

<u>Inhalt</u>

Zielsetzung	2
Abschaltung von IPAM	2
Planung der Migration	2
Migration von WS-IPM zu WS-MON	2
Neuinstallation des Servers WS-MON	2
Migration des Services PRTG	6
Vorbereitung	6
Installation von PRTG auf WS-MON	6
Datenübernahme	7
Anpassungen und Nacharbeiten	11
Migration des Services SYSLOG	18
Migration der Monitoring-Scripte von WS-RDS1	24
Nacharbeiten	28
Entfernen des alten Servers WS-IPM	28
Konfiguration der Datensicherung	28
Zusammenfassung	31

<u>Zielsetzung</u>

Mein Server WS-IPM läuft noch mit Windows Server 2012R2. Auf ihm laufen mein IPAM (IP Address Management), eine PRTG-Monitoring-Instanz und ein SYSLOG-Server für meine Firewall-Protokollierung. Im Rahmen meiner Migration auf Windows Server 2019 sollen die Services auf ein modernes Betriebssystem migriert werden.

Abschaltung von IPAM

Die IPAM-Instanz läuft seit 2013 nahezu durch und sammelt verschiedene, IP-basierte Informationen in einer Datenbank. Daraus können forensische Informationen abgeleitet werden. Zusätzlich hatte ich IPAM auch zur IP-Adressverwaltung verwendet. Die Idee war nicht schlecht. Aber mehrere Punkte stören mich:

- der Zugriff ist nur über den Servermanager möglich. Ein echtes Remoting ist sehr umständlich.
- Statische DNS-Einträge werden nicht erkannt. Man muss diese immer manuell einpflegen.
- Das Layout der Bereiche und Ranges ist nicht intuitiv.
- Es gibt außer einem Inplace-Upgrade keinen Migrationspfad für die Datenbank!

In der Folge habe ich den Service seit mehreren Monaten nicht mehr weiter gepflegt. Und wie vor einer Hausrenovierung stellt sich auch vor einer Migration die Frage: Brauche ich das wirklich noch? In meinem Fall lautet die Antwort nein.

Planung der Migration

So verbleiben nur noch 2 Services: Das PRTG-Monitoring und der SYSLOG-Server. Für beide gibt es ein Side-By-Side-Migrationsszenario. Ich kann also einen neuen Server erstellen und die Dienste übertragen. Da der IPAM nicht mitkommt, kann ich auch einen neuen Servernamen vergeben, der besser zum Anwendungsfall passt: WS-MON (Monitoring).

Zusätzlich werde ich noch einige Scriptaufgaben auf das neue System verschieben, die ich derzeit auf einem anderen Server bereitgestellt habe. Diese fallen in die Kategorie Monitoring und ergänzen das Angebot der Dienste.

Migration von WS-IPM zu WS-MON

Neuinstallation des Servers WS-MON

Als Betriebssystem empfiehlt der Hersteller von PRTG (Paessler) Windows Server 2019. Leider wird eine Server-Core-Version nicht supportet. Daher installiere ich einen Windows Server 2019 mit Desktop-Experience.

Aktuell läuft die alte VM mit dem Server WS-IPM auf meinem alten WS-HV1 (Hyper-V-Host mit Windows Server 2016). Auf diesem habe ich weder freien RAM noch ausreichend freien Speicher auf der Festplatte. Daher erstelle ich die VM auf meinem neuen WS-HV3. Nach der Migration aller Services wird die VM dann auf den alten Server verschoben. Die VM-Version muss also mit Windows Server 2016 kompatibel sein. Daher erstelle ich die VM mit der PowerShell. Die Windows-Installation hatte ich bereits vor einigen Wochen als Basis-VHDX vorbereitet. Diese kann ich nun einfach reinkopieren:

```
New-VM -Name 'WS-MON' -Path 'V:\Hyper-V' -Version '8.0' -Generation 2 -SwitchName 'LAN-100' `
    -NoVHD -MemoryStartupBytes 2GB
Set-VM -Name 'WS-MON' -ProcessorCount 4 -DynamicMemory -MemoryMaximumBytes 3GB `
    -MemoryMinimumBytes 1GB
Set-VM -Name 'WS-MON' -AutomaticStartAction Start -AutomaticStartDelay 45
Get-VMIntegrationService -VMName 'WS-MON' | Enable-VMIntegrationService
New-Item -Path 'V:\Hyper-V\WS-MON\Virtual Hard Disks' -ItemType Directory | Out-Null
Copy-Item -Path 'V:\Base\Win2019-1908.vhdx' `
    -Destination 'V:\Hyper-V\WS-MON\Virtual Hard Disks\HDD0-System.vhdx'
Add-VMHardDiskDrive -VMName 'WS-MON' -Path 'V:\Hyper-V\WS-MON\Virtual Hard Disks\HDD1-System.vhdx' `
    -ControllerType SCS1
New-VHD -Path 'V:\Hyper-V\WS-MON\Virtual Hard Disks\HDD1-Monitor.vhdx' -Dynamic -SizeBytes 100GB
Add-VMHardDiskDrive -VMName 'WS-MON' -Path 'V:\Hyper-V\WS-MON\Virtual Hard Disks\HDD1-Monitor.vhdx' `
    -ControllerType SCS1
Start-VM -Name 'WS-MON'
```



Ein OOBE später kann der Server in die Infrastruktur als WS-MON aufgenommen werden. Eine freie IPv4 habe ich auch herausgefunden: 192.168.100.18/24. Nach dem DomainJoin verschiebe ich noch das Computerkonto im AD in die richtige Organisationseinheit. Somit werden alle Gruppenrichtlinien angewendet:

Active Directory-Benutzer und -Computer		
Datei Aktion Ansicht ?		
← ⇒ 2 💼 🤾 🗉 🗙 💷 Q 🕞 🛛 🖬	1 🗏 🐮 👕 🍸 🗾 🎉	
 Active Directory-Benutzer und -Computer [WS-DC1 Gespeicherte Abfragen ws.its Domain Controllers ForeignSecurityPrincipals Keys LostAndFound Managed Service Accounts Microsoft Exchange Security Groups Program Data System Users AdminArea Benutzer Clients Server Server Server-HyperV Server-HZ Server-MX Server-RDS Server-Standard 	Name Image: WS-ATA Image: WS-CA1 Image: WS-CA1 Image: WS-CA1 Image: WS-CA1 Image: WS-FS1 Image: WS-FS2 Image: WS-FS1 Image: WS-FS1 Image: WS-FS1 Image: WS-FS1 Image: WS-FS1 Image: WS-WAND Image: WS-WAC	Typ Computer Computer Computer Computer Computer Computer Computer Computer Computer

Im alten WS-IPM hatte ich für die SYSLOG-Installation einfach einen Ordner auf Laufwerk c: erstellt. Dieser wurde im Laufe der Zeit immer größer und die Datensicherung der VM dauerte immer länger. Das soll auf dem neuen Server nicht passieren. Daher erstelle ich für die Protokolldateien ein eigenes Volume auf einer separaten VHDX. Das Volume ist schnell erstellt:



Auswahl bestätige Vorbemerkungen Server und Datenträger	CN Überprüfen Sie die folgenden dann auf "Erstellen".	Einstellungen auf Korre	ektheit, und klic	ken Sie	
Größe Laufwerkbuchstabe oder Dateisystemeinstellungen Bestätigung Ergebnisse	VOLUMEORT Server: Datenträger: Freier Speicherplatz: VOLUMEEIGENSCHAFTEN Volumegröße: Laufwerkbuchstabe oder -pfad: Volumebezeichnung: DATEISYSTEMEINSTELLUNGEN Dateisystem: Erstellung kurzer Dateinamen: Größe der Zuordnungseinheit:	WS-MON Datenträger "1" 100 GB E:\ Monitoring NTFS Deaktiviert Standard			

Damit die Logfiles der Monitoring-Partition nicht zu stark anwachsen, konfiguriere ich noch die Datendeduplizierung auf dem neuen Volume. Dazu ist aber auch die Rolle erforderlich:

🚰 Assistent zum Hinzufügen von Rollen und Features				-		×
Assistent zum Hinzufügen von Rollen und Features Serverrollen auswählen Vorbereitung Installationstyp Serverauswahl Serverrollen Features Bestätigung	ine Rolle aus, die auf dem Lightweight Directory Sen Domänendienste Rechteverwaltungsdienste Verbunddienste Zertfikatdienste	n ausgewählte vices	en Server installiert we Beschreibung Die Datenduplizien Einsparung von Sp dem Datenträger b dem Volume jeweil einzelne Kopie ider gespeichert wird.	ws rden so ung trä eicherp ei, inde s nur e ntische	ZIELSERV 5-MON.ws oll. igt zur olatz auf em auf eine r Daten	X /ER .its
Ergebnisse	ienste (1 von 12 installiert CSI-Dienste er dner che für Netzwerkdateien er-VSS-Agent-Dienst luplizierung espaces kation server speicheranbieter (VDS- ur en-Manager für Dateiserve NFS ste (Installiert)	t) nd VSS-ł er	gespeichert wird.			



	€ Server-M	anager • Dat	ei-/Speicł	nerdiens	te • Vol	umes •				• ③
	Server	Alle Volumes L	4 inscesamt							
i	Volumes	Filter	- insgesuite	<u>م</u> (iii) م	(■) ▼					
	Datenträger	★ 14.1	C L D C		D (1) (1)	IZ DOD	5 1 6 11			
	Freigaben	WS-MON (4)	Status Bezei	cnnung aes	Bereitstellung	g Kapazitat	Freier Speicr	erpiatz Dedu	plizierungsrate	Einsparungen
	iSCSI	\\?53	Wiede	erherstellung	Fest	499 MB	76,8 MB			
	Arbeitsordner	\\?a8 C:	Syster	n	Fest Fest	95,0 MB 99,4 GB	69,2 MB 86,5 GB			
		E:	Monit	oring	Fest	Neue F	eigabe			
						Neuer	virtueller iSCSI-	Datenträger		
						Dateisy	stem auf Fehle	r überprüfen		
		Zuletzt aktualisiert ar	n 08.09.2019 11:1	5:56		Laufwei	ksbuchstaben	und Zugriffspf	ade verwalten	
		a and a contract of	Selected by the			Format	eren			
		FREIGABEN				Volume Volume	erweitern löschen			
		Es sind keine zugehöri	gen Freigaben ve	rfügbar.		Datend	eduplizierung	konfigurieren		
			Es sind keine zuge	ehörigen Freiga	ben vorhander	Eigenso	haften	карагнан	100 GB	
Parks		ring (5.3.)"	_		~			100% 70080	ardnet	100 GB 7uc
i Dedu	plizierungseinstellungen für Monito	ring (E:\)		ᡖ ws-mon -	Deduplizierungsz	zeitplan			√ (23) 1 −	
Mo	nitoring (E:\)			WS-M0	ON.ws.its					
Dat	endeduplizierung aktivieren: Allg	emeiner Dateiserver		Hinter	grundoptimierun	g aktivieren				^
	Alter (in Tagen), ab dem Dateien ded Geben Sie die Dateierweiterungen eir	upliziert werden sollen: 1	olizierung	Die Da des Sy:	tendeduplizierun stems angehalten	g wird regelmäß , um die Leistun	ig mit niedriger g möglichst nich	Priorität ausgefüh t zu beeinträchtig	irt und bei Auslast jen.	ung g
3	usschließen möchten. Trennen Sie d doc,txt,png"	ie Erweiterungen durch ein Ko	omma. Beispiel:	🔽 Dure	hsatzoptimierung	aktivieren			($\overline{\mathbf{O}}$
,	Auszuschließende Standarddateierwe	iterungen: edb,	jrs	Währ ausge	end der angegeb eführt und verbra	enen Zeiten wir ucht die erforde	d die Datendedu rlichen Ressourc	plizierung mit nor en, um die Leistur	maler Priorität 19 zu maximieren.	
,	Auszuschließende benutzerdefinierte	Dateierweiterungen:		Woch	nentage:	✓ Montag ✓ Freitag	✓ Dienstag ✓ Samstag	✓ Mittwoch ✓ Sonntag	✓ Donnerstag	9
ſ	(licken Sie auf "Hinzufügen", um Ord	ner (incl. Dateien) von der Da	tendeduplizierung a	Start	tzeit:	<mark>15:00</mark> ~				
				Dau	er (in Stunden):	1				
				Zwei	ten Zeitplan für d	ie Durchsatzopt	imierung erstelle	n	(0
	Zeitplan für die Deduplizierung festle	:gen		Währ ausge	end der angegeb eführt und verbra	enen Zeiten wird ucht die erforde	d die Datendedu rlichen Ressourc	plizierung mit nor en, um die Leistur	maler Priorität 19 zu maximieren.	
			OK Abbre	Woch	nentage:	✓ Montag ✓ Freitag	✓ Dienstag ✓ Samstag	✓ Mittwoch ✓ Sonntag	✓ Donnerstag	9
				Start	tzeit:	09:00 ~				

Nun bekommt der Server noch alle genehmigten Windows Updates. Im WSUS verschiebe ich das Computerobjekt in den richtigen Container:

Update Services				
📷 Datei Aktion Ansicht Fenster ?				
🗢 🔿 🙍 🖬				
Update Services	Nich	t zugewiesene Computer (1 Computers von 1 angezeigt, 27 insgesamt)		
→ WS-CM → W Updates	Statu	s: Alle - 🔾 Aktualisieren		
🗸 🛃 Computer	0 N	lame	IP-Adresse	Betriebssystem
V Ne Alle Computer	A w	s-mon.ws.its	192.168.100.18	Windows Server 2019 Datacenter
 Clients Clients Clients Clients Update-Sofort Update-Verzoegert Downstreamserver Synchronisierungen Berichte Optionen 		Gruppenmitgliedschaft für Computer festlegen X Wahlen Sie die Gruppen aus, denen dieser Computer angehören die Gruppe "Nicht zugewiesene Computer" verschoben. Glients Glients Update-Safort Update-Verzoegent		

Nach dem Neustart ist das Basissystem einsatzbereit. Das Monitoring und das Backup konfiguriere ich im Schritt Nacharbeiten.

Migration des Services PRTG

Vorbereitung

Von PRTG gibt es eine detaillierte Anleitung zur Migration einer bestehenden PRTG-Installation. Ich verwende derzeit die freie Edition und möchte das auch beibehalten.

Für die Kommunikation mit den Servern von Paessler ist eine Freischaltung in meiner Firewall (PFSense) erforderlich. Ich nehme die neue IPv4 in die Gruppe auf:

		· · · · · ·							-
□ ✓ 0 /1.23 MiB	IPv4 TCP	ServerOut_ MXServer	*	Target_MXUpdate	e1 Ports_HTTPS	*	none	MXUpdate HTTPS	₺₡©⊘ ₫
2 /18.56 GiB	IPv4 TCP	ServerOut_ MXServer	*	Target_MXUpdate	e2 Ports_HTTP	*	none	MXUpdate HTTP	ᡫ᠕ᢕ⊘ ۩
□ ✓ 0 /20.13 ■ MiB	IPv4 TCP	ServerOut_ WinUpdate	*	Target_MSUpdate	e Ports_HTTPS	*	none	update.microsoft.com	ᡫ᠕ᢕ⊘ ۩
□ ✔ 0 /0 B	IPv4 TCP	ServerOut_ Paessler	*	Target_Paessler	Ports_HTTP	*	none	Zugriff *.paessler.com	ᢤ᠕ᢕ᠐ ۩
0 /11 KiB	IPv4 ICMP	*	*	*	*	*	none	ICMP	±.≁⊡0
Sense Syste	m - Inter	rfaces 🔻 🛛 F	irewall 👻	Services 🕶	VPN ▼ Status ▼	Diagr	nostics 👻	Help 🕶	¢
Firewall / Alias	es / Edit								0
Properties									
Name	e Server0 The nam)ut_Paessler ne of the alias m	ay only consi	ist of the character	s "a-z, A-Z, 0-9 and _".				
Description	n Zugriff ¹ A descrip	*.paessler.com ption may be en	tered here for	r administrative ref	erence (not parsed).				
Тур	e Host(s))			~				
Host(s)									
Hin	t Enter as re-resolve as 192.1	many hosts as o ed and updated. 68.1.16/28 may	desired. Host . If multiple IP also be ente	s must be specified s are returned by a red and a list of inc	d by their IP address or a DNS query, all are used dividual IP addresses wi	fully quali I. An IP ra II be gene	ified domain r ange such as erated.	name (FQDN). FQDN hostnames are 192.168.1.1-192.168.1.10 or a sma	e periodically Il subnet such
IP or FQD	192.168	3.100.14			WS-IPM (PRTG)			💼 Delete	

Installation von PRTG auf WS-MON

Der erste für mich relevante Schritt der Migrationsanleitung lautet "Step 1b: Install PRTG on the Target System". Ich starte die Installation:

🕥 Setup - PRTG Network Monitor — 🗆 🗙
Lizenzvereinbarung Lesen Sie bitte folgende, wichtige Informationen bevor Sie fortfahren.
Lesen Sie bitte die folgenden Lizenzvereinbarungen. Benutzen Sie bei Bedarf die Bildlaufleiste oder drücken Sie die "Bild Ab"-Taste.
Sie erklären sich mit den Lizenzvereinbarungen einverstanden, die Sie hier finden:
https://www.de.paessler.com/company/terms
Ich akzeptiere die Vereinbarung O Ich lehne die Vereinbarung ab www.paessler.com Weiter > Abbrechen





Die Installation läuft fehlerfrei durch.

<u>Datenübernahme</u>

Im nächsten Schritt "Step 2: Stop Core and Probe Services on Source and Target System" muss ich alle Services auf beiden PRTG-Maschinen beenden. Das bedeutet also einen Ausfall im Monitoring:

PRTG Prohe Service	Name 🔺	Beschreibung	Status	Starttyp		Anmelden als
RTG TTODE SELVICE	🔍 Plug & Play	Ermöglicht de	Wird au	Manuell		Lokales System
Den Dienst <u>beenden</u>	🌼 PRTG Core Server Service	Führt ein Mon		Automatisch		Lokales System
Den Dienst <u>neu starten</u>	🔍 PRTG Probe Service	Performs net	Wird au	Automatisch		Lokales System
	🐘 RAS-Verbindungsverwaltung	Verwaltet Ein		Manuell		Lokales System
Beschreibung:	Remotedesktopdienste	Ermöalicht Be	Wird au	Manuell		Netzwerkdienst
Performs network monitoring using	🔍 Remo	Dienststeuer	ung	×		Netzwerkdiens
arious network protocols (including	🔍 Remo		~		durch Auslöser)	Lokaler Dienst
letFlow, and others) for PRTG	Richtle Es wird versucht, den	Dienst auf "Lokaler C	omputer" zu l	beenden		Lokales System
letwork Monitor	Richtl PRTG Probe Service					Lokales System
www.paessler.com/prtg)	🔍 Routin					Lokales System
	RPC-E					Netzwerkdiens
	🔍 RPC-L					Netzwerkdienst
	🔍 Sekur	Schließen	1			Lokales System
	🖓 Server	Schieben				Lokales System
	Server tur Threadsortierung	Bietet eine na		ivianueli		Lokaler Dienst
	Shellhardwareerkennung	Zeigt Meldun	Wird au	Automatisch		Lokales System
	🗥 Cicharbaitekanta Managar	Durch dan Sta	Mirel au	Automatisch		Labolar Curtam

O Dienste (Lokal)					
PRTG Probe Service	Name	Beschreibung	Status	Starttyp	Anmelden als
Den Dienst <u>starten</u>	Plattformdienst f ür verbund Plug & Play PrintWorkflow_44da8	Dieser Dienst Ermöglicht de Druckworkflow	Wird au Wird au	Automa Manuell Manuell	Lokaler Dienst Lokales System Lokales System
Beschreibung: Performs network monitoring using	Programmkompatibilitäts PRTG Core Server Service	Dieser Dienst Führt ein Mon	Wird au	Manuell Automa	Lokales System Lokales System
SNMP, WMI, HTTP, packet sniffing, NetFlow, and others) for PRTG	RAS-Verbindungsverwaltung	Performs net Verwaltet Einw	Wird au	Automa Automa	Lokales System Lokales System
Network Monitor (www.paessler.com/prtg)	Registrierungsdienst f ür die Remotedesktopdienste	Führt Gerätere Ermöglicht Be	Wird au	Manuell Manuell	Lokales System Netzwerkdienst

Nun geht es an die Migration der alten Daten. Im Administrations-Tool (das findet man im Startmenü) kann der Datenpfad ausgelesen werden:

PRTG Networ	k Monitor - PRTG Adminis	tration Tool			×						
🖾 PAE	SSLER			PRTG Ne	twork Monitor						
Einstellunge	en Probe/Serververbindung	IP-Einstellungen für	das Monitoring	Dienst Start/Stop	Protokoll und Infos						
We	bserver	PRTG Server	Cluster		Administrator						
Verbind Verbin Verbin Verbin Verbin 12 12 12	Verbindungsverwaltung für Probes Verbindungen nur von der Local Probe zulassen (Standardeinstellung, lässt Remote Probes nicht zu) Verbindungen von Remote Probes auf allen IPs zulassen Verbindungen von Remote Probes nur auf den ausgewählten IPs zulassen: 192.168.100.18 127.0.0.1										
Lokaler Ordner:	Speicherort für Datenda C:\ProgramData\Paessler\	teien und Monitorir PRTG Network Monitor	ng-Datenbank								
	Achtung: Bitte kopieren Sie hier ändern.	Ihre PRTG Datendate	ien an den gewür	nschten Ort, BEVOR	Sie den Pfad						
			S	peichern & Schließer	Abbrechen						

Nun kann ich die Daten einfach kopieren. Ich wähle aber auf dem Zielserver WS-MON einen neuen Pfad unter Laufwerk E: aus:

	PRIG Network N	nomitor			JP La US ₹		PKIG		
Freigeben An	sicht			~ 🕜	Datei Start Freigeben	An	isicht		
鷆 « SYSTEM (C:)	ProgramData Paessler PRTG Netwo	ork Monitor 🗸 🗸	* 🖒 PRTG Networ	rk Monitor" dur 🔎	€ 💿 ▼ ↑ 퉬 ► Netzv	werk 🕨	ws-mon + e\$ + PRTG	~	C "PRTG" d
	Name	Änderungsdatum	Тур	Größe	☆ Favoriten	^	Name	Änderungsdatum	Тур
	퉬 Configuration Auto-Backups	08.09.2019 03:09	Dateiordner		Desktop		🎉 Report PDFs	22.02.2016 11:22	Dateiordner
	퉬 Log Database	08.09.2019 02:52	Dateiordner		🚺 Downloads		Sensordata (NonPersistent)	27.05.2019 18:35	Dateiordner
Jcht	퉬 Logs	08.09.2019 12:11	Dateiordner		📃 Zuletzt besucht		🎉 Syslog Database	04.12.2017 18:33	Dateiordner
	퉬 Logs (Debug)	09.03.2018 08:58	Dateiordner				🎉 System Information Database	19.09.2016 10:12	Dateiordner
	🍌 Logs (Sensors)	26.02.2016 17:45	Dateiordner		Desktop		鷆 Ticket Database	18.12.2016 17:40	Dateiordner
ephan - T1	퉬 Logs (System)	12.06.2018 11:55	Dateiordner		Walther, Stephan - T1		🎉 ToDo Database	22.02.2016 11:22	Dateiordner
	🌗 Logs (Web Server)	24.09.2018 05:27	Dateiordner		🖳 Dieser PC		鷆 Toplist Database	06.04.2017 16:54	Dateiordner
C:)	퉬 Monitoring Database	08.09.2019 02:52	Dateiordner		SYSTEM (C:)		PRTG Configuration.dat	08.09.2019 12:07	DAT-Datei
	Report PDFs	22.02.2016 11:22	Dateiordner		🔮 DVD-Laufwerk (D:)		PRTG Configuration.old	08.09.2019 03:09	OLD-Datei
er	Sensordata (NonPersistent)	27.05.2019 18:35	Dateiordner		🖵 Freigaben (M:)		PRTG Graph Data Cache.dat	08.09.2019 12:07	DAT-Datei
	퉬 Syslog Database	04.12.2017 18:33	Dateiordner		🕞 Bibliotheken		Configuration Auto-Backups	08.09.2019 03:09	Dateiordner
5	퉬 System Information Database	19.09.2016 10:12	-	7% abgaschi			퉬 Log Database	08.09.2019 02:52	Dateiordner
n Files (x86)	퉬 Ticket Database	18.12.2016 17:40		7% abgeschi	ossen		🎍 Logs	08.09.2019 12:11	Dateiordner
nme	퉬 ToDo Database	22.02.2016 11:22	7.724 Elemente v	verden von PRTG Networ	Monitor nach PRTG kopiert		🎉 Logs (Debug)	09.03.2018 08:58	Dateiordner
vs	퉬 Toplist Database	06.04.2017 16:54	7% abgeschl	ossen	II ×	=	🌽 Logs (Sensors)	26.02.2016 17:45	Dateiordner
werk (D:)	PRTG Configuration.dat	08.09.2019 12:07					🎉 Logs (System)	12.06.2018 11:55	Dateiordner
ı (M:)	PRTG Configuration.old	08.09.2019 03:09			Geschwindigkeit: 32,0 MB/s		퉬 Logs (Web Server)	24.09.2018 05:27	Dateiordner
n	PRTG Graph Data Cache.dat	08.09.2019 12:07					🎍 Monitoring Database	08.09.2019 02:52	Dateiordner
erung									
msteuerungselemer			Name: Device 20	049.prd	le un dine				
onten			Verbleibende Ele	mente: 6.665 (5.49 GB)	kunden				
١g									
te Bedienung			Warian Da			h .			
1			weniger De	talls					
und Internet					Darstellung				

Teile der Konfiguration scheinen in der Registry zu liegen ("Step 5: Export Settings of the Old Server and Local Probe from the Windows Registry to a File"). Also exportiere ich diese in eine reg-Datei:

WS IT-Solutions

đ

WSHowTo – Migration von PRTG & SYSLOG (WS-MON) 2019-09-08 Migration auf Windows Server 2019

ř.			Registrierungs-Editor
)atei Bearbeiten Ansicht Favoriten ?			
Computer HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT HKEY_LOCAL_MACHINE BCD0000000 HARDWARE SECURITY SECURITY SOFTWARE SOFTWARE OBEC POLICIES RegisteredApplications SoFrit SSPrint Wow6432Node SSPrint SSPrint Classes DOEC Microsoft MozillaPlugins DOEC MozillaPlugins DOEC MozillaPlugins DOEC MozillaPlugins DOEC MozillaPlugins DOEC MozillaPlugins DOEC MODEC DOEC MozillaPlugins DOBC DOBC	Name (Standard) exepath initial_installdate IsGetDesktopIconInstalled	Typ REG_SZ REG_SZ REG_DWORD REG_DWORD	Daten (Wert nicht festgelegt) C:\Program Files (x86)\PRTG Network Monitor\ 0x0000a5b6 (42422) 0x00000001 (1)
PRTG Network Monito Pebug Probe Poroe Policies RegisteredApplications Samsung SolarWinds Syslog Server Volatile Sch	Auzieren a hen chen benennen ortieren cktigungen lüsselmamen kopieren		

Auf dem neuen Server erstelle ich auf die gleiche Weise noch ein Backup. Danach importiere ich die Einstellungen aus der Exportdatei des alten Servers:

lame	Änderungsdatum	Тур	Größe
ΩG	08.09.2019 12:15	Dateiordner	
TG WS-IPM.reg	08.09.2019 12:20	Registrierungseint	14 KB
Durch das Hinzufügen vo gelöscht werden, so dass von E:\PRTG WS-IPM.reg hinzufügen. Möchten Sie den Vorgan	on Informationen können Werte Komponenten nicht mehr rich nicht vertrauen, sollten Sie die I g fortsetzen?	e unbeabsichtigt geände tig funktionieren. Wenn Informationen nicht zur	rt oder Sie der Quelle Registrierung

Nun starte ich das PRTG-Administrationstool aus dem Startmenü und kontrolliere die Einstellungen. Der alte Server lief mit HTTPS. Das wurde jetzt übernommen. Aber der Datenpfad ist noch auf c: gerichtet. Das muss ich anpassen:



G Networ	k Monitor - PRTG Admin	istration Tool				×
PAE	SSLER			PR	TG Net	work Monitor
instellunge	en Probe/Serververbindung	IP-Einstellungen für	das Monitoring	Dienst St	art/Stop	Protokoll und Infos
We	bserver	PRTG Server	Cluster		A	dministrator
Verbind	ungsverwaltung für Pro	obes				
Verbin	ndungen nur von der Local I	Probe zulassen (Standa	rdeinstellung, läss	st Remote F	Probes nich	t zu)
() Verbin	ndungen von Remote Probe	es auf allen IPs zulassen				
() Verbin	ndungen von Remote Probe	es nur auf den ausgewä	hlten IPs zulasser	1:		
	92.168.100.18					
1	27.0.0.1					
	c					
Ordeory		latelen und Pionitori	ng-Datenbank			
oruner:	Auf Standardofad zu	rücksatzen				
	Achtungu Ritte kensioren 6	in Uksetzen	vian an dan nawi	nachtan Or		ia dan Rfad
	hier ändern.	e Inie PRIG Dalendale	ien an uen gewu	schien or	L, DEVOR 3	ie uen riau
			5	neichern &	Schließen	Abbrechen

Vor dem Start exportiere ich noch das Zertifikat auf dem alten Server, da dieses bis 2020 gültig ist. Dieses installiere ich auf dem neuen Server:

R		PRTG Network Monitor	
• Monitorin	ig (E;)		
t Freigeb	en Ansicht		×
N 🕳 → Die	eser PC > Monitoring (← 🛛 & Zertifikatimport-Assistent	
^	Name		
r, Stephar	PRTG	Zu importierende Datei	
°C	鹶 PRTG WS-IPM.re	Geben Sie die Datei an, die importiert werden soll.	
n (C:)	🌛 prtg.ws.its.pfx		
oring (E:)		Dateiname:	
ben (M:)		E:\prtg.ws.its.pfx Durchsuchen	
iinArea		L'Environt Malance Zantificate luïcere in since Datai in falance des Comptes accordent	
räte		Hinweis: Mehrere Zertifikate konnen in einer Datei in rolgenden Formaten gespeichert werden:	
enzen		Privater Informationsaustausch - PKCS #12 (.PFX,.P12)	
tzwerk		Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)	
vices		Microsoft Serieller Zertifikatspeicher (.SST)	
herheit			
enutzerZ			
itlocker			
aspersky			
eePass			
1ail-Zertil			
asswortS		Weiter Abbrecher	n
erviceZer		The second se	•
entre V			

Nun starte ich die Services. Das dauert einige Minuten:



	nitor - PRTG Adminis	tration Tool				×
2 PAESS	LER				PRTG	Network Monitor
Webserver	PRTG Server	Cluster	Administra	ator	Einstellungen Pr	robe/Serververbindung
IP-Einstellunge	n für das Monitoring	Dienst S	tart/Stop	Prot	okoll und Infos	Bitte warten Sie
DILLE WARTEN	i sie, wanrend das i		SLFALION TOC	n die No	ugen Akuonen (urcinuirc
Dienst des F	PRTG Core Servers:	Starten anst	ehend			
Dienst des F PRTG Probe	PRTG Core Servers: -Dienst: Beendet	Starten anst	ehend			
Dienst des F PRTG Probe Current Sta	PRTG Core Servers: -Dienst: Beendet tus:	Starten anst	ehend			
Dienst des F PRTG Probe Current Sta	PRTG Core Servers: Dienst: Beendet tus:	Starten anst	ehend			

Leider kommt diese Fehlermeldung:

Network Mo	nitor - PRTG Admini	stration Tool							
PAESS	LER				PRTG	Network Monit			
Webserver	PRTG Server	Cluster	Administra	ator	Einstellungen Pr	obe/Serververbindung			
IP-Einstellunge	n für das Monitoring	Dienst S	Start/Stop	Pro	tokoll und Infos	Bitte warten Sie			
Bitte warten Sie, während das PRTG Administration Tool die nötigen Aktionen durchführt PRTG Administration Tool X									
	PRTG Core Timeout w	Server Service hile starting.	konnte nicht	gestart	et werden:	_			
					OK	J			
Dienst des I PRTG Probe Current Sta	PRTG Core Servers -Dienst: Beendet tus:	: Starten ans	tehend						
					Speichern & Schlie	eßen Abbrechen			

Beim 2. Versuch sind die Services dann hochgefahren. Daher ignoriere ich die Meldung.

Anpassungen und Nacharbeiten

Nun wird es Zeit für einen Zugriffstest. Intern verwende ich für den den Service den FQDN prtg.ws.its. Dieser zeigt im DNS aber noch auf den alten Server:



Hier passe ich den Zeiger an auf den FQDN ws-mon.ws.its. Auf meinem Testrechner prüfe ich die Anpassung. Die IP-Adresse wird korrekt aufgelöst. Nur das ICMP-EchoRequest kommt nicht durch die Firewall:



Nun muss ich aber auch den Zugriff auf diese IP für HTTPS in meiner Firewall freischalten. Auch für diesen Servicezugriff habe ich eine Aliasgruppe erstellt. Da ändere ich die IP-Adresse und die Beschreibung vom alten Server (192.168.100.14) in die Daten des neuen Servers (192.168.100.18):

WS IT-Solutions

WSHowTo – Migration von PRTG & SYSLOG (WS-MON) 2019-09-08 Migration auf Windows Server 2019

	System 👻	Interfaces 🗸	Firewall 👻	Services -	VPN -	Status 🕶	Diagnostics 👻	Help 👻	Þ
Firewall /	Aliases /	Edit							0
Properties									
	Name	ServerIn_HTTPS The name of the alia	s may only cons	sist of the charac	ters "a-z, A-Z,	0-9 and _".			
Des	scription	Services mit HTTPS A description may be	e entered here fo	or administrative	reference (no	ot parsed).			
	Туре	Host(s)				\sim			
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 spec IPs are returned ered and a list of	ified by their I by a DNS que individual IP	P address or fr ry, all are used. addresses will	ully qualified domain . An IP range such as be generated.	name (FQDN). FQI 192.168.1.1-192.1	DN hostnames are periodically 168.1.10 or a small subnet such
IP	or FQDN	192.168.100.18			W	S-MON (PRTG)			🗊 Delete
		192.168.100.7			W	S-RA1 (WAP)			💼 Delete
		192.168.100.17			W	S-RA2 (WAP)			🛍 Delete
		192.168.100.6			W	S-CA1 (PKI+CE	S)		🛍 Delete

Auch die anderen Ausnahmen übertrage ich auf die neue IPv4. So muss die PRTG-Instanz auch Mails versenden können:

COMMUNITY EDITION	Interfaces -	Firewall 🛨	Services 🕶	VPN -	Status 🕶	Diagnostics 🗸	Help 🗕	¢
Firewall / Aliases	/ Edit							0
Properties								
Name	ServerOut_TCP25							
	The name of the alias r	nay only consi	st of the charac	ters "a-z, A-Z,	0-9 and _".			
Description	Server mit SMTP							
	A description may be e	ntered here for	administrative	reference (no	ot parsed).			
Туре	Host(s)				~			
Host(s)								
Hint	Enter as many hosts as re-resolved and update as 192.168.1.16/28 ma	desired. Host d. If multiple IF ay also be ente	s must be spec Ps are returned l red and a list of	ified by their I by a DNS que individual IP	P address or f ry, all are used addresses wil	ully qualified domair . An IP range such a: l be generated.	name (FQDN). FQ 3 192.168.1.1-192.	DN hostnames are periodically 168.1.10 or a small subnet such
IP or FQDN	192.168.100.3			W	S-MX1			Delete
	192.168.100.13			W	S-MX2			🗊 Delete
	192.168.100.18			W	S-MON <mark> (</mark> PRTG	SMTP-Probes)		🗊 Delete

Nun sollte ich die PRTG-Website erreichen können. Aber anscheinend wurde mein Zertifikat nicht übernommen:

WS IT-Solutions



Ich bestätige die Sicherheitsausnahme und prüfe weiter. Jetzt kommt eine Lizenzierungsmeldung:



Klar. Der ProduktKey ist in der Registry gespeichert. Das System hat nun den alten Key installiert. Das erklärt auch das Problem beim Servicestart. Ich trage den neuen Key ein und führe die Aktivierung durch. Jetzt hat es funktioniert:



Lizenzstatus Activation was successful Lizenzname prtgtrial Lizenzschlüssel 000014-1TMKFM-8FFW87-KRNDJ4-2CY1BN-KAMCT8-NN24Z7-9BFK5Y-UHK23M-4TTP12 System ID SYSTEMID-SXPWUPMR-R7D5NMCO-HMBVLMM7-T2PD2GJN-W6GW50IA Lizenzierte Edition PRTG Network Monitor Trial (30 days left) (läuft am 08.10.2019 ab) Letztes Update 08.09.2019 12:50:08 Anzahl der Sensoren unbeschränkt viele						
Lizenzstatus Activation was successful Lizenzname prtgtrial Lizenzschlüssel 000014-1TMKFM-8FFW87-KRNDJ4-2CY1BN-KAMCT8-NN24Z7-9BFK5Y-UHK23M-4TTP12 System ID SYSTEMID-SXPWUPMR-R7D5NMCO-HMBVLMM7-T2PD2GJN-W6GW50IA Lizenzierte Edition PRTG Network Monitor Trial (30 days left) (läuft am 08.10.2019 ab) Letztes Update 08.09.2019 12:50:08 Anzahl der Sensoren unbeschränkt viele						
Lizenzname prtgtrial Lizenzschlüssel 000014-1TMKFM-8FFW87-KRNDJ4-2CY1BN-KAMCT8-NN24Z7-9BFK5Y-UHK23M-4TTP12 System ID SYSTEMID-SXPWUPMR-R7D5NMCO-HMBVLMM7-T2PD20GJN-W6GW50IA Lizenzierte Edition PRTG Network Monitor Trial (30 days left) (läuft am 08.10.2019 ab) Letztes Update 08.09.2019 12:50:08 Anzahl der Sensoren unbeschränkt viele	Activation was successful					
Lizenzschlüssel 000014-1TMKFM-8FFW87-KRNDJ4-2CY1BN-KAMCT8-NN24Z7-9BFK5Y-UHK23M-4TTP12 System ID SYSTEMID-SXPWUPMR-R7D5NMCO-HMBVLMM7-T2PD2GJN-W6GW50IA Lizenzierte Edition PRTG Network Monitor Trial (30 days left) (läuft am 08.10.2019 ab) Letztes Update 08.09.2019 12:50:08 Anzahl der Sensoren unbeschränkt viele	prtgtrial					
System ID SYSTEMID-SXPWUPMR-R7D5NMCO-HMBVLMM7-T2PD2GJN-W66W50IA Lizenzierte Edition PRTG Network Monitor Trial (30 days left) (läuft am 08.10.2019 ab) Letztes Update 08.09.2019 12:50:08 Anzahl der Sensoren unbeschränkt viele	000014-1TMKFM-8FFW87-KRND	J4-2CY1BN-KAMCT8-NN24Z	7-9BFK5Y-UHK23M-4TTP12			
Lizenzierte Edition PRTG Network Monitor Trial (30 days left) (läuft am 08.10.2019 ab) Letztes Update 08.09.2019 12:50:08 Anzahl der Sensoren unbeschränkt viele	SYSTEMID-SXPWUPMR-R7D5NN	ICO-HMBVLMM7-T2PD2GJN-	W6GW50IA			
Letztes Update 08.09.2019 12:50:08 Anzahl der Sensoren unbeschränkt viele	PRTG Network Monitor Trial (30 d	days left) <mark>(läuft am 08.10.201</mark>	9 ab)			
Anzahl der Sensoren unbeschränkt viele	08.09.2019 12:50:08					
	unbeschränkt viele					
		Activation was successful prtgtrial 000014-1TMKFM-8FFW87-KRND SYSTEMID-SXPWUPMR-R7D5NN PRTG Network Monitor Trial (30 of 08.09.2019 12:50:08 unbeschränkt viele	Activation was successful prtgtrial 000014-1TMKFM-8FFW87-KRNDJ4-2CY1BN-KAMCT8-NN24ZI SYSTEMID-SXPWUPMR-R7D5NMCO-HMBVLMM7-T2PD2GJN- PRTG Network Monitor Trial (30 days left) (läuft am 08.10.201 08.09.2019 12:50:08 unbeschränkt viele			

Das Monitoring läuft nun wieder an. Und alle meine Einstellungen sind noch vorhanden:

	Geräte	Bibliotheken	Sensoren	Alarme M	laps Berich	ite Protokol	ll Tickets	s Konfigu	ration			N
deräte												
Gruppe	WS-ITS											
<u> </u>	Übersicht	2 Tage	30 Tage	365 Ta	ige 🖌	Alarme	Protok	oll	🕏 Verwaltung	🍄 Einstellu	ngen	A Trigger für Be
₩4 ∨	/ 56 II 2 ? 37	(von 99) S M	L XL 🔅 🔛								Suche	
₩ws- 0 5 v 0 6 v 0 0 v	HTS WS-HTS E Gerät der Prob Serverzu Serverzu W3 Sense Server E Server E Server	a k⊐ tand 78% ✓ Systemzustar 10 ✓ 16 Sen_ r-V ♀ WS-DC1	rd V Zustand der Pr 00 \$? 2 Sens	Sensor hinzufügen WS-IPM	2 WS-MX1	7 WS-PFS1a	[?] WS-RA1	VWS-RDS1	Volume 10 C:	Volume 10 V: AS Volu	me 10 V:\S. ¥ Volum	e 10 V.18_
	? Disk	10 0 ? Disk 10 1	? Disk IO 2	? Disk IO 3	? Disk IO 4 C:	? Disk IO 5 V:	Volume IO E:	RAM 73	? WS-ATA	Sensor hinzufügen	UNE NE	55 4
r	🗆 📼 WS-MX1 🛱	-		-	-	-						
	✓ SMT	P 8 ms Mail Queu	ue DB-Jungbrunn 3 # Heat	thy DB-Privat Health	DB-System Mounted	DB-WSITS Mounted	SSL Security	+ Sensor hinzufügen				
1	⊡ == WS-MX2 == SMT	P Mail Que	ue V DB-Jungbrunn 2# Mount	ted DB-Privat	DB-System Healthy	DB-WSITS Healthy	SSL Security	+ Sensor hinzufügen				
1	🖻 📟 WS-RDS3 🎙 ? Hype	r-V Volume IC	0 C: ? WS-DC3	? WS-PFS2	? Disk IO 0 C:	? Disk IO 1 E:	+ Sensor hinzufügen					
1	WS-RA1 SSL: Only:	Security Strong Prot	* Sensor 382 ms hinzufügen									
1	WS-RA2 SSL Only	Security Strong Prot	146 ms Sensor hinzufügen									
1	🖾 WS-DC1 🖾 🖬	Active Dir	ector 🗸 Active Directo	r 🗸 ADFS	+ Sensor							

Es wird Zeit für das richtige Zertifikat. Im Webportal wird der Hinweis dazu gezeigt:

	O Standardsicherheit (TLS 1.0, TLS 1.1, TLS 1.2) (empfohlen) O Schwächere Sicherheit (SSL V3, TLS 1.0, TLS 1.1, TLS 1.2)
Importieren Sie Ihr eigenes Zertfikat	Tipp: Sie können ihr eigenes vertrauenswürdiges SSL-Zertifikat für PRTG installieren, um Warnungen des Webbrowsers zu vermeiden, wenn Sie sich mit dem PRTG Web-Interface verbinden. Um den import des Zertifikats zu vereinfachen, empfehlen wir ihnen den Einsatz des [PRTG Certificate importer Für weitere Informationen über dieses Freeware Tool schauen Sie bitte auf unsere Webseite , wo Sie den PRTG Certificate Importer auch herunterladen können.
Momentan aktive Kombinationen von IP- Adresse/Port 🖲	◆ IP-Adresse:Port

Ich lade das Tool herunter und starte es auf dem neuen Server. Mein zuvor manuell importiertes Zertifikat wird schon angezeigt:

WS IT-Solutions

🔿 PRTG Certificate Importer		– 🗆 X
🛛 PRTG C	ERTIFICATE IMPORTER	
Step 1: Select Certificate	Source	
Windows Certificate Sto	re Certificate for WS-MON(self-signed) - usable for server authentication Certificate for prtg.ws.its(self-signed) - usable for server authentication	
O Provide a directory		
 Paste from clipboard Sample: BEGIN CERTIFICATE 		^
END CERTIFICATE		v
Version v1.0.0 build 20		Next Step >
PRTG Certificate Importer		– 🗆 X
PRTG C	ERTIFICATE IMPORTER	
Step 3: Verifying Certific	ate	
Certificate information: Certificate for prtg.ws	.its(self-signed) - usable for server authentication	
🏹 Verifying that certific	ate public key and private key are a keypair	
🍸 Testing certificate wi	th an SSL connection	
Verification of certification	te successful	
Select target directory	C:\Program Files (x86)\PRTG Network Monitor\cert\	
	$\ensuremath{\boxdot}$ Backup the previous certificate files into a subdirectory	
Version v1.0.0 build 20		< Back Finish

Das Tool hat das Zertifikat aktiviert und den Webservice neu gestartet. Und was sagt der Browser dazu?

¢) → C	۵		i 🗖 🕯	https://prtg.ws.i	ts/group.htm?	id=0&tabid=	1	
0	DuckDuckGo	🗎 Devices	🚞 Links	🏂 Wie erst	ellt man eine e 📕	Remote Deskto	p HTM		
0	Startseite	Geräte	Bib	liotheken	Sensoren	Alarme	Maps	Berichte	Protokoll
#	Geräte								
	Gruppa	ис ттс							

Auf zum nächsten Test: Funktionieren die Sensoren noch? Ich prüfe einige strichprobenhaft durch. Es sieht gut aus. Man erkennt deutlich die Lücke in der Überwachung:





Ein Sensor bleibt rot. Dieser soll einen meiner WLAN-AccessPoints auslesen:

	20 ms	482 # Univ Strong Prot.	ninzurugen		
🖻 📟 ws-pfs2.ws.its	(WS-PFS2) 🏳				
	147 ms	146 # SSL-Sicherheit.	+ Sensor hinzufügen		
🗆 📼 ws-nas1 🏳					
✓ Synology	y Syste 48 °C (002) eth 2,65	0 Traf Disk Free: /vol. kbit/Sek. 22	Y Physical Disk: % 34 °C	Physical Disk: + 37 °C	Sensor hinzufügen
🖻 📼 WS-AP1 🏳					
HTTPS	58 ms	+ Sensor hinzufügen			
	lanes.				

Dir Ursache ist schnell gefunden: der Sensor verwendet SNMP. Und dafür muss auf dem Zielsystem eine Probe-IP eingetragen sein:

Ptp-link				Access Point	~ - (
Network	Wireless Mon	itoring	Management	Syste	em
System Log Web Serve	er Management Ac	cess LED	ON/OFF	SSH	Managemer
SNMP Agent					
SNMP Agent:	Enable				
SysContact:					
SysName:					
SysLocation:					
Get Community:	public				
Get Source:	0.0.0.0				
Set Community:					
Set Source:	192.168.100.14				

Eine Anpassung später wird der Sensor grün:

×	Synology	Syste 48 °C	(002) et 2,67	h0 Traf 7 kbit/Sek.	✓ Di	sk Free: /vol. 22	 Physical D	isk: 34 °C	~	Physica	l Disk: 37 °	+	Senso hinzufü
🖻 📼 WS-AP1													
~	HTTPS	50 ms	LAN 11	kbit/Sek.	+	Sensor hinzufügen							
🗆 📼 WS-Cor	eNet1 🖡	3											

Das Monitoring habe ich auch nach extern freigegeben, damit ich Benachrichtigungen auf mein Handy gepusht bekomme. Diese Konfiguration basierte aber bereits auf dem Service-FQDN und muss daher nicht angepasst werden:

Semotezugriffs-Verwaltungskonsole			
Konfiguration VPN	VERÖFFENTLICHTE WI Alle veröffentlichten Weban	BANWENDUNGE wendungen 4 insges	A N samt
Webanwendungsproxy	Filter	Q	
Dashboard			
We Vorgangsstatus	Name	Externe	URL des Back-End-Servers
💻 Remoteclientstatus	Monitor	https://	https://prtg.ws.its/
Berichterstellung	MX	https://	https://email.ws.its/
_	RDS	https://	https://rds.ws-its.de/

PRTG sollte damit erfolgreich umgezogen sein. Auf zum nächsten Service.

Migration des Services SYSLOG

Mit SYSLOG biete ich meinen Firewalls einen zentralen Datenspeicher für ihre Logfiles an. Warum ich die Logs aufhebe? Natürlich für nachträgliche forensische Analysen! Diesen Service muss ich unbedingt mitnehmen. Am Liebsten ohne Datenverlust...

Zuerst installiere ich die gleiche Version des SYSLOG-Servers auf WS-MON. Beim Setup wird eine Voraussetzung angezeigt:



Also installiere ich .net-Framework 3.5. Wie in der Vorgängerversion ist das Feature nur auf der Installations-DVD enthalten. Eine Installation kann mit der PowerShell und dem ISO vorgenommen werden:

<pre>1 Get-WindowsFeature *frame*</pre>		
PS C:\Windows\system32> Get-WindowsFeature *frame*		
Display Name	Name	Install State
 [] .NET Framework 3.5-Funktionen [] .NET Framework 3.5 (enthält .NET 2.0 und 3.0) [X] .NET Framework 4.7-Funktionen [X] .NET Framework 4.7 [] ASP.NET 4.7 [] Windows-Biometrieframework 	NET-Framework-Features NET-Framework-Core NET-Framework-45-Fea NET-Framework-45-Core NET-Framework-45-ASPNET Biometric-Framework	Available Removed Installed Installed Available Available



{.NET Framework 3.5 (enthält .NET 2.0 und ...

Nun lässt sich das Setup starten:

No

Success

True

	Installer – 🗆 🗙
solarwinds	Choose Operating Mode The program can be run as a Service or Application
Install Kiwi Syslog	Server as a Service
This option installs Kiwi Sy program to run without th installs the Kiwi Syslog Ser	slog Server as a Windows service, allowing the e need for a user to login to Windows. This option also ver Manager which is used to control the service.
🔘 Install Kiwi Syslog	Server as an Application
This option installs Kiwi Sy requiring a user to login to	slog Server as a typical Windows application, Windows before running the application.
SolarWinds, Inc	
	<back next=""> Cancel</back>
Kiwi Syslag Server 0.6.2	
🛃 Kiwi Syslog Server 9.6.3	Installer – – X
Solarwinds	Installer — — X Service Install Options Choose the account that you would like to use to install the Kiwi service.
Solar Winds	Installer — — X Service Install Options Choose the account that you would like to use to install the Kiwi service. Due are not using the LocalSystem account to install the service
Kiwi Syslog Server 9.6.3 Solar WINDS	Installer — — X Service Install Options Choose the account that you would like to use to install the Kiwi service. but are not using the LocalSystem account to install the service count that is a member of the local Administrators group.
Kiwi Syslog Server 9.6.3 Solar WINDS IMPORTANT NOTICE: If you then you MUST use an according Install the Service using:	Installer — — X Service Install Options Choose the account that you would like to use to install the Kiwi service. ou are not using the LocalSystem account to install the service count that is a member of the local Administrators group.
Kiwi Syslog Server 9.6.3 Solar WINDS IMPORTANT NOTICE: If ye then you MUST use an acc Install the Service using: The LocalSystem Acc	Installer — — X Service Install Options Choose the account that you would like to use to install the Kiwi service. Du are not using the LocalSystem account to install the service count that is a member of the local Administrators group.
Kiwi Syslog Server 9.6.3 SOLAR WINDS IMPORTANT NOTICE: If yi then you MUST use an acc Install the Service using: Install the Service using: An Admin Account:	Installer — — X Service Install Options Choose the account that you would like to use to install the Kiwi service. Due are not using the LocalSystem account to install the service count that is a member of the local Administrators group.
Kiwi Syslog Server 9.6.3 SOLAR WINCS IMPORTANT NOTICE: If yr then you MUST use an acc Install the Service using: Install the Service using: An Admin Account: Password:	Installer — — X Service Install Options Choose the account that you would like to use to install the Kiwi service. Dou are not using the LocalSystem account to install the service count that is a member of the local Administrators group. Count:
Kiwi Syslog Server 9.6.3 SOLAR WINDS IMPORTANT NOTICE: If yr then you MUST use an acc Install the Service using: () The LocalSystem Acc () An Admin Account: Password: Confirm password:	Installer — — — X Service Install Options Choose the account that you would like to use to install the Kiwi service. Due are not using the LocalSystem account to install the service count that is a member of the local Administrators group.
Kiwi Syslog Server 9.6.3	Installer — — — X Service Install Options Choose the account that you would like to use to install the Kiwi service. Dou are not using the LocalSystem account to install the service count that is a member of the local Administrators group. Count:
Kiwi Syslog Server 9.6.3 Solar WINCS IMPORTANT NOTICE: If ye then you MUST use an acc Install the Service using: O An Admin Account: Password: Confirm password: SolarWinds, Inc.	Installer – – × Service Install Options Choose the account that you would like to use to install the Kiwi service. Du are not using the LocalSystem account to install the service count that is a member of the local Administrators group.

Ich benötige die Konfiguration. Diese kann in der alten Konsole exportiert und in der neuen importiert werden:

WS IT-Solutions

WSHowTo – Migration von PRTG & SYSLOG (WS-MON) 2019-09-08 Migration auf Windows Server 2019

						Kiwi Syslog Service Mana <u>c</u>
File	Edit \	/iew Man	age Help		_	
	Setup			Ctrl+P	•	
	Send te	st message t	o localhost	Ctrl+T	me	Message
	Purge			•	0.250	filterlog: 5,,,1000000103,hn1,match,block,in,4,0x2,0,128,28415,0,DF,6,tcp,52,192.168.100.18,23.
	Import	settings fror	n INI file		0.250	filterlog: 5,,,1000000103,hn1,match,block,in,4,0x0,,128,64373,0,DF,6,tcp,52,192.168.100.41,8.25
	Export s	ettings to IN	ll file		0.250	filterlog: 5,,,1000000103,hn1,match,block,in,4,0x2,0,128,39861,0,DF,6,tcp,52,192.168.100.41,8.2
	Create 1	Fech-Suppo	rt File (Zip)		0.250	filterlog: 234,,,1567350310,hn1,match,block,in,4,0x0,,128,14293,0,DF,6,tcp,48,192.168.100.17,88
	Exit				0.250	filterlog: 5,,,1000000103,hn1,match,block,in,4,0x2,0,128,15063,0,DF,6,tcp,52,192.168.100.17,8.2
03-	UO-ZUIJ	13.31.23	LUCAIU.INIU	132.100.1	v0.250	filterlog: 5,,,1000000103,hn1,match,block,in,4,0x2,0,128,61737,0,DF,6,tcp,52,192.168.100.23,8.2
09-	08-2019	15:31:25	Local0.Info	192.168.1	00.250	filterlog: 5,,,1000000103,hn1,match,block,in,4,0x0,,128,54568,0,DF,6,tcp,52,192.168.100.18,93.1
09-	08-2019	15:31:25	Local0.Info	192.168.1	00.250	filterlog: 5,,,1000000103,hn2,match,block,in,4,0x0,,254,32844,0,DF,17,udp,516,172.19.130.104,1
09-	08-2019	15:31:24	Local0.Info	192.168.1	00.250	filterlog: 305,,,1517226547,hn1,match,pass,in,4,0x0,,128,16032,0,none,17,udp,115,192.168.100.2

Auf dem neuen Server geht es ebenso einfach:

🔓 Kiw	i Syslog	Service N	/lanager (Free)	/ersion 9.6)								
File Ed	dit Vie	w Mana	age Help									
ð 🖸	👌 🕢 📖 🛦 🖉 😡 Display 00 (Default) 🔄											
Date	Time	Priority	Hostname	Message								
			Confirm INI fi Fil Cri Cri Cri Is 1	le load X e: C:\Admin\Syslog Server Settings.ini eated with Syslog Server Ver: 9.6.3.3 eated on Sun, 08 Sep 2019 15:32:23 +0200 eated by user: stephan-T1 this the file you want to load?								
				Ja Nein Abbrechen								

Eine kleine Anpassung ist noch erforderlich: Der Protokollpfad soll auf das neue Laufwerk zeigen:

Alle dazugehörigen Dateien kopiere ich auf den neuen Server:

ieser PC 🔸	SYSTEM (C:) + Admin	~	C "Admin" durc	hsuchen	,P	🔄 💿 🔻 🕆 퉬 🕨 Netzwerk	▶ ws-mon ▶ c\$ ▶ Admin ▶	~	C "Admin"
	Name	Änderungsdatum	Тур	Größe		☆ Favoriten	Name	Änderungsdatum	Тур
	PSTranscript	08.09.2019 15:22	Dateiordner			Desktop	PSTranscript	08.09.2019 11:08	Dateiordner
	3 SnortMon	08.09.2019 15:29	Dateiordner			Downloads	ServerSicherung.xml	08.09.2019 15:29	XML-Dokumer
	Syslog	08.09.2019 00:00	Dateiordner			📃 Zuletzt besucht	Syslog Server Settings.ini	08.09.2019 15:32	Konfigurations
	backup.log	08.09.2019 02:40	Textdokument	1 KB			퉬 SnortMon	08.09.2019 15:29	Dateiordner
	ServerSicherung.xml	08.09.2019 15:29	XML-Dokument	4 KB		E Desktop	backup.log	08.09.2019 02:40	Textdokument
F1	Syslog Server Settings.ini	08.09.2019 15:32	Konfigurationsein	8 KB		🥦 Walther, Stephan - T1			
						I➡ Dieser PC SYSTEM (C:) _원 DVD-Laufwerk (D:)			

WS IT-Solutions 20

WSHowTo – Migration von PRTG & SYSLOG (WS-MON) 2019-09-08 Migration auf Windows Server 2019

Jetzt sind alle Komponenten einsatzbereit. In meiner PFSense trage ich die IPv4 zum neuen SYSLOG-Server ein:

COMMUNITY EDITION	✓ Interfaces ✓ Firewall ✓ Services ✓ VPN ✓ Status ✓ Diagnostics ✓ Help ✓	۵								
Status / System	Logs / Settings	0								
System Firewall	DHCP Captive Portal Auth IPsec PPP VPN Load Balancer OpenVPN NTP Settings									
General Logging Opt	tions									
Forward/Reverse Display	☑ Show log entries in reverse order (newest entries on top)									
GUI Log Entries	50 This is only the number of log entries displayed in the GUI. It does not affect how many entries are contained in the actual log files.									
Log file size (Bytes)	Bytes									
Remote Logging Opt	tions									
Enable Remote Logging	☑ Send log messages to remote syslog server									
Source Address	LAN_100_SERVER This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers, bind to all interfaces.	vers								
	NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.									
IP Protocol	IPv4 This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.									
Remote log servers	192.168.100.18:514 [IP[:port]									
Remote Syslog Contents	 □ Everything ☑ System Events ☑ Firewall Events □ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns) □ DNS Events (NUSS Descrete DUSS DEsc									

Und schon geht's rund. SYSLOG nimmt die Informationen der Firewall auf und speichert sie wie gewünscht auf der neuen Partition in je eine Textdatei pro Tag:

🛐 Kiwi Sysl	og Service N	fanager (Free Ve	ersion 9.6)		
File Edit	View Man	age Help			
a 🗹 🖬	🛕 🔯 🙆	Display 00 (Default) 🔻		
Date	Time	Priority	Hostname	Message	
09-08-2019	15:41:23	Local0.Info	192.168.100.250	filterlog: 5,,,1000000103,hn1,match,block,in,4,0x0,,128,46898,0,DF,6,tcp,52,192.168.100.41,93.184.220.29	1,65027,80,0,S,22
09-08-2019	15:41:21	Local0.Info	192.168.100.250	filterlog: 5,,,1000000103,hn0,match,block,in,4,0x0,,125,108,0,DF,6,tcp,52,192.168.111.100,192.168.100.51	,51874,9100,0,5
09-08-2019	15:41:20	Local0.Info	192.168.100.250	filterlog: 5,,,1000000103,hn1,match,block,in,4,0x2,0,128,28449,0,DF,6,tcp,52,192.168.100.18,23.37.43.27,	55947,80,0,SEC,3
09-08-2019	15:41:19	Local0.Info	192.168.100.250	filterlog: 368,,,1539840813,hn3,match,pass,in,4,0x0,,128,25432,0,DF,6,tcp,52,192.168.110.101,192.168.10	0.18,3701,443,0,
09-08-2019	15:41:19	Local0.Info	192.168.100.250	filterlog: 362,,,1539840761,hn3,match,pass,in,4,0x0,,128,27175,0,none,17,udp,59,192.168.110.101,192.168	3.100.1,58705,53
09-08-2019	15:41:18	Local0.Info	192.168.100.250	filterlog: 297,,,1487312135,hn1,match,pass,in,4,0x2,0,128,48253,0,DF,6,tcp,52,192.168.100.18,192.168.10	1.2,55950,49666
09-08-2019	15:41:18	Local0.Info	192.168.100.250	filterlog: 278,,,1547394294,hn0,match,pass,in,4,0x2,0,125,23101,0,DF,6,tcp,52,192.168.101.1,192.168.100	.23,52167,443,0,
09-08-2019	15:41:18	Local0.Info	192.168.100.250	filterlog: 297,,,1487312135,hn1,match,pass,in,4,0x2,0,128,48245,0,DF,6,tcp,52,192.168.100.18,192.168.10	1.2,55949,49666
09-08-2019	15:41:18	Local0.Info	192.168.100.250	filterlog: 368,,,1539840813,hn3,match,pass,in,4,0x0,,128,25372,0,DF,6,tcp,52,192.168.110.101,192.168.10	0.18,3698,443,0,
09-08-2019	15:41:18	Local0.Info	192.168.100.250	filterlog: 368,,,1539840813,hn3,match,pass,in,4,0x0,,128,25352,0,DF,6,tcp,52,192.168.110.101,192.168.10	0.18,3697,443,0,
09-08-2019	15:41:18	Local0.Info	192.168.100.250	filterlog: 368,,,1539840813,hn3,match,pass,in,4,0x0,,128,25328,0,DF,6,tcp,52,192.168.110.101,192.168.10	0.18,3696,443,0,
09-08-2019	15:41:18	Local0.Info	192.168.100.250	filterlog: 368,,,1539840813,hn3,match,pass,in,4,0x0,,128,25324,0,DF,6,tcp,52,192.168.110.101,192.168.10	0.18,3695,443,0,
09-08-2019	15:41:18	Local0.Info	192.168.100.250	filterlog: 368,,,1539840813,hn3,match,pass,in,4,0x0,,128,25321,0,DF,6,tcp,52,192.168.110.101,192.168.10	0.18,3694,443,0,
09-08-2019	15:41:18	Local0.Info	192.168.100.250	filterlog: 5,,,1000000103,hn2,match,block,in,4,0x0,,254,32979,0,DF,17,udp,516,172.19.130.104,139.7.117.	161,40264,500,49
09-08-2019	15:41:17	Local0.Info	192.168.100.250	filterlog: 278,,,1547394294,hn0,match,pass,in,4,0x2,0,125,23077,0,DF,6,tcp,52,192.168.101.1,192.168.100	.23,52160,443,0,
09-08-2019	15:41:17	Local0.Info	192.168.100.250	filterlog: 309,,,1505035102,hn1,match,pass,in,4,0x2,0,128,45218,0,DF,6,tcp,52,192.168.100.18,172.19.120	.254,55948,443,0
09-08-2019	15:41:17	Local0.Info	192.168.100.250	filterlog: 5,,,1000000103,hn1,match,block,in,4,0x2,0,128,46897,0,DF,6,tcp,52,192.168.100.41,93.184.220.2	9,65027,80,0,SE
09-08-2019	15:41:17	Local0.Info	192.168.100.250	Chulue, E. 1000000100 Le0 Let Liet 14 0.0 04 00000 0 0 00 170 10 100 404 47 70 170 00	F 441E0,5094,0,9
09-08-2019	15:41:17	Local0.Info	192.168.100.250	🖉 ≂ SYSLOG □	× 0,0,SEC,
09-08-2019	15:41:17	Local0.Info	192.168.100.250	Datei Start Freigeben Ansicht	v 🕜 2352,53,9
					0
				C	<u>þ</u>
				Schnellzugriff	2
				иевктор 📌 📄 2019-09-08.DXt	
				🖶 Downloads 🛷	

Auf dem alten Server kommen nun keine Datenpakete mehr an. Für die Datenmigration der bereits gesammelten Logfiles beende ich den alten SYSLOG-Service:

						Kiwi Syslog Service Manager (Free Version 9.6)
File Edit \	/iew	Man	age Help			_
a 📝 🖬	<u>a</u> (Start the Syslogd	service	Ctrl+F1	
Date	Т		Stop the Syslogd	service	Ctrl+F2	3
09-08-2019	15:4		Ping the Syslogd	service	Ctrl+F3	339): /xmlrpc.php: Resyncing OpenVPN instances.
09-08-2019	15:4		Show the Syslogo	d service state	Ctrl+F4	339]: /xmlrpc.php: Gateway, none 'available' for inet6, use the first one configured. "
09-08-2019	15:4		Debug options		+	eload_status: Reloading filter
09-08-2019	15:41	:11	User.Notice	192.168.100.251	check_r	reload_status: Syncing firewall
09-08-2019	15:41	:10	Syslog.Error	192.168.100.250	syslogd:	exiting on signal 15
09.08.2019	15-41	-10	Llear Notica	192 169 100 250	check i	ralaad, status: Suncing firowall

Als nächstes kopiere ich alle bisherigen Logfiles auf den neuen Server. Auf dem alten hatte ich nur die NTFS-Kompression zum Platzsparen aktiv. Auf dem Neuen wird das die Data-Deduplication übernehmen:

🎉 l 🕞 🚺 = I	Syslog			_ 🗆 X	_ 😺 I 🕞 🚯 ≑ I	SYSL	.OG	
Datei Start Freigeben .	Ansicht			~ (Datei Start Freigeben	Ansicht		
🛞 💿 🝷 🕇 퉬 🕨 Dieser PC	SYSTEM (C:) Admin Syslog	~ c	් "Syslog" du	rchsuchen 🔎	🛞 💿 🔻 🛉 🎽 🕨 Netzwerk	▶ ws-mon ▶ e\$ ▶ SYSLOG	✓ C "SYSLOG"	durchsuchen
🔆 Favoriten	Name	Änderungsdatum	Тур	Größe	🚖 Favoriten	^ Name	Änderungsdatum Typ	Größe
Desktop	2019-09-08-alt.bit	08.09.2019 15:41	Textdokument	34.441 KB	Desktop	2019-09-08.txt	08.09.2019 15:43 Textdokument	2
Downloads	2019-09-07.txt	08.09.2019 00:00	Textdokument	58.052 KB	Downloads			
📃 Zuletzt besucht	2019-09-06.txt	07.09.2019 00:00	Textdokument	66.178 KB	📃 Zuletzt besucht			
	2019-09-05.txt	06.09.2019 00:00	Textdokument	62.076 KB				
Desktop	2019-09-04.txt	04.09.2019 23:59	Textdokument	64.940 KB	Desktop			
Walther, Stephan - T1	2019-09-03 +++	04 09 2019 00-00	Textdokument	60.674 KB	🔋 Walther, Stephan - T1			
👰 Dieser PC	🗋 2019-09- 🗿 🛛 Eigenschaften	von 2019-09-03.txt,	× ent	55.352 KB	🛤 Dieser PC			
SYSTEM (C:)	2019-09-		ent	66.294 KB	SYSTEM (C:)			
Admin	2019-08-		ent	58.217 KB	DVD-Laufwerk (D:)			
PSTranscript	2019-08- 641 Dateien,	0 Ordner	ent	56.206 KB	🖵 Freigaben (M:)			
iii SnortMon	🗋 2019-08-		ent	59.277 KB	; Bibliotheken			
🁪 Syslog	2019-08- Typ: Alle your Typ	Textdokument	ent	55.603 KB	Netzwerk			
Benutzer	2019-08-		ent	55.169 KB	🛤 ws-mon			
鷆 inetpub	2019-08- OPE: Alle in C: yad	min (sysiog	ent	53.998 KB	👱 c5			
PerfLogs	2019-08- Größe: 22,0 GB (23.	670.695.353 Bytes)	ent	48.952 KB	January Admin			
鷆 Program Files (x86)	2019-08- Größe auf 6,63 GB (7.1	29.038.848 Bytes)	ent	54.651 KB	Benutzer	=		
鷆 Programme	2019-08-		ent	55.631 KB	PerfLogs			
Windows	2019-08- Attribute: Schreibge	schützt Erweite	ert	63.041 KB	Program Files (x86)			
🔮 DVD-Laufwerk (D:)	2019-08- Versteckt		ent	56.274 KB	Drogramme			
🖵 Freigaben (M:)	2019-08-		ent	66.904 KB	Windows			
See Section 1					1 A A			

Nach wenigen Minuten hat die Deduplication (manuell gestartet) ganze Arbeit geleistet:

📥 Serve	r-Manager							-				
\mathbf{E}	Server-Manager • Datei-/Speicherdienste • Volumes • • 😨 🏲 Verwalten Tools											
ii i	Server Volumes Datenträger	Alle Volumes 4 in	sgesamt (iii) •	• (8) •				AUFGABEN	•			
	Speicherpools Freigaben	▲ Volume Source Sou	Status Bezeichnung des	Bereitstellung Kapazi	ät Freier Speicherplatz	Deduplizierungsrate	Einsparungen durch Deduplizierung	Verwendeter P				
	iSCSI Arbeitsordner	\\?\Volume(53 \\?\Volume(a8	Wiederherstellung	Fest 499 Mi Fest 95,0 M	76,8 MB 69,2 MB				1			
		C:	System	Fest 99,4 Gi	84,3 GB	000/	22.5.60					
		E.	Monitoring	Fest 100,0 C	95,1 08	6270	22,3 06	•				

Zu dem SYSLOG-Service gehört noch ein ScriptTask von mir. Dieser wertet die Protokolle aus und schickt mir bei Bedarf Warnungen per Mail. Der Task ist einfach exportierbar:



Die XML-Datei importiere ich aus WS-MON:

WS IT-Solutions

WS IT-Solutions



Mein Script Snort-Monitor untersucht die Logfiles. Dazu muss es aber auch von dem neuen Pfad erfahren. Die Konfiguration passe ich in einer Variablen im Script selber an:



Ich starte das Script über den Task. Es dauert nicht lange bis zum nächsten Alarm. Damit ist auch diese Funktion getestet:

offen	offen											
Diese	Diese Nachricht wurde mit der Priorität "Hoch" gesendet.											
neue II	neue IPS-Alerts											
count	TotalCount	SourceIP	DestinationIP	SourcePort	DestPort	FirstSeen	LastSeen	Classification	AlertMessages	SourceName	DestinationName	
198	198	192.168.110.101	192.168.100.1	5655, 5656, 5659, 6201, 6202, 6203, 6470, 6471, 8588, 8589, 8590, 8591, 8931, 8932, 8933, 8934, 9814, 9815, 9816, 9817	5985	10:20:53	15:07:37	Potentially Bad Traffic	ET USER_AGENTS WinRM User Agent Detected - Possible Lateral Movement	WS-CL1.ws.its	WS-DC1.ws.its	
198	198	192.168.110.101	192.168.100.1	5655, 5656, 5659, 6201, 6202, 6203, 6470, 6471, 8588, 8589, 8590, 8591, 8931, 8932, 8933, 8934, 9814, 9815, 9816, 9817	5985	10:20:53	15:07:37	Potentially Bad Traffic	ET POLICY WinRM wsman Access - Possible Lateral Movement	WS-CL1.ws.its	WS-DC1.ws.its	
				10061,								

Weil ich gerade an den Aufgaben dran bin importiere ich auch die Aufgabe für meine Systemstate-Datensicherung. Mit dieser kann ich das System via BareMetalRecovery zuverlässig wiederherstellen. Das Script für die Sicherung muss unter einem gMSA-Account laufen. Diesen kann ich von meinem DomainController konfigurieren:



드 gM	ISA-Admin					— C	x c
vorhan	dene gMSA:		zugehörige Server:			zugehörige Gruppen:	
gMSA gMSA gMSA	ADFS (Service ADFS) Backup (TeakUser für BMR) Montor (TaskUser für Monto SQLDPM (Service SQL auf WS SQLDPM (Service SQL auf WS	а) -DPM)	WS-DC1.ws.its WS-FS1.ws.its WS-MX1.ws.its WS-CA1.ws.its WS-CA1.ws.its WS-CA1.ws.its WS-FS2.ws.its WS-FA2.ws.its WS-FA2.ws.its WS-RDS2.ws.its WS-RDS3.ws.its WS-RDS3.ws.its WS-RDS3.ws.its WS-DC2.ws.its WS-DC2.ws.its WS-DC2.ws.its WS-DC4.ws.its WS-WAC.ws.its WS-MON.ws.its	(online)		direkte Gruppen: GG-SEC-Server-JB-Admins GG-SEC-Server-BD-S-Admins GG-SEC-Server-MX-Admins GG-SEC-Server-HyperV-Admins GG-SEC-Clients-JB-Admins GG-SEC-Clients-JB-Admins GG-Admin-Backup Sicherungs-Operatoren indirekte Gruppen (durch Verschachtelung): LD-Admin-Backup LD-Admin-SQL-DPM LD-AD-Admin-Ara-R LD-SEC-Clients-JB-Admins LD-SEC-Clients-JB-MVinRM LD-SEC-Clients-VPerV-Admins LD-SEC-Server-HyperV-Login LD-SEC-Server-HyperV-RDP LD-SEC-Server-HyperV-WinRM	~
erst	elle gMSA lösche gMSA	bearbeite gMSA	weiterer Serve	er entferne Server	teste gMSA	weitere Gruppe entferne Gruppe	
Einsat	erstelle gMSA Tösche gMSA bearbeite gMSA Einsatz als: Task v Klicke in eine Zeile Server TaskName WS-MON nocapowatchdog		n die Optionen zu a	aktivieren.			
	Server	TaskName		Account		Pfad	<u>^</u>
	WS-MON	npcapwatchdog		SYSTEM		λ	
	WS-MON	ServerSicherung		ws\gMSA-Backup\$		N	
	WS-MON	SnortMonitor		SYSTEM		N	

Damit sind alle Funktionen außer IPAM auf den neuen Server übertragen.

Migration der Monitoring-Scripte von WS-RDS1

Zwei weitere Scripte, die ich für Auswertungen verwende, liegen noch auf einem anderen Server. Diese sind aber besser auf dem neuen WS-MON aufgehoben. Daher exportiere ich zunächst die dazugehörigen, geplanten Aufgaben auf dem aktuellen Server WS-RDS1:

🕑 Aufgabenplanung		- + (lit. 6	"WS-RDS1" auf "WS-HV1"
Datei Aktion Ansicht ?				
🗢 🏟 🖄 🖬 🔽 🖬				
 Aufgabenplanung (Lokal) Aufgabenplanungsbibliot 	Name CreateExplorerShellUnelevatedTask PrivilegedADUser-Analyse ServerMonitor ServerSicherung Allgemein Trigger Aktionen Bedir	Status Bereit Bereit Bereit	Trigger Bei Aufgabeners Jec Ausfüh Jec Beende Deaktiv Exporti Eigense Lösche	rstellung oder - modifizierung n 05:00 Ube inden Montag, beginnend mit dem 16:10 hren len ivieren tieren schaften en

Danach kopiere ich die Scriptdateien auf WS-MON:

🛛 🔄 🖬 🖬 Adm	iin			-		📕 🛃 🗖 = Admin				- 1	- ×
ei Start Fr	eigeben Ans	icht			~ 🕐	Datei Start Freigeben	Ansich	t			~ 🛛
→ • ↑	Dieser PC > S	öystem (C:) → Admin	∨ "A	dmin" durchsuchen	Q	← → × ↑ 📘 > Netzwer	k > ws-i	rds1 → c\$ → Admin → 🗸 🗸	ڻ "Admir	n" durchsuchen	Q,
🖨 Schnellzugriff	^	Name		Änderungsdatun	n Typ	SnortMon	^	Name	4	Ånderungsdatum	Тур
E. Desktop	*	PrivilegedADUser-Analyse		09.09.2019 16:50	Dateiordr	Desktop		PrivilegedADUser-Analyse	C	9.09.2019 05:00	Dateiord
Downloads	*	PSTranscript		08.09.2019 11:08	Dateiordr	& Walther, Stephan - T1		PSTranscript	C	9.09.2019 04:45	Dateiord
Dokumente		ServerMonitor		09.09.2019 16:50	Dateiordr	Dieser PC		RDS	C	5.04.2017 19:28	Dateiord
Dild		SnortMon		08.09.2019 16:15	Dateiordr			ServerMonitor	C	9.09.2019 04:45	Dateiord
Bilder	*	backup.log		09.09.2019 02:40	Textdoku	System (C:)		- Tools	C	5.04.2017 19:28	Dateiord
Admin	*					Monitoring (E:)		backup.log	C	9.09.2019 04:56	Textdoku
👝 Monitoring (E:)						🛖 Freigaben (M:)					
SnortMon						🐂 Bibliotheken					

Zuletzt importiere ich die Scriptaufgaben:

WS IT-Solutions

Datei Aktion Ansicht ? Aufgabenplanung (Lokal) 	Aufgabenplanung					
 	Datei Aktion Ansicht ?					
Image: Constraint of the second se	🗢 🔿 🔁 📰 🔽 📷					
	Aufgabenplanung (Lokal) Aufgabenplanungsbibliot	Name npcapwatchdog ServerSicherung SnortMonitor User_Feed_Synchro L	onization-{A6AB5720-6308-4662-916F-8AAI Einfache Aufgabe erstellen Neue Aufgabe erstellen <mark>Aufgabe importieren</mark> Aktualisieren	F6CFCB9E1}	Status Bereit Wird ausgeführt Bereit	Trigger Beim Systemstart Jeden Tag um 01:00 Uhr Es sind mehrere Trigger definiert. Jeden Tag um 02:01 Uhr - Trigger

Der ausführende Account ist bei beiden Aufgaben ein spezieller Group Managed Service Account (gMSA). Von diesem kennt nur der DomainController das Passwort. Da die Aufgabenkonsole das Importieren ohne Passwort nicht erlaubt ändere ich den Account temporär:

	Aufgabe erstellen	h.	Benutzer, Dienstkonto oder (Gruppe auswählen	×
	Allgemein Trigger	r Aktionen Bedingu	Objekttyp:		1
	Name:	ServerMonitor	Benutzer, Dienstkonto oder Int	egriertes Sicherheitsprinzipal	Objekttypen
ironization	Speicherort	1	Suchpfad:		
	Autor	WS\sysadm	Gesamtes Verzeichnis		Pfade
	Beschreibung:		Geben Sie die zu verwendende	en Objektnamen ein (<u>Beispiele</u>):	
	besenreibung.		admin-setup		Namen überprüfen
	Sicherheitsoption	nen	Erweitert	OK	Abbrechen
	Beim Ausführen	der Aufgaben folgende	es Benutzerkonto verwenden:		
	gMSA-Monitor\$			Benutzer oder Gruppe ände	rn
	O Nur ausführer	n, wenn der Benutzer a	angemeldet ist		
	Unabhängig	von der Benutzeranme	eldung ausführen		
	Kennwort	nicht speichern. Die A	ufgabe greift nur auf lokale Co	omputerressourcen zu.	
	Mit höcheten	Privilegien ausführen			
	Mit nochsten	r nviegien ausiumen			
		K C C	Mindaus (2) 7 Mindaus Cana	-71 2000 02	

Aufgabenplanung				
Datei Aktion Ansicht ?				
🗢 🄿 🙍 📰 🚺				
Aufgabenplanung (Lokal) > Aufgabenplanungsbibliot	Name (b) npcapwatchdog (c) PrivilegedADUser-An (c) ServerMonitor (c) ServerSicherung (c)	alyse	Status Bereit Bereit Bereit Bereit	Trigger Beim Systemstart Wöchentlich um 05:00 Jeden Tag um 04:45 Uh Jeden Tag um 01:00 Uh
	Allgemein Trigger Al Name: Pri Speicherort: Autor: W3 Beschreibung:	tionen Bedingungen Einstellungen vilegedADUser-Analyse	Verlauf	
	- Sicherheitsoptionen - Beim Ausführen der A admin-setup Nur ausführen, wu	ufgaben folgendes Benutzerkonto verwe inn der Benutzer angemeldet ist Jer Benutzeranmeldung ausführen	nden:	

Der Account admin-setup hat gar nicht die erforderlichen Rechte. Er ist aber auch nur ein Dummy, bis ich den richtigen Account mit meinem gMSA-Tool vom DomainController aus konfiguriere:

드 gMSA-Admin						-		×
vorhandene gMSA:		zugehörige Serv	er:		zugehörige Gruppe	n:		
gMSA-ADFS (Service ADFS) gMSA-Backup (TaskUser für gMSA-SQLDPM (Service SQL	BMR) Monitoring) auf WS-DPM)	WS-DC1.ws.its WS-IPM ws.its WS-MON.ws.its	online)		direkte Gruppen: GG-SEC-Server-J GG-SEC-Server-J GG-SEC-Server-N GG-SEC-Server-N GG-SEC-Server-N GG-SEC-Clients-J Domänen-Admins 		: pe	~
erstelle gMSA lösch	e gMSA bearbeite gMSA	weiterer Serve	r entferne Server	teste gMSA	weitere Gruppe	entferne Gruppe		
Einsatz als: Task	Klicke in eine Zeile un	m die Optionen zu a	ktivieren.					
Server	TaskName		Account		Pfad			^
WS-MON	PrivilegedADUser-Ana	llyse	gMSA-Monitor\$		λ.			
WS-MON	ServerMonitor		gMSA-Monitor\$		X			

Und nun passt es auch in der Aufgabenverwaltung:

NS IT-Solutions

④ Aufgabenplanung							
Datei Aktion Ansicht ?							
🗢 🄿 🙍 📰 🚺							
Aufgabenplanung (Lokal) Aufgabenplanungsbibliot	Name PrivilegedADUse ServerMonitor ServerSicherung	Analyse	Status Bereit Bereit Bereit Bereit	Trigger Beim Systemstart Wöchentlich um 05:00 Uh Jeden Tag um 04:45 Uhr Jeden Tag um 01:00 Uhr			
	Allgemein Trigger	Aktionen Bedingungen	Einstellungen	Verlauf			
	Name:	ServerMonitor					
	Speicherort:	١					
	Autor:	WS\sysadm					
	Beschreibung:						
	Sicherheitsoption	en					
	Beim Ausführen	der Aufgaben folgendes Benu	tzerkonto verwe	nden:			
	gMSA-Monitor\$						
	 Nur ausführe 	n, wenn der Benutzer angeme	ldet ist				
	📕 🔿 Unahhängiga	an dar Danutzaranmalduna -	fillbacer				

Beide Scripte benötigen das Feature RSAT-AD-PowerShell. Dieses installiere ich nach:

🚬 Adm	ninistrator: Windows	PowerShell		
PS C:\>	Add-WindowsFeat	ture RSAT-AD-P	owerShell	ſ
Success	Restart Needed	Exit Code	Feature Result	
True	No	Success	{Remoteserver-Verwaltungstools, Active Dir	
PS C:∖>	E			

Dann noch ein kleiner Testlauf, ob alles passt. Dazu starte ich beide Aufgaben und warte auf die üblichen Mails. Die erste Mail kommt nach wenigen Minuten:

Benutzer	Level	Policy	Lockout	ProtectedUser	Enabled	Description	SchedTasks	ServiceUser	LastLogon	PWfixed	PWendless	PWlastset	PWexpire	PWcomplex	P\
service- prtg	1	PSO- AdminUser	3	True	True	ServiceAccount für PRTG auf WS-IPM			2019-09-06 22:20:52	False	False	2019-09-08 13:30:56	2019-12- 07 13:30:56	True	Fa
sysadm	1	PSO- AdminUser	3	True	True	DefaultAdmin			2019-09-09 16:45:20	False	False	2019-07-01 20:17:20	2019-09- 29 20:17:20	True	Fa
stephan	2	PSO- StandardUser	10	False	True	Standardbenutzer Stephan			2019-09-05 09:05:54	False	False	2019-06-24 07:53:51	2019-09- 22 07:53:51	True	Fa
stephan- T1	2	PSO- AdminUser	3	True	True	AdminAccount für Stephan - Server			2019-09-04 09:18:38	False	False	2019-07-01 20:01:32	2019-09- 29 20:01:32	True	Fa
stephan- T2	2	PSO- AdminUser	3	False	True	AdminAccount für Stephan - Clients			2019-08-07 21:38:02	False	False	2019-07-01 20:07:12	2019-09- 29 20:07:12	True	Fa

Zusammenfassung:

offen

Generiert auf:	WS-MON			
Scriptversion:	V1.13			
Scan-Dauer	106 sec			

Und auch das andere Script arbeitet wie erwartet und sendet mir eine Mail. Fein. Auf dem alten Server WS-RDS1 deaktiviere ich die beiden Aufgaben. Ich möchte ja keine doppelten Mails haben:



Nacharbeiten

Entfernen des alten Servers WS-IPM

Den alten Server WS-IPM schalte ich einfach aus. IPAM hatte einige GPOs im ActiveDirectory erstellt. Diese kann ich einfach löschen:

GPO-Computer-Sicherheit-Scope-Server-Standar	10	CPO Computer Sigherhoit Audit	Main	
GPO-Computer-Sicherheit-Scope-Zero	17	GPO-Computer-Sicherheit-Funiore	Nein	J
GPO-Computer-Sicherheit-SmartCard	19	GPO-Server-Win2012R2	Nein	о Г
GPO-Computer-Sicherheit-UAC-light	19	GPO-Server-Win2016	Nein	J
GPO-Computer-Sicherheit-Zertifikate	20	GPO-Server-Win2019-Datenschutz	Nein	J
GPO-Computer-WSUS	21	GPO-Server-Win2019-Konfiguration	Nein	J
GPO-Computer-WSUS-Manuell	22	GPO-Server-Win2019-Sicherheit	Nein	J
GPO-IPAM-DC-NPS		—		
GPO-IPAM-DHCP				
GPO-IPAM-DNS				
GPO-Server-RDS				
GPO-Server-RDS-Sicherheit-Applocker				
GPO-Server-RDS-Sicherheit-User				
GPO-Server-Win2012R2				
GPO-Server-Win2016				
GPO-Server-Win2019-Datenschutz				
GPO-Server-Win2019-Konfiguration				
GPO-Server-Win2019-Sicherheit				
S 100 0 50				

Im AD lösche ich das Computerkonto. In ein paar Tagen entferne ich auch die VM aus meinem alten Hyper-V-Host und verschiebe die neue VM zur Lastverteilung dorthin.

Konfiguration der Datensicherung

Meine Datensicherung basiert auf 2 Plattformen, damit unterschiedliche Anforderungen erfüllt werden. Eine Plattform ist meine SystemState-Sicherung. Diese basiert auf das Windows-Backup-Feature und wird von einem zentralen Script befeuert. Alle Server rufen dieses Script über eine geplante Aufgabe auf. In einer zentralen Konfigurationsdatei kann ich dann die Sicherungseinstellungen definieren. Das Script rendert daraus individuelle wbadmin-commands und die Server sichern ihren SystemState im Rotationsverfahren auf ein Netzlaufwerk.

In der Datensicherungskonfiguration (eine kleine Textdatei) tausche ich den Eintrag des alten Servers gegen den neuen aus:

Sicherung.	ini - Editor				
Datei Bearbe	iten Forma	at Ansicht Hil	fe		
'Reporte p sendeMail= sender=ser MailSubjec recipients mailserver recipients mailserver	er Mail : an vice-mai tBackup= 1=logmai 1=email.u 2= 2=	senden ling@ws-its ServerSicheu ls@ws-its.do ws.its	.de rung e		
[Sicherung 'Optionen:	en] -ohneTa	g			
'Server	# Delay	# Tage	# JobName	# JobDefinition	<pre># Dest # Optionen</pre>
WS-CM	#0	# 3@135	# BMR	<pre># c: -systemstate -allCritical -vssFull</pre>	#1 #
WS-DC1	# 20	# 6@135	# BMR	<pre># c: -systemstate -allCritical -vssFull</pre>	#1 #
WS-FS1	# 40	# 3@135	# BMR	<pre># c: -systemstate -allCritical -vssFull</pre>	#1 #
WS-HV1	# 60	# 6@135	# BMR	<pre># c: -systemstate -allCritical -vssFull</pre>	#3 #
WS-RA1	# 80	# 6@135	# BMR	<pre># c: -systemstate -allCritical -vssFull</pre>	#1 #
WS-MON	# 100	# 6@135	# BMR	<pre># c: -systemstate -allCritical -vssFull</pre>	#1 #
WS-RDS1	# 120	# 6@135	# BMR	<pre># c: -systemstate -allCritical -vssFull</pre>	#1 #
WS-WAC	# 140	# 3@135	# BMR	<pre># c: -systemstate -allCritical -vssFull</pre>	#1 #
WS-MX1	# 160	# 6@135	# BMR	<pre># c: -systemstate -allCritical -vssFull</pre>	#1 #



Damit ist das Betriebssystem und die Installation sicher. Bisher genügte dies, denn alle Logfiles lagen ja auf Laufwerk C:. Jetzt verwende ich aber eine zusätzliche Partition für die Protokolle. Diese möchte ich mit meiner zweiten Plattform sichern: dem Data Protection Manager (DPM). Diesen verwende ich bevorzugt für Nutzdaten.

DPM benötigt einen lokal installierten Agent. Diesen kann ich über eine selber erstellte Freigabe herunterladen und installieren:

reigeben A	Ansicht	Verwalten Anwendungstools	Agent						
> Netzwerk >	ws-dpm	n → Agent							
		yt. yt	Name ^	Änderungsdatum 18.02.2019 10:33 13.01.2019 22:34	Typ Anwendung MANIFEST-Datei	Größe 230.229 KB 2 KB			
	-	* *	i dpmra.msi	18.02.2019 10:55	Windows Installer	216.048 KB		 	
an - T1		Seduredtu / 1639266/200	/U ef95CT Unstallagent.exe						^
::) :)				Microsoft System	n Center DPM Protectio	on Agent			
_				Time remaining: 1	seconds		Cancel		
ng									

Nach dem Setup definiere ich den DPM-Server und stelle eine Verbindung zwischen beiden mit der DPM-Konsole her:

C:\Windows\System52\cmd.exe	_	
onfiguring dpm server settings and firewall settings for dpm server =[ws-dpm.ws.its] onfiguring dpm server settings and firewall settings for dpm server =[ws.its\WS-DPM]		Â
he following firewall exceptions has been added: - Exception for DPMRA.exe in all profiles. - Exception for Windows Management Instrumentation service. - Exception for RemoteAdmin service. - Exception for DCOM communication on port 135 (TCP and UDP) in all profiles. onfiguration completed successfully!!!Drücken Sie eine beliebige Taste		

System Center 2019 DPM Adn Datei Aktion Ansicht ?	ministrator Co	onsole							
Hinzufügen Schutz En	ntfernen Co Server	mputerdrosselung Aktualisieren	VMware verwalten Anmeldei	Updates Optionen prüfen Optionen	i ? Info Hilfe Hilfe				
Produktionsserver		Liste unten durchsuchen							
Geschützt: 6		Computername		Тур	Clustername	Domäne	Ag	ent-Status	Ager
Ungeschützt: 2		Geschützte Computer n	nit Schutz-Ag	jent: (6 Computer)					
Upgrade verfügbar: 0		WS-FS2		Windows-Server	-	ws.its		Unbekannt	-
		WS-HV1		Windows-Server		ws.its		Unbekannt	-
Datenspeicher		WS-HV3		Windows-Server	-	ws.its		Unbekannt	-
Anzahl von Datenträgern:	0	WS-MX1		Windows-Server	DAG-1.ws.its	ws.its	1	Unbekannt	-
Anzahl von Volumes/Ordnern	n: 1	WS-MX2		Windows-Server	DAG-1.ws.its	ws.its		Unbekannt	-
Gesamtkapazität:	1.199,9	WS-RDS3		Windows-Server	-	ws.its		Unbekannt	-
314 92 GB		Ungeschützte Compute	r mit Schutz-	Agent: (2 Computer					
□ 885.00 GB		WS-FS1		Windows-Server	-	ws.its		Unbekannt	-
		WS-MON		Windows-Server	-	ws.its		<mark>)K</mark>	-
Online									
Registrierungsstatus:	Un								
Vareion dae Azura Backup Ar	nente: -								

Die Sicherung selber definiere ich über eine neue Schutzgruppe. In einer Schutzgruppe werden Quelle, Ziel, Aufbewahrungsdauer, Sicherungszeiten, ... erfasst:

Gruppenmitgli	len ieder auswählen
Wählen Sie die Dater	n aus, die geschützt werden sollen.
Schritte:	Aktivieren Sie die entsprechenden Kontrollkästchen unter 'Verfügbare Mitglieder', um die Daten auszuwählen, die geschützt
Willkommen	Wenn die Datenquellen, die Sie schützen möchten, nicht in der Struktur unten angezeigt werden, klicken Sie auf den folgen
Schutzgruppentyp auswählen	Nicht unterstützte Konfigurationen
	Vendgoale mitglieden Ausgewallte mitglieden
Grupperinitgieder auswahlen	Ausgewanite Mitglieder Computer
 Methode f ür die Datensicherheit ausw ählen 	ws-bpm ws-bpm ws-non-ws-ns
Kurzfristige Ziele auswählen	B WS-FS2
Konsistenzprüfungsoptionen	Bin
auswanien	B WS-MON
Status	
	Datenquellen aktualisieren Entfemen Klicken Sie auf "Aktualisieren", um den Cache zu Ausgeschlossene Ordner: 0 Anzeigen Aktualisieren 0 Dateien ausschließen
	< Zurück Weiter > Abbrechen Hilfe
Schritte: Willkommen	Schutzgruppenname: Schutz-Monitoring
Schutzgruppentyp auswählen	Wählen Sie die gewünschte Schutzmethode aus.
Gruppenmitglieder auswählen	💜 🗹 Ich möchte kurzfristigen Schutz per: 🛛 Datenträger 🗸 🗸
 Methode f ür die Datensicherheit ausw ählen 	
Kurzfristige Ziele auswählen	Ich möchte Onlineschutz Konfigurieren Sie den Onlineschutz auf der Seite "Verwaltung" um diese Ontion zu
Konsistenzprüfungsoptionen	aktivieren.
auswählen	Lch möchte langfristigen Schutz per Band
Zusammenfassung	Der Schutz mithilfe von Bandoptionen ist deaktiviert, weil keine Bandbibliotheken
Status	erkannt wurden oder weil die Schutzgruppe Datenqueilen entnalt, die nicht auf
log Neue Schutzgruppe erstell	len
Ein Schutzplan wird v	e ie angeben von DPM mithilfe Ihrer kurzfristigen Wiederherstellungsziele erstellt.
Schritte:	Geben Sie Ihre kurzfristigen Wiederherstellungsziele für den datenträgerbasierten Schutz an.
Willkommen	Beibehaltungsdauer: 30 🛋 Tage
Schutzgruppentyp auswählen	
Gruppenmitglieder auswählen	synchronisierungstrequenz: U Alle 15 Minuten
Methode für die	 Direkt vor einem wiedemersteilungspühkt
Datensicherheit auswählen	Dateiwiederherstellungspunkte
Datenspeicherzuordnung	Geben Sie Wiederherstellungspunkte für Dateimitglieder an.
überprüfen	Viederherstellungspunkte 18:00 Täglich
Replikaterstellungsmethode auswählen	
Konsistenzprüfungsoptionen auswählen	
Zusammenfassung	
Status	

🔯 Neue Schutzgruppe erstell	en						>			
Ein Schutzplan wird w	e le angeben on DPM mithilfe Ihrer k	urzfristigen Wiederhe	erstellungsziele	erstellt.						
Schritte:	Überprüfen Sie den	für jede Datenguelle	zugewiesenen	Speicherplatz, und	ändem Sie diesen o	egebenenfalls.				
Willkommen	Datenspeicherzuordnung für neue Mitglieder									
Schutzgruppentyp auswählen	Gesamtdatengröf	le:		5,11 GB						
•	In DPM bereitzus	tellender Datenspeic	her:			10,20 GB				
Gruppenmitglieder auswählen	Gruppenmitglieder auswahlen Durchschnittlich zugeordneter Datenspeicher für Änderungsjournal auf geschützten									
 Methode f ür die Datensicherheit ausw ählen 	Details zur Datensp	eicherzuordnung:								
Kurzfristige Ziele auswählen	Datenquelle	1		Datengröße	Speicherpl	Zielspeicher				
 Datenspeicherzuordnung überprüfen 	E:\ auf ws-m	ion.ws.its		5,11 GB 10,20 G		Pool-DPM - 874,81 GE				
 Replikaterstellungsmethode auswählen 										
 Konsistenzpr üfungsoptionen ausw ählen 										
Zusammenfassung										
 Status 	Verfügbarer Speich	er auf dem Zieldaten	träger:							
	Name /	Anzeigen	Zulässige	Date 0	äesamtsp F	reier Sp	Nicht gen			
	G:\	Pool-DPM	Alle	1	.199,93 GB	874,81 GB	0 KB			

Ich lasse die initiale Sicherung direkt starten:

System Center 2019 DPM Administrator Cons	sole									
Neu Andern Onlineschutz Löschen hinzufügen Schutzgruppe	Optimieren Konsistenzprüfung Vorgänge mit	Datenträger Online Band	Self-Service-Wiederherstellung Verwaltt	Bandkatalogbeibehaltung	Status der Wiederherstellungspunkte Berichte	Updates Optionen prüfen Optionen	info Hi			
✓ Integrität der Datenquelle ⊗ Kritisch (0)	Gruppieren nach: Schutzgrup	pe 🔿 Computer								
Ø OK (16) ⚠ Wamung (0)	Schutzgruppenmitglied /	Exchange (Mitglieder insgesamt: 8)		Тур	Schu	utzstatus				
 Alle Schutzgruppen Schutz-Exchange Schutz-Eilenenver 	Computer: ws-mx1.ws. Computer: ws-mx2.ws.	its								
Schutz-HyperV Schutz-JB Schutz-JB	Schutzgruppe: Schutz-Fileserver (Mitglieder insgesamt 2) Computer: we-fa2.waits Computer: we-fa2.wa									
	Gord Schutzgruppe: Schutz-Hyper (Mitglieder insgesamt 4) E Computer: ws-hv1.ws.its E Computer: ws-hv1.ws.its									
	Ornputer: ws-rds3.ws.its									
	Schutzgruppe: Schutz- Schutzgruppe: Schutz- Schutzgruppe: Schutz-	Schutzgruppe: Schutz-Monitoring (Mitglieder insgesamt. 1) E Computer: ws-mon.ws.its								
	El El			Volume	(i) Re	eplikaterstellung in Bearb	eitung			

Zusammenfassung

Na das hat doch mal super funktioniert. Ein weiterer Server mit seinen Services läuft auf Windows Server 2019! Dazu habe ich Funktionen eines anderen Servers auf eine geeignetere Plattform verschoben.

Und der IPAM war sehr einfach. Denn den gibt es nun nicht mehr.