

## Inhalt

1.	Szenario .....	1
	IST-Situation .....	1
	SOLL-Zustand .....	2
	Migrationsplan .....	2
2.	Migration WS-MX1 .....	2
	Entfernen des alten Servers .....	2
	Bereitstellung des neuen Servers .....	8
	Konfiguration des neuen Servers .....	12
	Abschalten der Datensicherung .....	17
3.	Migration WS-MX2 .....	19
	Entfernen des alten Servers .....	19
	Bereitstellung des neuen Servers .....	21
	Problem: Reparatur der SystemMailboxen .....	23
	Konfiguration des neuen Servers .....	25
	Konfiguration der Datensicherung .....	29
4.	Abschluss .....	32
	Diagnose .....	32
	Zusammenfassung .....	32

## 1. Szenario

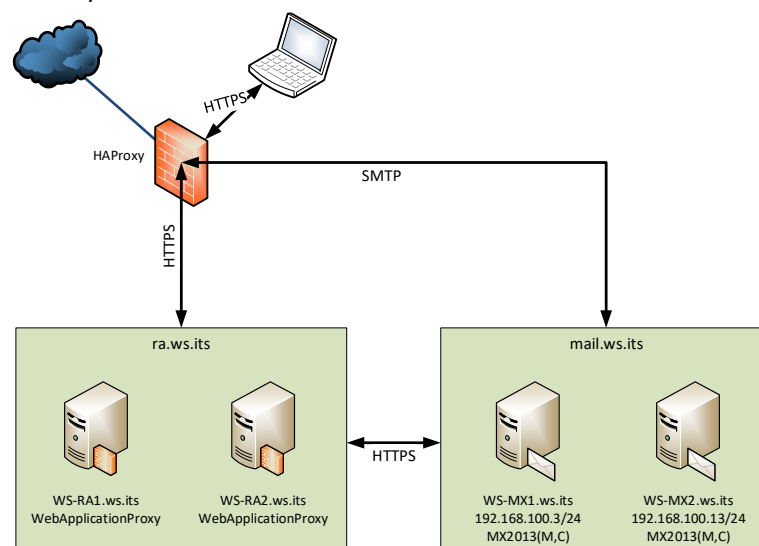
### IST-Situation

Aktuell wird der Service Exchange auf 2 Servern bereitgestellt: WS-MX1 und WS-MX2. Beide laufen mit Windows Server 2012 R2 und Exchange Server 2013 CU15 mit den Rollen ClientAccess und Mailbox. Beide Server

- senden Mails ins Internet
- empfangen Mails aus dem Internet
- sind unter dem Namen email.ws.its (2 Host-A-Records) intern erreichbar
- werden über einen Reverse-Proxy unter dem Namen email.ws-its.de von extern erreicht
- hosten 3 Mailboxdatenbanken. Diese werden in einer DAG repliziert und geschützt
- werden mit einem DPM 2016 gesichert
- werden mit PRTG überwacht

Alle Infrastrukturkomponenten und Services sind bereit für Exchange Server 2016.

Die Infrastruktur hat folgendes Layout:



### Bekannte Probleme:

- Die Betriebssysteme laufen seit dem letzten Windows Update recht unzuverlässig.
- Es gibt Probleme mit den SystemMailboxen
- Vor langer Zeit wurden 2 Systemzertifikate gelöscht. Seitdem wird das Eventlog täglich mit etlichen Fehlern beschrieben

### SOLL-Zustand

Die beiden Server sollen auf die aktuelle Version Exchange Server 2016 CU4 angehoben werden. Die Betriebssysteme sollen unter Windows Server 2016 laufen. Der ComputerName und die IP-Adresse soll an die neue Maschine übergeben werden. Das Monitoring und die Datensicherung sollen kompatibel weiter betrieben werden.

### Migrationsplan

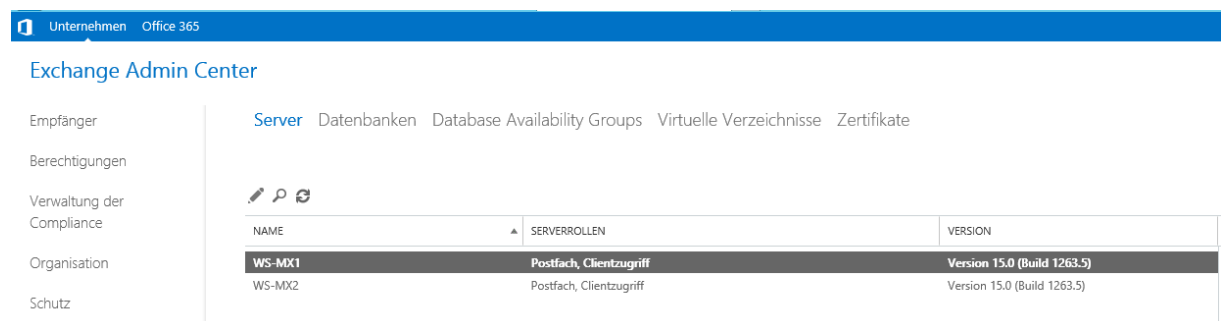
Da Name und IP wiederverwendet werden sollen, muss eine Wipe&Load-Migration ausgeführt werden: ein Server wird von seinen Diensten befreit und deinstalliert, durch den neuen Server ersetzt (kein Upgrade!) und darauf wird Exchange neu installiert. Die Funktionen werden dann SideBySide von dem 2. alten Server auf den ersten neuen Server übergeben. Danach kann der 2. alte Server deinstalliert werden. Zuletzt wird dieser neu aufgesetzt und die Verfügbarkeitsoptionen werden wieder konfiguriert.

Eine Zielsetzung ist eine Migration ohne DownTime aus Usersicht: zu jeder Zeit müssen Mails gesendet und empfangen werden können. Zu jeder Zeit muß ein Postfachzugriff über alle Kanäle (AS, OL, OWA) möglich sein.

## 2. Migration WS-MX1

### Entfernen des alten Servers

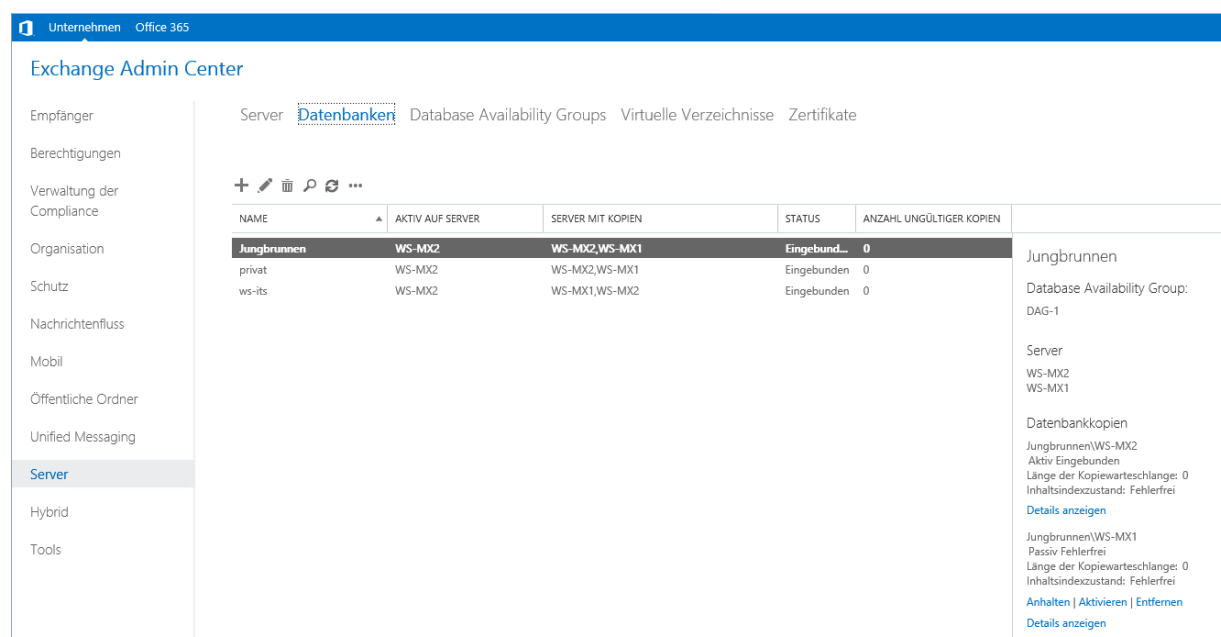
Beide Server sind auf einem Level, in dem Exchange Server 2016 eingesetzt werden kann:



Exchange Admin Center - Server

NAME	SERVERROLLEN	VERSION
WS-MX1	Postfach, Clientzugriff	Version 15.0 (Build 1263.5)
WS-MX2	Postfach, Clientzugriff	Version 15.0 (Build 1263.5)

Die Datenbanken arbeiten einwandfrei:



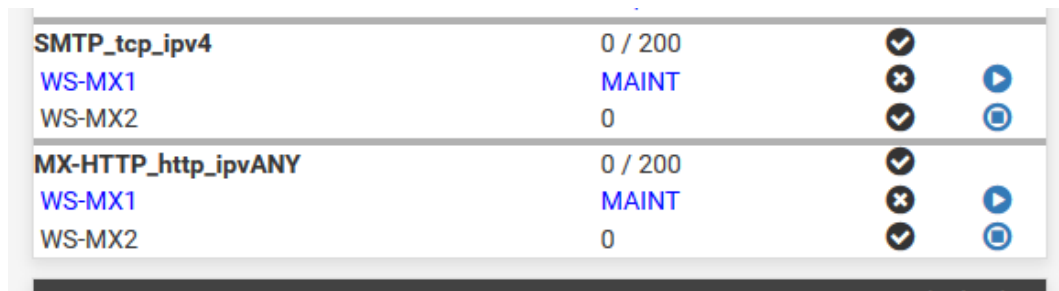
Exchange Admin Center - Datenbanken

NAME	AKTIV AUF SERVER	SERVER MIT KOPIEN	STATUS	ANZAHL UNGÜLTIGER KOPIEN
Jungbrunnen	WS-MX2	WS-MX2, WS-MX1	Eingebund...	0
privat	WS-MX2	WS-MX2, WS-MX1	Eingebunden	0
ws-its	WS-MX2	WS-MX1, WS-MX2	Eingebunden	0

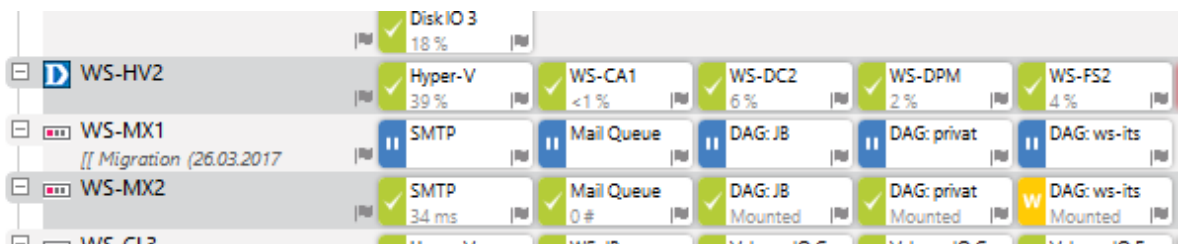
Details for Jungbrunnen DAG-1:

- Server: WS-MX2, WS-MX1
- Datenbankkopien:
  - Jungbrunnen\WS-MX2: Aktiv Eingebunden, Länge der Kopierwarteschlange: 0, Inhaltsindexzustand: Fehlerfrei
  - Jungbrunnen\WS-MX1: Passiv Fehlerfrei, Länge der Kopierwarteschlange: 0, Inhaltsindexzustand: Fehlerfrei

Damit es keine Probleme bei der Mailzustellung gibt, schalte ich im HA-Proxy die Weiterleitung von SMTP und HTTP an den WS-MX1 ab:



Auch das Monitoring des PRTG wird pausiert:



Im DNS lösche ich den Host-A-Record auf mail.ws.its für den Server, damit dieser auch nicht mehr als CAS verwendet wird.

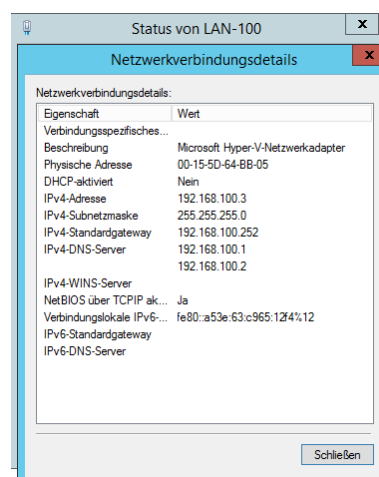
Nun können die DAG-MailboxDatenbankKopien auf WS-MX1 gelöscht werden. Ab jetzt ist der Server WS-MX2 alleine für die DBs zuständig:

```
Get-MailboxDatabaseCopyStatus -Server ws-mx1 | Remove-MailboxDatabaseCopy
```

Ebenso kann der Server WS-MX1 aus dem DAG-Cluster genommen werden:

```
Remove-DatabaseAvailabilityGroupServer -MailboxServer WS-MX1 -Identity DAG-1
```

Noch ein kurzer Blick auf die Netzwerk-Konfiguration:



Dateien, die ich auf dem neuen Server benötige, kopiere ich auf das Netzlaufwerk. Dazu gehören Zertifikate, Skripte und geplante Aufgaben.

Nun kann der Server angehalten werden. In der PowerShell prüfe ich noch einmal, ob noch Mails in der Transportwarteschlange stecken (get-queue). Da der HA-Proxy nichts weiter leitet ist die Queue leer. Also auf zur Deinstallation:


Name	Herausgeber	Installiert am	Größe	Versio
Local Administrator Password Solution	Microsoft Corporation	10.11.2016	129 KB	6.2.0.0
Microsoft Exchange Server 2013 Cumulative Update 15	Microsoft Corporation	23.03.2017		15.0.1
Microsoft Lync Server 2013, Bootstrapper Prerequisite...	Microsoft Corporation		188 MB	5.0.83
Microsoft Server Speech Platform Runtime (x64)	Microsoft Corporation		6,69 MB	11.0.7
Microsoft Silverlight	Microsoft Corporation	23.11.2014	22,6 MB	5.1.20
Microsoft Speech Platform VXML Runtime (x64)	Microsoft Corporation	11.07.2014	1,34 MB	11.0.7
Microsoft System Center 2016 DPM Protection Agent	Microsoft Corporation	06.02.2017	32,7 MB	5.0.24
Microsoft Unified Communications Managed API 4.0,...	Microsoft Corporation	11.07.2014	88,0 KB	5.0.83
Microsoft Visual C++ 2005 Redistributable (x64)	Microsoft Corporation	22.11.2014	6,92 MB	9.0.61

? X

## Bereitschaftsüberprüfung

Der Computer wird überprüft, um festzustellen, ob das Setup fortgesetzt werden kann.

Analyse der Voraussetzungen
100%



deinstallieren

Nach etlichen Minuten hält die Deinstallation an:

SETUP VON MICROSOFT EXCHANGE SERVER 2013, KUMULATIVES UPDATE 15

? X

## Setupstatus

Schritt 7 von 13: Clientzugriffsrolle: Clientzugriffs-Front-End-Dienst

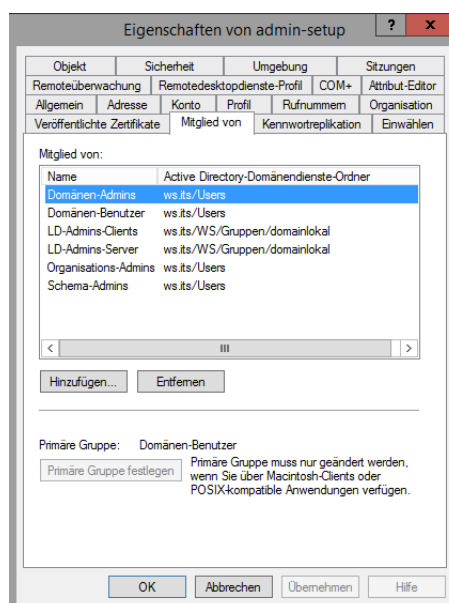
100%

```
Fehler:
Der folgende Fehler wurde generiert, als "Error.Clear();
if (!$isProvisionServerInitialized)
{
  $hasExchangeServersWriteAccess = test-ExchangeServersWriteAccess -DomainController $RoleDomainController -
ErrorAction SilentlyContinue;
  $provisionserver = get-provisionedexchangeserver -Identity $RoleNetBIOSName -DomainController $RoleDomainController
-ErrorAction SilentlyContinue;
  $isProvisionServerInitialized = $true;
}
if ($hasExchangeServersWriteAccess)
{
  remove-ExchangeServerGroupMember -ServerName $RoleNetBIOSName -DomainController $RoleDomainController
}
" ausgeführt wurde: "Microsoft.Exchange.Data.Directory.ADOperationException: Fehler bei Active Directory-Vorgang mit WS-
DC2.ws.its. Bei diesem Fehler ist kein Wiederholungsversuch möglich. Zusätzliche Informationen: Die Zugriffsrechte reichen für
diesen Vorgang nicht aus.
Active Directory-Antwort: 00002098: SecErr: DSID-03150E49, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0
--> System.DirectoryServices.Protocols.DirectoryOperationException: Der Benutzer verfügt nicht über die erforderlichen
```



beenden

Die Ursache ist schnell gefunden: der BenutzerAccount, den ich für die Deinstallation verwendete, hat zu wenig Rechte. Das lässt sich korrigieren:



Eine Wiederaufnahme des Setup-Prozesses ist dennoch nicht möglich:



Also deinstalliere ich mit der cmd:

```

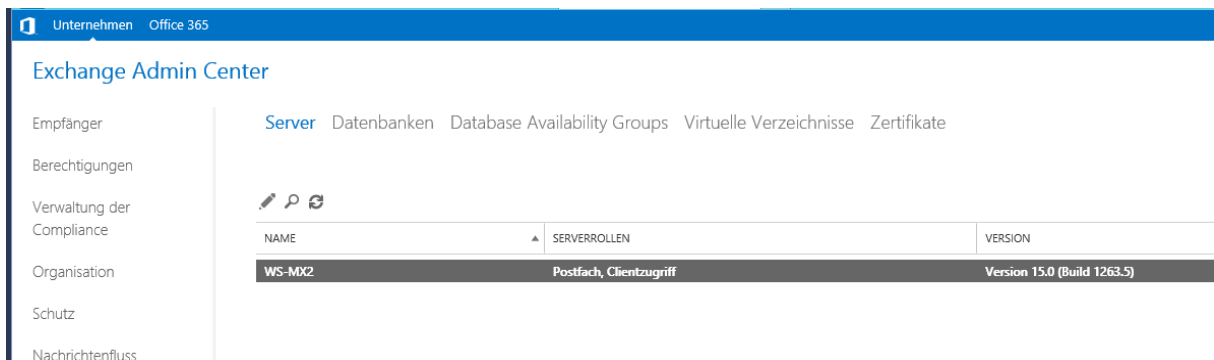
Administrator: Eingabeaufforderung
C:\Admin\MX>setup /mode:uninstall

Willkommen bei der unbeaufsichtigten Installation von Microsoft Exchange Server
2013, kumulatives Update 15
Postfachrolle: Postfachdienst
Postfachrolle: Unified Messaging-Dienst
Postfachrolle: Clientzugriffsdienst
Postfachrolle: Transportdienst
Clientzugriffsrolle: Front-End-Transport-Dienst
Clientzugriffsrolle: Clientzugriffs-Front-End-Dienst
Sprachen

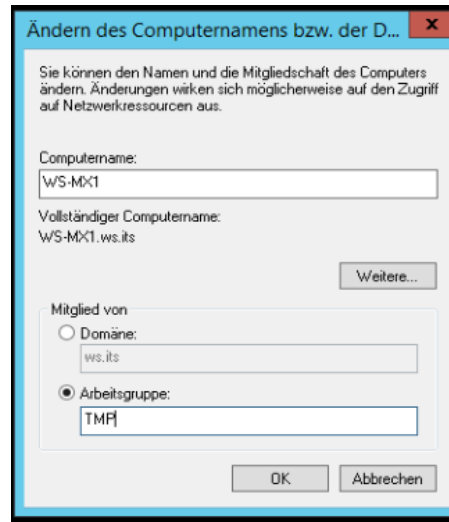
Die Voraussetzungen für Microsoft Exchange Server werden überprüft
    Voraussetzungen werden konfiguriert                ABGESCHLOSSEN
Microsoft Exchange Server wird konfiguriert
    Das Setup wird vorbereitet                          ABGESCHLOSSEN
    Clientzugriffsrolle: Clientzugriffs-Front-End-Dienst ABGESCHLOSSEN
    Sprachdateien                                       ABGESCHLOSSEN
    Dienste werden angehalten                          ABGESCHLOSSEN
    Die Exchange-Dateien werden entfernt               ABGESCHLOSSEN
    Dienste werden wiederhergestellt                  ABGESCHLOSSEN
    Das Setup wird abgeschlossen                       ABGESCHLOSSEN

Der Installationsvorgang von Exchange Server wurde erfolgreich abgeschlossen.
C:\Admin\MX>
    
```

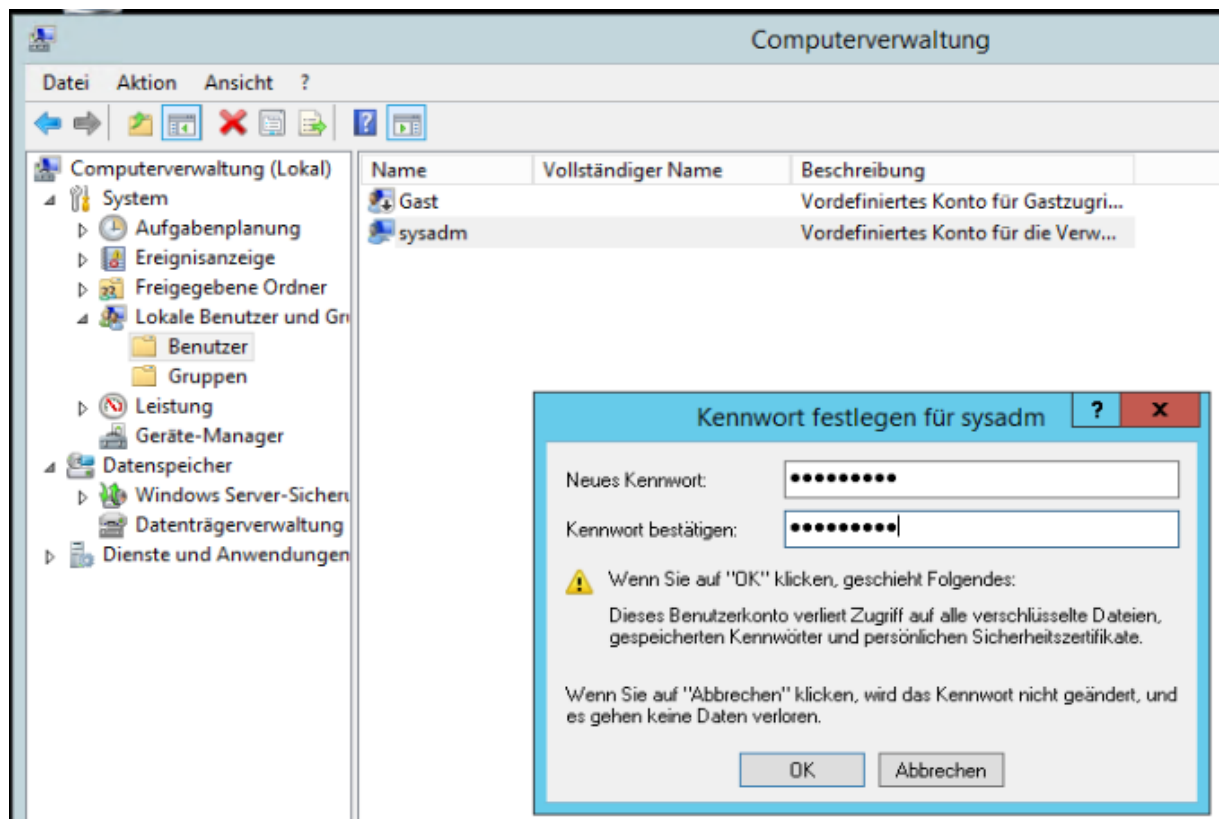
Das Ergebnis wird auf dem 2. MX angezeigt:



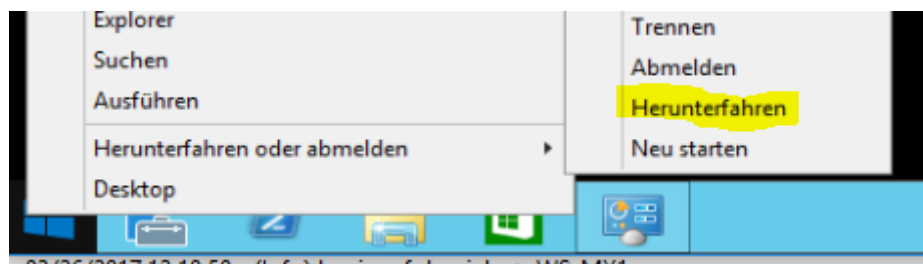
Nun kann ich den Server aus der Domäne entfernen und abschalten:



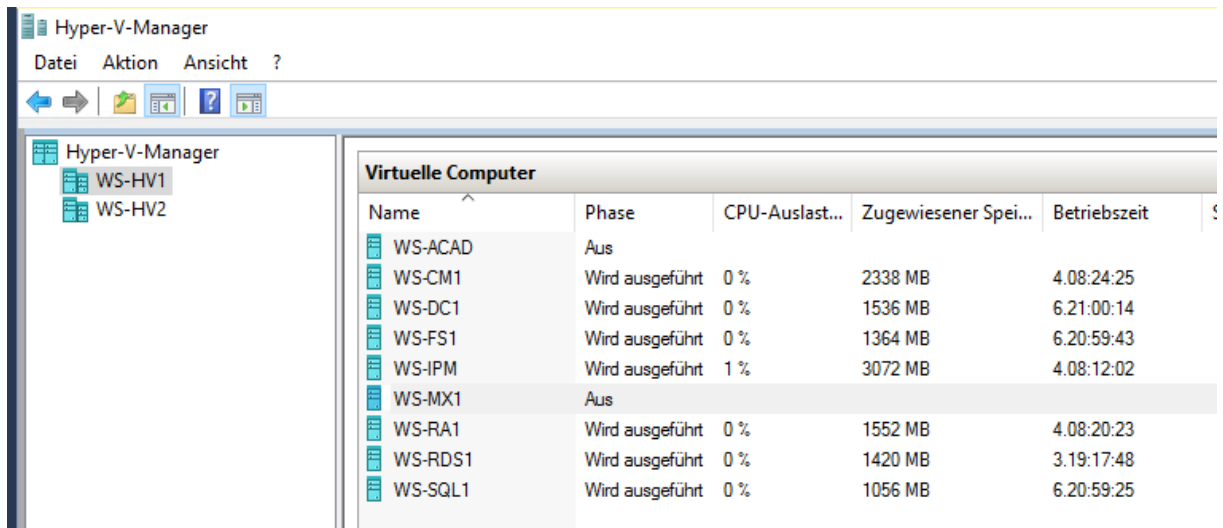
Da ich LAPS im Einsatz habe und den Server ggf. noch einmal benötige, ändere ich das Kennwort des lokalen Admins:



Good Bye:

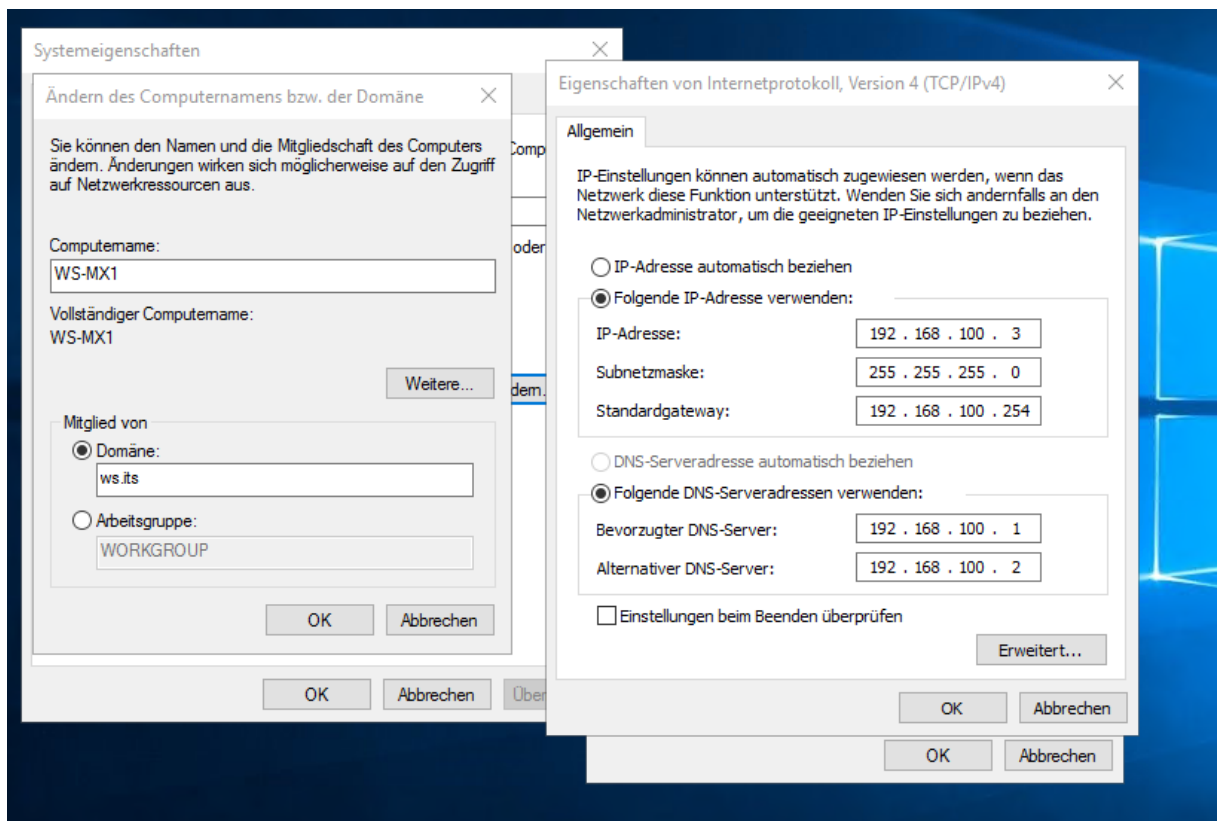


Die beiden Exchange-Server laufen als virtuelle Maschinen:



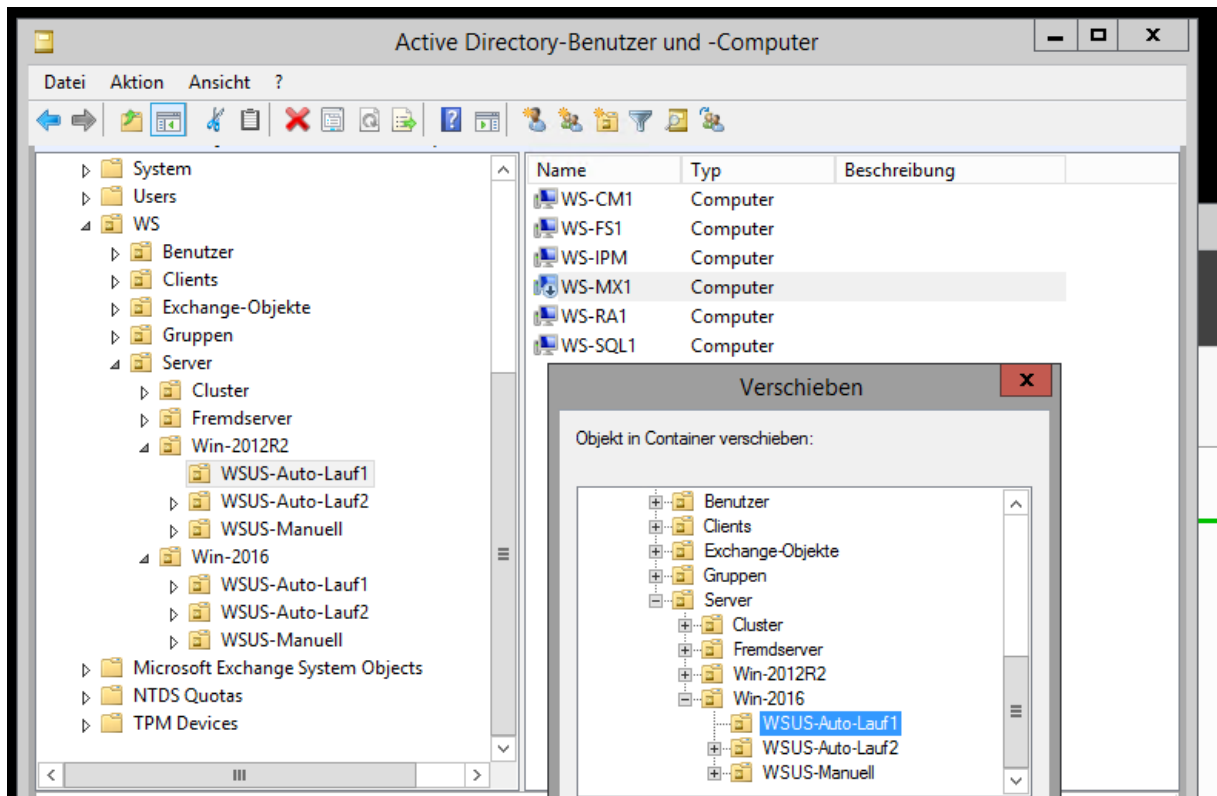
## Bereitstellung des neuen Servers

Der neue Server ist natürlich schon als Image verfügbar. ☺ In diesem sind bereits alle Windows Updates installiert. Als VM gestartet kann ich nun die IP-Adresse und den Namen beim AD-Join wiederverwenden:

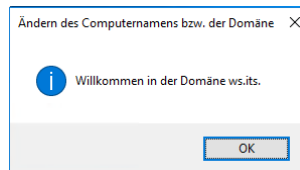


Für die neue Betriebssystemklasse gibt es natürlich schon vorbereitete Organisationseinheiten im AD. Der leere Computer-Account des alten Servers muß also verschoben werden:





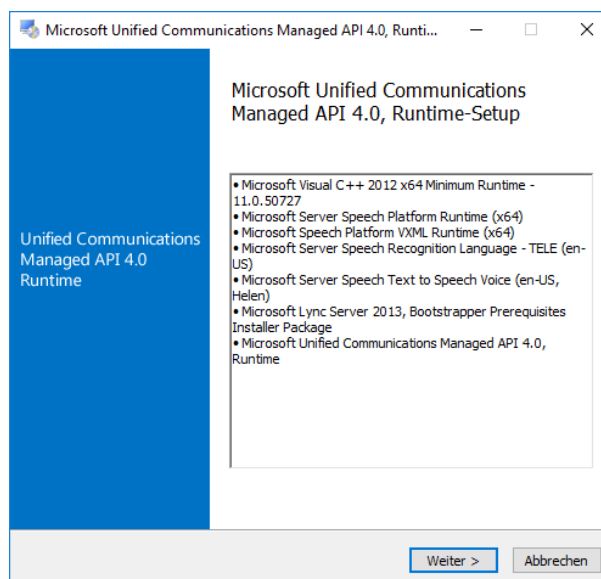
Der DomainJoin klappt:



Das Setup des Exchange Servers erfordert immer noch die Software Unified Communication Managed API, welche ihrerseits auf dem Windows-Feature Media-Foundation aufsetzt. Für andere Bereiche benötige ich weitere Features des OS. Also starte ich die Installation

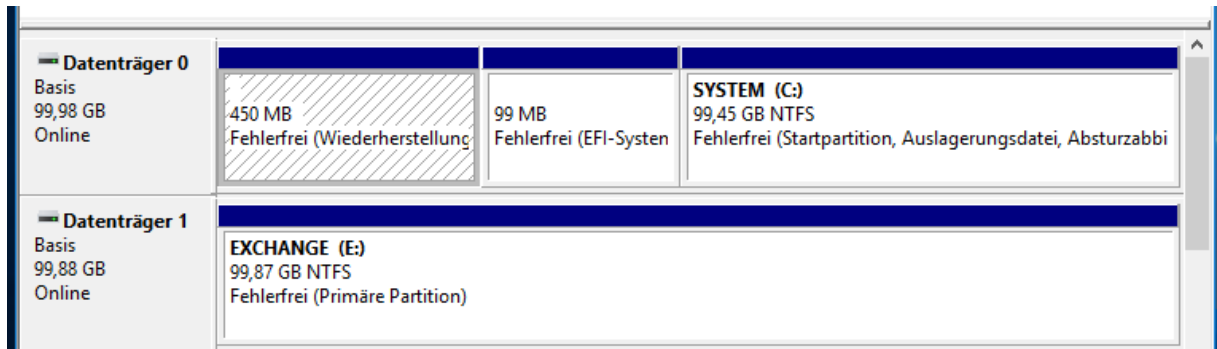
`Install-WindowsFeature RSAT-ADDS, RSAT-AD-PowerShell, Windows-Server-Backup`

Jetzt kann das UCMA installiert werden:

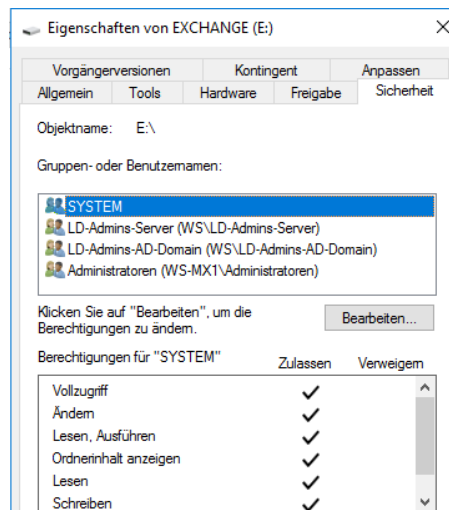


Nach einem Neustart melde ich mich mit einem Account an, der die Gruppenmitgliedschaften Organisations-Admin und Schema-Admin hat.

Zuerst bereite ich die 2. virtuelle Festplatte für die Exchange-Datenbanken vor. Diese bekommt NTFS, da ich außer der Empfehlung von Microsoft keinen Anlaß für ReFS habe:

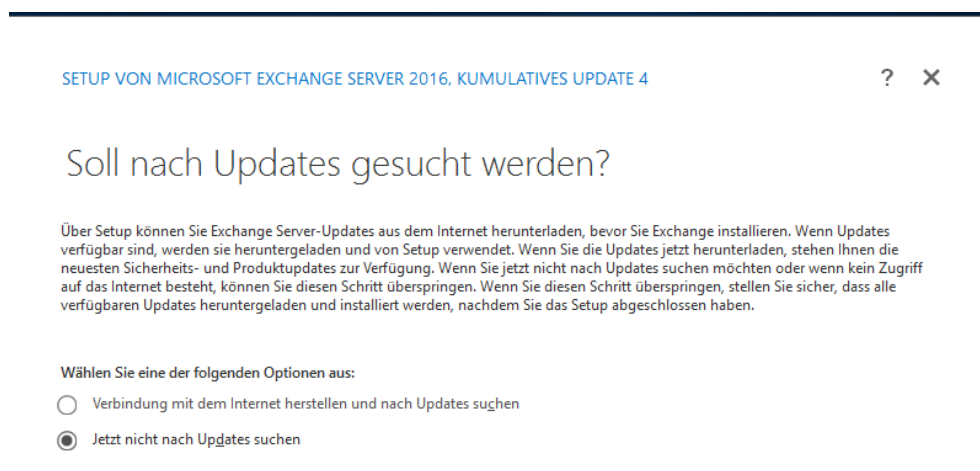


Ein neue Volume wird für den administrativen Zugriff vorbereitet:



Der Windows Server 2016 enthält als Virenschanner den Defender. In der Grundkonfiguration kann dieser das Setup behindern. Daher stoppe ich den Scanner mit einer Einstellung in der lokalen GPO

Das Setup ist als ISO in die VM eingebunden. Ich starte den grafischen Assistenten:



Ich nutze die erweiterte Auswahl:

SETUP VON MICROSOFT EXCHANGE SERVER 2016, KUMULATIVES UPDATE 4

? X

## Empfohlene Einstellungen

- Empfohlene Einstellungen verwenden
- Bei Fehlern sucht Exchange Server automatisch online nach Lösungen und stellt Microsoft Feedback zur Nutzung bereit, um Microsoft dabei zu unterstützen, zukünftige Exchange-Funktionen weiter zu verbessern.
- Empfohlene Einstellungen nicht verwenden
- Konfigurieren Sie diese Einstellungen manuell nach Abschluss der Installation (weitere Informationen finden Sie in der Hilfe).

Der Setup-Assistent soll sich um die notwendigen Rollen kümmern:

SETUP VON MICROSOFT EXCHANGE SERVER 2016, KUMULATIVES UPDATE 4

? X

## Serverrollenauswahl

Wählen Sie die Exchange-Serverrollen aus, die Sie auf diesem Computer installieren möchten:

- Postfachrolle
- Verwaltungspools
- Edge-Transport-Rolle
- Für die Installation von Exchange Server erforderliche Windows Server-Rollen und -Funktionen automatisch installieren

Das Verzeichnis belasse ich beim Standard:

SETUP VON MICROSOFT EXCHANGE SERVER 2016, KUMULATIVES UPDATE 4

? X

## Speicherplatz und Speicherort der Installation

Erforderlicher Speicherplatz: 8149 MB

Verfügbarer Speicherplatz: 84119,3 MB

Geben Sie den Pfad für die Exchange Server-Installation an:

C:\Program Files\Microsoft\Exchange Server\V15

Die Schadsoftwareprüfung lasse ich aktiviert:

SETUP VON MICROSOFT EXCHANGE SERVER 2016, KUMULATIVES UPDATE 4

? X

## Einstellungen zum Schutz vor Schadsoftware

Durch die Überprüfung auf Schadsoftware wird Ihre Nachrichtenumgebung geschützt, da Nachrichten erkannt werden, die Viren oder Spyware enthalten können. Die Überprüfung kann deaktiviert, durch andere Produkte ersetzt oder mit anderen Premiumdiensten kombiniert werden, um alle Schichten zu schützen.

Die Überprüfung auf Schadsoftware ist standardmäßig aktiviert. Sie können sie deaktivieren, wenn Sie ein anderes Produkt zum Schutz vor Schadsoftware verwenden. Wenn Sie die Überprüfung jetzt deaktivieren, können Sie sie nach der Installation von Exchange jederzeit erneut aktivieren.

Prüfung auf Schadsoftware deaktivieren:

- Ja
- Nein

Internetzugriff ist erforderlich, um das aktuelle Antischadsoftware-Modul und Definitionupdates herunterzuladen.

Beim Bereitschaftstest wird nun die vorhandene Installation des Exchange im AD erkannt – und auch das fehlende Schema-Update. Das Aktualisieren der AD belasse ich beim Setup, da meine Infrastruktur recht klein ist:

SETUP VON MICROSOFT EXCHANGE SERVER 2016, KUMULATIVES UPDATE 4

? X

## Bereitschaftsüberprüfung

Der Computer wird überprüft, um festzustellen, ob das Setup fortgesetzt werden kann.

Analyse der Voraussetzungen

100%

**Warnung:**  
 Setup bereitet die Organisation mithilfe von "Setup /PrepareAD" auf Exchange Server 2016 vor. In dieser Topologie wurden keine Exchange Server 2010-Rollen erkannt. Nach diesem Vorgang können Sie keine Exchange Server 2010-Rollen mehr installieren. Weitere Informationen finden Sie unter: [http://technet.microsoft.com/library\(EXCHG.150\)/ms.exch.setupreadiness.NoE14ServerWarning.aspx](http://technet.microsoft.com/library(EXCHG.150)/ms.exch.setupreadiness.NoE14ServerWarning.aspx)

 Exchange

installieren

Das Setup läuft durch. Als Abschluss gibt es einen Neustart:

SETUP VON MICROSOFT EXCHANGE SERVER 2016, KUMULATIVES UPDATE 4

? X

## Setup abgeschlossen

Setup wurde erfolgreich abgeschlossen. Starten Sie den Computer neu, um die Installation von Microsoft Exchange Server abzuschließen.

Weitere Aufgaben nach der Installation finden Sie online unter "<http://go.microsoft.com/fwlink/p/?LinkId=255372>". Sie können nach dem Fertigstellen von Setup auch das Exchange Admin Center starten.

Exchange Admin\_Center starten, nachdem Exchange-Setup fertig gestellt wurde.

Nach dem Neustart kontrolliere ich die SetupLogs und verschiebe diese in meine AdminFreigabe. Ebenso kontrolliere ich den Service-Start und die Eventlogs. Soweit passt alles.

### Konfiguration des neuen Servers

Im EAC wird der neue Server angezeigt:

Unternehmen Office 365

### Exchange Admin Center

Empfänger Server Datenbanken Database Availability Groups Virtuelle Verzeichnisse Zertifikate

Berechtigungen

Verwaltung der Compliance

Organisation

Schutz

NAME	SERVERROLLEN	VERSION
WS-MX1	Postfach, Clientzugriff	Version 15.1 (Build 669.32)
WS-MX2	Postfach, Clientzugriff	Version 15.0 (Build 1263.5)

Die weiteren Konfigurationen nehme ich mit der PowerShell vor. Ich beginne mit den bereits exportieren Zertifikaten für den internen und externen NameSpace:

```
# Zertifikate einspielen
Import-PfxCertificate -FilePath 'C:\Admin\MX-2016-01-22_email.ws.its.pfx' -Password (
    Read-Host -Prompt 'PWD' -AsSecureString) -CertStoreLocation Cert:\LocalMachine\My
Import-PfxCertificate -FilePath 'C:\Admin\MX-2016-08-03-extern.pfx' -Password (
    Read-Host -Prompt 'PWD' -AsSecureString) -CertStoreLocation Cert:\LocalMachine\My

Enable-ExchangeCertificate -Thumbprint 648CFFF368B1590ACFC3C1A744D45D5A34EE7FBD `
    -Services SMTP -Server WS-MX1
Enable-ExchangeCertificate -Thumbprint 23A67FA1CE2613B09EE03378F24992F3A6B0DE6F `
    -Services IIS -Server WS-MX1

Restart-Service MSExchangeTransport
```

Der HTS soll seine Mail.que nicht auf dem Systemlaufwerk ablegen. Also verschiebe ich diese nach e:\

```
# HTS konfigurieren
cd '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
```

Ich möchte, dass der Server sich mit dem externen FQDN meldet, wenn er Mails empfängt. Dafür muss ich den Default-Empfangskonnektor umbauen. Dann kann ich den neuen Konnektor erstellen. Ebenso soll der Server senden dürfen. Dieser Konnektor besteht bereits. Ich nehme also nur den Server in die Liste mit auf:

```
Get-ReceiveConnector -Identity 'WS-MX1\Default Frontend WS-MX1' |
    Set-ReceiveConnector -RemoteIPRanges '192.168.100.1-192.168.100.250',
    '192.168.101.1-192.168.101.254'

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 ws-mx1 -TransportRole FrontEndTransport

Get-SendConnector | Set-SendConnector -SourceTransportServers ws-mx1,ws-mx2
```

Der neue Exchange soll für AntiSpam und AntiMalware konfiguriert werden:

```
cd 'C:\Program Files\Microsoft\Exchange Server\V15\Scripts'
.\Enable-AntimalwareScanning.ps1
Restart-Service MExchangeTransport

.\install-AntispamAgents.ps1
Restart-Service MExchangeTransport
```

Die Logfiles sollen nicht auf dem Systemlaufwerk liegen, damit dieses schneller gesichert und wiederhergestellt werden kann:

```
# Logging
$Pfad = 'E:\Exchange-Logs\'
$exchangeservername = $env:computername

# Move the standard log files for the TransportService:
Set-TransportService -Identity $exchangeservername `
  -ConnectivityLogPath      "$Pfad\Hub\Connectivity" `
  -MessageTrackingLogPath  "$Pfad\MessageTracking" `
  -IrmLogPath               "$Pfad\other\IRMLogs" `
  -ActiveUserStatisticsLogPath "$Pfad\Hub\ActiveUsersStats" `
  -ServerStatisticsLogPath  "$Pfad\Hub\ServerStats" `
  -ReceiveProtocolLogPath   "$Pfad\Hub\ProtocolLog\SmtpReceive" `
  -RoutingTableLogPath      "$Pfad\Hub\Routing" `
  -SendProtocolLogPath      "$Pfad\Hub\ProtocolLog\SmtpSend" `
  -QueueLogPath             "$Pfad\Hub\QueueViewer" `
  -WlmLogPath               "$Pfad\Hub\WLM" `
  -PipelineTracingPath      "$Pfad\Hub\PipelineTracing" `
  -AgentLogPath             "$Pfad\Hub\AgentLog"

# move the path for the PERFMON logs from the C: drive to the L: drive
logman -stop ExchangeDiagnosticsDailyPerformanceLog
logman -update ExchangeDiagnosticsDailyPerformanceLog -o
"$Pfad\Diagnosics\DailyPerformanceLogs\ExchangeDiagnosticsDailyPerformanceLog"
logman -start ExchangeDiagnosticsDailyPerformanceLog
logman -stop ExchangeDiagnosticsPerformanceLog
logman -update ExchangeDiagnosticsPerformanceLog -o
"$Pfad\Diagnosics\PerformanceLogsToBeProcessed\ExchangeDiagnosticsPerformanceLog"
logman -start ExchangeDiagnosticsPerformanceLog

# Move the Log Path using the variable we got
$EdgeSyncServiceConfigVAR = Get-EdgeSyncServiceConfig
Set-EdgeSyncServiceConfig -Identity $EdgeSyncServiceConfigVAR.Identity `
  -LogPath "$Pfad\EdgeSync"

# Move the standard log files for the FrontEndTransportService
Set-FrontendTransportService -Identity $exchangeservername `
  -AgentLogPath             "$Pfad\FrontEnd\AgentLog" `
  -ConnectivityLogPath      "$Pfad\FrontEnd\Connectivity" `
  -ReceiveProtocolLogPath   "$Pfad\FrontEnd\ProtocolLog\SmtpReceive" `
  -SendProtocolLogPath      "$Pfad\FrontEnd\ProtocolLog\SmtpSend"

# Move the log path for the IMAP/pop3 server
Set-ImapSettings -LogFileLocation "$Pfad\Imap4"
Set-PopSettings -LogFileLocation "$Pfad\Pop3"

# Move the logs for the MailBoxServer
Set-MailboxServer -Identity $exchangeservername `
  -CalendarRepairLogPath    "$Pfad\other\Calendar Repair Assistant" `
  -MigrationLogFilePath     "$Pfad\other\Managed Folder Assistant"
```

```
# Move the standard log files for the MailboxTransportService
Set-MailboxTransportService -Identity $exchangeservername `
-ConnectivityLogPath "$pfad\Mailbox\Connectivity" `
-MailboxDeliveryAgentLogPath "$pfad\Mailbox\AgentLog\Delivery" `
-MailboxSubmissionAgentLogPath "$pfad\Mailbox\AgentLog\Submission" `
-ReceiveProtocolLogPath "$pfad\Mailbox\ProtocolLog\SmtpReceive" `
-SendProtocolLogPath "$pfad\Mailbox\ProtocolLog\SmtpSend" `
-PipelineTracingPath "$pfad\Mailbox\PipelineTracing"
```

Nun ist der CAS an der Reihe:

```
# CAS Konfiguration
$servername = "WS-MX1"
$internalhostname = "email.ws.its"
$externalhostname = "email.ws-its.de"
$autodiscoverhostname = "email.ws-its.de"

$owainturl = "https://$internalhostname/owa"
$owaexturl = "https://$externalhostname/owa"
$ecpinturl = "https://$internalhostname/ecp"
$ecpexturl = "https://$externalhostname/ecp"
$ewsinturl = "https://$internalhostname/EWS/Exchange.asmx"
$ewsexturl = "https://$externalhostname/EWS/Exchange.asmx"
$easinturl = "https://$internalhostname/Microsoft-Server-ActiveSync"
$easexturl = "https://$externalhostname/Microsoft-Server-ActiveSync"
$oabinturl = "https://$internalhostname/OAB"
$oabexturl = "https://$externalhostname/OAB"
$mapiinturl = "https://$internalhostname/mapi"
$mapiexturl = "https://$externalhostname/mapi"
$aduri = "https://$autodiscoverhostname/Autodiscover/Autodiscover.xml"

Get-OwaVirtualDirectory -Server $servername | Set-OwaVirtualDirectory -internalurl $owainturl `
-externalurl $owaexturl
Get-EcpVirtualDirectory -server $servername | Set-EcpVirtualDirectory -internalurl $ecpinturl `
-externalurl $ecpexturl
Get-WebServicesVirtualDirectory -server $servername | Set-WebServicesVirtualDirectory `
-internalurl $ewsinturl -externalurl $ewsexturl
Get-ActiveSyncVirtualDirectory -Server $servername | Set-ActiveSyncVirtualDirectory `
-internalurl $easinturl -externalurl $easexturl
Get-OabVirtualDirectory -Server $servername | Set-OabVirtualDirectory -internalurl $oabinturl `
-externalurl $oabexturl
Get-MapiVirtualDirectory -Server $servername | Set-MapiVirtualDirectory `
-externalurl $mapiexturl -internalurl $mapiinturl
Get-OutlookAnywhere -Server $servername | Set-OutlookAnywhere `
-externalhostname $externalhostname -internalhostname $internalhostname `
-ExternalClientsRequireSsl:$true -InternalClientsRequireSsl:$true `
-ExternalClientAuthenticationMethod 'Negotiate'
Get-ClientAccessService $servername | Set-ClientAccessService -AutoDiscoverServiceInternalUri $aduri
```

Als letzte Rolle kommt MBS. Ich benötige neue Datenbanken, in welche ich die bestehenden Postfächer verschieben muss, da der neue Exchange nicht in die alte DAG aufgenommen werden kann. Beim Setup wurde eine neue Datenbank erstellt. Diese verwende ich mit neuem Namen und anderem Pfad weiter:

```
# MBS Konfiguration
Get-MailboxDatabase -Server WS-MX1 | Set-MailboxDatabase -Name DB-System
Get-MailboxDatabase -Identity DB-System | Move-DatabasePath `
-EdbFilePath E:\Exchange\DB-System\DB-System.edb -LogFolderPath E:\Exchange\DB-System\Logs
```

Nun kann ich die neuen DBs erstellen und meine Grundkonfiguration aufspielen:

```
'WSITS','Jungbrunnen','Privat' | ForEach-Object {
    New-MailboxDatabase -Name "DB-$ " `
        -EdbFilePath "E:\Exchange\DB-$ \DB-$ .edb" `
        -LogFolderPath "E:\Exchange\DB-$ \Logs" -Server WS-MX1
    Mount-Database "DB-$_"
}

Get-MailboxDatabase -Server WS-MX1 |
    Set-MailboxDatabase `
        -RetainDeletedItemsUntilBackup $true `
        -DeletedItemRetention 65 `
        -MailboxRetention 30 `
        -ProhibitSendQuota unlimited `
        -ProhibitSendReceiveQuota unlimited `
        -OfflineAddressBook (Get-OfflineAddressBook).name
```

Es sind nun 4 neue DBs einsatzbereit. Die Mailboxen der 3 alten DBs verschiebe ich per PowerShell. Ich beginne mit den System-Mailboxen. Die Migration der PublicFolder ist seit Exchange 2013 kein Problem mehr: ☺

```
Get-MoveRequest | Remove-MoveRequest
Get-Mailbox -Arbitration | New-MoveRequest -TargetDatabase DB-System -BadItemLimit 10
Get-Mailbox sysadm | New-MoveRequest -TargetDatabase DB-System -BadItemLimit 10
Get-Mailbox extest* | New-MoveRequest -TargetDatabase DB-System -BadItemLimit 10

Get-Mailbox -Database Privat | New-MoveRequest -TargetDatabase DB-Privat
Get-Mailbox -Database ws-its | New-MoveRequest -TargetDatabase DB-wsits
Get-Mailbox -Database jungbrunnen | New-MoveRequest -TargetDatabase DB-jungbrunnen

Get-Mailbox -PublicFolder -Identity PF-Technik |
    New-MoveRequest -TargetDatabase DB-WSITS
Get-Mailbox -PublicFolder -Identity PF-Jungbrunnen |
    New-MoveRequest -TargetDatabase DB-Jungbrunnen

Get-MoveRequest | Get-MoveRequestStatistics
Get-MoveRequest | Remove-MoveRequest
```

Die SystemMailboxen des alten Servers benötige ich nicht mehr. Daher lösche ich nun die AD-Userobjekte:

```
Get-Mailbox -Server ws-mx2 -Monitoring | ForEach-Object {
    $CN = $_.name
    $DN = "CN=$CN,CN=Monitoring Mailboxes,CN=Microsoft Exchange System Objects,DC=ws,DC=its"
    Get-ADUser -Identity $DN | Remove-ADObject -Recursive -Confirm:$false
}
```

Die alten Datenbanken sollten nun leer sein. Leider kann ich nur eine löschen. Bei den anderen beiden werden noch aktive Mailboxen gemeldet. Da dies nicht der Fall ist und ich den alten Server aufgebe, lösche ich die AD-Objekte der Datenbanken:

```
Get-MailboxDatabase -Server WS-MX2 | Remove-MailboxDatabase # funktioniert nicht

Remove-MailboxDatabase -Identity privat # Fehler
Dismount-Database Privat
Remove-ADObject -Identity 'CN=Privat,CN=Databases,CN=Exchange Administrative Group
(FYDIBOHF23SPDLT),CN=Administrative Groups,CN=ORG-342356,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=ws,DC=its' -Recursive
Remove-MailboxDatabase -Identity jungbrunnen # funktioniert
Remove-MailboxDatabase -Identity ws-its # Fehler
Dismount-Database ws-its
Remove-ADObject -Identity 'CN=ws-its,CN=Databases,CN=Exchange Administrative Group
(FYDIBOHF23SPDLT),CN=Administrative Groups,CN=ORG-342356,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=ws,DC=its' -Recursive
```



Der alte Server kann nun aus der DAG entfernt werden. Diese ist danach frei – also kann der neue Server aufgenommen werden. Damit bleiben die Witness-Konfigurationen weiter bestehen:

```
# DAG Konfiguration
Remove-DatabaseAvailabilityGroupServer -MailboxServer WS-MX2 -Identity DAG-1
Add-DatabaseAvailabilityGroupServer -MailboxServer WS-MX1 -Identity DAG-1
```

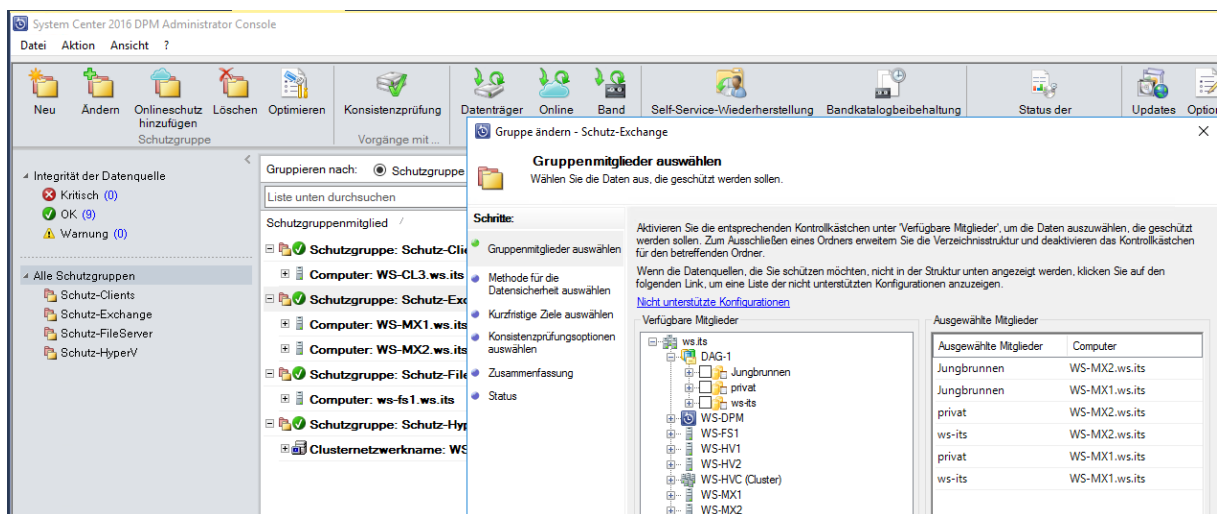
Bis hier hat alles funktioniert. Daher aktiviere ich nun den Server und Exchange:

```
# Aktivierung von MX und WS
slmgr.vbs /ipk 'xxxx-xxxx-xxxx-xxxx-xxxx'
slmgr /ato
Set-ExchangeServer -ProductKey 'xxxx-xxxx-xxxx-xxxx-xxxx' -Identity WS-MX1
```

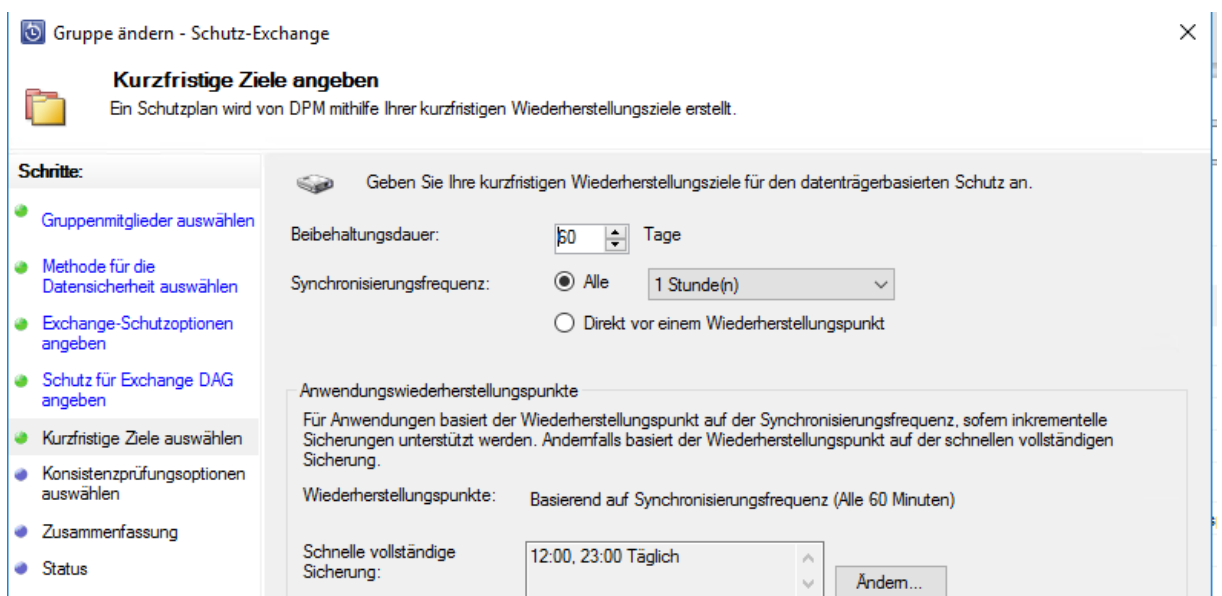
Im DNS registriere ich nun den Host-A-Record mail.ws.its wieder mit der IP des neuen Servers. Ab jetzt kann dieser alle CAS verwendet werden. Im Monitoring nehme ich den Server wieder aktiv. Auch der HAProxy darf nun Mails weiterleiten. Der neue Server ist einsatzbereit.

### Abschalten der Datensicherung

Im DPM 2016 kann ich leider keine Migration der Exchange-DBs abbilden. Daher lösche ich nun die Schutzgruppe, behalte aber zunächst die gesicherten DBs:



Die aktuelle Konfiguration merke ich mir mit diesem Snapshot:



The screenshot shows the 'Schutz-Exchange' protection group with 6 members. A dialog box titled 'Schutz beenden - Schutz-Exchange' is open, displaying a table of tasks and their results:

Aufgabe	Ergebnisse
Jungbrunnen wird entfernt	In Bearbeitung...
Jungbrunnen wird entfernt	In Bearbeitung...
privat wird entfernt	In Bearbeitung...
ws-its wird entfernt	In Bearbeitung...
privat wird entfernt	In Bearbeitung...
ws-its wird entfernt	In Bearbeitung...

Ab jetzt steht keine Datensicherung mehr bereit. In der Produktion hätte ich ein anderes Vorgehen gewählt:

- der DPM hätte bis zuletzt den alten Server gesichert
- parallel hätte ich den neuen Server in eine neue DAG aufgenommen und diese dem DPM ZUSÄTZLICH sichern lassen.

Die Agents kann ich wie gewohnt nicht deinstallieren, also nutze ich auf dem DPM die PowerShell, um die Agents zu entfernen:

The screenshot shows the 'Agents' section in the DPM Administrator Console. A table lists the protected computers:

Computername	Clustername	Domäne	Agent-Status
<b>Geschützte Computer mit Schutz-Agent: (6 Computer)</b>			
WS-CL3	-	ws.its	Unbekannt
WS-FS1	-	ws.its	OK
WS-HV1	WS-HVC.ws.its	ws.its	OK
WS-HV2	WS-HVC.ws.its	ws.its	OK
WS-MX1	DAG-1.ws.its		OK
WS-MX2	DAG-1.ws.its		OK

A context menu is open over the WS-MX1 agent, with 'Deinstallieren' highlighted.

The screenshot shows the 'Installations-Assistent des Schutz-Agents' dialog box. It displays the 'Schritte' (Steps) section:

- Agentbereitstellungsmethode auswählen
- Computer auswählen
- Anmeldeinformationen eingeben
- Methode für Neustart auswählen
- Zusammenfassung
- Installation

The 'Aufgaben' (Tasks) section shows:

Aufgabe	Ergebnisse
Schutz-Agent auf WS-MX1.ws.its installieren	In Bearbeitung...

```

DPM-Verwaltungsshell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Alle Rechte vorbehalten.

Willkommen

Vollständige Cmdlets-Liste: Get-Command
Nur DPM-Cmdlets: Get-DPMCommand
Allgemeine Hilfe: help
Cmdlet-Hilfe: help <Cmdlet-Name> oder <Cmdlet-Name> -?
Cmdlet-Definition: Get-Command <Cmdlet-Name> -Syntax
DPM-Beispielskripts: Get-DPMSampleScript

PS C:\Program Files\Microsoft System Center 2016\DPM\DPM\bin> Remove-ProductionServer.ps1 -DPMServerName ws-dpm.ws.its -
PSName ws-mx1.ws.its
WARNUNG: Die Verbindung mit DPM-Server "ws-dpm.ws.its" wird hergestellt.
Removed ProductionServer successfully
PS C:\Program Files\Microsoft System Center 2016\DPM\DPM\bin> Remove-ProductionServer.ps1 -DPMServerName ws-dpm.ws.its -
PSName ws-mx2.ws.its
WARNUNG: Die Verbindung mit DPM-Server "ws-dpm.ws.its" wird hergestellt.
Removed ProductionServer successfully
PS C:\Program Files\Microsoft System Center 2016\DPM\DPM\bin>
    
```

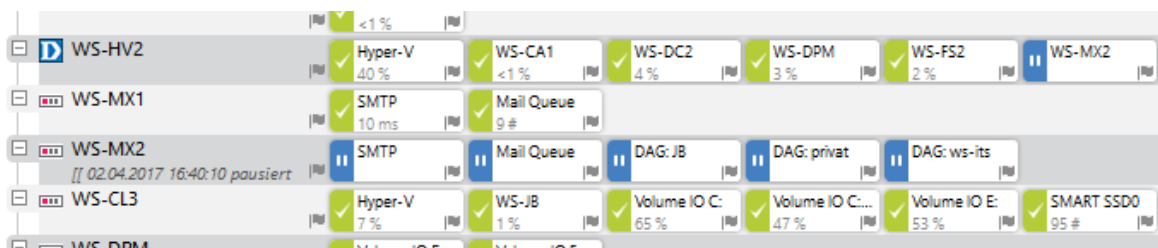
### 3. Migration WS-MX2

#### Entfernen des alten Servers

Beim 2. alten Server ist die Vorgehensweise ähnlich. Ich deaktiviere die Mailweiterleitung im HAProxy an den alten WS-MX2:

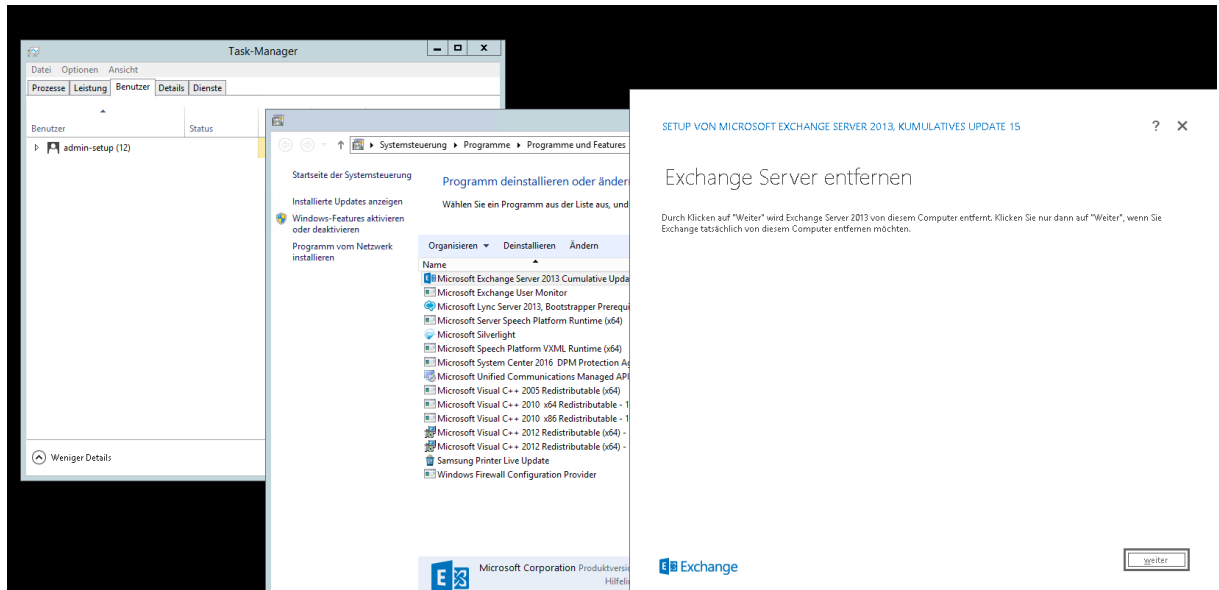
Haproxy		
Backend(s)/Server(s)	Sessions	Status
Backend(s)	(cur/max)	/
Server(s)	age/id	Actions
Client(s) addr:port	age/id	
<b>WS-RA_https_ipvANY</b>	10 / 200	✓
WS-RA1	MAINT	✗
WS-RA2	10	✓
87.138.129.242:32593	36m27s / 0x8025fe200	
87.138.129.242:32596	36m16s / 0x8025fc600	
87.138.129.242:1590	14m5s / 0x8025fde80	
87.138.129.242:1599	13m5s / 0x8025fd780	
87.138.129.242:1081	1m5s / 0x8025fcd00	
87.138.129.242:1082	49s / 0x8025ff700	
87.138.129.242:49525	30s / 0x802600500	
87.138.129.242:1084	5s / 0x802600f80	
87.138.129.242:62555	4s / 0x802601680	
87.138.129.242:49444	0s / 0x802602100	
<b>SMTP_tcp_ipv4</b>	0 / 200	✓
WS-MX1	0	✓
WS-MX2	MAINT	✗
<b>MX-HTTP_http_ipvANY</b>	0 / 200	✓
WS-MX1	0	✓
WS-MX2	MAINT	✗

Im Monitoring pausiere ich den Server WS-MX2:

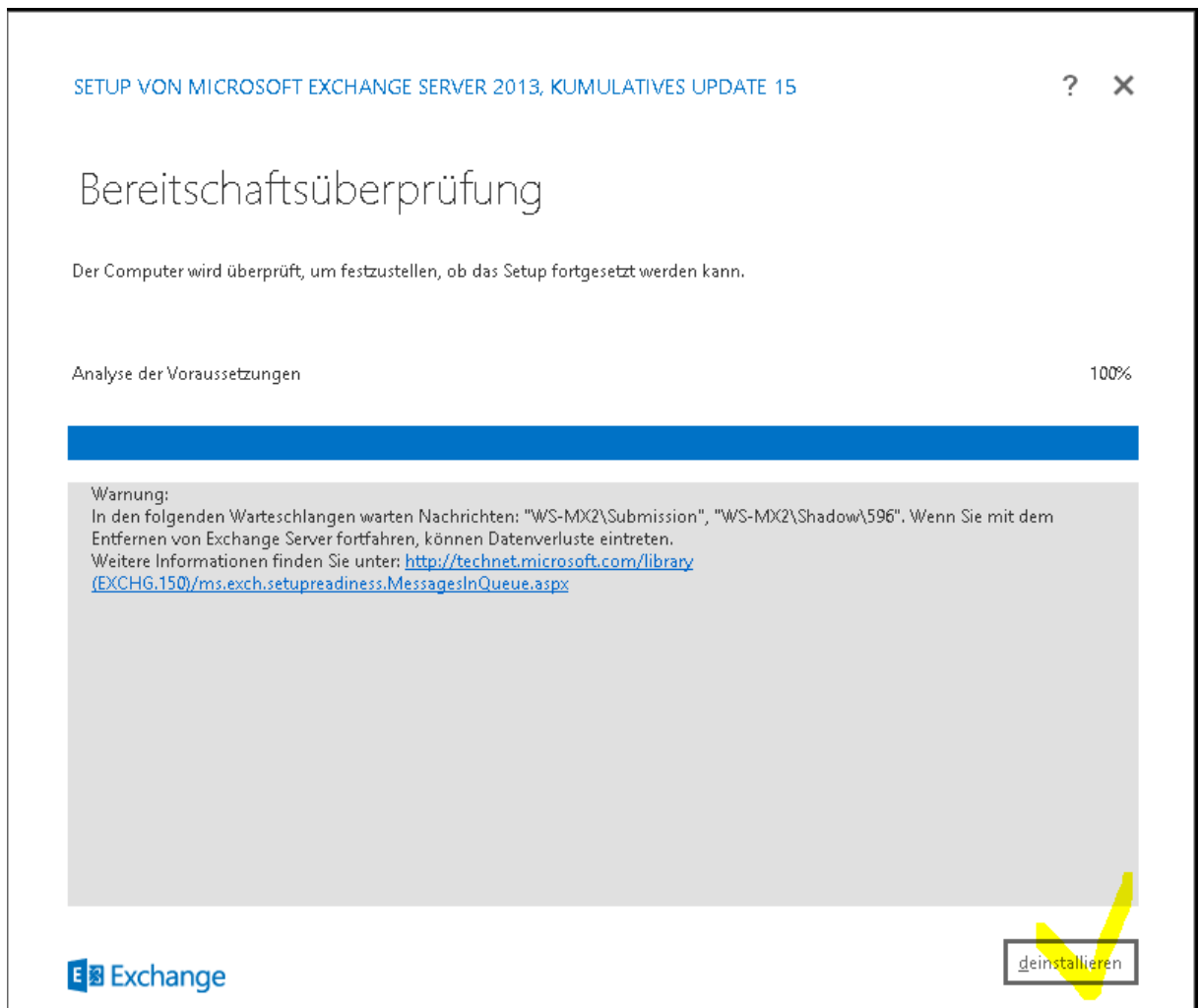


Im DNS lösche ich den Host-A-Record email.ws.its auf 192.168.100.13 (WS-MX2). Damit ist der Server nicht mehr erreichbar. Die Mail-Queue ist leer.

Es wurden bereits alle alten Maildatenbanken gelöscht. Der alte Server kann also entfernt werden:



Eine Warnung zeigt an, dass die ShadowQueue noch Redundanz-Mails enthält. Diese kann ich ignorieren, da der andere Server diese bereits zugestellt hat:



Die Deinstallation läuft fehlerfrei durch:

SETUP VON MICROSOFT EXCHANGE SERVER 2013, KUMULATIVES UPDATE 15

? X

## Setupstatus

Das Setup ist abgeschlossen

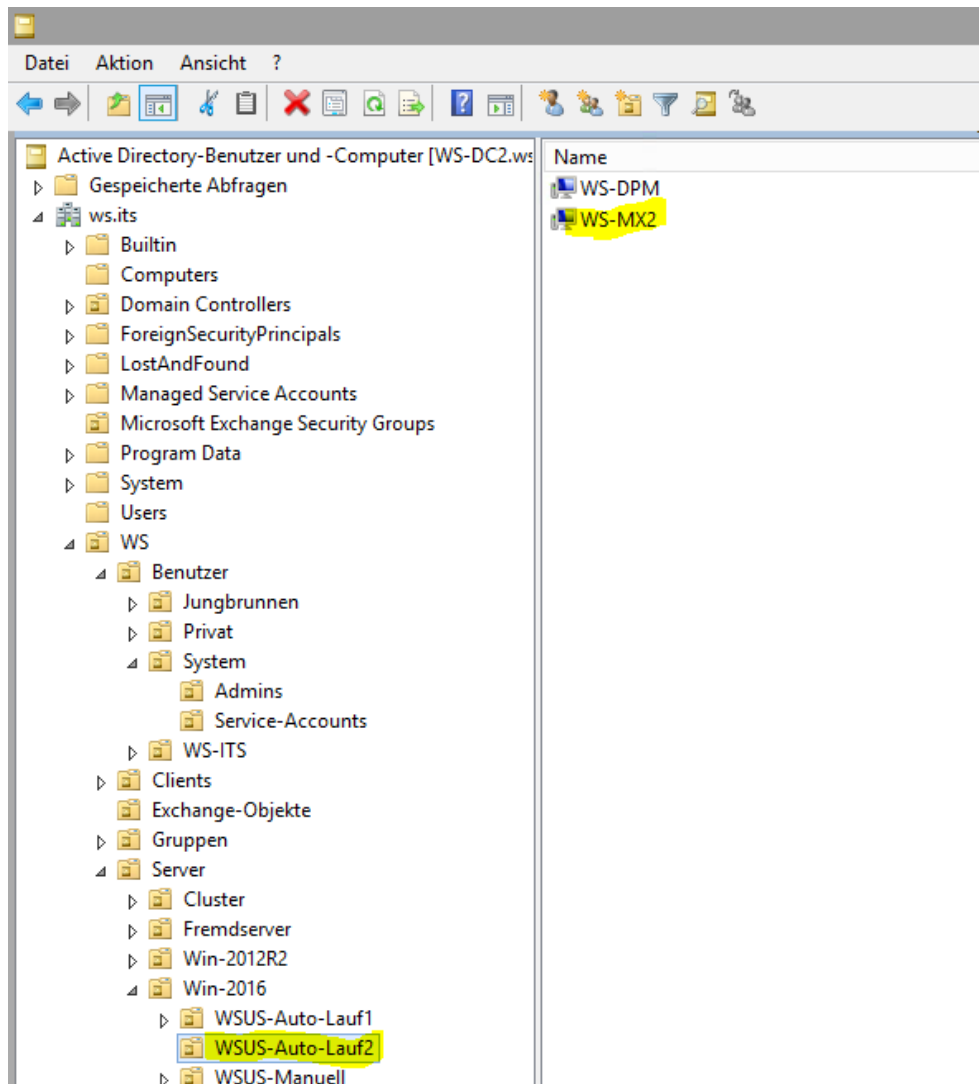
100%

Warnung:  
Um die Dateivorgänge für '[4934D1EA-BE46-48B1-8847-F1AF20E892C1]' abzuschließen, ist ein Neustart erforderlich. Starten Sie den Computer nach Abschluss von Setup neu.

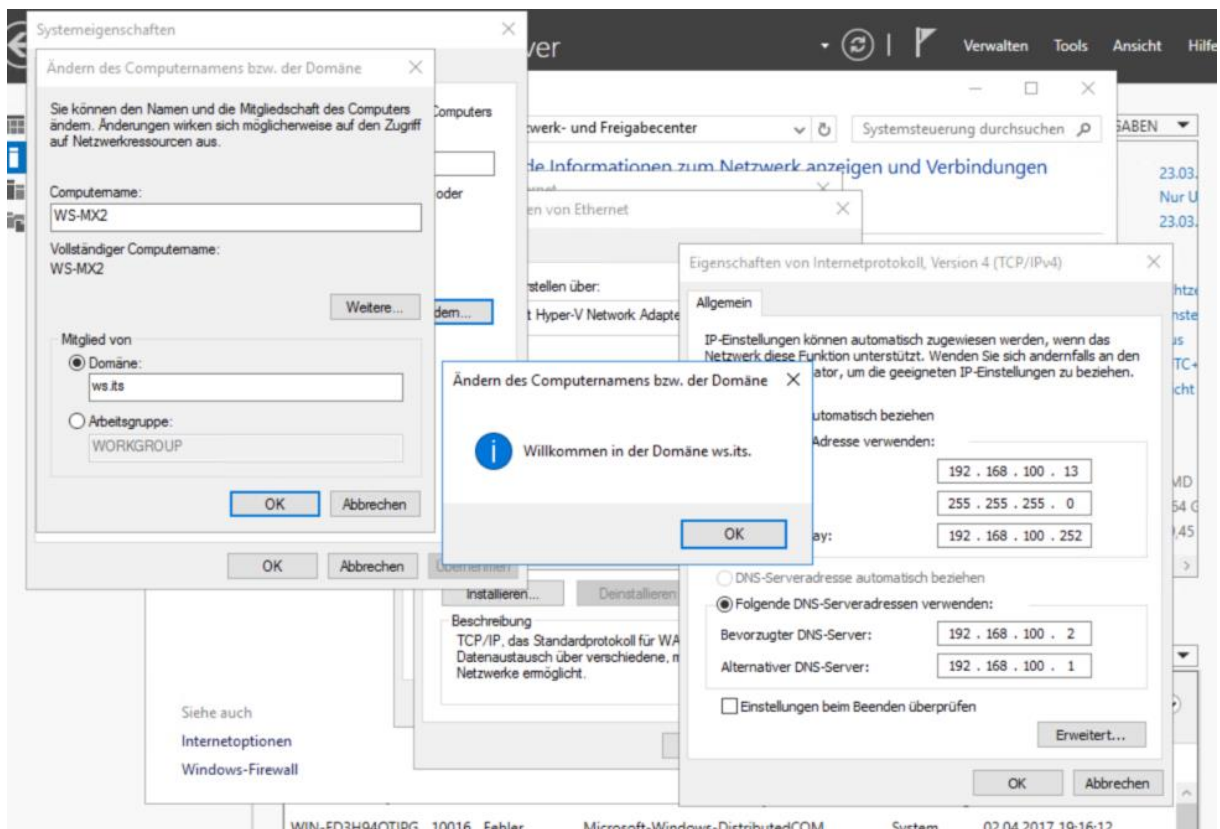
Nach dem Neustart sichere ich noch alle Daten, die ich später wieder gebrauchen kann (Dateien, Zertifikate, geplante Aufgaben, ...), nehme den Server aus der Domäne und schalte ihn aus. Jetzt habe ich eine Exchange-Organisation im nativen Modus 2016 CU4 – bestehend aus einem Mailserver...

### Bereitstellung des neuen Servers

Der neue Server steht als neue VM bereit. Im Active Directory bereite ich das alte Computer-Konto vor:



Der neue Server bekommt die alte IP und den alten Namen und betritt die Domain:



Nach dem Neustart beginne ich mit den Vorbereitungen. Ich benötige einige Windows-Features:

`Install-WindowsFeature Server-Media-Foundation,RSAT-ADDS,RSAT-AD-PowerShell,Windows-Server-Backup`

Danach installiere ich Unified Communication Managed API. Nach einem weiteren Neustart beginne ich die Installation des Exchange mit der GUI. Auch diesem Setup überlasse ich die Installation weiterer Windows-Features:



Das Setup läuft ... leider nur bis hierher:

SETUP VON MICROSOFT EXCHANGE SERVER 2016, KUMULATIVES UPDATE 4

? X

## Setupstatus

Schritt 7 von 14: Postfachrolle: Transportdienst

100%

```
Fehler:
Der folgende Fehler wurde generiert, als "Error.Clear();
if ( ($Server -eq $null) -and ($RolesDatacenter -ne $true) )
{
    Update-RmsSharedIdentity -ServerName $RoleNetBIOSName
}
" ausgeführt wurde: "Microsoft.Exchange.Data.DataValidationException: 'Database' ist für 'UserMailbox' verbindlich.
bei Microsoft.Exchange.Data.Directory.ADDataSession.Save(ADObject instanceToSave, IEnumerable`1 properties, Boolean
bypassValidation)
bei Microsoft.Exchange.Data.Directory.Recipient.ADRecipientObjectSession.Save(ADRecipient instanceToSave, String
callerFilePath, Int32 callerFileLine, String memberName)
bei Microsoft.Exchange.Management.Deployment.UpdateRmsSharedIdentity.Link()
bei Microsoft.Exchange.Management.Deployment.UpdateRmsSharedIdentity.InternalProcessRecord()
bei Microsoft.Exchange.Configuration.Tasks.Task.<ProcessRecord>b__c()
bei Microsoft.Exchange.Configuration.Tasks.Task.InvokeRetryableFunc(String funcName, Action func, Boolean
terminatePipelineIfFailed)".
```



beenden

### Problem: Reparatur der SystemMailboxen

Was ist das Problem? Eingangs habe ich erwähnt, dass ich seit langem Probleme mit den System-Mailboxen hatte. Beim Entfernen der alten Datenbanken kam dieser Effekt wieder zum Vorschein: ich konnte die alten DBs nicht löschen, weil da noch aktive Mailboxen drin wären... Die Datenbanken habe ich dann manuell gelöscht. Und danach zeigen SystemMailboxen nun ihr Problem:

```
192
193 Get-Mailbox -Arbitration

PS C:\Users\stephan-adv> Get-Mailbox -Arbitration

Name                Alias                ServerName           ProhibitSendQuota
-----
SystemMailbox{1f05a927... SystemMailbox{1f0... ws-mx1           Unlimited
WARNING: Das Objekt "ws.its/Microsoft.Exchange.System Objects/SystemMailbox{1f05a927-3d64-4b41-bdf9-831930508563}" wurde beschädigt oder ist mit Microsoft-Supportanforderungen nicht kompatibel und b
efindet sich in einem inkonsistenten Zustand. Folgender Überprüfungsfehler:
WARNING: 'Database' ist für 'UserMailbox' verbindlich.
SystemMailbox{bb558c35... SystemMailbox{bb5... ws-mx1           Unlimited
WARNING: Das Objekt "ws.its/Microsoft.Exchange.System Objects/SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}" wurde beschädigt oder ist mit Microsoft-Supportanforderungen nicht kompatibel und b
efindet sich in einem inkonsistenten Zustand. Folgender Überprüfungsfehler:
WARNING: 'Database' ist für 'UserMailbox' verbindlich.
SystemMailbox{e0dc1c29... SystemMailbox{e0d... ws-mx1           Unlimited
WARNING: Das Objekt "ws.its/Microsoft.Exchange.System Objects/SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823e99}" wurde beschädigt oder ist mit Microsoft-Supportanforderungen nicht kompatibel und b
efindet sich in einem inkonsistenten Zustand. Folgender Überprüfungsfehler:
WARNING: 'Database' ist für 'UserMailbox' verbindlich.
Migration.8f3e7716-201... Migration.8f3e771... ws-mx1           300 MB (314,572,800 bytes)
WARNING: Das Objekt "ws.its/Microsoft.Exchange.System Objects/Migration.8f3e7716-2011-4364-96b1-aba62d229136" wurde beschädigt oder ist mit Microsoft-Supportanforderungen nicht kompatibel und befind
et sich in einem inkonsistenten Zustand. Folgender Überprüfungsfehler:
WARNING: 'Database' ist für 'UserMailbox' verbindlich.
FederatedEmail1.4cf1408... FederatedEmail1.4c... ws-mx1           Unlimited
WARNING: Das Objekt "ws.its/Microsoft.Exchange.System Objects/FederatedEmail1.4cf1408b-8179-4148-93bf-00a95f1e042" wurde beschädigt oder ist mit Microsoft-Supportanforderungen nicht kompatibel und b
efindet sich in einem inkonsistenten Zustand. Folgender Überprüfungsfehler:
WARNING: 'Database' ist für 'UserMailbox' verbindlich.
SystemMailbox{D0E409A0... SystemMailbox{D0E... ws-mx1           Unlimited
```

Interessant dabei ist, dass diese längst in einer anderen DB bereitgestellt waren und das bei der Migration der Mailboxen bei Server WS-MX1 keine Probleme auftraten...

OK, es gibt eine Möglichkeit, die SystemMailboxen neu zu erstellen. Dafür muss ich zuerst die AD-Userobjekte löschen:

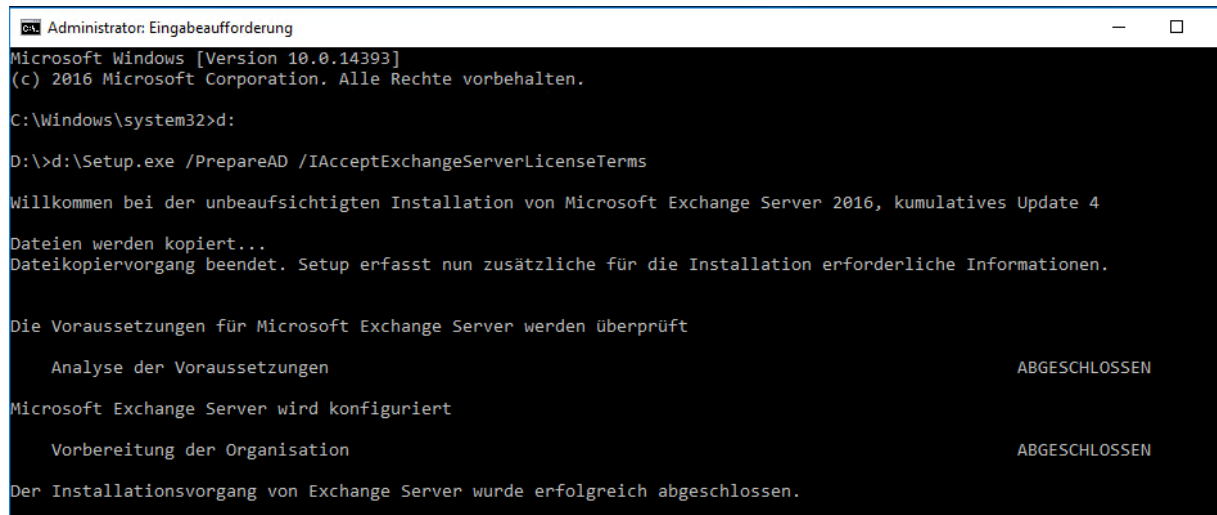
```
Get-Mailbox -Arbitration
```

```
Get-User -Arbitration
```

```
Get-Mailbox -Arbitration | ForEach-Object {  
    $CN = $_.name  
    $DN = "CN=$CN,CN=Microsoft Exchange System Objects,DC=ws,DC=its"  
    Get-ADUser -Identity $DN | Remove-ADObject -Recursive  
}
```

Danach kann das Setup im Modus PrepareAD die Mailboxuser wieder erstellen:

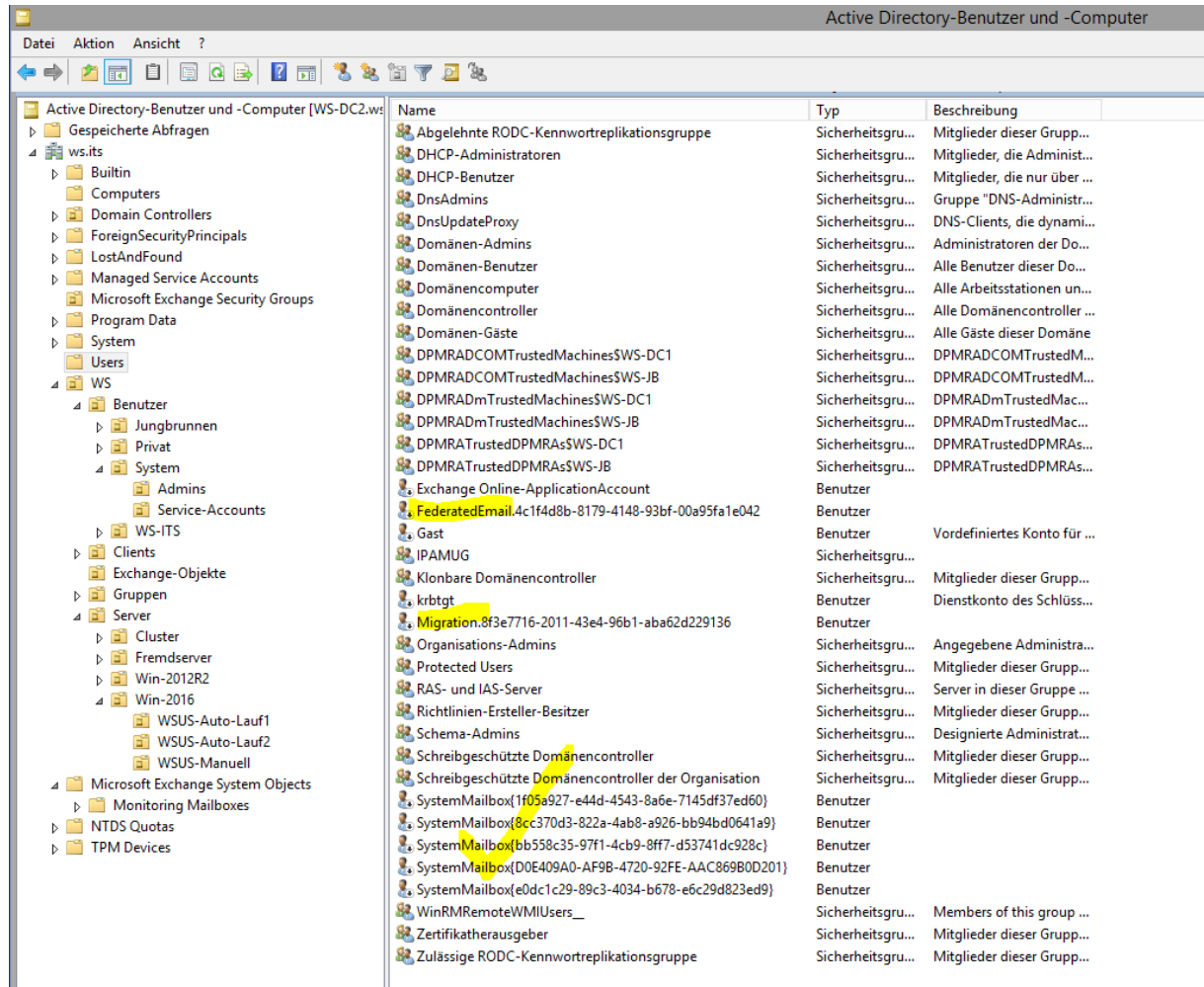
```
d:\Setup.exe /PrepareAD /IAcceptExchangeServerLicenseTerms
```



```
Administrator: Eingabeaufforderung  
Microsoft Windows [Version 10.0.14393]  
(c) 2016 Microsoft Corporation. Alle Rechte vorbehalten.  
C:\Windows\system32>d:  
D:\>d:\Setup.exe /PrepareAD /IAcceptExchangeServerLicenseTerms  
Willkommen bei der unbeaufsichtigten Installation von Microsoft Exchange Server 2016, kumulatives Update 4  
Dateien werden kopiert...  
Dateikopiervorgang beendet. Setup erfasst nun zusätzliche für die Installation erforderliche Informationen.  
  
Die Voraussetzungen für Microsoft Exchange Server werden überprüft  
    Analyse der Voraussetzungen                                ABGESCHLOSSEN  
Microsoft Exchange Server wird konfiguriert  
    Vorbereitung der Organisation                            ABGESCHLOSSEN  
Der Installationsvorgang von Exchange Server wurde erfolgreich abgeschlossen.
```

Eine Sichtprüfung zeigt die AD-Userobjekte an:





Name	Typ	Beschreibung
Abgelehnte RODC-Kennwortreplikationsgruppe	Sicherheitsgru...	Mitglieder dieser Grupp...
DHCP-Administratoren	Sicherheitsgru...	Mitglieder, die Administ...
DHCP-Benutzer	Sicherheitsgru...	Mitglieder, die nur über ...
DnsAdmins	Sicherheitsgru...	Gruppe "DNS-Administr...
DnsUpdateProxy	Sicherheitsgru...	DNS-Clients, die dynami...
Domänen-Admins	Sicherheitsgru...	Administratoren der Do...
Domänen-Benutzer	Sicherheitsgru...	Alle Benutzer dieser Do...
Domänencomputer	Sicherheitsgru...	Alle Arbeitsstationen un...
Domänencontroller	Sicherheitsgru...	Alle Domänencontroller ...
Domänen-Gäste	Sicherheitsgru...	Alle Gäste dieser Domäne
DPMRADCOMTrustedMachines\$WS-DC1	Sicherheitsgru...	DPMRADCOMTrustedM...
DPMRADCOMTrustedMachines\$WS-JB	Sicherheitsgru...	DPMRADCOMTrustedM...
DPMRADmTrustedMachines\$WS-DC1	Sicherheitsgru...	DPMRADmTrustedMac...
DPMRADmTrustedMachines\$WS-JB	Sicherheitsgru...	DPMRADmTrustedMac...
DPMRATTrustedDPMRAs\$WS-DC1	Sicherheitsgru...	DPMRATTrustedDPMRAs...
DPMRATTrustedDPMRAs\$WS-JB	Sicherheitsgru...	DPMRATTrustedDPMRAs...
Exchange Online-ApplicationAccount	Benutzer	
FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042	Benutzer	
Gast	Benutzer	Vordefiniertes Konto für ...
IPAMUG	Sicherheitsgru...	
Klonbare Domänencontroller	Sicherheitsgru...	Mitglieder dieser Grupp...
krbtgt	Benutzer	Dienstkonto des Schlüss...
Migration.8f3e7716-2011-43e4-96b1-aba62d229136	Benutzer	
Organisations-Admins	Sicherheitsgru...	Angegebene Administra...
Protected Users	Sicherheitsgru...	Mitglieder dieser Grupp...
RAS- und IAS-Server	Sicherheitsgru...	Server in dieser Gruppe ...
Richtlinien-Ersteller-Besitzer	Sicherheitsgru...	Mitglieder dieser Grupp...
Schema-Admins	Sicherheitsgru...	Designierte Administrat...
Schreibgeschützte Domänencontroller	Sicherheitsgru...	Mitglieder dieser Grupp...
Schreibgeschützte Domänencontroller der Organisation	Sicherheitsgru...	Mitglieder dieser Grupp...
SystemMailbox{1f05a927-e44d-4543-8a6e-7145df37ed60}	Benutzer	
SystemMailbox{8cc370d3-822a-4ab8-a926-bb94bd0641a9}	Benutzer	
SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}	Benutzer	
SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201}	Benutzer	
SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}	Benutzer	
WinRMRemoteWMIUsers_	Sicherheitsgru...	Members of this group ...
Zertifikat herausgeber	Sicherheitsgru...	Mitglieder dieser Grupp...
Zulässige RODC-Kennwortreplikationsgruppe	Sicherheitsgru...	Mitglieder dieser Grupp...

Ich starte das Setup neu. Dabei wird die vorherige teilweise Installation erkannt und wiederaufgenommen. Das Setup läuft nun vollständig durch. 😊

## Konfiguration des neuen Servers

Der neue Server benötigt noch ein wenig Konfiguration. Das Script des ersten Servers dient nun als Vorlage!

Zuerst spiele ich die Zertifikate aus pdx-Files ein:

```
# Zertifikate einspielen
Import-PfxCertificate -FilePath 'C:\Admin\MX-2016-01-22_email.ws.its.pfx' `
-Password (Read-Host -Prompt 'PWD' -AsSecureString) -CertStoreLocation Cert:\LocalMachine\My
Import-PfxCertificate -FilePath 'C:\Admin\MX-2016-08-03-extern.pfx' `
-Password (Read-Host -Prompt 'PWD' -AsSecureString) -CertStoreLocation Cert:\LocalMachine\My

Enable-ExchangeCertificate -Thumbprint 648CFFF368B1590ACFC3C1A744D45D5A34EE7FBD `
-Services SMTP -Server WS-MX1
Enable-ExchangeCertificate -Thumbprint 23A67FA1CE2613B09EE03378F24992F3A6B0DE6F `
-Services IIS -Server WS-MX1

Restart-Service MSExchangeTransport
```

Die Mail.que des Transportserver lege ich auch auf E:\ ab (Das Laufwerk habe ich zwischenzeitlich bereitgestellt...)

```
# HTS konfigurieren
cd '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
```

Wie beim ersten Server erstelle ich einen neuen Empfangskonnektor, der auf den externen FQDN antwortet. Dafür muss zuerst der Default-Konnektor editiert werden. Der Sendekonnektor wird wieder auf beide Server gesetzt:

```
Get-ReceiveConnector -Identity 'WS-MX2\Default Frontend WS-MX2' |
    Set-ReceiveConnector -RemoteIPRanges '192.168.100.1-192.168.100.250', `
        '192.168.101.1-192.168.101.254'

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 ws-mx2 -TransportRole FrontEndTransport

Get-SendConnector | Set-SendConnector -SourceTransportServers ws-mx1,ws-mx2
```

Ein wenig AntiSpam und AntiVirus dazu und der HTS ist bereit:

```
cd 'C:\Program Files\Microsoft\Exchange Server\V15\Scripts'
.\Enable-AntimalwareScanning.ps1
Restart-Service MSExchangeTransport

.\install-AntispamAgents.ps1
Restart-Service MSExchangeTransport
```

Alle relevanten Protokolle leite ich nach e:\ um:

```
# Logging
$Pfad = 'E:\Exchange-Logs\'
$exchangeservername = $env:computername

# Move the standard log files for the TransportService:
Set-TransportService -Identity $exchangeservername `
    -ConnectivityLogPath "$Pfad\Hub\Connectivity" `
    -MessageTrackingLogPath "$Pfad\Hub\MessageTracking" `
    -IrmLogPath "$Pfad\Hub\IRMLogs" `
    -ActiveUserStatisticsLogPath "$Pfad\Hub\ActiveUsersStats" `
    -ServerStatisticsLogPath "$Pfad\Hub\ServerStats" `
    -ReceiveProtocolLogPath "$Pfad\Hub\ProtocolLog\SmtpReceive" `
    -RoutingTableLogPath "$Pfad\Hub\Routing" `
    -SendProtocolLogPath "$Pfad\Hub\ProtocolLog\SmtpSend" `
    -QueueLogPath "$Pfad\Hub\QueueViewer" `
    -WlmLogPath "$Pfad\Hub\WLM" `
    -PipelineTracingPath "$Pfad\Hub\PipelineTracing" `
    -AgentLogPath "$Pfad\Hub\AgentLog"

# move the path for the PERFMON logs from the C: drive to the L: drive
logman -stop ExchangeDiagnosticsDailyPerformanceLog
logman -update ExchangeDiagnosticsDailyPerformanceLog -o
"$Pfad\Diagnosics\DailyPerformanceLogs\ExchangeDiagnosticsDailyPerformanceLog"
logman -start ExchangeDiagnosticsDailyPerformanceLog
logman -stop ExchangeDiagnosticsPerformanceLog
```

```

logman -update ExchangeDiagnosticsPerformanceLog -o
"$pfad\Diagnosics\PerformanceLogsToBeProcessed\ExchangeDiagnosticsPerformanceLog"
logman -start ExchangeDiagnosticsPerformanceLog

# Move the Log Path using the variable we got
$EdgeSyncServiceConfigVAR = Get-EdgeSyncServiceConfig
Set-EdgeSyncServiceConfig -Identity $EdgeSyncServiceConfigVAR.Identity `
-LogPath "$pfad\EdgeSync"

# Move the standard log files for the FrontEndTransportService
Set-FrontendTransportService -Identity $exchangeservername `
-AgentLogPath "$pfad\FrontEnd\AgentLog" `
-ConnectivityLogPath "$pfad\FrontEnd\Connectivity" `
-ReceiveProtocolLogPath "$pfad\FrontEnd\ProtocolLog\SmtptReceive" `
-SendProtocolLogPath "$pfad\FrontEnd\ProtocolLog\SmtptSend"

# Move the log path for the IMAP/pop3 server
Set-ImapSettings -LogFileLocation "$pfad\Imap4"
Set-PopSettings -LogFileLocation "$Pfad\Pop3"

# Move the logs for the MailBoxServer
Set-MailboxServer -Identity $exchangeservername `
-CalendarRepairLogPath "$pfad\other\Calendar Repair Assistant" `
-MigrationLogFileLocation "$pfad\other\Managed Folder Assistant"

# Move the standard log files for the MailboxTransportService
Set-MailboxTransportService -Identity $exchangeservername `
-ConnectivityLogPath "$pfad\Mailbox\Connectivity" `
-MailboxDeliveryAgentLogPath "$pfad\Mailbox\AgentLog\Delivery" `
-MailboxSubmissionAgentLogPath "$pfad\Mailbox\AgentLog\Submission" `
-ReceiveProtocolLogPath "$pfad\Mailbox\ProtocolLog\SmtptReceive" `
-SendProtocolLogPath "$pfad\Mailbox\ProtocolLog\SmtptSend" `
-PipelineTracingPath "$pfad\Mailbox\PipelineTracing"

```

Der CAS wird gleichgezogen:

```

# CAS Konfiguration
$servername = "WS-MX2"
$internalhostname = "email.ws.its"
$externalhostname = "email.ws-its.de"
$autodiscoverhostname = "email.ws-its.de"

$owainturl = "https://$internalhostname/owa"
$owaexturl = "https://$externalhostname/owa"
$ecpinturl = "https://$internalhostname/ecp"
$ecpexturl = "https://$externalhostname/ecp"
$ewsinturl = "https://$internalhostname/EWS/Exchange.asmx"
$ewsexturl = "https://$externalhostname/EWS/Exchange.asmx"
$easinturl = "https://$internalhostname/Microsoft-Server-ActiveSync"
$easexturl = "https://$externalhostname/Microsoft-Server-ActiveSync"
$soabinturl = "https://$internalhostname/OAB"
$soabexturl = "https://$externalhostname/OAB"
$mapiinturl = "https://$internalhostname/mapi"
$mapiexturl = "https://$externalhostname/mapi"
$aduri = "https://$autodiscoverhostname/Autodiscover/Autodiscover.xml"

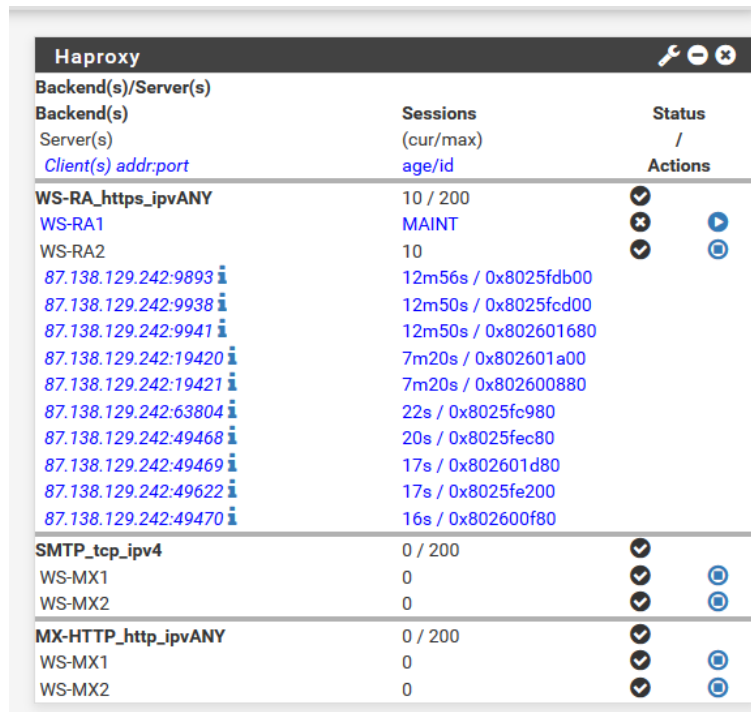
Get-OwaVirtualDirectory -Server $servername | Set-OwaVirtualDirectory `
-internalurl $owainturl -externalurl $owaexturl
Get-EcpVirtualDirectory -server $servername | Set-EcpVirtualDirectory `
-internalurl $ecpinturl -externalurl $ecpexturl

```

```

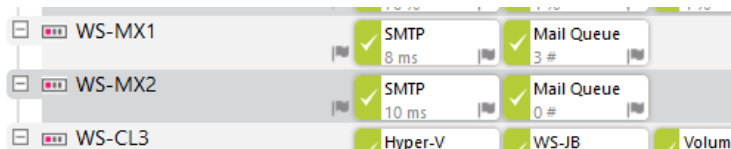
Get-WebServicesVirtualDirectory -server $servername |
    Set-WebServicesVirtualDirectory -internalurl $ewsinturl -externalurl $ewsexturl
Get-ActiveSyncVirtualDirectory -Server $servername |
    Set-ActiveSyncVirtualDirectory -internalurl $easinturl -externalurl $easexturl
Get-OabVirtualDirectory -Server $servername |
    Set-OabVirtualDirectory -internalurl $oabinturl -externalurl $oabexturl
Get-MapiVirtualDirectory -Server $servername |
    Set-MapiVirtualDirectory -externalurl $mapiexturl -internalurl $mapiinturl
Get-OutlookAnywhere -Server $servername | Set-OutlookAnywhere `
    -externalhostname $externalhostname `
    -internalhostname $internalhostname `
    -ExternalClientsRequireSsl:$true `
    -InternalClientsRequireSsl:$true `
    -ExternalClientAuthenticationMethod 'Negotiate'
Get-ClientAccessService $servername |
    Set-ClientAccessService -AutoDiscoverServiceInternalUri $aduri
    
```

Im DNS registriere ich nun wieder einen Host-A-Record für email.ws.its auf die IP des Servers WS-MX2. Damit ist der Server aus Sicht des WAP-Clusters für https wieder erreichbar. Im HAProxy nehme ich die Maintenance für SMTP wieder raus. Damit kann WS-MX2 Mails von außen empfangen:



Backend(s)/Server(s)	Sessions (cur/max)	Status	Actions
<b>WS-RA_https_ipvANY</b>	10 / 200	✓	
WS-RA1	MAINT	✗	⏸
WS-RA2	10	✓	⏸
87.138.129.242:9893	12m56s / 0x8025fdb00		
87.138.129.242:9938	12m50s / 0x8025fcd00		
87.138.129.242:9941	12m50s / 0x802601680		
87.138.129.242:19420	7m20s / 0x802601a00		
87.138.129.242:19421	7m20s / 0x802600880		
87.138.129.242:63804	22s / 0x8025fc980		
87.138.129.242:49468	20s / 0x8025fec80		
87.138.129.242:49469	17s / 0x802601d80		
87.138.129.242:49622	17s / 0x8025fe200		
87.138.129.242:49470	16s / 0x802600f80		
<b>SMTP_tcp_ipv4</b>	0 / 200	✓	
WS-MX1	0	✓	⏸
WS-MX2	0	✓	⏸
<b>MX-HTTP_http_ipvANY</b>	0 / 200	✓	
WS-MX1	0	✓	⏸
WS-MX2	0	✓	⏸

Im PRTG-Monitoring aktiviere ich die Überwachung wieder:



WS-MX1	SMTP	8 ms	Mail Queue	3 #
WS-MX2	SMTP	10 ms	Mail Queue	0 #
WS-CL3	Hyper-V		WS-JB	Volum

Der Server steht nun für Clients und SMTP-Server bereit. Allein die Konfiguration der Mailboxen fehlt noch. Beim Setup wurde eine leere Datenbank auf dem neuen Server erstellt. Diese lösche ich:

```

# MBS Konfiguration
Get-MailboxDatabase -Server WS-MX2 | Remove-MailboxDatabase
    
```

Nun kann ich die DAG konfigurieren. Ich nehme den Server in die Gruppe auf:

```

# DAG Konfiguration
Add-DatabaseAvailabilityGroupServer -MailboxServer WS-MX2 -Identity DAG-1
    
```

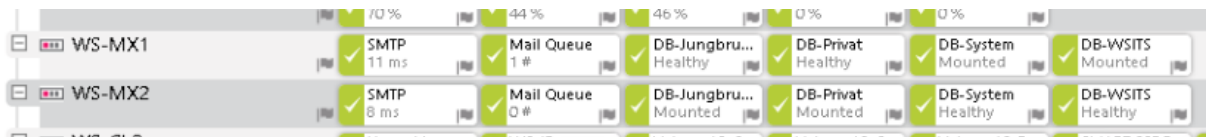
Nachdem der Server in der DAG angekommen ist, konfiguriere ich für die 4 Datenbanken auf WS-MX1 die Kopie auf WS-MX2:

```
Get-MailboxDatabase -Server WS-MX1 | ForEach-Object {
    Add-MailboxDatabaseCopy -MailboxServer WS-MX2 -Identity $_.name
}
```

Die Datenbanken werden initial kopiert und die Replikation beginnt. Zur besseren Lastverteilung setze ich 2 der 4 Datenbanken auf WS-MX2 als primär:

```
Set-MailboxDatabaseCopy -Identity DB-Jungbrunnen\WS-MX2 -ActivationPreference 1
Set-MailboxDatabaseCopy -Identity DB-Privat\WS-MX2 -ActivationPreference 1
```

Die Server gleichen innerhalb der DAG die Datenbanken automatisch aus. Nach einiger Zeit sind also auf jedem der beiden Server je 2 Datenbanken online geschaltet. Dafür erweitere ich nun mein PRTG-Monitoring:



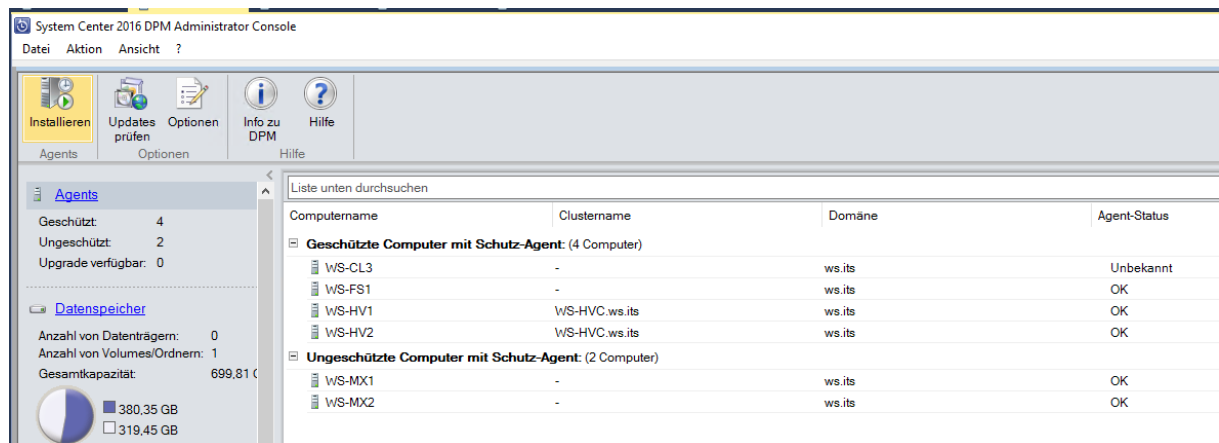
Server	SMTP	Mail Queue	DB-Jungbrunnen	DB-Privat	DB-System	DB-WSITS
WS-MX1	11 ms	1 #	Healthy	Healthy	Mounted	Mounted
WS-MX2	8 ms	0 #	Mounted	Mounted	Healthy	Healthy

Weitere Anpassungen können mit der Zeit erforderlich werden. Aktuell habe ich nun aber 2 Exchange Server 2016 CU4, die auf Windows Server 2016 laufen und alle relevanten Funktionen von Exchange redundant abbilden.

Bei der Konfiguration des 2. Servers habe ich nicht alle Schritte wiederholt. Natürlich habe ich auch hier den Windows Defender beim Setup angehalten, Windows Updates geprüft und eventlogs kontrolliert. 😊

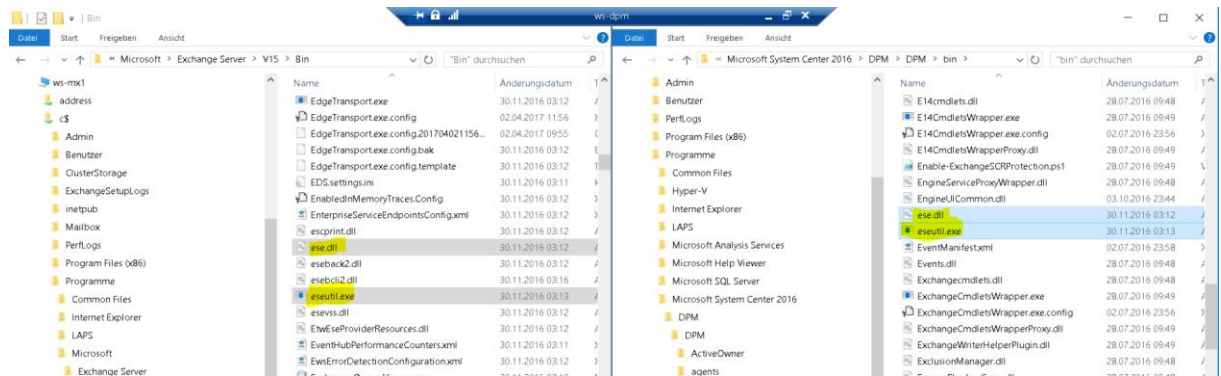
### Konfiguration der Datensicherung

Es bleibt noch die Thematik der Datensicherung offen. Auf beiden Servern installiere ich den Agent des DPM 2016 und verbinde diese mit meinem Sicherungsserver:

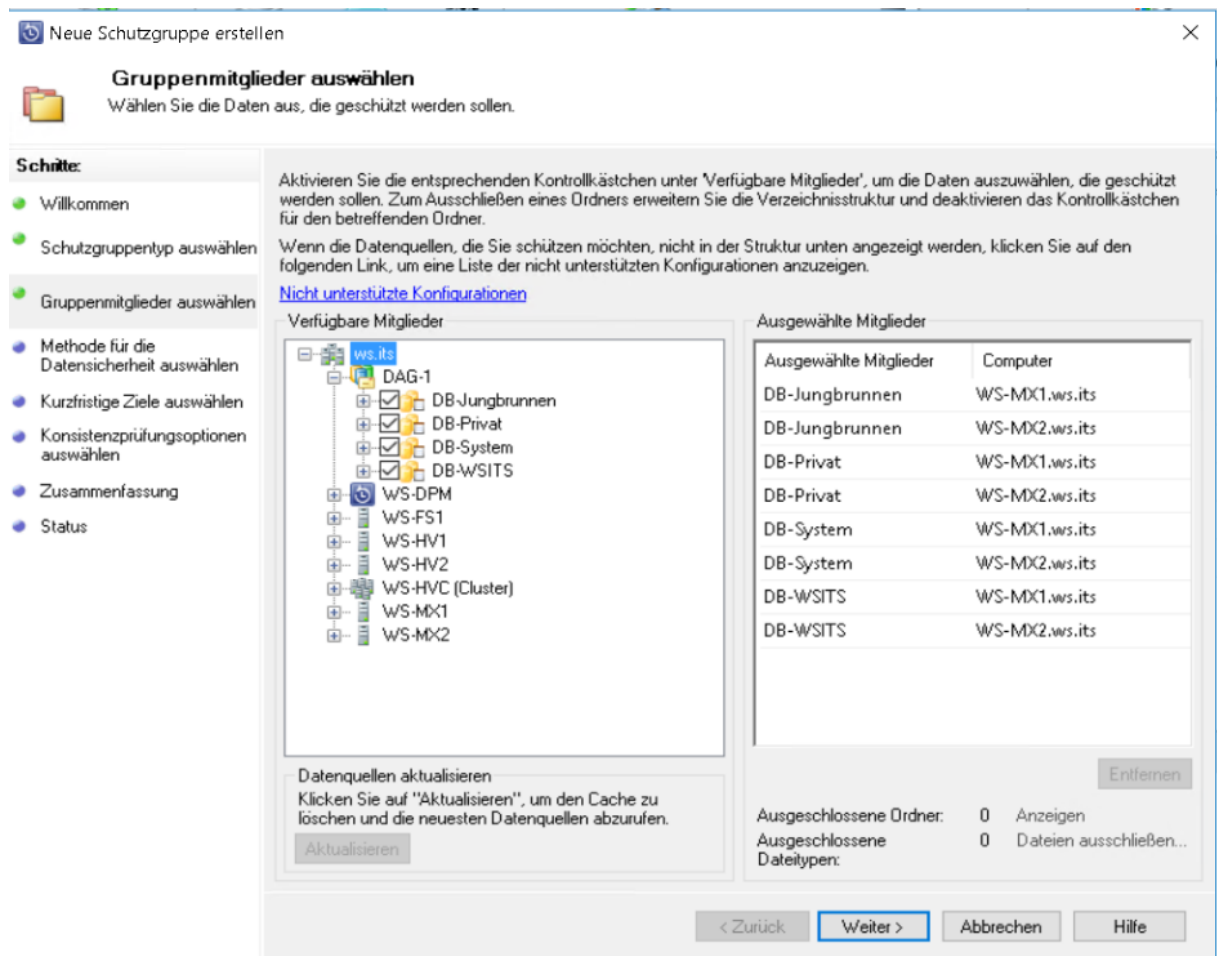


Agenten	Computers	Agent-Status
Geschützt: 4	<b>Geschützte Computer mit Schutz-Agent: (4 Computer)</b>	
Ungeschützt: 2	WS-CL3	Unbekannt
Upgrade verfügbar: 0	WS-FS1	OK
	WS-HV1	OK
	WS-HV2	OK
	<b>Ungeschützte Computer mit Schutz-Agent: (2 Computer)</b>	
	WS-MX1	OK
	WS-MX2	OK

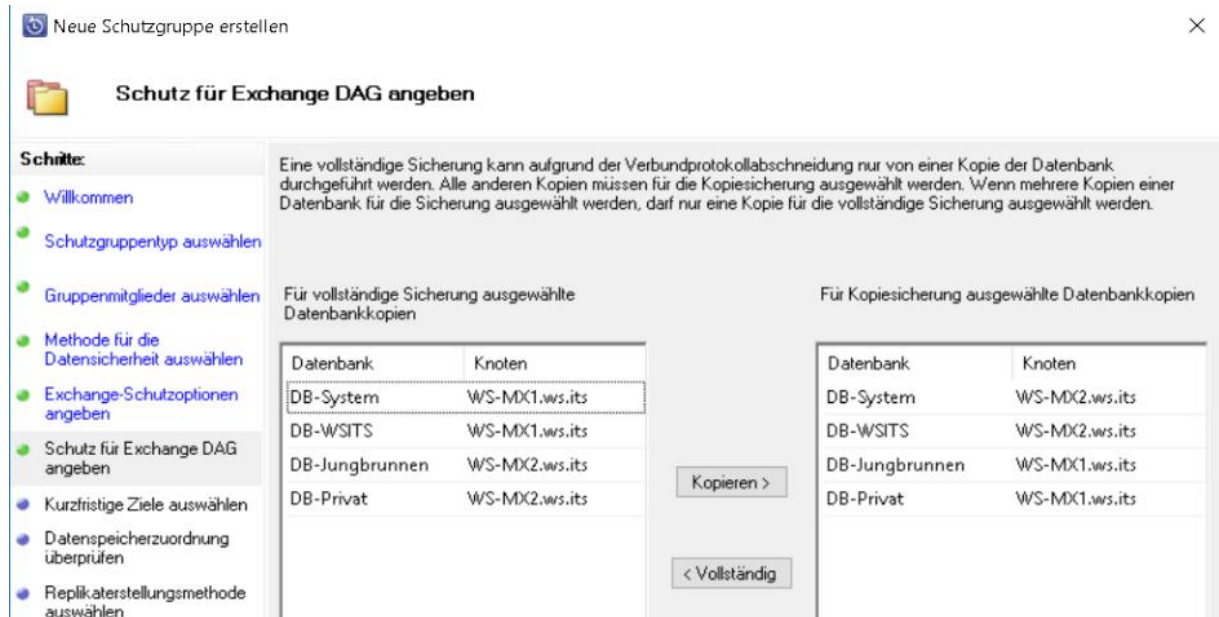
Die Exchange-Datenbanken werden online gesichert – also in einem Dirty-Shutdown-State bei einer Wiederherstellung entpackt. Damit der DPM das korrigieren kann, benötigt er eseutil in der Version der Datenbanken. Das bekomme ich vom Exchange Server:



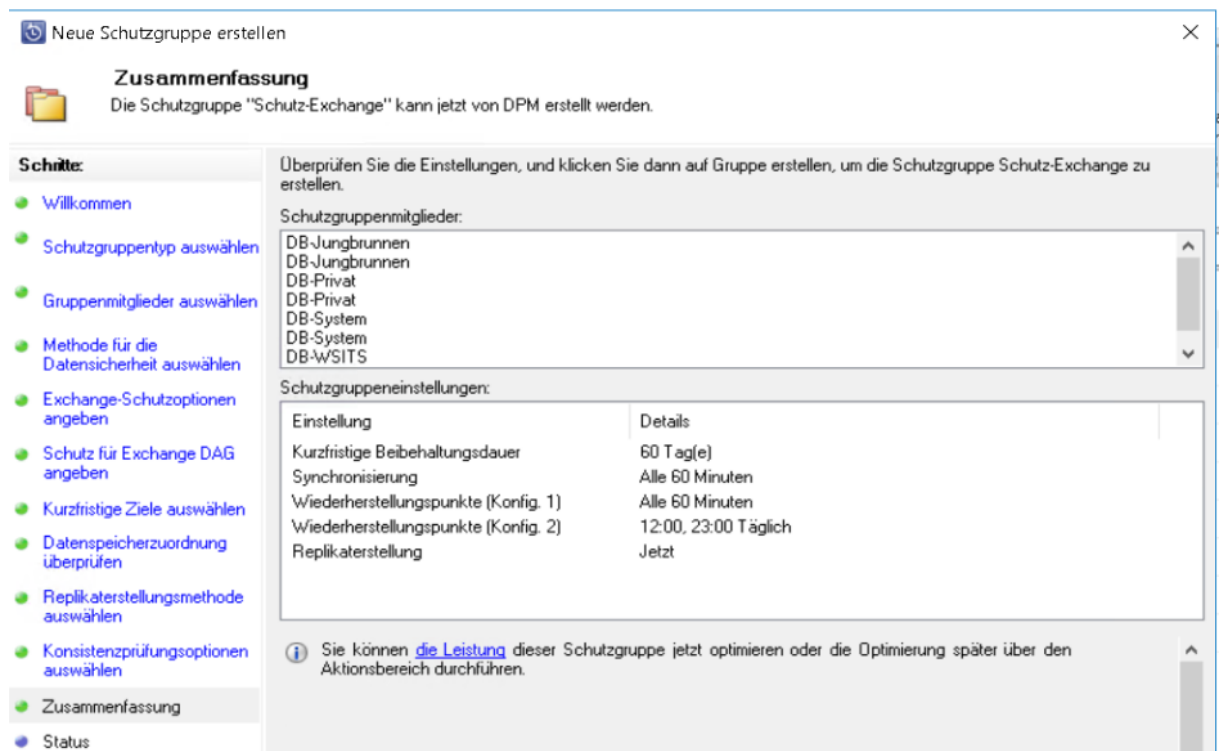
Nun kann ich eine neue Schutzgruppe bauen. Diese beziehe ich auf die DAG:



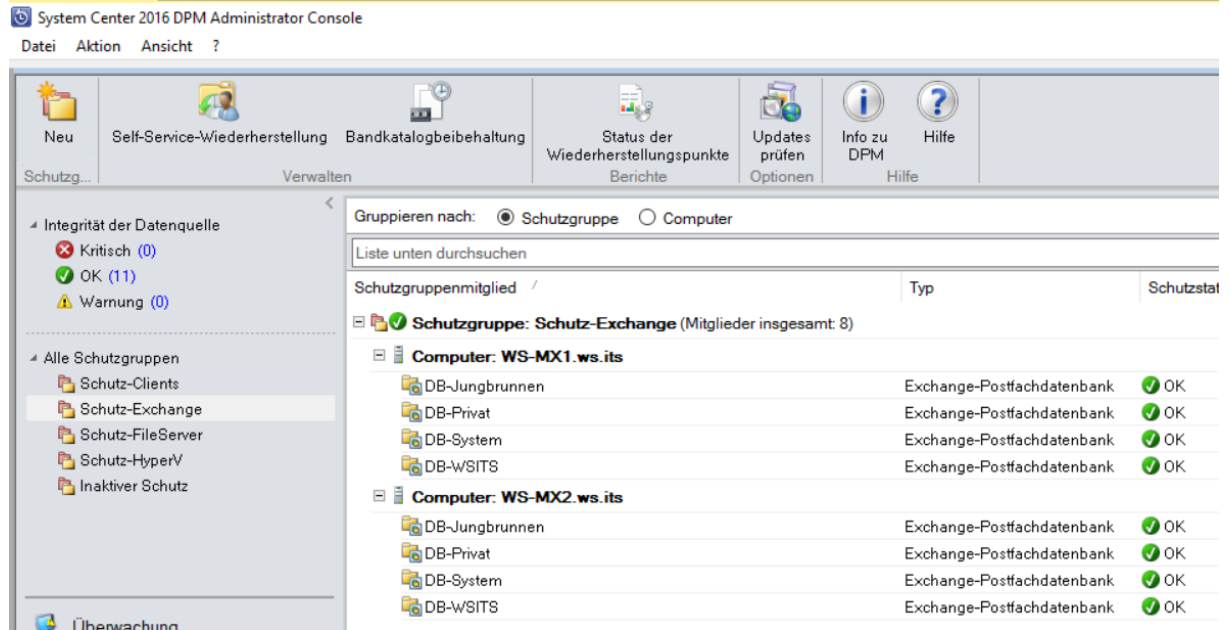
Bei der Sicherung wird die primäre Datenbank-Kopie mit einer Vollsicherung versehen, die sekundäre Kopie mit einer Kopiesicherung. Das muss mit der Konfiguration der Exchange-Datenbanken übereinstimmen. Zur Erinnerung: nachdem ich auf WS-MX2 alle Kopien von WS-MX1 eingerichtet habe, hab ich 2 davon als primär gekennzeichnet. Das sind die onlinegeschalteten Kopien, die der DPM gerne vollsichern möchte:



Die weiteren Konfigurationen übernehme ich aus der Dokumentation der bisherigen Schutzgruppe der alten Sicherung:



Die Sicherung startet ... und ist fertig:



The screenshot shows the System Center 2016 DPM Administrator Console interface. The main area displays a list of protection groups under the 'Schutzgruppe: Schutz-Exchange' category. The table below summarizes the data shown in the screenshot:

Computer	DB Name	Typ	Status
Computer: WS-MX1.ws.its	DB-Jungbrunnen	Exchange-Postfachdatenbank	OK
	DB-Privat	Exchange-Postfachdatenbank	OK
	DB-System	Exchange-Postfachdatenbank	OK
	DB-WSITS	Exchange-Postfachdatenbank	OK
Computer: WS-MX2.ws.its	DB-Jungbrunnen	Exchange-Postfachdatenbank	OK
	DB-Privat	Exchange-Postfachdatenbank	OK
	DB-System	Exchange-Postfachdatenbank	OK
	DB-WSITS	Exchange-Postfachdatenbank	OK

Im DPM sind noch die alten Datenbanksicherung vom Exchange Server 2013 enthalten. Diese kann ich nun löschen.

## 4. Abschluss

### Diagnose

### Zusammenfassung

Es gab bei der Migration einige Probleme, die ihre Ursache in vorhergehenden Ereignissen hatten. Diese wurden behoben. Ein stabiler Betrieb der neuen Server ist demnach möglich.

Wie geplant sind die Server mit den anderen Services und der Infrastruktur kompatibel.