

<u>Inhalt</u>

Einleitung	2
Zielsetzung	2
Analyse des alten Servers	2
Planung der Migration	5
Schritt 2 - Neuinstallation des Hyper-V-Services	5
Vorbereitung	5
Einbau neue SSD und Neuinstallation als WS-HV3	11
Installation der Rollen und Features	19
Konfiguration von Hyper-V und Migration der VMs	20
Absicherung mit Bitlocker	26
Absicherung mit DUO-2FA	31
Absicherung mit Notfall-Account und vSmartcard	
Konfiguration der Datensicherung – Windows Server Sicherung	43
Konfiguration des Monitoring	48
Einbau und Inbetriebnahme	51
Nacharbeiten	53
Gruppenanpassungen im Active Directory	53
Anpassungen im DFS-Namespace	55



<u>Einleitung</u>

Zielsetzung

Im meinem Außenstandort in Neufahrn habe ich einen Hyper-V-Host mit dem Namen WS-RDS3 aufgestellt. Dieser betreibt die virtuellen Maschinen mit den Services, die ich dort benötige. Der Server läuft aktuell mit Windows Server 2016.

Der Server soll auf Windows Server 2019 umgestellt werden. Dazu sind Anpassungen an den Services notwendig.

Die Umstellung findet in der Zeit des Betriebsurlaubes zwischen den Jahren (zwischen Weihnachten und Silvester) statt. Es kann also mit einer Downtime gearbeitet werden.

Die Hardware soll wiederverwendet werden.

Analyse des alten Servers

Der Server hat eine durchaus bewegte Vergangenheit hinter sich. Ich wollte ursprünglich nur einen Server in dem Standort aufstellen. Meine Kolleginnen sollten darauf alle Dienste und Anwendungen vorfinden, die zum Arbeiten erforderlich sind.

Da die Hardware sehr begrenzt ist (Quadcore, 16GB RAM, 120GB SSD, 1x Gbit) musste ich Dienste auf den Servern zusammenfassen. Auch eine RDP-Anmeldung sollte möglich sein (daher der Name WS-RDS3). Im Nachhinein war das keine so gute Idee. Aber mit dieser Migration kann ich jetzt einige Korrekturen vornehmen.

Zuerst verschaffe ich mir einen Überblick über die installierten Rollen und Features:

💹 Windows PowerShell			_	×	
PS C:\> Get-WindowsFeature where installed					^
Display Name	Name	Install State			
[X] Datei-/Speicherdienste	FileAndStorage-Services	Installed			
[X] Datei- und iSCSI-Dienste	File-Services	Installed			
[X] Dateiserver	FS-FileServer	Installed			
[X] DFS-Namespaces	FS-DFS-Namespace	Installed			
[X] DFS-Replikation	FS-DFS-Replication	Installed			
[X] Ressourcen-Manager für Dateiserver	F5-Resource-Manager	Installed			
[X] Speicherdienste	Storage-Services	Installed			
[X] Druck- und Dokumentalenste	Print-Services	Installed			
[X] bruckerserver	Print-Server	Installed			
[A] nyper-v [Y] NET Enamework 2 E-Eurktionen	NET-Enamework-Eastures	Installed			
[X] NET Framework 3.5-Funktionen [X] NET Enamework 3.5 (anthält NET 2.0 und 3.0)	NET-Framework-Features	Installed			
[X] NET Framework 4.6-Euristionen	NET-Framework-45-Fea	Installed			
[X] NET Framework 4.6	NET-Enamework-45-Cone	Installed			
[X] WCE-Dienste	NET-WE-Services45	Installed			
[X] TCP-Portfreigabe	NET_WCE_TCP_PortShar	Installed			
[X] Bitlocker-Laufwerkverschlüsselung	Bitlocker	Installed			
[X] Erweitertes Sneichern	EnhancedStorage	Installed			
[X] Remoteserver-Verwaltungstools	RSAT	Installed			
[X] Featureverwaltungstools	RSAT-Feature-Tools	Installed			
[X] Verwaltungshilfsprogramme für die BitLoc	. RSAT-Feature-Tools-B	Installed			
[X] BitLocker-Wiederherstellungskennwort	RSAT-Feature-Tools-B	Installed			
[X] Tools zur BitLocker-Laufwerkverschlü	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-Modul für Windows P	. RSAT-AD-PowerShell	Installed			
[X] AD DS-Tools	RSAT-ADDS	Installed			
[X] AD DS-Snap-Ins und -Befehlszeile	. RSAT-ADDS-Tools	Installed			
[X] Hyper-V-Verwaltungstools	RSAT-Hyper-V-Tools	Installed			
[X] Hyper-V-GUI-Verwaltungstools	Hyper-V-Tools	Installed			
[X] Hyper-V-Modul für Windows PowerShell	Hyper-V-PowerShell	Installed			
[X] DHCP-Servertools	RSAT-DHCP	Installed			
[X] DNS-Servertools	RSAT-DNS-Server	Installed			
[X] Tools für Dateidienste	RSAT-File-Services	Installed			
[X] DFS-Verwaltungstools	RSAT-DFS-Mgmt-Con	Installed			
[X] Tools für den Ressourcen-Manager für	. RSAT-FSRM-Mgmt	Installed			
[X] Tools für Druck- und Dokumentdienste	RSAT-Print-Services	Installed			
[X] Unterstutzung für die SMB 1.0/CIFS-Dateifreigabe	FS-SMB1	Installed			
[X] Windows Defender-Features	Windows-Defender-Fea	Installed			
[X] Windows Defender	Windows-Defender	Installed			
[X] Gui Tur Windows Detender	Windows-Detender-Gui	Installed			
[X] Windows PowerShell 5 1	PowerShell	Installed			
[X] Windows PowerShell 5.1	PowerShell V2	Installed			
[X] Windows PowerShell 2.0 Engine	PowerShell_TSC	Installed			
[X] Windows Server-Sicherung	Windows-Server-Backup	Installed			~
[A] windows Server-Stcherung	withdows-server-backup	Instanted			T

Der Server ist also ein Hyper-V-Host, ein Fileserver mit DFS-Namespace und DFS-Replica, und der lokale Druckserver.

Über Hyper-V werden diese beiden VMs bereitgestellt: ein Domain Controller mit DHCP und DNS und eine virtuelle PFSense (Firewall):

WS IT-Solutions

Hyper-V-Manager							
Datei Aktion Ansicht ?							
🗢 🔿 🗖 🖬 👔 🖬							
Hyper-V-Manager WS-RDS3	Virtuelle Computer						
	Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status	Konfig
	WS-DC3	Wird ausgeführt	8 %	4096 MB	15.04:01:04		8.0
	WS-PFS2	Wird ausgeführt	0 %	4096 MB	15.04:01:17		8.0

Alle Freigaben musste ich direkt auf die Systempartition ablegen – genauso auch die Dateien der virtuellen Maschinen. Für eine zusätzliche Partitionierung war einfach kein Platz mehr:

🚡 Server	-Manager			
$ \mathbf{E} $	∋ ▼ Server-N	√anager ∙ Date	i-/Speicherdienste • Freigaben	
	Server	FREIGABEN Alle Freigaben I 1	0 insgesamt AUFGA	BEN -
i ii	Volumes Datenträger	Filter	► (B) ▼	۲
	Speicherpools	Freigabe	Lokaler Pfad	Protokoll
÷	Freigaben	 WS-RDS3 (10) 		
B	iSCSI	Benutzerordner\$	C:\Admin\Hyper-V\FileServer\Benutzerordner	SMB
	Arbeitsordner	Benutzerprofile\$	C:\Admin\Hyper-V\FileServer\Benutzerprofile	SMB
		BMR-RDS3\$	E:\Backup\ServerSicherung	SMB
		DAG-1.ws.its	C:\Admin\DAG-Witness	SMB
		Freigaben	C:\Admin\Hyper-V\FileServer\DFS-Roots\Freigaben	SMB
		intern	C:\Admin\Hyper-V\FileServer\DFS-Roots\Intern	SMB
		Jungbrunnen\$	C:\Admin\Hyper-V\FileServer\Jungbrunnen	SMB
		Jungbrunnen-CRM\$	C:\Jungbrunnen-CRM	SMB
		MTATempStore\$	C:\Program Files\Microsoft Data Protection Manager\D	SMB
		print\$	C:\Windows\system32\spool\drivers	SMB

Nur eine weitere Festplatte ist noch über USB angeschlossen. Auf dieser werden Datensicherungen gespeichert. Auf dem Systemdatenträger ist kaum noch freier Platz vorhanden:



Vielleicht wird Speicherplatz durch nicht mehr benötigte Dateien belegt? Ich starte die Datenträgerbereinigung und durchsuche dabei auch Systemverzeichnisse. Naja, besser als Nichts:



Aligemein Tools Hardware Freigabe Sid Datenträgerbereinigung für system (C.) System	cin indssilizie	100	
System Typ: Lokaler Datenträger Datenträgerbereinigung Wetere Optionen Typ: Lokaler Datenträger Datenträgerbereinigung Durch das Bereinigen des Datenträgers können bis zu 6,88 GB Speicherplatz auf System (C.) freigegeben werden. Belegter Speicher: 92.301.369.344 Freier Speicher: 27.138.772.992 Speicherkapazität: 119.440.142.336 Laufwerk C: Bereinig Laufwerk komprimieren, um Speicherplatz zu sparen 2.2. Jassen, das für Dateien auf desem Laufwerk Irhalte zusätzlich zu Dateieigenschaften indiziet werden Wet funktioniert de Datenträgerbereinigung?	Freigabe Sic 🚔 Dat	tem (C:)	
System Typ: Lokaler Datenträger Dateisystem: NTFS Belegter Speicher: 92.301.369.344 85.9 GB Freier Speicher: 27.138.772.992 25.2 GB Speicherkapazität: 119.440.142.336 111 GB Laufwerk Komprimieren, um Speicherplatz zu sparen 2 Juassen, dass für Dateien auf desem Laufwerk Inhalte zusätzlich zu Dateieigenschaften indiziett werden 0.88 GB Speicherplatz auf System (C.) freigegeben wird: 2. Laufwerk komprimieren, um Speicherplatz zu sparen 2 Juassen, dass für Dateien auf desem Laufwerk Inhalte zusätzlich zu Dateieigenschaften indiziett werden We funktioniert die Datenträgerbereinigung?	Datent	tionen	
Typ: Lokaler Datenträger Dateisystem: NTFS Belegter Speicher: 92.301.369.344 85.9 GB Freier Speicher: 27.138.772.992 25.2 GB Speicherkapaztät: 119.440.142.336 111 GB Laufwerk C: Bereing Laufwerk C: Bereing Zulassen, dass für Dateien auf diesem Laufwerk inhalte zusätzlich zu Dateieigenschaften indiziet werden Windows erstellte Datei Windowsierstellte Datei Windows erstellte Datei		Datenträgers können bis zu	
Typ: Lokaler Datenträger Dateisystem: NTFS ■ Belegter Speicher: 92.301.369.344 85.9 GB ■ Freier Speicher: 27.138.772.992 25.2 GB Speicherkapaztät: 119.440.142.336 111 GB Laufwerk C: Bereino Laufwerk C: Bereino 2. Laufwerk komprimieren, um Speicherplatz zu sparen 2. Jusastende Auss für Dateieigenschaften indiziert werden		System (C:) freigegeben	
Dateisystem: NTFS Deteisystem: NTFS Belegter Speicher: 92.301.369.344 85.9 GB Freier Speicher: 27.138.772.992 25.2 GB Speicherkapazität: 119.440.142.336 111 GB Laufwerk C: Bareing Laufwerk C: Bareing Laufwerk C: Bareing Uastrophysical Content of Cont	Zulö		
Belegter Speicher: 92.301.369.344 85.9 GB Freier Speicher: 27.138.772.992 25.2 GB Speicherkapazitä: 119.440.142.336 111 GB Laufwerk C: Bereing Laufwerk C: Bereing Zulassen, das für Dateien auf diesem Laufwerk Inhalte Zulassen, das für Dateien auf diesem Laufwerk Inhalte We funktioniert die Datenträgerbereinigung?	2010		-
Freier Speicher: 27.138.772.992 25.2 GB Image: Constraint of the second of the s	69.344 85.9 GB	9,99 Ki	
Speicherkapazität: 119.440.142.336 111 GB 7,33 I Laufwerk C: Bereinig Beschreibung 6, Laufwerk Komprimieren, um Speicherplatz zu sparen Zulassen, dass für Dateieligenschaften indiziert werden Wei funktioniert die Daterträgerbereinigung?	772 992 25 2 GB	ndateien 0 Byte	
Speicherkapazität: 119.440.142.336 111 GB Image: Constraint of the second		7.33 MI	3
Laufwerk komptimieren, um Speicherplatz zu sparen Zulassen, dass für Dateien auf diesem Laufwerk Inhalte zusätzlich zu Dateieigenschaften indiziert werden Wie funktioniert die Datenträgerbereinigung?	42.336 111 GB	1.06 MI	3
Laufwerk komprimieren, um Speicherplatz zu sparen Zulassen, dass für Dateien auf diesem Laufwerk Inhalte zusätzlich zu Dateieigenschaften indiziert werden Wie funktioniert die Datenträgerbereinigung?	Speid	6.8	G
Laufwerk C: Bereing Laufwerk komprimieren, um Speicherplatz zu sparen Zulassen, dass für Dateien auf desem Laufwerk Inhalte Zusätzlich zu Dateieigenschaften indiziert werden Wie funktioniert die Datenträgerbereinigung?	Ber	0,01	-
Laufwerk C: Bereing Laufwerk komprimieren, um Speicherplatz zu sparen Zulassen, dass für Dateien auf diesem Laufwerk Inhalte zusätzlich zu Dateieigenschaften indiziert werden Wie funktioniert die Datenträgerbereinigung?	Vor		
Laufwerk komprimieren, um Speicherplatz zu sparen Zulassen, dass für Dateien auf diesem Laufwerk inhalte zusätzlich zu Dateieigenschaften indiziert werden Wie funktioniert die Datenträgerbereinigung?	Bereinig		
Laufwerk komprimieren, um Speicherplatz zu sparen Zulassen, dass für Dateien auf diesem Laufwerk Inhalte zusätzlich zu Dateieigenschaften indiziert werden Wie funktioniert die Datenträgerbereinigung?			
Laufwerk komprimieren, um Speicherplatz zu sparen Zulassen, dass für Dateien auf diesem Laufwerk Inhalte zusätzlich zu Dateieigenschaften indiziert werden Wie funktioniert die Datenträgerbereinigung?			
Zulassen, dass für Dateien auf diesem Laufwerk Inhalte zusätzlich zu Dateieigenschaften indiziert werden Wie funktioniert die Datenträgerbereinigung?	rplatz zu sparen		
zusätzlich zu Dateielgenschaften indiziert werden Wie funktioniert die Datenträgerbereinigung?	m Laufwerk Inhalte		
Wie funktioniert die Datenträgerbereinigung?	liziert werden		
The fail and the back and below and the	Wief	inigung?	
OK Ab		OK Abb	ed
OK Ab		OK Abbi	e

Warum ich nicht einfach eine weitere Festplatte einbaue? Ganz einfach: der Server ist eigentlich ein Mini-PC. Der kann nur eine 2,5"-Festplatte aufnehmen. Und mit externen Datenträgern möchte ich nicht in Kombination mit virtuellen Maschinen arbeiten.

Wie sieht es denn mit den anderen Ressourcen aus? Der Arbeitsspeicher ist noch etwas belastbarer. Aber eine Aufrüstung ist nicht möglich. Alle Slots sind belegt:



Ich durchsuche die installierten Anwendungen. Lokal ist ein Office 2016 vorhanden. Dieses war für den RDP-Zugriff gedacht, wird aber nicht (mehr) benutzt. Die Anmeldung ist mit DUO-Zweifaktor-Authentifizierung abgesichert. Und für eine spezielle Dateisicherung ist ein DPM-Agent installiert

Als weitere Besonderheit ist das Feature Bitlocker konfiguriert. Damit wird die gesamte SSD verschlüsselt.

Und zusätzlich habe ich meinen Exchange-Servern ein DAG-Witness-Share auf dem Server bereitgestellt.

In der Rolle Printserver ist nur ein Drucker freigegeben. Diese Freigabe hatte aber immer wieder Probleme und daher wird der Drucker von den Clients direkt angesprochen. Die Rolle wird nicht mehr verwendet.

Planung der Migration

Wenn ich die erforderlichen Services um die nicht mehr benötigten bereinige, dann verbleiben die Rollen Hyper-V und der Fileservice. Diese beiden haben keinen Bezug zueinander und sollten daher auch nicht in einem Betriebssystem konsolidiert sein. Daher werde ich den Server **WS-RDS3** durch die Server **WS-FS3** und **WS-HV3** ersetzen. WS-FS3 wird dabei als neue VM unter WS-HV3 laufen und zusammen mit den Freigaben auch den DFS-Namespace und die DFS-Replikation bereitstellen.

Die zusätzliche VM kann mit dem verbleibenden Arbeitsspeicher gut auskommen. Für die CPU und die Netzwerkkarte sehe ich keine Engpässe.

Aber die derzeitige SSD wird mit 120GB nicht mehr ausreichen. Daher werde ich die SSD durch eine neue ersetzen. Eine SSD mit 500GB sollte hier bis zum Ende der Hardwarelaufzeit genügen. Dies spielt mir auch beim Migrieren der VMs positiv zu, denn so muss ich die VMs im Vorfeld nicht erst verschieben. Ich werde nach der Installation des WS-HV3 auf der neuen SSD einfach die alte SSD über USB anschließen und die VMs kopieren.

Die Migration der Server wird in 2 Schritten erfolgen:

- Zuerst separiere ich den Fileservice auf eine neue VM. Damit kann ich auch die Lieferzeit der neuen SSD überbrücken, auch wenn es sehr eng auf der alten SSD werden wird.
- Im zweiten Schritt wird der Server dann als WS-HV3 neu installiert.

Schritt 2 - Neuinstallation des Hyper-V-Services

<u>Vorbereitung</u>

Die Herauslösung des Fileservices ist abgeschlossen. Damit stellt der Server WS-RDS3 nur noch den Service Hyper-V zur Verfügung. Aktuell läuft er mit Windows Server 2016. In diesem Schritt wird er als Windows Server 2019 neu installiert.

WS-RDS3 steht in meinem Außenstandort in Neufahrn Niederbayern. Dort ist er als Hyper-V-Host allein. Es gibt also keine weiteren Systeme, welche den Betrieb aufrechterhalten könnten. Das ist aber im Betriebsurlaub auch nicht erforderlich. Daher kann ich die Neuinstallation einfach vornehmen und die virtuellen Maschinen dabei ausgeschaltet lassen.

Der Server ist recht kompakt. Seine Hardware ist für den aktuellen Einsatz ausreichend. Nur die SSD ist mit 120GB Größe sportlich vollgelaufen. Daher werde ich diese für die durch eine größere erneuern. Das vereinfacht die Migration, da ich die VMs auf der alten Platte nicht verschieben muss. Ich schließe die alte Platte einfach später mit USB an und kopiere die VMs.

Den Umbau kann und möchte ich nicht im Außenstandort vornehmen. Daher modifiziere ich im ersten Schritt die Netzwerkkonfiguration des Servers. Aktuell ist nur eine Netzwerkkarte verbaut. Diese wird von den VMs und dem Hypervisor verwendet. Dennoch habe ich mein Netzwerk mit VLANs segmentiert. Die VLANs unterscheiden sich dabei natürlich von meinen im Hauptstandort. In Neufahrn verwenden die Server das VLAN 101:



Hyper-V-Manager				- 🗆 🗙
Datei Aktion Ansicht ?				
🗢 🔿 🙍 🖬 🚺 🖬				
Hyper-V-Manager	[Aktionen	
WS-RDS3	Virtuelle Computer		WS-RDS3	^
	Name Manager für virtuelle Switch	hes für "WS-RDS3"	- 🗆 X	•
	WS-FS3 WS-PFS2	rkswitch Name:	^	
	Intel(R) Ethernet Conne	ection I217 VLAN-101		
	Globale Netzwerkeinstel	llungen Anmerkung:		
	< MAC-Adressbereich 00-15-5D-64-AA-00 bis	00-15-5D	~	
	Prüfpunkte			
	WS-DC3	Verbindungstyp Womit sol dieser virtuelle Switch verbunden we Externes Netzwerk: Intel(R) Ethernet Connection 1217-LM Gemeinsames Verwenden dieses Netzw Verwaltungsbetriebssystem zulassen SR-IOV (Single-Root 1/O Virtualization) ; Internes Netzwerk Privates Netzwerk VLAN-LD	erden?	,
	Zusammenfae	Identifizierung virtueller LANs für das Verwaktiveren Mit der VLAN-ID wird das virtuelle LAN angegeb Verwalkungsbetriebssystem für die gesamte, ul abgewickelte Netzwerkkommunikation verwend sich nicht auf das Netzwerkk für virtuelle Compu 101 SR-IOV kann nur beim Erstellen des virtueller	altungsbetriebssystem ven, das vom ber diesen Netzwerkadapter et wird. Diese Einstellung wirkt ter aus. Entfermen a Switchs konfiguriert werden. Ein v	
		ОК	Abbrechen Anwenden	

Diese Konfiguration nehme ich raus, damit ich daheim ungetagged anschließen kann:

🔶 🔿 🖄 📰 🔯 📷		[
WS-RDS3	Virtuelle I Manager für virtuelle Switches für "WS-RI	DS3" — 🗆	×
	WS-D ★ Virtuelle Switches WS-F: ♣ Neuer virtueller Netzwerkswitch WS-P: ➡ VAN-101	Zu Eigenschaften für virtuellen Switch	- ^
	Intel(R) Ethernet Connection	VLAN-101	
	MAC-Adressbereich 00-15-5D-64-AA-00 bis 00-15-5D Prüfpunl	Anmerkung:	
		Verbindungstyp Womit soll dieser virtuelle Switch verbunden werden?	τ.
		Intel(R) Ethernet Connection I217-LM $$\sim$$	
	WS-DC3	Gemeinsames Verwenden dieses Netzwerkadapters für das Verwaltungsbetriebssystem zulassen SR-IOV (Single-Root I/O Virbualization) aktivieren Internes Netzwerk Privates Netzwerk	
		VLAN-ID Identifizierung virtueller LANs für das Verwaltungsbetriebssystem aktivieren Mit der VLAN-ID wird das virtuelle LAN angegeben, das vom	it.

Dazu stelle ich die statische Konfiguration für IPv4 auf dynamisch um. So bekommt der Server daheim eine IP-Adresse vom DHCP und ist im Netz administrierbar:



Organisieren 👻 Netzwerkgerät deaktivieren Verbind	g untersuchen Verbindung umbenennen Status der Verbindung anzeigen »	
Ethernet Aktiviert Intel(R) Ethernet Connection 1217	Internet (VLAN-101) Status von vEthernet (VLAN-101) Ilger Ilger Netzwerk Verbindung herstellen über: IF Intemetprotokoll, Version 4 (TCP/IPv4)	oll, Version 4 (TCP/IPv4) × ach zugewiesen werden, wenn das tzt. Wenden Sie sich andernfälls an den eigneten IP-Einstellungen zu beziehen. den den: 192.168.101.2 255.255.0 192.168.101.2 255.255.0 192.168.101.1 1 192.168.101.1 1 192.168.100.1 1 überprüfen Erweitert

Jetzt fahre ich alle VMs herunter. Danach kann ich den Server WS-RDS3 selbst herunterfahren und abbauen. Wenig später ist der Server daheim ans Servernetz angeschlossen und hochgefahren. Wie erwartet hat er nun eine IPv4-Konfiguration aus meinem heimischen Servernetz:

anisisten w			
Janisieren 🕈			
Ethernet	vEthernet (VLAN-101)		
Intel(R) Ethernet Connection 1217	Hy Status von vEther	net (VLAN-101) X	
	Allgemein	Netzwerkverbindungsdetails ×	
	Verbindung	Netzwerkverbindungsdetails:	
	IPv4-Konnektivitä IPv6-Konnektivitä Medienstatus: Dauer: Übertragungsrate Details Aktivität	Bgenschaft Weit ▲ Verbindungsspezfisches ws.ts Beschreibung Hyper-Virtual Ethemet Adapter Physische Adresse 90:18-0E-1F-F1-EE DHCP-aktiviert Ja IPv4-Adresse 192:168:100.150 IPv4-Adresse 192:168:100.150 IPv4-Adresse 192:168:100.252 IPv4-DHCP-Server 192:168:100.2 IPv4-DHCP-Server 192:168:100.1 IPv4-DHCP-Server 192:168:100.1	
	Pakete:	IPv4-WINS-Server NetBIOS über TCPIP ak Ja	
	Eigenschaften	Verbindungsokale IPV6 redutt9033/deb //4c/fte491%8 IPv6-Standardgateway IPv6-DNS-Server fec0:0:0ffff::1%1 v	
		Schließen	

Es geht weiter mit der Sichtung der Bestandskonfiguration. Damals habe ich aus Kapazitätsgründen die virtuellen Maschinen direkt auf die C-Partition gelegt. Das hat nur Nachteile. Aber heute werde ich es richten. Ebenso liegt hier der Ordner mit den Freigaben – bis vor wenigen Tagen war WS-RDS3 ja noch selber der Fileserver (so konnte ich mir eine virtuelle Maschine und deren Platz sparen): WS IT-Solutions

WSHowTo – Neuinstallation von WS-RDS3 als WS-HV3 2020-01-01 Migration auf Windows Server 2019



Demnach sind natürlich etliche Rollen und Funktionen auf dem kleinen Server installiert:

Z Administrator: Windows PowerShell			-	×
PS C:\> Get-WindowsFeature where installed				^
Display Name	Name	Install State		
[X] Datei-/Speicherdienste	FileAndStorage-Services	Installed		
[X] Datei- und iSCSI-Dienste	File-Services	Installed		
[X] Dateiserver	FS-FileServer	Installed		
[X] DFS-Namespaces	FS-DFS-Namespace	Installed		
[X] DFS-Replikation	FS-DFS-Replication	Installed		
[X] Ressourcen-Manager für Dateiserver	FS-Resource-Manager	Installed		
[X] Speicherdienste	Storage-Services	Installed		
[X] Druck- und Dokumentdienste	Print-Services	Installed		
[X] Druckerserver	Print-Server	Installed		
[X] Hyper-V	Hyper-V	Installed		
[X] .NET Framework 3.5-FUNKTIONEN	NET-Framework-Features	Installed		
[X] NET Framework 5.5 (enthalt .NET 2.0 und 5.0)	NET-Framework-Core	Installed		
[X] NET Framework 4.6-Funktionen	NET Framework 45 Care	Installed		
[X] WET Pramework 4.6	NET-Framework-45-Core	Installed		
[X] WCF-Dienste	NET-WCF-SerVices45	Installed		
[X] TCP-Portireigabe [X] Bitlockon Laufwankuonschlüsselung	PitLockon	Installed		
[X] BILLOCKER-Laurwerkverschrusserung	EnhancedStonage	Installed		
[X] Erweitertes Speichern	DEAT	Installed		
[X] Kenoleser ver -ver wartungstools	RSAT_Feature_Tools	Installed		
[X] Verwaltungstüdis	PSAT-Feature-Tools-R	Installed		
[X] Bitlocker-Wiederberstellungskennwort	PSAT-Feature-Tools-B	Installed		
[X] Tools zur Bitlocker-Laufwerkverschlü	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-Modul für Windows P	RSAT-AD-PowerShell	Installed		
[X] AD DS-Tools	RSAT-ADDS	Installed		
[X] AD DS-Snap-Ins und -Befehlszeile	RSAT-ADDS-Tools	Installed		
[X] Hyper-V-Verwaltungstools	RSAT-Hyper-V-Tools	Installed		
[X] Hyper-V-GUI-Verwaltungstools	Hyper-V-Tools	Installed		
[X] Hyper-V-Modul für Windows PowerShell	Hyper-V-PowerShell	Installed		
[X] DHCP-Servertools	RSAT-DHCP	Installed		
X1 DNS-Servertools	RSAT-DNS-Server	Installed		
[X] Tools für Dateidienste	RSAT-File-Services	Installed		
[X] DFS-Verwaltungstools	RSAT-DFS-Mgmt-Con	Installed		
[X] Tools für den Ressourcen-Manager für	RSAT-FSRM-Mgmt	Installed		
[X] Tools für Druck- und Dokumentdienste	RSAT-Print-Services	Installed		
[X] Unterstützung für die SMB 1.0/CIFS-Dateifreigabe	FS-SMB1	Installed		
[X] Windows Defender-Features	Windows-Defender-Fea	Installed		
[X] Windows Defender	Windows-Defender	Installed		
[X] GUI für Windows Defender	Windows-Defender-Gui	Installed		
[X] Windows PowerShell	PowerShellRoot	Installed		
[X] Windows PowerShell 5.1	PowerShell	Installed		
[X] Windows PowerShell 2.0 Engine	PowerShell-V2	Installed		
[X] Windows PowerShell ISE	PowerShell-ISE	Installed		
[X] Windows Server-Sicherung	Windows-Server-Backup	Installed		
[X] WoW64-Unterstützung	WoW64-Support	Installed		

Die SSD mit dem Betriebssystem ist mit Bitlocker verschlüsselt. Damit ich später die VMs via USB auf den neuen Server kopieren kann, halte ich die Verschlüsselung an. Dabei bleibt der eigentliche Inhalt der SSD verschlüsselt. Aber der dazu verwendete Schlüssel liegt jetzt unverschlüsselt auf dem Volume. Daher geht diese Aktion auch schön schnell:

WS IT-Solutions



Ich prüfe noch, welche Anwendungen auf dem Server installiert sind. Davon benötige ich fast alles nicht länger:



← → < ↑	rung > Programme > Programme und Features			~	Dre gramme u		
Startseite der Systemsteuerung	Programm deinstallieren oder ändern				PIDDIATITIP III	nd Features" d	Q
Startseite der Systemsteuerung	Programm deinstallieren oder ändern				0 Hogiannic a	iar catares a	~
Statistic del Systemsteactury	5						
Installierte Updates anzeigen	Wählen Sie ein Programm aus der Liste aus, und klicke	n Sie auf "Deinstallieren", "Ändern" o	oder "Reparieren	n", um es zu dei	nstallieren.		
Windows-Features aktivieren oder deaktivieren							
Programm vom Netzwerk	Organisieren 👻						?
N	lame	Herausgeber	Installiert am	Größe	Version		
ð	🖗 AMD Catalyst Install Manager	Advanced Micro Devices, Inc.	30.04.2017	23,0 MB	8.0.916.0		
•	Duo Authentication for Windows Logon x64	Duo Security, Inc.	30.04.2017	7,41 MB	3.0.0.85		
3	FRITZ!Box-Fernzugang einrichten	AVM Berlin	13.01.2018	1,77 MB	1.0.3		
	hMailServer 5.6.7-B2425		06.11.2018	11,2 MB			
2	Local Administrator Password Solution	Microsoft Corporation	30.04.2017	258 KB	6.2.0.0		
0	Microsoft Office Professional Plus 2016 - de-de	Microsoft Corporation	14.12.2019	1,21 GB	16.0.12228.20364		
6	Microsoft SQL Server Compact 3.5 ENU	Microsoft Corporation	06.11.2018	5,38 MB	3.5.5386.0		
	Microsoft System Center DPM Protection Agent	Microsoft Corporation	16.08.2019	553 MB	10.19.58.0		
	Microsoft Visual C++ 2008 Redistributable - KB24671	Microsoft Corporation	13.01.2018	3,93 MB	9.0.30729.5570		
	Microsoft Visual C++ 2008 Redistributable - x86 9.0.3	Microsoft Corporation	24.05.2019	3,29 MB	9.0.30729.6161		
t ti	Microsoft Visual C++ 2012 Redistributable (x64) - 11.0	Microsoft Corporation	02.05.2017	20,5 MB	11.0.51106.1		
t i	Microsoft Visual C++ 2012 Redistributable (x86) - 11.0	Microsoft Corporation	30.04.2017	17,3 MB	11.0.50727.1		
t t	Microsoft Visual C++ 2013 Redistributable (x64) - 12.0	Microsoft Corporation	31.05.2017	20,5 MB	12.0.40649.5		
•	Mozilla Firefox 68.0.2 (x64 de)	Mozilla	26.08.2019	181 MB	68.0.2		
i i i i i i i i i i i i i i i i i i i	🖄 Mozilla Maintenance Service	Mozilla	09.08.2018	278 KB	61.0.2		
	PDF-Viewer	Tracker Software Products Ltd	15.07.2017	32,9 MB	2.0.53.0		
	phonostar-Player Version 3.03.9		30.04.2017	46,1 MB			
<u> </u>	PowerChute Personal Edition 3.0.2	Schneider Electric	24.06.2018	172 MB	3.0.2		
1	Samsung Printer Live Update	Samsung Electronics Co., Ltd.	30.04.2017		1.01.00.04		
1	Samsung Universal Print Driver 2 PCL6	Samsung Electronics Co., Ltd.	01.05.2017		2.50.04.00		
E	TeamViewer 12	TeamViewer	31.12.2019		12.0.224043		
(WinPcap 4.1.3	Riverbed Technology, Inc.	31.05.2017		4.1.0.2980		
A	Wireshark 2.2.6 (64-bit)	The Wireshark developer comm	31.05.2017	170 MB	2.2.6		
	Momentan installierte Programme Gesam	taröße: 2.45 GB					
	23 Programm(e) installiert						

In der Konsole Aufgabenplanung prüfe ich auf Konfigurationen. Vielleicht ist ja hier noch was Brauchbares dabei? Der Task "Restart-NLA" ist interessant. Daher exportiere ich diesen.

(2) Aufgabenplanung	– 🗆 X
Datei Aktion Ansicht ?	
O Aufgabenplanung (Lokal) Name Status Trigger	Aktionen
Aufgabenplanungsbibliot @ OneDrive Standalone Update Task v2 Bereit Um 04:00 Uhr am 01.05,1992 - Nach Auslösung alle 1.00:00:00 unb	Aufgabenplanungsbibliothek 🔺 🖌
Restart-NLA Bereit Beim Systemstart	Einfache Aufgabe erstellen
ServerSicherung Bereit Jeden Tag um 01:00 Uhr	Aufgabe erstellen
	Aufgabe importieren
	Alle aktiven Aufgaben anzeigen
	Verlauf für alle Aufgaben deaktivieren
Allgemein Trigger Aktionen Bedingungen Einstellungen Verlauf	Neuer Ordner
Name: ServerSicherung	Ansicht
Sneicharort	Aktualisieren
Autor WSteenban-ad	👔 Hilfe
Beschreibung:	Ausgewähltes Element
	Ausführen
	Beenden
	Deaktivieren
Cichada iterationa	Exportieren
	• Eigenschaften
Beim Austunren der Aufgaben toigendes benutzerkonto verwenden:	🗙 Löschen
	The second secon

Natürlich lief hier auch mein Printservice drauf. Der hat aber immer wieder Probleme verursacht. Daher habe ich den Client direkt mit dem Netzwerkdrucker verbunden. Man sieht immer noch die alten Druckjobs:

WS IT-Solutions

Druckverwaltung	Druckemame		Warteschl	lange Au	iftrā Seniername	Treihern	ame	Aktionen		
🖗 Benutzerdefinierte Filter	Microsoft Print t	DDE	Poreit	ange Au	WS-PDS2 (loka) Microro	ft Drint To DDE	Drusker		
Druckerserver	Samsung Univer	sal Print Driver	Fehler	5	5 WS-RDS3 (lokal) S) Samsuni	n Universal Print Driver 2	Drucker		
V 📱 WS-RDS3 (lokal)	Send To OneNot	te 2016	Bereit 0	0 WS-RDS3 (lokal) Se) Send to	Microsoft OneNote 16 E	Weitere Aktionen			
> 🗰 Treiber					110 110 00 (1010	,		Samsung Universal Prir	nt Driver 2 PCL6	
> 🚰 Formulare								Weitere Aktionen		
Drucker										
🚃 Bereitgestellte Drucker										
Sameung Universal Brint Driver	2 0 0 1 6							_		1
Samsung Universal Print Driver	2 PCL6							-]
Samsung Universal Print Driver Drucker Dokument Ansicht	2 PCL6	1			~			-	D X	
Samsung Universal Print Driver Drucker Dokument Ansicht Dokumentname	2 PCL6 Status	Besitzer	Seiten (Größe	Gesendet	Ar	nschluss	-		1
Samsung Universal Print Driver Drucker Dokument Ansicht Dokumentname Microsoft Word - 2018-05-23	2 PCL6 Status	Besitzer stephan	Seiten (Größe 363 KB	Gesendet 10:39:10 11.08.20	Ar 18	ischluss	-		
Samsung Universal Print Driver Drucker Dokument Ansicht Dokumentname Microsoft Word - 2018-05-23 Microsoft Word -	Status	Besitzer stephan stephan	Seiten 4 2	Größe 363 KB 3,71 MB	Gesendet 10:39:10 11.08.20 10:38:38 11.08.20	An 18 18	nschluss	-		
Samsung Universal Print Driver Drucker Dokument Ansicht Dokumentname Microsoft Word - 2018-05-23 Microsoft Word - Samsung Microsoft Word - 2016-06-30	Status	Besitzer stephan stephan stephan	Seiten (4 2 2 2	Größe 363 KB 3,71 MB 338 KB	Gesendet 10:39:10 11.08.20 10:38:38 11.08.20 10:38:28 11.08.20	Ar 18 18 18	nschluss	-		
Samsung Universal Print Driver Drucker Dokument Ansicht Dokumentname Microsoft Word - 2018-05-23 Microsoft Word - 2016-06-30 Microsoft Word - 2016-06-30 Microsoft Word - 2017-01-15 Microsoft Word - 2017-01-15	Status	Besitzer stephan stephan stephan stephan	Seiten (4 : 2 : 1 :	Größe 363 KB 3,71 MB 338 KB 75,0 KB	Gesendet 10:39:10 11.08.24 10:38:38 11.08.24 10:38:28 11.08.24 10:37:56 11.08.24	Ar 18 18 18	nschluss			
Semsung Universal Print Driver Drucker Dokument Ansicht Dokumentname Microsoft Word - 2018-05-23 Microsoft Word - 2016-06-30 Microsoft Word - 2017-01-15 Microsoft Word - 2017-01-15	Status	Besitzer stephan stephan stephan	Seiten 4 2 2 1 1	Größe 363 KB 3,71 MB 338 KB 75,0 KB 1,99 MB	Gesendet 10:39:10 11.08.21 10:38:38 11.08.21 10:38:28 11.08.24 10:37:56 11.08.24 10:50:47 14.06.2	Ar 18 18 18 18 18 18	2.168.101.51	-		

Ich denke, jetzt habe ich alles. Daher schalte ich den Server aus.

Einbau neue SSD und Neuinstallation als WS-HV3

Ich trenne die Hardware von der Stromversorgung und entferne die alte SSD. Dann baue ich die neue ein. Diese hatt 500GB statt 120GB Kapazität. Danach schließe ich das System wieder an und starte den Server.

Aktuell ist er direkt mit meinem Servernetz verbunden. Daher startet er einen PXE-Boot mit IPv4. Hier wähle ich das Image für meinen Windows Server 2019 aus:

windows Boot Manager (Server IP: 192.168.100.4)
Choose an operating system to start: (Use the arrow keys to highlight your choice, then press ENTER.)
Windows Server 2019 x64 Windows 10 1709 x64 Mindows La Server Reines
To specify an advanced option for this choice, press F&. Seconds until the highlighted choice will be started automatically: 28





Die Bilder danach spare ich mir einmal. Ein Setup habt ihr bei mir schon oft gesehen.

Für die Installation verwende ich nur 100GB. Den restlichen Speicher auf der SSD lasse ich frei. Kurze Zeit später beende ich die Installation:

	lallo		
ها	ssen Sie uns zunächst einige grundlegende Dinge klären.		
W	as ist Ihr Heimatland/Ihre Heimatregion?		
ſ	Deutschland	~	
w	as ist Ihre bevorzugte App-Sprache?		
C	Peutsch (Deutschland)	✓	
W	elches Tastaturlayout möchten Sie verwenden?		
D	leutsch	►	
e			



Für den Domain Join bereite ich ein Computerkonto im Active Directory vor. Den Namen WS-HV3 hatte ich ja bereits durch das Umbenennen der beiden anderen Hyper-V-Hosts freibekommen:



Den Domain Join führe ich mit einem Benutzeraccount aus:



Für die Aktivierung des Betriebssystems muss der Server das Internet erreichen können. Das erlaubt meine Firewall standardmäßig nicht. Daher nehme ich den Server kurzfristig in eine vorbereitete Gruppe auf. So kann das System auch Treiberaktualisierungen von Microsoft herunterladen. Ich suche die erforderliche Firewall-Ausnahme in meiner PFSense. Ein Klick auf den Namen des Alias bringt mich zur Ausnahmeliste:

	System -	Interfaces -	Firewall - S	Service	s ▼ VPN ▼	Stati	ıs ▼ I	Diagnost	ics •	Help 👻			•
Firewall	/ Rules / F	loating										± Ш ■	0
Floating	DMZ_120_EXT	ERN LAN_1	100_SERVER DMZ	_130_I	NTERN LAN_	110_CL	IENTS	DMZ_1	140_GAME	ZONE	DMZ_150_ISOLAT	ΓΙΟΝ	
Rules (Dra	ıg to Change	Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	n	Actions	
	1 /1.25 GiB	IPv4 *	Site_GameZone	*	! Site_Intranets	*	*	none		Zugriff Ga	ameZone	±∥⊡(01
	44 /10.00 GiB	IPv4 TCP/UDP	ServerOut_Anywhere	*	! Site_Intranets	*	*	none		ServerOut	tAnywhere	±∥⊡(01
□ ★₩₹	0 /0 B	IPv4 *	pfB_Top_v4	*	*	*	*	none		pfB_Top_\	v4 auto rule	±00	01

Und hier trage ich die aktuelle IP-Adresse des neuen Servers ein:

NS IT-Solutions

WS IT-Solutions

WSHowTo – Neuinstallation von WS-RDS3 als WS-HV3 2020-01-01 Migration auf Windows Server 2019

	Interfaces -	Firewall 🗸	Services 🕶	VPN -	Status 🗸	Diagnostics 👻	Help 🗕	e
Firewall / Aliases	/ Edit							Θ
Properties								
Name	ServerOut_Anywher	e						
	The name of the alia	s may only cons	sist of the charac	ters "a-z, A-Z,	0-9 and _".			
Description	ServerOut Anywhere	e						
	A description may be	e entered here fo	or administrative	reference (no	ot parsed).			
Туре	Host(s)				~			
Hint	Enter as many hosts re-resolved and upda as 192.168.1.16/28 r	as desired. Hos ited. If multiple may also be ent	sts must be speci IPs are returned b ered and a list of	fied by their l by a DNS que individual IP	IP address or fi ry, all are used. addresses will	ully qualified domain An IP range such as be generated.	name (FQDN). FQE 192.168.1.1-192.1	N hostnames are periodically 68.1.10 or a small subnet such
IP or FQDN	192.168.99.99							🛅 Delete
	172.19.130.113							💼 Delete
	172.19.130.102							💼 Delete
	172.19.130.111							🛅 Delete
	192.168.100.150				MP WS-HV3			🛅 Delete
	🖺 Save 🕇 Add	Host						

Die Netzwerkkarte hat das System automatisch erkannt. Aber einige andere Teile fehlen. Für diese starte ich die Treiberaktualisierung:



Das System kann diese bei Microsoft selbst suchen:

Datei Akti	on Ansicht ?				
* • •	🖼 🖬 🐖 💺 🗙 💿				
* ∎` * ←	Treiber aktualisieren – PCI-Datensammlungs- und Signalverarbeitungscontroller Wie möchten Sie nach Treibern suchen?	×			
	→ Automatisch nach aktualisierter Treibersoftware suchen Windows durchsucht den Computer und das Internet nach aktueller Treibersoftware für das Gerät, sofern das Feature in den Geräteinstallationseinstellungen nicht deaktiviert wurde.			T	
> 0	→ Auf dem Computer nach Treibersoftware suchen Sie können Treibersoftware manuell suchen und installieren.				

Wenige Sekunden später ist dieses Element installiert:



Und so verfahre ich mit allen anderen Komponenten. Jetzt ist alles einsatzbereit:

WS IT-Solutions



Mit der Internetverbindung kann auch die Aktivierung des Windows Servers vorgenommen werden. Ich installiere den Produktschlüssel mit der cmd. Anschließend aktiviere ich die Installation:

Administrator:	Windows PowerShell		_	×
C:∖>slmgr /ipk K	Windows Script Host	×		^
C:\>slmgr /ato				
C:\>	Windows(R), ServerDatacenter edition (175a4401-9571-4483-b7ed-1418ac983e2b) wird aktiviert Das Produkt wurde erfolgreich aktiviert.			
	ОК			

Danach bekommt der Server seinen neuen Namen WS-HV3. Die Aktion schließe ich mit einem Neustart ab:



🔁 Server-Manager				- 🗆 X
Server-M	Manager • Lokaler Server		- © F	Verwalten Tools Ansicht Hilfe
Dashboard	EIGENSCHAFTEN Für WIN-KUAGB1ELKPA	Systemeigenschaften	×	AUFGABEN 🔻
Lokaler Server Alle Server Datei-/Speicherdienste	Computername WIN-KUAGB1 Arbeitsgruppe WORKGROUP	IKPA Sie können den Namen und die ändem. Änderungen wirken sich auf Netzwerkressourcen aus.	s bzw. der Domäne X Migliedschaft des Computers möglicherweise auf den Zugriff Nie	s automatisch mithilfe von Windows Up
	Windows Defender Firewall Privat Ein Remoteverwaltung Aktiviert Remotedesktop Aktiviert NIC-Teamvorgang Deaktiviert Ethernet IPv4-Adresse v	Computemame: WS-HV3 Voliständiger Computemame: WS-HV3 Mtglied von	Andern des Computernamens bzw. der Domäne Der Computer muss neu gestar werden, damit die Änderungen werden. Speichen Sie alle geöffneten Dateien, unter beiten der B	tet wirksam m, Berlin, Bern, Rom, Sto A041 (Aktiviert) d schließen
	Betriebssystemversion Microsoft Win Hardwareinformationen FUJITSU ESPRI	dows MO C WORKGROUP	99,4 Gi	ОК 170T CPU @ 2.90GHz 3
	EREIGNISSE Alle Ereignisse 16 insgesamt		OK Abbrechen OK Abbrechen Übemehmen	AUFGABEN 💌

Nach der Neuanmeldung nehme ich den Server in meine Domain auf. Dabei verwende ich den Account, den ich beim Erstellen des Computerkontos angegeben habe:

🛓 Server-Manager				- 🗆 X
€ Server-Ma	anager • Lokaler Se	erver		🔹 🗭 🚩 Verwalten Tools Ansicht Hilfe
Dashboard	EIGENSCHAFTEN Für WS-HV3		Systemeigenschaften Ändern des Computernamens	s baw. der Domäne X AUFGABEN V
Lokaler Server Alle Server Datei-/Speicherdienste	Computername Arbeitsgruppe	WS-HV3 WORKGROUP	Sie können den Namen und die N ändem. Änderungen wirken sich r auf Netzwerkressourcen aus.	Migliedschaft des Computers Nie möglicherweise auf den Zugriff Windows-Sicherheit X
	Windows Defender Firewall Remoteverwaltung Remotedesktop NIC-Teamvorgang Ethernet	Privat: Ein Aktiviert Aktiviert Deaktiviert IPv4-Adresse wird	Computername: WS-HV3 Vollständiger Computername: WS-HV3 Mtglied von © Domäne: ws.ts	Ändern des Computernamens bzw. der Domäne Geben Sie Namen und Kennwort eines Kontos ein, mit dem Sie dieser Domäne beitreten dürfen. admin-setup
	Betriebssystemversion Hardwareinformationen	Microsoft Window FUJITSU ESPRIMO	Arbeitsgruppe: WORKGROUP	OK Abbrechen
	EREIGNISSE Alle Freignisse I 19 insgesamt			OK Abbrechen Obernehmen AUFGABEN 🔻

Einen Neustart später ist das System Mitglied meiner Domain.

Jetzt fehlen noch die aktuellen Updates. Diese bekommt der Server dank Gruppenrichtlinien-Konfiguration von meinem WSUS-Server:

WS IT-Solutions

Einstellungen	- 🗆 X
ம் Startseite	Windows Update
Einstellung suchen	*Einige Einstellungen werden von Ihrer Organisation verwaltet. Konfigurierte Updaterichtlinien anzeigen
Update und Sicherheit	Es sind Updates verfügbar.
⊖ Windows Update	Letzte überprutung: Heute, 09:24
曲 Übermittlungsoptimierung	2019-12 Kumulatives Update für .NET Framework 3.5, 4.7.2 und 4.8 für Windows Server 2019 für x64 (KB4533094) Status: Wird installiert – 11%
Windows-Sicherheit	Windows-Tool zum Entfernen bösartiger Software x64 - Dezember 2019 (KB890830) Status: Installation ausstehend
Problembehandlung	Updateverlauf anzeigen
S Wiederherstellung	Erweiterte Optionen
Ø Aktivierung	
97	Suchen Sie Infos zu den neuesten Updates?
∥⊭ Für Entwickler	Weitere Informationen

Der neue Server hat sich in meinem WSUS eingetragen. Der Container "nicht zugewiesene Computer" bekommt bei mir immer alle Updates automatisch genehmigt. Damit werden neue Systeme immer auf den neusten Stand aktualisiert:



Für den Dauerbetrieb verwende ich 2 andere Server-Container. Diese bekommen zeitverzögert neue Updates genehmigt. So kann ich steuern, wann meine Server ihren erforderlichen Neustart ausführen. "Updates-sofort" ist eine Woche vor "Updates-verzoegert" dran. So kann ich schlechte Updates im laufenden Betrieb erkennen und verhindern, dass diese auf die Nachzügler angewendet werden. In der Gruppe "Updates-sofort" stehen demnach nur Server, deren Services hochverfügbar sind.

Mein Hyper-V-Service in Neufahrn wird aber nur vom Server WS-HV3 bereitgestellt. Daher bekommt er die Updates verzögert. Ich weise den Server der Gruppe zu:



Dpdate Services				
Tatei Aktion Ansicht Fenster	?			
🗢 🔿 🙋 📰 🛛 🖬				
by Update Services	Update-Verzoegert (13 Compute	ers von 13 angezeigt, 28 insgesamt)		
VIS-CM	Status: Alle	🕶 🞧 Aktualisieren		
Alle Updates	① Name	IP-Adresse	Betriebssystem	Prozentsatz "Installiert/Nicht zutreffend"
Wichtige Updates	ws-ata.ws.its	192.168.100.23	Windows Server 2019 Datacenter	100%
WSUS-Undates	ws-cm.ws.its	fe80::b545:c43c:5aa5:2c25%2	Windows Server 2016 Datacenter	100%
aktuelle Updates	ws-dc1.ws.its	192.168.100.1	Windows Server 2016 Datacenter	100%
🗸 💐 Computer	ws-dpm.ws.its	192.168.100.5	Windows Server 2019 Datacenter	100%
🗸 💕 Alle Computer	ws-fs2.ws.its	192.168.100.12	Windows Server 2019 Datacenter	100%
Nicht zugewiesene Co	ws-fs3.ws.its	192.168.101.3	Windows (Version 10.0)	99%
v Server	▲ ws-hv2.ws.its	192.168.100.10	Windows Server 2019 Datacenter	99%
🔮 Update-Sofort	ws-hv3.ws.its	192.168.100.150	Windows Server 2019 Datacenter	100%
💕 Update-Verzoeger	ws-mon.ws.its	192.168.100.18	Windows Server 2019 Datacenter	100%
Downstreamserver	ws-mx2.ws.its	192.168.100.13	Windows Server 2016 Datacenter	100%
Synchronisierungen	ws-nps1.ws.its	192.168.100.7	Windows Server 2019 Datacenter	100%
Dotionen	ws-rds1.ws.its	192.168.110.16	Windows Server 2019 Datacenter	100%
	ws-rds3.ws.its	192.168.100.150	Windows Server 2016 Datacenter	99%

Der Server hat nun alle Updates installiert und den erforderlichen Neustart ausgeführt.

Installation der Rollen und Features

So kann es zur Rolleninstallation gehen. Die Auswahl wird dieses mal auf das notwendige beschränkt: Das System soll nur noch als Hyper-V-Host arbeiten:

🔁 Server-Manager					– 🗆 X
Serve Serve	/er-Manager > Das 🏝 Assistent zum Hinzufügen von	hboard Rollen und Features	- C ×	Verwalten	Tools Ansicht Hilfe
 ■ Dashboard ■ Lokaler Server ■ Alle Server ■ Datei-/Speicherdien: 	Serverrollen ausw Vorbereitung Installationstyp Serverauswahl Features Hyper-V Virtuelle Switches Migration Standardspeicher Bestätigung Ergebnisse	Water Ser mindestens eine Rolle aus, die auf dem ausgewater Ausgewat	BARDEN BA	1	Ausblenden
		- Zurock	instancient rasificient		

Die Konfigurationsoptionen lasse ich bestehen. Das mach ich später richtig:



🔁 Server-Manager						- 0	×
Serv	ver-Manager 🕨 Dast 🚡 Assistent zum Hinzufügen von R	aboard ollen und Features	• (3) -	Verwa	ilten Tools	Ansicht	Hilfe
Image: Dashboard Image: Lokaler Server Image: Alle Server Image: Datei-/Speicherdien:	Assistent zum Hinzufügen von R Standardspeicher Vorbereitung Installationstyp Serverauswahl Serverrollen Features Hyper-V Virtuelle Switches Migration Standardspeicher Bestätigung Ergebnisse	ollen und Features Von Hyper-V werden Standardspeicherorte zum Speichern von VHD-Dateien und Kor der virtuellen Computer verwendet, es sei denn, Sie geben beim Erstellen der Dateien Speicherorte an. Sie können diese Standardspeicherorte jetzt ändern, oder Sie können Hyper-V-Einstellungen ändern. Standardspeicherort für VHD-Dateien: CAUsers/Public/Documents/Hyper-V/Virtual Hard Disks Standardspeicherort für Konfigurationsdateien für den virtuellen Computer: CAProgramData\Microsoft\Windows\Hyper-V	- X ZIELSERVER WS-HV3.ws.Rs andere n sie später in den Durchsuchen	1		Ausblen	den
		< Zurück Weiter > Installiere	n Abbrechen				

Aus den Features wähle ich noch den Bitlocker-Support dazu. Diesen benötige ich für die Festplattenverschlüsselung. Mit System Insights kann mein Windows Admin Center Prognosen zur Hardwareauslastung erstellen. Und die Windows Server Sicherung verwende ich für das Backup des SystemImages:

🔁 Server-Manager				_			- 0	×
Ser	ᡖ Assistent zum Hinzufügen von	Rollen und Features	- 0 ×	7	Verwalten	Tools	Ansicht	Hilfe
	Installationsauswa	ahl bestätigen	ZIELSERVER WS-HV3.ws.its					
Dashboard Lokaler Server Alle Server Datei-/Speicherdien	Vorbereitung Installationstyp Serverauswahl Serverrollen Features Hyper-V Virtuelle Switches Migration Standardspeicher Bestätigung Ergebnisse	Klicken Sie auf "Installieren", um die folgenden Rollen, Rollendienste und Feature ausgewählten Server zu installieren. Cielserver bei Bedarf automatisch neu starten Optionale Features (z. B. Verwaltungstools) können auf dieser Seite angezeigt w automatisch ausgewählt wurden. Wenn Sie diese optionalen Features nicht auto möchten, klicken Sie auf "Zurück", um die entsprechenden Kontrollikästchen zu or BitLocker-Laufwerkoerschlüsselung Erweitertes Speichern Hyper-V Remoteserver-Verwaltungstools Rollenverwaltungstools AD DS-tools AD DS-tools AD DS-tools Hyper-V-Verwaltungstools Hyper-V-Verwaltungstools Hyper-V-Verwaltungstools Hyper-V-Verwaltungstools Hyper-V-Verwaltungstools Hyper-V-Verwaltungstools Verwaltungstolf für Windows PowerShell Featureverwaltungstools Verwaltungstolf für die BitLocker-Laufwerkverschlüsselun Tools zur BitLocker-Laufwerkverschlüsselung BitLocker-Wiederherstellungskennwort-Viewer System Insights Module for Windows PowerShell Konfigurationseinstellungen exportieren Alternativen Quellpfad angeben	es auf dem erden, da sie matisch installieren deaktivieren.	1			Ausblen	den
		< Zurück Weiter > Inst	Abbrechen					

Die Rolleninstallation schließe ich mit einem Neustart ab.

Konfiguration von Hyper-V und Migration der VMs

Weiter geht es mit der Einrichtung des Hyper-V-Hosts. Die virtuellen Maschinen sollen nicht wie zuvor auf der Systempartition liegen. Dafür habe ich beim Setup reichlich Platz auf der SSD gelassen. Diesen freien Speicher nutze ich jetzt für ein neues Volume. Das erstelle ich mit dem Server-Manager:



Server-Manager	- □ × 1anager • Datei-/Speicherdienste • Volumes • • ⓒ 『 Verwalten Tools Ansicht Hilfe
Server Server Uolumes Datenträger	Alle Volumes 3 insgesamt Fitter P Image: Control of the second secon
Speicherpools	▲ Volume Status Bereitstellung Kapazität Freier Speicherplatz Deduplizierungsrate Einsparungen durch Deduplizierung • WS-HV3 (3) • • • • • • • \l\R\volume(6b • • • • • • • \l\R\volume(6b • • • • • • • \l\R\volume(bd Wiederherstellung Fest 499 MB 790 MB • • • C: • • • • • • • •
	Für die Verwendung dieses Features muss der Rollendienst für den Dateiserver installiert sein. Kit volumieglobel 122-482e=9-39-817 / 40/3646602e5) auf visi-n Auf GABLY

Ich verwende den verbliebenen Speicher, formatiere mit NTFS und vergebe den passenden Laufwerksbuchstaben V (wie VM). Diesen verwenden meine anderen Hyper-V-Hosts auch:

Server	Alle Volumes 3 insgesamt				AUFGABEN 🔻
Volumes Datenträger Speicherpools	Auswahl bestätig			- 🗆 X	Deduplizierung Verwendeter
	Vorbemerkungen Server und Datenträger Größe Laufwerkbuchstabe oder Dateisystemeinstellungen Zu Bestätigung Ergebnisse FRE Es si	Überprüfen Sie die folgenden dann auf "Erstellen". VOLUMEORT Server: Datenträger: Freier Speicherplatz: VOLUMEEIGENSCHAFTEN Volumegröße: Laufwerkbuchstabe oder -pfad: Volumebezeichnung: DATEISYSTEMEINSTELLUNGEN Dateisystem: Erstellung kurzer Dateinamen: Große der Zuordnungseinheit:	Einstellungen auf Korrektheit, u WS-HV3 Datenträger "0" 366 GB VA Hyper-V NTFS Deaktiviert Standard	nd klicken Sie) auf WS-H AUFGABEN 👻

Das neue Volume wird alle virtuellen Maschinen aufnehmen. Für den Zugriff auf das Volume möchte ich das Modell der Rollen-Administration verwenden. Meine administrativen Accounts haben keine statischen Gruppenmitgliedschaften. Mit meiner Privileged Access Management Lösung kann ich die erforderlichen Gruppenmitgliedschaften auf eine begrenzte Zeit verwenden. Damit sichere ich meine administrativen Konten ab. Und weiter gehe ich mit der Einschränkung des Datenzugriffs: Meine AdminAccounts haben auf Datenverzeichnisse keinen Zugriff, bis ich sie zusätzlich in eine Rollengruppe aufnehme.

Das muss natürlich vorbereitet sein. In diesem Fall handelt es sich um das Volume mit den virtuellen Maschinen. Da sollen nur Mitglieder der Rechtegruppe LD-Admins-HyperV-Storage Zugriff erhalten. Die Gruppe gibt es schon. Also editiere ich nur noch die NTFS-Berechtigungen. Zuerst entferne ich die Vererbung:



				_
💻 🔁 🔚 🖵 🛛 Ven	walten Dieser PC			- 🗆 X
Datei Computer Ansicht Laufw	verktools			~ 🕐
← → · ↑ 💻 → Dieser PC			~ Ū	"Dieser PC" durchsuchen 🔎
	d Laufworko (2)			
Schneizugriff Gerate und	tem (C)	Human V (VI)		
Desktop		DVD-RW-Laufwerk (D:)		
👗 Walther, Stephan - 👘 😽 85,	5 GB frei von 99,3 GB	365 GB frei voi	on 365 GB	
Dieser PC Vetzwerka	Eigenschaften von H	mer-V (V:)		
System (C:) Fre		here a first		
DVD-RW-Lautweri 69,	Vorgängerversionen I Allgemein Tools	Kontingent Anpassen Klassifizierung		
Hyper-V (V)	Objektnome: \//	Erweiterte Sicherheitseinstellungen für "Hyper-V (V:)"		- 🗆 X
Bibliotheken	objektname. V:\			
Netzwerk	Gruppen- oder Benutze	Name: V:\		
Systemsteuerung	Seder	Besitzer: Netzwerkdienst 🌍 Ändern		
Papierkorb	ERSTELLER-BES	Berechtigungen Überwachung Effektiver Zugriff		
	Administratoren (W			
	Senutzer (WS-HV1	Doppelklicken Sie auf einen Berechtigungseintrag, um zusätzliche Information Berechtigungseintrags den Eintrag aus, und klicken Sie auf "Bearbeiten" (sowei	nen zu erhalten. Wa eit vorhanden).	hlen Sie zum Andern eines
	Klicken Sie auf "Bearbe	Berechtigungseinträge:		
	Berechtigungen zu änd	Typ Prinzipal Zugriff Ge	eerbt von	Anwenden auf
	Berechtigungen für Jet	🚨 Zulas Administratoren (WS-HV3\Ad Vollzugriff Ke	eine	Diesen Ordner, Unterordner un
	Vollzugrift Ändern	SYSTEM Vollzugriff Ke	eine	Diesen Ordner, Unterordner un
	Lesen, Ausführen	Zulas ERSTELLER-BESTIZER Vollzugriff Ke Zulas Benutzer (WS-HV3\Benutzer) Lesen Ausführen Ke	eine	Nur Unterordner und Dateien Diesen Ordner, Unterordner un.
4 Elemente 1 Element ausgewählt	Ordnerinhalt anzeiger	Renutzer (WS-HV3\Benutzer) Ordner erstellen / Date Ke	aine	Diesen Ordner, Unterordner
	Schreiben	ateien erstellen / Date Ke	eine	Nur Unterordner
	Spezielle Berechtigur	at and a see	eine	Nur diesen Ordner
	Klicken Sie auf "Erweite			
	berechtigungen anzuze			
		Berechtigungen ändern Anzeigen		
	L			
		Γ	OK	Abbrechen Übernehmen
		-		

Dann schränke ich den Zugriff ein:

📃 🕑 🔚 🖛 Verwalten	Dieser PC				- 0	\times
Datei Computer Ansicht Laufwerktools						~ 📀
\leftrightarrow \rightarrow \checkmark \bigstar Dieser PC				~ Ö	"Dieser PC" durchsuchen	R
> 🖈 Schnellzugriff → Geräte und Laufwer	ke (3)					_
V Desktop System (C:)		DVD-RW-Laufwerk (D:)	Hyper-V (V:)		
> 🤱 Walther, Stephan - 🛛 🔍 85,5 GB frei von	n 99,3 GB	DWD	365 GB fre	ei von 365 GB		
✓	(1)					
> 🏪 System (C:) 🛛 🗧 Fre	chaften von Hyper-V (V) ×				
> 🖉 DVD-RW-Laufwerl 🛛 💦 Vorgänge	erversionen Kontingent	Anpassen Klassifizierung				
> 🛖 Freigaben (M:)	n Tools 📜 Erwei	terte Sicherheitseinstellungen für "I	Hyper-V (V:)"		- 0	×
> 🔜 Hyper-V (V:) Objektna	me: V:\					
> ¡ Bibliotheken Gruppen	- oder Benutzel Name	V:\				
> 💣 Netzwerk	Pasita	- Netzwerkdienst Är	adem			
> 🖭 Systemsteuerung	er Besitze	r: Netzwerkdienst Ar	luem			
Papierkorb 🔍 🕵 SYS	STEM Berech	igungen Überwachung Effek	ctiver Zugriff			
St. Adn	ninistratoren (W	Iklicken Sie auf einen Berechtigung	useintrag, um zusätzliche Informa	tionen zu erhalten. W	/ählen Sie zum Ändern eines	
	Berech	tigungseintrags den Eintrag aus, u	nd klicken Sie auf "Bearbeiten" (s	oweit vorhanden).		
Kicken S Bernehti	Sie auf "Bearbe Bereck	tigungseinträge:				
Berechtig	ungen für "Je	/p Prinzipal	Zugriff	f Geerbt von	Anwenden auf	
		ulas Administratoren (WS-HV3)	Administratoren) Vollzug	griff Keine	Diesen Ordner, Unterordner und D	at
Änden	n 🥵 Z	ulas SYSTEM	Vollzug	griff Keine	Diesen Ordner, Unterordner und D	at
Lesen	, Ausführen	ulas LD-Admin-HyperV-Storage	e (WS\LD-Admin-Hyp Volizug	griff Keine	Diesen Ordner, Unterordner und L	at
4 Elemente 1 Element ausgewählt Ordne	rinhalt anzeiger					
Schrei	ben					
Spezie	elle Berechtigur					
Kicken	Sie auf "Erweite					
Berechuş	Hir	zufügen Entfernen	Bearbeiten			
		Parashtinun pasintei as filo contacas	andanta Obialita durab urt-t		ing upp discore Objekt an-t	
		berechtigungseintrage für unterge	eoronete Objekte durch vererbbar	e berechtigungseintr	age von diesem Objekt ersetzen	
				ОК	Abbrechen Überne	hmen

Das wars auch schon. Jetzt geht es an die Feinkunfiguration des Hyper-V-Hosts:

VS IT-Solutions

Hyper-V-Mana	ger		-		×
Datei Aktion A	Ansicht ?				
🗢 🔿 🔁 📊	? 🖬				
💾 Hyper-V-Mana	ger Mintuelle Computer		Aktionen		
WS-HV ³	Neu >	Dhare CDU Auslant Zurzwisserer Cari Datisharek Catho	WS-HV3		•
	Virtuellen Computer importieren	Phase CPO-Ausiast Zugewiesener spei betriebszeit Status	Neu		•
	Huner-V-Finstellungen	Auf dem Server wurden keine virtuellen Computer gefunden.	强 Virtuellen Computer importieren		
	Manager für virtuelle Switches		Hyper-V-Einstellungen		
	Manager für virtuelle SANs		📲 Manager für virtuelle Switches		
	Datenträger bearbeiten		🛃 Manager für virtuelle SANs		
	Datenträger überprüfen		🚄 Datenträger bearbeiten		
	Dienst beenden		Datenträger überprüfen		
	Server entfernen	٢	Dienst beenden		
	Aktualisieren	Kein virtueller Computer ausgewählt.	× Server entfernen		
	Ansicht		Aktualisieren		
	1.006-		Ansicht		
	Hilfe		I Hilfe		

Den Standardspeicherort lege ich auf das neue Volume V: und zusätzlich aktiviere ich den erweiterten Sitzungsmodus. Mit diesem steht mir eine RDP-ähnliche Verbindung zu meinen VMs zur Verfügung:

Hyper-V-Manager Datei Aktion Ansicht ?	Virtuelle Computer Name PP	Hyper-V-Einstellungen für WS-HV3 Kerver Virtuelle Festplatten Virtyper-Vi Virtuelle Computer Virtyper-Vi Givrituelle Computer Virtyper-Vi Givrituelle Computer Virtuelle Computer Virt	Richtlinie für den erweiterten Sitzungsmodus Richtlinie für den erweiterten Sitzungsmodus Sie können Hyper-V so konfigurieren, dass Verbindungen im erweiterten Sitzungsmodus mit virtuelen Computerm auf desem Server zugelassen sind. Der erweiterten Sitzungsmodus zulassen Der erweiterten Sitzungsmodus ermöglicht das Umleiten von lokalen Geräten und Ressourcen von Computerm, auf denen eine Verbindung mit virtuelen Computern ausgeführt wird. Fird den erweiterten Sitzungsmodus sind ein unterstütztes Gastbetriebssystem und möglicherweise zusätzliche Konfigurationsschritte auf deen virtuelen Computer Gastbetriebssystems unterscheiden. Bi Änderung deser Einstellung müssen vorhandene Sitzungen der Verbindung mit virtuelen Computer möglicherweisen ung gestartet werden.	- C X
	< Prüfpunkte Details	Image: Uvenigrationen Reine Uvenigrationen Spechemigrationen 2 glechzeitige Migrationen Image: Uvenigrationen Image: Uvenigrationen <	Ausgeführt wird. Für den erweiterten Sitzungsmodus sind ein unterstütztes Gastbetiebssystem und möglicheweise zuskätche Konfigurationsschritte auf dem virbulein Computer erforderlich. Die Weiterleitungsmöglichkeiten können sich je nach Version des Gastbetiebssystems unterscheiden. Bei Änderung dieser Einstellung müssen vorhandene Sitzungen der Verbindung mit wituellen Computern möglicherweise neu gestartet werden.	Switches SANs n en

Den einen Netzwerkadapter benenne ich in der Systemsteuerung um. Das macht eigentlich keinen Sinn, aber so ist es mit den anderen Hyper-V-Hosts gleich konfiguriert. Ich liebe Standards...

😰 Netzwerkverbindungen			×
\leftrightarrow \rightarrow \checkmark \bigstar Systemsteuerung $ ightarrow$ Netzwerk und Internet $ ightarrow$ Netzwerkverbindungen $ ightarrow$	V Ö "Netzwerkverbinde	ungen" dur.	,P
Organisieren 🔻 Netzwerkgerät deaktivieren Verbindung untersuchen Verbindung umbenen	en Status der Verbindung anzeigen »	•	2
LAN-101 ws.its Intel(R) Ethernet Connection I217			

Nun aktiviere ich auf diesem Adapter einen neuen virtuellen Switch:

a opport o	in anger		
Datei Aktio	n Ansicht ?		
🗢 🔿 🖄			
Hyper-V-N	Aanager		Aktionen
WS-	Neu >		WS-HV3
	Virtuellen Computer importieren	Phase CPU-Auslast Zugewiesener Spei Betriebszeit Status	Neu
	Hyper-V-Einstellungen	Auf dem Server wurden keine virtuellen Computer gefunden.	Nituellen Computer importieren
	Manager für virtuelle Switches		Hyper-V-Finstellungen
	Manager für virtuelle SANs		Manager für virtuelle Switcher
	Datenträger bearbeiten		Manager für virtuelle SANs
	Datenträger überprüfen		
			> Datenträger bearbeiten
	Dienst beenden		Datentrager überprüfen
	Server entrernen		Dienst beenden
	Aktualisieren	Kein virtueller Computer ausgewählt.	X Server entfernen
	Ansicht >		Aktualisieren
	Hilfe		Ansicht
			Hilfe



Dieser muss als externer Switch fungieren. Ebenso muss ich den gemeinsamen Zugriff aktivieren. Denn anderenfalls kann mein Hyper-V-Host selber nicht mit dem Netzwerk kommunizieren. Das VLAN lasse ich noch raus. Wichtig ist, dass der vSwitch den gleichen Namen hat wie auf dem alten Server. Sonst bekomme ich beim VM-Import Probleme:

Hyper-V-Manager				- 🗆 X
Datei Aktion Ansicht ?	Г			
		Manager für virtuelle Switches für "WS-H	V3" — 🗆 🗙	
Hyper-V-Manager	Virtuelle Computer	Virtuelle Switches	The Eigenschaften für virtuellen Switch	
WS-HV3	^	Reuer virtueller Netzwerkswitch		▲
	Name Pr	VLAH-101 Intel(R) Ethernet Connection Globale Netzwerkeinstellungen MAC-Adressbereich 00-15-5D-64-96-00 bis 00-15-5D-6	Name: VLAN-101 Ammerkung:	mportieren m Switches SANs
	Netzwerkänderunge Prüfpunkte Prüfpunkte Durch au Netzwerk Werden Beim Überr Netzwerkv Dies kann s Netzwerkv Werden gg Überschnet statischen Netzwerkv Sie den Von	gen übernehmen × ausstehende Änderungen kann die trkkonnektivität unterbrochen sich auf derzeit ausgeführte vorgange auswirken. Mit diesen Änderungen eben. Wenn dies sechniet, müssen sie die Anderungen erneut übernehmen, um die konnektivität wiederherzustellen. Mochten organg fortsetzen? fragen Ja Nein	Verbindungstyp Weibindungstyp Weibindungstyp Weibindungstyp Weibindungstyp Weibindungstyp Weibindungstyp Intel(R) Ethernet Connection 12174M Intel(R) Ethernet	۰ ۳
I		,	OK Abbrechen Anwenden	
1				

Der Assistent erstellt einen virtuellen Adapter, mit dem der Hyper-V-Host über den virtuellen Switch an den realen Adapter angeschlossen ist. Die IPv4-Konfiguration wird in der Regel übernommen:

😰 Netzwerkverbindungen					- 0		×
\leftarrow \rightarrow \checkmark \bigstar Systemsteuerung \Rightarrow Netzwerk und Internet \Rightarrow Netzwerkverbindungen			ٽ ~	"Netzwerkverb	indungen"	dur ,	ρ
Organisieren 🔻 Netzwerkgerät deaktivieren Verbindung untersuchen Verbindung um	benennen Sta	atus der Verbindung anzeige	n »				?
LAN-101 Aktiviert Intel(R) Ethernet Connection I217	Status von vE	thernet (VLAN-101)	×		7		
	Verbindung	Netzwerkverbindungsdetails:					
	IPV4-Konnek IPv6-Konnek Medienstatus Dauer: Übertragung Details	Eigenschaft Verbindungsspezifisches Beschreibung Physische Adresse DHCP-aktiviert IPv4-Adresse IPv4-Subnetzmaske Lease einaft ab IPv4-Standardgateway IPv4-DHCP-Server IPv4-DHCP-Server	Weit ws.its Hyper-V Virtual Ethemet 90-IB-0E-IF-F1-EE Ja 192-168.100.150 255-255.0 Montag. 6. Januar 2020 Montag. 6. Januar 2020 192.168.100.1 192.168.100.1	t Adapter) 11:10:53) 15:10:52			
	Pakete:	IPv4-WINS-Server NetBIOS über TCPIP ak Verbindungslokale IPv6 IPv6-Standardgateway IPv6-DNS-Server	192.168.100.2 Ja fe80::95a3:e17e:1057 f	aca%8			
2 Elemente 1 Element ausgewählt				Schließen			

Jetzt kann ich die virtuellen Maschinen importieren. Dazu baue ich die alte Festplatte in eine Dockingstation ein und schließe diese mit USB3 an den Server an. Die alte Systempartition mit den VM-Dateien ist weiterhin mit Bitlocker verschlüsselt. Ich benötige aber keinen Recoverykey, da ich die Verschlüsselung zuvor angehalten hatte:



Die VMs sind jetzt nur Dateien und Ordner. Diese kopiere ich in einen neuen Ordner auf die neue SSD:



Danach importiere ich die 3 VMs mit dem Hyper-V-Manager:

Hyper-V-Man	ager					- C	
Datei Aktion	Ansicht ?						
🗢 🔿 🙍 🔜	?						
Hyper-V-Man	ager	Virtuelle Computer			Aktionen		
WS-HV3	Neu	virtuelle computer	Phase CPII-Auslast Zunewiesener Spei	Betriebszeit Status	WS-HV3		
	Virtuellen Compu	uter importieren	Phase Crowasiast Zugewiesener spein	Status	Neu		•
	Humor V Einstellu	ingen	Auf dem Server wurden keine virtuellen Comput	ter gefunden.	🔓 Virtueller	n Computer importieren	
	Manager für virtu	uelle Switches			Hyper-V	-Einstellungen	
	Manager für virtu	elle SANs			🕌 Manager	für virtuelle Switches	
	Datenträger bear	beiten			🔒 Manager	für virtuelle SANs	
	Datenträger über	prüfen			n Datenträ	ger bearbeiten	
	Dienst beenden				Datentră	ger überprüfen	
Datei Aktion	Ansicht ?					_	
Hyper-V-Mar	nager	Virtuelle Computer			Aktionen		
WS-HV3		Name					-
		INdifie	Virtuellen Computer Importieren		^		•
						Computer importieren	
			Ordner suchen			Einstellungen	
						für virtuelle Switches	
			Vorbemerkungen Geben Sie den Ordner mit	dem zu importierenden virtuellen Computer an.		für virtuelle SANs	
		<	Ordner: V:\Hyper-V\WS-t	DC3\	Durchsuchen	ger bearbeiten	
		Prüfpunkte	auswählen			ger überprüfen	
			Importtyp auswählen			tenden	
			Zusammenfassung			tternen	
						eren	
		III I					,

Die ID der VM behalte ich bei:

WS IT-Solutions



Hyper-V-Manager					- 0	\times
Datei Aktion Ansicht ?						
🗢 🏟 🖄 📰 🖬						
Hyper-V-Manager	Virtuelle Computer			Aktionen		
	Name	Virtuellen Computer impo	tieren	×		•
		The second secon			Computer importieren	
		тирогстур а	uswanien		Einstellungen	
					für virtuelle Switches	
		Vorbemerkungen	Wählen Sie den auszuführenden Importtyp aus:		für virtuelle SANs	
	1	Ordner suchen	 Virtuellen Computer direkt registrieren (die vorhandene eindeutige ID verwenden) 		ger bearbeiten	
	Bettfoundate	Virtuellen Computer auswählen	O Virtuellen Computer wiederherstellen (die vorhandene eindeutige ID verwenden)		ger überprüfen	
	Prutpunkte	Importtyp auswählen	O Virtuellen Computer kopieren (neue eindeutige ID erstellen)		enden	
		Zusammenfassung			tfernen	
					eren	

Nach wenigen Klicks sind die drei VMs registriert. Da lohnt sich ein PowerShell-Script nicht wirklich. Die VMs lasse ich noch ausgeschaltet, denn sie würden sich im falschen Netzwerksegment befinden. Vorher muss ich den Server doch wieder an seinen Platz im Außenstandort bringen:

Hyper-V-Manager										- 0	ı ×
Datei Aktion Ansicht ?											
🗢 🤿 🙇 🖬 👔 🖬											
Hyper-V-Manager	Virtuelle Computer							Aktionen			
WS-HV3	Name	Phase	CRU-Auclast	Zuggwierener Spei	Retriebczeit	Chatur		WS-HV3			•
	WS-DC2	Aug	CPO-Ausiast	Zugewiesener Spei	Berriebszeit	Status		Neu			+
	WS-FS3	Aus						🔥 Virtue	ellen Computer importie	ren	
	WS-PFS2	Aus						🛃 Нуре	r-V-Einstellungen		
								🕌 Mana	ger für virtuelle Switche	s	
								🔒 Mana	ger für virtuelle SANs		
								🏑 Dater	träger bearbeiten		
							>	🔄 Dater	träger überprüfen		
	Prutpunkte						۲	Diens	t beenden		
			Kata utati a	I							

Absicherung mit Bitlocker

Aber die Absicherung kann ich im Hauptstandort vornehmen. Der TPM ist noch vom Windows Server 2016 in Verwendung. Daher lösche ich seinen Inhalt. Die Aktion wird bei einem Neustart durchgeführt:

🐒 "Trusted Platform Module"-M	lanagement (TPM) auf dem lokalen Computer			- 🗆		\times
1 Datei Aktion Ansicht Fe	enster ?				-	8 ×
♦ ♦						
搧 TPM-Verwaltung auf dem loka	len (TPM-Verwaltung auf dem lokalen Computer	Ak	tionen		_	
🎾 Befehlsverwaltung		ТР	M-Verwaltung auf dem lokale	n Computer		
	TPM-Verwaltung auf dem lokalen Computer Konfiguriert das TPM und dessen Unterstützung durch die Windows-Plattform.		TPM vorbereiten			
		🖸	TPM löschen			
	Obersicht		Ansicht			•
		×	Neues Fenster hier öffnen			
	TPM-Sicherheitshardware verwalten	Q	Aktualisieren			
		?	Hilfe			
1	TPM löschen					
	Sie müssen den Computer neu starten, um die Einstellungen der TPM-Sicherheitshardware zu konfigurieren, damit das TPM gelöscht werden kann. Gehen Sie hierzu wie folgt vor:					
	Klicken Sie unten auf die Schaltfläche "Neu starten".					
	Bleiben Sie beim Computer, sodass Sie die Anweisungen befolgen können, die beim Startvorgang angezeigt werden.					
	Melden Sie sich bei Windows an, um den Assistenten automatisch fortzusetzen.					
	WARNUNG: Durch das Löschen des TPMs gehen alle TPM-Schlüssel verloren. Sie sollten diesen Vorgang nur ausführen, wenn Sie von Ihrem Systemadministrator dazu aufgeforde werden.	rt				
1						
1						
	Neu starten Abbreche	n				

Nun kann ich die Verschlüsselung der Volumes auf der neuen SSD vornehmen:

VS IT-Solutions



Damit ich den Server aus der Ferne neustarten kann bzw. damit er nach Updates neustartet, wähle ich die Option mit der automatischen Entsperrung. Das klingt vielleicht im ersten Moment unsicher, ist es aber nicht. Der TPM prüft beim Start mit der UEFI, ob sich relevante Bauteile der Serverhardwar verändert haben. Ebenso werden Firmwareveränderungen erkannt. Sollte es eine Manipulation geben, dann wird der TPM den Entschlüsselungsschlüssel nicht freigeben und die SSD bleibt verschlüsselt. Ist alles integer, dann wird die Platte freigegeben. Ab diesem Moment übernimmt das Betriebssystem die Absicherung. Nur bei Fehlern im TPM, der UEFI-Firmware oder der Verschlüsselung selber könnte zu einem unberechtigten Zugriff führen. Natürlich kann auch das laufende Betriebssystem über Lücken verfügen, welche den Zugriff gestatten. Aber diese würde ich nicht mit einem Start-PIN verhindern. Also wähle ich die Automatik:

1		
	Ditacles Lufwalaeseklöselung (C)	
	Reference contraction of the con	
	Festlegen, wie das Laufwerk beim Start entsperrt werden soll	
	Um den Schutz Ihrer Daten zu erhöhen, können Sie festlegen, dass Sie von BitLocker bei jedem Start des PCs zur Eingabe einer PIN oder zum Anschließen eines USB-Speichersticks aufgefordert werden.	
	\rightarrow PIN eingeben (empfohlen)	
	\rightarrow USB-Speicherstick anschließen	
	ightarrow Das Laufwerk soll von BitLocker automatisch entsperrt werden.	
	Abbrecher	1

Für die Wiederherstellungsschlüssel habe ich einen geschützten Ordner in meinem AdminShare. Zusätzlich wird der Schlüssel auch im Active Directory abgelegt. Hier sichere ich mich doppelt ab:



		×				
← 🏘 BitLocker-Laufwerkverschlüsselung (C:)						
Wie soll der Wiederherstellungsschlüssel gesichert wer	den?					
Ein Wiederherstellungsschlüssel kann für den Zugriff auf Dateien und O Ihren PC nicht entsperren können. Es wird empfohlen, mehrere Wiederh PC aufzubewahren.	RitLocker-Wiederherstell	ungsschlüssel speichern unter				×
	$\leftarrow \rightarrow \checkmark \uparrow $ s \sim Fr	eigaben (M:) > AdminArea > Sicherheit > Bitlo	cker	✓ Ö "Bitlock	er" durchsuchen	Q
\rightarrow Auf USB-Speicherstick speichern	Organisieren 👻 Neue	r Ordner				?
	🏪 System (C:) \land	Name	Änderungsdatum	Тур	Größe	^
→ In Datei <u>s</u> peichern	DVD-RW-Laufv	2012-11-03 BitLocker-Wiederherstellungs	03.11.2012 21:28	Textdokument	2 KB	
	🛖 Freigaben (M:)	2013-07-04 BitLocker-Wiederherstellungs	04.07.2013 18:51	Textdokument	2 KB	
→ Wiederherstellungsschlussel druc <u>k</u> en	📕 AdminArea	2013-09-08 BitLocker-Wiederherstellungs	08.09.2013 17:31	Textdokument	2 KB	
	Geräte	2013-12-27 BitLocker-Wiederherstellungs	27.12.2013 19:03	Textdokument	2 KB	
	Lizenzen	2013-12-27 BitLocker-Wiederherstellungs	27.12.2013 18:59	Textdokument	2 KB	
	Netzwerk	2016-04-13 WS-CL6 NVMe.TXT	13.04.2016 20:49	Textdokument	2 KB	
	Senvices	2016-04-13 WS-CL6 Samsung EVO 840 L	13.04.2016 08:24	Textdokument	2 KB	
Wie finde ich später meinen Wiederherstellungsschlüssel?	Cichachait	2017-11-16 WS-CL6 LWE D78651B6-9046	16.11.2017 19:01	Textdokument	2 KB	
	Sichemeit	2017-11-17 WS-CL6 LWC C023662C-158A	17.11.2017 07:59	Textdokument	2 KB	
	BenutzerZ	2017-11-18 WS-CL1 LWC 3F3F3063-6864	18.11.2017 22:19	Textdokument	2 KB	
	Bitlocker Y	2017-11-25 WS-CL1 LWC 3E0DD998-C15E	25.11.2017 10:17	Textdokument	2 KB	~
	Dateiname: 2020-	-01-06 WS-HV3 LWC BitLocker-Wiederherstellungss	chlüssel F1705083-C40	F-4F83-A370-F7C6B7	C08380.TXT	~
	Dateityp: Textd	ateien (*.txt)				~
	 Ordner ausblenden 			Speid	hern Abbre	chen

Die modernere Variante passt auf mein Szenario:

Г	×
~	RitLocker-Laufwerkverschlüsselung (C:)
L.	Zu verwendenden Verschlüsselungsmodus auswählen
L	Mit Windows 10 (Version 1511) wird ein neuer Datenträger-Verschlüsselungsmodus (XTS-AES) eingeführt. Dieser Modus unterstützt zusätzliche Integrität, ist mit älteren Windows-Versionen aber nicht kompatibel.
L	Bei einem Wechseldatenträger, den Sie mit einer älteren Windows-Version verwenden möchten, sollten Sie den kompatiblen Modus wählen.
	Bei einem Festplattenlaufwerk oder einem Laufwerk, das nur mit Geräten eingesetzt wird, auf denen Windows 10 (Version 1511) oder höher ausgeführt wird, sollten Sie den neuen Verschlüsselungsmodus wählen.
	Neuer Verschlüsselungsmodus (am besten für Festplattenlaufwerke auf diesem Gerät geeignet)
L	🔿 Kompatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werden können)
L	
L	
	Weiter Abbrechen

Die Systemprüfung lasse ich mit durchlaufen:



Nach Abschluss des Assistenten startet die Verschlüsselung.



Weiter geht es mit dem Volume mit den virtuellen Maschinen. Auch hier starte ich die Verschlüsselung:

	erung & System und Sicherheit & Bitlocker-I	aufwerbverschlüsselung		Systemstellerung durc	bsuchen	0
	erung / System und Schemeit / Dicocker-L	adiwerkverschlusseding	ŶŬ	systemstedering dure	nsuchen	~
Startseite der Systemsteuerung	BitLocker-Laufwerkverschlüsselun	g				
	Das Schützen der Laufwerke mit BitLocker trä zu schützen.	igt dazu bei, Dateien und Ordner vor nic	ht autorisiertem Zugriff			
	Betriebssystemlaufwerk					
	System (C:) BitLocker verschlüsse	elt		\bigcirc		
		 Ändern, wie das Laufwerk beim wird Wiederherstellungsschlüssel sich BitLocker deaktivieren 	Start entsperrt Iern			
			RitLocker-Laufwerksverschlüsselung	×		
	Festplattenlaufwerke		Verschlüsselung…			
	Hyper-V (V:) BitLocker deaktivier	t	Laufwerk "C:": 10.5 % abgeschlos	isen		
		BitLocker aktivieren				
				Schließen		
	Wechseldatenträger - BitLocker To	Go	BitLocker verwalten			
	Schließen Sie einen USB-Speicherstick an,	um BitLocker To Go zu verwenden.				

Dieses Volume ist nicht das Startvolume. Es soll aber mit diesem automatisch entsperrt werden:

÷	RitLocker-Laufwerkverschlüsselung (V:)
	Methode zum Entsperren des Laufwerks auswählen
	Kennwort zum Entsperren des Laufwerks verwenden
	Kennwörter sollten Groß- und Kleinbuchstaben, Zahlen, Leerzeichen und Symbole enthalten.
	Kennwort eingeben
	Kennwort erneut eingeben
	Smartcard zum Entsperren des Laufwerks verwenden
	Sie müssen Ihre Smartcard einstecken. Die Smartcard-PIN ist erforderlich, wenn Sie das Laufwerk entsperren.
	Laufwerk auf diesem Computer automatisch entsperren
	Weiter Abbrechen

Auch dieser Wiederherstellungsschlüssel landet im AdminShare:



÷	🏘 BitLocker-Laufwerkverschlüsselung (V:)		×					
	Wie soll der Wiederherstellungsschlüss	el gesichert werden?						
	Wenn Sie das Kennwort vergessen oder die Smartca Wiederherstellungsschlüssels auf das Laufwerk zug	ard verlieren, können Sie mithilfe reifen.	e eines					
	→ Auf USB-Speicherstick speichern	🍕 BitLocker-Wiederherstellu	ngsschlüssel speichern unter					×
		← → × ↑ 📙 « Frei	gaben (M:) > AdminArea > Sicherheit > Bitlo	cker	√ Ö	"Bitlocker" d	urchsuchen	Q
	-> In Datei <u>s</u> peichern	Organisieren 👻 Neuer	Ordner					?
	ightarrow Wiederherstellungsschlüssel druck	🏰 System (C:) \land	Name	Änderungsdatum	Тур	(Größe	^
		DVD-RW-Laufv	2012-11-03 BitLocker-Wiederherstellungs	03.11.2012 21:28	Textdoku	ment	2 KB	- 11
		🛖 Freigaben (M:)	2013-07-04 BitLocker-Wiederherstellungs	04.07.2013 18:51	Textdoku	ment	2 KB	
		🔒 AdminArea	2013-09-08 BitLocker-Wiederherstellungs	08.09.2013 17:31	Textdoku	ment	2 KB	- 11
		Geräte	2013-12-27 BitLocker-Wiederherstellungs	27.12.2013 19:03	Textdoku	ment	2 KB	
		Lizenzen	2013-12-27 BitLocker-Wiederherstellungs	27.12.2013 18:59	Textdoku	ment	2 KB	- 11
	Wie finde ich später meinen Wiederherstellungssch	Netzwerk	2016-04-13 WS-CL6 NVMe.TXT	13.04.2016 20:49	Textdoku	ment	2 KB	- 1
-		- Freedowerk	📄 2016-04-13 WS-CL6 Samsung EVO 840 L	13.04.2016 08:24	Textdoku	ment	2 KB	
		Services	2017-11-16 WS-CL6 LWE D78651B6-9046	16.11.2017 19:01	Textdoku	ment	2 KB	
		Sicherheit	2017-11-17 WS-CL6 LWC C023662C-158A	17.11.2017 07:59	Textdoku	ment	2 KB	
		BenutzerZ	2017-11-18 WS-CL1 LWC 3F3F3063-6864	18.11.2017 22:19	Textdoku	ment	2 KB	
		Bitlocker Y	2017-11-25 WS-CL1 LWC 3E0DD998-C15E	25.11.2017 10:17	Textdoku	ment	2 KB	× ×
		Dateiname: 2020-0	2-06 WS-HV3 LWV BitLocker-Wiederherstellungsso	hlüssel F1EC0D0C-EC	81-4454-8F6	0-40C4F9DE25	F1.TXT	\sim
		Dateityp: Textdat	teien (*.txt)					~
		∧ Ordner ausblenden				Speicherr	Abbre	chen

Das Volume ist neu und kaum belegt. Daher wähle ich die schnelle Variante. Bei normalen Daten könnten ggf. einzelne Fragmente ausgelesen werden. Bei mir liegen aber VHDX Contailerfiles auf dem Volume. Deren Fragmente sind durch die logische, interne Struktur so gut wie ausgeschlossen lesbar:

	X
←	RitLocker-Laufwerkverschlüsselung (V:)
	Auswählen, wie viel Speicherplatz des Laufwerks verschlüsselt werden soll
	Bei der Einrichtung von BitLocker auf einem neuen Laufwerk oder PC muss nur der derzeit verwendete Teil des Laufwerks verschlüsselt werden. Beim Hinzufügen neuer Daten werden diese von BitLocker automatisch verschlüsselt.
	Falls Sie BitLocker auf einem bereits verwendeten PC oder Laufwerk aktivieren, sollten Sie das gesamte Laufwerk verschlüsseln. Durch die Verschlüsselung des gesamten Laufwerks wird der Schutz aller Daten sichergestellt. Dazu gehören auch gelöschte Daten, die möglicherweise immer noch abrufbare Informationen enthalten.
	Nur verwendeten Speicherplatz verschlüsseln (schneller, optimal für neue Computer und Laufwerke)
	 Gesamtes Laufwerk verschlüsseln (langsamer, aber optimal für PCs und Laufwerke, die bereits verwendet werden)
	Weiter Abbrechen

Der Rest des Assistenten ist Standard:

	;
÷	🏘 BitLocker-Laufwerkverschlüsselung (V:)
	7
	Zu verwendenden verschlusselungsmodus auswahlen
	Mit Windows 10 (Version 1511) wird ein neuer Datenträger-Verschlüsselungsmodus (XTS-AES) eingeführt. Dieser Modus unterstützt zusätzliche Integrität, ist mit älteren Windows-Versionen aber nicht kompatibel.
	Bei einem Wechseldatenträger, den Sie mit einer älteren Windows-Version verwenden möchten, sollten Sie den kompatiblen Modus wählen.
	Bei einem Festplattenlaufwerk oder einem Laufwerk, das nur mit Geräten eingesetzt wird, auf denen Windows 10 (Version 1511) oder höher ausgeführt wird, sollten Sie den neuen Verschlüsselungsmodus wählen.
	Neuer Verschlüsselungsmodus (am besten für Festplattenlaufwerke auf diesem Gerät geeignet)
	○ Kompatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werden können)
	Weiter Abbrechen

Jetzt ist der Inhalt des Datenträgers offline geschützt:

VS IT-Solutions

RitLocker-Laufwerkverschlüsselun	g			_		×
← → × ↑ 🏘 > Systemsteu	erung > System und Sicherheit > BitLocker-L	aufwerkverschlüsselung	~ Ō	Systemsteuerung durch	suchen	9
Startseite der Systemsteuerung	BitLocker-Laufwerkverschlüsselun	g				?
	Das Schützen der Laufwerke mit BitLocker trä zu schützen.	gt dazu bei, Dateien und Ordner vor nicht autorisiertem Zugriff				
	Betriebssystemlaufwerk					
	System (C:) BitLocker aktiviert			\odot		
		 Schutz anhalten Ändern, wie das Laufwerk beim Start entsperrt wird Wiederherstellungsschlüssel sichern BitLocker deaktivieren 				
	Festplattenlaufwerke					
	Hyper-V (V:) BitLocker aktiviert			\odot		
		 Wiederherstellungsschlüssel sichern Kennwort hinzufügen Smartcard hinzufügen Automatische Entsperrung deaktivieren BitLocker deaktivieren 				

Absicherung mit DUO-2FA

Aber auch den Online-Zugriff auf das laufende Betriebssystem möchte ich absichern. Dazu implementiere ich für die Anmeldung lokal und via RDP eine Zweifaktor-Authentifizierung. Als Anbieter wählte ich vor einiger Zeit DUO – für kleine Strukturen ist die Lösung kostenfrei.

Im DUO-Onlineportal existiert noch der alte Anmeldeschutz des Servers WS-RDS3. Jede Absicherung im DUO wird als Application bezeichnet:

DU O	Q. Search for users, groups, applications	, or devices	sw st	ephan.walther ID:	Stephan Walther 🗸
Dashboard Policies	Dashboard > Applications				
Applications Protect an Application	Applications				Protect an Application
Users				Export V Q Se	earch
Groups 2FA Devices	Name 🔺	Туре	Application Policy	Group Policies	
Administrators	RD-Gateway	Microsoft RD Gateway			
Reports	RDP on WS-HV1	Microsoft RDP			
Settings Billing	RDP on WS-HV2	Microsoft RDP			
Support	RDP on WS-RDS1	Microsoft RDP			
<u>Upgrade your plan</u> for support. Account ID	RDP on WS-RDS3	Microsoft RDP			
	RDP WS-RDS1	Microsoft RDP			

Nach der Auswahl dieser Application kann ich sie löschen:

WS IT-Solutions

DUO	 Search for users, groups, applications, or devices 	stephan.walther ID: Contraction Stephan Walther V
Dashboard	Dashboard > Applications > RDP on WS-RDS3	
Policies	RDP on WS-RDS3	Authentication Log In Remove Application
Applications		
Protect an Application	See the RDP documentation of to integrate Duo into your Microsoft RDP deployment.	
Users		
Groups		
2FA Devices	Details	Reset Secret Key

Anschließend erstelle ich eine neue Application:

DU o	Q Search for users, groups, a	applications, or devices	sw) step	nan.walther ID:	her 🗸
Dashboard	Dashboard > Applications				
Policies	Applications			Detect on Applicat	
Applications	Applications				
Protect an Application					
Users				Export V Search	
Groups	Name 🔺	Туре	Application Policy	Group Policies	
2FA Devices					
Administrators	RD-Gateway	Microsoft RD Gateway			

Im nächsten Schritt wähle ich einen passenden Typ aus. Die RDP-Application kann Rmeotezugriffe und lokale Anmeldungen absichern:

Bilt	Search for use	ers, groups, applications, or devices		so stephan.waither ID:	Stephan Walther 🗸
Dashboard	Dashboard > Appl	ications > Protect an Application			
Policies	Drotoot	an Application			
Applications	FIOLECI	an Application			
Protect an Application	microsoft				
Users					
Groups		Microsoft Azure Active Directory	Protect this Application	Read the documentation 🗳	
2FA Devices					
Administrators					
Reports		Microsoft OWA	Protect this Application	Read the documentation 🗹	
Settings					
Billing			B		
		MICrosoft RD Gateway	Protect this Application	Read the documentation L	
Support					
Account ID		Microsoft RD Web	Protect this Application	Read the documentation M	
			i i otoot tino rippiloadori i j		
Deployment ID Feeting 더					
Helpful Links		Microsoft RDP	Protect this Application	Read the documentation 🗗	
Documentation User Guide C	-				

Details zur Einrichtung gibt es hinter diesem Link. Dort steht auch der Download der msi-Installationsdatei für den Zielserver zur Verfügung:

ÐUÐ	Q Search for users, groups, applications, or devices	😻 stephan.waither ID: 🖤 Stephan Waither 🗸
Dashboard Policies	Successfully added Microsoft RDP to protected applications. Add another.	
Applications Protect an Application Users	Dashboard > Applications > Microsoft RDP Microsoft RDP	Authentication Log 🗐 Remove Application
Groups 2FA Devices Administrators	See the RDP documentation C to integrate Duo into your Microsoft RDP deployment.	
Reports	Details	Reset Secret Key

Ich lade die aktuelle msi-Datei herunter:

WS IT-Solutions

+

Product Use	Cases Pricing About Partners Resources Docs Support Contact Sales Free Trial
Contents	Security key (U2F) support is limited to Offline Access only.
Important Notes	
System Requirements	First Steps
Duo Factor support	•
First Steps	Before moving on to the deployment steps, it's a good idea to familiarize yourself with Duo administration
Enroll a User	concepts and features like options for applications, available methods for enrolling Duo users, and Duo policy
Run the Installer	settings and how to apply them. See all Duo Administrator documentation.
Test Your Setup	1 Sign up for a Duo account.
Offline Access	
Jpdating Duo Authentication for Vindows Logon	2 Log in to the <u>Duo Admin Panel</u> and navigate to Applications .
Advanced Deployment and Configuration using Group Policy	3 Click Protect an Application and locate Microsoft RDP in the applications list Click Protect this
Froubleshooting	Application to get your integration key, secret key, and API hostname. (See Getting Started for help.) Yo
letwork Diagram	will need this information to install the Duo application.
Related	We recommend setting the New User Policy for your Microsoft RDP application to Deny Access, as no
Instructions	unenrolled user may complete Duo enrollment via this application.
FAQ	
Release Notes	5 Download the Duo Authentication for Windows Logon installer package. View checksums for Duo downloads here.
AD Group Policy	
	6 If you'd like to enable <u>offline access</u> with Duo MFA you can do that now, or return to the Admin Panel later to configure offline access after first verifying logon success with two-factor authentication

Das Setup starte ich auf dem neuen WS-HV3. Hier werden einige Fragen gestellt, für die ein wenig Hintergrundwissen sinnvoll ist. Der Anmeldeprozess wird durch die Installation verändert:

- Bei einer Anmeldung am System wird zuerst ganz regulär die Kombination aus Benutzername und Passwort geprüft. Ist diese falsch, dann gibt es die bekannte Fehlermeldung.
- Ist die Anmeldung aber korrekt, dann wird das Plugin von DUO gestartet. Es sendet an einen API-Hostname (FQDN eines Servers im Internet) eine Anmeldeanfrage für den aktuellen Benutzernamen.
- Die Cloudkomponente prüft, ob der Account bekannt ist und ob für ihn ein zweiter Faktor registriert ist.
- Dann wird eine Push-Notification an die Smartphone-App des Benutzers gesendet.
- Bestätigt der Benutzer die Anmeldung am Smartphone, dann sendet die App an die Cloudkomponente das OK zurück.
- Diese wiederum kommuniziert mit der noch offenen Verbindung zum DUO-Plugin auf dem Server und reicht das OK durch.
- Erst dann wird die Anmeldung fortgesetzt.

IT-Solutions

Jede Unterbrechung, Fehlkonfiguration oder Verzögerung (es gibt Timeouts) wird dazu führen, dass die Anmeldung am Server fehlschlägt.

Jetzt ist der Dialog des Setup auf dem Server etwas sprechender, oder?

WS IT-Solutions



Für die Anmeldung ist eine ausgehende Internetverbindung erforderlich. In meinem Netzwerk ist in der zentralen Firewall erst einmal nichts erlaubt. Das gilt auch für die DUO-Authentication. Ich habe für diese eine eigene Regel mit einer Gruppe erstellt. Hier trage ich temporär die IPv4 des Servers ein. Die Adresse werde ich nach dem Umzug des Servers in seinen Standort wieder entfernen:

· ►	0 /558.09 MiB	IPv4 TCP	ServerOut_TCP	980 * *		Ports_HTTP *	none	HTTP ins Internet erlaubt	℄ℰℿ℧ ℿ
	0 /0 B	IPv4 UDP	ServerIn_WDS	Alias details				WDS Callback	≟∥⊡⊘ ∎
	1 /107 KiB	IPv4 TCP	ServerOut_ DuoSecurity	Value 192.168.110.16 192.168.100.10	Description WS-RDS1 WS-HV2			Zugriff DuoSecurity	≟∥⊡⊘ ∎
	0 /88 KiB	IPv4 TCP	ServerOut_ MXServer	192.168.100.9 192.168.100.150	WS-HV1 Entry added Mon,	06 Jan 2020 12:50:	29 +0100	MXUpdate HTTPS	±∥⊡0 ∎
 				· -					1 460

Der API-Hostname bleibt für die Application immer gleich. Eine Firewall-Ausnahme ist also sehr einfach konfigurierbar. Ich lese den Hostname aus dem DUO-AdminPortal aus. Hier gibt es auch den Integration Key, der meine Installation eindeutig dieser Application zuordnet. Und auch das Plugin muss sich am API-Hostname anmelden. Dazu wird der Secret-Key verwendet:

DUƏ	Q Search for users, groups, a	pplications, or devices	s	stephan.waither ID:	Stephan Walther 🗸
Dashboard					
Policies	Successfully added Microso	ft RDP to protected applications. Add another.			
Applications	Dashboard > Applications > M	icrosoft RDP			
Users	Microsoft RD	P		Authentication Log	Remove Application
Groups					
2FA Devices	See the RDP documentation	n 🗹 to integrate Duo into your Microsoft RDP deployn	ient.		
Administrators					
Reports	Details				Reset Secret Key
Settings	Integration key		select		
Billing					
	Secret key	Click to view.	select		
Support Upgrade your plan for support.		Don't write down your secret key or share it with anyone.			
Account ID	API hostname	duosecurity.com	select		

Gleichzeitig mit dem Auslesen der 3 Werte aktiviere ich noch den Offline-Zugriff. Mit diesem kann ich das Plugin bei der Anmeldung mit einem Offline-Token bestätigen. Das ist bei Netzwerkproblemen sehr hilfreich:

Offline access	Offline login and enrollment is enabled These settings will take effect the next time the application connects to the internet.
Limit access by groups	Only allow offline login from users in certain groups Select groups If Permitted groups is enabled, users must also be members of a permitted group to be allowed to log in offline.
Prevent offline login after	10 offline logins 7 days offline These counts reset each time the application connects to the internet
Offline authentication methods	Duo Mobile Passcode Security Key When offline, these settings override all other authentication method policies.

Die im Portal ausgelesenen Werte gebe ich in das Setup am Server ein:

> 📌 Schnellzugriff	ivame	Anderungsdatum Typ	GIODE
✓ 🛄 Desktop	🕞 duo-win-login-4.0.7.exe	06.01.2020 12:47 Anwendung	7.674 KB
> 🤱 Walther, Stephan - T1			
🗸 💻 Dieser PC	🖟 Duo Authentication for Windows	Logon x64 - InstallShield Wizard	×
> 🏰 System (C:) > 🥥 DVD-RW-Laufwerk (D:) > 🜩 Freigaben (M:)	Duo Security Account Details Please enter the keys provided by D		•
> 🛃 AdminArea	Integration Key:		-
> 🔊 Bibliothek > 📄 Business	Secret Key:		
> 🗾 Jungbrunnen > 🗾 Privat	These keys can be found in the <u>Duo</u> a Microsoft RDP application.	Admin Panel under Applications, configure or select	
> 🌄 Programmierung > 🌄 Software			
> Storage			
> 🛃 Zwischenablage	Please refer to the Duo Windows Lo	gon <u>documentation</u> for more information.	
> 🚔 Hyper-V (V:)	InstallShield	(Bed) Next > Coord	
> Ribliotheken		< DACK Next > Cance	<u></u>

Ich erlaube keinen Bypass. Dabei würde nach Ablauf eines Timeouts das Plugin auch ohne Onlinebestätigung die Anmeldung des Benutzers fortsetzen. Mit einem lokalen Zugriff auf den Server könnte ich also den Netzwerkstecker bei der Anmeldung ziehen und der zweite Faktor wäre umgangen – natürlich wäre Benutzername und Passwort immer noch notwendig. Aber auch mit einem RDP-Connect wäre es denkbar, dass ich den API-Hostname mit einem Denial-of-Service kurzfristig lahmlege. Dafür müsste ich wissen, welchen FQDN dieser geheime Server hat. Aber er wird ja mittels DNS aufgelöst – im Klartext. Kontrolliere ich als Angreifer einige Netzwerkkomponenten, dann wäre das Denkbar. Nein, das ist keine Option. Abgesehen davon verwende ich den Offline-Zugriff über die Offline-Tokens.

Die zweite Option erlaubt es dem Plugin, auch lokale Anmeldungen abzusichern:

WS IT-Solutions



Den Smartcard-Support habe ich beim ersten Setup vergessen. Daher funktioniert später ein anderes, abgesichertes Anmeldeverfahren nicht. Ich lasse die Bilder aber mal im Protokoll drin. Auch aus Fehlern kann man lernen:

🖈 Schnellzugriff	Name	Anderungsdatum	Тур	Größe		
Desktop	🕞 duo-win-login-4.0.7.exe	06.01.2020 12:47	Anwendung	7.674 KB		
a Walther, Stephan - T1						
Dieser PC	😸 Duo Authentication for Windows I	.ogon x64 - InstallShield W	izard	×		
System (C:)	Due integration entions					
DVD-RW-Laufwerk (D:)	Configure the behavior for the Count	Card and day				
🛖 Freigaben (M:)	Configure the behavior for the smart	Card provider				
AdminArea						
Backup	Enable Smart Card support	Enable Smart Card support				
🛃 Bibliothek						
Business	Protect smart card login with Duo					
🛃 Jungbrunnen	two-factor authentication.	Both smart card and username/password primary login is followed by Duo two-factor authentication.				
Privat	O Enable smart card login	C Enable smart card login without Duo				
Programmierung	Allow use of the Windows password login with Duo ty	Allow use of the Windows smart card login provider as an alternative to password login with Duo two-factor authentication.				
Software						
Storage						
	Please refer to the Duo Windows Log	on <u>documentation</u> for more i	nformation.			
🚔 Hyper-V (V:)	InstallShield					
🐂 Bibliotheken		< <u>B</u> ack N	ext > Can	:el		
A Netzwerk	L					

Das war auch schon alles. Mein administrativer Account ist bereits bei DUO mit meinem Smartphone assoziiert. Daher kann ich direkt in den Test einsteigen. Ich melde mich als Admin erneut am Server an. Benutzername und Passwort sind korrekt, daher wird das Plugin gestartet:

O Duo Security	Device: P-Stephan (+XX XXXX	× × × × × × × × × × × × × × × × × × ×	Weever,
	Choose an authentication method		
Powered by Duo Security	고 Duo Push	Send Me a Push	
	ලීා Call Me	Call Me	P- 342
	Passcode	Enter a Passcode	
Pushed a login request	to your device	Cancel	-1816 - 1944

Ich bestätige am Smartphone die Anmeldeanfrage. Damit bin ich für die Anmeldung autorisiert. Mit dem Connect zum Cloudserver hat das Plugin aber den gewünschten Offline-Zugriff erkannt und startet die Einrichtung:





Ich nutze dafür die gleiche DUO-Mobileapp wie für die Online-Anfragen. Die Einrichtung ist denkbar einfach. Mit der App scanne ich den gezeigten QR-Code:



Anschließend zeigt mir die App den ersten Zahlencode. Diesen gebe ich zur Bestätigung ein:

😑 Duo Security		×
Powered by Duo	Two-Factor Authentication Enter your six-digit passcode:	
	Back to QR Code	Activate Offline Login

Das war es auch schon. Diese Hürde ist hoch. Angriffe auf das System sollten nahezu unmöglich sein. Und das mit relativ viel Komfort!

Absicherung mit Notfall-Account und vSmartcard

VS IT-Solutions

Die nächste Absicherung ist ein spezielles Notfall-Szenario in meiner Infrastruktur. Folgende Punkte erfordern diese Lösung:

- Meine Infrastruktur hat ausschließlich virtuelle Domain Controller. Diese laufen auf unterschiedlichen Hyper-V-Hosts.
- Meine administrativen Accounts haben keine Rechte auf den Hyper-V-Hosts. Die Rechte vergebe ich nur temporär mit einer Privileged Access Management Lösung. Dieses PAM benötigt Zugriff auf die Domain Controller (denn da werden die Gruppenmitgliedschaften verändert).
- Meine administrativen Accounts sind Mitglied der Gruppe "Protected Users". Daher werden erfolgreiche Anmeldungen nicht zwischengespeichert. Für jede Anmeldung ist der Kontakt zu einem Domain Controller erforderlich.
- Jeder Server hat bei mir genau einen lokalen, administrativen Account. Deren Passworte werden durch LAPS (Local Administrator Password Solution) regelmäßig verändert. Die aktuellen Passworte kann ich in den Domain Controllern auslesen.

Und mit diesen Konfigurationen wird das Problem erkennbar: Ich benötige für jede Anmeldung zwingend eine Verbindung zu einem Domain Controller! Das ist ja eigentlich auch wünschenswert. Es existieren aber eine Reihe von Problemszenarien:

- Nach einem Stromausfall, der meine USV-Kapazität übersteigt, könnten die Hyper-V-Hosts Probleme beim Hochfahren der virtuellen Domain Controller haben. Und ich kann mich nicht anmelden, um zu helfen.
- Fehler im Active Directory könnten zum gleichen Problem führen.

Beide Fälle habe ich bereits durchlebt. Bisher konnte ich immer über Umwege auf einen Domain Controller im anderen Standort zugreifen und so das Passwort des lokalen Admins auslesen. Aber da war auch immer viel Glück im Spiel. Daher habe ich einen speziellen AdminAccount erstellt: den admin-notfall. Dieser Account ist stark eingeschränkt:

- Er kann sich ausschließlich auf den Hyper-V-Hosts anmelden
- Auf den Hyper-V-Hosts hat er keine administrativen Systemrechte, kann aber den Service Hyper-V administrieren.
- Er benötigt für die Anmeldung eine Smartcard.
- Er ist aber kein Mitglied der Gruppe "Protected User". Daher kann jeder Hyper-V-Host seine Anmeldung zwischenspeichern.

Mit diesem Account kann ich mich auf einem Hyper-V-Host anmelden und den virtuellen Maschinen (also auch den Domain Controllern) Starthilfe geben. Ich verwende virtuelle Smartcards. Diese muss ich auf jedem Computer neu erstellen. Dazu muss ich mich mit dem Account einmal ohne Smartcard anmelden. Ich entferne also die Option:

Active Directory-Benutzer und -Computer		
Datei Aktion Ansicht ?		
← ⇒ 2 📰 🠇 📋 🗙 🗒 🖬 📓 🖬 📍	l 🐮 👕 🍸 🔟 🐍	
Active Directory-Benutzer und -Computer [WS-DC1.ws.it	Name	Typ Beschreibung
> 🧮 Gespeicherte Abfragen	🚰 admin	Benutzer Admin ATA Probe
✓ III ws.its	🔏 admin-ata	Benutzer Admin ATA
> Builtin	🛃 admin-audit	Benutzer Nessus-Audit-Account
> Computers	🛃 admin-backup	Benutzer Backup Reader
Domain Controllers Economy Security Drive size la	Administrator	Benutzer DefaultAdmin
	admin-Notfall	Benutzer NotfallAccount für externe Einwahl
LostAndFound	🛃 admin-setup	Denutere Admin Agrount für Setup
Managed Service Accounts	🐣 Walther, Stephan - T1	Eigenschaften von admin-Notfall ? X count für Stephan - Server
> 📓 Microsoft Exchange Security Groups	🐣 Walther, Stephan - T2	W 100 ut to 7 ut to 10 the total 10 us total to 10 the The The The
> 🧮 Program Data		Objekt Sieherteit Umachung Sitzungen
> 🧮 System		Bemotauliberwachung Bemotadeektoodianeta-Profil COM+ Attribut-Editor
> 🛗 Users		Allaemein Adresse Konto Profil Bufnummern Organisation
✓ 💼 WS		
✓ I AdminArea		Benutzeranmeldename:
Benutzer		admin-Notfall @ws.its ~
> Gruppen		Benutzeranmeldename (Prä-Windows 2000):
Suctem		WS\ admin-Notfall
> Benutzer		
> Clients		Anmeldezeiten Anmelden an
> 📓 Exchange-Objekte		
> 🗊 Gruppen		Kontosperrung aufheben
> 🖬 Server		
> Microsoft Exchange System Objects		Kontooptionen:
> MTDS Quotas		Kennwort mit umkehrbarer Verschlüsselung speichem
> C TPM Devices		Konto ist deaktiviert
		Benutzer muss sich mit einer Smartcard anmelden
		Konto ist vertraulich und kann nicht delegiert werden.
		Konto läuft ab



Mit meinem administrativen Account bereite ich im TPM-Chip eine neue, virtuelle Smartcard vor. Das geht nicht in einer RDP-Sitzung. Ich wechsle also in eine lokale Anmeldung:



Dann melde ich mich als admin-notfall am Server lokal an. Die Berechtigung dazu habe ich bereits im Active Directory über AD-Gruppen und Gruppenrichtlinien auf die Hyper-V-Server konfiguriert. Das ist ja auch schon der dritte Server.

Jetzt fordere ich ein neues Smartcard-Zertifikat an:

🛃 Windows PowerShell				- 0	×			
Windows PowerShell Copyright (C) Microsoft Corporation. Alle	Rechte vorbehalten.				^			
PS C:\Users\admin-notfall> certmgr.msc PS C:\Users\admin-notfall>								
Section - [Zertifikate - Aktueller Datei Aktion Ansicht ?	Benutzer\Eigene Zertifikate\Zertifikate]	ŊII.				-		×
 Zertifikate - Aktueller Benutzer Eigene Zertifikate Zertifikate Zertifikate Vertrauenswürdige Stammzer 	Ausgestellt für 🔨	Ausgestellt WS-ITS-Ze	von rtifizierungsstelle-CA1	Zertifikatvorlage WS-ITS-Benutzer-V2	Ablaufdatum 05.01.2021	Beabsichtigte Zwec Clientauthentifizier	Anzeigena <keine></keine>	ame
> Crganisationsvertrauen > C Zwischenzertifizierungssteller	Alle Aufgaben	>	Neues Zertifikat anfo	rdern				
> Active Directory-Benutzerobj Vertrauenswürdige Herausgel	Aktualisieren		Importieren					
> C Nicht vertrauenswürdige Zert	Ausgestellt für Ausge admin-Notfall WS-IT Alle Aufgaben Aktualisieren Liste exportieren Ansicht		Erweiterte Vorgänge	>				
> Drittanbieter-Stammzertifizie > Vertrauenswürdige Personen	Ansicht	>						
 Clientauthentifizierungsausst Zertifikatregistrierungsanford Smotford verterungsaufford 	Symbole anordnen Am Raster ausrichten	>						
	Hilfe							
< >	<							
Fordert ein neues Zertifikat von einer Z	Zertifizierungsstelle in der Domäne an.							

Der Benutzer hat auch dafür das erforderliche Recht in meiner PKI:



➢ Windows PowerShell Windows PowerShell Copyright (C) Microsoft Corporation. Alle	e Rechte vorbehalten.			*		
PS (:\Users\admin-notfall> certmgr.msc PS C:\Users\admin-notfall>	r Benutzer\Eigene Zertifikate\Z	Zertifikate]				X
Zertifikate - Aktueller Benutzer Eigene Zertifikate Zertifikate Organisationsvertrauen Curschenzertfizierungsstelle Active Directory-Benutzerob Nicht vertrauenswürdige Zer Dirttanbieter-Stammzertifizie Vertrauenswürdige Personen Clientauthentifizierungsauss	Ausgestellt für admin-Not Zertifik Folg klick	Ausgestellt von satregistrierung tifikate anfordern ende Zertifikattypen sind abrufbar. V en Sie anschließend auf "Registriere 'S IT-Solutions Zertifikatverteilung	Zertifikatvorlage Vählen Sie die Zertifikate aus, die 1 ".	Ablaufdatum 	Beabsichtigte Zwec.	. Anzeigename <keine></keine>
 Zertifikatregistrierungsanfor Tantcard vertrauenswürdig Smartcard vertrauenswürdig Der Speicher "Eigene Zertifikate" enth 	a alt 1 Zertifikat.] WS-ITS-Benutzer-V2] WS-ITS-SmartCard] Alle Vorlagen anzeigen	(i) STATUS: Verfügbar (i) STATUS: Verfügbar		Details V Details V	

Die Vorlage habe ich so erstellt, dass Zertifikate auf einem entsprechenden Key Storage Provider gespeichert werden müssen. Hier meldet sich gleich die neue, virtuelle Smartcard. Das Zertifikat wird mit der PIN geschützt, die ich vorhin beim Erstellen eingegeben habe:

🔀 Windows PowerShell			- 0	×		
Windows PowerShell Copyright (C) Microsoft Corporation. Alle	Rechte vorbehalten.			^		
PS C:\Users\admin-notfall> certmgr.msc PS C:\Users\admin-notfall>						
Datei Aktion Ansicht ?	Benutzer\Eigene Zertifikate\.	Zertifikate]			9-	×
🗢 🄿 🙋 📷 🗈 🛛 🐼 🕞 🛛	? 🖬					
Zertifikate - Aktueller Benutzer	Ausgestellt für	Ausgestellt von	Zertifikatvorlage	Ablaufdatum	Beabsichtigte Zwec	Anzeigename
Zertifikate Vertrauenswürdige Stammzer Granisationsvertrauen Zwischenzertifizierungssteller Active Directory-Benutzerobj Vertrauenswürdige Herausgel Nicht vertrauenswürdige Zertifizie Oritanbieter-Stammzertifizie Vertrauenswürdige Personen Clientauthentifizierungsansford Smartcard vertrauenswürdige	Zertifi Zer Zun V V V	tifik Windows-Sicherheit Red Registrierung für: W Geben Sie Ihre PIN ein.	/S-ITS-SmartCard	zu	erhalten.	<rene></rene>
Der Speicher "Eigene Zertifikate" enth	ält 1 Zertifikat.	ОК	Abbrech	nen		
				3.3 		

Und das war es auch schon. Die Smartcard mit dem Zertifikat ist einsatzbereit:





Jetzt aktiviere ich die Anforderung "Smartcard erforderlich" wieder im Active Directory. Das Passwort des Accounts genügt nicht mehr:



Die lokale Berechtigung zum Steuern des Hyper-V-Services habe ich nicht zentralisiert. Daher editiere ich die lokale Gruppe mit dem Administratoraccount:

WS IT-Solutions

🔙 Computerverwaltung		- D >	<
Datei Aktion Ansicht ?			
🗢 🄿 🖄 📰 🔀	2 1		
Computerverwaltung (Lokal)	Name Beschreibung	Aktionen	_
V 👔 System	Administratoren Administratoren haben uneingesc	Gruppen	
> 🕒 Aufgabenplanung > 🛃 Ereignisanzeige	Benutzer Eigenschaften von Hyper-V-Administratoren Y Spistributed CC	Weitere Aktionen	۲
> 👔 Freigegebene Ordner	Weight Allgemein	Hyper-V-Administratoren	•
 Eckale Benutzer und Gn Benutzer Gruppen Seräte-Manager Datenspeicher Windows Server-Sicheru Datenträgerverwaltung Dienste und Anwendungen 	Ereignisprotok Gerätebesitzer Gäste Gäste Hauptbenutze Hyper-V-Adm Beschreibung: Die Mitglieder dieser Gruppe erhalten Uneingeschränkten Zugrff auf sämtliche Features von Mitglieder: Leistungsproto Kryptografie-C Mitglieder: Leistungsproto RoDS-Endpunk RDS-Remoteze Remotedeskto Remotedeskto Remoteverwal Replikations-C Mitglieder: Anderungen der Gruppennitgliedschaft	Weitere Aktionen	•
	Arr Storage Repl. / Hinzufugen Entemen ues benutzers werden erst bei der nächsten Anmeldung wirksam. Arr Zertifikatdiens OK Abbrechen Übernehmen Hife		

Den Testlauf führe ich später durch.

Konfiguration der Datensicherung – Windows Server Sicherung

Wie bei jedem neuen Server ist auch hier eine Datensicherung erforderlich. Die Systemstate-Sicherung übernimmt wieder meine Scriptlösung um die Windows Server Sicherung. Den Sicherungstask importiere ich wie üblich aus einer fertigen xml-Datei:



Und wie üblich trage ich einen Dummy-Account als Prinzipal ein:



Aufgabenplanung								— [• ×
Datei Aktion Ansicht ?		Aufgabe erstellen					×		
Aufgabenplanung (Lokal)	Name	Allgemein Trigger	r Aktionen Be	dingungen Einstel	lungen			nen	
	() User_Feed_	Name:	ServerSicherun	g				benplanungsbibliothek	
		Speicherort:	N					infache Aufgabe erstellen	
		Autor:	WS\stephan					ufgabe erstellen	
		Beschreibung:						ufgabe importieren	
				Aufgabenplanung	?	×		Ille aktiven Aufgaben anzeigen	
	<					2		erlauf für alle Aufgaben deaktivieren	
				J.V				leuer Ordner	
		Sicherheitsoption	ien					insicht	•
		Beim Ausführen	der Autgaben tol	Geben Sie Benutzer	contoinformationen zum Ausführe	en dieser		ktualisieren	
		WS\admin-setup		Adigabe elli.			be andern	lilfe	
		O Nur ausführer	n, wenn der Beni	Benutzername:	😨 WS\admin-setup	×			
		Unabhängig v	/on der Benutzer	Kennwort:	•••••				
		Kennwort	nicht speichern.						
		Mit höchsten	Privilegien ausfü						
		Ausgeblendet	Konfigurieren		OK Abb	orechen	~		

Danach wechsle ich auf meinen Domain Controller und richte den Group Managed Service Account für die Sicherung ein. Mein GUI-Script hilft mir dabei. Hier entferne ich zuerst den alten Server WS-RDS3:

🖕 gMSA-Admin		– 🗆 ×
vorhandene gMSA:	zugehörige Server:	zugehörige Gruppen:
gMSA-ADFS (Service ADFS) gMSA-Backup (TaskUserfur BMR) gMSA-Montor (TaskUserfur Monitoring) gMSA-SQLDPM (Service SQL auf WS-DPM)	WS-DC1.ws.its WS-HX1.ws.its WS-MX1.ws.its WS-MX2.ws.its WS-HX2.ws.its WS-RDS2.ws.its WS-RDS2.ws.its WS-DC2.ws.its WS-DC2.ws.its WS-DC2.ws.its WS-DC2.ws.its WS-DC2.ws.its WS-DPM.ws.its WS-DPM.ws.its WS-HV2.ws.its WS-HV2.ws.its WS-HV1.ws.its WS-HV1.ws.its WS-HV1.ws.its WS-W1.ws.its	
erstelle gMSA lösche gMSA bearbeite gMSA	weiterer Server entferne Server teste gMSA	weitere Gruppe entferne Gruppe
Einsatz als:		

Dann kommt der neue Server in die Liste:

gMSA-Admin			- 0	×
vorhandene gMSA:	zugehörige Serve	r.	zugehörige Gruppen:	
gMSA-ADFS (Service ADFS) gMSA-Backup (TaskUser für Monitoring) gMSA-Monitor (TaskUser für Monitoring) gMSA-SQLDPM (Service SQL auf WS-DPM)	WS-DC1.ws.its WS-FS1.ws.its WS-MX1.ws.its WS-MX2.ws.its WS-M22.ws.its WS-FS2.ws.its WS-RDS1.ws.its WS-RDS2.ws.its WS-DC3.ws.its	neuer Server für gMSA	direkte Gruppen: GG-SEC-Server-Monitoring-Admins GG-SEC-Server-IB-Admins GG-SEC-Server-RDS-Admins GG-SEC-Server-Standard-Admins GG-SEC-Server-HyperV-Admins GG-SEC-Clients-JB-Admins GG-SEC-Clients-JB-Admins	*
	WS-FS3.ws.its WS-DPM.ws.its WS-DPM.ws.its WS-WAC.ws.its WS-HV2.ws.its WS-ATA.ws.its WS-MON.ws.its WS-MON.ws.its	Geben Sie den Namen (nicht den FQDN) zusätzlichen Servers ein	Verschachtelung):	
	WS-NPS I.WS.Its	wo-nvaj	LD-SEC-Server-HyperV-Login LD-SEC-Server-HyperV-RDP	~
erstelle gMSA lösche gMSA bearbeite gMSA	weiterer Server	entferne Server teste gMSA	weitere Gruppe entferne Gruppe	
Einsatz als:				

Danach trage ich den neuen gMSA als Sicherungstask-User ein. Die Aktion wird über PowerShell-Remoting durchgeführt:



드 gMSA-Admin			- 🗆 X
vorhandene gMSA:	zugeł	örige Server:	zugehörige Gruppen:
gMSA-ADFS (Service ADFS) (dMSA-Backup (TaskUser für BMR) gMSA-Monitor (TaskUser für Monitoring gMSA-SQLDPM (Service SQL auf WS-) DPM) WS-R WS-R WS-F WS-F WS-F WS-F WS-C WS-C WS-C WS-C WS-C WS-C WS-C WS-C	C1.ws.its S1.ws.its IX1.ws.its IX2.ws.its IX2.ws.its IX2.ws.its IDS2.ws.its	direkte Gruppen: GG-SEC-Server-Monitoring-Admins GG-SEC-Server-RD-S-Admins GG-SEC-Server-RD-S-Admins GG-SEC-Server-RD-S-Admins GG-SEC-Server-HyperV-Admins GG-SEC-Server-HyperV-Admins GG-SEC-Server-HyperV-Admins GG-Admin-Backup Sicherungs-Operatoren indirekte Gruppen (durch Verschachtelung): LD-Admin-SGL-DPM LD-Admin-Backup LD-Admin-Backup LD-Admin-SBC-DIents-JB-Admins LD-SEC-Clients-JB-Admins LD-SEC-Clients-JB-MinRM LD-SEC-Clients-JB-WinRM LD-SEC-Clients-JB-WinRM LD-SEC-Server-HyperV-Admins LD-SEC-Server-HyperV-RDP LD-SEC-Server-HyperV-RDP LD-SEC-Server-
erstelle gMSA lösche gMSA Einsatz als: Task ~	bearbeite gMSA wei Klicke in eine Zeile um die Op	terer Server entferne Server teste	gMSA weitere Gruppe entferne Gruppe
Server	TaskName	Account	Pfad ^
WS-HV3	ServerSicherung	ws\gMSA-Backup\$	N III
WS-HV3	User_Feed_Synchronization-{1	607/35 WC UV3	X
WS-HV3	Server Initial Configuration Tas	k Erfolg X	\Microsoft\Windows\
WS-HV3	.NET Framework NGEN v4.0.3	8031	\Microsoft\Windows\.NET Framework\
WS-HV3	.NET Framework NGEN v4.0.3	1031 Der Task wurde <mark>umges</mark> tellt!	\Microsoft\Windows\.NET Framework\
WS-HV3	.NET Framework NGEN v4.0.3	8031	\Microsoft\Windows\.NET Framework\
WS-HV3	.NET Framework NGEN v4.0.3	031 OK	\Microsoft\Windows\.NET Framework\
WS-HV3	AD RMS Rights Policy Templa	te M	\Microsoft\Windows\Active Directory Rights Management Se
lese alle Server setze gMSA ein bereit			

Weil ich auf WS-HV3 gerade bei den Aufgaben bin importiere ich gleich noch eine andere Aufgabe, die alle Hyper-V-Hosts bei mir aussführen. Diese Aufgabe kopiert die Konfigurationsdateien der virtuellen Maschinen in ein Verzeichnis, dass von der SystemState-Sicherung erfasst wird:

						-	- 🗆	×
Datei Aktion Ansicht ?								
🗢 🔿 🞽 📅 🚺 🗊								
 Oufgabenplanung (Lokal) Aufgabenplanungsbibliot 	Name ServerSicherung User_Feed_Synchronization-{16074259-72DC-4958-8 Einfache Aufgabe erstellen Neue Aufgabe erstellen Aufgabe importieren Aktualisieren <	Status Bereit 429-2ECB254353DE} Bereit	Trigger Jeden Tag um 01:00 Uhr Jeden Tag um 14:52 Uhr	- Trigger läuft ur	Aktionen Aufgabenpli Image: Second	anungsbibliothek e Aufgabe erstellen e erstellen e importieren iven Aufgaben anzeiger für alle Aufgaben deakt)rdner ieren) ivieren	• •
Aufacherer known								
Datei Aktion Ansicht ?	Name	Status	Trigger		Aktionen		_ [) ×
Datei Aktion Ansicht ? Aufgabenplanung (Lokal) > Aufgabenplanungsbibliot	Name ® ServerSicherung	Status Bereit	Trigger Jeden Tag um 01:00 Uhr	r	Aktionen Aufgabenp	lanungsbibliothek	_ [× [
Datei Aktion Ansicht ? → → →	Name ServerSicherung Nature Orchaer	Status Bereit	Trigger Jeden Tag um 01:00 Uhr V (0) ("Admin" du	urchsuchen	Aktionen Aufgabenp × fact p fgat gat	anungsbibliothek ne Aufgabe erstellen be erstellen be importieren) × [
Datei Aktion Ansicht ? → → →	Name ServerSicherung Netzwerk > ws-hv2 > c\$ > Admin > NeuerOrdner	Status Bereit	Trigger Jeden Tag um 01:00 Uhr V (0) ("Admin" du	urchsuchen	Aktionen Aufgabenpu × fact gat gat a ak	lanungsbibliothek ne Aufgabe erstellen se erstellen se importieren tiven Aufgaben anzeig	[× [
Datei Aktion Ansicht ? → → ☆ □ □ ☑ □ ② Aufgabenplanung (Lokal) > ③ Aufgabenplanung sbibliot ④ Offnen ← → ~ ↑ Organisieren ~ ↓ Privat	Name ServerSicherung Netzwerk > ws-hv2 > c\$ > Admin > Neuer Ordner Name	Status Bereit Änderungsdatum	Trigger Jeden Tag um 01:00 Uhr V (0) "Admin" du Typ	urchsuchen	Aktionen Aufgabenpl × fact p fgat gat gat ak auf	lanungsbibliothek ne Aufgabe erstellen ze erstellen ze importieren tiven Aufgaben anzeig i für alle Aufgaben deal	En ctivieren	× 1
Datei Aktion Ansicht ? → → ▲ □ □ ④ □ ④ Aufgabenplanung (Lokal) → ♂ Aufgabenplanungsbibliot Ø Offnen ← → ~ ↑ Organisieren → ↓ Progr	Name ServerSicherung Netzwerk > ws-hv2 > c\$ > Admin > Neuer Ordner Name Mame Hyper-V	Anderungsdatum 11.08.2019 14:42	Trigger Jeden Tag um 01:00 Uhr V O (Typ) Dateiordner	urchsuchen BEE 🔻 🛄 Größe	Aktionen Aufgabenpl × fach gat gat gat ak lauf uer	lanungsbibliothek ne Aufgabe erstellen se erstellen se importieren tiven Aufgaben anzeigr f für alle Aufgaben deal Ordner	en ktivieren) X
Datei Aktion Ansicht ? → → 2 m 2 m 2 m Aufgabenplanung(Loka) > → Aufgabenplanungsbibliot Organisieren → Crganisieren → Drivat Aufgabenplanungsbibliot	Name ServerSicherung Netzwerk > ws-hv2 > c\$ > Admin > Neuer Ordner Name Ammier Hyper-V are	Anderungsdatum 11.08.2019 14:42 04.01.2020 01:04	Trigger Jeden Tag um 01:00 Uhr V Ø (* Admin* du Typ Dateiordner Dateiordner	urchsuchen BEE 🕶 🔲 Größe	Aktionen Aufgabenpl × fach gat gat auf uer sich	lanungsbibliothek te Aufgabe erstellen se erstellen se importieren tiven Aufgaben anzeig f für alle Aufgaben deal Ordner tt	en) ×
Datei Aktion Ansicht ? → → ♪ □ □ 2 □ → Aufgabenplanung (Lokal) → → Aufgabenplanungsbibliot → Organisieren → Organisieren → - Privat - Privat - Progr - Softw	Name ServerSicherung Netzwerk > ws-hv2 > c\$ > Admin > Neuer Ordner Name Hyper-V are ge	Anderungsdatum 11.08.2019 14:42 04.01.2020 01:04 07.08.2019 14:02	Trigger Jeden Tag um 01:00 Uhr V (C) Admin* du Typ Dateiordner Dateiordner Dateiordner	urchsuchen Größe	Aktionen Aufgabenpi X fach gat gat auf auf uer sich ual	anungsbibliothek te Aufgabe erstellen se erstellen se importieren tiven Aufgaben anzeigu 'für alle Aufgaben deak Ordner tt	en) ×
Datei Aktion Ansicht ? Aufgabenplanung (Lokal) Aufgabenplanung Sbibliot Organisieren ↓ Organisieren ↓ Progr Softw Stora Zwisc	Name ServerSicherung Netzwerk > ws-hv2 > cS > Admin > Neuer Ordner Name Ammier Ammer PSTranscript Backup-Hyper-VMs.xml	Status Status Bereit Bereit Ånderungsdatum 11.08.2019 14:42 04.01.2020 01:04 07.08.2019 19:00 06.01.2020 11:21 19:00	Trigger Jeden Tag um 01:00 Uhr V Ö "Admin" du Typ Dateiordner Dateiordner Dateiordner XML-Dokument	urchsuchen Größe 4 KB	Y Aktionen Aufgabenpi Y fact gat gat gat uer sich ual	anungsbibliothek te Aufgabe erstellen pe erstellen pe importieren tiven Aufgaben anzeigu für alle Aufgaben deak Ordner t t	en tivieren) ×

Ich starte diese Aufgabe:

WS IT-Solutions

WSHowTo – Neuinstallation von WS-RDS3 als WS-HV3 2020-01-01 Migration auf Windows Server 2019

🕑 Aufgabenplanung		- [- X
Datei Aktion Ansicht ?			
🗢 🔿 🙍 📅 🚺 🖬			
 Aufgabenplanung (Lokal) Aufgabenplanungsbibliot 	Name Statu Trigger Backup-HyperV-VMs Bereit Jeden Tag um 23:50 Uhr ServerSicherung Bereit Jeden Tag um 01:00 Uhr User_Feed_Synchronization-{16074259-72DC-4958-8429-2ECB254353DE} Bereit Jeden Tag um 14:52 Uhr - Trigger Jauft um 06:01:2030 14:52:20 ab.	Nächste Laufzeit 06.01.2020 23:50:00 07.01.2020 01:00:00 06.01.2020 14:52:20	Letzte Lauf 30.11.1999 30.11.1999 30.11.1999
	Kilonen Bedingungen Einstellungen Verlauf Beim Erstellen einer Aufgabe müssen Sie die Aktion angeben, die beim Starten der Aufgabe ausgeführt werden soll. Sie können diese Aktionen änderr Eigenschaftenseite der Aufgabe müssen Sie die Aktion Beim Eigenschaften" offnen. Aktion Details Programm starten robocopy vs.\Hyper-V C:\Admin\Hyper-V\VMConfigs /XF *.*vhd* /XF *.bin /XF *.VMRS /MIR /R:0 /LOG:C:\Admin\Hyper-V\Backstark	n, indem Sie die nekup-VMConfigs.log	>

Danach sind die Konfigurationsdateien der VMs in einem Verzeichnis unter dem Systemlaufwerk dupliziert. Mit diesen Dateien kann ich die VMs ohne deren virtuelle Festplatten wiederherstellen:



Für das Backup des SystemStates verwende ich wie bereits erwähnt eine Scriptlösung. Der lokale Task ist bereits eingerichtet. Aber die Steuerung muss mit der ini-Datei noch angepasst werden. Der neue Server WS-HV3 wird selber ein Sicherungsziel mit einer externen USB-Festplatte über eine Freigabe anbieten. Alle Server im Außenstandort werden dort hin sichern. In der ini-Datei verändere ich den Parameter und gebe den neuen Namen an:



Im zweiten Block der ini-Datei trage ich auch die Zeile des Servers selber ein. Es ist eigentlich ganz einfach: Das Script wird über den Task gestartet, sucht in der ini-Datei nach der Zeile, die mit dem Namen des Servers beginnt. In der Zeile steht am Ende eine Ziffer. Diese stellt das Sicherungsziel dar. Die Ziffer 2 verweist dann auf das SMB-Share \\ws-hv3.ws.its\BMR-HV3\$. Und dort wird dann gemäß Definition reingesichert:

Sicherur	ng.ini - Editor									-	×
Datei Bearl	beiten Form	at Ansicht H	Hilfe								
[Sicherur	ngenl										
⁰ 0ptioner	n: -ohneTa	ag									
'Server	# Delay	/ # Tage	# JobName	# JobDefinition			# Dest	# Optionen			
WS-CM	# 0	# 3@135	# BMR	<pre># c: -systemstate</pre>	-allCritical -v	ssFull	# 1	#			
WS-DC1	# 20	# 6@135	# BMR	# c: -systemstate	-allCritical -v	ssFull	# 1	#			
WS-FS1	# 40	# 3@135	# BMR	# c: -systemstate	-allCritical -v	ssFull	# 1	#			
WS-HV1	# 60	# 6@135	# BMR	# c: -systemstate	-allCritical -v	ssFull	# 3	#			
WS-NPS1	# 80	# 6@135	# BMR	# c: -systemstate	-allCritical -v	ssFull	# 1	#			
WS-MON	# 100	# 6@135	# BMR	# c: -systemstate	-allCritical -v	ssFull	# 1	#			
WS-RDS1	# 120	# 6@135	# BMR	# c: -systemstate	-allCritical -v	ssFull	# 1	#			
WS-WAC	# 140	# 3@135	# BMR	# c: -systemstate	-allCritical -v	ssFull	# 1	#			
WS-MX1	# 160	# 6@135	# BMR	# c: -systemstate	-allCritical -v	ssFull	# 1	#			
WS-HV2	# 0	# 6@246	# BMR	# c: -systemstate	-allCritical -v	ssFull	# 3	#			
WS-DC2	# 20	# 6@246	# BMR	# c: -systemstate	-allCritical -v	ssFull	# 1	#			
WS-FS2	# 40	# 3@246	# BMR	<pre># c: -systemstate</pre>	-allCritical -v	ssFull	# 1	#			
WS-RDS2	# 80	# 6@246	# BMR	<pre># c: -systemstate</pre>	-allCritical -v	ssFull	# 1	#			
WS-DPM	# 110	# 6@246	# BMR	<pre># c: -systemstate</pre>	-allCritical -v	ssFull	# 3	#			
WS-CA1	# 130	# 3@246	# BMR	<pre># c: -systemstate</pre>	-allCritical -v	ssFull	# 1	#			
WS-ATA	# 150	# 3@246	# BMR	<pre># c: -systemstate</pre>	-allCritical -v	ssFull	# 1	#			
WS-MX2	# 170	# 6@246	# BMR	<pre># c: -systemstate</pre>	-allCritical -v	ssFull	# 1	#			
WS-DC3	# 0	# 3@246	# BMR	# C: -systemstate	-allcritical -v	ssFull	# 2	#			
WS-HV3	# 0	# 3@135	# BMR	# C: -systemstate	-allcritical -v	ssFull	# 2	#			
WS-FS3	# 60	# 3@135	# BMR	# C: -systemstate	-allcritical -v	ssFull	# 2	#			

Das Sicherungsziel ist eine USB-Festplatte. Diese schließe ich jetzt an den neuen Server an. Die Freigabe existiert natürlich noch nicht. Aber das lässt sich einfach nachholen:



Zusätzlich schütze ich aber noch den Datenstrom mit SMB3-Encryption. Der Effekt ist mit dem Wechsel von http zu https vergleichbar: Die Daten können auf dem Transportweg nicht mehr im Klartext mitgelesen werden. Und das ist auch gut so. Denn auch mein virtueller Domain Controller wird in das Sicherungsziel sichern und dabei seine AD-Datenbank mit übertragen...





Die externe Festplatte selber stellt natürlich auch ein Sicherheitsrisiko dar. Daher verschlüssele ich die Partition mit Bitlocker To Go:



Konfiguration des Monitoring

Weiter geht es mit der Integration in das Monitoring. Im PRTG hatte ich die Sensoren des alten Servers WS-RDS3 pausiert:





Den Eintrag kann ich editieren. Ich verändere den Anzeigenamen und den FQDN des Zielservers:

	3eräte Biblio	heken Sen	isoren 4	Alarme	Maps	Berichte	Protokoll	Tickets	Konfiguration		
🗌 Geräte WS-ITS 💌	Server 🔻 WS-R	IS3 🔻									
Gerät WS-RDS	3 2 ****										
Ö Übersicht	t 2 Tage	30 Ta	ge 30	65 Tage	🔺 Alarr	ne	Systeminformati	onen	Protokoll	🌣 Einstellungen	🌲 Trigger für Benachrichtigungen
	Allgemeir	e Geräteeinst	ellungen								
					Name d	es Geräts 🔍	WS-HV3				
						Oberture ()	Contartat				
						Status	Obestarter				
							Pausiert				
						P-Version	IPv4-Geröt				
						Veraion	O IT IT OCIUL				
							O IPv6-Gerat				
				10	Pv4-Adrosso/D	NS-Namo 0	we had we ite				
				16	TH Mulesse/D	No Naille V	maning wo.its				
					Übergeord	nete Tags 🕕					
						Tags 🕕	0				

Die Assoziierung wird aber nicht komplett übernommen. Die Einträge für meine VMs sind nicht funktional. Und der neue Datenträger wird auch nicht erkannt. Egal, ich lösche sie und erstelle sie neu:

6	Startseite	Geräte	Bibliotheken	Sensoren	Alarme	Maps	Berichte	Protokoll	Tickets	Konfiguration			Neue Ala	irme 3 Ne
#	Geräte WS Gerät WS	SHTS ▼ Serv S-HV3 ^P ★	er ▼ WS-HV3 ▼ ★★☆☆											
	🔿 Üb	ersicht	2 Tage	30 Tage	36	5 Tage	A Alar	me	O Systeminfo	rmationen	Protokoll	🌣 Einstellung	en 🌲 Tr	rigger für B
	Wer	nn Sie hier Sens	sortachos sehen möc	hten, ändern Sie d	ie Priorität vo	n einem ode	r mehreren Sens	soren zu ★	★★☆ / ★★★★★					
	Pos. 🔻	Sensor	÷			s	tatus ≑	Nachrid	:ht			Graph	Priorität ≑	Ø
	4 1.	🗸 Нур	er-V			C	к	ОК				CPU-Last ges 1 %	***	Ø
	. ↔ 2.	Volu	ume IO C:			С	к	ок				Freier Platz % 83 %	★★★ ☆☆	Ø
	.	‼ ws-	DC3			F	ehler					CPU-Last ges Keine Daten	***	C
	++ 4.	!! ws-	FS3			F	ehler	WMI: Die	e VM ist ausgeschalt	et. (Code: PE065) - Pe	erfCounter: No data to	CPU-Last ges Keine Daten	素素素公立	Ø
	. ↔ 5.	W WS-	PFS2			v	/arnung					CPU-Last ges Keine Daten	***	Ø
	. ↔ 6.	tt Disi	< 10 0 C:			F	ehler	WMI: Ins	tanz(en) nicht gefur	iden: "Win32_PerfRaw	Data_PerfDisk_Physic	Lesezeit (%) Keine Daten	青青青白白	Ø
	. 7.	V Disk	(IO 1 E:			C	к	ОК				Lesezeit (%) 0 %	***	Ø

Dazu suche ich nach dem Sensor für physikalische Datenträger:



I

WSHowTo – Neuinstallation von WS-RDS3 als WS-HV3 2020-01-01 Migration auf Windows Server 2019

Startseite	Geräte Bibliotheken	Sensoren Al	arme Maps	Berichte	Protokoll	Tickets	Konfiguration			Neue Alarme 3	Neue Protoko
Geräte WS	-ITS • Server • WS-HV3	Sensor hinzufügen (Schr	itt 1 von 2)								
Senso	r hinzufügen zum Ger	ät WS-HV3 [ws-hv	3.ws.its]								
		<u>v</u>	Vas soll gemonito	ort werder	ו?			Art des Zielsystem	ns?		
		C	Verfügbarkeit	OProzesso		O Hardware-I		Windows	O Speicher- und Datei-Server	Cloud-Dienste	
		C	Bandbreite / Datenverkehr	ODatenträ		O Netzwerk-I		O Linux / macOS	C E-Mail-Server		
		C	Geschwindigkeit / Leistung	Speicher		Benutzerde		O Virtuelles OS	ODatenbank		
					Eingese	etzte Tech	nologie?				
							Онттр	OPowerShell			
					O SNMP		O SSH	O Push-Benach			
					OWM		O Packet Sniffin	g OPRTG Cloud			
					OLeistung		O NetFlow, sFlo				
< Senso	rerstellung abbrechen										> Suchen \$
	5										
			Suche Q physik	alischer da	atenträger				1 Pas	sende Sensort	ypen
Verfü	gbare Sensortypen										
Terra	goare sensor open										
Window Datent	<mark>ws Physikalischer</mark> räger E/A BETA	?									
Monitor	t angesammelte Daten von	d									
-bytes, &	Übertragungszeit,	-									
Pro itict	in das Cisatellussos sisse										
übergeor Zugangs	m um Einsteilungen eines dneten Objekts (Gerät, Gruppe) gültig daten für Windows-Systeme.	re									
100	0										

Der Dialog ist selbsterklärend:

Geräte WS-ITS	Geräte Bibliotheken Sensorer	n Alarme Maps gen (Schritt 2 von 2)	Berichte Protok	oll Tickets	Konfiguration		Neue Alarme 3	Neue Proto
	Sensor hinzufügen zum Ger	ät WS-HV3 [ws-hv3.ws.	its]					
	< Abbrechen							
	Allgemeine Sensoreinstell	ungen	Übergeordnete Tags 💿					
			Tags 🕕	wmiphysicaldisks	ensor 🗙 O			
			Priorität 🖲	***				
	Einstellungen für Windows Physikalischer Datenträge	C Laufwerke						
		 ✓ 0 C: V: ☐ 1 E: 						
		□ _Total						
	Abfrageintervall							
	übernehmen von WS-HV3 (Abfrageintervall: 60 Sekunden, Sensor für	1 I)						

Mit den virtuellen Maschinen verfahre ich gleich. Zuerst werden die Einträge gelöscht und dann wieder neu dazu genommen. Der Zustand bleibt zwar im Status "fehlerhaft", aber die Meldung ist korrekt: die VMs sind ausgeschaltet:



I

artseite	Geräte	Bibliotheken	Sensoren	Alarme	Maps	Berichte	Protokoll	Tickets	Konfiguration				N	leue Alarme 3
ieräte Verät V	VS-ITS VS-ITS Serve	▼ WS-HV3 ▼ ★☆☆												
0	Übersicht	2 Tage	30 Tage	365 Ta	age	Alarme	0	Systeminforma	itionen	Protokoll	Eins	tellungen	🐥 Tr	igger für Benac
W	/enn Sie hier Senso	rtachos sehen möc	hten, ändern Sie die	Priorität von ei	inem oder meł	reren Sensore	n zu 🔺	₽/ ★★★★★ .						
Pos.	- Sensor				Status	¢	Nachricht				Graph		Priorität 🗘	C
4 1.	✓ Нуре	r-V			ОК		ок				CPU-Last ges	1%	专专专会会	Ø
4 2.	Volur	ne IO C:			ОК		ок				Freier Platz %	83 %	常常常会会	Ø
.	!! ws-D	C3			Fehler		WMI: Die VM	ist ausgeschaltet. (Code: PE065) - P	erfCounter: No data to	CPU-Last ges Kei	ne Daten		Ø
.	‼ WS-F	\$3			Fehler		WMI: Die VM	ist ausgeschaltet. (Code: PE065) P	erfCounter: No data to	CPU-Lastges Kei	ne Daten	***	ß
.	!! WS-F	FS2			Fehler		WMI: Die VM	ist ausgeschaltet. (Code: PE065) P	erfCounter: No data to	CPU-Last ges Kei	ne Daten	***	ľ
+ 6.	🗸 Disk	0 0 C: V:			ОК		ОК				Lesezeit (%)	0 %	***	đ
.	🗸 Disk	0 1 E:			ОК		ОК				Lesezeit (%)	0%	***	8
							1 bis 7 von 7							

Für den bevorstehenden Umbau belasse ich die Sensoren im Pause-Modus:



Einbau und Inbetriebnahme

Der Server ist einsatzbereit. Es wird Zeit, dass er seine alte Position einnimmt. Zuerst editiere ich alle VMs für einen automatischen Start:



Virtuelle	omputer	🖹 Einstellungen für "WS-FS3" auf "WS-HV3"	- 🗆 🗙	
Name WS-DG WS-PF WS-PF Prüfpunk WS-F53 Zusamme	e Erstellt: Konfigurationsversion: Generation: Anmerkung:	WS-F53 A Hardware Hardware Hardware Hardware Femmale Yon Datal starten Scherer Start It aldiviet Johnson Avtuelle Prozesore Avtuelle Prozesore Avtuelle Prozesore Avtuelle Prozesore Motol-Solenvinds Hettige Prozesore Vice Pottolette Hood-Hold Hettige Pottolette Vice Pottolette Pottolett	Automatische Startaktion Welche Aktion soll beim Start des physischen Computers für den virtuellen Computer augeführt verden? Keine Aktion Automatisch starten, falls die Ausführung beim Beenden des Dienste stattfand Wirtuellen Computer immer automatisch starten Automatischer Start mit Verzögerung Geben Sie anle Start verzögerung an, um Ressourcenkonflikte zwischen den wirtuellen Computer mut verzieheden. Start verzögerung: 3) Selunden	Computer importieren Einstellungen für virtuelle Switches jer überpröfen enden tfernen ren h ggen tionsversion upgraden t en n nen , naktivieren

Dann bearbeite ich lokal die Einstellung des virtuellen Hyper-V-Switches. Der Server benötigt für das Zielnetzwerk wieder eine VLAN-ID:

Virtuelle Computer		🚰 Manager für virtuelle Switches für "WS-HV	/3" — 🗆	×
Name WS-DC3 WS-FS3 WS-PFS2 WS-PFS2 WS-FS3 WS-FS3 Koof Gen Anm Zusammerfassung Ado	Phase Aus Aus Aus Aus Aus Aus Aus settemption gurationsversion: 8 reation: 2 staspeicher Netzwerk	Yortucile Switches		Computer importierer Einstellungen für virtuelle Switches jer bastbeiten er überprüfen enden Hernen sen b gen stionsversion upgraden t en st na na na na na na na na

Auch die statische IPv4-Konfiguration trage ich wieder ein:

<pre>\> ncpa.cpl</pre>	Netzwerkv	rerbindungen				- 0
	$\leftarrow \rightarrow \cdot$	↑ 😰 > Systemsteuerung > Ne	tzwerk und Internet → Netzwer	kverbindungen >	v Ö	"Netzwerkverbindungen" dur
	Organisieren	 Netzwerkgerät deaktivieren 	Verbindung untersuchen	Verbindung umbenennen Status der V	Verbindung anzeigen	S : • II
	Ak Int	IN-101 tiviert lel(R) Ethernet Connection I217 Status von vEthernet (VLANs)	vEthernet (VLANs) ws.its Hyper-V Virtual Ethern	et Adapter	X	
		Verbindung		Netzwerk		
		IPv4-Konnektivität:	Kein Netzwerkzugriff	Verbindung herstellen über:		
		IPv6-Konnektivität:	Kein Netzwerkzugriff	🚽 Hyper-V Virtual Ethernet Adapter	Eigenschaften von Internetprotokoll,	Version 4 (TCP/IPv4)
		Dauer:	00:04:31		Allgemein	
		Übertragungsrate:	1,0 GBit/s	Diese Verbindung verwendet folgende Elemen	te IP-Einstellungen können automatisch z	ugewiesen werden, wenn das
		Details		Clent für Microsoft-Netzwerke Clent für Microsoft-Netzwerke Qos-Paketplaner Qos-Paketplaner Internetprotokoll, Version 4 (TCP/IPv- Microsoft-Mitipleyonmitokoll für Netz	Netzwerk diese Funktion unterstutzt. \ Netzwerkadministrator, um die geeigne IP-Adresse automatisch beziehen IP-Adresse automatisch beziehen IP-Adresse automatisch beziehen IP-Adresse verwenden: IP-IP-IP-IP-IP-IP-IP-IP-IP-IP-IP-IP-IP-I	venden sie sich andernfalls an den eten IP-Einstellungen zu beziehen.
		6		Imcrosoft-Mutplexofprotokoli fur Netzw Imcrosoft-LLDP-Treiber Internetprotokoli, Version 6 (TCP/IPv6)	IP-Adresse:	192.168.101.2
		Gesender	Emplangen		6) Subnetzmaske:	255.255.255.0
		Pakete: 4.463	3.788	Installieren Deinstallieren	Standardgateway:	192 . 168 . 101 . 252
		Segenschaften Deakt	ivieren Diagnose	Beschreibung TCP/IP, das Standardprotokoll für WAN-Ne Datenaustausch über verschiedene, miteina	DNS-Serveradresse automatisch	beziehen erwenden:
			Schließen	Netzwerke ermöglicht.	Bevorzugter DNS-Server:	192.168.101.1
	2 Elemente	r cierrient ausgewannt	Joincoch		Alternativer DNS-Server:	192 . 168 . 100 . 1
				01	K Einstellungen beim Beenden über	rprüfen
						Erweitert

Es ist soweit: Ich schalte den Server im Hauptstandort aus und bringe in zum Außenstandort. Dort angeschlossen schalte ich das System ein und warte einen Moment. Die virtuellen Maschinen starten wie erwartet im Hintergrund. Mit dem Start der virtuellen PFSense wird auch das Netzwerk wieder aktiv. Der Domain Controller WS-DC3 repliziert die verpassten Änderungen des AD und der Fileserver WS-FS3 startet seine DFS-Replikation.

Die Umstellung des Servers scheint abgeschlossen zu sein.

<u>Nacharbeiten</u>

IT-Solutions

Gruppenanpassungen im Active Directory

Aber wie so oft gibt es noch Reste, die eine Bereinigung benötigen. Im Active Directory gibt es beispielsweise einige AD-Gruppen, die den alten Servernamen im eigenen Bezeichner und der Beschreibung verwenden. Das stört mich. Daher suche ich diese Einträge und passe sie an:

Active Directory-Benutzer und -Computer			
Datei Aktion Ansicht ?			
← ⇒ 2 📰 🐇 🖹 🗙 🖾 🗟 🕞 🛛 🗊 🖏) 🐮 🗑 🍸 🗾 🕱		
Active Directory-Benutzer und -Computer [WS-DC1.ws.if > ■ Gespeichert Abfragen > ➡ wsits > ➡ Builtin > ■ Domputers > ■ Domputers > ■ ForeignSecurityPrincipals > ■ LostAndFound	Name SG-RDS-RemoteApps-AdminTools GG-RDS-RemoteApps-Standard GG-VPN-Benutzer GG-Zugriff-DAC-Junbrunnen-Mitarbeiter GG-Zugriff-DAC-Junbrunnen-Verwaltung GG-Zugriff-R-AdminArea GG-Szugriff-R-Backup	Typ Sicherheitsgruppe - Global Sicherheitsgruppe - Global Sicherheitsgruppe - Global Sicherheitsgruppe - Global Sicherheitsgruppe - Global Sicherheitsgruppe - Global	Beschreibung Mitglieder dürfen Admin-RemoteApps UND StandardApps verwenden Mitglieder dürfen Standard-RemoteApps verwenden Rolle UPN-Zugriff (RRAS) Rolle DAC auf \\ws.its\freigaben\Jungbrunnen Rolle DAC auf \\ws.its\freigaben\Jungbrunnen Rolle Lesen auf \\ws.its\freigaben\Jungbrunnen Rolle Lesen auf \\ws.its\freigaben\Jungbrunnen
Managed Service Accounts Microsoft Exchange Security Groups Gamma Data	GG-Zugriff-R-Backup-BMR-DPM GG-Zugriff-R-Backup-BMR-HV2 GG-Zugriff-R-Backup-BMR-HV2 GG-Zugriff-R-Backup-BMR-BDS3	Sicherheitsgruppe - Global Sicherheitsgruppe - Global Sicherheitsgruppe - Global	Rolle Lesen auf \\ws.its\freigaben\Backup\BMR-DPM Rolle Lesen auf \\ws.its\freigaben\Backup\BMR-HV2 Rolle Lesen auf \\ws.its\freigaben\Backup\BMR-HV2
> System > System > Sers > WS	GG-Zugriff-R-Backup-ClientSicherung GG-Zugriff-R-Backup-ServerSicherung GG-Zugriff-R-Bibliothek	Sicherheitsgruppe - Global Sicherheitsgruppe - Global Sicherheitsgruppe - Global	Rolle Lesen auf \\ws.its\freigaben\Backup\CitentScherung Rolle Lesen auf \\ws.its\freigaben\Backup\CitentScherung Rolle Lesen auf \\ws.its\freigaben\Backup\ServerSicherung Rolle Lesen auf \\ws.its\freigaben\Bibliothek
> 3 AdminArea > 3 Benutzer > 3 Clients > 3 Exchange-Objekte	題。GG-Zugriff-R-Business 題。GG-Zugriff-R-Images 題。GG-Zugriff-R-Jungbrunnen 恩。GG-Zugriff-R-Privat	Sicherheitsgruppe - Global Sicherheitsgruppe - Global Sicherheitsgruppe - Global Sicherheitsgruppe - Global	Rolle Lesen auf \\ws.its\freigaben\Business Rolle Lesen auf \\ws.its\freigaben\Storage\Images Rolle Lesen auf \\ws.its\freigaben\Jungbrunnen Rolle Lesen auf \\ws.its\freigaben\Privat
 ✓ all Gruppen > all domainlokal g global > all Verteiler > all Server 	GG-Zugriff-R-Privat-Familie GG-Zugriff-R-Privat-Familie-alle GG-Zugriff-R-Privat-Familie-Amtliches GG-Zugriff-R-Privat-Familie-Multimedia GG-Zugriff-R-Privat-Familie-Multimedia	Sicherheitsgruppe - Global Sicherheitsgruppe - Global Sicherheitsgruppe - Global Sicherheitsgruppe - Global Sicherheitsgruppe - Global	Rolle Lesen auf \\ws.its\freigaben\Privat\Familie Rolle Lesen auf \\ws.its\freigaben\Privat\Familie\alle Rolle Lesen auf \\ws.its\freigaben\Privat\Familie\Anttiches Rolle Lesen auf \\ws.its\freigaben\Privat\Familie\Auttimedia Rolle Lesen auf \\ws.its\freigaben\Privat\Familie\Auttimedia\Audio

Für die Suche verwende ich eine PowerShell-Abfrage:

WS IT-Solutions WSHO

WSHowTo – Neuinstallation von WS-RDS3 als WS-HV3 2020-01-01 Migration auf Windows Server 2019



Die Umbenennung ist für 5 Gruppen inklusive Anpassung der Beschreibung etwas aufwändig. Daher ändere ich die Werte manuell:



Eine Kontrolle mit der PowerShell zeigt die Bereinigung:

WS IT-Solutions WSHowTo

PS C:\> Get-ADGroup -Filter	"name -like '*hv3*'" -Properties description Format-Table -Property name,description
name GG-Zugriff-R-Backup-BMR-HV3 GG-Zugriff-W-Backup-BMR-HV3 LD-Zugriff-R-Backup-BMR-HV3 LD-Zugriff-W-Backup-BMR-HV3 LD-Zugriff-L-Backup-BMR-HV3	description Rolle Lesen auf \\ws.its\freigaben\Backup\BMR-HV3 Rolle Schreiben auf \\ws.its\freigaben\Backup\BMR-HV3 Recht Lesen auf \\ws.its\freigaben\Backup\BMR-HV3 Recht Schreiben auf \\ws.its\freigaben\Backup\BMR-HV3 Recht Listen auf \\ws.its\freigaben\Backup\BMR-HV3

Anpassungen im DFS-Namespace

Auch in meinem DFS-Namespace existiert ein Ordner mit dem Namen des alten Servers. Über diesen Link konnte ich elegant auf die versteckte Freigabe des Sicherungsvolumes zugreifen. Zuerst ändere ich das Ziel. Dazu erstelle ich einen Link mit dem Pfad und dem Namen des neuen Servers:

🐴 DFS-Verwaltung						×	
🐴 Datei Aktion Ansicht Fenster ?					_ 6	5 ×	
🗢 🔿 🙍 🖬 🛛 🖬							
🚳 DFS-Verwaltung	BMR-RDS3				Aktionen	_	
V 🏭 Namespaces	Ordnerziele Realikation				BMR-RDS3		
V 🚵 \\ws.its\Freigaben	1 Finträge				Ordnerziel hinzufügen		
Backup	T Enlange			_	Ordner umbenennen		
💑 BMR-DPM	Typ Verweisstatus	Standort	Pfad	1	Ordane umberiehen		
BMR-HV2	Aktiviert	<unbekannt></unbekannt>	WS-RDS3.ws.its/BMR-RDS3\$	_	Ordner verschieben		
😹 BMR-RDS3					Ordner replizieren		
Clientsicherung	Neues	Ordnerziel	×		Ansicht	•	
Bibliothek					Neues Fenster hier öffnen		
Business	Ordner	1063			🐇 Ausschneiden		
Jungbrunnen	DMR-P	1053			X Löschen		
🎥 Privat	Names	pacepfad:			Aktualiziaren		
Rogrammierung	\\WS.IC	s (rreigaben \backup \binn-rubs)					
Software	Pfad z	um Ordnerziel:			Ligenschaften		
> Storage	[\\WS-	HV3.ws.its\BMR-HV3\$	Durchsuchen		Hilfe		
>	Beispie	I: \\Server\treigegebener Ordner\Ordner					
> 🚯 Replikation			OK Abbrechen				

Ich richte keine Replikation ein. Den alten Server gibt es ja nicht mehr:

DFS-Verwaltung Datei Aktion Ansicht Fenster ?		×
Y → → ↓ Y ≥ Namespaces Y ≥ \Wx.it\SFreigaben B AdminArea	BMR-RDS3 Ordnerziele Replikation 1 Enträge	Aktionen BMR-RDS3 Ordnerziel hinzufügen
✓ ■ Backup	Typ Verweisstatus Standort Pfad	Ordner umbenennen Ordner verschieben Ordner replizieren Ansicht Neues Fenster bier öffnen
 Bibliothek Bibliothek Business Jungbrunnen Privat Privat Software Storage Storage 	Mit einer Replikationsgruppe können diese Ordnerziele in synchronisiertem Zustand gehalten werden. Möchten Sie eine Replikationsgruppe erstellen?	✓ Ausschneiden ✓ Löschen ☑ Attualisieren ☑ Eigenschaften ☑ Hilfe

Dafür lösche ich den Link auf den alten Server. Jetzt werde ich auf das neue Share umgeleitet:

💁 DFS-Verwaltung					×
🗞 Datei Aktion Ansicht Fenster ?				- 6	ē ×
CFS-Verwaltung	BMR-RDS3			Aktionen	
V 🔉 Namespaces	Ordnerziele Replikation			BMR-RDS3	-
AdminArea	2 Einträge	Ordnerziel hinzufügen			
V Backup	Typ Verweisstatus	Standort	Pfad /	Ordner umbenennen	
BMR-DPM	Aktiviert	Neufahm	\\WS-HV3.ws.its\BMR-HV3\$	Ordner verschieben	
BMR-RDS3	😤 Aktiviert	Im Explorer öffnen	\\WS-RDS3.ws.its\BMR-RDS3\$	Ordner replizieren	
Clientsicherung		Ordnerziel deaktivieren		Ansicht	►
Bibliothek		Eigenschaften		Neues Fenster hier öffnen	
Business		Löschen		🔏 Ausschneiden	
🛃 Jungbrunnen		104-		🗙 Löschen	
Privat		niire		Q Aktualisieren	

Den Namen des Ordners kann ich einfach umbenennen:

WS IT-Solutions

🐴 DFS-Verwaltung							-	×
🐴 Datei Aktion Ansicht	Fenster ?							_ 8 ×
🗢 🔿 🖄 🖬 🚺								
Carter Server And		BMR-RDS3					Aktionen	
🗸 🏭 Namespaces		Ordnerziele	Deallistics				BMR-RDS3	
✓ ¾ \\ws.its\Freigaben		1 Entrãos	Replikation				Ordnerziel hinzufügen	
Backup		T Linuage					Ordner umbenennen	
🛃 BMR-DPM		Тур	Verweisstatus	Standort	Pfad	/	Ordner verschieben	
BMR-HV2			Aktiviert	Neufahm	\\WS-HV3.ws.i	ts\BMR-HV3\$	Ordner verschieben	
BMR-RDS3							Ordner replizieren	
Serversich	Ordnerziel hinzufü	gen					Ansicht	•
Bibliothek	Ordner umbenenn	ien					Neues Fenster hier öffnen	
🎅 Business	Ordner verschiebe	n					🐇 Ausschneiden	
🔒 Jungbrunnen	Ordner replizieren.	••					🔀 Löschen	
Privat	Ansicht		>				Aktualisieren	
Software	Neues Fenster hier	öffnen					Eigenschaften	
							_	
~								
Main DFS-Verwaltung								
🐴 Datei Aktion Ansicht	Fenster ?							_ 8 ×
🗢 🏟 🖄 📰 🚺 🖬								
🐴 DFS-Verwaltung		BMR-RDS3					Aktionen	
🗸 🏭 Namespaces		Ordnerziele	Replikation				BMR-RDS3	
✓ ▲ \\ws.its\Freigaben		1 Fintrãoe	перікціот				Ordnerziel hinzufügen	
Backup		T Canadage					Ordner umbenennen	
BMR-DPM		Тур	/erweisstatus	Standort	Pfad	/	Ordner verschieben	
BMR-HV2			ktiviert	Neutahm	\\WS-HV3.ws.r	s\BMR-HV3\$	Ordiner Verschieben	
BMR-RDS3				Ordner umbenennen	×		Ordner replizieren	
Serversicher	ing						Ansicht	•
Bibliothek	ang			Aktueller Name:			Neues Fenster hier öffnen	
🔂 Business				BMR-RDS3			of Ausschneiden	
🔒 Jungbrunnen				Neue Name:			🗙 Löschen	
Privat	-			Diminitivaj			Aktualisieren	
Software	9			Vorschau auf den neuen Namespacepfad: \\ws.its\Freigaben\Backun\BMB-HV3			Eigenschaften	
> Storage				Consider Forgeben (Dackup (BHINTIV)			Hilfe	
🔒 Zwischenablage				OK	Abbrechen		La rime	
> 🏄 \\ws.its\intern							\\WS-HV3.ws.its\BMR-HV3\$	•
A second seco						1		

Die Änderung wird gemäß meiner Voreinstellung innerhalb von knapp 2 Minuten im Client aktiv.