Netz-Weise
Lernen von den Besten.

Office 365 Single Sign on und Verzeichnissynchronisation

von Holger Voges

Version 1.0

Freundallee 13 a
30173 Hannover
www.netz-weise.de

Inhalt

Einführung in Office 365 und Azure AD

Wofür brauche ich Azure AD, wenn ich doch Office 365 einsetze?

Azure AD (Actice Directory) ist ein Benutzerverzeichnis, das von Microsoft ohne Installation eines eigenen Servers auf den Microsoft-Servern bereitgestellt wird. Office 365 verwendet Azure AD zur Speicherung Ihrer Office 365 Benutzerkonten. Dafür wird beim Anlegen eines Office 365-Accounts automatisch ein Azure-AD Verzeichnis angelegt.

Azure speichert Ihre Benutzerinformationen. Immer, wenn Sie im Office 365 einen neuen Benutzeraccount anlegen oder Benutzerinformationen ändern, werden tatsächlich Änderungen im Azure AD durchgeführt.

Benutzer mit einem lokalen AD zusammenführen

Um zu verhindern, dass Ihre Benutzer sich mehrere Kennwörter merken müssen – eins für Ihr Outlook und SharePoint, und eins für Ihre lokale Anmeldung am PC – hat Microsoft die Möglichkeit zur Verfügung gestellt, Ihre Benutzerkonten ins Azure AD zu synchronisieren. Dafür benötigen Sie ein Tool namens AD Connect (ehemals Dirsync), das Sie auf einem Server in Ihrem Netzwerk installieren („On Premise“). AD Connect prüft in regelmäßigen Abständen Ihre Verzeichnisse (lokales AD oder, wenn eine Rücksynchronisation gewünscht wird, auch Ihr Azure AD) und synchronisiert Daten wie Kennwörter zwischen den Verzeichnissen. Die synchronisierten Verzeichnisse bleiben nach wir vor getrennt, aber die Daten können auf dem gleichen Stand gehalten werden. Die Synchronisation kann jederzeit abgebrochen werden.

Durch AD Connect brauchen Ihre Benutzer sich nur noch ein Kennwort zu merken, da die Kennwörter im lokalen AD und im Internet immer gleich sind. Was Azure AD jedoch nicht leisten kann ist ein Single Sign on, wie er normalerweise auf einem Domänen-PC ausgeführt wird. Das bedeutet, dass z.B. der Zugriff auf Ihren Office 365 SharePoint eine zusätzliche Anmeldung auf der SharePoint Website erfordert, auch wenn das Kennwort lokal wie auf dem SharePoint dank AD Connect dasselbe ist. Um einen Single Sign on zu ermöglichen, benötigen Sie ADFS (Active Directory Federation Services).

Single Sign on mit Office 365

Damit Ihre Benutzer nicht für jede Office 365 Ressource eine Anmeldung durchführen müssen, sondern wie in einem lokalen Netzwerk üblich nur eine Anmeldung am PC durchführen und dann Zugriff auf alle Ressourcen haben, benötigen Sie Active Directory Federation Services (ADFS).

ADFS ist ein Dienst, der dazu dienst, die Anmeldungen von Websites „befreundeter“ Unternehmen in Ihr AD umzuleiten. Ein Beispiel für ähnliche Dienste, die Sie vermutlich zumindest schon oft gesehen haben, sind die Anmeldungen auf Websites via Google oder Facebook. Anstatt auf einer Website ein neues Benutzerkonto anzulegen, verwenden Sie einfach Ihren Google-Account. Das Prinzip dahinter funktioniert so, dass die Website, an der Sie sich anmelden, Ihren Client im Hintergrund an den Anmeldeserver von Google weiterleitet. Ihre Google-Anmeldeinformationen werden von Google überprüft, und wenn Sie sich korrekt angemeldet haben, wird Ihrem Client ein Anmeldetoken ausgestellt und digital signiert (vor Änderungen geschützt und mit einem Stempel versehen, der sicherstellt, dass das Anmeldetoken wirklich von Google erzeugt wurde). Dieses Anmeldetoken gibt Ihre Clientsoftware an die Website zurück. Da die Website Google vertraut, kann Sie nun die Anmeldeinformationen von Google verwenden, um für Sie ein Konto zu erstellen, dass mit dem Google-Konto verknüpft ist.

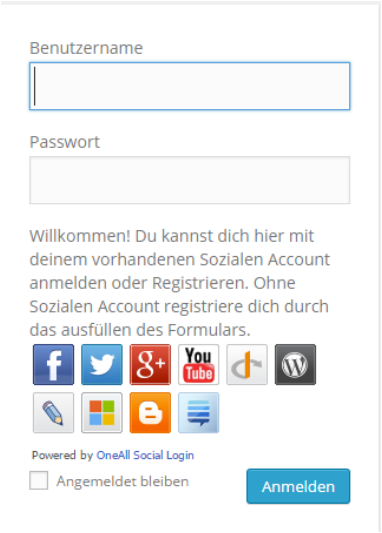


Abbildung 1 - Anmeldung per Google, Facebook, Twitter...

ADFS ist die Microsoft Implementierung dieses Dienstes. Bei Office 365 drehen Sie das Prinzip allerdings ein wenig um, denn die Website, an der Sie sich anmelden, ist in diesem Fall eine von Microsoft (Office 365-Dienste eben), und das Verzeichnis, an dem Sie sich anmelden, ist Ihr lokales AD. Die Benutzer werden jetzt also tatsächlich in Ihrem AD angemeldet! Grundsätzlich entfällt dadurch auch die Notwendigkeit, Ihr AD mit dem Azure AD zu synchronisieren, allerdings ist es empfehlenswert, AD Connect trotzdem einzurichten, da ein Ausfall oder die Nichterreichbarkeit Ihres ADFS-Servers sonst einen Totalausfall Ihres Office 365 bedeuten würde, da Ihre Benutzer sich nicht mehr anmelden könnten. Ist Ihr AAD Connect aktiv, ist nur kein Single Sign On mehr möglich.

Zugriff auf Azure AD und Office 365:

Der Zugriff auf Office 365 und Azure AD findet über zwei verschiedene Portale statt. Verwenden Sie folgende Links zur Anmeldung:

Office 365:
https://portal.office.com

Azure AD:
https://manage.windowsazure.com/
Azure AD wird derzeit noch über das alte Azure-Portal verwaltet.

Einrichtung von Azure AD

Wenn Sie eine neue Office 365 Organisation anlegen, wird automatisch ein neues Azure AD angelegt. Um auf dieses AD aber direkt zugreifen zu können, benötigen Sie einen Azure-Account. Den können Sie normalerweise direkt im Office 365 Portal anlegen. Wenn Sie allerdings bereits einen Azure-Account haben und Ihre Office 365 AD in diesen Account integrieren möchten, wird es etwas komplizierter.

Um ein bestehendes Azure mit einem neuen Office 365-Account zu verknüpfen, muss die Office365-Organisation dem Azure-AD hinzugefügt werden. Diese Zuordnung findet im alten Azure-Portal statt. Melden Sie Sich hierzu im Portal an und suchen Sie den Menüpunkt Active Directory. Klicken Sie dann unten in der Menüleiste auf Neu, um ein neues Verzeichnis anzulegen.

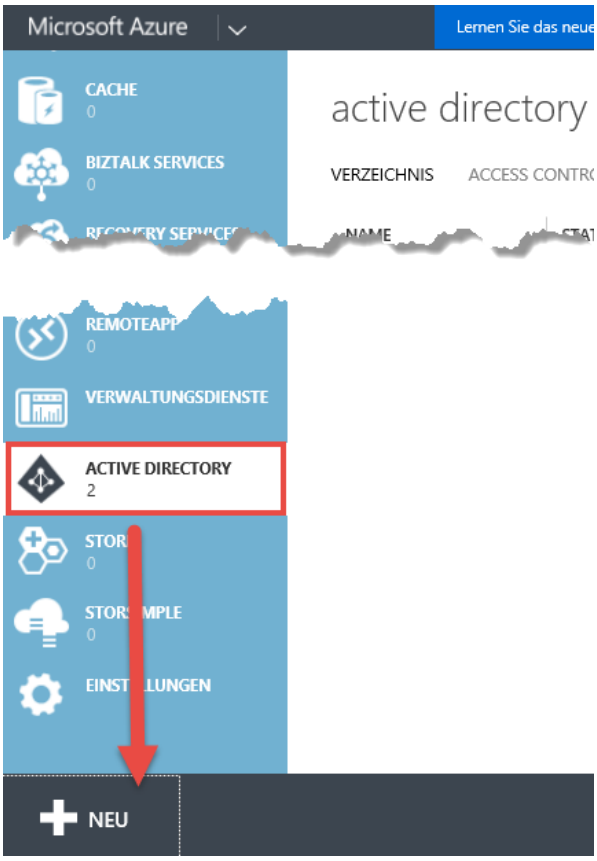


Abbildung 2 - zuerst wird ein neues Verzeichnis angelegt

Abbildung 3 - Über App-Services müssen Sie sagen, dass Sie ein Verzeichnis anlegen wollen

Da Sie ein bestehendes Office 365 AD in Ihr Azure-AD übernehmen wollen, wählen Sie „Vorhandenes Verzeichnis erstellen“.

Abbildung 4 - Jetzt geben Sie die Verzeichnisinformationen ein

Wenn Sie jetzt wählen „Ich bin für die Abmeldung bereit“, werden Sie abgemeldet. Melden Sie sich im anschließenden Anmeldefenster mit einem globalen Office 365 Administratorkonto an, um das Office 365 mit Ihrem Azure AD zu verknüpfen.

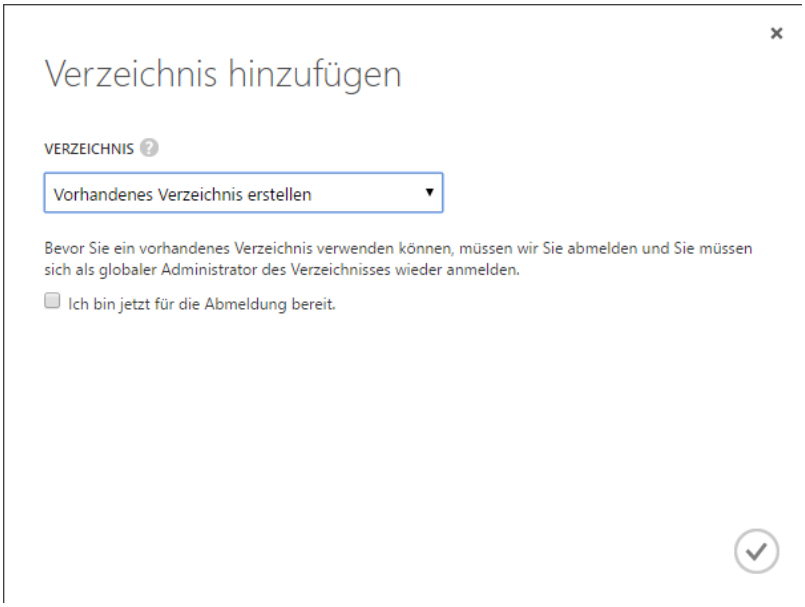


Abbildung 5 - Abmelden und mit Office 365 Administrator anmelden

Wenn Sie das Verzeichnis verknüpft haben, müssen Sie es auf Ihr Standardverzeichnis umstellen. Gehen Sie dafür im linken Menü auf den untersten Punkt, Einstellungen (nicht im Menü Active Directory!), wählen Sie Ihr Abonnement und wählen Sie Verzeichnis bearbeiten.

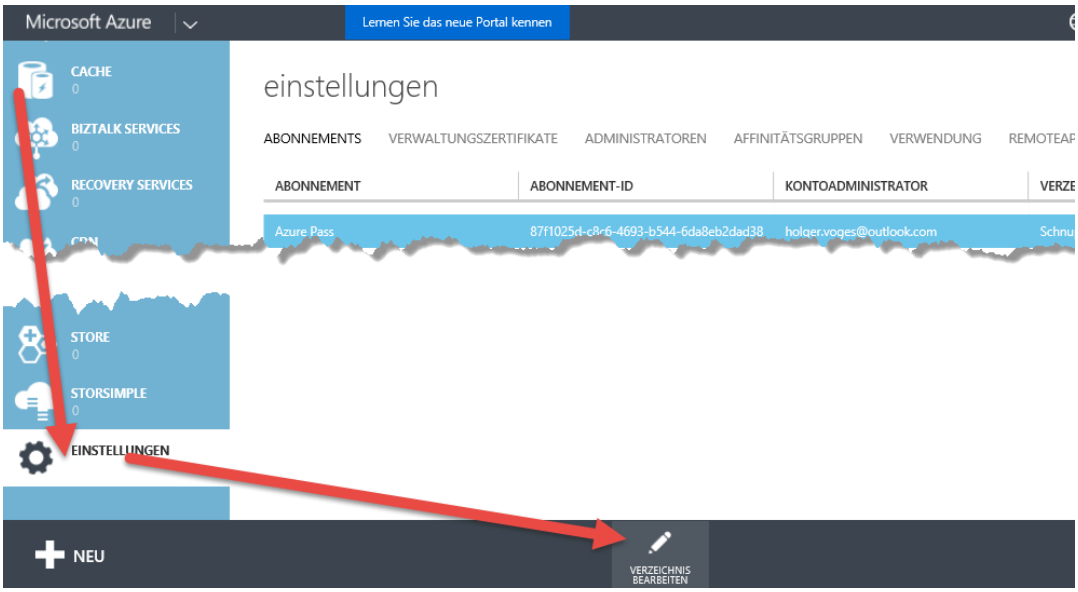


Abbildung 6 - Bearbeiten Sie Ihr Verzeichnis

Wählen Sie nun oben das Abonnement (können mehrere sein, wenn Ihrem Konto mehrere Abonnements zugeordnet sind) und unten das mit Ihrem Office 365 hinzugefügte Verzeichnis aus.

Abbildung 7 - Wählen Sie oben Ihre Azure Abonnement und im Drop-Down-Fenster das AD-Verzeichnis

Nun berechtigen Sie **die Office365-Administratoren, die Berechtigungen im AD haben sollen,** als Co-Administrator, damit er Zugriff auf das Azure-AD hat.

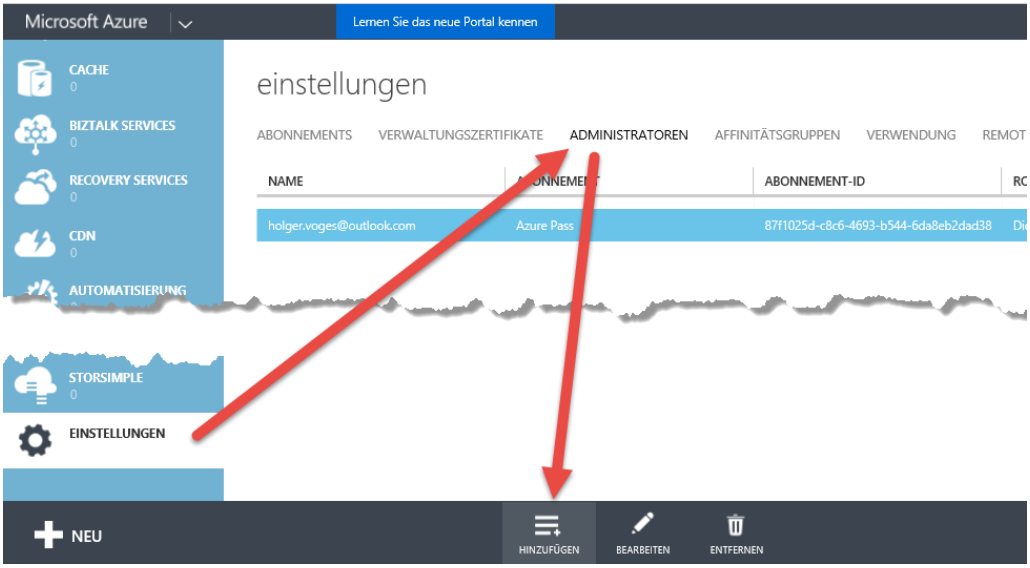


Abbildung 8 - Gehen Sie auf Einstellungen - Administration

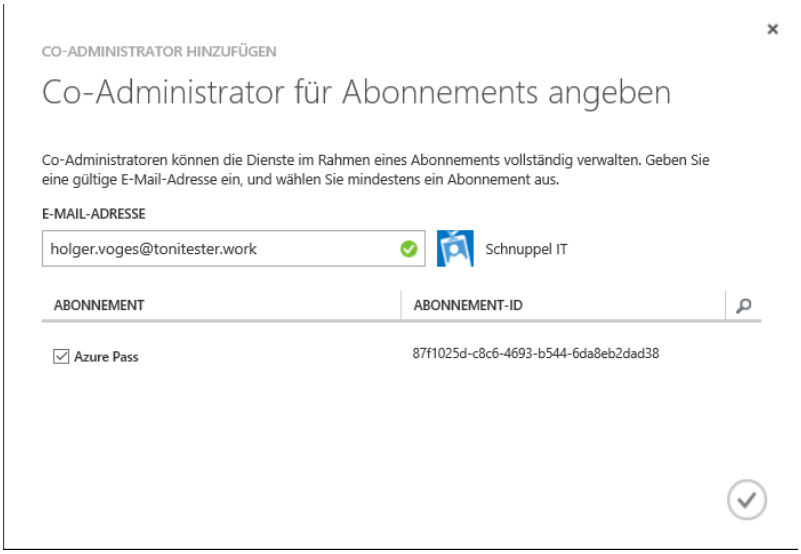


Abbildung 9 - Wenn die AD-Zuordnung funktioniert hat, finden Sie hier Ihre Office 365 Benutzer

Office 365 und Azure AD sind jetzt miteinander verknüpft.

ADFS

ADFS benötigen Sie für den Single Sign on. Mindestvoraussetzung, um ADFS nutzen zu können, ist ein ADFS-Server. Da ohne den ADFS-Dienst eine Anmeldung an Ihrem AD nicht mehr möglich ist, sollten Sie für Produktivumgebungen eine ADFS-Farm in Betracht ziehen. ADFS-Farmen machen Ihre ADFS-Server hochverfügbar (mehr dazu weiter unten). Zusätzlich benötigen Sie vermutlich einen ADFS-Proxy. Ein ADFS-Proxy ist ein Reverse-Proxy, der die Client-Anfragen aus dem Internet in Ihr lokales Netzwerk weiterleitet.

ADFS installieren

Für die Installation des ADFS-Servers benötigen Sie in öffentliches SSL-Zertifikat. Hier beschreibe ich, wie Sie ein 90 Tage gültiges Testzertifikat bei Comodo beantragen und für die Installation bereitstellen können.

SSL Zertifikats-Request erstellen

Um ein Zertifikat bei einer Zertifizierungsstelle zu beantragen, benötigen Sie eine Zertifikats-Anforderung (Certificate Request). Die kann Ihnen z.B. von der IIS-Konsole erstellt werden. Einfacher geht es aber mit einem freien Tool von Digicert, die selber auch Zertifikatsanbieter sind. Laden Sie dazu einfach das Digicert Certificate Utility for Windows https://www.digicert.com/util/ auf den Rechner, auf dem das Zertifikat erstellt werden soll, herunter. Wichtig ist, dass Sie das Tool wirklich auf dem Rechner starten, auf dem das Zertifikat installiert werden soll, da mit der Zertifikatsanforderung ein privater Schlüssel erstellt wird, der den Rechner nicht verlässt und der zusammen mit dem Zertifikat benötigt wird. Den Schlüssel später auf den Zielrechner zu exportieren ist zwar möglich, aber sehr umständlich. Das Certificate Utility muss auch nicht installiert werden, insofern sollte der Aufruf auch auf einem Server unproblematisch sein.

Das Tool kommt in einem Zip-File. Entpacken Sie es und starten Sie DigicertUtil.exe. Nachdem Sie dem Lizenzvertrag zugestimmt haben, öffnet sich die Digicert-Konsole. Hier Wählen Sie gleich im ersten Fenster oben rechts den Eintrag „Create CSR“.

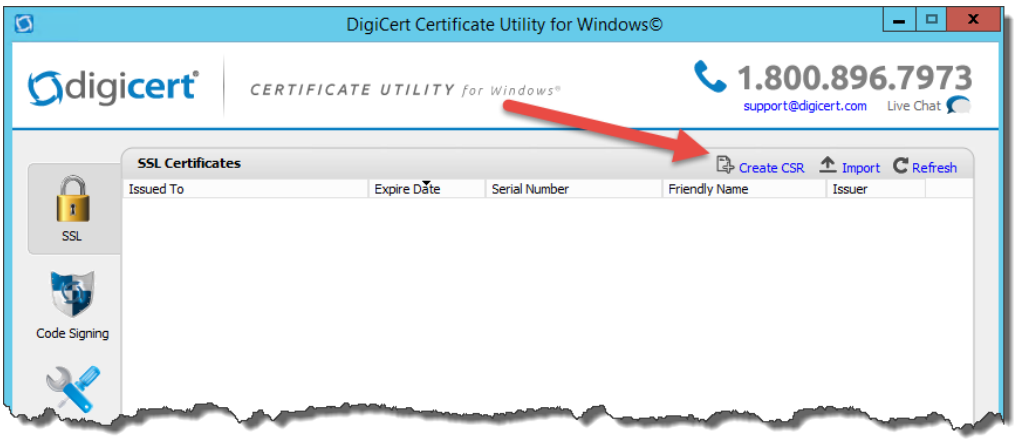


Abbildung 10 - Starten Sie den Assistenten über "Create CSR"

Geben Sie jetzt die Zertifikatsinformationen ein. Das Utility gibt dabei auch Hilfestellung – auf der rechten Seite finden Sie Informationen zu den Daten, die gewünscht sind.

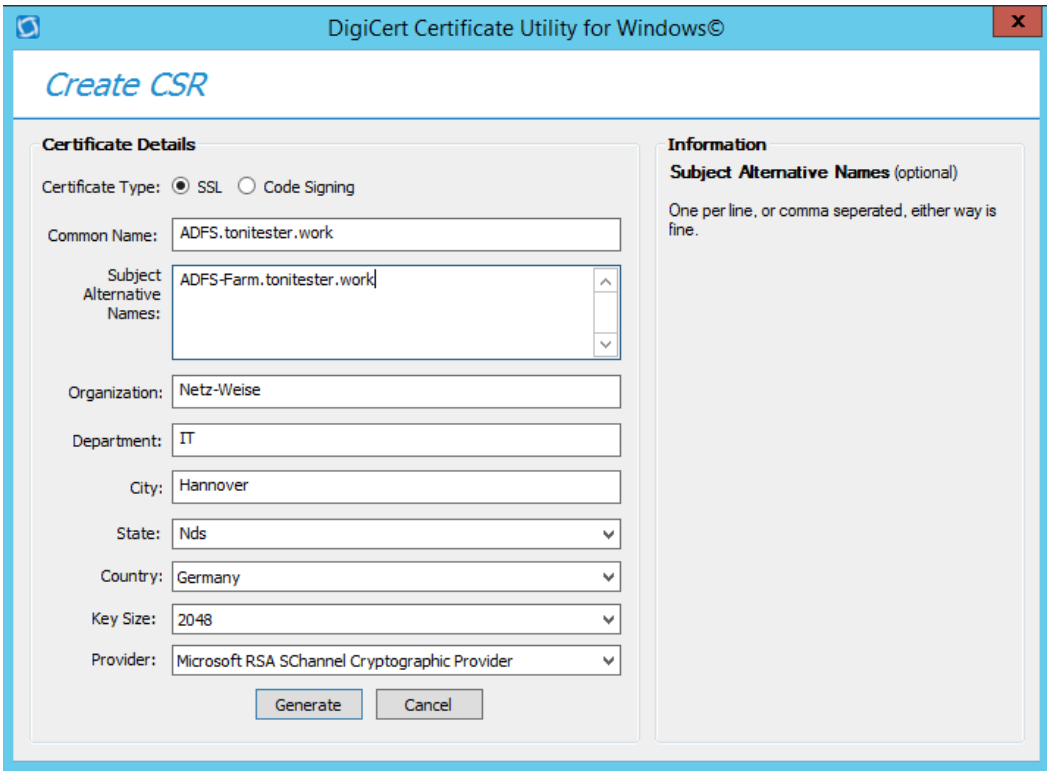


Abbildung 11 - Geben Sie die relevanten Zeritifikatsinformationen ein

Die meisten Daten hier sind selbsterklärend. Als Zertifikatstyp wählen Sie in unserem Fall SSL. Code Signing Zertifikate benötigen Sie für die Signatur von Programmen oder Powershell-Scripten. Als Common Name (CN) wählen Sie den DNS-Namen, unter dem der Server angefragt wird (in meinem Fall ADFS.Tonitester.work). Wenn Ihr Server unter mehreren Namen erreichbar sein soll, können Sie im Feld „Subject Alterative Names“ weitere Namen eingeben. Im Feld Key Size übernehmen sie am besten die Standardvorgabe von 2048 Bit. Anschließend klicken Sie auf „Generate“. Das Zertifikats-Utility generierte Ihnen dann einen Textschlüssel, der den Request darstellt und den Sie bei der Zertifikats-Registrierungsstelle einreichen müssen. Den Request können Sie in einer Textdatei speichern oder gleich ins Clipboard kopieren.

SSL-Zertifikat beantragen

Gehen Sie jetzt zu www.comodo.com. Comodo ist ein Anbieter für offiziell anerkannte Zertifikate. Wählen Sie auf der Startseite „SSL Certificate“ und dann „Free SSL Certificate“.

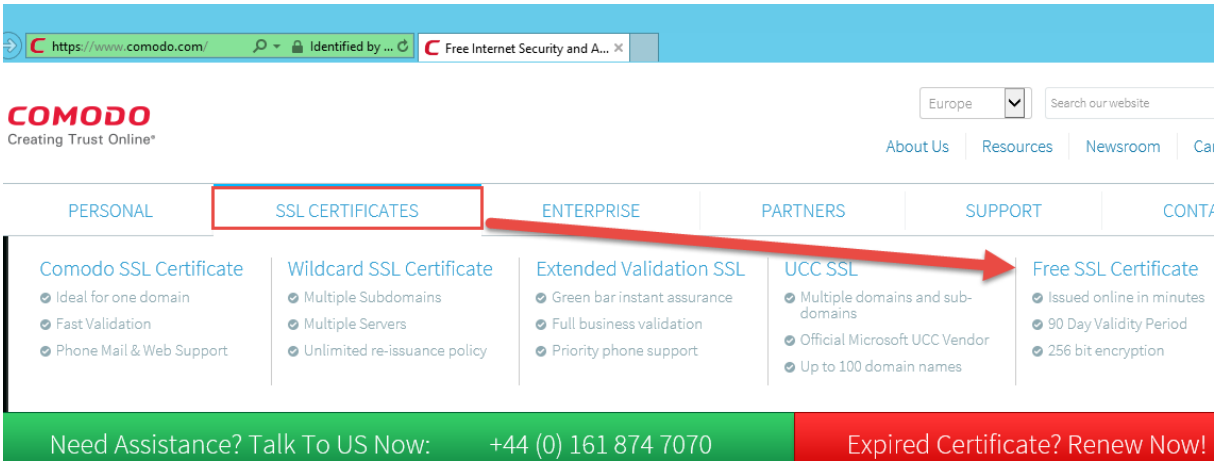


Abbildung 12 - Freies SSL-Zertifikat beantragen

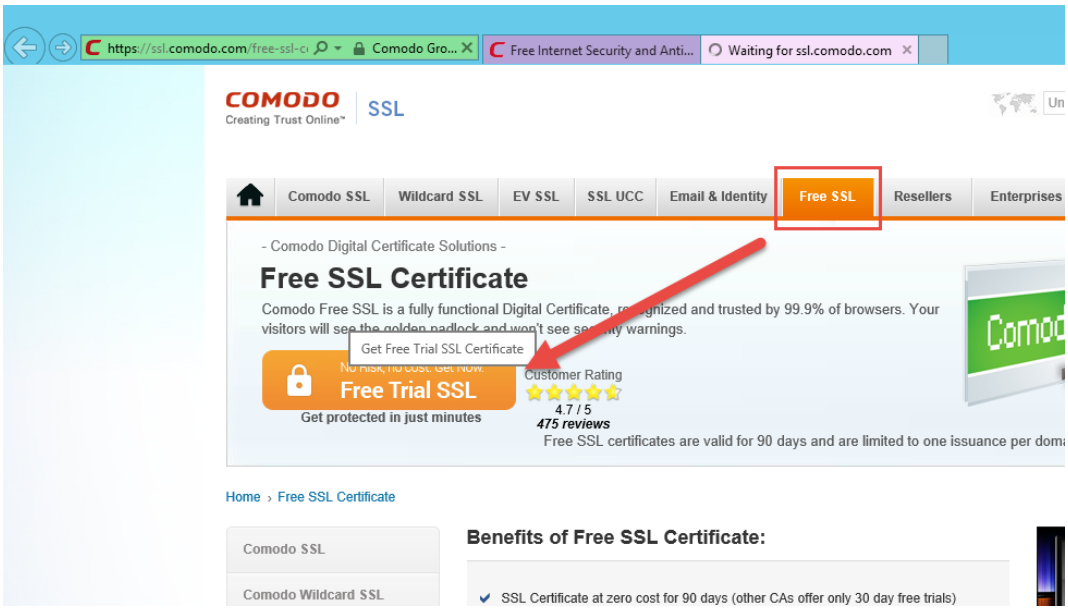


Abbildung 13 - Klicken Sie auf Free Trial SSL

Nun benötigen Sie den Zertifikats-Request, den Certutil Ihnen erzeugt hat. Kopieren Sie ihn in das entsprechende Feld unter „Provide your CSR“.

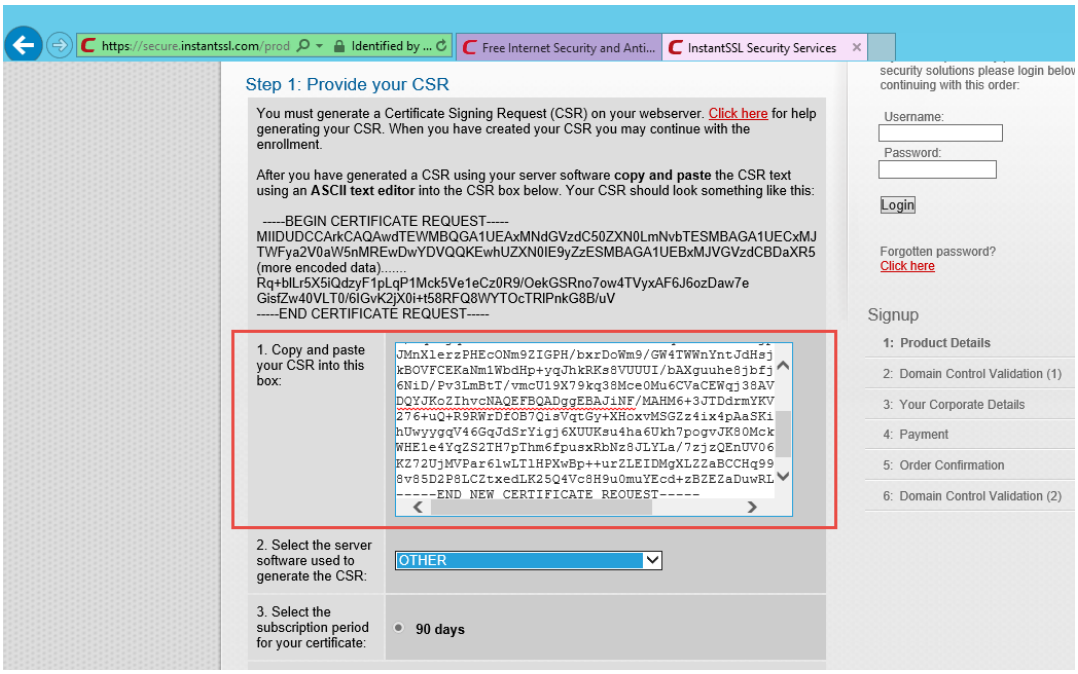


Abbildung 14 - Reichen Sie Ihren SSL-Zertifikatsrequest ein

Um zu validieren, dass Sie wirklich der Besitzer der Domäne sind, liest Comodo den Admin-C aus Ihrem DNS-Eintrag. Es werden auch alternative Adressen angegeben. Die Adresse wird verwendet, um eine Validierungsmail zu schicken.

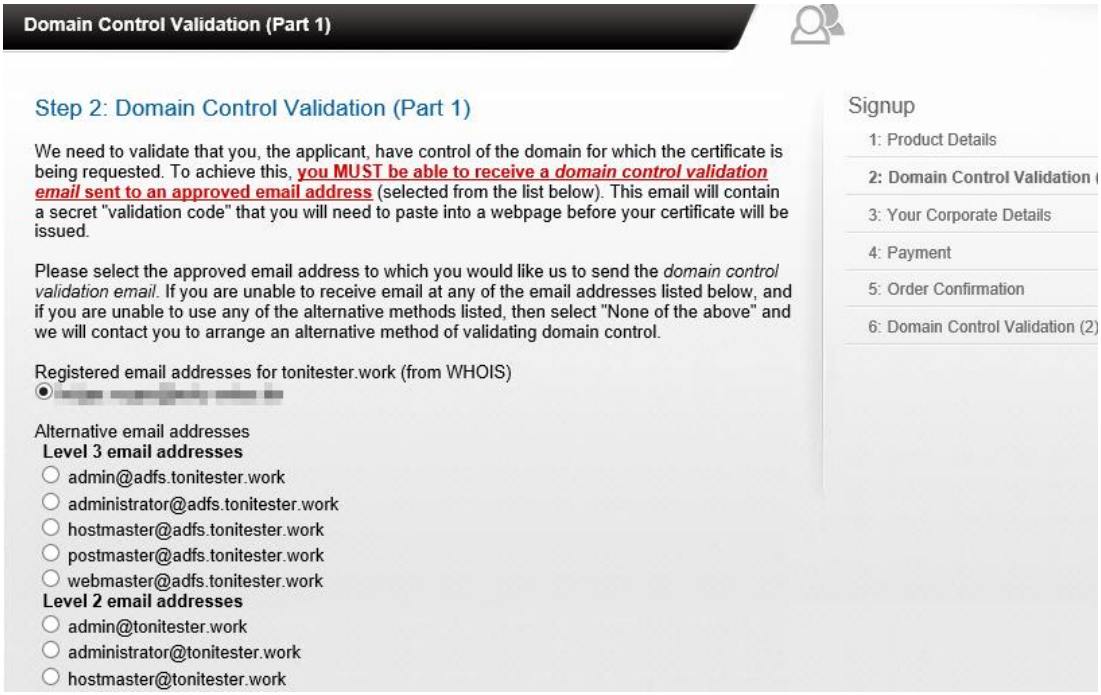


Abbildung 15 - Ihr Zertifikat wird überprüft.

Legen Sie außerdem ein Benutzerkonto bei Comodo an.

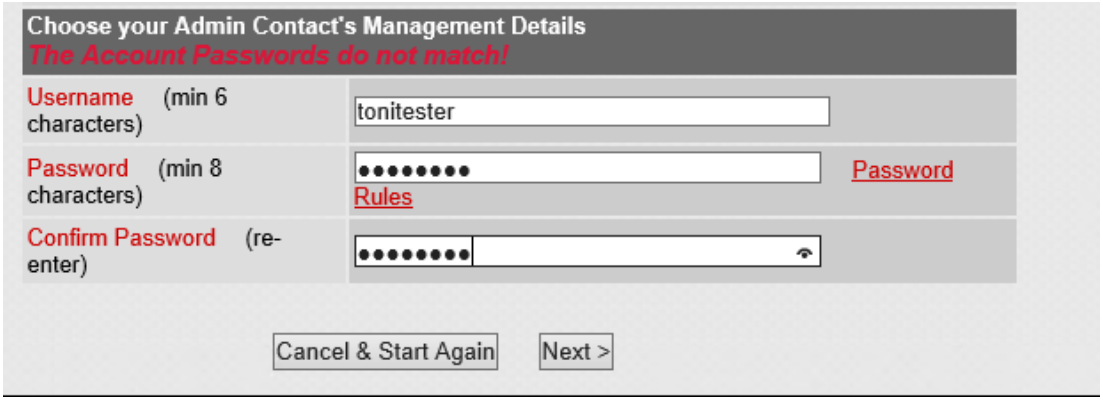


Abbildung 16 - Adminkontakt anlegen

Es wird ein Validierungscode an die ausgewählte email-Adresse verschickt. Dieser muss unter Domain Control Validation eingegeben werden.

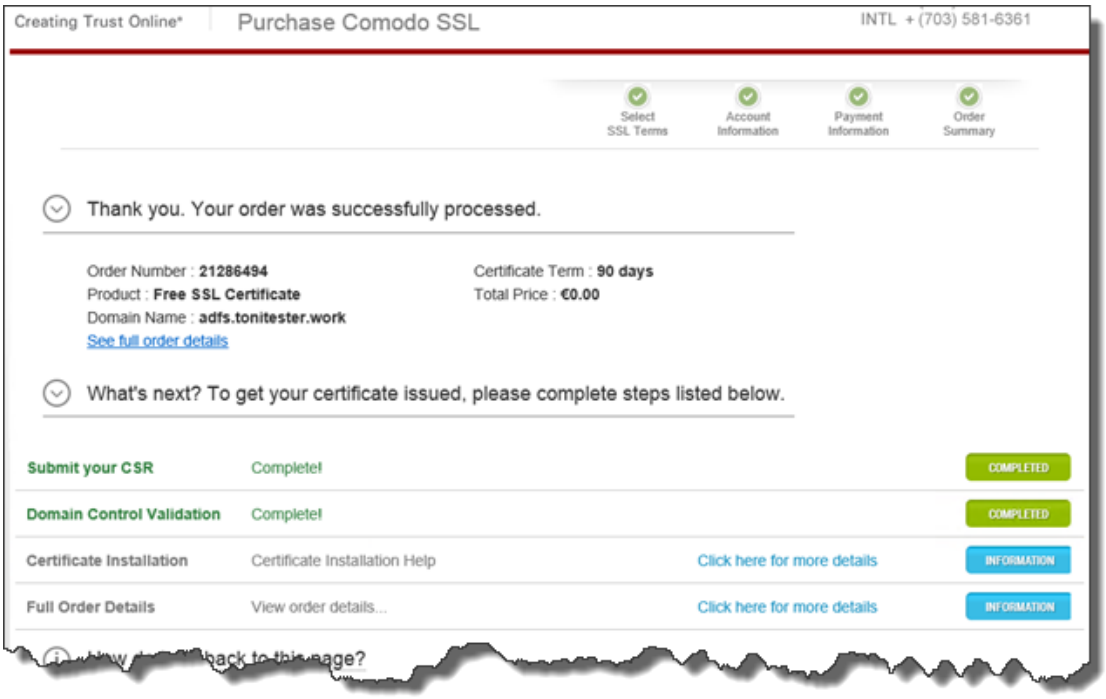


Abbildung 17 - Die Beantragung ist abgeschlossen

Das Zertifikat kommt innerhalb weniger Minuten als ZIP-Datei per email. Kopieren Sie die ZIP-Datei auf den ADFS-Server, entpacken Sie sie und installieren Sie die crl-Datei, die dem Namen Ihrer Domäne entspricht. Die anderen mitgelieferten Zertifikate sind die Zertifikate der Stammzertifizierungsstelle und die Zertifikatskette. Sie werden nicht benötigt.

Zur Installation öffnen Sie einfach das Kontextmenü des Zertifikats und wählen „Install Certificate“.

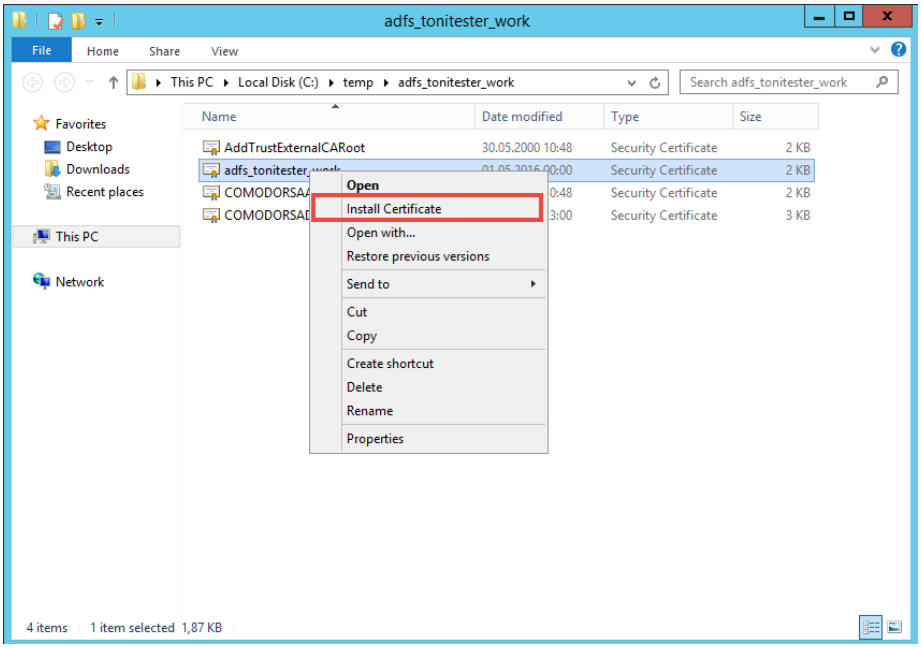


Abbildung 18 - Kopieren Sie das Zertifikat auf den ADFS-Server und instalieren Sie es

Wählen Sie den Zertifikatsspeicher des Computers aus.

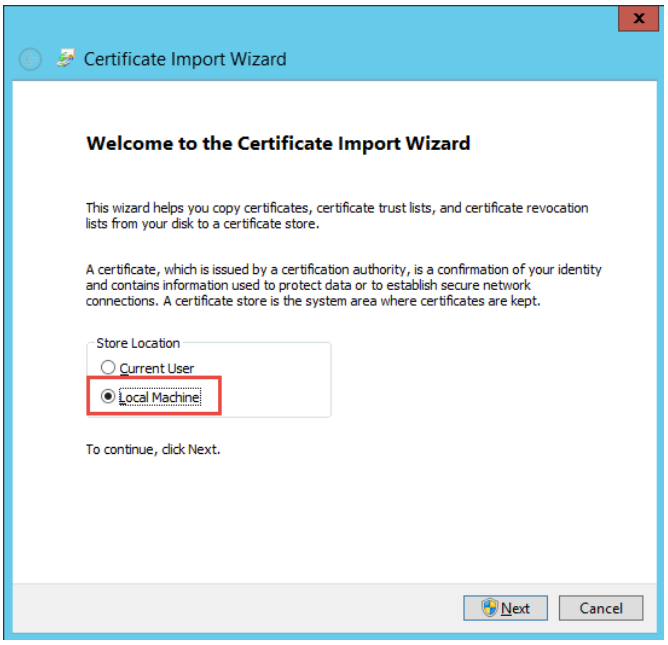


Abbildung 19 - Installation in den Zertifikatsspeicher des Computers

ADFS-Server installieren (Windows Server 2012 R2)

Im nächsten Schritt installieren Sie den ADFS-Dienst. Dieser muß zuerst über den Servermanager oder Powershell hinzugefügt werden. Starten Sie hierzu den Server Manager (Windows Server 2012 / 2012 R2) und wählen den *Add Roles and Features Wizard* im Menü *Manage* aus.

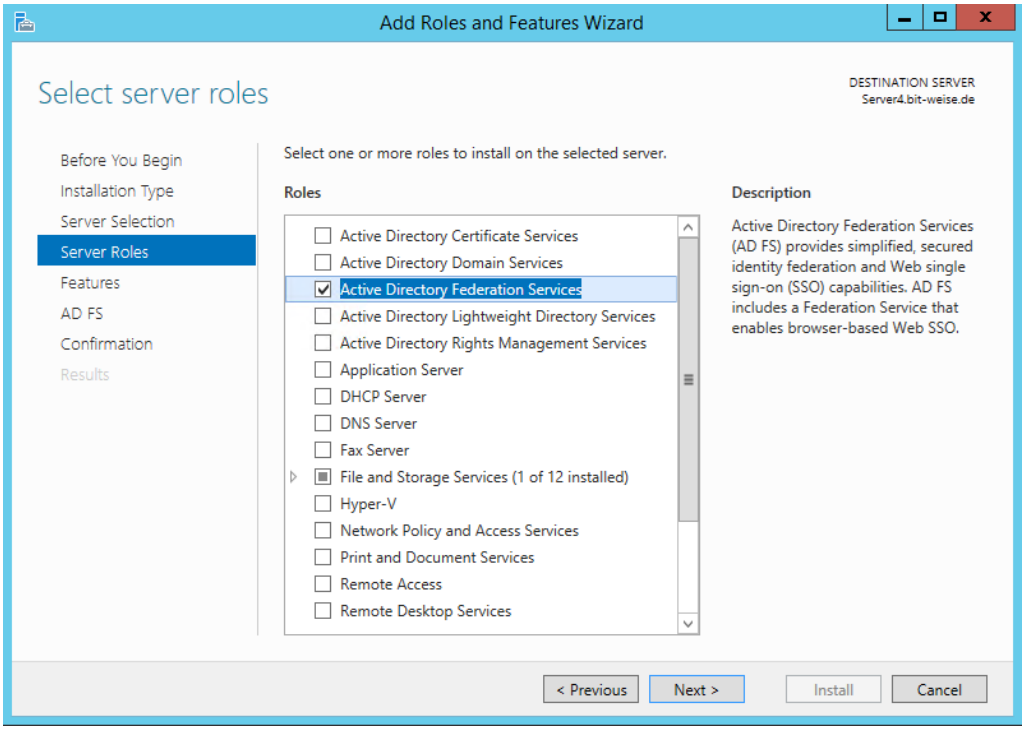


Abbildung 20 - Add Roles and Features Wizard

Alternativ können Sie die Rolle auch über Powershell nachinstallieren:

```
Install-WindowsFeature -Name ADFS-Federation -IncludeAllSubFeature -
IncludeManagementTools
```

Wenn die Installation abgeschlossen ist, können Sie direkt aus dem Wizard heraus den Installationsassistenten für ADFS starten.

Im Willkommens-Fenster müssen Sie angeben, ob Sie den ersten Server in einer Farm installieren möchten, oder schon eine Farm haben und weitere Server hinzufügen wollen. Farmen benötigen Sie für die Hochverfügbarkeit von ADFS. Sie können die Zugriffe über einen Load-Balancer dann auf mehrere Server verteilen. Eine Farm benutzt eine gemeinsame SQL-Server Datenbank. Weitere Anpassungen sind nicht notwendig. Insofern können weitere Server einfach der Farm hinzugefügt werden, nachdem der erste Server die Farm erstellt hat. Im Beispiel erstellen wir den ersten Server in einer neuen Farm.

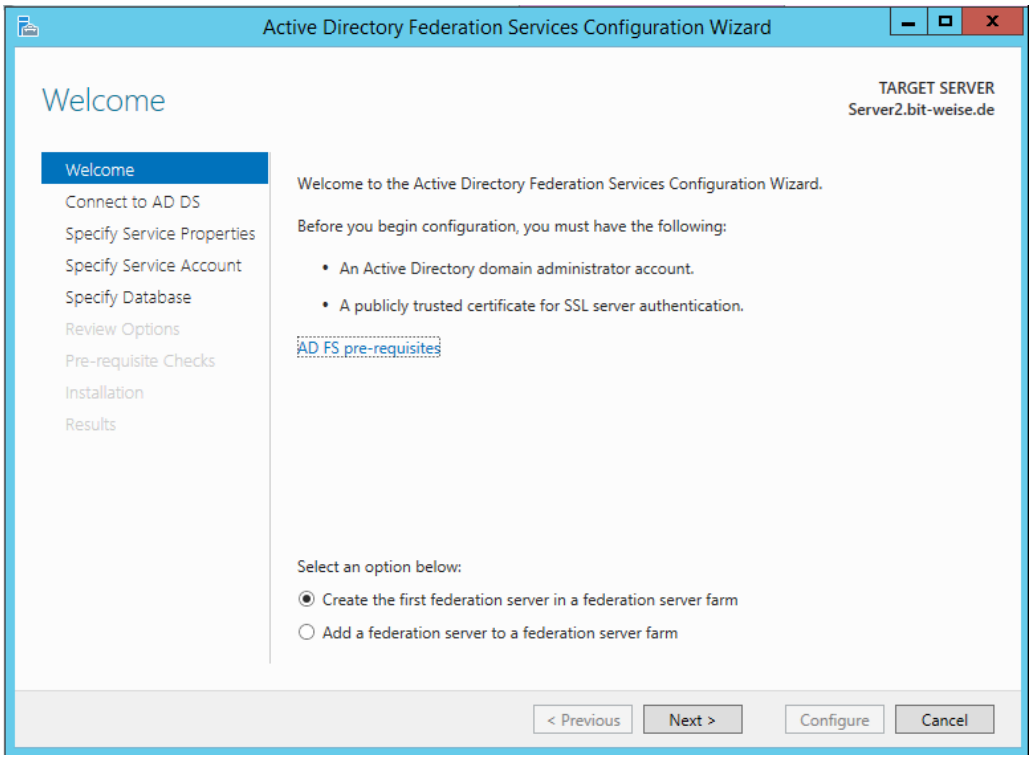


Abbildung 21 - Create the first federation server farm

Im nächsten Schritt gegen Sie einen Domänen-Account an, mit dem der Zugriff auf das AD für die Installation hergestellt werden soll. Ich verwendet hier den Domänen-Admin, da der Account für die Konfiguration-Anpassungen Domänen-Admin-Rechte benötigt.

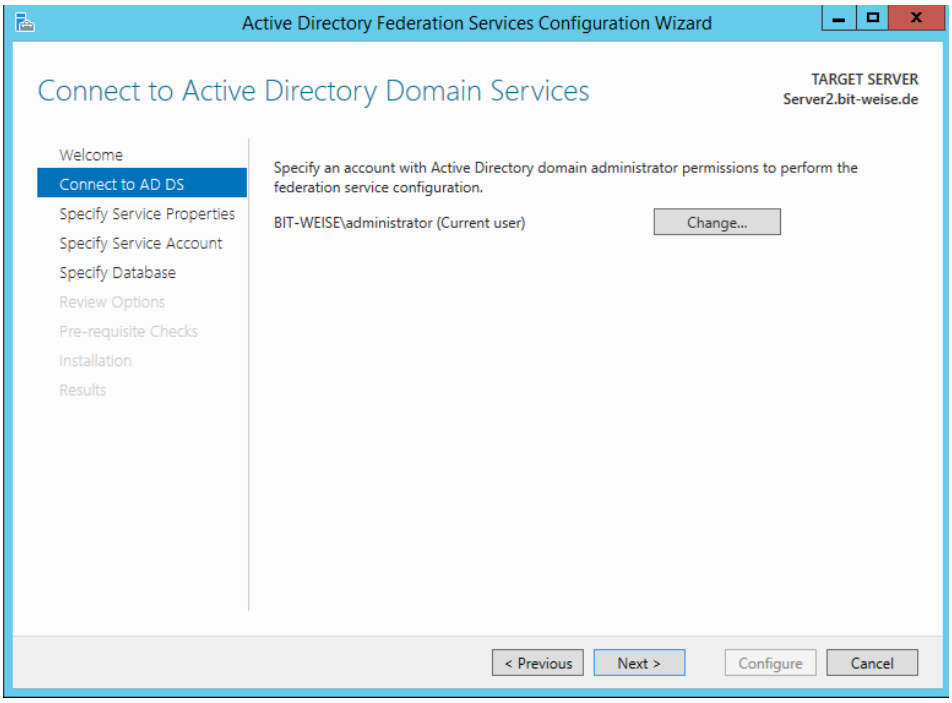


Abbildung 22 - Angeben des Domänen-Admin-Accounts

Wenn Sie das SSL-Zertifikat korrekt installiert haben, finden Sie im nächsten Fenster das SSL-Zertifikat für Ihren ADFS-Server im Dropdown-Fenster SSL-Certificate angegeben. Geben Sie auch den Anzeigenamen für die ADFS-Farm an. Dieser Name wird im Anmeldefenster angezeigt.

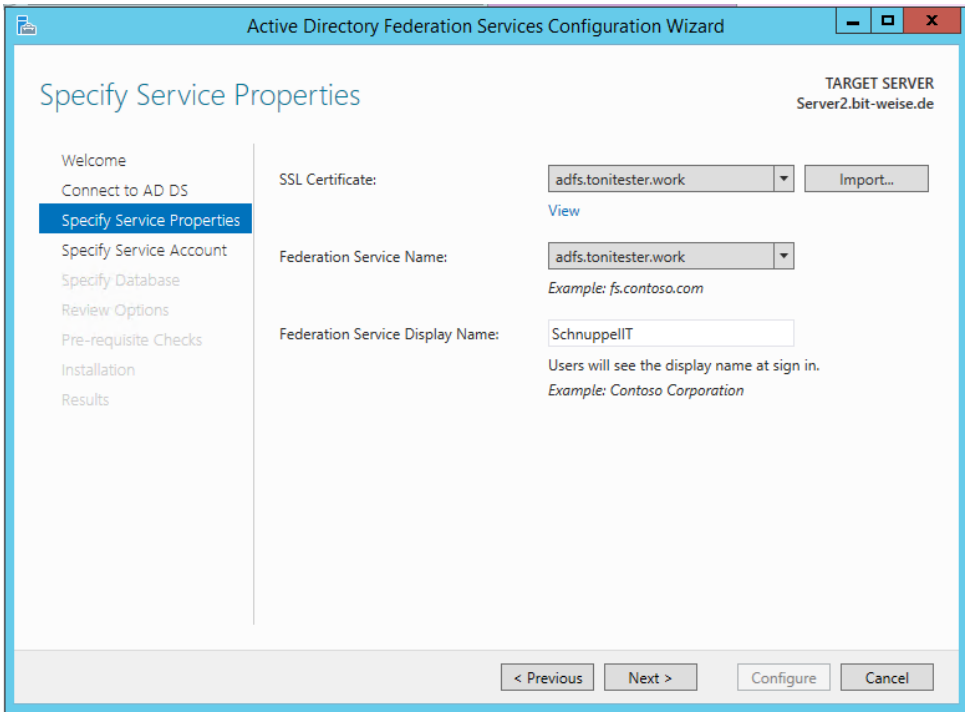


Abbildung 23 - SSL-Zertifikat angeben.

Der Service-Account benötigt keine speziellen Berechtigungen, kann aber auch ein Group managed Service Account (gmsa) sein.

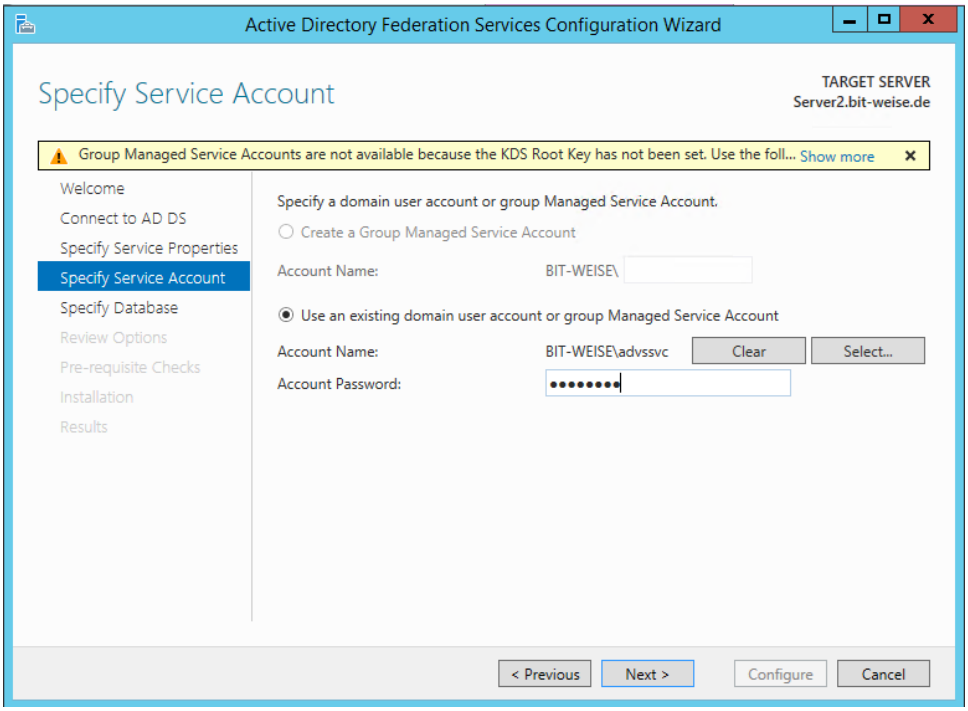


Abbildung 24 - Service-Account angeben.

ADFS-Farmen speichern Ihre Daten in einer zentralen Datenbank. Sie können hier die Windows Internal Database (WID) oder einen ausgewachsenen SQL-Server verwenden.

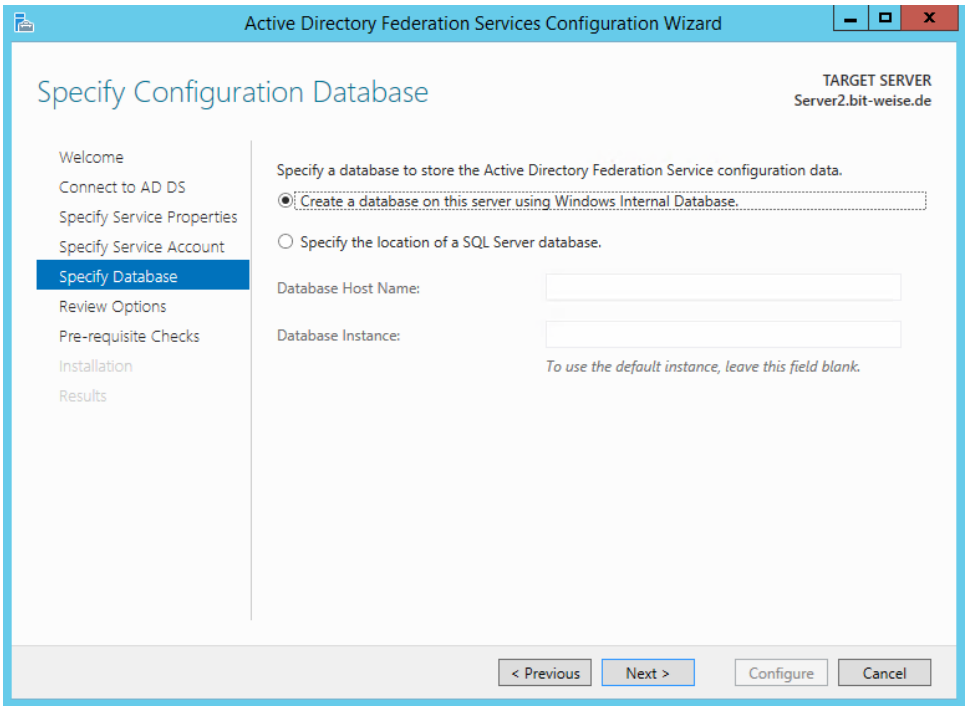
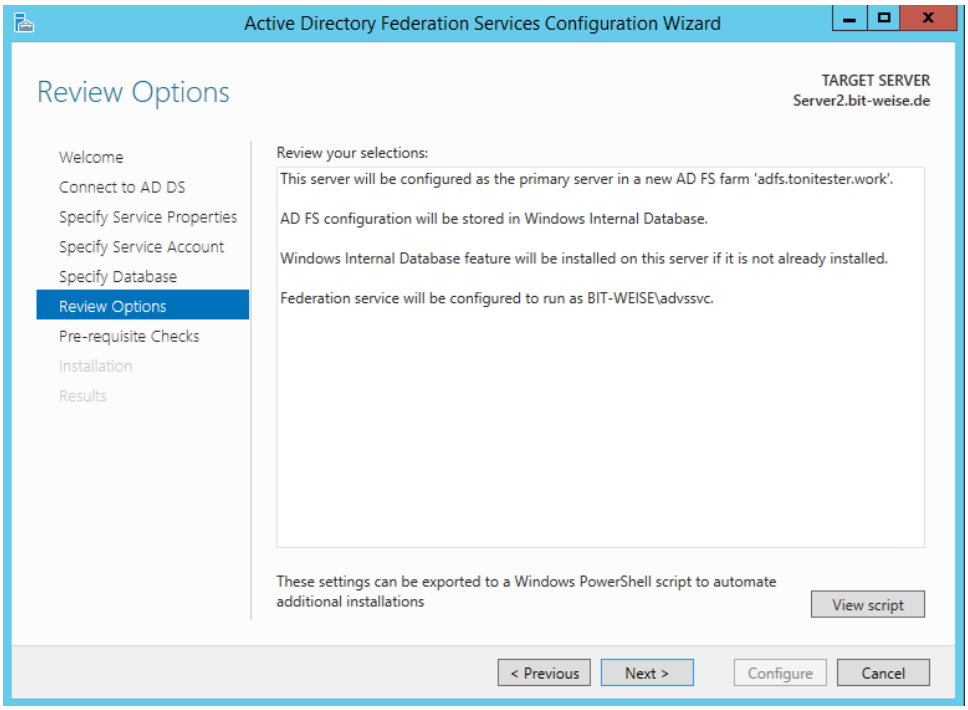
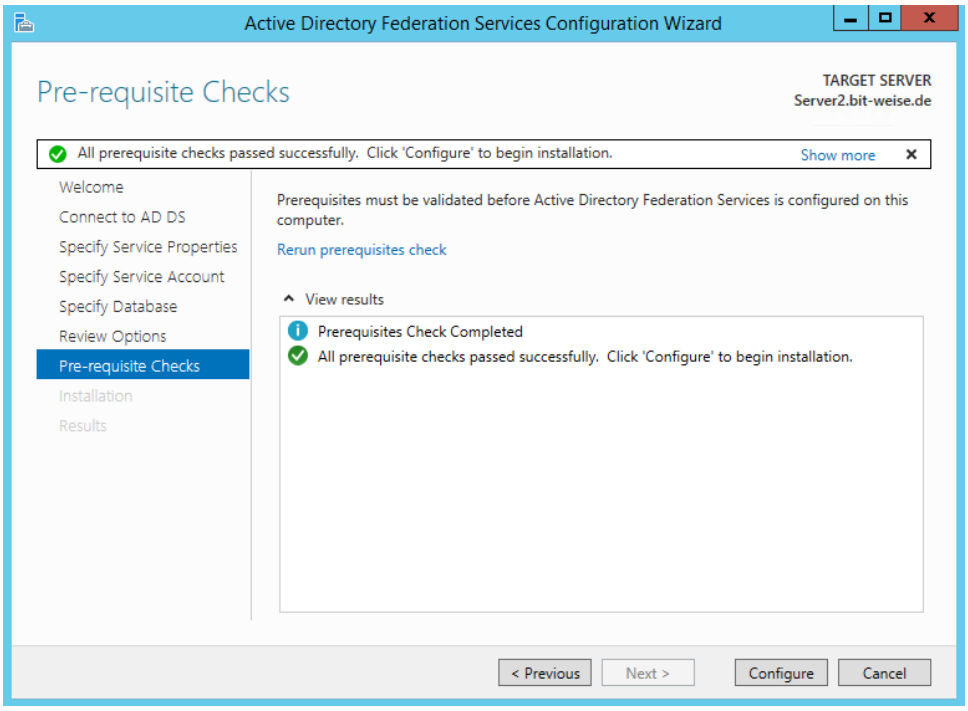
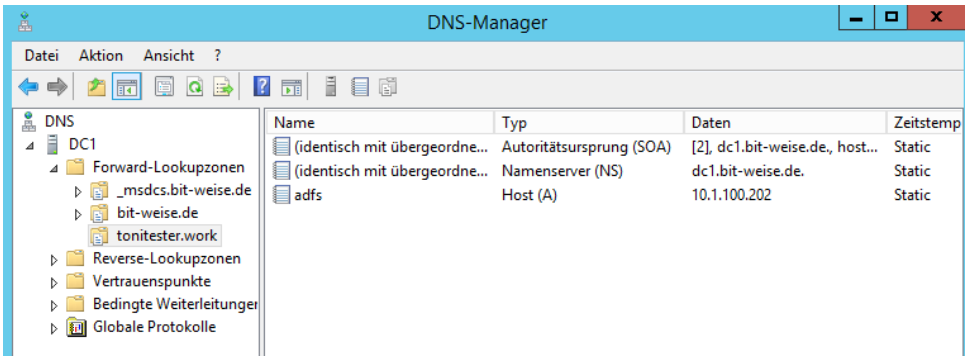


Abbildung 25 - Datenbank angeben





Wenn Sie die Installation abgeschlossen haben, müssen Sie den ADFS-Namen noch im internen DNS eintragen. Der Name entspricht dem Namen, der auf dem Zertifikat als ADFS-Name angegeben wurde. Er ist für interne wie externe Clients identisch!



Anschließend können Sie die Installation testen, indem Sie folgende URLs aufrufen:
https://<Ihre ADFS-Server-Farm>/federationmetadata/2007-06/federationmetadata.xml
https://<Ihre ADFS-Server-Farm>/adfs/ls/idpinitiatedsignon.htm

Konnektieren mit Office 365

Als nächstes muss der ADFS mit Office 365 verbunden werden. Am ADFS-Server selber muss nichts mehr eingerichtet werden – den Rest erledigt Powershell für uns. Für die Einrichtung müssen als erstes zwei weitere Installationen vorgenommen werden. Das kann auch auf einem Admin-Client geschehen. Es handelt sich um den Online Services Single Sign In Assistant und das Azure AD-Modul für Powershell. Wenn Office 365 auf dem Client bereits installiert ist, ist der Online Services Single Sign In Assistant bereits installiert.

Installieren des Online Services Sinlge Sign In Assistant (Dienst):
http://go.microsoft.com/fwlink/?LinkID=286152

Installieren des Azure AD Moduls für Powershell:
http://go.microsoft.com/fwlink/p/?linkid=236297

Einrichten des Verbunds

Wenn Sie das Azure AD-Modul installiert haben, kann es losgehen. Starten Sie Ihre Powershell und geben Sie die folgenden 4 Cmdlets ein. Connect-MSOLService ruft ein Anmeldefenster auf, mit dem Sie sich gegen Office 365 als Administrator identifizierten müssen. Als Anmeldekonto müssen Sie ein Konto verwenden, dass **nicht aus Ihrer offiziellen Domäne entstammt**, da Sie sonst bei einem Ausfall Ihres Verbunds keine Möglichkeit mehr hätten, sich am Office 365 administrativ anzumelden! Verwenden Sie daher einen globalen Administrator mit der Endung .onmicrosoft.com.

```
Connect-MsolService
Get-MsolDomain
Set-MsolADFSContext -Computer adfs.meinedomain.com #internen ADFS-Name!
Convert-MsolDomainToFederated -Domainname MeineDomain.com
```

AD-Connect installieren

Azure AD Connect ist der Nachfolder von Dirsync. Die Aufgabe von AD Connect ist es, Benutzer und Gruppen aus Ihrem lokalen (On Premise) AD ins Azure AD zu kopieren und die Benutzer und Gruppen anschließend zu synchronisieren. Obwohl AD Connect eigentlich hauptsächlich dafür da ist, Ihre Benutzer in die Cloud zu synchronisieren, kann es auch Daten wie Kennwörter oder neue Gruppen aus dem Azure-AD ins lokale AD synchronisieren, wenn Sie das möchten. Eine ausführliche Beschreibung über den Synchronisationsprozess weiter unten. Eine sehr empfehlenswerte Einführung finden Sie auch in diesem sehr guten Einführungsartikel von Simon May:

http://simon-may.com/setting-up-a-solid-identity-and-access-management-foundation/

Für die Installation von AD-Connect benötigen Sie einen Server in Ihrem Netzwerk. Der Server muss Internetzugriff haben, aber eingehende Verbindungen werden ausdrücklich nicht benötigt. Daher sind keine speziellen Firewall-Regeln notwendig.

Das Setup kann als Express-Setup oder als Erweitertes Setup ausgeführt werden. Folgend wird das Express-Setup beschrieben.

Abbildung 26 - AD-Connect Setup starten

Wählen Sie aus, welche Single Sign On Lösung Sie nutzen wollen. Im Beispiel wählen wir Password Synchronization aus, da AD Connect unsere Kennwörter ins Azure-AD synchronisieren soll. Auch wenn Sie ADFS verwenden, kann es sinnvoll sein, eine vollständige Kennwortsynchronisation zu konfigurieren, wenn Sie nicht 100% sicherstellen können, dass Ihre ADFS-Server immer erreichbar sind, denn ohne ADFS ist sonst kein Login in die Office365-Dienste mehr möglich.

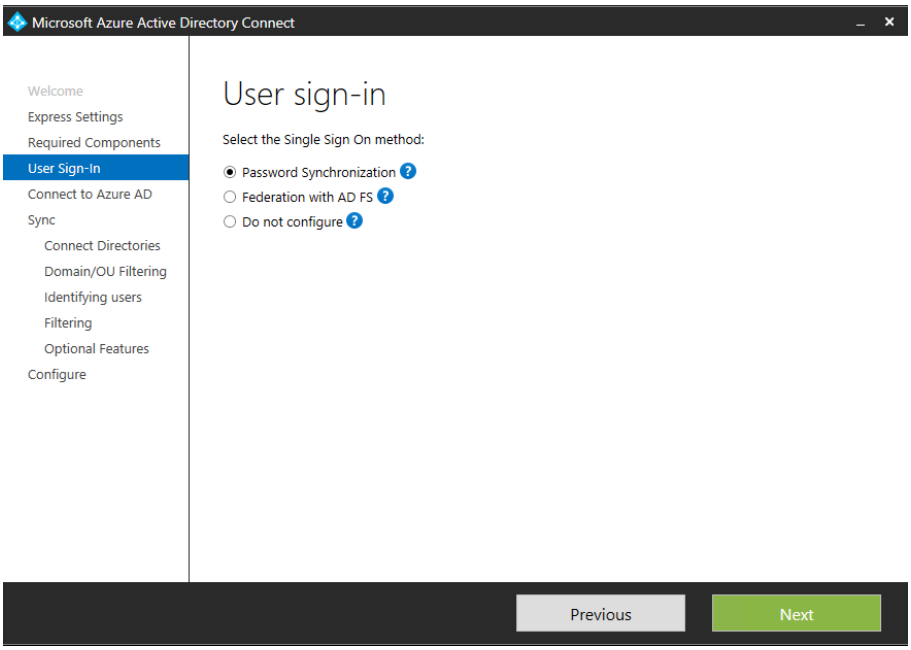


Abbildung 27 - Auswahl des Synchronisationsmodus

Geben Sie einen Account mit Administrativen Rechten im AD an. Wie man diesen erstellt, wird oben beschrieben. Dieser Account wird nicht im System hinterlegt, sondern zum Anlegen eines Service-Accounts und zur Berechtigungsvergabe benötigt.

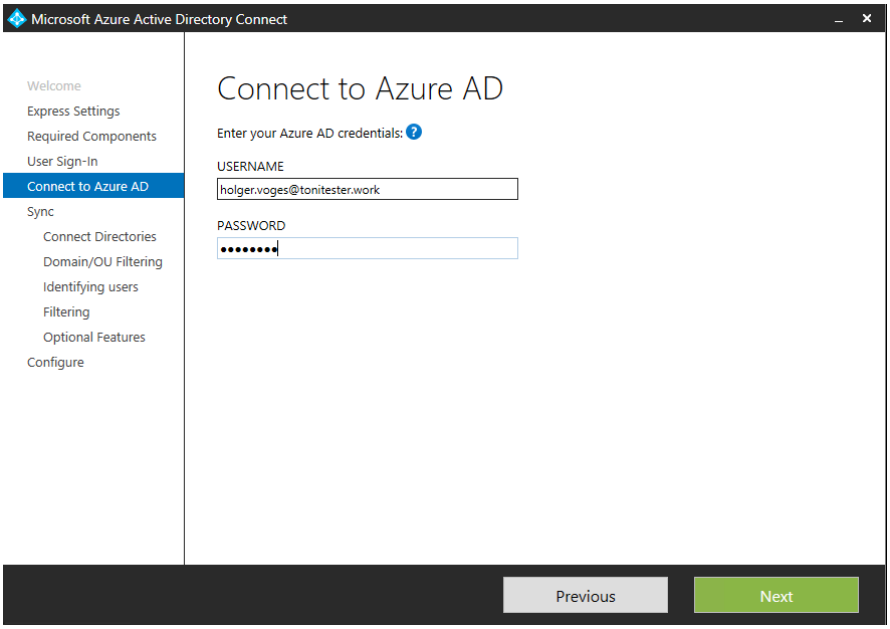


Abbildung 28 - Melden Sie sich an Azure an

Als nächstes müssen Sie den oder die Gesamtstrukturen (Forests) angeben, aus denen Sie synchronisieren wollen. Sie müssen außerdem ein Konto angeben, dass AD Connect zum Auslesen der Benutzerdaten verwendet. Es handelt sich um ein Domänenkonto mit Leserechten. Soll das Konto außerdem Kennwörter synchronisieren, müssen zusätzliche Rechte vergeben werden.

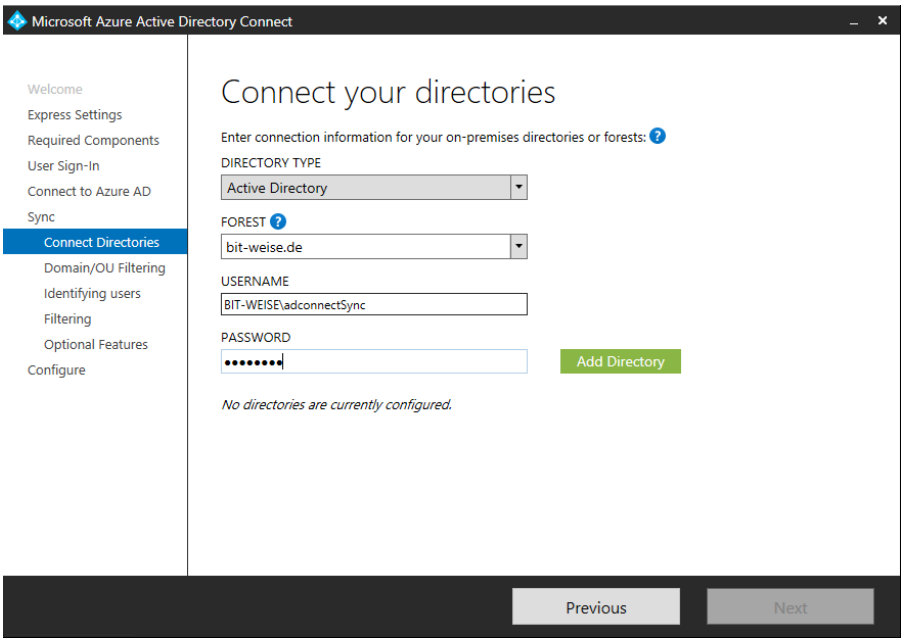


Abbildung 29 - Anmelden am lokalen AD

Zum Synchronisieren der Benutzerdaten benötigt das Synchronisationskonto Berechtigungen. Diese werden vom Express-Setup automatisch auf dem Domänenobjekt vergeben, von wo aus diese Daten vererbt werden. Um Berechtigungen unter AD Benutzer und Computer angezeigt zu bekommen, wählen Sie im AD Benutzer und Computer unter Ansicht „Erweiterte Features“ aus.

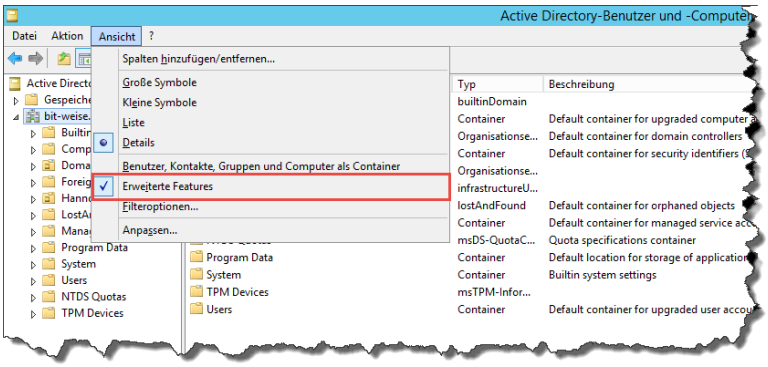


Abbildung 30 - Erweiterte Features in AD Benutzer und Computer aktivieren

Die Berechtigungen sehen Sie, wenn Sie das Kontextmenü des Domänenobjekts auswählen und den Reiter Sicherheit öffnen. Hier finden Sie den angegebenen Benutzer wieder, im Beispiel mit den Rechten „Verzeichnisänderungen replizieren“ und „Alle Verzeichnisänderungen replizieren“. Die Auflistung über alle Berechtigungen finden Sie in der Azure AD Dokumentation:

Azure AD Connect: Accounts and permissions
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-accounts-permissions/.

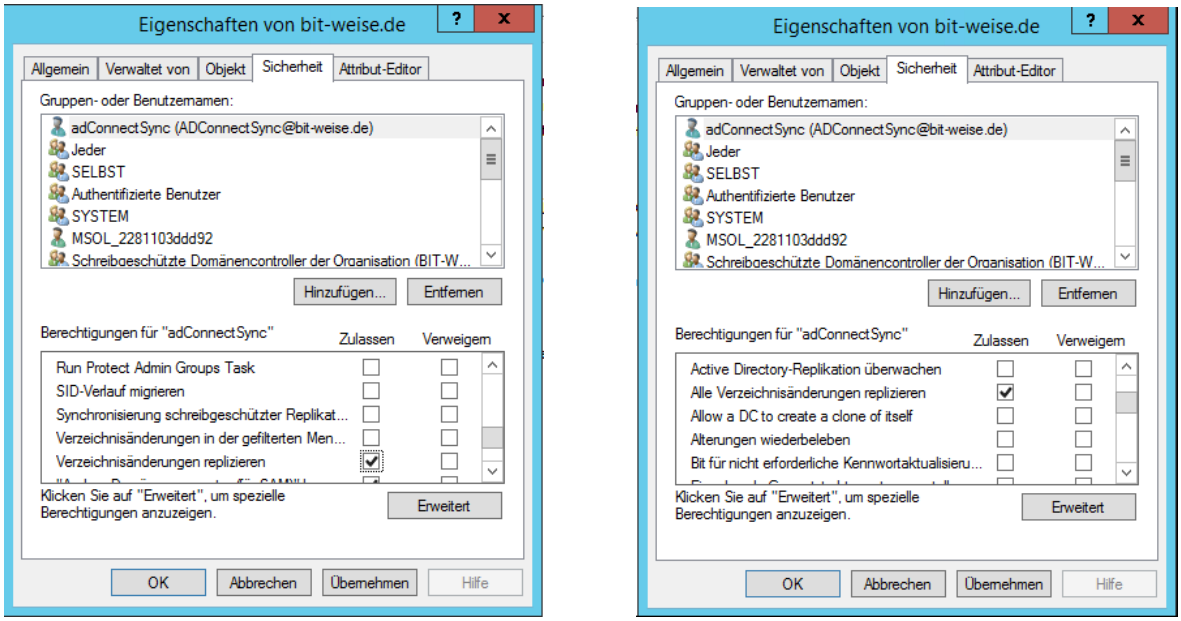


Abbildung 31 - Verzeichnisänderungen replizieren und Alle Verzeichnisänderungen replizieren

Das Verzeichnis ist jetzt verbunden. Sie können weitere Verzeichnisse replizieren, indem Sie weitere Verzeichnisse hinzufügen.

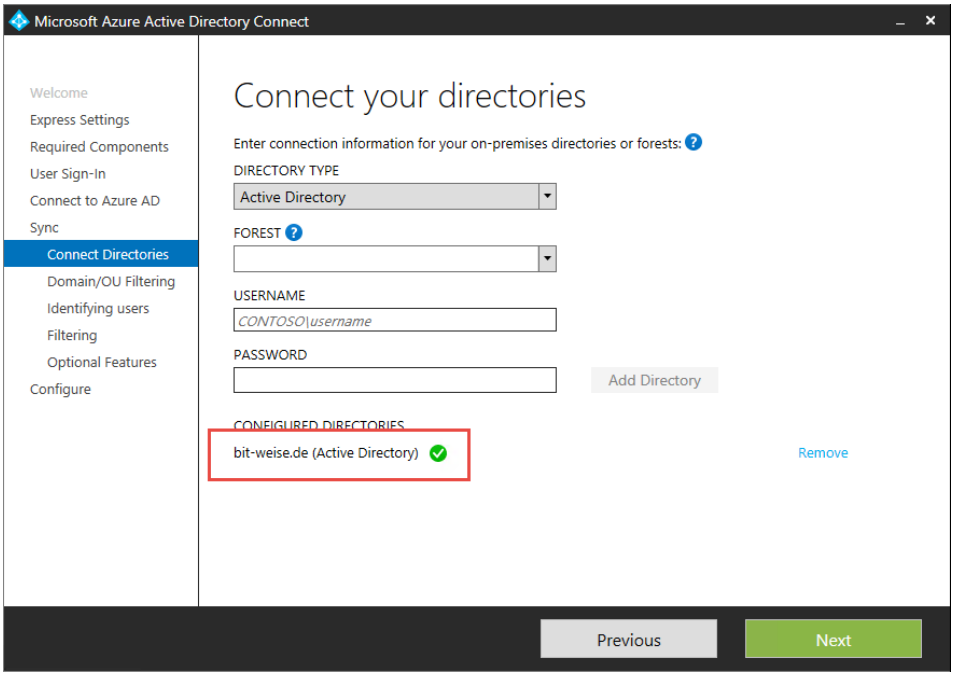


Abbildung 32 - Das Verzeichnis ist verbunden

Mit AD-Connect können Sie nun Filter auf Basis von Organizational Units hinzufügen. Nur Objekte der angegebenen OUs werden synchronisiert.

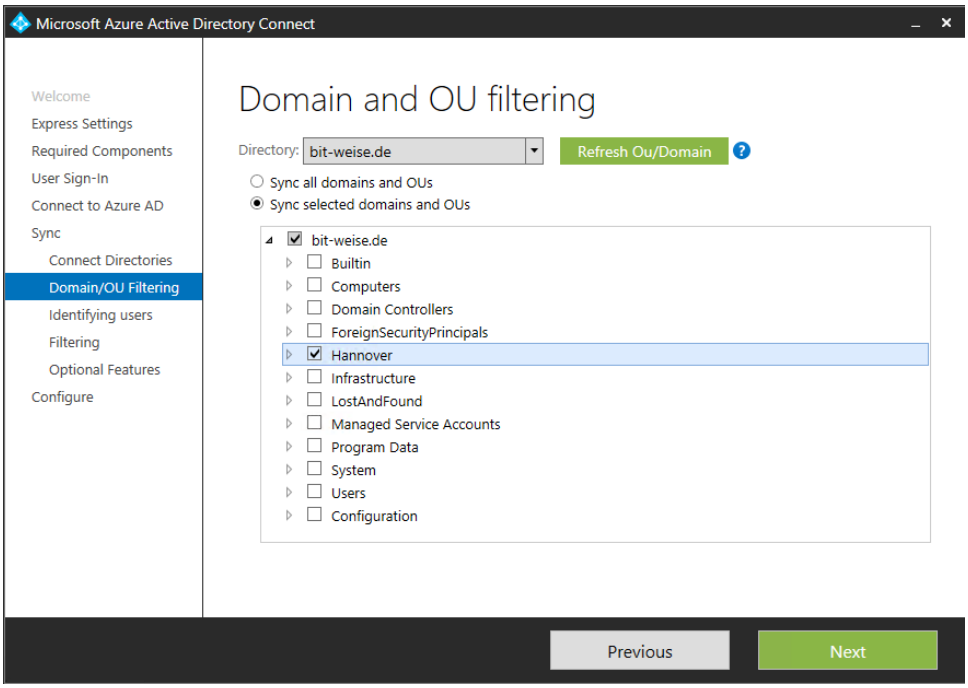


Abbildung 33 - Filtern Sie Domänen und Container

Wenn die Replikation innerhalb eines Forest stattfindet, ist das Identifizieren von Objekten über die ObjectGUID einfach möglich. Die ObjectGUID ist ein eindeutiger Bezeichner, der über den gesamten Forest eindeutig ist. Werden Objekte über mehrere Forest repliziert, ist es notwendig, einen anderen, eindeutigen Bezeichner zu bestimmen. Dies könnte z.B. ein selbstdefiniertes Custom Attribute sein, wie Exchange es zur Verfügung stellt, oder die E-Mail-Adresse.
Damit AD Connect jedes Objekt eindeutig identifizieren kann, wird für alle Objekte ein eindeutiger Identifier in der Eigenschaft „SourceAnchorBinary“ gespeichert. Repliziert man nur über einen Forest, verwendet man hier am besten einfach die ObjectGUID.

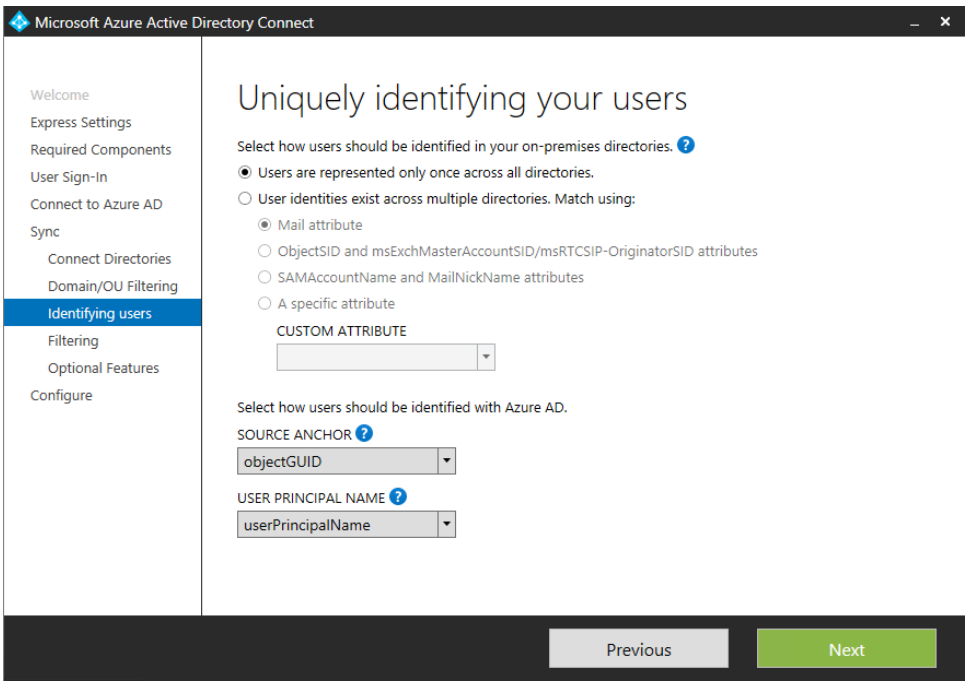


Abbildung 34 - Legen Sie den Source-Anchor fest

Nur Benutzer synchronisieren, die Mitglied in einer bestimmten Gruppe sind. Diese Funktion ist vor allem für die Testphase gedacht, in der noch nicht alle Benutzerkonten synchronisiert werden sollen.

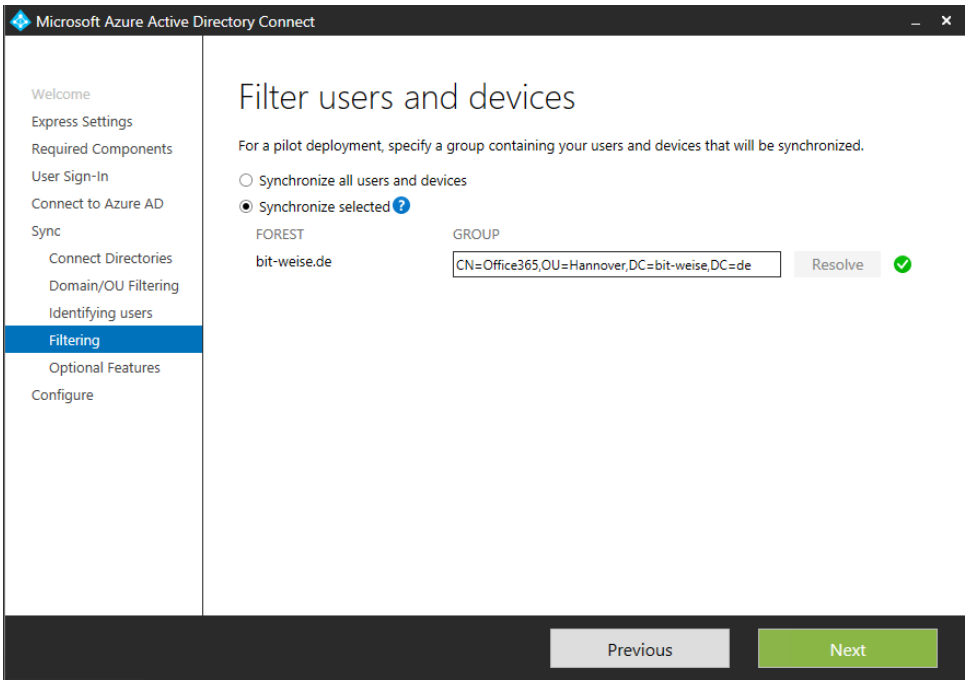


Abbildung 35 - Eine Gruppe angeben, die in der Testphase die PIlot-Benutzer festlegt

Zum Schluß können noch weitere Features wie die Kennwort-Zwei-Wege Synchronisation von Azure zum lokalen AD aktiviert werden. Achten Sie darauf, dass der Synchronisationsbenutzer, den Sie weiter oben konfiguriert haben, erweiterte Berechtigungen benötigt!

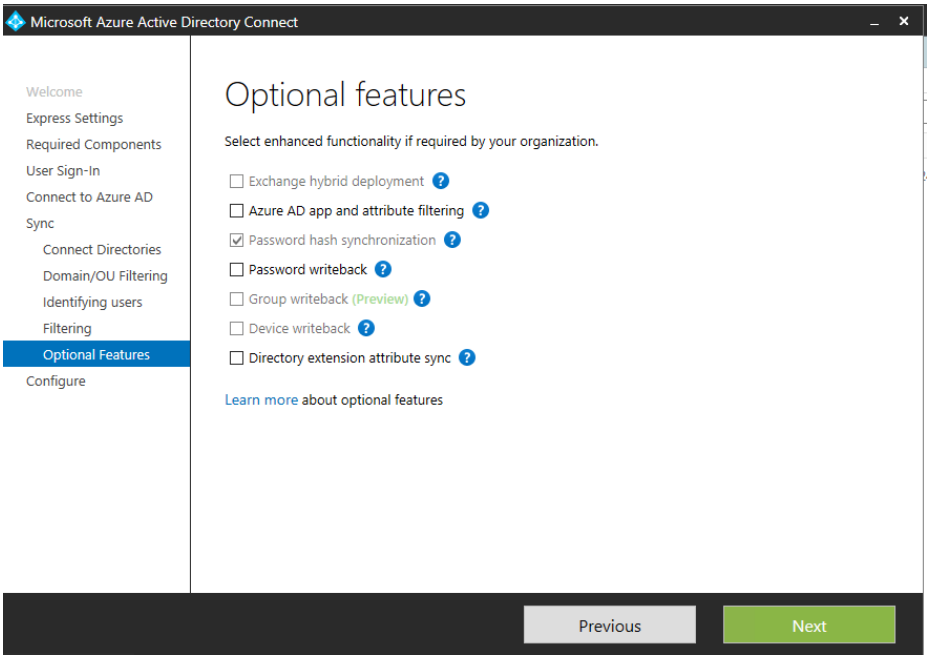


Abbildung 36 - legen Sie weitere Funktionen wie die Kennwort-Zwei-Wege-Synchronisation fest

Im letzten Auswahlfenster haben Sie die Möglichkeit, den Server in den Staging-Mode zu versetzen. Im Staging-Mode wird der Server als reiner Import-Server installiert, der keine Daten exportiert. Eine ausführliche Beschreibung zum Staging-Mode finden Sie auf S. 39Staging Mode - Staging Mode.

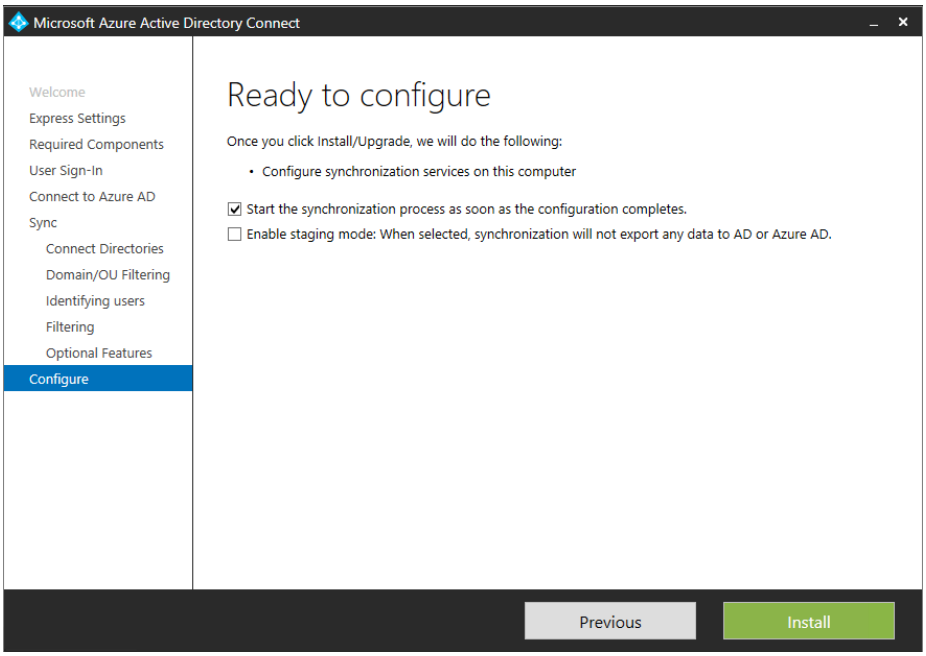


Abbildung 37 - Starten Sie die Synchronisation oder aktiveren Sie den Staging Mode

Eine Beschreibung der Konfiguration von Password- und Device-Writeback finden Sie hier:

Implementing password synchronization with Azure AD Connect sync
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-implement-password-synchronization/#trigger-a-full-sync-of-all-passwords

Azure AD Connect: Enabling device writeback
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-feature-device-writeback

Die AD Connect Synchronisation

AD-Connect ist das Tool, das Microsoft zur Synchronisation des lokalen (on Premise) Active Directory mit Azure AD zur Verfügung stellt. Es ist der Nachfolger von DirSync und wird seit der Version 1.1 automatisch über Windows Update aktualisiert. Ob das automatische Update bei Ihnen aktiviert ist, finden Sie über Powershell heraus:

```
Get-ADSyncAutoUpgrade
```

Weitere Informationen zum Auto-Update und wie Sie es konfigurieren können, finden Sie in der Azure-Dokumentation:

Azure AD Connect: Automatic Upgrade
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-feature-automatic-upgrade

Während in diesem Dokument nur die Synchronisation zwischen einem lokalen und einem Azure AD behandelt wird, kann AD Connect prinzipiell auch andere Verzeichnisdienste anbinden.

Der Prozess der Synchronisation zwischen verschiedenen Verzeichnisdiensten wird in AD Connect von einem zentralen Dienst gesteuert, der Sync Engine. Die Sync Engine steuert den Vorgang des Im- und Exports und wird durch die Installation von AD Connect bereitgestellt.

Die Sync-Engine führt keine direkte Synchronisation zwischen Quelle und Ziel durch, sondern speichert die Daten in einer Datenbank. Diese Datenbank besteht aus mehreren getrennten Bereichen oder Partitionen, und zwar der Metaverse, in der eine konsistente Repräsentation aller replizierenden Objekte gespeichert ist, und den Connector Spaces. Die Metaverse wird normalerweise in SQL-Server gespeichert.

Wofür benötigt man diese Partitionen? Die Metaverse ist eine Art Paralleluniversum zwischen dem lokalen AD und dem Azure AD, das für den Transit der Objekte verwendet wird. In der Metaverse werden alle Objekte zusammengeführt. Existiert ein Benutzer z.B. in mehreren Forests, dargestellt durch ein Anmeldekonto und einen Kontakt, so werden nicht Kontakt und Benutzer als Einzelobjekte gespeichert, sondern in der Metaverse zu einem Objekt zusammengeführt.

Die Replikation findet aber nicht direkt in die Metaverse statt, sondern wird durch Konnektoren über Connector-Spaces durchgeführt. Die Konnektoren lesen die Daten aus den verbundenen Verzeichnissen oder synchronisieren geänderte Daten in die verbundenen Verzeichnisse. Dabei verfügt jedes angebundene Verzeichnis über einen eigenen Connector. Der Connector arbeitet agentenlos, es muss auf den Servern in den angebundenen Verzeichnissen keine zusätzliche Software installiert werden.

Die Konnektoren lesen und schreiben nicht direkt in- und aus der Metaverse, sondern verwenden die Connector-Spaces. Wenn ein Connector ein neues Objekt in einem angebundenen Verzeichnis findet, so legt er eine Repräsentation dieses Objektes im Connector-Space an. Hier wird es gespeichert und bleibt während seiner gesamten Lebensdauer dort. Der Konnektor synchronisiert grundsätzlich immer den Connector-Space, und nicht die Metaverse. Erst der Synchronisationsvorgang zwischen dem Connector-Space und der Metaverse liest die Daten aus dem Connector-Space und schreibt Änderungen in die Metaverse. Connector-Spaces halten also immer eine lokale Repräsentation eines Objektes aus einem Verzeichnis, während die Metaverse die Daten aus allen Connector-Spaces zusammenführt, um ein konsistentes Gesamtbild des Objekts zu generieren.

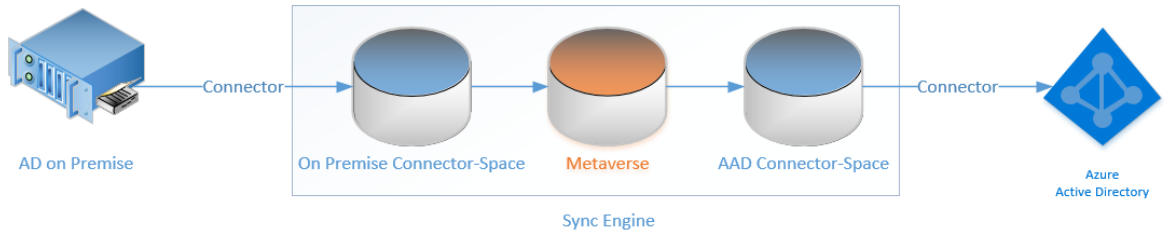


Abbildung 38 - AD-Connect Komponenten

Während eines Replikationsvorgangs liest der Connector anhand der Synchronisations-Regeln aus, welche Objekte und welche Objekt-Attribute repliziert werden sollen. Ist ein Objekt noch nicht vorhanden, wird anhand einer Join-Regel ein neues Objekt im Connector-Space angelegt. Im ersten Durchlauf des Konnektors werden also zuerst einmal alle Objekte im Connector-Space erzeugt. Jedes Objekt muss später zwischen allen Verzeichnisdiensten und allen Replikationsdatenbanken eindeutig identifizierbar sein. Die Sync-Engine verwendet hierfür ein Attribut namens **Source Anchor**, in das eine eindeutige Kennung, die sogenannte immutable ID, kopiert wird. Werden nur die Domänen eines einzigen Forrest repliziert, so wird normalerweise die Object-GUID eines Objekts als eindeutige Kennung verwendet. Der Source-Anchor darf sich im Laufe des Lebens eines Objektes niemals ändern, da sonst die Verbindung zum Objekt verloren geht! Wird über mehrere Forests repliziert, ist die Object-GUID keine eindeutige ID mehr, da ein Kontakt-Objekte in einem anderen Forest (s. Beispiel oben) ein eigenes Objekt mit einer eigenen Objekt-GUID ist. In diesem Fall muss ein anderes Attribut wie z.B. die E-Mail-Adresse zur eindeutigen Identifizierung herangezogen werden.

Sobald ein Objekt im Connector-Space angelegt wurde, werden nur noch Änderungen zwischen der Quelle und dem Connector synchronisiert. Das Objekt bleibt im Connector-Space erhalten, bis es gelöscht wird.

Vom Connector-Space werden die Objekte in die Metaverse kopiert. Hier können auch Objekte aus mehreren Verzeichnissen, die das gleich Objekte repräsentieren (z.B. ein Benutzerobjekt und ein Kontakt-Objekt aus einem anderen Forrest), zusammengeführt werden. Objekte in der Metaverse können nicht direkt bearbeitet werden, sondern werden immer über die Synchronisation mit den Connector-Spaces aktualisiert. Von der Metaverse aus kann ein Objekt jetzt in den Connector-Space des Azure AD kopiert werden (bzw. synchronisiert, wenn es bereits existiert). Der Azure AD Connector ist dafür verantwortlich, die Daten ins Azure AD zu synchronisieren.

Eine ausführliche Beschreibung der Funktionsweise von AD Connect finden Sie in der Azure AD Doku:

Azure AD Connect sync: Understanding the architecture
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-understanding-architecture

Die AD-Connect Verwaltungs-Werkzeuge

Nach der Installation von AD-Connect stehen 4 Tools zur Anpassung von AD-Connect zur Verfügung. Grundsätzlich sollte AD-Connect nach Durchlaufen des Installations-Assistenten sofort automatisch funktionieren, aber in komplexen Umgebungen oder zur späteren Anpassung kann man sehr genau Einfluss auf die Replikation nehmen.

Zur allgemeinen Anpassung von AD-Connect verwendet man das Tool mit dem Namen Azure AD Connect.

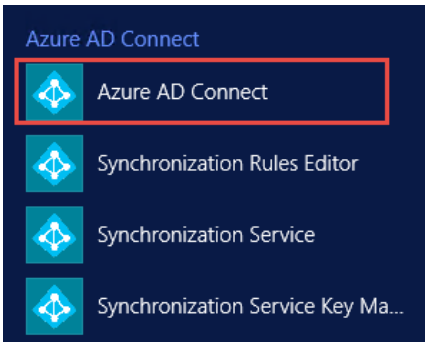


Abbildung 39 - Azure AD Connect nimmt Diensteinstellungen vor

AD Connect startet einen Wizard, mit dem man AD-Connect nach der Installation anpassen kann. Eine vollständige Beschreibung zu den Optionen finden Sie auch bei Microsoft:

Azure AD Connect Sync: Running the installation Wizard a second time
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-installation-wizard

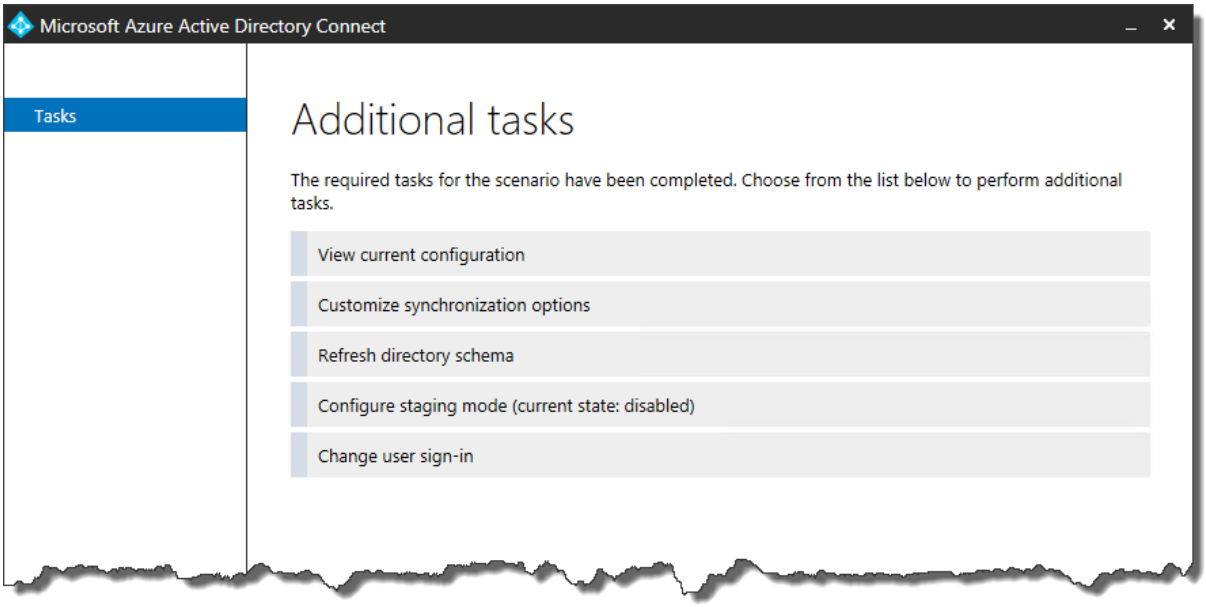


Abbildung 40 - Der AD Connect Configuration Wizard

View current configuration zeigt eine Zusammenfassung der aktuellen Konfiguration an:

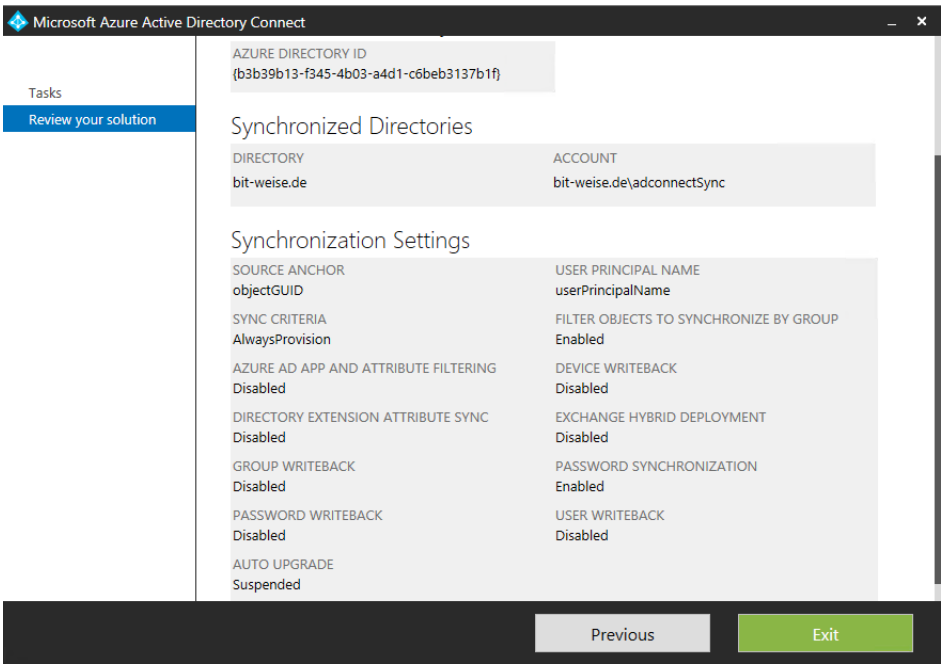


Abbildung 41 - Die derzeitige Konfiguration anzeigen

Customize synchronization options

Mit der Option „Customize synchronization options“ können Sie einen Großteil der Einstellungen konfigurieren, ohne direkt die Synchronisationseinstellungen anpassen zu müssen. Dies ist der bequemste und sicherste Weg, wenn es z.B. darum geht, zusätzliche Objekt-Filter zu setzen oder bestimmte AD-Attribute mit in die Replikation aufzunehmen. Außerdem kann der Wizard zusätzliche Konnektoren für weitere Domänen hinzufügen.

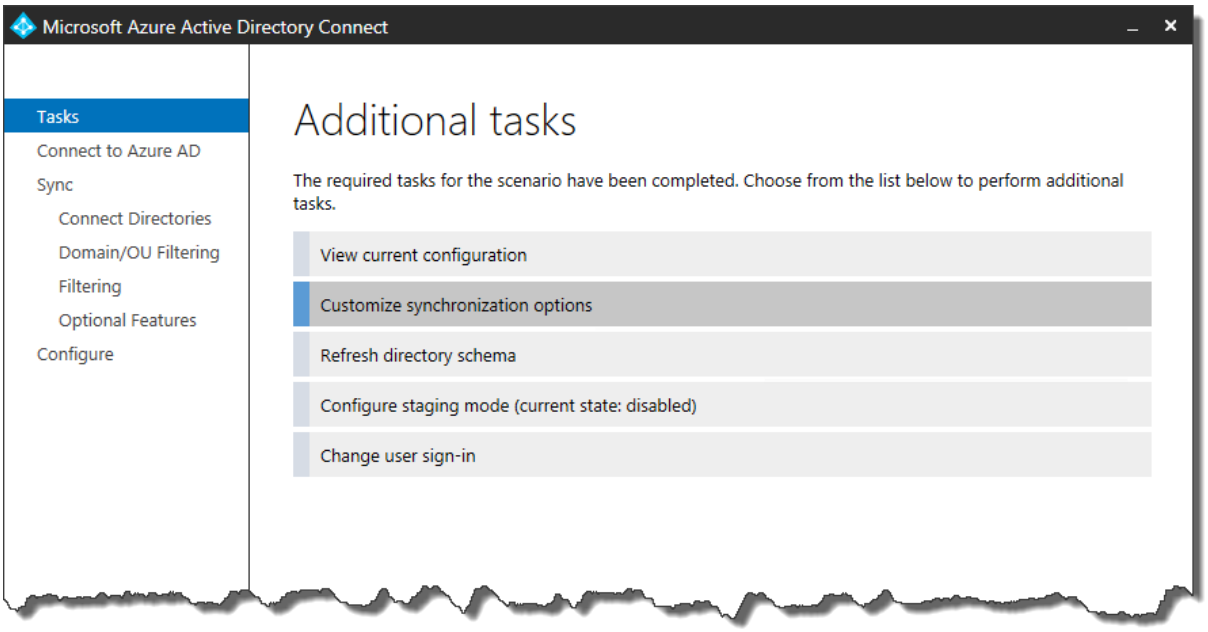


Abbildung 42 - Customize synchronization options erlaubt die einfache Anpassung der Synchronisation

Verbinden Sie sich zuerst mit Ihrem Azure AD, indem Sie sich mit einem Azure AD Administrator Konto anmelden.

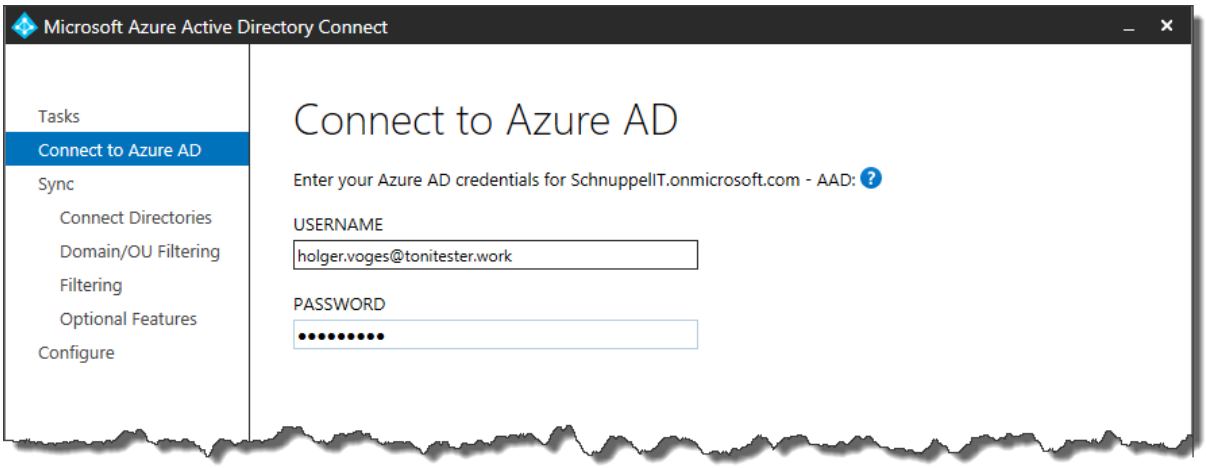


Abbildung 43 - Anmeldung am Azure AD

Im nächsten Fenster geben Sie an, mit welchem lokalen AD (on Premise) Sie sich verbinden wollen. Welche Berechtigungen dieser Account benötigt, hängt von Ihrem Einsatzszenario ab. Während Sie bei der Ersteinrichtung Domänen-Administrator Rechte benötigen, reicht später evtl. ein normaler Benutzer mit Lese-Rechten im AD. Eine Auflistung der Aufgaben und der dazu notwendigen Berechtigungen finden Sie in der Azure Doku:

Azure AD Connect: Accounts und Permissions
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-accounts-permissions/#create-the-ad-ds-account

Wenn Sie eine weitere Domäne in Ihre Synchronisation aufnehmen wollen, geben Sie hier die neue Domäne mit Anmeldeinformationen ein und wählen Sie den Button „Add Directory“.

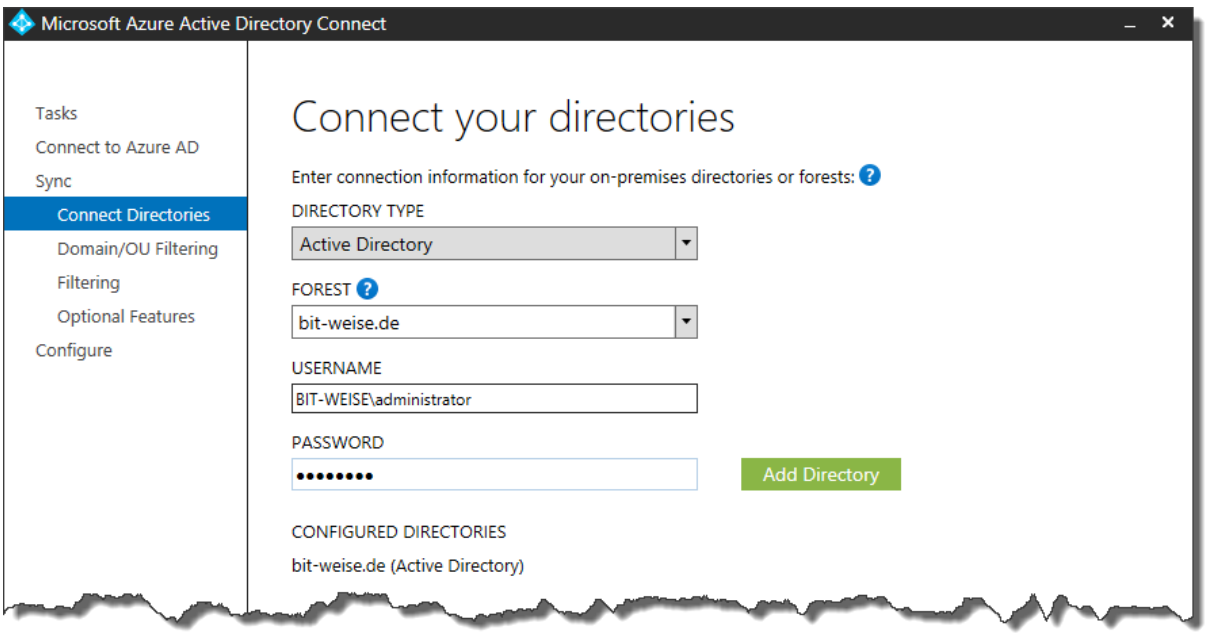


Abbildung 44 - Welche Berechtigungen benötigt werden, hängt vom Anwendungeszenario ab

Im folgenden Fenster können Sie Domänen- und OU Filterung einstellen. Hier legen Sie fest, aus welchen Domänen und OUs Objekte synchronisiert werden sollen. Objekte, die sich außerhalb dieses Bereichs befinden, werden nicht synchronisiert. Administrator-Konten und systemrelevante Konten werden von der Replikation standardmäßig ausgenommen. Mehr hierzu finden Sie weiter unten im

Kapitel „Mehr Informationen zu den Connector-Einstellungen finden Sie in der Azure-Dokumentation:

Azure AD Connect sync: Synchronization Service Manager
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-service-manager-ui-connectors/

Synchronization Manager Metaverse Designer Menü

Im Metaverse-Designer können Sie die Objektvorlagen der Metaverse einsehen und bearbeiten. Hier fällt eins sofort auf: Die Metaverse unterscheidet standardmäßig Objekte nur zwischen person, group und device. Alle Objekte werden auf diese Basisobjekte abgebildet. Ein Objekte vom Type InetorgPerson und ein AD User und ein Kontakt sind für die Metaverse alle ein Person Objekt.

Grundsätzlich ist es nur dann sinnvoll, an den Vorlagen Änderungen vorzunehmen, wenn man Attribute replizieren muss, die in den Vorlagen nicht vorhanden sind. Sie können weitere Attribute einfach hinzufügen, indem Sie über *Add Attribute* im Actions-Menü weitere Attribute hinzufügen.

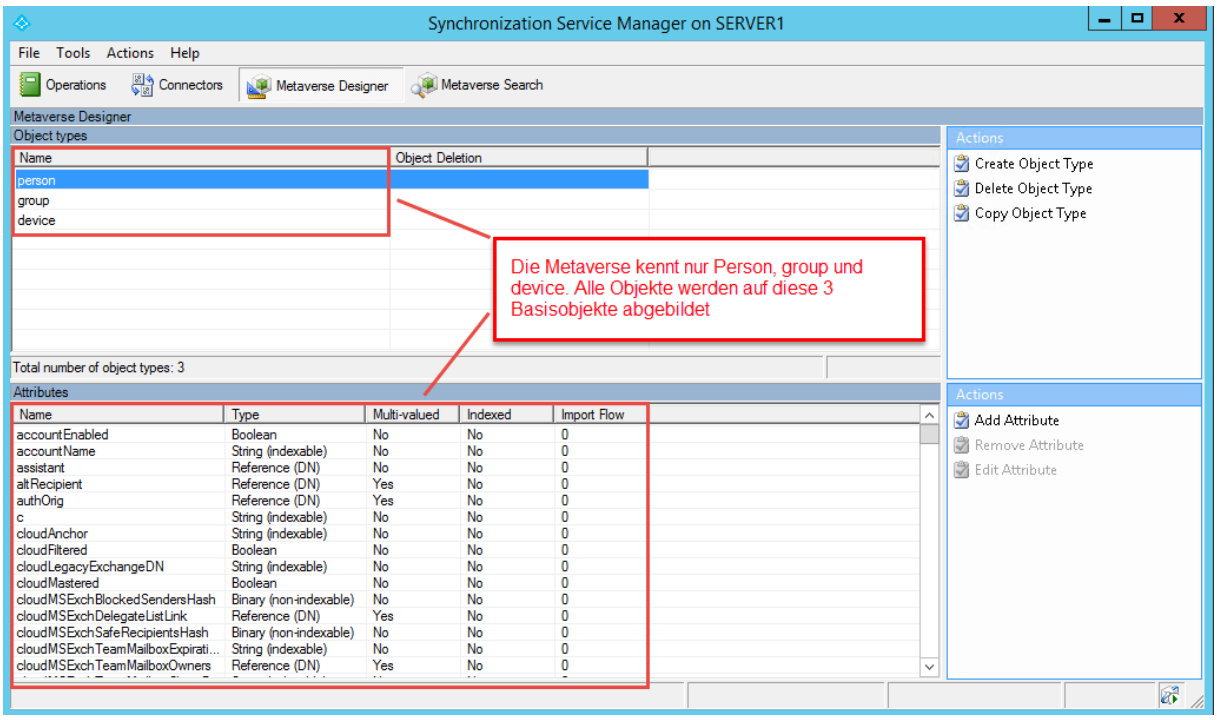
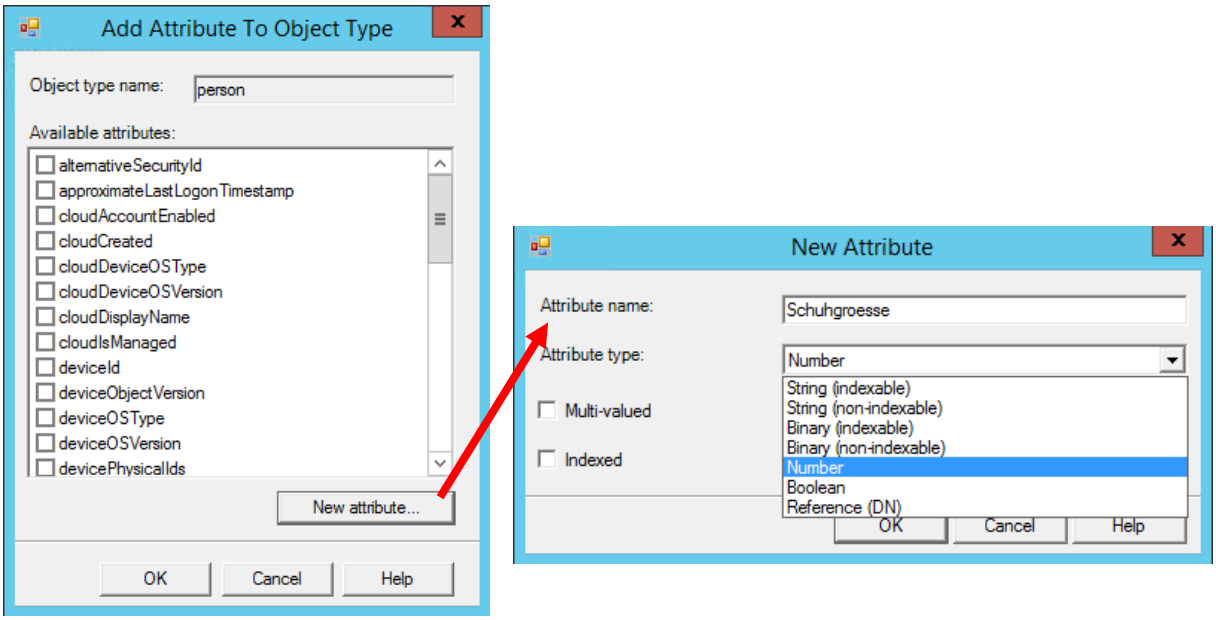


Abbildung 74 - Die Objektevorlagen der Metaverse

Wenn Sie Attribute hinzufügen wollen, können Sie zuerst aus einer Auswahl von bereits vorhandenen Attributen wählen. Sie können über *New Attribute* auch ein komplett neues Attribut erzeugen.



Um das Attribut zu füllen, benötigen Sie jetzt noch eine Synchronisationregel, die die Attribute befüllt.

Synchronization Manager Metaverse Search Menü

Während Sie im Connectors Menü die Objekte einsehen können, die in den Connectors Spaces gespeichert sind, finden Sie unter Metaverse Search die Objekte, die in der Metaverse gepeichert sind.

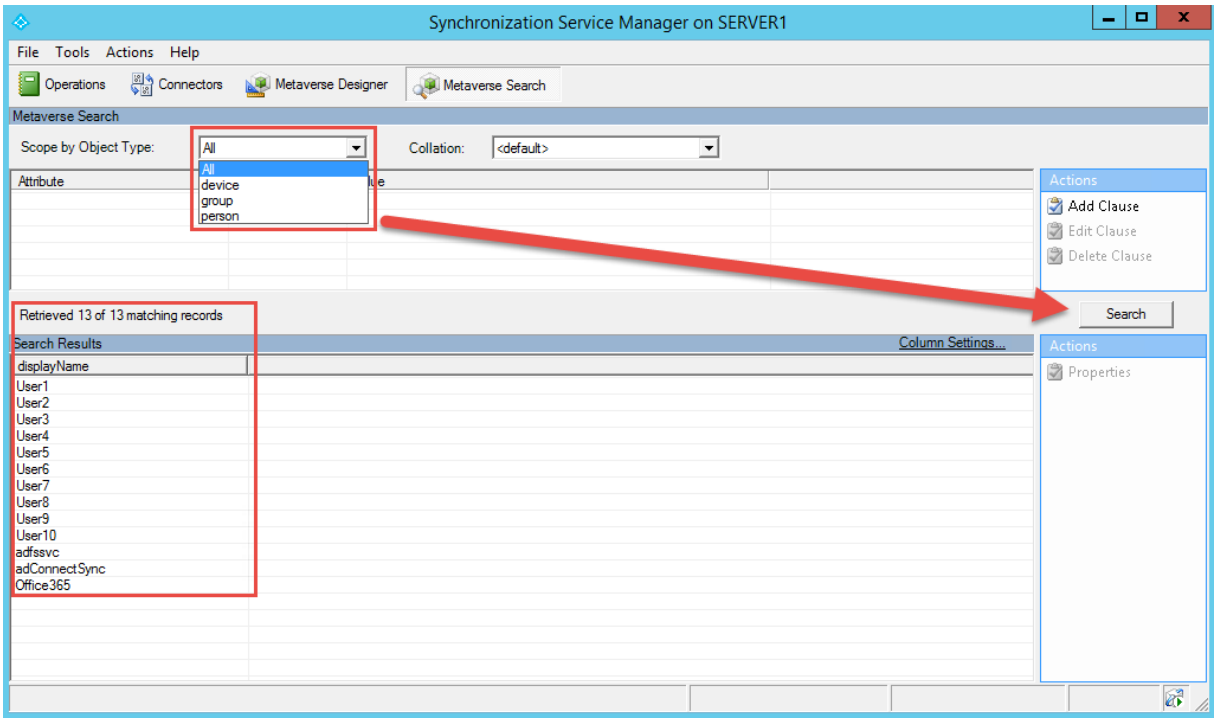


Abbildung 76 - Die Metaverse durchsuchen

Die Metaverse-Suche gestaltet sich recht einfach. Sie können den Suchfilter unter „Scope by Object Type“ auf die Vorlagen einschränken, die Sie anzeigen wollen, oder Sie können einfach alle Objekte anzeigen, die die Metaverse gespeichert hat. Klicken Sie hierfür einfach auf Search. Sie bekommen

dann im untern Fenster die Suchergebnisse angezeigt. Sie können die Suche über erweiterte Suchabfragen einschränken, indem Sie im Action-Fenster eine Clause (einen Suchfilter) eintragen. Im linken Fenster wird dann eine Suchbedingung eingeblendet. Wählen Sie das Attribut aus, nach dem Sie filtern wollen. Der Vergleichsoperator verändert sich je nach Datentype des Attributs, dass Sie auswählen. Im Beispiel habe ich zwei Suchfilter hinzugefügt:

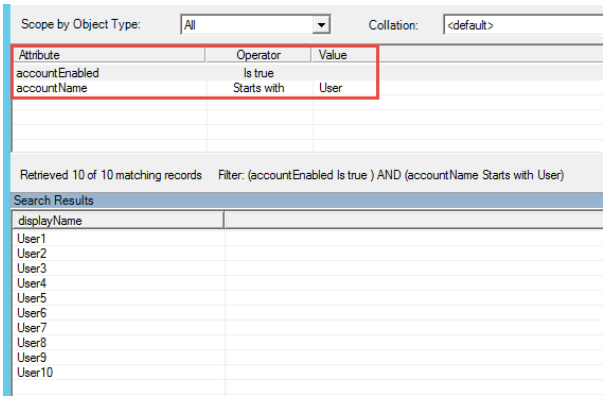


Abbildung 77 - Mit Suchfiltern die Objektanzeige einschränken

Die Collation bezieht sich auf die Zeichentabelle, die bei der Abfrage verwendet werden soll. Die Daten müssen aus dem Verzeichnisdienst in den SQL-Server übertragen werden. Der SQL-Server verwendet zur Angabe der unterstützten Zeichensätze Collations (Sortierungen im Deutschen). Die Collation bestimmt letztendlich, wie Sie Sonderzeichen ausgegeben bekommen. Wenn Sie also Sonderzeichen in Benutzernamen nicht richtig angezeigt bekommen, versuchen Sie doch mal eine andere Collation. Die wichtigsten Kürzel bei der Anzeige der Collations sind CI für Case Insensitive bzw. CS für Case Sensitive und AS für Accent Sensitive. Case bezieht sich also auf Groß-Kleinschreibung (CS ist eine gute Wahl, denn diese Collation unterscheidet Groß- und Kleinbuchstaben), während AI oft keine gute Wahl ist, da Sonderzeichen wie Ä dann wie ein A behandelt werden. Bei BIN handelt es sich um Binärsortierungen, die Daten werden bei der Ausgabe nach Ihrem Auftreten in der ASCII-Tabelle und nicht nach dem Alphabet sortiert.

Die Eigenschaften der gefundenen Objekte können Sie sich jetzt wieder anzeigen lassen, indem Sie das Objekte auswählen und dann unter Actions Properties anklicken.

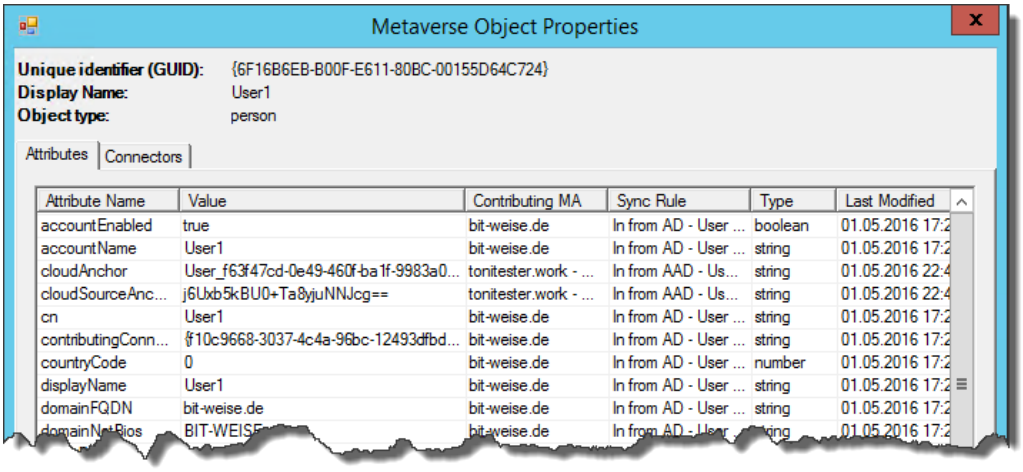


Abbildung 78 - Die Details eines Objekts in der Metaverse

Die Synchronisations-Regeln verstehen“.

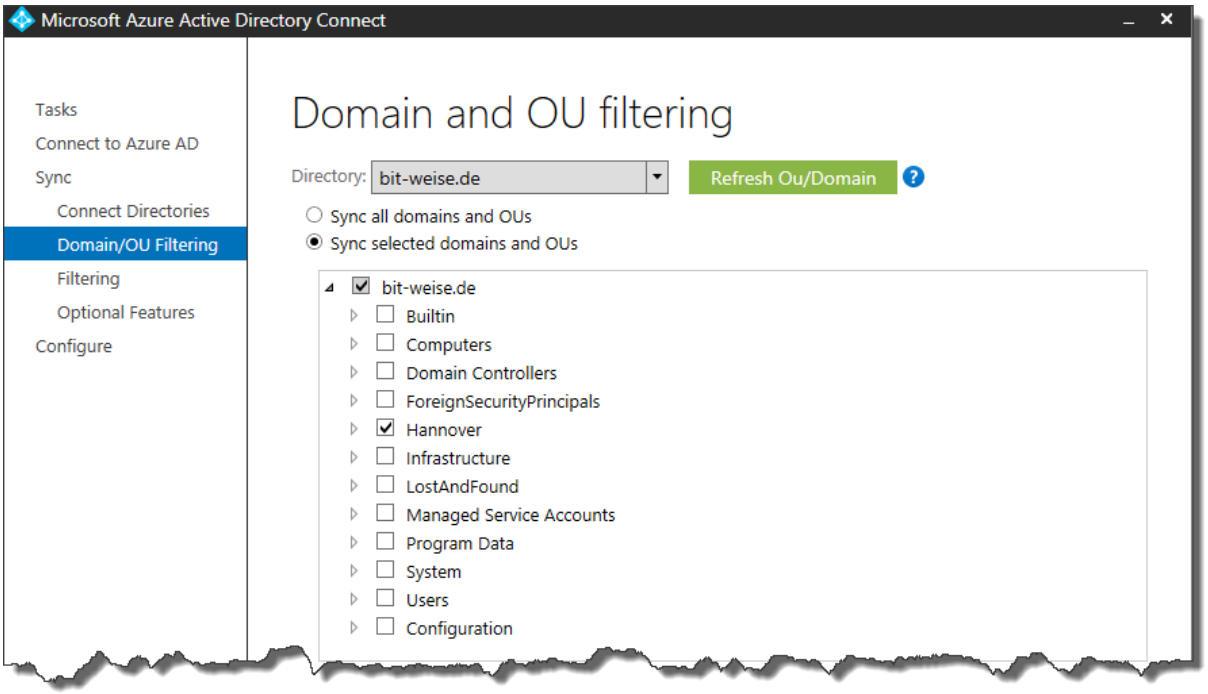


Abbildung 45 - Es werden nur Objekte aus der OU "Hannover" synchronisiert

Zusätzlich zur OU kann man auch über eine Gruppe steuern, welche Objekte repliziert werden sollen. Diese Gruppe wird zusätzlich zur OU als Filter verwendet! Die Idee ist, über die angegebene Gruppe erst einmal Testbenutzer zu synchronisieren.

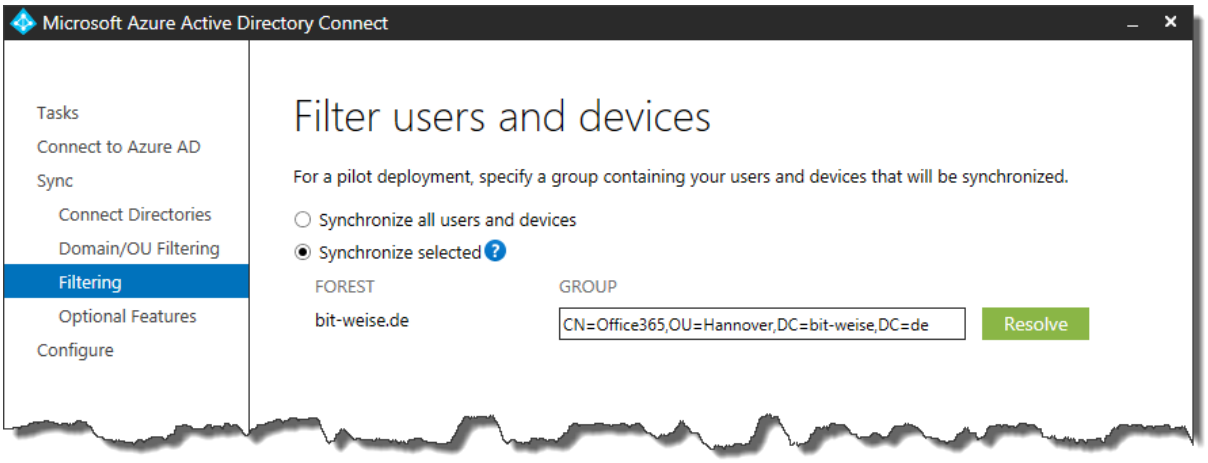


Abbildung 46 - Geben Sie eine Gruppe an, die als Filter verwendet werden soll.

Als nächstes können optionale Features wie die Kennwort-Rücksynchronisation (Password Writeback) festgelegt werden. Die Writeback-Features ermöglichen die 2-Wege-Synchronisation. So kann beispielsweise ein Benutzer sein Kennwort in Office 365 ändern, und die Kennwortänderung wird dann ins AD zurück repliziert. Das kann beispielsweise bei Nutzern sinnvoll sein, die normalerweise gar keine Anmeldung mehr am lokalen AD durchführen oder nur mit den Web-Anwendungen arbeiten. Außerdem können hier neben den AD-Attributen, die standardmäßig synchronisiert werden, weitere AD-Attribute zur Synchronisation hinzugefügt werden.

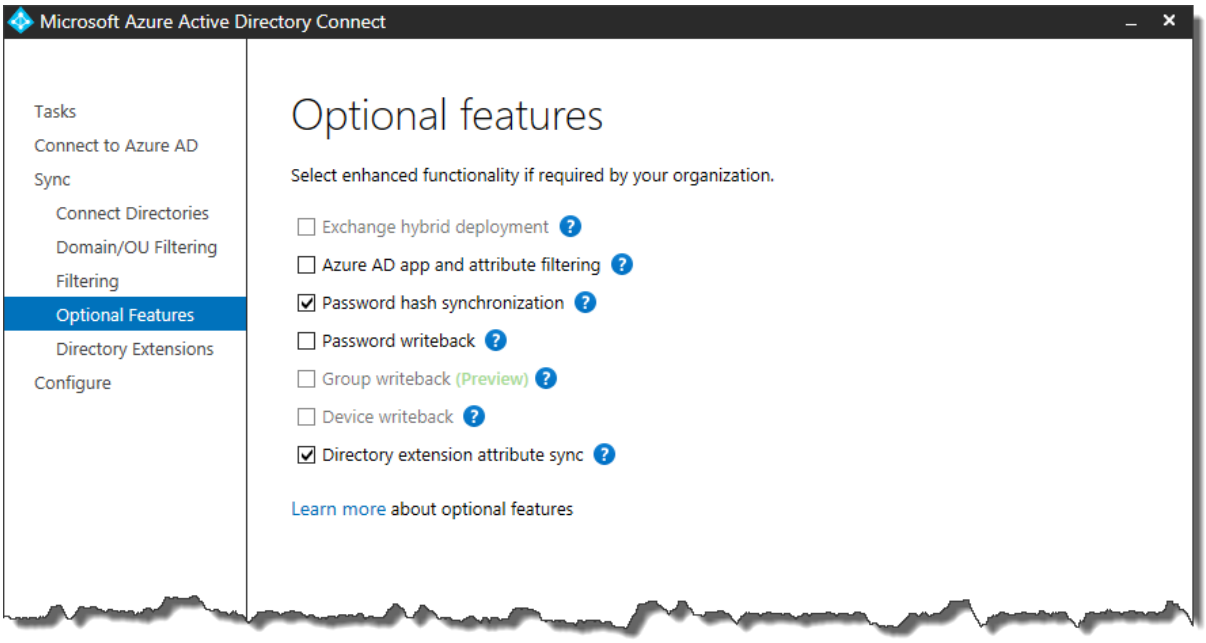


Abbildung 47 - Aktivieren oder deaktivieren von Features

Haben Sie *Directory extension attribute sync* ausgewählt, folgt als nächstes ein Auswahlfenster, dass Ihnen alle verfügbaren AD-Attribute anzeigt. Wählen Sie hier die Attribute aus, die sie zusätzlich in die Synchronisation mit aufnehmen wollen, indem Sie die Attribute markieren und mit dem Pfeil aus dem Fenster *Available Attributes* in *Selected Attributes* verschieben. Eine Mehrfachauswahl ist bei gedrückter STRG-Taste möglich.

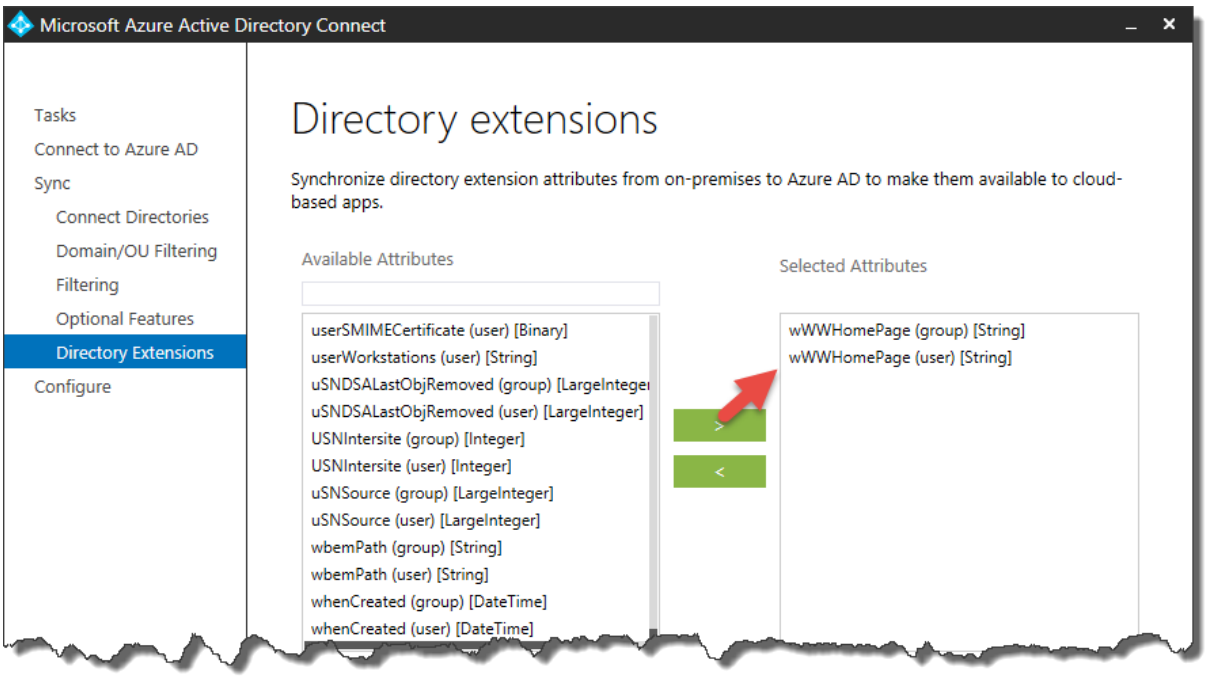


Abbildung 48 - Weitere AD-Attribute zur Synchronisation hinzufügen

Starten Sie nun die Konfiguration, indem Sie auf Next klicken.

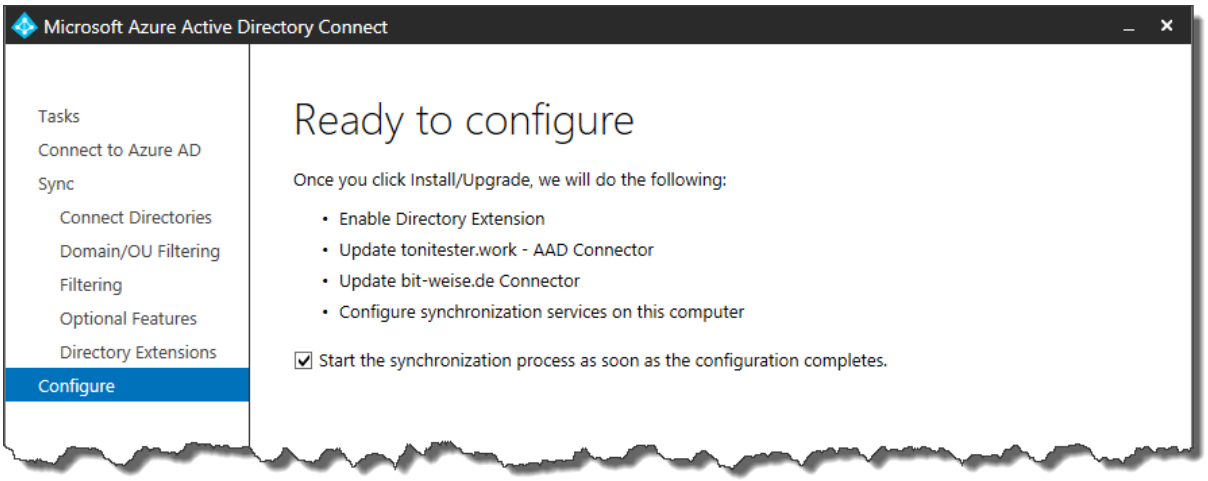


Abbildung 49 - Die Änderungen werden konfiguriert, sobald Sie Next klicken.

Refresh Directory Schema

Die Option *Refresh directory Schema* ist notwendig, um Änderungen des AD-Schema in die Metaverse zu kopieren, und wird immer nur dann benötigt, wenn das Schema erweitert wurde, wie beim Update des AD auf eine neue Windows-Version oder bei der Installation von Exchange. Wählen Sie hierzu einfach Refresh Directory Schema aus, melden Sie sich an Ihrem AD mit Forest-Administrator an und wählen Sie aus, welche Domänen / Forests Sie aktualisieren wollen.

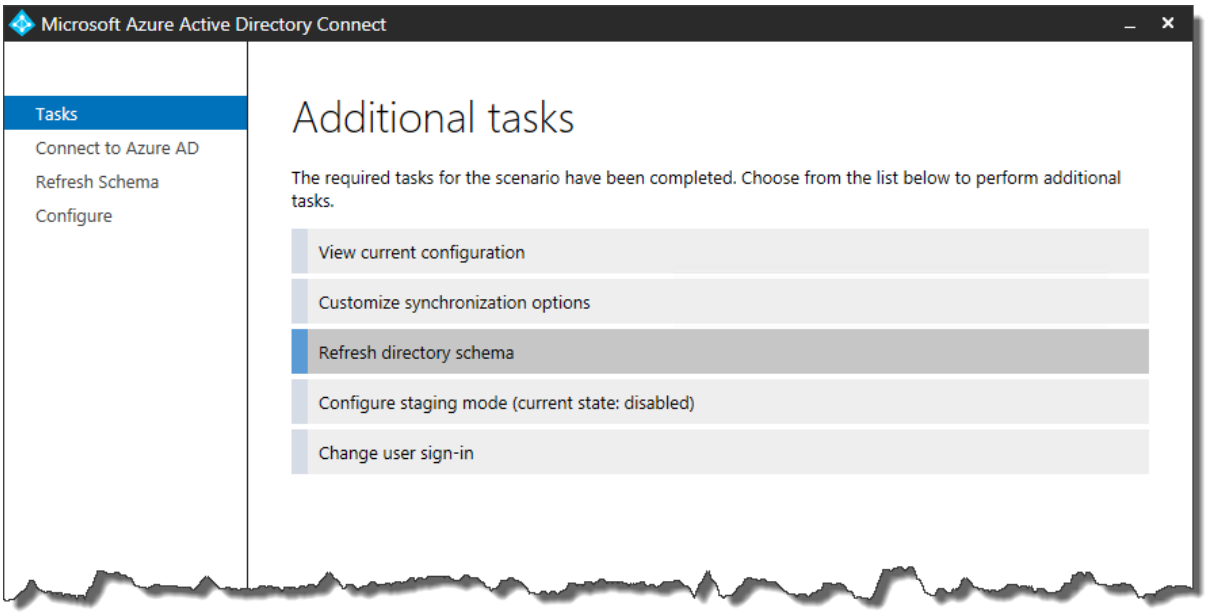


Abbildung 50 - Schema-Aktualisierungen in die Metaverse importieren

Geben Sie als nächstes wieder einen globalen Administrator für Ihr Azure AD ein.

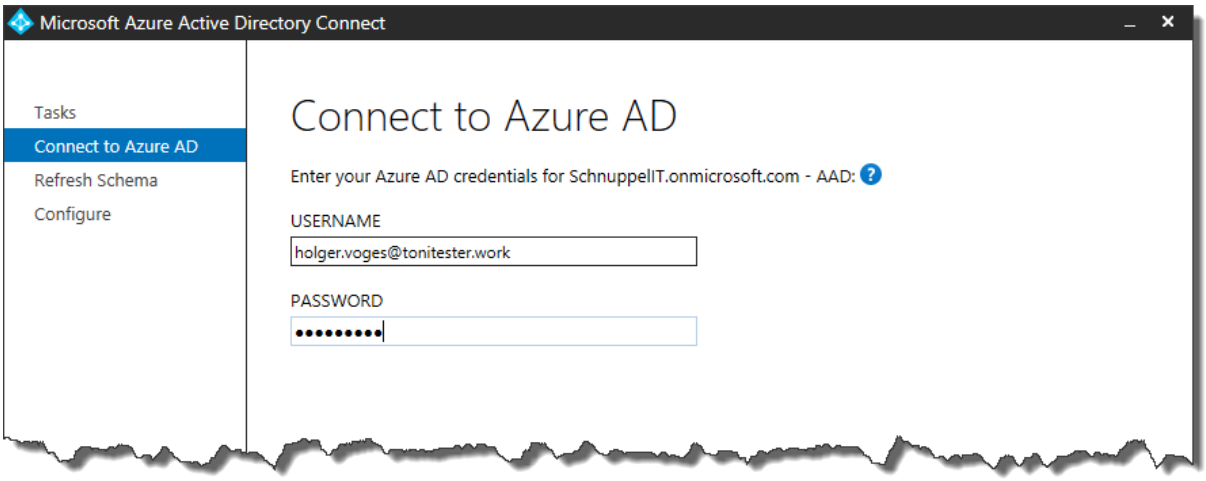


Abbildung 51 - mit globlalem Admin anmelden

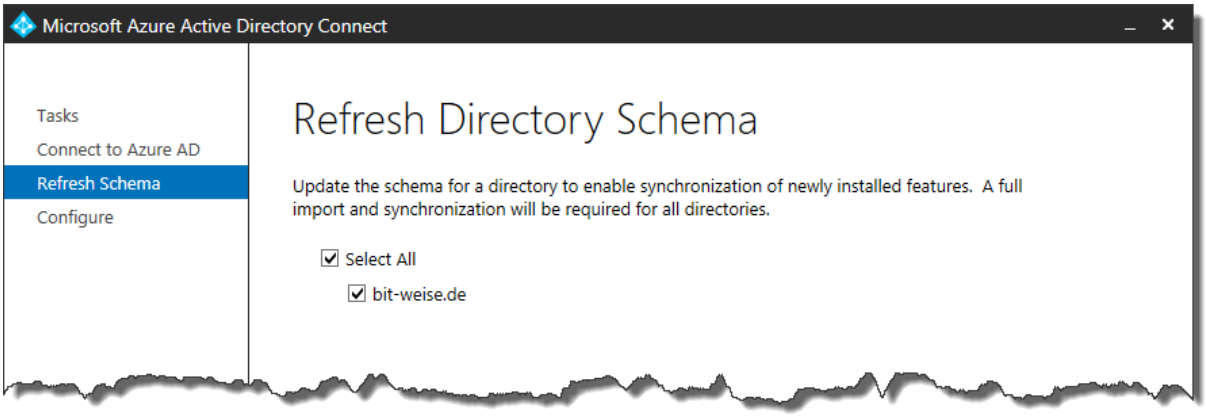


Abbildung 52 - Wählen Sie die Domänen aus, die aktualisiert werden sollen

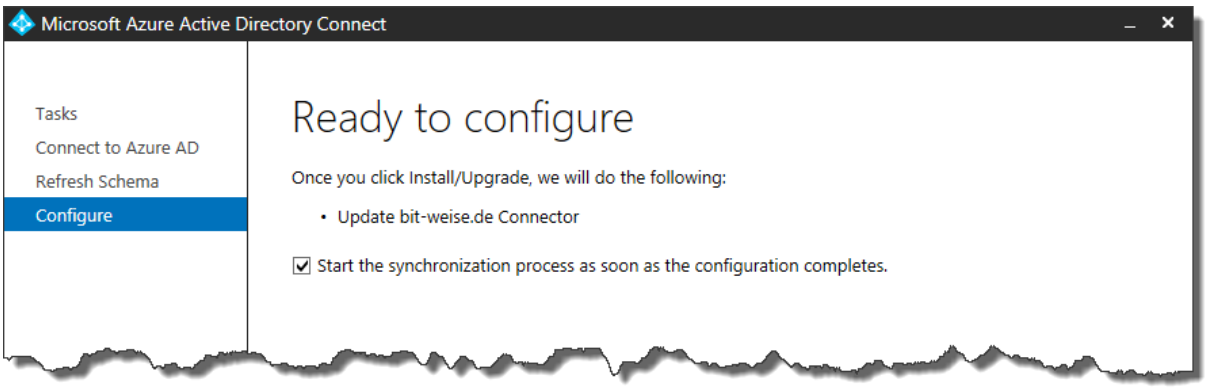


Abbildung 53 - und starten Sie den Synchronisationsprozess

Staging Mode

Im Staging Mode wird bei der Synchronisation nur ein Im- aber kein Export durchgeführt. Für den Staging-Mode gibt es mehrere Einsatzszenarien. Zum einen kann man im Staging-Mode die Importieren Daten testen, bevor man ein System live schaltet. Mit Hilfe des Synchronization-Managers kann man alle importierten Daten in der Metaverse einsehen. Der Export wird aber erst aktiviert, sobald der Staging-Mode deaktiviert ist.

Zum anderen ist der Staging-Mode die einzige Möglichkeit, in einem Fehlerausfall schnell einen alternativen Server für die Replikation verfügbar zu haben. AD Connect hat keine eingebaute Fehlertoleranz. Der Ausfall des Synchronisations-Servers beendet die Synchronisation zwischen den verknüpften Verzeichnissen. Da der AD-Connect Server aber selber keine Daten generiert, kann die Replikation durch einen neuen Server relativ schnell wiederaufgebaut werden. Um den Prozess zu beschleunigen, kann man einen zweiten Server bereits vorbereiten. Da jedoch nicht beide Server Ihre Daten exportieren dürfen, dürfen alle zusätzlichen AD Connect Server nur als Staging-Server betrieben werden. Sobald der Hauptserver dann ausfällt, kann sofort ein Staging-Server aus dem Staging-Mode genommen werden. Der Hauptvorteil ist, dass die initiale Beladung der Metaverse entfallen kann, da dies im Staging-Mode bereits geschehen ist.

Außerdem kann man mit dem Staging-Mode die Ablösung eines alten Servers durch einen neuen vorbereiten.

Zum aktivieren des Staging-Mode wählen Sie *Configure Staging Mode* aus:

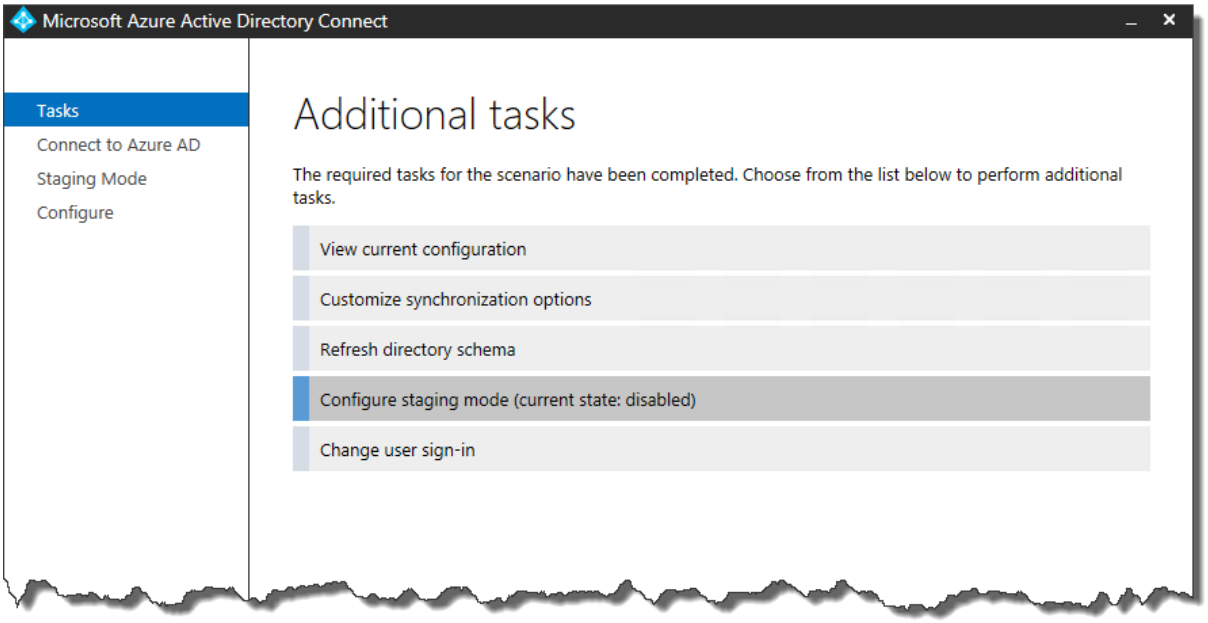


Abbildung 54 - Aktivieren des Staging-Mode

Verbinden Sie sich jetzt mit dem Azure AD

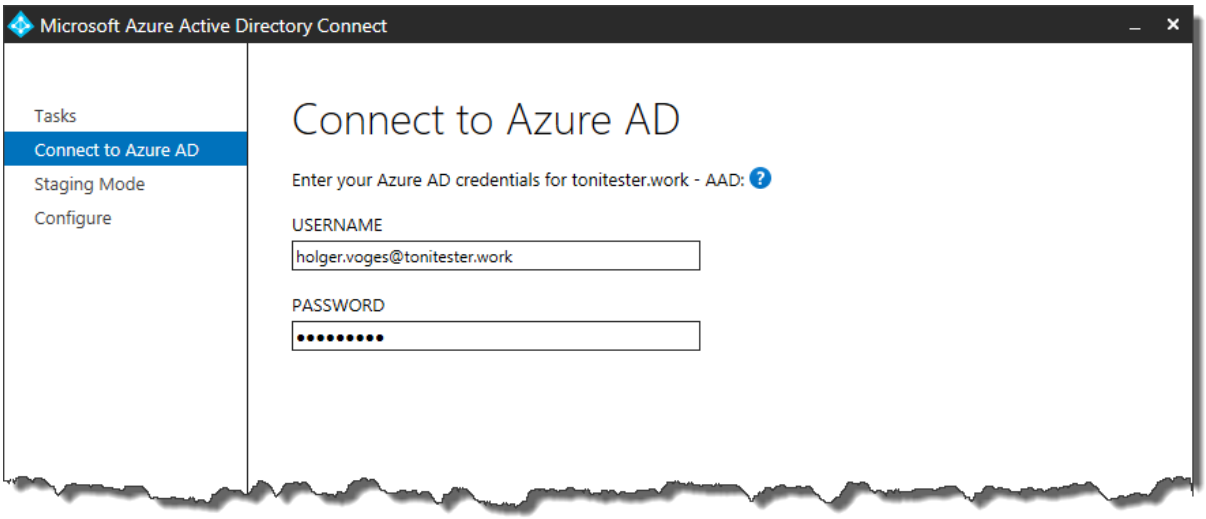


Abbildung 55 - Anmelden am AAD

Und nun aktivieren Sie den Staging Mode

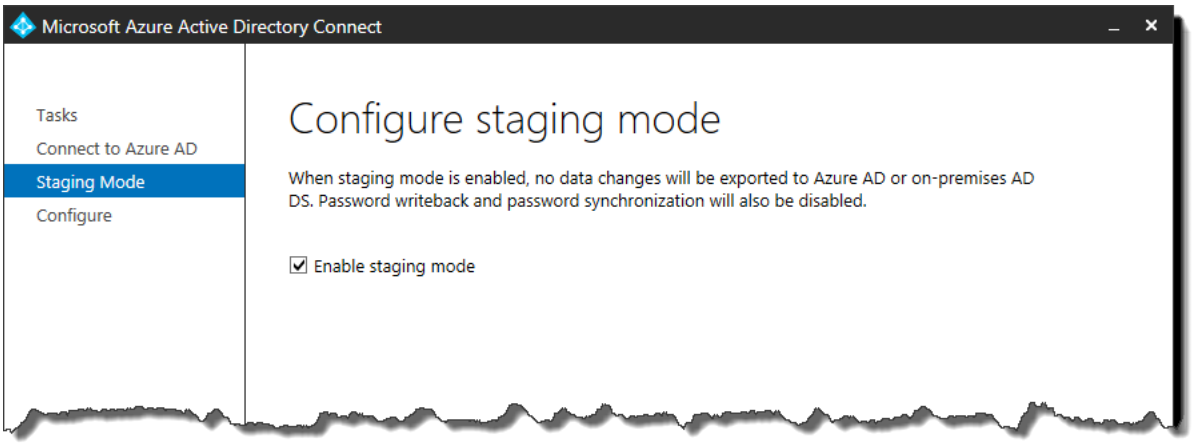


Abbildung 56 - Haken setzen, um den Staging-Mode zu aktivieren

Anschließend müssen Sie auswählen, ob Sie sofort eine Synchronisation starten wollen.

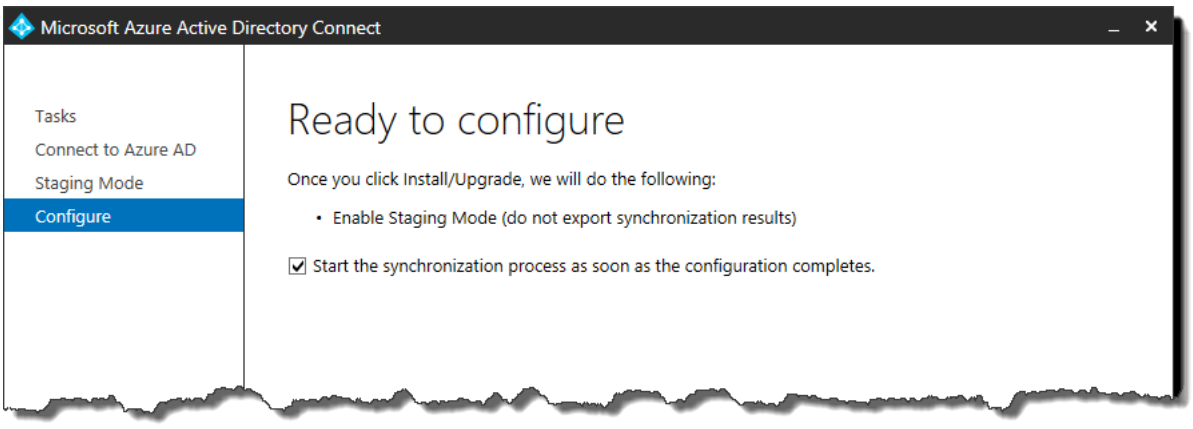


Abbildung 57 - Starten des Synchronisierung

Um den aktuellen Status des Staging Mode abzufragen, nutzen Sie Powershell:

```
Get-ADSyncScheduler | select-object StagingmodeEnabled
```

Um den Server aus dem Staging-Mode zurück in den Normalbetrieb zu schalten, verwenden Sie einfach wieder den Assistenten und entfernen den Haken bei Staging Mode.

Eine genaue Beschreibung der Konfiguration finden Sie in der AD Connect Dokumentation:

Azure AD Connect sync: Operational tasks and consideration
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-operations/

Konfigurieren des 2. Servers im Staging-Mode

Der 2. Staging-Mode-Server muß manuell konfiguriert werden. Haben Sie von den Standardeinstellungen abweichende Konfigurationen vorgenommen, müssen diese auf dem Staging-Mode Server explizit noch einmal angewendet werden, indem Sie auch auf diesem den Konfigurations-Assistenten durchlaufen lassen. Nur die Synchronisationsregeln können als Powershell-Script exportiert und dann wieder importiert werden. Sie finden zwar im Synchronization Manager einige Einstellungen, mit denen Konfigurationen exportiert werden können, aber diese sind unter Umständen nicht vollständig. Sehen Sie hierzu auch in der Azure AD Connect FAQ den Artikel unter Custom Configuration:

https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-faq/

Konfigurieren des Synchronization Service

Der Synchronization-Service erlaubt Ihnen das Steuern der Synchronisation und die Konfiguration der Konnektoren.

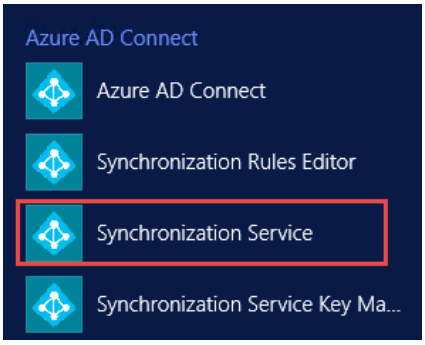


Abbildung 58 - Starten der Sync-Service GUI

Er gibt auf vier Reitern einen Überblick über die **letzten Synchronisationen**, die **konfigurierten Konnektoren** und die angebundenen Verzeichnisse, den **Status der Metaverse** und den **Inhalt der Metaverse-Datenbank**. Hier können auch neue Konnektoren manuell erstellt und Synchronisationen manuell angeworfen werden.

Synchronization Manager Operations Menü

Wann die Synchronisation zum letzten Mal stattgefunden hat, findet man auf der ersten Seite des Synchronization Managers im Menü Operations. Hier wird für jeden Synchronisationsvorgang ein Log angelegt, das anzeigt, ob eine Synchronisation erfolgreich war, wann Sie durchgelaufen ist und wie viele Objekte verändert worden sind.

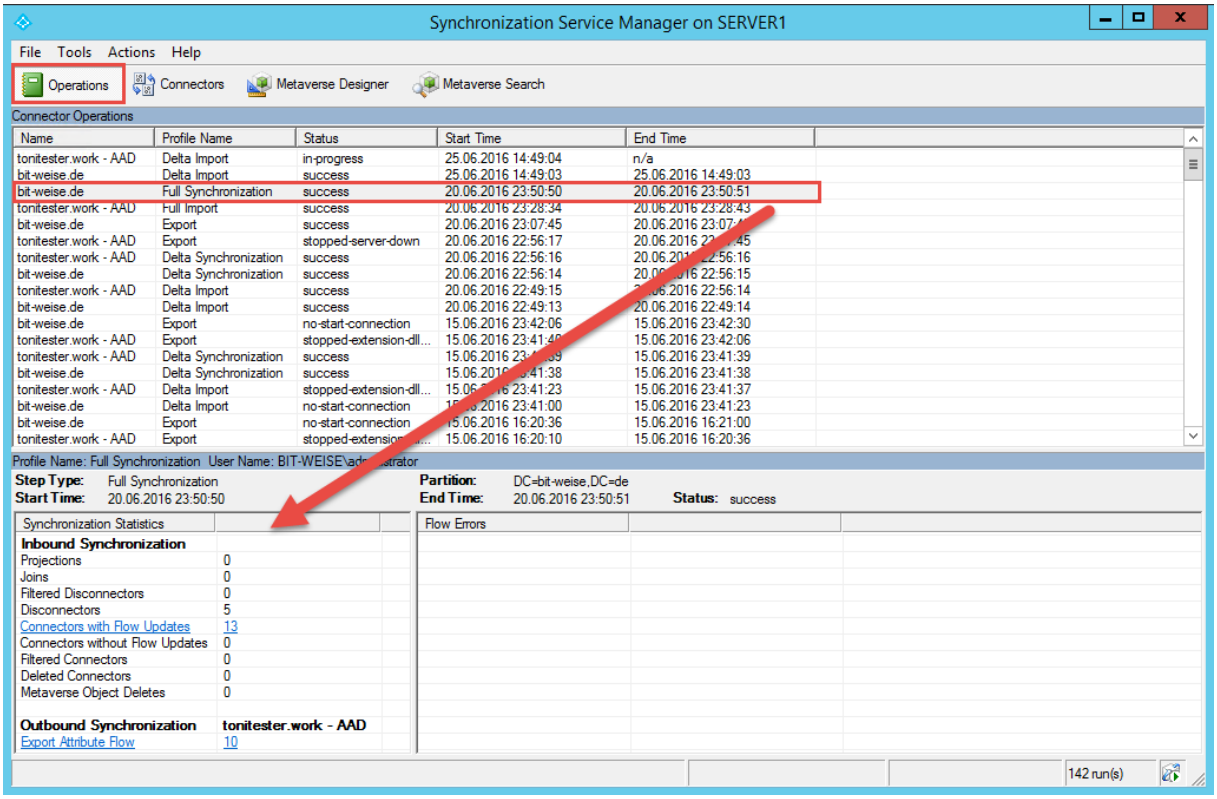


Abbildung 59 - Log der durchgeführen Synchronisationen

Jeder Eintrag in der Tabelle Connector Operations entspricht einer Synchronisation. In der Spalte „Profile Name“ kann man ersehen, was für ein Typ (Synchronisations-Profil) stattgefunden hat. Ein Konnektor kann z.B. Vollständig oder Inkrementell (Delta) synchronisieren, und er kann einen Im- oder Export ausführen. Die einzelnen Profile für die einzelnen Konnektoren kann man unter dem Reiter „Connectors“ für jeden einzelnen Konnektor einstellen:

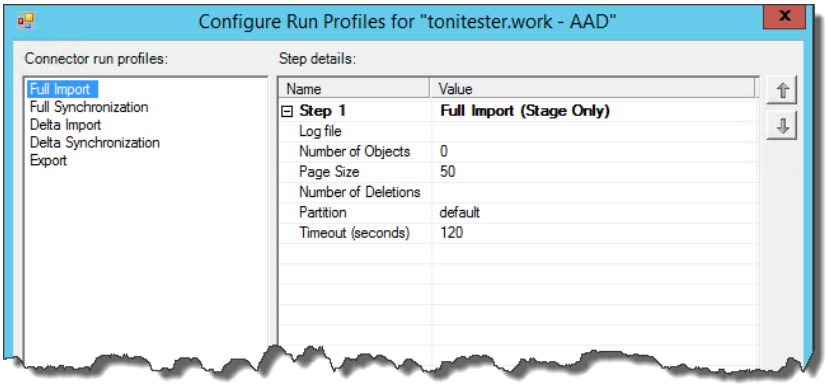


Abbildung 60 - Die Synchronisations Profile für den Connector "tonitester.work - AAD"

Unter Synchronization-Statistics findet man eine Auflistung über die einzelnen Aktionen, die während des Durchlaufs ausgeführt worden sind. In unserem Beispiel sieht man also, dass keine Objekte neu angelegt (Joins) oder gefiltert worden sind. Insgesamt sind 13 Objekte (Connectors) von dem Konnektor erfasst worden, 5 Objekte werden nicht repliziert (Disconnectors).

In diesem Fenster kann man auch manuell eine Synchronisation starten oder stoppen, indem man das Kontextmenü eines Eintrags unter „Connector Operations“ aufruft.

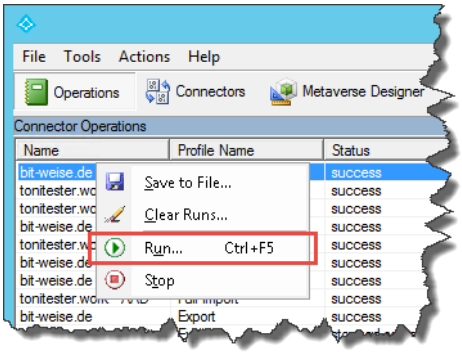


Abbildung 61 - manuelles starten einer Synchronisation

Wählt man RUN, wird man in einem weiteren Fenster nach dem Konnektor und dem Run-Profil gefragt:

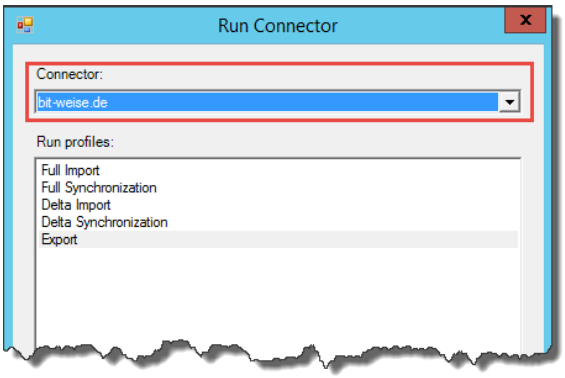


Abbildung 62 - Auswahl des Connectors und des Run-Profils

Synchronization Manager Connectors Menü

Im zweiten Fenster (Menü Connectors) findet man die ein-und ausgehenden Konnektoren und Ihren Status.

Jeder Connector stellt eine Verbindung zwischen einem Verzeichnisdienst und der Metaverse dar. In unserem einfachen Beispielszenario gibt es nur einen eingehenden Connector vom lokalen AD zum Sync-Service, und einen ausgehenden Connector zum Azure AD. Im Action-Fenster rechts neben den Konnektoren können wir den Connector bearbeiten (Properties), die Synchronisations-Profile konfigurieren, neue Konnektoren anlegen (was aber, wie beschrieben, für Active-Directory Verbindungen durch das AD Connect Konfigurationstool einfacher ist), den letzten Synchronisationslauf eines Connectors einsehen und den Verbindungsstatus zum DC sehen.

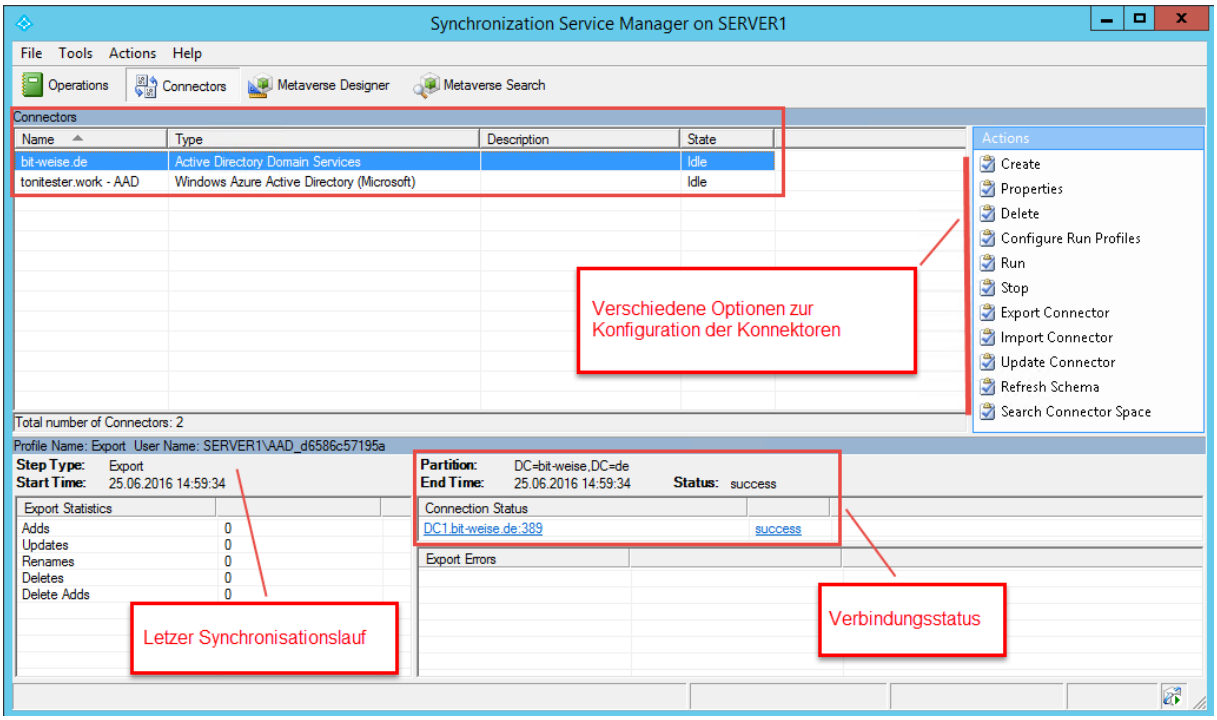


Abbildung 63 - Konnektor-Konfiguration

Wenn Sie einen Konnektor auswählen und im Action-Menü Properties auswählen, können Sie den Konnektor konfigurieren. Je nach Konnektor-Typ gibt es unterschiedliche

Konfigurationsmöglichkeiten. Im Folgenden finden Sie die Einstellungen des Active Directory Domain Services Connectors.

Im ersten Fenster finden Sie den Namen und den Typ.

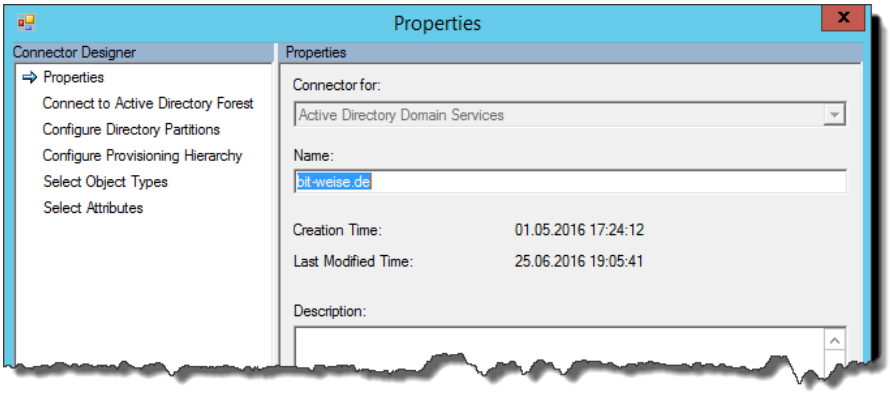


Abbildung 64 - Eigenschaften des Konnektors

Unter *Connect to Active Directory Forest* sind die Verbindungseinstellungen hinterlegt. Hier finden Sie die Domäne, mit der der Konnektor sich verbindet, und den Benutzernamen des Synchronisationskontos. Das Synchronisationskonto wird verwendet, um sich am AD anzumelden. Je nach aktivieren Funktionen muss das Konto über unterschiedliche Berechtigungen verfügen (siehe Wenn die Replikation innerhalb eines Forest stattfindet, ist das Identifizieren von Objekten über die ObjectGUID einfach möglich.)

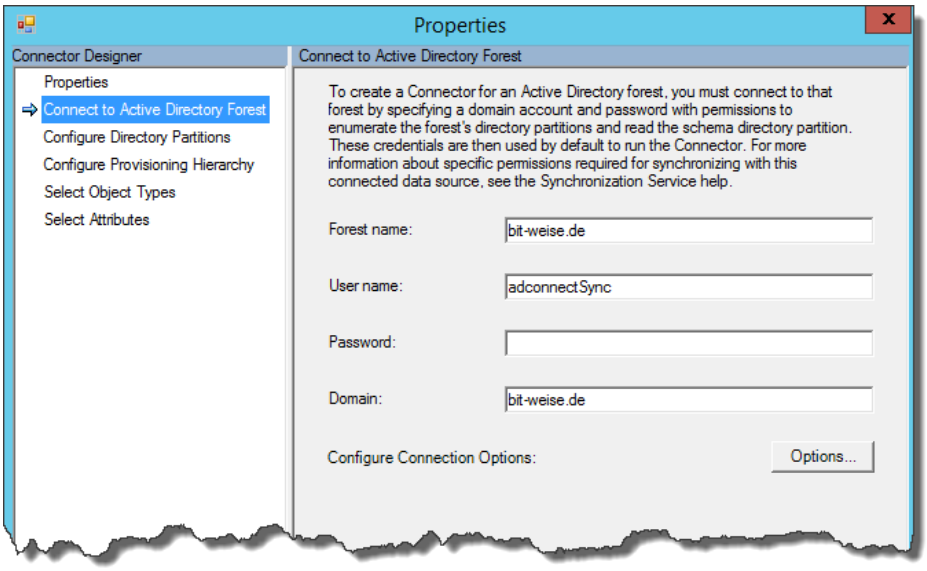
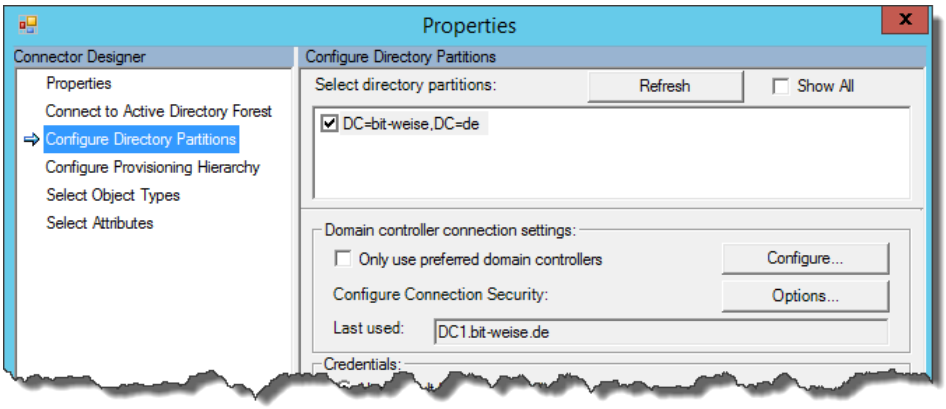


Abbildung 65 - Der DNS-Name des Zielverzeichnisses und das Verbindungskonto

Unter *Configure Directory Partitions* können Sie die Partitionen festlegen, aus denen Objekte repliziert werden sollen. Standardmäßig finden Sie hier die Datenpartition der der Zieldomäne.



Wählen Sie *Show All* aus, müssen Sie zuerst das Kennwort des Verbindungskontos eingeben. Nach erfolgreicher Anmeldung werden alle Partitionen angezeigt. Wählen Sie eine Partition aus, können Sie konfigurieren, über welchen Domänencontroller die Synchronisation stattfinden soll, Sie können für die Verbindung mit der Partition ein alternatives Verbindungskonto angeben, und Sie können unter Containers die Objekte auf bestimmt OU´s im AD filtern – diese Einstellung haben wir bei der Installation des AD Connectors bereits angepasst. Auch diese Einstellung kann man über das AD Connect Konfigurationstool einfacher anpassen (siehe auch S. 36).

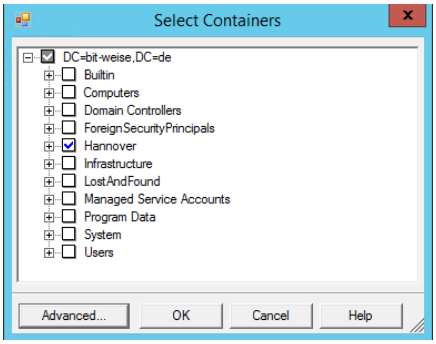


Abbildung 66 - Filtern nach OUs

Eine interessante Einstellung finden Sie, wenn Sie auf den Button Advanced klicken. Hier finden Sie alle Container noch einmal wieder:

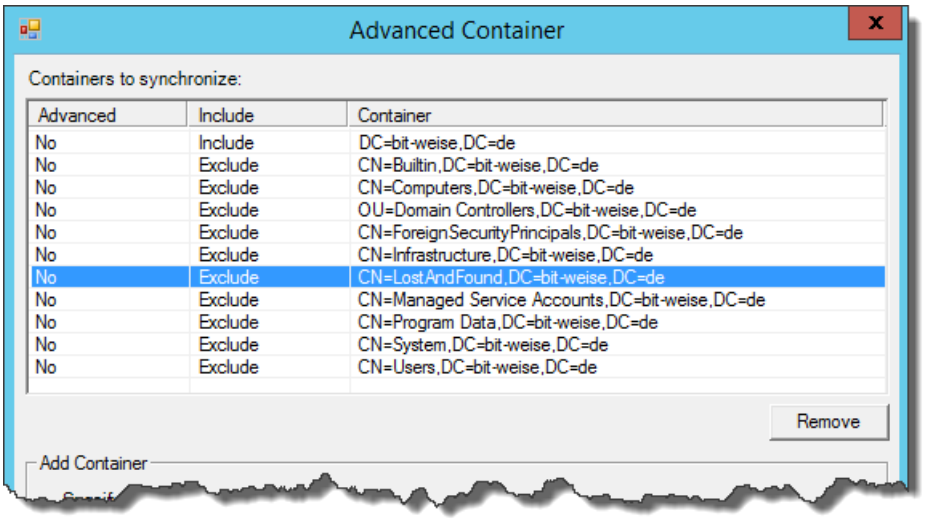
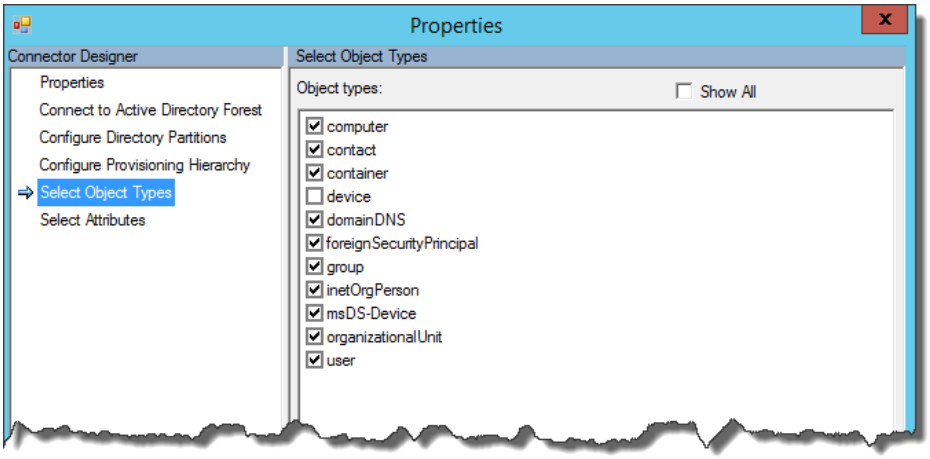


Abbildung 67 - Erweiterte Container Filterung

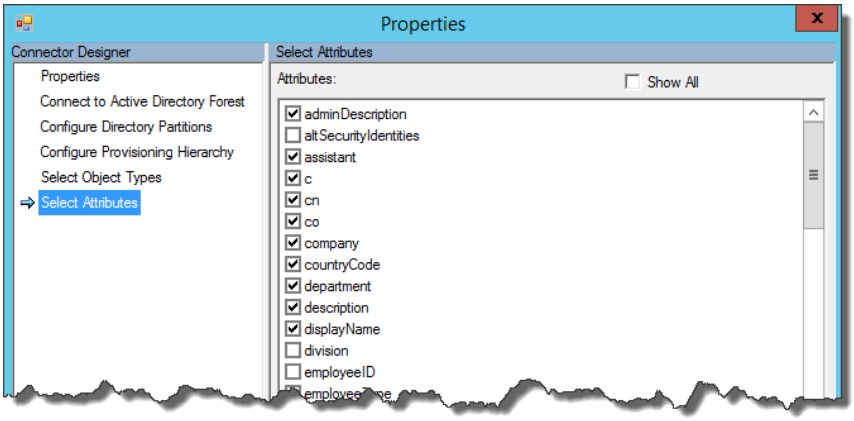
Anders als im vorigen Fenster sind hier aber alle Container explizit ausgenommen. AD Connect konfiguriert zuerst einen Include auf die Domäne, muss dann aber alle anderen Container explizit ausfiltern.

Im Fenster *Configure Provision History* legen Sie fest, wie der Connector mit Objekten umgeht, deren Container noch nicht existiert. In der Standardkonfiguration hat der Connector keine Provisionierungs-Regeln definiert. Wählen Sie unter *Configure Provisioning Hierarchy* ou aus und im Auswahlfenster *Directory ObjectClass* Organizational Unit und bestätigen dann mit New wird eine neue Provisionierungssregel angelegt, die fehlende OUs einfach anlegt. Da Azure AD aber keine Hierarchien unterstützt, ist das hier nicht notwendig.

Unter *Select Object Types* legen Sie die Objekte fest, die synchronisiert werden sollen.



Im Menü *Select Attributes* wählen Sie die Attribute, die synchronisiert werden.



Aus den Objekt- und Attributs-Informationen baut die Sync-Engine dann die Synchronisationsregeln auf.

Wenn Sie einen Connector auswählen, können Sie über *Search Connector Space* die Objekte einsehen, die im Connector gespeichert sind.

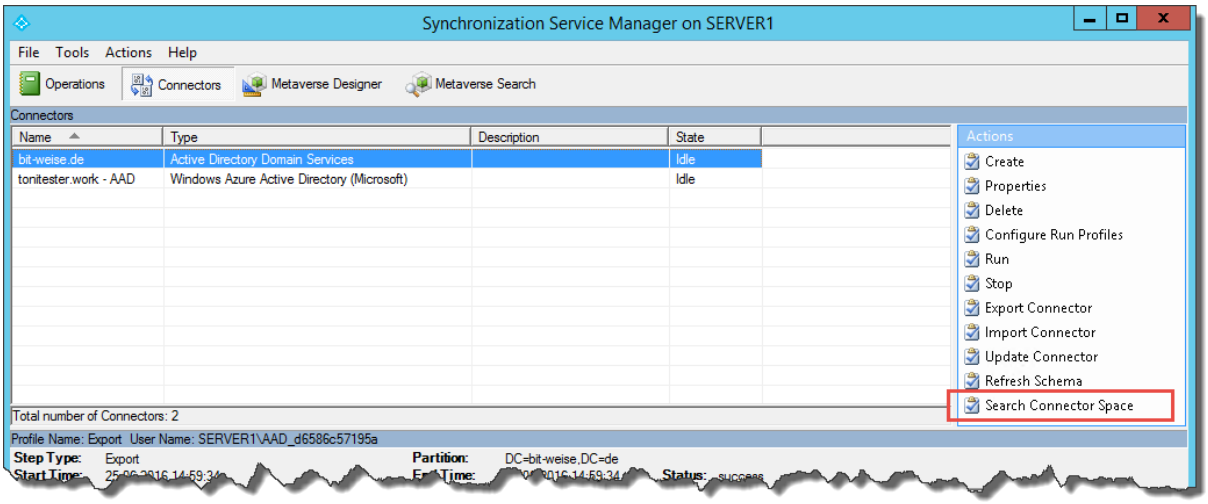


Abbildung 68 - Objekte im Connector-Space anzeigen

Klicken Sie im Suchfenster einfach auf Search, bekommen Sie eine ungefilterte Ansicht. Ansonsten können Sie auch einen Suchfilter definieren, indem Sie den Distinguished Name des Containers angeben, dessen Objekte Sie anzeigen möchten.

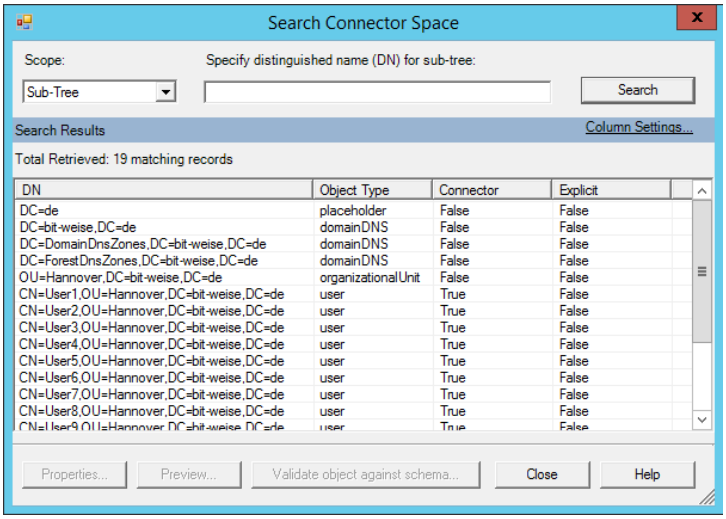


Abbildung 69 - Durchsuchen der Connector-Spaces

Wählen Sie ein Objekt aus, können Sie über den Button Properties den aktuellen Status des Objektes im Connector Space einsehen.

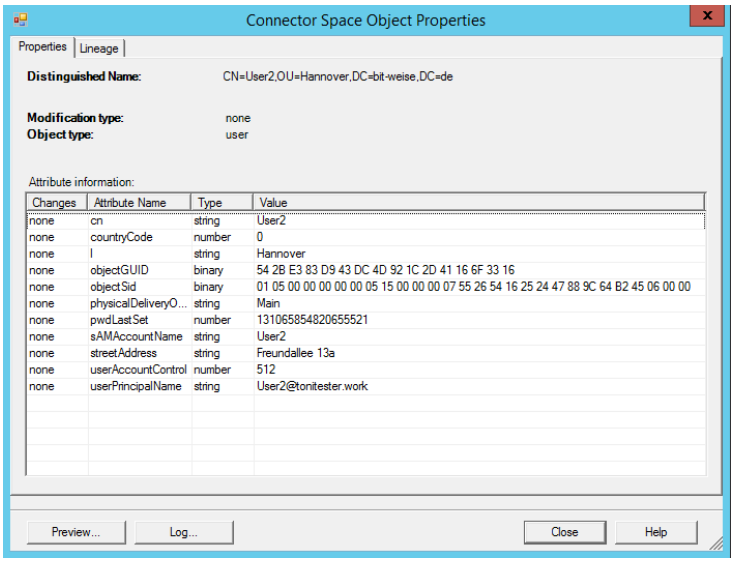


Abbildung 70 - Der Status des Objekts, wie er im Connector Space hinterlegt ist

Über den Reiter *Lineage* (Abstammung) sehen Sie, über welche Synchronisations-Regeln die Eigenschaften im- und exportiert worden sind. Klicken Sie auf *Metaverse Object Properties*, sehen Sie den Zustand des Objekts in der Metaverse. Hier sind sämtliche Attribute, die zuständige Synchronisationsregel und das letzte Änderungsdatum hinterlegt. Über den Reiter *Connectors* können Sie wiederum sehen, welche Konnektoren an der Replikation des Objekts beteiligt sind.

Wenn Sie auf den Button Preview klicken, können Sie die Replikation eines einzelnen Objektes erzwingen.

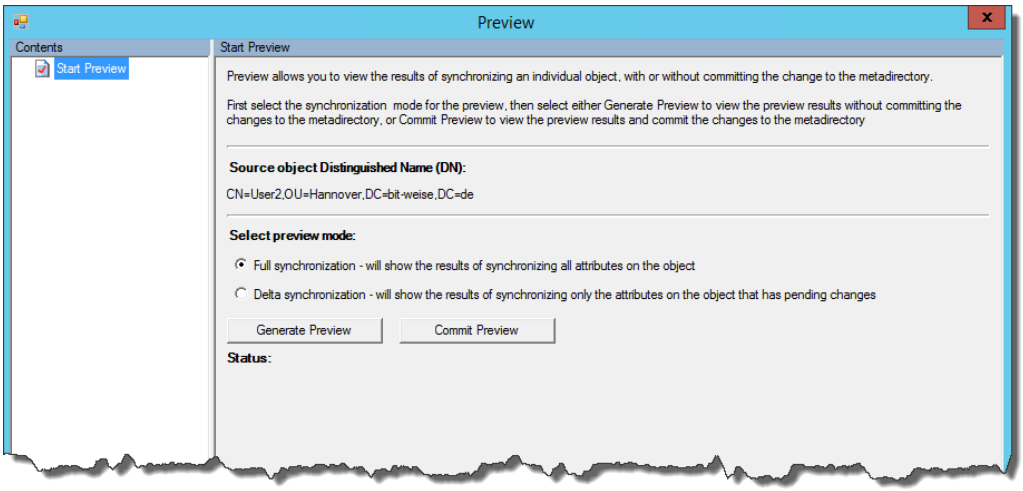


Abbildung 71 - Synchronization Preview kann auch Einzelobjekte synchronisieren

Eine Full Synchronization erzwingt eine vollständige Replikation des Objekts (Full Import / Export Profile), während eine Delta-Synchronization nur die Änderungen repliziert. Klicken Sie auf Generate Preview, werden die Änderungen nicht durchgeführt, sondern nur berechnet. Ein Commit führt eine Änderung der Objekte in den Zielverzeichnissen durch.

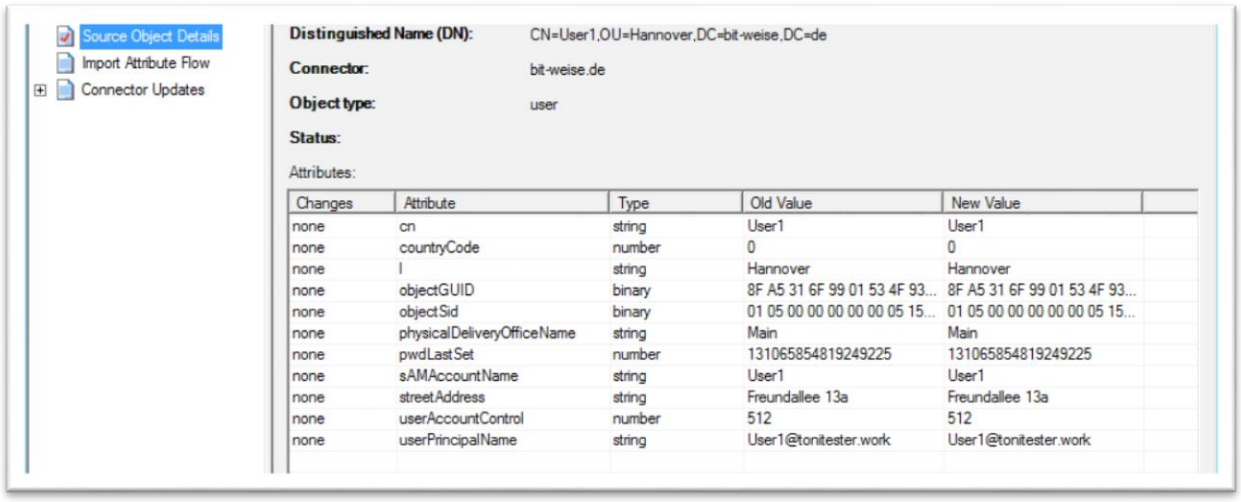


Abbildung 72 - nach dem Erzeugen des Preview wird das Quellobjekt gezeigt

Das System führt eine Berechnung aller anzuwendenden Synchronisationsregeln durch. Im Fenster „Import Attribute Flow“ werden die Import-Regeln angezeigt, zusammen mit den Startwert und den veränderten Attributen. Unter Connector-Updates findet man die Exportierten Attribute, aufgelistet nach Konnektoren.

Wenn es zu unerwarteten Ergebnissen bei der Replikation kommt, oder wenn man Änderungen an Synchronisationsregeln erst einmal an Testobjekten durchführen möchte, kann man hier genau die Auswirkungen testen. Möchte man die Änderungen nicht nur testen, sondern auch ausführen, kann man dies erreichen, indem man statt *„Generate Preview“ „Commit Preview“* auswählt.

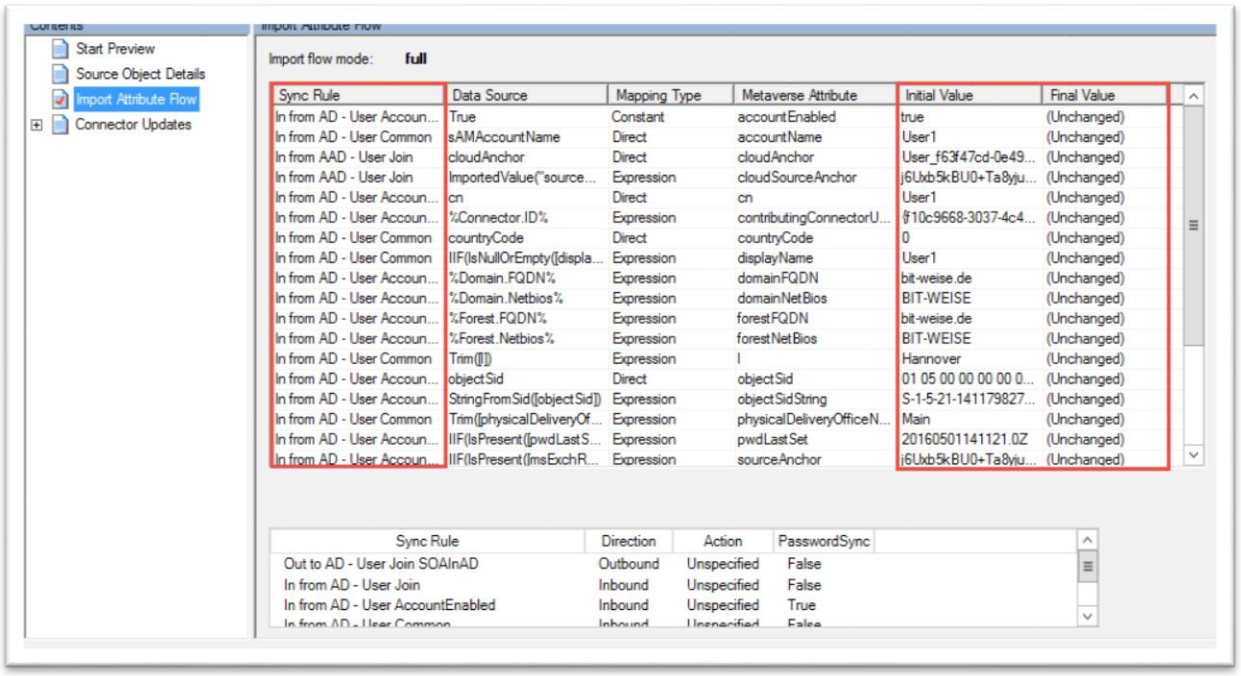
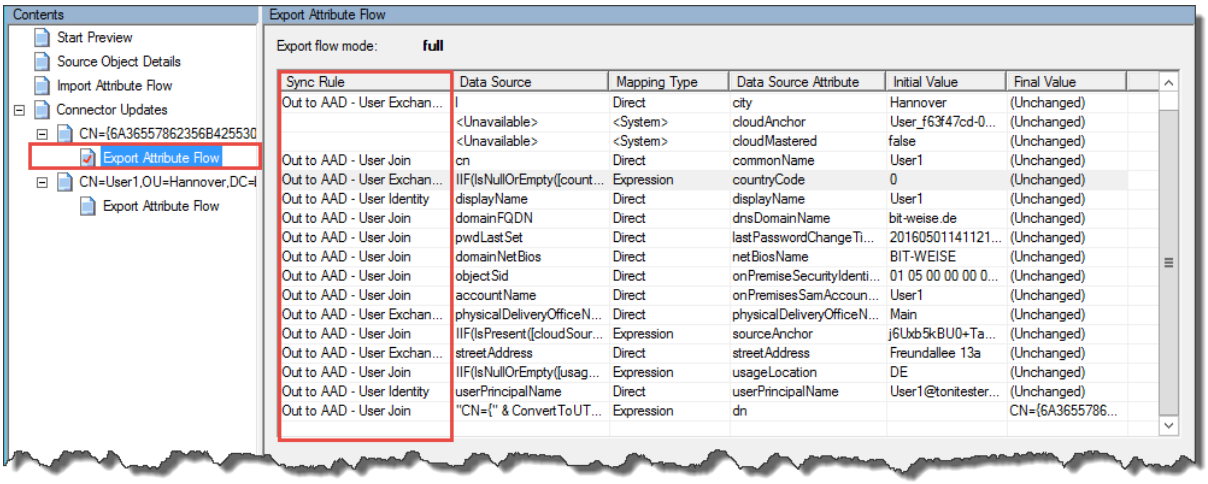


Abbildung 73 - Der Assistent zeigt einem den alten und neuen Zustand der Objekte an



Mehr Informationen zu den Connector-Einstellungen finden Sie in der Azure-Dokumentation:

Azure AD Connect sync: Synchronization Service Manager
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-service-manager-ui-connectors/

Synchronization Manager Metaverse Designer Menü

Im Metaverse-Designer können Sie die Objektvorlagen der Metaverse einsehen und bearbeiten. Hier fällt eins sofort auf: Die Metaverse unterscheidet standardmäßig Objekte nur zwischen person, group und device. Alle Objekte werden auf diese Basisobjekte abgebildet. Ein Objekte vom Type InetorgPerson und ein AD User und ein Kontakt sind für die Metaverse alle ein Person Objekt.

Grundsätzlich ist es nur dann sinnvoll, an den Vorlagen Änderungen vorzunehmen, wenn man Attribute replizieren muss, die in den Vorlagen nicht vorhanden sind. Sie können weitere Attribute einfach hinzufügen, indem Sie über *Add Attribute* im Actions-Menü weitere Attribute hinzufügen.

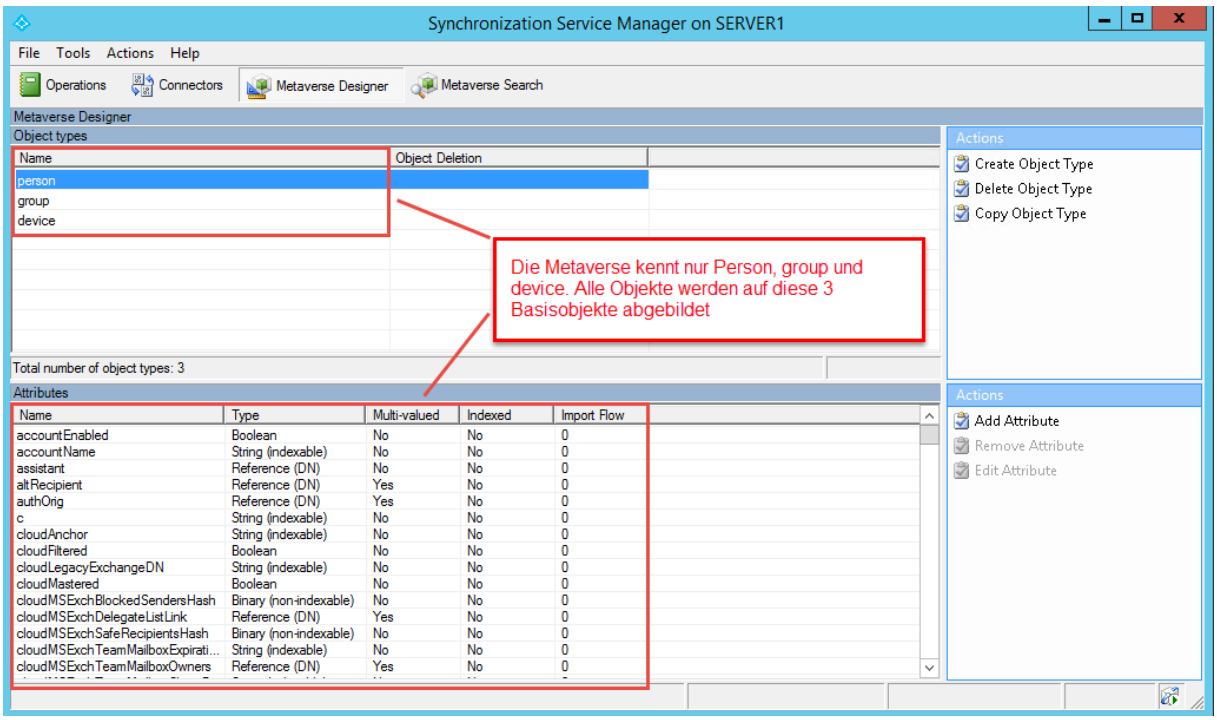


Abbildung 74 - Die Objektevorlagen der Metaverse

Wenn Sie Attribute hinzufügen wollen, können Sie zuerst aus einer Auswahl von bereits vorhandenen Attributen wählen. Sie können über *New Attribute* auch ein komplett neues Attribut erzeugen.

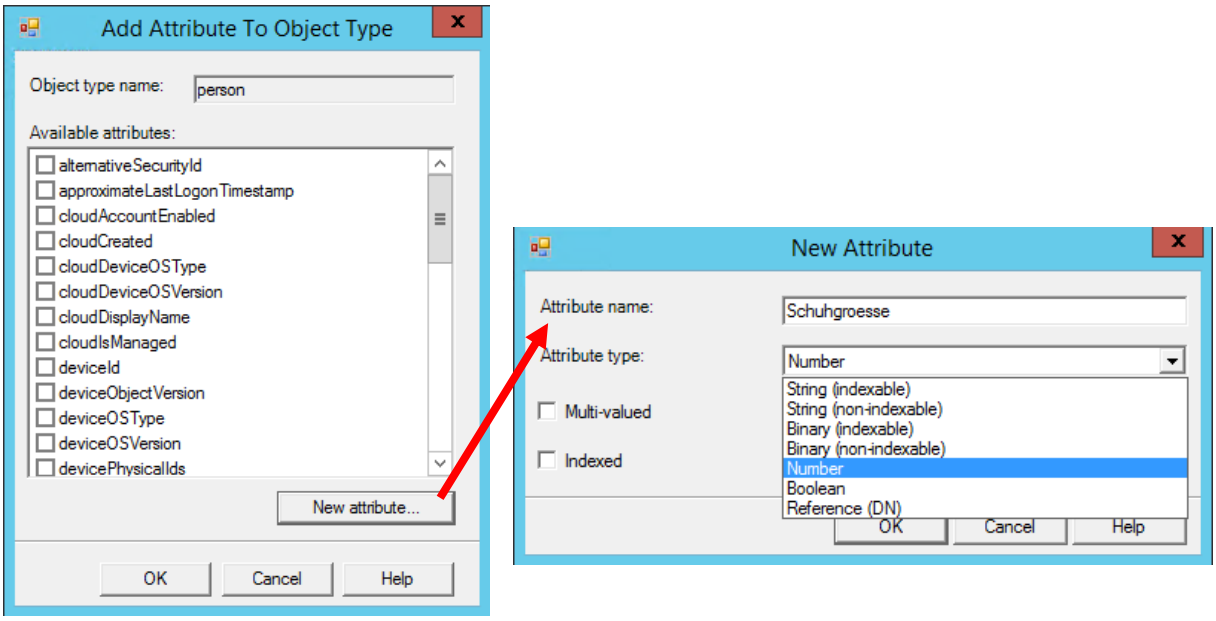


Abbildung 75 - Ein neues Attribut hinzufügen

Um das Attribut zu füllen, benötigen Sie jetzt noch eine Synchronisationregel, die die Attribute befüllt.

Synchronization Manager Metaverse Search Menü

Während Sie im Connectors Menü die Objekte einsehen können, die in den Connectors Spaces gespeichert sind, finden Sie unter Metaverse Search die Objekte, die in der Metaverse gepeichert sind.

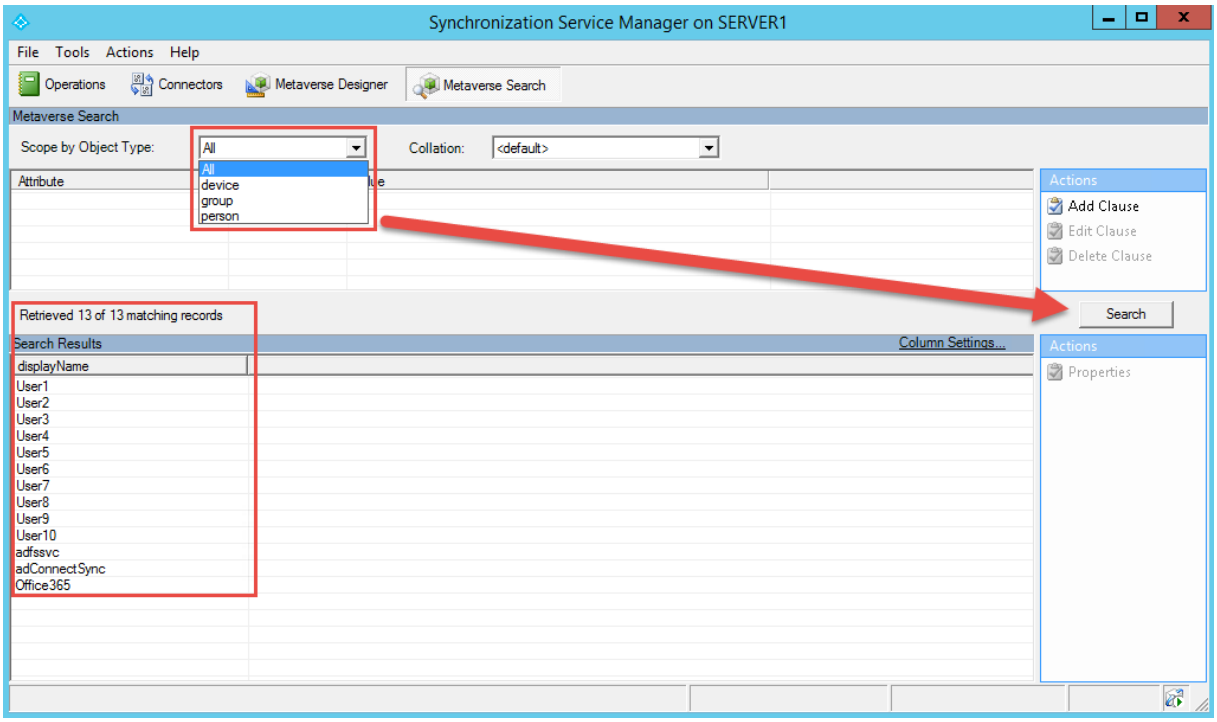


Abbildung 76 - Die Metaverse durchsuchen

Die Metaverse-Suche gestaltet sich recht einfach. Sie können den Suchfilter unter „Scope by Object Type“ auf die Vorlagen einschränken, die Sie anzeigen wollen, oder Sie können einfach alle Objekte anzeigen, die die Metaverse gespeichert hat. Klicken Sie hierfür einfach auf Search. Sie bekommen dann im untern Fenster die Suchergebnisse angezeigt. Sie können die Suche über erweiterte Suchabfragen einschränken, indem Sie im Action-Fenster eine Clause (einen Suchfilter) eintragen. Im linken Fenster wird dann eine Suchbedingung eingeblendet. Wählen Sie das Attribut aus, nach dem Sie filtern wollen. Der Vergleichsoperator verändert sich je nach Datentype des Attributs, dass Sie auswählen. Im Beispiel habe ich zwei Suchfilter hinzugefügt:

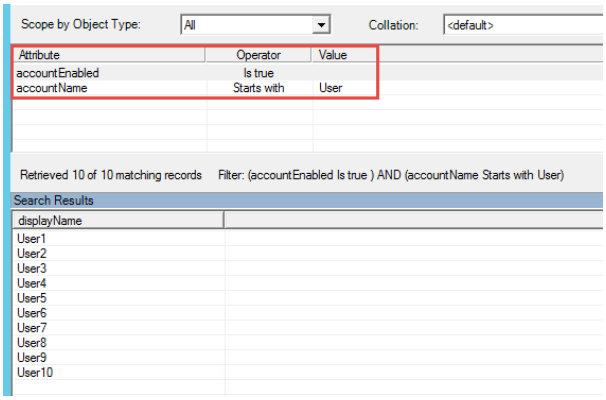


Abbildung 77 - Mit Suchfiltern die Objektanzeige einschränken

Die Collation bezieht sich auf die Zeichentabelle, die bei der Abfrage verwendet werden soll. Die Daten müssen aus dem Verzeichnisdienst in den SQL-Server übertragen werden. Der SQL-Server verwendet zur Angabe der unterstützten Zeichensätze Collations (Sortierungen im Deutschen). Die Collation bestimmt letztendlich, wie Sie Sonderzeichen ausgegeben bekommen. Wenn Sie also Sonderzeichen in Benutzernamen nicht richtig angezeigt bekommen, versuchen Sie doch mal eine andere Collation. Die wichtigsten Kürzel bei der Anzeige der Collations sind CI für Case Insensitive bzw. CS für Case Sensitive und AS für Accent Sensitive. Case bezieht sich also auf Groß-Kleinschreibung (CS ist eine gute Wahl, denn diese Collation unterscheidet Groß- und Kleinbuchstaben), während AI oft keine gute Wahl ist, da Sonderzeichen wie Ä dann wie ein A behandelt werden. Bei BIN handelt es sich um Binärsortierungen, die Daten werden bei der Ausgabe nach Ihrem Auftreten in der ASCII-Tabelle und nicht nach dem Alphabet sortiert.

Die Eigenschaften der gefundenen Objekte können Sie sich jetzt wieder anzeigen lassen, indem Sie das Objekte auswählen und dann unter Actions Properties anklicken.

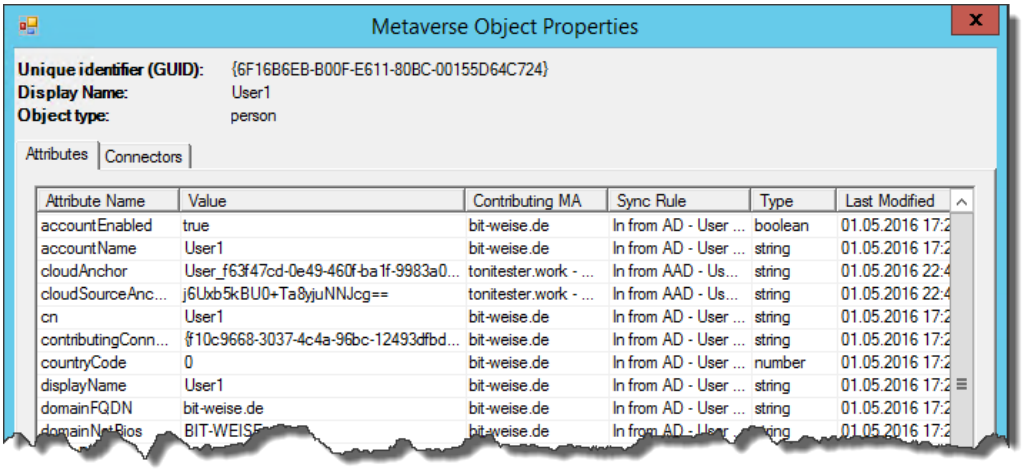


Abbildung 78 - Die Details eines Objekts in der Metaverse

Die Synchronisations-Regeln verstehen

Die Synchronisation über die Konnektoren wird über eine Reihe von Synchronisations-Regeln gesteuert. Die Synchronisations-Regeln können im *Synchronization Rules Editor* eingesehen und konfiguriert werden.

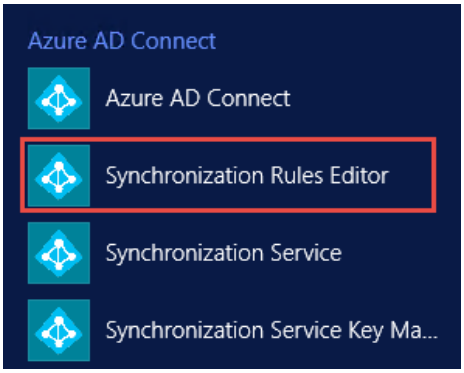
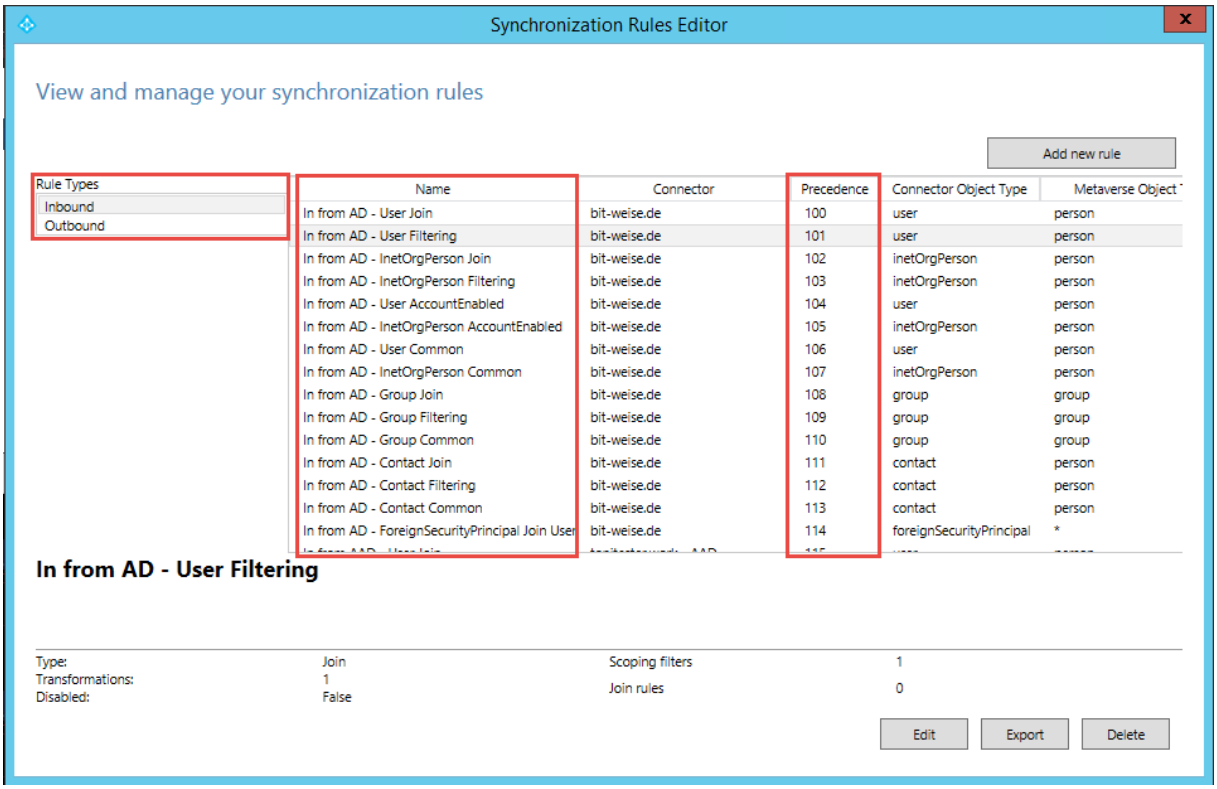


Abbildung 79 - Synchronization Rules Editor starten

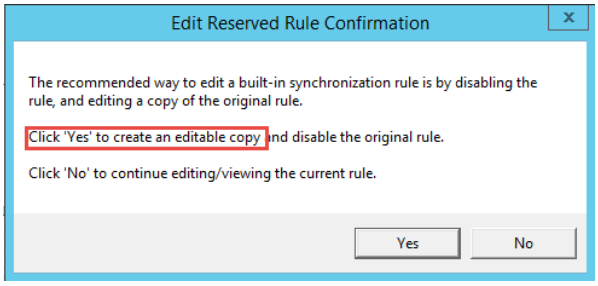
Im Synchronization-Rules Editor finden wir eine ganze Reihe von Standard-Regeln, die mit der Installation von AD-Connect automatisch angelegt wurden und die die Synchronisation normalerweise ohne Änderungen wunderbar durchführen. Es ist nur selten notwendig, selber Hand an die Synchronisationsregeln zu legen.

Die Synchronisations-Regeln existieren einmal als eingehende (inbound) und einmal als ausgehende (outbound) Regeln. Eingehend und Ausgehend bezieht sich dabei immer auf den Connector-Space. Eingehende Regeln synchronisieren also Objekte in den Connector-Space und die Metaverse, Ausgehende Regeln synchronisieren Objekte in dem Connector-Space und von dort einen Verzeichnisdienst.

Wenn man sich die Synchronisationsregeln in der Liste ansieht, so fällt auf, dass Sie in der Reihenfolge der Precedence aufgelistet sind. Die Precedence gibt die Verarbeitungsreihenfolge der Synchronisationsregeln an und bestimmt damit auch automatisch, welche Regeln bei einem Konflikt Vorrang haben. Zu Konflikten kann es kommen, da in der Metaverse ja mehrere Objekte zusammengeführt werden, und es keinen Prozess gibt, der sicherstellt, dass zwischen zwei Verzeichnissen die Eigenschaften eine Benutzers und eines Kontakts immer gleich sind. Außerdem können mehrere Regeln sich auf das gleiche Objekt beziehen.



Wenn wir die erste Regel öffnen, indem wir auf Edit klicken, bekommen wir sofort eine Warnung, dass der empfohlene Weg ist, eine Regel niemals zu bearbeiten, sondern Sie zu kopieren und die Standardregel zu deaktivieren. Dieses Vorgehen sollten sie auf keinen Fall ignorieren, da die **Standardregeln bei einem Update neu erstellt** werden.

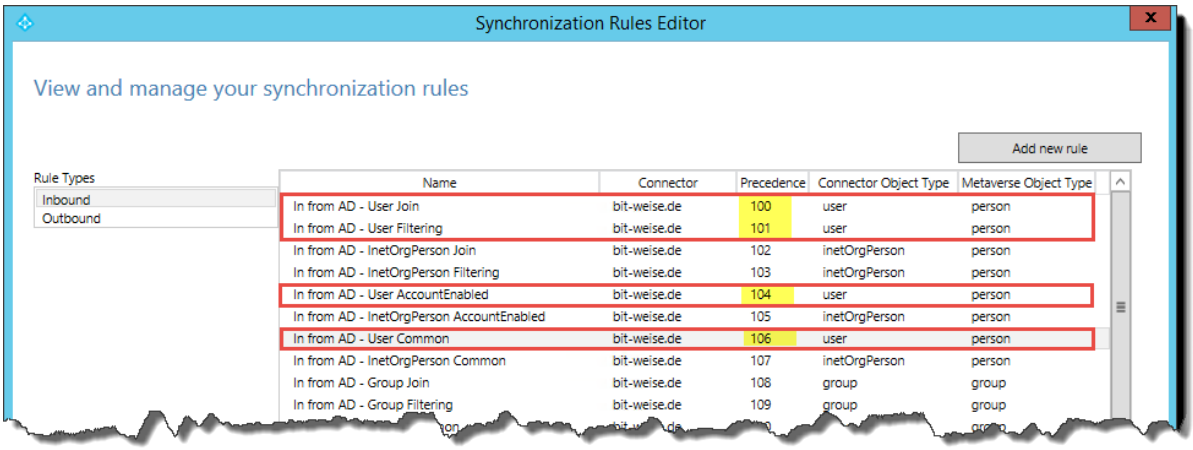


Wählen Sie also *yes*, um eine Kopie der Regel zu erstellen. Im Folgenden wird ein Fenster geöffnet, das alle Bestandteile einer Regel anzeigt. Eine Regel besteht dabei aus 4 Teilen:

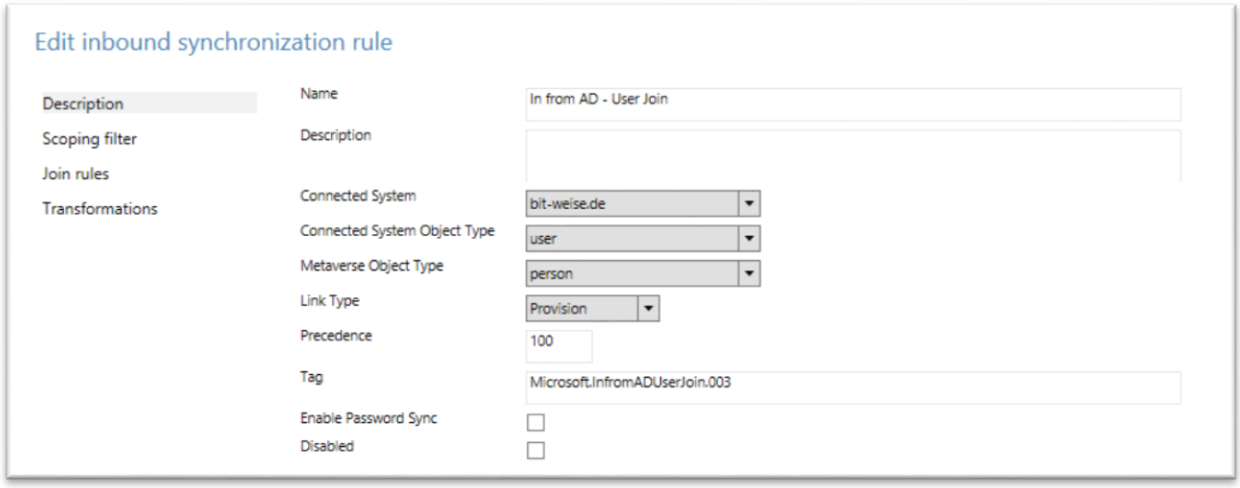
Description	Neben der Beschreibung ist hier auch festgelegt, auf welchem Connector die Regel aktiviert ist (*Connected System*), welcher Objekttyp von der Regel betroffen ist und auf welchen Objekttyp in der Metaverse dieses Objekte synchronisiert werden soll
Scoping filter	Der Scoping filter legt fest, welche Objekte synchronisiert werden sollen.
Join rules	Die Join-Rules definieren, über welche Attribute ein neues Objekt identifiziert (und dann angelegt) wird
Transformations	Hier wird der Attributs-Fluss definiert, also welche Attribute synchronisiert werden

Eine Regel muss einen Scoping-Filter haben, da sie sonst nicht angewendet wird. Eine Join-Rule ist allerdings nur notwendig, um ein neues Objekte anzulegen. Transformations wiederum können unabhängig von einer Join-Rule sein – tatsächlich haben wir die Join-Rule zum Anlegen und die

Transformations für den Attributs-Fluss in den Standard-Regeln immer getrennt. Schauen wir uns z.B. die Sychronisations-Regeln für Benutzer an, so finden wir 4 Regeln:



Die erste Regel „In from AD – User Join“ hat die höchste Priorität und wird zum Anlegen von neuen Benutzern angewendet. Der Link-Type ist auf Provision gesetzt – wenn die Regel zutrifft, wird das Objekte neu angelegt.



Die Filterregel bestimmt, dass die Regel nur dann zutrifft, wenn das Objekt das Attribut „isCriticalSytemObject“ nicht auf True gesetzt hat.

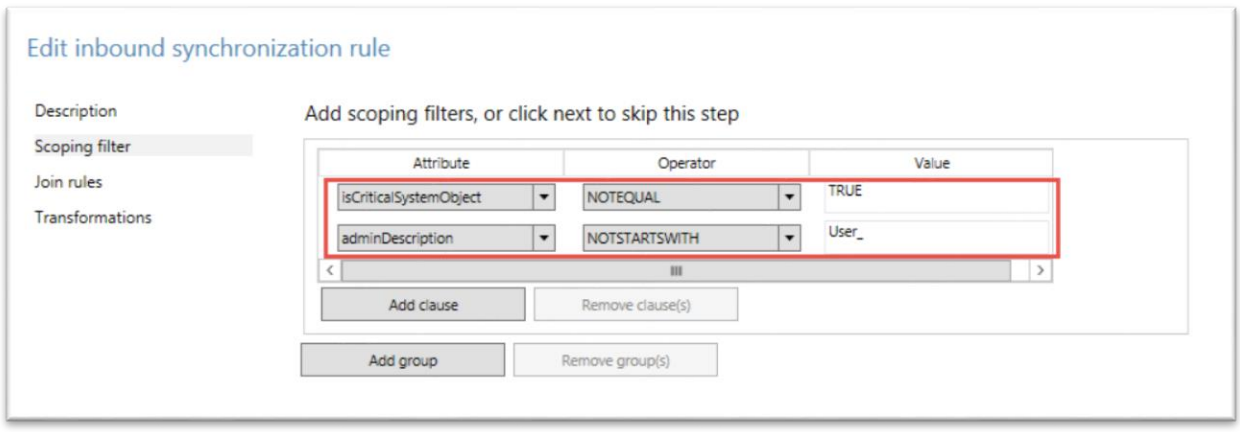


Abbildung 80 - Die Filterregel bestimmt, welche Objekte von der Regel verarbeitet werden

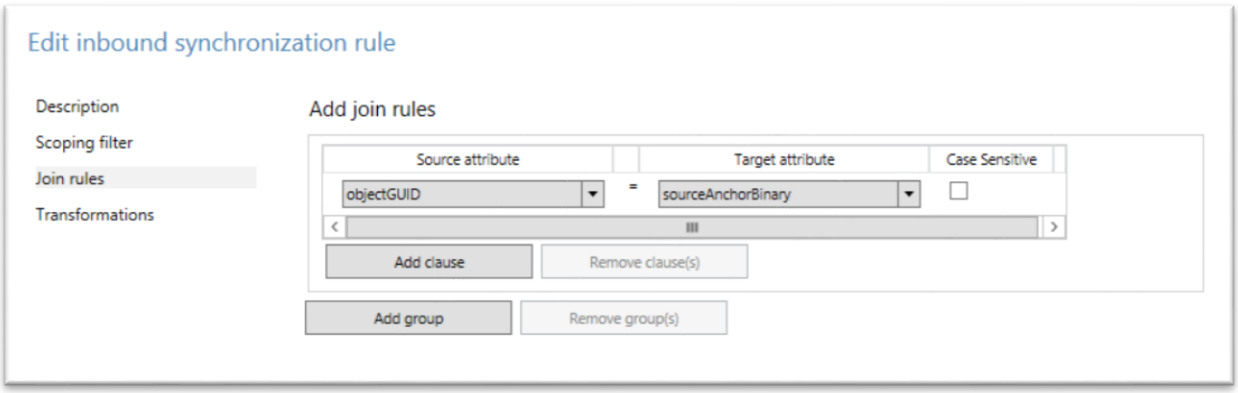
Mit der Join rule wird festgelegt, anhand welcher Attribute der Konnektor bestimmt, ob 2 Objekte im Connector Space und in der Metaverse identisch sind. Das Source attribute legt das Attribut fest, das in der Quelle zum Vergleich verwendet werden soll, das Target Attribut legt fest, mit welchem Attribut im Ziel verglichen werden soll, um die Identität zu bestimmen. Unsere Standardregel in der Abbildung vergleicht die objectGUID aus dem AD mit dem Attribut sourceAchorBinary. Diese Regel haben wir bei der Installation von AD Connect festgelegt. (siehe S. Wenn die Replikation innerhalb eines Forest stattfindet, ist das Identifizieren von Objekten über die ObjectGUID einfach möglich. 25).

Grundsätzlich können mehrere Attribute definiert werden, die alle zusammen gleich sein müssen (AND-Verknüpft), indem über *Add clause* mehrer Bedingungen hinzufügen. Es können auch mehrere Gruppen von Attributen evaluiert werden. Wenn mehrere Gruppen definiert sind, wertet der Konnektor die Bedingungen nacheinander aus. Gruppen sind OR-verknüpft, es muss also nur eine der Gruppen zutreffen, damit die Regel zwei Objekte als gleich identifiziert. Gruppen werden über den Button *Add* Group hinzugefügt.

Werden zwei Objekte als gleich identifiziert, führt der Konnektor sie anhand der Transformations-Regeln zusammen. Kann kein übereinstimmendes Objekt gefunden werden, greift der Connector auf den Link-Typ zurück, der unter Description festgelegt ist. Ist der Link-Typ Provision, wird das Objekt in der Metaverse neu angelegt – oder im Connector-Space, wenn es sich um eine ausgehende Regel handelt.

Wenn das Objekt angelegt wird, wird es automatisch mit dem Quellobjekt verknüpft und bei anschließenden Durchläufen des Konnektors nicht mehr überprüft – eine Join-Regel wird also nur einmal zum Erstellen des Objekts angewendet. Die Verknüpfung bleibt bis zur Löschung des Objekts bestehen. Daher ist es wichtig, dass sich die Eigenschaft, die auf den Source Anchor abgebildet wird, nicht ändert, da sonst die Verknüpfung verloren geht.

Für jedes Objekt darf es nur eine Join rule geben, da ansonsten ein Fehler generiert und das Objekt nicht angelegt wird. Die Standardregeln generieren daher für jeden Objekttyp nur eine Join Rule, die den Namen Join trägt.



Transformationen bestimmen, wie die Attribute aus der Quelle zum Ziel fließen sollen. Dafür kann für jedes Quellattribut eine eigene Transformation angegeben werden.

Eine Transformation kann aus einem von 3 Typen bestehen:

Constant	Constant definiert einen festen Wert. Es findet also im eigentlichen Sinne kein Attributsfluss statt, sondern es wird immer ein fester Wert gesetzt
Direct	Der Wert des Quellattributs wird in das Zielattribut geschrieben

Expression	Mit Hilfe von VBA-Ausdrücken kann ein Ausdruck festgelegt werden, über den quasi beliebige Werte in die Quelle geschrieben werden können

Eine ausführliche Beschreibung, wie Expressions erzeugt werden, gibt es in der AD Connect Dokumentation:

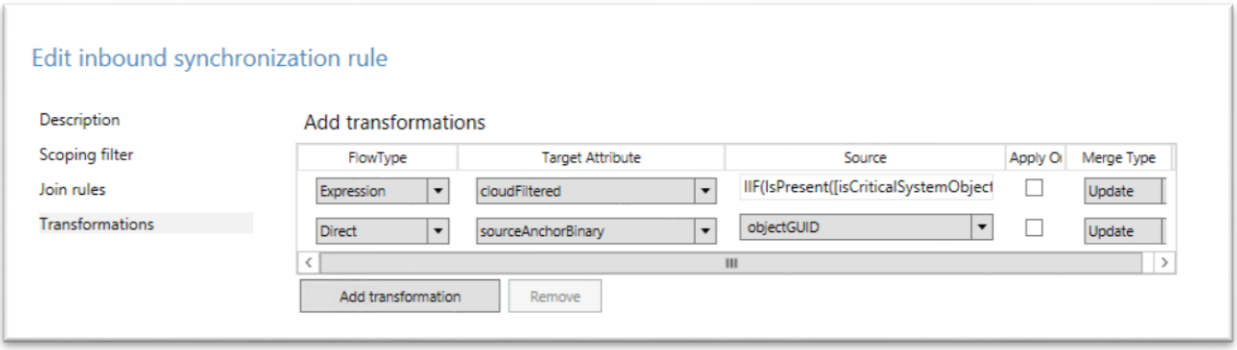
Azure AD Connect Sync: Understanding Declarative Provisioning Expressions
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-understanding-declarative-provisioning-expressions/

Azure AD Connect sync: Functions Reference
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-functions-reference/

Unsere Transformation kopiert lediglich 2 Attribute in das Objekt. Einmal wird das sourceAnchorBinary-Attribut mit der objectGUID befüllt, zum anderen wird das Attribut Cloudfiltered anhand eines Ausdrucks gesetzt.

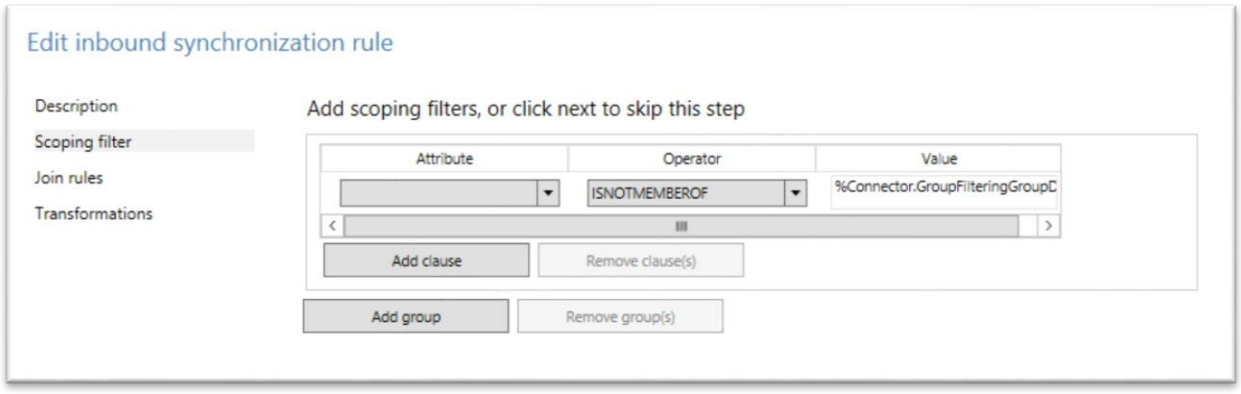
```
IIF(IsPresent([isCriticalSystemObject]) || IsPresent([sAMAccountName]) = False ||
[sAMAccountName] = "SUPPORT_388945a0" || Left([mailNickname], 14) =
"SystemMailbox{" || Left([sAMAccountName], 4) = "AAD_" || (Left([mailNickname], 4)
= "CAS_" && (InStr([mailNickname], "}") > 0)) || (Left([sAMAccountName], 4) =
"CAS_" && (InStr([sAMAccountName], "}") > 0)) || Left([sAMAccountName], 5) =
"MSOL_" ||
CBool(IIF(IsPresent([msExchRecipientTypeDetails]),BitAnd([msExchRecipientTypeDetail
s],&H21C07000) > 0,NULL)) || CBool(InStr(DNComponent(CRef([dn]),1),"\\0ACNF:")>0),
True, NULL)
```

Ohne auf die Details einzugehen, kann man hier schon grob erkennen, dass eine Liste von Bedingungen mit Hilfe eines IF abgefragt wird. || entspricht einem OR.

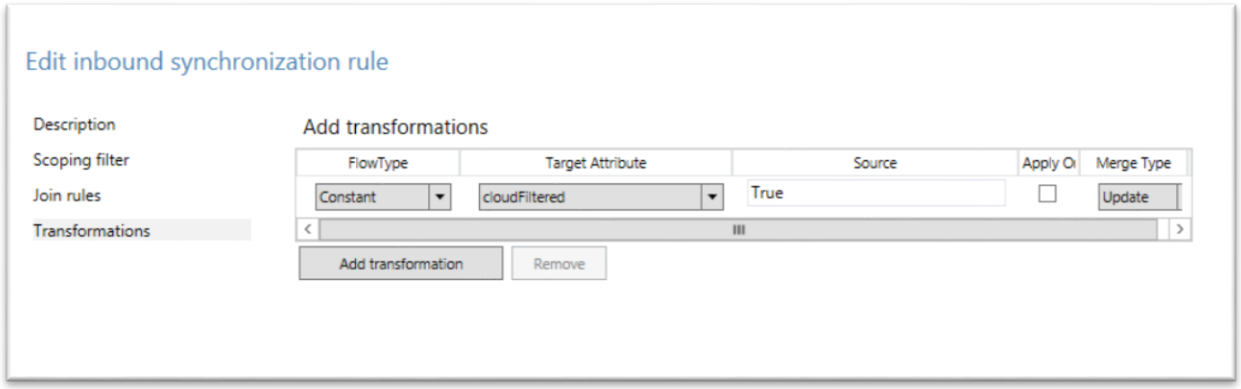


Damit haben wir eine Regel, die neue Objekte anlegt, aber nicht alle Attribute kopiert. Stattdessen werden noch 3 weitere Regeln abgearbeitet. Die nächste Regel ist die Regel „In from AD – User Filtering“.

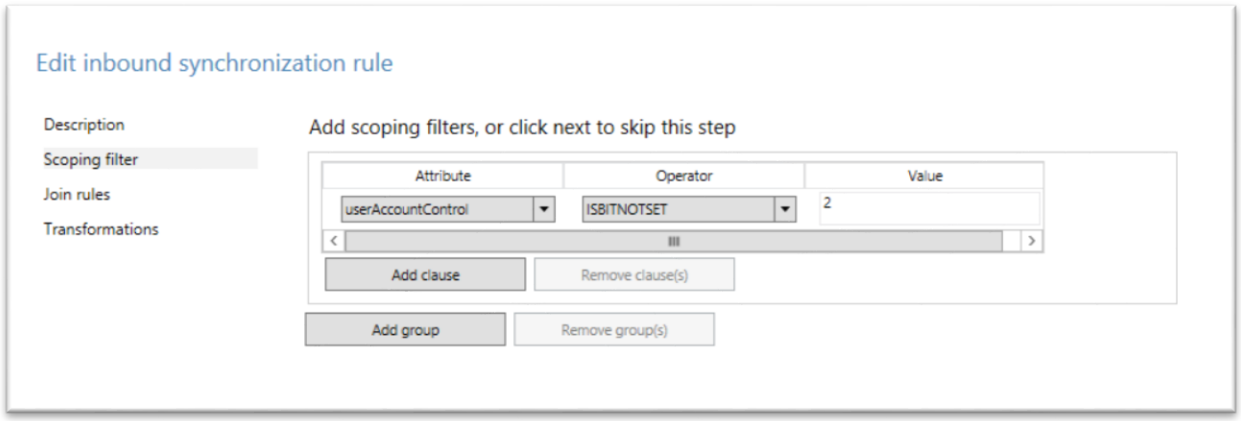
Ihr Scoping-Filter filtert auf eine Gruppenmitgliedschaft. Die Variable %Connector.GroupFilteringGroupDn% beinhaltet den Gruppennamen, der bei der Installation für die Gruppe definiert wurde, die als einzige synchronisiert werden soll. (siehe S. 36).



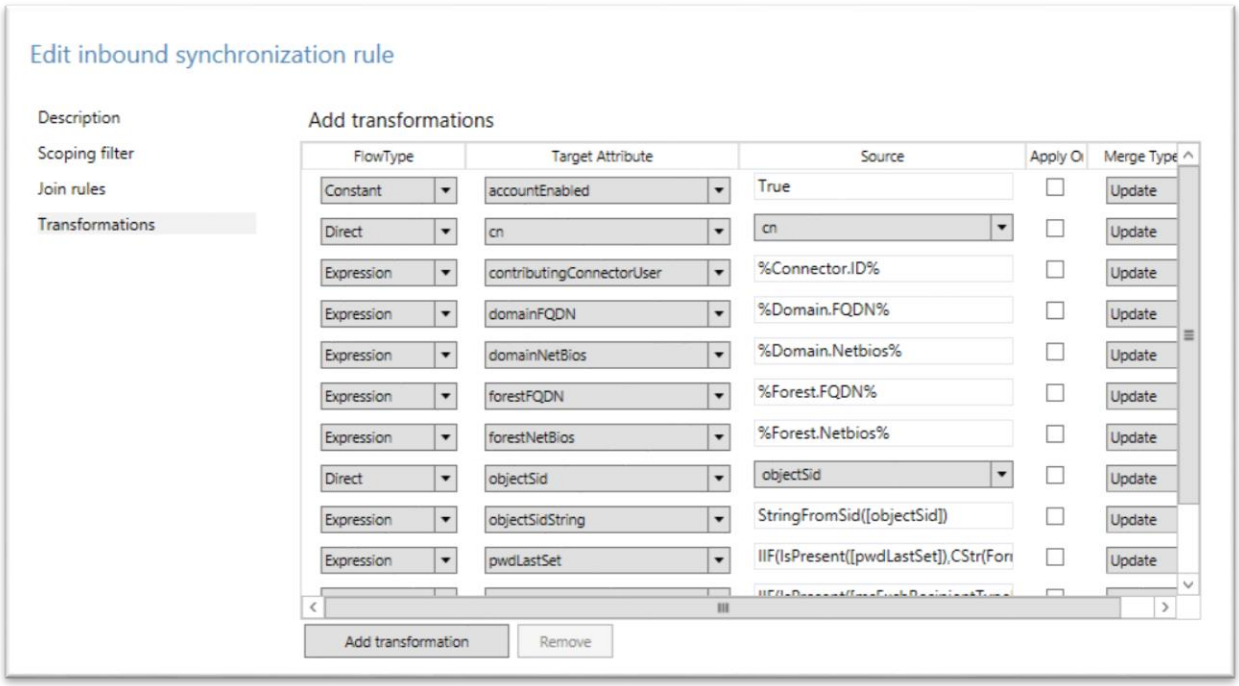
Diese Regel hat keine *Join rules* definiert. Sie regelt nur den Attribut-Fluss für verknüpfte Objekte. Es wird lediglich das Attribut cloudFiltered auf True gesetzt.



Die nächste Regel, die bearbeitet wird, ist die Regel *In from AD – User AccountEnabled*. Sie filtert auf alle Benutzer, deren Konten aktiviert sind. Die Eigenschaft userAccountControl ist ein Bitmuster. Ist das 2. Bit auf 1 gesetzt, ist der Account deaktiviert. Daher prüft der Operator auf „IsBitNotSet“, der Value gibt hier nicht den Wert an, der gesetzt sein soll, sondern gibt die Bitstelle an, die geprüft wird. Die Filterung auf aktivierte und nicht aktivierte Benutzer ist z.B. für Resourcendomänen und Exchange Resourcenkonten wichtig.



Auch hier ist die Join rule wieder nicht gesetzt. Dafür werden über diese Regel endlich die Attribute der Benutzer gesetzt.



Die letzte Regel filtert Benutzerinformationen aus dem globalen Adressbuch. Da ihre Precedence am niedrigsten ist, werden Informationen hier nur noch transformiert, wenn sie nicht bereits durch eine vorige Regel befüllt worden sind.

Eine ausführliche Beschreibung der Standard-Synchronisationsregeln finden Sie wieder in der Azure AD Doku:

Azure AD Connect sync: Understanding Users and Contacts
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-understanding-users-and-contacts/?cdn=disable

Azure AD Connect sync: Understanding the default configuration
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-understanding-default-configuration/

Notizen:

As a result of this, any objects in Azure AD that were previously synchronized but were then filtered are deleted in Azure AD.

When installing Azure AD Connect, prevent accidental deletes will be enabled by default and configured to not allow an export with more than 500 deletes

The default value of 500 objects can be changed with PowerShell using `Enable-ADSyncExportDeletionThreshold`.

The actual data flow of the **password synchronization** process is similar to the synchronization of user data such as DisplayName or Email Addresses. However, passwords are synchronized more frequently than the standard directory synchronization window for other attributes. The password synchronization process **runs every 2 minutes**. You cannot modify the frequency of this process. When you synchronize a password, it overwrites the existing cloud password. Password sync is only supported for the object type user in Active Directory. It is **not supported for the iNetOrgPerson** object type. A digest of the Active Directory password hash is used for the transmission between the on-premises AD and Azure Active Directory. The digest of the password hash cannot be used to access resources in your on-premises environment.

If a user is in the scope of password synchronization, the cloud account password is set to "*Never Expire*." You can continue to sign in to your cloud services using a synchronized password that has been expired in your on-premises environment. Your cloud password is updated the next time you change the password in the on-premises environment.

https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-implement-password-synchronization/#troubleshoot-password-synchronization

Die AD-Connect Synchronisation verwalten

AD-Connect unterscheidet zwischen der Kennwortsynchronisation und Objekt-/Attributsynchronisation und verwaltet dafür auch unterschiedliche Zeitplaner. Um den Zeitplaner für Objekt-und Attributssynchronisation, der seit ADSync 1.1.105.0 Bestandteil des Synchronisationsdienstes ist, zu konfigurieren, wird Powershell verwendet. Sollten die angegebenen Befehle nicht angezeigt werden, versuchen Sie, das ADSync-Modul manuell zu laden:

```
Import-Module -Name ADSync
```

Zum Anzeigen der Konfiguration verwenden Sie Get-ADSyncScheduler:

```
PS > Get-ADSyncScheduler

AllowedSyncCycleInterval            : 00:30:00
CurrentlyEffectiveSyncCycleInterval : 00:30:00
CustomizedSyncCycleInterval         :
NextSyncCyclePolicyType             : Delta
NextSyncCycleStartTimeInUTC         : 26.06.2016 21:24:09
PurgeRunHistoryInterval             : 7.00:00:00
SyncCycleEnabled                    : True
MaintenanceEnabled                  : True
StagingModeEnabled                  : False
```

AllowedSynCycleInterval	gibt das niedrigste von Microsoft unterstützten Synchronisierungs-Intervall an
CurrentlyEffectiveCycleInterval	gibt an, in welchen Zeitabständen eine Synchronisation gestartet wird
CustomizedSyncCycleInterval*	Wenn das Synchronisierungsintervall manuell gesetzt wurde, steht hier das manuelle Intervall
NextSyncCyclePolicyType*	Typ der nächsten Synchronisierung
NextSyncCycleStartTimeInUTC	Start des nächsten Synchronisierungszyklus
PurgeRunHistoryInterval*	Tage, die die Synchronisationslogs beibehalten werden. Die Logs können im Synchronisations-Manager eingesehen werden (siehe S. 43)
SyncCycleEnabled*	Wenn dieser Wert auf False gesetzt ist, führt der Scheduler keine Synchronisation aus, bis eine manuelle Synchronisation ausgeführt wurde.
MaintenanceEnabled*	Aktualisiert Zertifikate und löscht die Logs, wenn aktiviert
StagingModeEnabled	Zeigt an, ob das System sich im Staging-Mode befindet. Diese Konfiguration kann über den grafischen Assistenten umgestellt werden (siehe S. 39).

* Diese Werte können mit Set-ADSynchScheduler gesetzt werden.

Das AllowedSyncCyleInterval ist ein fester Wert. Er gibt den niedrigsten Wert an, den Microsoft für die Synchronisation unterstützt. Das ist per Default auch der aktiviert Wert, zu sehen unter CurrentlyEffectiveCycleInterval.

Um die Synchronisationseinstellungen zu konfigurieren, wird das Kommando Set-ADSyncScheduler verwendet. Er kann die Werte verändern, die in der Tabelle mit einem Stern versehen sind.

Um eine Synchronisation zu starten, verwenden Sie Start-ADSyncSyncCycle. Mit PolicyType könne Sie eine vollständige (initial) Synchronisierung auf allen Konnektoren oder eine Synchronisierung der Änderungen erzwingen (Delta)

```
Start-ADSyncSyncCycle -PolicyType Delta
```

Eine Beschreibung, wie Sie bei älteren Versionen von ADSync die Synchronisation steuern können, finden Sie im Windows 250 Hello Blog:

How To Run Manual DirSync / Azure Active Directory Sync Updates
https://blogs.technet.microsoft.com/rmilne/2014/10/01/how-to-run-manual-dirsync-azure-active-directory-sync-updates/

Um den laufenden Synchronisationsvorgang zu stoppen, müssen Sie sowohl die Powershell als auch die GUI bemühen.

Stoppen Sie die Replikation zuerst auf dem Scheduler mit

```
Stop-ADSyncSyncCyle
```

Anschließend müssen Sie den Connector noch manuell davon überzeugen, seinen Synchronisationsvorgang zu beenden.

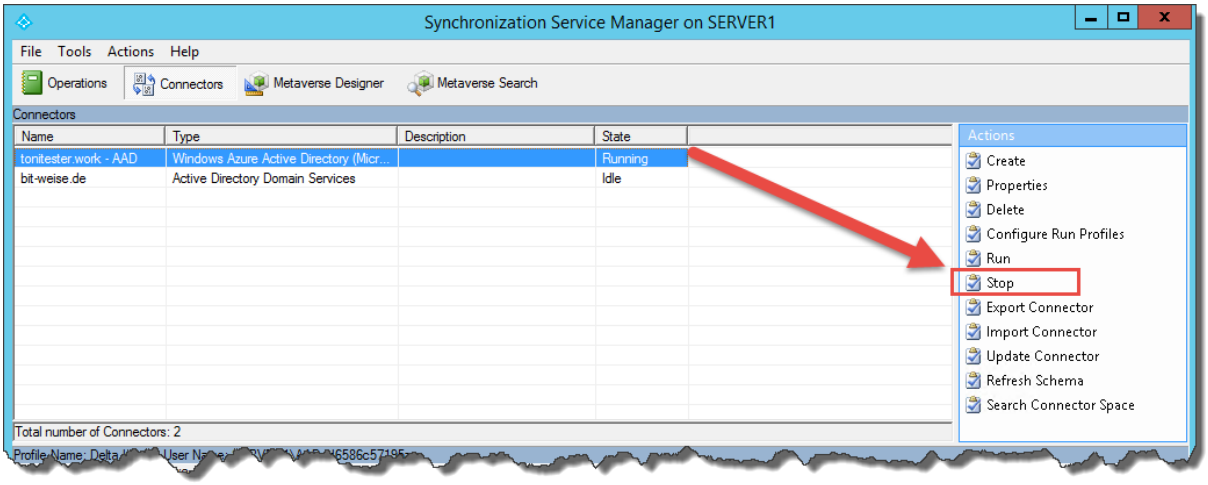


Abbildung 81 - Stoppen des laufenden Synchronisationsvorgangs

Die Synchronisation kann auch manuell ausgeführt werden. Verwenden Sie hierfür das Cmdlet Invoke-ADSyncRunprofile. Das Cmdlet benötigt als Eingabe den Connectornamen und das Runprofile. Diese können Sie sich über Powershell anzeigen lassen:

```
Get-ADSyncConnector | Select-Object Name
```

Um sich die Konnektoren anzeigen zu lassen, verwenden Sie

```
Get-ADSyncConnector | Select-Object -ExpandProperty Runprofiles
```

Starten Sie die Synchronisation über

```
Invoke-ADSyncRunProfile -ConnectorName <Name des Connectors> -RunProfile <Name des Profils>
```

Um den aktuellen Status der Konnektoren anzuzeigen, nutzen Sie

```
Get-ADSyncConnectorRunStatus
```

Mehr Informationen über die manuelle Steuerung der Synchronisation finden Sie unter:

Azure AD Connect sync: Scheduler
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-feature-scheduler/

Weiterführende Links in der Azure Dokumentation

Setting up a solid identity and access management foundation with Azure AD Sync
http://simon-may.com/setting-up-a-solid-identity-and-access-management-foundation

Azure AD Connect: Accounts and permissions
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-accounts-permissions/

Topologies for Azure AD Connect
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-topologies/

Azure AD Connect sync: Configure Filtering
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-configure-filtering

Azure AD Connect sync service features
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsyncservice-features/

Azure AD Connect: Enabling device writeback
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-feature-device-writeback/

Implementing password synchronization with Azure AD Connect sync
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-implement-password-synchronization/#trigger-a-full-sync-of-all-passwords

FILTERING OBJECTS FROM AZURE ACTIVE DIRECTORY
Eine gutes Beispiel zur Beschreibung einer Synchronisationsregel
http://www.lewisroberts.com/2015/09/06/filtering-objects-from-azure-active-directory

Referenzlisten

Azure AD Connect: Version Release History
Die verschiedenen Versionen von AD Connect und Ihre Änderungen
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-version-history/#111890

Azure AD Connect sync: Attributes synchronized to Azure Active Directory
Eine Auflistung der synchronisierten Attribute und für welche Dienste sie benötigt werden
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-attributes-synchronized/

Azure AD Connect sync: Functions Reference
Funktionsreferenz für VBA-Funktionen der Synchronisations-Regeln
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-functions-reference/

Documentation Articles for Azure Active Directory
Kalalogsuche über alle Dokumentationen
https://azure.microsoft.com/en-us/documentation/articles/?product=active-directory

Hybrid Identity Required Ports and Protocols
Auflistung der notwendigen Ports, aufgelistet nach Diensten
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-ports

Über den Autor

Holger Voges ist IT-Trainer und Consultant. Seine IT-Karriere begann mit einem Atari ST 512 Mitte der 80er Jahre. Seine ersten Erfahrungen mit großen Netzwerken hat er im Systembetrieb der Volkswagen Financial Services 1999 gewonnen. Ab dem Jahr 2000 war er dann als freiberuflicher IT-Trainer für verschiedene Schulungsunternehmen im Bereich Braunschweig und Hannover tätig, bis er 2002 mit 2 Mitstreitern sein erstes Schulungsunternehmen LayerDrei in Braunschweig gründete. Nach seinem Ausstieg bei LayerDrei war er dann mehrere Jahre als freiberuflicher Consultant vor allem im SQL-Server Umfeld u.a. für T-Home Entertain, e.on und Hewlett-Packard unterwegs. 2012 gründete er dann das Schulungsunternehmen Netz-Weise IT-Training.

Netz-Weise IT-Training hat sich auf Firmenschulungen im professionellen IT-Umfeld spezialisiert und bietet Schulungen u.a. im Bereich Microsoft, VMware, Linux und Oracle an.