Inhalt

Zielsetzung

Zur Zeit verwende ich System Center Data Protection Manager 2016 (DPM), der auf einem Windows Server 2016 läuft. Diese Version ist nicht mit Windows Server 2019 kompatibel. Da eine Datensicherung ein wichtiger Bestandteil meiner Infrastruktur ist, muss mein DPM auf die aktuelle Version 2019 aktualisiert werden. Dabei soll eine möglichst verlustfreie Migration des alten DPM-Servers durchgeführt werden: die bestehende Datensicherung soll also übernommen werden.

Für die Umstellung sind 2 Schritte laut Microsoft erforderlich:

- eine Inplace-Aktualisierung des DPM von 2016 auf 2019 auf dem Windows Server 2016
- eine Inplace-Aktualisierung des Betriebssystems von Windows 2016 auf 2019

Nur so können die bestehenden Sicherungen übernommen werden.

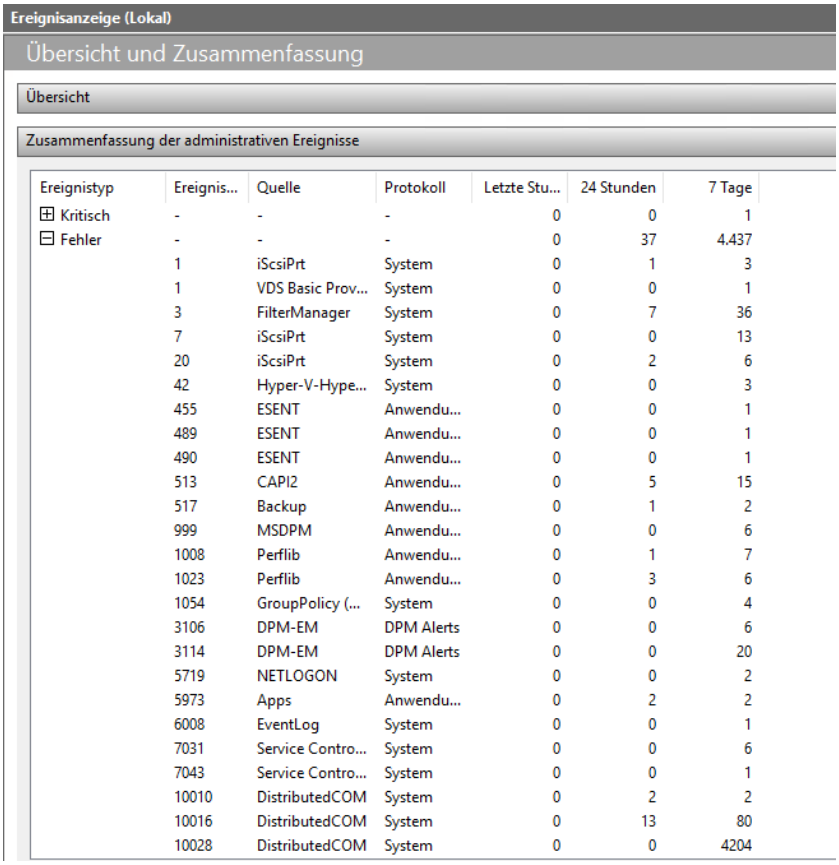
Mein DPM nimmt auch die SystemState-Backups meiner Windows Server entgegen. Alle Server speichern diese in eine SMB-Freigabe. Der DPM wiederum lenkt die Daten auf eine via iSCSI angebundene NAS um. BMR steht hier für BareMetalRecovery und ermöglicht die Wiederherstellung eines Windows Servers in einen leeren Computer. Das bietet sich besonders bei Problemen mit dem Betriebssystem (nach einem Update, einer verpatzten Konfiguration, …) an. Auch diese Funktion soll das System weiter ausführen.

Upgrade vom Server WS-DPM

Vorarbeiten

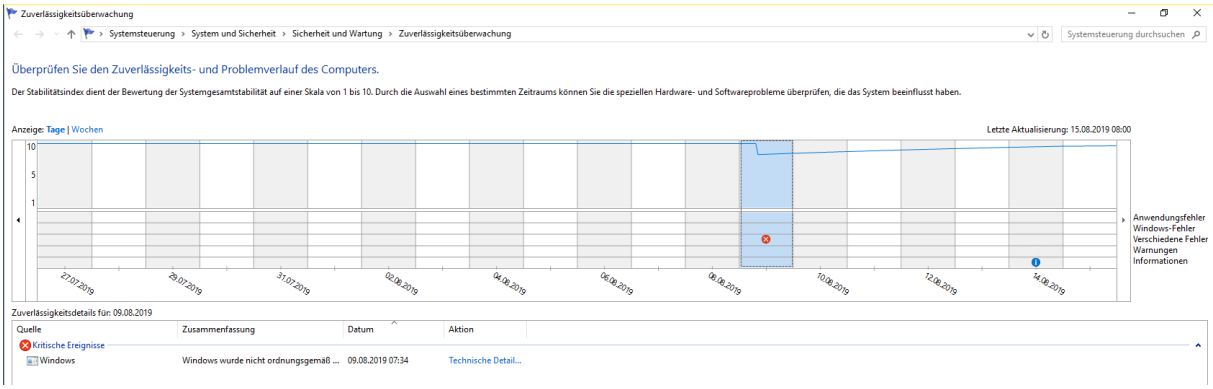
Zuerst prüfe ich den aktuellen Systemzustand. Die Datensicherung funktioniert tadellos. Das Betriebssystem ist UpToDate. Es ist ausreichend freier Speicher vorhanden.

Auch in den Eventlogs finde ich keine Probleme:



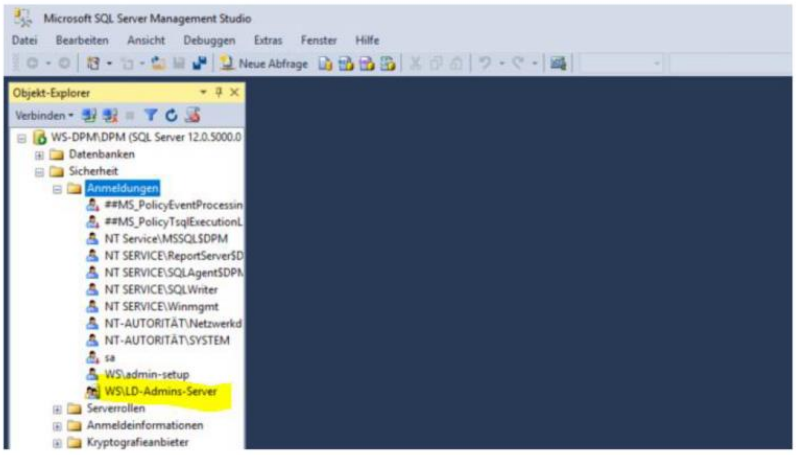
Ereignistyp	Ereignis...	Quelle	Protokoll	Letzte Stu...	24 Stunden	7 Tage
⊞ Kritisch	-	-	-	0	0	1
⊟ Fehler	-	-	-	0	37	4.437
	1	iScsiPrt	System	0	1	3
	1	VDS Basic Prov...	System	0	0	1
	3	FilterManager	System	0	7	36
	7	iScsiPrt	System	0	0	13
	20	iScsiPrt	System	0	2	6
	42	Hyper-V-Hype...	System	0	0	3
	455	ESENT	Anwendu...	0	0	1
	489	ESENT	Anwendu...	0	0	1
	490	ESENT	Anwendu...	0	0	1
	513	CAPI2	Anwendu...	0	5	15
	517	Backup	Anwendu...	0	1	2
	999	MSDPM	Anwendu...	0	0	6
	1008	Perflib	Anwendu...	0	1	7
	1023	Perflib	Anwendu...	0	3	6
	1054	GroupPolicy (...	System	0	0	4
	3106	DPM-EM	DPM Alerts	0	0	6
	3114	DPM-EM	DPM Alerts	0	0	20
	5719	NETLOGON	System	0	0	2
	5973	Apps	Anwendu...	0	2	2
	6008	EventLog	System	0	0	1
	7031	Service Contro...	System	0	0	6
	7043	Service Contro...	System	0	0	1
	10010	DistributedCOM	System	0	2	2
	10016	DistributedCOM	System	0	13	80
	10028	DistributedCOM	System	0	0	4204

Der Zuverlässigkeitsverlauf ist eine schnelle Möglichkeit für einen Systemcheck. Auch hier gibt es außer einem ungeplanten Shutdown keine Probleme:



Der DPM verwendet für die Verwaltung seiner Backups eine lokale SQL-Datenbank. Von dieser erstelle ich noch schnell eine Datenbanksicherung, denn die Aktualisierung des DPM wird auch das Schema dieser DB verändern. Mein Serveradmin hat aber nicht (mehr) die erforderlichen Berechtigungen. Der Zugriff auf die DB wird verweigert. Aber dank meiner (fast) lückenlosen Dokumentation fand ich im Installationslog des DPM 2016 den richtigen Hinweis. Folgender Account ist berechtigt:

Die Berechtigungen im SQL passe ich wieder mit dem SSMS an:

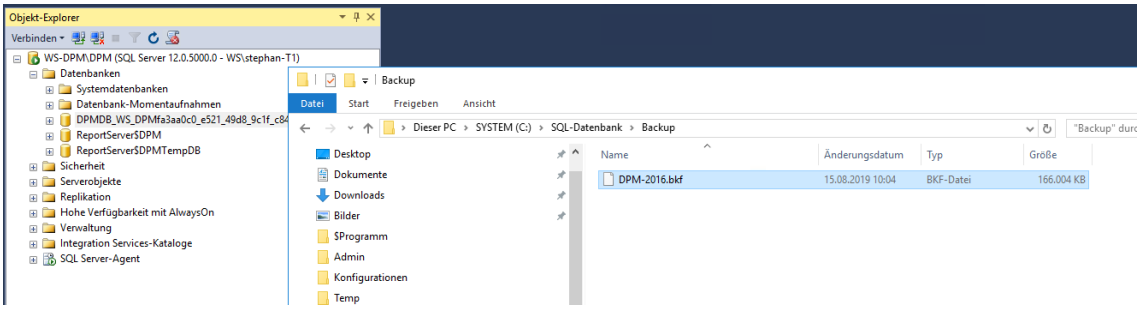


Wegen dem SQL-Setup und dem .net starte ich den Server neu.

Installation des DPM 2016

Die Setup-VHDX habe ich in den neuen Server mit eingebunden. Ich kann also das Setup des DPM direkt starten:

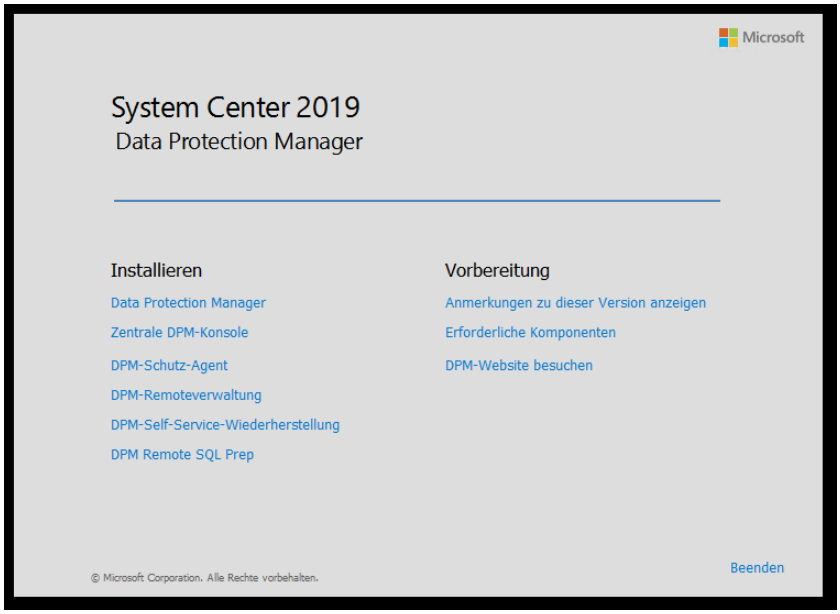
Nun korrigiere ich die Berechtigungen mit dem Account admin-setup und berechtige eine neue AD-Gruppe, in der mein Serveradmin nun Mitglied ist. So kann die Sicherung erstellt werden:

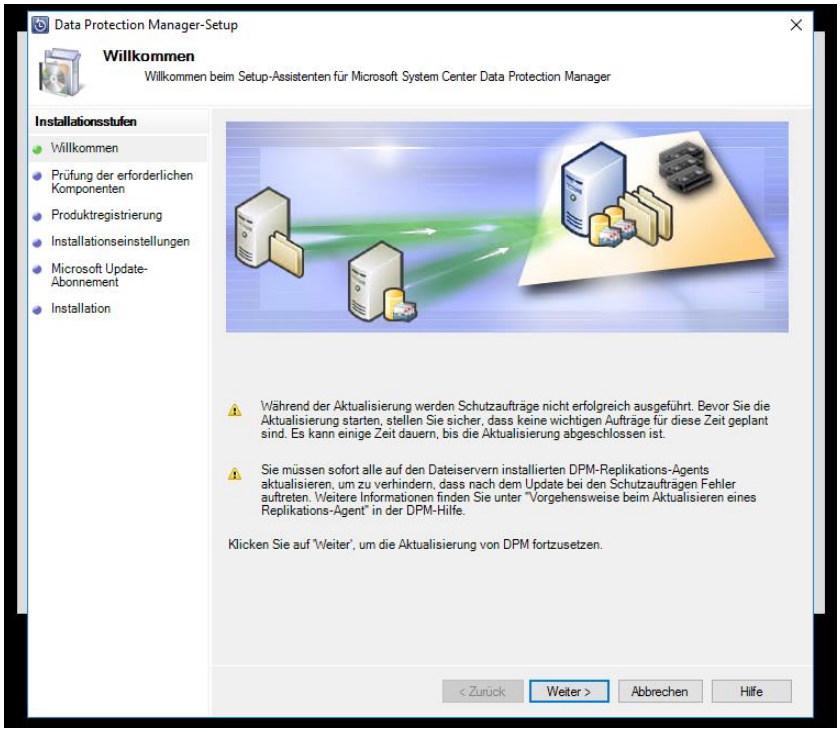


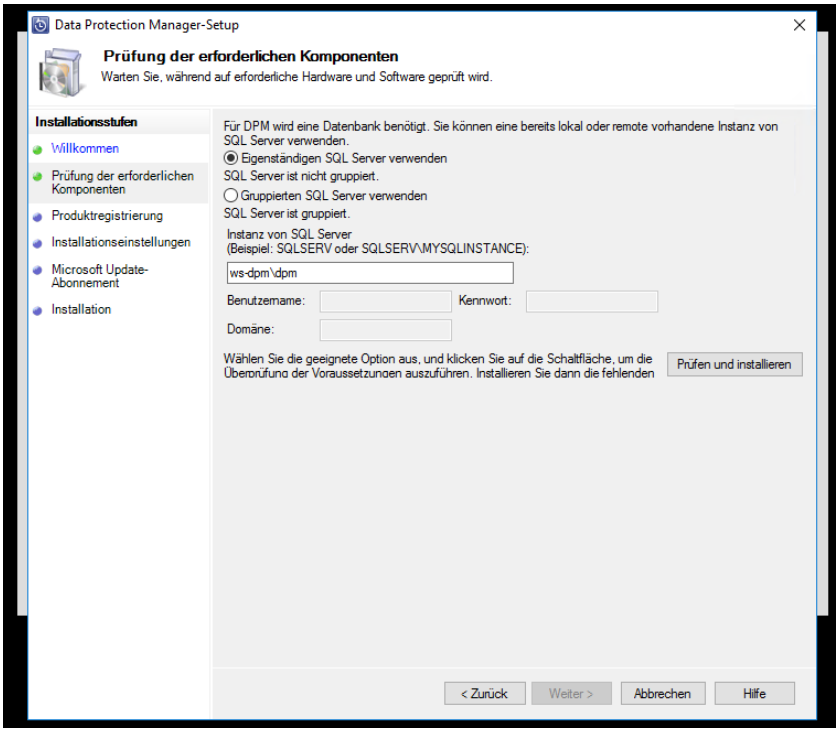
Nun folgt noch ein Blick auf das Ergebnis der letzten Serversicherung. Hier gab es 2 Aussetzer. Aber eine Sicherung steht zur Verfügung. Es sollte also bei Problemen ein Rollback möglich sein.

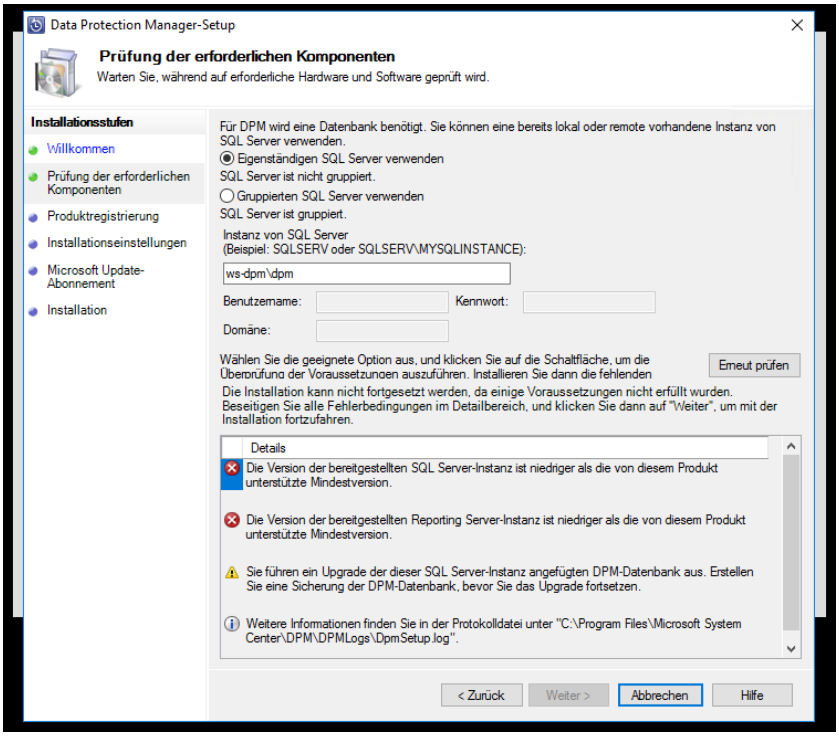
Upgrade von System Center Data Protection Manager 2019

Schritt 1 der Anweisungen von Microsoft ist die Aktualisierung des DPM von Version 2016 auf 2019. Das wird durch Ausführung des Setups erledigt:







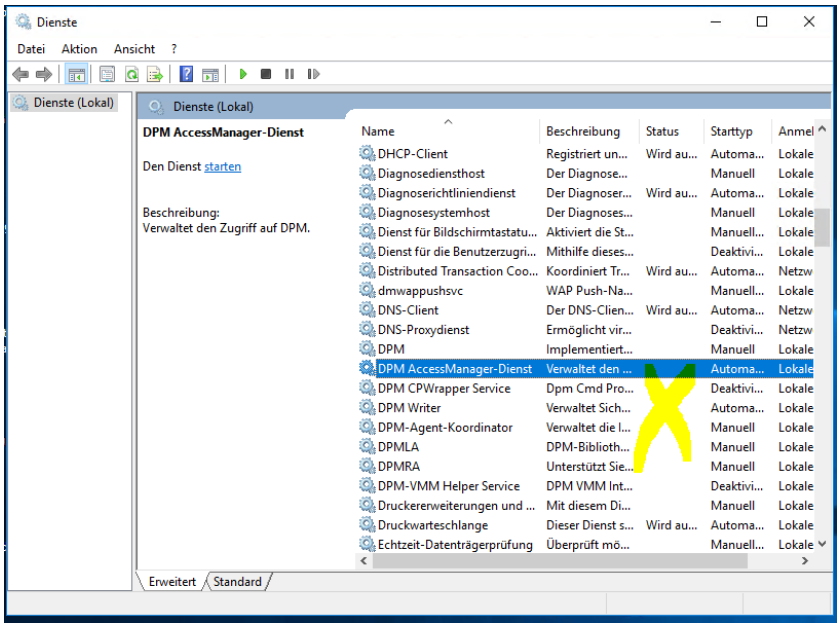


Die Vorprüfung ergibt, dass hier noch weitere Vorarbeiten erforderlich sind: der SQL-Server hat eine zu alte Version. Stimmt, hier werkelt noch ein SQL Server 2012 drunter. Also beende ich das Setup des DPM und aktualisiere den SQL-Server Inplace auf Version 2017.

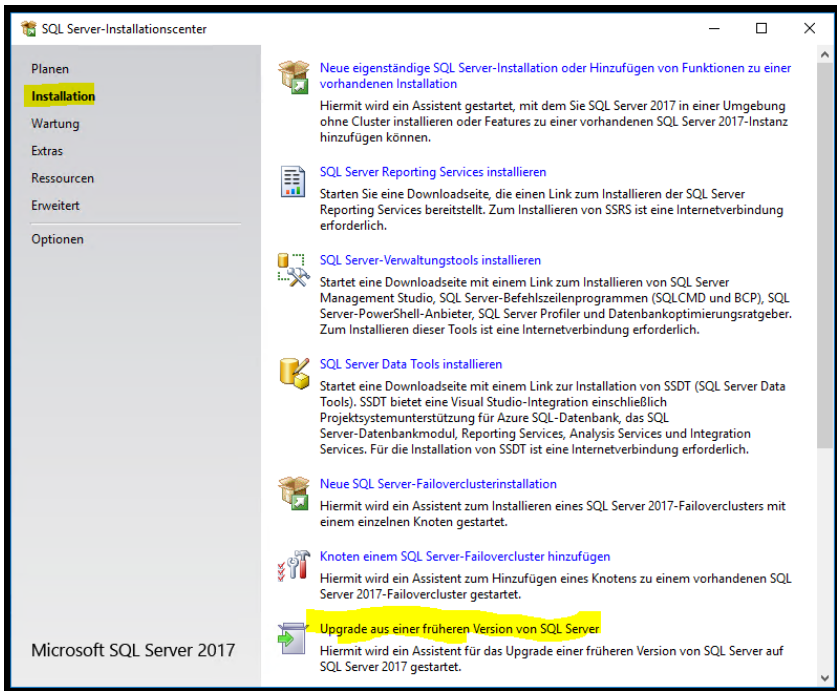
3 Inplace-Updates … ob das gut geht??

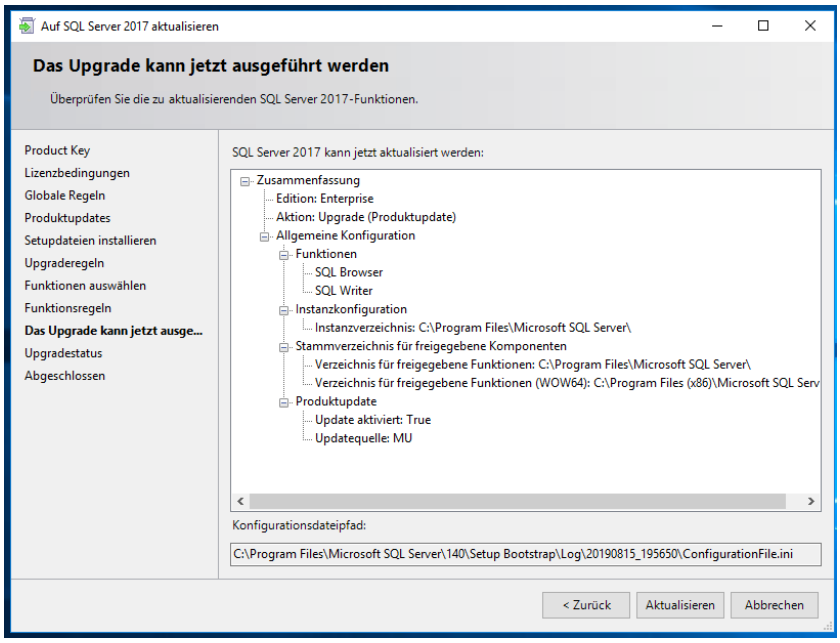
Aktualisierung des SQL-Servers auf SQL 2017

Für das Update der SQL-Instanz beende ich den DPM-Service. So ist die Datenbank frei von Zugriffen:



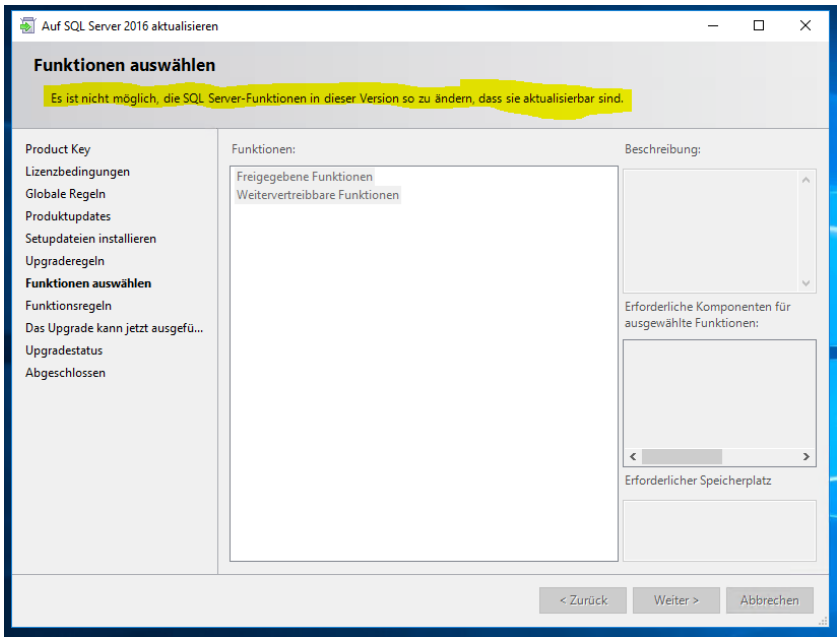
Auch der SQL-Server wird über das Setup aktualisiert:





Aber einen Moment mal. Hier stimmt was nicht: die SQL-Engine wird nicht in der Zusammenfassung gelistet. Das wird nicht ausreichen!

Naja, im Bereich SQL-Server bin ich etwas eingerostet. Vielleicht kann ich die Version auf 2016 statt 2017 aktualisieren? Leider nein, dieses Setup zeigt sogar einen Fehler an:



Stop! Das artet in ein Gefummel aus: erst wehrt sich der SQL-Server beim Upgrade, danach vielleicht auch der DPM. Und selbst wenn das alles irgendwie funktioniert – wer weiß, ob das Betriebssystem-Upgrade sauber durchläuft??

Ganz ehrlich: ich denke, eine Neuinstallation ohne Mitnahme der bestehenden Backups ist auf lange Sicht betrachtet die bessere Alternative! Ich habe den Vorteil, dass meine Backups nicht so viel Speicherplatz belegen und relativ schnell wieder aufgebaut sind. Große Unternehmen haben hier eher einen Nachteil. Natürlich kann man auch SideBySide (alt neben neu) migrieren und die neuen Backups erstellen, während die alten noch verfügbar sind. Nur kostet diese Variante für die Übergangszeit auch entsprechend viel Speicherplatz.

Ob das bei anderen Sicherungsprogrammen auch so kompliziert ist?

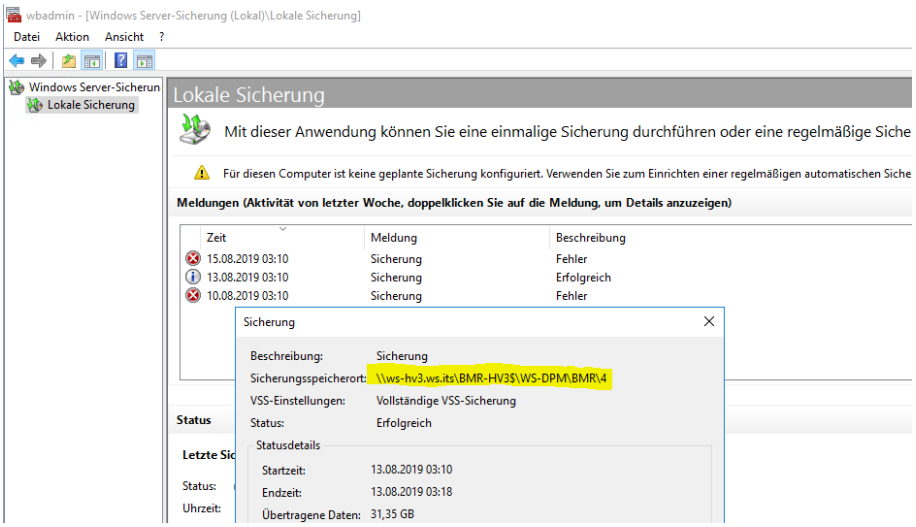
Dokumentation der aktuellen Sicherung und Entfernung der alten Agents

OK, für den Neuaufbau möchte ich zuerst einmal die aktuelle Konfiguration des DPM auslesen und dokumentieren. Also aktiviere ich die zuvor beendeten Dienste des DPM. Nur leider lassen sich diese nicht wieder einschalten! Der Fehler scheint am SQL-Server zu liegen. Offensichtlich haben meinen Aktualisierungsversuche am SQL die Instanz beschädigt. Super!

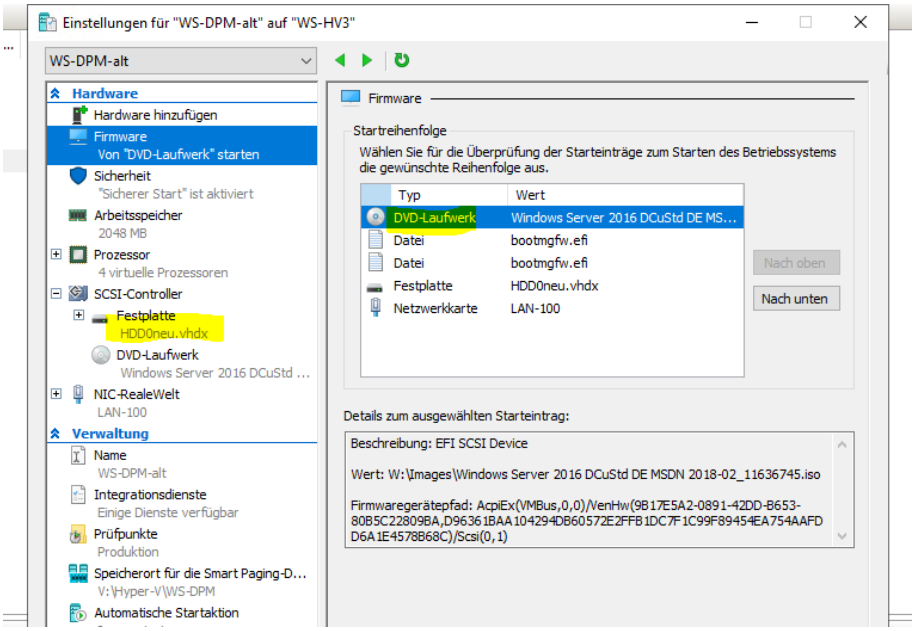
Aber ich habe ja ein Backup des Betriebssystems. Genau für diese Szenarien prüft man VORHER den Zustand des Systems inklusive der Datensicherung. 😊

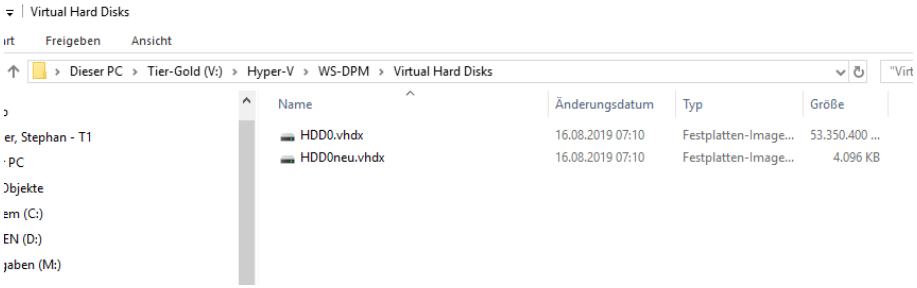
Durchführung einer BMR (BareMetalRecovery)

Ich sichere meine Betriebssysteme mit Windows Boardmitteln (Windows Backup) über eine zentral gesteuerte Scriptlösung auf mehrere Netzlaufwerke. Dazu kommt ein Rotationsverfahren. Ich muss also zuerst herausfinden, in welches Verzeichnis zuletzt erfolgreich gesichert wurde:

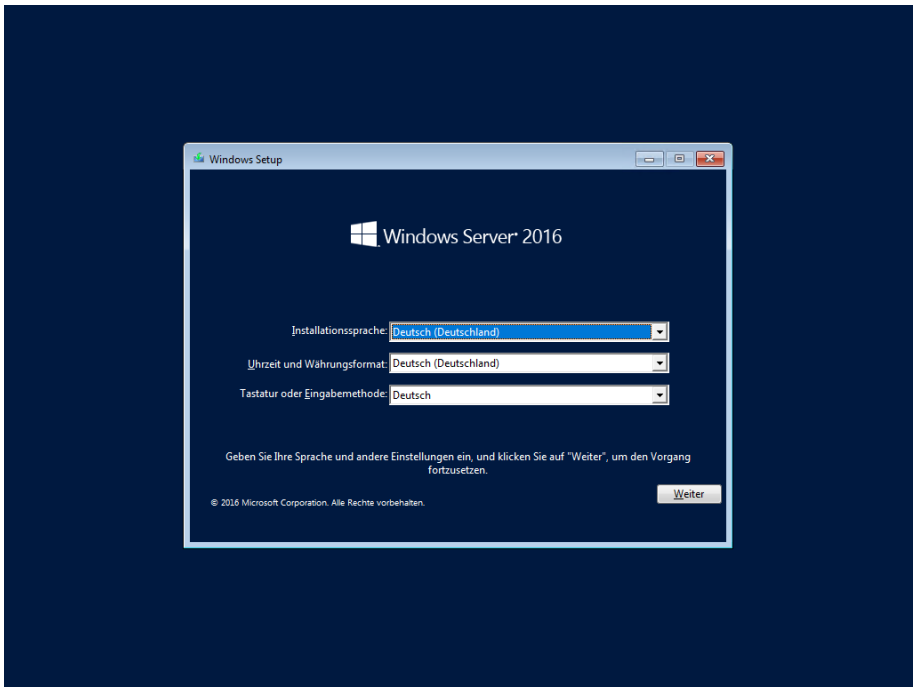


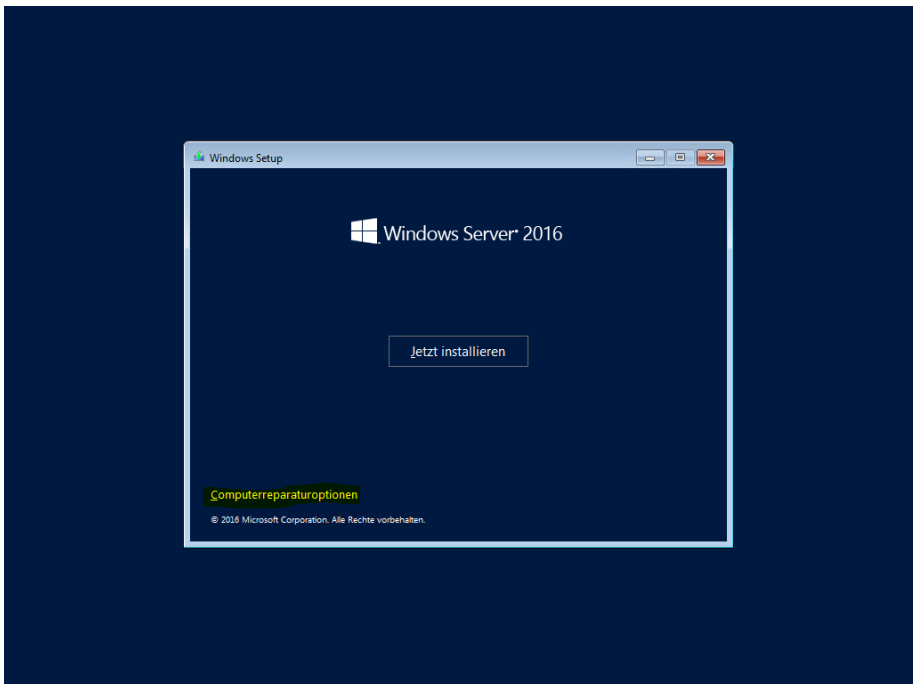
Damit nicht noch mehr verlorengeht, erstelle ich im Hyper-V für die VM des DPM eine neue VHDX-Datei. So kann ich bei Bedarf auf den aktuellen Zustand zurückgehen.

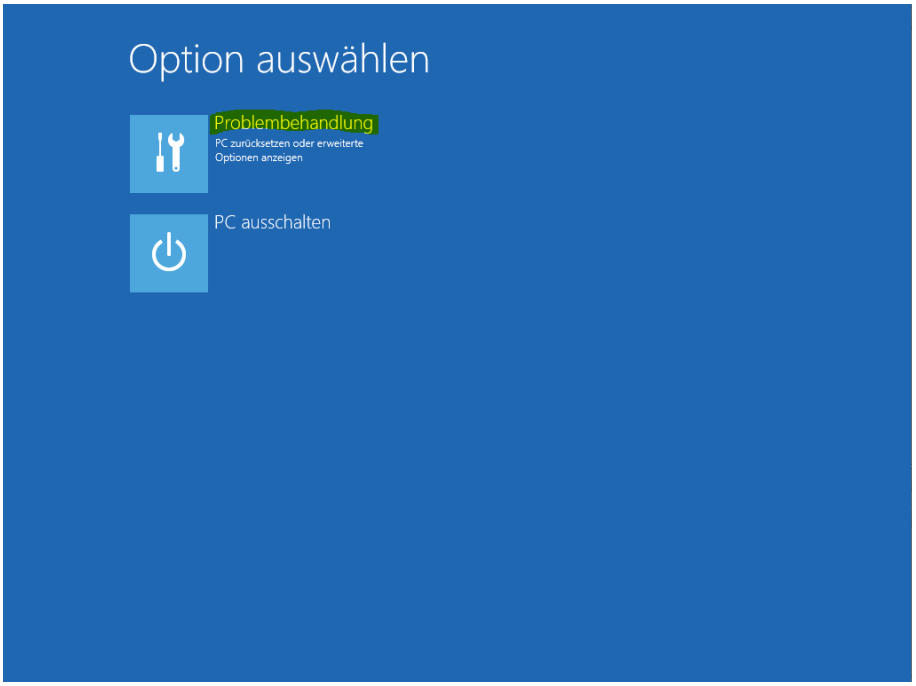


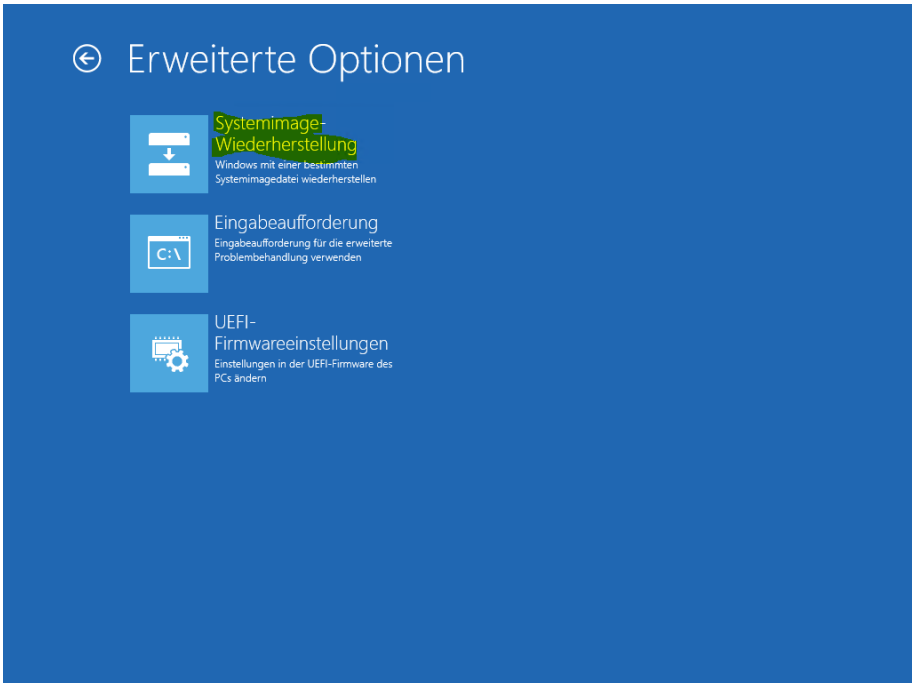


Nun starte ich die VM mit einem Installationsdatenträger und hangele mich zu der SystemImageRecovery:

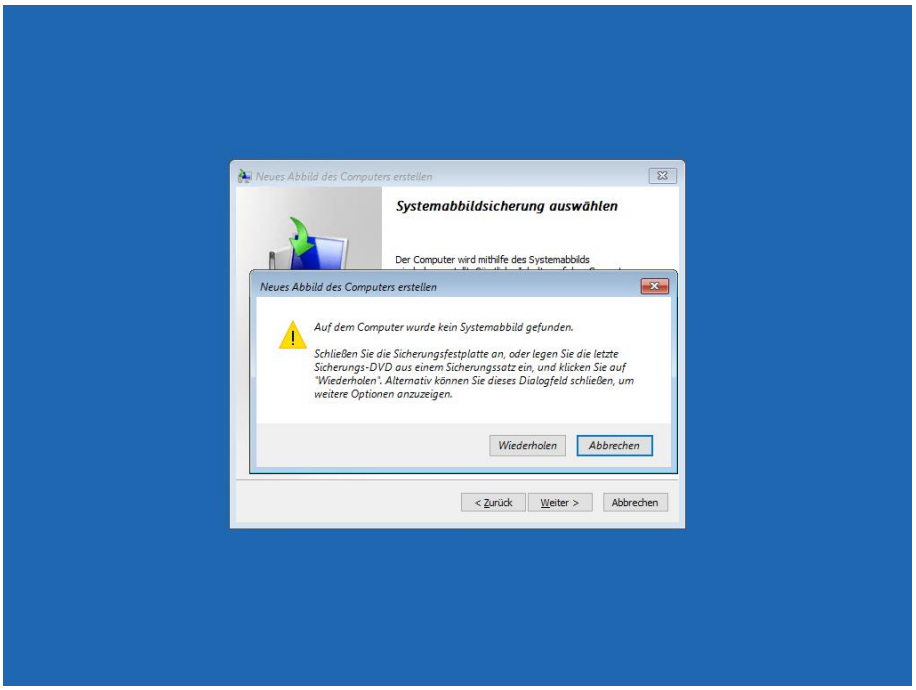




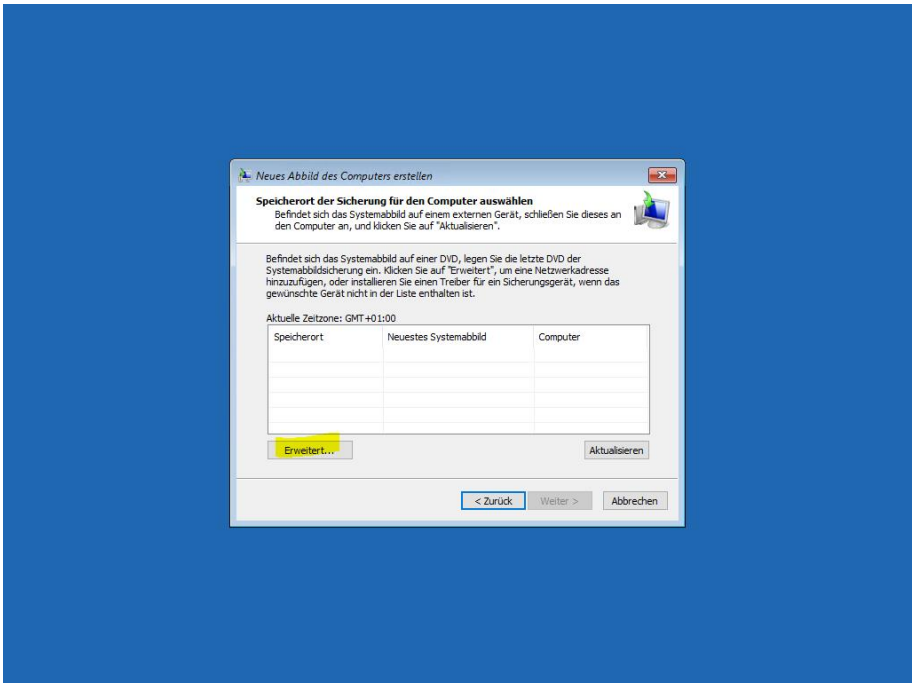


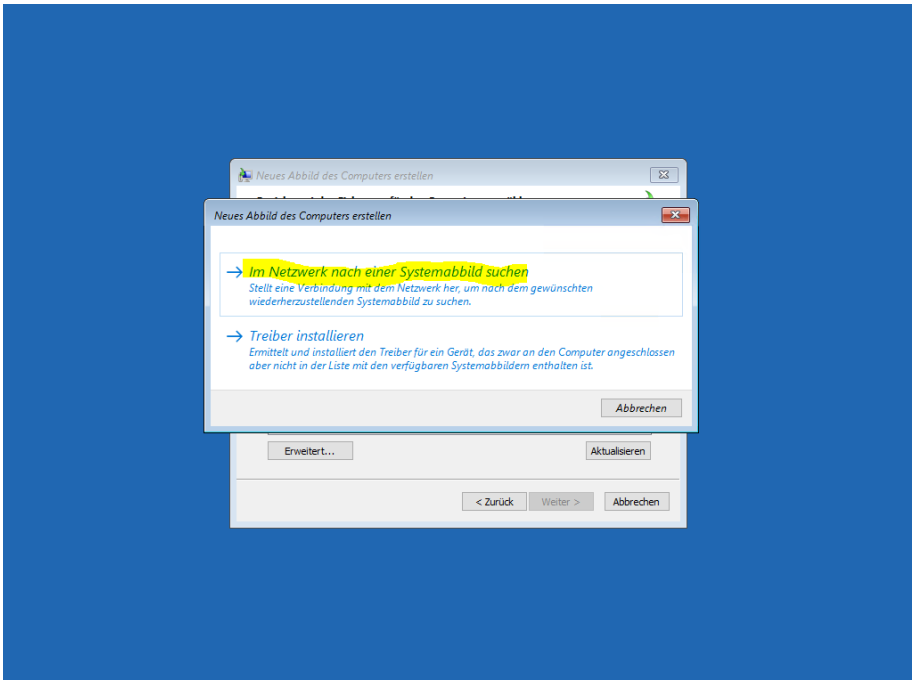


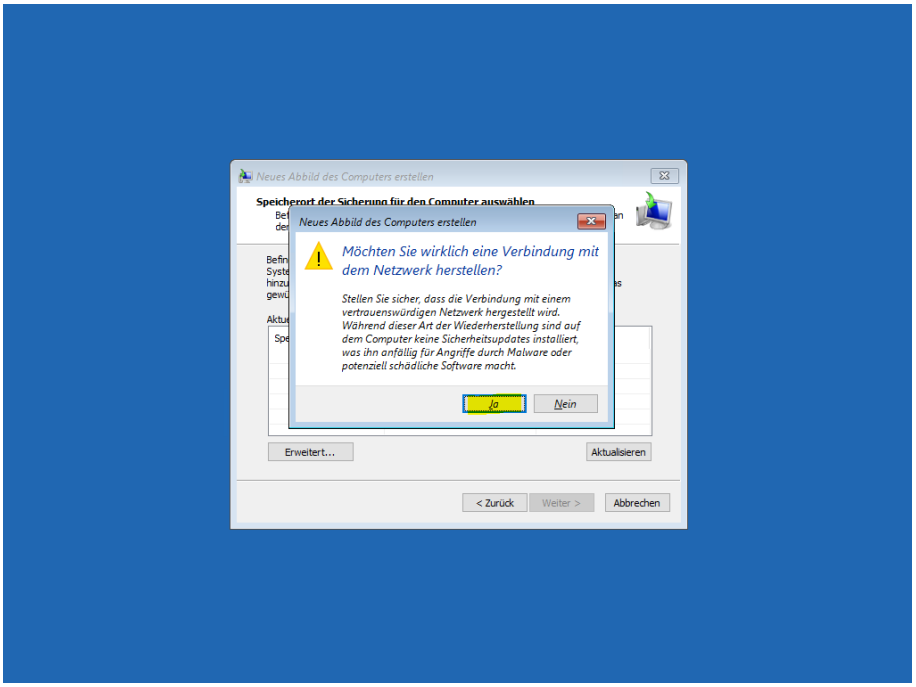
Die Datensicherung liegt nicht lokal. Daher zeigt das Setup eine Fehlermeldung an:

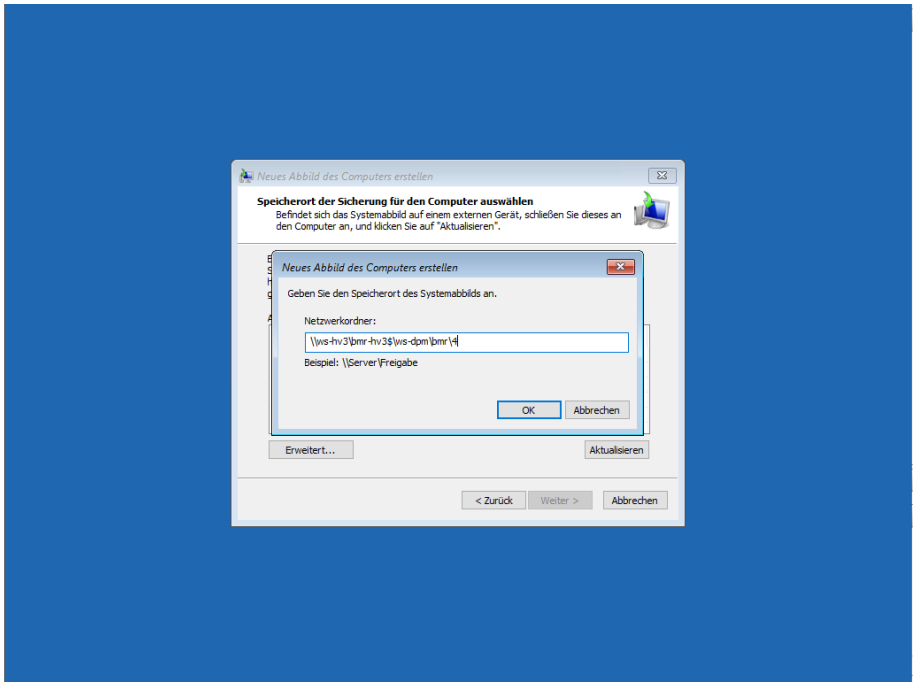


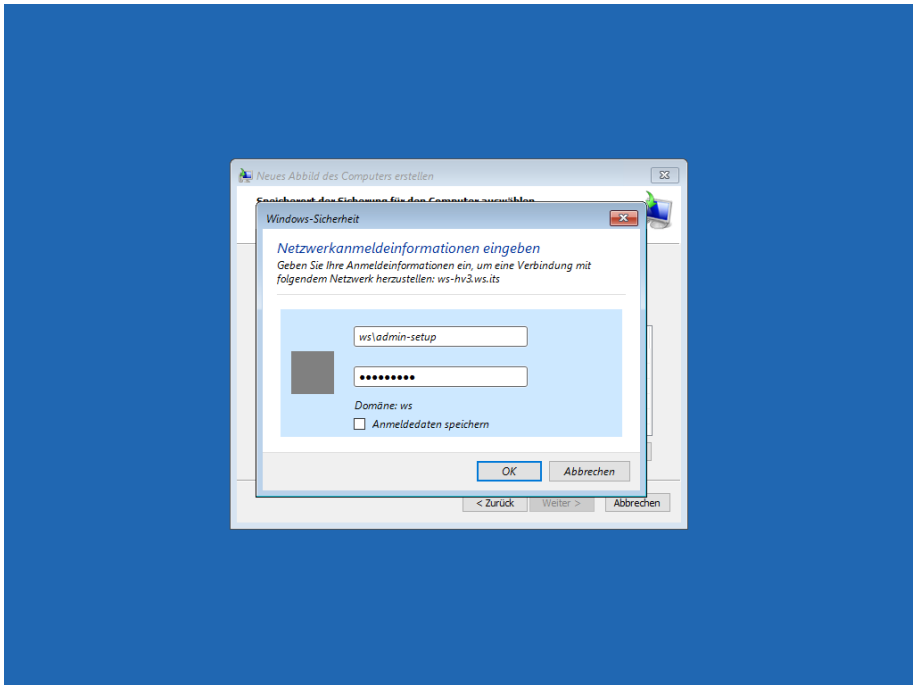
Über „erweitert“ kann aber eine Verbindung zum Netzwerk hergestellt werden. Dazu ist aber ein DHCP-Server erforderlich:

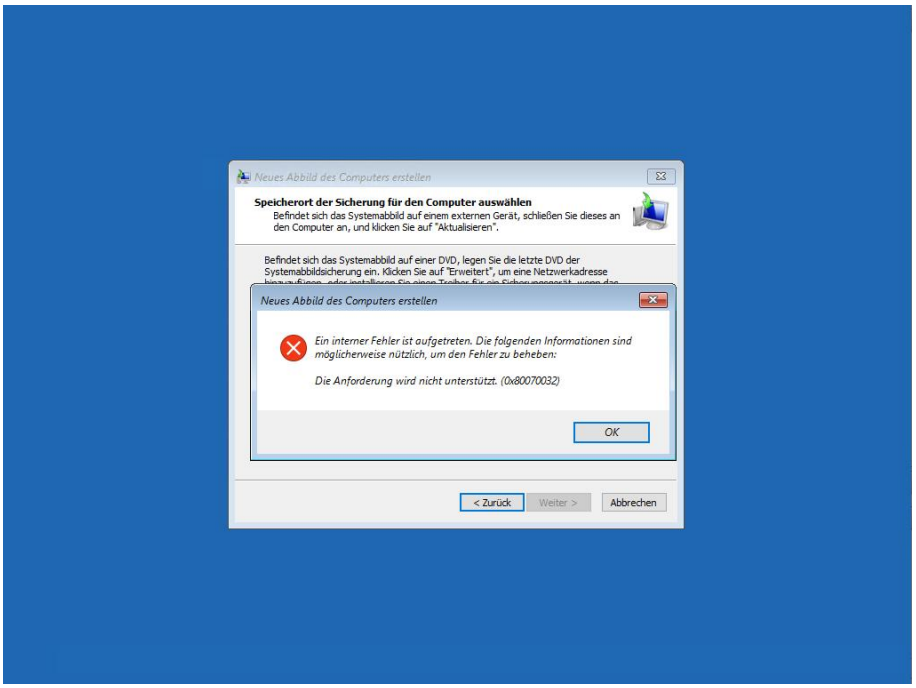



Neues Abbild des Computers erstellen
Neues Abbild des Computers erstellen
Im Netzwerk nach einer Systemabbild suchen
Stellt eine Verbindung mit dem Netzwerk her, um nach dem gewünschten wiederherzustellenden Systemabbild zu suchen.
Treiber installieren
Ermittelt und installiert den Treiber für ein Gerät, das zwar an den Computer angeschlossen aber nicht in der Liste mit den verfügbaren Systemabbildern enthalten ist.
Abbrechen
Erweitert...
Aktualisieren
< Zurück
Weiter >
Abbrechen


Neues Abbild des Computers erstellen
Speicherort der Sicherung für den Computer auswählen
Neues Abbild des Computers erstellen
Möchten Sie wirklich eine Verbindung mit dem Netzwerk herstellen?
Stellen Sie sicher, dass die Verbindung mit einem vertrauenswürdigen Netzwerk hergestellt wird. Während dieser Art der Wiederherstellung sind auf dem Computer keine Sicherheitsupdates installiert, was ihn anfällig für Angriffe durch Malware oder potenziell schädliche Software macht.
Ja
Nein
Erweitert...
Aktualisieren
< Zurück
Weiter >
Abbrechen


Neues Abbild des Computers erstellen
Speicherort der Sicherung für den Computer auswählen
Befindet sich das Systemabbild auf einem externen Gerät, schließen Sie dieses an den Computer an, und klicken Sie auf "Aktualisieren".
Neues Abbild des Computers erstellen
Geben Sie den Speicherort des Systemabbilds an.
Netzwerkordner:
\\ws-hv3\bmr-hv3$\ws-dpm\bmr\4
Beispiel: \\Server\Freigabe
OK
Abbrechen
Erweitert...
Aktualisieren
< Zurück
Weiter >
Abbrechen


Neues Abbild des Computers erstellen
Windows-Sicherheit
Netzwerkanmeldeinformationen eingeben
Geben Sie Ihre Anmeldeinformationen ein, um eine Verbindung mit folgendem Netzwerk herzustellen: ws-hv3.ws.its
ws\admin-setup
Domäne: ws
Anmeldedaten speichern
OK
Abbrechen
< Zurück
Weiter >
Abbrechen



Mmh, das ist mir neu! Dem Benutzer admin-setup habe ich die erforderlichen Berechtigungen gewährt. Er sollte das Backup erreichen können. Was ist wohl die Ursache? Ich führe regelmäßig Wiederherstellungsversuche durch. Und diese habe mit diesem Account immer funktioniert. Was ist hier los?

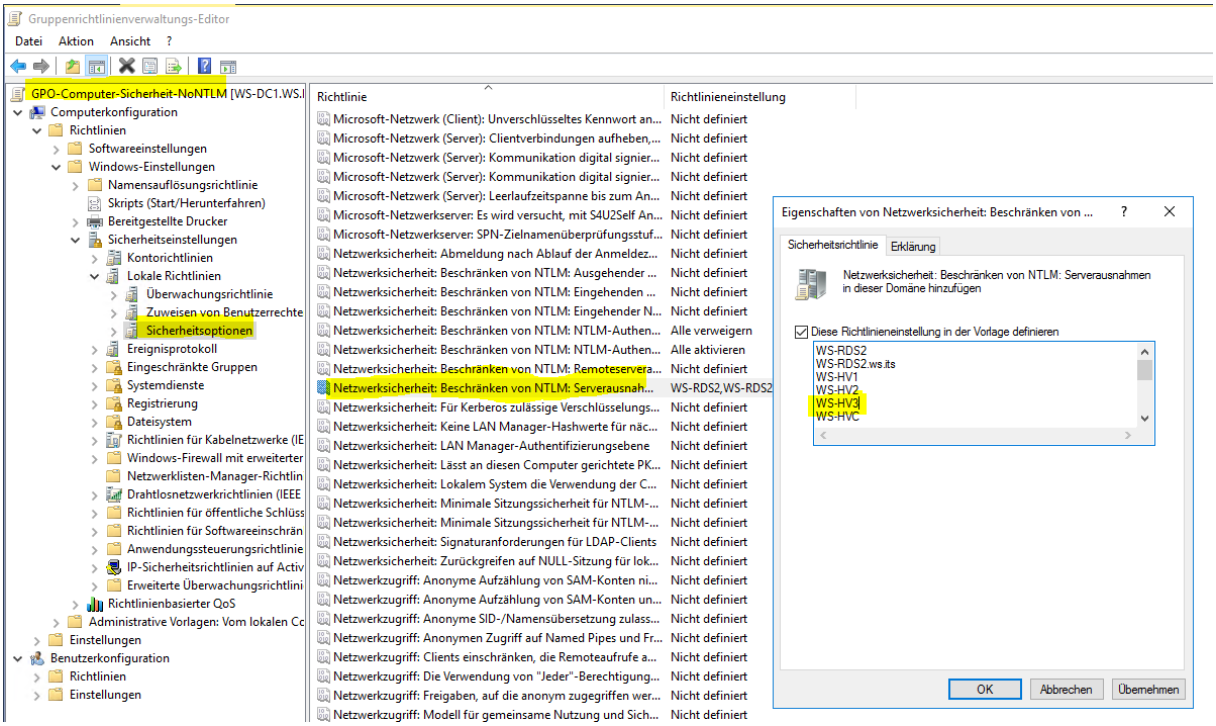
Na klar! Die Anmeldung am Zielsystem wird über NTLM durchgeführt, da das Recovery-OS kein DomainMember ist und somit kein Kerberos verwenden kann. Und vor einiger Zeit hatte ich in meiner Umgebung NTLM deaktiviert. Auf den DomainControllern kann man das dank des NTLM-Audits sehr schön sehen:

Suche-NTLMAuths.ps1*

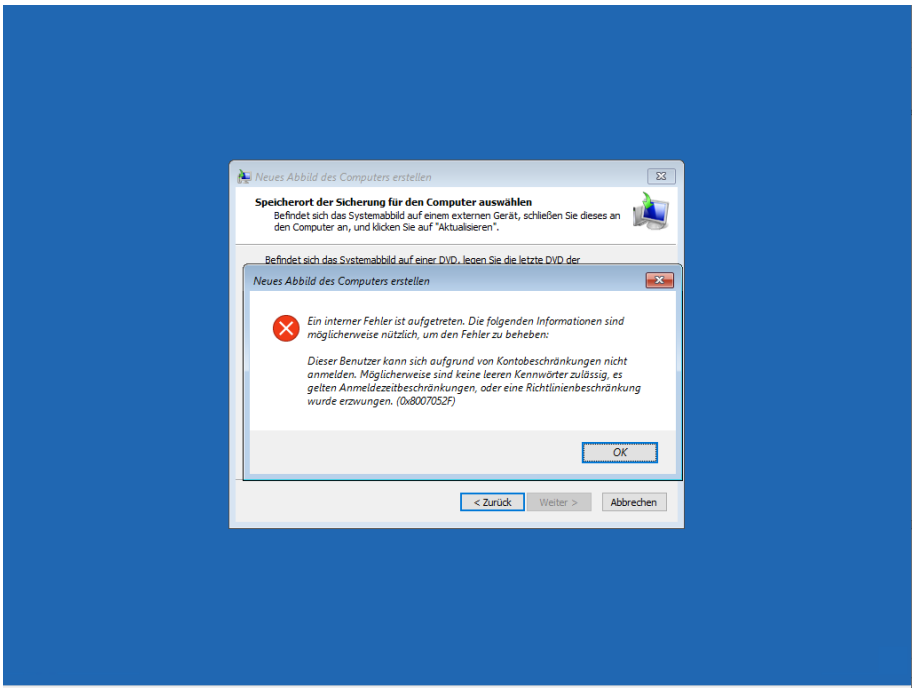
```
cls;
Invoke-Command -ComputerName (Get-ADDomain).ReplicaDirectoryServers -ScriptBlock {
    Get-WinEvent -Path C:\Windows\System32\Winevt\Logs\Microsoft-Windows-NTLM%4Operational.evtx -MaxEvents 5 -ErrorAction SilentlyContinue |
        Select-Object -Property @{ n='DC'       ; e={ $env:COMPUTERNAME                                                                                                  } },
                @{ n='Datetime' ; e={ (Get-Date -Date $_.TimeCreated -Format u) -replace 'z'                                                                             } },
                @{ n='Client'   ; e={ (($_.Message -split "`n" | select-string 'Arbeitsstationsname') -split ':')[1].trim()          } },
                @{ n='Server'   ; e={ (($_.Message -split "`n" | select-string 'Name des sicheren Kanals') -split ':')[1].trim() } },
                @{ n='Domain'   ; e={ (($_.Message -split "`n" | select-string 'Domänenname') -split ':')[1].trim()          } },
                @{ n='User'     ; e={ (($_.Message -split "`n" | select-string 'Benutzername') -split ':')[1].trim()          } }
} | Sort-Object -Property Datetime |
    Format-Table -Property DC,Datetime,Client,Server,Domain,User
```

```
DC     Datetime            Client    Server  Domain User
--     --------            ------    ------  ------ ----
WS-DC3 2019-08-15 08:31:29 WS-IPM    WS-RDS3 ws     service-prtg
WS-DC3 2019-08-15 08:31:29 WS-IPM    WS-RDS3 ws     service-prtg
WS-DC3 2019-08-15 08:54:29 WS-IPM    WS-RDS3 ws     service-prtg
WS-DC3 2019-08-15 08:54:29 WS-IPM    WS-RDS3 ws     service-prtg
WS-DC2 2019-08-16 03:59:38 WS-DC2    WS-RA2  ws.its service-ata
WS-DC2 2019-08-16 04:15:44 \\WS-DC2 WS-NAS1 ws.its service-ata
WS-DC2 2019-08-16 04:20:26 WS-DC2    WS-RA1  ws.its service-ata
WS-DC2 2019-08-16 04:31:34 WS-DC2    WS-RDS1 ws.its service-ata
WS-DC3 2019-08-16 06:45:36 WS-MON    WS-CL3  ws.its service-ata
WS-DC2 2019-08-16 07:17:43 WS-MON    WS-RA2  ws.its service-ata
WS-DC1 2019-08-16 07:35:41 MINWINPC WS-HV3  ws     admin-setup
WS-DC1 2019-08-16 07:36:11 MINWINPC WS-HV3  ws     stephan
WS-DC1 2019-08-16 07:36:11 MINWINPC WS-HV3  ws     stephan
WS-DC1 2019-08-16 07:43:57 MINWINPC WS-HV3  ws     admin-setup
WS-DC1 2019-08-16 07:43:57 MINWINPC WS-HV3  ws     admin-setup
```

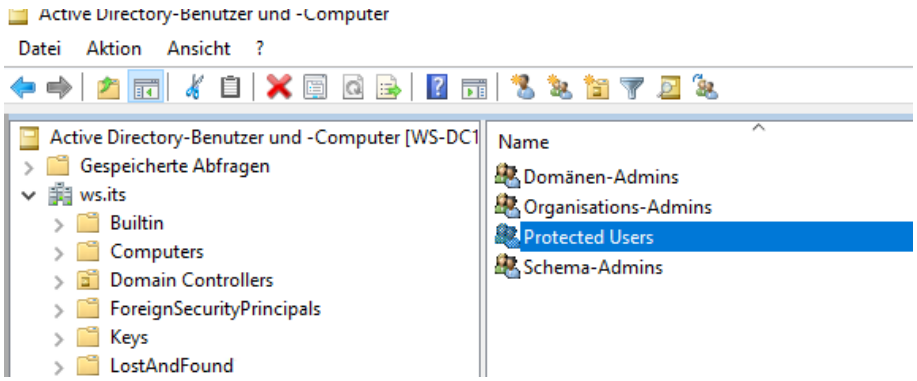
Dafür gibt es in der GPO aber die Option von Ausnahmen. Und hier sieht man das Problem: Bisher wurde die Datensicherung von meinem DPM-Server auf WS-HV2 gespeichert. Diesen Server habe ich aber vor einigen Tagen durch WS-HV3 ersetzt. Und dieser Server steht NICHT in den Ausnahmen. Das hole ich nun nach:



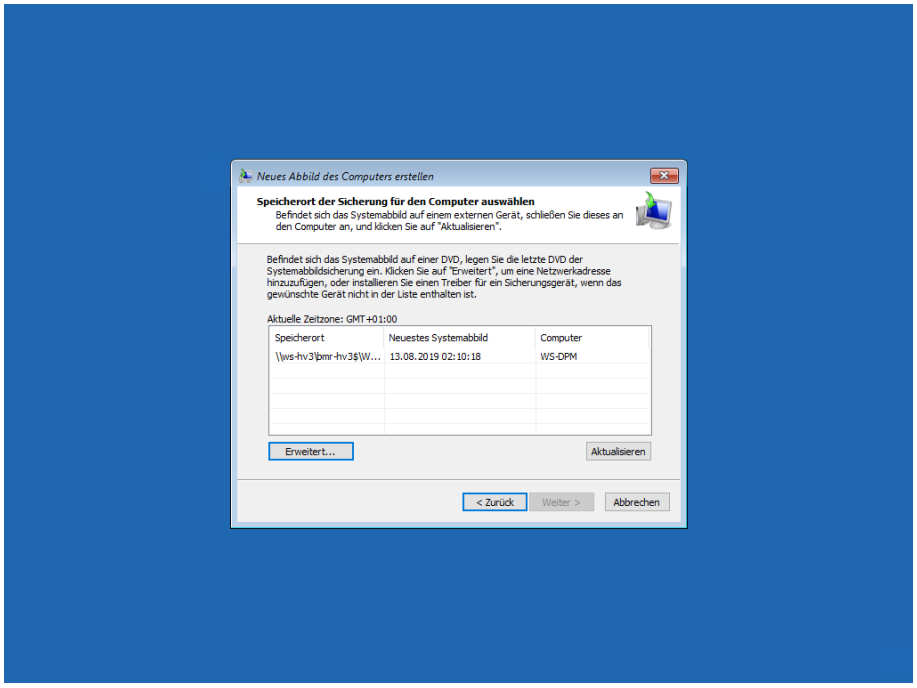
Ich starte einen neuen Versuch. Aber auch dieser scheitert:

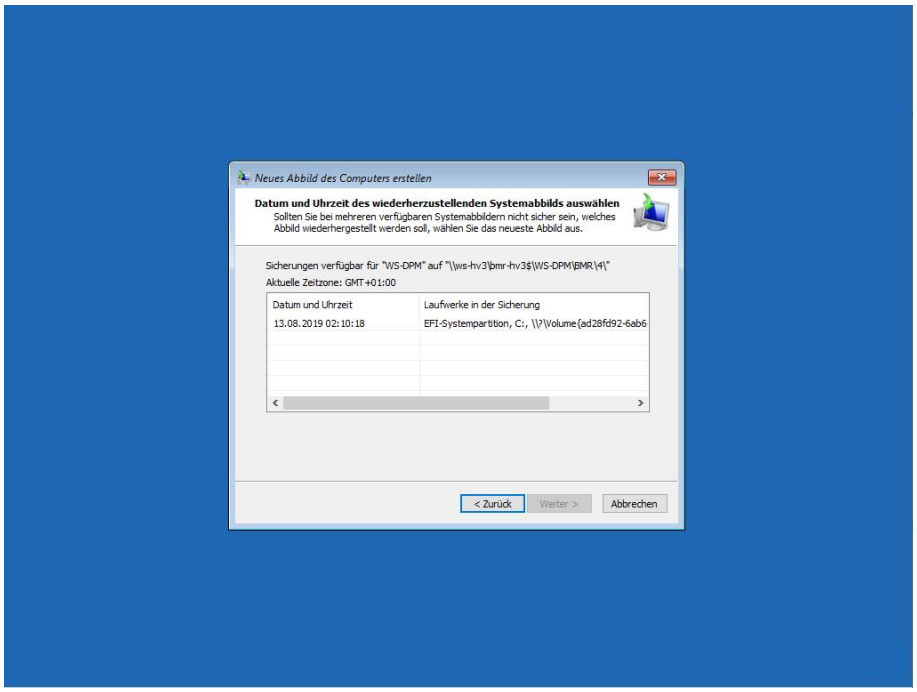


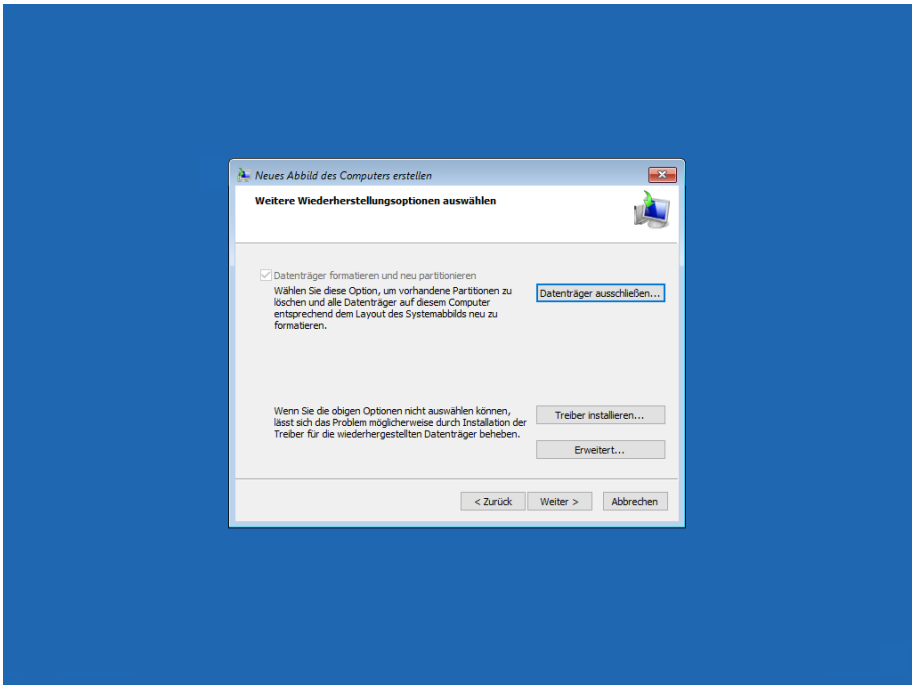
Die GPO wurde mit der Änderung erfolgreich verarbeitet. Die Ursache ist aber immer noch die Gleiche: NTLM wird nicht erlaubt. Auch hier kommt eine kleine Änderung am Account admin-setup zum Tragen: der Benutzer ist seit Neustem Mitglied der Gruppe „Protected Users“. Und diese dürfen kein NTLM verwenden…

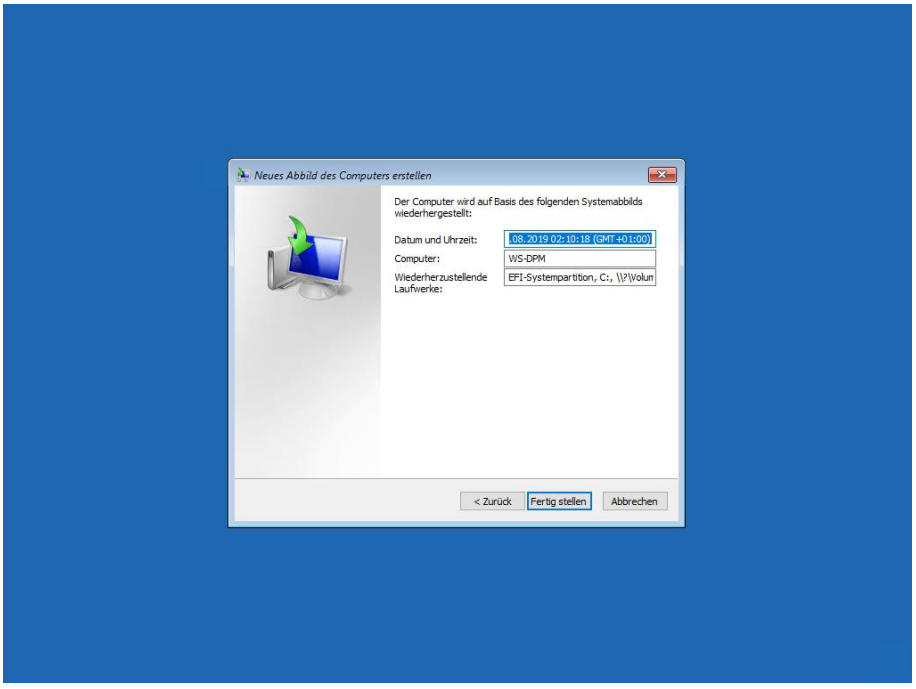


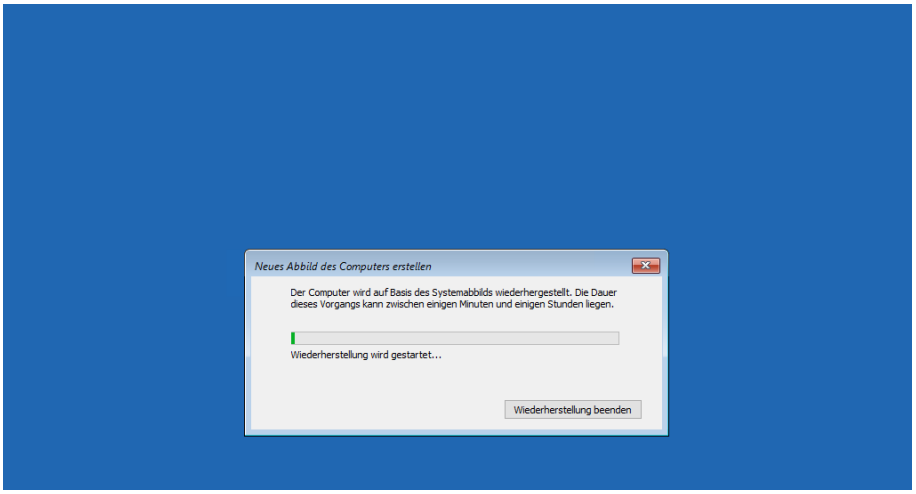
Also nehme ich den Benutzer aus der Gruppe heraus und versuche es erneut. Dieses Mal mit Erfolg:



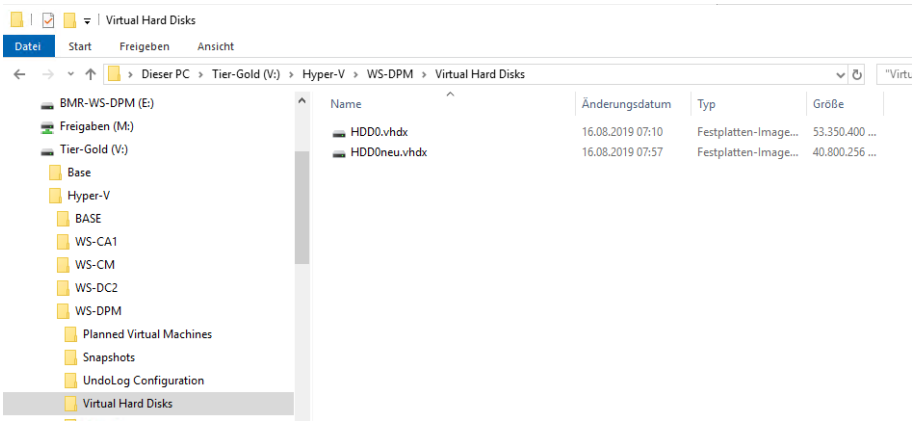



Neues Abbild des Computers erstellen
Weitere Wiederherstellungsoptionen auswählen
Datenträger formatieren und neu partitionieren
Wählen Sie diese Option, um vorhandene Partitionen zu löschen und alle Datenträger auf diesem Computer entsprechend dem Layout des Systemabbilds neu zu formatieren.
Datenträger ausschließen...
Wenn Sie die obigen Optionen nicht auswählen können, lässt sich das Problem möglicherweise durch Installation der Treiber für die wiederhergestellten Datenträger beheben.
Treiber installieren...
Erweitert...
< Zurück
Weiter >
Abbrechen

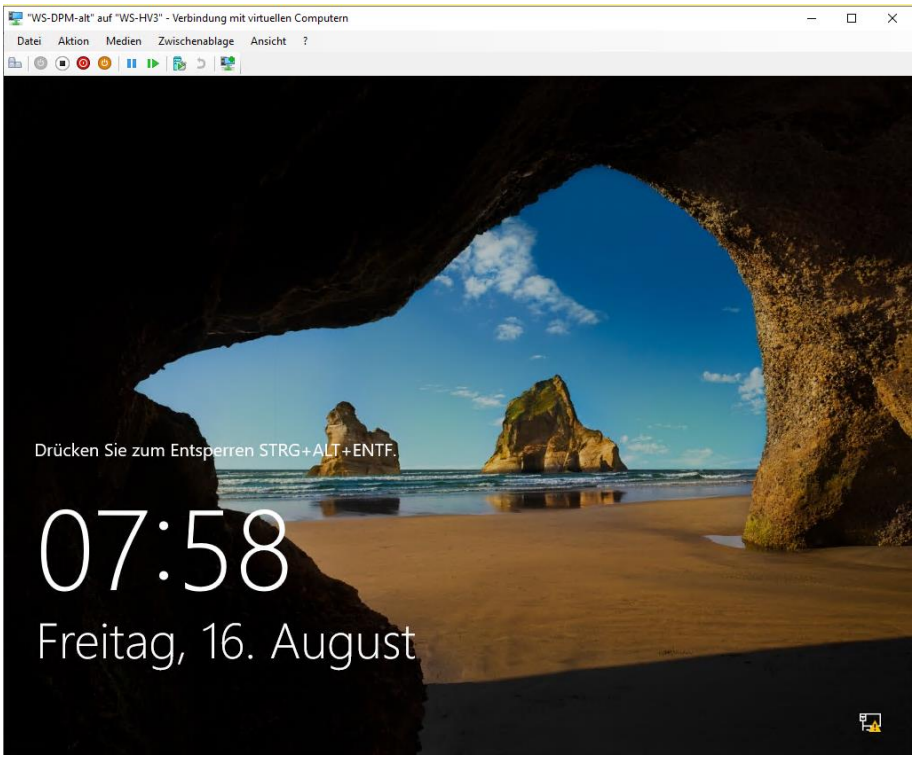

Neues Abbild des Computers erstellen
Der Computer wird auf Basis des folgenden Systemabbilds wiederhergestellt:
Datum und Uhrzeit:
08.2019 02:10:18 (GMT+01:00)
Computer:
WS-DPM
Wiederherzustellende Laufwerke:
EFI-Systempartition, C:, \\?\Volum
< Zurück
Fertig stellen
Abbrechen


Neues Abbild des Computers erstellen
Der Computer wird auf Basis des Systemabbilds wiederhergestellt. Die Dauer dieses Vorgangs kann zwischen einigen Minuten und einigen Stunden liegen.
Wiederherstellung wird gestartet...
Wiederherstellung beenden

Die Wiederherstellung läuft. Im Hyper-V beobachte ich das Anwachsen der neuen VHDX:



Nach einigen Minuten ist das System wieder online:



Hier sieht man, wie wichtig regelmäßige Wiederherstellungen in der Produktion sind! Stellt euch dieses Szenario mal mit einem wichtigen Produktionssystem vor! Wenn dann der Stresspegel nach oben schnellt, wird der Erfolg der Recovery gefährdet sein! Bei meiner nächsten Test-Recovery hätte ich diese Fehlkonfiguration bemerkt und völlig stressfrei korrigiert.

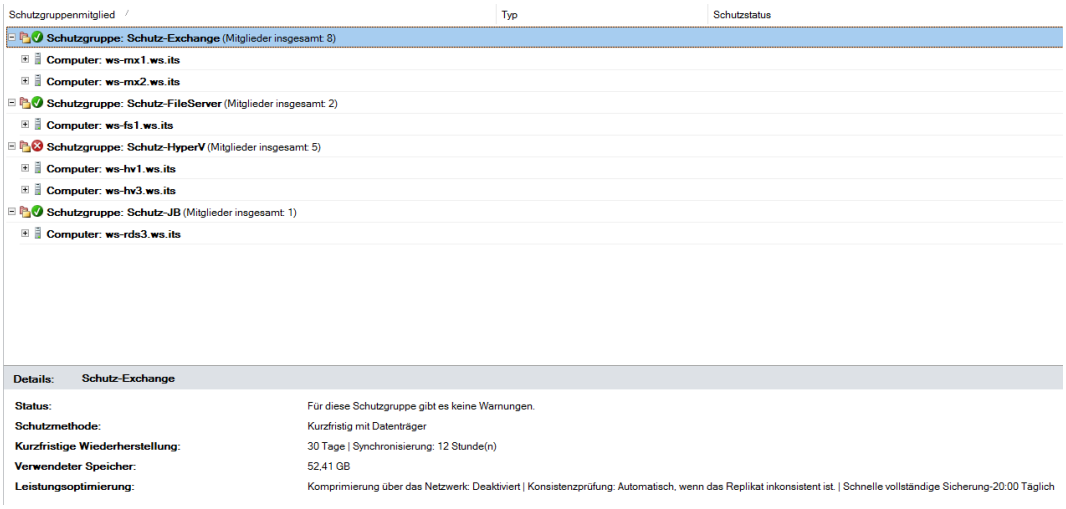
Zwei Bemerkungen noch am Rande:

- Ich spreche Kunden und Kursteilnehmer regelmäßig auf Recovery-Versuche an. Oft höre ich, dass diese in Testumgebungen ausgeführt werden. Ich bin kein Fan dieser Vorgehensweise. Eine Testumgebung wird niemals das Original wiederspiegeln können. Diese Infrastrukturen sind meist idealisierte und minimierte Umgebungen ohne reale Anforderungen. Führt die Tests besser in der Produktion aus.
- Wie das geht? Genauso, wie ich eben wiederhergestellt habe: ich suche mir ein System heraus. In den allermeisten Fällen ist das eine VM. Diese wird (in der Wartungszeit) heruntergefahren und bekommt eine neue virtuelle Festplatte. Dann starte ich die Recovery. Wenn diese abgeschlossen ist, dann kann die VM entweder weiterbetrieben werden oder sie wird heruntergefahren und die alte Festplatte wird wieder eingebaut. Hierfür sind gute Kenntnisse des Services in der VM erforderlich. Aber die sind im Recovery-Fall immer wichtig! Und auch reale Hosts können getestet werden: entweder auf Reserve-Hardware oder in einer leeren VM (P2V).

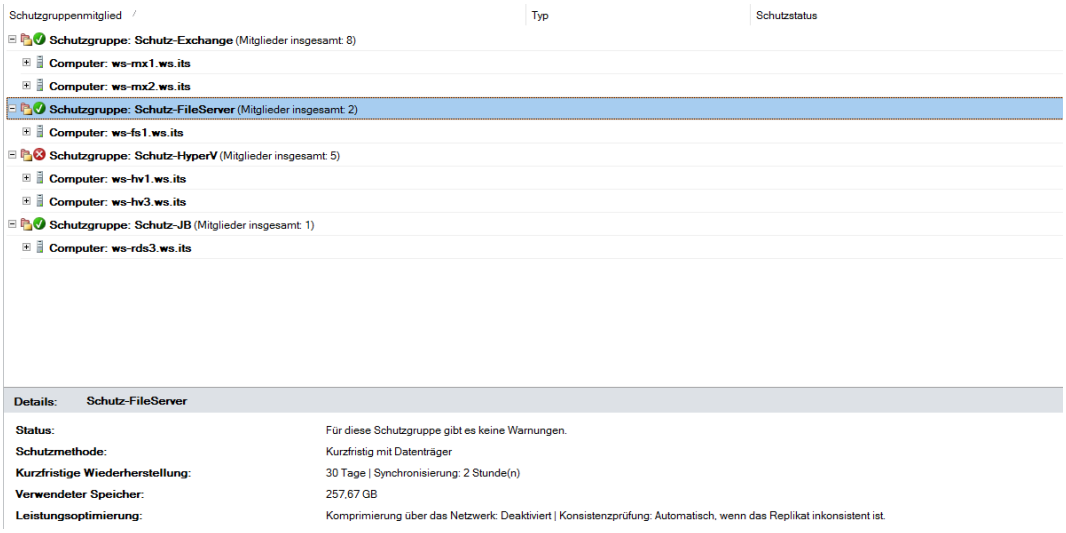
Dokumentation der aktuellen Sicherung und Entfernung der alten Agents (2. Versuch)

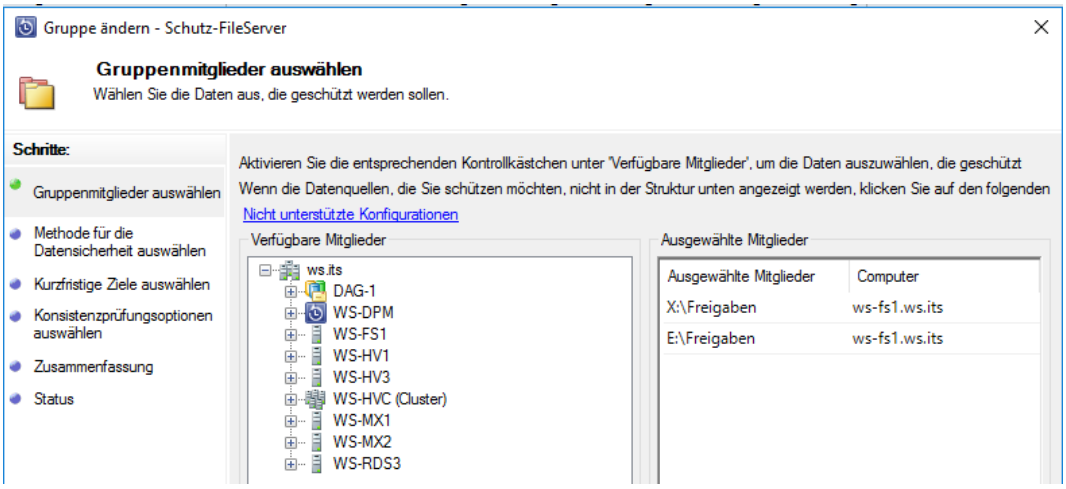
Nun kann ich die bestehenden Sicherungsaufgaben erfassen und dokumentieren. Diese habe ich nach dem Typ der zu sichernden Daten definiert.

Die erste Schutzgruppe sichert meine Exchange-Server-Datenbanken:

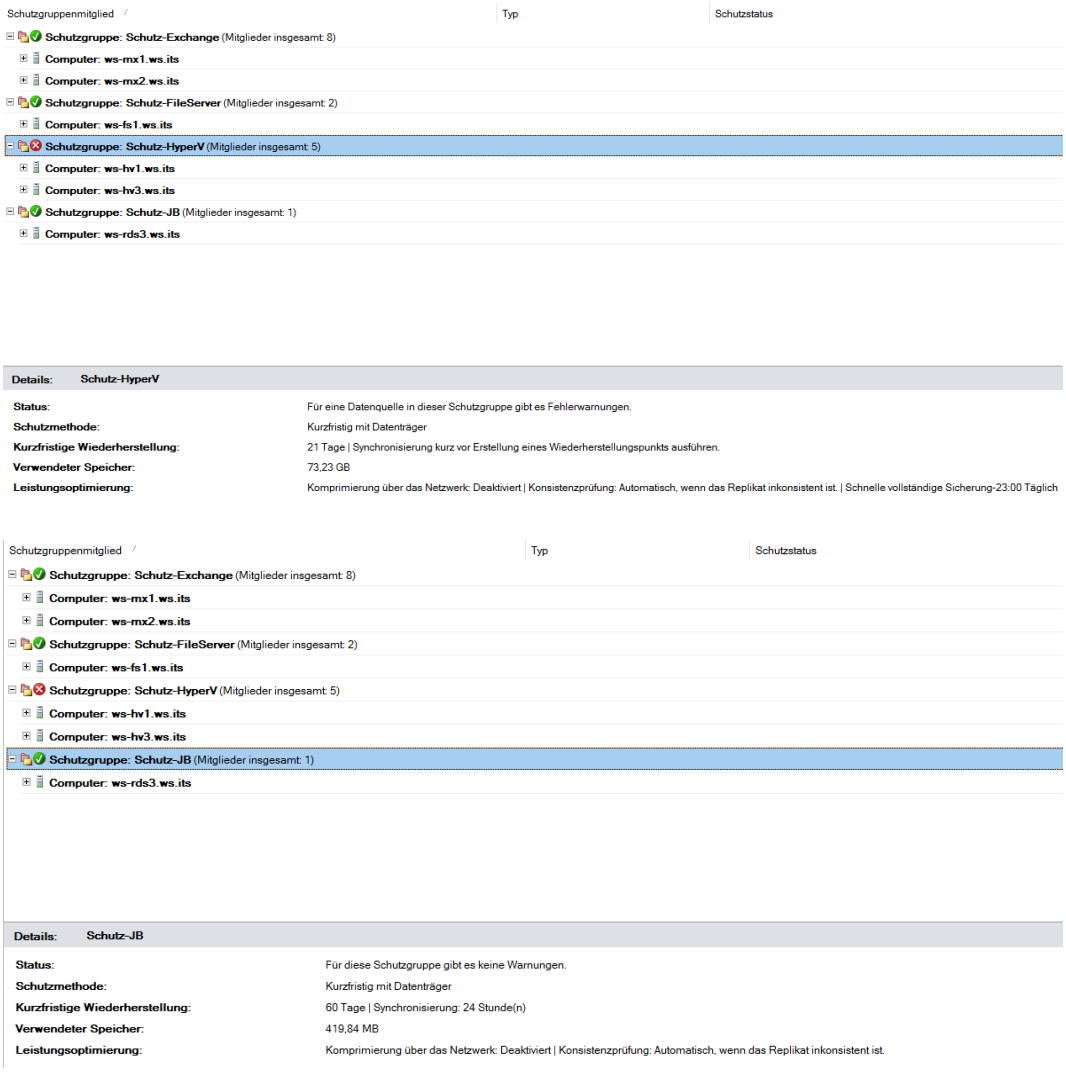


Die 2. schützt meine Fileservices:

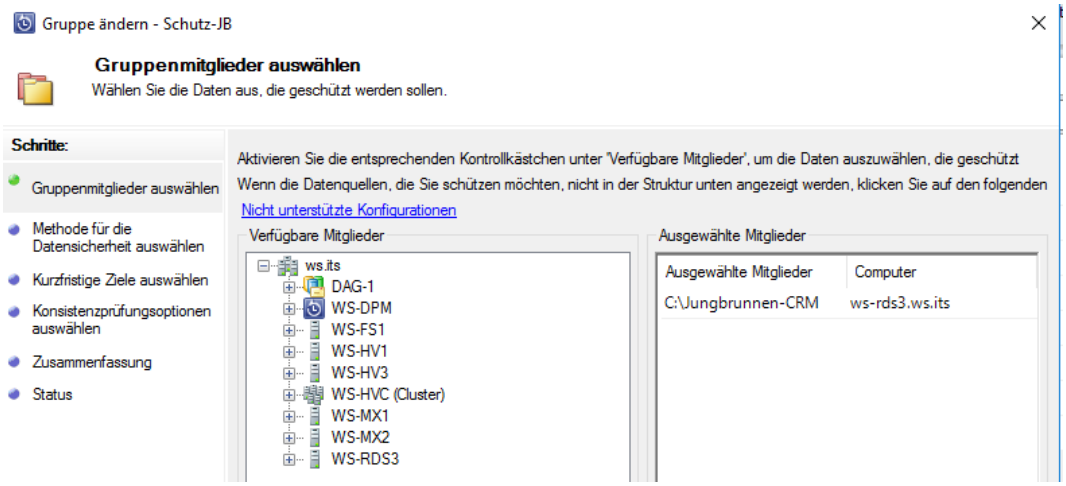




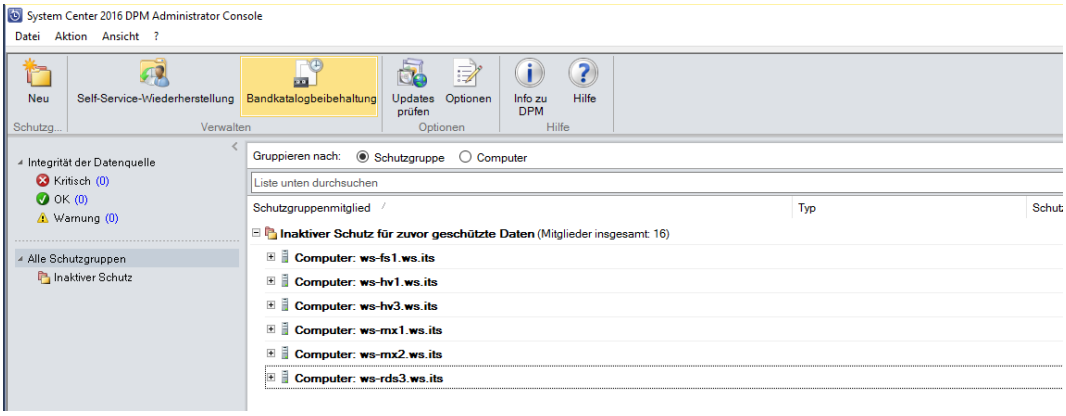
In der 3. sichere ich alle VMs, die ich nicht mit der Windows -Serversicherung intern erfassen kann – also meine Linux-Systeme:



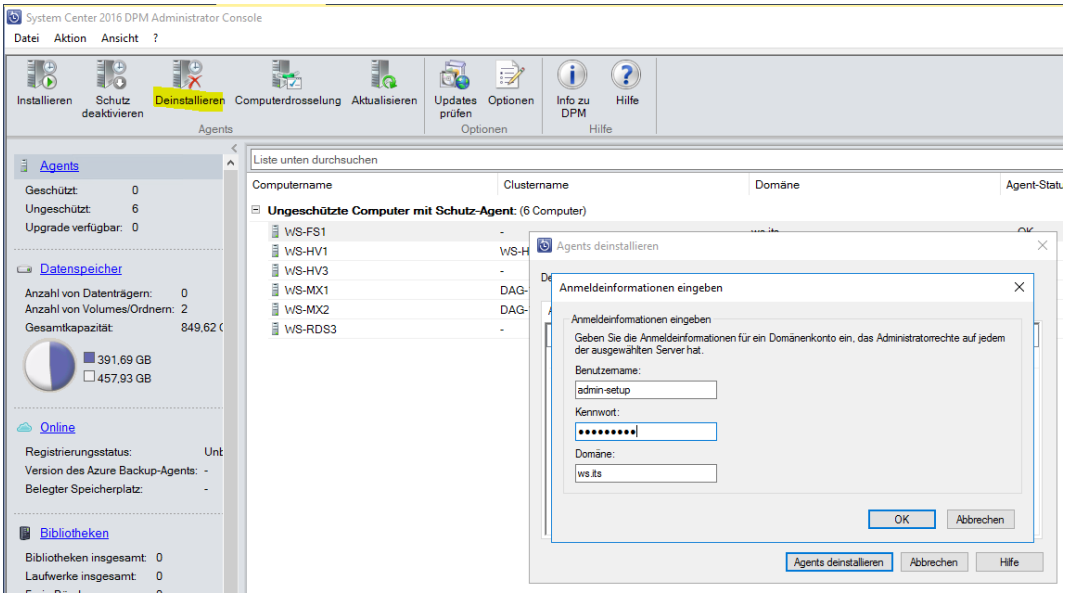
Die 4. Gruppe ist etwas spezieller. Hier sichere ich standortübergreifend eine Anwendung meines anderen Geschäfts:

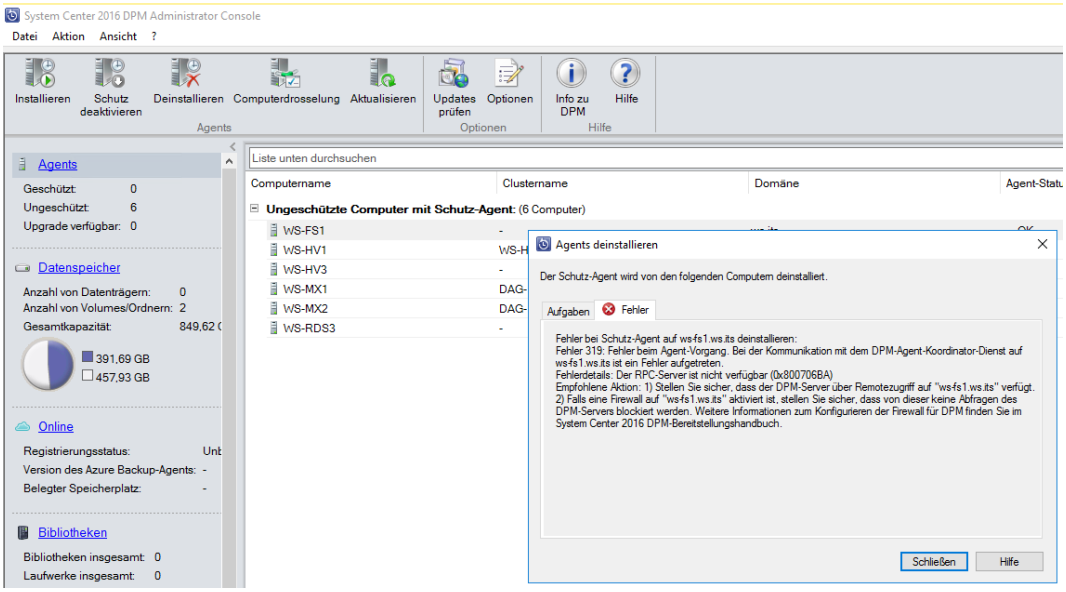


Die Sicherungen werden auf den Quellservern über dort installierte Agents erstellt. Diese Agents sind mit DPM 2019 nicht kompatibel. Da ich nicht abschätzen kann, ob es bei deren Neuinstallation zu Problemen kommt, werde ich sie jetzt deinstallieren. Das lässt der DPM 2016 aber nur zu, wenn die Agents keine zugewiesenen Sicherungsaufgaben mehr haben. Also muss ich die Schutzgruppen zuerst löschen:

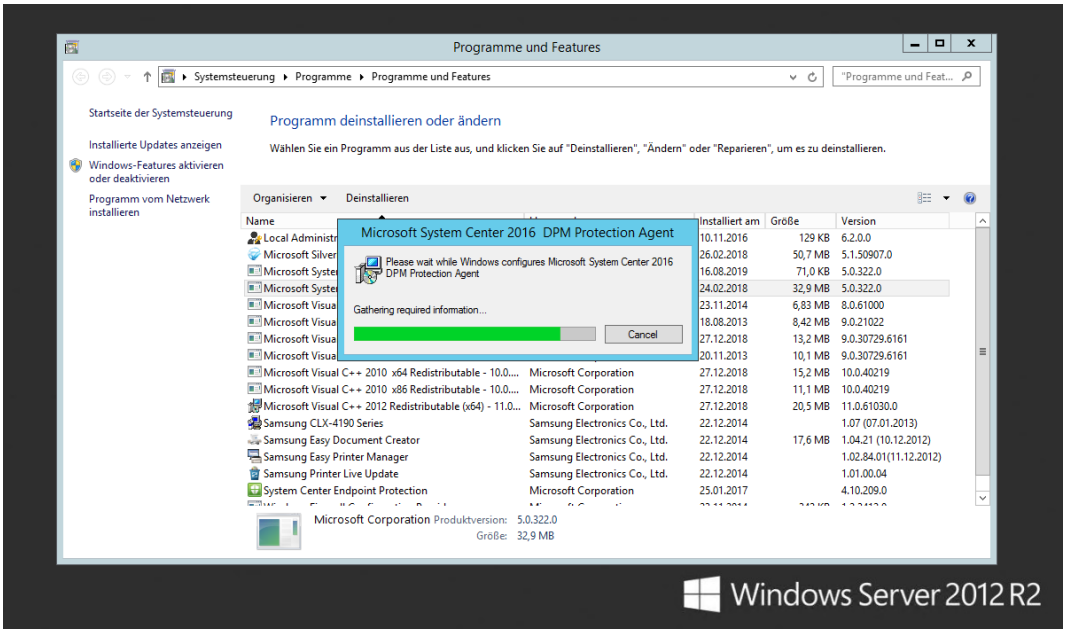


Nun deinstalliere ich die Agents:





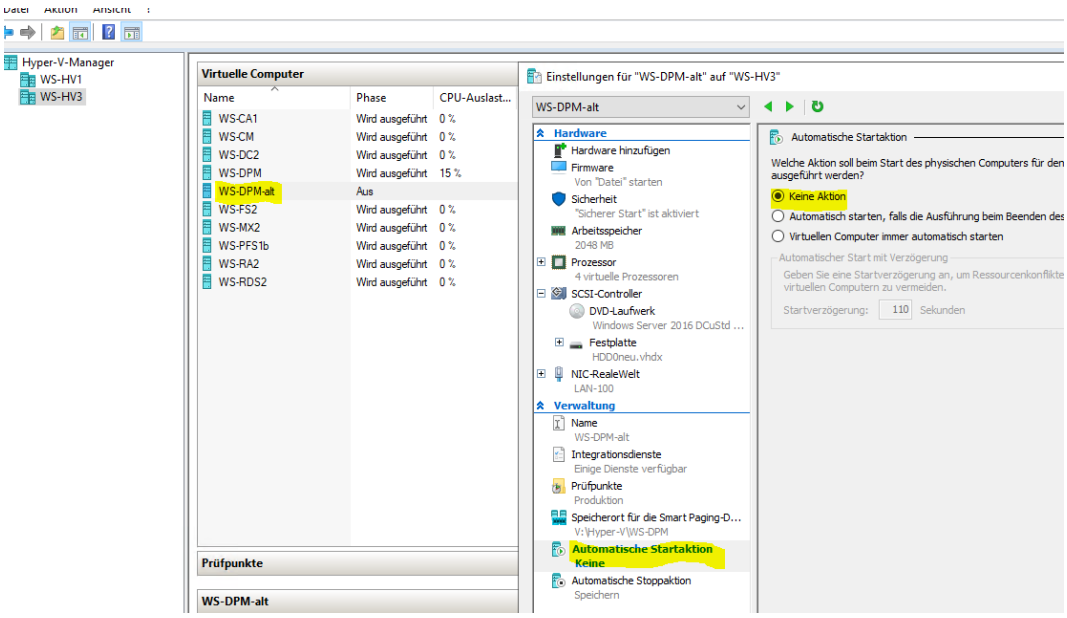
Oder auch nicht. Na gut. Dann eben lokal auf den Quellservern:



Auf dem Server sind noch einige Aufgaben und Scripte vorhanden, die den Zustand der Datensicherung überwachen sollen. Diese exportiere ich auf mein AdminShare.

Abschaltung des DPM 2016

Und nun kann ich den alten DPM-Server abschalten. Die VM hebe ich noch etwas auf, falls ich noch was vergessen habe. Zudem könnte ich über den alten DPM immer noch auf die bisherige Datensicherung zugreifen. Aber das System soll nicht mehr automatisch mitstarten. Daher benenne ich die VM im Hyper-V-Manager um und verhindere den automatischen Start:



Im Monitoring pausiere ich die Sensoren, damit mein Handy Ruhe gibt.

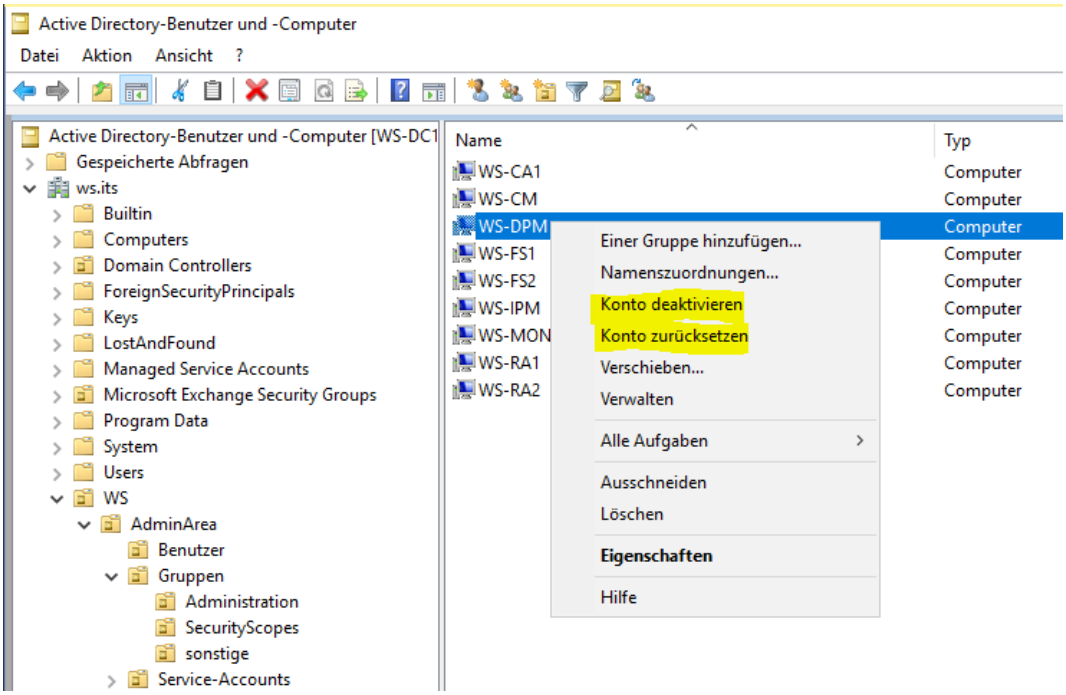
Neuinstallation vom Server WS-DPM

neue VM erstellen

Nun habe ich eine grüne (Backup-)Wiese. Es wird Zeit für den neuen DPM 2019. In der realen Welt würde ich diese Schritte natürlich vorziehen, damit die alte Sicherung parallel noch weiterläuft.

Für den neuen DPM 2019 erstelle ich eine VM mit Windows Server 2019 als Basis. Das Image war bereits vorbereitet und es startet im OOBE-Modus. Nach wenigen Eingaben war das Betriebssystem bereit.

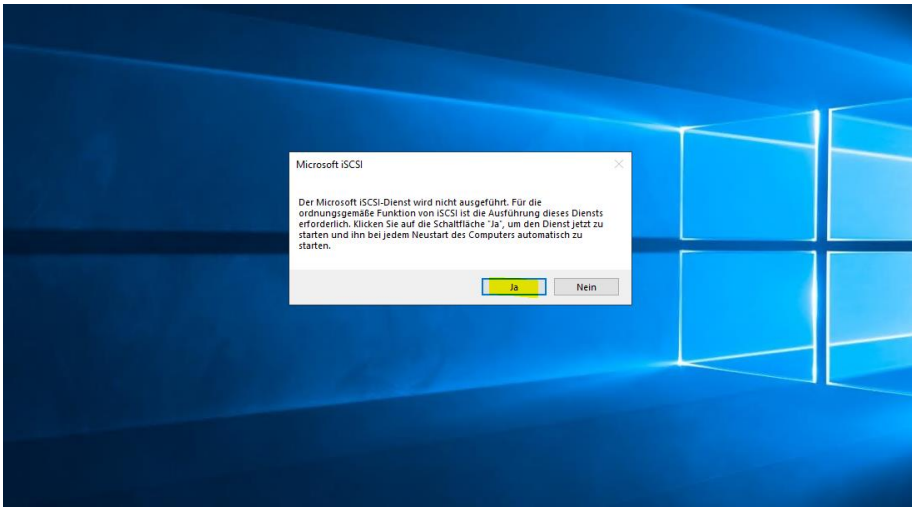
Ich möchte gerne den Namen des Servers wiederverwenden. Daher setze ich das Konto im AD zurück und benenne den neuen Server in WS-DPM um. Danach darf er der Domain beitreten:

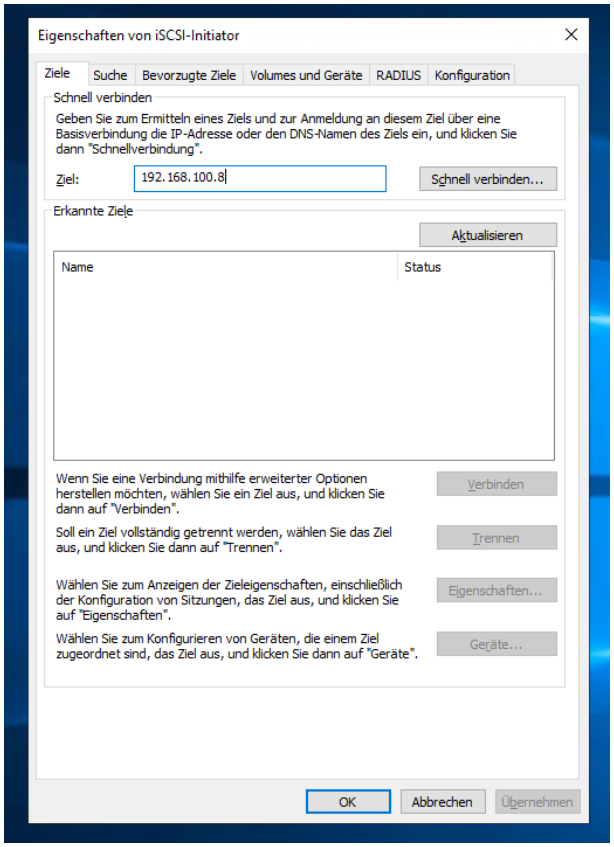


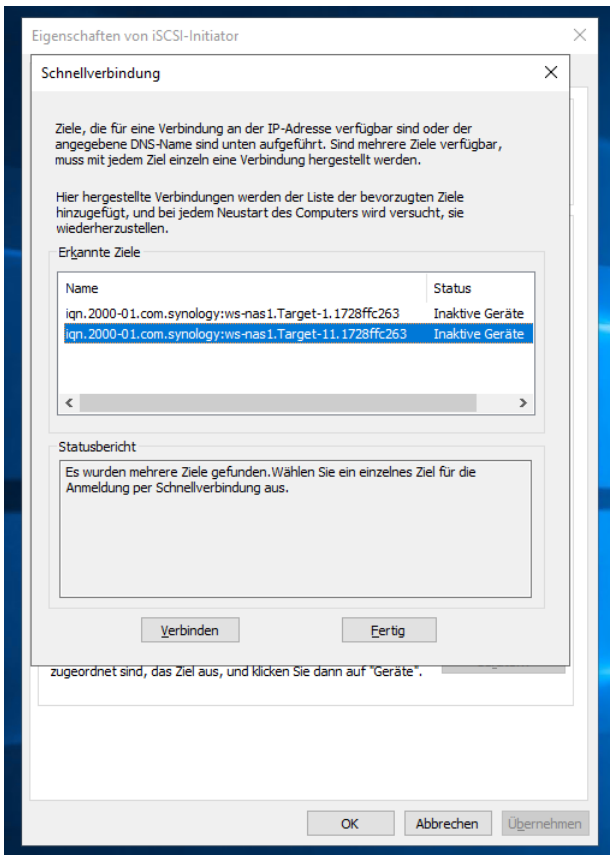
Auch die IPv4 möchte ich weiterverwenden und trage die 192.168.100.5/24 ein. Damit erspare ich mir die Anpassung der Firewall-Regeln.

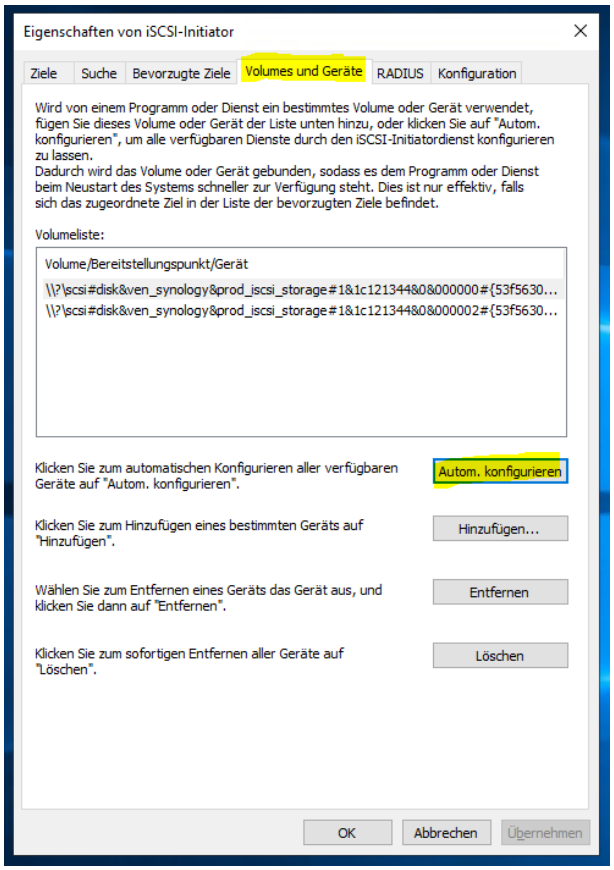
Noch ein kurzer Blick auf die Windows Updates: hier ist alles UpToDate, da ich das Image erst erstellt hatte.

Nun bekommt der Server Zugriff auf die Datenträger für die Sicherung. Diese werden über iSCSI von einer NAS bereitgestellt. Ich starte die iSCSI-Konfiguration:

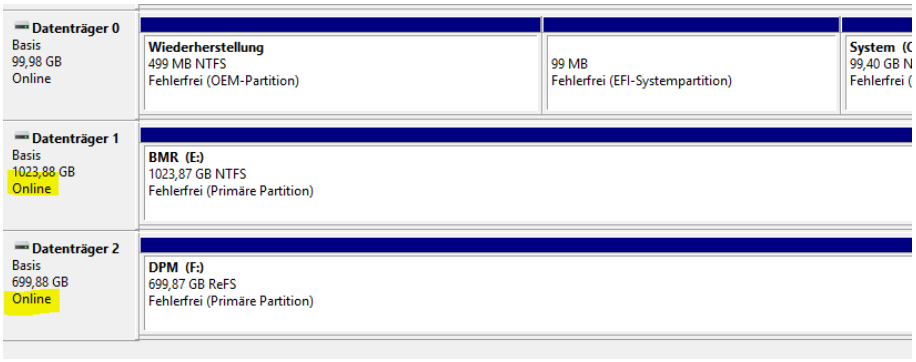



Eigenschaften von iSCSI-Initiator
Ziele
Suche
Bevorzugte Ziele
Volumes und Geräte
RADIUS
Konfiguration
Schnell verbinden
Geben Sie zum Ermitteln eines Ziels und zur Anmeldung an diesem Ziel über eine Basisverbindung die IP-Adresse oder den DNS-Namen des Ziels ein, und klicken Sie dann "Schnellverbindung".
Ziel:
192.168.100.8
Schnell verbinden...
Erkannte Ziele
Aktualisieren
Name
Status
Wenn Sie eine Verbindung mithilfe erweiterter Optionen herstellen möchten, wählen Sie ein Ziel aus, und klicken Sie dann auf "Verbinden".
Verbinden
Soll ein Ziel vollständig getrennt werden, wählen Sie das Ziel aus, und klicken Sie dann auf "Trennen".
Trennen
Wählen Sie zum Anzeigen der Zieleigenschaften, einschließlich der Konfiguration von Sitzungen, das Ziel aus, und klicken Sie auf "Eigenschaften".
Eigenschaften...
Wählen Sie zum Konfigurieren von Geräten, die einem Ziel zugeordnet sind, das Ziel aus, und klicken Sie dann auf "Geräte".
Geräte...
OK
Abbrechen
Übernehmen


Eigenschaften von iSCSI-Initiator
Schnellverbindung
Ziele, die für eine Verbindung an der IP-Adresse verfügbar sind oder der angegebene DNS-Name sind unten aufgeführt. Sind mehrere Ziele verfügbar, muss mit jedem Ziel einzeln eine Verbindung hergestellt werden.
Hier hergestellte Verbindungen werden der Liste der bevorzugten Ziele hinzugefügt, und bei jedem Neustart des Computers wird versucht, sie wiederherzustellen.
Erkannte Ziele
Name
Status
iqn.2000-01.com.synology:ws-nas1.Target-1.1728ffc263
Inaktive Geräte
iqn.2000-01.com.synology:ws-nas1.Target-11.1728ffc263
Inaktive Geräte
Statusbericht
Es wurden mehrere Ziele gefunden. Wählen Sie ein einzelnes Ziel für die Anmeldung per Schnellverbindung aus.
Verbinden
Fertig
zugeordnet sind, das Ziel aus, und klicken Sie dann auf "Geräte".
OK
Abbrechen
Übernehmen



Beide Datenträger wurden korrekt eingebunden:

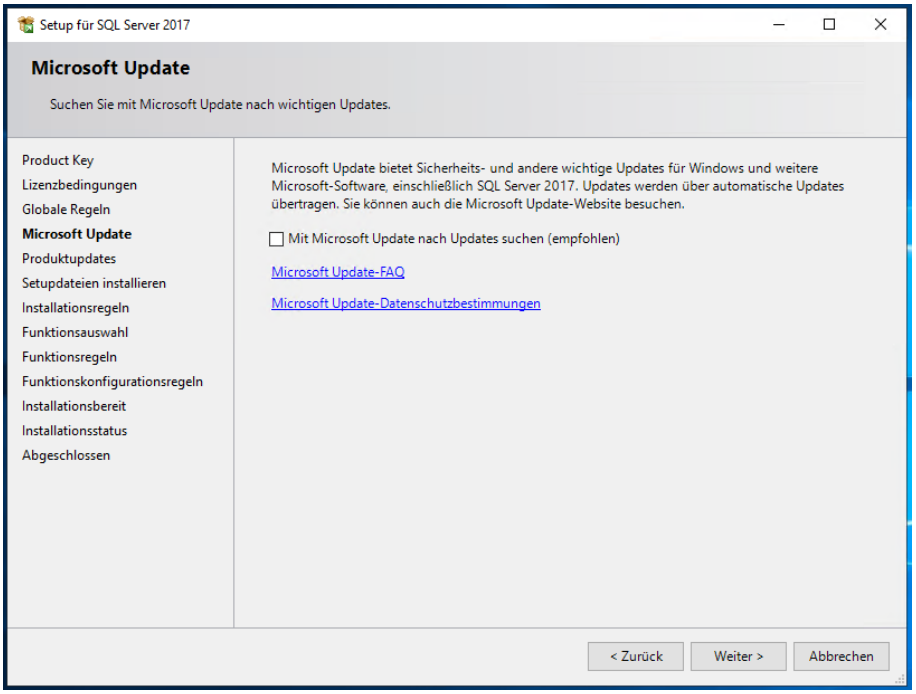


Das Betriebssystem ist nun eingerichtet.

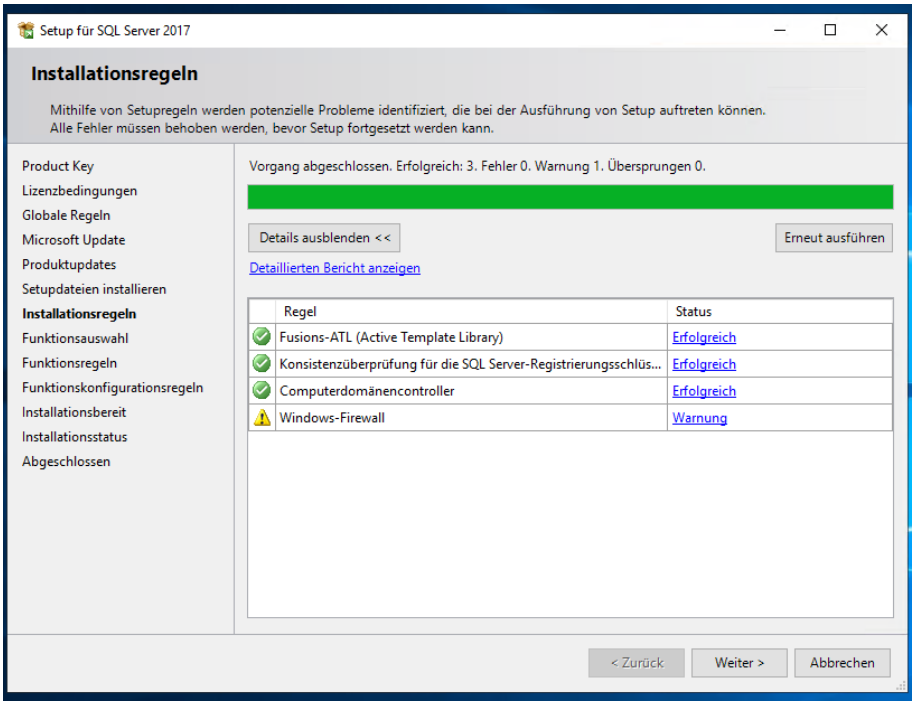
Installation SQL Server 2017

Es fehlt noch ein SQL-Server, den der DPM 2019 für seine Konfigurationen verwenden kann. Diesen installiere ich aus Restore-Gründen lokal: sollte es zu einem Totalausfall meiner Infrastruktur kommen, dann muss ich „nur“ den DPM-Server mit seiner BMR (wie oben gezeigt) recovern und dann habe ich Zugriff auf meine Nutzdatensicherung. 😊

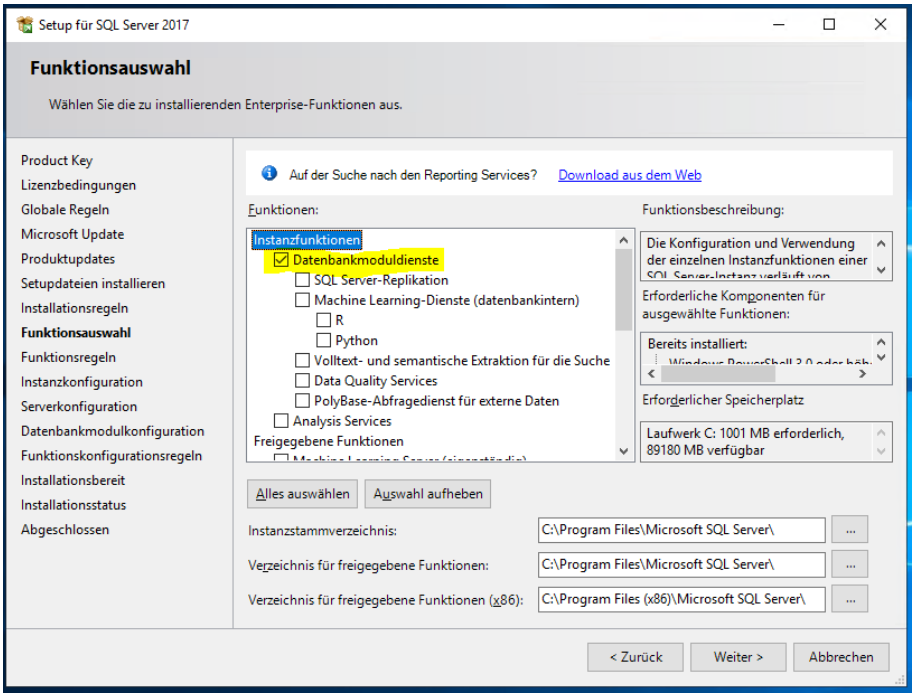
Der SQL-Server soll die Version 2017 verwenden. Ich starte das Setup:



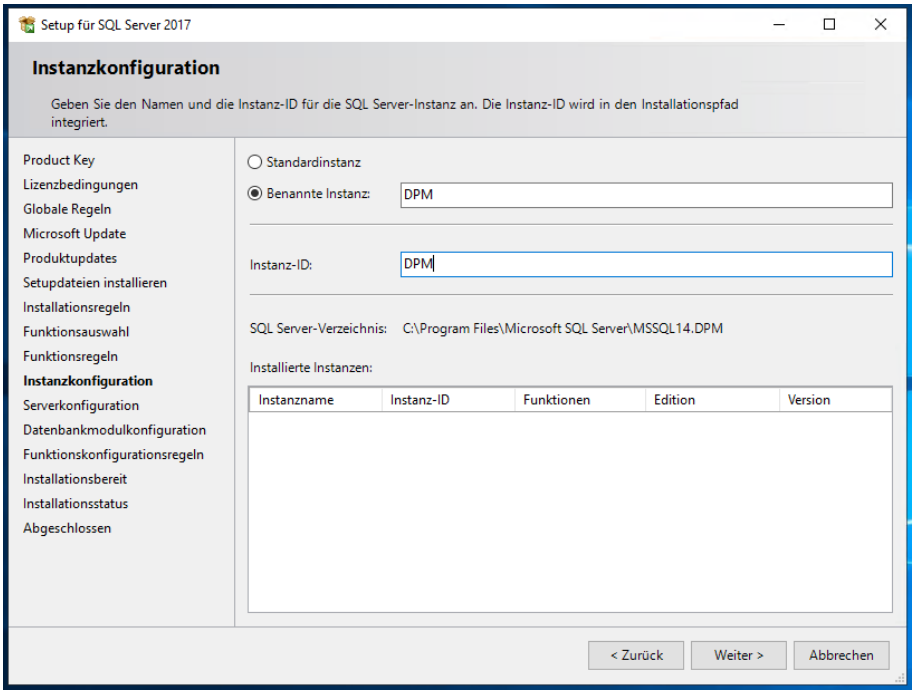
Die Warnung ignoriere ich. Eine Firewall-Ausnahme kann ich später noch erstellen:



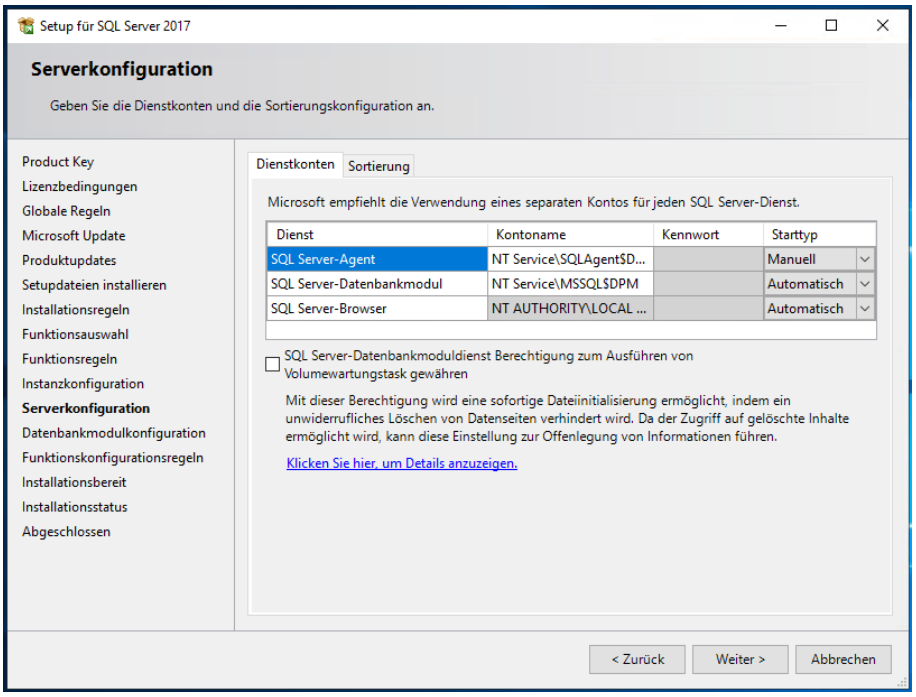
Ich installiere nur die notwendigen Features:



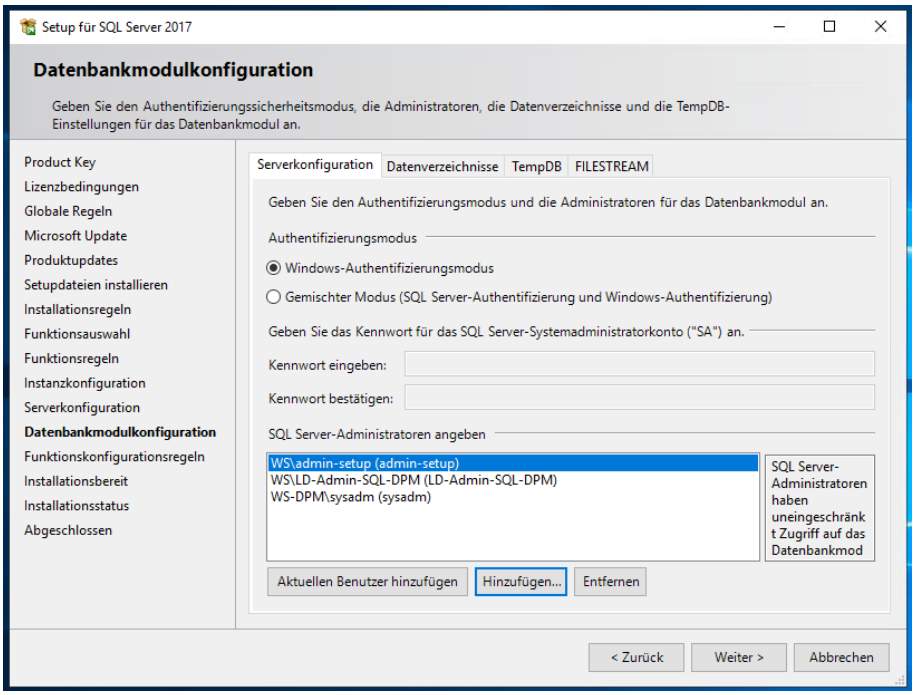
Dazu bekommt die Instanz einen hübschen Namen. Dem DPM kanns egal sein:



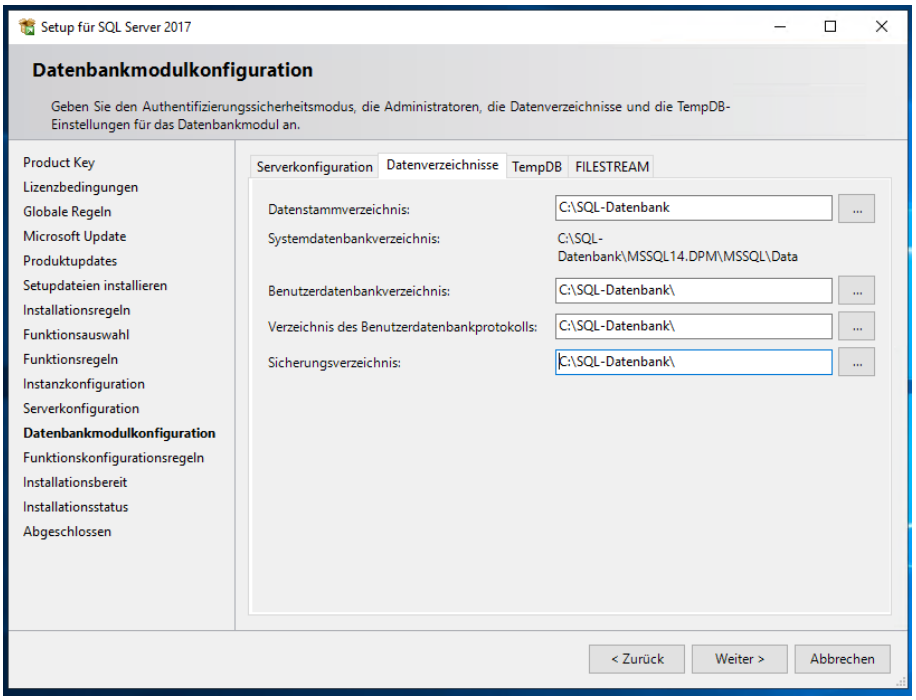
Die Principals der Services lasse ich unverändert. Das kann ich bei Bedarf auch nach dem Setup anpassen:

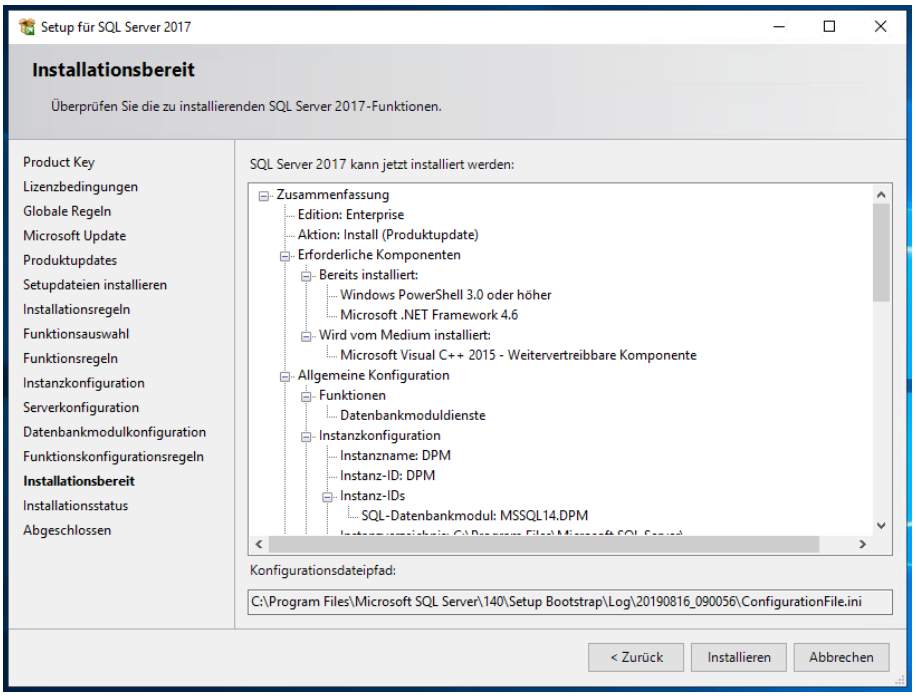


Ganz wichtig ist aber der Zugriff auf die Instanz. Lokale Administratorenrechte genügen seit Langem nicht mehr. Und weiter oben hat man gesehen was passiert. Wie gut, wenn man eine Dokumentation hat. Und passende AD-Gruppen zur Rechtedelegation:

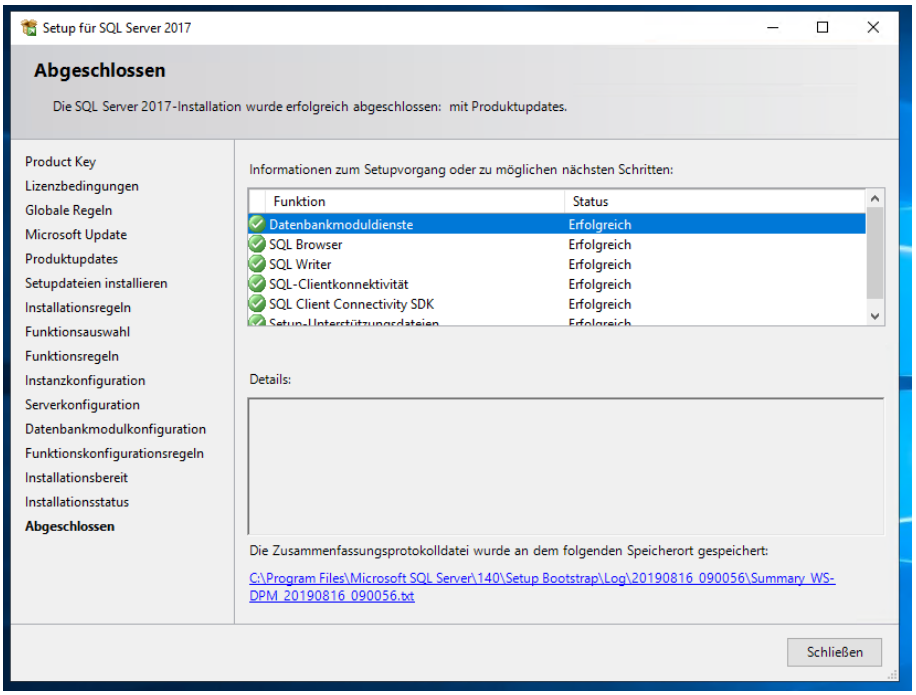


Die Datenbank-Pfade lege ich etwas klarer an:

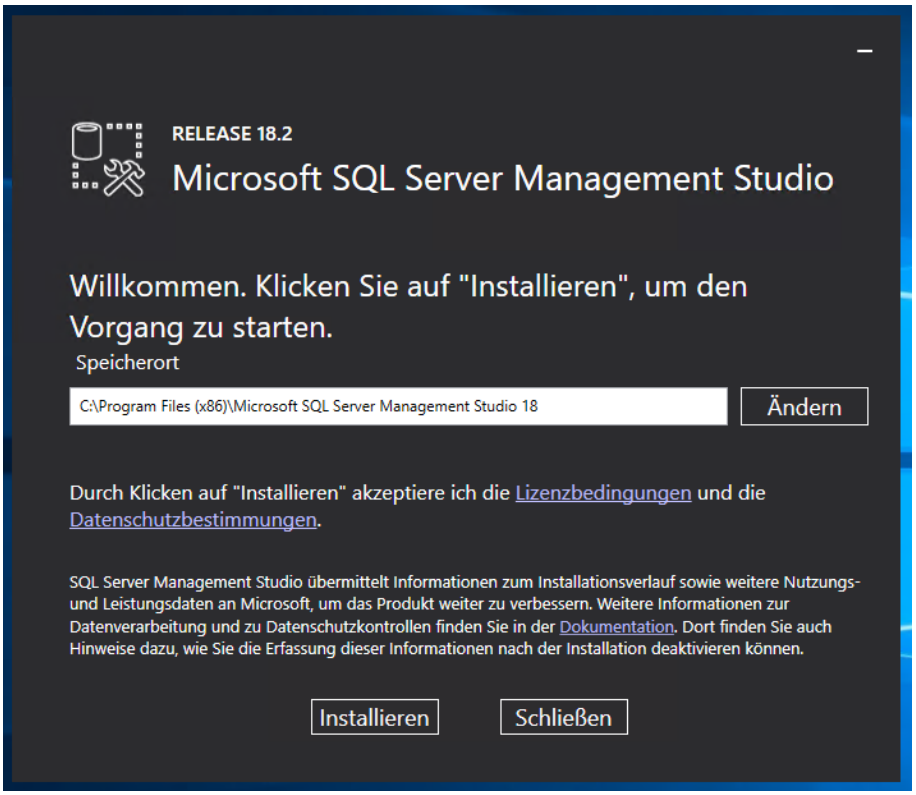


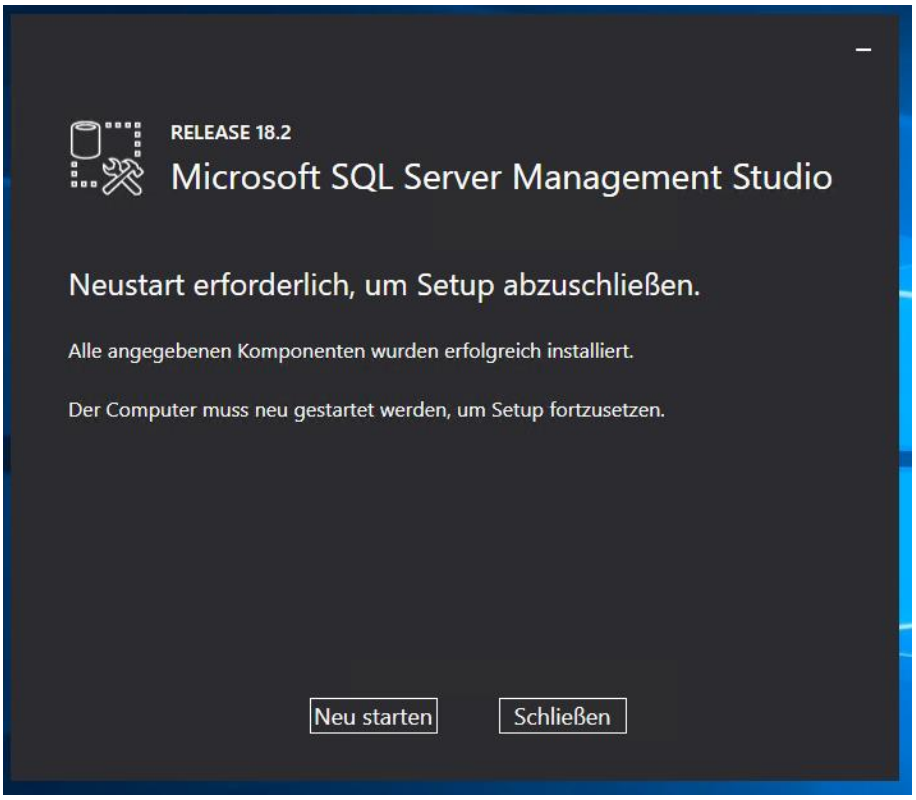


So kann das Setup starten. Und nach wenigen Minuten ist die Instanz bereitgestellt:

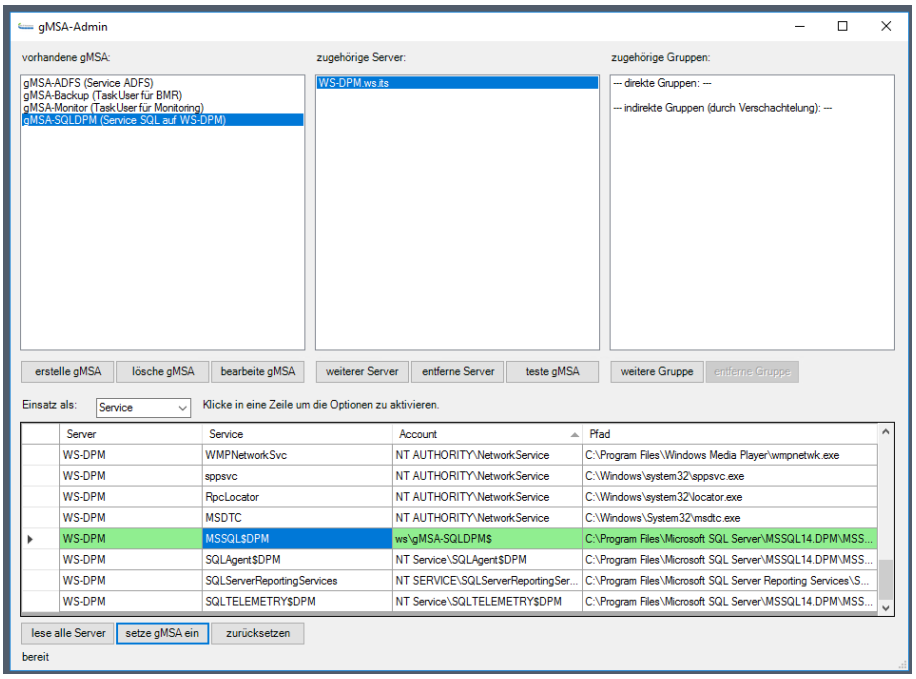


Nun installiere ich noch das SQL-Server Management Studio (SSMS). Dieses soll im Problemfall einen schnellen und komfortablen Datenbankzugriff ermöglichen:

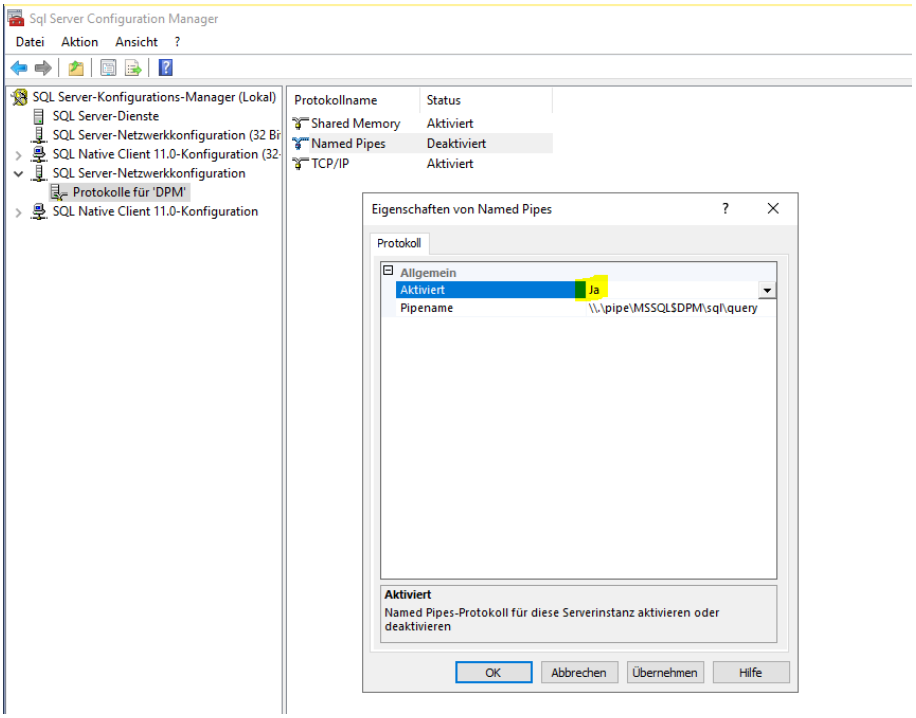




Nach dem Neustart konfiguriere ich nun die Services des SQL-Servers. Im Active Directory habe ich einen Group Managed Service Account (gMSA) eingerichtet, welcher die Instanz betreiben soll. Für die Konfiguration kann nicht die GUI des SQL verwendet werden. Hier hat Microsoft leider nur die PowerShell vorgesehen. Aber vor einiger Zeit habe ich mir eine GUI mit der PowerShell programmiert (die gibt's im Blog von ws-its.de). Mit dieser kann der Account leicht konfiguriert werden:



Nun aktiviere ich noch die Named Pipes, da der DPM die für den Zugriff benötigt:

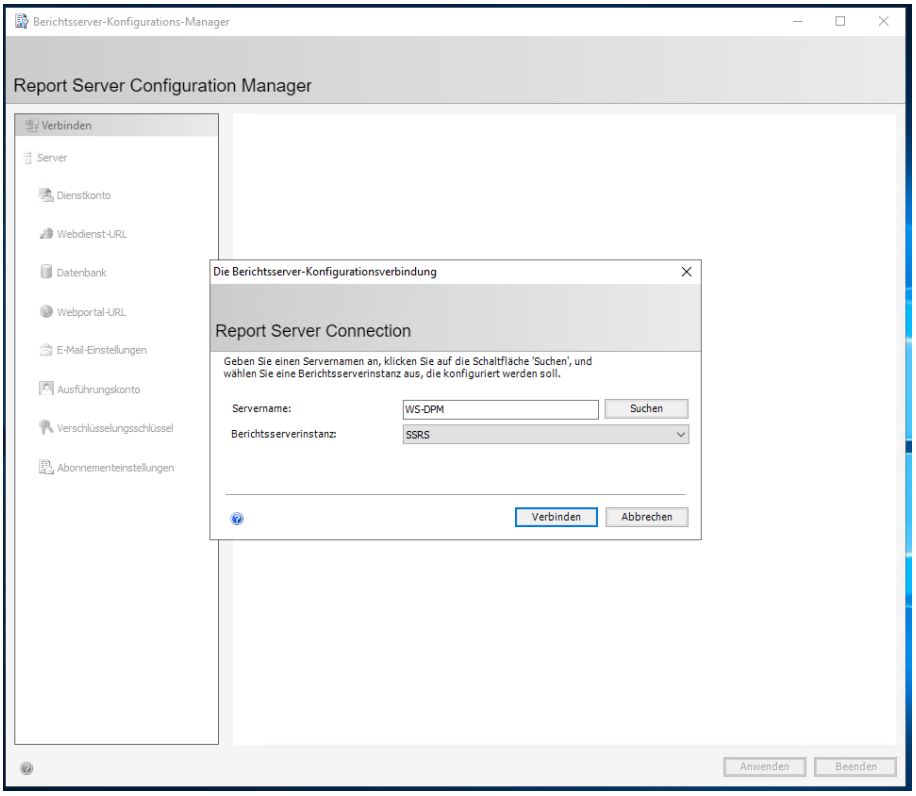


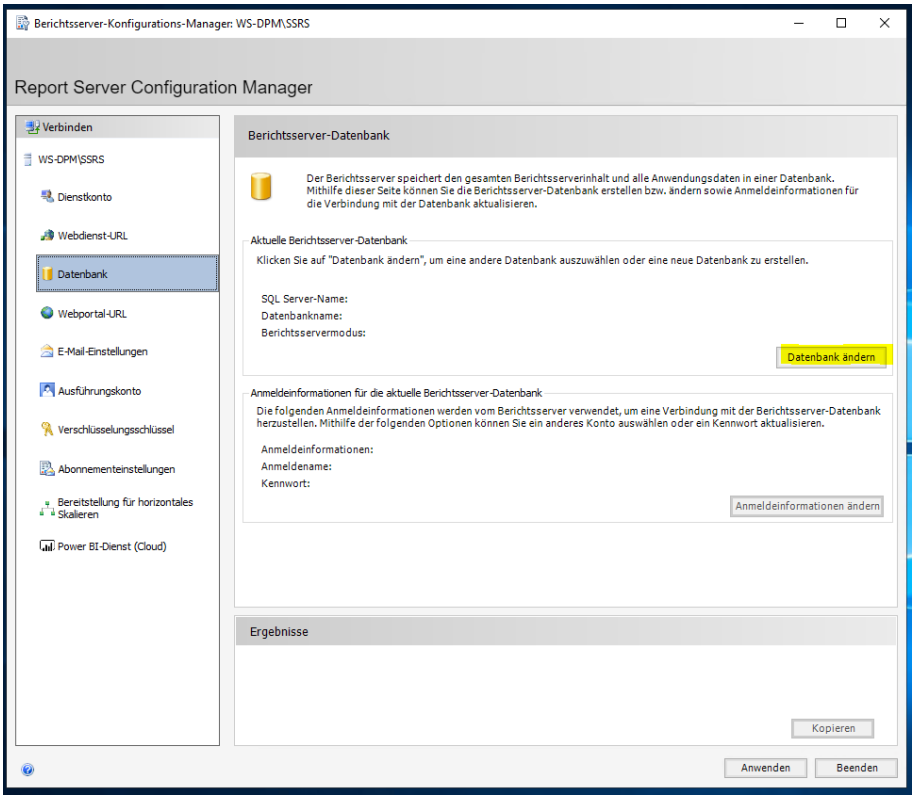
Der DPM 2019 braucht aber auch die Reporting-Services in der Version 2017. Diese werden über ein separates Setup installiert:

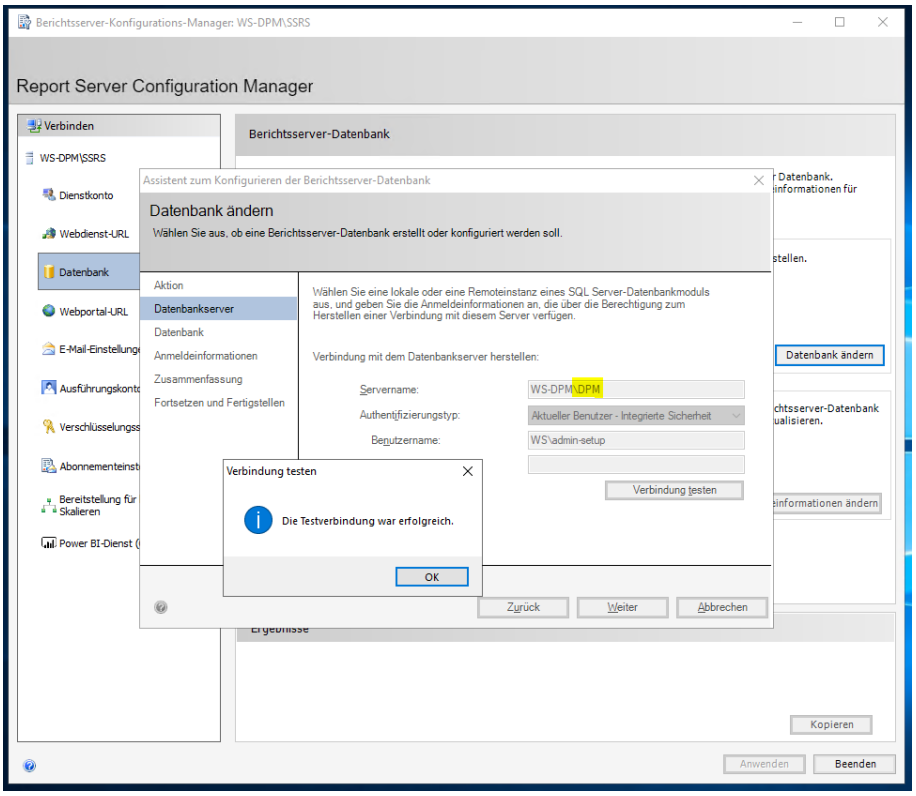

Microsoft SQL Server 2017 Reporting Services
(Oktober 2017)
Datenbankmodul installieren
Sie benötigen eine Instanz des SQL Server-Datenbankmoduls, um die Berichtsserver-Datenbank zu speichern.
Nur Reporting Services installieren
Sie müssen eine Datenbankmodulinstanz auf diesem oder einem anderen Server installieren oder bereits installiert haben.
Weitere Informationen zu unterstützten Datenbankmodulversionen und -editionen
Abbrechen
< Zurück
Weiter >


Microsoft SQL Server 2017 Reporting Services
(Oktober 2017)
Paketfortschritt
Microsoft System CLR Types for SQL Server 2017
Gesamtstatus
Abbrechen

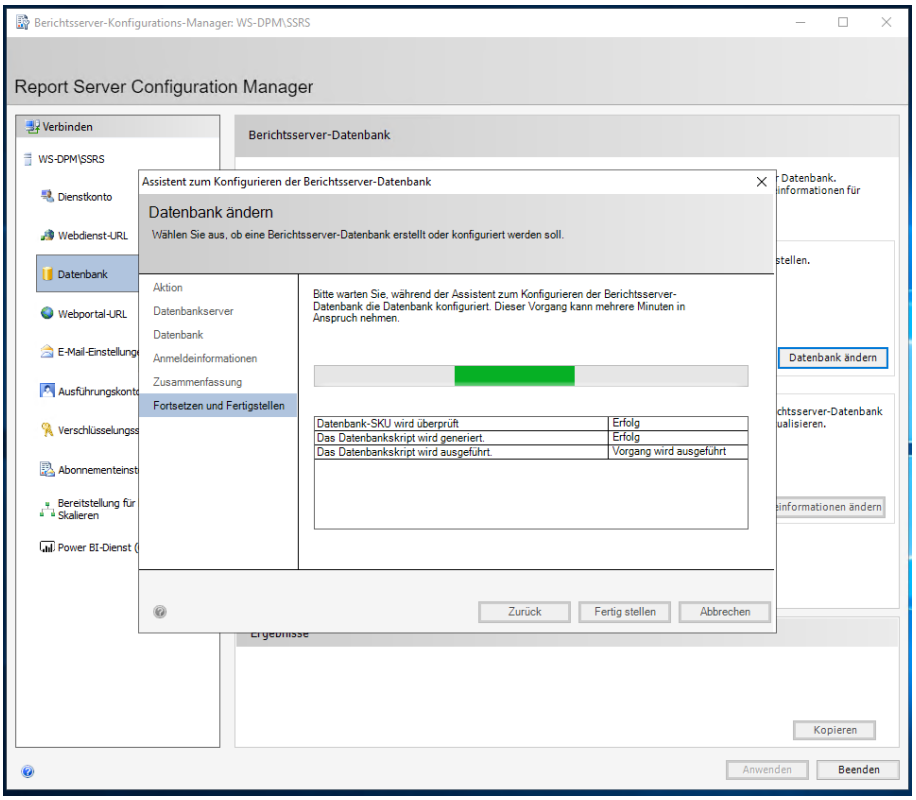
Nach dem Setup benötigt der Reporting Service noch eine Einrichtung. Dafür steht ein eigenes Tool bereit:

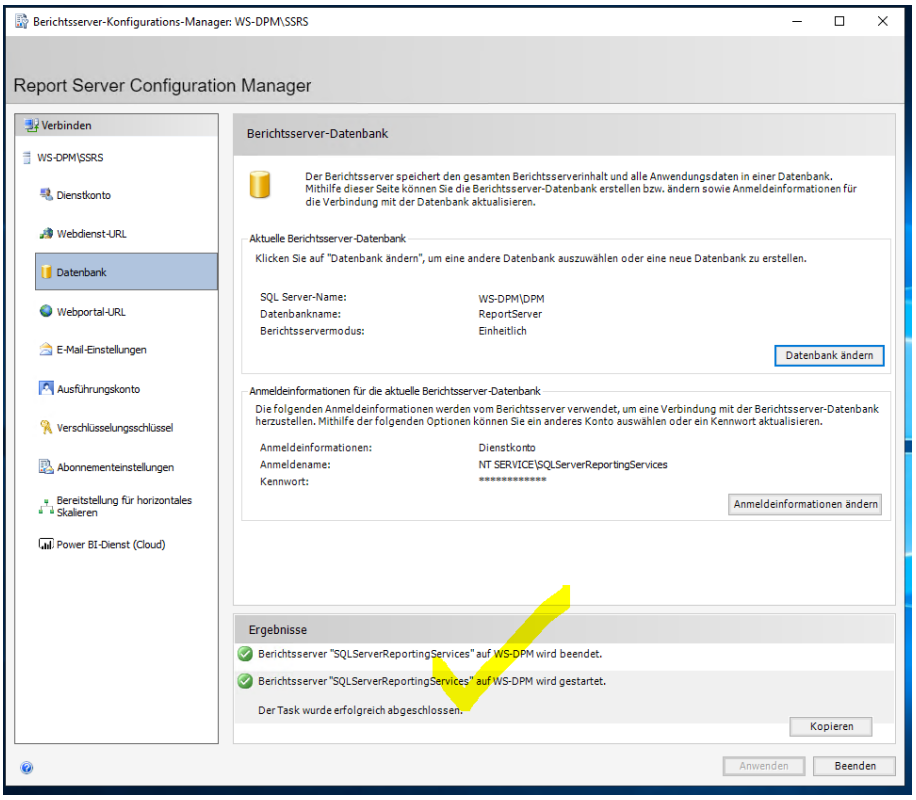






Die weiteren Fragen bestätige ich einfach durch:

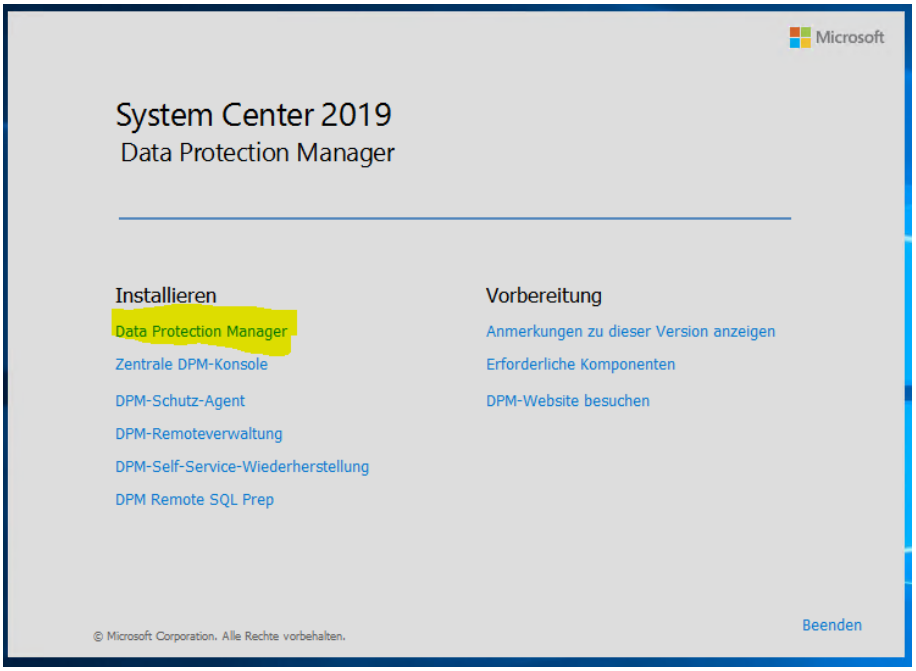


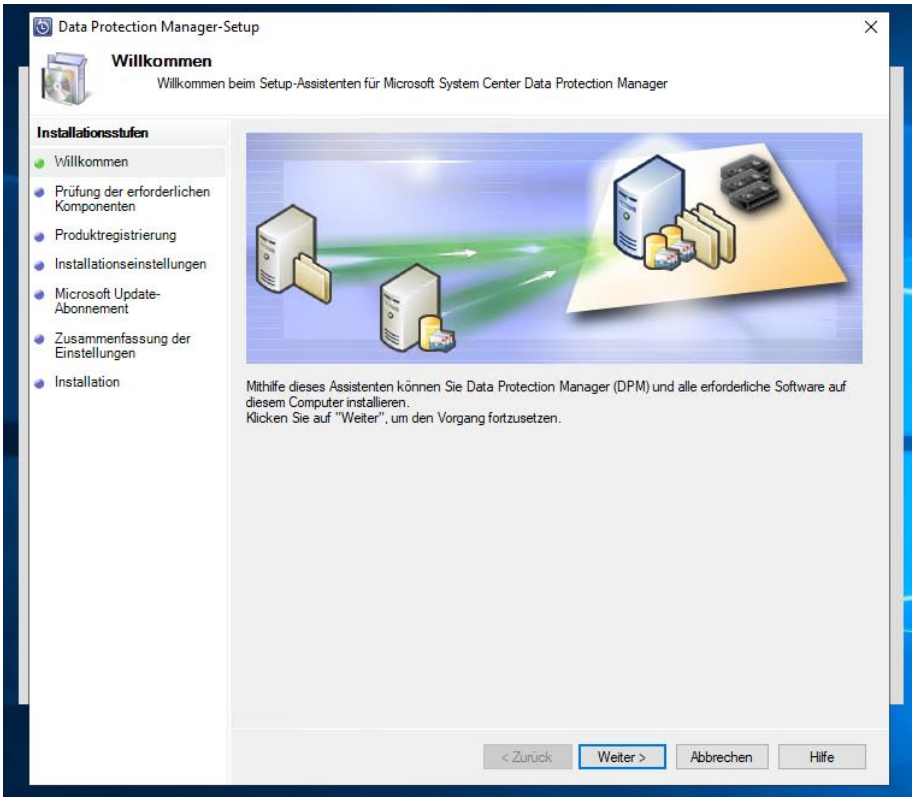


Nun ist der SQL-Server einsatzbereit.

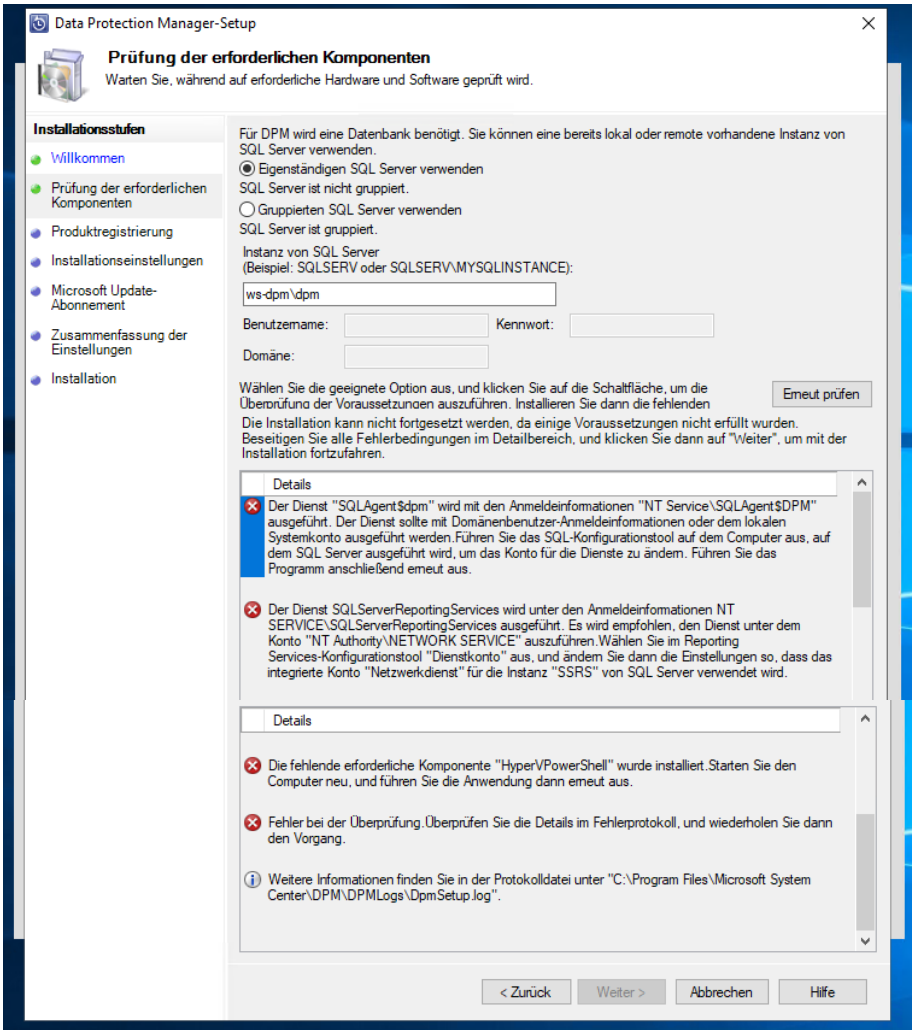
Installation des DPM 2019

Jetzt kann der DPM 2019 installiert werden. Das Setup bietet auch hier eine geführte Installation:

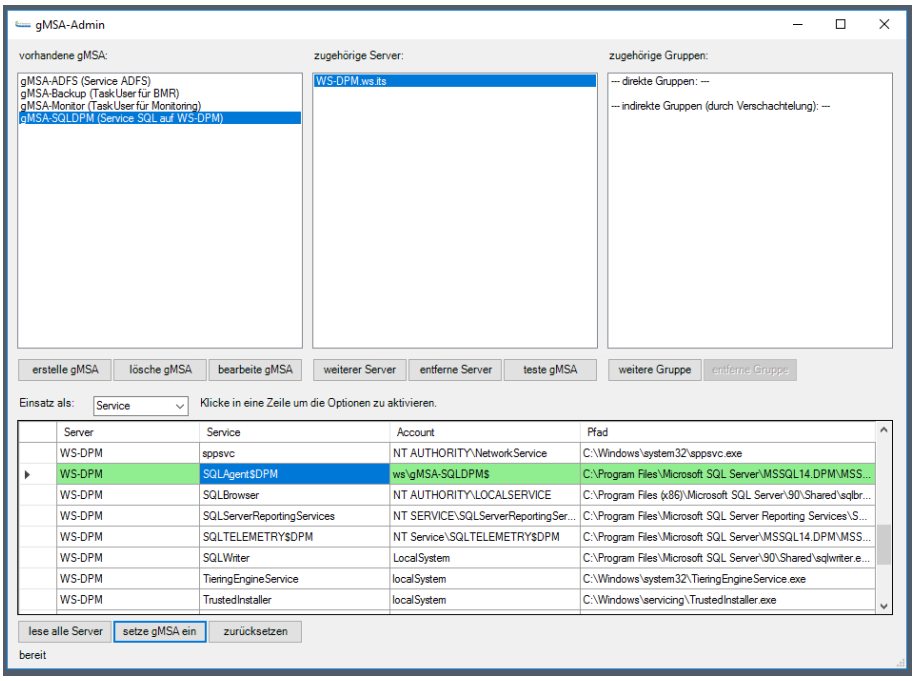




Hier gebe ich den SQL-Server mit seiner Instanz an. Wenn man keine Named Instance installiert hat, genügt der Servername:

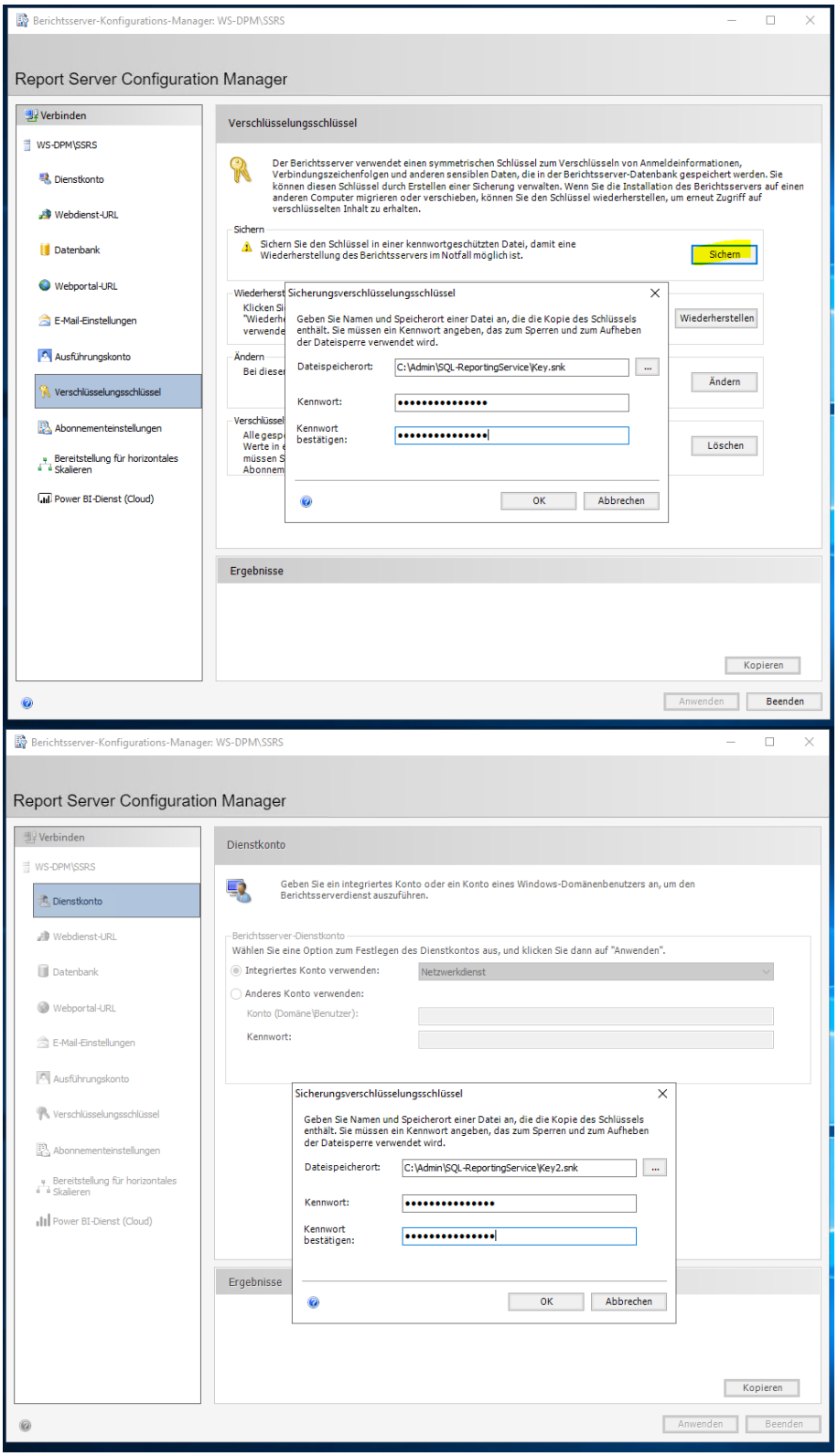


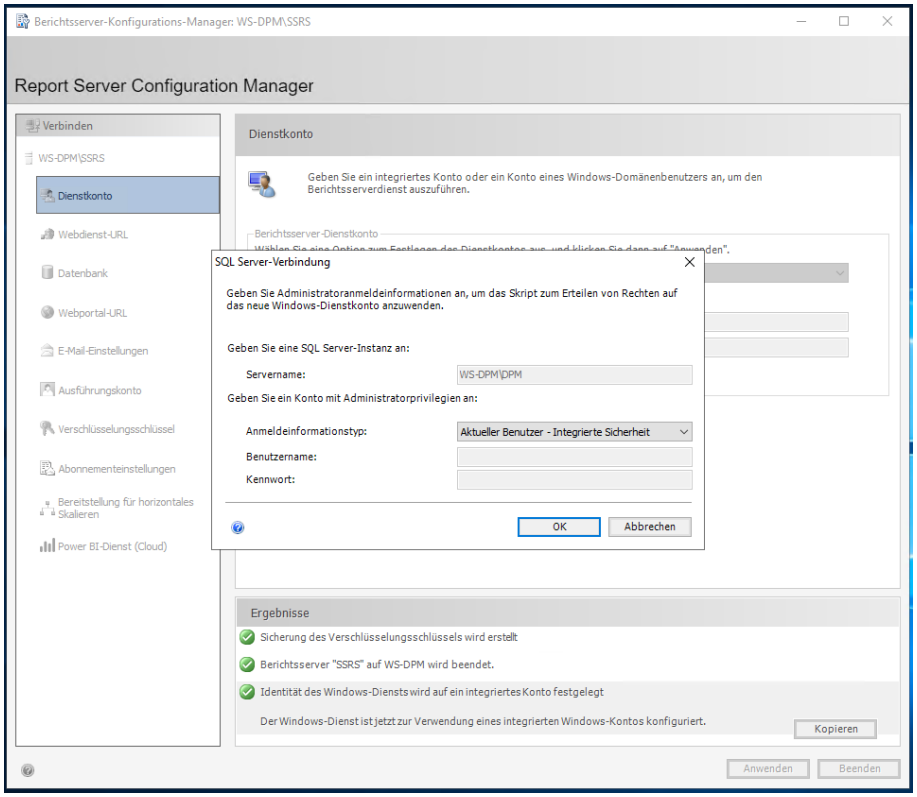
OK, ich hatte meinen gMSA nur für den SQL-Service konfiguriert. Aber der Agent soll diesen auch verwenden. Also starte ich noch einmal meine GUI für die gMSA-Administration (auf meinem DomainController):



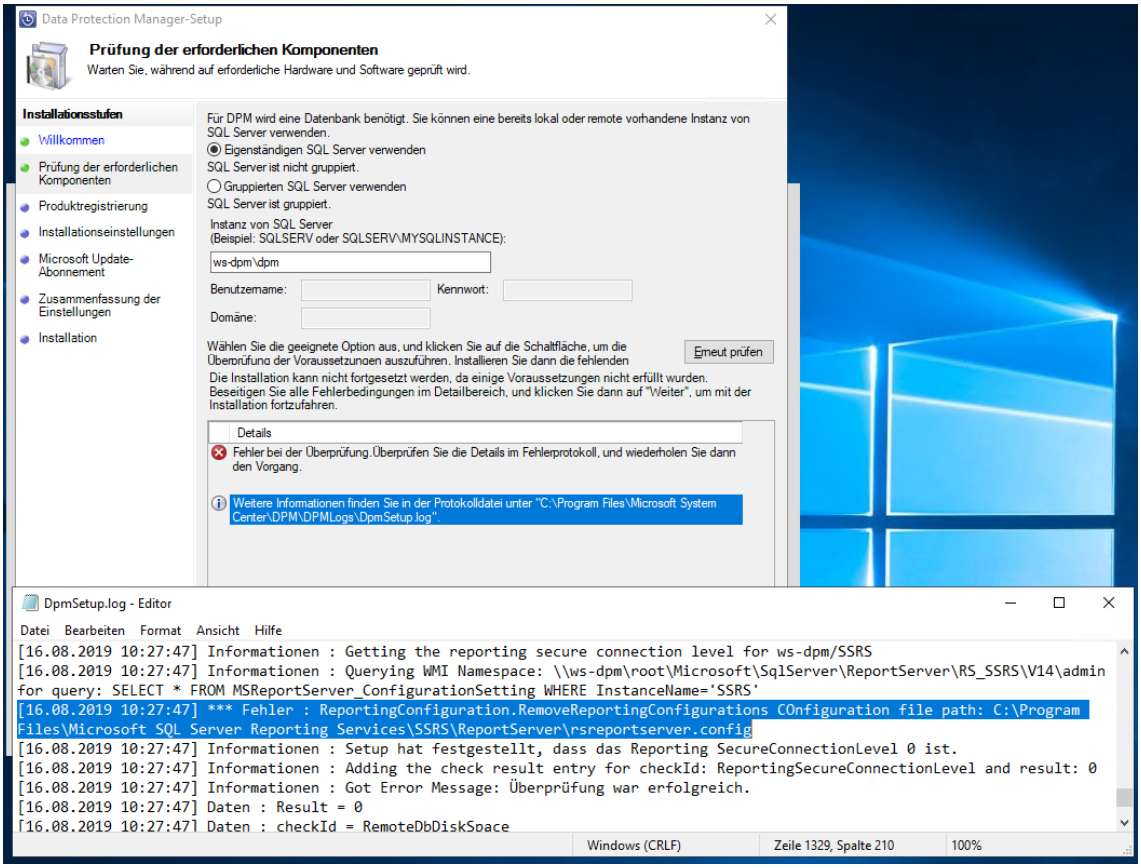
Und natürlich setze ich den SQL-Agentservice auf AutoStart.

Aber auch das Dienstkonto der Reporting-Services benötigt eine Anpassung. Da es schon konfiguriert ist muss ich die Verschlüsselungsschlüssel der RS-Datenbank sichern. Das geht wieder in der RS-Konfigurationsoberfläche:

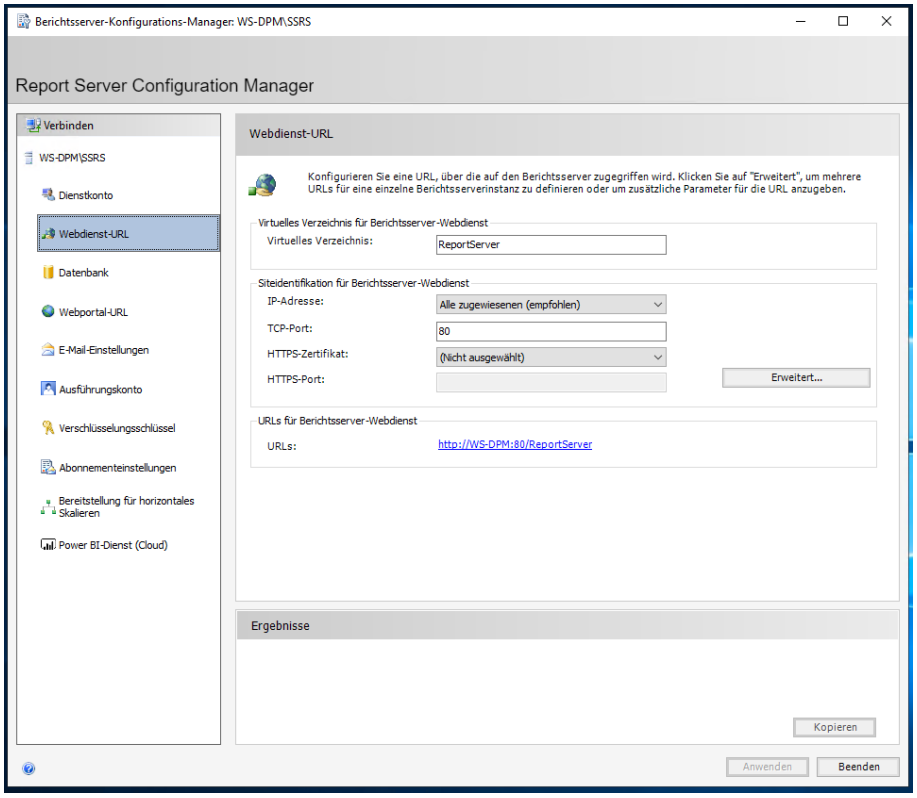


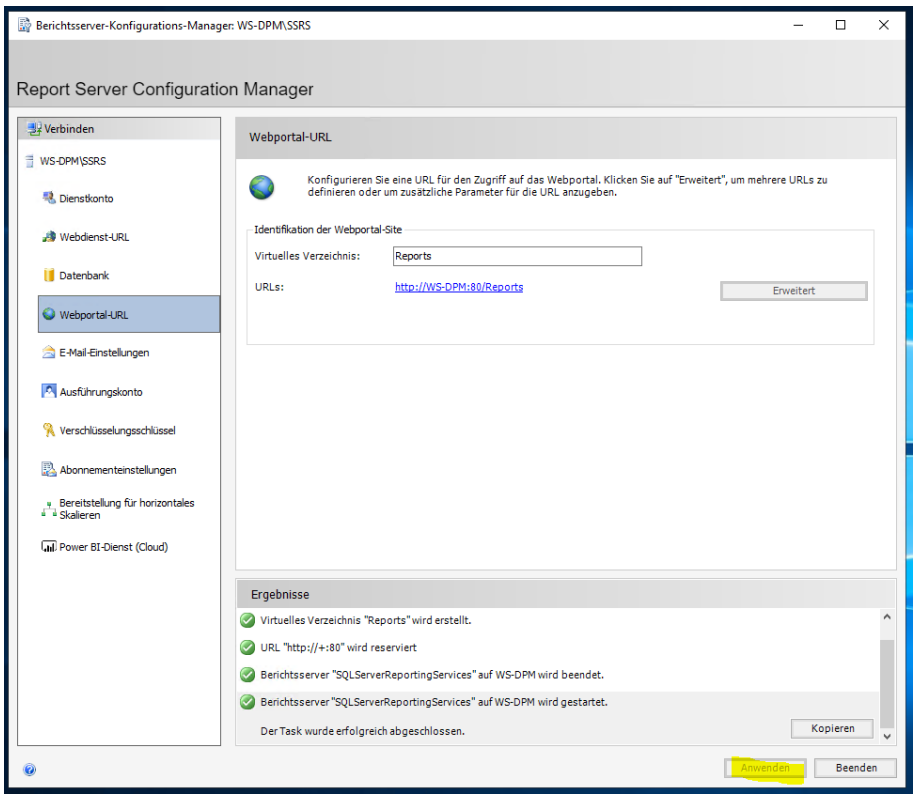


Nach einem Neustart sind alle SQL-Services passend konfiguriert. Nun starte ich das DPM-Setup bis zur Vorprüfung erneut. Leider wird aber noch ein Fehler gemeldet. Details dazu finde ich in einer Textdatei:

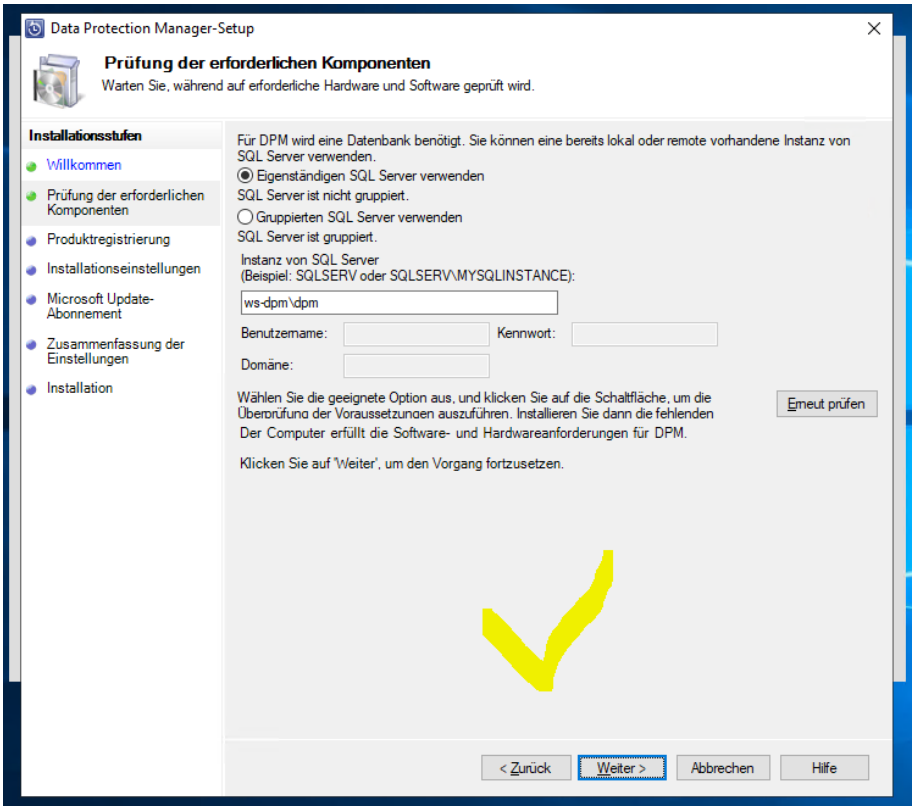


Aha. Das passt etwas mit den Reporting-Services nicht. Ich starte dessen Konfiguration erneut und prüfe noch einmal alle Optionen. Schade: Ich hatte die Webdienst-URL vergessen:

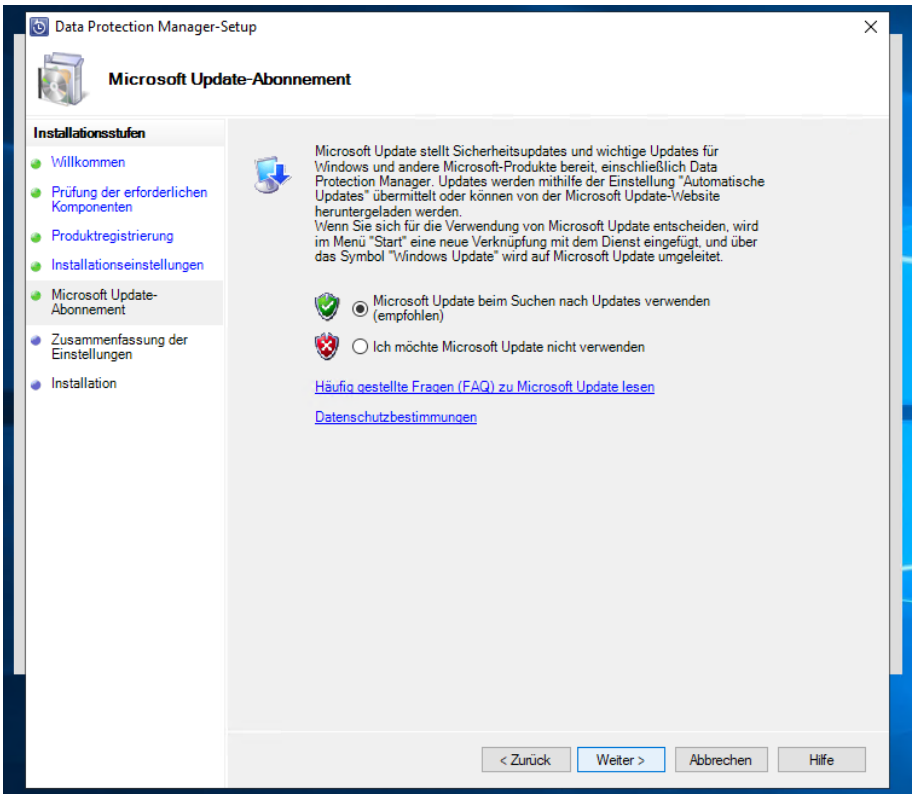


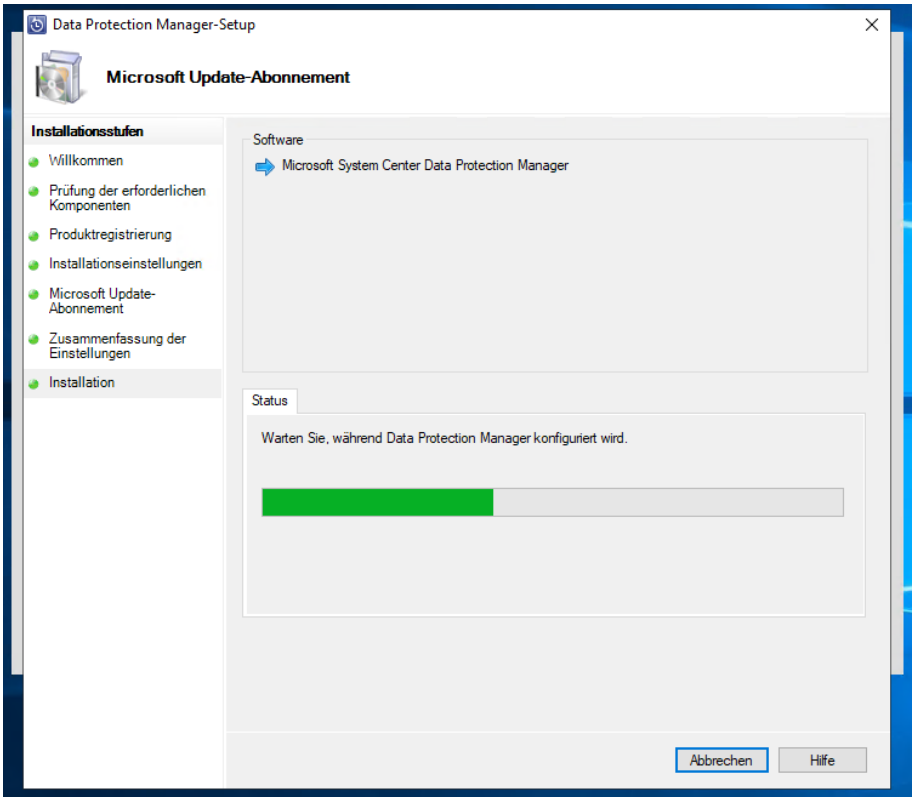


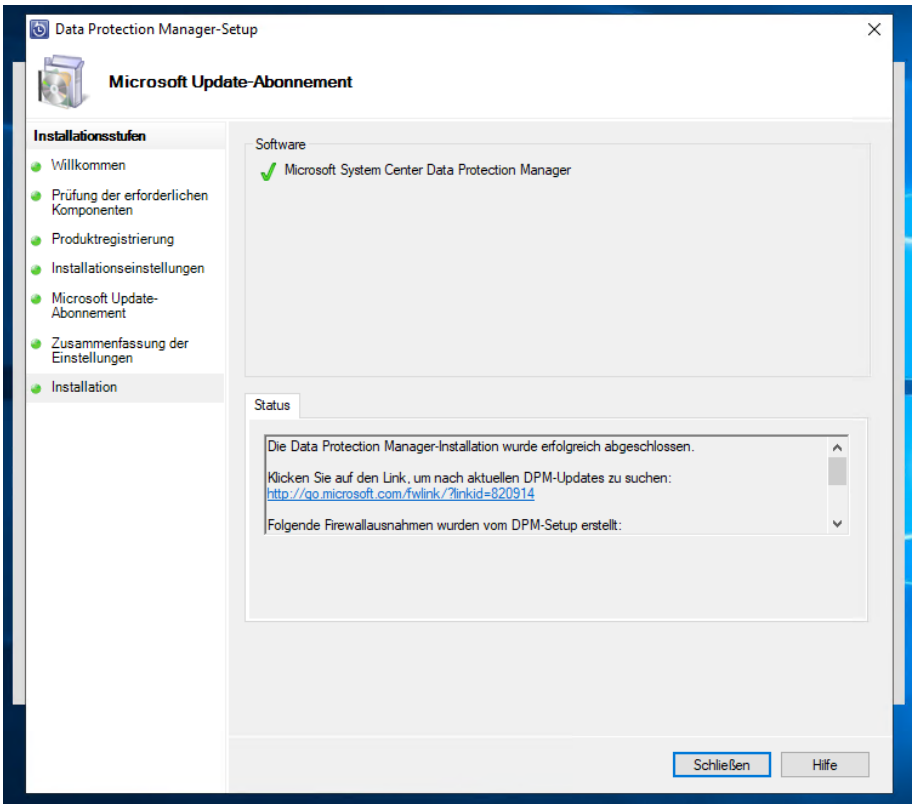
Das sieht besser aus. Und was sagt das DPM-Setup dazu? Eine erneute Prüfung gibt mir grünes Licht:



Aktualisierungen erhält der DPM über meinen WSUS-Server:



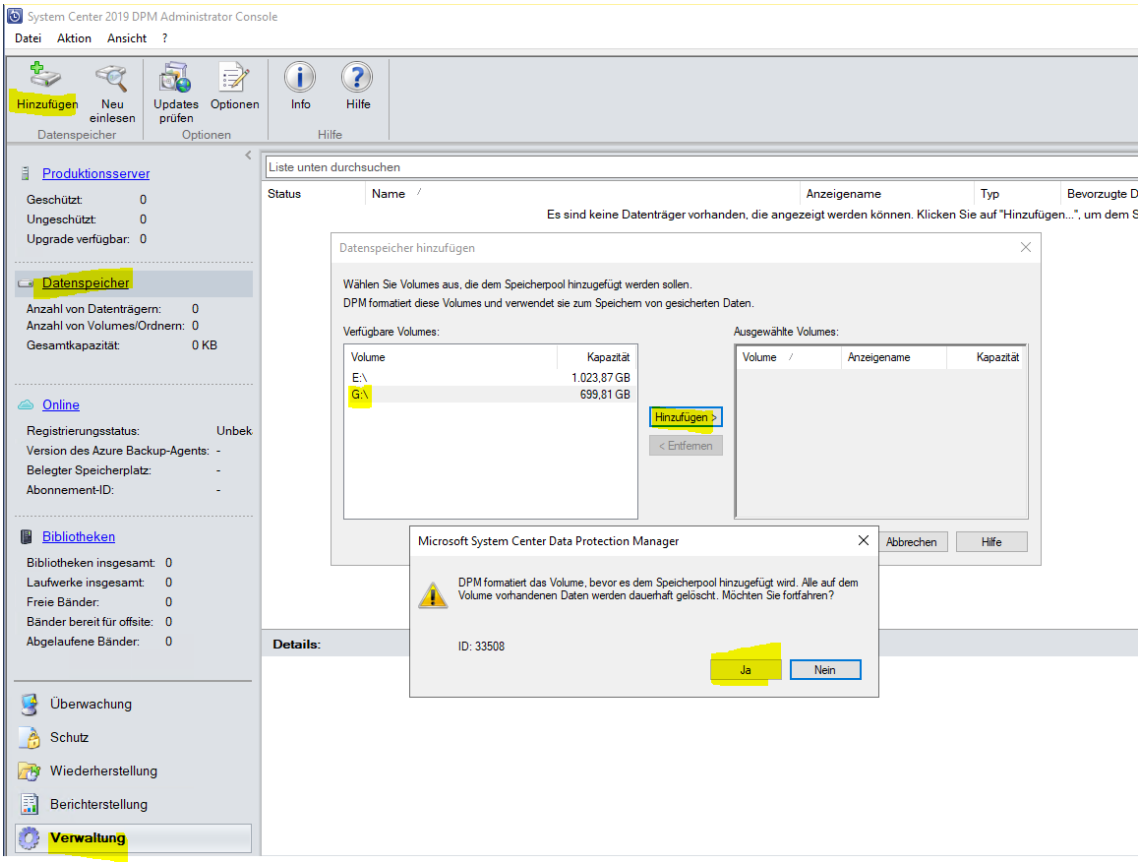


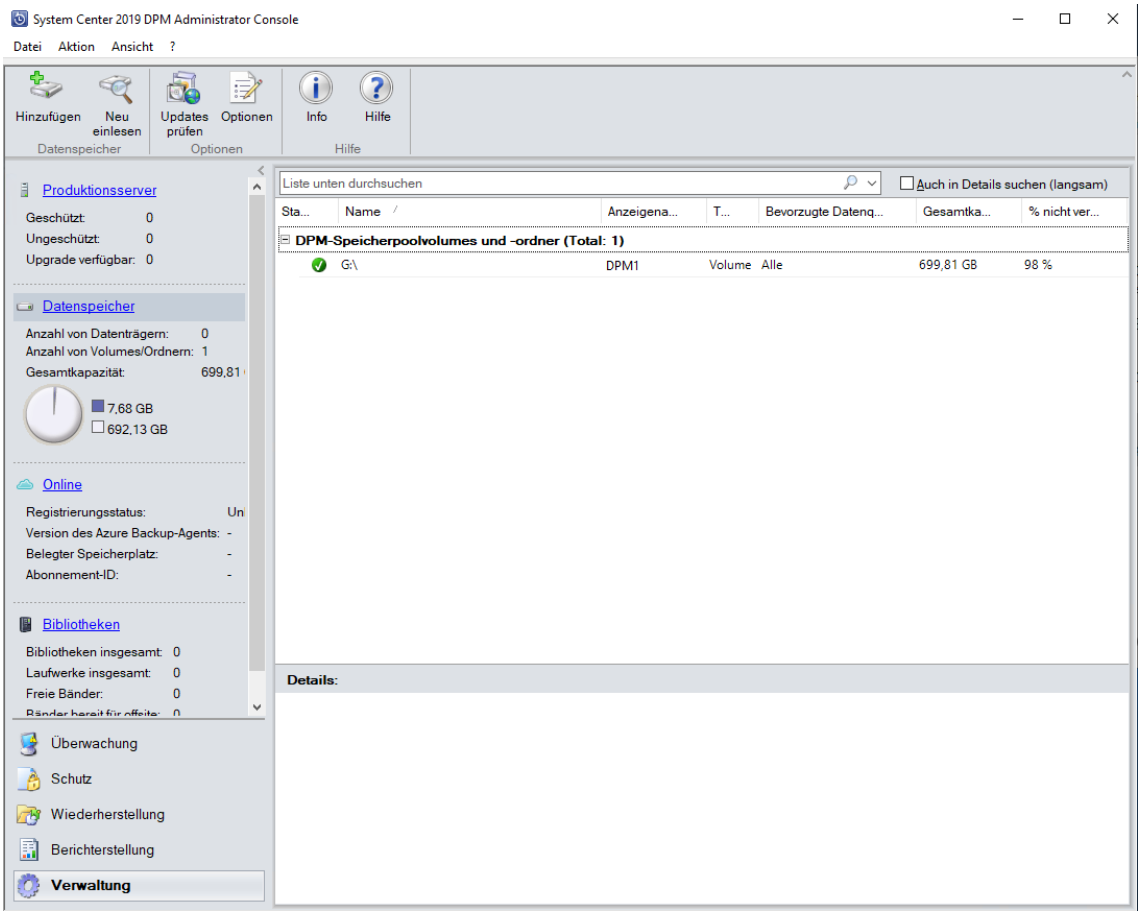


Nach wenigen Minuten ist der DPM 2019 einsatzbereit.

Konfiguration des DPM 2019

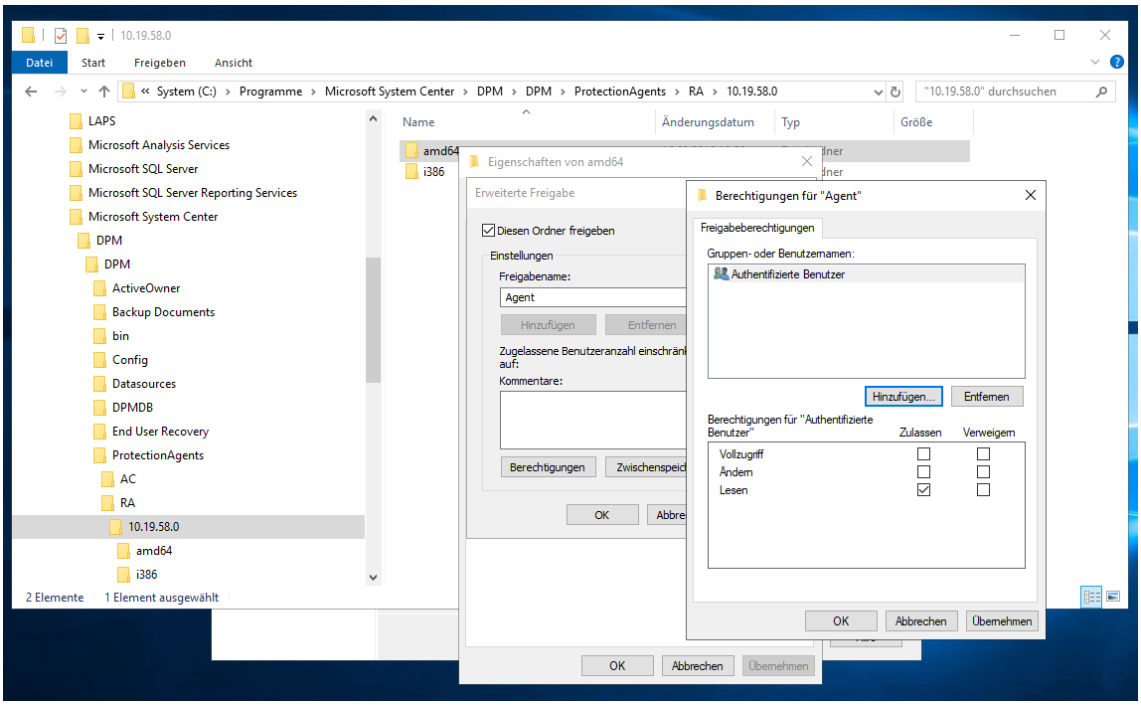
In der Verwaltungsoberfläche füge ich zuerst den Datenspeicher dazu. Auf diesen sichert der DPM meine Nutzdaten. Der Datenträger ist aktuell eine LUN auf meiner Backup-NAS – angebunden durch iSCSI:



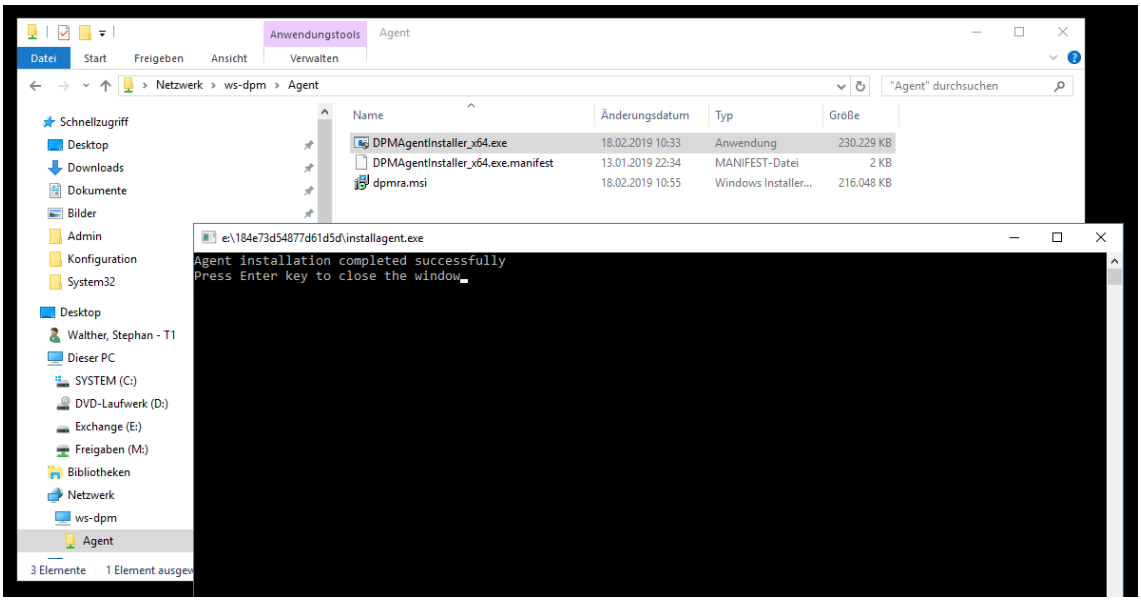


Nun installiere ich die Sicherungs-Agents auf den Quell-Servern. In den vorherigen Versionen des DPM gab es immer Probleme bei der Push-Installation vom DPM aus, wenn die Zielserver eine aktive Windows Firewall haben. Daher

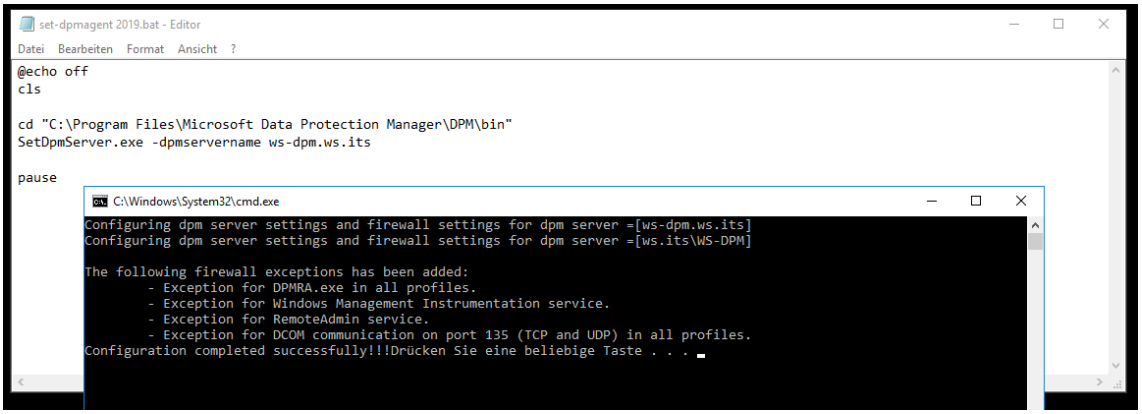
installiere ich die Agents lieber lokal auf meinen Servern. Für einen bequemen Zugriff auf die Installer erstelle ich daher auf dem DPM eine Freigabe:



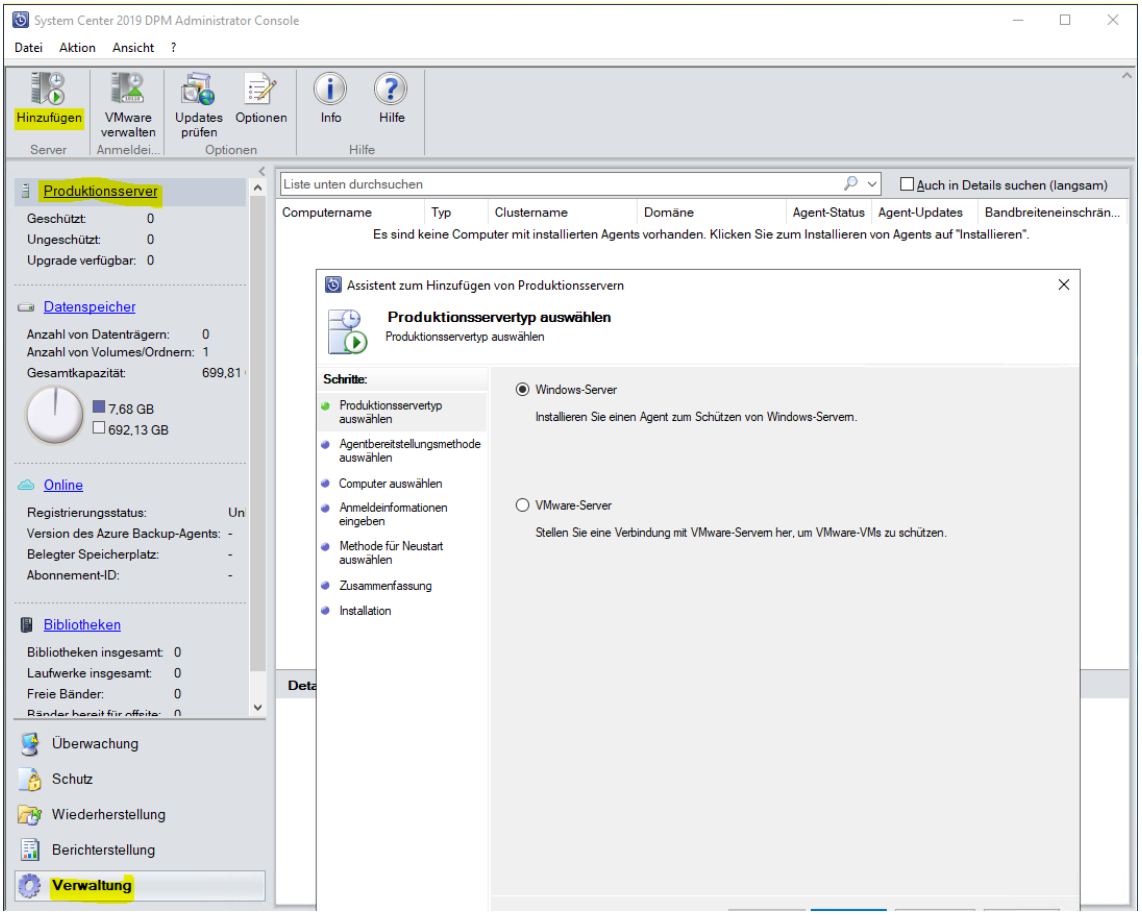
Mit einem passenden Account melde ich mich nun auf meinem Fileserver, meinen Exchange-Servern und den Hyper-V-Hosts an und installiere das Setup:

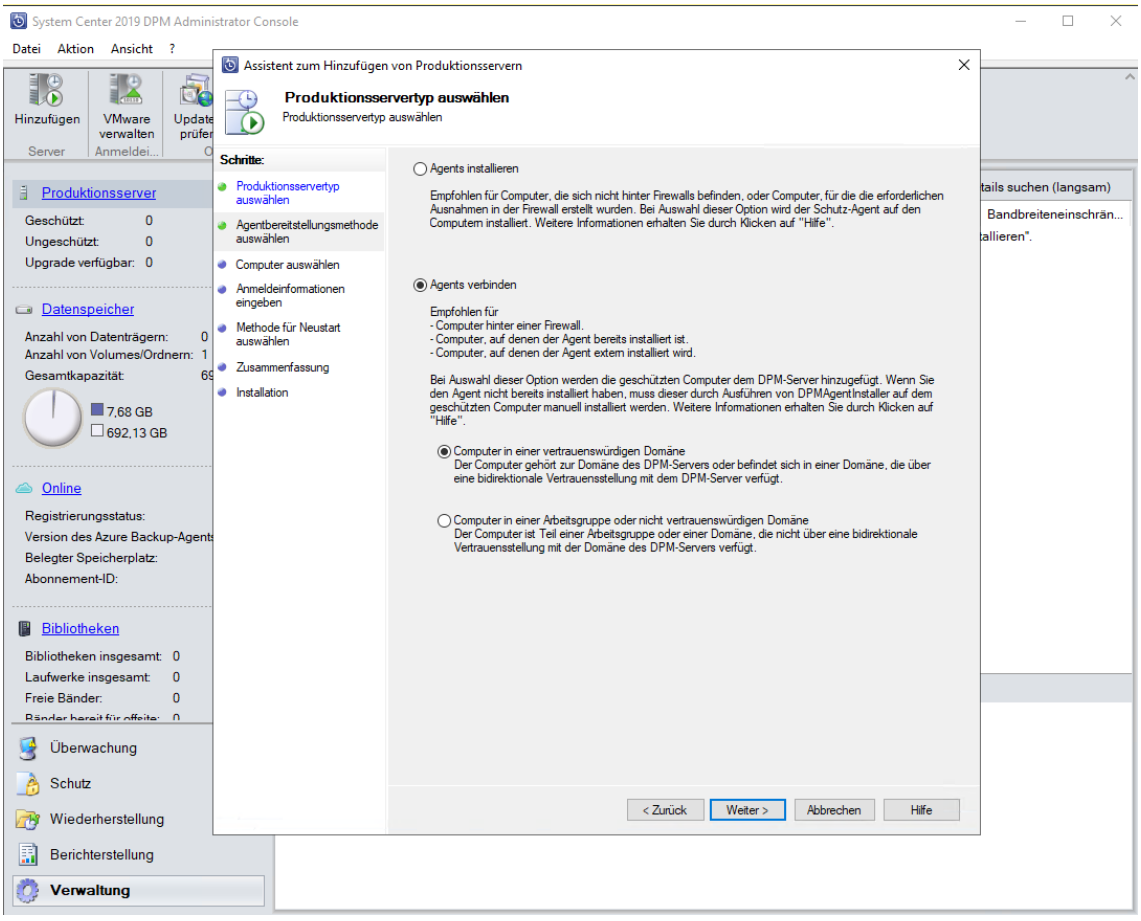


Leider hat das Setup keine Konfigurationsdatei (das wäre ja intuitiv). Daher muss ich auf den Agent-Systemen noch einen Befehl in der cmd absetzen. Dafür habe ich ein Script erstellt:

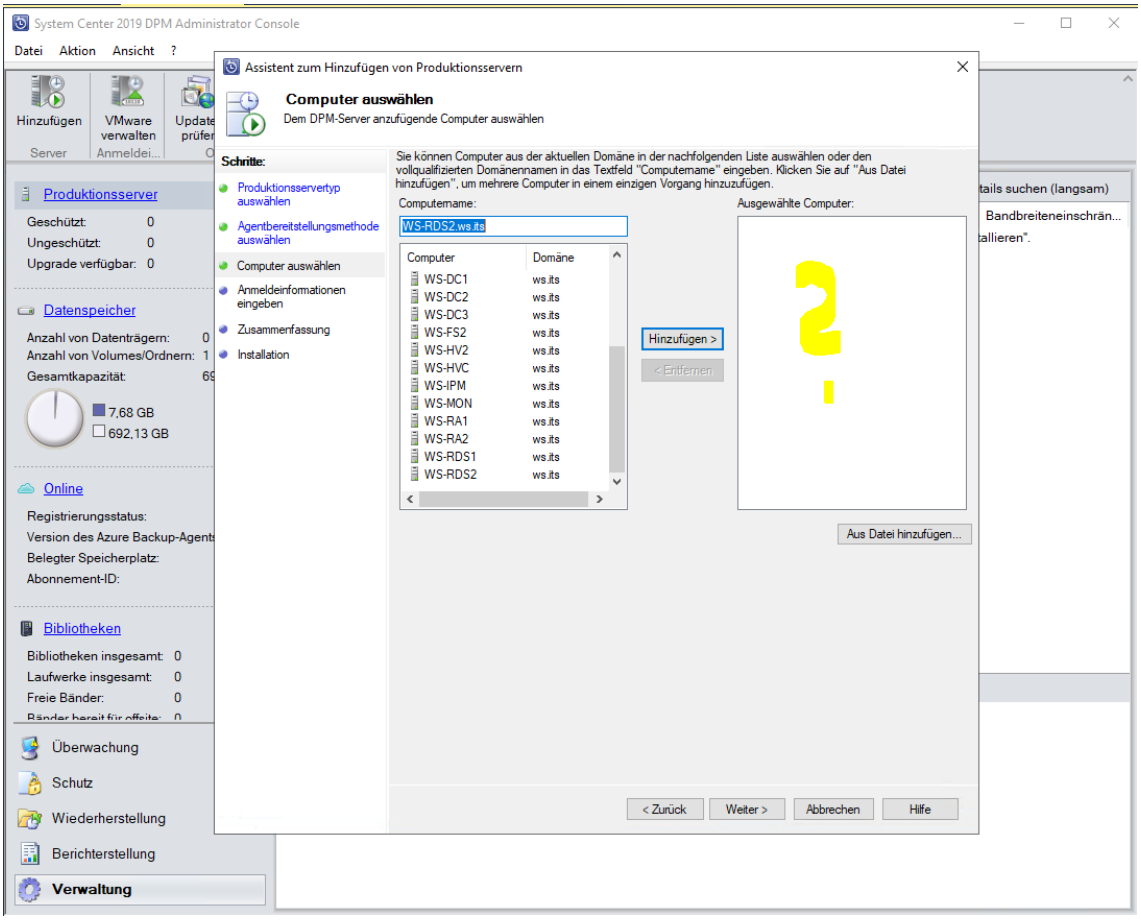


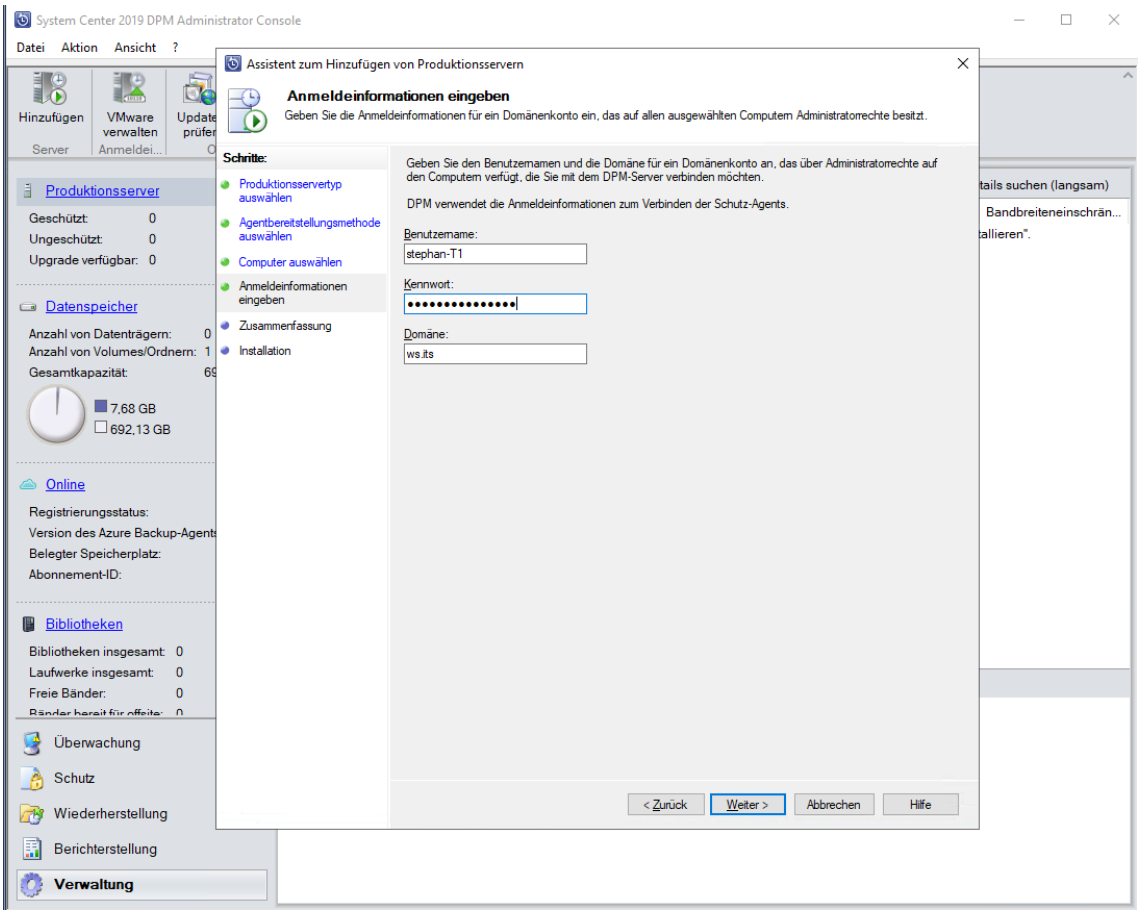
Nun wissen die Quellserver, welchen DPM sie verwenden sollen. Der DPM selber muss aber auch noch unterrichtet werden. Dafür gibt es die Option „Agents verbinden“:

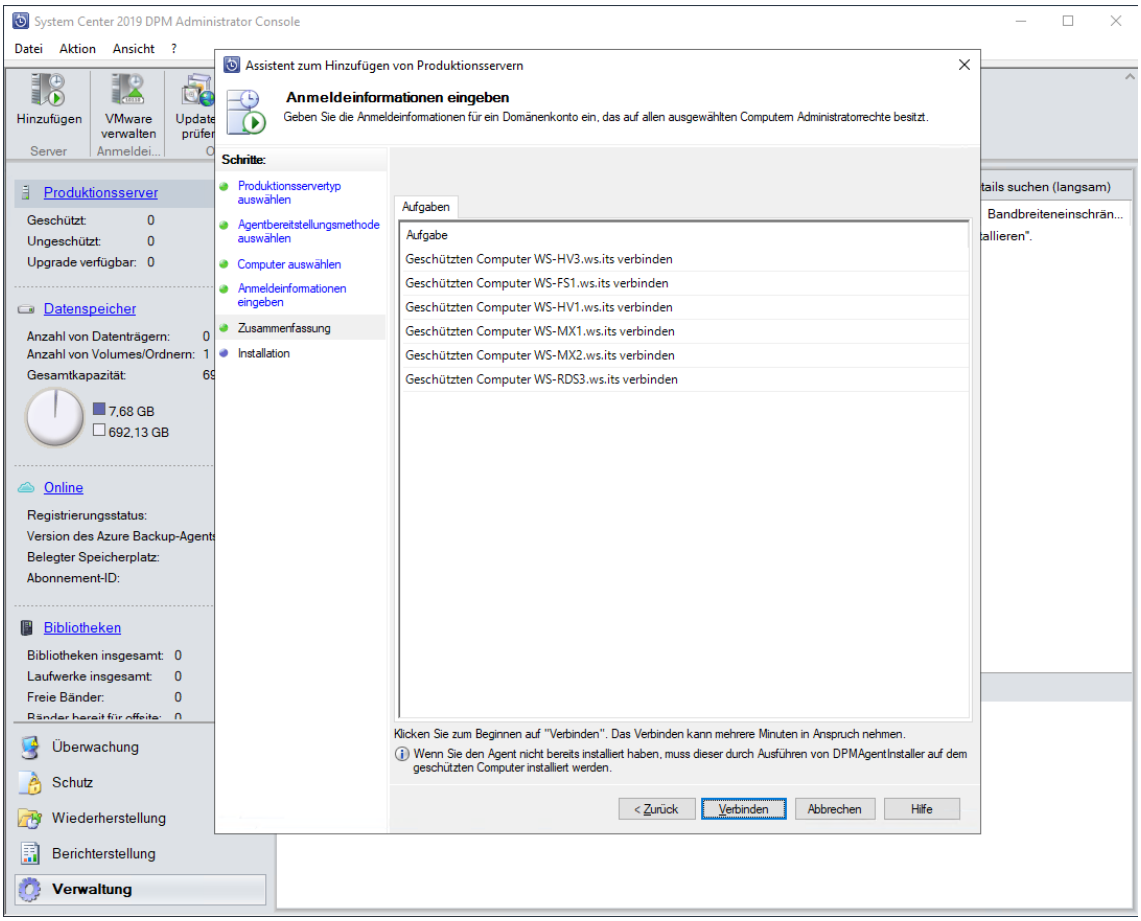


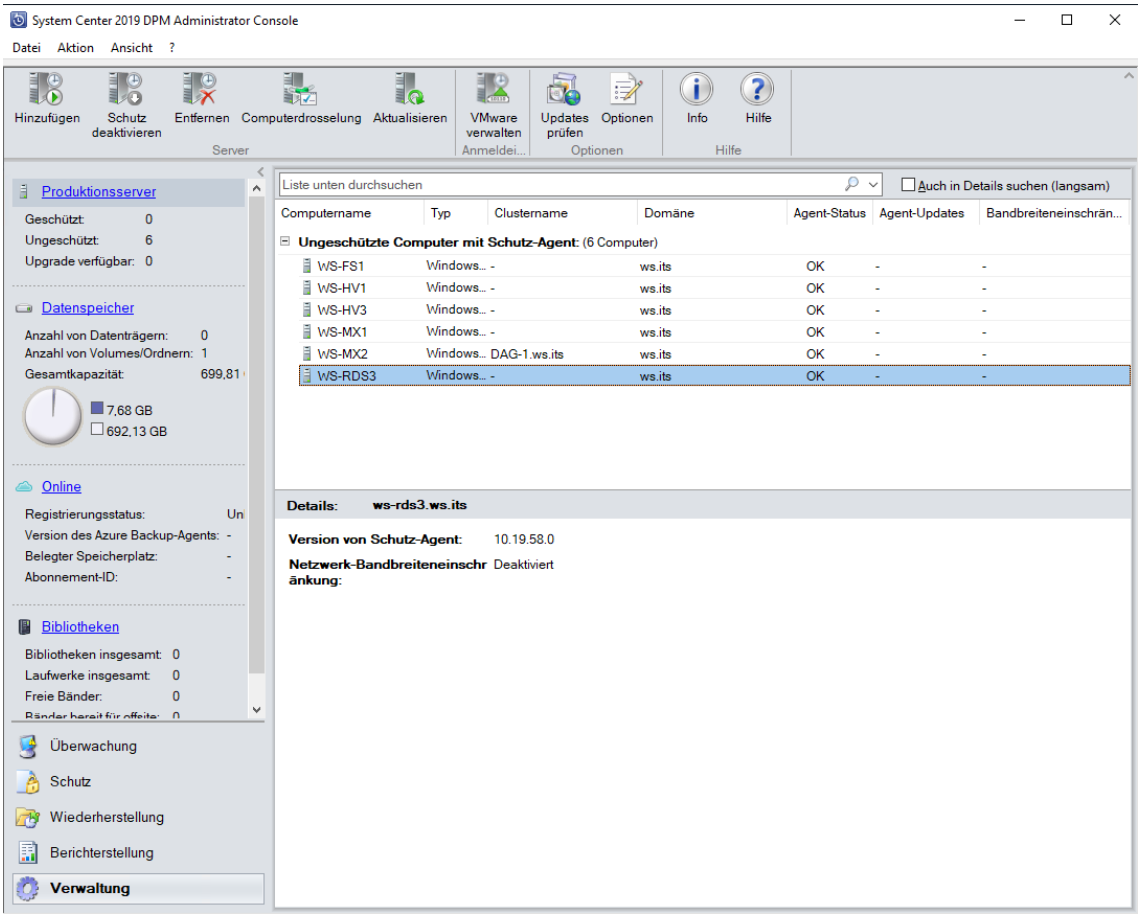


Der Dialog zeigt die hinzugefügten Server leider nicht an. Ein harmloser Bug…

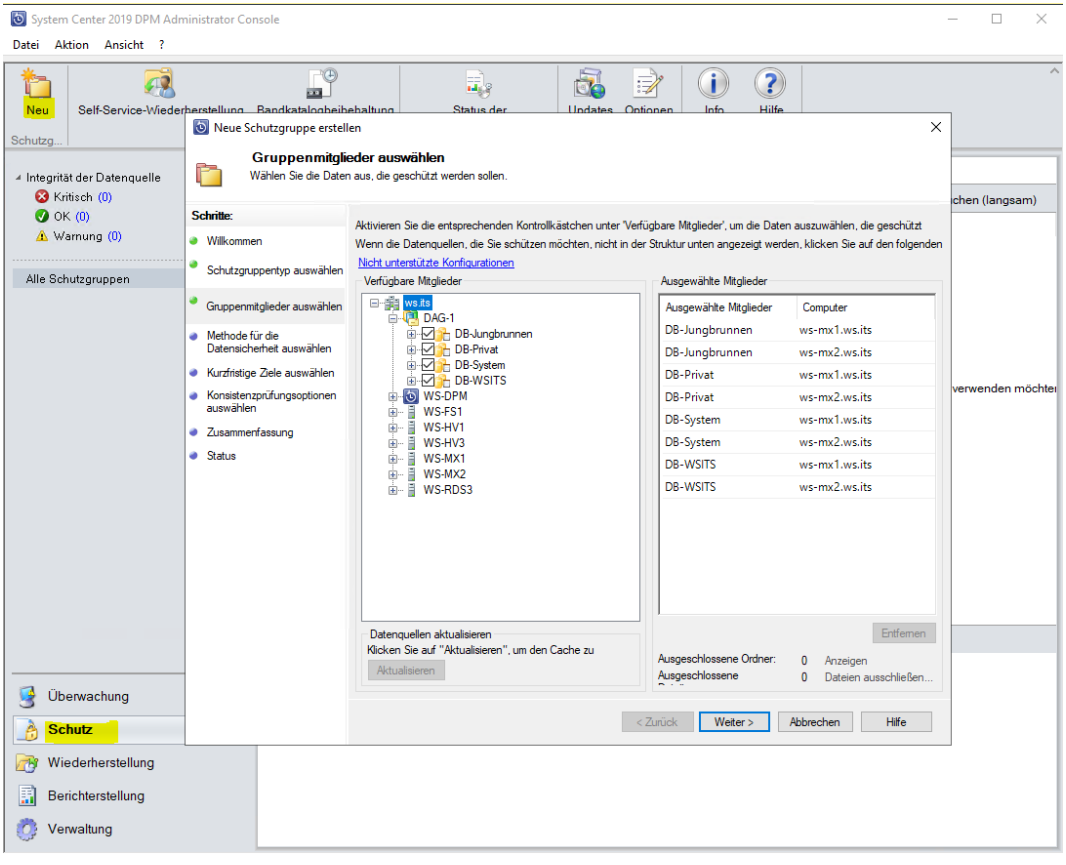


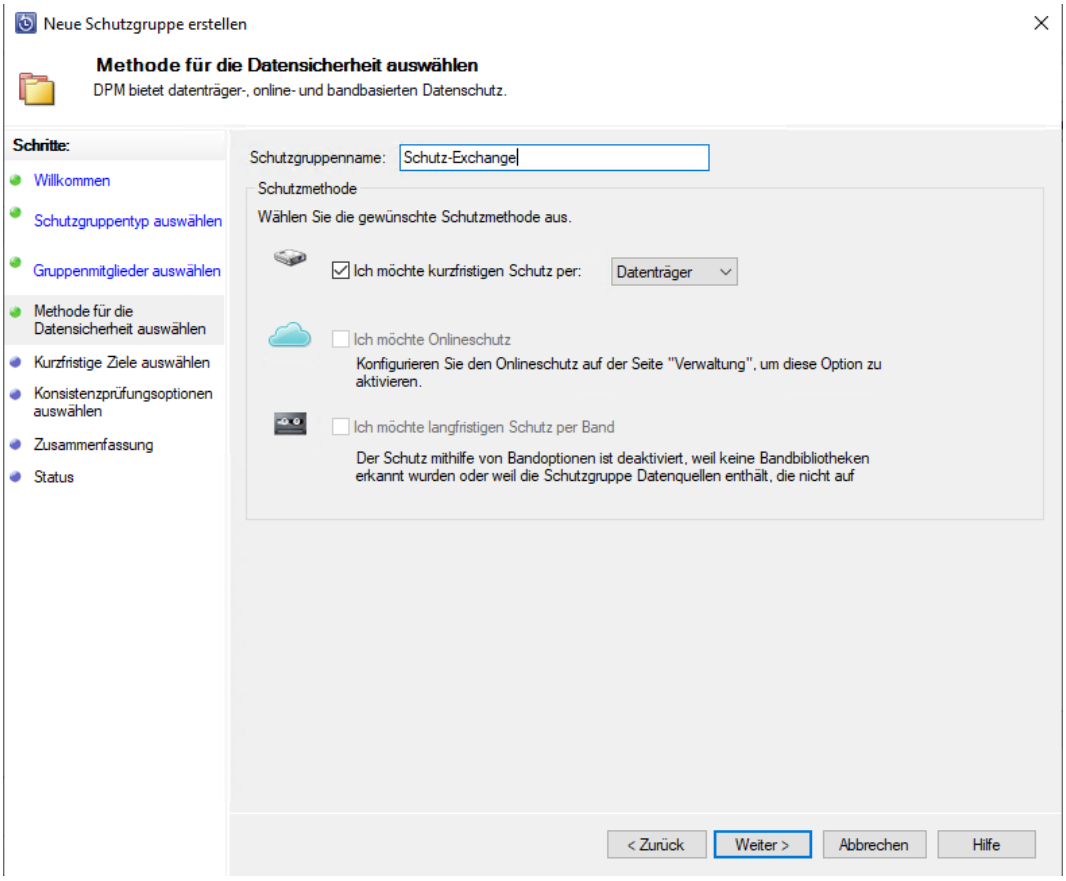

System Center 2019 DPM Administrator Console
Datei Aktion Ansicht ?
Hinzufügen
VMware verwalten
Server
Produktionsserver
Geschützt: 0
Ungeschützt: 0
Upgrade verfügbar: 0
Datenspeicher
Anzahl von Datenträgern: 0
Anzahl von Volumes/Ordnern: 1
Gesamtkapazität:
7,68 GB
692,13 GB
Online
Registrierungsstatus:
Version des Azure Backup-Agents
Belegter Speicherplatz:
Abonnement-ID:
Bibliotheken
Bibliotheken insgesamt: 0
Laufwerke insgesamt: 0
Freie Bänder: 0
Überwachung
Schutz
Wiederherstellung
Berichterstellung
Verwaltung
Assistent zum Hinzufügen von Produktionsservern
Anmeldeinformationen eingeben
Geben Sie die Anmeldeinformationen für ein Domänenkonto ein, das auf allen ausgewählten Computern Administratorrechte besitzt.
Schritte:
Produktionsservertyp auswählen
Agentbereitstellungsmethode auswählen
Computer auswählen
Anmeldeinformationen eingeben
Zusammenfassung
Installation
Geben Sie den Benutzernamen und die Domäne für ein Domänenkonto an, das über Administratorrechte auf den Computern verfügt, die Sie mit dem DPM-Server verbinden möchten.
DPM verwendet die Anmeldeinformationen zum Verbinden der Schutz-Agents.
Benutzername:
stephan-T1
Kennwort:
Domäne:
ws.its
< Zurück
Weiter >
Abbrechen
Hilfe


System Center 2019 DPM Administrator Console
Datei Aktion Ansicht ?
Hinzufügen
VMware verwalten
Server
Produktionsserver
Geschützt: 0
Ungeschützt: 0
Upgrade verfügbar: 0
Datenspeicher
Anzahl von Datenträgern: 0
Anzahl von Volumes/Ordnern: 1
Gesamtkapazität:
7,68 GB
692,13 GB
Online
Registrierungsstatus:
Version des Azure Backup-Agents
Belegter Speicherplatz:
Abonnement-ID:
Bibliotheken
Bibliotheken insgesamt: 0
Laufwerke insgesamt: 0
Freie Bänder: 0
Überwachung
Schutz
Wiederherstellung
Berichterstellung
Verwaltung
Assistent zum Hinzufügen von Produktionsservern
Anmeldeinformationen eingeben
Geben Sie die Anmeldeinformationen für ein Domänenkonto ein, das auf allen ausgewählten Computern Administratorrechte besitzt.
Schritte:
Produktionsservertyp auswählen
Agentbereitstellungsmethode auswählen
Computer auswählen
Anmeldeinformationen eingeben
Zusammenfassung
Installation
Aufgaben
Aufgabe
Geschützten Computer WS-HV3.ws.its verbinden
Geschützten Computer WS-FS1.ws.its verbinden
Geschützten Computer WS-HV1.ws.its verbinden
Geschützten Computer WS-MX1.ws.its verbinden
Geschützten Computer WS-MX2.ws.its verbinden
Geschützten Computer WS-RDS3.ws.its verbinden
Klicken Sie zum Beginnen auf "Verbinden". Das Verbinden kann mehrere Minuten in Anspruch nehmen.
Wenn Sie den Agent nicht bereits installiert haben, muss dieser durch Ausführen von DPMAgentInstaller auf dem geschützten Computer installiert werden.
< Zurück
Verbinden
Abbrechen
Hilfe

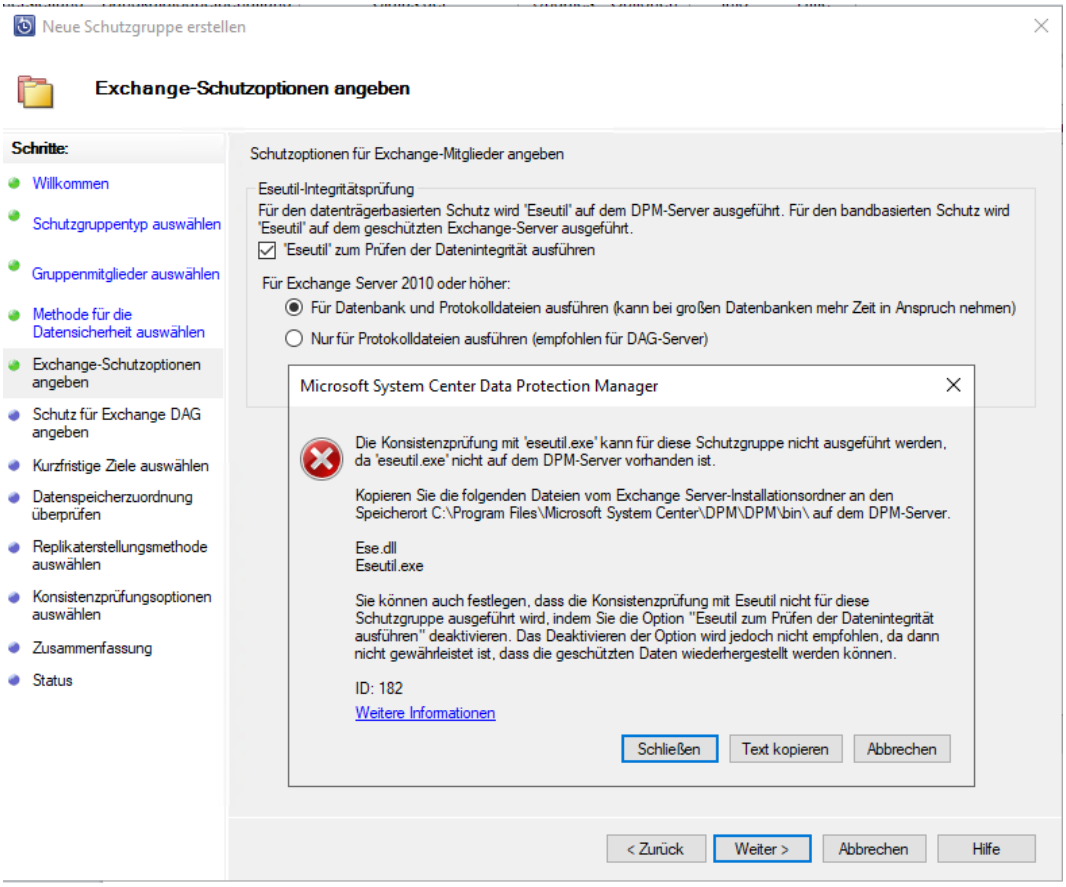


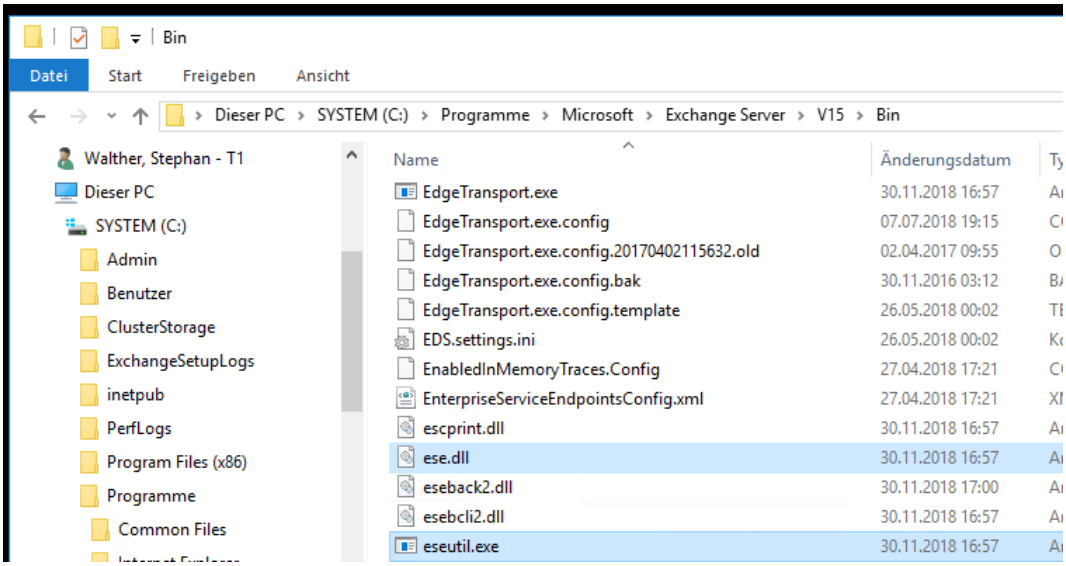
Nun kann der DPM mit den Quellservern kommunizieren. Es fehlen noch die Sicherungsaufgaben (Schutzgruppen). Ich beginne mit dem „Schutz-Exchange“: Das System erkennt zuverlässig meine Exchange-DAG:

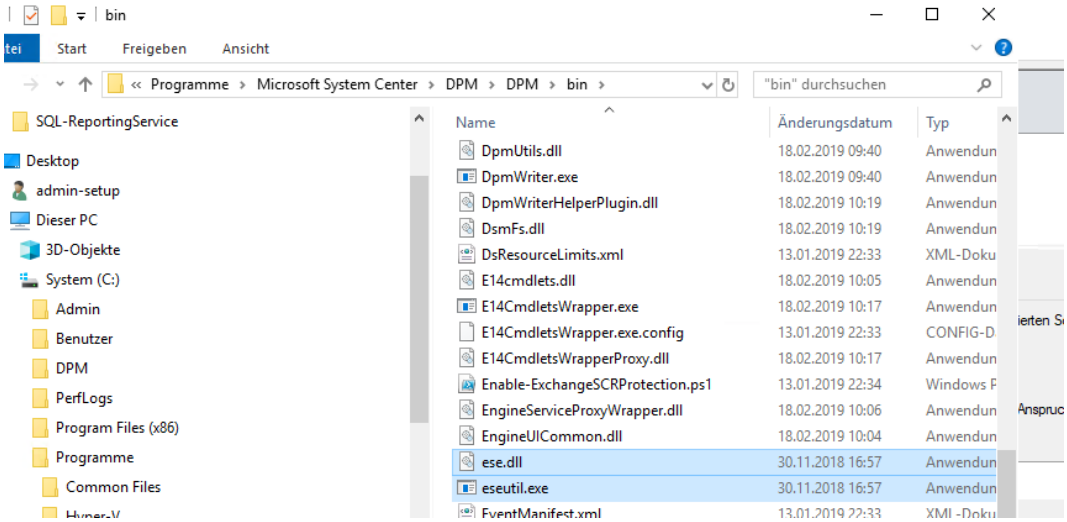




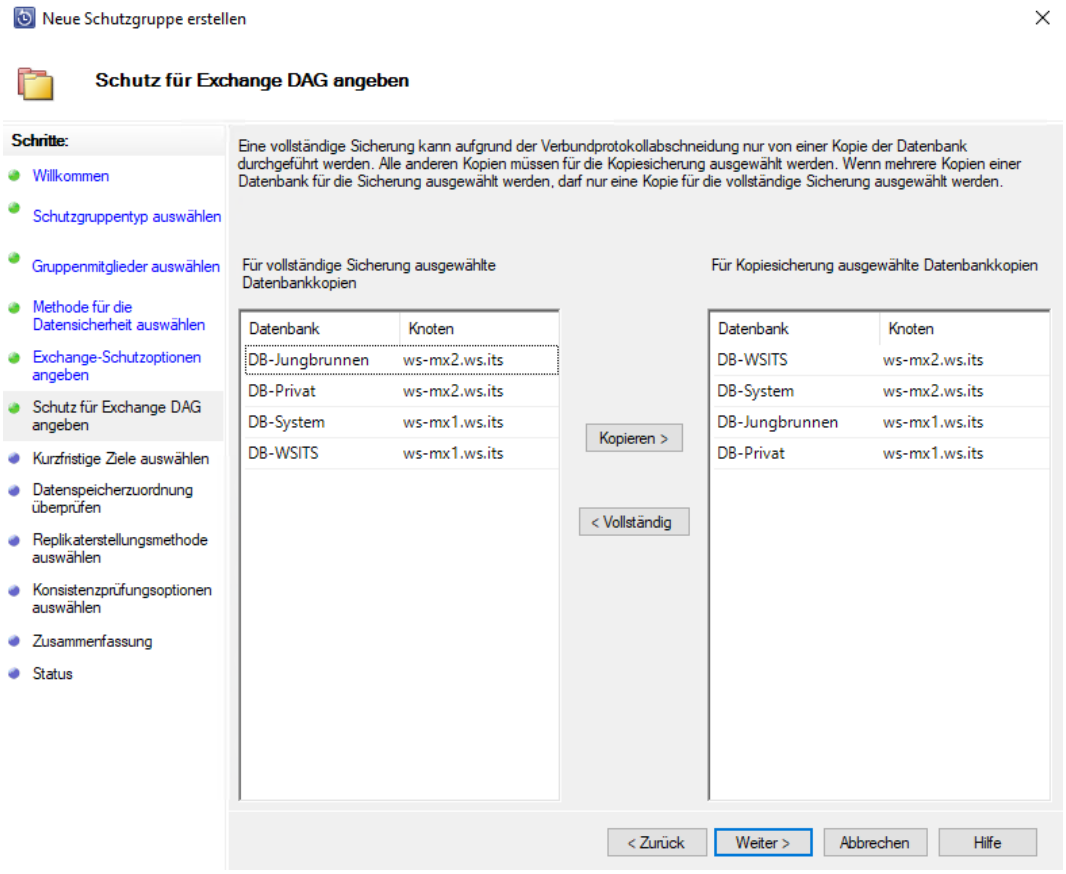
Wie in der Vorgängerversion wird auch beim DPM 2019 die zum Exchange-Server passende eseutil-Anwendung benötigt, wenn der DPM die gesicherten Datenbanken in seinem Repository in einen Clean-Shutdown-State überführen soll. Diese Dateien hat der Exchange-Server gespeichert. Ein paar Klicks später liegen sie auch im DPM bereit:



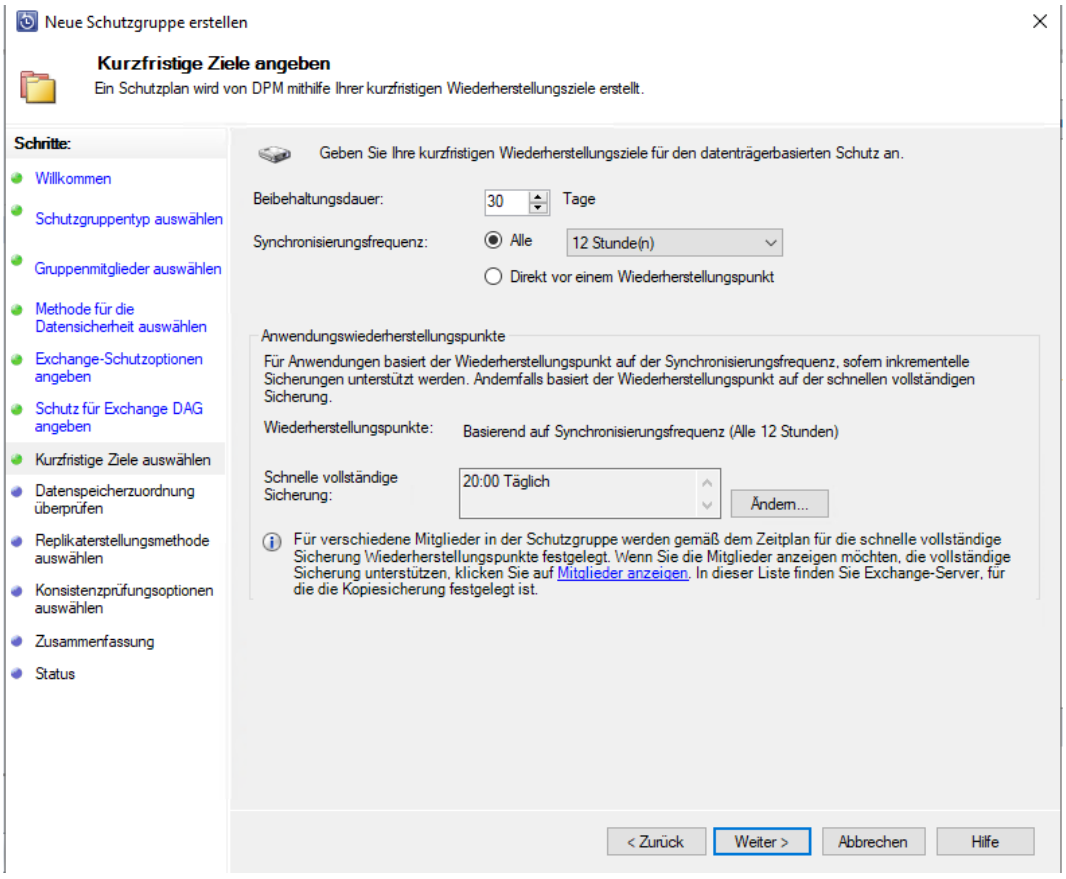




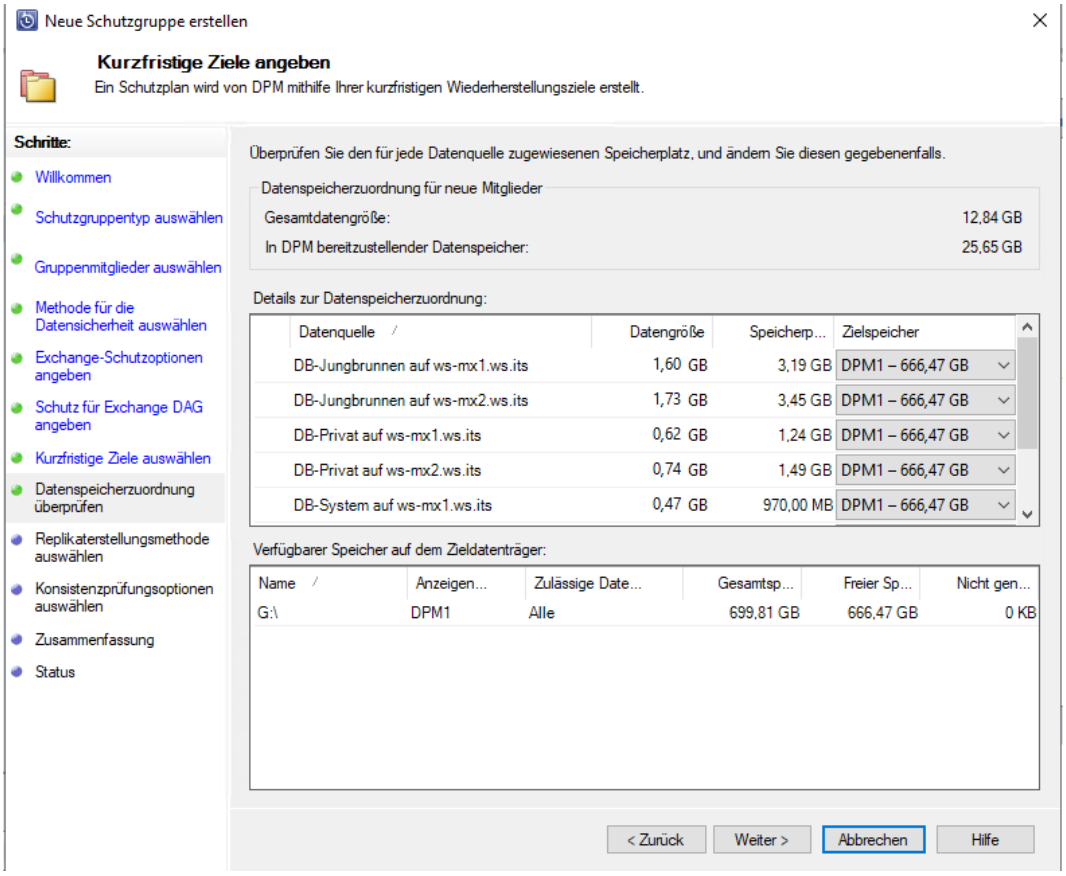
Nun kann ich die Datenbanken dem richtigen Sicherungsverfahren zuweisen. Meine aktiven DBs bekommen eine Vollsicherung. Die Kopiesicherungen sind für die passiven DBs:



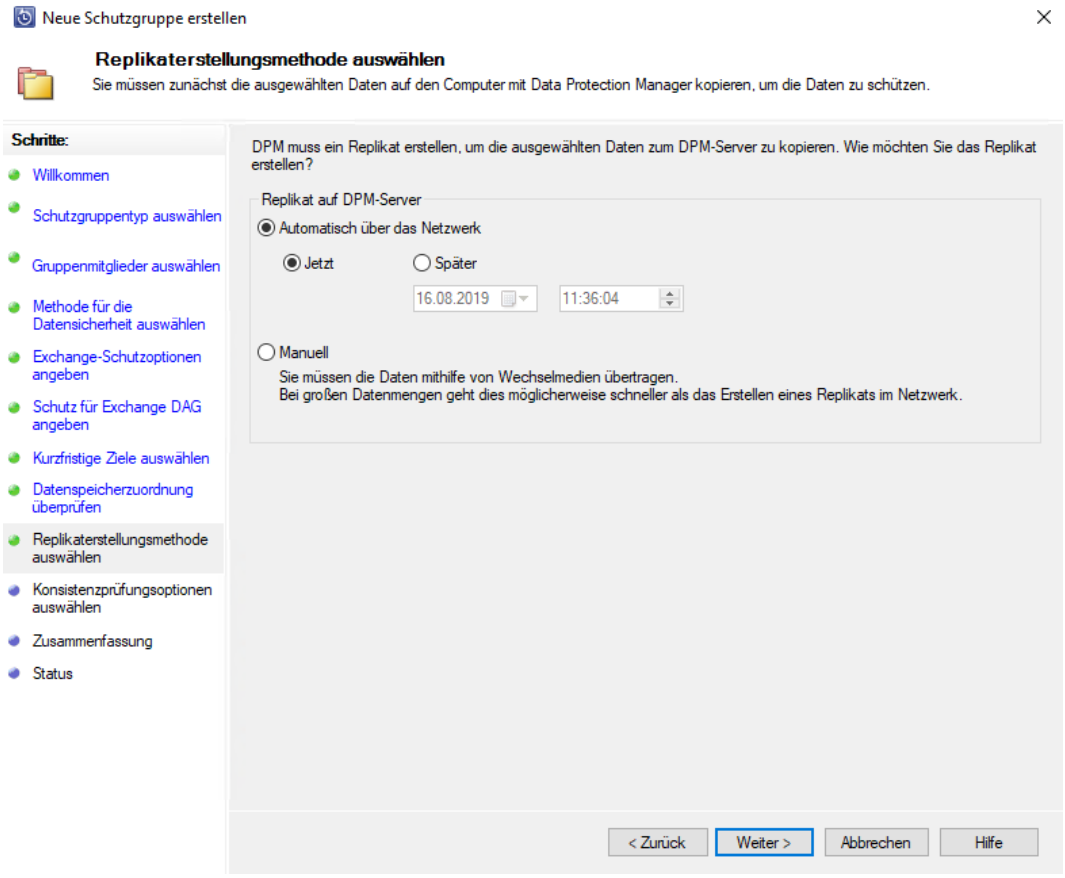
Die Sicherung bekommt auch einen Zeitplan:

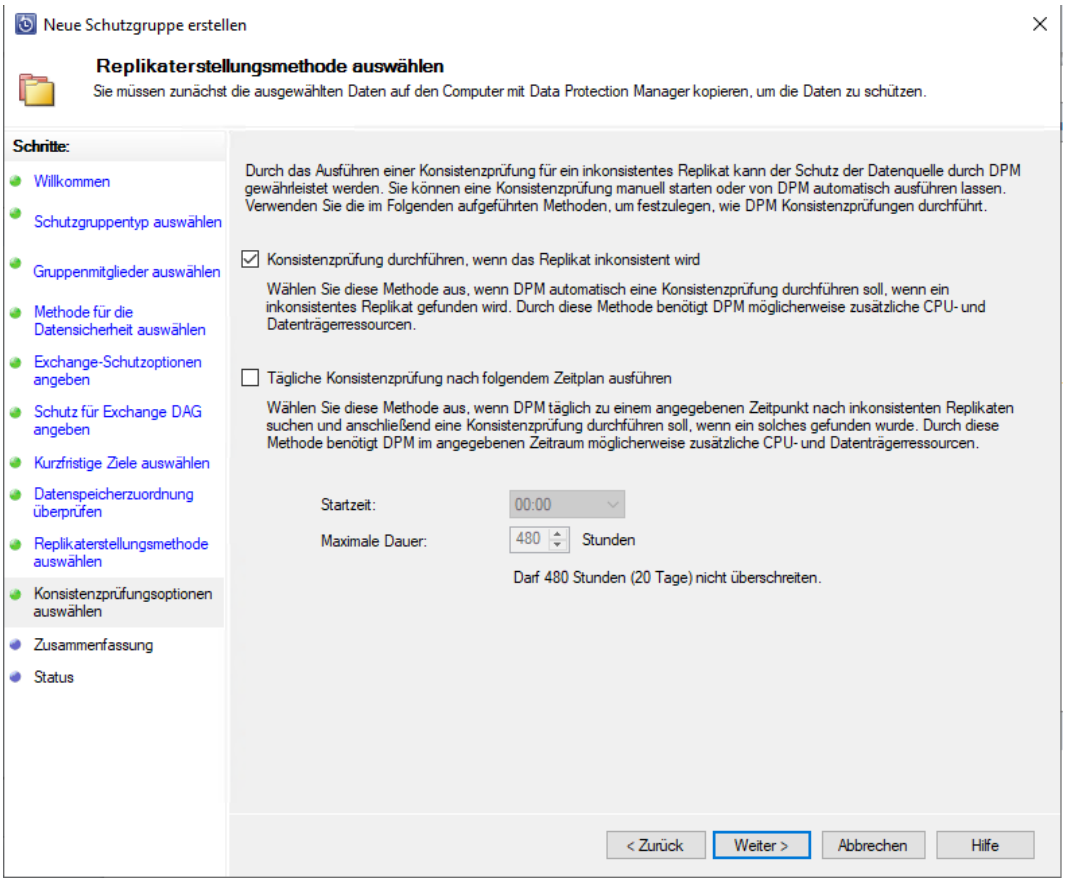


Als Sicherungsziel wähle ich die eine Partition auf der iSCSI-Disk:

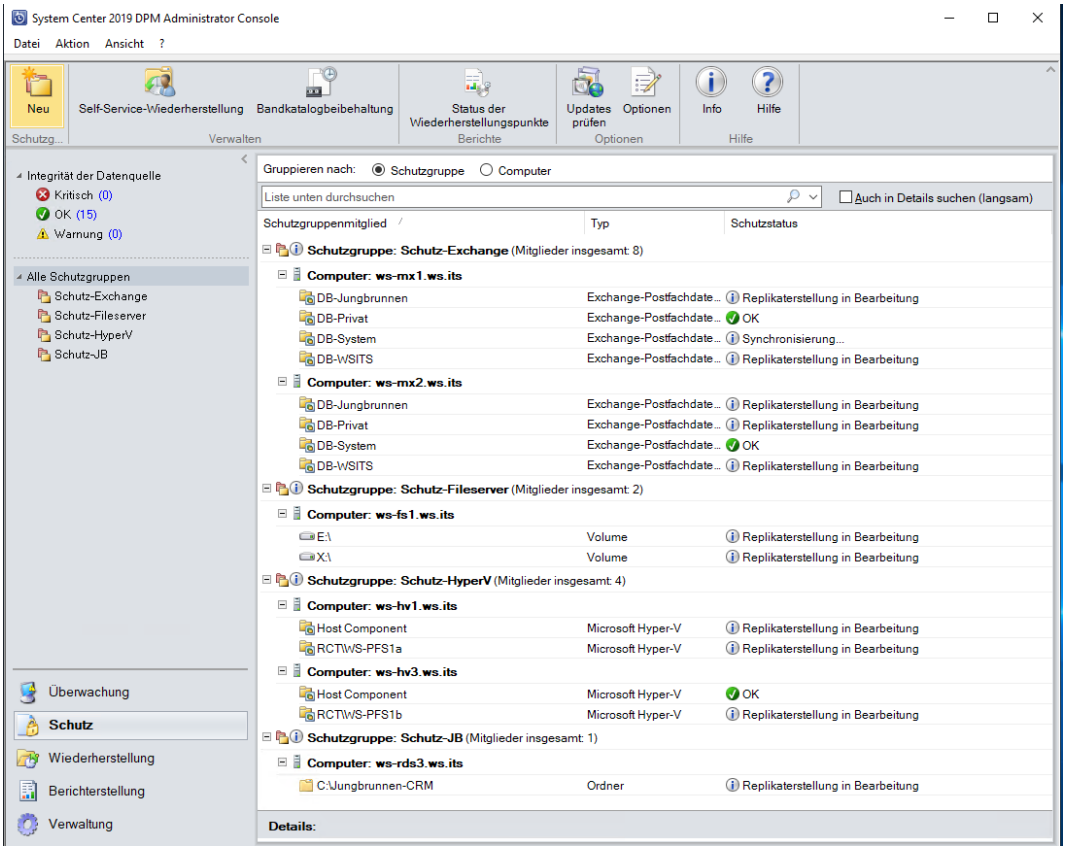


Der DPM darf die initiale Sicherung sofort beginnen. Die Sicherung wird online erstellt. Es sollte also keine Serviceunterbrechung für meine Exchange-Benutzer geben:



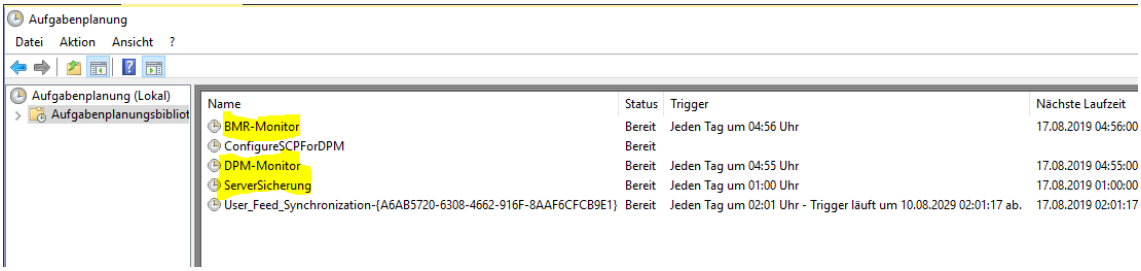


Die Sicherung läuft an. Analog verfahre ich mit den Schutzgruppen „Schutz-Fileserver“, „Schutz-HyperV“ und „Schutz-JB“ (CRM). Somit ergibt sich folgender Sicherungsstand:

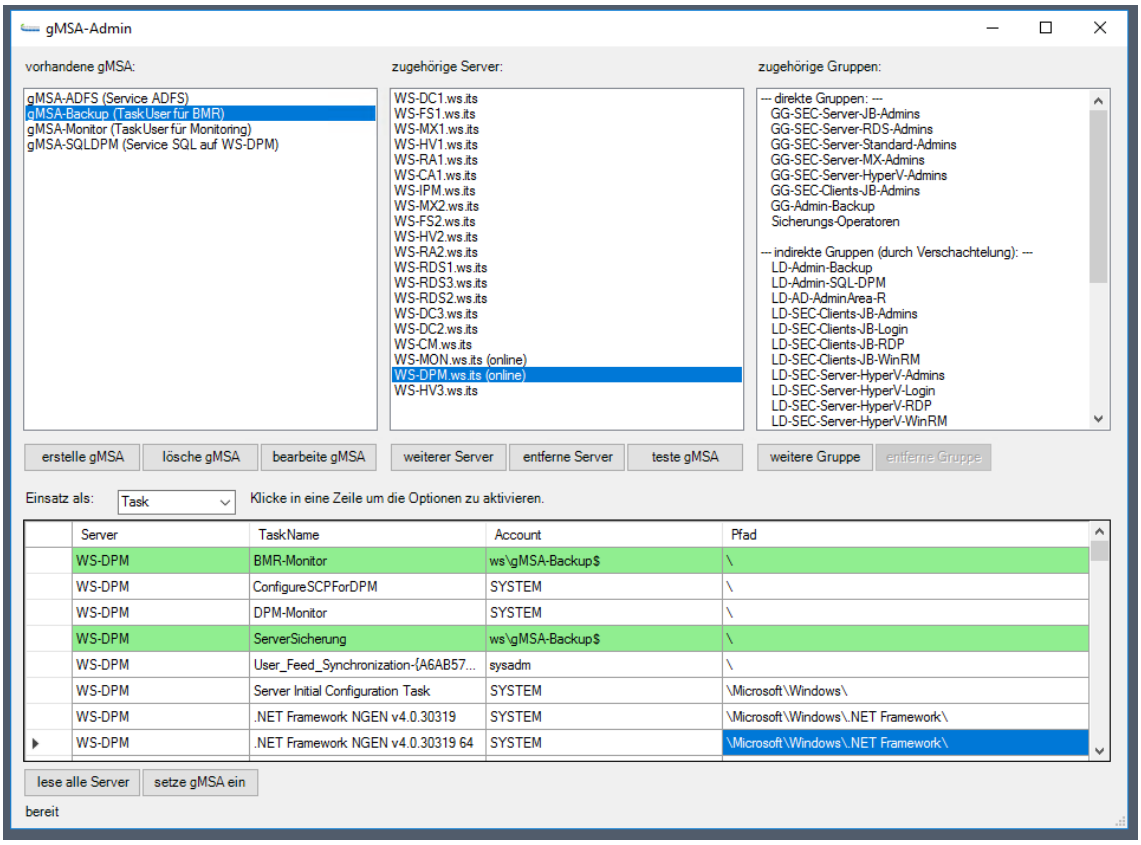


Sonstiges

Da der DPM 2019 seinem Vorgänger extrem ähnlich sieht rechne ich nicht mit einer Verbesserung im Monitoring. Daher importiere ich meine eigene Scriptlösung, die mich jeden Morgen über den Sicherungserfolg informiert. Dazu erhält der Server weitere Aufgaben. Diese hatte ich im alten DPM einfach als XML exportiert:



Einige der Aufgaben laufen wieder im Kontext eines gMSA-Accounts. Diese weise ich wieder mit meiner PowerShell-GUI vom DomainController aus zu:



Nun erstelle ich noch die Freigabe für meine BMR-Sicherungen, konfiguriere die Deduplizierung und entferne im Hyper-V-Server die alte VM.

Im Monitoring gab es keine Anpassung, da ich die IPv4 und den Namen des Servers wiederverwende.

Feintuning und TroubleShooting

Probleme mit der iSCSI-Disk

Die initiale Sicherung lief eigentlich ganz gut durch. Dennoch hat der DPM-Monitor (mein PowerShell-Script) immer wieder Fehler gemeldet:

DPM Monitor

An

DPM-Monitor

Protectiongroup	ServerName	DataSource	JobCounter	LastState
Schutz-Exchange	ws-mx1.ws.its	DB-Jungbrunnen	2/2	pass
Schutz-Exchange	ws-mx1.ws.its	DB-Privat	2/2	pass
Schutz-Exchange	ws-mx1.ws.its	DB-System	2/3	pass
Schutz-Exchange	ws-mx1.ws.its	DB-WSITS	2/4	pass
Schutz-Exchange	ws-mx2.ws.its	DB-Jungbrunnen	3/3	pass
Schutz-Exchange	ws-mx2.ws.its	DB-Privat	2/4	pass
Schutz-Exchange	ws-mx2.ws.its	DB-System	2/2	pass
Schutz-Exchange	ws-mx2.ws.its	DB-WSITS	1/3	pass
Schutz-Fileserver	ws-fs1.ws.its	E:\	8/9	pass
Schutz-Fileserver	ws-fs1.ws.its	X:\	9/9	pass
Schutz-HyperV	ws-hv1.ws.its	Host Component	4/4	pass
Schutz-HyperV	ws-hv1.ws.its	RCT\WS-PFS1a	4/4	pass
Schutz-HyperV	ws-hv3.ws.its	Host Component	4/4	pass
Schutz-HyperV	ws-hv3.ws.its	RCT\WS-PFS1b	4/4	pass
Schutz-JB	ws-rds3.ws.its	C:\	4/4	pass

Informationen:

Generiert auf:	WS-DPM

Man erkennt deutlich, dass einige Sicherungen fehlschlagen. Das kann ich so nicht gebrauchen. Und auch meine BMR-Sicherungen, die von Windows-Server-Backup erstellt werden schlagen immer wieder fehl.

In den Eventlogs finde ich zahlreiche iSCSI-Fehler. Kann der Windows Server 2019 etwa nicht vernünftig mit meiner NAS kommunizieren?? Als Test binde ich einen anderen Windows Server 2019 via iSCSI an das NAS-Target an und kopiere testweise ein paar Daten. Und auch dieser kommt ins Stocken!!! Zur Validierung versuche ich das Gleiche von einem Windows Server 2016 – und auch dieser hat Probeme! Puh, es ist nicht das Betriebssystem. In der NAS, die nun auch schon einige Jahre im 24/7-Betrieb operiert, kommen die Platten an ihre Grenzen. Offenbar ist das vorher nicht aufgefallen, da der DPM keine Vollsicherungen erstellt, sondern nur Incrementals vom Quellserver zieht. Die komplette Vollsicherung meiner Nutzdaten war wohl zuviel.

In meinem neuen Hyper-V-Host hatte ich aber noch ne andere 4TB-Platte verbaut. Auf dieser erstellte ich eine neue VHDX und wies sie dem DPM zu. Natürlich musste er die gesamte Sicherung erneut erstellen, denn beim Versuch die Daten vom iSCSI-NAS auf VHDX zu verschieben kam das System wieder an seine Schmerzgrenze. Aber nun laufen alle Backups ohne Probleme durch!

Und auch die BMR-Sicherungen meiner Windows Server landen nun in einer weiteren VHDX, die im DPM freigegeben ist. Für die räumliche Trennung meiner Datensicherung habe ich schon eine andere Idee. Daher können die Sicherungen primär auf einer anderen Disk im gleichen Server landen.

HDD-Auslastung

Die DPM-Sicherungen laufen hervorragend. Nur meine BMR-Sicherungen kommen nicht nach. Diese werden über eine zentral gesteuerte Scriptlösung von den Servern nacheinander (!) ab 01:00 täglich ausgeführt. Bisher reichte das Zeitfenster bis kurz vor 04:45. Danach erfasst ein anderes Script das Ergebnis und berichtet mir per Mail. Nach der Umstellung sehen die Mails leider so aus:

ACHTUNG-ServerSicherung

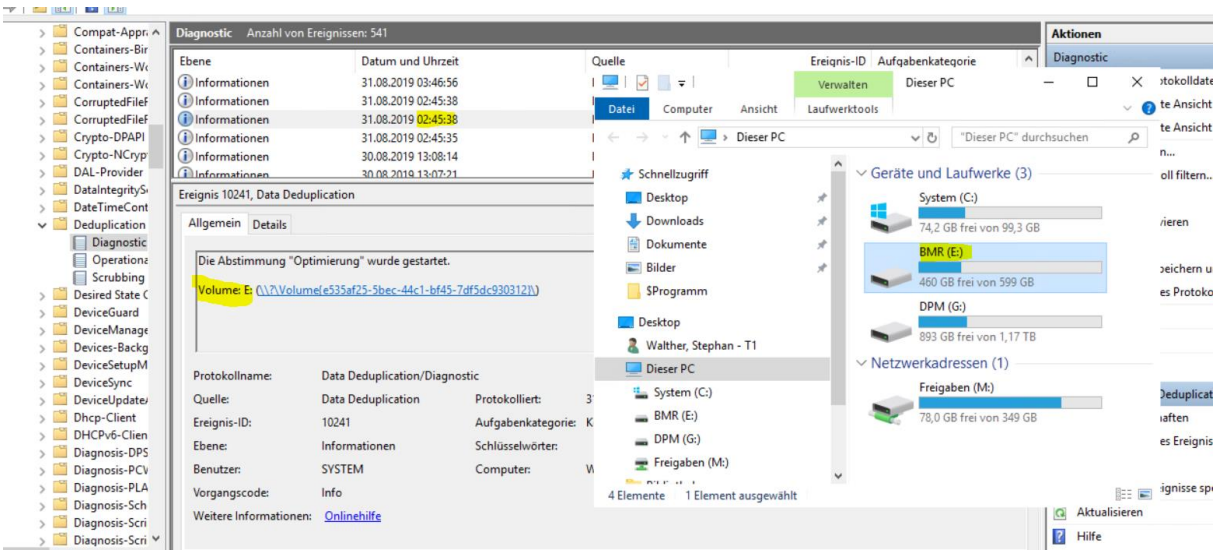
An Logmails

Server	JobName	StartZeit	EndZeit	Groesse	Status	Zeitplan	Slot
WS-RDS2	BMR	--	--	0	OK	246	--
WS-ATA	BMR	--	--	0	OK	246	--
WS-RA2	BMR	--	--	0	OK	246	--
WS-HV3	BMR	--	--	0	OK	246	--
WS-MX2	BMR	--	--	0	OK	246	--
WS-FS2	BMR	--	--	0	OK	246	--
WS-DC2	BMR	--	--	0	OK	246	--
WS-DC3	BMR	--	--	0	OK	246	--
WS-CA1	BMR	--	--	0	OK	246	--
WS-HV2	BMR	--	--	0	OK	7	--
WS-DPM	BMR	--	--	0	OK	246	--
WS-RDS1	BMR	??	??	0	Fehler	135	??
WS-RA1	BMR	??	??	0	Fehler	135	??
WS-WAC	BMR	??	??	0	Fehler	135	??
WS-IPM	BMR	??	??	0	Fehler	135	??
WS-MX1	BMR	??	??	0	Fehler	135	??
WS-CM	BMR	01:00:02	01:15:35	34842	OK	135	1
WS-RDS3	BMR	01:00:03	01:42:08	83726	Warnung -4	135	3
WS-DC1	BMR	01:20:03	02:43:17	29126	OK	135	4
WS-FS1	BMR	01:40:03	03:15:09	21717	OK	135	1
WS-HV1	BMR	02:00:02	02:29:25	7720	Fehler -3	135	1

Statistik:

Die rot markierten Server mit den ?? haben erfolgreich gesichert. Nur leider nicht mehr innerhalb des Sicherungszeitfensters. Die Sicherung ist nun oft erst nach 08:00 abgeschlossen!

Doch was ist die Ursache? Es muss etwas mit der Auslastung der physischen Festplatte zu tun haben. Das könnte ein anderer Task sein, der zur gleichen Zeit die Platte intensiv belastet. Und da hab ich auch schon einen Treffer: um Plattenplatz zu sparen habe ich auf dem DPM-Server die Deduplizierung des Volumes der BMR-Sicherungen aktiviert (da spart man richtig viel Speicher!). Blöderweise läuft diese 02:45 an – genau während der Sicherung:



Die Zeitplanung lässt sich aber im Servermanager anpassen.

Zusammenfassung

Insgesamt habe ich mein Ziel erreicht: Der DPM läuft mit der aktuellen Version 2019 auf einem Windows Server 2019. Nur der Weg sah leider nicht so aus, wie ich es geplant hatte. Durch ein Inplace-Upgrade des SQL-Servers, des DPM-Servers und des Windows-Servers hätte ich meine alten Datensicherungen einfach weiterführen können. Aber Inplace … wie es aussehen kann habe ich seitenweise beschrieben. Und selbst wenn ich einen Weg durch die Probleme des Upgrades finde:

Wer garantiert mir, dass der DPM danach auf lange Sicht betrachtet auch wirklich stabil läuft – und im Worstcase auf zuverlässig die Backups erfolgreich wiederherstellt?? Eben.

In meiner kleinen Umgebung konnte ich auf meinen Backupbestand verzichten. In großen Infrastrukturen muss die Sicherung Side-By-Side neu aufgebaut werden. Noch einmal ein Inplace? Nein danke!