



SMEXhybrid Lab-Guide

V 2.6, 14.3.2024
Christian Schindler

Inhalt

Lab 1:	Vorbereitungen	4
Übung 1:	Konfiguration des Routers.....	4
Übung 2:	Konfiguration AD + DNS.....	6
Übung 3:	Konfiguration von Exchange Server 2019	7
Lab 2:	AAD Connect	9
Übung 1:	Vorbereitung Active Directory.....	9
Übung 2:	Vorbereitung Office 365	10
Übung 3:	Installation AAD Connect.....	13
Übung 4:	AAD Connect Anpassung	16
Lab 3:	Identity Federation	22
Übung 1:	ADFS-Installation/Konfiguration.....	22
Übung 2:	Aktivieren der Federation.....	25
Lab 4:	Exchange Hybrid.....	27
Übung 1:	Vorbereitungen	27
Übung 2:	Hybrideinrichtung.....	30
Übung 3:	Bereinigung der Empfänger.....	32
Lab 5:	Empfängerverwaltung.....	35
Übung 1:	Postfächer.....	35
Übung 2:	Onboarding.....	37
Übung 3:	Konfigurieren der Exchange Recipient Management Shell.....	39
Lab 6:	Public Folders	41
Übung 1:	Koexistenz.....	41
Übung 2:	Vorbereitungen zur Migration.....	43
Übung 3:	Migration	44
Übung 4:	Abschließen der Migration	46
Lab 7:	Exchange Online Protection	49
Übung 1:	MX und SPF Record	49
Übung 2:	DKIM	51

Bevor es los geht...

Kennwörter

Das Kennwort für alle bestehenden Konten (außer lokaler Admin auf ROUTER) lautet:

Pa\$\$w0rd

Um eine eventuelle Fehlersuche zu erleichtern, verwenden Sie bitte dieses Kennwort auch bei der Neuanlage von Benutzern!

Kennwort lokaler Admin auf Router:

IhhFfa018FSQura4

Zugriff auf Tools-Share am Trainer Rechner

Auf Ihrem Host finden sie das Laufwerk „T:“. Dieses ist verbunden auf den Trainer Rechner. Ihr Trainer wird Ihnen über dieses Laufwerk eventuell weitere Kursmaterialien zur Verfügung stellen bzw. Werden Sie dort Infos und Dateien hochladen.

Arbeiten mit den VMs

Bitte verwenden Sie zur Verbindung mit den VMs den **Remote Desktop Connection Manager**



(Icon in der Taskleiste). Dort sind alle notwendigen Verbindungen bereits konfiguriert. Dieser bietet die Möglichkeit von Copy/Paste (auch Dateien), etc.

Mitschriften

Auf dem Host ist Office installiert. Für Mitschriften eignet sich am besten **OneNote** – damit können Sie **Screenshots** mittels der Tastenkombination **Windowstaste+SHIFT+S** einfach erzeugen.

Starten der VMs

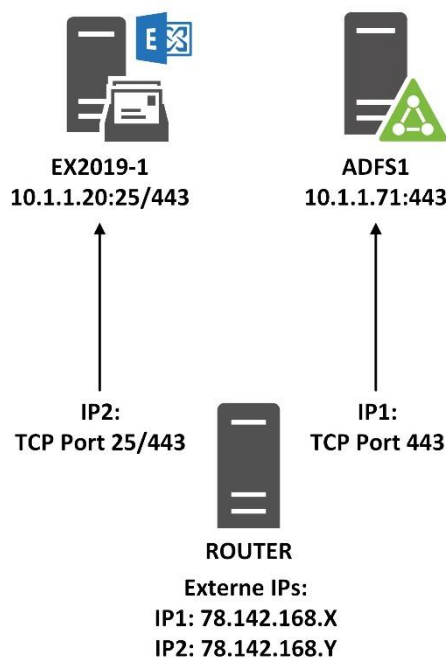
1. Auf dem physischen Host öffnen Sie eine PowerShell als Administrator
2. Navigieren Sie zu „D:\Scripts“
3. Führen Sie das Script „Start-VM.ps1“ aus

Lab 1: Vorbereitungen

Übung 1: Konfiguration des Routers

Einleitung:

In dieser Übung wird der Router für eine direkte Verbindung mit dem Internet konfiguriert. Dabei werden die Ihnen zugewiesenen IP-Adressen auf die externe NIC gebunden und anschließend folgende NAT-Port-Mappings, wie hier gezeigt, eingetragen:



Aufgaben:

1. Konfigurieren der Netzwerkkarte und NAT-Regeln

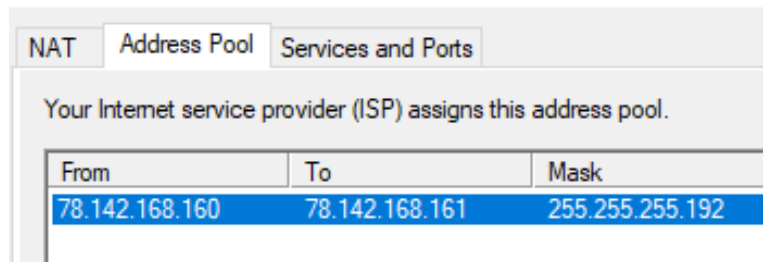
Detaillierte Anleitung:

Aufgabe 1: Konfigurieren der Netzwerkkarte und NAT-Regeln

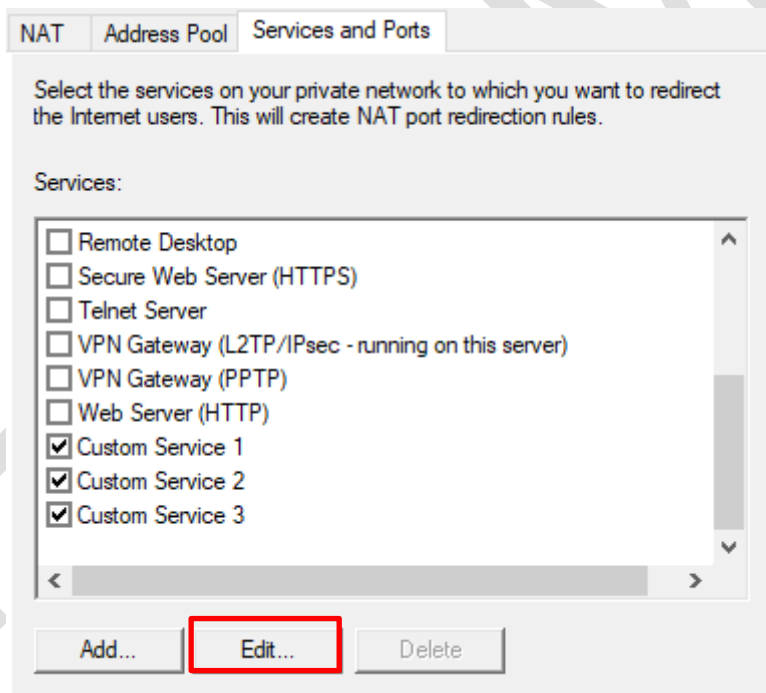
1. Melden Sie sich an Router als „**\Administrator**“ an
2. Öffnen Sie einen **CMD-Prompt als Administrator (keine PowerShell!)** und wechseln ins Verzeichnis „**D:**“
3. Konfigurieren Sie den Router mittels Batchdatei. Geben Sie dazu als Parameter Ihre IP-Adressen, getrennt durch ein Leerzeichen, an:

ConfigureRouter.cmd 78.142.168.X 78.142.168.Y (X = IP1, Y = IP2)

4. Lassen Sie den CMD-Prompt geöffnet
5. Öffnen Sie die Routing and Remote Access Konsole von der Taskbar
6. Navigieren Sie zu „**ROUTER/Ipv4/NAT**“
7. Öffnen Sie die Netzwerkkarte „**Internet**“
8. Wechseln Sie zum Reiter „**Address Pool**“
9. Stellen Sie sicher, dass es einen Eintrag gibt, der Ihren IP-Adressen entspricht:



10. Wechseln Sie zum Reiter „**Services and Ports**“
11. Überprüfen Sie, ob es die folgenden NAT-Mappings gibt:



Public Address	Protocol	Incoming Port	Private Address	Outgoing Port
IP 1	TCP	443	10.1.1.71	443
IP 2	TCP	25	10.1.1.20	25
IP 2	TCP	443	10.1.1.20	443

12. Wechseln Sie zum CMD-Prompt und testen Sie die Internetverbindung mit PING:

ping 8.8.8.8

Übung 2: Konfiguration AD + DNS

Einleitung:

In dieser Übung wird der interne DNS-Server vorbereitet, um Anfragen für Ihre E-Mail Domain zu beantworten.

Aufgaben:

1. Erzeugen der DNS-Zone
2. Hinzufügen eines UPN-Suffixes

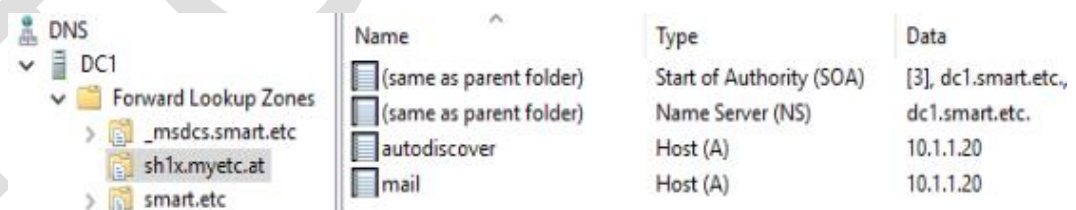
Detaillierte Anleitung:

Aufgabe 1: Erzeugen der DNS-Zone

1. Melden Sie sich an DC1 als „**Smart\Administrator**“ an
2. Öffnen Sie eine Windows PowerShell als Administrator
3. Erzeugen Sie eine neue DNS-Zone mittels Scripts. Geben Sie beim Parameter „**Domain**“ Ihre Custom-Domain an:

```
L:
cd \scripts
.\CreatedDNSZone.ps1 -Domain shx.myetc.at
```

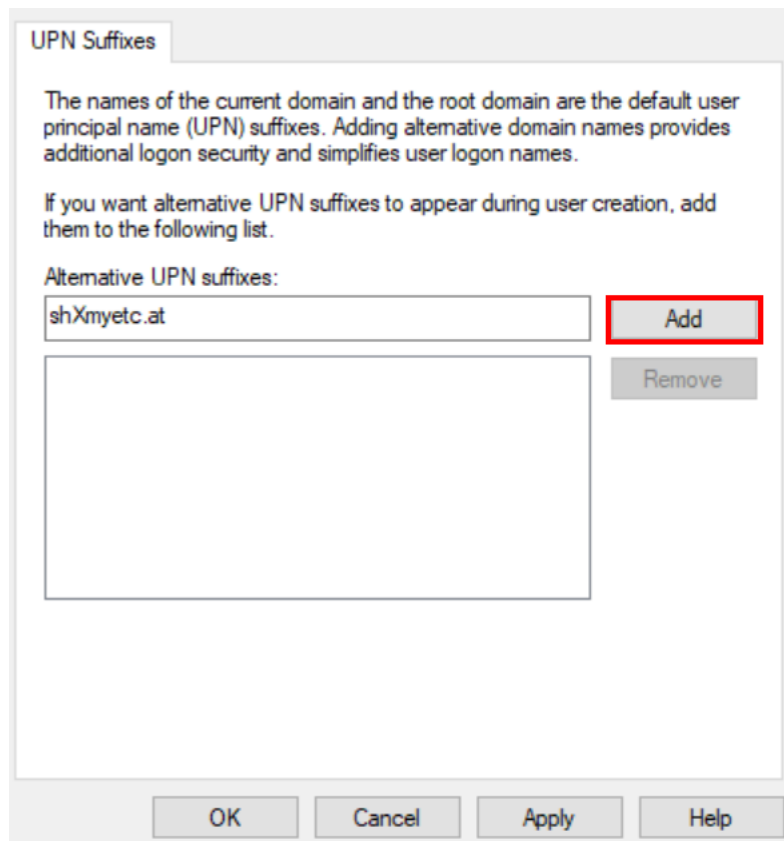
4. Öffnen Sie die DNS Management Konsole und überprüfen Sie, ob die Zone erfolgreich angelegt wurde:



5. Lassen Sie die Windows PowerShell geöffnet

Aufgabe 2: Hinzufügen eines UPN-Suffixes

1. Öffnen Sie die „**Active Directory Domains and Trusts**“ Console
2. Klicken Sie rechts auf „**Active Directory Domains and Trusts**“ und wählen „**Properties**“
3. Fügen Sie ihre Custom-Domain (**shX.myetc.at**) als UPN-Suffix hinzu:



Übung 3: Konfiguration von Exchange Server 2019

Einleitung:

In dieser Übung wird die Exchange Server 2019 Umgebung auf Ihre Custom-Domain angepasst.

Aufgaben:

1. Anpassen der Konfiguration
2. Aktivieren des Exchange ACL Sync

Detaillierte Anleitung:

Aufgabe 1: Anpassen der Konfiguration

1. Melden Sie sich an EX2019-1 als „**Smart\Administrator**“ an
2. Öffnen Sie eine Exchange Management Shell als Administrator
3. Führen Sie das Script zur Änderung der Konfiguration aus. Geben Sie als Parameter die Ihnen zugewiesen Teilnehmer-Domain an:

```
L:  
cd \Scripts  
.\ConfigureExchange.ps1 -Domain shX.myetc.at
```

4. Sollte ein Fehler bezüglich administrativen Rechten auftreten, führen Sie ein IISRESET durch
5. Lassen Sie die Shell geöffnet

Aufgabe 2: Aktivieren des Exchange ACL Sync

1. In der Exchange Management Shell aktivieren sie die Synchronisation der Full Access Permissions für Mailboxen:

```
Set-OrganizationConfig -ACLableSyncedObjectEnabled $true
```


Lab 2: AAD Connect

Übung 1: Vorbereitung Active Directory

Einleitung:

In dieser Übung werden die Vorbereitungen für den Betrieb von AAD Connect im Active Directory getroffen.

Aufgaben:

1. Anpassen der UPNs
2. Erzeugen der Service Accounts

Detaillierte Anleitung:

Aufgabe 1: Anpassen der UPNs

1. Wechseln Sie zu DC1
2. Wechseln Sie zur Windows PowerShell
3. Geben Sie folgenden Befehl ein, um den UPN aller Benutzer gleich der E-Mail-Adresse zu setzen:

```
Get-ADUser -SearchBase "ou=accounts,dc=smart,dc=etc"
-Filter * -Properties mail | % {Set-ADUser
-Identity $_.SamAccountName -UserPrincipalName $_.mail}
```

4. Öffnen Sie die Active Directory Users and Computers Konsole und überprüfen Sie bei einem Benutzer unterhalb der „Accounts“ OU, ob der User Logon Name gleich der E-Mail-Adresse ist

Aufgabe 2: Erzeugen der Service Accounts

1. In der Windows PowerShell geben Sie folgenden Befehl ein, um einen KDS Root Key zu erzeugen:

```
Add-KdsRootKey -EffectiveTime (get-date).AddHours(-10)
```

2. Überprüfen Sie, ob der KDS Root Key erzeugt wurde:

Get-KdsRootKey

3. Erzeugen Sie einen neuen Group Managed Service Account für AAD Connect:

```
New-ADServiceAccount -Name gmsa_aadc  
-DNSHostName gmsa_aadc.smart.etc  
-PrincipalsAllowedToRetrieveManagedPassword ADFS1$
```

4. Überprüfen Sie, ob der Service Account erzeugt wurde:

Get-ADServiceAccount -Filter *

5. Wechseln Sie zur Active Directory Users and Computers Konsole.
6. Erzeugen Sie einen AAD Connect Service Account für den Zugriff ins AD mit folgenden Daten:

- Full ame: svc_aadc
- User logon name (pre-Windows 2000): svc_aadc
- OU: „smart.etc/Operations/Users“
- Password: unser bekanntes Standardpasswort
- Password never expires gesetzt

Übung 2: Vorbereitung Office 365

Einleitung:

In dieser Übung wird Office 365 für die Synchronisation mit AAD Connect vorbereitet

Aufgaben:

1. Hinzufügen der Custom-Domain zu Office 365

Detaillierte Anleitung:

Aufgabe 1: Hinzufügen der Custom-Domain zu Office 365

1. Melden Sie sich an ADFS1 als „**smart\Administrator**“ an
2. Öffnen Sie den EDGE-Browser und navigieren Sie zum Office 365 Admin Portal
<https://admin.microsoft.com>
3. Melden Sie den Tenant-Admin an (admin@shXmyetcat.onmicrosoft.com)

4. Bestätigen Sie die Abfrage nach der Anmeldung mit „**Yes**“
5. Klicken Sie in der Navigationsleiste links auf „**Setup**“
6. Klicken Sie den Link „**Get your custom domain set up**“
7. Klicken Sie „**Get Started**“
8. Bei „**Add a domain**“ geben Sie Ihre **Custom-Domain** ein und klicken „**Use this domain**“:

Add a domain

If you already own a domain like contoso.com, you can add it to your account here.

Domain name

shX.myetc.at

9. Stellen Sie sicher das „**Add a TXT record to the...**“ ausgewählt ist und klicken Sie „**Continue**“
10. Kopieren Sie den Wert bei „**TXT value**“ und lassen den Browser geöffnet:

TXT name

sh1x (or skip if not supported by provider)

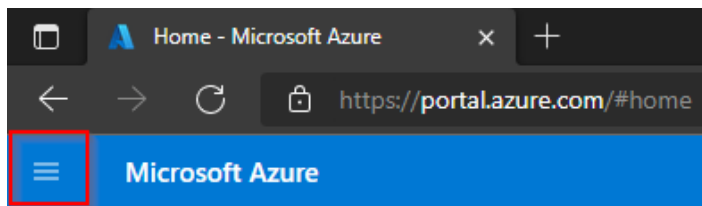
TXT value

MS=ms78125614

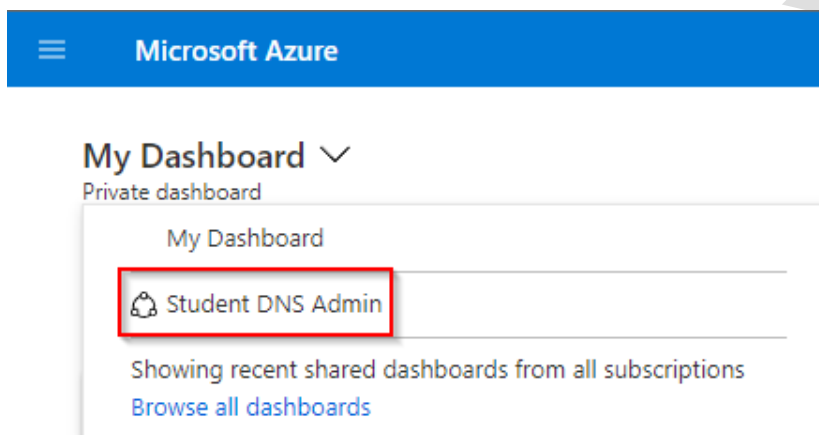
TTL

3600 (or your provider default)

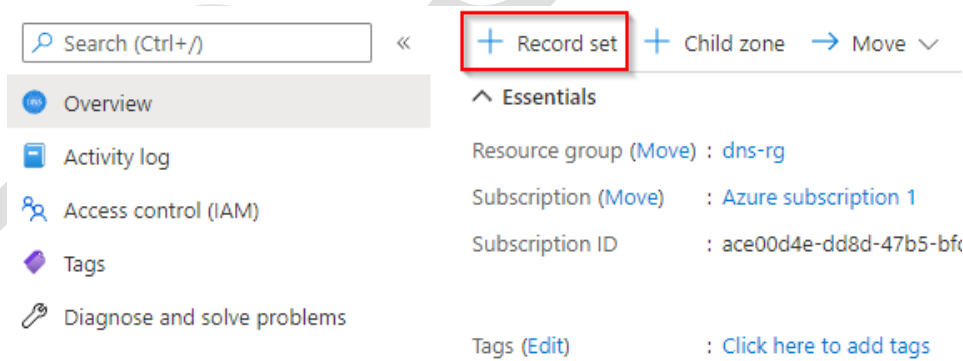
11. Öffnen Sie einen EDGE-Browser InPrivate Tab (CTRL+SHIFT+N) und öffnen das Azure Portal: <https://portal.azure.com>
12. Melden Sie sich mit Ihrem Azure DNS User an (shX@myetc.at)
13. Klicken Sie auf „**Maybe later**“
14. Klicken Sie in der Navigation links auf das Menüsymbol.



15. Wählen Sie **Dashboard** aus der Liste
16. IM Dashboard klicken Sie links oben auf „**My Dashboard**“ und wählen das „**Student DNS Admin**“ Dashboard aus:



17. In der Kachel „**All resources**“ klicken Sie auf „**shX.myetc.at**“
18. Klicken Sie auf „**+ Record set**“:



19. Erzeugen Sie das Recordset mit folgenden Daten:

Name	Type	TTL	Value
@	TXT	300 Sekunden	Der zuvor im Portal kopierte Wert (MS=msXXXXXXXXX)

20. Wechseln Sie zurück zum EDGE-Browser mit dem Office 365 Admin Portal
21. Klicken Sie „**Verify**“
22. Klicken Sie „**More options**“, wählen „**Skip and do this later...**“ und klicken „**Continue**“

23. Klicken Sie „**Done**“
24. Wechseln Sie zum Browser mit dem Azure Portal
25. Entfernen Sie den TXT-Record der in Schritt 19 erzeugt wurde
26. Bleiben Sie in beiden Browserfenstern angemeldet

Übung 3: **Installation AAD Connect**

Einleitung:

In dieser Übung wird AAD Connect installiert.

Aufgaben:

1. Installation der AAD Connect Binaries
2. Vergabe der Service Account Berechtigungen
3. Installation AAD Connect
4. Überprüfung der Synchronisation

Detaillierte Anleitung:

Aufgabe 1: Installation der AAD Connect Binaries

1. Melden Sie sich an ADFS1 als „**smart\Administrator**“ an
2. Öffnen Sie einen EDGE-Browser und navigieren Sie zu
<https://www.microsoft.com/en-us/download/details.aspx?id=47594>
3. Laden Sie AAD Connect herunter
4. Nachdem der Download abgeschlossen ist, führen Sie die MSI Datei aus.
5. Lassen Sie den Installationsdialog geöffnet

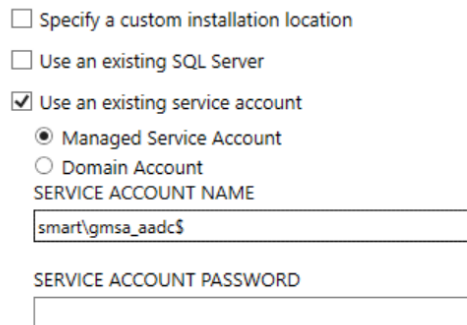
Aufgabe 2: Vergabe der Service Account Berechtigungen

1. Öffnen Sie eine Windows PowerShell als Administrator
2. Vergeben Sie die Berechtigungen für den AAD Connect Service Account mittels Scripts:

```
L:
cd \Scripts
.\SetAADAccountPermissions.ps1
```

Aufgabe 3: Installation AAD Connect

1. Wechseln Sie zurück zum Installationsdialog
2. Aktivieren Sie die Checkbox „I agree...” und klicken „Continue“
3. Klicken Sie auf „Customize“
4. Aktivieren Sie die Checkbox „Use an existing service account“
5. Geben Sie die Information für den Service Account ein und klicken „Install“
(dauert ein wenig...):



☐ Specify a custom installation location

☐ Use an existing SQL Server

☒ Use an existing service account

☒ Managed Service Account
☐ Domain Account

SERVICE ACCOUNT NAME

smart\gmsa_aadc\$

SERVICE ACCOUNT PASSWORD

6. Auf der Seite „User sign-in“ belassen Sie die Einstellungen und klicken „Next“
7. Auf der Seite „Connect to Azure AD“ geben sie die Anmeldeinformationen ihre Tenants ein und klicken „Next“:

Connect to Azure AD

Enter your Azure AD global administrator credentials. ?



USERNAME

admin@sh1xmyetcat.onmicrosoft.com

PASSWORD

.....

8. Auf der Seite „Connect your directories“ klicken sie „Add Directory“
9. Geben sie den zuvor erstellen Service Account für die Verbindung mit AD an, klicken „OK“ und dann „Next“:

AD forest account

An AD account with sufficient permissions is required for Connect to create the account for you. Alternatively, you can create the account manually with the required permissions. [Learn more](#) about managing accounts.

The first option is recommended and requires you to enter the following information:

Select account option.

- ☐ Create new AD account
- ☒ Use existing AD account

DOMAIN USERNAME

SMART\svc_aadc

PASSWORD

.....

10. Auf der Seite „**Azure AD sign-in configuration**“ aktivieren Sie die Checkbox „**Continue without matching...**“ und klicken „**Next**“
11. Auf der Seite „**Domain and OU filtering**“ wählen Sie „**Sync selected domains and OUs**“ aus
12. Wählen Sie anschließend nur die „**Accounts**“ OU aus und klicken „**Next**“:

- ☐ Sync all domains and OUs
- ☒ Sync selected domains and OUs

☒ smart.etc

- ☒ Accounts
- ☐ Builtin
- ☐ Computers

13. Auf den Seiten „**Uniquely identify your users**“ und „**Filter users and devices**“ klicken Sie „**Next**“
14. Auf der Seite „**Optional features**“ wählen Sie die folgenden Funktionen aus und klicken „**Next**“:
 - Exchange hybrid deployment
 - Exchange Mail Public Folders
15. Klicken Sie „**Install**“
16. Nach der Installation klicken Sie auf „**Exit**“

Aufgabe 4: Überprüfung der Synchronisation

1. Im geöffneten Browser klicken Sie im Admin Portal links auf „**Users/Active Users**“
2. Stellen Sie sicher, dass die Benutzer erfolgreich synchronisiert wurden und dass der UPN richtig gesetzt ist (muss der Custom-Domain entsprechen):

Display name ↑		Username	Licenses
Alexander Fritsch	:	Alexander.Fritsch@sh1x.myetc.at	Unlicensed
Anna Stickler	:	Anna.Stickler@sh1x.myetc.at	Unlicensed

Übung 4: AAD Connect Anpassung

Einleitung:

In dieser Übung wird die AAD Connect Installation angepasst.

Aufgaben:

1. Custom Sync Rules
2. Gruppenbasierten Lizenzierung

Detaillierte Anleitung:

Aufgabe 1: Custom Sync Rules

1. Wechseln Sie zu ADFS1
2. Melden Sie sich ab und wieder als „Smart\Administrator“ an
3. Öffne Sie das Startmenü, navigieren Sie zur Gruppe „**Azure AD Connect**“ und öffnen das „**Synchronization Rules Editor**“ Tool
4. Erzeugen Sie eine neue Regel mit einem Klick auf „**Add new rule**“
5. Geben Sie folgende Daten auf der ersten Seite ein:
 - Name: **Custom_In from AD_User-NoSync**
 - Connected System: **smart.etc**
 - Connected System Object Type: **user**
 - Metaverse Object Type: **person**
 - Precedence: **1**
6. Auf der Seite „**Scoping filter**“ klicken Sie „**Add group**“
7. Klicken Sie „**Add clause**“ und geben folgende Daten ein und klicken zweimal „**Next**“:
 - Attribut: **msDS-cloudExtensionAttribute1**
 - Operator: **EQUAL**

- Value: **nosync**

Attribute	Operator	Value
msDS-cloudExtensionAttribut	EQUAL	nosync

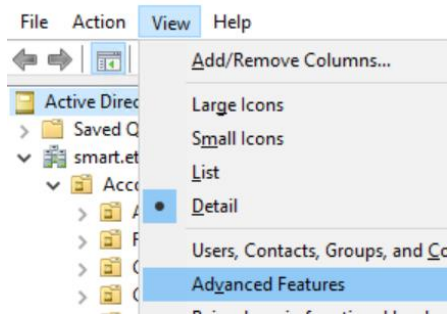
- Auf der Seite „**Transformations**“ klicken Sie „**Add transformation**“
- Geben Sie folgende Daten ein und klicken „**Add**“:
 - FlowType: **Constant**
 - Target Attribute: **cloudFiltered**
 - Source: **True**
- Klicken Sie „**OK**“, um die Meldung zu bestätigen
- Öffnen Sie eine neue Windows PowerShell als Administrator
- Starten Sie einen Sync:

Start-ADSyncSyncCycle

- Öffne Sie das Startmenü, navigieren Sie zur Gruppe „**Azure AD Connect**“ und öffnen das „**Synchronization Service**“ Tool
- Überprüfen anhand der Spalten „**Status**“ und „**End Time**“ ob der letzte Sync erfolgreich abgeschlossen wurde:

Connector Operations					
Name	Profile Name	Status	Start Time	End Time	
smart.etc	Export	success	05.01.2021 13:53:34	05.01.2021 13:53:34	
sh1Xmyetcat.onmicro...	Export	success	05.01.2021 13:53:28	05.01.2021 13:53:33	
sh1Xmyetcat.onmicro...	Delta Synchronization	success	05.01.2021 13:53:28	05.01.2021 13:53:28	
smart.etc	Full Synchronization	success	05.01.2021 13:53:27	05.01.2021 13:53:27	
sh1Xmyetcat.onmicro...	Delta Import	success	05.01.2021 13:53:22	05.01.2021 13:53:26	
smart.etc	Full Import	success	05.01.2021 13:53:22	05.01.2021 13:53:22	

- Öffnen Sie die **Active Directory Users and Computers Konsole**.
- Aktivieren Sie im Menü „**View**“ die Advanced Features:



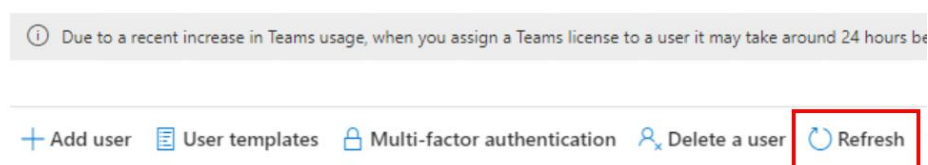
17. Navigieren Sie zur „**Accounts/Akademie/Lektoren**“ und öffnen Sie die Eigenschaften des Benutzers „**Anna Stickler**“
18. Wechseln Sie zum Reiter „**Attribute Editor**“
19. Scrollen Sie zum Attribut „**msDS-cloudExtensionAttribute1**“, befüllen dieses mit dem Wert „**nosync**“ und klicken „**OK**“:

Attributes:

Attribute	Value
msDS-AllowedToDelegateTo	<not set>
msDS-AssignedAuthNPolicy	<not set>
msDS-AssignedAuthNPolicySilo	<not set>
msDS-AuthenticatedAtDC	<not set>
msDS-Cached-Membership	<not set>
msDS-Cached-Membership-Tim...	<not set>
msDS-CloudAnchor	<not set>
msDS-cloudExtensionAttribute1	nosync
msDS-cloudExtensionAttribute10	<not set>

20. Wiederholen Sie Schritt 12, um einen Sync anzustoßen
21. Wechseln Sie zum „**Synchronization Service**“ Tool und überprüfen Sie das der Sync erfolgreich abschließt
22. Nach Abschluss des Sync wechseln Sie zum geöffneten Browser
23. Überprüfen Sie im Admin Portal im Browser das der Benutzer von Anna Stickler nicht mehr vorhanden ist (kann eine Weile dauern...). Benutzen Sie den Refresh Button im Portal (!) um die Ansicht zu aktualisieren:

Active users



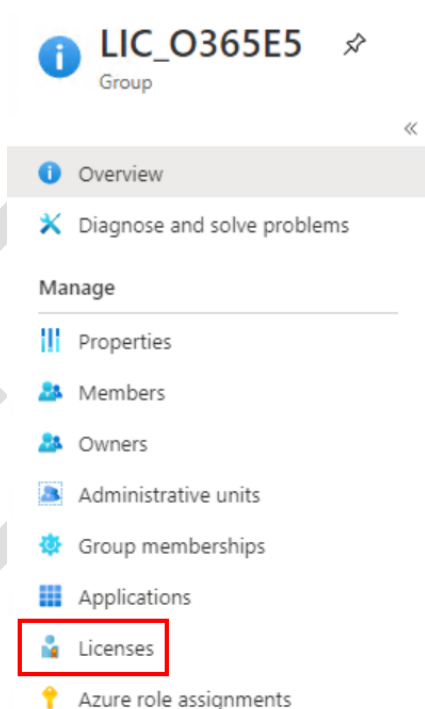
24. Schließen Sie den Synchronization Rules Editor


Aufgabe 2: Gruppenbasierten Lizenzierung

1. Wechseln Sie zu ADFS1
2. Wechseln Sie zur **Active Directory Users and Computers Konsole**
3. Erstellen Sie in der OU „**Accounts/Gruppen**“ zwei neue Gruppen mit folgenden Daten und Mitgliedern:

Name	Typ	Mitglieder
LIC_O365E5	Universal	Thomas Stickler
LIC_O365Apps	Universal	Petra Stickler

4. Starten Sie einen AAD Connect Sync (Schritt 11)
5. Wechseln Sie zum Browser und klicken Sie im Admin Portal in der Navigationsleiste links auf „... **Show all**“
6. Klicken Sie in der Navigationsleiste „**Identity**“
7. Im neuen Reiter klicken Sie links in der Navigationsleiste „**Groups/All groups**“
8. Sie sollten die Lizenzgruppen sehen...
9. Klicken Sie auf die „**LIC_O365E5**“ Gruppe
10. Im Groups Blade klicken Sie „**Licenses**“:



11. In der Menüleiste klicken Sie  **Assignments**
12. Bei „**Select licenses**“ wählen Sie die Office 365 E5 Lizenz aus und klicken

anschließend „Save“

13. Klicken Sie in der Navigationsleiste oben auf „LIC_O365E5“:

Dashboard > ETC > Groups > LIC_O365E5

14. Klicken Sie nochmals „Licenses“. Die Zuweisung sollte nun aufscheinen

15. Wiederholen Sie die Schritte 7-13 für die Gruppe „LIC_O365Apps“. Bei der Zuweisung in Schritt 11, entfernen Sie alle Checkboxes bis auf „Microsoft 365 Apps for enterprise“:

- ☐ Yammer Enterprise
- ☒ Microsoft 365 Apps for enterprise
- ☐ Skype for Business Online (Plan 2)
- ☐ Exchange Online (Plan 2)
- ☐ SharePoint (Plan 2)
- ☐ Office for the web

Save

16. Wechseln Sie im Browser zum Office 365 Admin Portal

17. Überprüfen Sie unter „Users/Active Users“, ob die Zuweisung der Lizenzen erfolgreich war:

<input type="checkbox"/>	Petra Stickler	:	Petra.Stickler@sh24111.myetc.at	Microsoft 365 E5
<input type="checkbox"/>	Raum4711	:	Raum4711@M365x08994905.onmicrosoft.com	Unlicensed
<input type="checkbox"/>	Richard Krenn	:	Richard.Krenn@sh24111.myetc.at	Unlicensed
<input type="checkbox"/>	Roland Tach	:	Roland.Tach@sh24111.myetc.at	Unlicensed
<input type="checkbox"/>	Rosa Stickler	:	Rosa.Stickler@sh24111.myetc.at	Unlicensed
<input type="checkbox"/>	Thomas Stickler	:	Thomas.Stickler@sh24111.myetc.at	Microsoft 365 E5

18. Klicken Sie auf Petra Stickler

19. Im Reiter „Licenses and apps“ überprüfen Sie, ob Petra Stickler tatsächlich nur Office zugewiesen hat:



Petra Stickler

Reset password Block sign-in Delete user

Account Devices **Licenses and apps** Mail OneDrive

View and manage Microsoft services for this user.

View products Turn on Turn off

<input type="checkbox"/>	App name	Status
<input type="checkbox"/>	Exchange Online (Plan 2)	Off
<input type="checkbox"/>	Microsoft 365 Apps for Enterprise	On
<input type="checkbox"/>	Microsoft Teams	Off
<input type="checkbox"/>	Office for the Web	Off
<input type="checkbox"/>	SharePoint (Plan 2)	Off

Lab 3: Identity Federation

Übung 1: ADFS-Installation/Konfiguration

Einleitung:

In dieser Übung wird auf dem Server ADFS1 die Active Directory Federation Service Rolle installiert und konfiguriert.

Aufgaben:

1. Konfigurieren von DNS
2. Anfordern eines Zertifikates
3. Anpassung der Gruppenrichtlinien
4. Installation ADFS
5. Single Sign On Test

Detaillierte Anleitung:

Aufgabe 1: Konfigurieren von DNS

1. Auf ADFS1 wechseln Sie zum **InPrivate** Fenster des EDGE-Browsers, in dem Sie im Azure Portal angemeldet sind
2. Navigieren Sie zur Ihrer DNS-Zone „**shX.myetc.at**“
3. Erzeugen Sie ein neues Recordset mit den folgenden Daten:

Name	Type	TTL	IP address
sts	A	300 Sekunden	Externe IP #1

4. Auf DC1 öffnen Sie die DNS Management Console
5. Erzeugen Sie in „**shX.myetc.at**“ einen neuen Record mit folgenden Daten:

Typ: A

Name: sts

IP address: 10.1.1.71

Aufgabe 2: Anfordern eines Zertifikates

1. Auf ADFS-1 öffnen Sie einen Command Prompt als Administrator

2. Fordern Sie ein Zertifikat bei Let's Encrypt für Ihre Domäne an:

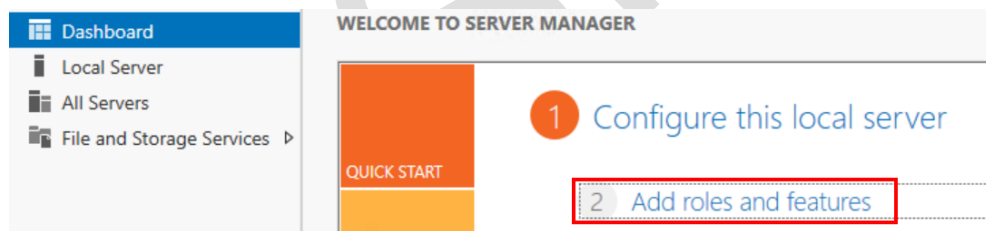
```
L:
Cd \Scripts
ADFSCertificate.cmd shX.myetc.at
```

(Beim Fehler „**Preliminary validation failed: no TXT records found**“, bitte Retry abwarten...)

3. Geben Sie „**certlm.msc**“ und drücken ENTER, um die Konsole für die Maschinen-Zertifikate zu öffnen
4. Navigieren Sie zu „**Personal/Certificates**“.
5. Überprüfen Sie, ob das Let'sEncrypt (R3) Zertifikat vorhanden ist

Aufgabe 3: Installation ADFS

1. Wechseln Sie zu ADFS1
2. Öffnen Sie den Server Manager
3. Klicken Sie „**2 Add roles and features**“



4. Klicken Sie „**Next**“ bis zur Seite „**Select server roles**“
5. Wählen Sie die Rolle „**Active Directory Federation Services**“ aus
6. Klicken Sie dreimal „**Next**“ und dann „**Install**“ – lassen Sie den Dialog geöffnet und warten Sie, bis die Installation fertig gestellt wurde...
7. Klicken Sie auf „**Configure the federation service on this server**“
8. Im ADFS Wizard klicken Sie zweimal „**Next**“
9. Auf der Seite „**Specify Service Properties**“ wählen Sie aus dem ersten Dropdown das Let's Encrypt Zertifikat aus, geben im Feld „**Federation Service Display Name**“ „**shX Federation Service**“ ein und klicken „**Next**“.
10. Auf der Seite „**Specify Service Account**“ geben Sie im Feld „**Account Name**“ „**gmsa_adfs**“ ein und klicken zweimal „**Next**“:

Specify a domain user account or group Managed Service Account.

☒ Create a Group Managed Service Account

Account Name: SMART\

11. Überprüfen Sie die von Ihnen eingegebenen Parameter und klicken „**Next**“
12. Klicken Sie „**Configure**“, um die Konfiguration zu starten
13. Nachdem der Server erfolgreich konfiguriert wurde, starten Sie ihn neu

Aufgabe 4: Anpassung der Gruppenrichtlinien

1. Wechseln Sie zu DC1
2. Öffnen Sie die Group Policy Management Konsole
3. Bearbeiten Sie die GPO „**User-Base-Policy**“
4. Im Group Policy Management Editor navigieren Sie zu „**User Configuration / Policies / Administrative Templates / Windows Components / Internet Explorer / Internet Control Panel / Security Page**“
5. Öffnen Sie Einstellung „**Site to Zone Assignment List**“
6. Klicken Sie auf „**Show**“
7. Fügen sie der Liste der Namen „**sts.shX.myetc.at**“ mit dem Wert „**1**“ hinzu und klicken „**OK**“:

Enter the zone assignments here.

	Value name	Value
	*.smart.etc	1
	smart.etc	1
▶	sts.sh1x.myetc.at	1

8. Klicken Sie „**OK**“ und schließen Sie den Group Policy Management Editor

Aufgabe 5: Single Sign On Test

1. Warten Sie 1 Minute und melden Sie sich dann an ADFS1 als „**smart\Administrator**“ an
2. Öffnen Sie eine Windows PowerShell als Administrator
3. Aktivieren Sie die IDP-Testseite im ADFS-Server:

`Set-AdfsProperties -EnableIdPInitiatedSignonPage $true`

4. Fügen Sie die Mozilla Browser als unterstützte Engine für integrierte Authentifizierung hinzu:

```
L:
cd \scripts
.\AddMozillaWIAAgent.ps1
```

5. Auf CL1 melden Sie sich als „**smart\sticklert**“ an
6. Öffnen Sie einen Command Prompt und führen Sie ein manuelles Update der GPOs durch:

Gpupdate /force
7. Öffnen Sie einen EDGE-Browser und navigieren Sie zu folgendem Link:

<https://sts.shX.myetc.at/adfs/ls/idpinitiatedsignon>
8. Klicken Sie den „**Sign in**“ Button – sie sollten automatisch angemeldet werden
9. Wiederholen Sie die Schritte 5 bis 7 auf dem physischen Host. Dieses Mal müssen Sie die Anmeldeinformation für „**smart\sticklert**“ eingeben, da der Host nicht mit Kerberos authentifizieren kann...

Übung 2: Aktivieren der Federation

Einleitung:

In dieser Übung wird die Authentication Federation mit Office 365 eingerichtet

Aufgaben:

1. Umschalten der Domain
2. Testen der Federated Authentication

Detaillierte Anleitung

Aufgabe 1: Umschalten der Domain

1. Wechseln Sie zu ADFS1
2. Öffnen Sie eine Windows PowerShell als Administrator
3. Installieren Sie das Microsoft Online PowerShell Modul – bestätigen Sie die

Abfrage mit „y“:

Install-Module msonline -Force

4. Bauen Sie eine Verbindung zum Entra ID auf – verwenden Sie zur Anmeldung Ihren Tenant-Admin:

Connect-MsolService

5. Rufen Sie die Liste der registrierten Domains ab:

Get-MsolDomain

```
PS C:\Users\administrator.SMART> Get-MsolDomain
```

Name	Status	Authentication
sh1Xmyetcat.onmicrosoft.com	Verified	Managed
sh1x.myetc.at	Verified	Managed
sh1Xmyetcat.mail.onmicrosoft.com	Verified	Managed

6. Konvertieren Sie ihre Custom-Domain in eine Federated Domain:

Convert-MsolDomainToFederated -DomainName shx.myetc.at -SupportMultipleDomain

7. Rufen Sie nochmals die Liste der registrierten Domains ab:

Get-MsolDomain

```
PS C:\Users\administrator.SMART> Get-MsolDomain
```

Name	Status	Authentication
sh1Xmyetcat.onmicrosoft.com	Verified	Managed
sh1x.myetc.at	Verified	Federated
sh1Xmyetcat.mail.onmicrosoft.com	Verified	Managed

Aufgabe 2: Testen des Zugriffs

1. Auf CL1 melden Sie sich als „smart\sticklert“ (Thomas Stickler) an
2. Öffnen Sie den EDGE-Browser und navigieren Sie zu <https://portal.office.com>
3. Melden Sie sich mit thomas.stickler@shx.myetc.at an – es darf keine Passwortabfrage kommen...

Lab 4: Exchange Hybrid

Übung 1: Vorbereitungen

Einleitung:

In dieser Übung werden die Vorbereitungen für den Exchange Hybrid getroffen. Die notwendigen DNS-Einträge werden erzeugt, ein Migrationsuser wird angelegt, die Synchronisierung von Mailbox-Berechtigungen wird aktiviert und anschließend der externe Zugriff getestet.

Aufgaben:

1. Hinzufügen von DNS-Einträgen
2. Anfordern eines Zertifikates
3. Erzeugen eines Migrationsusers
4. Test des externen Zugriffs

Detaillierte Anleitung:

Aufgabe 1: Hinzufügen von DNS-Einträgen

1. Auf ADFS1 öffnen Sie einen EDGE-Browser InPrivate Tab (CTRL+SHIFT+N) und öffnen das Azure Portal: <https://portal.azure.com>
2. Melden Sie sich mit Ihrem Azure DNS User (!) an
3. Navigieren Sie zur Ihrer DNS-Zone „shX.myetc.at“
4. Erzeugen Sie zwei neue Recordsets mit den folgenden Daten:

Name	Type	TTL	IP adress
mail	A	300 Sekunden	Externe IP#2
autodiscover	A	300 Sekunden	Externe IP#2

Aufgabe 2: Anfordern eines Zertifikates

1. Auf EX2019-1 öffnen Sie einen **Command Prompt (!)** als Administrator
2. Fordern Sie ein Zertifikat bei Let's Encrypt für Ihre Domäne an – das Zertifikat wird automatisch in Exchange eingebunden:

L:

```
Cd \Scripts
ExchangeCertificate.cmd shX.myetc.at
```

(Beim Fehler „**Preliminary validation failed: no TXT records found**“, bitte Retry abwarten...)

3. Wechseln Sie zur Exchange Management Shell
4. Kontrollieren Sie, ob ein Zertifikat von Let's Encrypt angefordert und den Exchange Diensten zugewiesen wurde:

```
Get-ExchangeCertificate | ? Subject -like "*myetc.at*" | fl
```

```
AccessRules      : {System.Security.AccessControl.CryptoKeyAccessRule,
                    System.Security.AccessControl.CryptoKeyAccessRule,
                    System.Security.AccessControl.CryptoKeyAccessRule,
                    System.Security.AccessControl.CryptoKeyAccessRule}
CertificateDomains : {mail.sh2138t.myetc.at, autodiscover.sh2138t.myetc.at}
HasPrivateKey     : True
IsSelfSigned      : False
Issuer            : CN=R3, O=Let's Encrypt, C=US
NotAfter          : 19.12.2021 19:44:31
NotBefore         : 20.09.2021 20:44:32
PublicKeySize     : 3072
RootCAType        : ThirdParty
SerialNumber      : 04D7202FAAA4DA05A9A370979EDED2967025
Services          : IMAP, POP, IIS, SMTP
Status            : Valid
```

Aufgabe 3: Test des Zugriffs nach Extern

1. Wechseln Sie zum EDGE-Browser und navigieren Sie zu <https://aka.ms/hybridconnectivity> - speichern Sie das Modul im Downloads Ordner
2. Wechseln Sie zur Exchange Management Shell
3. Importieren Sie das Hybrid Connectivity Modul:

```
cd ~\Downloads
Unlock-File .\HybridManagement.psm1
Import-Module .\HybridManagement.psm1
```

4. Testen Sie die Connectivity zu Microsoft:

```
Test-HybridConnectivity -Test0365Endpoints
```

Die Ausgabe zeigt die Tests zu den Microsoft Endpunkten (FQDNs + Ports):

```

PS C:\Users\Hybrid\Downloads> Test-HybridConnectivity -test0365Endpoints
Testing connection to mscl.microsoft.com on port 80
Testing connection to csl.microsoft.com on port 80
Testing connection to ocsps.msocsp.com on port 80
Testing connection to www.microsoft.com on port 80
Testing connection to login.windows.net on port 443
Testing connection to login.microsoftonline.com on port 443
Testing connection to aadap-portcheck-seaus.connectorporttest.msappproxy.net on port 8080
Performing GET on https://aadap-portcheck-seaus.connectorporttest.msappproxy.net:8080
Testing connection to watchdog.servicebus.windows.net on port 443
Performing GET on https://watchdog.servicebus.windows.net:443
Testing connection to outlook.office.com on port 443
Performing GET on https://outlook.office.com:443
Testing connection to outlook.office365.com on port 443
Performing GET on https://outlook.office365.com:443
Testing connection to nexus.microsoftonline-p.com on port 443
Performing GET on https://nexus.microsoftonline-p.com:443
Testing connection to login.microsoftonline.com on port 443
Performing GET on https://login.microsoftonline.com:443
WARNING: Registry Key does not exist: HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Client
WARNING: TLS 1.2 is not explicitly enabled. Please enable it.
PS C:\Users\Hybrid\Downloads>

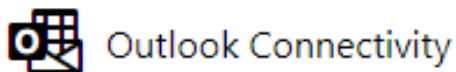
```

Aufgabe 4: Erzeugen eines Migrationsusers

1. Öffnen Sie die **Active Directory Users and Computers** Konsole
2. Erzeugen Sie in der OU **"Accounts/IT"** einen neuen Benutzer mit folgenden Eigenschaften:
 - Fullname: **Migrationuser**
 - Username: **Migrationuser**
 - Userprincipalname: **Migrationuser@shX.myetc.at**
 - Passwort: **das bekannte Standardpasswort**
 - **Password Never expires**
 - Gruppenmitgliedschaft: **Recipient Management**


Aufgabe 5: Test des Zugriffs von Extern

1. Wechseln Sie zu CL1
2. Öffnen Sie einen EDGE-Browser und navigieren zu <https://aka.ms/ExRca>
3. Klicken Sie in der Navigationsleiste links auf **„Exchange Server“**
4. Klicken Sie auf die Kachel **„Outlook Connectivity“**:



5. Geben Sie folgende Daten für den Test ein:
 - Email address: Thomas.Stickler@shX.myetc.at
 - Domain\Username (UPN): Thomas.Stickler@shX.myetc.at
 - Password: **das bekannte Standard-Passwort**
6. Aktivieren Sie die Option **„I understand that...“**
7. Geben Sie die Zeichen des Captchas ein und klicken **„Verfiy“**

8. Klicken Sie „**Perform Test**“
9. Der Test dauert einige Minuten. Der Test schlägt möglicherweise Fehl. Öffnen sie

den kompletten Report mittels  Expand All und überprüfen Sie das Ergebnis. Der Zugriff über Mapi/http muss funktionieren. Fehler beim Zugriff über RPC/HTTPS (ganz unten) können ignoriert werden...

- ✓ Testing MAPI over HTTP connectivity to server mail.sh1x.myetc.at
MAPI over HTTP connectivity was verified successfully.
- ✗ Attempting to ping RPC proxy mail.sh1x.myetc.at.
RPC Proxy can't be pinged.

Übung 2: Hybrideinrichtung

Einleitung:

In dieser Übung führen Sie den Hybrid Wizard aus, um die Hybridkonfiguration einzurichten.

Aufgaben:

1. Ausführen des Hybrid Wizards
2. Anpassen der Hybridumgebung
3. Installation des Exchange Online Management Shell Modules

Detaillierte Anleitung:

Aufgabe 1: Ausführen des Hybrid Wizards

1. Wechseln Sie zu EX2019-1
2. Öffnen Sie einen EDGE-Browser und navigieren zu <https://aka.ms/hybridwizard>
3. Klicken Sie auf „**OK**“, um die Ausführung der App zu bestätigen
4. Klicken Sie „**Install**“, um den Download und die Installation zu starten
5. Klicken Sie „**Run**“ und anschließend „**Next**“, um den Wizard zu starten
6. Auf der Seite „**On-premises Exchange Server Organization**“ belassen Sie die Standardeinstellungen und klicken „**Next**“
7. Klicken Sie „**sign in...**“ und geben Sie anschließend die Anmeldeinfo vom Tenant

Admin ein

8. Warten Sie, bis die Anmeldung erfolgt ist und klicken „**Next**“
9. Sobald die Verbindung auf beiden Seiten hergestellt ist, klicken Sie „**Next**“
10. Auf der Seite „**Hybrid Features**“ wählen Sie „**Full Hybrid Configuration**“ aus und klicken „**Next**“
11. Auf der Seite „**Hybrid Topology**“ belassen Sie die Standardeinstellung und klicken „**Next**“
12. Auf der Seite „**On-premises Account for Migration**“ klicken Sie „**Enter**“ und geben die Anmeldeinformationen von „**smart\Administrator**“ an
13. Klicken Sie „**Next**“
14. Auf der Seite „**Hybrid Configuration**“ belassen Sie die Standardeinstellung und klicken „**Next**“
15. Auf der Seite „**Receive Connector Configuration**“ wählen Sie EX2019-1 aus dem Dropdown, aktivieren die Checkbox und klicken „**Next**“
16. Auf der Seite „**Send Connector Configuration**“ wählen Sie EX2019-1 aus dem Dropdown, aktivieren die Checkbox und klicken „**Next**“
17. Auf der Seite „**Transport Certificate**“ wählen Sie das R3 Zertifikat aus dem Dropdown und klicken „**Next**“
18. Auf der Seite „**Organization FQDN**“ geben Sie „mail.shX.myetc.at“ ein und klicken „**Next**“
19. Klicken Sie „**Update**“, um die Konfiguration zu starten
20. Die Konfiguration dauert eine Weile und sollte erfolgreich abgeschlossen werden.

Aufgabe 2: Anpassen der Hybridumgebung

1. Öffnen Sie einen EDGE-Browser und navigieren zu <https://admin.exchange.microsoft.com>
2. Melden Sie sich mit dem Tenant-Admin an
3. Im Dashboard links klicken Sie „**Migration**“
4. Klicken Sie rechts oben auf „**Endpoints**“
5. Wählen Sie den Endpunkt in der Liste aus und klicken „**Edit**“
6. Klicken Sie auf „**Update**“

Migration endpoint

Hybrid Migration Endpoint - EWS (...)

Associated administrator **Update**

SMART\migrationuser

7. Tauschen Sie den Administrator durch den von uns erzeugten User „**smart\migrationuser**“ aus
8. Klicken Sie auf „**Save**“

Aufgabe 3: Installation des Exchange Online Management Shell Modules

1. Öffnen Sie eine Windows PowerShell als Administrator
2. Installieren Sie das Exchange Online Management Shell Module (bestätigen Sie die Abfrage mit **“y”**):

Install-Module ExchangeOnlineManagement -Force

3. Öffnen Sie eine Verbindung zur Exchange Online – verwenden Sie die Anmeldeinfo des Tenant-Admins:

Connect-ExchangeOnline

4. Zum Test fragen Sie die Liste der Mailboxen ab:

Get-EXOMailbox**Übung 3: Bereinigung der Empfänger****Einleitung:**

In dieser Übung bereinigen Sie E-Mail-Adressen und Aliase in Mailboxen und mail-enabled Public Folders.

Aufgaben:

1. Bereinigung der Postfächer
2. Bereinigung der Public Folder

Detaillierte Anleitung:

Aufgabe 1: Bereinigung der Postfächer

1. Wechseln Sie zu EX2019-1
2. Doppelklicken Sie den „**Exchange Admin Center**“ Shortcut vom Desktop
3. Navigieren Sie zu „**recipients/mailboxes**“
4. Öffnen Sie die Eigenschaften der Mailbox von „**Alexander Fritsch**“
5. Wechseln Sie zum Reiter „**email address**“
6. Aktivieren Sie die Checkbox „**Automatically update email addresses based on the email address policy applied to this recipient**“ und klicken anschließend **Save**
7. Wiederholen Sie die Schritte 4-6 bei den Postfächern „**Franz Wurm**“, „**Office**“ (Shared Mailbox) und „**Raum 4711**“ (Resource Mailbox)
8. Wechseln Sie zur Exchange Management Shell
9. Führen Sie ein Script aus um die „**smart.etc**“ Adressen von allen Mailboxen zu entfernen:

[.\RemoveEmailDomainFromMailbox.ps1](#)

Aufgabe 2: Bereinigung der Public Folder

1. Wechseln Sie zum EDGE-Browser und wählen Sie den Reiter mit dem OnPremises ECP aus
2. Navigieren Sie zu „**public folders**“
3. Bearbeiten Sie die Eigenschaften des Public Folder „**\Vertrieb\AT**“ – bestätigen Sie
4. Löschen Sie beim Alias alle Zeichen ab dem „**@**“ Zeichen. Der Alias sollte nun „**Vertrieb-AT**“ lauten.
5. Klicken Sie „**Save**“
6. Bearbeiten Sie erneut die Eigenschaften von „**\Vertrieb\AT**“
7. Wechseln Sie zum Reiter „**email address**“
8. Aktivieren Sie die Checkbox „**Automatically update email addresses based on the email address policy applied to this recipient**“ und klicken anschließend

“Save”

9. Bearbeiten Sie nochmals die Eigenschaften von „\Vertrieb\AT“
10. Wechseln Sie zum Reiter „**email address**“
11. Entfernen Sie die E-Mail-Adresse mit der Domäne „@smart.etc“
12. Wiederholen Sie die Schritte 3-11 für den Ordner „\Vertrieb\CZ“
13. Bearbeiten Sie den Ordner „\Vertrieb“
14. Entfernen Sie die E-Mail-Adresse mit der Domäne „@smart.etc“
15. Wiederholen Sie die Schritte 9 -11 für den Ordner „\HR\Recruiting“

Lab 5: Empfängerverwaltung

Übung 1: Postfächer

Einleitung:

In dieser Übung lernen Sie die Verwaltung der Postfächer in einer Hybridumgebung kennen.

Aufgaben:

1. Anlage einer neuen Remote Mailbox
2. Anlage einer Remote Mailbox für einen existierenden Benutzer
3. Anlage einer Remote Mailbox Raum-Ressource
4. Anlage einer freigegebenen Remote Mailbox

Detaillierte Anleitung:

Aufgabe 1: Anlage einer neuen Remote Mailbox

1. Wechseln Sie zu CL1
2. Öffnen Sie im EDGE-Browser einen neuen Reiter und öffnen das Exchange Control Panel: <https://mail.shX.myetc.at/ecp>
3. Melden Sie sich als „**administrator**“ an
4. Navigieren Sie zu „**recipients/mailboxes**“
5. Klicken Sie auf das Plus-Symbol und wählen „**Office 365 mailbox**“ aus
6. Erzeugen Sie eine neue Usermailbox mit folgenden Daten:
 - Firstname: Ihr Vorname
 - Lastname: Ihr Nachname
 - Organizational Unit: Accounts/IT
 - User logon name: vorname.nachname@shX.myetc.at
 - Mailbox type: User mailbox
 - Password: Pa\$\$w0rd
7. Wechseln Sie zum Server ADFS1 und starten Sie eine Directory Synchronisation
8. Wechseln Sie zu CL1
9. Öffnen Sie im EDGE-Browser den Reiter mit dem Exchange Admin Center

10. Navigieren Sie zu „**Recipients/Mailboxes**“
11. Stellen Sie sicher, dass die Mailbox erzeugt wurde.

Aufgabe 2: Anlage eine Remote Mailbox für einen existierenden Benutzer

1. Wechseln Sie zu EX2019-1
2. Öffnen Sie die Active Directory Users and Computers Konsole
3. Erzeugen Sie einen neuen Benutzer in der „Accounts/IT“ OU – der Name ist frei wählbar
4. Öffnen Sie eine Exchange Management Shell als Administrator
5. Aktivieren Sie für den zuvor erstellten Benutzer ein Exchange Online Postfach:

`Enable-RemoteMailbox -Identity Username
-RemoteRoutingAddress Username@m365xyz.mail.onmicrosoft.com`

6. Starten Sie auf ADFS1 eine Directory Synchronisation und prüfen anschließend, ob das Postfach in Office 365 erstellt wurde

Aufgabe 3: Anlage einer Remote Mailbox Raum-Ressource

1. Wechseln Sie zu CL1
2. Wechseln Sie zum EDGE-Browser und wählen Sie den Reiter mit dem OnPremises ECP aus
3. Navigieren Sie zu „**recipients/mailboxes**“
4. Klicken Sie auf das Plus-Symbol und wählen „**Office 365 mailbox**“ aus
5. Erzeugen Sie eine neue Usermailbox mit folgenden Daten:
 - Lastname: Raum42
 - Organizational Unit: Accounts/Resources
 - User logon name: raum42@shX.myetc.at
 - Mailbox type: Room mailbox
6. Starten Sie auf ADFS1 eine Directory Synchronisation und prüfen anschließend, ob das Postfach in Office 365 erstellt wurde

Aufgabe 4: Anlage einer freigegebenen Remote Mailbox

1. Auf EX2019-1 wechseln Sie zur Exchange Management Shell

2. Erzeugen Sie ein neues Exchange Online Ressourcen Postfach:

```
New-RemoteMailbox -Name ITSupport -DisplayName ITSupport
-Shared -UserPrincipalName ITSupport@shX.myetc.at
-RemoteRoutingAddress ITSupport@m365xyz.mail.onmicrosoft.com
-OnPremisesOrganizationalUnit "smart.etc/Accounts/IT"
```

3. Starten Sie auf ADFS1 eine Directory Synchronisation und prüfen anschließend, ob das Postfach in Office 365 erstellt wurde

Übung 2: Onboarding

Einleitung:

In dieser Übung verschieben Sie ein Postfach von OnPremises zu Exchange Online. Zuerst wird das Postfach im Hintergrund vormigriert. Anschließend wird die Migration abgeschlossen und der Zugriff sowie die Funktion getestet.

Aufgaben:

1. Pre-Staging der Postfächer
2. Abschließen des Onboardings
3. Test: Zugriff/Mailversand/Frei- Gebucht Zeiten

Detaillierte Anleitung:

Aufgabe 1: Pre-Staging der Postfächer

1. Auf CL1 melden Sie sich am Exchange Admin Center mit dem Tenant Admin an:
<https://admin.exchange.microsoft.com>
2. In der Menüleiste wechseln Sie zu „**Migration**“
3. Klicken „**Add migration batch**“ in der Symbolleiste
4. Geben Sie als Name für den Migration Batch „**Thomas Stickler**“ ein und klicken „**Next**“
5. Auf der Seite **Migration Onboarding** bei „**Select the migration type**“ wählen Sie „**Remote move migration**“ aus der Liste aus und klicken zweimal „**Next**“
6. Auf der Seite **Set endpoint** wählen Sie aus dem Dropdown den existierenden Migration Endpoint aus und klicken „**Next**“
7. Auf der Seite **Add user mailboxes** klicken Sie „**Manually add users to migrate**“,

- wählen aus der Liste „**Thomas Stickler**“ aus und klicken „**Next**“
8. Auf der Seite **Move configuration** wählen Sie die vorkonfigurierte Target Domain aus dem Dropdown und klicken „**Next**“
 9. Auf der Seite **Schedule batch migration** klicken Sie „**Save**“
 10. In der Liste der Migrationbatches klicken Sie auf „**Thomas Stickler**“
 11. Im Menü rechts klicken Sie auf „**View Details**“
 12. Prüfen Sie den Status des Batches (Validating oder Syncing odä.)
 13. Klicken Sie auf den Eintrag **Thomas Stickler** – Details der Migration werden angezeigt...
 14. Klicken Sie in der Navigationsleiste auf „**Migration**“:



Migration > **Thomas Stickler**

 Refresh

15. Prüfen Sie regelmäßig den Status der Batches (Refresh Button in der Symbolleiste) – sobald der Batch den Status „**Synced**“ zeigt, fahren Sie mit Aufgabe 2 fort...

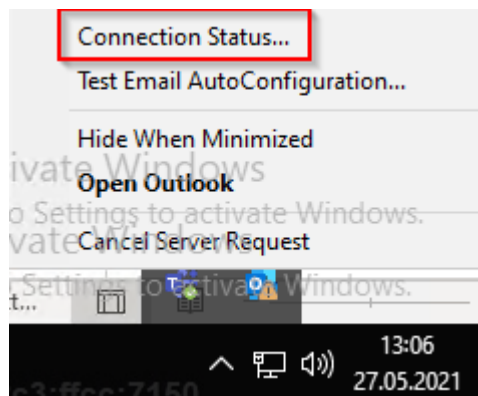
Aufgabe 2: Abschließen des Onboardings

1. Wählen Sie auf den Batch aus und klicken in der Symbolleiste „**Complete migration batch**“
2. Klicken Sie „**Confirm**“ und anschließend „**Close**“
3. Prüfen Sie regelmäßig den Status der Batches (Refresh Button in der Symbolleiste) – sobald der Batch den Status „**Completed**“ zeigt, fahren Sie mit Aufgabe 3 fort...lassen Sie den Browser geöffnet.

Aufgabe 3: Test: Zugriff/Mailversand/Frei-Gebucht Zeiten

1. Melden Sie sich an CL1 mit „**smart\sticklert**“ an
2. Starten Sie Outlook – der Start sollte normal funktionieren da Outlook über Autodiscover das Profil aktualisiert
3. Halten Sie die STRG-Taste gedrückt und klicken auf das Outlook Symbol rechts

unten und wählen „**Connection Status**“:



4. Stellen Sie sicher, dass die Verbindung zu <https://outlook.office365.com/>...
Hergestellt wurde. Sollte die Verbindung noch zum OnPremises Exchange bestehen, schließen Sie Outlook und versuchen es in ein paar Minuten nochmals...
5. Erstellen Sie eine neue Besprechungsanfrage
6. Laden Sie **Daniela Handl** zur Besprechung ein
7. Wechseln Sie zum Reiter „**Scheduling Assistant**“
8. Stellen Sie sicher, dass die Frei-Gebucht Zeiten angezeigt werden (es darf kein schraffierter Balken angezeigt werden)

	09:00	10:00	11:00	12:00	13:00
All Attendees					
Required Attendee					
<input checked="" type="checkbox"/> Thomas Stickler					
<input checked="" type="checkbox"/> Daniela Handl					

Übung 3: Konfigurieren der Exchange Recipient Management Shell

Einleitung:

In dieser Übung richten Sie die Exchange Recipient Management Shell ein um Empfänger auch ohne Exchange Server verwalten zu können.

Aufgaben:

1. Konfigurieren von Active Directory

Detaillierte Anleitung:

Aufgabe 1: Konfigurieren von Active Directory

1. Auf EXCH2019-1 öffnen Sie eine Windows PowerShell als Administrator
2. Laden Sie das Recipient Mangement Snap-In:
`Add-PSSnapin *recipientManagement`
3. Wechseln Sie in den Scripts Ordner der Exchange Installation:
`cd 'C:\Program Files\Microsoft\Exchange Server\V15\Scripts\'`
4. Starten Sie das Script zur Konfiguration des Active Directories:
`.\Add-PermissionForEMT.ps1`
5. Überprüfen Sie, ob im AD die Gruppe zur Verwaltung der Exchange Recipients erzeugt wurde:

```
Get-ADGroup -Filter {Name -like "*Recipient*EMT"}
```

```
DistinguishedName : CN=Recipient Management EMT,CN=Users,DC=smart,DC=etc
GroupCategory      : Security
GroupScope         : Universal
Name               : Recipient Management EMT
ObjectClass        : group
ObjectGUID         : 39dcbc2e-54c5-4e6a-a149-9e485c41d487
SamAccountName     : Recipient Management EMT-1-1386506633
SID                : S-1-5-21-2534669932-3506564176-2090214430-30615
```


Lab 6: Public Folders

Übung 1: Koexistenz

Einleitung:

In dieser Übung richten Sie die Koexistenz für den Public Folder Zugriff zwischen OnPremises und Exchange Online ein

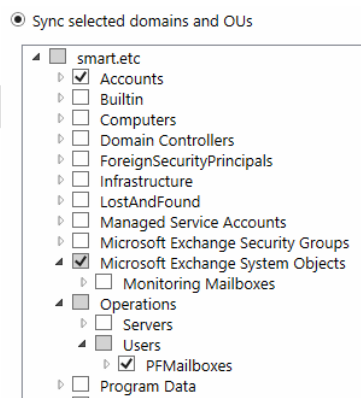
Aufgaben:

1. Anpassen der AAD Connect Synchronisation
2. Synchronisation der Mail Public Folder
3. Konfigurieren des Tenants
4. Testen des Public Folder Zugriffs

Detaillierte Anleitung:

Aufgabe 1: Anpassen der AAD Connect Synchronisation

1. Wechseln Sie zu ADFS1
2. Starten Sie den **AAD Connect** Wizard vom Desktop
3. Klicken Sie „**Configure**“
4. Wählen Sie „**Customize synchronization options**“ und klicken „**Next**“
5. Melden Sie sich mit Ihrem Tenant Admin Konto an
6. Klicken Sie „**Next**“ bis Sie zur Seite „**Domain/OU Filtering**“ kommen
7. Fügen Sie die OU „**PfMailboxes**“ und den Container „**Microsoft Exchange System Objects**“ (ohne untergeordnete Container!) zum Filter hinzu:



8. Klicken Sie zweimal „**Next**“ und anschließen „**Configure**“, um die Änderungen zu übernehmen

Aufgabe 2: Synchronisation der Mail Public Folder

1. Wechseln Sie zu EX2019-1
2. Wechseln Sie zur Exchange Management Shell
3. Benennen Sie die Remote Routing Domain um:

```
Set-AcceptedDomain -Identity IHRE-TENANT-ID.mail.onmicrosoft.com
-Name PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99
```

4. Erzeugen Sie einen neuen Ordner „C:\PF-Mig“

```
md C:\PF-Mig
```

5. Navigieren Sie zu „L:\Scripts\PF“ und starten das Script zur Synchronisation der Mail Public Folder (anmelden als Tenant-Admin):

```
L:
cd \Scripts\PF
.\Sync-ModernMailPublicFolders.ps1 -CsvSummaryFile
C:\PF-Mig\summary.txt -Confirm:$false
```

Aufgabe 3: Konfigurieren des Tenants

1. Verbinden Sie sich zur Exchange Online Management Shell:
2. Überprüfen Sie in der Exchange Management Shell, ob das Public Folder Postfach bereits als Mailuser angezeigt wird

```
Get-EOMailuser -Identity pfmailbox01@shx.myetc.at
```

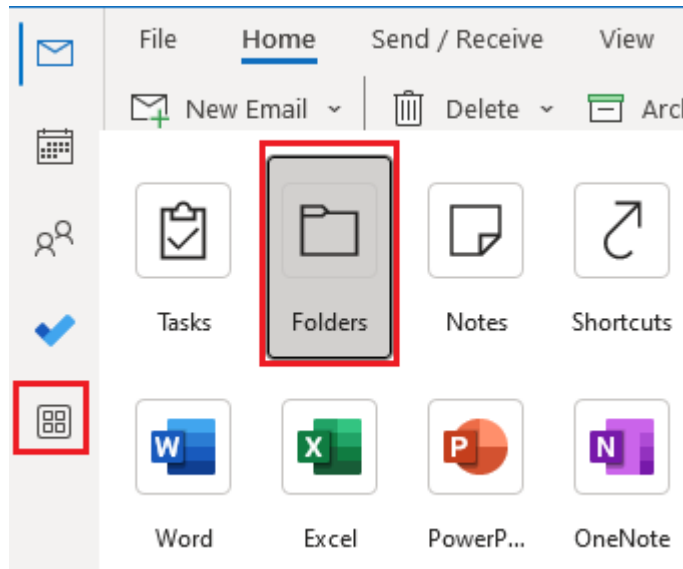
Warten Sie mit dem nächsten Schritt, bis der Mailuser angezeigt wird...

3. Konfigurieren Sie im Tenant Public Folder Zugriffe über OnPremises:

```
Set-EOOrganizationConfig -PublicFoldersEnabled Remote
-RemotePublicFolderMailboxes pfmailbox01@shx.myetc.at
```

Aufgabe 4: Testen des Public Folder Zugriffs

1. Auf CL1 melden Sie sich als „smart\sticklert“ an
2. Starten Sie Outlook
3. Wechseln Sie zur Ordnerliste



4. Stellen Sie sicher, dass die Public Folder angezeigt werden. Sollte dies nicht gleich funktionieren, versuchen Sie es zu einem späteren Zeitpunkt noch einmal...

Übung 2: Vorbereitungen zur Migration

Einleitung:

In dieser Übung bereinigen Sie die Public Folder in der OnPremises Exchange Umgebung und synchronisieren die Mail Public Folder zu Exchange Online.

Aufgaben:

1. Public Folder Mapping Datei erstellen
2. Public Folder Mailboxen in Exchange Online erstellen

Detaillierte Anleitung:

Aufgabe 1: Public Folder Mapping Datei erstellen

1. Erstellen Sie die Datei für die Public Folder Statistik

```
L:
cd .\Scripts\PF
.\Export-ModernPublicFolderStatistics.ps1
-ExportFile C:\PF-Mig\pfstat.txt
```

2. Öffnen Sie die Datei „C:\PF-Mig\pfstat.txt“ – die Statistik aller Ordner ist inkludiert
3. Erstellen Sie Mapping-Datei für die Migration

```
.\ModernPublicFolderToMailboxMapGenerator.ps1
-MailboxSize 50GB -MailboxRecoverableItemSize 25GB
-ImportFile C:\PF-Mig\pfstat.txt -ExportFile
C:\PF-Mig\pfmap.txt
```

4. Öffnen Sie die Datei „C:\PF-Mig\pfmap.txt“ – die Ordner sollten in 2 Postfächer aufgeteilt sein
5. Bearbeiten Sie die Datei und ersetzen „Mailbox“ durch „PFMailbox“ (Nummern bleiben erhalten)

Aufgabe 2: Public Folder Mailboxen in Exchange Online erstellen

1. Wechseln Sie zur Exchange Management Shell
2. Erzeugen Sie die Exchange Online Public Folder Mailboxen

```
1..2 | % {New-EOMailbox -PublicFolder -Name PFMailbox$_
-IsExcludedFromServingHierarchy $false -HoldForMigration:
>true}
```

Übung 3: Migration

Einleitung:

In dieser Übung migrieren Sie die Public Folder von OnPremises zu Exchange Online.

Aufgaben:

1. Erzeugen des Migrationsendpunktes
2. Pre-Staging der Postfächer

Detaillierte Anleitung:

Aufgabe 1: Erzeugen des Migrationsendpunktes

1. In der Exchange Management Shell erzeugen Sie den Migrationsendpunkt für Public Folder in der Cloud (sollte ein Fehler ausgegeben werden, versuchen Sie es nach einigen Minuten nochmals):

```
$SCredential = Get-Credential smart\administrator
$SRemoteServer = "mail.shx.myetc.at"
$PfEndpoint = New-EOMigrationEndpoint -PublicFolder -Name PFEP
-RemoteServer $SRemoteServer -Credentials $SCredential
-SkipVerification
```

Aufgabe 2: Pre-Staging der Postfächer

1. Speichern Sie die GUID der OnPremises Root Public Folder Mailbox in eine Variable:

```
$Guid = Get-OrganizationConfig
$Guid = $Guid.RootPublicFolderMailbox.HierarchyMailboxGuid.Guid
```

2. Speichern Sie die Public Folder mapping Datei als Byte-Folge in eine Variable:

```
[byte[]]$bytes = Get-Content C:\Pf-Mig\pfmap.txt -Encoding Byte
```

3. Erzeugen Sie den Migrationsbatch:

```
New-EOMigrationBatch -Name PFMig -CSVData $bytes -SourceEndpoint
$PfEndpoint.Identity -SourcePfPrimaryMailboxGuid $Guid
-AutoStart -NotificationEmails administrator@shx.myetc.at
```

4. Öffnen Sie das Exchange Admin Center in einem EDGE-Browser:
<https://admin.exchange.microsoft.com>
5. Navigieren Sie zu „**Migration**“
6. Wählen Sie den Public Folder Migration Batch in der Liste aus und klicken Sie rechts auf „**View Details...**“
7. Beobachten Sie den Status der beiden Benutzer und aktualisieren Sie regelmäßig... Fahren Sie erst mit Übung 4 fort, wenn der Status beider Benutzer „**Synced**“ zeigt

Übung 4: Abschließen der Migration

Einleitung:

In dieser Übung schließen Sie die Public Folder Migration zu Exchange Online ab.

Aufgaben:

1. Cutover Vorbereiten
2. Cutover
3. Test der Funktionalität

Aufgabe 1: Cutover Vorbereiten

1. Wechseln Sie zur Exchange Management Shell
2. Bereiten Sie die OnPremises Organisation für den Cutover vor:

`Set-OrganizationConfig`

`-PublicFolderMailboxesLockedForNewConnections $true`

3. Testen Sie die Auswirkung des vorigen Befehls – es sollte die Fehlermeldung „**Couldn't find the public folder mailbox**“ erscheinen...:

`Get-PublicFolder`

4. Wechseln Sie zum EDGE-Browser und wählen den Tab, in dem das alte Exchange Admin Center geöffnet ist
5. Navigieren Sie zu „**Migration**“
6. Wählen Sie den Public Folder Migration Batch in der Liste aus
7. Klicken Sie rechts auf den Link „**Complete this migration batch**“
8. In der Exchange Management Shell setzen Sie den gewünschten Zeitpunkt, zu dem die Migration abgeschlossen sein soll, auf 10 Minuten in die Vergangenheit:

`Set-EOMigrationBatch PFMIG -ApproveSkippedItems`

`Set-EOMigrationBatch -Identity PFMIG -CompleteAfter`

`(get-date).AddMinutes(-10)`

9. Aktualisieren Sie regelmäßig den Status des Batches – beginnen Sie erst mit Aufgabe 2, wenn der Status des Batches „**Completed**“ zeigt

Aufgabe 2: Cutover

1. Wechseln Sie zur Exchange Management Shell
2. Tragen Sie bei allen Mail-enabled Public Folders die Remote Routing Adresse ein:

```
L:
Cd \Scripts\PF
.\SetMailPublicFolderExternalAddress.ps1 -ExecutionSummaryFile
C:\PF-Mig\SetMailPublicFolderExternalAddress.txt -Confirm:$false
```

3. Speichern Sie die E-Mail-Adresse des Exchange Online Public Folder Postfachs „PFMailbox1“ in eine Variable

```
$emailaddress = (Get-EOMailbox -PublicFolder -Identity
pfmailbox1).windowsemailaddress
```

4. Erzeugen Sie einen OnPremises Mail User mit der Adresse der Exchange Online Public Folder Mailbox:

```
Cd ..
.\CreateMailUserForPFMailbox.ps1 -EmailAddress $emailaddress
```

5. Führen Sie den Cutover durch und konfigurieren den Remote Zugriff auf die Public Folder:

```
Set-OrganizationConfig -PublicFoldersEnabled Remote
-PublicFolderMailboxesMigrationComplete:$true
-RemotePublicFolderMailboxes pfmailbox1-exo
```

6. Schalten Sie den Public Folder Zugriff in Exchange Online auf „Local“ um:

```
Set-EOOrganizationConfig -PublicFoldersEnabled Local
-RemotePublicFolderMailboxes $null
```

7. Starten Sie den Autodiscover Application Pool neu:

```
Restart-WebAppPool MSExchangeAutodiscoverAppPool
```

Aufgabe 3: Test der Funktionalität

1. Auf CL1 melden Sie sich mit „smart\sticklert“ an
2. Starten Sie Outlook und warten Sie ein paar Minuten

3. Wechseln Sie zur Ordnerliste und überprüfen Sie den Zugriff auf die Public Folder – sollte der Zugriff nicht funktionieren, versuchen Sie es in einigen Minuten wieder... (Caching in der Cloud...)
4. Nach erfolgreichem Test melden Sie sich ab und wiederholen die Schritte 1-3 mit dem Benutzer „**smart\sticklerp**“

Lab 7: Exchange Online Protection

Übung 1: MX und SPF Record

Einleitung:

In dieser Übung erzeugen Sie den MX und SPF Record für den Mailversand von/an Exchange Online Protection.

Aufgaben:

1. Eintragen des MX und SPF Records

Detaillierte Anleitung:

Aufgabe 1: Eintragen des MX und SPF Records

1. Auf CL1 öffnen Sie das Office 365 Admin Portal im EDGE-Browser
<https://admin.microsoft.com>
2. Navigieren Sie zu „**Settings/Domains**“ (eventuell müssen Sie die Navigation erst mit „**Show all**“ erweitern...)
3. Wählen Sie Ihre Domain „**shX.myetc.at**“ aus



4. Klicken Sie in der Symbolleiste „**Manage DNS**“
5. Klicken Sie auf „**More options**“
6. Belassen Sie die Einstellungen und klicken Sie „**Continue**“
7. Erweitern Sie die Ansicht unter „**MX Records**“ und kopieren Sie den Eintrag für den MX-Record:

<div> <div> MX Records (1) </div> <div> View instructions for MX Records </div> </div>		
Record	Host Name	Points to address or value
Expected	sh2138t	sh2138t-myetc-at.mail.protection.outlook.com

8. Öffnen Sie einen EDGE-Browser InPrivate Tab (CTRL+SHIFT+N) und öffnen das

Azure Portal: <https://portal.azure.com>

9. Navigieren Sie zur Ihrer DNS-Zone „shX.myetc.at“

10. Erzeugen Sie ein neues Recordset mit den folgenden Daten:

Name	Type	TTL	Preference	Mail exchanger
@	MX	1 Stunde	0	Einfügen des Werts aus Schritt 6

11. Lassen Sie den Browser geöffnet

12. Wechseln Sie zum EDGE-Browser mit dem Office 365 Admin Portal

13. Erweitern Sie die Ansicht unter „TXT Records“ und kopieren Sie den Eintrag für den SPF-Record:

▼ **TXT Records (1)**
[View instructions for TXT Records](#)

Record	TXT name	TXT value
Expected	sh2138t	v=spf1 include:spf.protection.outlook.com -all

14. Öffnen Sie ein Notepad

15. Fügen Sie den in Schritt 13 kopierten Wert ein

16. Bearbeiten Sie den SPF-Record, sodass der OnPremises Exchange Server auch eingetragen ist:

v=spf1 include:spf.protection.outlook.com a:mail.shX.myetc.at -all

17. Kopieren Sie den neuen SPF-Record

18. Wechseln Sie zum EDGE-Browser mit dem Azure Portal

19. Erzeugen Sie ein neues Recordset mit den folgenden Daten:

Name	Type	TTL	Value
@	TXT	1 Stunde	Einfügen des Werts aus Schritt 16

20. Lassen Sie den Browser geöffnet

21. Wechseln Sie zum Browser mit dem Office 365 Admin Portal





22. Scrollen sie auf der Seite ganz hinunter

23. Aktivieren Sie „Domainkeys Identified Mail (DKIM)“

24. Kopieren Sie den ersten Wert der unter „Points to address or value“ angezeigt wird:

▼ CNAME Records (2)

[View instructions for CNAME Records](#)

Record	Host Name	Points to address or value
Expected	 selector1._domainkey.sh2411T	 selector1-sh2411T-myetc-at._domainkey.M365x41262608.onmicrosoft.com
Expected	 selector2._domainkey.sh2411T	 selector2-sh2411T-myetc-at._domainkey.M365x41262608.onmicrosoft.com

25. Wechseln Sie zum EDGE-Browser mit dem Azure Portal

26. Erzeugen Sie ein neues Recordset mit den folgenden Daten:

Name	Type	TTL	Value
Selector1._domainkey	CNAME	1 Stunde	Einfügen des Werts aus Schritt 24

27. Wiederholen Sie die Schritte 24-26 für den zweiten Wert in der Anzeige der DKIM DNS Einträge (Name des CNAME; selector2._domainkey)

28. Wechseln Sie zum Browser mit dem Office 365 Admin Portal

29. Klicken Sie „Continue“ – die DNS-Einträge werden überprüft – lediglich der Eintrag für „Autodiscover“ wird nicht richtig aufgelöst.

Übung 2: DKIM

Einleitung:

In dieser Übung richten Sie DKIM für ihre Custom-Domain ein.

Aufgaben:

1. Erzeugen der DKIM-Schlüssel
2. DKIM testen

Detaillierte Anleitung:

Aufgabe 1: Erzeugen der DKIM-Schlüssel

1. Auf EX2019-1 wechseln Sie zur Exchange Management Shell
2. Fragen Sie den DKIM-Status ab:

Get-EODkimSigningConfig

3. Wenn keine Ausgabe erfolgt, erzeugen Sie eine DKIM-Konfiguration:

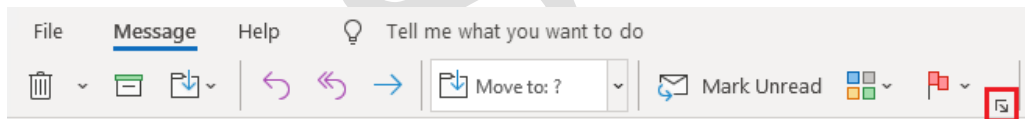
```
New-EODkimSigningConfig -DomainName shX.myetc.at -Enabled $true
```

4. Rufen Sie die DKIM Konfig ab:

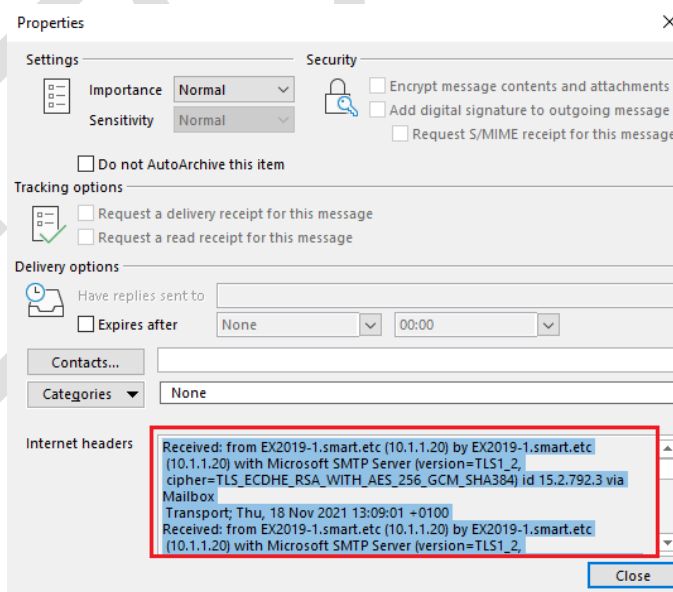
```
Get-EODkimSigningConfig
```

Aufgabe 2: DKIM testen

1. Auf CL1 melden Sie sich als Petra Stickler an
2. Öffnen Sie Outlook
3. Öffnen Sie ein InPrivate Fenster des EDGE-Browsers
4. Öffnen Sie <https://outlook.office365.com>
5. Melden Sie sich als thomas.stickler@shX.myetc.at an
6. Senden Sie ein E-Mail an Petra Stickler
7. Schalten Sie um zu Outlook und öffnen Sie das E-Mail von Thomas Stickler
8. Öffnen Sie die Emaileigenschaften:



9. Kopieren Sie die komplette Header Information:



10. Öffnen Sie in einem EDGE-Browser die Seite <https://mha.azurewebsites.net>

11. Fügen Sie die zuvor kopierte Header Info in das Feld ein und klicken auf „**Analyze Headers**“
12. Drücken Sie STRG+F und suchen Sie nach DKIM
13. Es sollte ein DKIM-Header angezeigt werden:

Microsoft Antispam Header		
Bulk Complaint Level <u>0</u>		
Source header <u>BCL:0;</u>		
Other headers		
#↓	Header	
1	ARC-Seal	i=1; a=rsa-sha256; s=ar +YR3tiSR6Tt4+rgpl5KPj
2	ARC-Message-Signature	i=1; a=rsa-sha256; c=re fyguYJPQ5GzPZ5gZCJBg uKqILQnxilrZwFMf/dcvL
3	ARC-Authentication-Results	i=1; mx.microsoft.com 1
4	DKIM-Signature	v=1; a=rsa-sha256; c=re YZwW2sriPGSItUgCWO IGebBnA9aWRu6CTcWl