

Inhalt

Vorbereitung	2
Beschreibung	2
Prüfung der Voraussetzungen	2
Datensicherung & Rollback	2
Bereitstellung von TestSzenarien	2
Interner Zugriff mit Outlook 2016	2
externer Zugriff mit Outlook 2016	2
externer Zugriff mit Outlook 2010	2
externer Zugriff mit ActiveSync	2
Umstellung auf Kerberos	2
Umstellung	2
Erstellen des ASA-Accounts	2
Konfiguration der Exchange Server	2
Konfiguration der SPN	4
Umstellung der Authentifizierung im Exchange	4
Testlauf	5
Interner Zugriff mit Outlook 2016	5
externer Zugriff mit Outlook 2016	8
externer Zugriff mit Outlook 2010	8
externer Zugriff mit ActiveSync	8
Nacharbeiten	8

Vorbereitung

Beschreibung

Die Konfiguration wird nach dieser aktuellen Anleitung durchgeführt: <https://docs.microsoft.com/en-us/Exchange/architecture/client-access/kerberos-auth-for-load-balanced-client-access?view=exchserver-2019>

Dabei wird ein AD-Computerobjekt erstellt, das mit einem Exchange-Script auf allen Exchange-Servern referenziert wird. Diesem Computerobjekt werden die erforderlichen SPN für die Exchange-Verbindung zugewiesen. Auf den CAS-Servern wird durch die Aushandlungsauthentifizierung Kerberos als bevorzugtes Authentifizierungsprotokoll verwendet.

Prüfung der Voraussetzungen

Laut der Anleitung sind Exchange Server 2016/2019 hinter einem LoadBalancer unterstützt. Meine Testumgebung besteht aus 2 Exchange Server 2016, die über eine DAG eine hochverfügbare Infrastruktur bereitstellen. Der Clientzugriff wird über einen vorgelagerten LoadBalancer (OSI Layer 4) für interne und externe Clients bereitgestellt.

Datensicherung & Rollback

Für einen möglicherweise erforderlichen Rollback wird die letzte Datensicherung geprüft. Ein Rollback kann aber auch durch das Entfernen der SPN-Konfiguration eingeleitet werden.

Die letzten Sicherungen waren auf beiden Exchange Servern erfolgreich.

Bereitstellung von TestSzenarien

Interner Zugriff mit Outlook 2016

Die Simulation wird von einem Client mit Outlook 2016 durchgeführt. Dieser läuft als RDS-SessionHost mit Windows Server 2016. Outlook wird vor der Umstellung gestartet, um ggf. auftretende Nebeneffekte zu erkennen. Zusätzlich wird zum Zeitpunkt der Umstellung der Netzwerkdatenstrom mit WireShark analysiert.

externer Zugriff mit Outlook 2016

Der Testlauf wird von einem Windows 10 1803 mit Outlook 2016 durchgeführt. Das System ist mit einem öffentlichen Netzwerk verbunden und stellt die Verbindung zur Exchange-Infrastruktur mit MAPI-http her.

externer Zugriff mit Outlook 2010

Der Testlauf wird von einem Windows 7 mit Outlook 2010 durchgeführt. Das System befindet sich in einem fremden Netzwerk und stellt die Verbindung zur Exchange-Infrastruktur mit MAPI-http her.

externer Zugriff mit ActiveSync

Hierfür wird ein Mobiltelefon verwendet.

Umstellung auf Kerberos

Umstellung

Erstellen des ASA-Accounts

Der zusätzliche Account wird als AD-Computeraccount eingerichtet:

```
New-ADComputer -Name EXCH2016ASA -AccountPassword (Read-Host 'Enter password' -AsSecureString) -
Description 'Alternate Service Account credentials for Exchange' -Enabled:$True -SamAccountName
EXCH2016ASA
```

Für den Account wird ein moderner EncryptionType verwendet:

```
Set-ADComputer EXCH2016ASA -add @{ "msDS-SupportedEncryptionTypes"="28" }
```

Konfiguration der Exchange Server

Die Einrichtung des ASA-Accounts wird auf dem ersten Exchange-Server mit einem Script vorgenommen:

```
Set-Location -Path $exscripts
.\RollAlternateServiceAccountPassword.ps1 -ToSpecificServers $env:COMPUTERNAME -
GenerateNewPasswordFor 'WS\service-MX$'
```

```

Computer: WS-MX1.ws.its

Willkommen bei der Exchange-Verwaltungsschell.

Vollständige Liste der Cmdlets: Get-Command
Nur Exchange-Cmdlets: Get-ExCommand
Cmdlets, die einer bestimmten Zeichenfolge entsprechen: Hilfe *<string>*
Allgemeine Hilfe abrufen: Hilfe
Hilfe für ein Cmdlet abrufen: Help <cmdlet name> oder <cmdlet name> -?
Exchange-Teamblog: Get-ExBlog
Vollständige Ausgabe für einen Befehl anzeigen: <command> | Format-List

Kurzübersichtsleitfaden anzeigen: QuickRef
Tipp des Tages Nr. 20:

Bevor Sie ein Objekt mithilfe des Remove-Verbs entfernen, verwenden Sie den Parameter WhatIf, um zu überprüfen, ob die e
rwarteten Ergebnisse auftreten.

AUSFÜHRlich: Verbindung mit WS-MX1.ws.its wird hergestellt.
AUSFÜHRlich: Verbunden mit WS-MX1.ws.its.
[PS] C:\Windows\system32>Set-Location -Path $exscripts
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts> .\RollAlternateServiceAccountPassword.ps1 -ToSpecificSer
vers WS-MX1.ws.its -GenerateNewPasswordFor 'WS\service-MX$'

===== Starting at 07/24/2019 13:17:44 =====
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

Prior to pushing new credentials, all existing credentials that are invalid or no longer work will be removed from the d
estination servers.
Pushing credentials to server WS-MX1
Setting a new password on Alternate Service Account in Active Directory

Password change
Do you want to change password for WS\service-MX$ in Active Directory at this time?
[J] Ja [N] Nein [H] Anhalten [?] Hilfe (Standard ist "J"): j
Preparing to update Active Directory with a new password for WS\service-MX$ ...
Resetting a password in the Active Directory for WS\service-MX$ ...
New password was successfully set to Active Directory.
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 13:18:17

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: 24.07.2019 13:18:03, WS\service-MX$
          Zuvor: <Not set>

===== Finished at 07/24/2019 13:18:19 =====

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

```

Auf allen anderen Exchange Servern wird nun der neue Account mit dem neuen Passwort angefordert:

```

Set-Location -Path $exscripts
.\RollAlternateServiceAccountPassword.ps1 -ToSpecificServers $env:COMPUTERNAME -CopyFrom 'WS-MX1'

```

```

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

===== Starting at 07/24/2019 13:32:05 =====
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

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 13:24:37

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: 24.07.2019 13:32:11, WS\service-MX$
          Zuvor: <Not set>

===== Finished at 07/24/2019 13:32:12 =====
THE SCRIPT HAS SUCCEEDED
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>

```

Abschließend kann die Verteilung über alle Server ausgelesen werden:

```

PS C:\Users\stephan-ad\Desktop> Get-ClientAccessService -IncludeAlternateServiceAccountCredentialStatus | Format-List Name, AlternateServiceAccountConfigur

Name
----
WS-MX1
AlternateServiceAccountConfiguration : Zuletzt: 24.07.2019 13:35:21, WS\service-MX$
                                      Zuvor: 24.07.2019 13:32:11, WS\service-MX$

Name
----
WS-MX2
AlternateServiceAccountConfiguration : Zuletzt: 24.07.2019 13:35:54, WS\service-MX$
                                      Zuvor: 24.07.2019 13:35:54, WS\service-MX$

```

Konfiguration der SPN

Nun können die URLs als SPN an den ASA-Account angebunden werden:

```

# Prüfung
$URLs | ForEach-Object { setspn -F -Q "http/$_" }

# SPN registrieren
$URLs | ForEach-Object { setspn -S "http/$_" "$($env:userdomain)\$ASA_Name$('$_') " }

```

Umstellung der Authentifizierung im Exchange

Abschließend wird die Authentifizierung auf „Aushandlung“ umgestellt. Diese beinhalten Kerberos und bei einem Fehler auch NTLM:

```

Get-OutlookAnywhere | Format-List -Property Server,InternalClientAuthenticationMethod
Get-OutlookAnywhere | Set-OutlookAnywhere -InternalClientAuthenticationMethod Negotiate

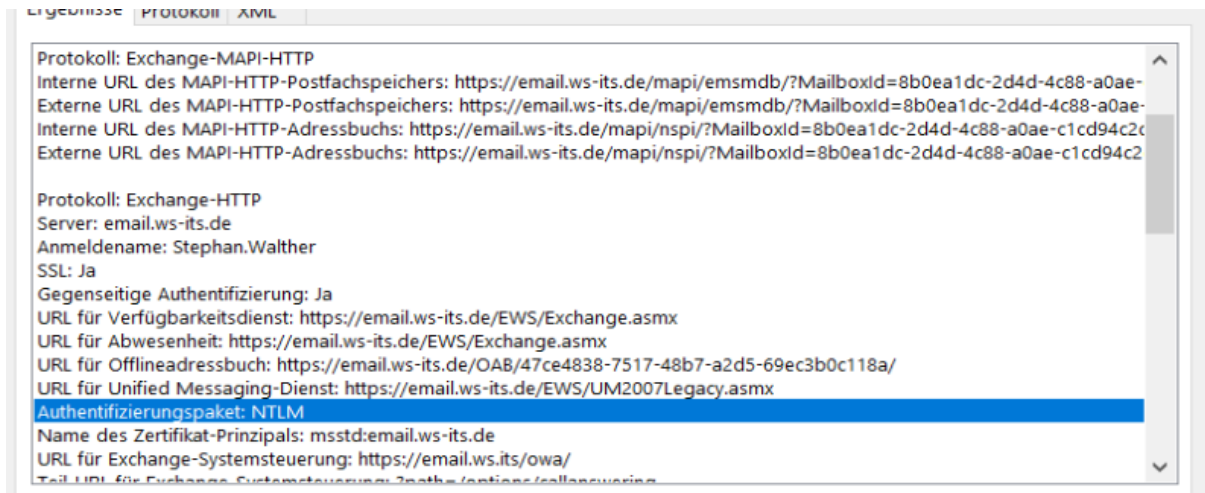
Get-MapiVirtualDirectory | Format-List -Property Server,IISAuthenticationMethods
Get-MapiVirtualDirectory | Set-MapiVirtualDirectory -IISAuthenticationMethods oauth,Negotiate

```

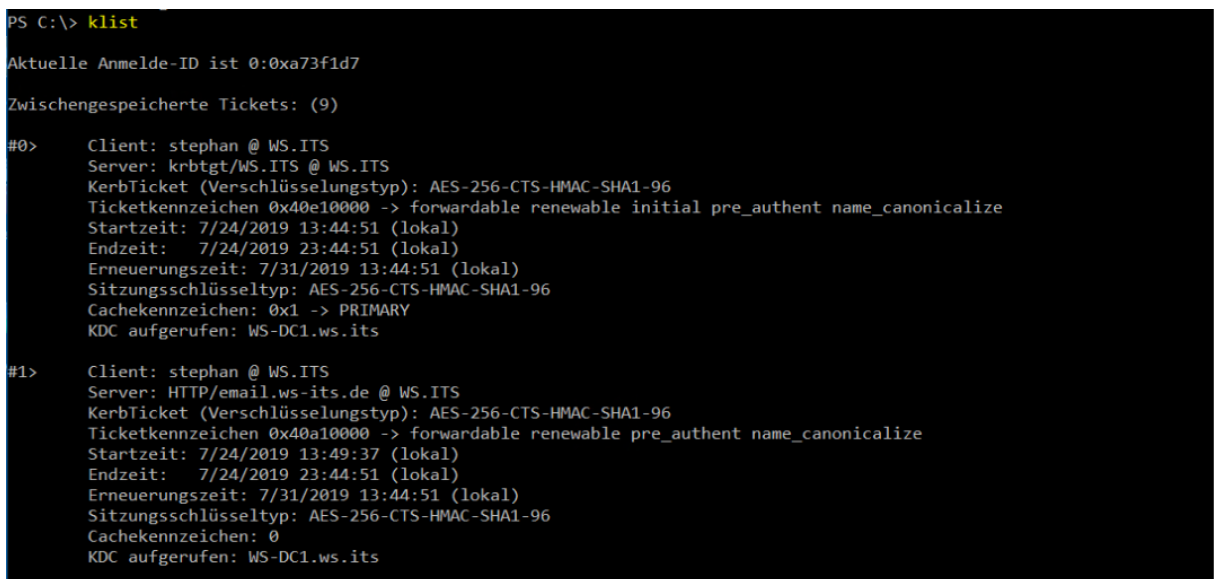
Testlauf

Interner Zugriff mit Outlook 2016

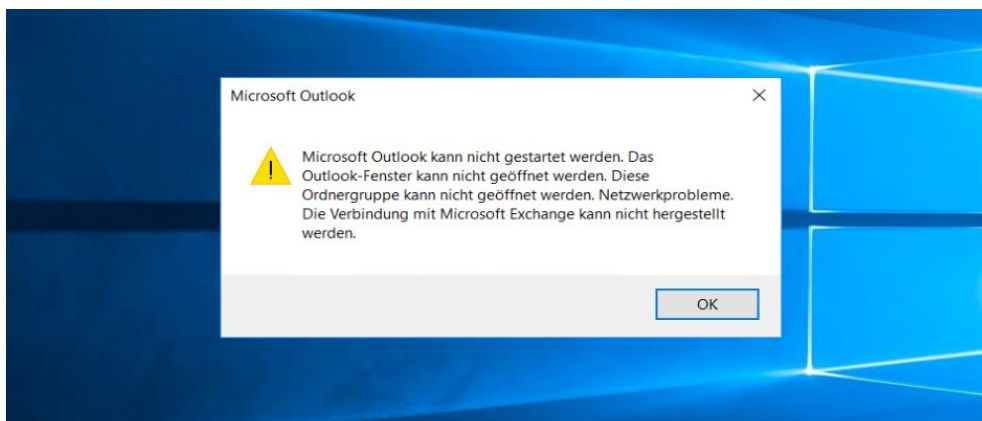
Das laufende Outlook handelt keine neue Anmeldung aus und arbeitet einfach weiter. Daher starte ich Outlook neu. Dennoch gibt es kein Kerberos-Ticket. Untersuche Autodiscover:



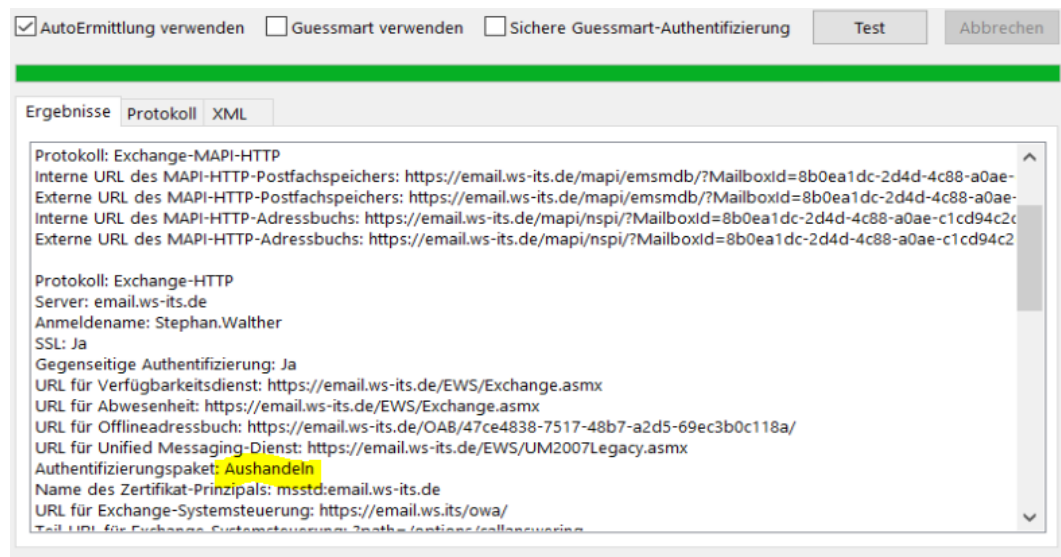
Das Problem: es war noch eine Instanz von Outlook geöffnet. Nachdem alle geschlossen waren gab es beim Start ein Ticket:



Dennoch startet Outlook nicht:



Offenbar brauchen die Mailserver einen Augenblick zum Schwenken. Kurz darauf startet Outlook mit einem Kerberos-Ticket. Denn im Autodiscover wird nun „Aushandeln“ statt „NTLM“ gelistet:



Zur genaueren Prüfung starte ich WireShark, lösche das Ticket und starte Outlook neu. Man kann sehr schön den Request des Tickets sehen:

No.	Time	Source	Destination	Protocol	Length	Info
2039	4.794129	192.168.110.21	192.168.100.1	TCP	66	51668 → 88 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460
2040	4.794986	192.168.110.1	192.168.110.21	TCP	66	88 → 51668 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=
2041	4.795053	192.168.110.21	192.168.100.1	TCP	54	51668 → 88 [ACK] Seq=1 Ack=1 Win=525568 Len=0
2042	4.795084	192.168.110.21	192.168.100.1	KRB5	1805	TGS-REQ
2043	4.795636	192.168.100.1	192.168.110.21	TCP	60	88 → 51668 [ACK] Seq=1 Ack=1752 Win=525568 Len=0
2044	4.798188	192.168.100.1	192.168.110.21	TCP	1514	88 → 51668 [ACK] Seq=1 Ack=1752 Win=525568 Len=1460 [TCP s
2045	4.798189	192.168.100.1	192.168.110.21	KRB5	671	TGS-REP

> Ethernet II, Src: Microsof_64:98:08 (00:15:5d:64:98:08), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)

> Internet Protocol Version 4, Src: 192.168.110.21, Dst: 192.168.100.1

> Transmission Control Protocol, Src Port: 51668, Dst Port: 88, Seq: 1, Ack: 1, Len: 1751

▼ Kerberos

> Record Mark: 1747 bytes

▼ tgs-req

pvno: 5

msg-type: krb-tgs-req (12)

> padata: 2 items

▼ req-body

Padding: 0

> kdc-options: 40810000 (forwardable, renewable, canonicalize)

realm: WS.ITS

▼ sname

name-type: kRB5-NT-SRV-INST (2)

▼ sname-string: 2 items

SNameString: HTTP

SNameString: email.ws-its.de

till: 2037-09-13 02:48:05 (UTC)

nonce: 1637009538

> etype: 5 items

> enc-authorization-data

tcp.stream eq 15						
No.	Time	Source	Destination	Protocol	Length	Info
2039	4.794129	192.168.110.21	192.168.100.1	TCP	66	51668 → 88 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460
2040	4.794986	192.168.100.1	192.168.110.21	TCP	66	88 → 51668 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
2041	4.795053	192.168.110.21	192.168.100.1	TCP	54	51668 → 88 [ACK] Seq=1 Ack=1 Win=525568 Len=0
2042	4.795084	192.168.110.21	192.168.100.1	KRB5	1805	TGS-REQ
2043	4.795636	192.168.100.1	192.168.110.21	TCP	60	88 → 51668 [ACK] Seq=1 Ack=1752 Win=525568 Len=0
2044	4.798188	192.168.100.1	192.168.110.21	TCP	1514	88 → 51668 [ACK] Seq=1 Ack=1752 Win=525568 Len=1460 [TCP
2045	4.798189	192.168.100.1	192.168.110.21	KRB5	671	TGS-REP

> Frame 2045: 671 bytes on wire (5368 bits), 671 bytes captured (5368 bits) on interface 0

> Ethernet II, Src: Microsof_64:bb:26 (00:15:5d:64:bb:26), Dst: Microsof_64:98:08 (00:15:5d:64:98:08)

> Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.110.21

> Transmission Control Protocol, Src Port: 88, Dst Port: 51668, Seq: 1461, Ack: 1752, Len: 617

> [2 Reassembled TCP Segments (2077 bytes): #2044(1460), #2045(617)]

▼ Kerberos

> Record Mark: 2073 bytes

▼ tgs-rep

pvno: 5

msg-type: krb-tgs-rep (13)

crealm: WS.ITS

> cname

▼ ticket

tkt-vno: 5

realm: WS.ITS

▼ sname

name-type: KRB5-NT-SRV-INST (2)

▼ sname-string: 2 items

SNameString: HTTP

SNameString: email.ws-its.de

> enc-part

> enc-part

Auch im DomainController finde ich das passende Eventlog:

Ereigniseigenschaften - Ereignis 4769, Microsoft Windows security auditing.

Allgemein Details

Ein Kerberos-Dienstticket wurde angefordert.

Kontoinformationen:

Kontoname: stephan@WS.ITS

Kontodomäne: WS.ITS

Anmelde-GUID: {1fb9d95d-5f32-e6dc-6643-b78fa0baf3a3}

Dienstinformationen:

Dienstname: service-MXS

Dienst-ID: WS\service-MXS

Netzwerkinformationen:

Clientadresse: ::ffff:192.168.110.21

Clientport: 51870

Weitere Informationen:

Ticketoptionen: 0x40810000

Ticketverschlüsselungstyp: 0x12

Fehlercode: 0x0

Übertragene Dienste: -

Protokollname: Sicherheit

Quelle: Microsoft Windows security Protokolliert: 24.07.2019 14:38:53

Ereignis-ID: 4769 Aufgabenkategorie: Ticketvorgänge des Kerberos-Diensts

Ebene: Informationen Schlüsselwörter: Überwachung erfolgreich

Benutzer: Nicht zutreffend Computer: WS-DC2.ws.its

Vorgangscode: Info

Leider wird nur „Aushandeln“ vom Client angezeigt. Dieses beinhaltet Kerberos und NTLM. Ein Fallback auf NTLM könnte also ebenfalls zu einer Verbindung zwischen Exchange und Outlook führen. Daher teste ich zusätzlich noch die Blockierung von NTLM für die Exchange-Server. Das interne Outlook kann sich ohne Probleme verbinden. Alle externen Clients verlieren die Verbindung und fragen nach Anmeldeinformationen. Das ist gut in den NTLM-Logs auf den DomainControllern erkennbar:

WS-DC2	2019-07-24	14:52:37	WS-CL1	WS-MX2	WS	stephan-jb
WS-DC2	2019-07-24	14:52:39	WS-CL1	WS-MX2	WS	stephan-jb
WS-DC2	2019-07-24	14:52:39	N67E0A2068	WS-MX2	WS	stephan
WS-DC2	2019-07-24	14:52:40	N67E0A2068	WS-MX2	WS	stephan
WS-DC2	2019-07-24	14:52:40	WS-CL1	WS-MX2	WS	stephan-jb
WS-DC2	2019-07-24	14:52:40	WS-CL1	WS-MX2	WS	stephan-jb
WS-DC2	2019-07-24	14:52:40	WS-CL1	WS-MX2	WS	stephan-jb
WS-DC2	2019-07-24	14:52:45	WS-CL1	WS-MX2	WS	stephan
WS-DC2	2019-07-24	14:52:46	WS-CL1	WS-MX2	WS	stephan-privat
WS-DC2	2019-07-24	14:52:48	N67E0A2068	WS-MX2	WS	stephan
WS-DC2	2019-07-24	14:52:49	WS-CL1	WS-MX2	WS	stephan-privat
WS-DC2	2019-07-24	14:52:49	WS-CL1	WS-MX2	WS	stephan-privat

externer Zugriff mit Outlook 2016

Der Client kann von extern kein Kerberos verwenden und bleibt bei NTLM. Ein Neustart des Clients funktioniert problemlos.

externer Zugriff mit Outlook 2010

Der Client kann von extern kein Kerberos verwenden und bleibt bei NTLM. Ein Neustart des Clients funktioniert problemlos.

externer Zugriff mit ActiveSync

Auch das Mobiltelefon hat keine Probleme beim Verbindungsaufbau.

Nacharbeiten

Es sind keine Nacharbeiten erforderlich.