan	g Autor . crashw
	Öffnen						×	
	← → ×  📑 > Di	eser PC > System (C:) > Admin		√ Ū	"Admin" durchsu	chen	Q	
	Crganisieren - Neue	r Ordner			8	•	0	>
	A Schnellzugriff	Name	Änderungsdatum	Тур	Größe			
	Admin	DNS-Server	02.06.2020 11:12	Dateiordner				
	System32	PSTranscript	02.06.2020 10:13	Dateiordner				
		Scripte	02.06.2020 11:34	Dateiordner				
	Desktop	LAPS-History.xml	02.06.2020 08:28	XML-Dokumer	nt 4 K	В		
	👗 Administrator	Sicherung-GPO.xml	02.06.2020 08:28	XML-Dokumer	nt 4 K	В		
	Dieser PC							
	🏪 System (C:)							
	Admin							
	DNS-Server							
	PSTranscrip							
	Scripte							
	Benutzer Y							
	Detail				VML Datains (*			
	Date	name: Sicherung-GPO.xml		~	XIVIL-Dateien (*.x	mi)	<u> </u>	
					Öffnon	Abbrochou		

Auch hier stand NT-Autorität\System als Taskaccount in der XML-Datei drin. Ich verändere den Account auf System. So lässt sich die Aufgabe ohne den XML-Fehler speichern:

Aufgabenplanung					- 0	$\times$
Datei Aktion Ansicht ?						
🗢 🔿 🙍 🔜						
<ul> <li>Aufgabenplanung (Lokal)</li> <li>Aufgabenplanungsbibliot</li> <li>Aufgabenplanungsbibliot</li> </ul>	Aufgabe ersteller Check-ADSta Allgemein Trigge Name: Speicherort: Autor: Beschreibung:	r Aktionen Bedingungen Einstellungen Sicherung-GPO \ WS\sysadm	×	ufzeit 20 11:37:19	Ergebnis der letzten Ausführung Die Aufgabe wird momentan	Autor crash
	Sicherheitsoption Beim Ausführen SYSTEM Nur ausführe © Unabhängig	nen der Aufgaben folgendes Benutzerkonto verwenden: n, wenn der Benutzer angemeldet ist von der Benutzeranmeldung ausführen	Benutzer oder Gruppe ändern			
	Kennwort     Mit höchsten     Ausgeblendet	t nicht speichern. Die Aufgabe greift nur auf lokale Con Privilegien ausführen Konfigurieren für: Windows® 7, Windows Server	nputerressourcen zu. " 2008 R2 ~ OK Abbrechen			

Ich starte den Task. Wenig später erhalte ich eine Mail mit der Information zur erfolgreichen Sicherung meiner GPO:

3	Sicherung GPO
offen	

64 GPOs erfolgreich auf WS-DC1 gesichert

#### Datensicherung LAPS (Script LAPS-History)

Ein weiteres Script sichert mir jeden Tag die Passwörter der lokalen Adminkonten aller Memberserver und Clients. Diese werden alle 30 Tage automatisch neu vergeben. Der Task ist schnell importiert. Das dazugeförige Script liegt bereits unter c:\admin\scripte:



Aufgabenplanung						- 0	×	
Datei Aktion Ansicht ?								
🗢 🔿 🙍 🖬 🚺								
Aufgabenplanung (Loka)     Solution	Name Check-ADStart LAPS-History Sicherung-GPO Allgemein Trigge Name:	Status Bereit Wird ausgeführt Bereit ar Aktionen Bedir LAPS-History	Trigger Beim Systemstart - Nach Auslösung alle 5 Minuten für die Daue Jeden Tag um 22:30 Uhr Jeden Tag um 04:45 Uhr	Nächste Laufzeit 02.06.2020 22:30:00 03.06.2020 04:45:00	Letzte Laufzeit 02.06.2020 11:37:19 02.06.2020 11:44:40 02.06.2020 11:39:44	Ergebnis der letzten Ausführung Der Vorgang wurde erfolgreic Der Vorgang wurde erfolgreic Der Vorgang wurde erfolgreic	Auto crash WS\s WS\s >	
	Speicherort: Autor: Beschreibung:	\ WS\sysadm						
< >>	Sicherheitsoptionen Beim Ausführen der Aufgaben folgendes Benutzerkonto verwenden: NT-AUTORITÄT\SYSTEM Nur ausführen, wenn der Benutzer angemeldet ist Unabhängig von der Benutzeranmeldung ausführen Kennwort nicht speichern. Die Aufgabe greift nur auf lokale Ressourcen zu. Mit höchsten Berechtigungen ausführen							

Es handelt sich um ein PowerShell-Script:



Das Script kann auch direkt gestartet werden. Dann zeigt es eine grafische Oberfläche, in der ich nach einem Computer suchen kann. Dann zeigt es mir alle gespeicherten Passwörter an. Die sensiblen Informationen werden natürlich gut geschützt: Das Script verschlüsselt die Daten mit einem Public-Key, der als CER-Datei im Scriptverzeichnis liegt:

📙   📝 🛄 🖛   History						- 0	) X	
Datei Start Freigeben Ansicht							~ 🕐	
← → ~ ↑ 📙 > Dieser PC > System (C:) > Admi	n > Scripte > LAPS-History > Hi	istory			~ Ō	History" durchsuchen	Q	
LAPS-History	Name		Änderungsdatum	Тур	Größe			
History	LAPS-History-2020-06-02-11-4	49-20.txt	02.06.2020 11:49	Textdokument	90 KB			
Benutzer								
PerfLogs		🛃 LAPS-Hist	tory				_	×
Program Files (x86)		Consultation		-				
LAPS-History-2020-06-02-11-49-20.txt - Editor	- 🗆 ×	Computerivan	wsts	2		lesen		
Datei Bearbeiten Format Ansicht Hilfe 98265055459565958941024447745505650670368	•	Com	puter	Password	Expiration of the second	on		
176,48,243,21,142,58,85,32,173,39,111,14,1	64,245,165,62,99,24	► WS-F	-52	8H18avUwPePJtv	02.06.20	J20 14:56:14		
172, 31, 80, 75, 162, 55, 249, 33, 247, 187, 17, 149,	77,237,48,103,159,2							
43,65,44,182,103,78,241,153,153,247,182,82	,108,83,108,116,193							
2,80,194,114,166,164,103,223,186,10,251,85	,200,238,8,90,225,1							
10,220,51,101,204,9,145,245,255,51,200,111	,234,17,30,01,39,9, 152 136 46 229 80 2							
152.171.2.173.204.200.133.43.172.207.253.1	48.239.4.93.120.98.							
,163,155,58,104,209,26,42,105,126,158,139,	152,127,51,255,230,							
151,65,246,53,225,33,130,4,94,132,231,85,1	0,146,207,102,9,26,							
84,139,142,165,43,246,191,26,225,73,146,85	,108,33,197,173,241							
129,87,73,107,230,237,141,39,200,44,223,22	6,13,105,84,18,33,1							
135,226,109,40,116,84,86,64,38,113,242,75,	255,220,131,78,246,							
<	>							
Windows (CF	Zeile 1, Spalte 100%							
Cursors 🗸								
1 Element 1 Element ausgewählt (89,4 KB)								

Seite 76 von 94



Nur der Owner des dazugehörigen Private-Keys kann mit dem Script die Daten entschlüsseln.

#### Hintergrund:

Warum ich mir die alten LAPS-Passwörter merke? Ganz einfach: Für Recovery-Szenarien. Ich hab mal das typische Szenario mit einer Zeitachse dargestellt:



Der Computer erstellt zum Zeitpunkt 1 eine Datensicherung. Das Passwort ist mit dem Active Directory synchron. Zum Zeitpunkt 2 verändert der Computer sein Passwort und speichert es im Active Directory ab. Zum Zeitpunkt 3 muss der Server wiederhergestellt werden. Dabei wird die Sicherung vom Zeitpunkt 1 verwendet. Jetzt ist das Passwort des lokalen Admins nicht mehr mit dem Active Directory synchron. Eine Anmeldung mit dem lokalen Admin ist nicht mehr möglich.

Jetzt gibt es nur noch 3 Optionen:

- 1) Das Computerkonto wird ebenfalls auf den Zeitpunkt 1 wiederhergestellt. Dafür ist eine gefilterte, autorisierende Wiederherstellung notwendig. Inklusive der Downtime eines Domain Controllers...
- 2) Man hackt sich in den Windows Server rein. Mit den Standardschutzmechanismen dauert das keine 5 Minuten.
- 3) Man hat eine LAPS-History und sucht darin das Passwort zum Zeitpunkt 1 heraus.

#### Datensicherung Windows Server

Nun fehlt noch die Datensicherung des Servers. Diese nehme ich wieder mit der Windows Server Sicherung und meinem zentralen Script-Task vor. Ich importiere die Aufgabe. Dabei gebe ich wieder meinen Dummy-Admin an:



Den eigentlichen Sicherungs-Account trage ich wieder mit meinem PowerShell-Script gMSA-Admin ein:

🥌 gN	/ISA-Admin						- 🗆	$\times$
vorhar	ndene gMSA:	Z	ugehörige Serv	/er:		zugehörige Gruppen:		
gMSA gMSA gMSA erst	+Backup (TaskUser für BMR) -Monitor (TaskUser für Monitoring -SQLDPM (Service SQL auf WS- telle gMSA lösche gMSA tz als: Task	)) DPM) W W W W W W W W W W W W W W W W W W W	VS-DC1.ws.its VS-FS1.ws.its VS-KA1.ws.its VS-KA1.ws.its VS-K2.ws.its VS-FS2.ws.its VS-DC3.ws.its VS-DC3.ws.its VS-DC3.ws.its VS-DC4.ws.its VS-DC4.ws.its VS-FS3.ws.its VS-MVA.ws.its VS-MVA.ws.its VS-MVA.ws.its VS-MVA.ws.its VS-MVA.ws.its VS-HV1.ws.its VS-HV2.ws.its VS-HV2.ws.its VS-HV2.ws.its VS-HV2.ws.its VS-HV2.ws.its VS-HV2.ws.its VS-HV2.ws.its VS-HV2.ws.its VS-HV2.ws.its VS-HV1.ws.its VS-HV3.ws.its VS-HV3.ws.its VS-HV4.ws.its VS-HV3.ws.its VS-HV4.ws.its VS-HV4.ws.its VS-HV4.ws.its VS-HV4.ws.its VS-HV4.ws.its VS-HV4.ws.its VS-HV51.ws.its VS-HV4.ws.its VS-HV51.ws.its VS-HV51.ws.its VS-HV6.ws.its	online) 3 5 Erfolg Der Task wurde umgestellt!	X pMSA	direkte Gruppen:     GG-SEC-Server-Monitoring-Admins     GG-SEC-Server-Standard-Admins     GG-SEC-Server-RDS-Admins     GG-SEC-Server-MperV-Admins     GG-SEC-Server-HyperV-Admins     GG-SEC-Server-HyperV-Admins     GG-SEC-Server-HyperV-Admins     GG-SEC-Server-File-Admins     Sicherungs-Operatoren	elung):	~
	Server	TaskName		Account		Pfad		^
	WS-DC1	Check-ADStart		NT-AUTORITÄT\SYSTEM		١		
	WS-DC1	LAPS-History		NT-AUTORITÄT\SYSTEM		N		
•	WS-DC1	ServerSicherung		ws\gMSA-Backup\$		N		
	WS-DC1	Sicherung-GPO		NT-AUTORITÄT\SYSTEM		X		
	WS-DC1 Server Initial Configuration Task		Task	NT-AUTORITÄT\SYSTEM		\Microsoft\Windows\		
	WS-DC1 .NET Framework NGEN v4.0.30319		NT-AUTORITÄT\SYSTEM		\Microsoft\Windows\.NET Framework\			
	WS-DC1	.NET Framework NGEN v4	4.0.30319 64	NT-AUTORITÄT\SYSTEM		\Microsoft\Windows\.NET Framework\		
	WS-DC1	.NET Framework NGEN v4	4.0.30319 6	NT-AUTORITÄT\SYSTEM		\Microsoft\Windows\.NET Framework\		~
lese bereit	alle Server setze gMSA ein							:

Die Konfiguration der Sicherung muss ich nicht anpassen. Der Server ist mit den vorherigen Einstellungen kompatibel.

#### **TroubleShooting Monitoring**

Ich kontrolliere nun das Mnoitoring. Vorhin habe ich mein Script SecEV-Monitor auf den Server WS-MON verschoben. Den alten WS-DC1 konnte ich damit einfach weiter kontrollieren. Der neue Server wehrt sich aber. Das kann ich im Runtime.log sehen:



SecEv-Monitor					_	ПХ	_	
Datai Start Fraigaban Apricht								
Statt Heigeben Anstatt				1=1				
← → · · ↑ 📴 > Dieser PC > System (C:) > A	dmin > SecEv-Monitor >			~ Ū	"SecEv-Monitor" durc	hsuchen 🔎		
🖈 Schnellzugriff	Name	Änderungsdatum	Тур	Größe				
Desktop	CSV Reports	02.06.2020 10:11 02.06.2020 08:57	Dateiordner Dateiordner					
	Statistik	02.06.2020 09:01	Dateiordner					
Dieser PC	RunTime.log	02.06.2020 11:14	Textdokument	5 KB				
System (C:)	SecEv-Monitor.ini	30.04.2020 17:48	Konfigurationsein	3 KB				
Admin	SecEv-Monitor.ps1	25.06.2019 17:40	Windows PowerS	86 KB				
PrivilegedADUser-Analyse	SecEv-Monitor.xml	02.06.2020 08:28	XML-Dokument	5 KB				
PSTranscript	RunTime.log - Editor						- 0	з х
SecEv-Monitor	Datei Bearbeiten Format Ansicht	Hilfe						
ServerMonitor	starte RemoteJobs							^
SnortMon	INFO: WS-DC2 - lese Sec	urity-Eventlog	ab 2020-06-02 1	1:12:10				
Benutzer	INFO: WS-DC2 - lese NIL INFO: WS-DC2 - dupcheuc	M-Eventlog ab 2	020-06-02 11:12	:10				
PerfLogs	INFO: WS-DC2 - keine Tr	effer						
Program Files (x86)	Der Pfad "HKLM:\SOFTWARE\W	S.ITS\SecEv-Mor	itor" kann nich	t gefunden	werden, da er ni	cht vorhand	en ist.	
Programme	+ CategoryInfo	: ObjectNotFo	ound: (HKLM:\SOF	TWARE\WS.IT	S\SecEv-Monitor:	String) [Ge	t-ItemProper	rty],
Windows	ItemNotFoundException	d · PathNotFour	d Microsoft Pow	anShall Com	mands GetItemPro	nentvComman	a l	
- Monitoring (Fr)	+ PSComputerName	: WS-DC1.ws.i	ts	er brieff.com	marius.decicem ro	per cyconinani		
Excitation (14)	Der Pfad "HKLM:\SOFTWARE\W	S.ITS\SecEv-Mor	itor" kann nich	t gefunden	werden, da er ni	cht vorhand	en	
	ist.							
adminarea v	+ CategoryInto	: UDJectNotFo	ound: (HKLM:\SOF	IWARE \WS.II	S\SectV-Monitor:	String) [Ge	τ-1τ	
7 Elemente	+ FullyOualifiedErrorI	d : PathNotFour	nd.Microsoft.Pow	erShell.Com	mands.GetItemPro	pertvComman	d	
	+ PSComputerName	: WS-DC1.ws.i	ts					
	Sie müssen ein Objekt für	das Cmdlet "Get	-Member" angegel	ben.				
	+ CategoryInfo	: CloseError:	(:) [Get-Membe	r], Invalid	OperationExcepti	on		
	+ FullyQualifiedErrorI	d : NoObjectIn	etMember,Micros	oft.PowerSh	ell.Commands.Get	MemberComma	nd	
	+ rocomputerName Sie müssen ein Objekt für	das (mdlet "Get	.TS -Member" angege	hen				
	+ CategoryInfo	: CloseError:	(:) [Get-Membe	r], Invalid	OperationExcepti	on		
	+ FullyQualifiedErrorI	d : NoObjectIn	etMember,Micros	oft.PowerSh	ell.Commands.Get	MemberComma	nd	
	+ PSComputerName	: WS-DC1.ws.	ts					, ×
				Windows (CP	RIF) Zeile 1 9	inalte 1	100%	
				windows (Ci	Zelle 1, 3	aparce i	10070	

OK, da fehlen Registry-Keys auf dem neuen WS-DC1. Die sollte das Script eigentlich selber erstellen. Aber es ist immer noch eine unfertige Version. Daher helfe ich mal manuell nach:

Der nächste Lauf des Scriptes erstellt die Einträge:



Und damit ist auch dieses Problem behoben:

Datei Start Freigeben Ansicht					- 0	× ~ ?		
← → ~ ↑ 📙 > Dieser PC > System (C:) > Adm	nin > SecEv-Monitor			~ Ō	"SecEv-Monitor" durchsuchen	<i></i>		
> 🖈 Schnellzugriff	Name	Änderungsdatum	Тур	Größe				
✓      ✓      Desktop      & Walther, Stephan - T1      ✓      Dieser PC	CSV Reports Statistik	02.06.2020 10:11 02.06.2020 08:57 02.06.2020 09:01	Dateiordner Dateiordner Dateiordner	4 VD				
✓ ≝ System (C:)	SecEv-Monitor.ini	30.04.2020 17:48	Konfigurationsein	4 KB				
Admin     PrivilegedADUser-Analyse	SecEv-Monitor.xml	02.06.2020 08:28	XML-Dokument	5 KB				
PSTranscript     SecEv-Monitor     ServerMonitor	RunTime.log - Editor Datei Bearbeiten Format Ansich yNotFoundException,Mic	nt Hilfe rosoft.ActiveDir	rectory.Manageme	nt.Commands	GetADUser		- 0	×
SnortMon Benutzer PerfLogs Program Files (x86) Program Files (x86) Windows Monitoring (E:) Frigaben (M:) AdminArea TElemente 1 Element ausgewählt (3,32 KB)	<pre>+ PSComputerName INF0: WS-DC1 - 1 moegl analysiere und protokolli Events werden verarbe ermittle Zeitgrenze erstelle die Arbeits fuelle die Arbeits speichere Zusammenf speichere Details i Statistik ist aktuell erstelle Verlaufsdiagr erstelle den HTML-Beri speichere den Beric berechne Bewertung:</pre>	: WS-DC1.ws. icher Treffer ere das Ergebnis itet: n stabelle abelle assung in Datei m Datei 'C:\Admin' amme: cht ht in 'C:\Admin' rad 'Info' zu ge derlich ll-Aufzeichnung	tts 'C:\Admin\SecEv in\SecEv-Monitor \SecEv-Monitor\R Pring	-Monitor\St \CSV\2020-0 eports\aktu	atistik\Zusammenfassung G-02.csv' ell.htm'	g.csv'		
	<			Windows (CR	LF) Zeile 1, Spalte 1	1009	6	>

Und was sagt mein PRTG zum neuen WS-DC1? Nicht viel, denn der Server ist noch pausiert. Ich setze die Sensoren fort. Es dauert dann einige Sekunden:



								Neue Protokolleinträg
0	Startseite	Geräte	Bibliotheken	Sensoren	Alarme	Maps	Berichte	Pr
#	Geräte							
	Gruppe WS-ITS							
	O Übersicht	2 Tage	30 Tage 365 Ta	ge 🔺 Alarme	Protokoll	≢ Verwaltung	Cinstellungen	🜲 Trigger fi
	!1 W1 ✓90	U 1 ? 6 (von 9	) S M L XL (Ç				Suche	Q
	白 <i>略</i> WS-I	MX1 12 Base WS-MX1 3,6%	Services WS-M MX-CAS	1# SMTP 9 ms	✓ Queue 0 # ✓ DB-He	alth 100 % ServerCompon 100 #	+ Sensor hinzufügen	^
	⊡ <i>№</i> WS-I	Base WS-MX2 5,35 % OC1 IC Base WS-DC1	Services WS-M MX-CAS     34 #      Services AD     PDNS	1 # SMTP 34 ms ? Active Director	✓ Queue 0 # ✓ DB-He ? Active Director +	alth 100 % ServerCompon 100 #	+ Sensor hinzufügen	
	⊡ # WS-I	0C2 F7 Base WS-DC2 0%	Services AD 13 #	Active Director 1 ms 0 #	Sensor     hinzufügen	zufugen		- 1
	□ <sup>殿</sup> WS-I	C3 戸 Base WS-DC3 1,15%	Services AD DNS	80 ms	+ Sensor hinzufügen			

Dann tauchen Fehlermeldungen auf. Die Sensoren sind nicht 100% kompatibel:

					Ne	ue Alarme 1 Neue Protok	olleinträge 2
	Geräte	Bibliotheken	Sensoren	Alarme	Maps	Berichte	
Willkommen bei PRTG	erver 🔻 WS-DC1 🔻	Base WS-DC1 💌					
Als Startseite festlegen	DC1 <sup>P</sup> *** <sup>☆☆</sup>						
🔿 Übersicht	(••) Livedaten 2	Tage <b>30</b> Tage	365 Tage 🕍 I	Historische Daten	Protokoll	🌣 Einstellungen	🜲 Trig
CPU		NIC Ethernet empfange	n NIC Ethernet sender	RAM frei	RAM S	eitenfehler	
		0 MB/s	0 MB/s	38%	1,99 f/	s 🖓	
		Vol. System frei	Vol. SYSTEM frei	Vol. System les	en Vol. SY	STEM lesen	
		87 %	Keine Daten	o∓ 0 kB/s	Keine	Daten 🔿 🖡	
	×	Vol. System schreiben	Vol. SYSTEM schreil	ben Vol. System Wa	arteschlange Vol. SY	STEM Warteschlange	
1,88 %	0 % 100 %	0 ∓ 255 kB/s	Keine Daten	o.#_ 0.#	Keine	Daten 🔿 🕱	

Der Sensor ist ein von mir erstelltes PowerShell-Script. Da stimmt was mit den Historischen Daten nicht. Daher lösche ich den Sensor:

tartseite	G	eräte	Biblio	theken	Sensoren	Alarme	Maps	Berichte	
Geräte WS-I	TS 🔻 Serve	er 🔻 WS-D	)C1 🔻						
ierät <mark>WS</mark> -	DC1 🏱 🎌	<b>*★</b> ☆☆							
O Übersi	cht 2	Tage 3	30 Tage	365 Tage	Alarme	<b>O</b> Systeminformationen	Protokoll	🌣 Einstellunger	n J
Wenn	Sie hier Sens	ortachos seł	nen möchten, ä	ndern Sie die Prio	rität von einem c	der mehreren Sensoren zu 🔰	<b>****</b> ☆/ <b>****</b> *.		
Pos. 🕶	Sensor 🌻			Status	Nachrich	t	Graph	Priorität 🗘	
Pos. ▼ ∳1.	Sensor 🗘	5	Sensormenü	Status Fehler	Nachrich OK	t	Graph	Priorität ≑	
Pos. ▼	Sensor 🗘	<ul> <li>Z Jetzt abr</li> <li>Q Details</li> </ul>	Sensormenü fragen	Status Fehler OK	Nachrich OK AD Service	t es are running	Graph CPU data confiderations and Services AD	Priorität ≑ 1885 ★★★☆☆ 11= ★★★☆☆	
Pos. ▼	Sensor 🖗	<ul> <li>S Jetzt ab'</li> <li>Q Details</li> <li>☑ Bearbeit</li> <li>✓ Alarm be</li> </ul>	Sensormenü fragen en estätigen	Status Fehler OK OK	Nachrich OK AD Service OK: 192.1	t es are running 58.100.1	Graph CPU Alus Action Action Services AD Antwortzeit	Priorität ≑           1283         ★★★☆☆           11 #         ★★★☆☆           2ms         ★★★☆☆	
Pos. ▼	Sensor + H Base V Servic DNS Active	<ul> <li>S Jetzt ab'</li> <li>Q Details</li> <li>Ø Bearbeit</li> <li>✓ Alarm be</li> <li>Icöschen</li> <li>Coschen</li> </ul>	Sensormenü fragen	Status Fehler OK OK	Nachrich OK AD Service OK: 192.10 Ok	t es are running 68.100.1	Graph CPU Services AD Antwortzeit Last Sync Rer	Priorität =           1885         *********           11=         ********           2ms         ********           0=         ********	
Pos. ▼	Sensor Base V Servic DNS Active	<ul> <li>S</li> <li>S Jetzt ab</li> <li>Q Details</li> <li>G Bearbeit</li> <li>✓ Alarm be</li> <li>Cöschen</li> <li>Cischen</li> <li>Cershie</li> </ul>	Sensormenü fragen esestätigen	Status Fehler OK OK OK	Nachrich OK AD Service OK: 192.11 Ok	t es are running 58.100.1	Graph CPU Alist Activity added Alistander Services AD Antwortzeit Last Sync Res Last Sync Res	Priorität *           128*         ************************************	



#### Anschließend kann ich ihn neu erstellen:

									Neue P
0	Startseite	Geräte	Bibliothe	ken	Sensoren	Alarme	Maps	Berichte	
# (	Geräte WS-IT	S ▼ Server ▼ WS-I DC1 <sup>PD</sup> ★★★☆☆	DC1 🔻						
	O Übersicl	ht 2 Tage	30 Tage 36	5 Tage	Alarme	O Systeminformationer	n 🔲 Protokoll	🌣 Einstellungen	🐥 Tri
	Wenns	Sie hier Sensortachos se	hen möchten, ände	ern Sie die Prior	ität von einem o	der mehreren Sensoren zu	****		
								Senso	r hinzufügen
	Pos. 🕶	Sensor 🌻		Status 🏺	Nachrich	t	Graph	Priorität ≑	
	<b>4</b> 1.	Services AD		ОК	AD Servic	es are running	Services AD	11年 ★★★☆☆	
	<b>4</b> 2.	V DNS		ОК	OK: 192.1	58.100.1	Antwortzeit	<u>1</u> ms ★★★☆☆	
	<b>4</b> 3.	Active Directory Re	eplication Errors to	OK	Ok		Last Sync Res	0# ★★★☆☆	
	<b>4</b> .	Active Directory Re	eplication Errors to	OK	Ok		Last Sync Res	0# ★★★☆☆	
					<< < 1 bis 4	von 4 >>>			

Ich editiere den Namen und wähle mein Sensor-Script für die Basisdaten eines Windows Servers aus:

Sensor hinzufügen zum Gerät WS-DC1 [WS-DC1		(Sc
< Abbrechen		
Allgemeine Name des Sen Sensoreinstellungen	Base WS-DC1	
Übergeordnete	ags <sup>()</sup>	
	ags 🕚 xmlexesensor 🗙 O	
Pric	ität 0 ★★★☆☆	
Sensoreinstellungen	Die ausführbare Datei wird auf der Maschine ausgeführt, auf der die <b>übergeordnete Probe</b> installiert ist, nicht auf dem übergeordneten Gerät. Das Arbeitsverzeichnis für EXE-Dateien ist das Verzeichnis der Probevbs-, .ps1- oder andere Skriptdateien können andere Arbeitsverzeichnisse verwenden.	
Programm/S	ript 0 WSSensor-ServerBaseline.ps1	~
Paran	eter 0	

Noch eine kurze Verschiebung nach oben und ein paar Sekunden warten zeigen wieder alles in einem frischen grün an:



								Neue Protokolleinträge
0	Startseite	Geräte	Bibliotheken	Sens	oren Alarme	Maps	Berichte	Pro
*	Geräte WS-ITS	Server VKS-I	0C1 💌					
	Gerat <b>WS-D</b>	C1 - 22288						
	O Übersich	t 2 Tage	30 Tage 365 Tag	e 🔺 Alarme	O Systeminformatio	nen 🗏 Protokoll	Cinstellunge	n 🖡 Trigger
	Wenn S	ie hier Sensortachos sel	nen möchten, ändern Sie	die Priorität von ein	em oder mehreren Sensoren a	zu ★★★★☆ / ★★★★★	k.	
								•
	Pos. 🗸	Sensor 🗢		Status 🗘 Nac	hricht	Graph	Priorität 🗢	
	<b>4</b> 1.	Base WS-DC1		ок ок		CPU	0% <b>★★★</b> ☆☆	
	<b>4</b> 2.	Services AD		OK AD S	ervices are running	Services AD	11# ★★★☆☆	
	<b></b> 3.	V DNS		DK OK: 1	92.168.100.2	Antwortzeit	<u>5ms</u> ★★★☆☆	
	<b>-‡</b> • 4.	Active Directory Re	plication Errors to	DK Ok		Last Sync Res	0# <b>★★★</b> ☆☆	
	<b>.</b>	Active Directory Re	plication Errors to	DK Ok		Last Sync Res	0# ★★★☆☆	
				<< < 1	bis 5 von 5 🔉 🔉			

#### **Integration ins ATA**

Mein ATA sollte eigentlich auch keine Probleme haben, da ich ja die neue Netzwerkkarte des neuen WS-DC1 bereits für die Datenspiegelung vorbereitet hatte. Und so zeigt es mir auch das Dashboard des ATA an: Alle Domain Controller sind erreichbar:

Microsoft Ad	Vicrosoft Advanced Threat Analytics   Konfigurationen								
	System								
	Center	Gateways							
	Gateways								
	Updates	Gatewaysetup	Gatewaysetup Laden Sie dieses Paket herunter, um ein Gateway oder ein Lightweight-Gateway zu installieren.						
	Datenquellen		_						
	Verzeichnisdienste	NAME		75/0	DOMÉNICA CONTRO	VERSION	DIENCTETATILE	INTECDITÄT	
	SIEM	NAME	^	TAB	DOMANEN-CONTRO	VERSION	DIENSISIATUS	INTEGRITAT	
	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		

Zwischenzeitlich hatte ich aber eine Mail vom ATA erhalten. Der Wipe & Load- Vorgang blieb nicht unbemerkt:

Microsoft Advanced Threat Analytics 🗧 Microsoft
Mittel
Kein Datenverkehr vom Domänencontroller empfangen Es wurde über "WS-ATA" seit "Eine Stunde" kein Datenverkehr von "ws-dc1.ws.its" empfangen.
Bitte prüfen
" <u>Benachrichtigungseinstellungen</u> " verwalten



Sehr interessant ist auch diese Meldung. Die musste ich aber im Computerobjekt im ATA suchen. Etwas Neugier schadet wohl nicht:

osoft Advanced Threat Analytics $\mid$ WS-DC	1				a 🗐 📙 Micr				
				Neuest	te 100 unterschiedliche Entitäten anzeig				
	0	0	4	0	1				
	Offene verdächtige Aktivitäten	Angemeldete Benutzer	Ressourcen, auf die zugegriffen wurde	VPN-Standorte, auf die zugegriffen wurde	Verwendete IP-Adressen				
WS-DC1 Windows Server 2019 Datacenter, 10.0 (1		E Wechseln zu ∨      V Filtern nach ∨     E Downloadaktivitäten							
Sensibel	Heute								
	12:04 Fehler b     Aufgetreter	ei der Anmeldung von "Administra = 61 in "10 Minuten"   mit "Ntlm"   für "2 Compu	tor": Fehler "AccountRestriction"						
Domäne Erstmals angezeigt ® ws.its 25.08.2019	0 10:51 Das Betr geänder	fiebssystem wurde von "Windows ! t.	Server 2016 Datacenter, 10.0 (14393)	" in "Windows Server 2019 Datac	enter, 10.0 (17763)"				
SAM-Name Erstellt am <sup>(2)</sup> WS-DC1\$ 10.08.2013	0 10:51 🔺 Dem	10:51 Dem Konto wurde die Delegierung erlaubt (nur Kerberos).							
	10:11 Anmelde mit "Ntim"	eversuch über "Nicht vorhandenes  für "WS-DC2"	Konto "ws.its\Administrator*"						
	10:11 Das Kon	tokennwort wurde geändert.							
	09:37 Fehler b Aufgetreter	ei der Anmeldung von "Administra ¤ 85 in "eine Stunde"   mit "Ntlm"   für "2 Compi	itor": Fehler "AccountRestriction" utem"						
	08:13 "Admini: mit "Kerber	strator" hat von "WS-CL1" aus übe os"   für "WS-DC1"   WS-CL1: 192.168.110.101	er RDP eine Verbindung hergestellt.						

#### PowerShell JEA-PAM-AdminGUI

Final konfiguriere ich den neuen Server als JEA-Endpunkt für mein PAM-Script. Mit dieser selbstprogrammierten Lösung kann ich gesichert meine administrativen Accounts temporär in spezielle Berechtigungsgruppen aufnehmen. Dazu habe ich im Blog 2 weitere Artikel.

Die Installation ist denkbar einfach, denn ich habe dafür ein Script. Ich führe alle Zeilen der Region "Variablen" aus:



Und dann den Regionsblock "Setup/Update":



So werden die erforderlichen Dateien erstellt und im Windows Remote Management regirstriert:



Ich starte das clientseitige Frontend. Die PowerShell rendert mir eine hübcshe GUI und verbindet sich mit dem neuen WS-DC1. Die Einrichtung war erfolgreich:

to DAM Admin CUI	we does not blue post of	V						$\sim$
- PAM-AdminGUI - verbi	unden mit WS-DCT (	version v i.i l)				-	ш	~
Modus:	Admins	Gruppen		Ziel-DC: W	/S-DC2 ~	zu D	C replizie	eren
Zeitraum [min]:	15	~				alle (	DC replizi	eren
Admins:		mögliche Gruppen:	Mitglied:					
admin admin-audit admin-Notfall admin-wetup admin-wac stephan-T1 stephan-T2 sysadm		DHCP-Administratoren DnsAdmins Domänen-Admins GG-Admin-ADJoin GG-Admin-ADJoin GG-Admin-Backup GG-Admin-Backup GG-Admin-Beckup GG-Admin-GPO GG-Admin-PKI GG-Admin-PKI GG-Admin-Setup-Applocker-Ausnahme-uberall GG-Admin-Setup-Applocker-Ausnahme-uberall GG-Admin-Setup-Applocker-Ausnahme-uberall GG-Admin-Setup-Applocker-Ausnahme-uberall GG-Admin-Setup-Applocker-Ausnahme-uberall GG-Admin-Setup-Applocker-Ausnahme-uberall GG-Admin-Setup-Applocker-Ausnahme-uberall GG-Admin-Setup-Applocker-Ausnahme-AdminDir GG-SEC-Clients-JB-Admins GG-SEC-Clients-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-MDS-Admins GG-SEC-Server-MIN-Admins Organization Management Protected Users Schema-Admins	Gültigkei	t	Gruppe			

#### TroubleShooting des Zeitservers

Diese Funktion wird gerne vergessen: korrekte Zeiten sind für das Authentifizierungsprotokoll enorm wichtig. Der neue Server ist mein PDC-Emulator. Daher muss er selber über eine geeignete Zeitquelle verfügen. Ohne diese gibt es schnell Abweichungen. Mit w32tm /stripchart kann ich die Differenz zu einem öffentlichen NTP-Server auswerten. Der Stern liegt nicht in der mitte zwischen den eckigen Klammern. Die Zeiten sind nicht synchron:

Administrator: Windows PowerShell			_	×
PS C:\> w32tm /stripchart /computer:de.pool.ntp.org de.pool.ntp.org wird verfolgt [5.9.121.21:123]. Fs ist 02.06.2020 14:06:28.				^
14:06:28, d:+00.0213208s o:+01.1971917s [ 14:06:30, d:+00.0244532s o:+01.1987099s [ 14:06:33, d:+00.0198222s o:+01.1998844s [		] ] ]		
14:06:39, d:+00.02729185 0:+01.20147865 [ 14:06:39, d:+00.02729185 0:+01.20147865 [ 14:06:39, d:+00.02471105 0:+01.19735565 [ PS C:\>	*	]		

Die anderen Domain Controller holen sich ihre Uhrzeit beim PDC. Das funktioniert ohne Konfiguration. Meine beiden anderen DCs sind synchron mit der Zeit vom WS-DC1. Alle weichen gemeinsam ab:

WS IT-Solutions

## WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019

Administrator: Windows PowerShell		-	$\times$
PS C:\> w32tm /stripchart /computer:ws-dc2.ws.its			~
ws-dc2.ws.its wird verfolgt [192.168.100.2:123].			
Es ist 02.06.2020 14:07:09.			
14:07:09, d:+00.0006848s o:+00.0517196s [	]		
14:07:11, d:+00.0008191s o:+00.0516126s [	]		
14:07:13, d:+00.0008554s o:+00.0516146s [	]		
PS C:\>			
PS C:\>			
PS C:\> w32tm /stripchart /computer:ws-dc3.ws.its			
ws-dc3.ws.its wird verfolgt [192.168.101.1:123].			
Es ist 02.06.2020 14:07:19.			
14:07:19, d:+00.0315870s o:-00.0647807s [	]		
14:07:21, d:+00.0259422s o:-00.0670591s [	]		
14:07:23, d:+00.0310147s o:-00.0648002s [	]		
PS C:\>			

Ich konfiguriere den Zeitservice und trage einen öffentlichen NTP-Server statisch ein:

Administrator: Windows PowerShell	_	×
PS C:\> <mark>net</mark> stop w32time Windows-Zeitgeber wird beendet. Windows-Zeitgeber wurde erfolgreich beendet.		^
PS C:\> w32tm /config /syncfromflags:manual /manualpeerlist:de.pool.ntp.org Der Befehl wurde erfolgreich ausgeführt. PS C:\> net start w32time Windows-Zeitgeber wird gestartet.		

Dann prüfe ich wieder die Abweichungen. Einige Sekunden passiert nichts. Und dann ist die Zeit vom neuen Server synchron. Leider werden hier viele Fehler ausgegeben:

Administrator: Windows PowerShell				×
PS C:\> w32tm /stripchart /computer:de.pd de.pool.ntp.org wird verfolgt [159.69.144	pol.ntp.org 4.253:123].			^
14:08:24, d:+00.0229245s o:+01.2032955s	r	*	1	
14:08:26, d:+00.0224158s o:+01.2028507s	i i	*	i	
14:08:28, d:+00.0226681s o:+01.2037066s	fi in the second se	*	j	
14:08:30, d:+00.0208721s o:+01.2028855s			j	
14:08:32, d:+00.0206393s o:+01.2021553s	i i i i i i i i i i i i i i i i i i i		i	
14:08:34, d:+00.0232884s o:+01.2039012s	(		]	
14:08:36, d:+00.0221085s o:+01.2032274s	1		]	
14:08:38, d:+00.0238765s o:+01.2016475s	ſ[	*	]	
14:08:40, d:+00.0283335s o:+01.2020742s	1	*	]	
14:08:42, d:+00.0232629s o:+01.2011622s	[	*	]	
14:08:44, d:+00.0270292s o:+01.2026048s	[	*	1	
14:08:46, d:+00.0269709s o:+01.2013362s			1	
14:08:48, d:+00.0257431s o:+01.199894/s		*	1	
14:08:50, d:+00.02414/45 0:+01.19883955				
14:08:52, d:+00.02808005 0:+01.19005075	l		1	
14:08:54, d:+00.02350675 0:+01.20020205			1	
14:08:50, d:+00.341/4525 0:+01.55612625			1	
14:00:01 Eablac: 0x80070584	L		1	
14:09:01, Fehler: 0x80070584				
14:09:07. Fehler: 0x80070584				
14:09:10, d:+00.02200995 o:-00.01100495	r		1	
14:09:12, Fehler: 0x800705B4			1	
14:09:15, Fehler: 0x800705B4				
14:09:18, Fehler: 0x800705B4				
14:09:22, d:+00.0252060s o:-00.0126030s	[		1	
14:09:24, Fehler: 0x800705B4				
14:09:27, Fehler: 0x800705B4				
14:09:30, Fehler: 0x800705B4				
14:09:33, Fehler: 0x800705B4				
14:09:36, Fehler: 0x800705B4				
14:09:39, Fehler: 0x800705B4				
14:09:42, d:+00.0262771s o:-00.0131385s	1		]	
14:09:44, Fehler: 0x800705B4				
14:09:47, Fehler: 0x800705B4				
14:09:50, Fehler: 0x800705B4				
14:09:53, d:+00.0231564s o:-00.0115/82s		*	]	
14:09:56, Fenler: 0x800/0584				
14:09:59, Fenler: 0x80070584				
14:10:02, Fenter: 0X000/0564		*	1	
14:10:05, 0.+00.02004855 0.+00.01002413	L		1	

Vielleicht hat das etwas bei der Konfiguration Probleme verursacht? Ich setze die Einstellungen zurück:



Z Administrator: Windows PowerShell	_	×
PS C:\Windows\system32≻ net stop w32time Windows-Zeitgeber wird beendet.		^
Windows-Zeitgeber wurde erfolgreich beendet.		
PS C:\Windows\system32> <mark>w32tm.exe</mark> /unregister W32Time wurde erfolgreich deregistriert.		
PS C:\Windows\system32> w32tm.exe /register		
PS C:\Windows\system32> net start w32time		
Windows-Zeitgeber wurde erfolgreich gestartet.		
PS C:\Windows\system32> <mark>w32tm</mark> /query /configuration [Konfiguration]		
EventLogFlags: 2 (Lokal)		
TimeJumpAuditOffset: 28800 (Lokal)		
MinPollInterval: 6 (Lokal) MaxPollInterval: 10 (Lokal)		
MaxNegPhaseCorrection: 172800 (Lokal) MaxPosPhaseCorrection: 172800 (Lokal)		
MaxAllowedPhaseOffset: 300 (Lokal)		
FrequencyCorrectRate: 4 (Lokal) PollAdiustFactor: 5 (Lokal)		
LargePhaseOffset: 50000000 (Lokal)		
LocalClockDispersion: 10 (Lokal)		
HoldPeriod: 5 (Lokal) PhaseCorrectRate: 7 (Lokal)		
UpdateInterval: 100 (Lokal)		
[Zeitanbieter]		
NtpClient (Lokal) DllName: C:\Windows\SYSTEM32\w32time.DLL (Lokal)		
Enabled: 1 (Lokal) InputProvider: 1 (Lokal)		
CrossSiteSyncFlags: 2 (Lokal)		
ResolvePeerBackoffMinutes: 15 (Lokal)		
ResolvePeerBackoffMaxTimes: 7 (Lokal) CompatibilityFlags: 2147483648 (Lokal)		
EventLogFlags: 1 (Lokal) LargeSampleSkew: 3 (Lokal)		
SpecialPollInterval: 1024 (Lokal) Type: NT5DS (Lokal)		
NtpServer (Lokal)		
DllName: C:\Windows\SYSTEM32\w32time.DLL (Lokal) Enabled: 1 (Lokal)		
InputProvider: 0 (Lokal) AllowNonstandardModeCombinations: 1 (Lokal)		
VMICTimeProvider (lokal)		
D11Name: C:\Windows\System32\vmictimeprovider.dll (Lokal)		
InputProvider: 1 (Lokal)		~

Sofort ist die Zeit wieder verschoben:

🔀 Administrator: Windows PowerShell			_	×
14:14:32, d:+00.0251306s o:-00.0125653s [	*	]		~
14:14:34, Fehler: 0x800705B4				
14:14:37, Fehler: 0x800705B4				
PS C:\> w32tm /stripchart /computer:de.pool.ntp.org				
de.pool.ntp.org wird verfolgt [213.209.109.44:123].				
Es ist 02.06.2020 14:14:44.				
14:14:44, d:+00.0261667s o:+01.1588124s [		]		
14:14:46, d:+00.0313873s o:+01.1607190s [		]		
14:14:48, d:+00.0295111s o:+01.1593509s [		]		
14:14:50, d:+00.0267471s o:+01.1583601s [		]		
14:14:52, d:+00.0297391s o:+01.1571887s [		]		
14:14:54, d:+00.0276282s o:+01.1567548s [		]		
14:14:56, d:+00.0300676s o:+01.1574096s [		]		
14:14:58, d:+00.0247776s o:+01.1571202s [		]		
14:15:01, d:+00.0249558s o:+01.1567783s [		]		
14:15:03, d:+00.0235330s o:+01.1538630s [		]		
PS C:\>				

Das kann nur eines bedeuten: Der Server WS-DC1 hat noch einen anderen Zeitgeber! Wer in den ersten Bildern dieses Beitrages genau hingeschaut hat, wird das Problem schnell erkennen. Der Übeltäter ist mein Hyper-V-Host. Dieser gibt seine Systemzeit an den virtuellen WS-DC1 weiter. Blöderweise holt er sich als Domain Member von einem DC seine eigene Zeit ab... Die Einstellung kann ich in den Einstellungen der virtuellen Maschine sehen. Ich entferne den Haken:



Datei Aktion Ansicht ?	- Einstellungen für "WS-DC1" auf "WS-HV1	·	×
Image: The second se	WS-DC1       ★ Hardware       Image: Primage intermediation       Yend Termination       Sicherheit       Sicherheit       Sicherheit       2048 MB       Image: Prozessor       4 virtuelle Prozessoren       Image: Sicherheit       Image: Sicherheit	Integrationsdienste     Wählen Sie die Dienste aus, die von Hyper-V für den virtuellen Computer bereitgestellt Wahlen Sie die Dienste aus, die von Hyper-V für den virtuellen Computer bereitgestellt mussen sie vom Gastbetriebssystem unterstützt werden. Zu den Diensten, die unter dem Gastbetriebssystem möglicherweise nicht verfügbar sind, zählen beispielsweise die Volumeschattenkopie-Dienste oder der Dienst zum Herunterfahren des Betriebssystems     Tetronomouseun     Datenaustausch     Tat     Sicherung (Volumeschattenkopie)     Gastdienste	Konfiguratio           8.0           9.0           8.0           9.0           8.0           9.0           8.0           9.0           8.0           9.0           8.0           9.0           8.0           9.0           8.0           9.0           8.0           9.0           8.0           9.0           8.0

Jetzt wiederhole ich die Zeitkonfiguration. Anschließend prüfe ich wieder die Differenz zur öffentlichen Systemzeit:



Mmh, das ist leider der gleiche Fehler wie vorher. Daher nehme ich bei der Konfiguration noch eine Option /Update dazu:

WS IT-Solutions

## WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019

Administrator: Windows PowerShell			_	×
PS C:\> <mark>net</mark> stop w32time Windows-Zeitgeber wird beendet. Windows-Zeitgeber wurde erfolgreich beendet.				î
PS C:\> w32tm /config /syncfromflags:manual /manualpe Folgender Fehler ist aufgetreten: Der Dienst wurde ni PS C:\> net start w32time Windows-Zeitgeber wird gestartet. Windows-Zeitgeber wurde erfolgreich gestartet.	eerlist:de.pool.ntp.org /update icht gestartet. (0x80070426)			
PS C:\> <sup>AC</sup> PS C:\> w32tm /resync Befehl zum erneuten Synchronisieren wird an den lokal Der Befehl wurde erfolgreich ausgeführt. PS C:\> <b>_</b>	len Computer gesendet.			
				¥
🔁 Administrator: Windows PowerShell			_	×
PS C:\> w32tm /stripchart /computer:de.pool.ntp.org de.pool.ntp.org wird verfolgt [185.90.160.100:123]. Fs ist 0 66 2020 14:21-31				^
14:21:31, d:+00.02772755 o:+00.24658845 [	*  -	]		
14:21:33, d:+00.0180/3/s 0:+00.2426116s [ 14:21:36, d:+00.0204282s 0:+00.2407867s [	*  *	i i		
14:21:38, d:+00.0226127s o:+00.2376872s [	*	i		
14:21:40, d:+00.0224171s o:+00.2338762s [	*	]		
14:21:42, d:+00.022/281s o:+00.229/481s [	*  *	ļ		
14:21:46, d:+00.0206832s o:+00.2198983s [	*  *	1		
14:21:48, d:+00.0218926s o:+00.2167615s [	*	j		
14:21:50, d:+00.0219566s o:+00.2118427s [	*	]		
14:21:52, d:+00.0200281s o:+00.2109377s [	*  ↓	]		
14:21:54, d:+00.01898435 0:+00.2060/935 [ 14:21:56 d:+00.02430455 0:+00.20515445 [	*  *	J 1		
14:21:58, d:+00.0204037s o:+00.1985389s	*  *	1		
14:22:00, d:+00.0202930s o:+00.1956697s [	*	j		
14:22:02, d:+00.0211300s o:+00.1930967s [	*	]		
14:22:04, d:+00.0200326s o:+00.1865081s [	*  -	]		
14:22:06, d:+00.022545/s 0:+00.18/9/18s [	*  *	ļ		
14:22:10, d:+00.0193171s o:+00.1818267s	*	1		
14:22:12, d:+00.0187174s o:+00.1780863s [		j		
14:22:14, d:+00.0208919s o:+00.1749209s [		ĵ		
				~

Das wars. Jetzt ist der Server synchron. Und jetzt holen sich die anderen Domain Controller die korrekte Zeit. Das kann einen Moment dauern, da die Zeit schrittweise angepasst wird:

C Administrator: Eingabeaufforderung			- 🗆 X
C:\>w32tm /resync Befehl zum erneuten Synchronisieren wird an den lok Der Befehl wurde erfolgreich ausgeführt.	kalen Computer gesendet.		Â
Eingabeaufforderung - w32tm /stripchart/computer:ws-dc1			– 🗆 🗙
C:\>w32tm /stripchart /computer:ws-dc1 ws-dc1 wird verfolgt [192.168.100.1:123]. Es ist 02.06.2020 14:26:42.			Â
14:26:42, d:+00.0006953s o:+01.1356675s [	*	1	
14:26:44, d:+00.0062543s o:+01.1330107s [	*	j	
14:26:46, d:+00.0008348s o:+01.1362494s [	*	j	
14:26:48, d:+00.0016119s o:+01.1368429s [		]	
14:26:50, d:+00.0007687s o:+01.1365221s [	*	]	
14:26:52, d:+00.0004879s o:+01.1368193s [		]	
14:26:54, d:+00.0008155s o:+01.1370462s [	*	]	
14:26:56, d:+00.0008722s o:+01.1374168s [	*	]	
14:26:58, d:+00.0006978s o:+01.1375306s [	*	]	
14:27:00, d:+00.0006889s o:+01.1247599s [	*	]	
14:27:02, d:+00.0009225s o:+01.1049523s [	*	]	
14:27:04, d:+00.0007418s o:+01.0853079s [	*	]	
14:27:06, d:+00.0006278s o:+01.0660700s [	*	]	
14:27:08, d:+00.0006932s o:+01.0472312s [	*	]	
14:27:10, d:+00.0007851s o:+01.0287091s [	*		
14:27:12, d:+00.0006324s o:+01.0104027s [	*	]	
14:27:15, d:+00.0006808s o:+00.9925000s [	*		
14:27:17, d:+00.0009404s o:+00.9748629s [			
			~



Und auch mein WS-DC3 im anderen Standort gleicht sich an. Hier erkennt man sehr gut die zwei kollidierenden Zeitquellen PDC und Hyper-Visor:

Administrator: C:\Windows\system32\cmd.exe			- <b>D</b> X
C:\>w32tm /resync Befehl zum erneuten Synchronisieren wird an den lokalen C Der Befehl wurde erfolgreich ausgeführt.	omputer gesendet.		^
C:\>			~
Administrator: C:\Windows\system32\cmd.exe - w32tm /stripchart /computer:ws-	·dc1		= <b>D</b> X
14:31:28, d:+00.0291797s o:+01.2647737s [	*	1	^
14:31:30, d:+00.0355820s o:+01.2625612s [		j	
14:31:33, d:+00.0343670s o:+01.2630329s [		j	
14:31:35, d:+00.0300007s o:+01.2660689s [		]	
14:31:37, d:+00.0775265s o:+01.2879666s [	*	<u>]</u>	_
14:31:39, d:+00.03079775 o:+01.26661515	*	]	
14:31:41, d:+00.03135335 0:+01.26668645 [		ļ	_
14:31:43, d:+00.03268/95 0:+01.266/6835 [		ļ	_
14:31:45, 0:+00.03211935 0:+01.27091395 [	*	ļ	
14:31:47, 0:+00.03244995 0:+01.20991815 [		ļ	
14.31.49, $d.+00.03938013$ $0.+01.20020293$ [ 14.31.51 $d.+00.03938013$ $0.+01.20020293$ [		1	
14:31:53, d:+00.03195213 0:+01.27038313 [		ł	_
14:31:55, d:+00.0334900s o:+01.2703876s [		i	_
14:31:57, d:+00.03138855 o:+01.27202985		i	_
14:31:59, d:+00.0297398s o:+01.2732522s [		i	_
14:32:01, d:+00.0295496s o:+01.2737123s [		i	_
14:32:03, d:+00.0336045s o:+01.2724817s [		j	_
14:32:05, d:+00.0311702s o:+01.2749197s [		j	_
14:32:08, d:+00.0343783s o:+01.2736403s [		]	_
14:32:10, d:+00.0311840s o:+01.2773041s [		]	_
14:32:12, d:+00.0314903s o:+01.2756725s [		j	_
14:32:14, d:+00.0290404s o:+01.2777111s [	*	]	_
14:32:16, d:+00.02977985 o:+01.27899365	*	ļ	_
14:32:18, d:+00.03038495 o:+01.27820415	*	ļ	_
14:32:20, d:+00.0310/245 0:+01.2/985515 [		ļ	
14:32:22, d:+00.221/3215 0:+01.18409195 [		ļ	_
14:32:24, 0:+00.03/05405 0:+01.28139045 [	*	ļ	_
14.32.28, d:+00.03632345 0:+01.28001485 [			
14:32:30. Fehler: 0x800705B4			
14:32:33, d:+00.0317232s o:+01.2814765s			
14:32:35, d:+00.0334175s o:+01.2803194s [		j	

Ich rekonfiguriere also die Zeiteinstellung der virtuellen Maschine:

Hyper-V-Manager									
Datei Aktion Ansicht ?									
🗢 🄿 🗾 🖬 🚺 🖬									
Hyper-V-Manager	Virtuelle Computer								
	Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status			Konf
	WS-DC3	Wird ausgeführt	5 %	4096 MB	7.10:42:33				8.0
	Einstellungen f ür "WS-DC:	3" auf "WS-HV3"				_		Х	9.0
	WS-DC3      Hardware     Hardware hinzufügen     Firmware     Von 'Datei" starten     Sicherheit     "Sicherer Start" ist akti     M Arbeitsspeicher	viert	Wählen Sie die D werden sollen. D müssen sie vom Zu den Diensten sind, zählen beis Herunterfahren	vienste	r-V für den virtuel ewählten Dienste v rstützt werden. iebssystem möglich attenkopie-Dienste	en Computer bei rerwendet werde ierweise nicht ve e oder der Dienst	reitgestell: en können, erfügbar t zum	 t	8.0
	4096 MB Prozessor 4 virtuelle Prozessoren SCSI-Controller Festplatte HDD0./hdx		Dienste	ahren des Betriebssyster ronisierung tausch	ns				> •
	Netzwerkkarte     VLANs     Verwaltung		Gastdiens	(volumeschattenkopie) te					lerfrei)

Und nahc wenigen Minuten ist die Uhrzeit synchron:

WS IT-Solutions

## WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019

Administrator: C:\Windows\system32\cmd.exe			- <b>-</b> ×
C:\>w32tm /resync Befehl zum erneuten Synchronisieren wird an den lokal Der Befehl wurde erfolgreich ausgeführt.	en Computer gesendet.		
C:\>			~
Administrator C//Windows/system22).cmd.eva_w22tm_/strinshart/sommu	tornur, del		
Administrator. C. (Windows (system 52 (cind.exe + w52tm / surpenare/compu	ter.ws-dc1		
C:\Users\sysadm>w32tm /stripchart /computer:ws-dc1			
ws-dc1 wird verfolgt [192.168.100.1:123].			
Es ist 02.06.2020 14:34:04.			
14:34:04, d:+00.0349267s 0:+01.2585068s	*	ļ	
14:34:00, 0:+00.03325455 0:+01.23798875 [ 14:34:08 d:+00.03926455 0:+01.21738965 [		4	
14:34:10, d:+00.0310750s o:+01.1949315s [			
14:34:12, d:+00.0310978s o:+01.1740366s [		1	
14:34:14, d:+00.0918414s o:+01.1583256s [		j j	
14:34:16, d:+00.0307344s o:+01.1336128s [		]	
14:34:18, d:+00.0310594s o:+01.1134059s [			
14:34:21, d:+00.0410209s o:+01.0959157s [	*	]	
14:34:23, d:+00.0348601s 0:+01.0/41300s			
14:34:25, 0:+00.03840405 0:+01.05380315 [	*	4	
14:34:29, d:+00.0337152s o:+01.0339307s [		4	
14:34:31, d:+00.0303493s o:+01.0019786s		i .	
14:34:33, d:+00.0442839s o:+00.9775026s		1	
14:34:35, d:+00.0399534s o:+00.9621828s [		j	
14:34:37, d:+00.0309686s o:+00.9505238s [		]	
14:34:39, d:+00.0302245s o:+00.9342535s [			
14:34:41, d:+00.0320286s o:+00.9174455s [	*	]	
14:34:43, d:+00.03327585 0:+00.90081665	*	ļ	
14:34:45, 0:+00.0341/085 0:+00.88/3//85 [ 14:24:48, d:+00.02820865 0:+00.88/3//85 [	*	4	
14.34.50 d+400 0317723s 0.400 8562043s [		f f	

#### TroubleShooting LDAPS

Alle Domain Controller sollten das sichere LDAPS beherrschen. Das kann recht einfach mit LDP.exe getestet werden. Mein neuer Domain Controller hat wohl noch Probleme:

🔝 Ldp					—		×
Verbindung	Durchsuchen	Ansicht	Optionen	Hilfsprogra	mme ?		
	ld = Err 3); Err Ser Err	<ul> <li>Idap_sslini</li> <li>or 0 = Idap_</li> <li>or 81 = Idap</li> <li>rver error: </li> <li>or &lt;0x51&gt;:  </li> </ul>	t("ws-dc1", 6 set_option(hl _connect(hL4 :empty> Fail to connect	36, 1); .dap, LDAP_O dap, NULL); tto ws-dc1.	PT_PROTO	DCOL_VE	RSION,
		Ldp	Verbindun	g kann nicht l	hergestell	t werden	× 1.
						OK	
Fertig							

Das eigentlich Gemeine an dem Problem: Es fällt zunächst nicht auf, wenn noch ein anderer Domain Controller LDAPS anbietet. Die Clients weichen einfach aus. Aber wenn dieser Domain Controller dann mal nicht erreichbar ist bzw. auch migriert wird, dann knallt es richtig. Die Ursache ist einfach: Der DC benötigt ein Zertifikat für LDAPS. Aber er hat kein passendes im Speicher:

🚪 certlm - [Zertifikate - Lokaler Computer\Eigene Zertifikate\Zertifikate]							- 0	×
Datei Aktion Ansicht ?								
🗢 🏟 🖄 📰 📋 🙆 📑	?							
<ul> <li>Zertifikate - Lokaler Computer</li> <li>Eigene Zertifikate</li> <li>Zertifikate</li> <li>Yertrauenswürdige Stammzer</li> <li>Organisationsvertrauen</li> <li>Zwischenzertifizierungssteller</li> </ul>	Ausgestellt für ^ PalWS-DC1	Ausgestellt von WS-ITS-Zertifizierungsstelle-CA1	Ablaufdatum 02.06.2021	Beabsichtigte Zwec Clientauthentifizier	Anzeigename <keine></keine>	Status	Zertifikatvorlage WS-ITS-Computer-\	/2



Merkwürdig. Eigentlich sollte er sich von meiner internen PKI ein Zertifikat basierend auf dieser Vorlage automatisch beziehen:



Ich habe vor einer Weile an den Vorlagen der Zertifikate herumgespielt. Und die Verteilung läuft über einen CEPCES. Das ist ein Webservice, der als Vermittler zwischen Client und Zertifizierungsstelle steht und gesichert über https angesprochen werden kann. Der CEP merkt sich dabei gerne die verfügbaren Informationen der Zertifizierungsstelle in einem Cache. Der sollte eigentlich alle 30 Minuten aktualisiert werden. Ich helfe mal durch einen iisreset nach (der CEPCES läuft natürlich in einem Windows Internet Information Service):



Auch der Client – hier ist es mein Domain Controller – merkt sich die letzte CEP-Antwort in einer Cache-Datei. Diese lösche ich. Dazu sind administrative Rechte erforderlich:



Dann versuche ich es erneut. Das AutoEnrollment meiner Zertifikate wird alle 8 Stunden angetriggert. Aber auch ein gpupdate kann da nachhelfen. Der Domain Controller kontaktiert den CEPCES, lädt sich die Infomationen in seine Cache-Datei herunter, erkennt, dass er ein neues Zertifikat bekommen soll und startet automatisch das Enrollment: WS IT-Solutions

# WSHowTo – Migration eines Domain Controllers auf 2019 (WS-DC11) 2020-06-02 Migration auf Windows Server 2019

🔀 Administrator: Wind	lows PowerShell			_		×		
PS C:\> gpupdate /fo Die Richtlinie wird	orce aktualisiert					^		
Die Aktualisierung (	der Computerricht	linie wurde erfolgreich abgeschlossen.						
Die Aktualisierung ( PS C:\>	der Benutzerricht.	inie wurde erfolgreich abgeschlossen.				~		
X509Enrollment							- 🗆 ×	
$\leftarrow \rightarrow \checkmark \uparrow \square$ > Dieser PC >	System (C:) > Progra	mData > Microsoft > Windows > X509Enroll	ment		~ Ō	"X509	Enrollment" durchsuchen 🔎	
📌 Schnellzugriff	^	Name	Änderungsdatum	Тур	Größe			
Admin		399ad5e6c33ead8eaffa12c03d72afd80be9	02.06.2020 14:02	Datei	12 KI	3		
LAPS-History								
System32								
<b>- N</b> 11	~						_	
1 Element								
🔽 satis (Zatifista dalais Car	······································	t-) Z-difflict-1						~
Datei Aktion Ansicht ?	nputer\Eigene Zertifika	te\Zertifikatej						^
	?							
Zertifikate - Lokaler Compute A     Eigene Zertifikate     Zertifikate     Organisationsvertrauen     Crganisationsvertrauen     Zvischenzertifizierungsste     Vertrauenswürdige Herau:      Vertauenswürdige Herau:	Ausgestellt für	Ausgestellt von WS-ITS-Zertifizierungsstelle-CA1 WS-ITS-Zertifizierungsstelle-CA1	Ablaufdatum 02.06.2021 02.06.2021	Beabsichtigte Zwec Clientauthentifizier KDC-Authentifizier	Anzeig <keine> <keine></keine></keine>	Status	Zertifikatvorlage WS-ITS-Computer-V2 WS-ITS-DomainController-V2	
Der Speicher enthält "Eigene Zertifikate	e" 2 Zertifikate.							

Das sollte eigentlich von alleine passieren. Aber wie so oft gilt bei Automatisierungen: Vertrauen ist gut, Kontrolle ist besser. Jetzt kann der neue Domain Controller auch LDAPS-Anfragen bedienen:



## <u>Zusammenfassung</u>



Mein Active Directory arbeitet jetzt mit dem ersten Windows Server 2019. Funktional hat sich nichts mehr seit dem Windows Server 2016 verändert. Aber ich bin wieder einen Schritt weiter in Richtung Zielgerade. Die verbliebenen Altserver lassen sich nun an einer Hand abzählen.

Wie man sehen konnte, ist der Umstellungsprozess nicht sonderlich schwer. Dennoch gibt es eine Vielzahl von Stolpersteinen und Problemszenarien, auf die man sich vorbereiten sollte.