

Inhalt

Zielsetzung	2
Migration der Windows Server und der Exchange Server	2
Der Mailservice	2
Vorbereitung	3
Aufbau der neuen VM.....	3
Bereitstellung des neuen Betriebssystems	4
Sammlung von Informationen und Elementen im alten Server	7
Maintenance vorbereiten.....	9
Entfernung der alten Exchange-Installation	12
Bereinigungen in der Rolle MBS	12
Umbenennen der neuen Datenbanken	13
Bereinigungen in der Rolle HTS.....	17
Deinstallation des Exchange Servers	17
Entfernung des alten Servers und Austausch der VM.....	22
Bereitstellung des neuen Mailservers (MX2019).....	26
Grundkonfiguration des Betriebssystems.....	26
Einrichtung der Datensicherung (BMR mit Windows Server Sicherung)	31
Installation des Exchange Servers 2019 CU4.....	33
Konfiguration der Rolle CAS.....	40
Konfiguration der Virtual Directories.....	40
Installation des Serverzertifikates	41
Umstellung auf Kerberos-Authentication	41
Testlauf im Loadbalancer	43
Produktivschaltung der CAS-Rolle	44
Konfiguration der Rolle HTS	45
Verschiebung der Transportdatenbank.....	45
Aktivierung der AntiSpam und AntiMalware-Features.....	46
Konfiguration der Konnektoren	48
Testlauf und Produktivschaltung	49
Konfiguration der Rolle MBS.....	51
Beitritt zur Datenbankverfügbarkeitsgruppe	51
Konfiguration der Datenbanken – Problem beim Seeding.....	51
Konfigurieren der Datenbanken – mit Erfolg	58
Konfiguration der Datensicherung mit dem DPM.....	59
Integration des neuen Servers im DPM – Problem: keine Sicherung.....	59
Problem: Clusterfehler	65
Nacharbeiten	80
Lizensierung des Exchange Servers.....	80
Logfile-Optimierung.....	80
Konfiguration des Monitorings.....	81
Abschluss der Migration.....	83
Zusammenfassung.....	83

Zielsetzung

Migration der Windows Server und der Exchange Server

Meine Infrastruktur soll auf Windows Server 2019 aktualisiert werden. In diesem Abschnitt der Umstellung sind meine beiden Exchange Server dran. Beide laufen als virtuelle Maschine auf je einem Hyper-V-Host.

Mit Windows Server 2019 als Betriebssystem kann ich gleichzeitig auf Exchange Server 2019 migrieren.

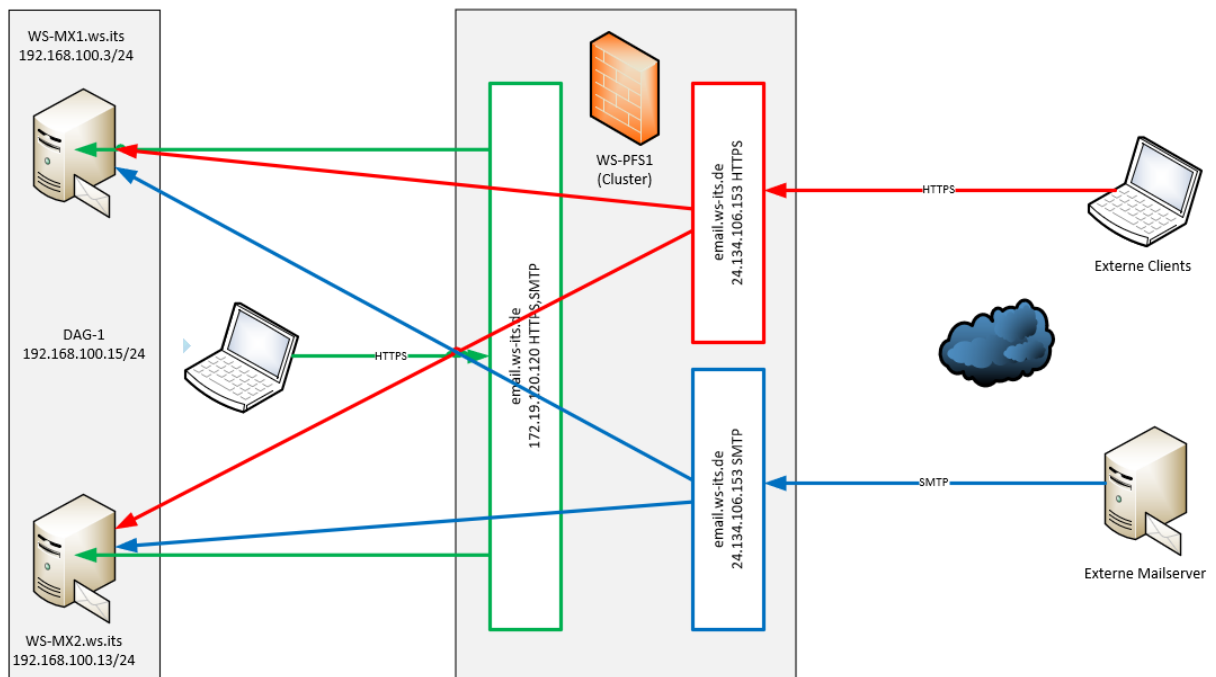
Die Migration wird durch ein Wipe & Load je Server durchgeführt. Dabei deinstalliere ich jeweils einen Exchange Server, entferne das alte Betriebssystem, installiere einen neuen Windows Server 2019 und installiere darauf den neuen Exchange Server.

Wichtig ist mir dabei, dass der Mailservice ohne Unterbrechung weiterläuft. Die fehlende Hochverfügbarkeit während der Umstellung kann ich akzeptieren.

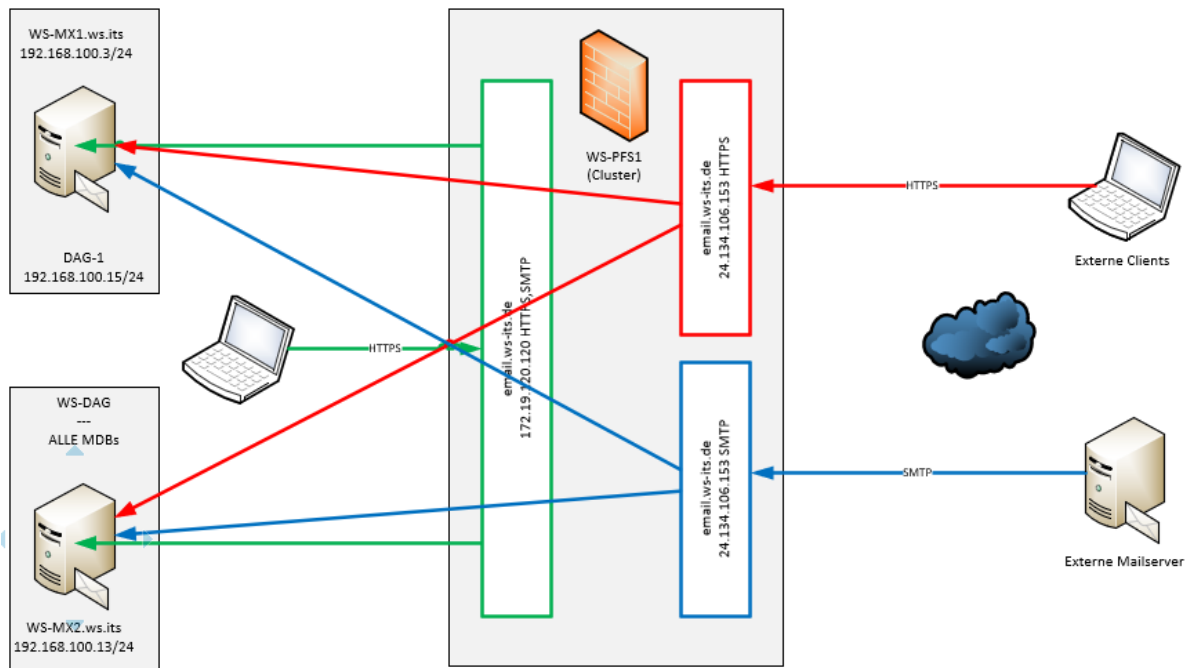
Der Mailservice

Den Mailserver WS-MX2 habe ich bereits auf Windows Server 2019 und Exchange Server 2019 umgestellt. Jetzt ist der Server WS-MX1 an der Reihe. Auf diesem sind nur noch die Rollen Hubtransport und ClientAccess aktiv. Alle Datenbanken laufen bereits auf dem neuen Server. Nach der Neuinstallation soll eine Datenbankverfügbarkeitsgruppe die Ausfallsicherheit gewährleisten. Aktuell ist die Verfügbarkeit also eingeschränkt.

Das war meine ursprüngliche Mailserver-Infrastruktur:



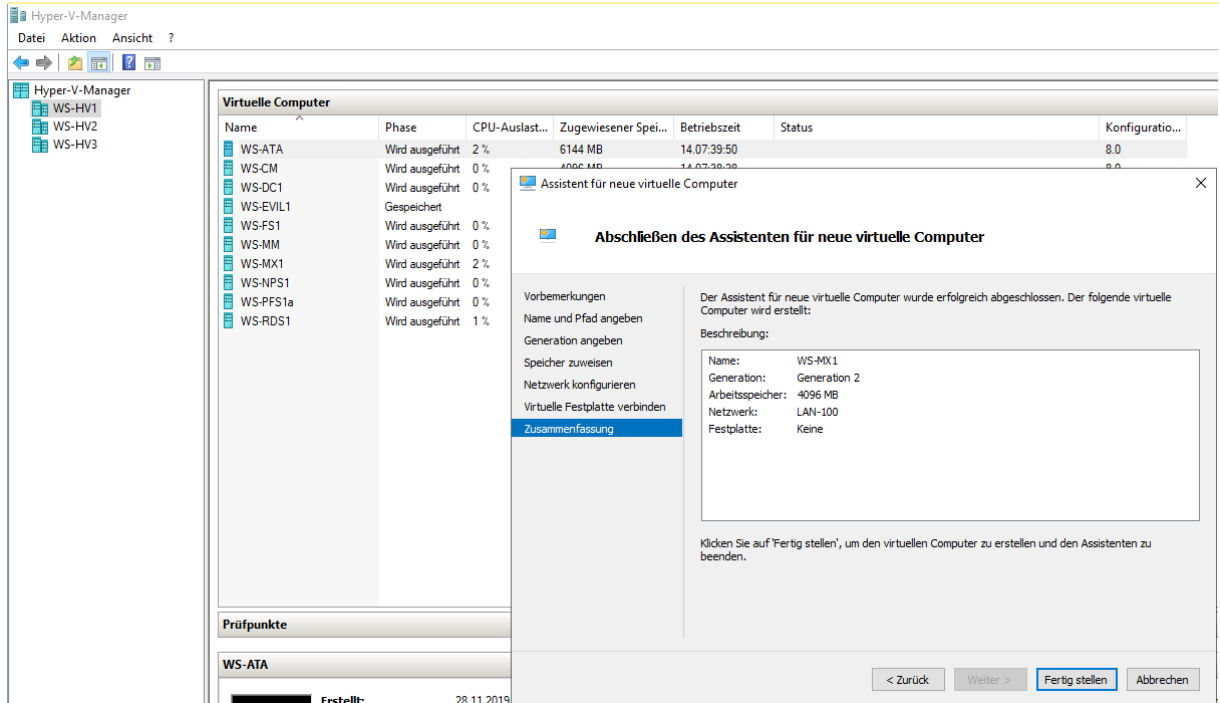
Und das ist der aktuelle Stand:



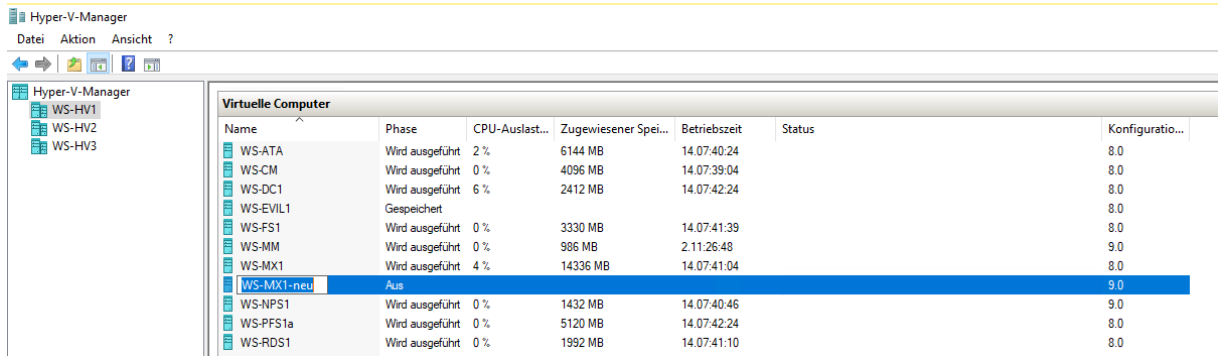
Vorbereitung

Aufbau der neuen VM

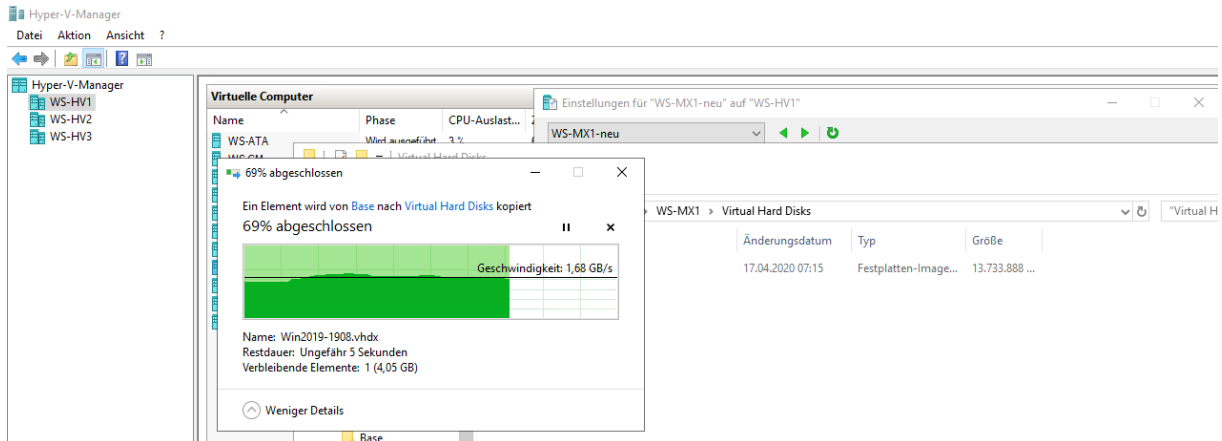
Zuerst baue ich eine neue virtuelle Maschine in dem gleichen Hyper-V-Host, der auch den alten Mailserver beheimatet. Ich führe die Migration als Wipe & Load aus, daher verwende ich die Namen und IP-Adressen der Server wieder:



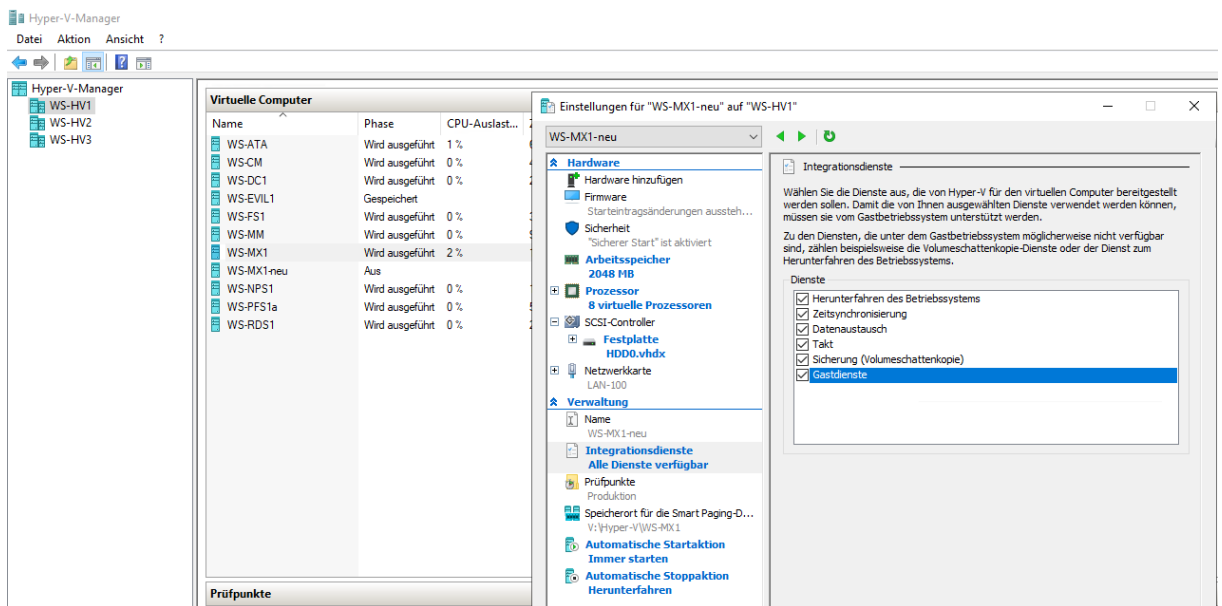
Damit ich zwischenzeitlich nicht durcheinander komme, benenne ich den neuen Server um:



Die Installation führe ich wie immer mit einer vorinstallierten VHDX aus. Diese enthält ein vorbereitetes Betriebssystem:



Die Kopie meiner Basefile hänge ich in die VM ein. Ebenso gibt es noch etwas mehr Hardware:



Der gesamte Vorgang dauert nur wenige Minuten.

Bereitstellung des neuen Betriebssystems

Nach dem Einschalten der neuen VM kann ich mich mit der Konsole verbinden. Hier wartet nach wenigen Sekunden der Einrichtungsassistent auf mich:

Hallo

Lassen Sie uns zunächst einige grundlegende Dinge klären.

Was ist Ihr Heimatland/Ihre Heimatregion?


Deutschland

Was ist Ihre bevorzugte App-Sprache?

Deutsch (Deutschland)

Welches Tastaturlayout möchten Sie verwenden?

Deutsch

 [Weiter](#)


Einstellungen anpassen

Geben Sie ein Kennwort für das integrierte Administratorkonto ein, mit dem Sie sich an diesem Computer anmelden können.

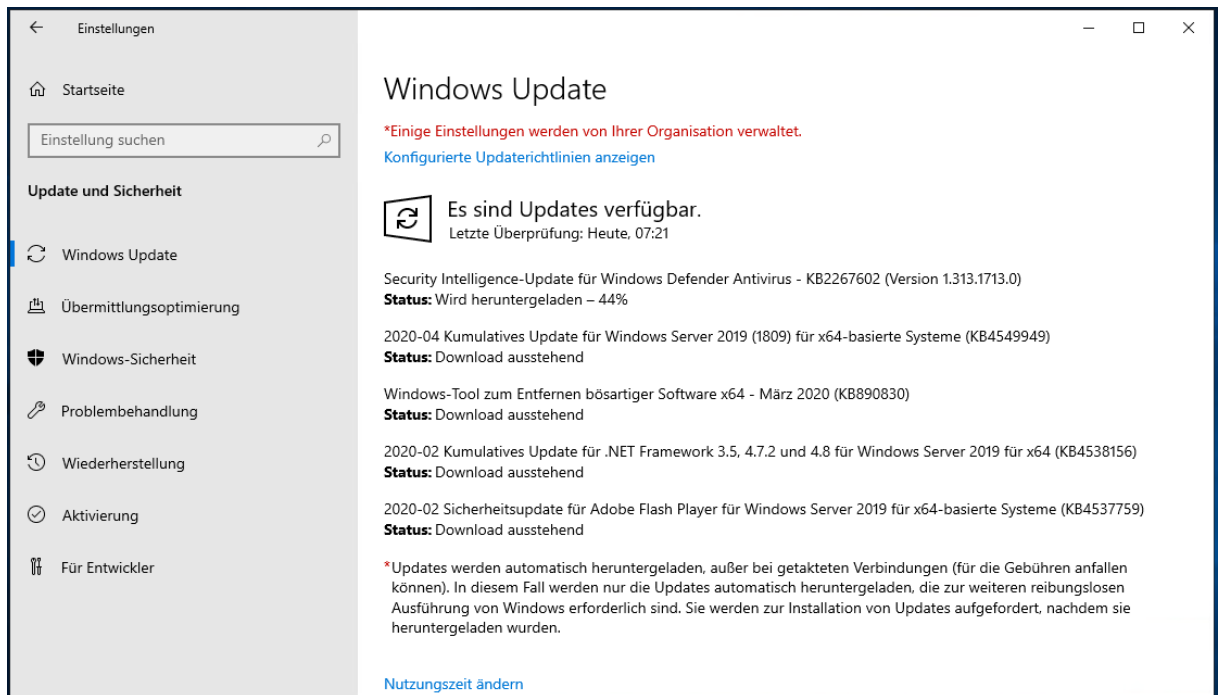
Benutzername: Administrator

Kennwort:

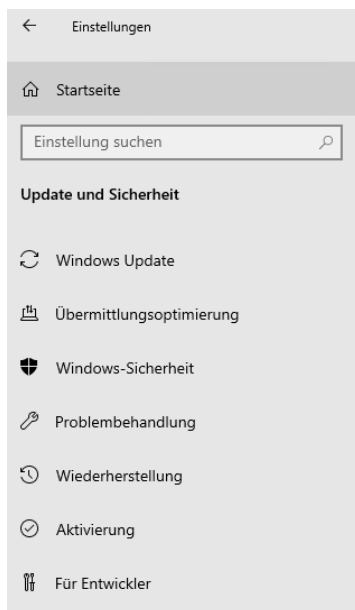
Kennwort erneut eingeben:

 [Zurück](#) [Fertig stellen](#)

Danach kann ich mich bereits lokal anmelden. Ich verschiebe den Server fix ins Client-LAN, damit ich die Aktivierung und neue Patches online beziehen kann – im Servernetz sind die Systeme isoliert. Die Updates sind schnell gefunden:



Nach einem Neustart suche ich weitere Updates:



Dann ist das System Up-To-Date:

← Einstellungen

Updateverlauf anzeigen

[Updates deinstallieren](#)

[Wiederherstellungsoptionen](#)

Updateverlauf

✓ Qualitätsupdates (3)

[2020-02 Kumulatives Update für .NET Framework 3.5, 4.7.2 und 4.8 für Windows Server 2019 für x64 \(KB4538156\)](#)

Erfolgreich installiert am 17.04.2020

[2020-02 Sicherheitsupdate für Adobe Flash Player für Windows Server 2019 für x64-basierte Systeme \(KB4537759\)](#)

Erfolgreich installiert am 17.04.2020

[2020-04 Kumulatives Update für Windows Server 2019 \(1809\) für x64-basierte Systeme \(KB4549949\)](#)

Erfolgreich installiert am 17.04.2020

✓ Definitionsupdates (2)

[Update für Windows Defender Antivirus-Antischadsoftwareplattform – KB4052623 \(Version 4.18.2003.8\)](#)

Erfolgreich installiert am 17.04.2020

[Security Intelligence-Update für Windows Defender Antivirus - KB2267602 \(Version 1.313.1713.0\)](#)

Erfolgreich installiert am 17.04.2020

✓ Weitere Updates (1)

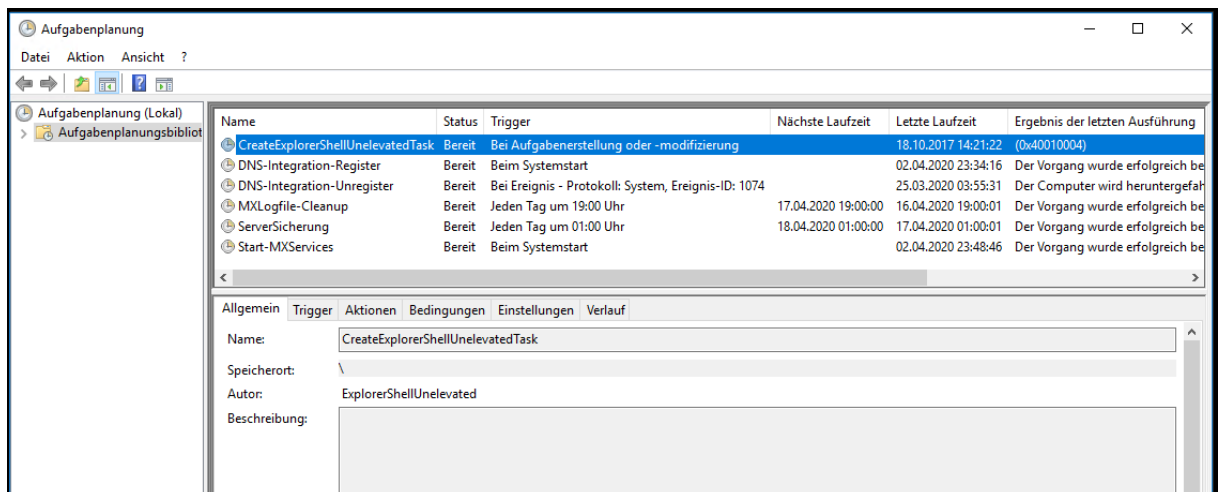
[Windows-Tool zum Entfernen bösartiger Software x64 - März 2020 \(KB890830\)](#)

Erfolgreich installiert am 17.04.2020

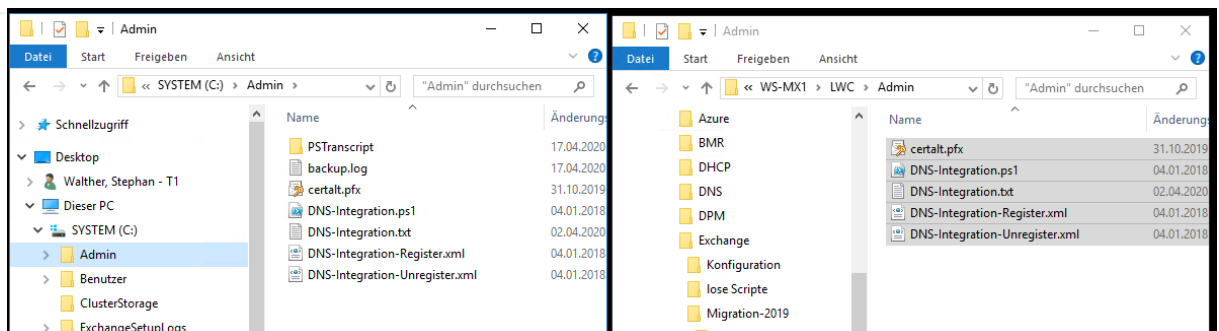
Die Aktivierung ist ebenfalls erledigt.

Sammlung von Informationen und Elementen im alten Server

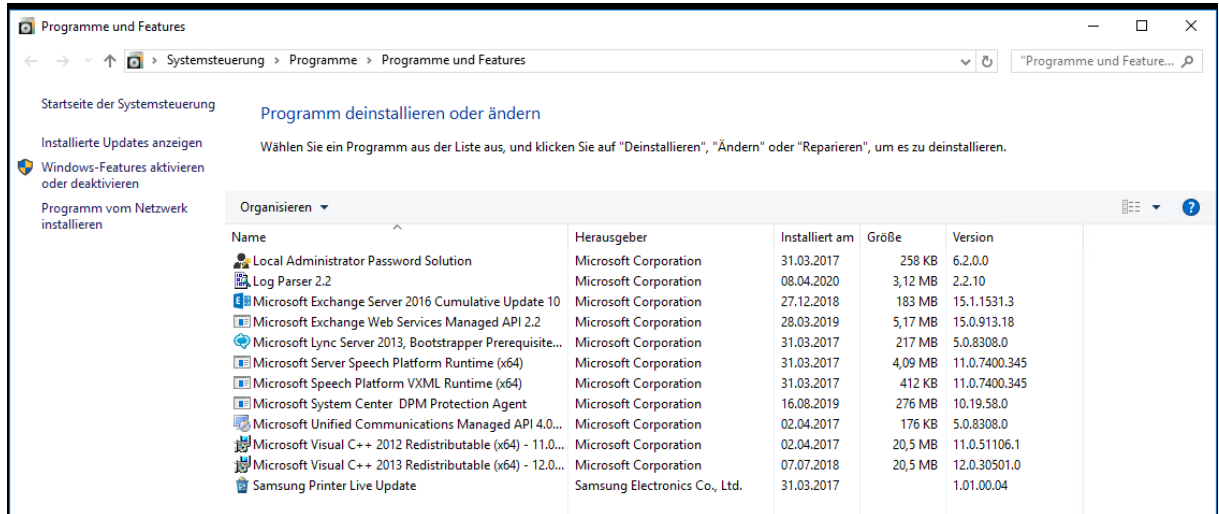
Nun geht es weiter auf dem alten Server. Hier sammle ich wieder Informationen. Dazu gehören geplante Aufgaben. Diese kann ich mit einem einfachen Rechtsklick in xml-Dateien exportieren:



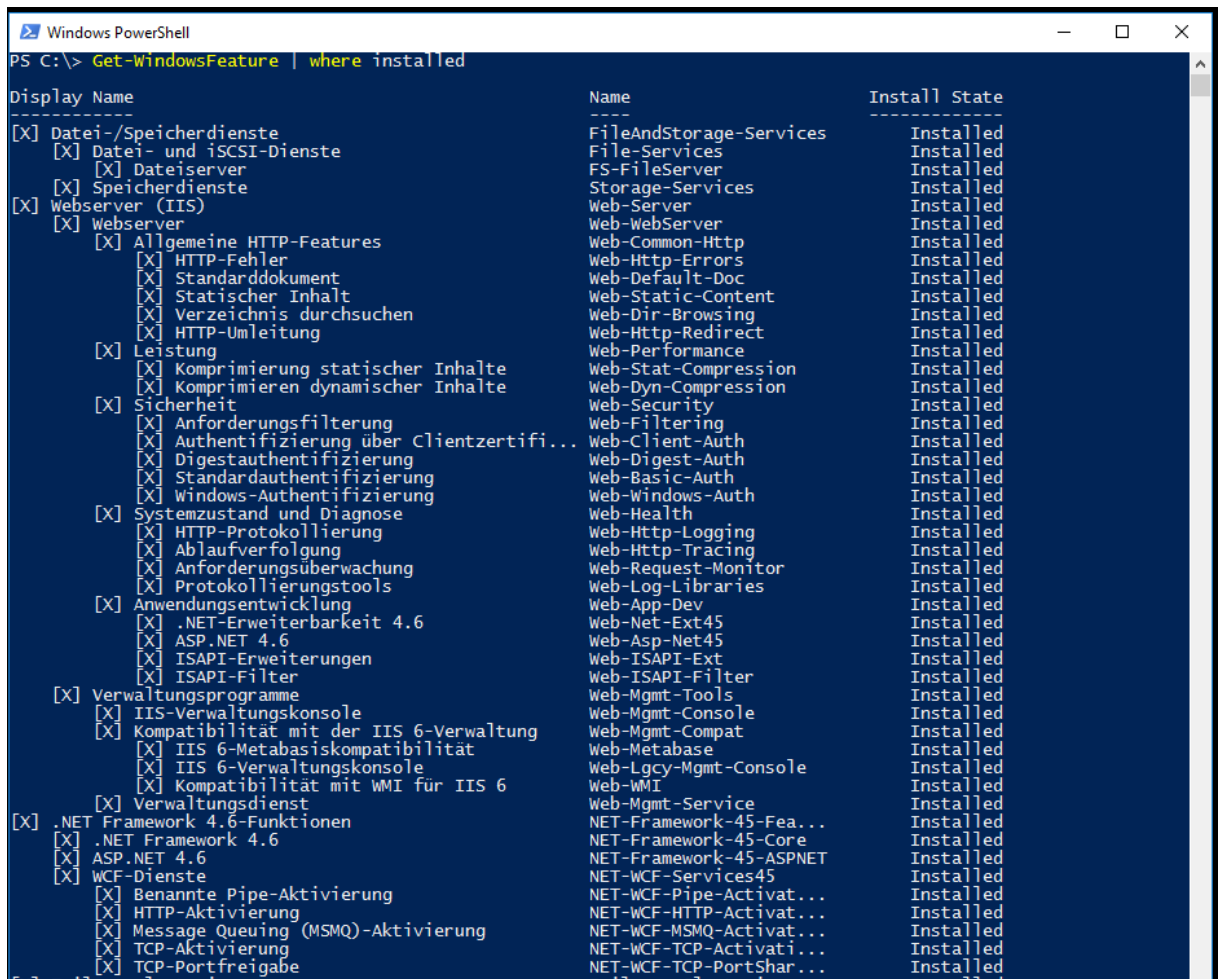
Die Dateien lege ich in meinem Admin-Verzeichnis lokal ab. Das gesamte Verzeichnis kopiere ich auf meinen Fileserver:



Danach verschaffe ich mir einen Überblick über lokal installierte Anwendungen:



Wichtig sind auch die installierten Rollen und Features:



[X] Failoverclustering	Failover-Clustering	Installed
[X] Media Foundation	Server-Media-Foundation	Installed
[X] Message Queuing	MSMQ	Installed
[X] Message Queuing-Dienste	MSMQ-Services	Installed
[X] Message Queuing-Server	MSMQ-Server	Installed
[X] Remoteserver-Verwaltungstools	RSAT	Installed
[X] Featureverwaltungstools	RSAT-Feature-Tools	Installed
[X] Failoverclustering-Tools	RSAT-Clustering	Installed
[X] Failoverclustermodule für Windows Pow...	RSAT-Clustering-Powe...	Installed
[X] Failovercluster-Verwaltungstools	RSAT-Clustering-Mgmt	Installed
[X] Failovercluster-Befehlschnittstelle	RSAT-Clustering-CmdI...	Installed
[X] Server für Failoverclusterautomatisi...	RSAT-Clustering-Auto...	Installed
[X] Rollenverwaltungstools	RSAT-Role-Tools	Installed
[X] AD DS- und AD LDS-Tools	RSAT-AD-Tools	Installed
[X] Active Directory-Modul für Windows P...	RSAT-AD-PowerShell	Installed
[X] AD DS-Tools	RSAT-ADDS	Installed
[X] Active Directory-Verwaltungszentrum	RSAT-AD-AdminCenter	Installed
[X] AD DS-Snap-Ins und -Befehlszeile...	RSAT-ADDS-Tools	Installed
[X] DNS-Servertools	RSAT-DNS-Server	Installed
[X] RPC-über-HTTP-Proxy	RPC-over-HTTP-Proxy	Installed
[X] Unterstützung für die SMB 1.0/CIFS-Dateifreigabe	FS-SMB1	Installed
[X] Windows Defender-Features	Windows-Defender-Fea...	Installed
[X] Windows Defender	Windows-Defender	Installed
[X] GUI für Windows Defender	Windows-Defender-Gui	Installed
[X] Windows Identity Foundation 3.5	Windows-Identity-Fou...	Installed
[X] Windows PowerShell	PowerShellRoot	Installed
[X] Windows PowerShell 5.1	PowerShell	Installed
[X] Windows PowerShell ISE	PowerShell-ISE	Installed
[X] Windows Server-Sicherung	Windows-Server-Backup	Installed
[X] Windows-Prozessaktivierungsdienst	WAS	Installed
[X] Prozessmodell	WAS-Process-Model	Installed
[X] Konfigurations-APIs	WAS-Config-APIs	Installed
[X] Wow64-Unterstützung	Wow64-Support	Installed

Die IP-Konfiguration ist mir bekannt. Eine schnelle Dokumentation kann aber nicht schaden:

```

Windows PowerShell
PS C:\> ipconfig /all

Windows-IP-Konfiguration

    Hostname . . . . . : WS-MX1
    Primäres DNS-Suffix . . . . . : ws.its
    Knotentyp . . . . . : Peer-Peer
    IP-Routing aktiviert . . . . . : Nein
    WINS-Proxy aktiviert . . . . . : Nein
    DNS-Suffixsuchliste . . . . . : ws.its

Tunneladapter LAN-Verbindung* 2:

    Medienstatus. . . . . : Medium getrennt
    Verbindungsspezifisches DNS-Suffix:
    Beschreibung. . . . . : Microsoft Failover Cluster Virtual Adapter
    Physische Adresse . . . . . : 02-A2-04-77-4E-B1
    DHCP aktiviert. . . . . : Nein
    Autokonfiguration aktiviert . . . : Ja

Ethernet-Adapter Ethernet:

    Verbindungsspezifisches DNS-Suffix:
    Beschreibung. . . . . : Microsoft Hyper-V Network Adapter
    Physische Adresse . . . . . : 00-15-5D-F9-A7-0E
    DHCP aktiviert. . . . . : Nein
    Autokonfiguration aktiviert . . . : Ja
    Verbindungslokale IPv6-Adresse . . : fe80::c4cd:dae5:a734:bc11%3(Bevorzugt)
    IPv4-Adresse . . . . . : 192.168.100.3(Bevorzugt)
    Subnetzmaske . . . . . : 255.255.255.0
    IPv4-Adresse . . . . . : 192.168.100.15(Bevorzugt)
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.100.252
    DHCPv6-IAID . . . . . : 50337117
    DHCPv6-Client-DUID. . . . . : 00-01-00-01-26-18-12-91-00-15-5D-F9-A7-0E
    DNS-Server . . . . . : 192.168.100.1
    . . . . . : 192.168.100.2
    NetBIOS über TCP/IP . . . . . : Aktiviert

Tunneladapter isatap.{242C468F-47C3-4724-96CF-E244D12FFF31}:
  
```

Mehr ist auf dem Server nicht zu finden.

Maintenance vorbereiten

Jetzt kann ich die Wartung für die Deinstallation einleiten. So verhindere ich unnötige Alarm-Meldungen von meinem Monitoring. Ich pausiere im PRTG einfach alle zum Server WS-MX1 gehörenden Sensoren:

Der ClientAccess-Service ist noch aktiv. Vorgeschaltet arbeitet meine PfSense mit einem HAProxy als Loadbalancer. Der Traffic ist rechts im Bild sichtbar:

In der Backend-Konfiguration des HAProxies kann ich den Server deaktivieren. Das nehme ich für CAS und HTS vor:

Services / HAProxy / Backend / Edit

Settings Frontend Backend Files Stats Stats FS Templates

Edit HAProxy Backend server pool

Name: SMTP

Server list

Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Action
disabled	WS-MX1	Address+Port	192.168.100.3	25	<input type="checkbox"/>	<input type="checkbox"/>		
active	WS-MX2	Address+Port:	192.168.100.13	25	no	no		

Services / HAProxy / Backend / Edit

Settings Frontend Backend Files Stats Stats FS Templates

Edit HAProxy Backend server pool

Name: MX

Server list

Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Action
disabled	WS-MX1	Address+Port	192.168.100.3	443	<input type="checkbox"/>	<input type="checkbox"/>		
active	WS-MX2	Address+Port:	192.168.100.13	443	no	no		

Neue Verbindungen von Clients und neue SMTP-Verbindungen werden jetzt nur noch dem neuen Server WS-MX2 zugewiesen:

Short Alerts

Interface/Time	Src/Dst Address	Description
DMZ_120_EXTERN Apr 17 07:36:59	192.168.110.104:49682 52.167.64.67:80	ET USER_AGENTS Microsoft Device Metadata Retrieval...
LAN_110_CLIENTS Apr 17 07:36:59	192.168.110.104:49682 52.167.64.67:80	ET USER_AGENTS Microsoft Device Metadata Retrieval...
DMZ_120_EXTERN Apr 17 07:36:59	192.168.110.104:49688 23.214.174.91:80	ET USER_AGENTS Microsoft Device Metadata Retrieval...
LAN_110_CLIENTS Apr 17 07:36:59	192.168.110.104:49688 23.214.174.91:80	ET USER_AGENTS Microsoft Device Metadata Retrieval...
DMZ_120_EXTERN Apr 17 07:36:59	192.168.110.104:49682 52.167.64.67:80	ET USER_AGENTS Microsoft Device Metadata Retrieval...

Firewall Logs

Act	Time	IF	Source	Destination

HAProxy

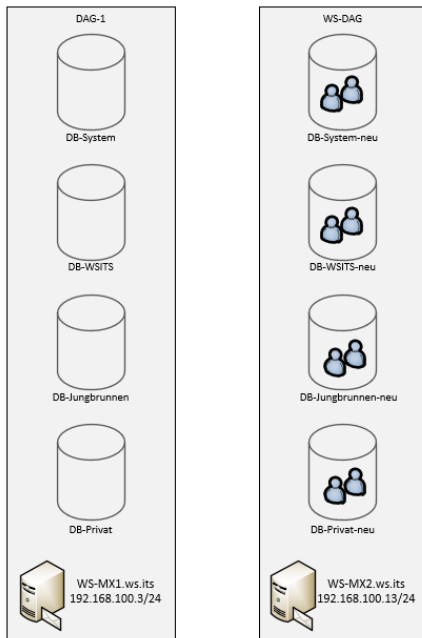
Backend(s)/Server(s)	Sessions (cur/max)	Status / Actions
RDSWEB_ipvANY WS-RDS1	0 / 200	
MX_ipvANY WS-MX1 WS-MX2	1 / 200 MAINT 1	
192.168.100.22:59873	9s / 0x80242ac00	
RDS_ipvANY WS-RDS2	0 / 200	
PRTG_ipvANY WS-MON	0 / 200	
SMTP_ipv4 WS-MX1 WS-MX2	0 / 200 MAINT 0	

Jetzt kann die Deinstallation des alten Servers beginnen.

Entfernung der alten Exchange-Installation

Bereinigungen in der Rolle MBS

Eine Deinstallation des Exchange Servers 2016 kann nur gelingen, wenn alle Voraussetzungen erfüllt sind. Eine davon sagt: Es dürfen keine Mailboxdatenbanken zugewiesen sein. Der alte Server hat noch 4 leere Datenbanken und ist noch Mitglied in der alten DAG. Die Mailboxen hatte ich bei der letzten Migration schon in 4 neue Datenbanken auf den neuen Server verschoben. Die Namen der Datenbanken musste ich dabei neu vergeben, da Exchange die Namen nur einmal in der Organisation vergeben kann. Das hier ist also das aktuelle Layout:



Diese alten, leeren Datenbanken entferne ich mit einer Anweisung in der PowerShell ISE. Die Warnungen kann ich ignorieren:

```

247
248 #region Entfernung der Rolle MBS auf WS-MX1
249 # Entfernen der alten Datenbanken
250 Get-MailboxDatabase -Server "WS-MX1" | Remove-MailboxDatabase

PS C:\> Get-MailboxDatabase -Server "WS-MX1" | Remove-MailboxDatabase
WARNUNG: Fehler beim Entfernen von Überwachungspostfachobjekt von Datenbank "DB-System". Ausnahme: Fehler bei Active Directory
-Vorgang mit WS-DC2.ws.its. Bei diesem Fehler ist kein Wiederholungsversuch möglich. Zusätzliche Informationen: Zugriff verweigert.
Active Directory-Antwort: 00000005: SecErr: DSID-03152763, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0

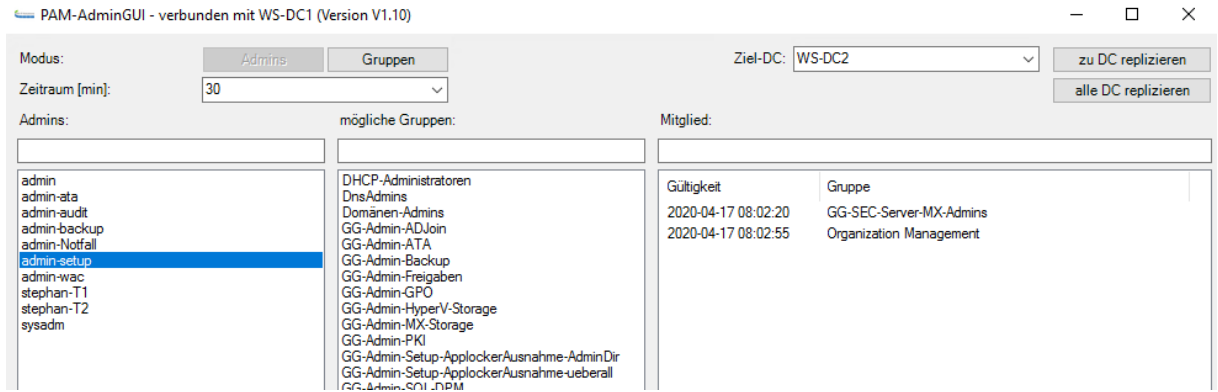
WARNUNG: Die angegebene Datenbank wurde entfernt. Sie müssen die Datenbankdatei unter dem Pfad E:\Exchange\DB-System\DB-System.edb manuell vom Computer entfernen, wenn sie vorhanden ist. Angegebene Datenbank: DB-System
WARNUNG: Mit dem Cluster auf Server 'WS-MX1.ws.its' konnte keine Verbindung hergestellt werden. Fehler: Fehler beim Ausführen eines Clustervorgangs. Fehler: Fehler für Cluster-API: "Fehler von IsInstalled(WS-MX1.ws.its) mit 0x5. Fehler: Zugriff verweigert"
WARNUNG: Fehler beim Entfernen von Überwachungspostfachobjekt von Datenbank "DB-WSITS". Ausnahme: Fehler bei Active Directory-Vorgang mit WS-DC2.ws.its. Bei diesem Fehler ist kein Wiederholungsversuch möglich. Zusätzliche Informationen: Zugriff verweigert.
Active Directory-Antwort: 00000005: SecErr: DSID-03152763, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0

WARNUNG: Die angegebene Datenbank wurde entfernt. Sie müssen die Datenbankdatei unter dem Pfad E:\Exchange\DB-WSITS\DB-WSITS.edb manuell vom Computer entfernen, wenn sie vorhanden ist. Angegebene Datenbank: DB-WSITS
WARNUNG: Mit dem Cluster auf Server 'WS-MX1.ws.its' konnte keine Verbindung hergestellt werden. Fehler: Fehler beim Ausführen eines Clustervorgangs. Fehler: Fehler für Cluster-API: "Fehler von IsInstalled(WS-MX1.ws.its) mit 0x5. Fehler: Zugriff verweigert"
WARNUNG: Fehler beim Entfernen von Überwachungspostfachobjekt von Datenbank "DB-Jungbrunnen". Ausnahme: Fehler bei Active Directory-Vorgang mit WS-DC2.ws.its. Bei diesem Fehler ist kein Wiederholungsversuch möglich. Zusätzliche Informationen: Zugriff verweigert.
Active Directory-Antwort: 00000005: SecErr: DSID-03152763, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0

WARNUNG: Die angegebene Datenbank wurde entfernt. Sie müssen die Datenbankdatei unter dem Pfad E:\Exchange\DB-Jungbrunnen\DB-Jungbrunnen.edb manuell vom Computer entfernen, wenn sie vorhanden ist. Angegebene Datenbank: DB-Jungbrunnen
WARNUNG: Mit dem Cluster auf Server 'WS-MX1.ws.its' konnte keine Verbindung hergestellt werden. Fehler: Fehler beim Ausführen eines Clustervorgangs. Fehler: Fehler für Cluster-API: "Fehler von IsInstalled(WS-MX1.ws.its) mit 0x5. Fehler: Zugriff verweigert"
WARNUNG: Fehler beim Entfernen von Überwachungspostfachobjekt von Datenbank "DB-Privat". Ausnahme: Fehler bei Active Directory-Vorgang mit WS-DC2.ws.its. Bei diesem Fehler ist kein Wiederholungsversuch möglich. Zusätzliche Informationen: Zugriff verweigert.

```

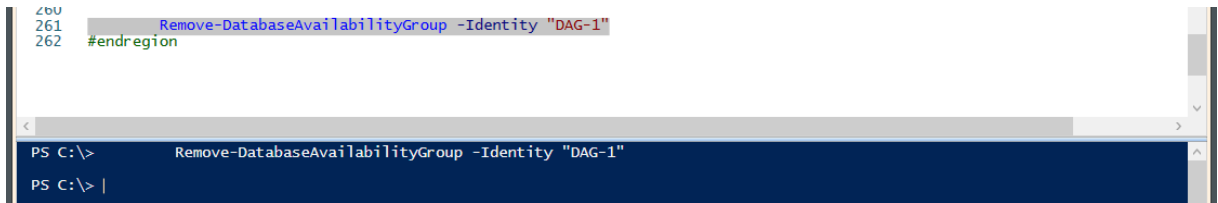
Weiter geht es mit dem alten DAG-Cluster. Die Administration gelingt nur mit einem NTLM-fähigen AdminAccount. Da mein regulärer Account durch die Mitgliedschaft in der Gruppe „Protected Users“ kein NTLM verwenden kann, konfiguriere ich mir mit meinem PAM-Tool einen temporären AdminAccount:



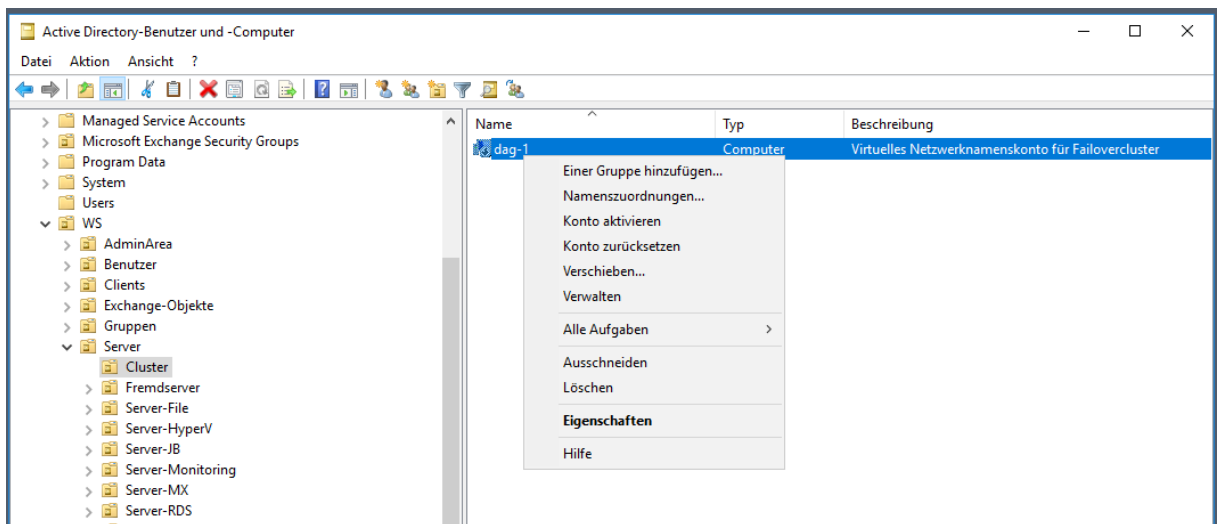
Mit dem Login Admin-Setup starte ich eine Exchange Management Shell. Jetzt kann ich den Server aus dem DAG-Cluster entfernen:



Danach entferne ich die nun leere DAG-1:

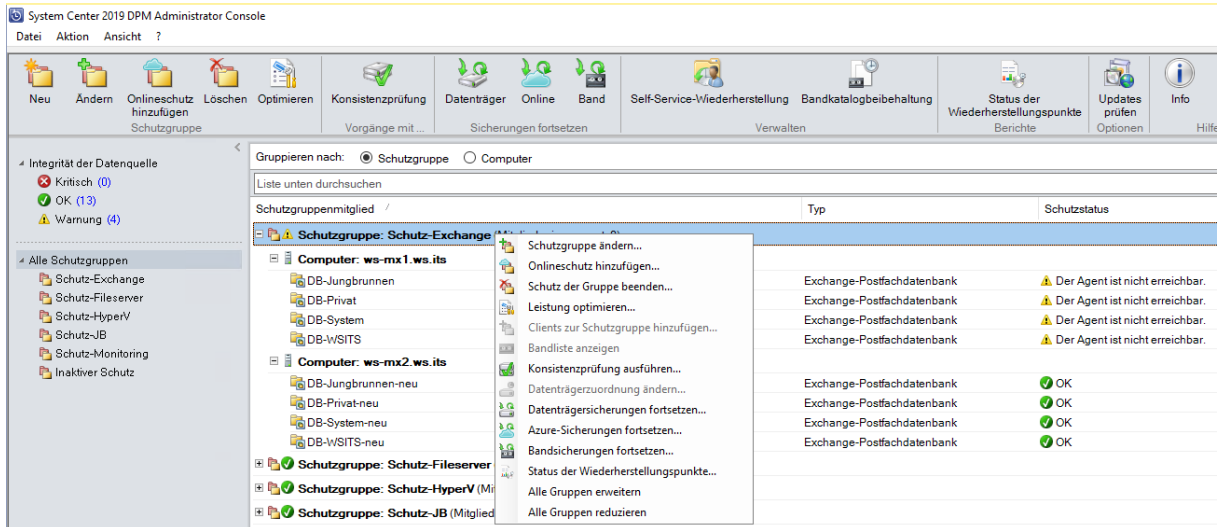


Das dazugehörige AD-Computerkonto entferne ich im Active Directory:

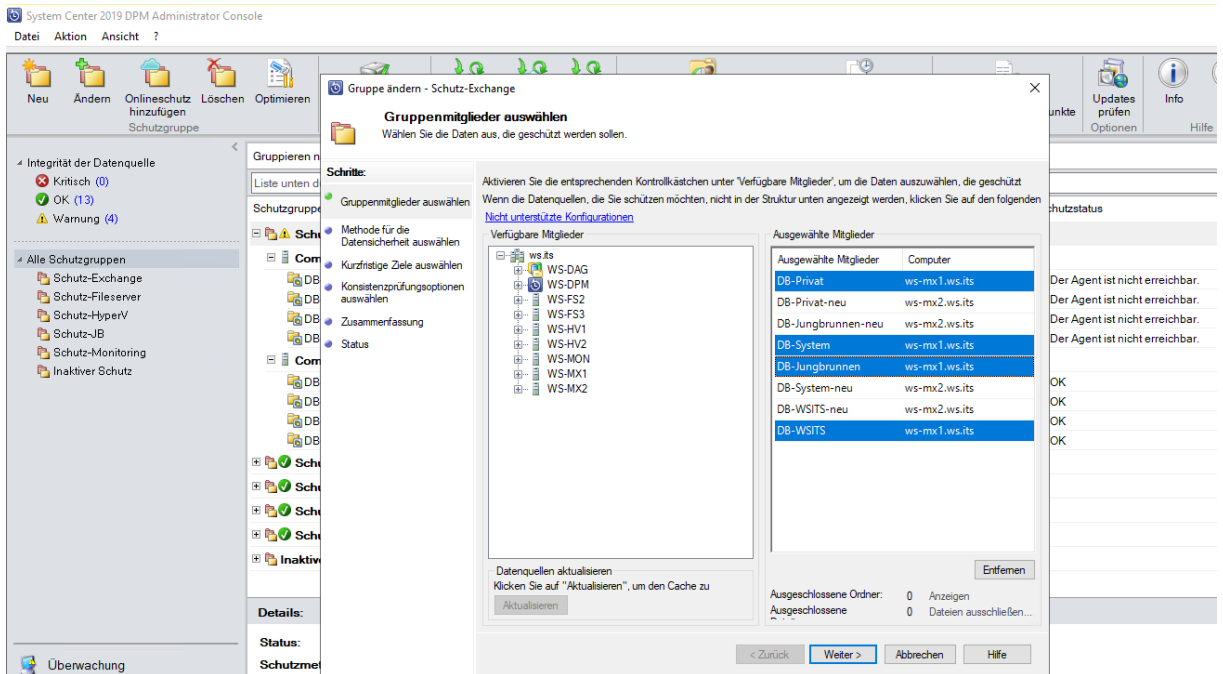


Umbenennen der neuen Datenbanken

Jetzt kann ich die Namen der neuen Datenbanken anpassen und den Suffix ,-neu' entfernen. Vorher passe ich aber meine Datensicherung im Data Protection Manager an. Hier sind die leeren, alten Datenbanken und auch die neuen mit dem temporären Namen gelistet:



Ich entferne die alten Datenbanken aus der Sicherung:



Ein paar Klicks später sind nur noch die neuen DBs gelistet. Diese kann ich nun im Exchange Server WS-MX2 umbenennen. Das könnte ich mit 4 Einzeilern erledigen. Wenn es mehr Datenbanken werden, bietet sich eine Foreach-Schleife an:

```

279 #region Umbenennen der Datenbanken
280 # Konfiguration der bestehenden Datenbanken
281 Get-MailboxDatabase |
282 ForEach-Object {
283     $NameAkt = $_.name
284     $NameNeu = $NameAkt -replace '-neu'
285
286     Set-MailboxDatabase -Identity $NameAkt -Name $NameNeu
287 }
288 #endregion
    
```



```

PS C:\> Get-MailboxDatabase

Name                Server      Recovery    ReplicationType
-----
DB-System-neu       WS-MX2     False      None
DB-WSITS-neu        WS-MX2     False      None
DB-Jungbrunnen-neu WS-MX2     False      None
DB-Privat-neu       WS-MX2     False      None
    
```



```

PS C:\> Get-MailboxDatabase |
ForEach-Object {
    $NameAkt = $_.name
    $NameNeu = $NameAkt -replace '-neu'

    Set-MailboxDatabase -Identity $NameAkt -Name $NameNeu
}

PS C:\> Get-MailboxDatabase

Name                Server      Recovery    ReplicationType
-----
DB-System           WS-MX2     False      None
DB-WSITS            WS-MX2     False      None
DB-Jungbrunnen     WS-MX2     False      None
DB-Privat           WS-MX2     False      None
    
```

Meine Hoffnung ist nun, dass der Data Protection Manager die Datenbanken nicht nach ihrem Anzeigenamen, sondern deren GUID identifiziert. Dann müsste er den Anzeigenamen bei der nächsten Sicherung anpassen. Das probiere ich jetzt aus:

System Center 2019 DPM Administrator Console

Gruppieren nach: Schutzgruppe Computer

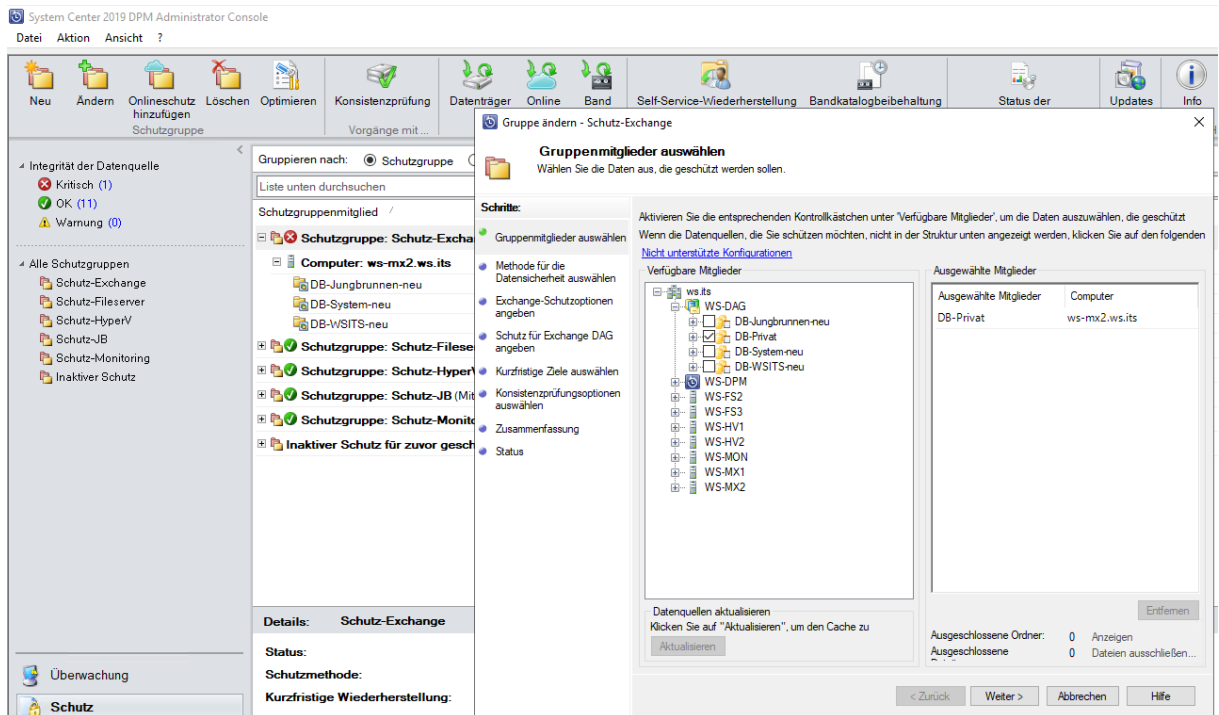
Schutzgruppenmitglied	Typ	Schutzstatus
Schutzgruppe: Schutz-Exchange (Mitglieder insgesamt: 4)		
Computer: ws-mx2.ws.its		
DB-Jungbrunnen-neu	Exchange-Postfachdatenbank	OK
DB-Privat-neu	Exchange-Postfachdatenbank	OK
DB-System-neu	Exchange-Postfachdatenbank	OK
DB-WSITS-neu	Exchange-Postfachdatenbank	OK

System Center 2019 DPM Administrator Console

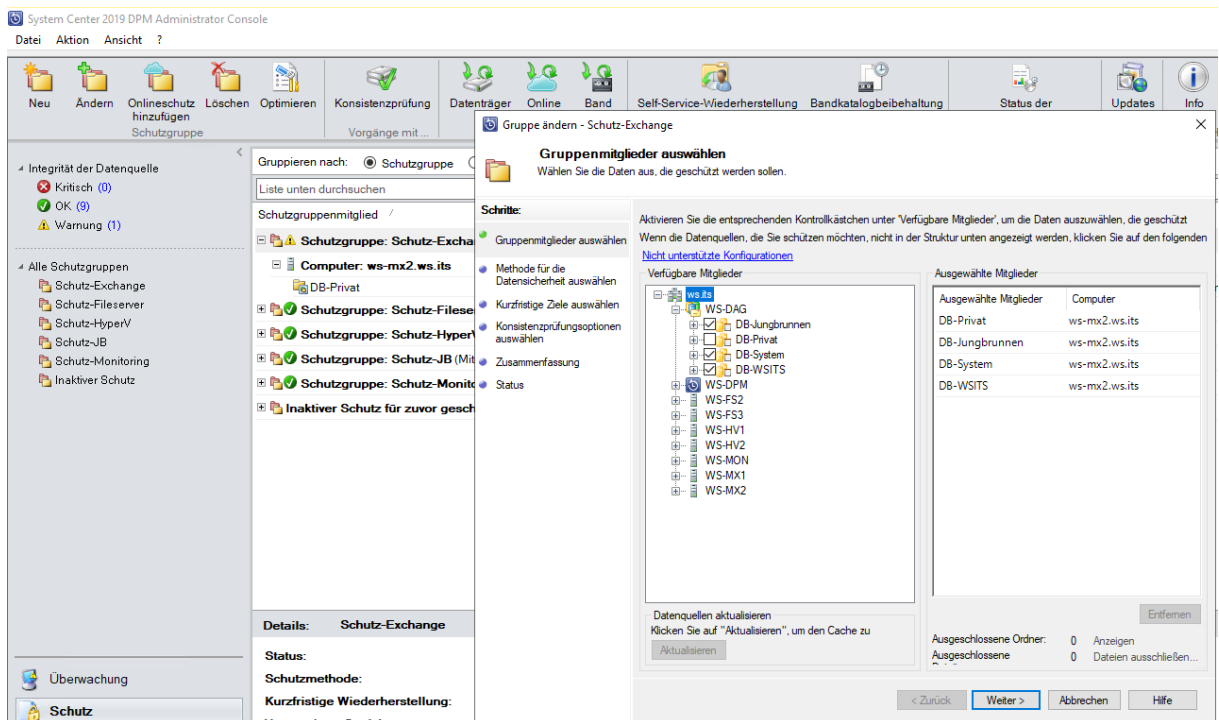
Gruppieren nach: Schutzgruppe Computer

Schutzgruppenmitglied	Typ	Schutzstatus
Schutzgruppe: Schutz-Exchange (Mitglieder insgesamt: 4)		
Computer: ws-mx2.ws.its		
DB-Jungbrunnen-neu	Exchange-Postfachdatenbank	Replikat inkonsistent
DB-Privat-neu	Exchange-Postfachdatenbank	OK
DB-System-neu	Exchange-Postfachdatenbank	OK
DB-WSITS-neu	Exchange-Postfachdatenbank	OK

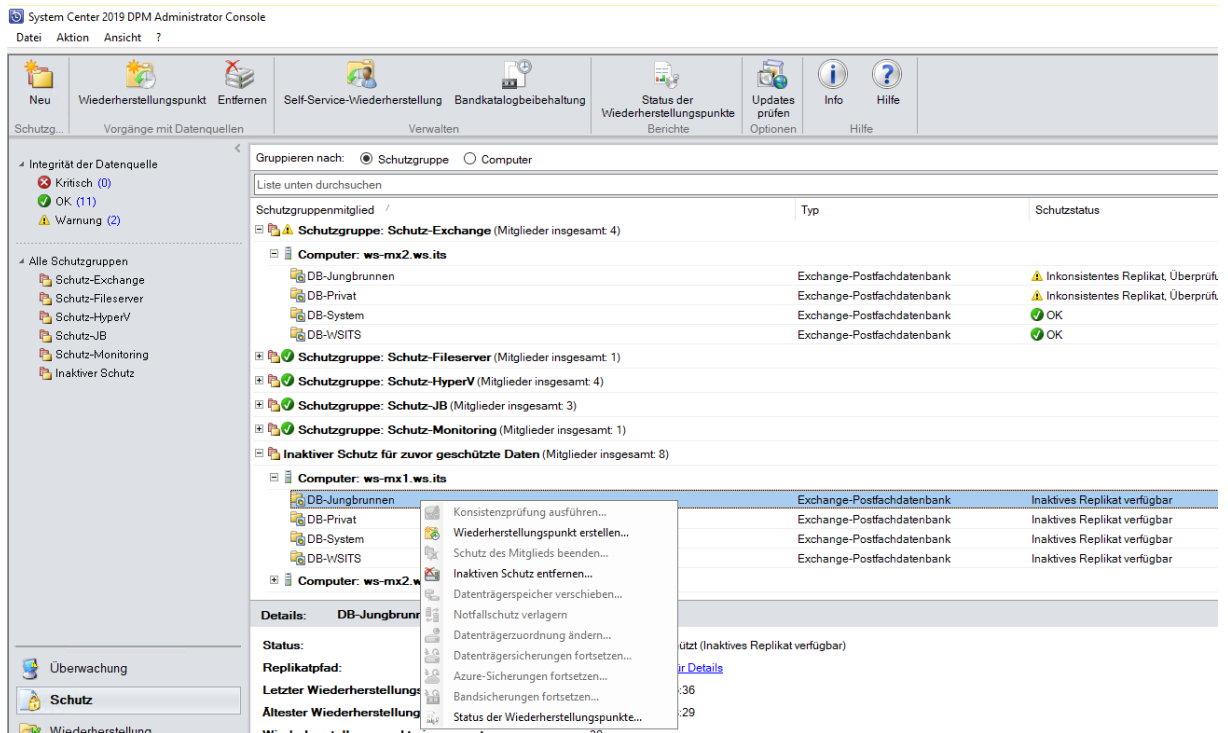
Leider ist auch dieses Produkt an den Anzeigenamen gekoppelt... Also entferne ich testweise eine der neuen Datenbanken, um sie dann wieder mit dem neuen Namen anzufügen:



Das hat funktioniert. Also entferne ich auch die anderen 3 Datenbanken und füge sie neu an:



Die Sicherung läuft. Nach dem Abschluss entferne ich die alten, getrennten Sicherungen:



Die Rolle MBS ist nun fertig konfiguriert.

Bereinigungen in der Rolle HTS

Weiter geht es mit dem HubTransport. Hier muss ich nur den Sende-Konnektor vom Server WS-MX1 entfernen, indem ich WS-MX2 als alleinigen SourceTransportServer definiere. Von den Empfangs-Konnektoren erstelle ich einen Dump in einer Textdatei:

```

265 #region Entfernung der Rolle HTS auf WS-MX1
266 # Rekonfiguration der Sende-Konnektoren
267 Get-SendConnector | Format-Table -Property Identity,SourceTransportServers
268
269 Set-SendConnector -Identity 'Mail-ins-Internet' -SourceTransportServers @('WS-MX2')
270
271 # Sichtung der Receive-Konnektoren
272 Get-ReceiveConnector -Server WS-MX1 |
273 Format-List -Property * |
274 Out-File -FilePath M:\AdminArea\Services\Exchange\Migration-2019\WS-MX1\Receive-Konnektoren.txt
275 #endregion

```

```

PS C:\> Get-SendConnector | Format-Table -Property Identity,SourceTransportServers
Identity           SourceTransportServers
-----
Mail-ins-Internet {WS-MX2, WS-MX1}

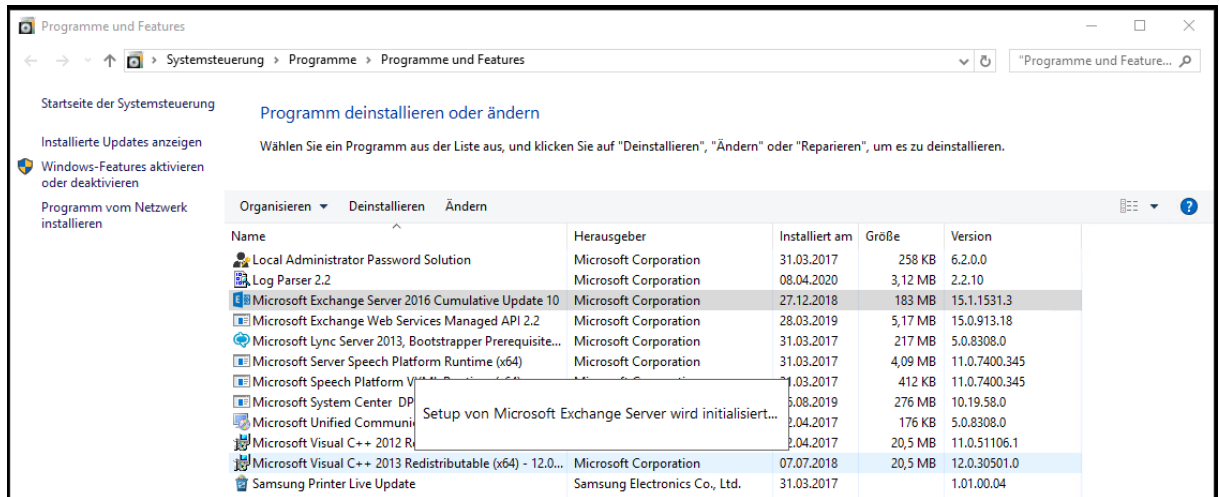
PS C:\> Set-SendConnector -Identity 'Mail-ins-Internet' -SourceTransportServers @('WS-MX2')
PS C:\> Get-ReceiveConnector -Server WS-MX1 |
Format-List -Property * |
Out-File -FilePath M:\AdminArea\Services\Exchange\Migration-2019\WS-MX1\Receive-Konnektoren.txt

```

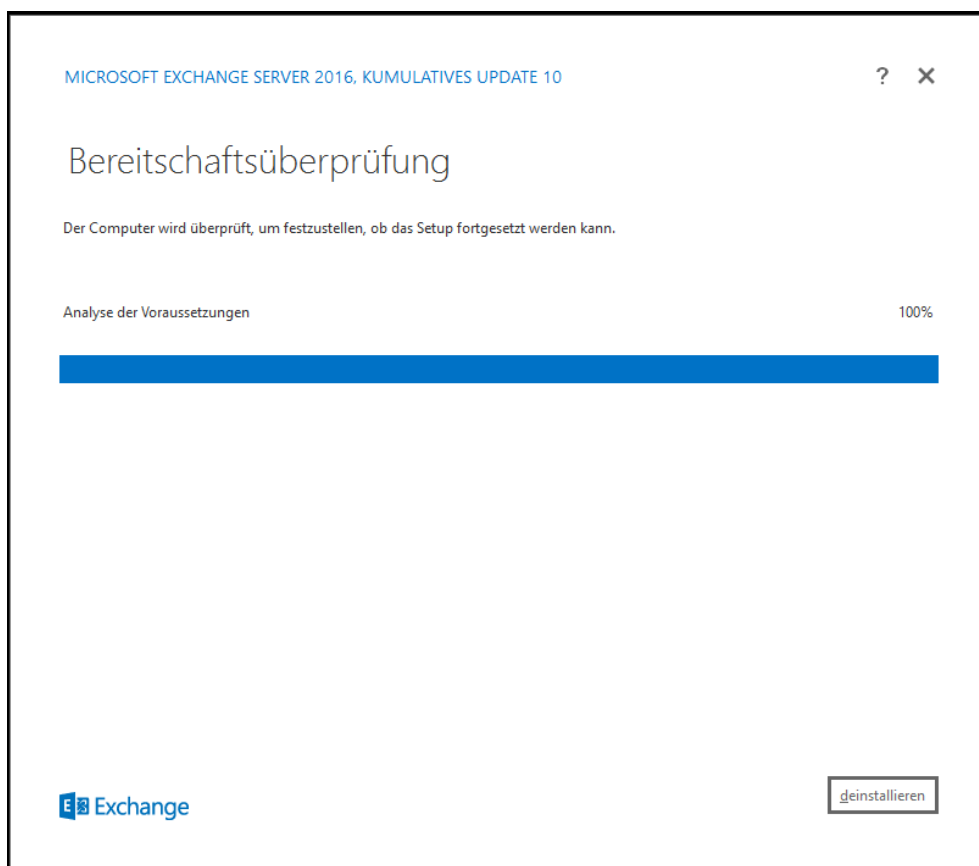
Das war auch schon alles. Der ClientAccess-Service muss nicht zurückgebaut werden.

Deinstallation des Exchange Servers

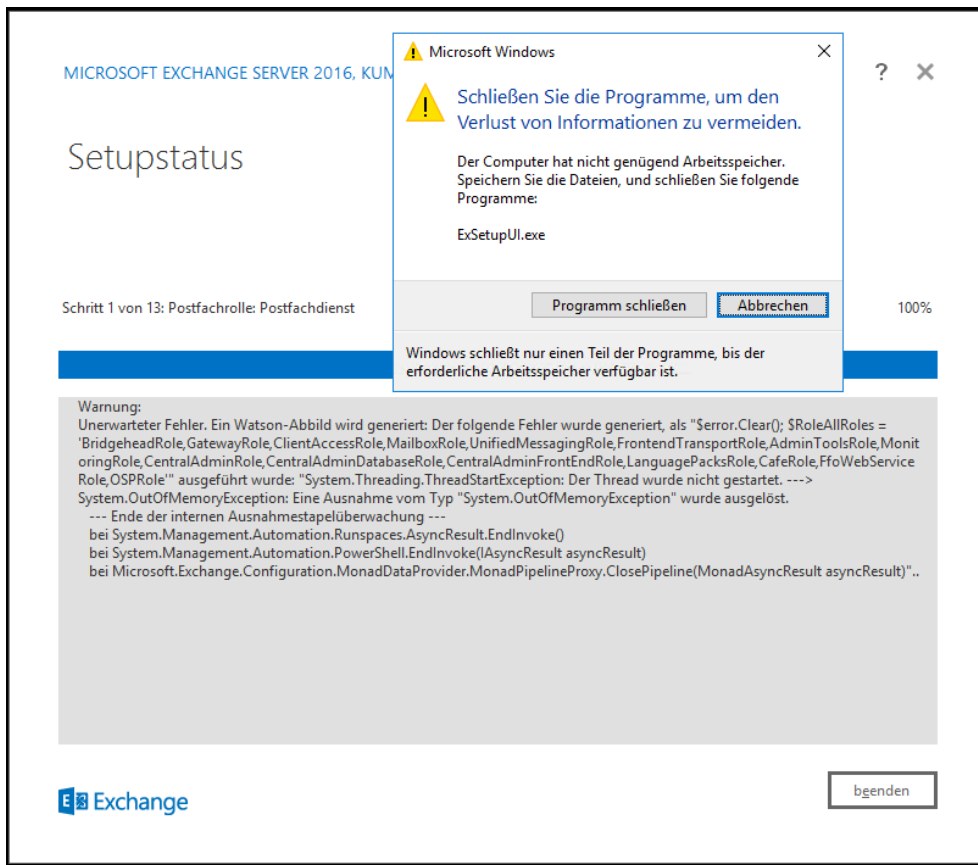
Dann kann ich jetzt die Deinstallation in der Systemsteuerung starten.



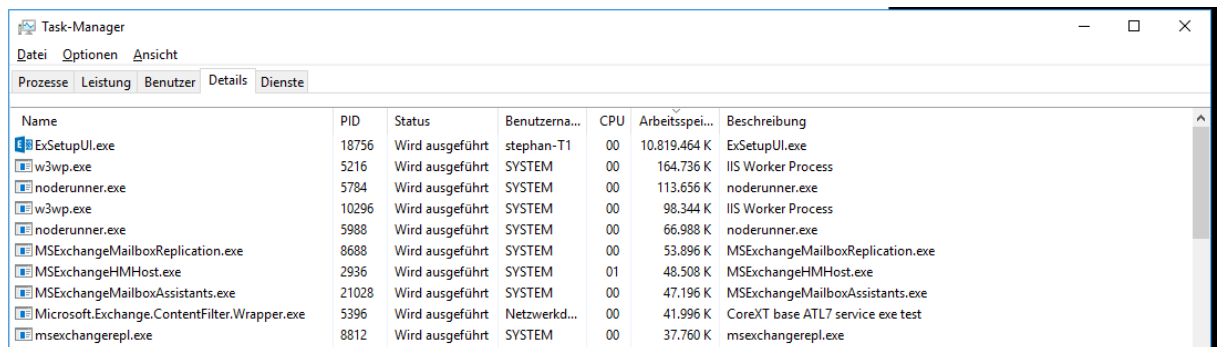
Wie erwartet sind alle Voraussetzungen erfüllt.



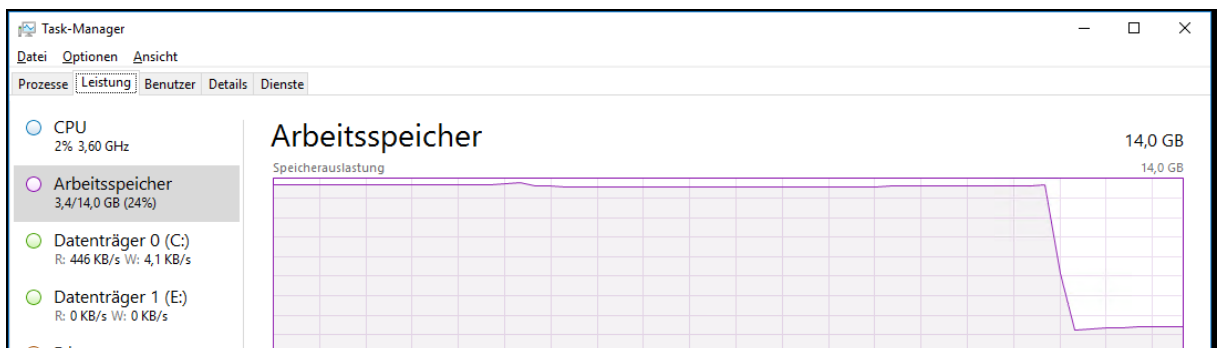
Das Setup bricht aber nach wenigen Sekunden mit der gleichen Fehlermeldung wie beim andern Mailserver WS-MX2 ab. Offensichtlich reicht der Arbeitsspeicher nicht aus:



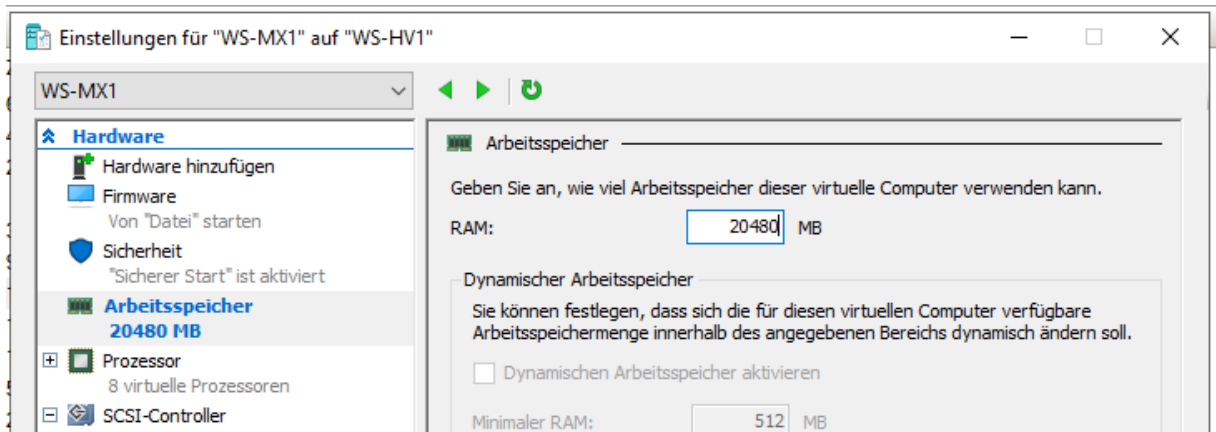
Wie beim Server WS-MX2 hat sich auch hier das Setup einen großen Teil des Arbeitsspeichers geholt:



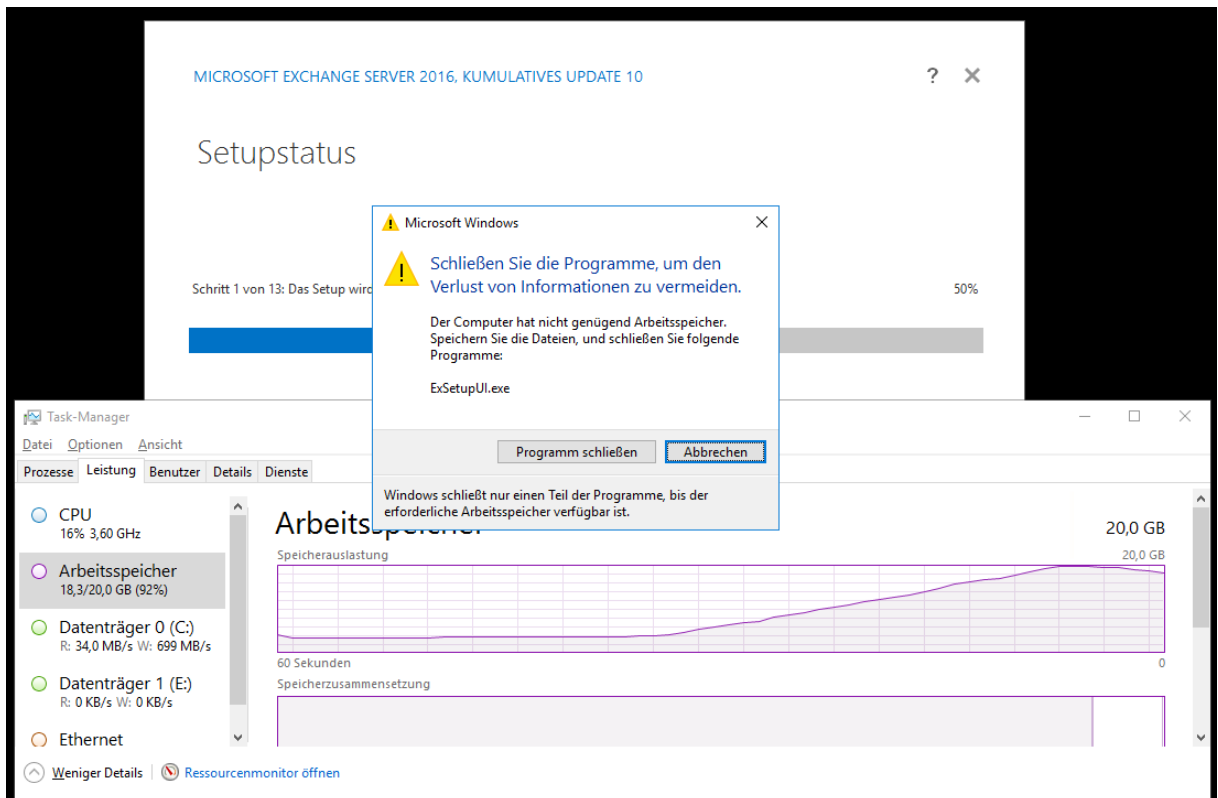
Ich breche das Setup ab. Der Server hat eigentlich genug Speicher:



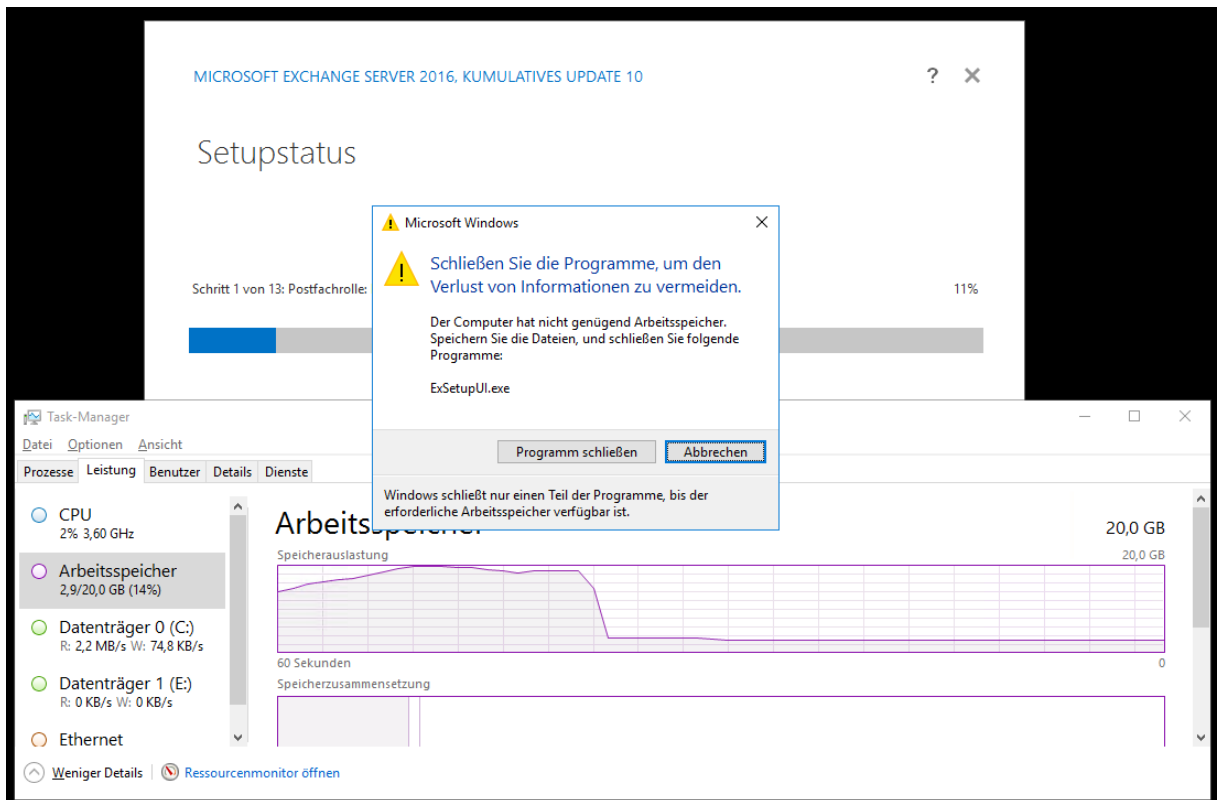
Da der neue Server noch ausgeschaltet ist, kann ich dem alten Server mehr RAM konfigurieren:



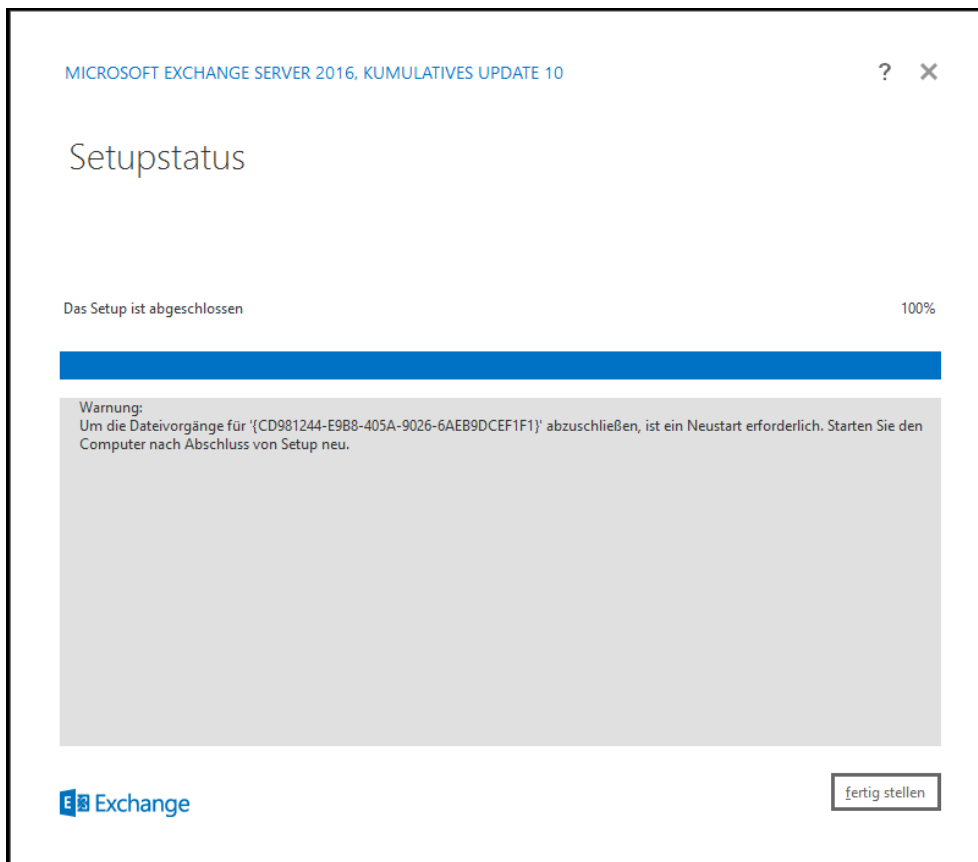
Aber das Setup braucht nur ein paar Sekunden mehr, um auch diese Reserve zu belegen:



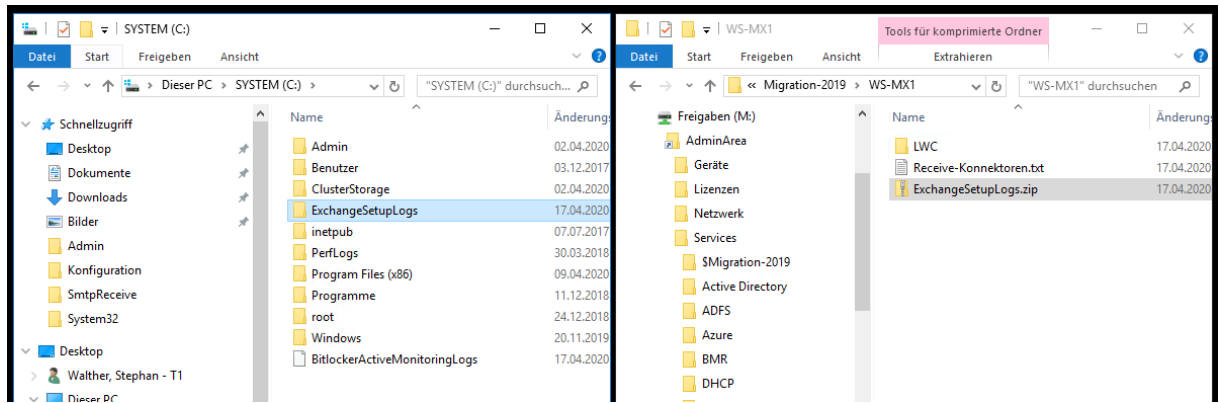
Während ich diese Screenshots erstelle, vergehen weitere Sekunden. In diesen „erholt“ sich das Setup. Die Meldung bleibt. Sie kommt aber auch vom Betriebssystem:



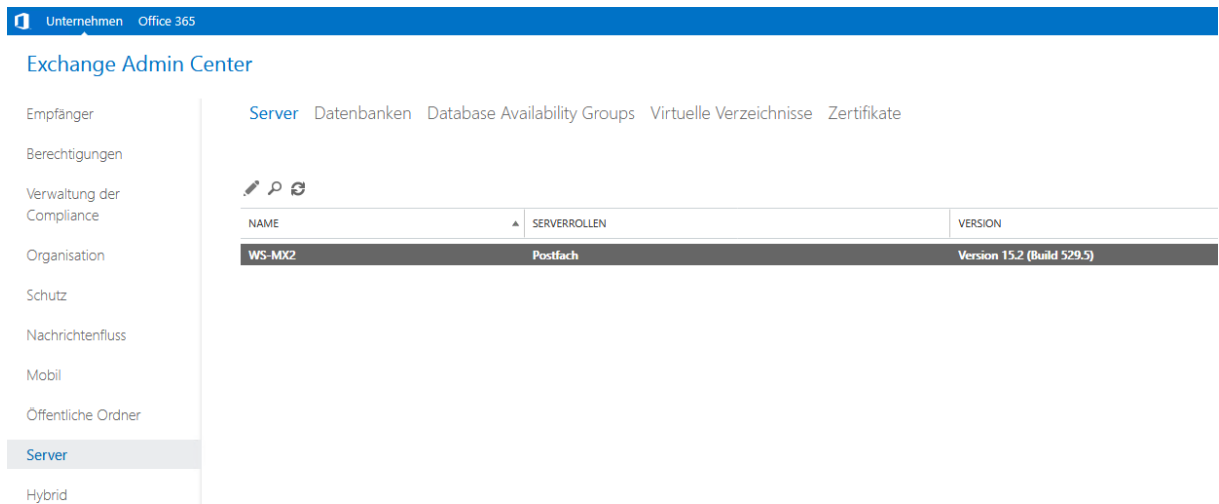
Das Setup läuft weiter. Nach wenigen Minuten wurde Exchange Server 2016 vom Server WS-MX1 deinstalliert. Nun steht noch ein Neustart aus:



Ich sichere noch das Verzeichnis C:\ExchangeSetupLogs auf mein AdminShare:

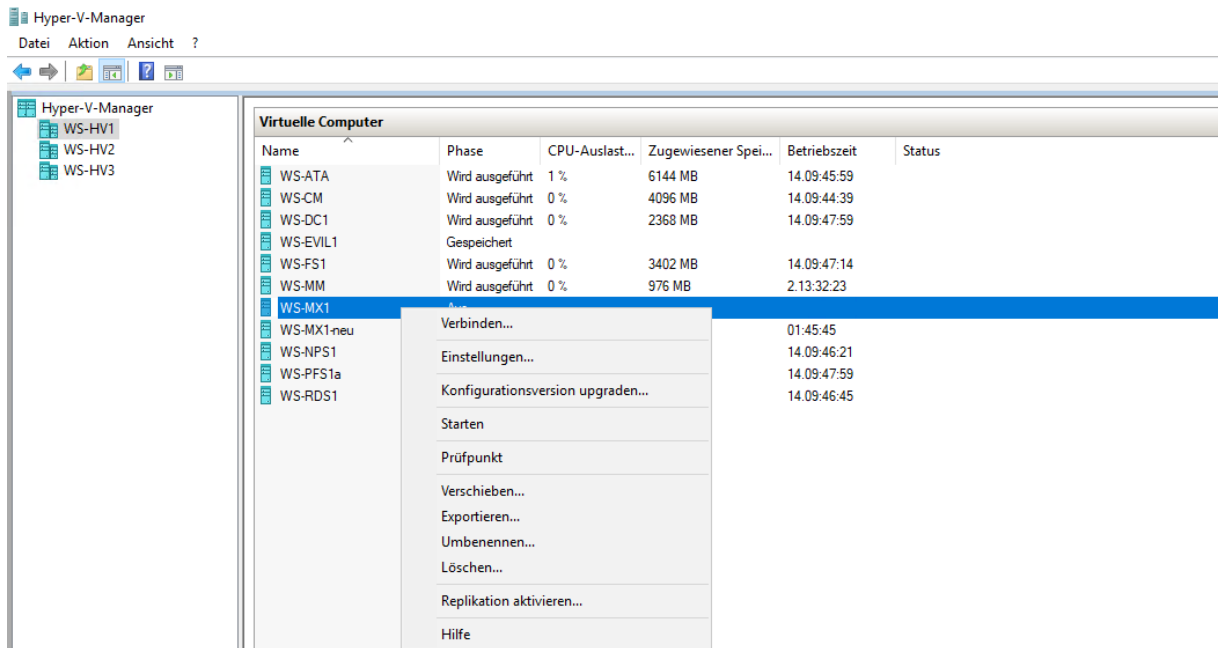


Dann gibt es den Neustart. Im EAC ist nun nur noch der neue WS-MX2 mit Exchange Server 2019 gelistet:

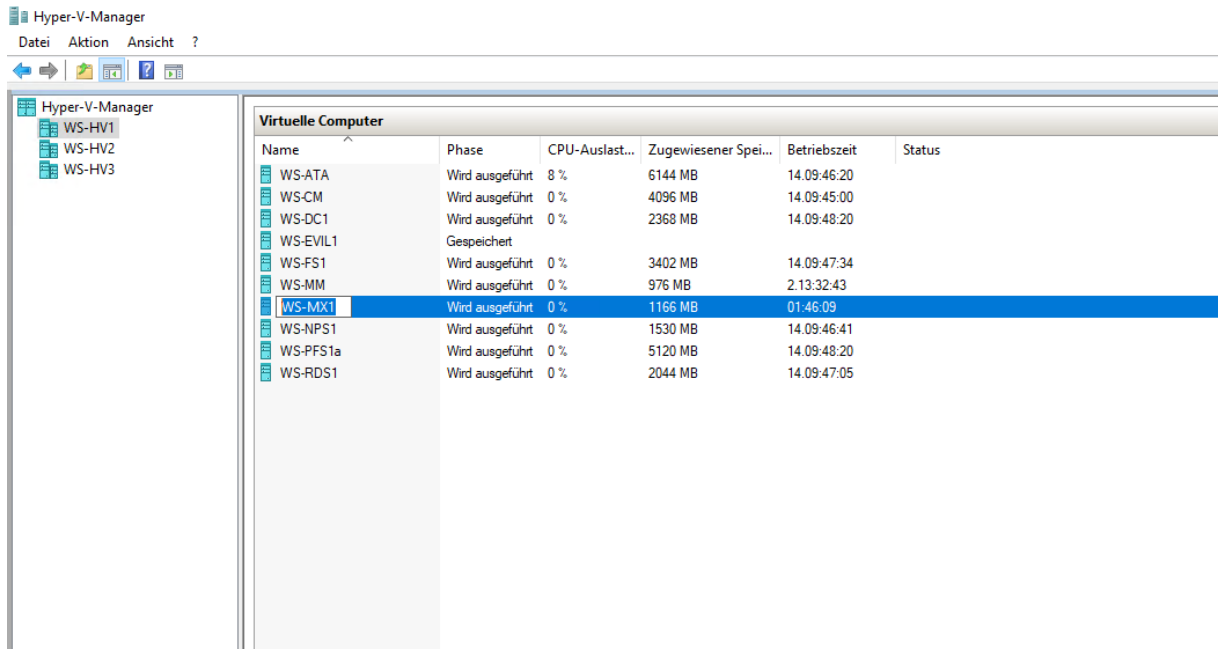


Entfernung des alten Servers und Austausch der VM

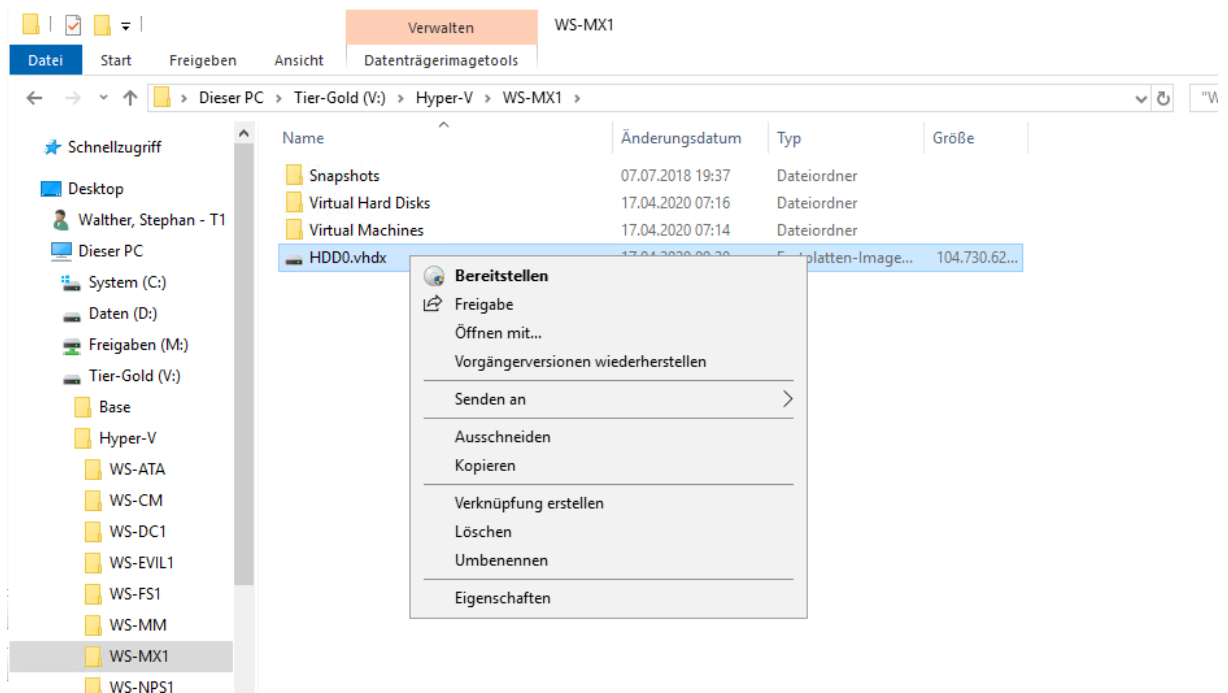
Nach dem Neustart fahre ich den alten Server herunter. Dann entferne ich die virtuelle Maschine im Hyper-V:

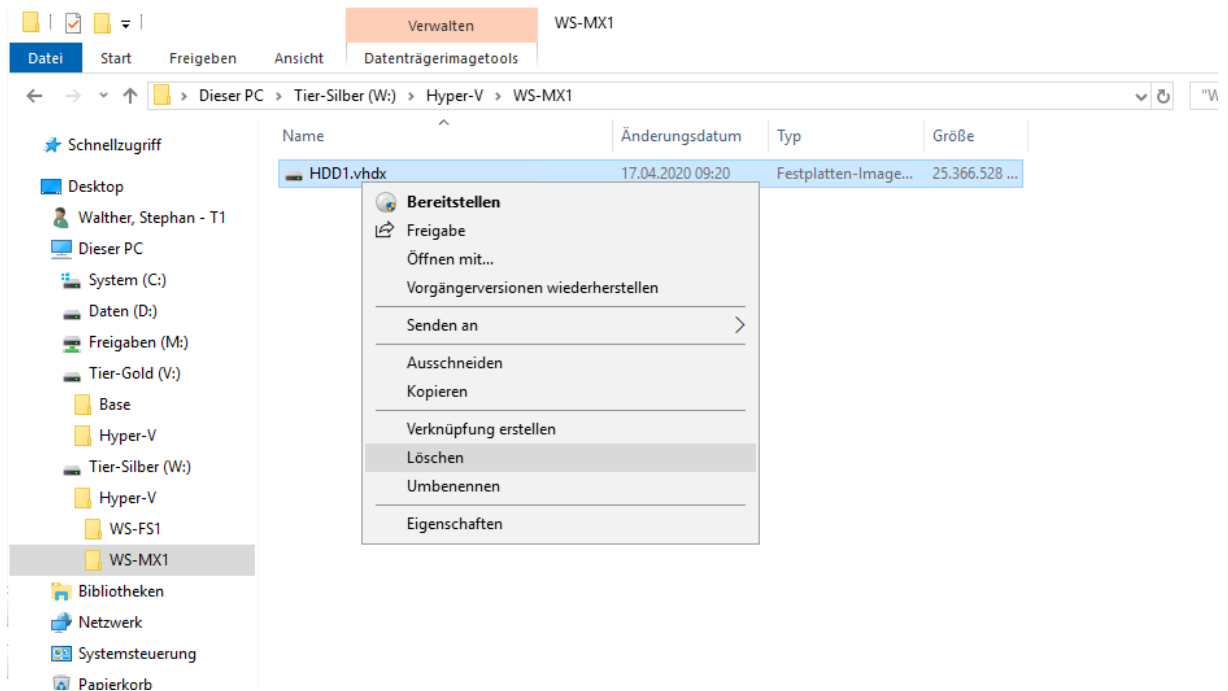


Die neue VM erhält ihren finalen Anzeigenamen:

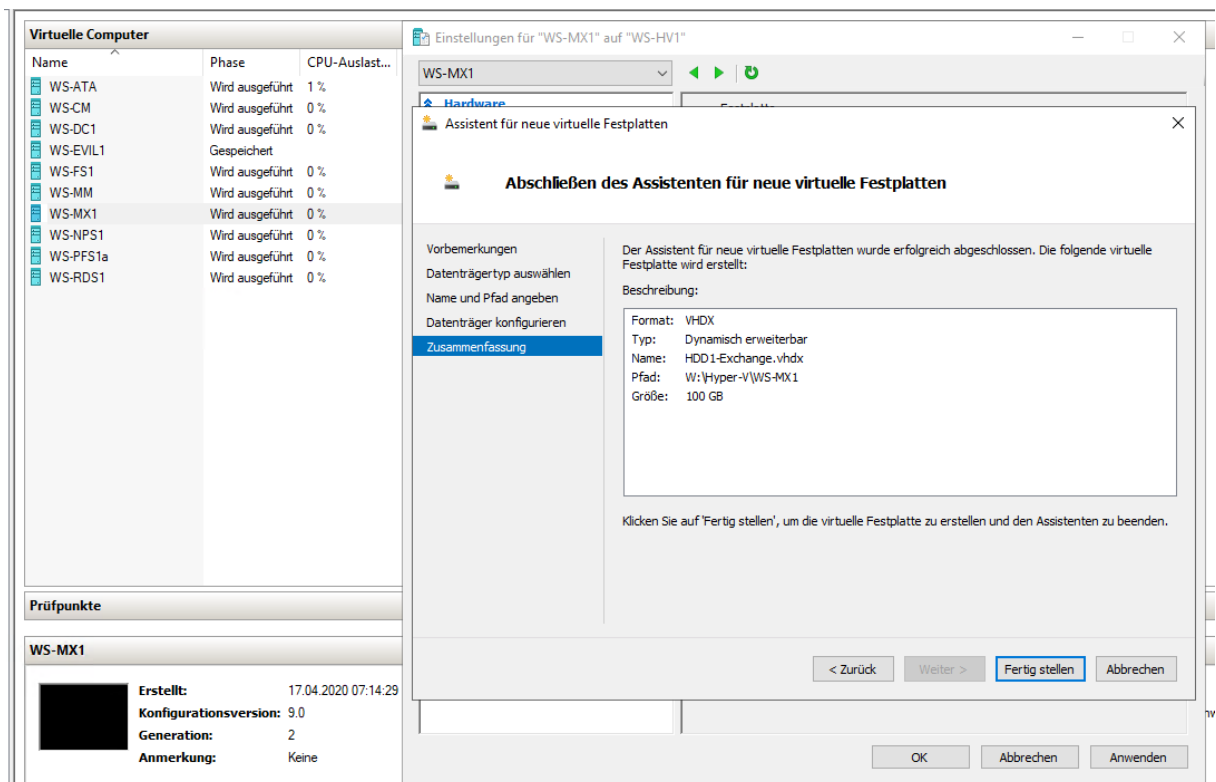


Nun muss ich noch die virtuellen Festplattendateien vom Hyper-V-Storage entfernen. Die VHDX habe ich auf 2 Volumes aufgeteilt:





Der neue Server verfügt aktuell nur über eine System-Festplatte. Jetzt kommt noch eine weitere für die Exchange Datenbanken dazu:



Virtuelle Computer

Name	Phase	CPU-Auslast...
WS-ATA	Wird ausgeführt	1 %
WS-CM	Wird ausgeführt	0 %
WS-DC1	Wird ausgeführt	0 %
WS-EVIL1	Gespeichert	
WS-FS1	Wird ausgeführt	0 %
WS-MM	Wird ausgeführt	0 %
WS-MX1	Wird ausgeführt	0 %
WS-NPS1	Wird ausgeführt	0 %
WS-PFS1a	Wird ausgeführt	0 %
WS-RDS1	Wird ausgeführt	0 %

Prüfpunkte

WS-MX1

Erstellt: 17.04.2020 07:14:29
 Konfigurationsversion: 9.0
 Generation: 2
 Anmerkung: Keine

Einstellungen für "WS-MX1" auf "WS-HV1"

Hardware

- Festplatte: HDD1-Exchange.vhdx

Verwaltung

- Speicherort für die Smart Paging-D...: V:\Hyper-V\WS-MX1

Festplatte

Sie können auswählen, wie die virtuelle Festplatte dem virtuellen Computer zugeordnet werden soll. Ist auf dem Datenträger ein Betriebssystem installiert, kann der virtuelle Computer nach dem Ändern der Zuordnung möglicherweise nicht mehr gestartet werden.

Controller: SCSI-Controller Speicherort: 1 (wird verwendet)

Medien

Eine virtuelle Festplatte kann durch Bearbeiten der zugehörigen Datei komprimiert, konvertiert, erweitert, zusammengeführt, erneut verbunden oder verkleinert werden. Geben Sie den vollständigen Pfad der Datei an.

Virtuelle Festplatte: W:\Hyper-V\WS-MX1\HDD1-Exchange.vhdx

Physische Festplatte:

OK **Abbrechen** **Anwenden**

Den Arbeitsspeicher konfiguriere ich statisch. Dazu muss ich die VM noch einmal herunterfahren:

Hyper-V-Manager

Hyper-V-Manager

- WS-HV1
- WS-HV2
- WS-HV3

Virtuelle Computer

Name	Phase	CPU-Auslast...
WS-ATA	Wird ausgeführt	0 %
WS-CM	Wird ausgeführt	0 %
WS-DC1	Wird ausgeführt	0 %
WS-EVIL1	Gespeichert	
WS-FS1	Wird ausgeführt	1 %
WS-MM	Wird ausgeführt	0 %
WS-MX1	Aus	
WS-NPS1	Wird ausgeführt	0 %
WS-PFS1a	Wird ausgeführt	0 %
WS-RDS1	Wird ausgeführt	0 %

Prüfpunkte

WS-MX1

Erstellt: 17.04.2020 07:14:29
 Konfigurationsversion: 9.0
 Generation: 2
 Anmerkung: Keine

Einstellungen für "WS-MX1" auf "WS-HV1"

Arbeitsspeicher

Geben Sie an, wie viel Arbeitsspeicher dieser virtuelle Computer verwenden kann.

RAM: 14336 MB

Dynamischer Arbeitsspeicher

Sie können festlegen, dass sich die für diesen virtuellen Computer verfügbare Arbeitsspeichermenge innerhalb des angegebenen Bereichs dynamisch ändern soll.

Dynamischen Arbeitsspeicher aktivieren

Minimaler RAM: 512 MB
 Maximaler RAM: 10240 MB

Geben Sie den Prozentsatz des Arbeitsspeichers an, der von Hyper-V als Puffer reserviert werden soll. Hyper-V ermittelt anhand des Prozentsatzes und des aktuellen Speicherbedarfs den vom Puffer benötigten Arbeitsspeicher.

Arbeitsspeicherpuffer: 20 %

Arbeitsspeicherrumfang

Geben Sie an, wie die Arbeitsspeicherverfügbarkeit für den virtuellen Computer im Vergleich zu anderen virtuellen Computern auf diesem Computer priorisiert werden soll.

Niedrig Hoch

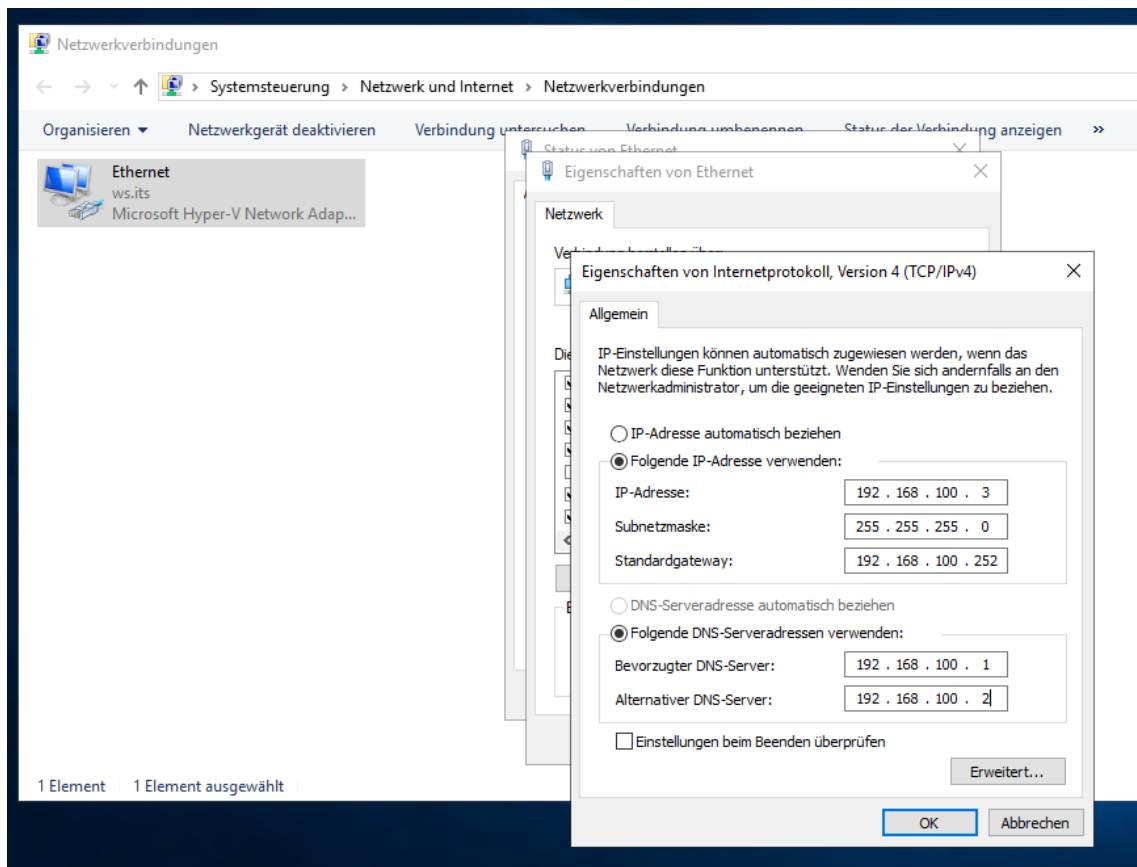
OK **Abbrechen** **Anwenden**

Der neue Server ist nun konfigurationsbereit.

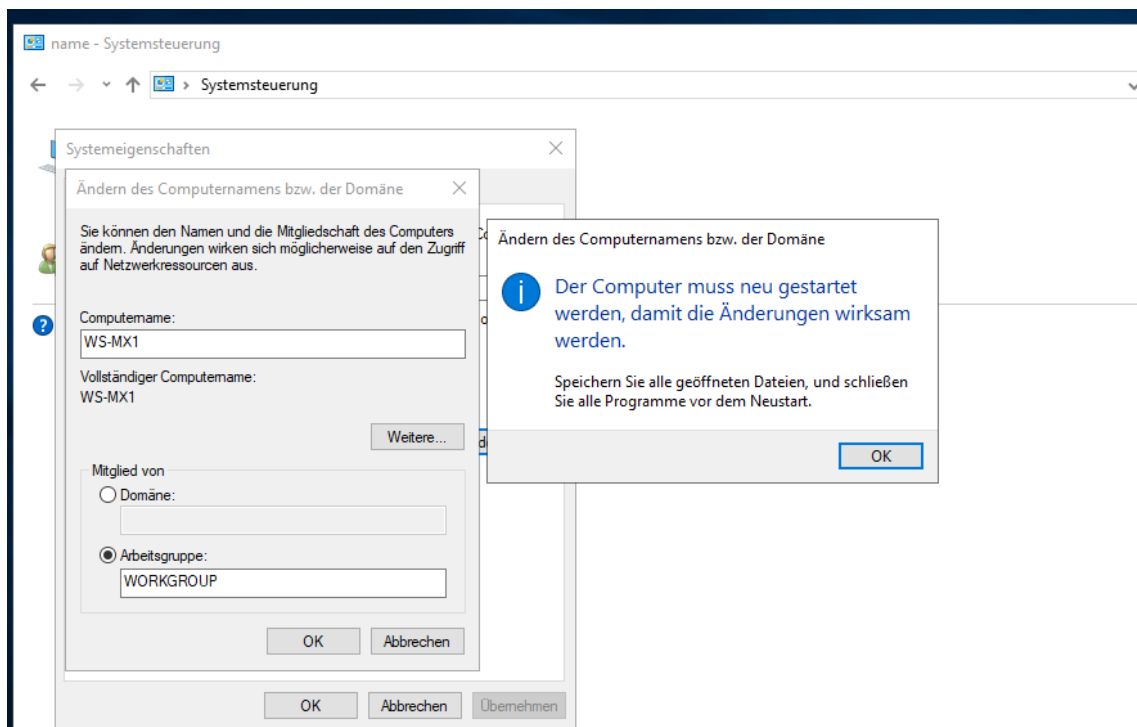
Bereitstellung des neuen Mailservers (MX2019)

Grundkonfiguration des Betriebssystems

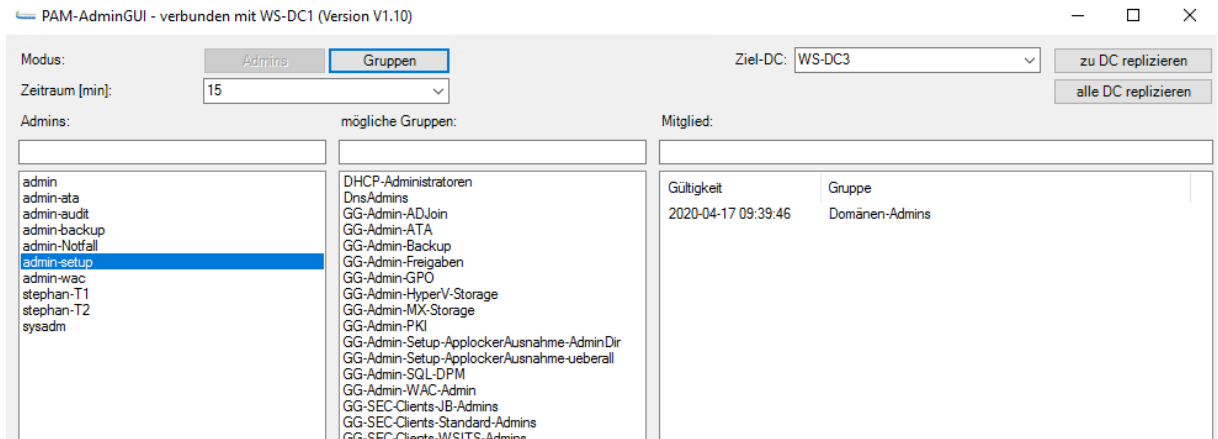
Weiter geht es mit der Konfiguration der IP-Adresse. Der neue Server erbt die alte IP-Konfiguration. So spare ich mir einige Umstellungen in meiner PFSense-Firewall:



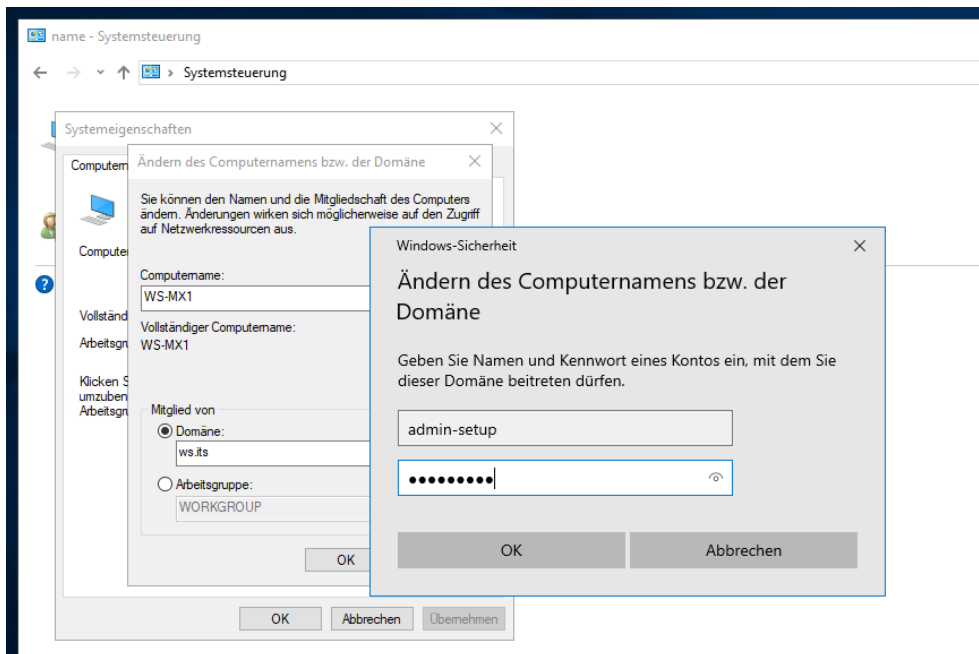
Danach benenne ich den Server um und starte ihn neu



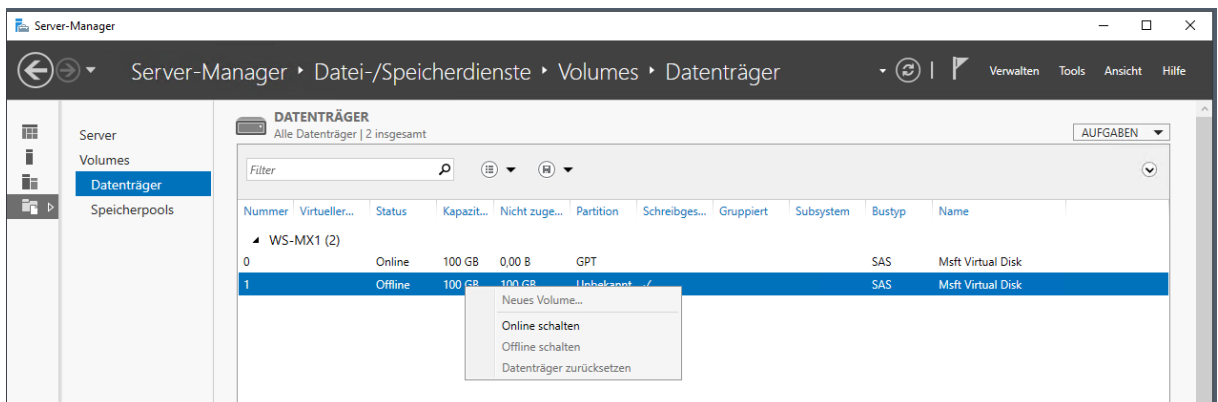
Nach dem Neustart bereite ich ein Admin-Konto mit einer temporären Berechtigung für den Domain Join vor:



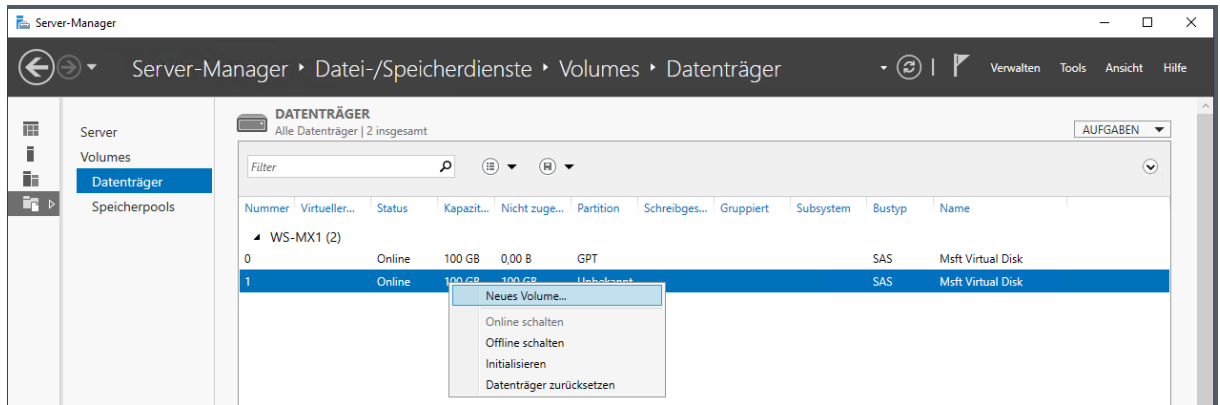
Danach kann der Server ins Active Directory aufgenommen werden. Dabei übernimmt er das freigewordene AD-Computerkonto des alten Servers:



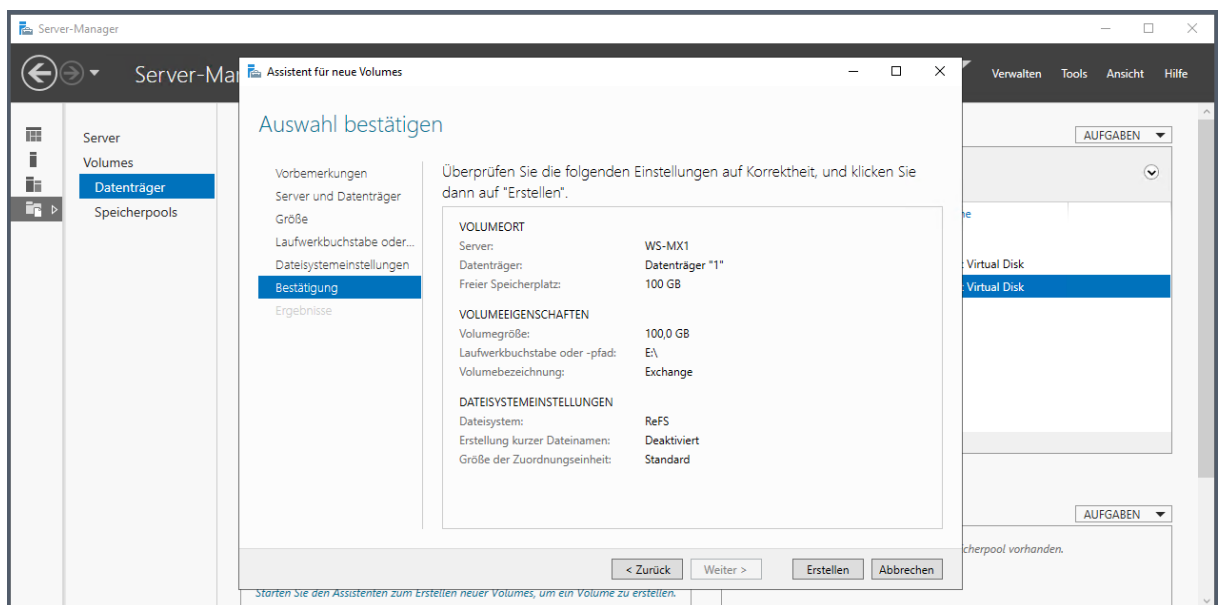
Nach dem Neustart konfiguriere ich die zusätzliche Festplatte. Hier soll der Exchange Server später seine Datenbanken ablegen können. Der Datenträger ist noch offline:



Jetzt erstelle ich das neue Volume:



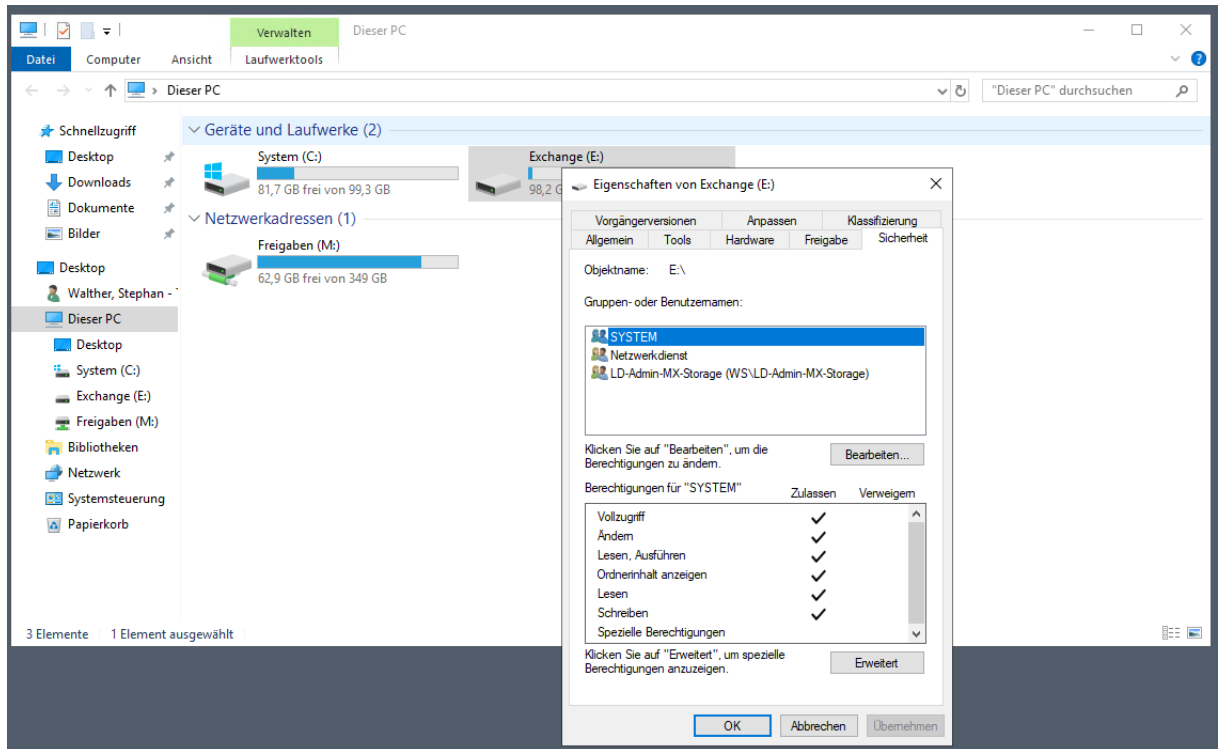
Ich verwende den maximalen Speicherplatz und formatiere wie auf WS-MX2 mit ReFS – das bevorzugte Dateisystem für Exchange Datenbanken. Wichtig ist zudem, dass der Laufwerksbuchstabe mit dem vom anderen Mailserver identisch ist. Nur so kann ich später die Datenbanken in einer DAG synchronisieren:



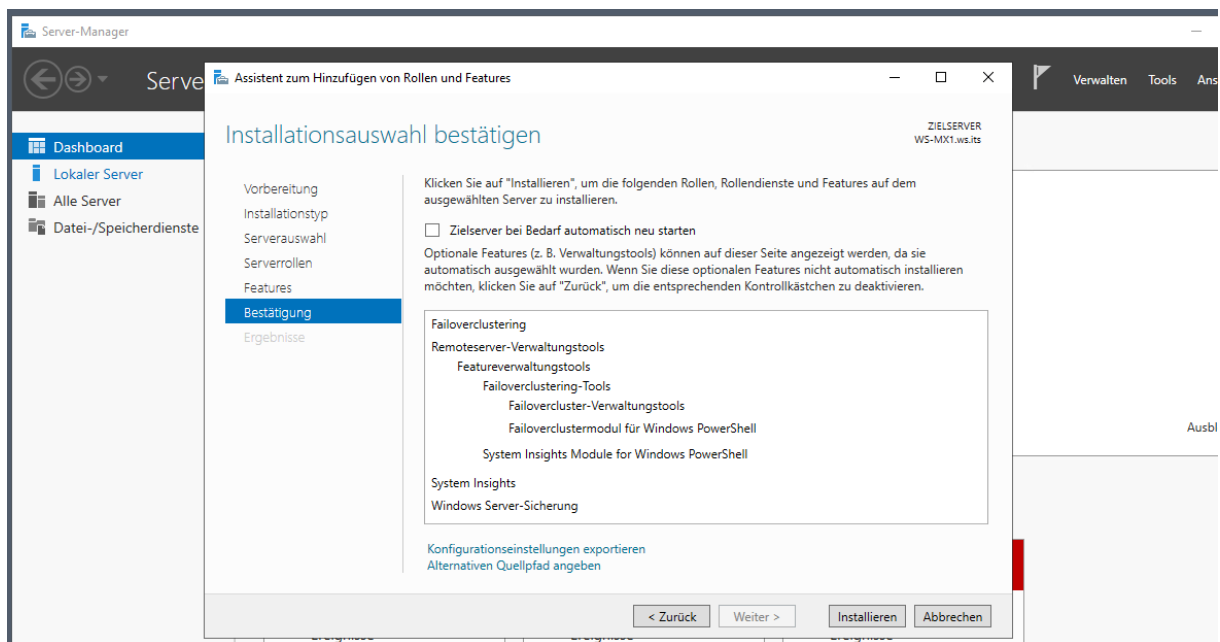
Danach ist das Volume fertig. Ich verändere noch die ACL für den Zugriff. In meinem Active Directory habe ich eine spezielle Rechtegruppe für den Zugriff auf diese Volumes. Nur diese und das System sollen darauf zugreifen dürfen. Das Ziel dieser Änderung ist einfach erklärt: Ich habe danach 3 Rechtegruppen für die Administration, die sich gegenseitig ergänzen:

- die Admingruppe „LD-SEC-ServerMX-Admins,“ für die Betriebssystem-Administration
- die Admingruppe „Organization Management“ für die Exchange-Administration
- die Admingruppe „LD-Admin-MX-Storage“ für die Speicher-Administration

Je nach anstehender Aufgabe nehme ich meine Adminkennung temporär in die dazugehörige Gruppe auf. Stehen beispielsweise Windows Updates an, dann brauche ich keinen Storage-Zugriff oder Rechte im Exchange Dienst.



Weiter geht es mit den zusätzlichen Rollen und Features, die nicht zwingend etwas mit Exchange Server zu tun haben:



Danach gibt es noch einmal einen Neustart. Ein Feature hatte ich vergessen. Das hole ich noch fix mit der PowerShell nach:

```

Administrator: Windows PowerShell
PS C:\>
PS C:\> Get-WindowsFeature -Name RSAT-ADDS-Tools

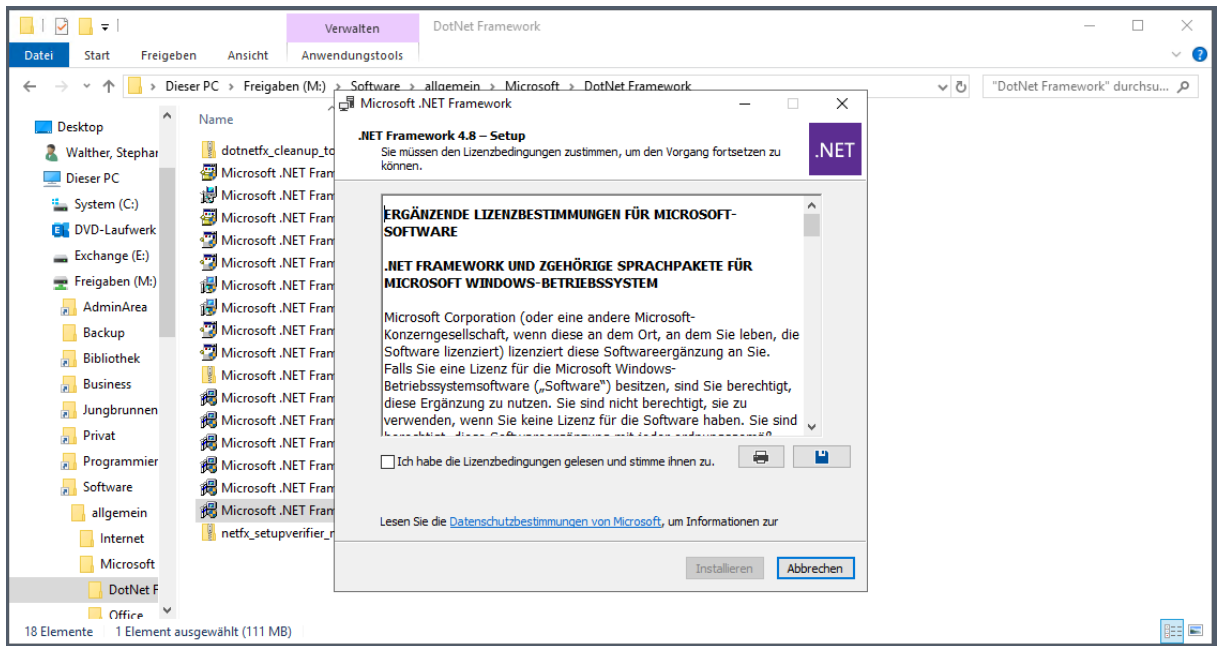
Display Name                                     Name                                     Install State
-----
[ ] AD DS-Snap-Ins und -Befehlszeile... RSAT-ADDS-Tools                         Available

PS C:\> Get-WindowsFeature -Name RSAT-ADDS-Tools | Add-WindowsFeature

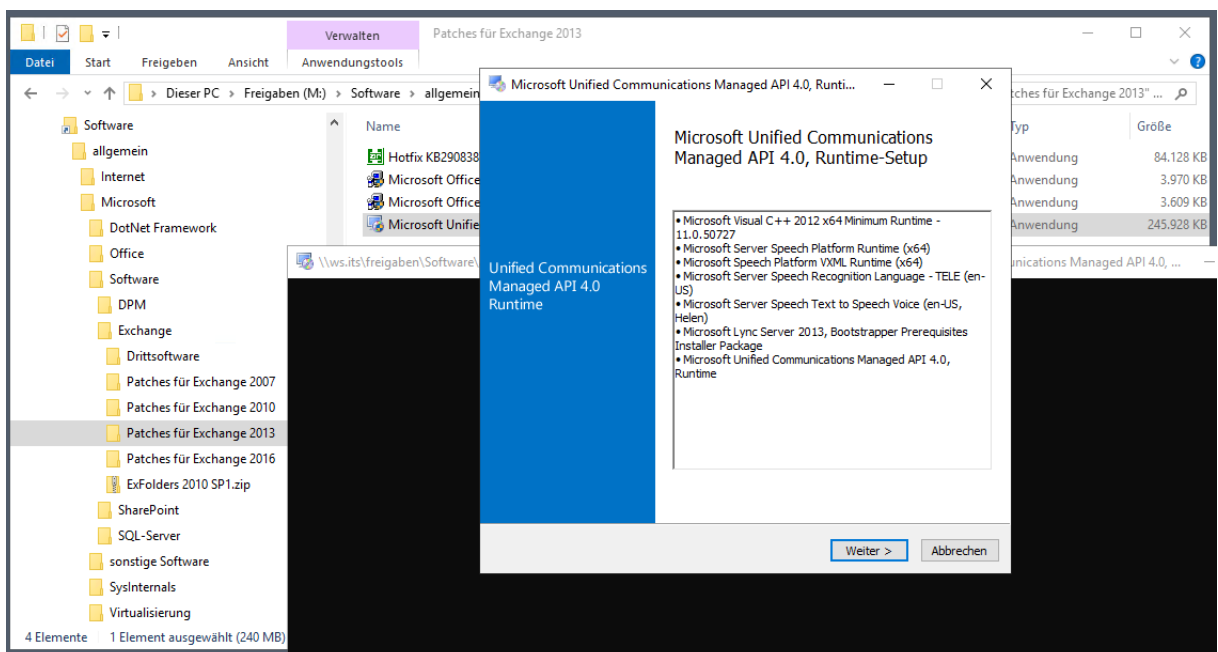
Success Restart Needed Exit Code      Feature Result
-----
True      No           Success      {AD DS- und AD LDS-Tools, AD DS-Tools, AD ...

PS C:\>
    
```

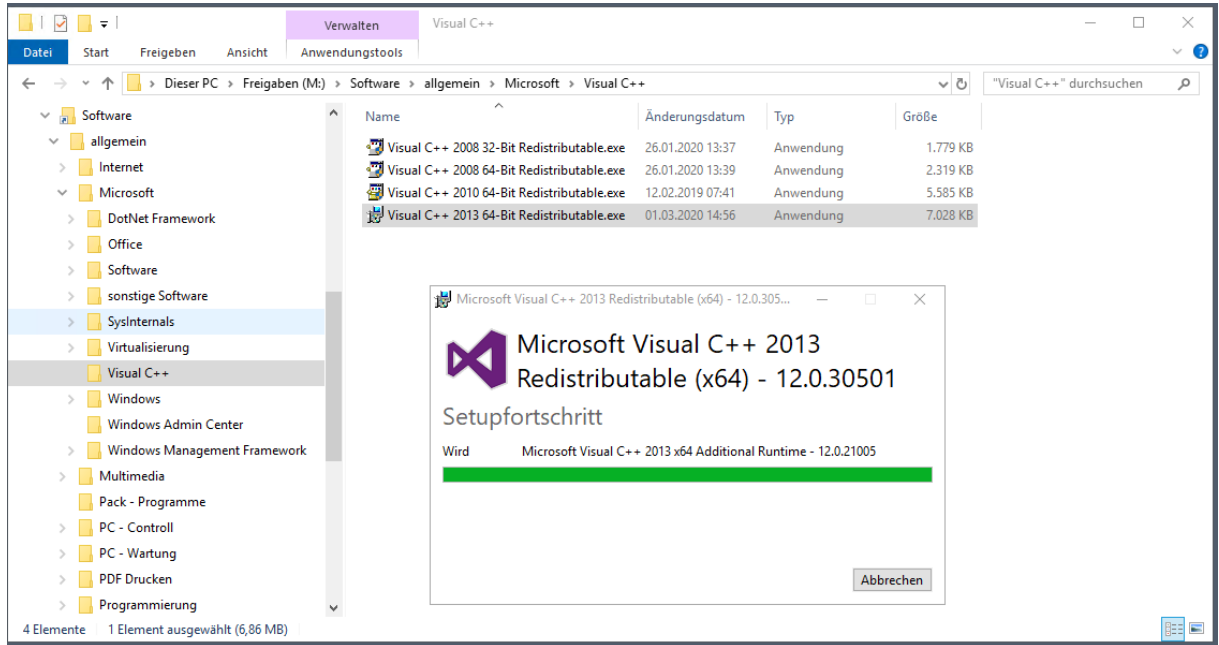
Der neue Exchange Server 2019 benötigt das .net-Framework 4.8. Das installiere ich mit einem Offline-Installer, der auf meinen Software-Share liegt:



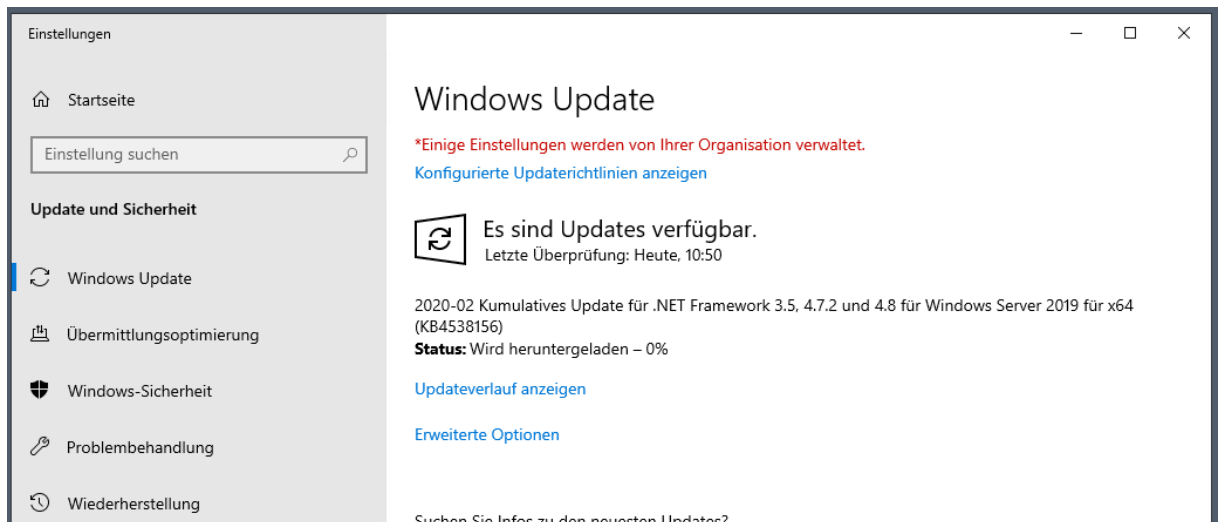
Ebenso wird das Microsoft Unified Communications Managed API 4.0 als Runtime benötigt:



Und auch Visual C++ 2013 Redist wird benötigt:

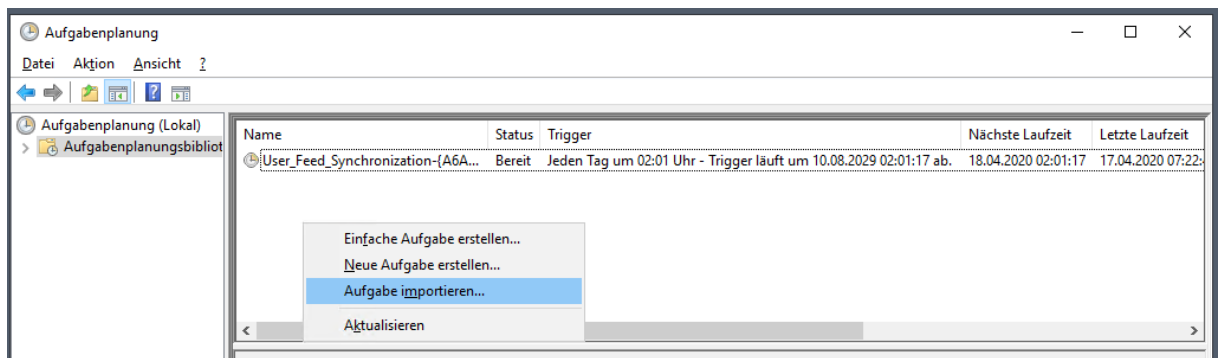


Alle Setups lassen sich problemlos installieren. Danach wird es Zeit für ein Windows Update. Das .net-Framework muss aktualisiert werden:

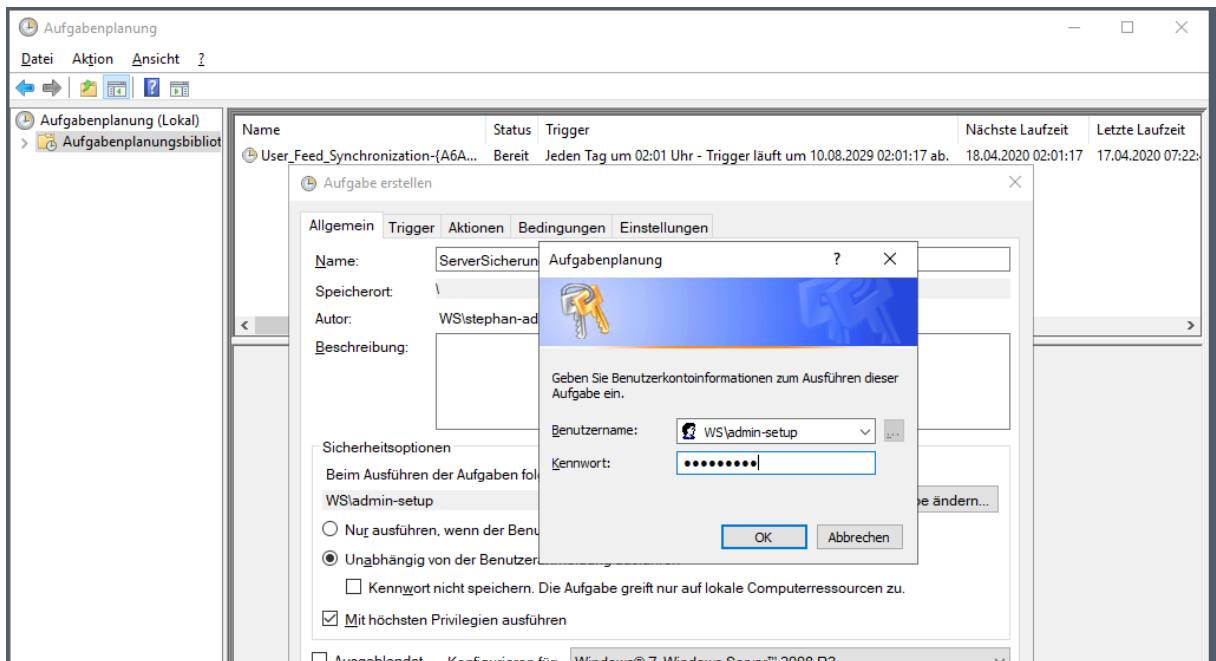


Einrichtung der Datensicherung (BMR mit Windows Server Sicherung)

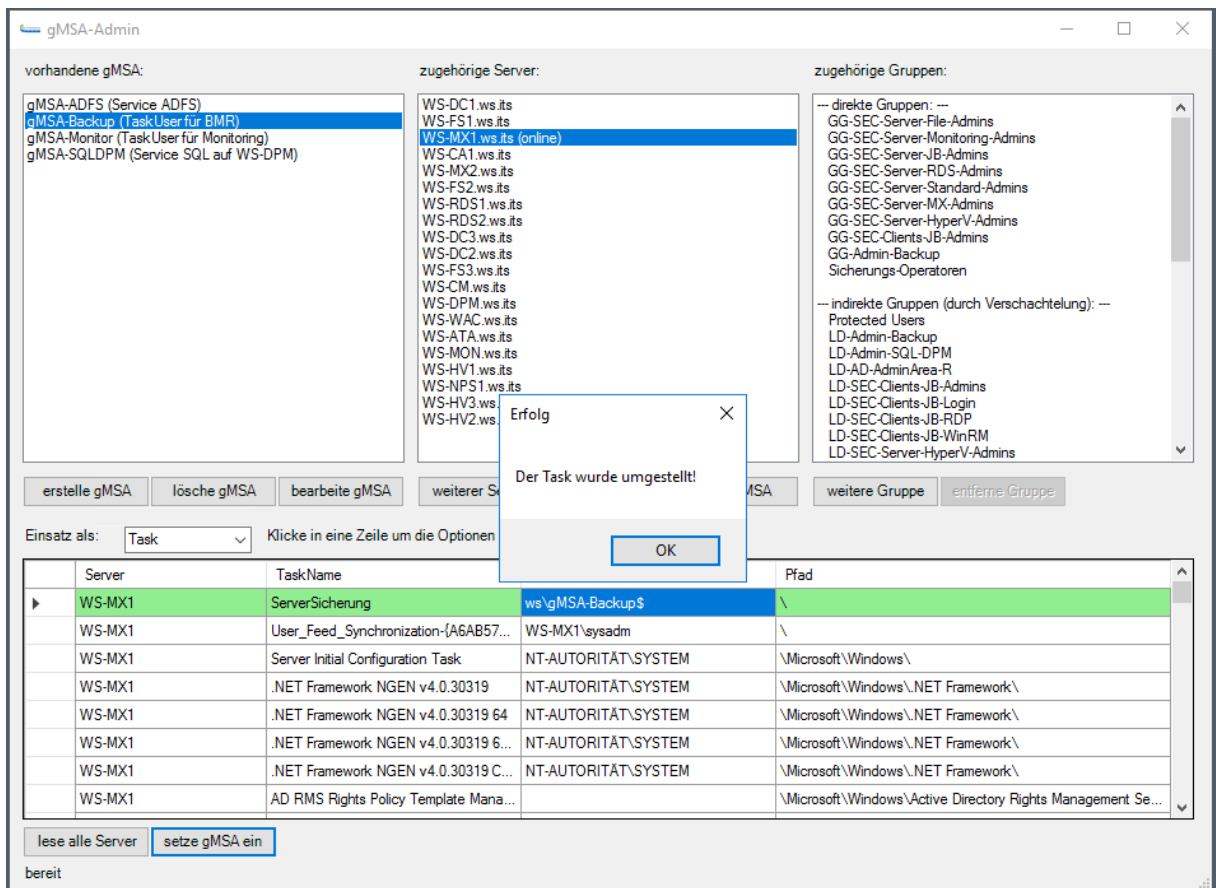
Bevor der Server in die Produktion geht, konfiguriere ich die Datensicherung. Diese splittet sich wie bereits bei meinen anderen Servern in 2 Teile auf. Hier soll das Betriebssystem durch regelmäßige SystemState-Images gesichert werden. Dafür importiere ich eine Aufgabe:



Der Sicherungsaccount ist ein Group Managed Service Account. Diesen kann ich beim Import nicht angeben. Daher trage ich hier einen Dummy ein:



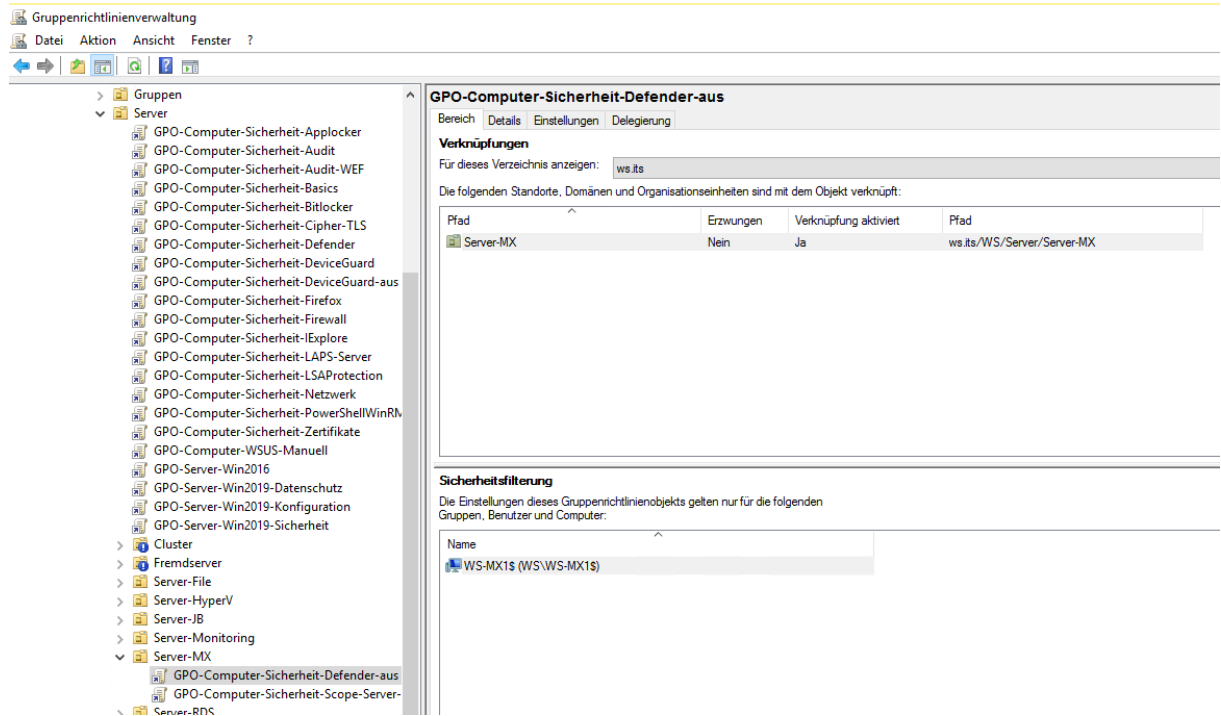
Die Umstellung auf den gMSA nehme ich mit meiner PowerShell-GUI vom Domain Controller aus vor:



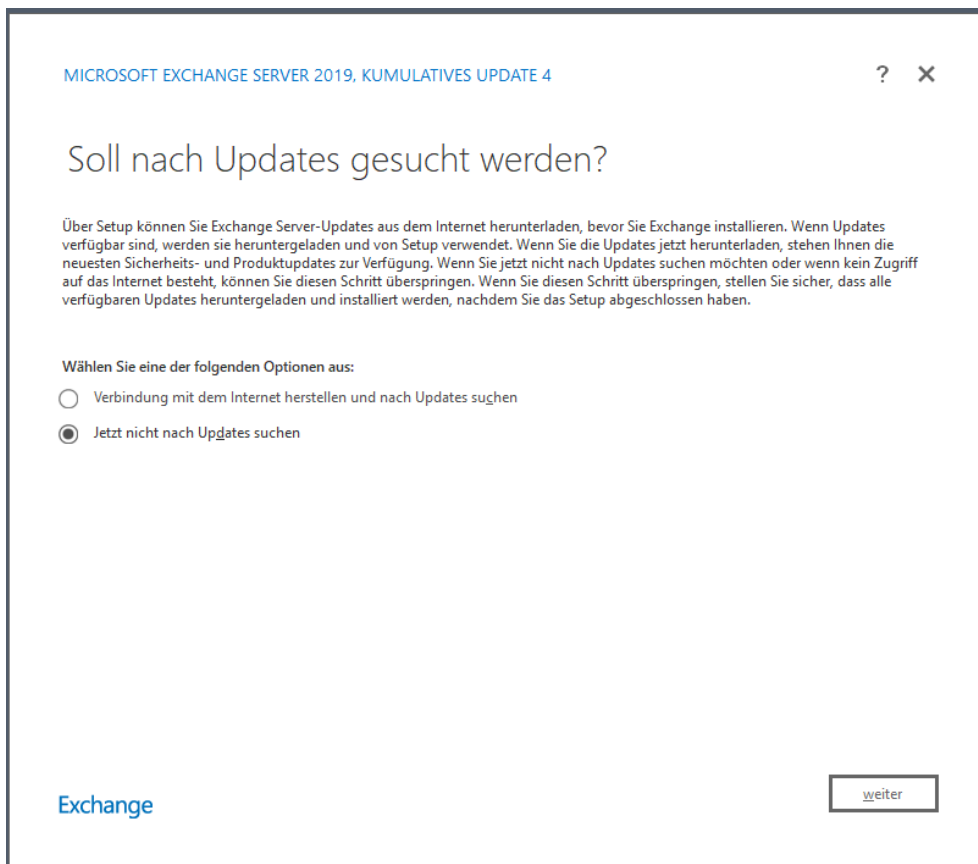
Die geplante Aufgabe wird jeden Tag ein Script auf meinem Sicherungsserver aufrufen. Dieses liest eine Konfigurationsdatei ein und sichert das Betriebssystem nach den darin enthaltenen Vorgaben mit Windows Server Backup auf eine geschützte Freigabe. Die Konfiguration ist auf den Servernamen ausgerichtet. Da dieser übernommen wurde, muss ich keine weiteren Anpassungen vornehmen.

Installation des Exchange Servers 2019 CU4

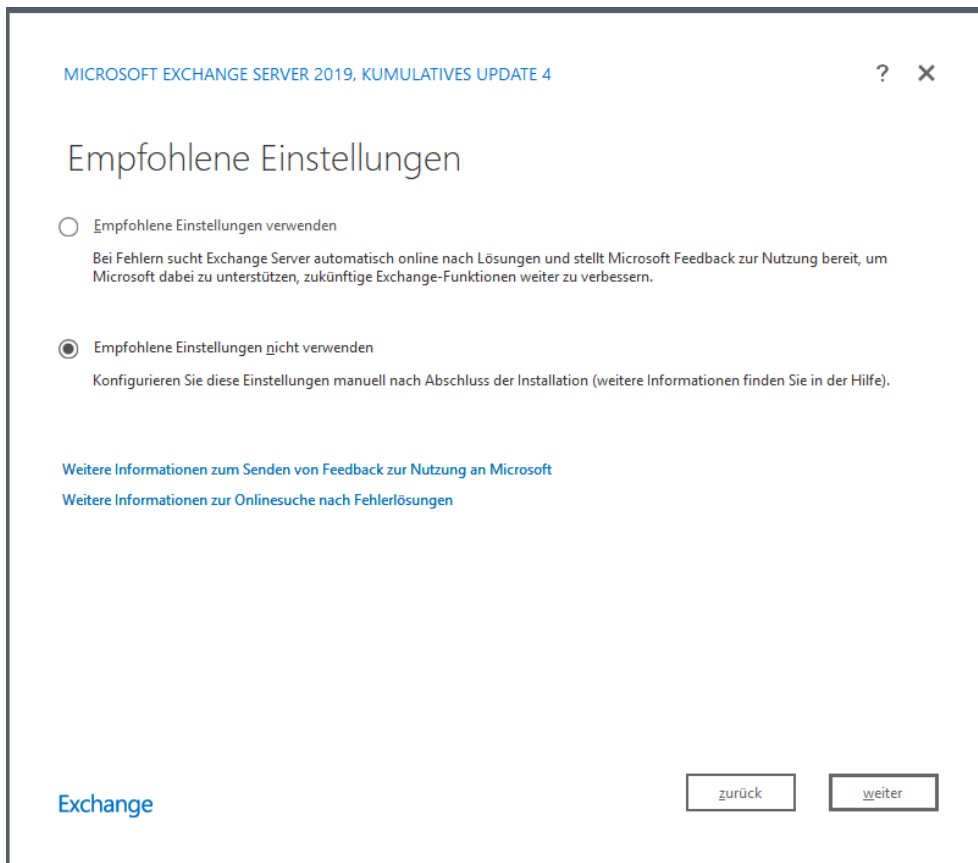
Für das Exchange Server Setup halte ich noch den Windows Defender an. Dafür habe ich eine passende GPO. In diese muss ich nur den Server im Sicherheitsfilter hinterlegen. Ein gpupdate später ist der Defender auf WS-MX1 aus:



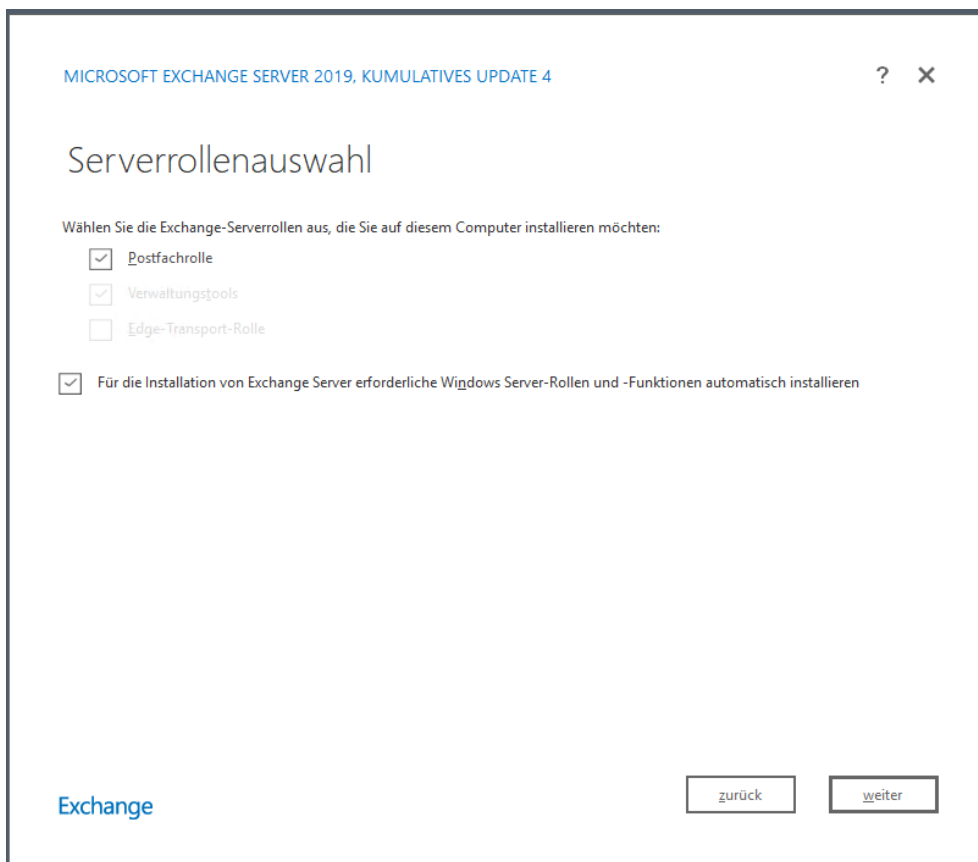
Das ISO mit Exchange Server 2019 CU4 habe ich eingelegt. Ich starte das grafische Setup. Updates wird der Server dank meiner Firewall nicht finden. Also spare ich mir diese Zeit:



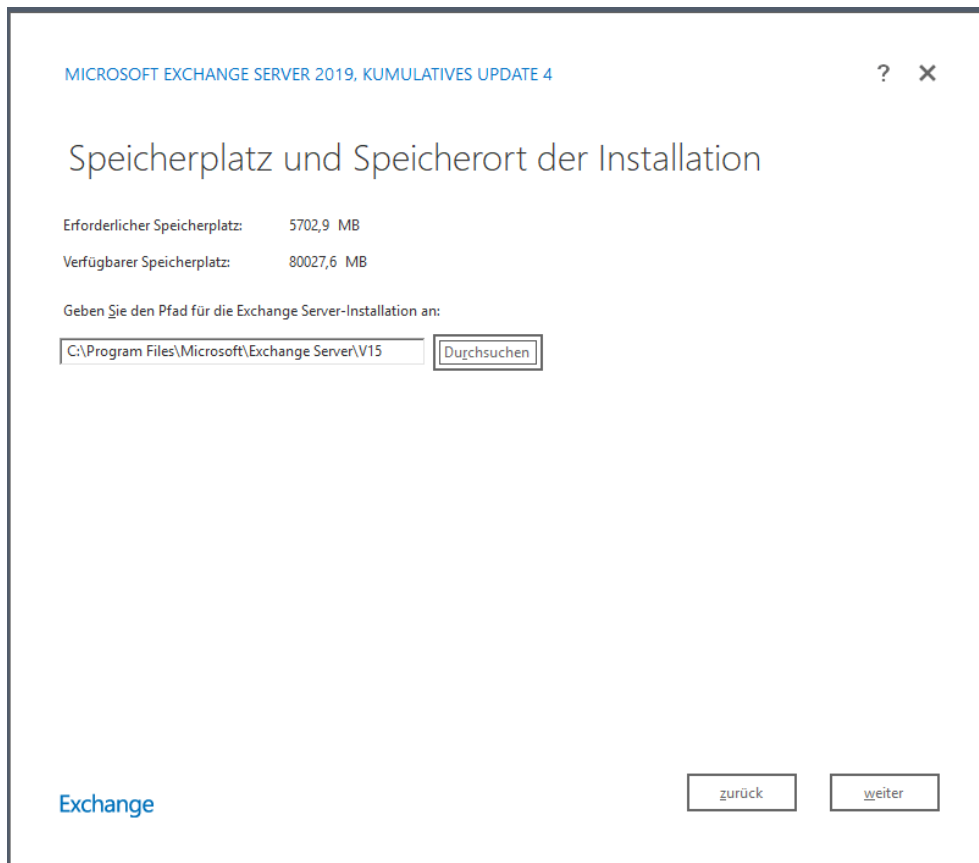
Das Setup selber führe ich benutzerdefiniert aus:



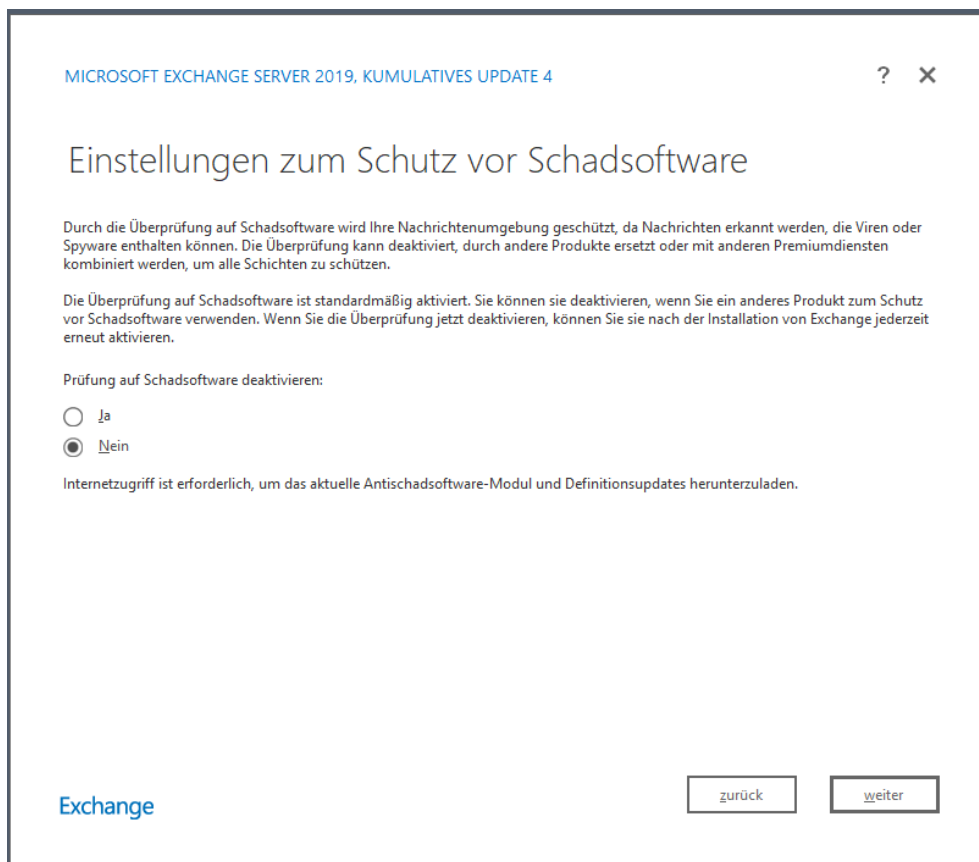
Hier kann man wenig falsch machen:



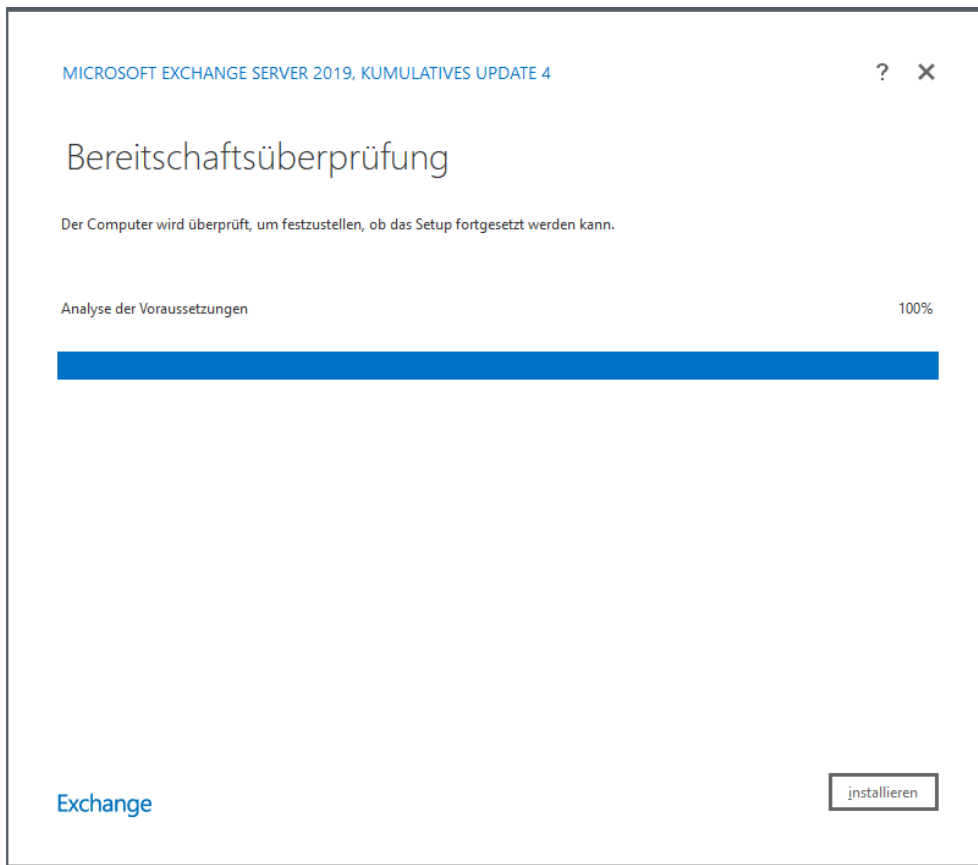
Auch den Speicherpfad belasse ich auf dem Systemlaufwerk:



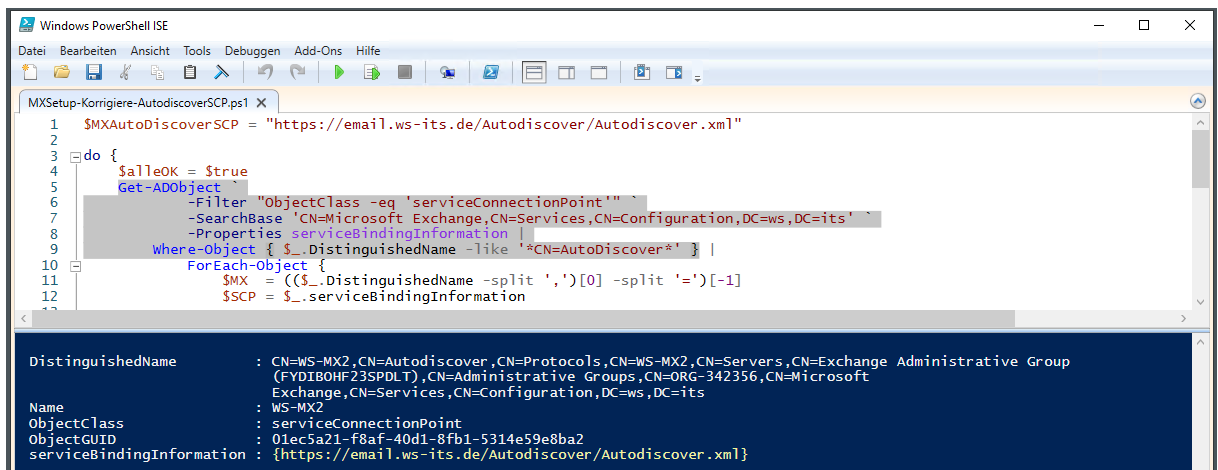
Diesen Schutz möchte ich später weiter verwenden:



Das Setup analysiert die Voraussetzungen für die Installation. Hier passt alles:



Bevor ich das Setup starte, bringe ich ein PowerShell-Script in Stellung. Dieser Code korrigiert den ServiceConnectionPoint aller Exchange Server, indem er bei allen die URL meines LoadBalancers einträgt. Das hatte ich bei meinem ersten Mailserver WS-MX2 bereits ausführlich erläutert (<https://www.ws-its.de/serie-mig2019-ws-mx2/> im Punkt „Installation des Exchange Servers 2019 CU4“).



```

1 $MXAutoDiscoverSCP = "https://email.ws-its.de/Autodiscover/Autodiscover.xml"
2
3 do {
4     $alleOK = $true
5     Get-ADObject
6         -Filter "ObjectClass -eq 'serviceConnectionPoint'"
7         -SearchBase 'CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=ws,DC=its'
8         -Properties serviceBindingInformation
9         -Where-Object { $_.DistinguishedName -like '*CN=AutoDiscover*' } |
10        ForEach-Object {
11            $MX = ((($_.DistinguishedName -split ',')[0] -split '=')[1])
12            $SCP = $_.serviceBindingInformation

```

```

DistinguishedName      : CN=WS-MX2,CN=Autodiscover,CN=Protocols,CN=WS-MX2,CN=Servers,CN=Exchange Administrative Group
                        (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=ORG-342356,CN=Microsoft
                        Exchange,CN=Services,CN=Configuration,DC=ws,DC=its
Name                   : WS-MX2
ObjectClass            : serviceConnectionPoint
ObjectGUID             : 01ec5a21-f8af-40d1-8fb1-5314e59e8ba2
ServiceBindingInformation : {https://email.ws-its.de/Autodiscover/Autodiscover.xml}

```

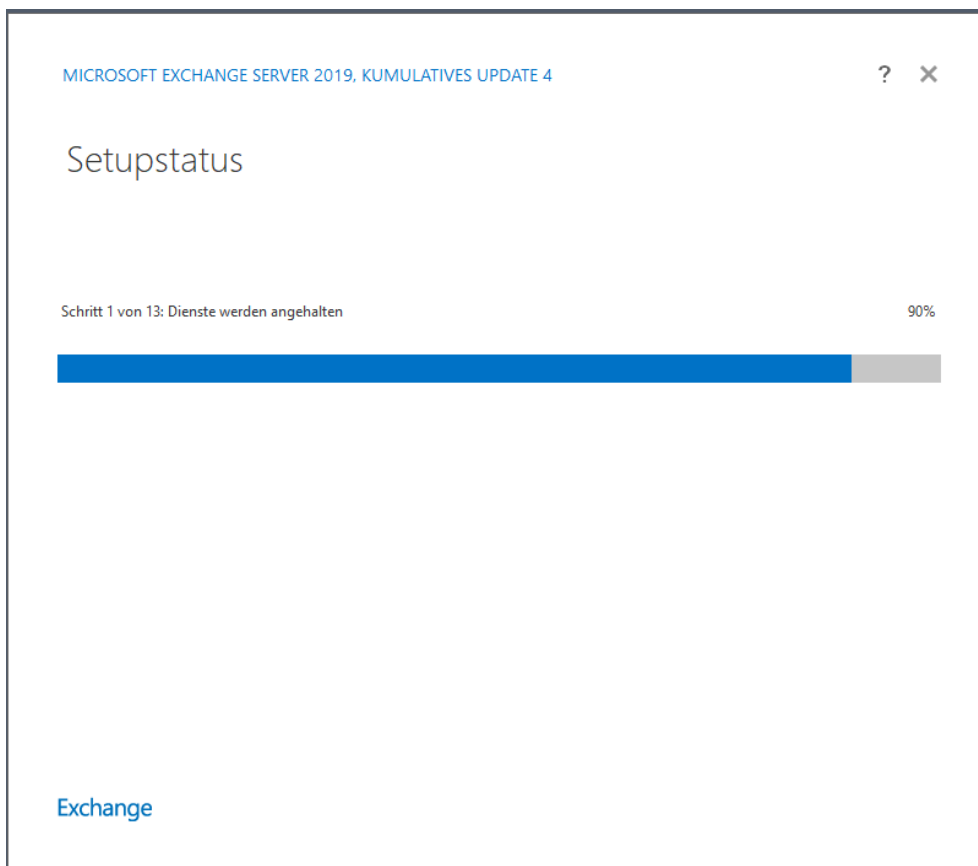
Das Script läuft und kontrolliert im Sekundentakt auf abweichende Records:

```

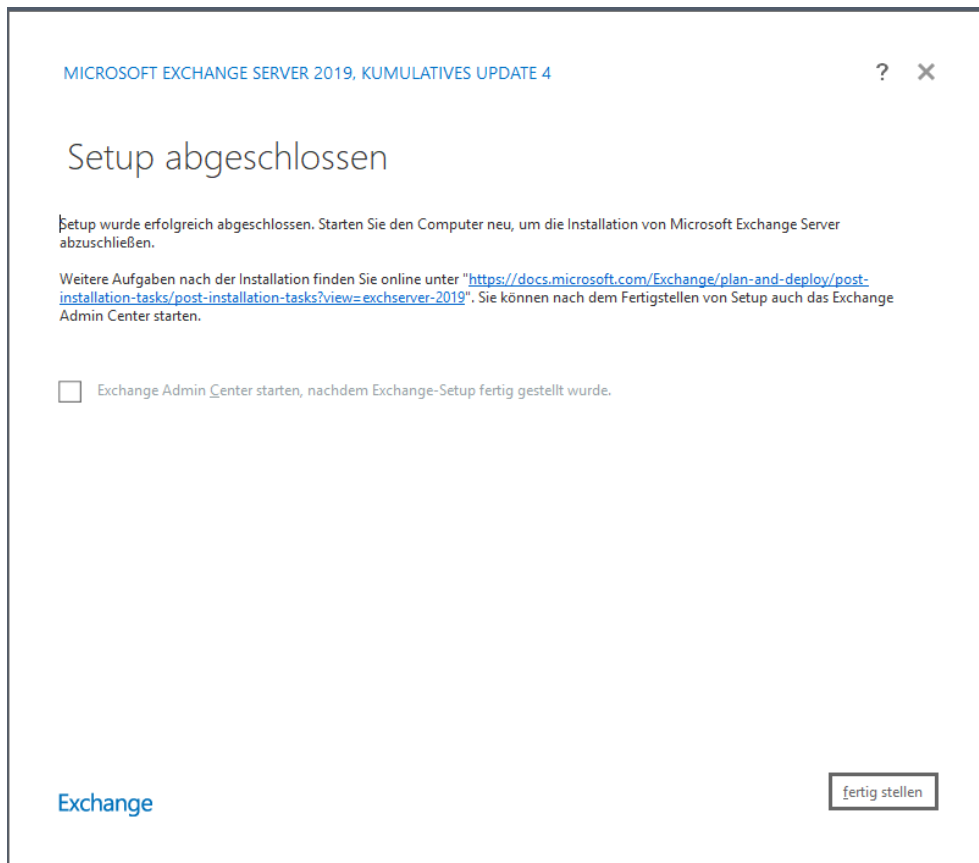
MXSetup-Korrigiere-AutodiscoverSCP.ps1 X
1 $MXAutoDiscoverSCP = "https://email.ws-its.de/Autodiscover/Autodiscover.xml"
2
3 do {
4     $alleOK = $true
5     Get-ADObject `
6         -Filter "ObjectClass -eq 'serviceConnectionPoint'" `
7         -SearchBase 'CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=ws,DC=its' `
8         -Properties serviceBindingInformation |
9     Where-Object { $_.DistinguishedName -like '*CN=AutoDiscover*' } |
10    ForEach-Object {
11        $MX = ((($_.DistinguishedName -split ',')[0] -split '=')[1])
12        $SCP = $_.serviceBindingInformation
13
14        if ( $SCP -ne $MXAutoDiscoverSCP ) {
15            Write-Host "$(get-date -format 'HH:mm:ss') - SCP von $MX ist falsch: $SCP" -ForegroundColor Yellow
16
17            $alleOK = $false
18            Set-ADObject -Identity $_.DistinguishedName -Replace @{{serviceBindingInformation=$MXAutoDiscoverSCP}}
19        }
20    }
21    if ( $alleOK ) { Write-Host "$(get-date -format 'HH:mm:ss') - alles SCP sind ok." -ForegroundColor Green }
22
23    Start-Sleep -Seconds 1
24 } while ($true)
    
```

PS C:\> C:\Users\stephan-t1\Desktop\MXSetup-Korrigiere-AutodiscoverSCP.ps1
 13:08:04 - alles SCP sind ok.
 13:08:05 - alles SCP sind ok.
 13:08:06 - alles SCP sind ok.
 13:08:07 - alles SCP sind ok.
 13:08:08 - alles SCP sind ok.

Jetzt starte ich das Setup:



Einige Minuten später ist es abgeschlossen:



Während der Server neustartet, kontrolliere ich mein SCP-Korrektur-Script. Hier gab es ein paar Verzögerungen durch die AD-Replikation:

```

13:26:43 - alles SCP sind ok.
13:26:44 - alles SCP sind ok.
13:26:45 - alles SCP sind ok.
13:26:46 - alles SCP sind ok.
13:26:47 - alles SCP sind ok.
13:26:48 - alles SCP sind ok.
13:26:49 - alles SCP sind ok.
13:26:50 - alles SCP sind ok.
13:26:51 - alles SCP sind ok.
13:26:52 - alles SCP sind ok.
13:26:53 - alles SCP sind ok.
13:26:54 - alles SCP sind ok.
13:26:55 - alles SCP sind ok.
13:26:56 - alles SCP sind ok.
13:26:57 - alles SCP sind ok.
13:26:58 - alles SCP sind ok.
13:26:59 - alles SCP sind ok.
13:27:00 - alles SCP sind ok.
13:27:01 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
Set-ADObject : Verzeichnisobjekt nicht gefunden
In C:\Users\stephan-t1\Desktop\MXSetup-Korrigiere-AutodiscoverSCP.ps1:18 Zeichen:21
+ ... Set-ADObject -Identity $_.DistinguishedName -Replace @{$se ...
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (CN=WS-MX1,CN=Au...on,DC=ws,DC=its:ADObject) [Set-ADObject], ADIdentityNotFoundExcep
tion
+ FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityNotFoundException,Microsoft.Act
iveDirectory.Management.Commands.SetADObject

13:27:02 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
Set-ADObject : Verzeichnisobjekt nicht gefunden
In C:\Users\stephan-t1\Desktop\MXSetup-Korrigiere-AutodiscoverSCP.ps1:18 Zeichen:21
+ ... Set-ADObject -Identity $_.DistinguishedName -Replace @{$se ...
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (CN=WS-MX1,CN=Au...on,DC=ws,DC=its:ADObject) [Set-ADObject], ADIdentityNotFoundExcep
tion
  
```

Das führte zu mehreren Sekunden, in denen der FQDN des neuen Servers veröffentlicht wurde:

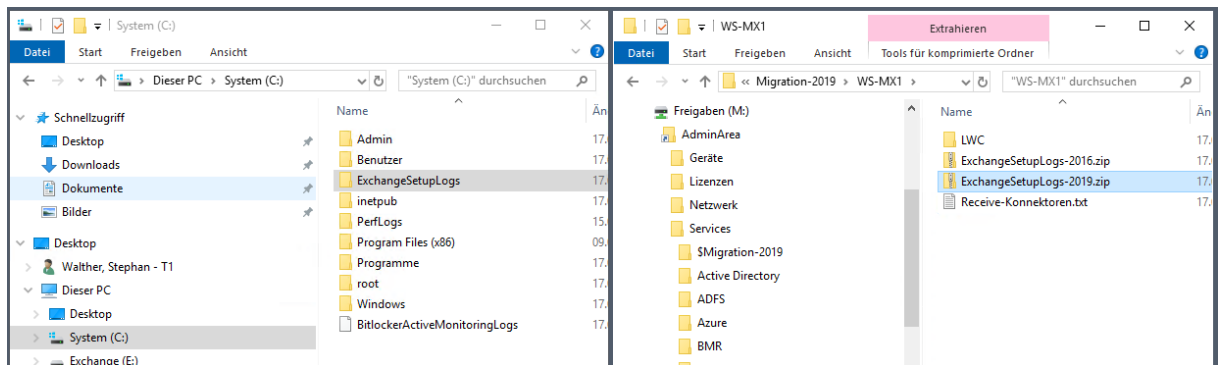
```
+ CategoryInfo          : ObjectNotFound: (CN=WS-MX1,CN=Au...on,DC=ws,DC=its:ADObject) [Set-ADObject], ADIdentityNotFoundExcept
tion
+ FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityNotFoundExceptio
n,Microsoft.ActiveDirectory.Management.Commands.SetADObject

13:27:10 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
Set-ADObject : Verzeichnisobjekt nicht gefunden
In C:\Users\stephan-t1\Desktop\MXSetup-Korrigiere-AutodiscoverSCP.ps1:18 Zeichen:21
+ ... Set-ADObject -Identity $_.DistinguishedName -Replace @{se ...
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (CN=WS-MX1,CN=Au...on,DC=ws,DC=its:ADObject) [Set-ADObject], ADIdentityNotFoundExcept
tion
+ FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityNotFoundExceptio
n,Microsoft.ActiveDirectory.Management.Commands.SetADObject

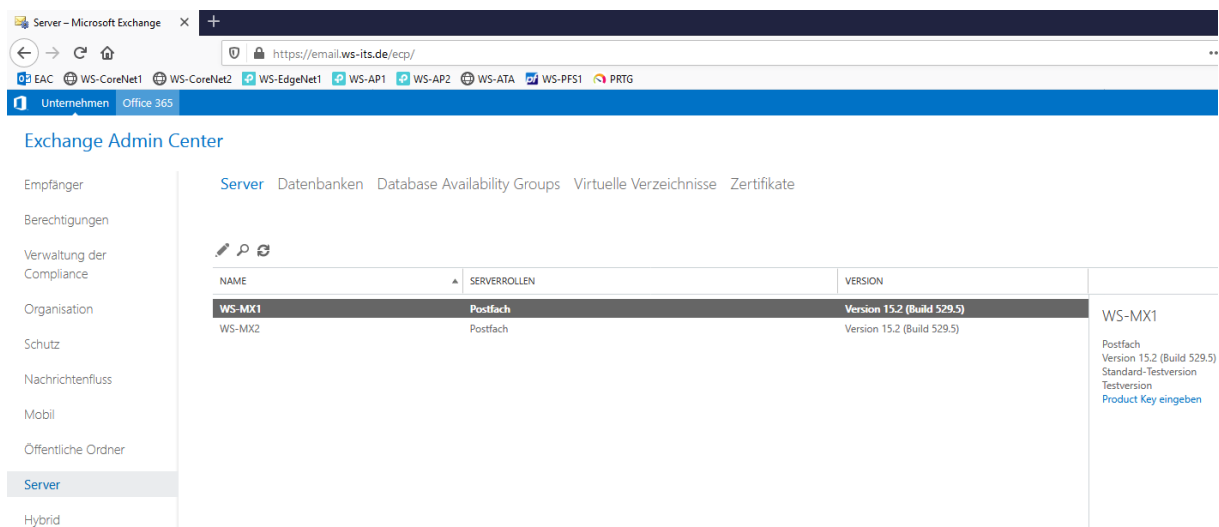
13:27:11 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:12 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:13 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:14 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:15 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:16 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:17 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:18 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:19 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:20 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:21 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:22 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:23 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:24 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:25 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:26 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:27 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:28 - SCP von WS-MX1 ist falsch: https://WS-MX1.ws.its/Autodiscover/Autodiscover.xml
13:27:29 - alles SCP sind ok.
13:27:30 - alles SCP sind ok.
```

Praxistipp: Zur Sicherheit sollte jetzt auf JEDEM Exchange Server im IIS-Manager der ApplicationPool für das AutoDiscover durchgestartet werden. Diese Webanwendungen speichern sich unter Umständen diese falschen Informationen aus dem Active Directory für 30 Minuten!

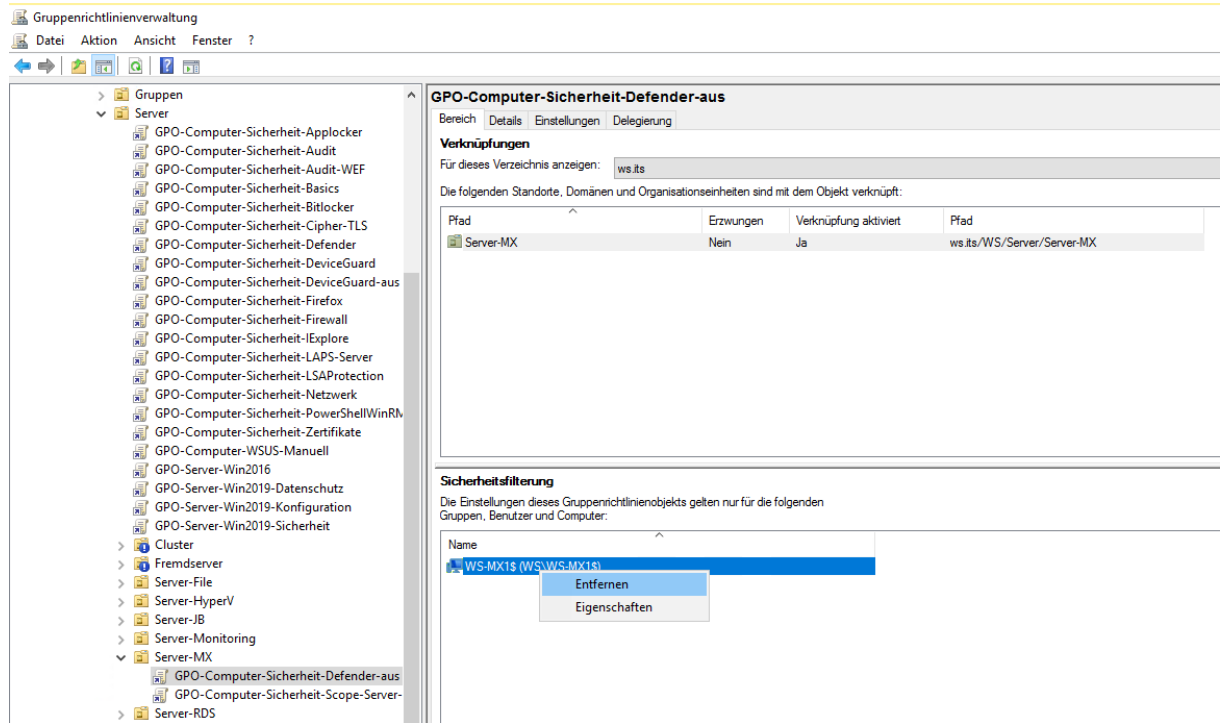
Das ExchangeSetupLog-Verzeichnis archiviere ich wieder in meinem AdminShare:



Im Exchange Admin Center wird der neue Server gelistet:



Zuletzt entferne ich die Gruppenrichtlinie mit der Deaktivierung des Windows Defender:



Das Setup ist damit abgeschlossen. Weiter geht es mit der Rollenkonfiguration.

Konfiguration der Rolle CAS

Konfiguration der Virtual Directories

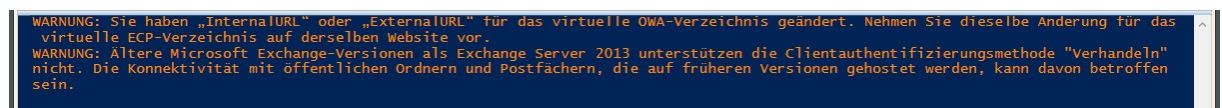
Ich beginne mit der Rolle ClientAccessService. Die Konfiguration habe ich vom anderen Server kopiert. Ich definiere die VirtualDirectories:

```

290 #region Konfiguration der Rolle CAS auf WS-MX1
291 # Variablen
292 $servername = "WS-MX1"
293
294 # Konfiguration der VirtualDirectories
295 $internalhostname = "email.ws-its.de"
296 $externalhostname = "email.ws-its.de"
297 $autodiscoverhostname = "email.ws-its.de"
298
299 $owaurl = "https://$internalhostname/owa"
300 $owaexternalurl = "https://$externalhostname/owa"
301 $ecpurl = "https://$internalhostname/ecp"
302 $ecpexternalurl = "https://$externalhostname/ecp"
303 $ewsurl = "https://$internalhostname/EWS/Exchange.asmx"
304 $ewsexternalurl = "https://$externalhostname/EWS/Exchange.asmx"
305 $asurl = "https://$internalhostname/Microsoft-Server-ActiveSync"
306 $asexternalurl = "https://$externalhostname/Microsoft-Server-ActiveSync"
307 $oaburl = "https://$internalhostname/OAB"
308 $oabexternalurl = "https://$externalhostname/OAB"
309 $mapiurl = "https://$internalhostname/mapi"
310 $mapiexternalurl = "https://$externalhostname/mapi"
311 $adurl = "https://$autodiscoverhostname/Autodiscover/Autodiscover.xml"
312
313 Get-OwaVirtualDirectory -Server $servername | Set-OwaVirtualDirectory -internalurl $owaurl -external
314 Get-EcpVirtualDirectory -Server $servername | Set-EcpVirtualDirectory -internalurl $ecpurl -external
315 Get-WebServicesVirtualDirectory -Server $servername | Set-WebServicesVirtualDirectory -internalurl $ewsurl -external
316 Get-ActiveSyncVirtualDirectory -Server $servername | Set-ActiveSyncVirtualDirectory -internalurl $asurl -external
317 Get-OabVirtualDirectory -Server $servername | Set-OabVirtualDirectory -internalurl $oaburl -external
318 Get-MapiVirtualDirectory -Server $servername | Set-MapiVirtualDirectory -internalurl $mapiurl -external
319 Get-ClientAccessService -Identity $servername | Set-ClientAccessService -AutoDiscoverServiceInternalUri $adurl
320 Get-OutlookAnywhere -Server $servername | Set-OutlookAnywhere -externalhostname $externalhostname -
321 -internalhostname $internalhostname -
322 -ExternalClientsRequireSsl:$true -
323 -InternalClientsRequireSsl:$true -
324 -ExternalClientAuthenticationMethod 'Negotiate'
325
326

```

Die Warnungen können ignoriert werden –das ECP und das OWA Virtual Directory wurden nacheinander konfiguriert:



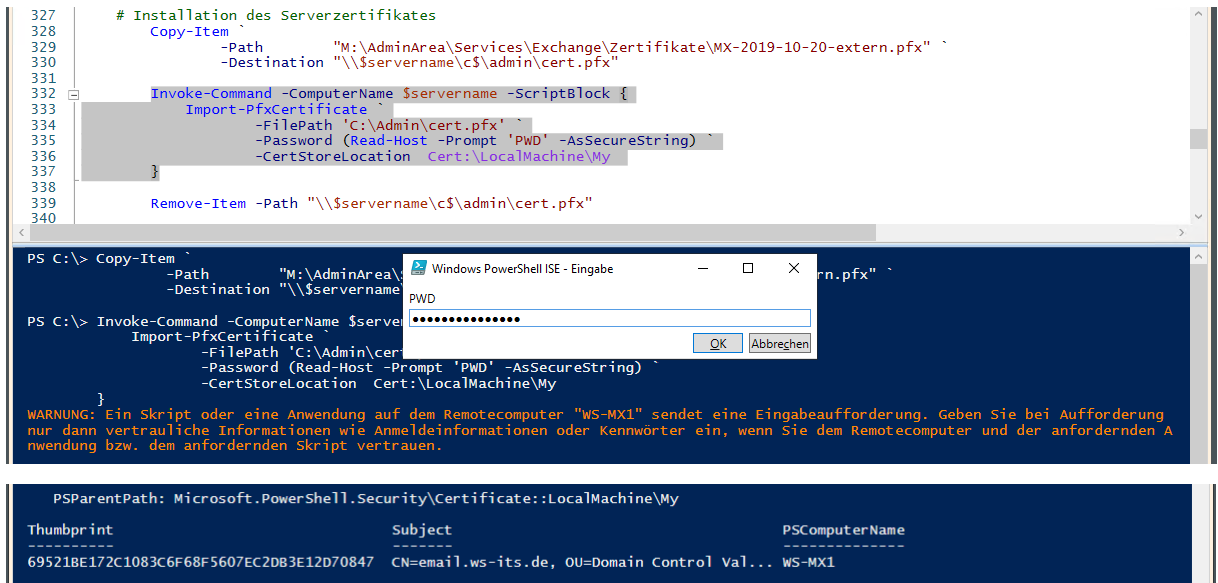
Installation des Serverzertifikates

Der CAS ist ein Webdienst. Hier ist ein Serverzertifikat eine zwingende Voraussetzung. Die PKCS12-Datei importiere ich mit der PowerShell:

```

327 # Installation des Serverzertifikates
328 Copy-Item `
329     -Path "M:\AdminArea\Services\Exchange\Zertifikate\MX-2019-10-20-extern.pfx" `
330     -Destination "\\$servername\c$\admin\cert.pfx"
331
332 Invoke-Command -ComputerName $servername -ScriptBlock {
333     Import-PfxCertificate `
334         -FilePath 'C:\Admin\cert.pfx' `
335         -Password (Read-Host -Prompt 'PWD' -AsSecureString) `
336         -CertStoreLocation Cert:\LocalMachine\My
337 }
338
339 Remove-Item -Path "\\$servername\c$\admin\cert.pfx"
340

```



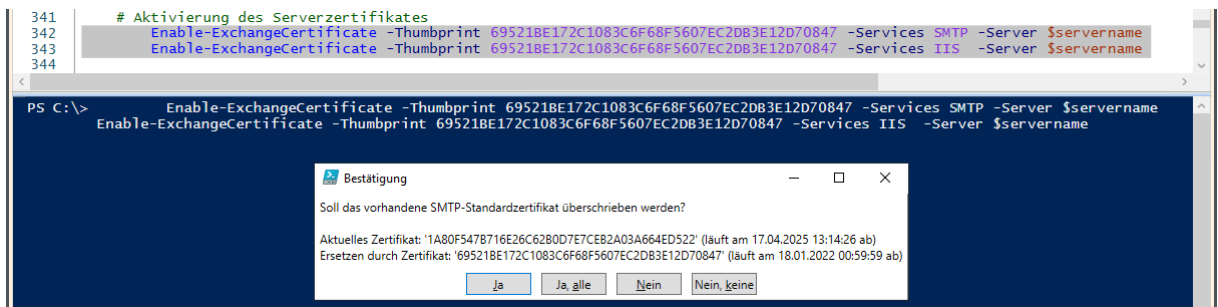
Thumbprint	Subject	PSComputerName
69521BE172C1083C6F68F5607EC2DB3E12D70847	CN=email.ws-its.de, OU=Domain Control Val...	WS-MX1

Danach aktiviere ich die Verwendung des neuen Zertifikates im IIS und auch gleich für den Hubtransport:

```

341 # Aktivierung des Serverzertifikates
342 Enable-ExchangeCertificate -Thumbprint 69521BE172C1083C6F68F5607EC2DB3E12D70847 -Services SMTP -Server $servername
343 Enable-ExchangeCertificate -Thumbprint 69521BE172C1083C6F68F5607EC2DB3E12D70847 -Services IIS -Server $servername
344

```



Bestätigung

Soll das vorhandene SMTP-Standardzertifikat überschrieben werden?

Aktuelles Zertifikat: '1A80F547B716E26C6280D7E7CEB2A03A664ED522' (läuft am 17.04.2025 13:14:26 ab)
 Ersetzen durch Zertifikat: '69521BE172C1083C6F68F5607EC2DB3E12D70847' (läuft am 18.01.2022 00:59:59 ab)

Ja Ja, alle Nein Nein, keine

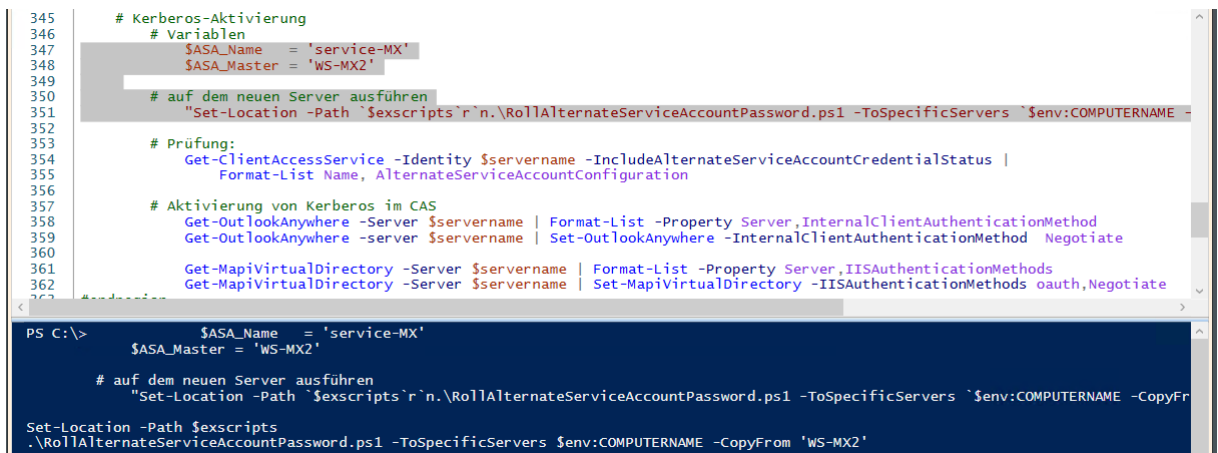
Umstellung auf Kerberos-Authentification

Im nächsten Schritt aktiviere ich die Anmeldung mit Kerberos auf dem neuen Exchange Server. Die Konfiguration ist auf dem anderen Server bereits aktiv. Daher soll sich der neue Server dessen Informationen holen. In meinem PowerShell-Skript wird der Aufruf als Text ausgegeben. Das Ergebnis sind Befehle. Dies kopiere ich in die Zwischenablage:

```

345 # Kerberos-Aktivierung
346 # Variablen
347 $ASA_Name = 'service-MX'
348 $ASA_Master = 'WS-MX2'
349
350 # auf dem neuen Server ausführen
351 "Set-Location -Path `"$exscripts\r\n.\Ro11AlternateServiceAccountPassword.ps1 -ToSpecificServers `"$env:COMPUTERNAME
352
353 # Prüfung:
354 Get-ClientAccessService -Identity $servername -IncludeAlternateServiceAccountCredentialStatus |
355     Format-List Name, AlternateServiceAccountConfiguration
356
357 # Aktivierung von Kerberos im CAS
358 Get-OutlookAnywhere -Server $servername | Format-List -Property Server,InternalClientAuthenticationMethod
359 Get-OutlookAnywhere -server $servername | Set-OutlookAnywhere -InternalClientAuthenticationMethod Negotiate
360
361 Get-MapiVirtualDirectory -Server $servername | Format-List -Property Server,IISAuthenticationMethods
362 Get-MapiVirtualDirectory -Server $servername | Set-MapiVirtualDirectory -IISAuthenticationMethods oauth,Negotiate
363

```



```

PS C:\> $ASA_Name = 'service-MX'
        $ASA_Master = 'WS-MX2'

# auf dem neuen Server ausführen
"Set-Location -Path `"$exscripts\r\n.\Ro11AlternateServiceAccountPassword.ps1 -ToSpecificServers `"$env:COMPUTERNAME -CopyFr
Set-Location -Path $exscripts
.\Ro11AlternateServiceAccountPassword.ps1 -ToSpecificServers $env:COMPUTERNAME -CopyFrom 'WS-MX2'

```

Dann starte ich auf dem Exchange Server WS-MX1 eine Exchange Management Shell und füge anschließend die Befehle aus der Zwischenablage ein:

```

Computer: WS-MX1.ws.its
[PS] C:\>Set-Location -Path $exscripts
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>. \RollAlternateServiceAccountPassword.ps1 -ToSpecificServers
$env:COMPUTERNAME -CopyFrom 'WS-MX2'

===== Starting at 04/17/2020 13:43:42 =====
Destination servers that will be updated:

Name      PSComputerName
-----
WS-MX1 ws-mx1.ws.its

Credentials that will be pushed to every server in the specified scope (recent first):

UserName          Password
-----
WS\service-MX$ System.Security.SecureString
WS\service-MX$ System.Security.SecureString

Prior to pushing new credentials, all existing credentials will be removed from the destination servers.
Pushing credentials to server WS-MX1
Retrieving the current Alternate Service Account configuration from servers in scope
Alternate Service Account properties:

StructuralObjectClass QualifiedUserName Last Pwd Update      SPNs
-----
computer              WS\service-MX$  24.07.2019 13:35:23 http/email.ws-its.de
                    http/email.ws.its

Per-server Alternate Service Account configuration as of the time of script completion:

Array: {email.ws-its.de, email.ws-its.de}

Identity AlternateServiceAccountConfiguration
-----
WS-MX1  Zuletzt: 17.04.2020 13:43:52, WS\service-MX$
        Zuvor: 17.04.2020 13:43:52, WS\service-MX$

===== Finished at 04/17/2020 13:43:53 =====

THE SCRIPT HAS SUCCEEDED
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>

```

Der Prozess war erfolgreich. Das bestätigt mir auch die Abfrage in der PowerShell-ISE:

```

353 # Prüfung:
354 Get-ClientAccessService -Identity $servername -IncludeAlternateServiceAccountCredentialStatus |
355 Format-List Name, AlternateServiceAccountConfiguration
356
Name : WS-MX1
AlternateServiceAccountConfiguration : Zuletzt: 17.04.2020 13:43:52, WS\service-MX$
                                       Zuvor: 17.04.2020 13:43:52, WS\service-MX$

```

Jetzt kann ich Kerberos für den Outlook-Zugriff konfigurieren:

```

357 # Aktivierung von Kerberos im CAS
358 Get-OutlookAnywhere -Server $servername | Format-List -Property Server,InternalClientAuthenticationMethod
359 Get-OutlookAnywhere -server $servername | Set-OutlookAnywhere -InternalClientAuthenticationMethod Negotiate
360
361 Get-MapiVirtualDirectory -Server $servername | Format-List -Property Server,IISAuthenticationMethods
362 Get-MapiVirtualDirectory -Server $servername | Set-MapiVirtualDirectory -IISAuthenticationMethods oAuth,Negotiate
363 #endregion
364
#region Konfiguration der Rolle IIS auf WS-MX1
Server : WS-MX1
InternalClientAuthenticationMethod : NTlm

WARNUNG: Ältere Microsoft Exchange-Versionen als Exchange Server 2013 unterstützen die Clientauthentifizierungsmethode "Verhandeln" nicht. Die Konnektivität mit öffentlichen Ordnern und Postfächern, die auf früheren Versionen gehostet werden, kann davon betroffen sein.

Server : WS-MX1
IISAuthenticationMethods : {Ntlm, OAuth, Negotiate}

```

Das war auch schon alles.

Testlauf im Loadbalancer

Der ClientAccessService ist fertig konfiguriert. Es wird Zeit für einen Testlauf. Der vorgeschaltete LoadBalancer in meiner PfSense leitet aktuell alle Clients auf den anderen Mailserver um:

The screenshot shows the pfSense Firewall Logs interface. The 'Snort Alerts' and 'Firewall Logs' sections are visible. The 'Firewall Logs' table shows several entries with a red 'X' icon, indicating errors. The 'Description' column for these entries reads 'ET INFO Observed DNS Query to .cloud TLD'. The 'Source' and 'Destination' columns show IP addresses and ports.

Act	Time	IF	Source	Destination
X	Apr 17 13:45	LAN_100_SERVER	192.168.100.13	93.184.221.240:80
X	Apr 17 13:45	LAN_100_SERVER	192.168.100.9	93.184.220.29:80
X	Apr 17 13:45	DMZ_120_EXTERN	172.19.120.254	172.19.130.101:80
X	Apr 17 13:45	LAN_100_SERVER	192.168.100.13	93.184.221.240:80
✓	Apr 17 13:45	DMZ_140_GAMEZONE	172.19.140.101	62.67.238.148:443
X	Apr 17 13:45	LAN_100_SERVER	192.168.100.13	92.123.213.9:80

In meiner kleinen Umgebung drehe ich nun das Backend des LoadBalancers um und leite alle Clientanfragen auf den neuen Server. Das würde ich in einer größeren Umgebung anders lösen. Da könnte z.B. die HOSTS-Datei eines Testclients modifiziert werden, damit der Client direkt beim neuen Mailserver herauskommt.

The screenshot shows the pfSense HAProxy Backend configuration page. The 'Backend' tab is selected. The 'Name' field is set to 'MX'. The 'Server list' section contains a table with two entries: 'WS-MX1' (active) and 'WS-MX2' (disabled). The 'Forwardto' field is set to 'Address+Port'.

Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Action
active	WS-MX1	Address+Port	192.168.100.3	443	<input type="checkbox"/>	<input type="checkbox"/>		
disabled	WS-MX2	Address+Port	192.168.100.13	443	<input type="checkbox"/>	<input type="checkbox"/>		

Die Verbindungen werden umgelenkt:

The screenshot shows the pfSense interface. On the left, there's a sidebar with system information. The main area is divided into three panels:

- Snort Alerts:** A table showing alerts from the DMZ_120_EXTERN interface. All alerts are of type 'ET INFO Observed DNS Query to .cloud TLD' and occurred on April 17, 2020.
- HAProxy:** A table showing the status of various backends. Backends include RDSWEB_ipvANY, MX_ipvANY (with servers WS-MX1 and WS-MX2), RDS_ipvANY, PRTG_ipvANY, and SMTP_ipv4. Sessions and status are indicated for each.
- Firewall Logs:** A table showing a single log entry for an outgoing connection from LAN_100_SERVER to 192.168.101.1:5985.

Mein Outlook hat mit dem neuen Server keine Probleme. Ebenso funktioniert mein ActiveSync am Smartphone:

The screenshot shows the 'Outlook-Verbindungsstatus' window. It displays a table of connection logs for various email accounts. The columns include VID, SMTP-Adresse, Anzeigename, Proxyserver, Servername, Status, Protokoll, Authn, Versc..., RPC-Port, Typ, Anfr/Fehler, Reaktion..., Bearb (0), Sitzungstyp, and Schr. The status for all listed connections is 'hergestellt' (established).

Produktivschaltung der CAS-Rolle

CAS ist also einsatzbereit. Final aktiviere ich beide Exchange Server im LoadBalancer:

The screenshot shows the 'Edit HAProxy Backend server pool' configuration in pfSense. The name of the backend is 'MX'. Below, a table lists the servers in the pool:

Mode	Name	Forwardto	Address	Port	SSL Encrypt(SSL)	checks	Weight	Action
active	WS-MX1	Address+Port	192.168.100.3	443	<input type="checkbox"/>	<input type="checkbox"/>		
active	WS-MX2	Address+Port	192.168.100.13	443	<input type="checkbox"/>	<input type="checkbox"/>		

Beide Mailserver arbeiten nun gemeinsam die Clientanfragen ab:

The screenshot shows the pfSense web interface. The 'HAProxy' configuration is visible, showing a list of backends with their session counts and status. Below it, the 'Snort Alerts' table shows several alerts related to DNS queries to .cloud TLD. The 'Firewall Logs' table at the bottom shows a log entry for an allowed connection from 109.168.100.18 to 102.168.101.195.

Backend(s) / Server(s)	Sessions (cur/max)	Status / Actions
RDSWEB_ipvANY / WS-RDS1	0 / 200	✓
MX_ipvANY / WS-MX1	2 / 200	✓
192.168.100.22:60997	1	✓
WS-MX2	15s / 0x80242ac00	✓
172.19.130.105:49309	5s / 0x80242b000	✓
RDS_ipvANY / WS-RDS2	0 / 200	✓
PRTG_ipvANY / WS-MON	0 / 200	✓
SMTP_ipv4 / WS-MX1	0 / 200	✓
WS-MX2	0	✓

Interface/Time	Src/Dst Address	Description
DMZ_120_EXTERN / Apr 17 13:35:31	192.168.100.2:64177 / 172.19.120.254:53	ET INFO Observed DNS Query to .cloud TLD
DMZ_120_EXTERN / Apr 17 13:33:39	192.168.100.2:63999 / 172.19.120.254:53	ET INFO Observed DNS Query to .cloud TLD
DMZ_120_EXTERN / Apr 17 13:32:15	192.168.100.1:64485 / 172.19.120.254:53	ET INFO Observed DNS Query to .cloud TLD
DMZ_120_EXTERN / Apr 17 13:28:39	192.168.100.2:62225 / 172.19.120.254:53	ET INFO Observed DNS Query to .cloud TLD
DMZ_120_EXTERN / Apr 17 13:28:39	192.168.100.1:65397 / 172.19.120.254:53	ET INFO Observed DNS Query to .cloud TLD

Act	Time	IF	Source	Destination
✓	Apr 17 13:40	LAN	109.168.100.18	102.168.101.195

Damit ist diese Funktion wieder hochverfügbar.

Konfiguration der Rolle HTS

Verschiebung der Transportdatenbank

Auch die zweite der drei Hauptfunktionen – der Mailfluss im HubTransportService – benötigt nicht viel Zeit. Zuerst verschiebe ich die Transportdatenbank auf die neue Partition. Diese DB kann ebenfalls schnell sehr groß werden und würde auf der Systempartition nur Probleme verursachen. Die Verschiebung gelingt mit einem Exchange-Script in der Management Shell:

```

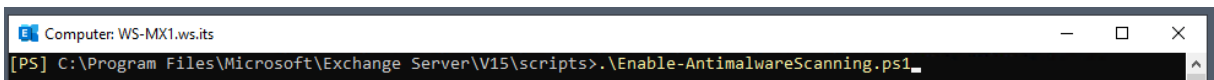
[PS] C:\Windows\system32>cd $exscripts
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>.\Move-TransportDatabase.ps1
>> -queueDatabasePath e:\Exchange\Transport
>> -queueDatabaseLoggingPath e:\Exchange\Transport
>> -ipFilterDatabasePath e:\Exchange\Transport\IPFilter
>> -ipFilterDatabaseLoggingPath e:\Exchange\Transport\IPFilter
>> -temporaryStoragePath e:\Exchange\Transport
Queue Database Logging : Originalpfad ist C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\data\Queue; neuer Pfad ist e:\Exchange\Transport
Temporary Storage : Originalpfad ist C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\data\Temp; neuer Pfad ist e:\Exchange\Transport
IP Filter Database Logging : Originalpfad ist C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\data\IpFilter; neuer Pfad ist e:\Exchange\Transport\IPFilter
IP Filter Database : Originalpfad ist C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\data\IpFilter; neuer Pfad ist e:\Exchange\Transport\IPFilter
Queue Database : Originalpfad ist C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\data\Queue; neuer Pfad ist e:\Exchange\Transport
Erforderlicher Speicherplatz: 2168455168 Bytes. Freier Speicherplatz auf Ziellaufwerk e: ist 105528856576 Bytes.
Erforderlicher Speicherplatz: 2147483648 Bytes. Freier Speicherplatz auf Ziellaufwerk e: ist 105528856576 Bytes.
Erforderlicher Speicherplatz: 2149580800 Bytes. Freier Speicherplatz auf Ziellaufwerk e: ist 105528856576 Bytes.
Erforderlicher Speicherplatz: 2155945984 Bytes. Freier Speicherplatz auf Ziellaufwerk e: ist 105528856576 Bytes.
Erforderlicher Speicherplatz: 2155945984 Bytes. Freier Speicherplatz auf Ziellaufwerk e: ist 105528856576 Bytes.
e:\Exchange\Transport ist bereits vorhanden. Die Verzeichniserstellung wird übersprungen.
NetworkServiceSid hat bereits Vollzugriff auf das Verzeichnis.
LocalSystemSid hat bereits Vollzugriff auf das Verzeichnis.
BuiltinAdministratorsSid hat bereits Vollzugriff auf das Verzeichnis.
e:\Exchange\Transport ist bereits vorhanden. Die Verzeichniserstellung wird übersprungen.
NetworkServiceSid hat bereits Vollzugriff auf das Verzeichnis.
LocalSystemSid hat bereits Vollzugriff auf das Verzeichnis.
BuiltinAdministratorsSid hat bereits Vollzugriff auf das Verzeichnis.
e:\Exchange\Transport\IPFilter wird erstellt.
Für NetworkServiceSid wird Vollzugriff auf das Verzeichnis hinzugefügt.
Für LocalSystemSid wird Vollzugriff auf das Verzeichnis hinzugefügt.
Für BuiltinAdministratorsSid wird Vollzugriff auf das Verzeichnis hinzugefügt.
e:\Exchange\Transport\IPFilter ist bereits vorhanden. Die Verzeichniserstellung wird übersprungen.
NetworkServiceSid hat bereits Vollzugriff auf das Verzeichnis.
LocalSystemSid hat bereits Vollzugriff auf das Verzeichnis.
BuiltinAdministratorsSid hat bereits Vollzugriff auf das Verzeichnis.
e:\Exchange\Transport ist bereits vorhanden. Die Verzeichniserstellung wird übersprungen.
NetworkServiceSid hat bereits Vollzugriff auf das Verzeichnis.
LocalSystemSid hat bereits Vollzugriff auf das Verzeichnis.
BuiltinAdministratorsSid hat bereits Vollzugriff auf das Verzeichnis.
stop für den MSExchangeTransport-Dienst wird vorbereitet...
WARNUNG: Warten auf Beendigung des Diensts "Microsoft Exchange-Transport (MSExchangeTransport)"...
WARNUNG: Warten auf Beendigung des Diensts "Microsoft Exchange-Transport (MSExchangeTransport)"...
Der MSExchangeTransport-Dienst wurde erfolgreich gestoppt.
  
```

```

Der MExchangeTransport-Dienst wurde erfolgreich stopped.
Eine Kopie der ursprünglichen Konfigurationsdatei wird in C:\Program Files\Microsoft\Exchange Server\V15\bin\EdgeTranspo
rt.exe.config.20200417135100.old gespeichert.
Datei trn.log wurde zum Ziel verschoben.
Datei trntmp.log wurde zum Ziel verschoben.
Datei Trnres00001.jrs wurde zum Ziel verschoben.
Datei Trnres00002.jrs wurde zum Ziel verschoben.
Die Datei Temp.edb wird übersprungen, weil sie nicht vorhanden ist.
Der Queue Database Logging-Pfad wird zu e:\Exchange\Transport aktualisiert.
Der Temporary Storage-Pfad wird zu e:\Exchange\Transport aktualisiert.
Datei trn.log wurde zum Ziel verschoben.
Datei trntmp.log wurde zum Ziel verschoben.
Datei Trnres00001.jrs wurde zum Ziel verschoben.
Datei Trnres00002.jrs wurde zum Ziel verschoben.
Die Datei Temp.edb wird übersprungen, weil sie nicht vorhanden ist.
Der IP Filter Database Logging-Pfad wird zu e:\Exchange\Transport\IPFilter aktualisiert.
Datei IPFiltering.edb wurde zum Ziel verschoben.
Datei trn.chk wurde zum Ziel verschoben.
Der IP Filter Database-Pfad wird zu e:\Exchange\Transport\IPFilter aktualisiert.
Datei mail.que wurde zum Ziel verschoben.
Datei trn.chk wurde zum Ziel verschoben.
Der Queue Database-Pfad wird zu e:\Exchange\Transport aktualisiert.
start für den MExchangeTransport-Dienst wird vorbereitet...
WARNUNG: Warten auf Start des Diensts "Microsoft Exchange-Transport (MExchangeTransport)"...
Der MExchangeTransport-Dienst wurde erfolgreich started.
Die Ausführung des Skripts wurde erfolgreich abgeschlossen.
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>_
  
```

Aktivierung der AntiSpam und AntiMalware-Features

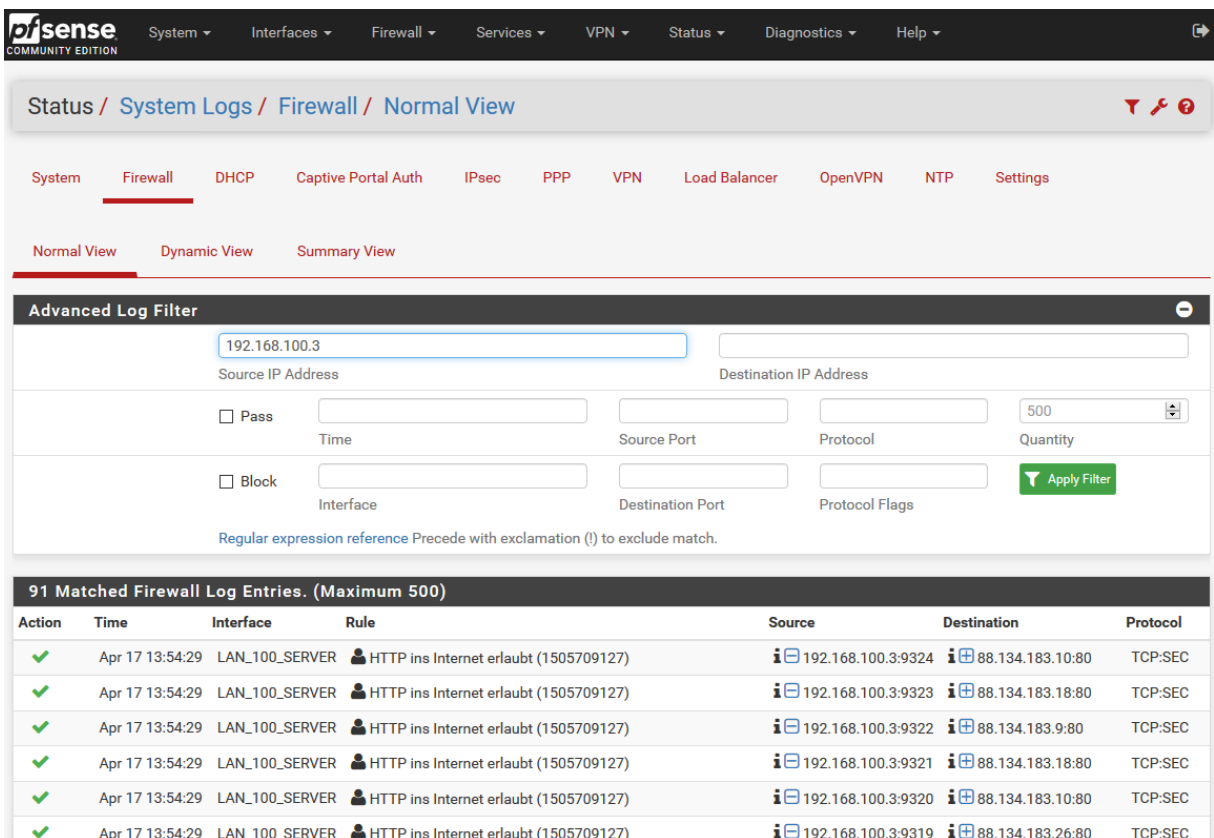
Bevor die ersten Mails den Server passieren, brauche ich AntiSpam und AntiMalware-Features. Dafür verwende ich die Boardmittel des Exchange Servers. Das erste Feature aktiviere ich in der Management Shell:



```

[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>.\Enable-AntimalwareScanning.ps1_
  
```

Das Script startet eine Aktualisierung. Die Dateien sollen aus dem Internet heruntergeladen werden. Da hat meine PFSense-Firewall aber etwas dagegen. Die entsprechende Ausnahme lässt den Server nach draußen:



The screenshot shows the pfSense Firewall configuration page. The 'Advanced Log Filter' section is active, with the source IP address set to 192.168.100.3. Below this, a table displays 91 matched firewall log entries. The table has columns for Action, Time, Interface, Rule, Source, Destination, and Protocol.

Action	Time	Interface	Rule	Source	Destination	Protocol
✓	Apr 17 13:54:29	LAN_100_SERVER	HTTP ins Internet erlaubt (1505709127)	192.168.100.3:9324	88.134.183.10:80	TCP:SEC
✓	Apr 17 13:54:29	LAN_100_SERVER	HTTP ins Internet erlaubt (1505709127)	192.168.100.3:9323	88.134.183.18:80	TCP:SEC
✓	Apr 17 13:54:29	LAN_100_SERVER	HTTP ins Internet erlaubt (1505709127)	192.168.100.3:9322	88.134.183.9:80	TCP:SEC
✓	Apr 17 13:54:29	LAN_100_SERVER	HTTP ins Internet erlaubt (1505709127)	192.168.100.3:9321	88.134.183.18:80	TCP:SEC
✓	Apr 17 13:54:29	LAN_100_SERVER	HTTP ins Internet erlaubt (1505709127)	192.168.100.3:9320	88.134.183.10:80	TCP:SEC
✓	Apr 17 13:54:29	LAN_100_SERVER	HTTP ins Internet erlaubt (1505709127)	192.168.100.3:9319	88.134.183.26:80	TCP:SEC

Wenige Minuten später ist ein Neustart des Services fällig:


```
PS C:\> Get-TransportAgent
```

Identity	Enabled	Priority
Transport Rule Agent	True	1
DLP Policy Agent	True	2
Retention Policy Agent	True	3
Supervisory Review Agent	True	4
Malware Agent	True	5
Text Messaging Routing Agent	True	6
Text Messaging Delivery Agent	True	7
System Probe Drop SmtP Agent	True	8
System Probe Drop Routing Agent	True	9
Content Filter Agent	True	10
Sender Id Agent	True	11
Sender Filter Agent	True	12
Recipient Filter Agent	True	13
Protocol Analysis Agent	True	14

Konfiguration der Konnektoren

Für den Empfang der Nachrichten führe ich die gleichen Befehle wie beim Server WS-MX2 aus. Damit editiere ich den Default-Connector zum Empfang interner Nachrichten und aktiviere das Logging:

```
389 # Konfiguration der Empfangskonnektoren
390 Get-ReceiveConnector -Server $servername |
391 Where-Object { $_.Identity -like '*Default Frontend*' } |
392 Set-ReceiveConnector -RemoteIPRanges '192.168.100.0/24','192.168.101.0/24','192.168.111.0/24'
393
394 Get-ReceiveConnector -Server $servername |
395 Where-Object { $_.Identity -like '*Default*' } |
396 Set-ReceiveConnector -ProtocolLoggingLevel 'verbose'
397
```

```
PS C:\> Get-ReceiveConnector -Server $servername |
Where-Object { $_.Identity -like '*Default Frontend*' } |
Set-ReceiveConnector -RemoteIPRanges '192.168.100.0/24','192.168.101.0/24','192.168.111.0/24'

PS C:\> Get-ReceiveConnector -Server $servername |
Where-Object { $_.Identity -like '*Default*' } |
Set-ReceiveConnector -ProtocolLoggingLevel 'verbose'
```

WARNUNG: Der Befehl wurde erfolgreich abgeschlossen, es wurden jedoch keine Einstellungen von 'WS-MX1\Default Frontend WS-MX1' geändert.

Und mit einem neuen Connector kann das System Mails aus dem Internet empfangen:

```
398 New-ReceiveConnector `
399 -Name 'Mails-vom-Internet' `
400 -MaxMessageSize 50MB `
401 -Enabled $true `
402 -ProtocolLoggingLevel 'verbose' `
403 -AuthMechanism 'Tls' `
404 -Fqdn 'email.ws-its.de' `
405 -PermissionGroups 'AnonymousUsers' `
406 -RemoteIPRanges '0.0.0.0-255.255.255.255' `
407 -Bindings '0.0.0.0:25' `
408 -Server $servername `
409 -TransportRole 'FrontEndTransport'
410
```

```
PS C:\> New-ReceiveConnector `
-Name 'Mails-vom-Internet' `
-MaxMessageSize 50MB `
-Enabled $true `
-ProtocolLoggingLevel 'verbose' `
-AuthMechanism 'Tls' `
-Fqdn 'email.ws-its.de' `
-PermissionGroups 'AnonymousUsers' `
-RemoteIPRanges '0.0.0.0-255.255.255.255' `
-Bindings '0.0.0.0:25' `
-Server $servername `
-TransportRole 'FrontEndTransport'
```

Identity	Bindings	Enabled
WS-MX1\Mails-vom-Internet	{0.0.0.0:25}	True

Da mein Monitoring und mein LoadBalancer permanent die SMTP-Services kontaktieren, erstelle ich einen weiteren Connector, trage dort die IP-Adressen ein und lasse die Protokollierung deaktiviert. So kann ich bei Zustell-Problemen die Logfiles viel leichter kontrollieren:


```

411 New-ReceiveConnector `
412     -Name 'ProbeMails' `
413     -Enabled $true `
414     -ProtocolLoggingLevel 'none' `
415     -AuthMechanism 'Tls' `
416     -PermissionGroups 'AnonymousUsers' `
417     -RemoteIPRanges '192.168.100.18','192.168.100.250' `
418     -Bindings '0.0.0.0:25' `
419     -Server $servername `
420     -TransportRole 'FrontEndTransport' `
421     -Comment 'Probemails ohne Logging' `
422
PS C:\> New-ReceiveConnector `
-Name 'ProbeMails' `
-Enabled $true `
-ProtocolLoggingLevel 'none' `
-AuthMechanism 'Tls' `
-PermissionGroups 'AnonymousUsers' `
-RemoteIPRanges '192.168.100.18','192.168.100.250' `
-Bindings '0.0.0.0:25' `
-Server $servername `
-TransportRole 'FrontEndTransport' `
-Comment 'Probemails ohne Logging'

Identity Bindings Enabled
-----
WS-MX1\ProbeMails {0.0.0.0:25} True
  
```

Das ist das Ergebnis:

```

PS C:\> Get-ReceiveConnector | Format-Table -Property Identity,Bindings,Enabled,ProtocolLoggingLevel

Identity Bindings Enabled ProtocolLoggingLevel
-----
WS-MX2\Default WS-MX2 {0.0.0.0:2525, [::]:2525} True Verbose
WS-MX2\Client Proxy WS-MX2 {[:]:465, 0.0.0.0:465} True None
WS-MX2\Default Frontend WS-MX2 {[:]:25, 0.0.0.0:25} True Verbose
WS-MX2\Outbound Proxy Frontend WS-MX2 {[:]:717, 0.0.0.0:717} True Verbose
WS-MX2\Client Frontend WS-MX2 {[:]:587, 0.0.0.0:587} True None
WS-MX2\Mails-vom-Internet {0.0.0.0:25} True Verbose
WS-MX2\ProbeMails {0.0.0.0:25} True None
WS-MX1\Default WS-MX1 {0.0.0.0:2525, [::]:2525} True Verbose
WS-MX1\Client Proxy WS-MX1 {[:]:465, 0.0.0.0:465} True None
WS-MX1\Default Frontend WS-MX1 {[:]:25, 0.0.0.0:25} True Verbose
WS-MX1\Outbound Proxy Frontend WS-MX1 {[:]:717, 0.0.0.0:717} True Verbose
WS-MX1\Client Frontend WS-MX1 {[:]:587, 0.0.0.0:587} True None
WS-MX1\Mails-vom-Internet {0.0.0.0:25} True Verbose
WS-MX1\ProbeMails {0.0.0.0:25} True None
  
```

Jetzt trage ich den neuen Server noch in meinen Sende-Konnektor ein. Wichtig ist hier, dass BEIDE Server gelistet sind. Würde nur der neue Server angegeben werden, dann würde der bestehende Server herausfallen:

```

425 # Konfiguration des Sendekonnektors
426 Get-SendConnector | Set-SendConnector -SourceTransportServers 'ws-mx1','ws-mx2'
427 #endregion
428
PS C:\> Get-SendConnector | Set-SendConnector -SourceTransportServers 'ws-mx1','ws-mx2'
  
```

Testlauf und Produktivschaltung

Die Rolle HTS hat nun alle erforderlichen Konfigurationen erhalten. Es wird Zeit für einen Testlauf. Mein PFSense-LoadBalancer arbeitet auch eingehende Mails ab und verteilt diese auf die beiden Mailserver. Aktuell ist aber nur der WS-MX2 aktiv. Ich drehe wie beim CAS die Verbindungen um. Neue Mails kommen nun über den neuen Mailserver rein:

The screenshot shows the pfSense web interface for editing the HAProxy Backend server pool named 'SMTP'. The 'Server list' table is as follows:

Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Action
active	WS-MX1	Address+Port	192.168.100.3	25	<input type="checkbox"/>	<input type="checkbox"/>		
disabled	WS-MX2	Address+Port	192.168.100.13	25	<input type="checkbox"/>	<input type="checkbox"/>		

Natürlich habe ich einen Test vorbereitet. Die Werkzeuge von mxtoolbox können einen externen Mailversand simulieren. Die Testmail kommt über den neuen Server rein:

The screenshot shows the pfSense web interface. The 'Snort Alerts' section displays several alerts from the DMZ_120_EXTERN interface, all with a severity of 'ET INFO Windows OS'. The 'Firewall Logs' section shows a successful connection from LAN_100_SERVER to 192.168.101.1:5985.

Interface/Time	Src/Dst Address	Description
DMZ_120_EXTERN Apr 18 18:37:55	192.168.100.22:59289 52.167.64.67:80	ET INFO Windows OS Submitting USB Metadata to...
DMZ_120_EXTERN Apr 18 18:37:55	192.168.100.22:59289 52.167.64.67:80	ET USER_AGENTS Microsoft Device Metadata Retrieval...
LAN_100_SERVER Apr 18 18:37:55	192.168.100.22:59289 52.167.64.67:80	ET INFO Windows OS Submitting USB Metadata to...
LAN_100_SERVER Apr 18 18:37:55	192.168.100.22:59289 52.167.64.67:80	ET USER_AGENTS Microsoft Device Metadata Retrieval...
DMZ_120_EXTERN Apr 18 18:37:55	192.168.100.22:59288 2.16.212.108:80	ET USER_AGENTS Microsoft Device Metadata Retrieval...

Das Tool meckert zwar wegen der Transaction Time, aber da hab ich kein Problem mit:

The screenshot shows the MXToolbox SuperTool Beta7 interface. The test results for smtp:email.ws-its.de are as follows:

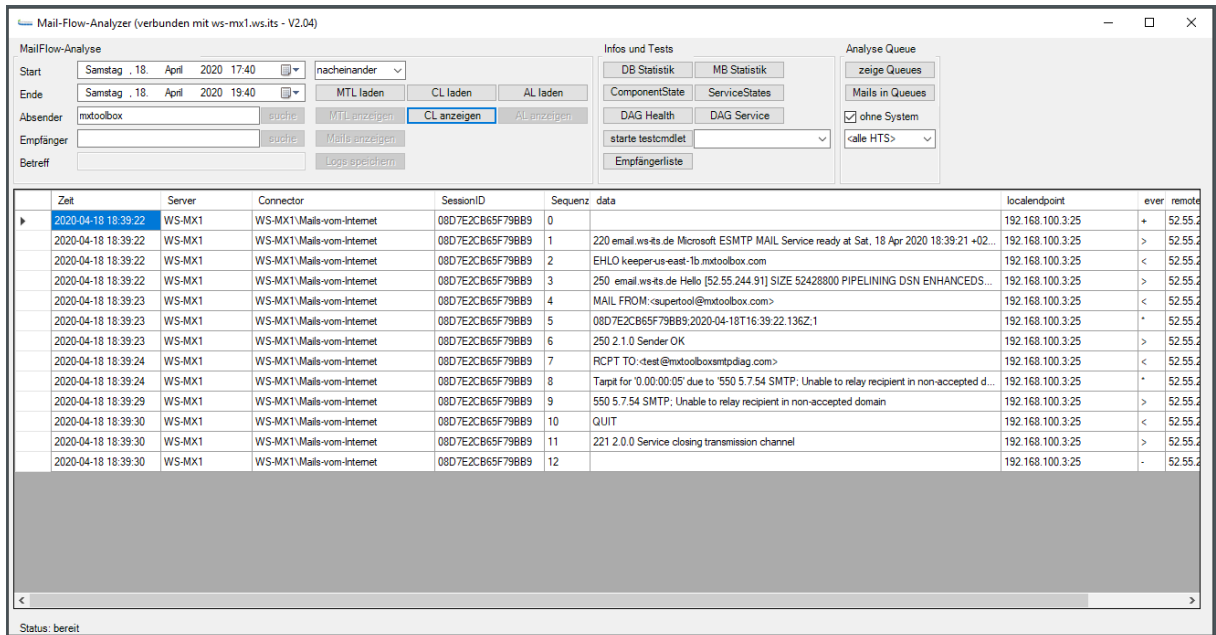
Test	Result
SMTP Transaction Time	8.141 seconds - Not good! on Transaction Time
SMTP Reverse DNS Mismatch	OK - 24.134.106.153 resolves to email.ws-its.de
SMTP Valid Hostname	OK - Reverse DNS is a valid Hostname
SMTP Banner Check	OK - Reverse DNS matches SMTP Banner
SMTP TLS	OK - Supports TLS.
SMTP Connection Time	0.844 seconds - Good on Connection time
SMTP Open Relay	OK - Not an open relay.

Session Transcript:

```

Connecting to 24.134.106.153
220 email.ws-its.de Microsoft ESMTP MAIL Service ready at Sat, 18 Apr 2020
18:39:21 +0200 [719 ms]
EHLO keeper-us-east-1b.mxtoolbox.com
250-email.ws-its.de Hello [52.55.244.91]
250-SIZE 52428800
250-PIPELINING
250-DSN
    
```

Mit meinem PowerShell-Tool Exchange-PSGUI kann ich die Logfiles des Nachrichtenflusses gezielt untersuchen. In den Connectivity-Logs finde ich den Zustellversuch von mxtoolbox:



Mail-Flow-Analyse (verbunden mit ws-mx1.ws-its - V2.04)

Start: Samstag, 18. April 2020 17:40 | nacheinander

Ende: Samstag, 18. April 2020 19:40 | MTL laden | CL laden | AL laden

Absender: mxtoolbox | suche | MTL anzeigen | CL anzeigen | AL anzeigen

Empfänger: | suche | Mail anzeigen

Betreff: | Logs speichern

Infos und Tests: DB Statistik | MB Statistik | ComponentState | ServiceStates | DAG Health | DAG Service | starte testcmdlet | Empfängerliste

Analyse Queue: zeige Queues | Mails in Queues | ohne System | <alle HTS>

Zeit	Server	Connector	SessionID	Sequenz	data	localendpoint	ever	remote
2020-04-18 18:39:22	WS-MX1	WS-MX1.Mails-vom-Internet	08D7E2C865F798B9	0		192.168.100.3:25	+	52.55.2
2020-04-18 18:39:22	WS-MX1	WS-MX1.Mails-vom-Internet	08D7E2C865F798B9	1	220 email.ws-its.de Microsoft ESMTMP MAIL Service ready at Sat, 18 Apr 2020 18:39:21 +02...	192.168.100.3:25	>	52.55.2
2020-04-18 18:39:22	WS-MX1	WS-MX1.Mails-vom-Internet	08D7E2C865F798B9	2	EHLO keeper-us-east-1b.mxtoolbox.com	192.168.100.3:25	<	52.55.2
2020-04-18 18:39:22	WS-MX1	WS-MX1.Mails-vom-Internet	08D7E2C865F798B9	3	250 email.ws-its.de Hello [52.55.244.91] SIZE 52428800 PIPELINING DSN ENHANCEDDS...	192.168.100.3:25	>	52.55.2
2020-04-18 18:39:23	WS-MX1	WS-MX1.Mails-vom-Internet	08D7E2C865F798B9	4	MAIL FROM:<supertool@mxtoolbox.com>	192.168.100.3:25	<	52.55.2
2020-04-18 18:39:23	WS-MX1	WS-MX1.Mails-vom-Internet	08D7E2C865F798B9	5	08D7E2C865F798B9:2020-04-18T16:39:22.136Z:1	192.168.100.3:25	*	52.55.2
2020-04-18 18:39:23	WS-MX1	WS-MX1.Mails-vom-Internet	08D7E2C865F798B9	6	250 2.1.0 Sender OK	192.168.100.3:25	>	52.55.2
2020-04-18 18:39:24	WS-MX1	WS-MX1.Mails-vom-Internet	08D7E2C865F798B9	7	RCPT TO:<test@mxtoolboxsmtpdiag.com>	192.168.100.3:25	<	52.55.2
2020-04-18 18:39:24	WS-MX1	WS-MX1.Mails-vom-Internet	08D7E2C865F798B9	8	Tarpit for '0.00.00.05' due to '550 5.7.54 SMTP: Unable to relay recipient in non-accepted d...	192.168.100.3:25	*	52.55.2
2020-04-18 18:39:29	WS-MX1	WS-MX1.Mails-vom-Internet	08D7E2C865F798B9	9	550 5.7.54 SMTP: Unable to relay recipient in non-accepted domain	192.168.100.3:25	>	52.55.2
2020-04-18 18:39:30	WS-MX1	WS-MX1.Mails-vom-Internet	08D7E2C865F798B9	10	QUIT	192.168.100.3:25	<	52.55.2
2020-04-18 18:39:30	WS-MX1	WS-MX1.Mails-vom-Internet	08D7E2C865F798B9	11	221 2.0.0 Service closing transmission channel	192.168.100.3:25	>	52.55.2
2020-04-18 18:39:30	WS-MX1	WS-MX1.Mails-vom-Internet	08D7E2C865F798B9	12		192.168.100.3:25	-	52.55.2

Status: bereit

Das sieht fein aus. Der HTS ist einsatzbereit. Zum Abschluss aktiviere ich in der PFSense beide Mailserver für den Mailempfang. Damit sind 2/3 Rollen hochverfügbar.

Konfiguration der Rolle MBS

Beitritt zur Datenbankverfügbarkeitsgruppe

Die letzte der 3 Rollen ist der Datenbankservice. Hier soll die Verfügbarkeit durch eine Datenbankverfügbarkeitsgruppe abgebildet werden. Diese arbeitet mit dem Windows Failover Cluster Feature und kann Datenbanken über die beteiligten Server replizieren.

Die DAG „WS-DAG“ hatte ich bereits mit dem anderen Server WS-MX2 aufgebaut. Der neue Server WS-MX1 muss diesem Cluster nur noch beitreten:

```

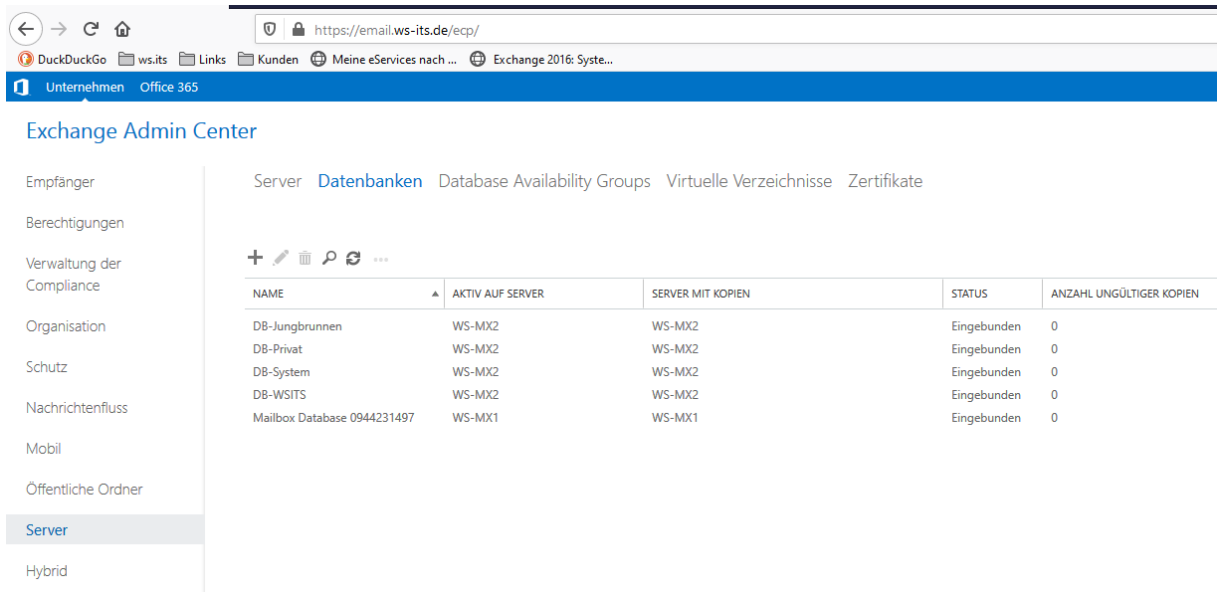
429 #region Konfiguration der Rolle MBS auf WS-MX1
430 # Konfiguration der DAG
431     Add-DatabaseAvailabilityGroupServer -MailboxServer "WS-MX1" -Identity "WS-DAG"
432
433

```

In Bearbeitung.
Der Cluster mit dem Namen 'WS-DAG' wird auf Server 'WS-MX1' gebildet.

Konfiguration der Datenbanken – Problem beim Seeding

Die Datenbanken werden aber nicht automatisch geschützt. Die Kopien müssen von Hand erstellt werden. Aktuell sollen es 4 Produktionsdatenbanken sein. Das EAC zeigt aber noch eine Default-DB auf dem neuen Server an:



NAME	AKTIV AUF SERVER	SERVER MIT KOPIEN	STATUS	ANZAHL UNGÜLTIGER KOPIEN
DB-Jungbrunnen	WS-MX2	WS-MX2	Eingebunden	0
DB-Privat	WS-MX2	WS-MX2	Eingebunden	0
DB-System	WS-MX2	WS-MX2	Eingebunden	0
DB-WSITS	WS-MX2	WS-MX2	Eingebunden	0
Mailbox Database 0944231497	WS-MX1	WS-MX1	Eingebunden	0

Die Default-DB entferne ich mit der PowerShell. Die Datenbankdatei entferne ich später:

```

433 # Entfernen der Standard-Datenbank
434 Get-MailboxDatabase -Server "WS-MX1" | Remove-MailboxDatabase -Verbose
435
PS C:\> Get-MailboxDatabase -Server "WS-MX1" | Remove-MailboxDatabase -Verbose
WARNUNG: Fehler beim Entfernen von Überwachungspostfachobjekt von Datenbank "Mailbox Database 0944231497". Ausnahme: Fehler bei Active Directory-Vorgang mit WS-DC2.ws.its. Bei diesem Fehler ist kein Wiederholungsversuch möglich. Zusätzliche Informationen: Zugriff verweigert.
Active Directory-Antwort: 00000005: SecErr: DSID-03152763, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0
.
WARNUNG: Die angegebene Datenbank wurde entfernt. Sie müssen die Datenbankdatei unter dem Pfad C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 0944231497\Mailbox Database 0944231497.edb manuell vom Computer entfernen, wenn sie vorhanden ist.
.
Angegebene Datenbank: Mailbox Database 0944231497
  
```

Jetzt erstelle ich für jede Datenbank eine lokale Kopie. Leider ist der Befehl schlecht programmiert:

```

436 # Konfiguration der Datenbank-Kopien
437 Get-MailboxDatabase |
438   ForEach-Object {
439     $DB = $_.name
440     Add-MailboxDatabaseCopy -Identity $DB -MailboxServer "WS-MX1"
441   }
442
PS C:\> Get-MailboxDatabase |
ForEach-Object {
$DB = $_.name
Add-MailboxDatabaseCopy -Identity $DB -MailboxServer "WS-MX1"
}
WARNUNG: Der Task wurde erfolgreich beendet, doch werden die aktuellen Ergebnisse erst nach Erfolgen der Replikation von Active Directory übernommen. Fehler: "Unerwarteter Fehler beim Aufruf des Microsoft Exchange Active Directory-Topologiediensts auf Server 'WS-MX2.ws.its'. Fehlerdetails: ".
Fehler beim Seedingvorgang, Fehler: Fehler beim Ausführen des Seedingvorgangs. Fehler: Fehler beim Verarbeiten einer Anforderung auf dem Server 'WS-MX2.ws.its'. Fehler: Das Sicherungsdateihandle für Datenbank "DB-System" auf Server "WS-MX2" konnte nicht geöffnet werden. HRESULT: 0x9. Fehler: Die angegebene Datenbank ist nicht vorhanden.. [Datenbank: DB-System, Server: WS-MX1.ws.its]
+ CategoryInfo          : InvalidOperation: (:) [Add-MailboxDatabaseCopy], SeedInProgressException
+ FullyQualifiedErrorId : [Server=WS-MX1,RequestId=7649a165-deb1-40f7-a077-a01c45a6c3e8,TimeStamp=17.04.2020 12:03:39] [Failur
eCategory=Cmdlet-SeedInProgressException] CA24BAB2,Microsoft.Exchange.Management.SystemConfigurationTasks.AddMailboxDatabaseCo
py
+ PSComputerName       : ws-mx1.ws.its
  
```

Hintergrund:

Der Befehl `Add-MailboxDatabaseCopy` erstellt eine Datenbankkopie auf dem angegebenen Server. Anschließend wird das sogenannte „Seeding“ gestartet, mit dem der aktuelle Datenstand importiert wird. Die beiden Aktionen werden von zwei unterschiedlichen Diensten ausgeführt. In meinem Fall hat der Replikationsdienst versucht, die Daten zu importieren, bevor der InformationService die Datenbank-Instanz erstellt hat. Da spielt die AD-Integration eine Rolle. Denn das Vorhandensein einer Datenbank wird im Active Directory hinterlegt. Das hätte man besser konfigurieren können.

In der Praxis bietet es sich daher an, das Seeding manuell zu einem späteren Zeitpunkt zu starten. Dafür wird der SwitchParameter `-SeedingPostponed` verwendet:

```

Computer: WS-MX1.ws.its
[PS] C:\>get-help -name Add-MailboxDatabaseCopy -Parameter seedingp*

-SeedlingPostponed <SwitchParameter>
Der Parameter SeedlingPostponed gibt an, dass der Task kein Seeding der Datenbankkopie vornimmt. Sie müssen das
Seeding der Datenbankkopie dann explizit durchführen.

Erforderlich?           false
Position?               Named
Standardwert
Pipelineeingaben akzeptieren?False
Platzhalterzeichen akzeptieren?false

[PS] C:\>
    
```

Das Seeding kann dann nach einigen Minuten mit Update-MailboxDatabaseCopy gestartet werden.

In meinem Fall sind die 4 Kopien erstellt worden. Nun warte ich einige Minuten:

The screenshot shows the Exchange Admin Center interface. On the left, the navigation pane is open to 'Server'. The main area displays a table of database replication information:

NAME	AKTIV AUF SERVER	SERVER MIT KOPIIEN	STATUS	ANZAHL UNGÜLTIGER KOPIIEN
DB-Jungbrunnen	WS-MX2	WS-MX2,WS-MX1	Eingebunden	1
DB-Privat	WS-MX2	WS-MX2,WS-MX1	Eingebunden	1
DB-System	WS-MX2	WS-MX2,WS-MX1	Eingebunden	1
DB-WSITS	WS-MX2	WS-MX2,WS-MX1	Eingebunden	1

On the right side, there is a detailed view for 'DB-Jungbrunnen', showing it is 'Aktiv Eingebunden' with a 'Länge der Kopierwarteschlange: 0' and 'Inhaltsindexzustand: NichtAnwendbar'.

Nach der Wartezeit versuche ich das Update-MailboxDatabaseCopy für alle Kopien zu starten:

The screenshot shows a PowerShell session with the following command:

```

442 Get-MailboxDatabase
443 ForEach-Object {
444     $DB = $_.name
445     Update-MailboxDatabaseCopy -Identity "$DB\WS-MX1"
446 }
447 #endregion
448
449
    
```

A confirmation dialog box appears with the text: 'Möchten Sie diese Aktion wirklich ausführen? Seeding der Datenbankkopie "DB-System\WS-MX1" wird durchgeführt.' The buttons are 'Ja', 'Ja, alle', 'Nein', and 'Nein, keine'.

Leider kommen hier auch nur Fehlermeldungen als Ergebnis:

The screenshot shows the PowerShell session with error output:

```

PS C:\> Get-MailboxDatabase |
ForEach-Object {
    $DB = $_.name
    Update-MailboxDatabaseCopy -Identity "$DB\WS-MX1"
}

Fehler beim Seedingvorgang. Fehler: Fehler beim Ausführen des Seedingvorgangs. Fehler: Fehler beim Verarbeiten einer Anforderung
auf dem Server 'WS-MX2.ws.its'. Fehler: Das Sicherungsdateihandle für Datenbank "DB-System" auf Server "WS-MX2" konnte nicht
geöffnet werden. Hresult: 0x9. Fehler: Die angegebene Datenbank ist nicht vorhanden.. [Datenbank: DB-System, Server: WS-MX1.ws.its]
+ CategoryInfo          : InvalidOperation: (:) [Update-MailboxDatabaseCopy], SeedInProgressException
+ FullyQualifiedErrorId : [Server=WS-MX1,RequestId=1bf62d39-8ae1-4cb9-b783-a1580492094d,TimeStamp=17.04.2020 12:07:13] [Failur
eCategory=Cmldlet-SeedInProgressException] 35C269D0,Microsoft.Exchange.Management.SystemConfigurationTasks.UpdateDatabaseCopy
+ PSComputerName       : ws-mx1.ws.its
    
```

A confirmation dialog box is also visible, with text: 'Die Postfachdatenbankkopie "DB-System\WS-MX1" konnte nicht vom Server aktualisiert werden. Möchten Sie die Updatesanforderung jetzt bereinigen? Das Seeding kann nicht für die gleiche Datenbankkopie angefordert werden, bis die fehlerhafte Anforderung vom Server bereinigt wurde. Dies sollte innerhalb von 15 Minuten automatisch erfolgen.'

Ich versuche es man mit dem cmdlet Update-MailboxDatabaseCopy. Leider auch ohne Erfolg:

```

448
449
450 Get-MailboxDatabase |
451   ForEach-Object {
452     $DB = $_.name
453     Resume-MailboxDatabaseCopy -Identity "$DB\WS-MX1"
454   }
455 #endregion

```

```

PS C:\> Get-MailboxDatabase |
        ForEach-Object {
            $DB = $_.name
            Resume-MailboxDatabaseCopy -Identity "$DB\WS-MX1"
        }

```

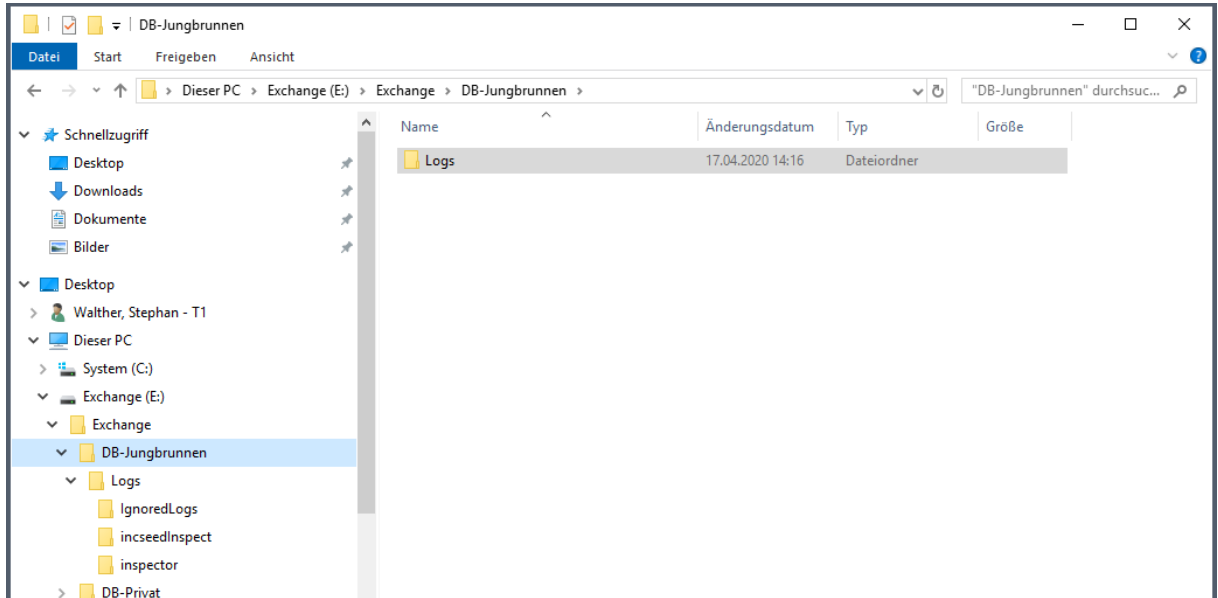
Die grafische Oberfläche gibt mir bei einem weiteren Versuch eine sprechendere Fehlermeldung aus. Aber auch die angegebene Option bringt nichts:

Ich starte den neuen Server mal durch und versuche es erneut. Jetzt kann ich einen Server auswählen. Die angezeigte Aktion entspricht dem cmdlet Update-MailboxDatabaseCopy:

Die Fehlermeldung ist aber wieder die gleiche:

Fehler beim Seedingvorgang. Fehler: Fehler beim Ausführen des Seedingvorgangs. Fehler: Fehler beim Verarbeiten einer Anforderung auf dem Server 'WS-MX2.ws.its'. Fehler: Das Sicherungsdateihandle für Datenbank "DB-Jungbrunnen" auf Server "WS-MX2" konnte nicht geöffnet werden. Hresult: 0x9. Fehler: Die angegebene Datenbank ist nicht vorhanden.. [Datenbank: DB-Jungbrunnen, Server: WS-MX1.ws.its]

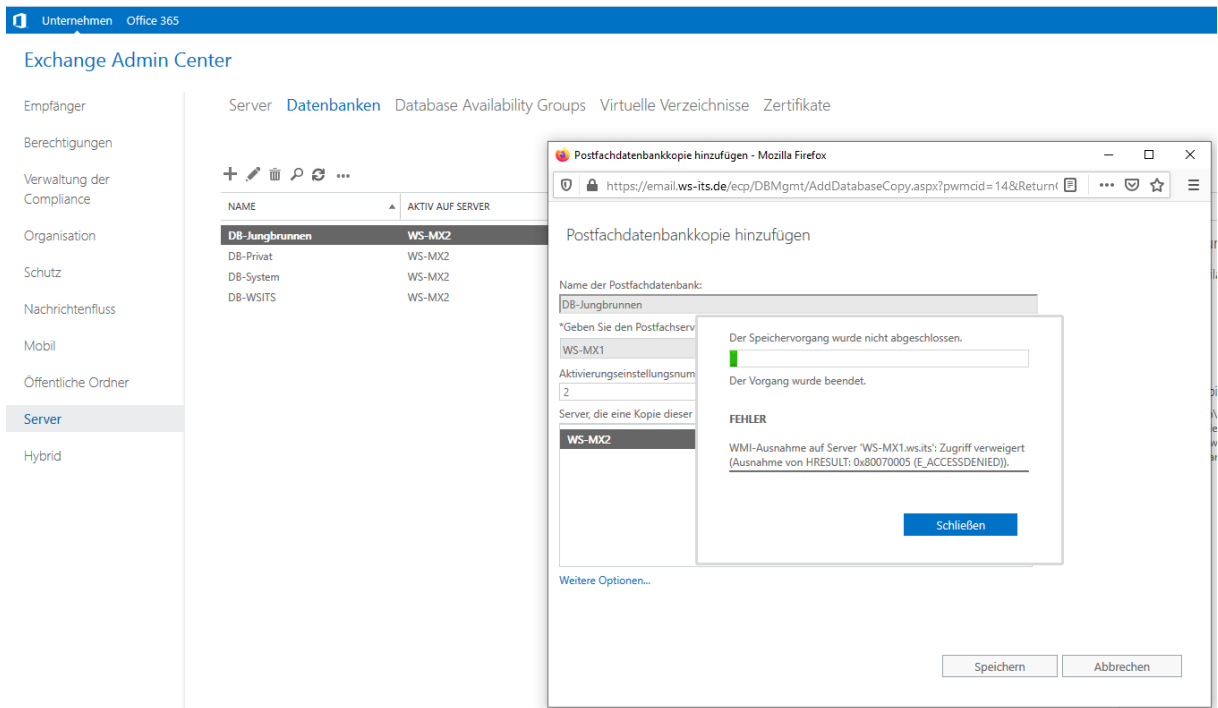
Und es stimmt: Die Datenbank fehlt. Aber genau darum geht es ja beim Seeding:



Auch mit den anderen Parametern bekomme ich keine Erfolgsmeldung:



Also rolle ich einen Schritt zurück und entferne die nicht existenten Kopien vom Server WS-MX1. Dann erstelle ich eine neue Kopie. Doch auch so bekomme ich nur eine Fehlermeldung:

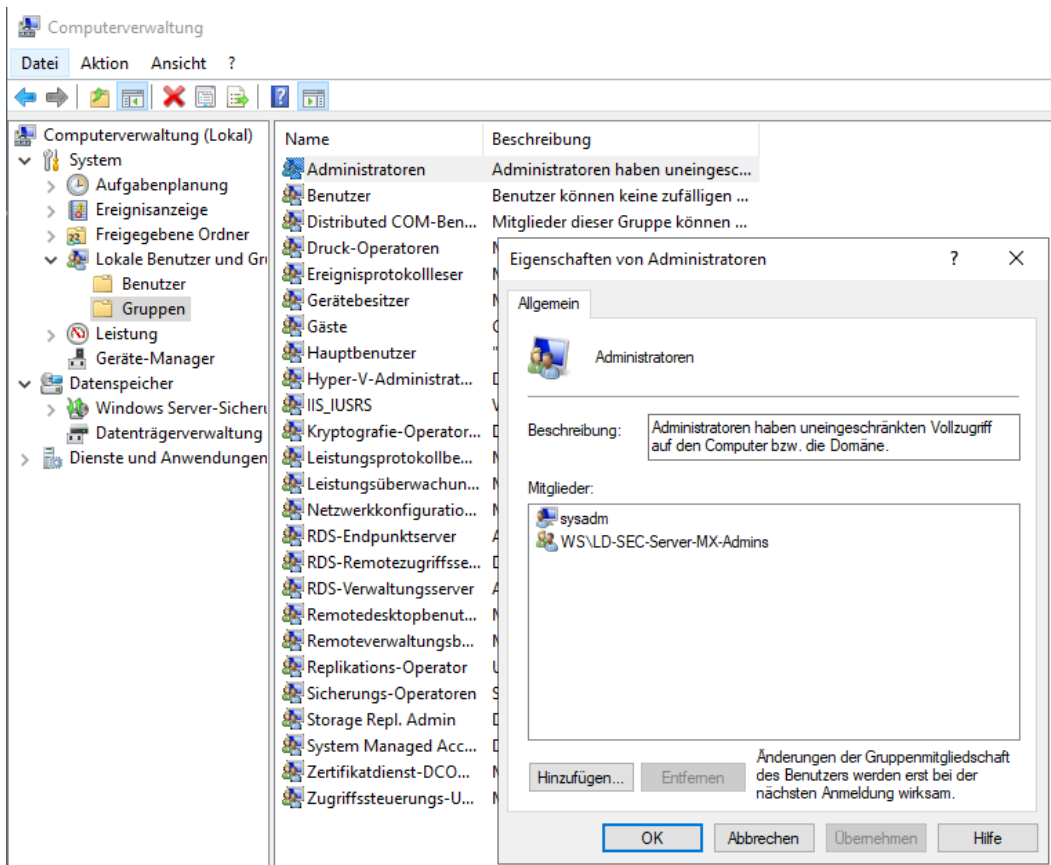


Access Denied? Ich habe doch die erforderlichen Rechte? Die PowerShell meldet das gleiche:

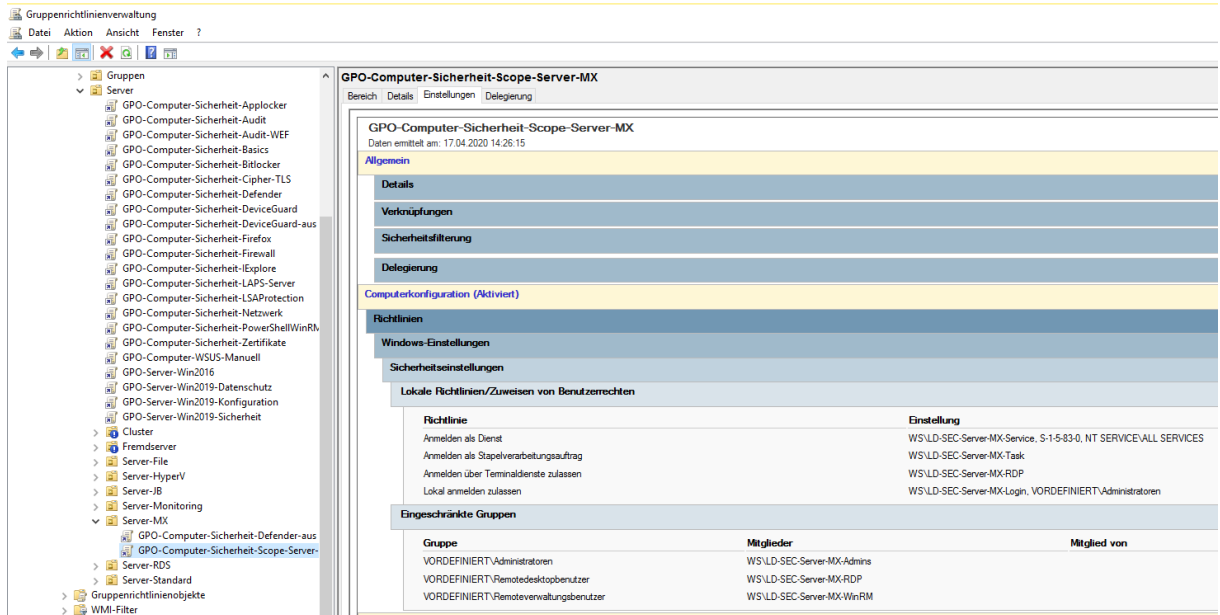
```

Computer: WS-MX2.ws.its
[PS] C:\>Add-MailboxDatabaseCopy -Identity DB-System -MailboxServer "WS-MX1"
WMI-Ausnahme auf Server 'WS-MX1.ws.its': Zugriff verweigert (Ausnahme von HRESULT: 0x80070005 (E_ACCESSDENIED)).
+ CategoryInfo          : NotSpecified: (:) [Add-MailboxDatabaseCopy], WmiException
+ FullyQualifiedErrorId : [Server=WS-MX2,RequestId=0b0614db-aa18-411b-b5f2-c6ff7a70a904,TimeStamp=17.04.2020 12:25:12] [FailureCategory=Cmdlet-WmiException] D23AC42F,Microsoft.Exchange.Management.SystemConfigurationTasks.AddMailboxDatabaseCopy
+ PSComputerName        : ws-mx2.ws.its
[PS] C:\>
  
```

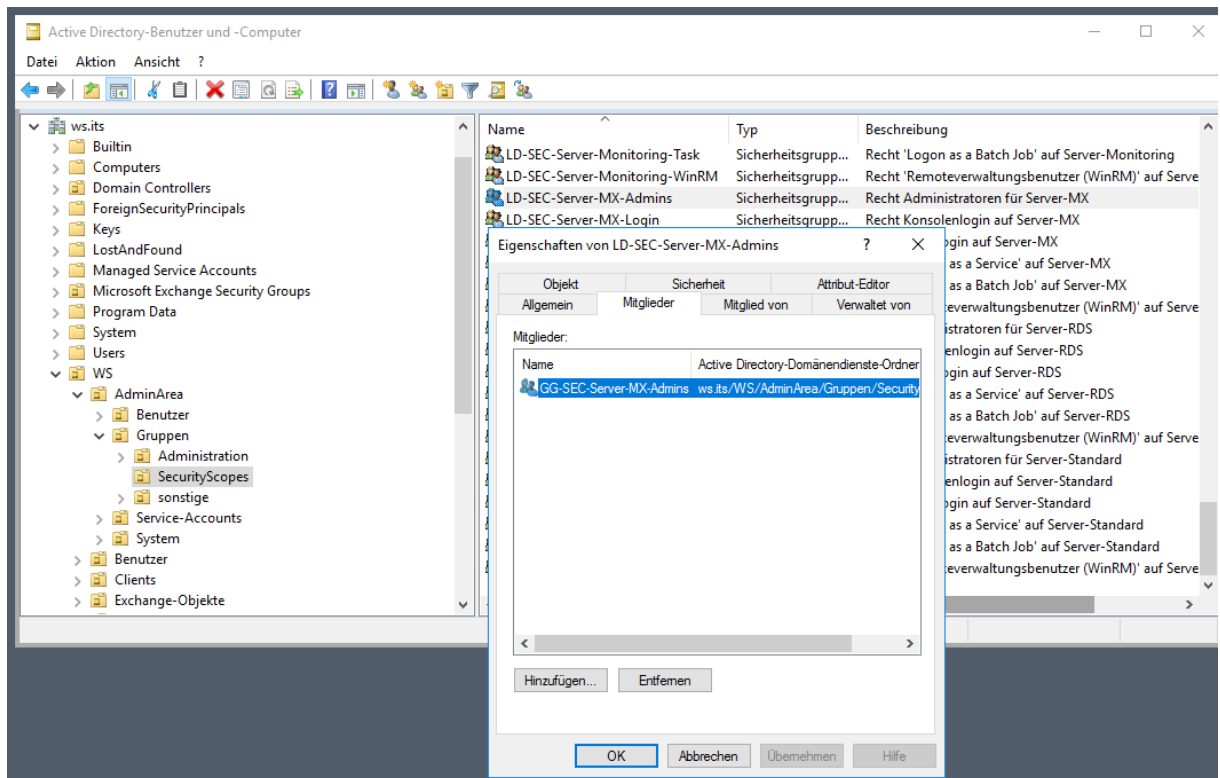
Ich habe durch Gruppenrichtlinien ein Tier-Management für meine Administration aufgebaut. Vielleicht ist ja hier etwas durcheinandergeraten? Die Mitgliedschaft der lokalen Administratoren zeigt nur den lokalen Admin und eine AD-Gruppe. Die Domain Admins hab ich hier explizit verbannt...



Die Einstellung kommt wie gewünscht durch meine GPO zustande:

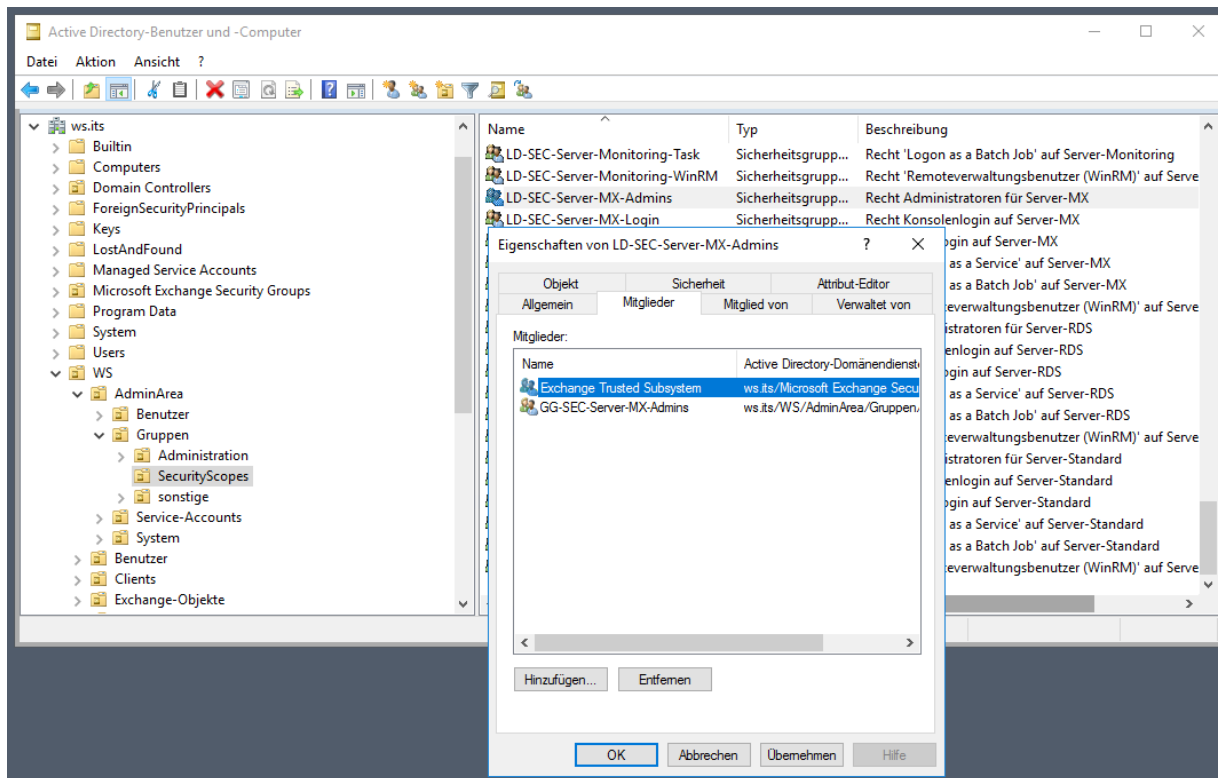


in die LocalDomain-Gruppe „LD-SEC-Server-MX-Admins“ ist eine globale Gruppe verschachtelt:



Und das ist mein Problem: Die Exchange Server können sich untereinander administrieren. Dafür existiert eine Active Directory Gruppe „Exchange Trusted Subsystems“. Diese wird beim Setup automatisch in die lokale Gruppe „Administratoren“ aufgenommen. Meine GPO arbeitet aber im Modus „Ersetzen“. Damit verlieren die Exchange Server ihre Rechte!!!

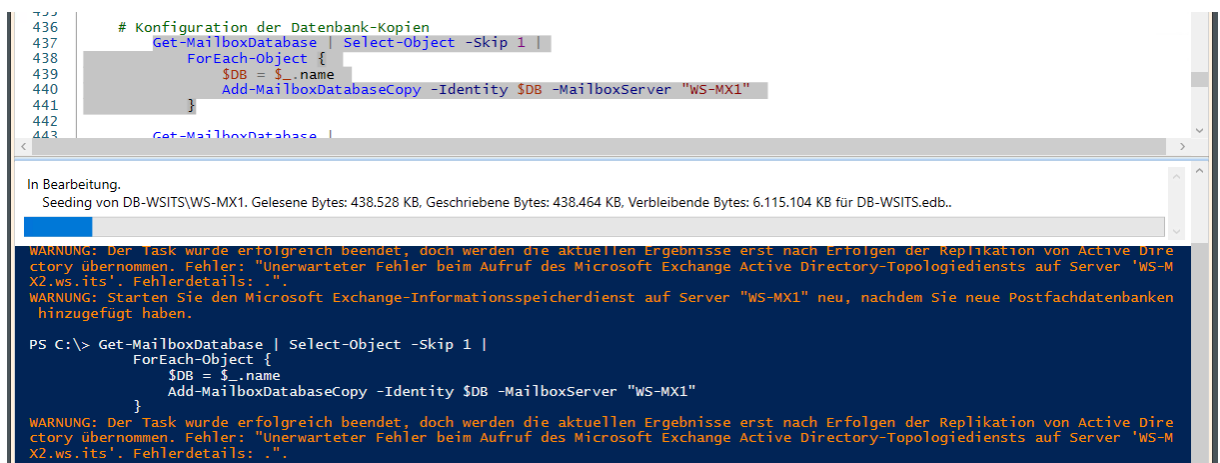
Also nehme ich die Gruppe durch eine Verschachtelung wieder auf: „Exchange Trusted Subsystems“ → GG-SEC-Server-MX-Admins → LD-SEC-Server-MX-Admins → .\Administratoren



Die Übernahme braucht wahrscheinlich einen Neustart. Der ist schnell durchgeführt.

Konfigurieren der Datenbanken – mit Erfolg

Dann probiere ich es noch einmal. Und kaum macht man es richtig, schon funktioniert es:



Meine Datenbanken sind nicht sehr groß, daher dauert das Erstellen der 4 Kopien nicht sehr lange:

Unternehmen Office 365

Exchange Admin Center

Empfänger
Berechtigungen
Verwaltung der Compliance
Organisation
Schutz
Nachrichtenfluss
Mobil
Öffentliche Ordner
Server
Hybrid

Server **Datenbanken** Database Availability Groups Virtuelle Verzeichnisse Zertifikate

NAME	AKTIV AUF SERVER	SERVER MIT KOPIEN	STATUS	ANZAHL UNGÜLTIGER KOPIEN
DB-Jungbrunnen	WS-MX2	WS-MX2,WS-MX1	Eingebunden	0
DB-Privat	WS-MX2	WS-MX2,WS-MX1	Eingebunden	0
DB-System	WS-MX2	WS-MX2,WS-MX1	Eingebunden	0
DB-WSITS	WS-MX2	WS-MX2,WS-MX1	Eingebunden	0

DB-System
Database Availability Group: WS-DAG
Server
WS-MX2
WS-MX1
Datenbankkopien
DB-SystemWS-MX2
Aktiv Eingebunden
Länge der Kopierwarteschlange: 0
Inhaltsindexzustand: NichtAnwendbar
[Details anzeigen](#)
DB-SystemWS-MX1
Passiv Fehlerfrei
Länge der Kopierwarteschlange: 0
Inhaltsindexzustand: NichtAnwendbar
[Anhalten](#) | [Aktivieren](#) | [Entfernen](#)
[Details anzeigen](#)

Jetzt Sorge ich noch für eine Lastverteilung, indem ich 2 der 4 Datenbanken primär auf dem neuen Server ausführen lasse:

```

443 # Lastverteilung
444 | Set-MailboxDatabaseCopy -Identity 'DB-WSITS\WS-MX1' -ActivationPreference 1
445 | Set-MailboxDatabaseCopy -Identity 'DB-System\WS-MX1' -ActivationPreference 1
446 #endregion
447
PS C:\> Set-MailboxDatabaseCopy -Identity 'DB-WSITS\WS-MX1' -ActivationPreference 1
PS C:\> Set-MailboxDatabaseCopy -Identity 'DB-System\WS-MX1' -ActivationPreference 1

```

Die Bereitstellung wird nach einer Weile automatisch geschwenkt.

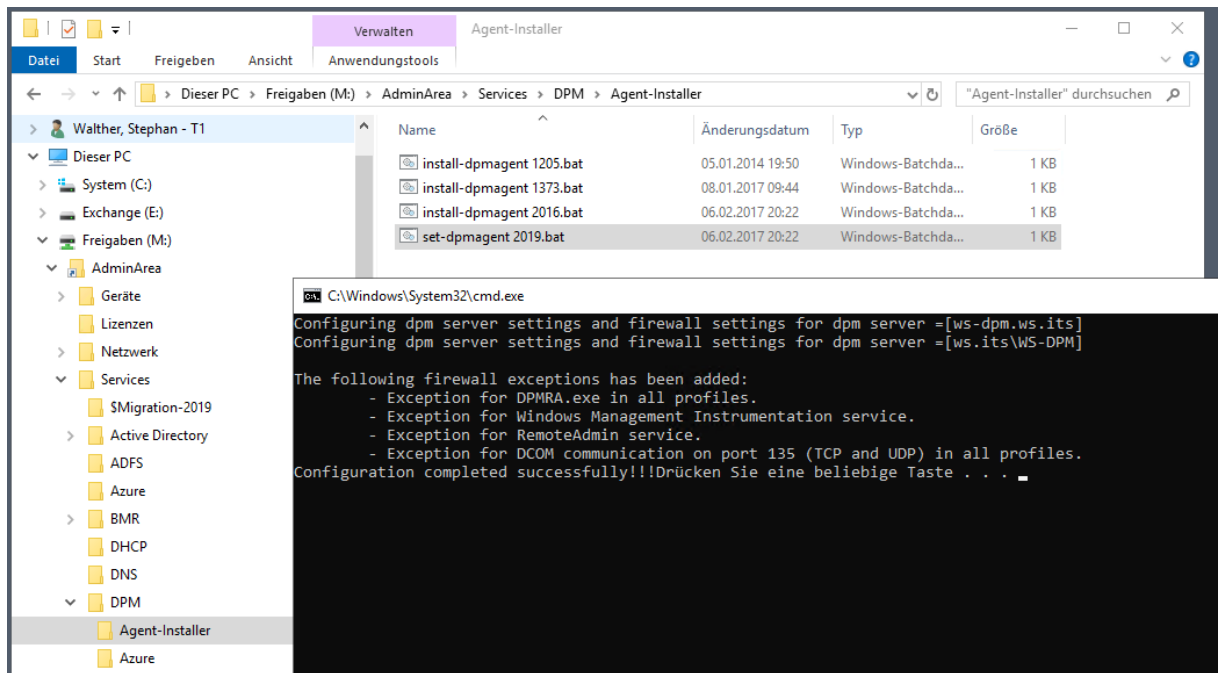
Konfiguration der Datensicherung mit dem DPM

Integration des neuen Servers im DPM – Problem: keine Sicherung

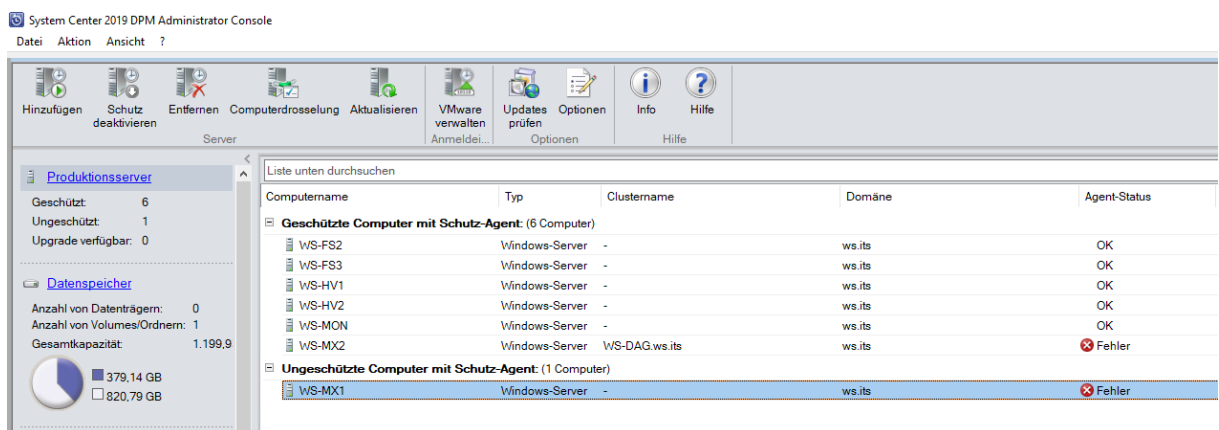
Jetzt kommt die Datensicherung der Datenbanken dran. Diese werden ja bereits von meinem Data Protection Manager 2019 auf dem anderen Mailserver WS-MX2 gesichert. Daher sollten hier nur noch Feinheiten notwendig sein.

Der neue Server benötigt den DPM-Agent installiert. Das nehme ich lokal vor. Das Setup liegt in einer Freigabe des DPM:

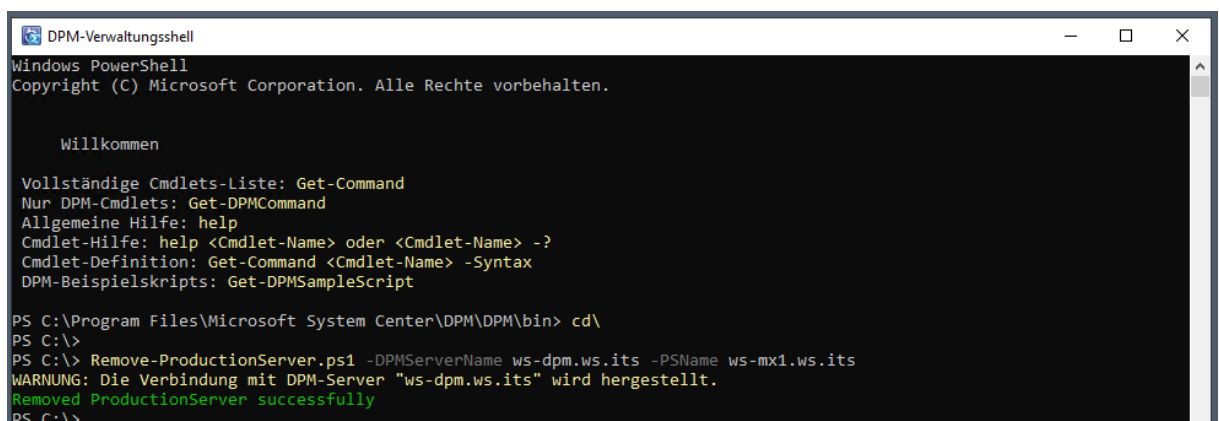
Auch die Konfiguration des Agents starte ich auf dem Exchange Server mit einer Batch-Datei:



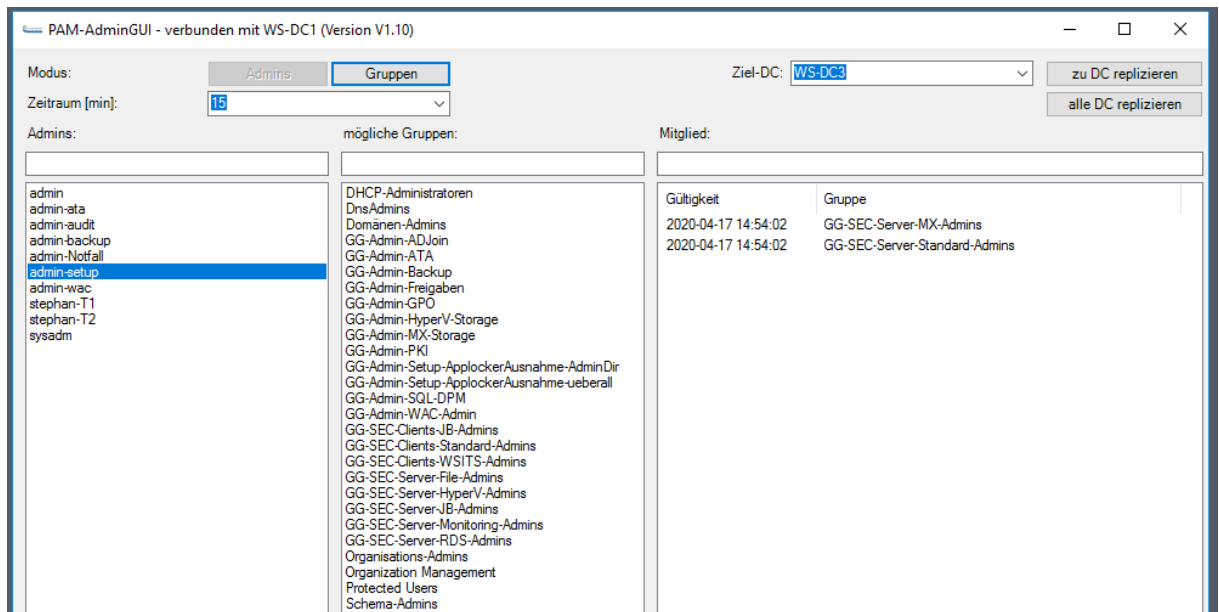
In der DPM-Konsole ist der alte Server noch gelistet:



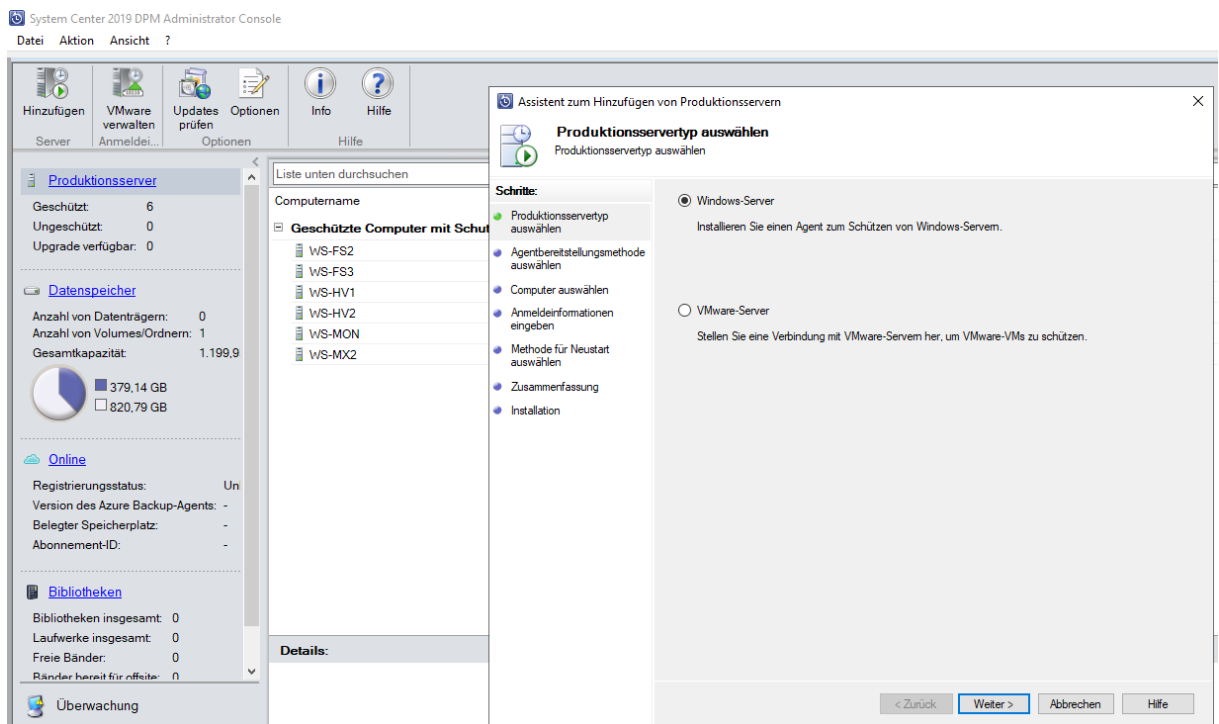
Den Eintrag kann man in der GUI nicht entfernen. Daher nehme ich den Powershell-Befehl:



Für die Verbindung zwischen Agent und DPM ist ein NTLM-fähiger Account erforderlich. Den richte ich mir fix mit meinem PAM-Tool her:



Und dann kann ich den Agent im DPM einbinden:



System Center 2019 DPM Administrator Console

Datei Aktion Ansicht ?

The screenshot shows the 'Assistent zum Hinzufügen von Produktionsservern' (Assistant for adding production servers) dialog box. The 'Agentbereitstellungsmethode auswählen' (Select agent installation method) step is active. The left pane shows a list of protected computers: WS-FS2, WS-FS3, WS-HV1, WS-HV2, WS-MON, and WS-MX2. The right pane provides instructions for three options: 'Agents installieren' (not recommended), 'Agents verbinden' (recommended), and 'Computer in einer vertrauenswürdigen Domäne' (recommended for protected computers). The 'Weiter' button is highlighted.

System Center 2019 DPM Administrator Console

Datei Aktion Ansicht ?

The screenshot shows the 'Assistent zum Hinzufügen von Produktionsservern' dialog box at the 'Computer auswählen' (Select computer) step. It prompts the user to select a computer from a list of protected computers. A table lists the available computers and their domains:

Computer	Domäne
WS-CL8	ws.its
WS-CM	ws.its
WS-DC1	ws.its
WS-DC2	ws.its
WS-DC3	ws.its
WS-FS1	ws.its
WS-HV3	ws.its
WS-MX1	ws.its
WS-NPS1	ws.its
WS-RDS1	ws.its
WS-RDS2	ws.its
WS-WAC	ws.its

The 'WS-MX1' computer is selected. The 'Hinzufügen >' button is highlighted. The 'Erweitert...' button is also visible at the bottom right.

System Center 2019 DPM Administrator Console

The screenshot shows the 'Assistent zum Hinzufügen von Produktionsservern' wizard in the 'Anmeldeinformationen eingeben' step. The main console window displays a list of servers under 'Produktionsserver', including WS-FS2, WS-FS3, WS-HV1, WS-HV2, WS-MON, and WS-MX2. The wizard's progress bar shows the following steps: 'Produktionsservertyp auswählen', 'Agentbereitstellungsmethode auswählen', 'Computer auswählen', 'Anmeldeinformationen eingeben' (current step), 'Methode für Neustart auswählen', 'Zusammenfassung', and 'Installation'. The 'Anmeldeinformationen eingeben' step includes fields for 'Benutzername' (admin-setup), 'Kennwort' (masked), and 'Domäne' (ws.its).

System Center 2019 DPM Administrator Console

The screenshot shows the 'Assistent zum Hinzufügen von Produktionsservern' wizard in the 'Installation' step. The main console window shows that WS-MX1 is now listed under 'Ungeschützte Computer mit Schutz'. The wizard's progress bar shows the following steps: 'Produktionsservertyp auswählen', 'Agentbereitstellungsmethode auswählen', 'Computer auswählen', 'Anmeldeinformationen eingeben', 'Zusammenfassung', and 'Installation' (current step). The 'Installation' step includes a table of tasks:

Aufgabe	Ergebnisse
Geschützten Computer WS-MX1.ws.its verbinden	Erfolgreich

Das war problemlos.

Jetzt müssen die Datenbanken des Server WS-MX1 nur noch in die Schutzgruppe aufgenommen werden. Diese listet aber schon Probleme...

System Center 2019 DPM Administrator Console

Datei Aktion Ansicht ?

Neu Ändern Onlineschutz hinzufügen Löschen Optimieren Konsistenzprüfung Datenträger Online Band Self-Service-Wiederherstellung Bandkatalogbeibehaltung Status der Wiederherstellungspunkte Updates prüfen Optionen

Integrität der Datenquelle

- Kritisch (0)
- OK (9)
- Warnung (4)

Alle Schutzgruppen

- Schutz-Exchange
- Schutz-Fileserver
- Schutz-HyperV
- Schutz-JB
- Schutz-Monitoring
- Inaktiver Schutz

Gruppieren nach: Schutzgruppe Computer

Liste unten durchsuchen

Schutzgruppenmitglied	Typ	Schutzstatus
Computer: ws-mx2.ws.it		
Exchange-Postfachdatenbank		Der Agent ist nicht erreichbar.
Exchange-Postfachdatenbank		Der Agent ist nicht erreichbar.
Exchange-Postfachdatenbank		Der Agent ist nicht erreichbar.
Exchange-Postfachdatenbank		Der Agent ist nicht erreichbar.

Schutzgruppe ändern...

- Onlineschutz hinzufügen...
- Schutz der Gruppe beenden...
- Leistung optimieren...
- Clients zur Schutzgruppe hinzufügen...
- Bandliste anzeigen
- Konsistenzprüfung ausführen...
- Datenträgerzuordnung ändern...
- Datenträgersicherungen fortsetzen...
- Azure-Sicherungen fortsetzen...
- Bandsicherungen fortsetzen...
- Status der Wiederherstellungspunkte...
- Alle Gruppen erweitern
- Alle Gruppen reduzieren

Schutzgruppe: Schutz-Exchange

Computer: ws-mx2.ws.it

Computer: ws-fs2.ws.it

Computer: ws-hv1.ws.it

Computer: ws-hv2.ws.it

Computer: ws-fs3.ws.it

Schutzgruppe: Schutz-Monitoring (Mitglieder insgesamt: 1)

System Center 2019 DPM Administrator Console

Datei Aktion Ansicht ?

Gruppe ändern - Schutz-Exchange

Gruppenmitglieder auswählen

Wählen Sie die Daten aus, die geschützt werden sollen.

Schritte:

- 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	Ausgewählte Mitglieder
ws-its	Computer
WS-DAG	ws-mx2.ws.its
DB-Jungbrunnen	ws-mx2.ws.its
DB-Privat	ws-mx2.ws.its
DB-System	ws-mx2.ws.its
DB-WSITS	ws-mx2.ws.its
WS-DPM	ws-mx1.ws.its
WS-FS2	ws-mx1.ws.its
WS-FS3	ws-mx1.ws.its
WS-HV1	ws-mx1.ws.its
WS-HV2	ws-mx1.ws.its
WS-MON	ws-mx1.ws.its
WS-MX1	ws-mx1.ws.its
WS-MX2	ws-mx1.ws.its

Datenquellen aktualisieren

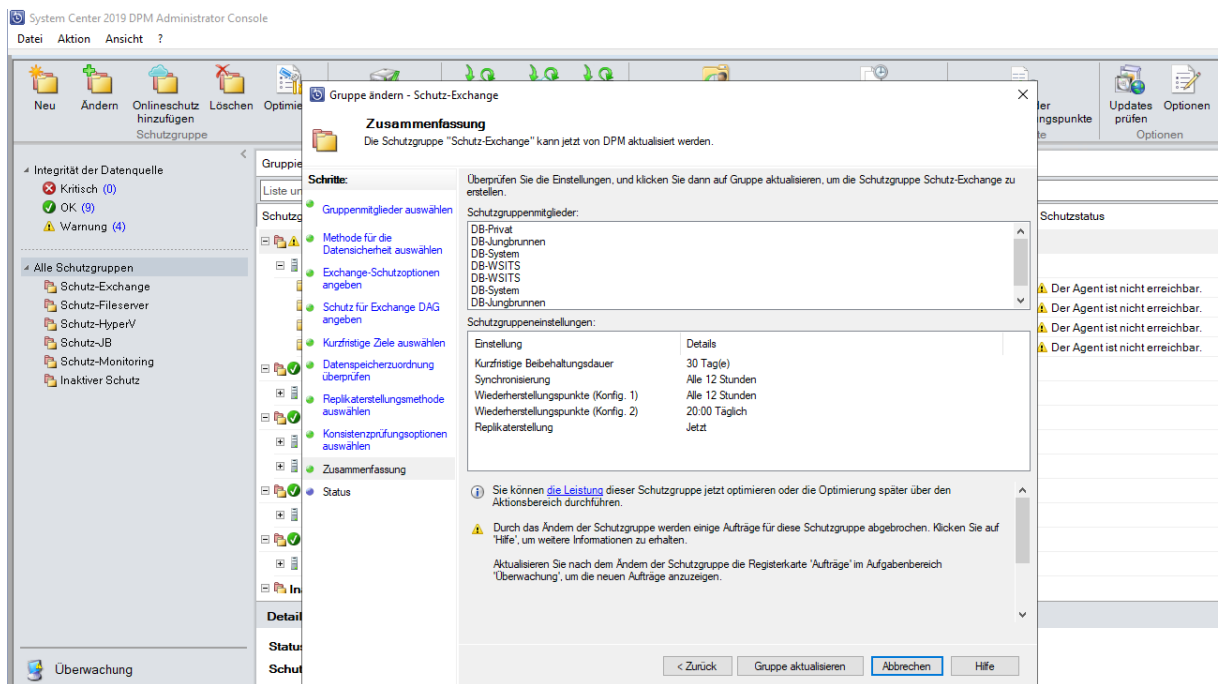
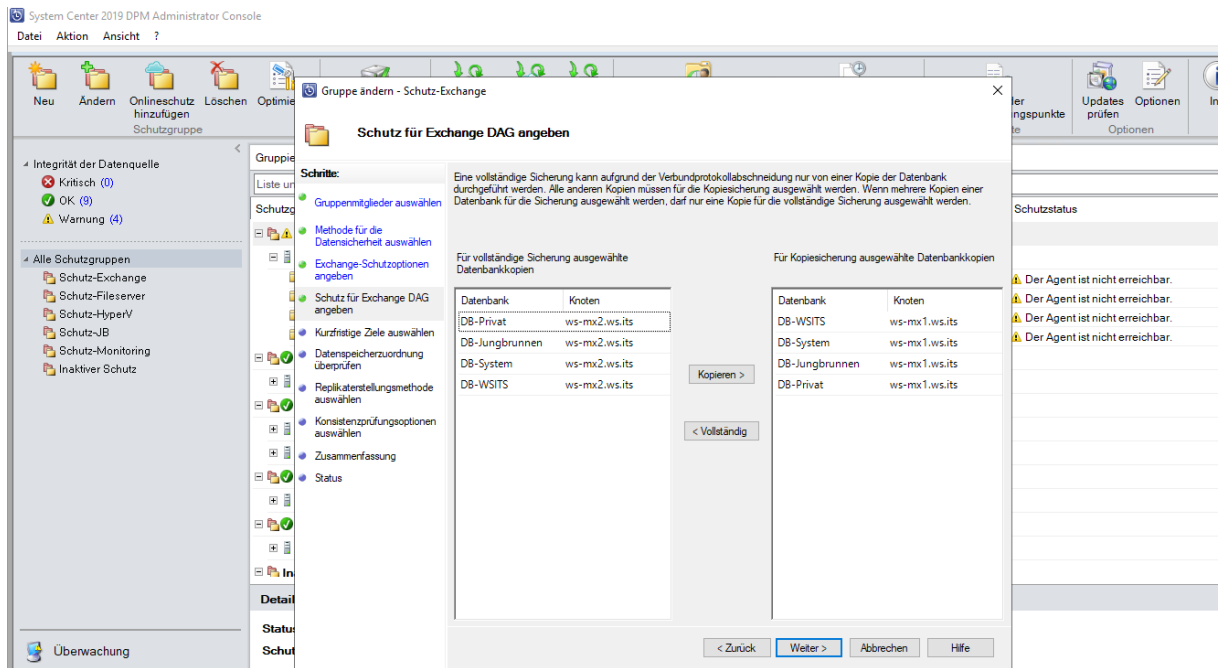
Klicken Sie auf "Aktualisieren", um den Cache zu aktualisieren.

Ausgeschlossene Ordner: 0 Anzeigen

Ausgeschlossene Dateien: 0 Dateien ausschließen...

Erntern

< Zurück Weiter > Abbrechen Hilfe



Die Datenbanken sind eingetragen. Aber die Sicherung läuft nicht mehr an. Der DPM hat sich komplett verkeilt... Es wird Zeit für ein TroubleShooting.

Problem: Clusterfehler

Bevor ich mit meinen Produktionsdatenbanken weiter experimentiere, erstelle ich mir lieber eine Test-Datenbank in meiner DAG:

Enterprise Office 365

Exchange admin center

recipients permissions compliance management organization protection mail flow mobile public folders **servers** hybrid

servers **databases** database availability groups virtual directories certificates

NAME	ACTIVE ON SERVER	SERVERS WITH COPIES	STATUS	BAD COPY COUNT
DB-Jungbrunnen	WS-MX2	WS-MX2,WS-MX1	Mounted	0
DB-Privat	WS-MX2	WS-MX2,WS-MX1	Mounted	0
DB-System	WS-MX2	WS-MX1,WS-MX2	Mounted	0
DB-WSITS	WS-MX2	WS-MX1,WS-MX2	Mounted	0
Test	WS-MX1	WS-MX1,WS-MX2	Mounted	0

Test
Database availability group: WS-DAG
Servers
WS-MX1
WS-MX2
Database copies
Test\WS-MX1
Active Mounted
Copy queue length: 0
Content index state: NotApplicable
[View details](#)
Test\WS-MX2
Passive Healthy
Copy queue length: 0
Content index state: NotApplicable
[Suspend](#) | [Activate](#) | [Remove](#)
[View details](#)

Die Datenbank lässt sich aber nicht schwenken...

Enterprise Office 365

Exchange admin center

recipients permissions compliance management organization protection mail flow mobile public folders **servers** hybrid

servers **databases** database availability groups virtual directories certificates

NAME	ACTIVE ON SERVER	SERVERS WITH COPIES	STATUS	BAD COPY COUNT
DB-Jungbrunnen	WS-MX2	WS-MX2,WS-MX1	Mounted	0
DB-Privat	WS-MX2	WS-MX2,WS-MX1	Mounted	0
DB-System	WS-MX2	WS-MX1,WS-MX2	Mounted	0
DB-WSITS	WS-MX2	WS-MX1,WS-MX2	Mounted	0
Test	WS-MX1	WS-MX1,WS-MX2	Mounted	0

Saving isn't finished.

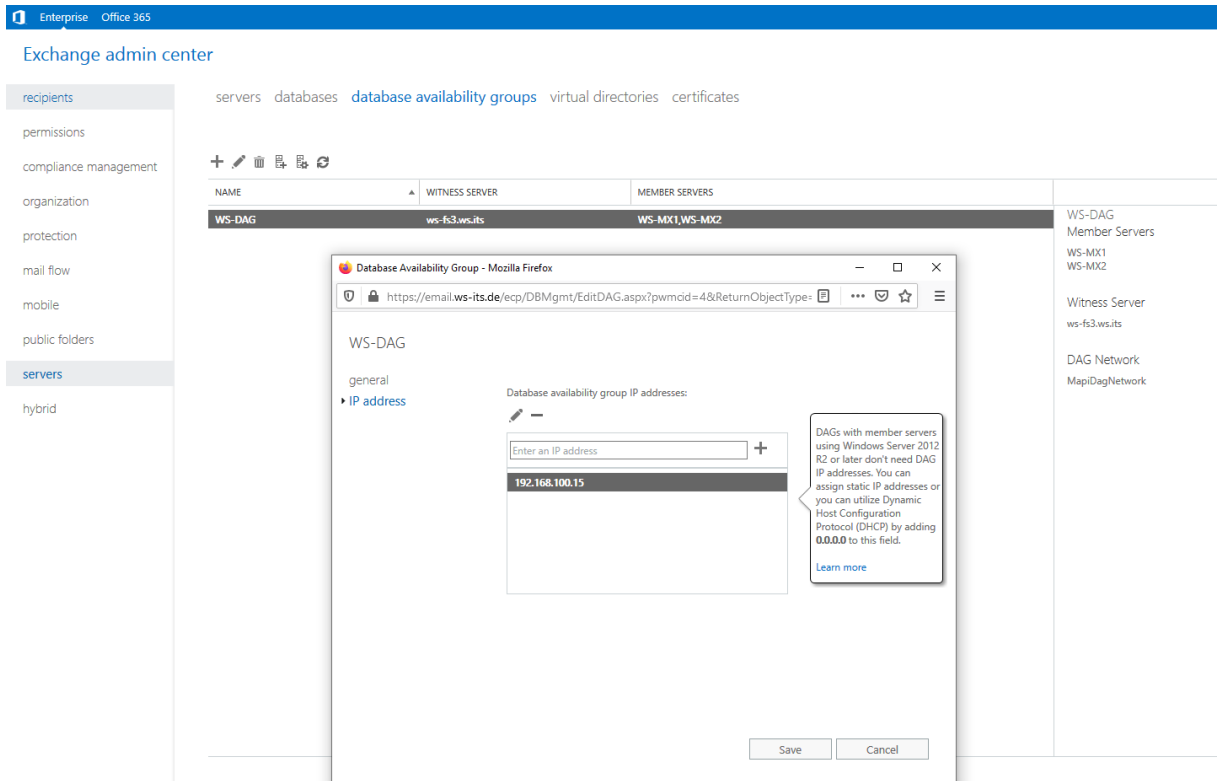
The operation has been stopped.

Datenbankkopie für eine mögliche Aktivierung zu überprüfen, ist ein Fehler aufgetreten: WS-MX2: Server 'WS-MX2.ws.its' ist gemäß Windows-Failoverclusterdienst nicht betriebsbereit. (Database: Test, Server: WS-MX1.ws.its)

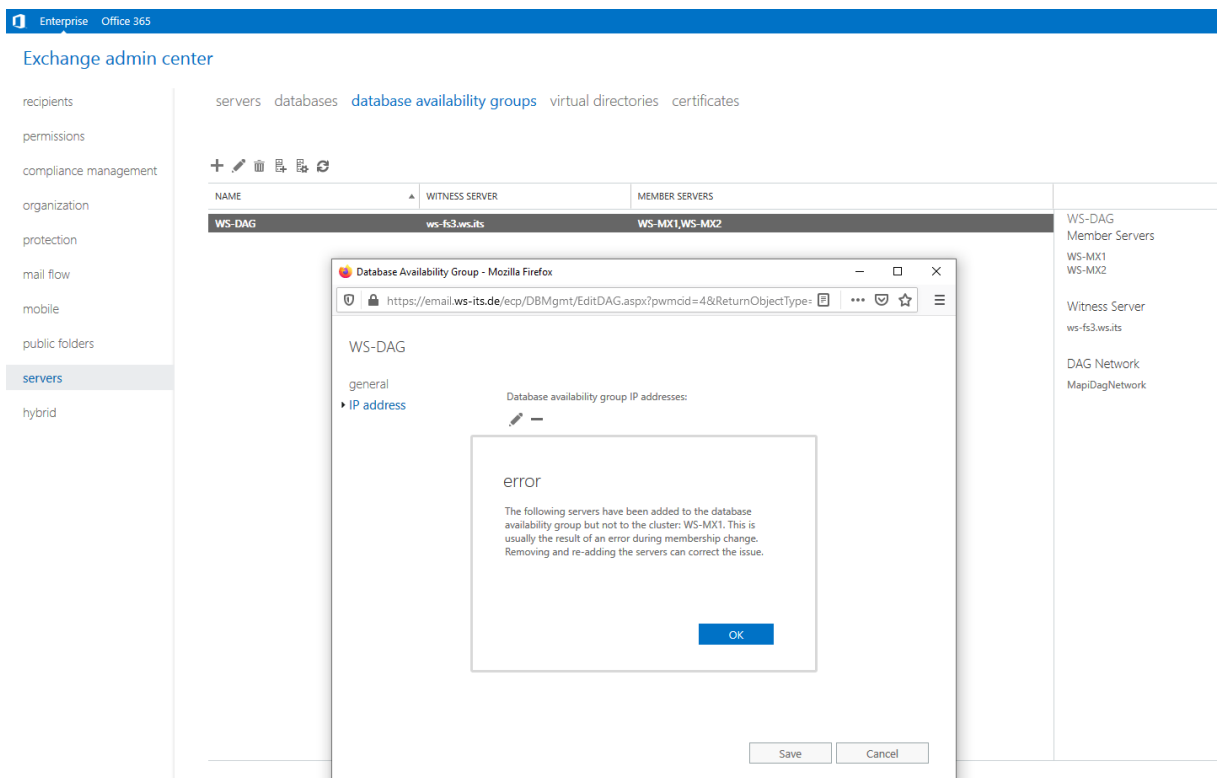
[Close](#)

Test
Database availability group: WS-DAG
Servers
WS-MX1
WS-MX2
Database copies
Test\WS-MX1
Active Mounted
Copy queue length: 0
Content index state: NotApplicable
[View details](#)
Test\WS-MX2
Passive Healthy
Copy queue length: 0
Content index state: NotApplicable
[Suspend](#) | [Activate](#) | [Remove](#)
[View details](#)

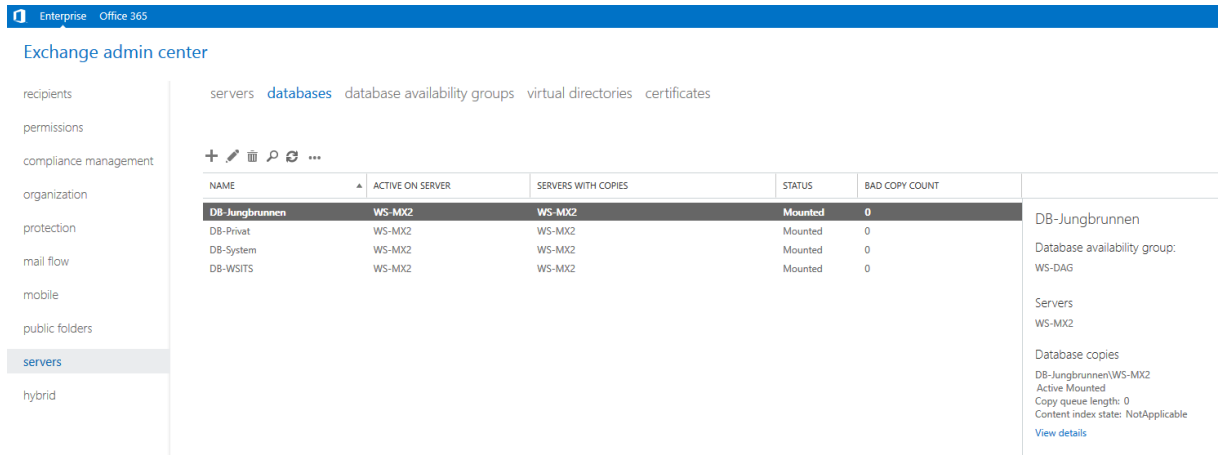
Für ein weiteres TroubleShooting benötigt mein DAG-Cluster eine IPv4-Adresse. Diese trage ich im EAC ein:



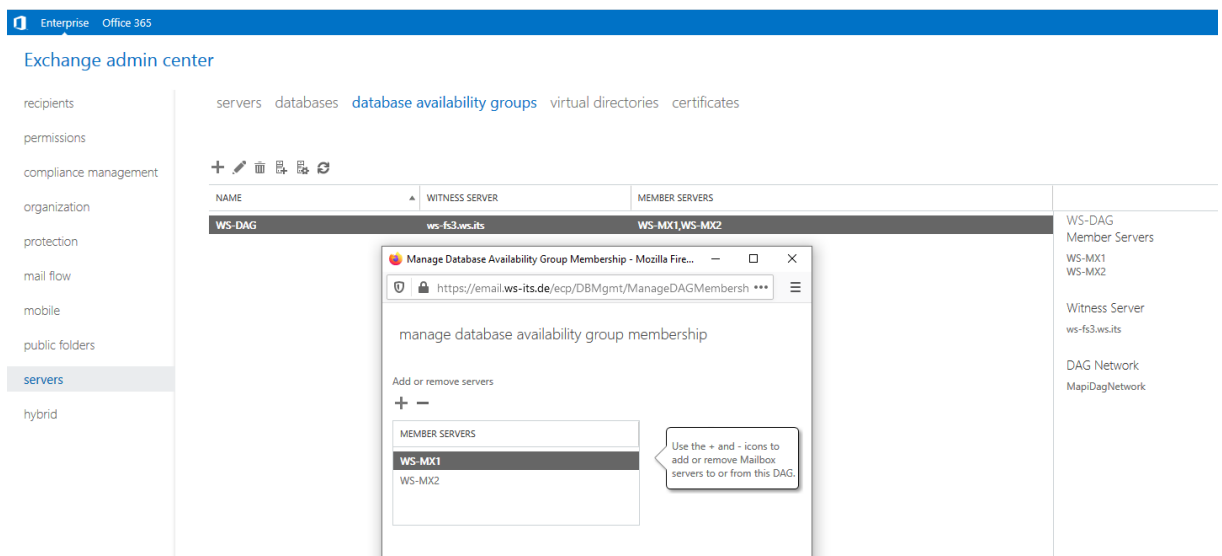
Und dann meldet das EAC, der Server WS-MX1 sei nicht korrekt im Cluster Mitglied??



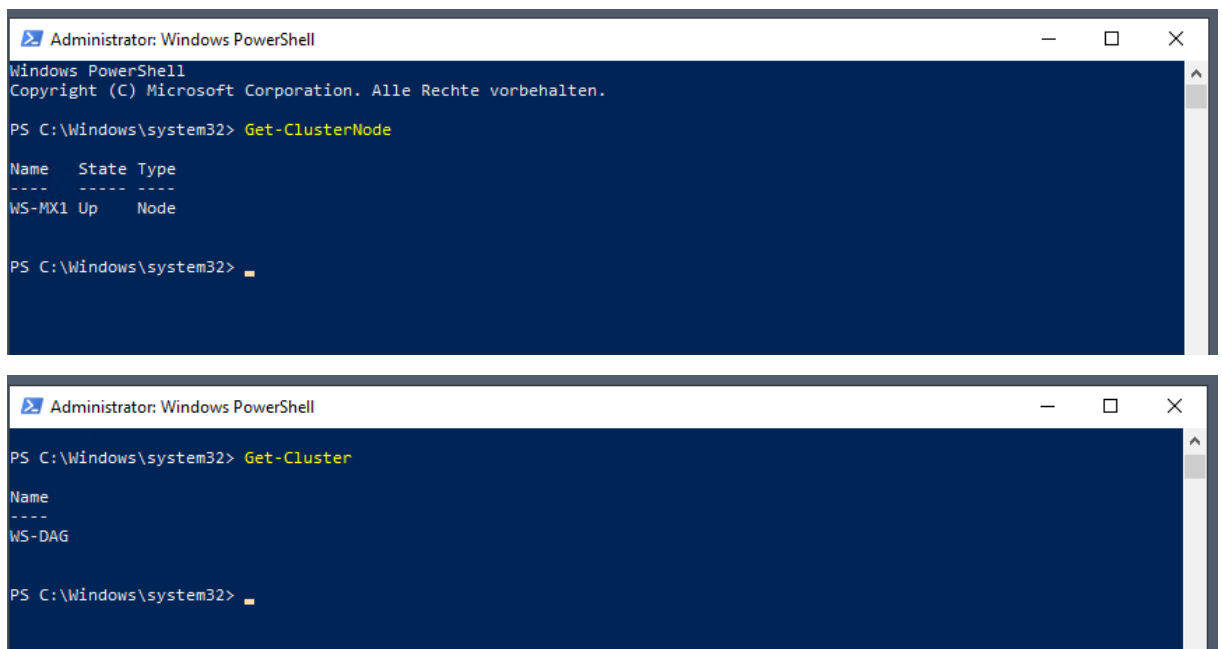
Da muss ich ihn wohl noch einmal neu joinen. Leider muss ich dazu alle Datenbank-Kopien wieder entfernen:



Laut dem Active Directory sind beide Server DAG-Member:



Der Server WS-MX1 sieht sich aber alleine in der DAG:



Ich versuche, den Cluster des Servers zu entfernen. Dieser scheint eine Dublette zu sein.

```

Administrator: Windows PowerShell

PS C:\Windows\system32> Get-Cluster | Remove-Cluster

Remove-Cluster
Möchten Sie den Cluster WS-DAG wirklich vollständig entfernen?
[Y] Ja [N] Nein [H] Anhalten [?] Hilfe (Standard ist "Y"): j
PS C:\Windows\system32>
    
```

Ich versuche erneut, die IPv4 dem Cluster zuzuweisen. Dieses mal mit Erfolg:

The screenshot shows the Exchange Admin Center interface for configuring a Database Availability Group (DAG). The 'IP address' section is active, showing a list of IP addresses: 192.168.100.15 and 255.255.255.255. A tooltip provides information: "DAGs with member servers using Windows Server 2012 R2 or later don't need DAG IP addresses. You can assign static IP addresses or you can utilize Dynamic Host Configuration Protocol (DHCP) by adding 0.0.0.0 to this field." The interface also shows a sidebar with navigation options like 'recipients', 'permissions', and 'servers', and a right-hand pane listing DAG components like 'Member Servers' and 'DAG Network'.

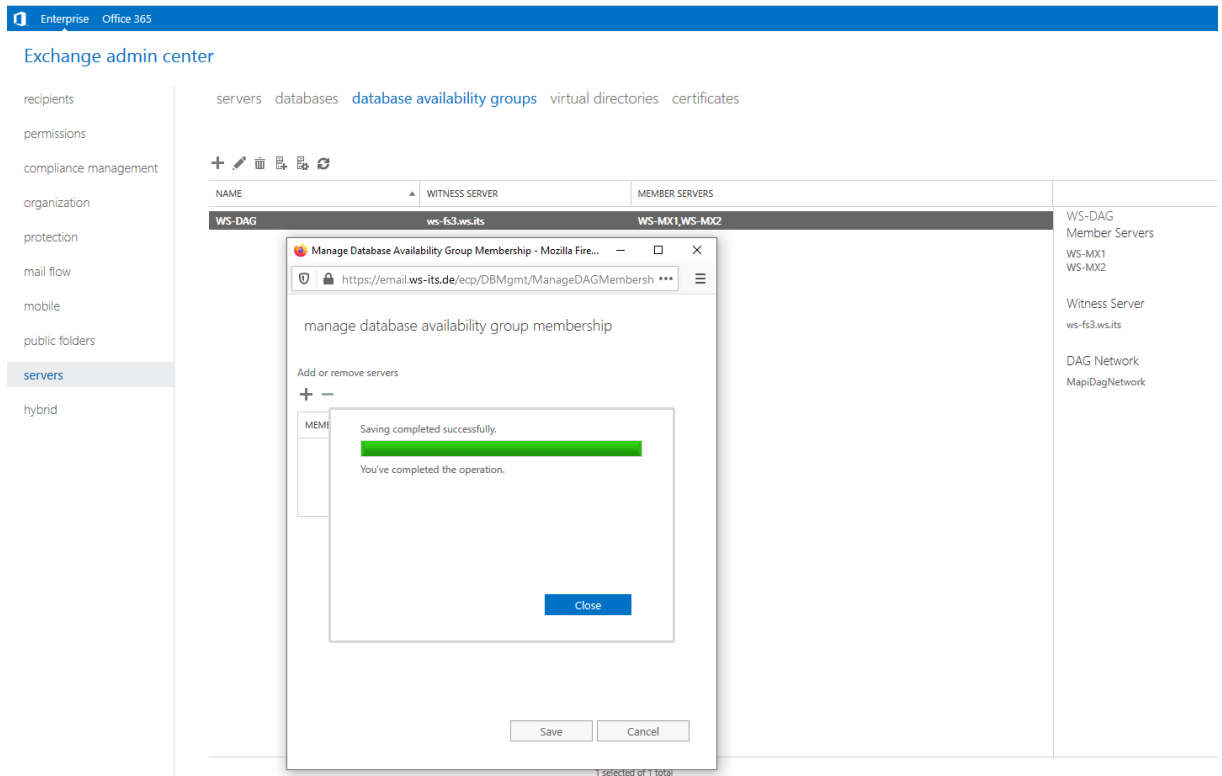
Den WS-MX1 hole ich direkt mit der EAC dazu:

The screenshot shows the Exchange Admin Center interface with the 'Manage Database Availability Group Membership' dialog box open. The 'Select Server' dialog is also open, displaying a table of servers available for selection:

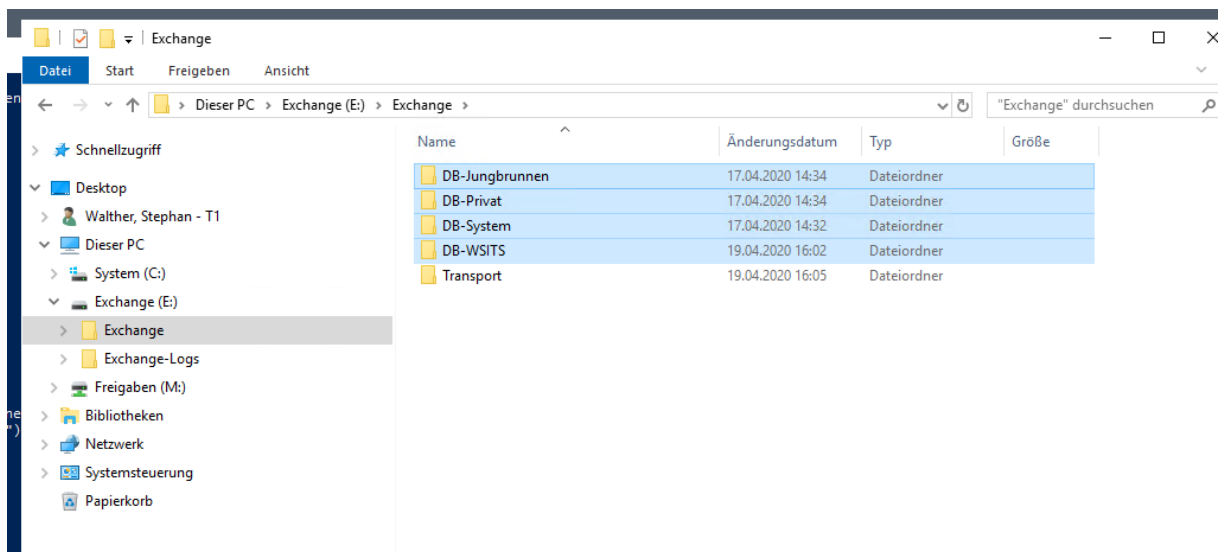
NAME	VERSION	DATABASE
WS-MX1	Version 15.2 (Build 529.5)	
WS-MX2	Version 15.2 (Build 529.5)	WS-DAG

The 'add ->' button is highlighted, and the 'WS-MX1 [remove:]' button is visible below the table. The background shows the Exchange Admin Center interface with the 'servers' section selected in the sidebar.

Der Vorgang war wohl erfolgreich:



Jetzt entferne ich die lokalen Datenbank-Kopien auf dem neuen Cluster-Member:



Danach nehme ich mir das Erstellen der Datenbank-Kopien vor:

Enterprise Office 365

Exchange admin center

recipients permissions compliance management organization protection mail flow mobile public folders **servers** hybrid

servers **databases** database availability groups virtual directories certificates

NAME	SERVER	SERVICES WITH COPIES	STATUS	BAD COPY COUNT
DB-Jungbrunnen		WS-MX2	Mounted	0
DB-Privat	WS-MX2	WS-MX2	Mounted	0
DB-System	WS-MX2	WS-MX2	Mounted	0
DB-WSITS	WS-MX2	WS-MX2	Mounted	0

DB-System
Database availability group: WS-DAG
Servers: WS-MX2
Database copies: DB-System/WS-MX2, Active Mounted, Copy queue length: 0, Content index state: NotApplicable
[View details](#)

Enterprise Office 365

Exchange admin center

recipients permissions compliance management organization protection mail flow mobile public folders **servers** hybrid

servers **databases** database availability groups virtual directories certificates

add mailbox database copy

Mailbox database name: DB-System

*Specify Mailbox server: WS-MX1 Browse...

Activation preference number: 1

Servers hosting a copy of this database: WS-MX2

More options...

Save Cancel

Use this field to select the DAG member on which you want to add the new database copy. Click Browse... select the server that will host the copy from list, and click OK.

Enterprise Office 365

Exchange admin center

recipients permissions compliance management organization protection mail flow mobile public folders **servers** hybrid

servers **databases** database availability groups virtual directories certificates

add mailbox database copy

Mailbox database name: DB-System

*Specify Mailbox server: WS-MX1

Activation preference number: 1

Servers hosting a copy of this database: WS-MX2

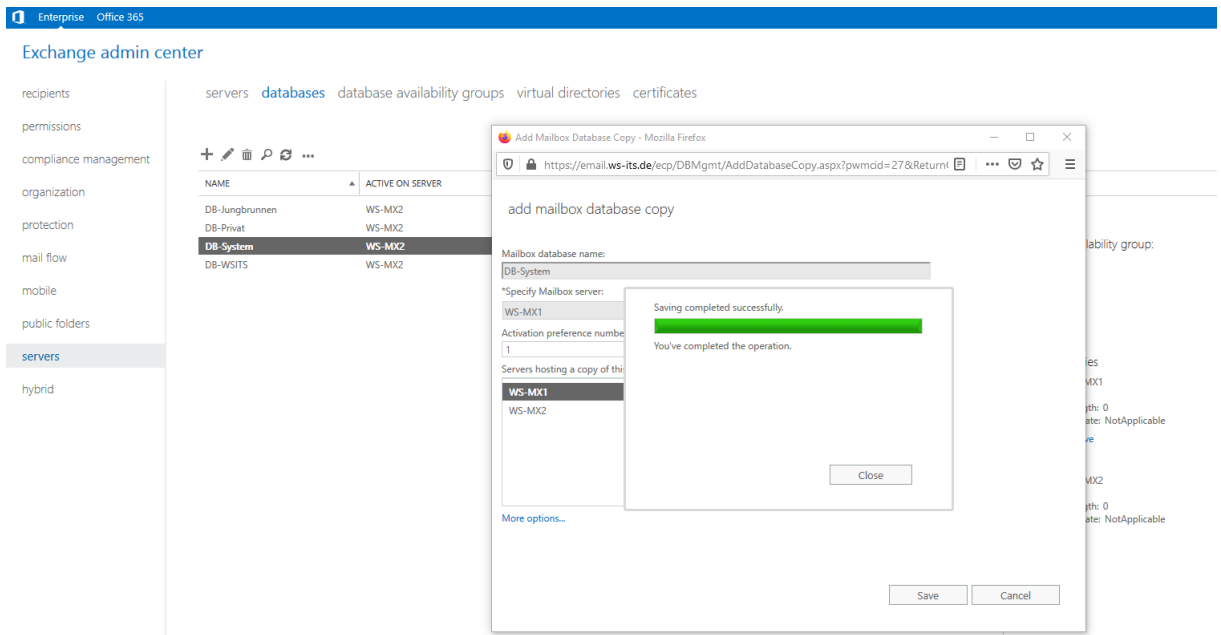
More options...

Save Cancel

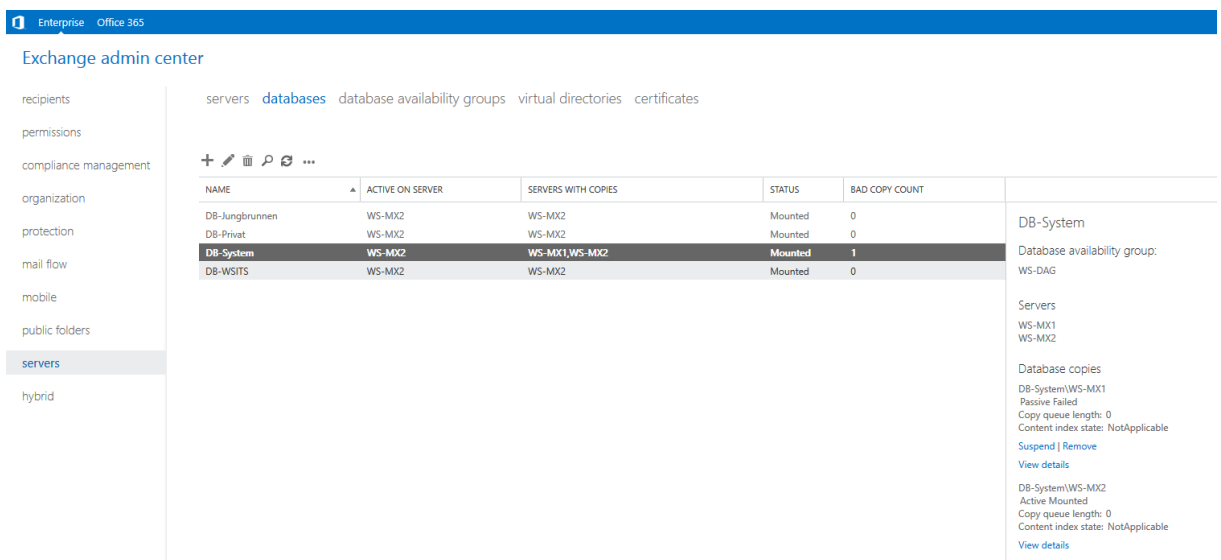
Seeding DB-System/WS-MX1. Bytes Read: 98,304KB, Written: 98,240KB, Remaining: 32,800KB for DB-System.edb.

Click 'Stop' to cancel the operation. Stopping the operation won't undo the changes already applied.

stop



Dank der geringen Größe der Datenbank ging das recht schnell. Dennoch wird eine Kopie im Anschluss wieder als defekt angezeigt:



Offenbar ist der Cluster WS-DAG defekt. Daher baue ich jetzt alles neu auf. Die eine Datenbank-Kopie entferne ich wieder. im Anschluss nehme ich beide Server aus der DAG heraus. Danach entferne ich die DAG. Jetzt kann ich eine neue DAG erstellen:

Unternehmen Office 365

Exchange Admin Center

Server Datenbanken Database Availability Group

Empfänger
Berechtigungen
Verwaltung der Compliance
Organisation
Schutz
Nachrichtenfluss
Mobil
Öffentliche Ordner
Server
Hybrid

NAME	ZEUGENSERVER
Es gibt keine Elemente.	

Database Availability Group - Mozilla Firefox

https://ws-mx2.ws.its/ecp/DBMgmt/NewDAG.aspx

Neue Database Availability Group

*Database Availability Group-Name:

Zeugenserver:

Zeugenverzeichnis:

Database Availability Group-IP-Adressen:

IP-Adresse eingeben

192.168.100.15

Speichern Abbrechen

https://ws-mx2.ws.its/ecp/DBMgmt/NewDAG.aspx?pwncid=6&ReturnObjectType=1#

DAGs mit Mitgliedservern, die Windows Server 2012 R2 oder höher verwenden, benötigen keine DAG-IP-Adressen. Sie können statische IP-Adressen zuweisen, oder sie können das Dynamic Host Configuration-Protokoll (DHCP) nutzen, indem Sie diesem Feld 0.0.0.0 hinzufügen.

[Weitere Informationen](#)

Ich nehme den ersten Mailserver als Member auf:

Unternehmen Office 365

Exchange Admin Center

Server Datenbanken Database Availability Group

Empfänger
Berechtigungen
Verwaltung der Compliance
Organisation
Schutz
Nachrichtenfluss
Mobil
Öffentliche Ordner
Server
Hybrid

NAME	ZEUGENSERVER
WS-DAG	ws.fs3.ws.its

Mitgliedschaft in Database Availability Group verwalten - Mozil...

https://ws-mx2.ws.its/ecp/DBMgmt/ManageDAGMemb...

Mitgliedschaft in Database Availability Group verwalten

Server hinzufügen oder entfernen

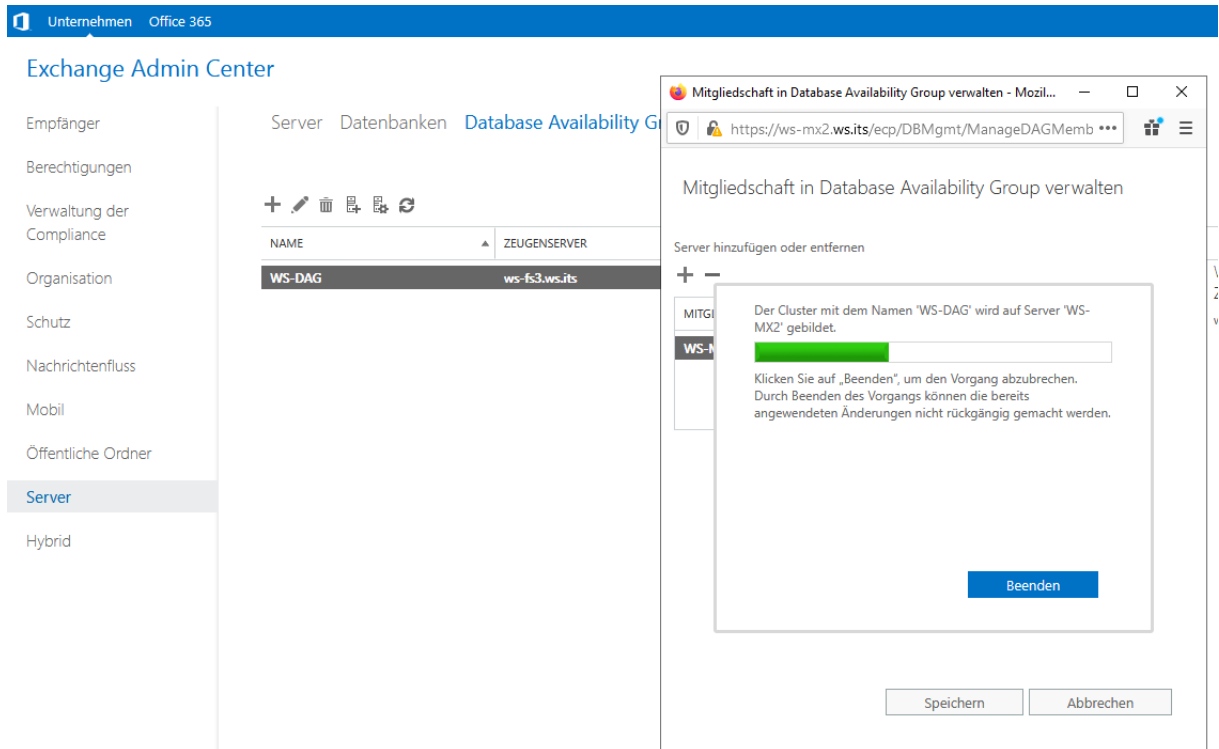
MITGLIEDSERVER

WS-MX2

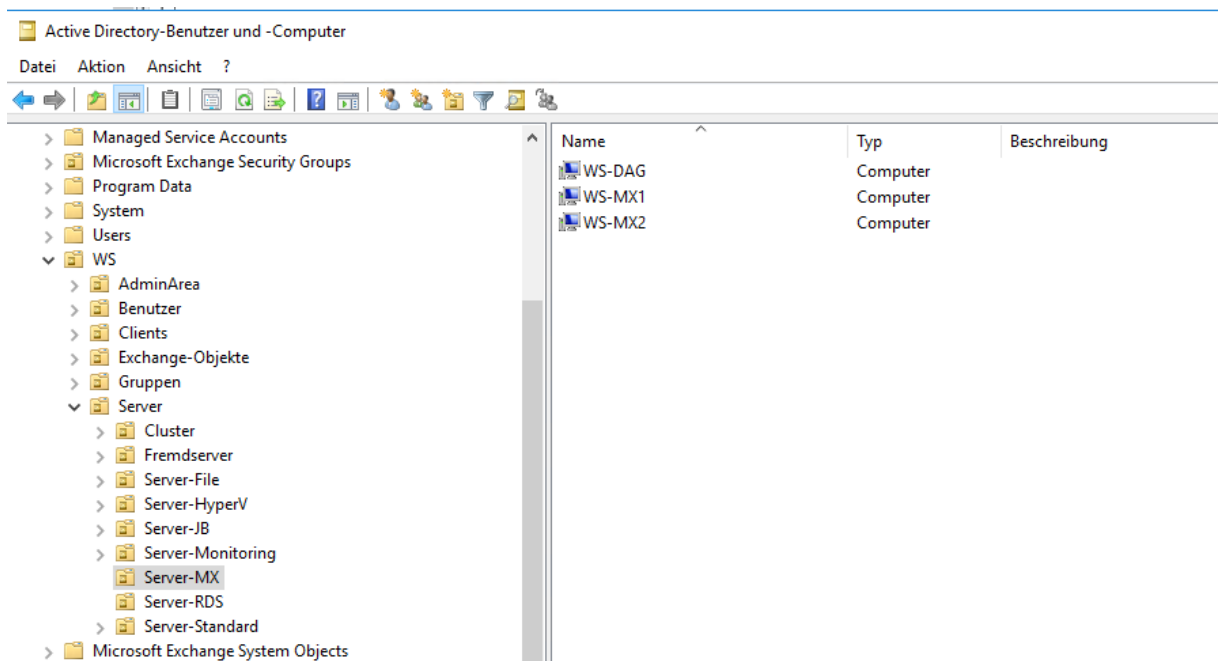
Speichern Abbrechen

Über die Symbole + und - können Sie Postfachserver zu dieser DAG hinzufügen oder daraus entfernen.

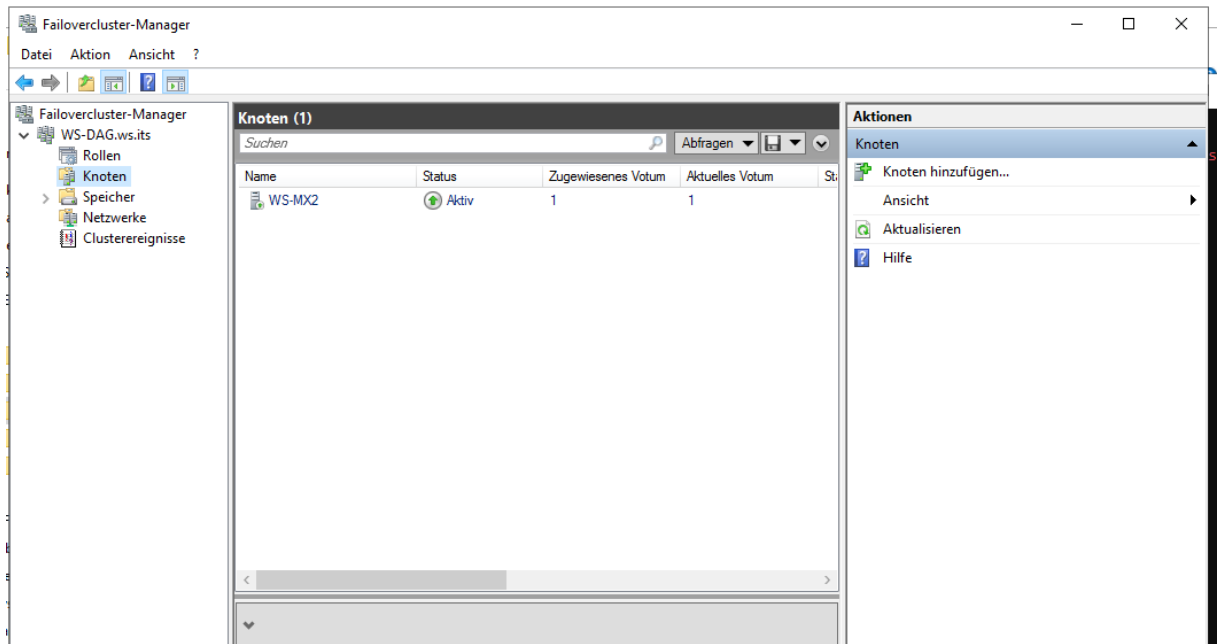
Dabei wird der Cluster gebildet:



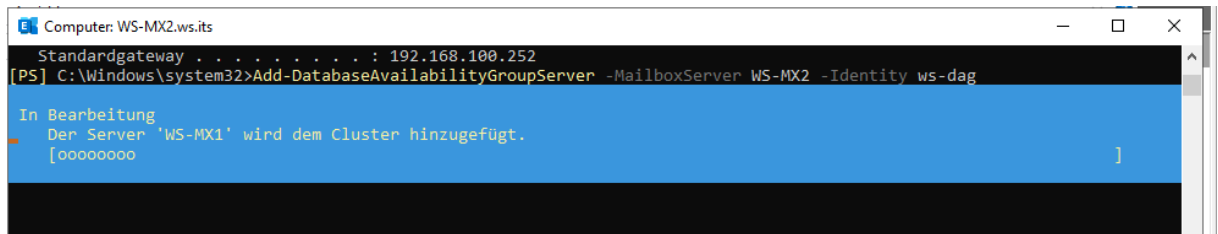
Hierbei handelt es sich um einen traditionellen Windows Failover Cluster mit IPv4 und einem Cluster-Computerkonto im Active Directory:



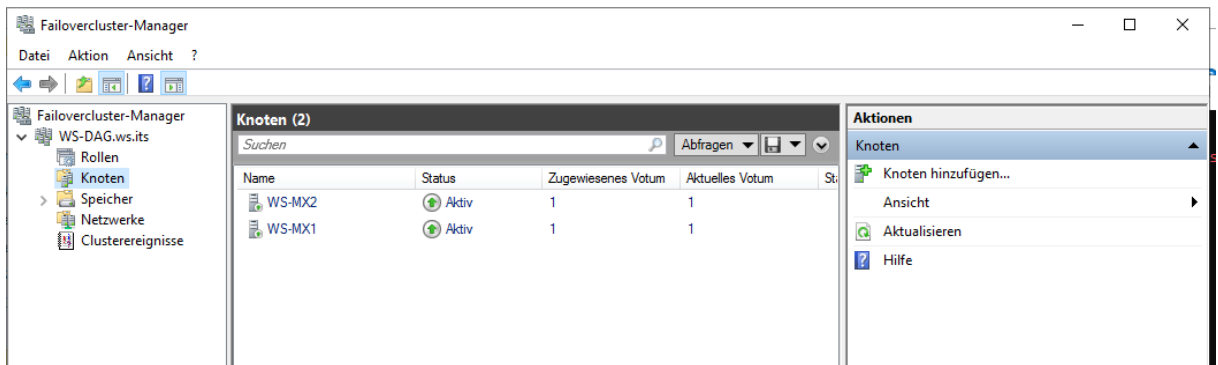
Mit dieser traditionellen Bauart kann ich jetzt auch den Cluster-Manager verwenden:



Jetzt hole ich den anderen Server dazu:



Beide sind jetzt online:



Es wird wieder Zeit für die Datenbank-Kopien. Ich teste mit der kleinen DB-System:

NAME	SERVER MIT KOPIEN	STATUS	ANZAHL UNGÜLTIGER KOPIEN
DB-Jungbrunnen	WS-MX2	Eingebunden	0
DB-Privat	WS-MX2	Eingebunden	0
DB-System	WS-MX2	Eingebund...	0
DB-WSITS	WS-MX2	Eingebunden	0

Die Aktivierungseinstellungennummer wird im Rahmen des Active Manager-Prozesses zur Auswahl der besten Kopie und der erneuten Verteilung aktiver Postfachdatenbanken beim DAG-Ausgleich verwendet. Der Wert ist 1 oder eine größere Zahl, wobei 1 an oberster Stelle in der Einstellungsreihenfolge steht. Die Positionsnummer kann nicht größer als die Anzahl von Kopien der Postfachdatenbank sein.

Der Speichervorgang wurde nicht abgeschlossen.
Der Vorgang wurde beendet.
Fehler beim Seedingvorgang. Fehler: Beim Ausführen von Vorbedingungenprüfungen ist ein Fehler aufgetreten: Die angegebene Datenbank ist nicht für die Replikation konfiguriert und kann daher nicht für Seedingvorgänge verwendet werden... [Datenbank: DB-System, Server: WS-MX2]

Hier war die Replikation zu schnell. Ich warte also ab, bis die EAC den „Aktualisieren“-Schalter zeigt:

Unternehmen Office 365

Exchange Admin Center

Server **Datenbanken** Database Availability Groups Virtuelle Verzeichnisse Zertifikate

Empfänger
Berechtigungen
Verwaltung der Compliance
Organisation
Schutz
Nachrichtenfluss
Mobil
Öffentliche Ordner
Server
Hybrid

NAME	AKTIV AUF SERVER	SERVER MIT KOPIEN	STATUS	ANZAHL UNGÜLTIGER KOPIEN
DB-Jungbrunnen	WS-MX2	WS-MX2	Eingebunden	0
DB-Privat	WS-MX2	WS-MX2	Eingebunden	0
DB-System	WS-MX2	WS-MX1,WS-MX2	Eingebunden	1
DB-WSITS	WS-MX2	WS-MX2	Eingebunden	0

DB-System

Database Availability Group:
WS-DAG

Server
WS-MX1
WS-MX2

Datenbankkopien
DB-System\WS-MX1
Passiv Getrennt und erneute Synchronisierung
Länge der Kopierwarteschlange: 1816
Inhaltsindexzustand: NichtAnwendbar
[Anhalten](#) | [Aktivieren](#) | [Entfernen](#)
[Details anzeigen](#)

DB-System\WS-MX2
Aktiv Eingebunden
Länge der Kopierwarteschlange: 0
Inhaltsindexzustand: NichtAnwendbar
[Details anzeigen](#)

Jetzt ist es soweit. Das kleine Detail kann man leicht übersehen:

Unternehmen Office 365

Exchange Admin Center

Server **Datenbanken** Database Availability Groups Virtuelle Verzeichnisse Zertifikate

Empfänger
Berechtigungen
Verwaltung der Compliance
Organisation
Schutz
Nachrichtenfluss
Mobil
Öffentliche Ordner
Server
Hybrid

NAME	AKTIV AUF SERVER	SERVER MIT KOPIEN	STATUS	ANZAHL UNGÜLTIGER KOPIEN
DB-Jungbrunnen	WS-MX2	WS-MX2	Eingebunden	0
DB-Privat	WS-MX2	WS-MX2	Eingebunden	0
DB-System	WS-MX2	WS-MX1,WS-MX2	Eingebunden	1
DB-WSITS	WS-MX2	WS-MX2	Eingebunden	0

DB-System

Database Availability Group:
WS-DAG

Server
WS-MX1
WS-MX2

Datenbankkopien
DB-System\WS-MX1
Passiv Fehlgeschlagen und angehalten
Länge der Kopierwarteschlange: 0
Inhaltsindexzustand: NichtAnwendbar
[Fortsetzen](#) | [Aktualisieren](#) | [Entfernen](#)
[Details anzeigen](#)

DB-System\WS-MX2
Aktiv Eingebunden
Länge der Kopierwarteschlange: 0
Inhaltsindexzustand: NichtAnwendbar
[Details anzeigen](#)

Das Seeding erwartet einen Quellserver:

Unternehmen Office 365

Exchange Admin Center

Empfänger
Berechtigungen
Verwaltung der Compliance
Organisation
Schutz
Nachrichtenfluss
Mobil
Öffentliche Ordner
Server
Hybrid

Server **Datenbanken** Database Availability Groups

NAME	AKTIV AUF SERVER
DB-Jungbrunnen	WS-MX2
DB-Privat	WS-MX2
DB-System	WS-MX2
DB-WSITS	WS-MX2

Datenbankkopie aktualisieren

Name der Postfachdatenbank:
DB-System

Servername:
WS-MX1

Geben Sie einen Quellserver für das Seeding an:

Klicken Sie auf „Durchsuchen“, um einen Postfachserver mit einer Kopie der Postfachdatenbank auszuwählen, die als Quelle für den Seedingvorgang verwendet werden soll. Wenn Sie keinen Postfachserver auswählen, wird der Server, der die aktive Kopie der Datenbank hostet, als Quelle für den Seedingvorgang verwendet.

Details anzeigen

Danach geht es recht schnell:

Unternehmen Office 365

Exchange Admin Center

Empfänger
Berechtigungen
Verwaltung der Compliance
Organisation
Schutz
Nachrichtenfluss
Mobil
Öffentliche Ordner
Server
Hybrid

Server **Datenbanken** Database Availability Groups

NAME	AKTIV AUF SERVER
DB-Jungbrunnen	WS-MX2
DB-Privat	WS-MX2
DB-System	WS-MX2
DB-WSITS	WS-MX2

Datenbankkopie aktualisieren

Name der Postfachdatenbank:
DB-System

Servername:
WS-MX1

Geben Sie einen Quellserver für das Seeding an:

Der Speichervorgang wurde erfolgreich abgeschlossen.

Sie haben den Vorgang abgeschlossen.

Details anzeigen

Das sieht doch viel besser aus:

Unternehmen Office 365

Exchange Admin Center

Server **Datenbanken** Database Availability Groups Virtuelle Verzeichnisse Zertifikate

+ ✎ 🗑️ 🔄 ⋮

NAME	AKTIV AUF SERVER	SERVER MIT KOPIEN	STATUS	ANZAHL UNGÜLTIGER KOPIEN	
DB-Jungbrunnen	WS-MX2	WS-MX2	Eingebunden	0	DB-System Database Availability Group: WS-DAG Server WS-MX1 WS-MX2 Datenbankkopien DB-System\WS-MX1 Passiv Fehlerfrei Länge der Kopierwarteschlange: 0 Inhaltsindexzustand: NichtAnwendbar Anhalten Aktivieren Entfernen Details anzeigen DB-System\WS-MX2 Aktiv Eingebunden Länge der Kopierwarteschlange: 0 Inhaltsindexzustand: NichtAnwendbar Details anzeigen
DB-Privat	WS-MX2	WS-MX2	Eingebunden	0	
DB-System	WS-MX2	WS-MX1,WS-MX2	Eingebunden	0	
DB-WSITS	WS-MX2	WS-MX2	Eingebunden	0	

Aber so weit war ich schon mal. Lässt sich die Datenbank auch verschieben?

Unternehmen Office 365

Exchange Admin Center

Server **Datenbanken** Database Availability Groups Virtuelle Verzeichnisse Zertifikate

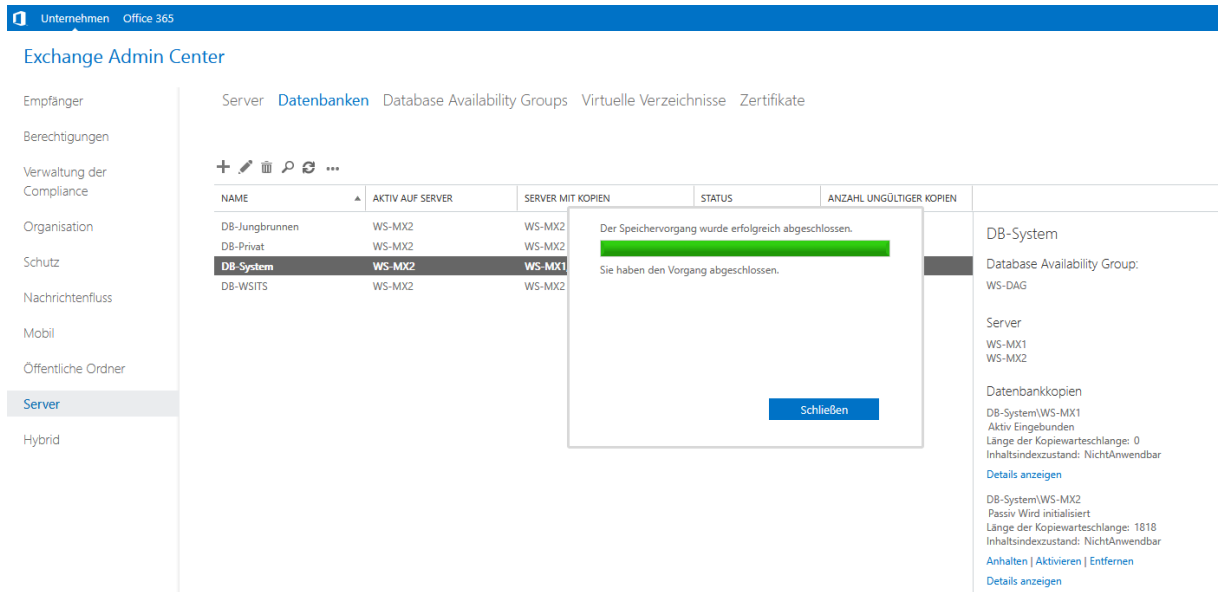
+ ✎ 🗑️ 🔄 ⋮

NAME	AKTIV AUF SERVER	SERVER MIT KOPIEN	STATUS	ANZAHL UNGÜLTIGER KOPIEN	
DB-Jungbrunnen	WS-MX2	WS-MX2	Eingebunden	0	DB-System Database Availability Group: WS-DAG Server WS-MX1 WS-MX2 Datenbankkopien DB-System\WS-MX1 Passiv Fehlerfrei Länge der Kopierwarteschlange: 0 Inhaltsindexzustand: NichtAnwendbar Anhalten Aktivieren Entfernen Details anzeigen DB-System\WS-MX2 Aktiv Eingebunden Länge der Kopierwarteschlange: 0 Inhaltsindexzustand: NichtAnwendbar Details anzeigen
DB-Privat	WS-MX2	WS-MX2	Eingebunden	0	
DB-System	WS-MX2	WS-MX1	Eingebunden	0	
DB-WSITS	WS-MX2	WS-MX2	Eingebunden	0	

Warnung

Möchten Sie die Datenbankkopie DB-System\WS-MX1 aktivieren?

JA! Endlich hab ich eine funktionale DAG!

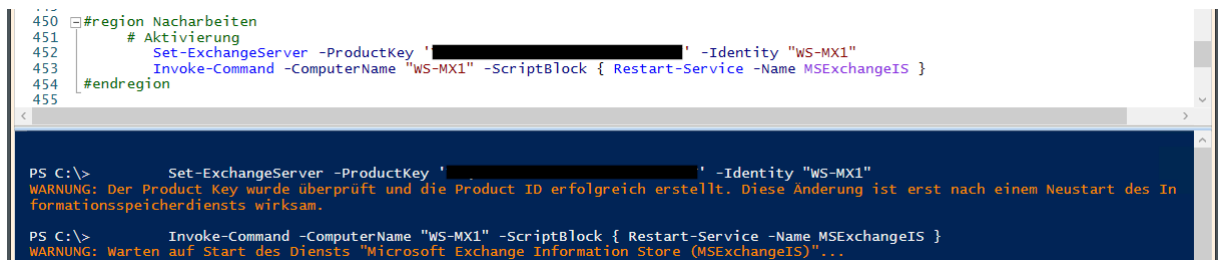


Ich erstelle nun auch für die anderen Datenbanken die fehlende Kopie.

Nacharbeiten

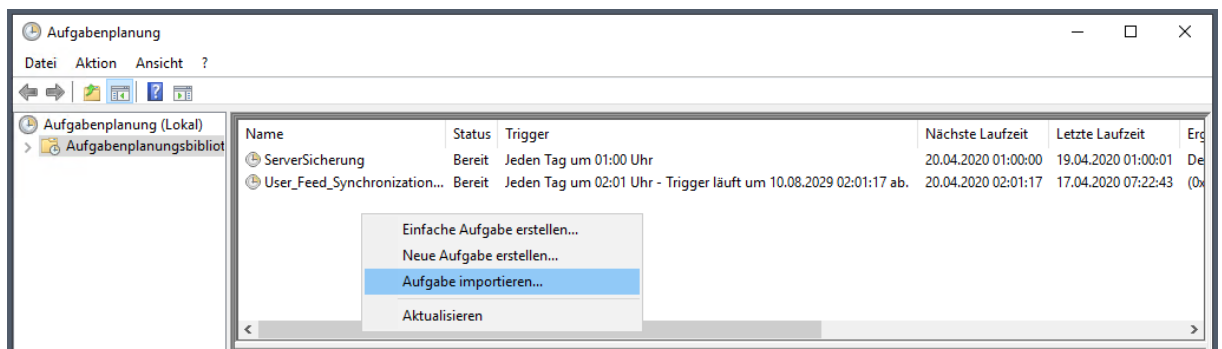
Lizensierung des Exchange Servers

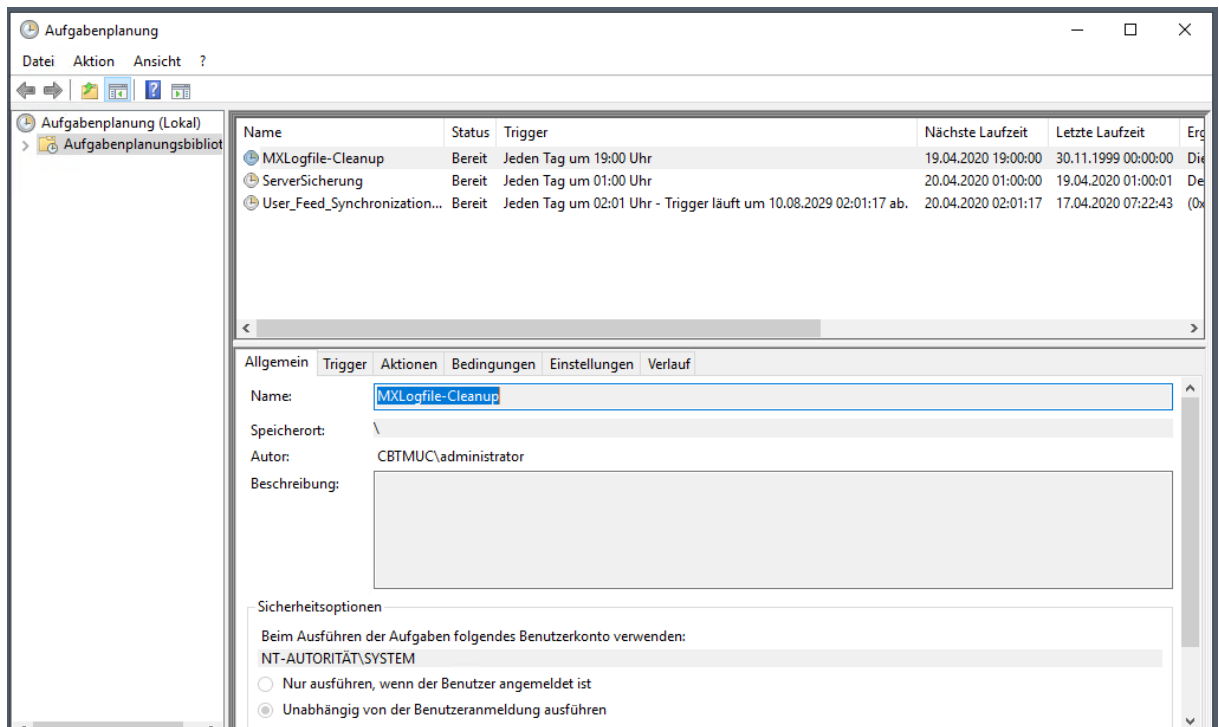
Die letzten Arbeitsschritte führen zur Aktivierung des neuen Servers:



Logfile-Optimierung

Ebenso benötige ich eine automatische Bereinigung der unzähligen Logdateien. Dazu importiere ich den gleichen Scripttask wie beim anderen Server:





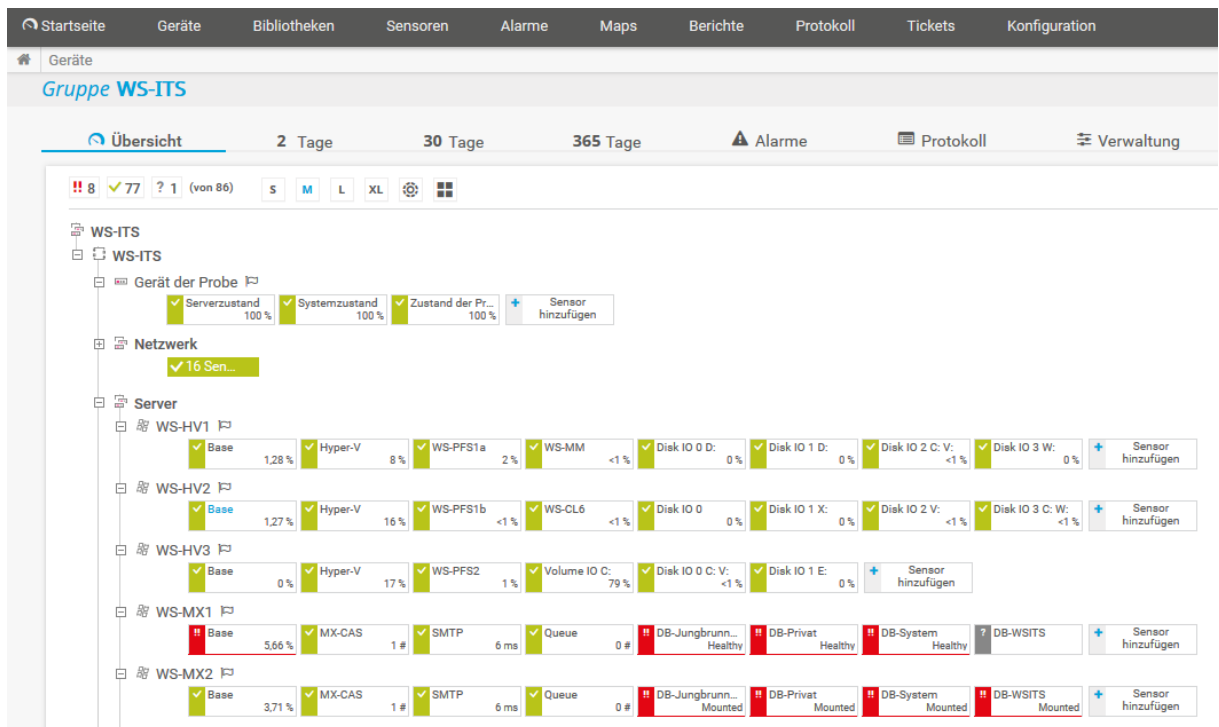
Der Task startet diesen Code:

```

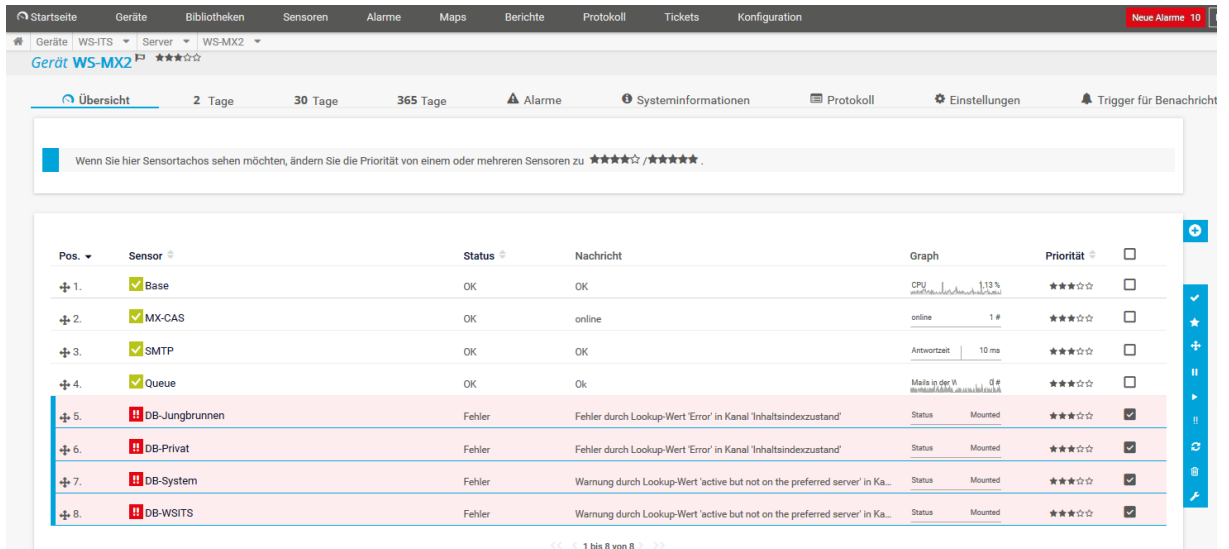
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe "& {Get-ChildItem -Path 'C:\Program Files\Microsoft\Exchange Server\V15\Logging','C:\inetpub\logs\LogFiles' -Include '*.log','*.bak','*.blg' -Recurse | Where-Object { $_.LastWriteTime -le (Get-Date).AddDays(-14) } | Remove-Item -Confirm:$false -ErrorAction SilentlyContinue}"
    
```

Konfiguration des Monitorings

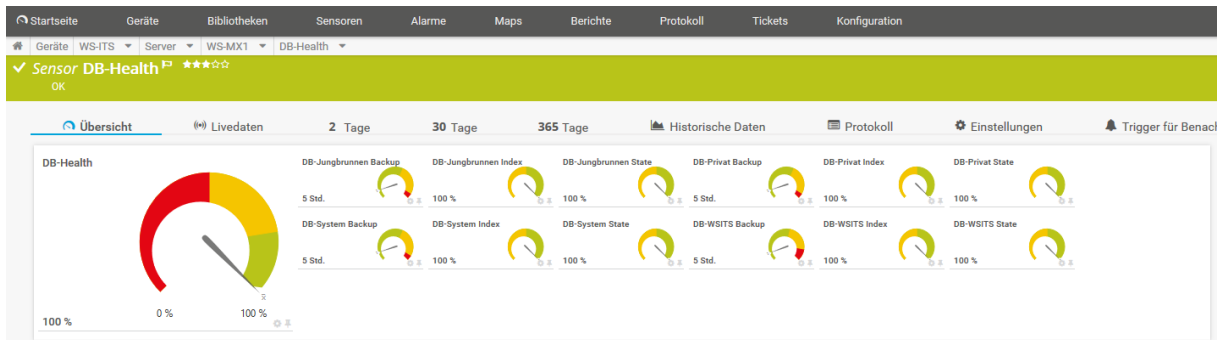
Nun fehlt nur noch das Monitoring. Hier stehe ich vor einem Problem: der mitgelieferte Sensor von PRTG kann mit Exchange Server 2019 Datenbanken nicht umgehen. Diese haben eine andere Form der Datenindizierung. Da die alte Variante fehlt – aber geprüft wird – gibt es Fehler:



Im Detail kann man es besser erkennen:

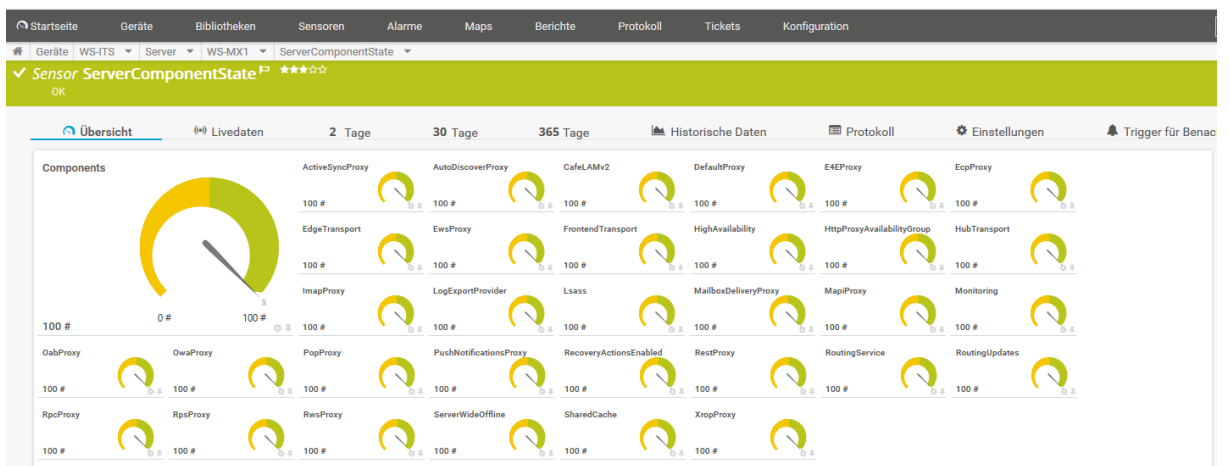


Also erstelle ich mir eigene Sensoren mit der PowerShell und binde diese ein:



Das neue Script kann bis zu 16 Datenbanken je Server überwachen – in einem Sensor (zur Info: bei PRTG wird unter anderem nach der Anzahl der Sensoren lizenziert. Die hauseigenen Exchange-Sensoren können nur eine Datenbank je Sensor überwachen). Integriert habe ich je Datenbank die Bereitstellung, den Indexstand und das Alter der Datensicherung. Und schon ist wieder alles im grünen Bereich.

Und weil ich gerade dabei bin gibt es noch einen weiteren neuen Sensor (selbstprogrammiert). Mit diesem kann ich die ServerComponentStates überwachen:



Damit sollte ich Probleme beim Exchange Service rechtzeitig kommen sehen.

Abschluss der Migration

Zusammenfassung

Endlich sind die beiden Mailserver umgezogen. Das war viel Arbeit. Aber nun trennen mich nur noch wenige Server von meinem Ziel einer reinen Windows Server 2019 Umgebung!