

Inhalt

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

Zielsetzung

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

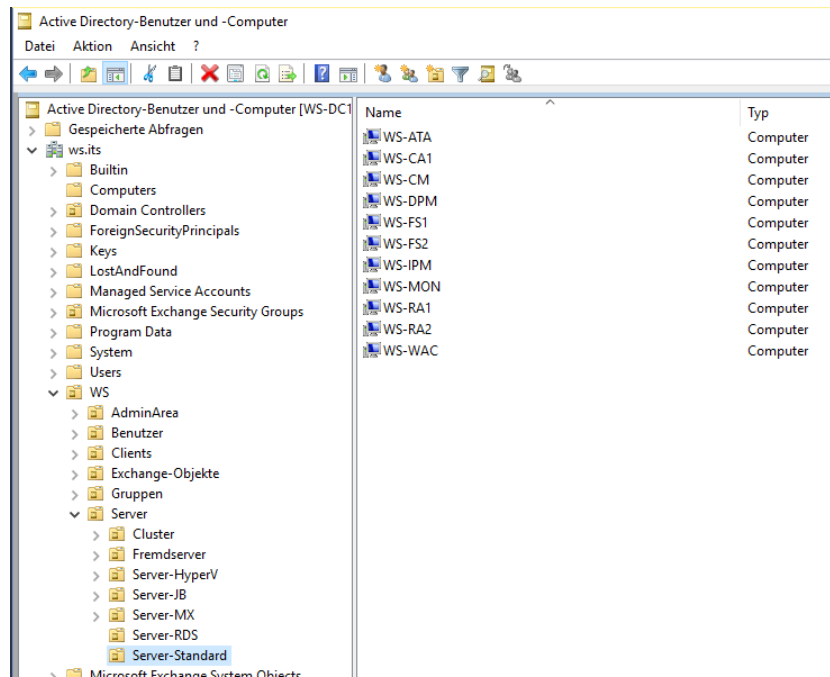
New-Item -Path 'V:\Hyper-V\WS-MON\Virtual Hard Disks' -ItemType Directory | Out-Null

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\HDD0-System.vhdx' `
- ControllerType SCSI

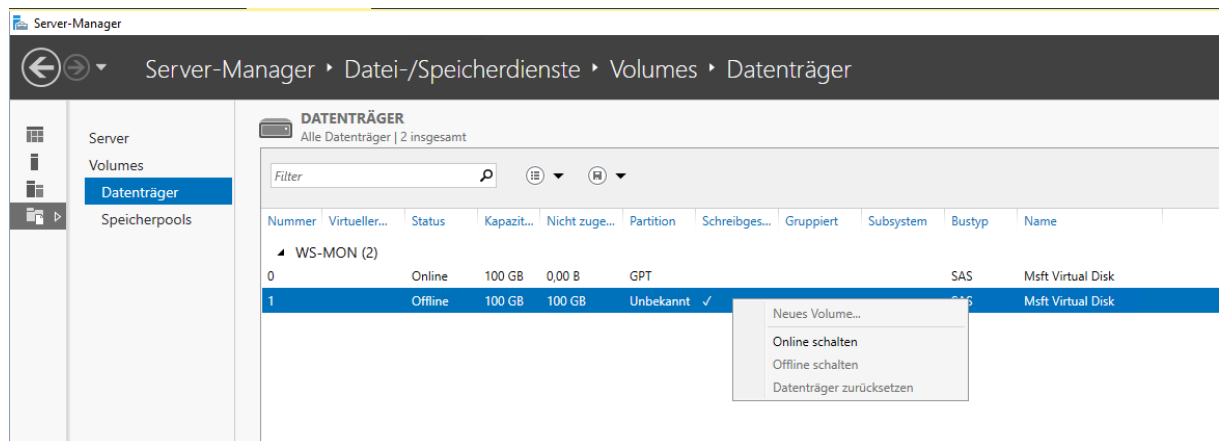
New-VHD -Path 'V:\Hyper-V\WS-MON\Virtual Hard Disks\HDD1-Monitor.vhdx' -Dynamic -SizeBytes 100GB
Add-VMHardDiskDrive -VMName 'WS-MON' -Path 'V:\Hyper-V\WS-MON\Virtual Hard Disks\HDD1-Monitor.vhdx' `
- ControllerType SCSI

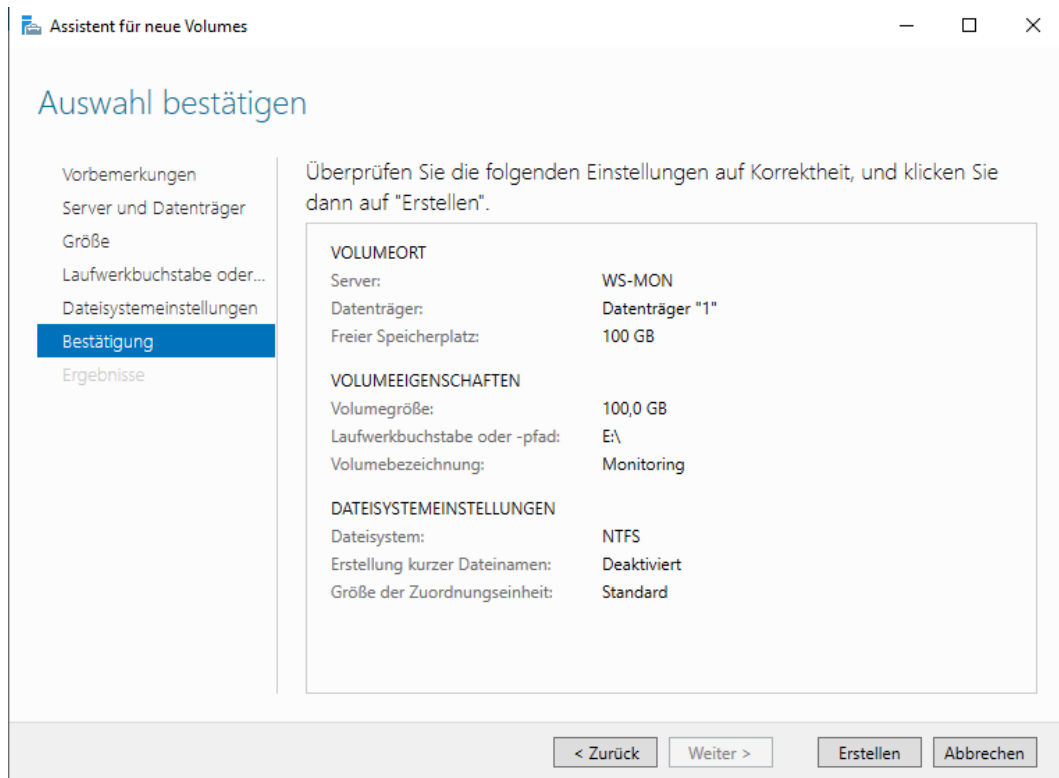
Start-VM -Name 'WS-MON'
```

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:

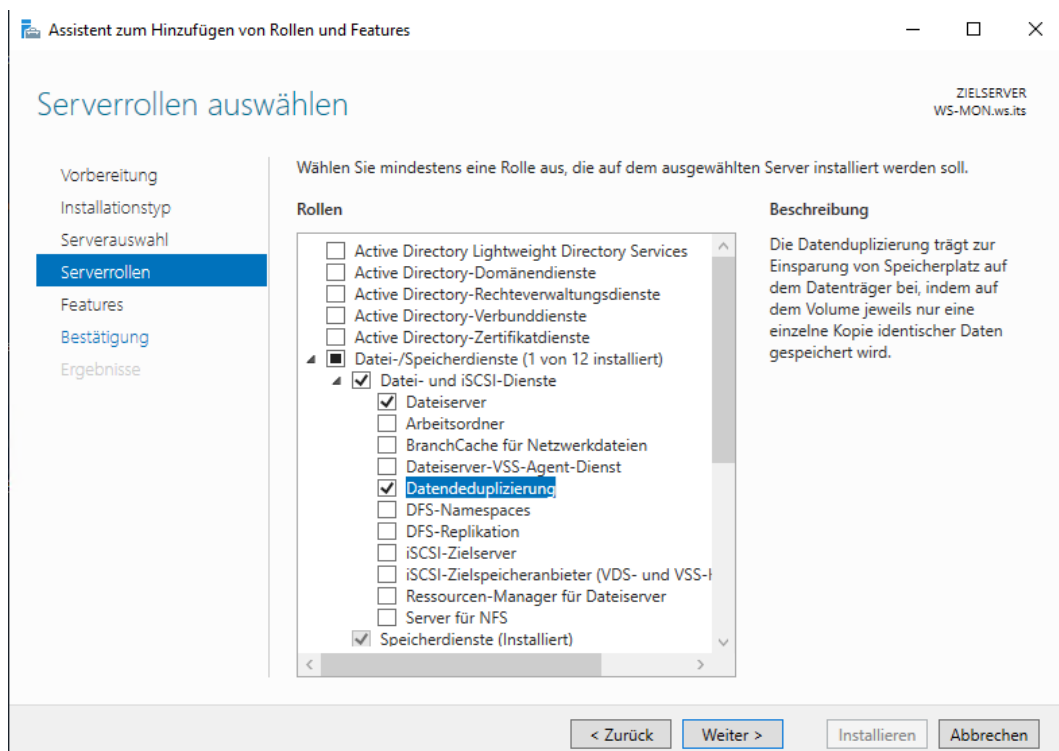


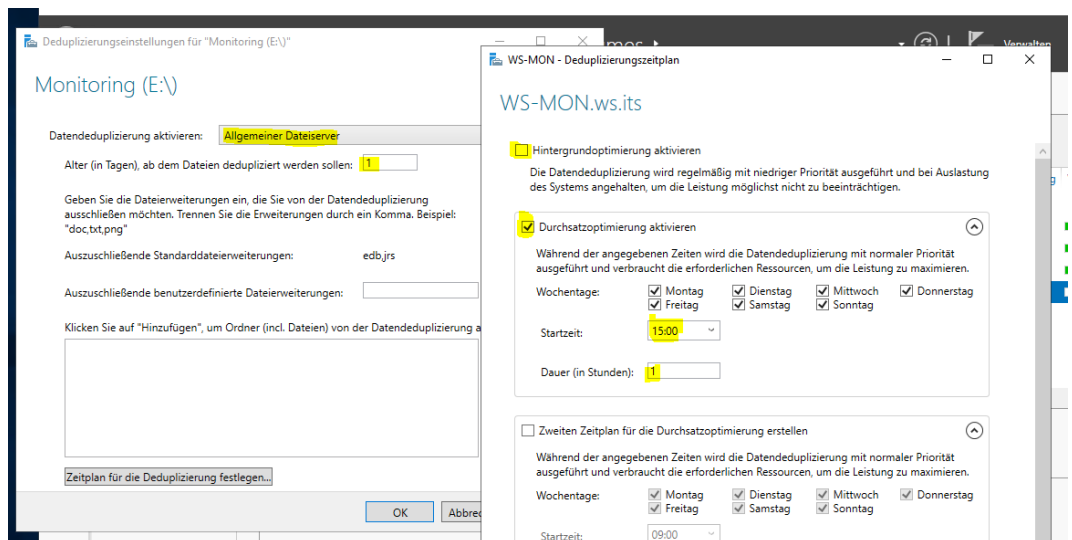
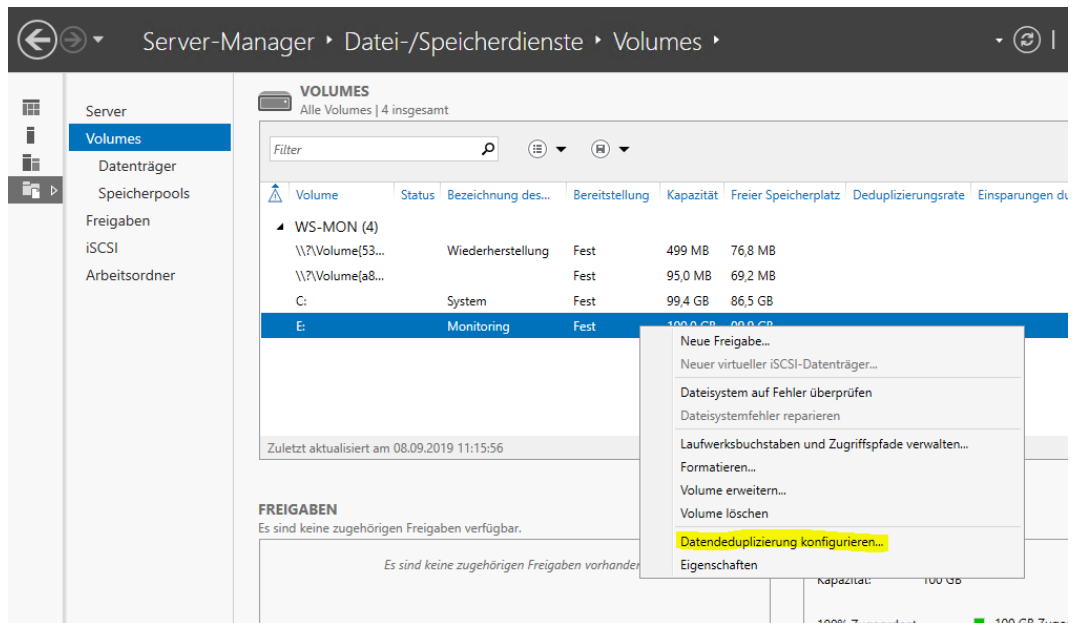
Im alten WS-IPM hatte ich für die SYSLOG-Installation einfach einen Ordner auf Laufwerk c: erstellt. Dieser wurde im Laufe der Zeit immer größer und die Datensicherung der VM dauerte immer länger. Das soll auf dem neuen Server nicht passieren. Daher erstelle ich für die Protokolldateien ein eigenes Volume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



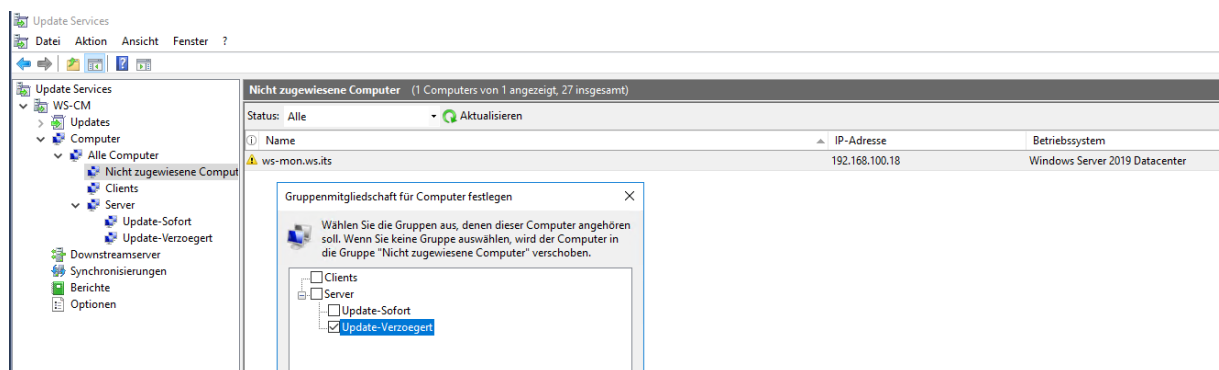


Damit die Logfiles der Monitoring-Partition nicht zu stark anwachsen, konfiguriere ich noch die Datendeduplizierung auf dem neuen Volume. Dazu ist aber auch die Rolle erforderlich:





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



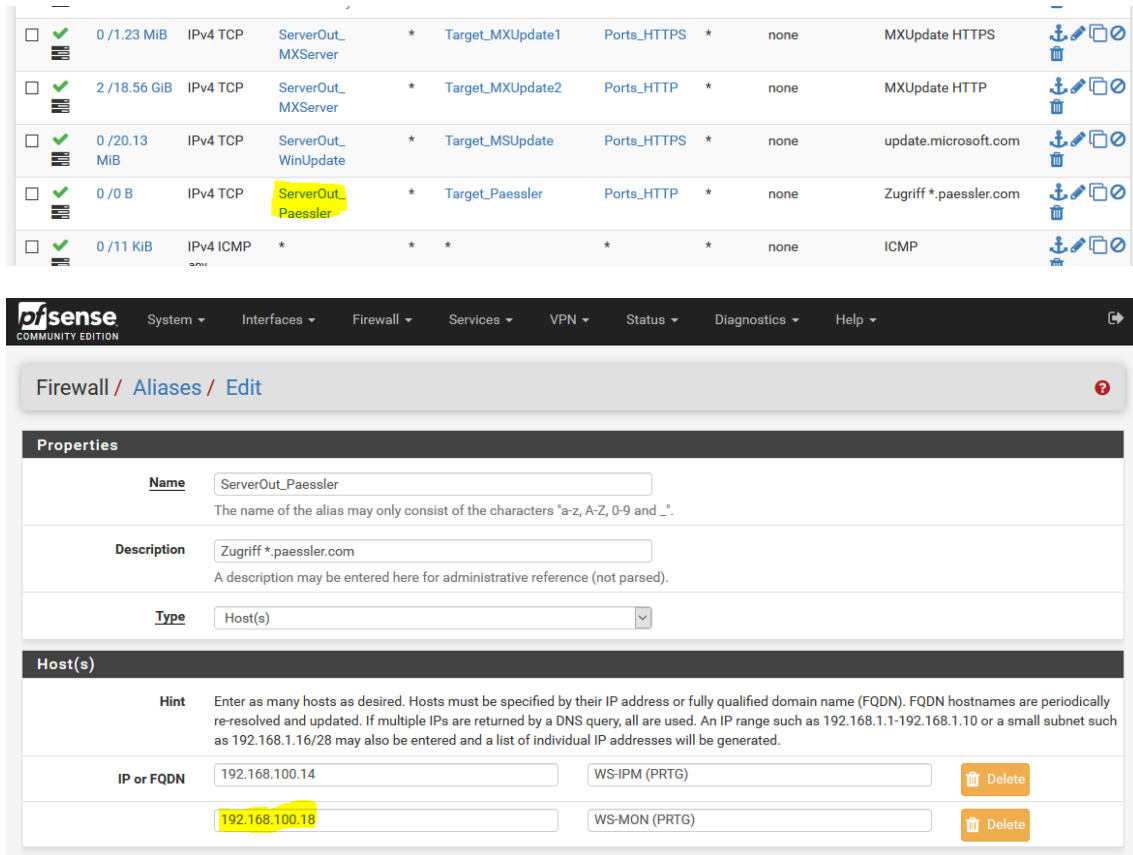
Nach dem Neustart ist das Basissystem einsatzbereit. Das Monitoring und das Backup konfiguriere ich im Schritt Nacharbeiten.

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.

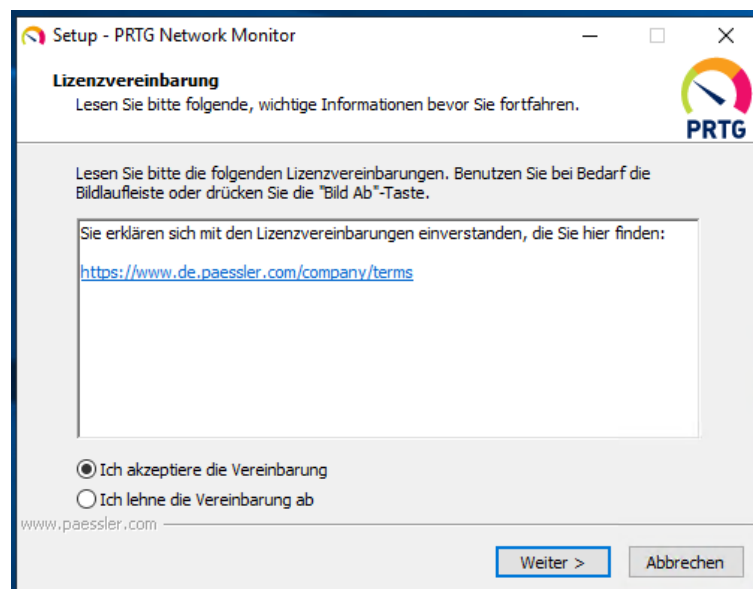
Für die Kommunikation mit den Servern von Paessler ist eine Freischaltung in meiner Firewall (PFSense) erforderlich. Ich nehme die neue IPv4 in die Gruppe auf:



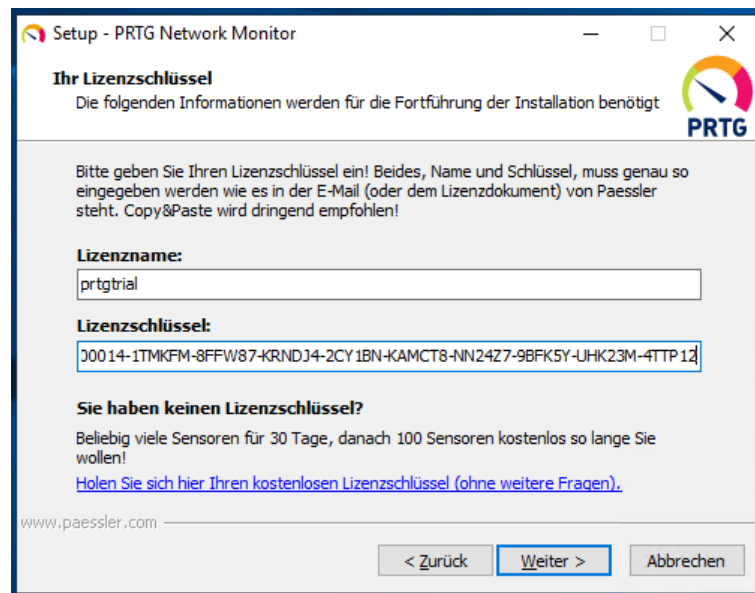
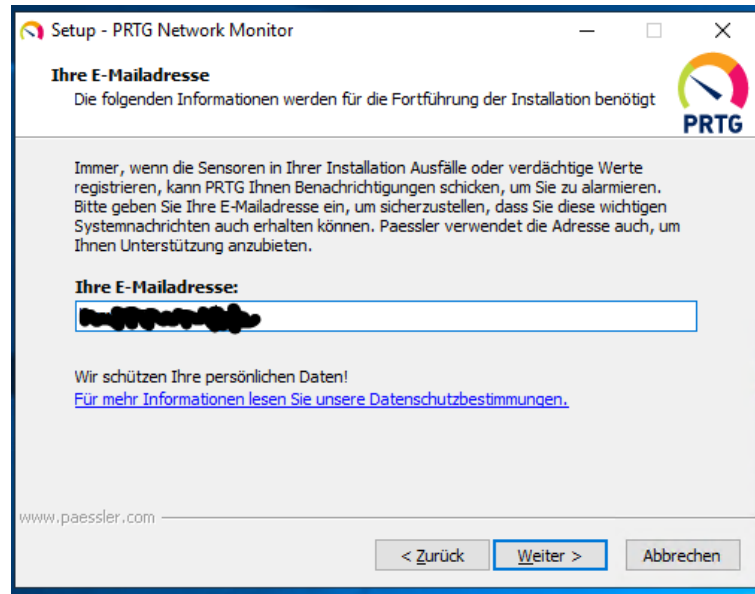
The screenshot shows the PFSense Firewall configuration interface. At the top, a table lists several aliases. The entry for 'ServerOut_Paessler' is highlighted in yellow. Below this, the 'Edit' page for the 'ServerOut_Paessler' alias is shown. The 'Name' field contains 'ServerOut_Paessler' and the 'Description' contains 'Zugriff *.paessler.com'. Under the 'Host(s)' section, two IP addresses are listed: '192.168.100.14' (labeled 'WS-IPM (PRTG)') and '192.168.100.18' (labeled 'WS-MON (PRTG)'). The IP '192.168.100.18' is highlighted in yellow.

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:



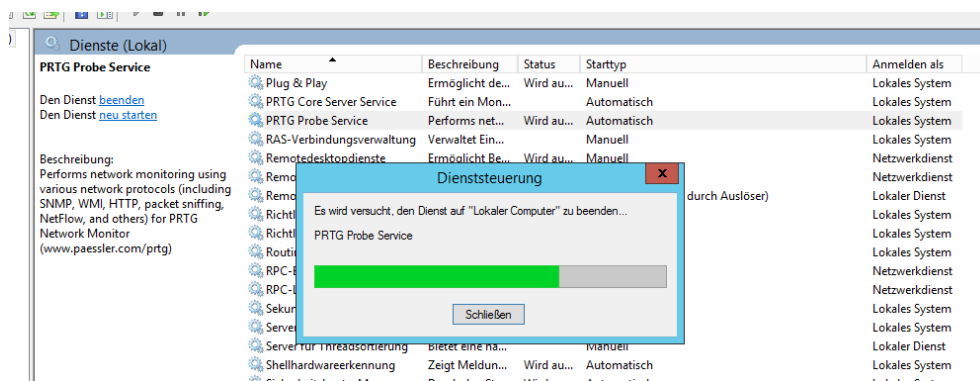
The screenshot shows the 'Setup - PRTG Network Monitor' window. The title bar reads 'Setup - PRTG Network Monitor'. The main content is a license agreement titled 'Lizenzvereinbarung'. It asks the user to read the terms and accept them. A link is provided: <https://www.de.paessler.com/company/terms>. At the bottom, there are two radio buttons: 'Ich akzeptiere die Vereinbarung' (selected) and 'Ich lehne die Vereinbarung ab'. There are also 'Weiter >' and 'Abbrechen' buttons.

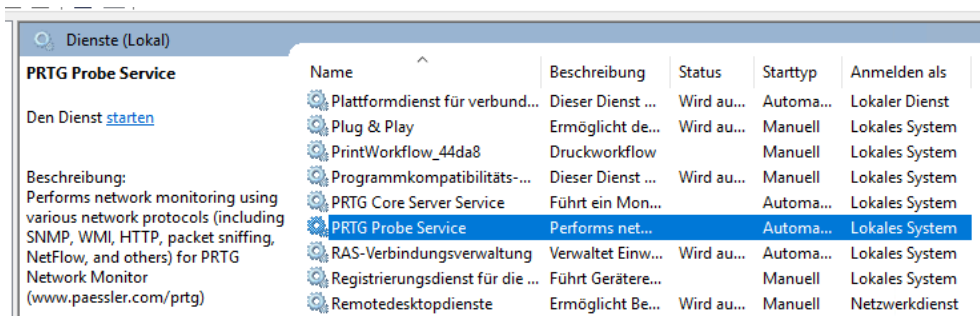


Die Installation läuft fehlerfrei durch.

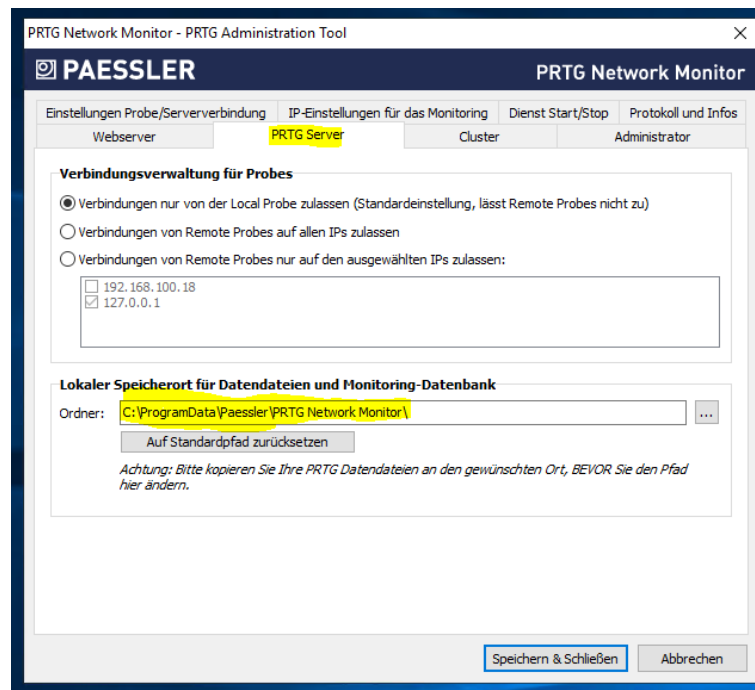
Datenübernahme

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:

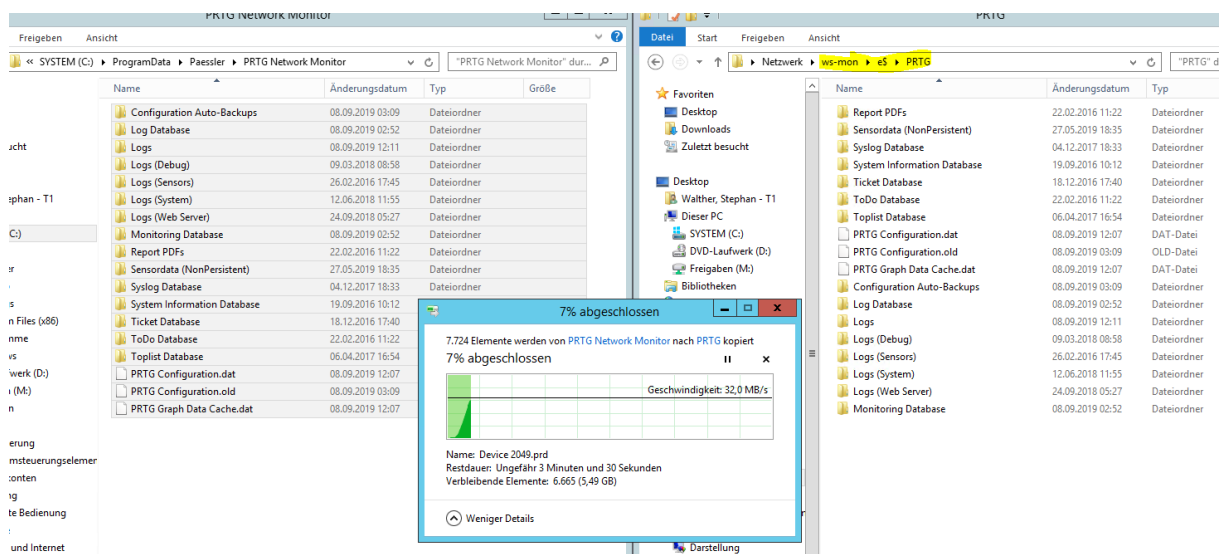




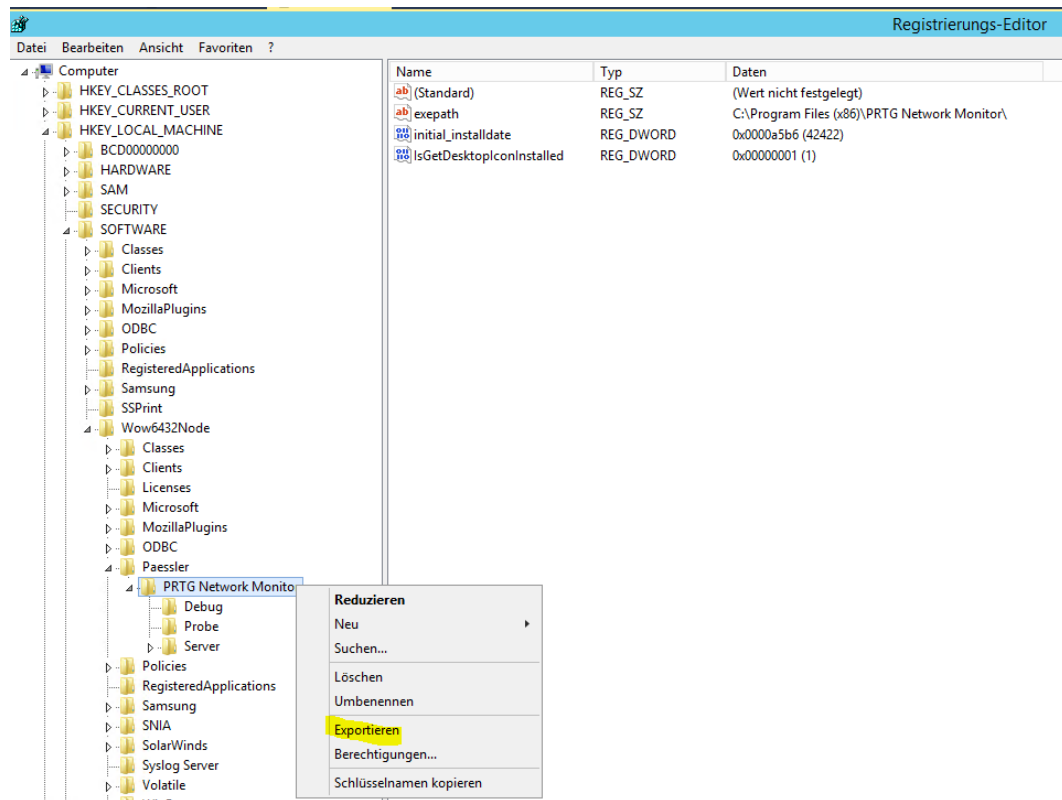
Nun geht es an die Migration der alten Daten. Im Administrations-Tool (das findet man im Startmenü) kann der Datenpfad ausgelesen werden:



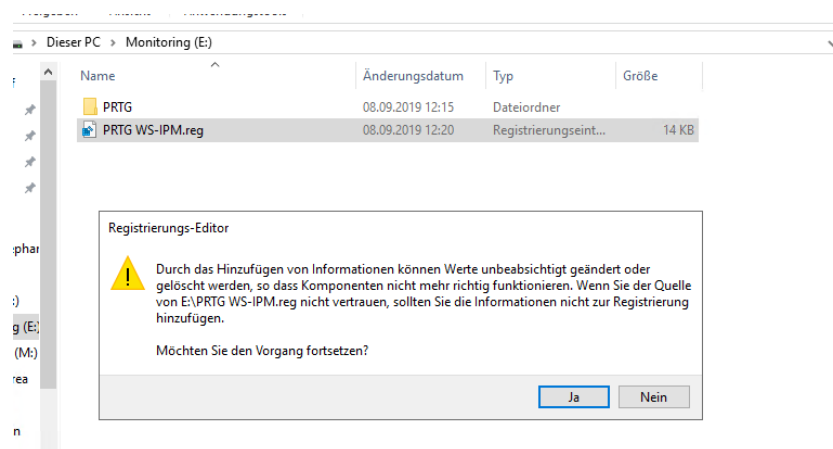
Nun kann ich die Daten einfach kopieren. Ich wähle aber auf dem Zielsystem WS-MON einen neuen Pfad unter Laufwerk E:



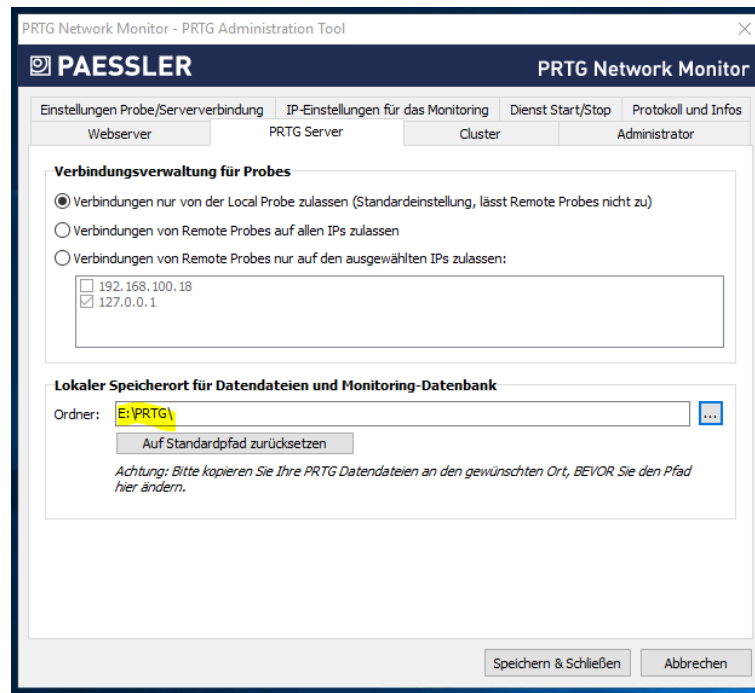
Teile der Konfiguration scheinen in der Registry zu liegen („Step 5: Export Settings of the Old Server and Local Probe from the Windows Registry to a File“). Also exportiere ich diese in eine reg-Datei:



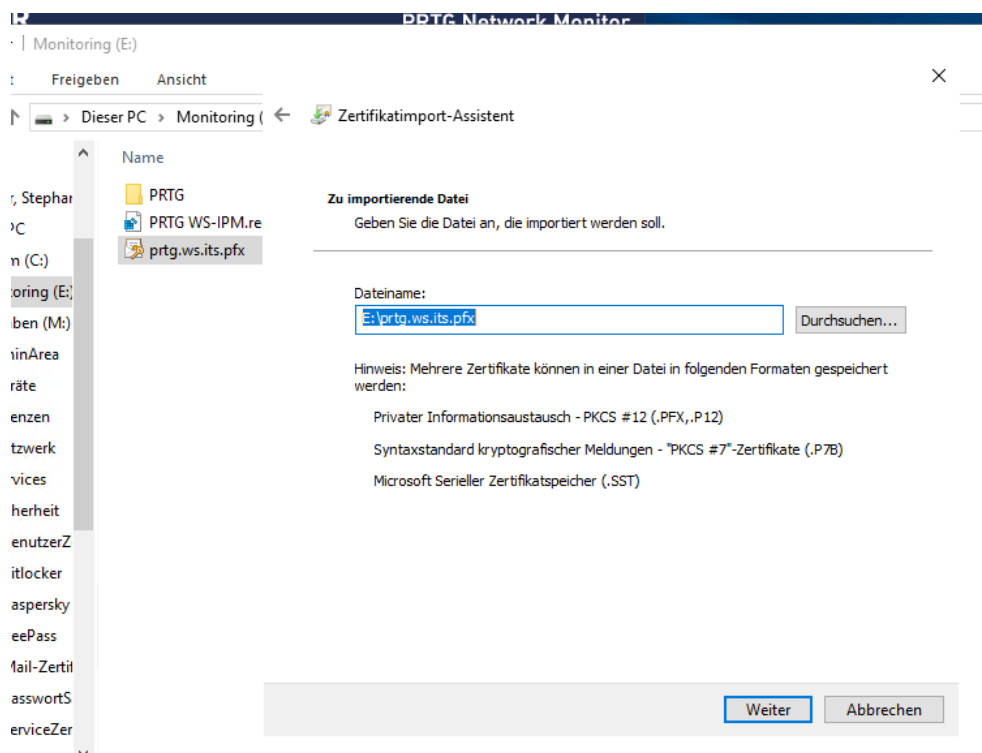
Auf dem neuen Server erstelle ich auf die gleiche Weise noch ein Backup. Danach importiere ich die Einstellungen aus der Exportdatei des alten Servers:



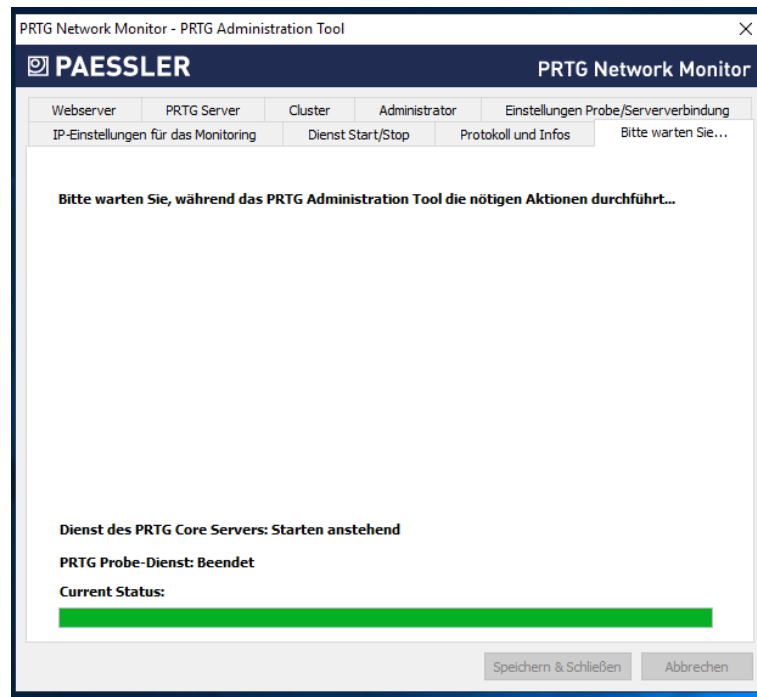
Nun starte ich das PRTG-Administrationstool aus dem Startmenü und kontrolliere die Einstellungen. Der alte Server lief mit HTTPS. Das wurde jetzt übernommen. Aber der Datenpfad ist noch auf c: gerichtet. Das muss ich anpassen:



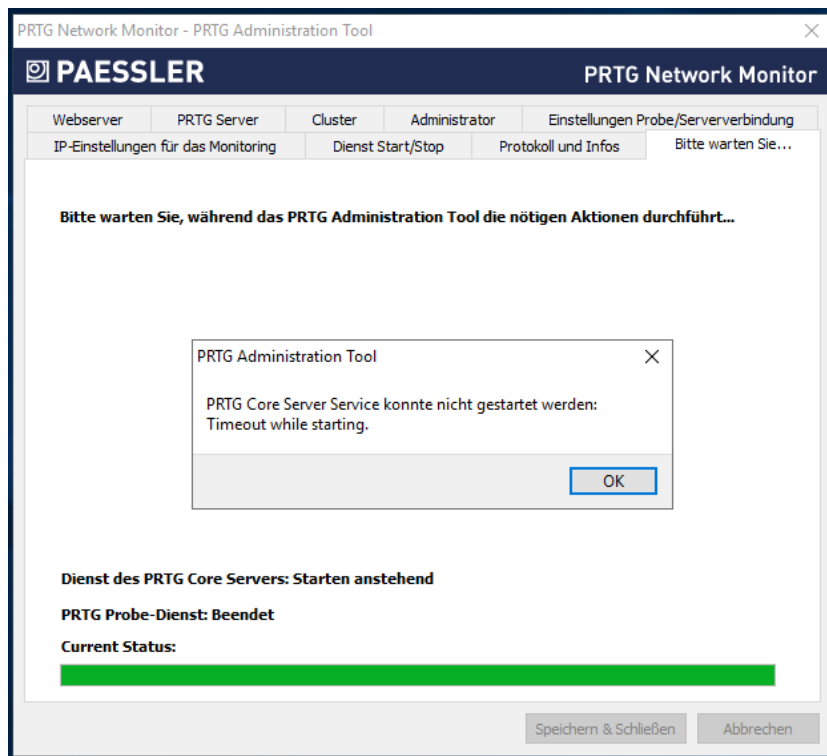
Vor dem Start exportiere ich noch das Zertifikat auf dem alten Server, da dieses bis 2020 gültig ist. Dieses installiere ich auf dem neuen Server:



Nun starte ich die Services. Das dauert einige Minuten:



Leider kommt diese Fehlermeldung:



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:

name	typ	daten	zeitstempel
WS-WAC	Host (A)	192.168.100.22	07.09.2019 14:00:00
ata	Host (A)	192.168.100.23	Static
WS-ATA	Host (A)	192.168.100.23	08.09.2019 03:00:00
WS-EdgeNet1	Host (A)	192.168.100.249	Static
WS-PFS1a	Host (A)	192.168.100.250	Static
WS-PFS1b	Host (A)	192.168.100.251	Static
WS-PFS1	Host (A)	192.168.100.252	Static
WS-CoreNet1			
WS-AP1			
email			
WS-MX1			
WS-CM			
WS-HV3			
WS-DPM			
Drucker-1			
WS-CA1			
WS-RA1			
WS-NAS1			
WS-HV1			
(identisch mit übergeordne...			
WS-DC3			
WS-RDS3			
WS-PFS2			
WS-Corenet2			
WS-CL1			
WS-CL7			
WS-RDS2			
WS-PFS1			
WS-CL3			
WS-PFS2			
Drucker-2			
(identisch mit übergeordne...	Autoritätsursprung (SOA)	[32447], ws-dc1.ws.its, ho...	Static
autodiscover	Alias (CNAME)	email.ws.its	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc1.ws.its	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc2.ws.its	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc3.ws.its	Static
prtg	Alias (CNAME)	ws-ipm.ws.its	Static
crl	Alias (CNAME)	ws-ra1.ws.its	Static

Eigenschaften von prtg

Alias (CNAME) Sicherheit

Aliasname (bei Nichtangabe wird übergeordnete Domäne verwendet):

Vollqualifizierter Domänenname:

Vollqualifizierter Domänenname des Zielhosts:

Eintrag löschen, sobald er verfällt

Zeitstempel des Eintrags:

Gültigkeitsdauer (TTL): : : : (TTTTT:HH.MM.SS)

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:

```

Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Users\stephan> Clear-DnsClientCache
PS C:\Users\stephan> ping prtg

Ping wird ausgeführt für ws-mon.ws.its [192.168.100.18] mit 32 Bytes Daten:

```

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):

The screenshot shows the 'Firewall / Aliases / Edit' page in Pfsense. The 'Name' field is 'ServerIn_HTTPS' and the 'Description' is 'Services mit HTTPS'. The 'Type' is set to 'Host(s)'. Under the 'Host(s)' section, there is a table of IP addresses and their corresponding aliases:

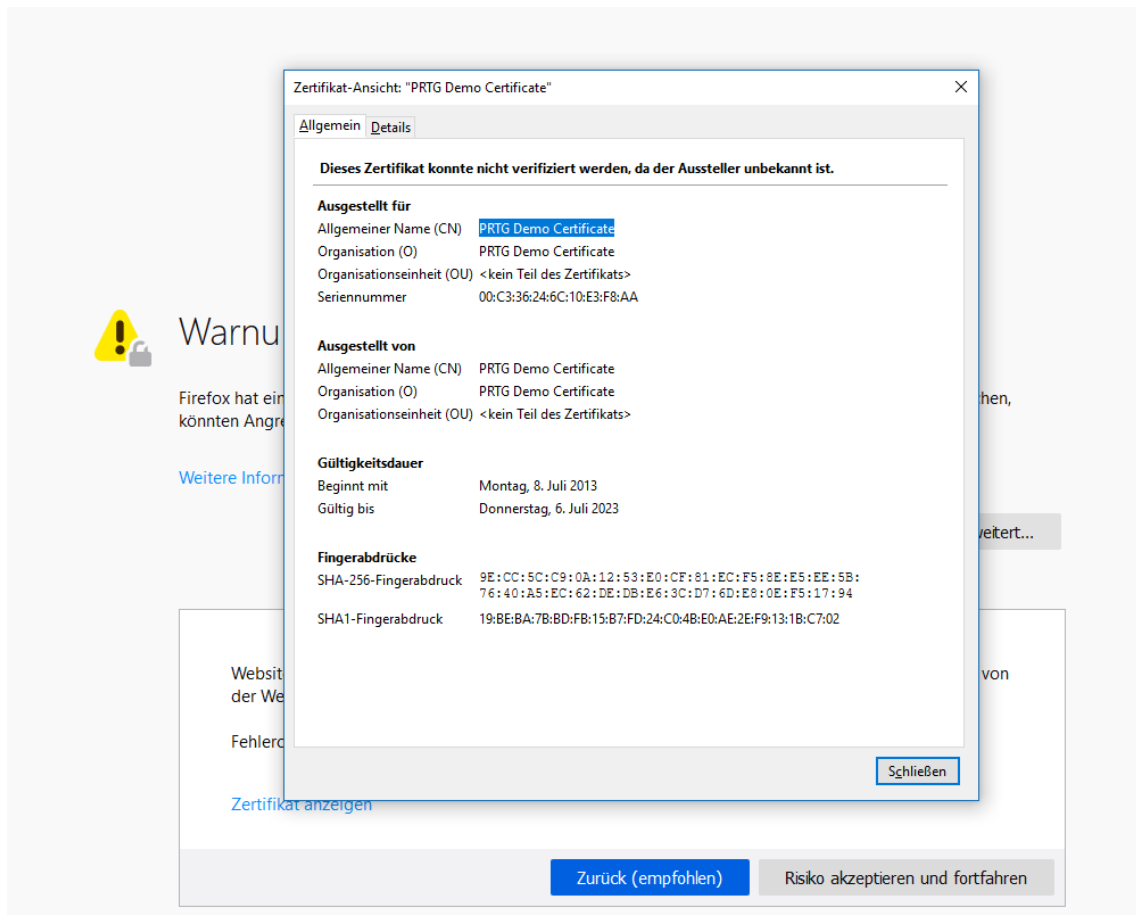
IP or FQDN	Alias	Action
192.168.100.18	WS-MON (PRTG)	Delete
192.168.100.7	WS-RA1 (WAP)	Delete
192.168.100.17	WS-RA2 (WAP)	Delete
192.168.100.6	WS-CA1 (PKI+CES)	Delete

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

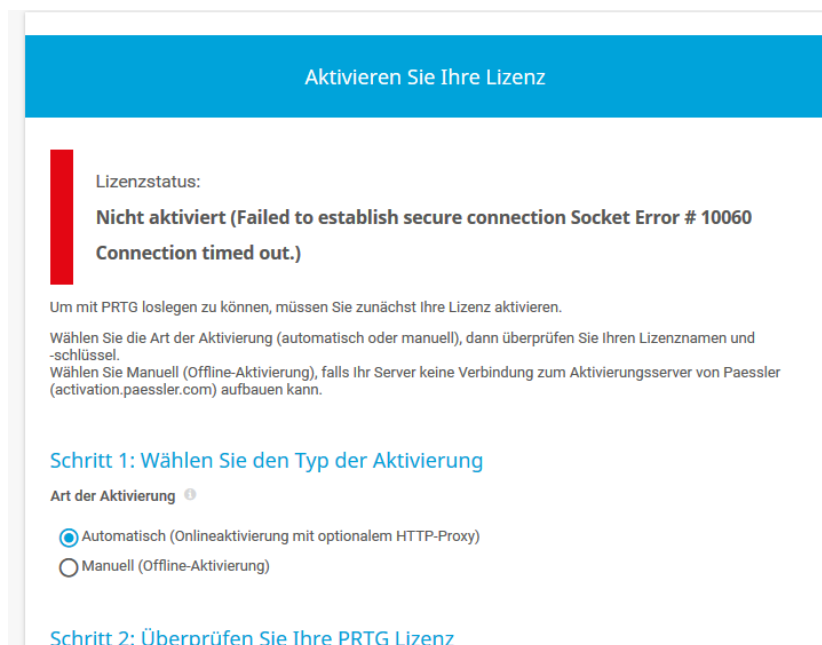
The screenshot shows the 'Firewall / Aliases / Edit' page in Pfsense. The 'Name' field is 'ServerOut_TCP25' and the 'Description' is 'Server mit SMTP'. The 'Type' is set to 'Host(s)'. Under the 'Host(s)' section, there is a table of IP addresses and their corresponding aliases:

IP or FQDN	Alias	Action
192.168.100.3	WS-MX1	Delete
192.168.100.13	WS-MX2	Delete
192.168.100.18	WS-MON (PRTG SMTP-Probes)	Delete

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



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:

✓ Status
Protokoll

Lizenzierung

Lizenzstatus	Activation was successful
Lizenzname	prtgtrial
Lizenzschlüssel	000014-1TMKFM-8FFW87-KRNDJ4-2CY1BN-KAMCT8-NN24Z7-9BFBK5Y-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

Lizenzschlüssel ändern
Informationen aktualisieren

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

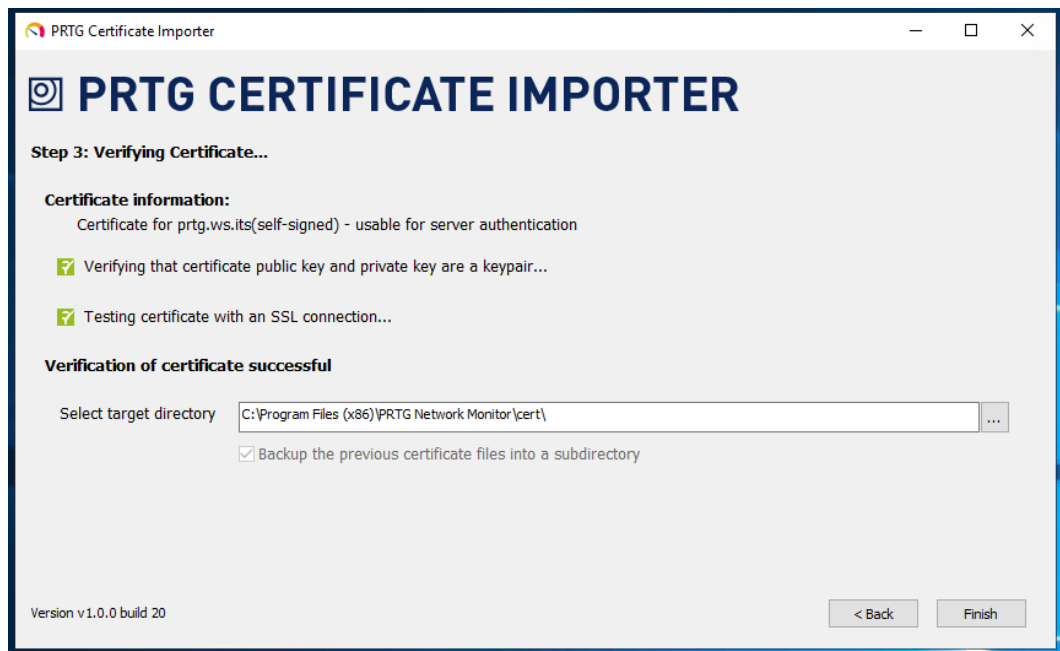
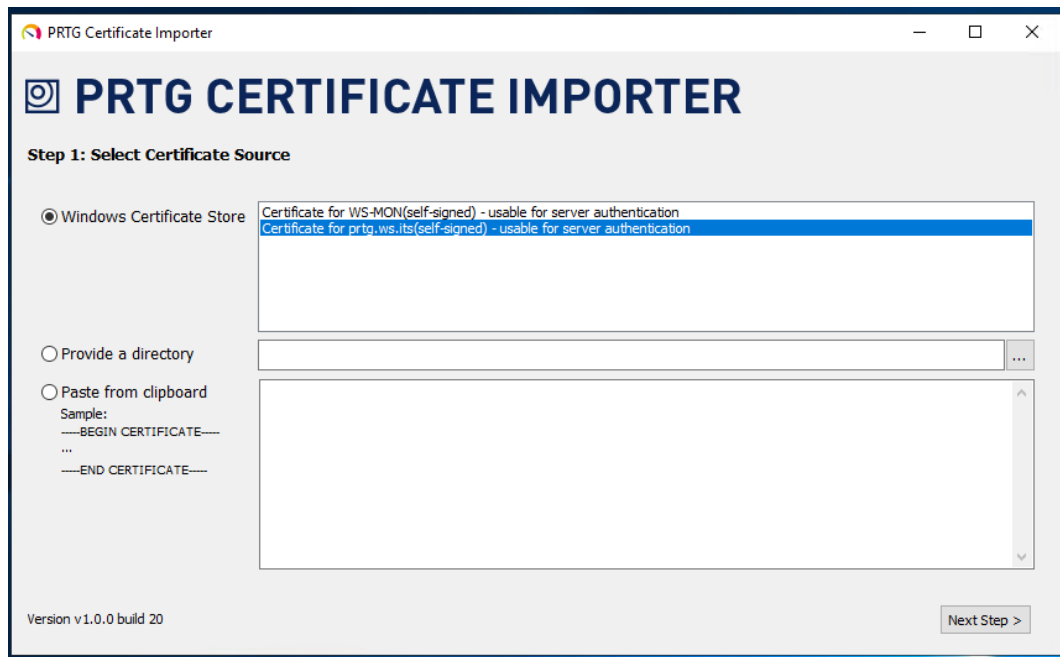
Es wird Zeit für das richtige Zertifikat. Im Webportal wird der Hinweis dazu gezeigt:

Standardsicherheit (TLS 1.0, TLS 1.1, TLS 1.2) (empfohlen)
 Schwächere Sicherheit (SSL V3, TLS 1.0, TLS 1.1, TLS 1.2)

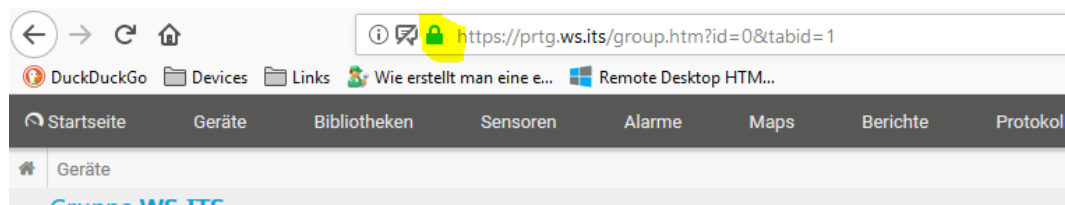
Importieren Sie Ihr eigenes Zertifikat
 Tipp: Sie können Ihr eigenes vertrauenswürdigen SSL-Zertifikat für PRTG installieren, um Warnungen des Webbrowsers zu vermeiden, wenn Sie sich mit dem PRTG Web-Interface verbinden. Um den Import des Zertifikats zu vereinfachen, empfehlen wir Ihnen den Einsatz des [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

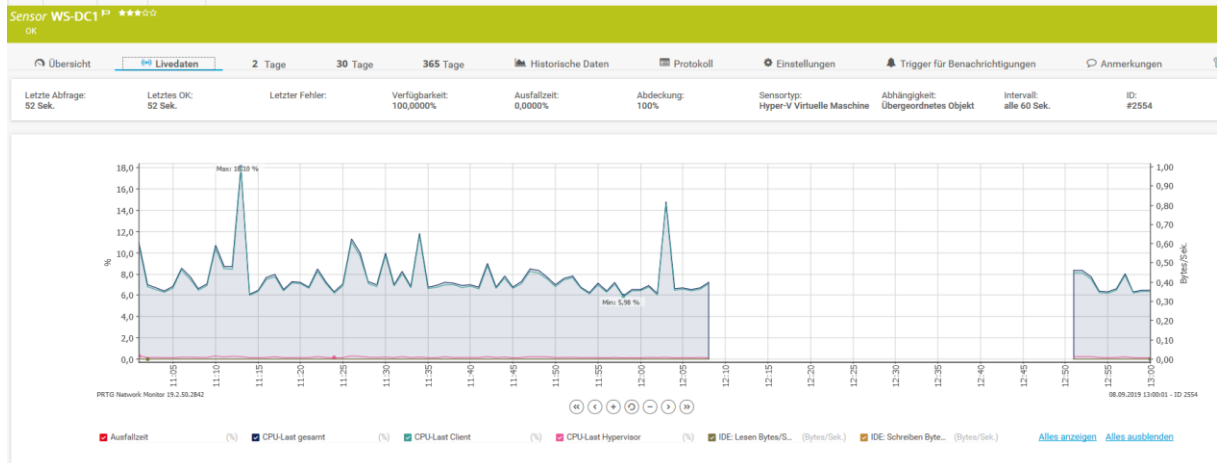
Ich lade das Tool herunter und starte es auf dem neuen Server. Mein zuvor manuell importiertes Zertifikat wird schon angezeigt:



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



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:

The screenshot shows the configuration for a PRTG sensor named 'WS-AP1'. The sensor is currently in a red state. The configuration includes: 'HTTPS' (147 ms), 'Zertifikat' (146 #), 'SSL-Sicherheit...' (Only Strong Prot...), and 'Sensor hinzufügen'. Below this, there are several other sensors: 'Synology Systeme...' (48 °C), '(002) eth0 Traf...' (2,65 kbit/Sek.), 'Disk Free: /vol...' (22%), 'Physical Disk: ...' (34 °C), and 'Physical Disk: ...' (37 °C). The 'WS-AP1' sensor has 'HTTPS' (58 ms) and 'LAN' (red status) listed. A 'Sensor hinzufügen' button is visible next to the LAN sensor.

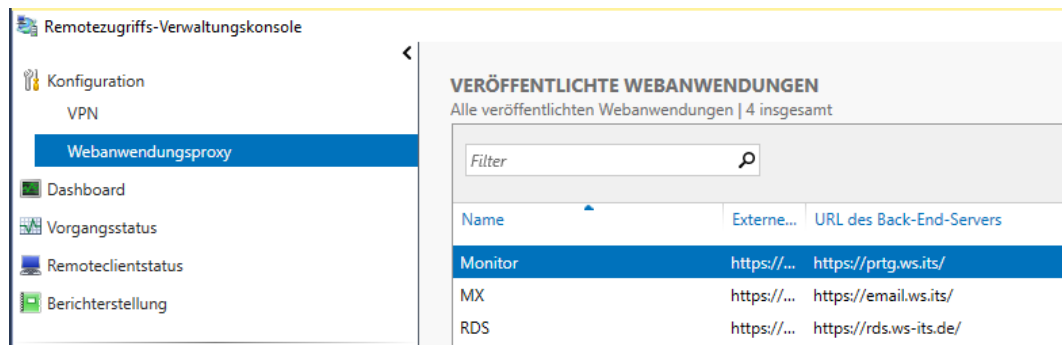
Die Ursache ist schnell gefunden: der Sensor verwendet SNMP. Und dafür muss auf dem Zielsystem eine Probe-IP eingetragen sein:

The screenshot shows the TP-Link web interface for an Access Point. The 'Management' tab is selected. Under the 'SNMP Agent' section, the 'Enable' checkbox is checked. The configuration fields are: 'SysContact:', 'SysName:', 'SysLocation:', 'Get Community: public', 'Get Source: 0.0.0.0', 'Set Community: [redacted]', and 'Set Source: 192.168.100.14'.

Eine Anpassung später wird der Sensor grün:

The screenshot shows the configuration for the 'WS-AP1' sensor after adjustment. The 'LAN' sensor now shows a green status and a value of 11 kbit/Sek. The other sensors remain the same as in the previous screenshot.

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:

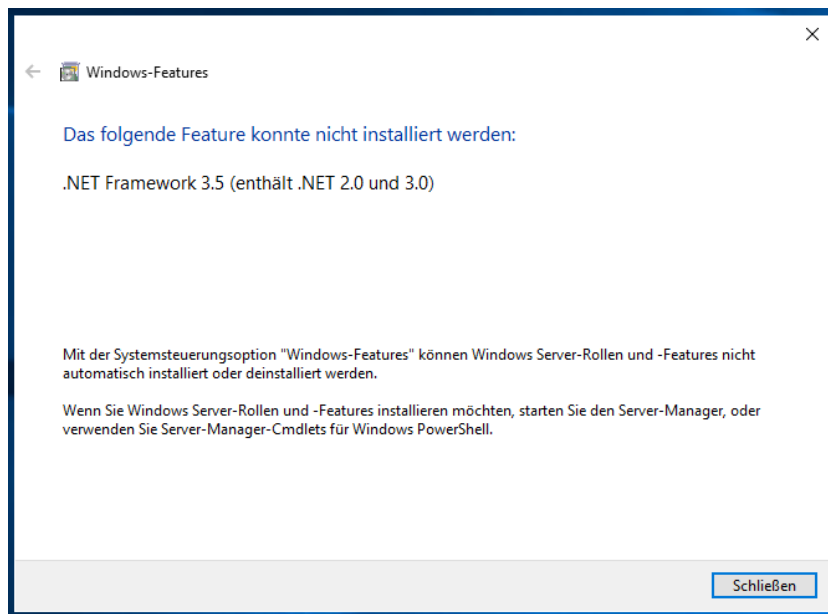


PRTG sollte damit erfolgreich umgezogen sein. Auf zum nächsten Service.

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:

```
1 Get-WindowsFeature *frame*
```

```
PS C:\Windows\system32> Get-WindowsFeature *frame*
```

Display Name	Name	Install State
[] .NET Framework 3.5-Funktionen	NET-Framework-Features	Available
[] .NET Framework 3.5 (enthält .NET 2.0 und 3.0)	NET-Framework-Core	Removed
[X] .NET Framework 4.7-Funktionen	NET-Framework-45-Fea...	Installed
[X] .NET Framework 4.7	NET-Framework-45-Core	Installed
[] ASP.NET 4.7	NET-Framework-45-ASPNET	Available
[] Windows-Biometrieframework	Biometric-Framework	Available

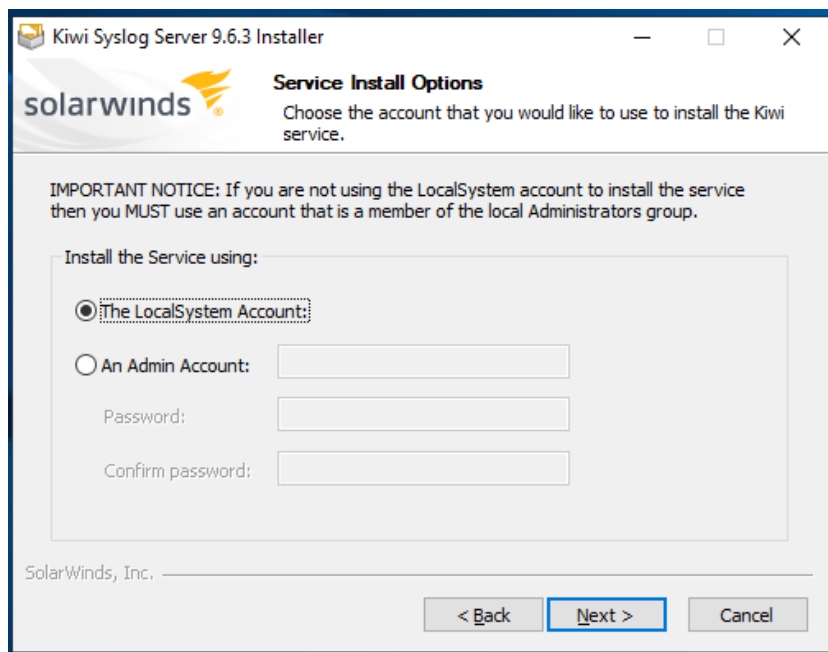
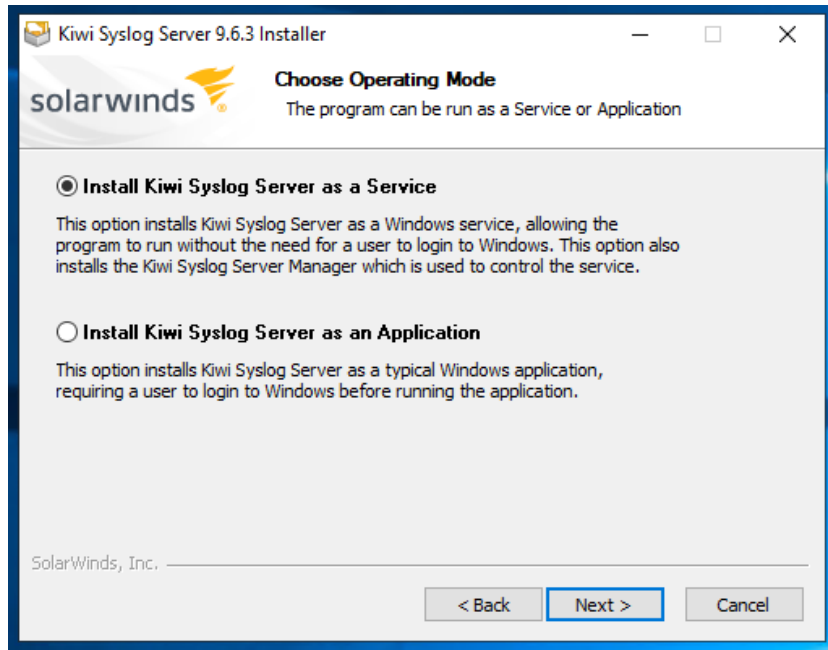
```

2
3 Add-WindowsFeature -Name NET-Framework-Core -Source d:\sources\sxs

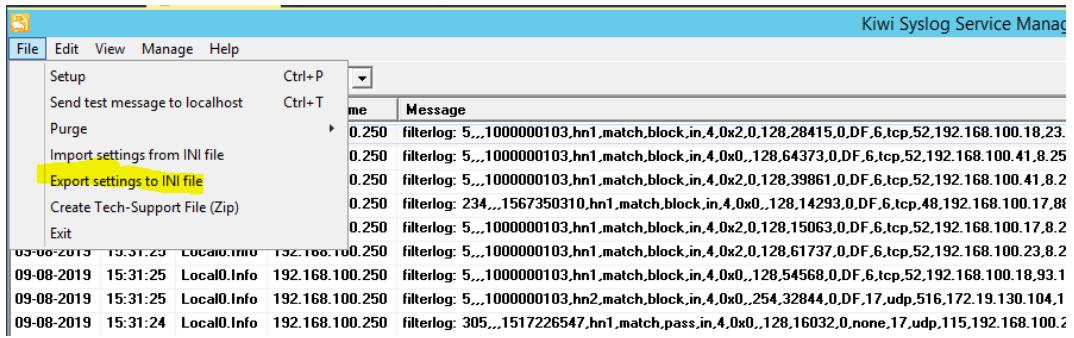
```

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{.NET Framework 3.5 (enthält .NET 2.0 und ...

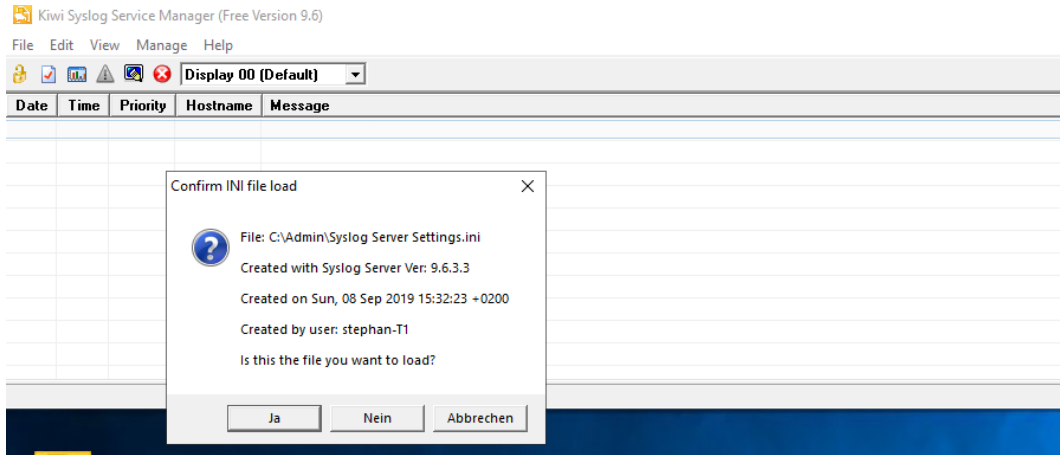
Nun lässt sich das Setup starten:



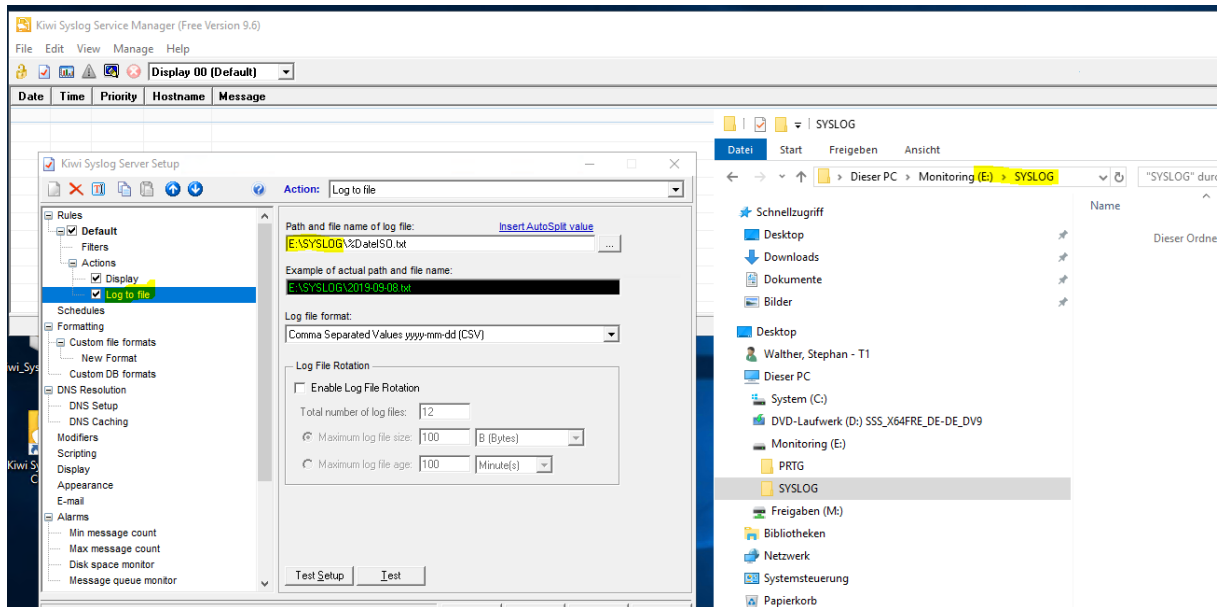
Ich benötige die Konfiguration. Diese kann in der alten Konsole exportiert und in der neuen importiert werden:



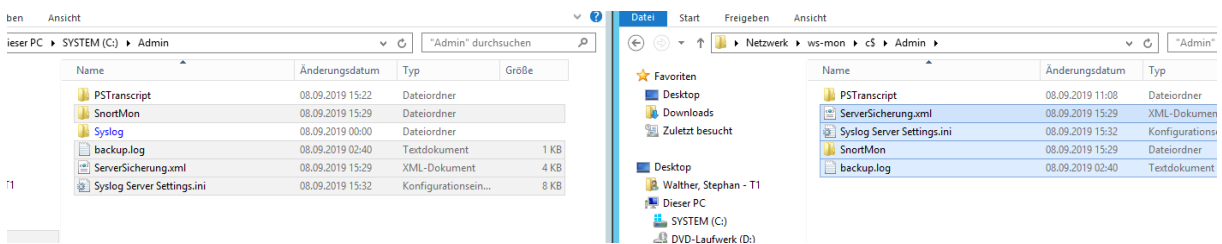
Auf dem neuen Server geht es ebenso einfach:



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



Alle dazugehörigen Dateien kopiere ich auf den neuen Server:



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

The screenshot shows the pfSense web interface, specifically the 'Settings' page under 'System Logs'. The 'Remote Logging Options' section is expanded, showing the following configuration:

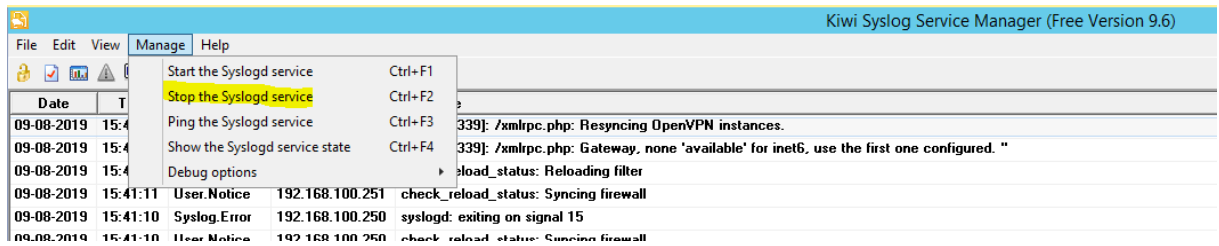
- General Logging Options:**
 - Forward/Reverse Display: Show log entries in reverse order (newest entries on top)
 - GUI Log Entries: 50
 - Log file size (Bytes): Bytes
- Remote Logging Options:**
 - Enable Remote Logging: Send log messages to remote syslog server
 - Source Address: LAN_100_SERVER
 - IP Protocol: IPv4
 - Remote log servers: 192.168.100.18:514
 - Remote Syslog Contents:
 - Everything
 - System Events
 - Firewall Events
 - DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdnsm)
 - DHCP Events (DHCP Server, DHCP Relay, DHCP Client)

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:

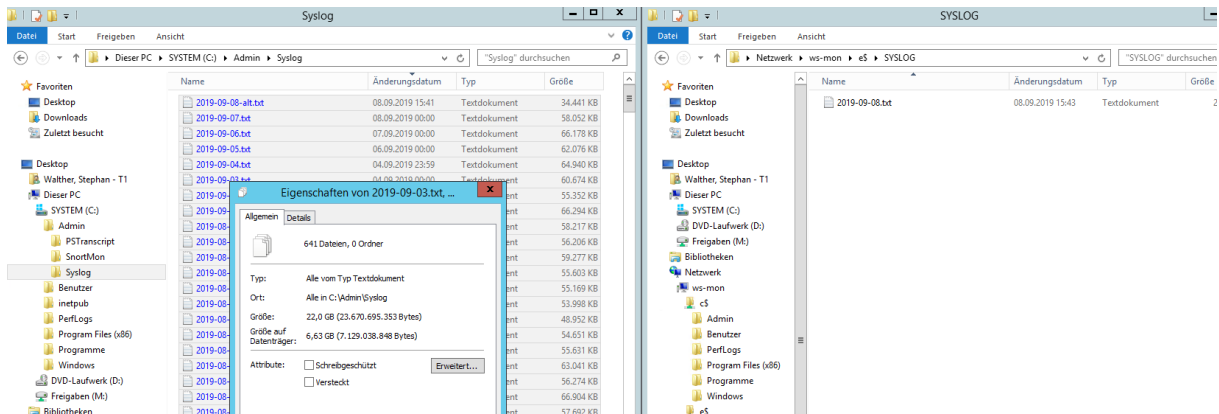
The screenshot shows the Kiwi Syslog Service Manager (Free Version 9.6) interface. The main window displays a list of log entries with columns for Date, Time, Priority, Hostname, and Message. The messages are filtered log entries from the firewall. Below the log list, a file explorer window is open, showing the directory path 'Dieser PC > Monitoring (E) > SYSLOG'. A file named '2019-09-08.txt' is visible in the file list.

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,52,192.168.100.41,93.184.220.29,65027,80,0,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,S,
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,;
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,52,192.168.110.101,192.168.100.18,3701,443,0,
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,59,192.168.110.101,192.168.100.1,58705,53
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,52,192.168.100.18,192.168.101.2,55950,49666
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,52,192.168.100.18,192.168.101.2,55949,49666
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,52,192.168.110.101,192.168.100.18,3698,443,0,
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,52,192.168.110.101,192.168.100.18,3697,443,0,
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,52,192.168.110.101,192.168.100.18,3696,443,0,
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,52,192.168.110.101,192.168.100.18,3695,443,0,
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,52,192.168.110.101,192.168.100.18,3694,443,0,
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,516,172.19.130.104,139.7.117.161,40264,500,4,
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,52,192.168.100.41,93.184.220.29,65027,80,0,SE
09-08-2019	15:41:17	Local0.Info	192.168.100.250	filterlog: 5,,,1000000103,hn2.match.block.in.4.0x0.,254,32979,0,DF,17,udp,516,172.19.130.104,139.7.117.161,40264,500,4,
09-08-2019	15:41:17	Local0.Info	192.168.100.250	filterlog: 5,,,1000000103,hn3.match.block.in.4.0x0.,128,25352,0,DF,6,tcp,52,192.168.110.101,192.168.100.18,3697,443,0,
09-08-2019	15:41:17	Local0.Info	192.168.100.250	filterlog: 5,,,1000000103,hn3.match.block.in.4.0x0.,128,25328,0,DF,6,tcp,52,192.168.110.101,192.168.100.18,3696,443,0,
09-08-2019	15:41:17	Local0.Info	192.168.100.250	filterlog: 5,,,1000000103,hn3.match.pass.in.4.0x0.,128,25324,0,DF,6,tcp,52,192.168.110.101,192.168.100.18,3695,443,0,
09-08-2019	15:41:17	Local0.Info	192.168.100.250	filterlog: 5,,,1000000103,hn3.match.pass.in.4.0x0.,128,25321,0,DF,6,tcp,52,192.168.110.101,192.168.100.18,3694,443,0,

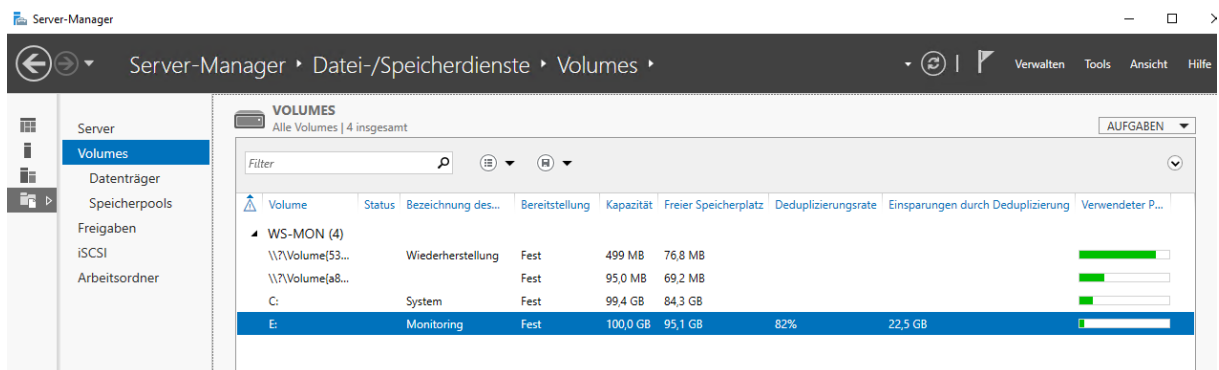
Auf dem alten Server kommen nun keine Datenpakete mehr an. Für die Datenmigration der bereits gesammelten Logfiles beende ich den alten SYSLOG-Service:



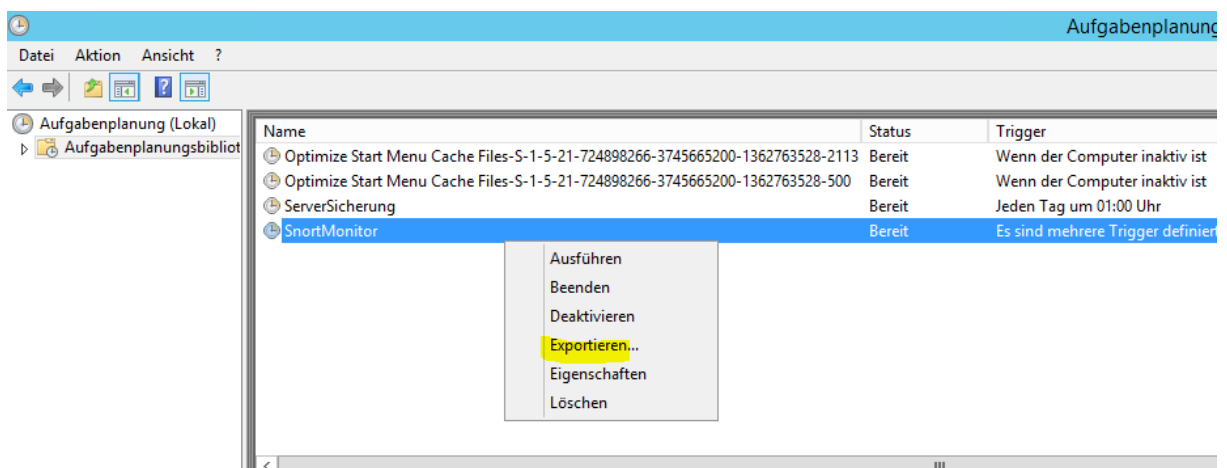
Als nächstes kopiere ich alle bisherigen Logfiles auf den neuen Server. Auf dem alten hatte ich nur die NTFS-Kompression zum Platzsparen aktiv. Auf dem Neuen wird das die Data-Deduplication übernehmen:



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



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:

Name	Status	Trigger	Nächste L
npcapwatchdog	Bereit	Beim Systemstart	
ServerSicherung	Bereit	Jeden Tag um 01:00 Uhr	09.09.2019
SnortMonitor	Wird ausgeführt	Es sind mehrere Trigger definiert.	09.09.2019
User_Feed_Synchronisation-{A6AB5720-6308-4662-916F-8AAF6CFCB9E1}	Bereit	Jeden Tag um 02:01 Uhr - Trigger läuft um 10.08.2029 02:01:17 ab.	09.09.2019

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:

```

4 # Version:      V1.03
5 # Programmierer: Stephan Walther
6 #####
7
8 # Variablen
9 $ScriptDir     = 'C:\Admin\SnortMon'
10 $ScriptVersion = "v1.03"
11 $MailAn        = 'logmails@ws-its.de'
12 $MailVon       = 'service-mailing@ws-its.de'
13 $MailServer    = 'email.ws.its'
14 $MailAktiv     = $true
15 $MailInterval  = 5
16
17 $LogFolder     = 'E:\SYSLOG'
18 $AlertsToIgnore = @('120:8:2', '119:4:1', '120:3:1')
19 $Interval      = 300
20
21 Get-Variable -Scope global | Where-Object {$_.name -eq 'ProcessedLinesCounter'} | Remove-Variable -Scope
22

```

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

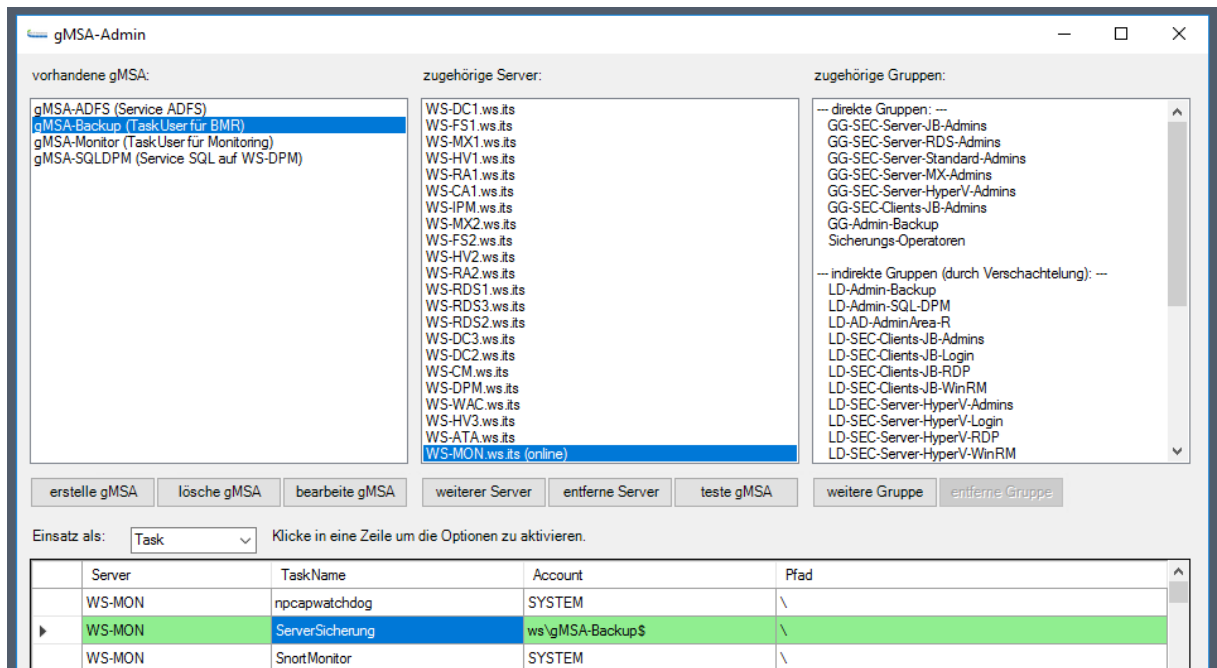
offen

Diese Nachricht wurde mit der Priorität "Hoch" gesendet.

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, 10062							

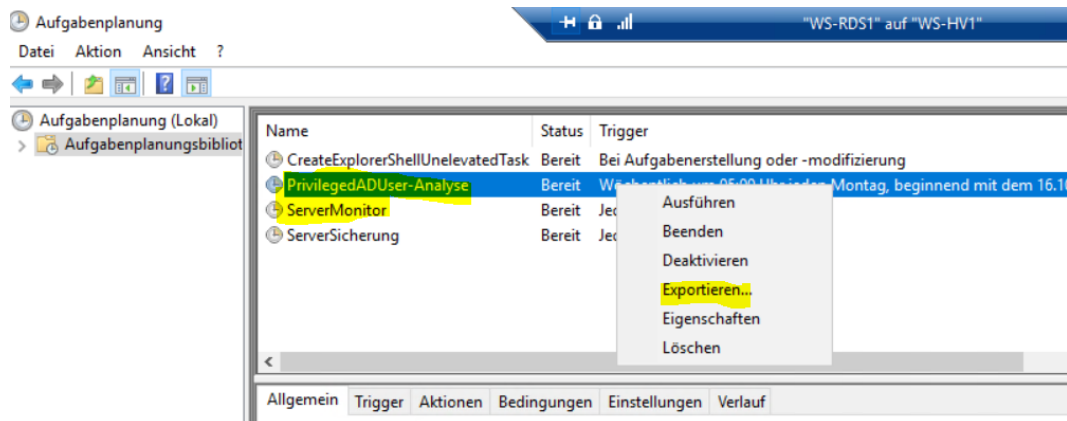
Weil ich gerade an den Aufgaben dran bin importiere ich auch die Aufgabe für meine Systemstate-Datensicherung. Mit dieser kann ich das System via BareMetalRecovery zuverlässig wiederherstellen. Das Script für die Sicherung muss unter einem gMSA-Account laufen. Diesen kann ich von meinem DomainController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



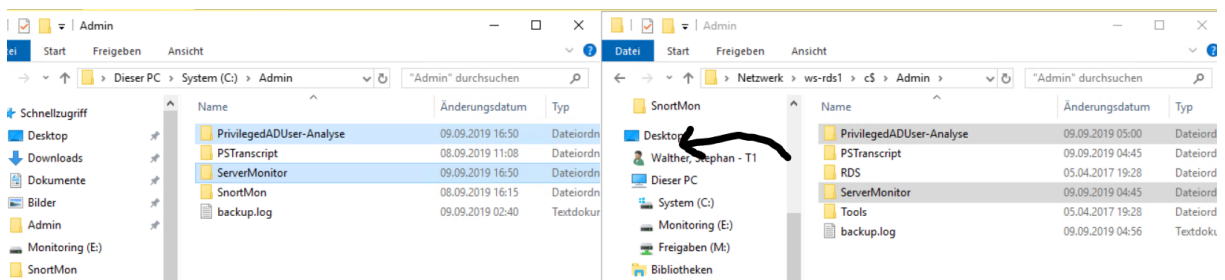
Damit sind alle Funktionen außer IPAM auf den neuen Server übertragen.

Migration der Monitoring-Scripte von WS-RDS1

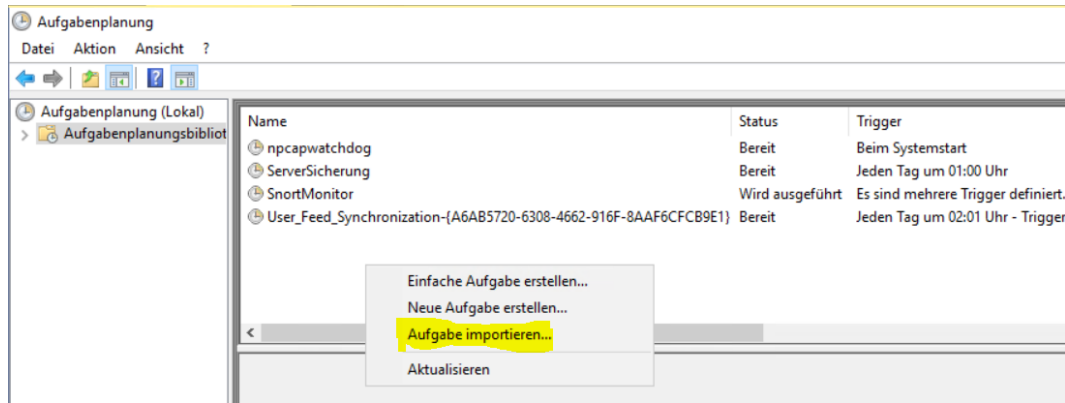
Zwei weitere Scripte, die ich für Auswertungen verwende, liegen noch auf einem anderen Server. Diese sind aber besser auf dem neuen WS-MON aufgehoben. Daher exportiere ich zunächst die dazugehörigen, geplanten Aufgaben auf dem aktuellen Server WS-RDS1:



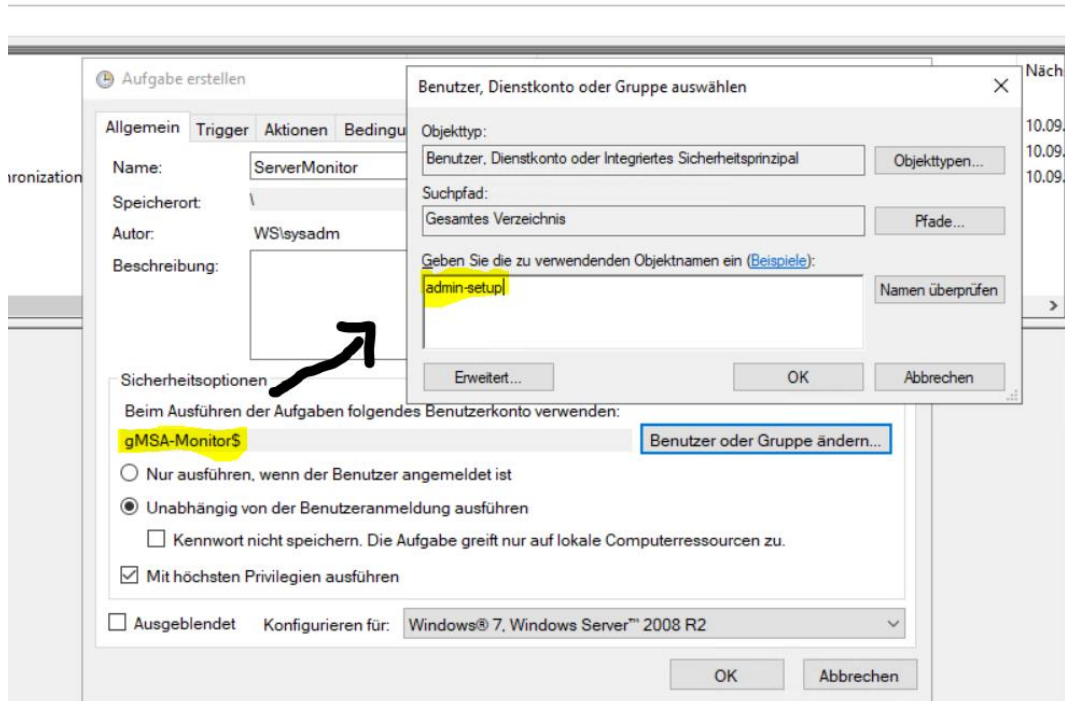
Danach kopiere ich die Scriptdateien auf WS-MON:

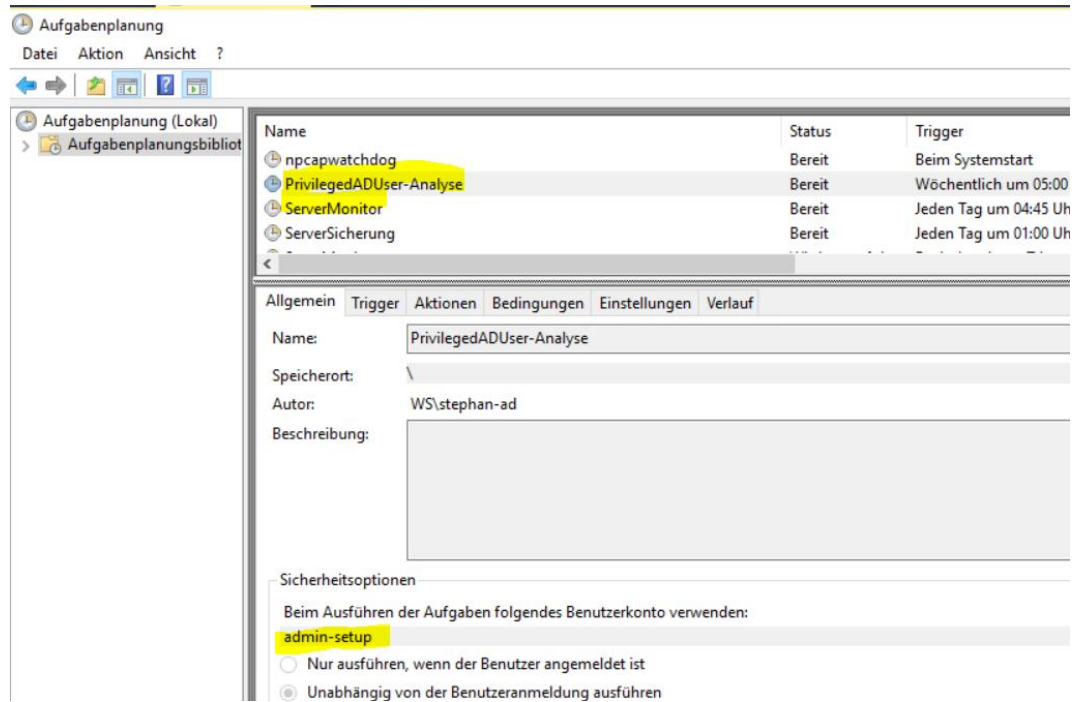


Zuletzt importiere ich die Scriptaufgaben:

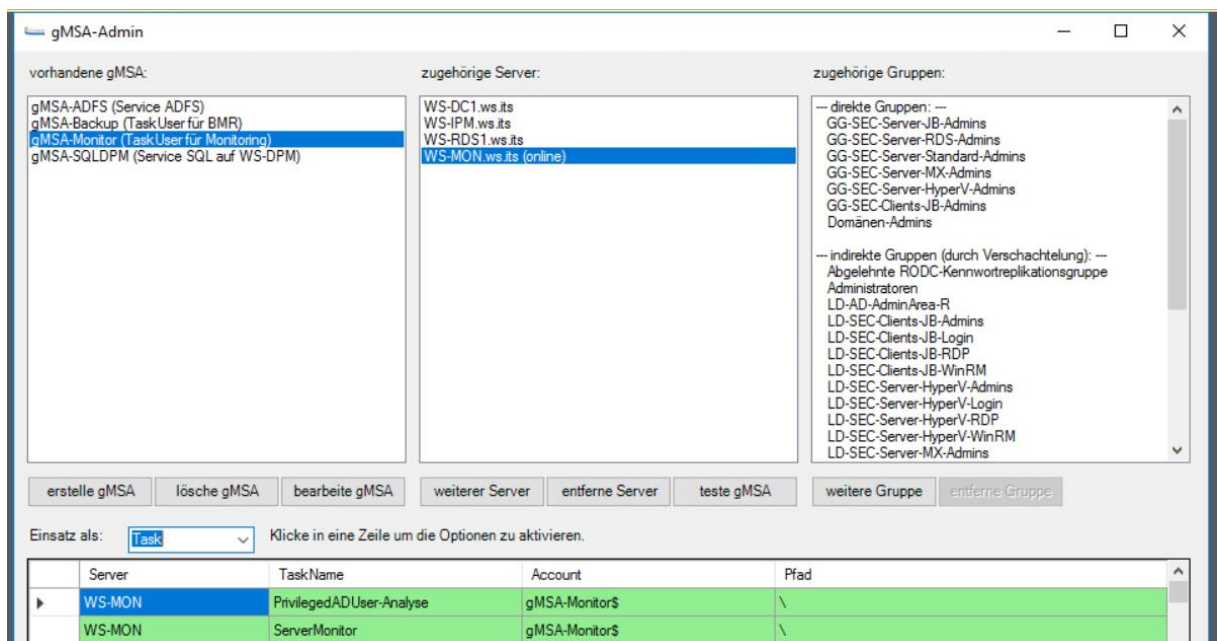


Der ausführende Account ist bei beiden Aufgaben ein spezieller Group Managed Service Account (gMSA). Von diesem kennt nur der DomainController das Passwort. Da die Aufgabenkonsole das Importieren ohne Passwort nicht erlaubt ändere ich den Account temporär:

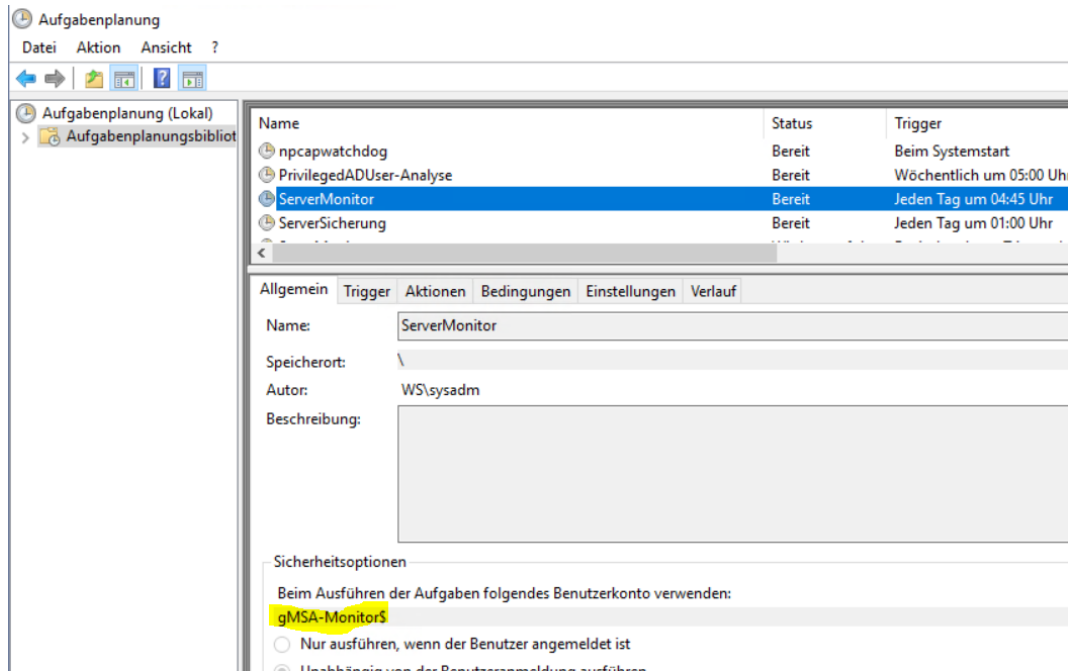




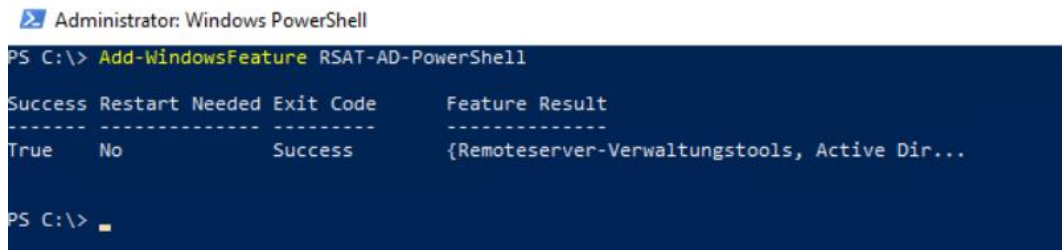
Der Account admin-setup hat gar nicht die erforderlichen Rechte. Er ist aber auch nur ein Dummy, bis ich den richtigen Account mit meinem gMSA-Tool vom DomainController aus konfiguriere:



Und nun passt es auch in der Aufgabenverwaltung:



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



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:

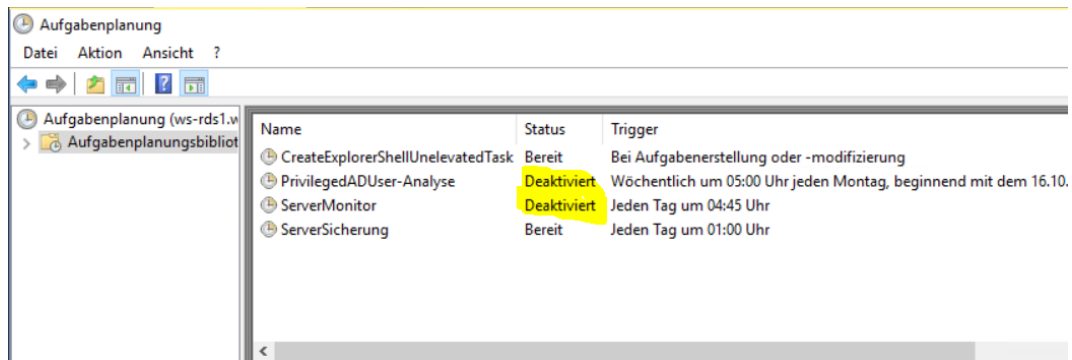
offen

Benutzer	Level	Policy	Lockout	ProtectedUser	Enabled	Description	SchedTasks	ServiceUser	LastLogon	PWfixed	PWendless	PWlastset	PWexpire	PWcomplex	PW
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	False
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	False
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	False
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	False
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	False

Zusammenfassung:

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

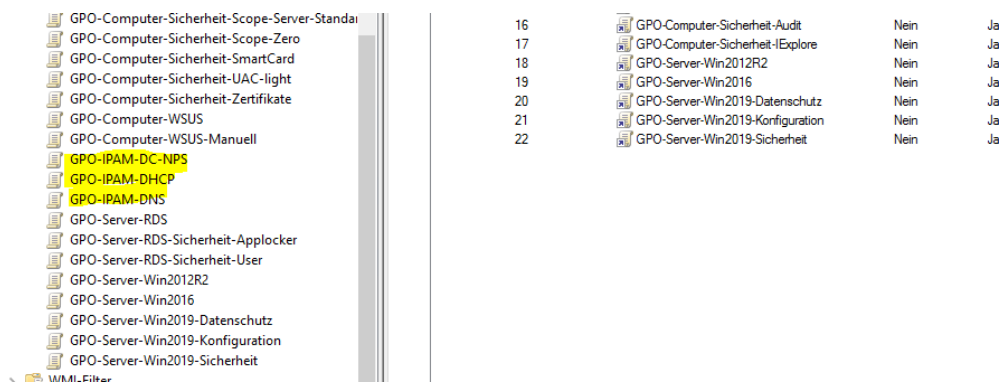
Und auch das andere Script arbeitet wie erwartet und sendet mir eine Mail. Fein. Auf dem alten Server WS-RDS1 deaktiviere ich die beiden Aufgaben. Ich möchte ja keine doppelten Mails haben:



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:



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 wadmin-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:

```

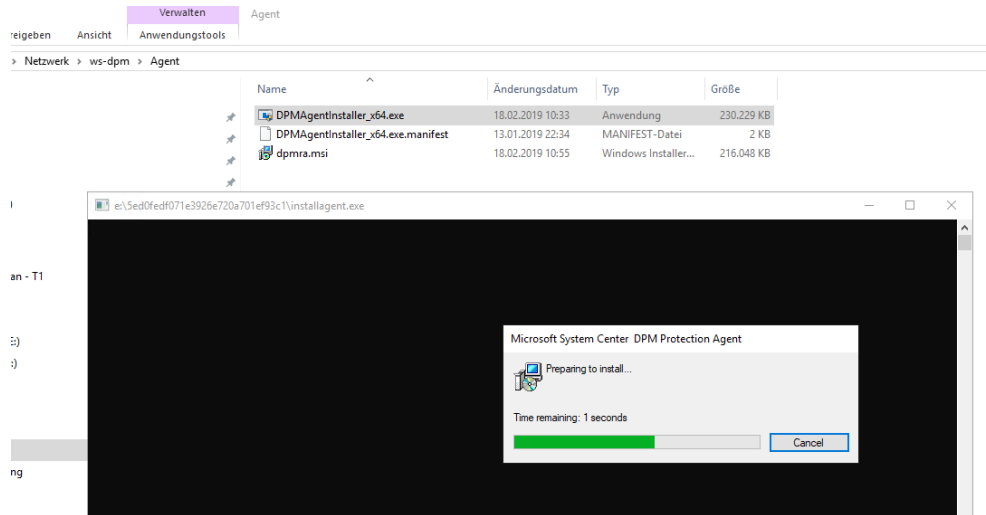
Sicherung.ini - Editor
Datei Bearbeiten Format Ansicht Hilfe

*Reporte per Mail senden
sendeMail=an
sender=service-mailing@ws-its.de
MailSubjectBackup=ServerSicherung
recipients1=logmails@ws-its.de
mailserver1=email.ws.its
recipients2=
mailserver2=

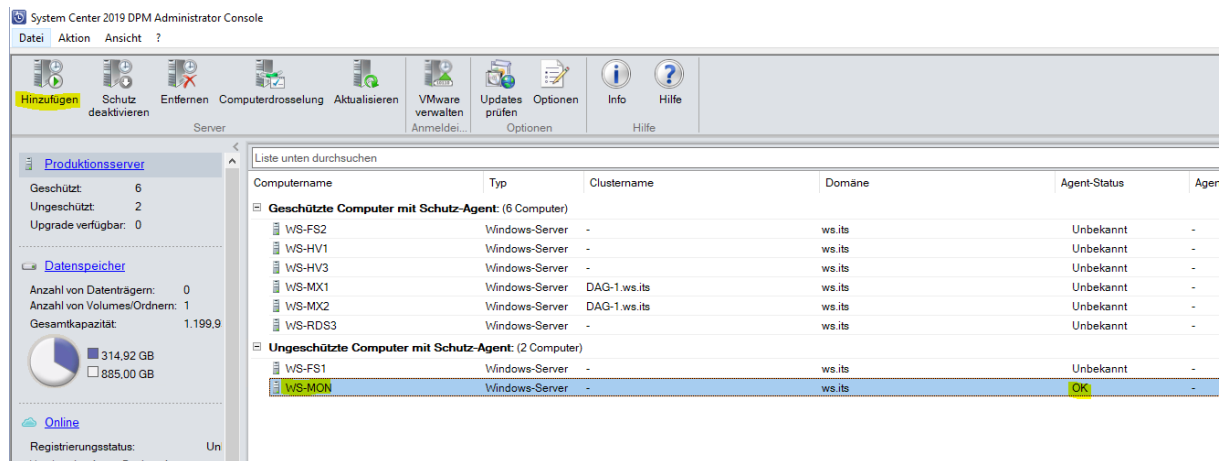
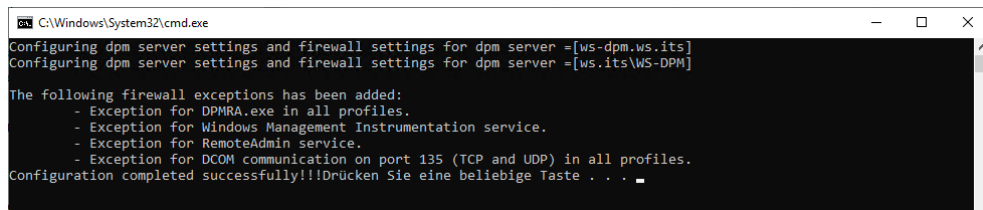
[Sicherungen]
*Optionen: -ohneTag
*Server # Delay # Tage # JobName # JobDefinition # Dest # Optionen
WS-CM # 0 # 3@135 # BMR # c: -systemstate -allCritical -vssFull # 1 #
WS-DC1 # 20 # 6@135 # BMR # c: -systemstate -allCritical -vssFull # 1 #
WS-FS1 # 40 # 3@135 # BMR # c: -systemstate -allCritical -vssFull # 1 #
WS-HV1 # 60 # 6@135 # BMR # c: -systemstate -allCritical -vssFull # 3 #
WS-RA1 # 80 # 6@135 # BMR # c: -systemstate -allCritical -vssFull # 1 #
WS-MON # 100 # 6@135 # BMR # c: -systemstate -allCritical -vssFull # 1 #
WS-RDS1 # 120 # 6@135 # BMR # c: -systemstate -allCritical -vssFull # 1 #
WS-WAC # 140 # 3@135 # BMR # c: -systemstate -allCritical -vssFull # 1 #
WS-MX1 # 160 # 6@135 # BMR # c: -systemstate -allCritical -vssFull # 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:



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



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

Neue Schutzgruppe erstellen

Gruppenmitglieder auswählen

Wählen Sie die Daten aus, die geschützt werden sollen.

Schritte:

- Willkommen
- Schutzgruppentyp auswählen
- Gruppenmitglieder auswählen**
- Methode für die Datensicherheit auswählen
- Kurzfristige Ziele auswählen
- Konsistenzprüfungsoptionen auswählen
- Zusammenfassung
- Status

Aktivieren Sie die entsprechenden Kontrollkästchen unter "Verfügbare Mitglieder", um die Daten auszuwählen, die geschützt werden sollen. Wenn die Datenquellen, die Sie schützen möchten, nicht in der Struktur unten angezeigt werden, klicken Sie auf den folgenden [Nicht unterstützte Konfigurationen](#).

Verfügbare Mitglieder

- ws.its
- DAG-1
- WS-DPM
- WS-FS1
- WS-FS2
- WS-HV1
- WS-HV3
- WS-MON
- Alle Freigaben
- Alle Volumes
- C:\
- E:\
- System Protection
- WS-MX1
- WS-MX2
- WS-RDS3

Datenquellen aktualisieren
Klicken Sie auf "Aktualisieren", um den Cache zu aktualisieren.

Aktualisieren

Ausgewählte Mitglieder

Ausgewählte Mitglieder	Computer
E:\	ws-mon.ws.its

Entfernen

Ausgeschlossene Ordner: 0 [Anzeigen](#)
Ausgeschlossene Dateien: 0 [Dateien ausschließen...](#)

< Zurück Weiter > Abbrechen Hilfe

Neue Schutzgruppe erstellen

Methode für die Datensicherheit auswählen

DPM bietet datenträger-, online- und bandbasierten Datenschutz.

Schritte:

- Willkommen
- Schutzgruppentyp auswählen
- Gruppenmitglieder auswählen
- Methode für die Datensicherheit auswählen**
- Kurzfristige Ziele auswählen
- Konsistenzprüfungsoptionen auswählen
- Zusammenfassung
- Status

Schutzgruppenname:

Schutzmethode

Wählen Sie die gewünschte Schutzmethode aus.

Ich möchte kurzfristigen Schutz per:

Ich möchte Onlineschutz
Konfigurieren Sie den Onlineschutz auf der Seite "Verwaltung", um diese Option zu aktivieren.

Ich möchte langfristigen Schutz per Band
Der Schutz mithilfe von Bandooptionen ist deaktiviert, weil keine Bandbibliotheken erkannt wurden oder weil die Schutzgruppe Datenquellen enthält, die nicht auf

Neue Schutzgruppe erstellen

Kurzfristige Ziele angeben

Ein Schutzplan wird von DPM mithilfe Ihrer kurzfristigen Wiederherstellungsziele erstellt.

Schritte:

- Willkommen
- Schutzgruppentyp auswählen
- Gruppenmitglieder auswählen
- Methode für die Datensicherheit auswählen
- Kurzfristige Ziele auswählen**
- Datenspeicherzuordnung überprüfen
- Replikaterstellungsmethode auswählen
- Konsistenzprüfungsoptionen auswählen
- Zusammenfassung
- Status

Geben Sie Ihre kurzfristigen Wiederherstellungsziele für den datenträgerbasierten Schutz an.

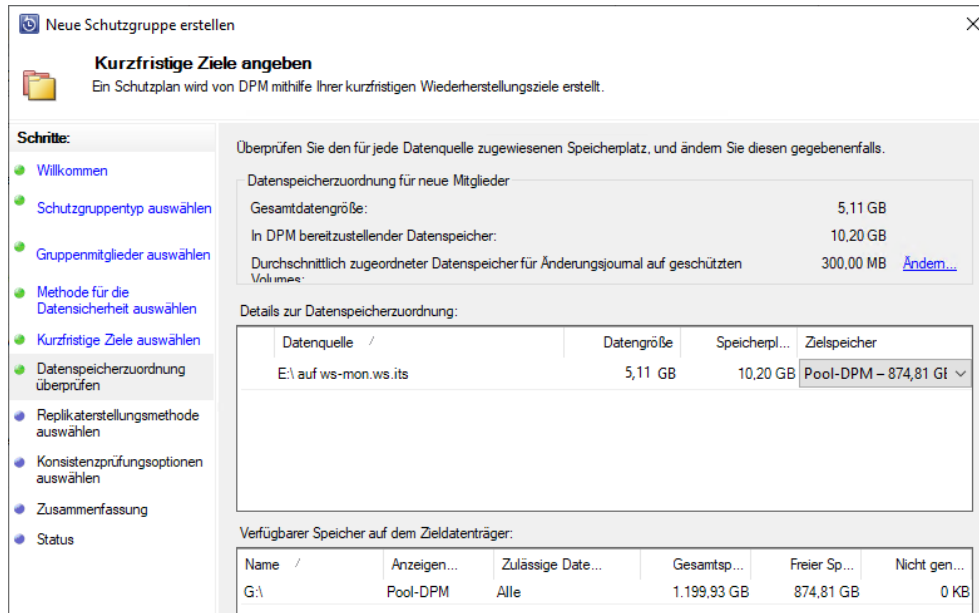
Beibehaltungsdauer: Tage

Synchronisierungsfrequenz: Alle Direkt vor einem Wiederherstellungspunkt

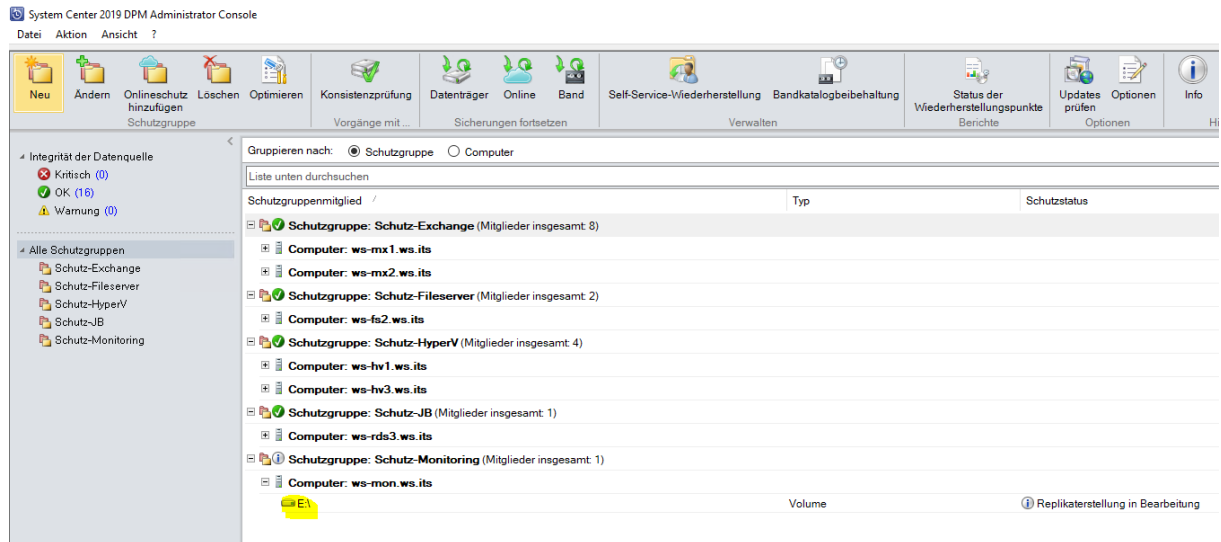
Dateiwiederherstellungspunkte

Geben Sie Wiederherstellungspunkte für Dateimitglieder an.

Wiederherstellungspunkte für Dateien: [Andern...](#)



Ich lasse die initiale Sicherung direkt starten:



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.