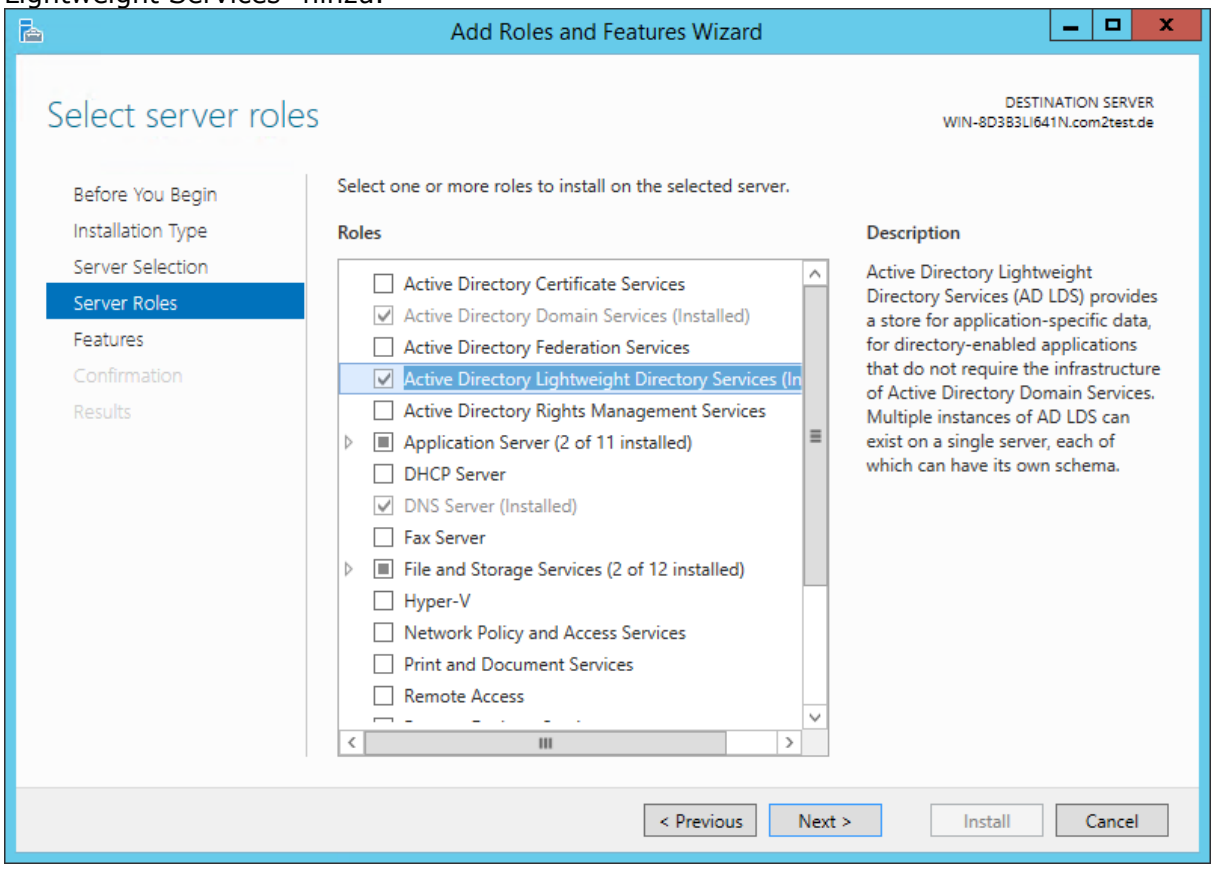
Produkt: NetOrchestra® MA
Kurzbeschreibung: ***LDAP-Import aus AD LDS konfigurieren***

Diese Anleitung hilft Ihnen, das nachfolgend geschilderte Problem zu beheben. Dazu sollten Sie über gute bis sehr gute Kenntnisse im Betriebssystem Windows verfügen. Im Zweifelsfall empfehlen wir, einen Spezialisten hinzuzuziehen. ***Die com2 Communications & Security GmbH gibt keine Funktionsgarantie und übernimmt keine Haftung für Schäden oder Verlust an Hard- oder Software und/oder Datenbeständen, die durch Anwendung dieser Anleitung entstehen könnten.***

Installation der Active Directory Lightweight Directory Services (AD LDS)

Die Installation von AD LDS erfolgt zweistufig. Als erstes muss die Software installiert werden. Öffnen Sie hierzu den Server Manager und fügen die Rolle „Active Directory Lightweight Services" hinzu.

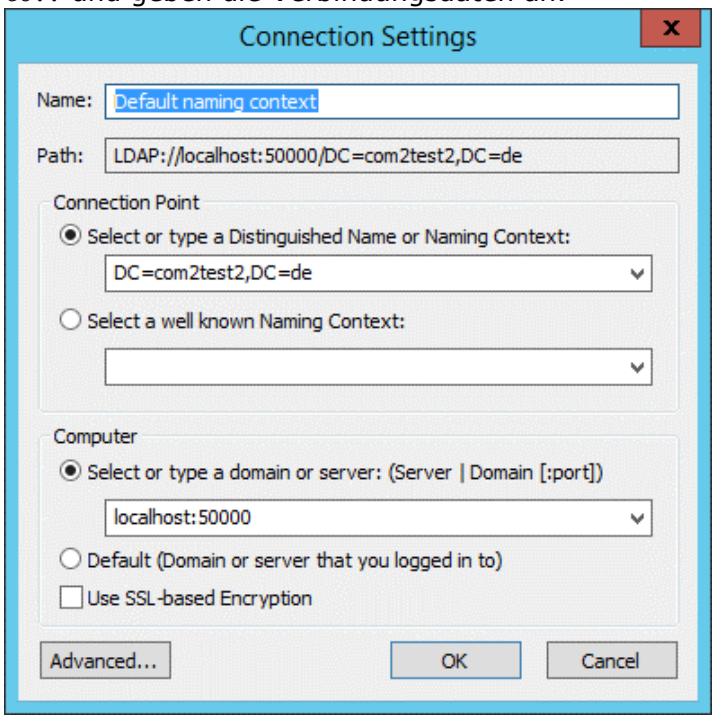


Nach der Installation muss eine Instanz angelegt werden. Achten Sie darauf in dem Wizard das LDIF-File MS-User.LDF für die Userklassen zu importieren.
Mehr Informationen zu der Einrichtung finden Sie unter:
https://forsenergy.com/en-us/adam/html/46d1d997-1dff-451f-8c02-d82ade1ae81c.htm

Verwaltung der Instanz über ADSI-Edit

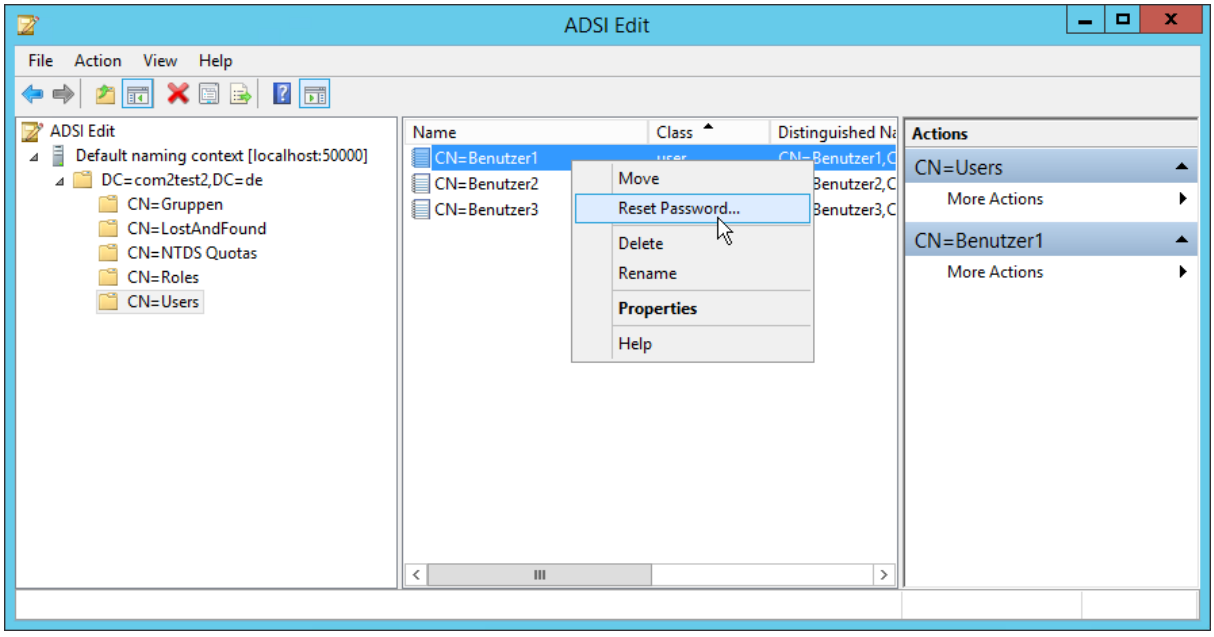
Mit Hilfe der Anwendung ADSI-Edit können Sie nun eine Verbindung mit der neu erstellten Instanz aufbauen um hierrüber das AD zu verwalten.

Starten Sie die Anwendung, öffnen die Verbindungseinstellungen über `Action` > `Connect to..` und geben die Verbindungsdaten an.

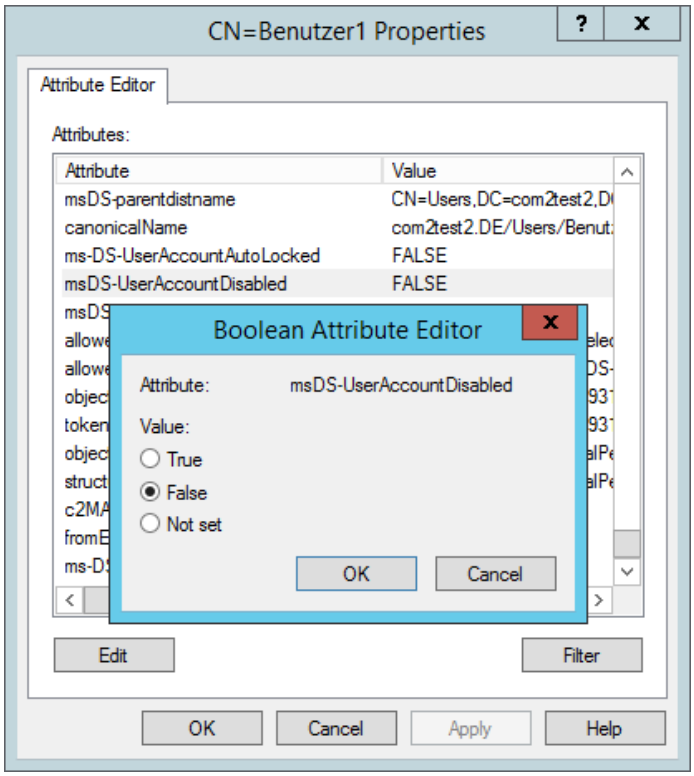


Mit der Instanz verbunden können Sie nun nach Bedarf neue Benutzer, Gruppen und Container anlegen, sowie Rechte vergeben. Damit die MA per LDAP auf das AD zugreifen darf, benötigen wir einen Benutzer der Reader- oder Administratorengruppe.

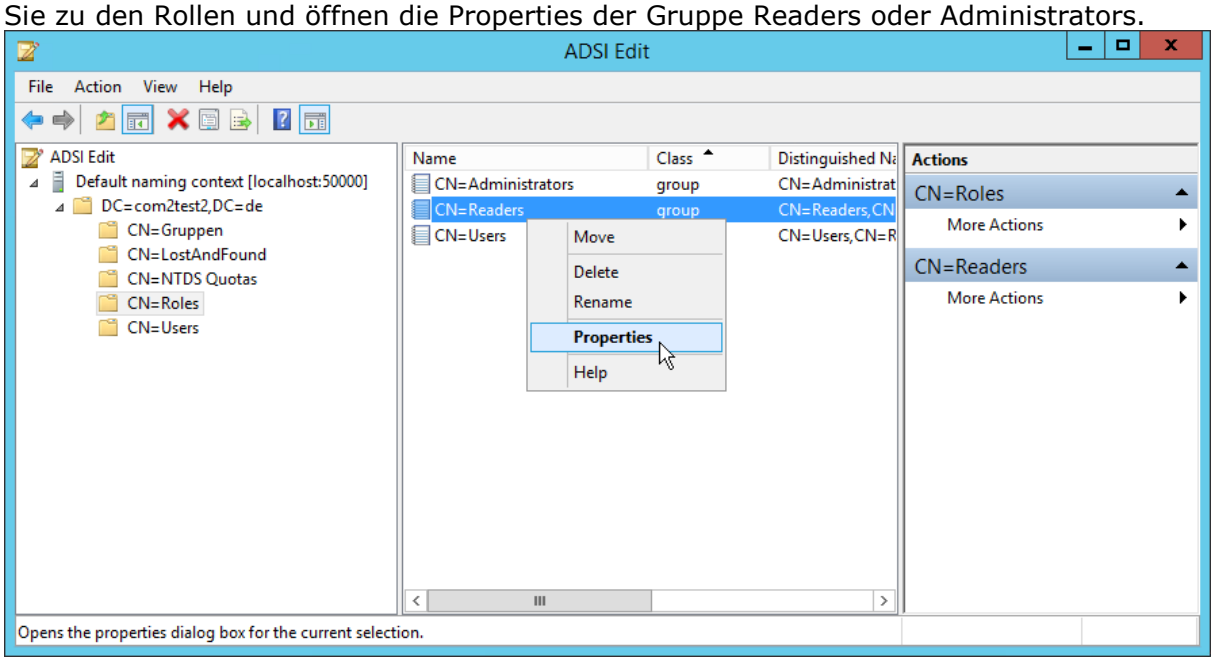
Legen Sie falls notwendig ein neues Objekt der Klasse User an und vergeben den neuen Benutzer ein Kennwort.



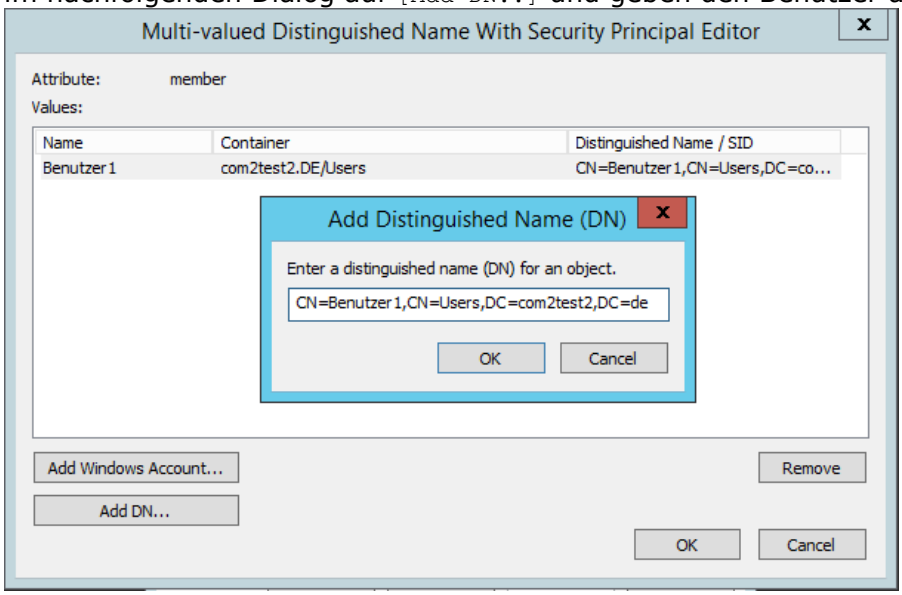
Danach muss sichergestellt werden dass der Benutzer aktiviert ist. Öffnen hierzu per Rechtsklick > Properties den Attribute-Editor und setzen wenn notwendig das Attribut `msDS-UserAccountDisabled` auf `FALSE`.



Um nun den Benutzer die für den LDAP-Import notwendige Rechte zuzuweisen, wechseln Sie zu den Rollen und öffnen die Properties der Gruppe Readers oder Administrators.



Wählen Sie im Attribute-Editor das Attribut `member` aus, editieren es mit `[Edit]`, klicken im nachfolgenden Dialog auf `[Add DN..]` und geben den Benutzer an.

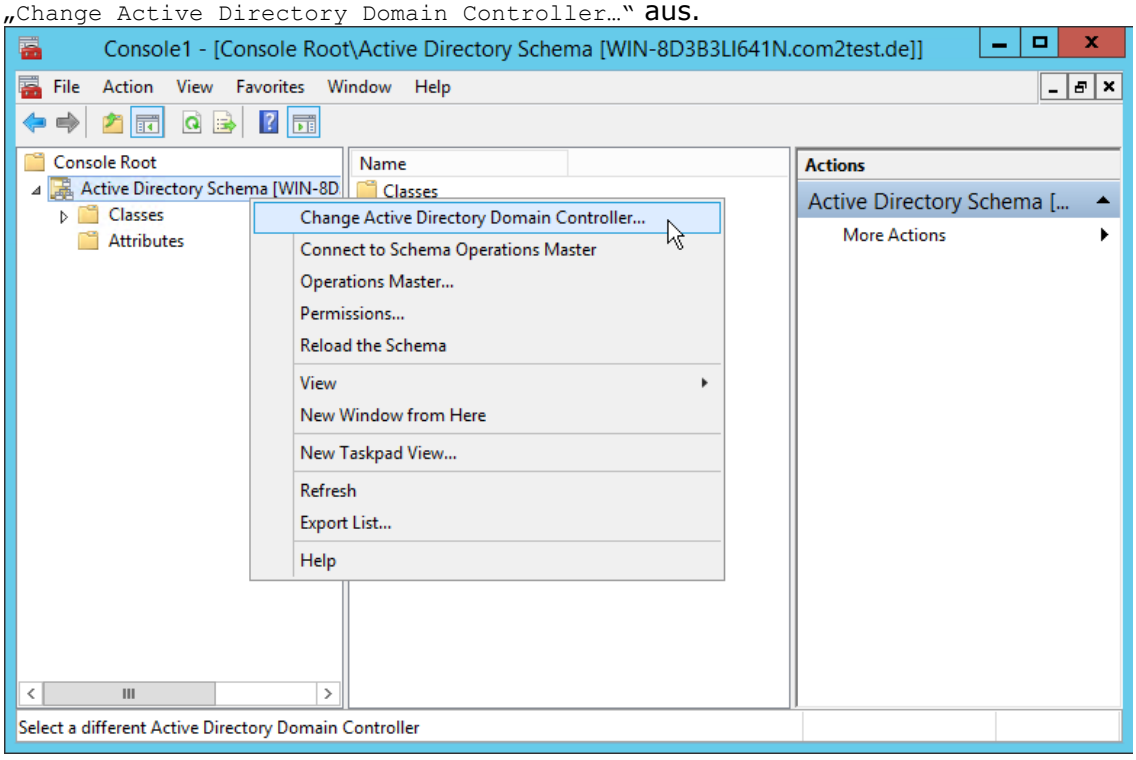


AD LDS Schema um neue Attribute erweitern

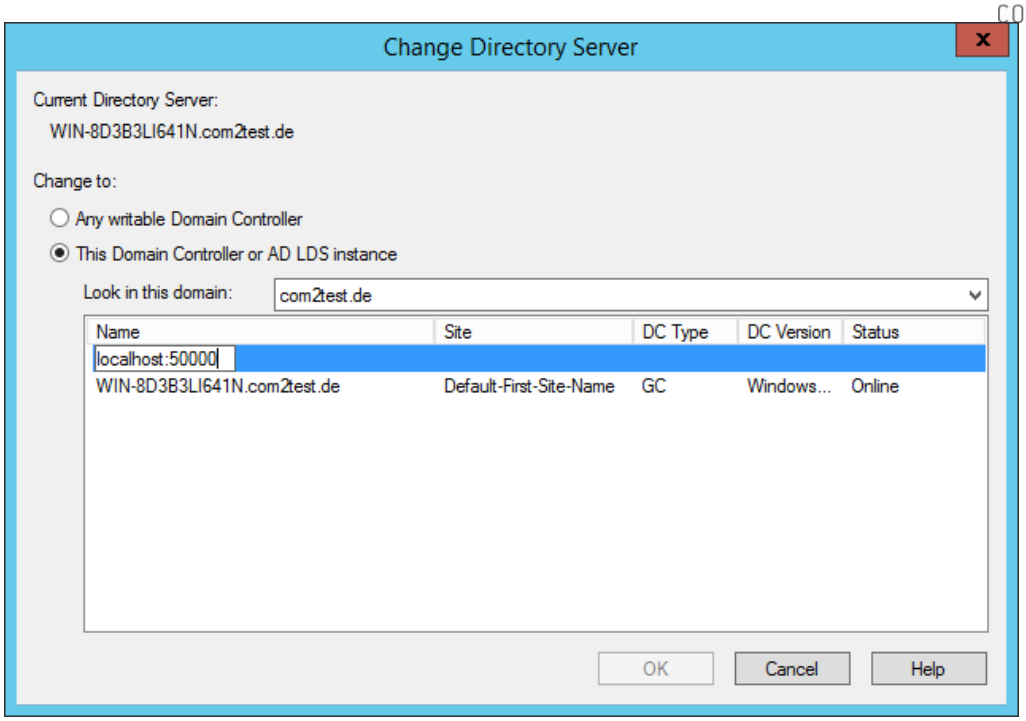
Wie die für das Mailarchiv spezifischen Attribute erstellt werden ist in unserem Technote der Schemaerweiterung beschrieben.

Wenn Sie das MMC Snap-In Active Directory Schema aufrufen müssen Sie lediglich darauf achten eine Verbindung mit der korrekten Instanz aufzubauen.

Klicken Sie dazu nachdem Sie das SnapIn hinzugefügt haben über das Kontextmenü „`Change Active Directory Domain Controller…`“ aus.



Nun können Sie die Adresse und den Port Ihrer AD LDS Instanz angeben.



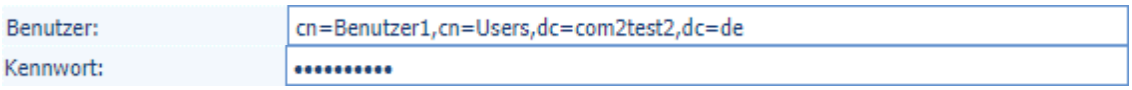
LDAP-Import auf der Net-Orchestra MA ausführen

Ist der Port für die AD LDS Instanz in der Firewall freigegeben, wie zuvor beschrieben ein Benutzer mit genügend Rechte erstellt worden und sind die zu importierenden Benutzer vollständig im AD gepflegt, können auf der Webadministration der NetOrchestra MA die neuen Verbindungsdaten für den LDAP-Import eingetragen werden.

Öffnen Sie die Webadministration Ihrer NetOrchestra MA und wechseln in die Ansicht Benutzerverwaltung > LDAP-Benutzer.

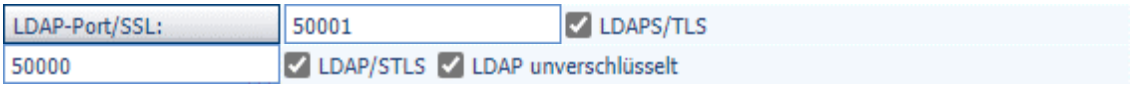
Da sich die LDAP-Abfrage mit der für einen Import aus AD DS unterscheidet und ein Import aus AD LDS über die Webadministration bisher nicht offiziell unterstützt wird, müssen die Felder wie folgt ausgefüllt werden:

Dieses Feld bitte leer lassen.



Tragen Sie den DN des für LDAP berechtigten Benutzers ein und geben das Kennwort an. Achten Sie darauf „cn=" und „dc=" wie in der Abbildung kleinzuschreiben.
<u>Achtung</u>: Wenn Sie die Webadministration neu aufrufen, werden Ihre Angaben wieder verworfen. Daher müssen Sie bevor Sie nach erneutem Laden der Webseite die Konfiguration speichern, erneut den Benutzer angeben.

Bei der Angabe des LDAP-Servers gibt es keine Besonderheiten.



Tragen Sie die Ports der AD LDS Instanz ein und wählen die zu verwendenden Verfahren aus.

Benutzersuchbasis:	DC=com2test2,DC=de
Benutzername-Feld:	sAMAccountName
Gruppensuchbasis:	CN=Gruppen,DC=com2test2,DC=de
Gruppenname-Feld:	cn

Für einen erfolgreichen Import muss der DC festgelegt werden. Um die Suche zu verfeinern können Sie zusätzlich den Container aus dem importiert werden soll angeben.

Benutzersuchfilter:	(&(|(objectClass=user)(objectClass=person)(objectClass=organizationalPerson))(!(ob
Anmeldename-Feld:	cn
Gruppensuchfilter:	(&(objectClass=group)(|(&(cn=*)(mail=*))(c2MaArchiveGroupEnabled=*)))

Den Benutzersuchfilter können Sie nach Ihrem belieben anpassen.
Fehlt bei den zu importierenden Archivierungsgruppen das Attribut `msExchRecipientDisplayType`, müssen Sie die Bedingung `(msExchRecipientDisplayType=*)` aus dem Filter entfernen.

Sind alle Voraussetzungen erfüllt können Sie nun den Import starten.