

1 Objektfiltrierung bei der Active Directory-Synchronisierung

Das optionale *Verzeichnissynchronisierungstool* von Office 365 hat grundsätzlich die Aufgabe, im lokalen Active Directory vorhandene Benutzer-, Gruppen- und Kontakt-Objekte im Verzeichnisdienst eines Office 365-Kontos automatisiert zu verwalten, also beispielsweise anzulegen, zu deaktivieren, modifizieren, löschen etc. Der Konfigurationsassistent zur Einrichtung dieser Synchronisierung erlaubt dabei keine Auswahl, welche Objekte synchronisiert werden sollen und welche nicht. Es werden einfach grundsätzlich alle Objekte der drei beschriebenen Typen synchronisiert.

Mit der aktuellen Version des Verzeichnissynchronisierungstools können Sie nun nach verschiedenen Strategien bestimmte Objekte von der Synchronisierung ausschließen. Dies geht immer noch nicht mit dem Konfigurationsassistenten, aber mit dem Konfigurationswerkzeug des *Forefront Identity Manager 2010*, der sich um den Synchronisierungsvorgang kümmert.

Achtung: Es ist davon auszugehen, dass diese Konfigurationen ein Update auf eine neuere Version des Verzeichnissynchronisierungstools nicht überstehen. Sollten Sie einmal eine neuere Version des Tools installieren, sollten sie noch vor (!) dem nächsten Synchronisierungsvorgang überprüfen, ob die Filterkonfiguration Ihren Vorstellungen entspricht.

1.1 Konfiguration

In diesem Dokument werden drei unterschiedliche Verfahren zur Filter-Konfiguration für die Active Directory-Synchronisierung vorgestellt:

- Organisationseinheiten filtern
- Domänen filtern
- Eigenschaftsbasierte Filterung

1.1.1 Organisationseinheiten filtern

Ein einfaches Vorgehen beim Ausschluss von Objekten aus der Synchronisierung ist die Abwahl von Organisationseinheiten, die bei weiteren Synchronisationsläufen nicht mehr berücksichtigt werden sollen.

Achtung: Schließen Sie eine Organisationseinheit von der Synchronisierung aus, nachdem diese bereits früher einmal synchronisiert wurde, werden die darin enthaltenen Objekte aus dem Office 365-Verzeichnisdienst gelöscht. Das ist besonders bei Benutzerkonten problematisch. Wie Sie später noch lesen werden, ist eine Wiederherstellung der Benutzerkonten jedoch innerhalb von 30 Tagen möglich.

Zur Konfiguration, welche Organisationseinheiten bei der Synchronisierung berücksichtigt werden sollen, gehen Sie wie folgt vor:

1. Melden Sie sich an dem Server an, auf dem das Verzeichnissynchronisierungstool ausgeführt wird. Verwenden Sie dabei ein Benutzerkonto, das Mitglied der lokalen Sicherheitsgruppe MIISAdmins ist, beispielsweise der lokale Benutzer, den Sie bei der Konfiguration der Verzeichnissynchronisierung angegeben haben.
2. Führen Sie aus dem Pfad *Program Files\Microsoft Online Directory Sync\SYNCBUS\Synchronization Service\UIShell* (bzw. wenn Sie die 32-Bit-Version des Verzeichnissynchronisierungstools verwenden aus dem Pfad *Program Files\Microsoft Online Directory Sync\SYNCBUS\UIShell*) die Datei *miisclient.exe* aus. Dabei handelt es sich um die Verwaltungskonsole des Forefront Identity Managers (siehe Abbildung 1.1).

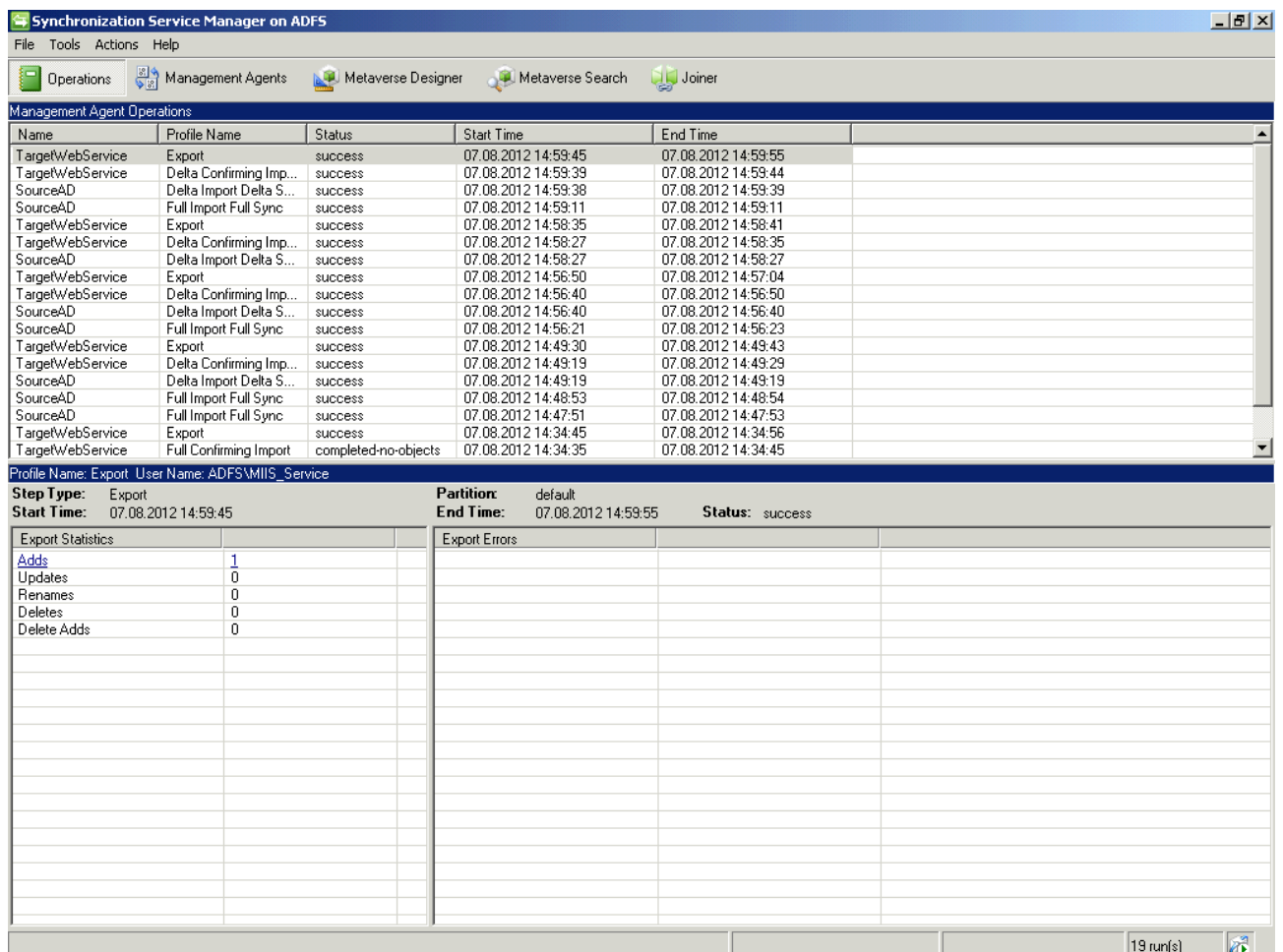


Abbildung 1.1: Verwaltungskonsole des Forefront Identity Managers

3. Wechseln Sie zum Bereich MANAGEMENT AGENTS.
4. Klicken Sie doppelt auf die Zeile SOURCEAD.
5. Wählen Sie den Bereich CONFIGURE DIRECTORY PARTITIONS und klicken dann auf die Schaltfläche CONTAINERS (siehe Abbildung 1.2).

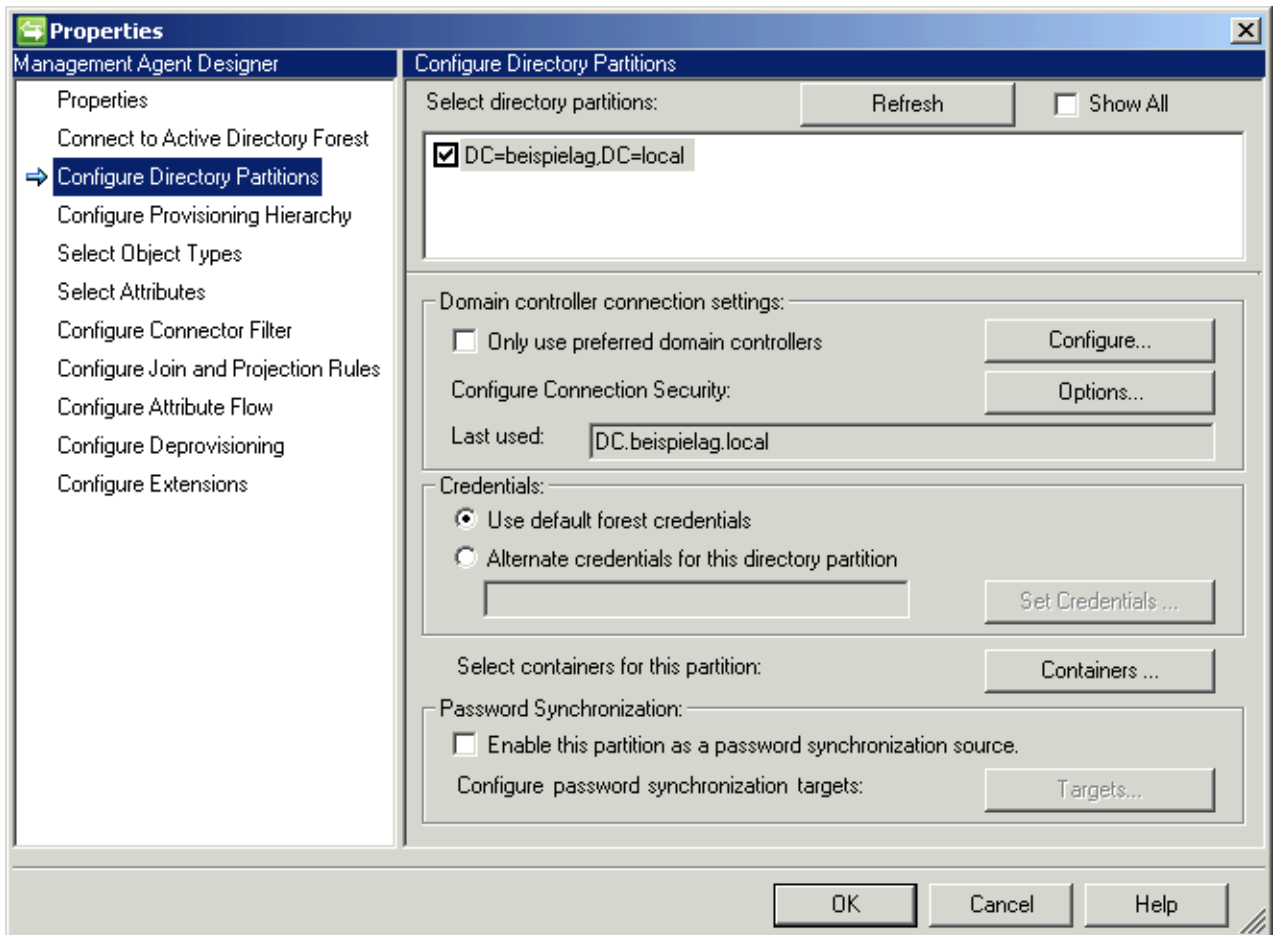


Abbildung 1.2: SourceAD-Eigenschaften

6. Geben sie die Benutzerdaten an, mit dem Sie sich am Server angemeldet haben.
7. Deaktivieren Sie alle Organisationseinheiten, deren Elemente während des Synchronisierungsvorgangs nicht berücksichtigt werden sollen (siehe Abbildung 1.3).

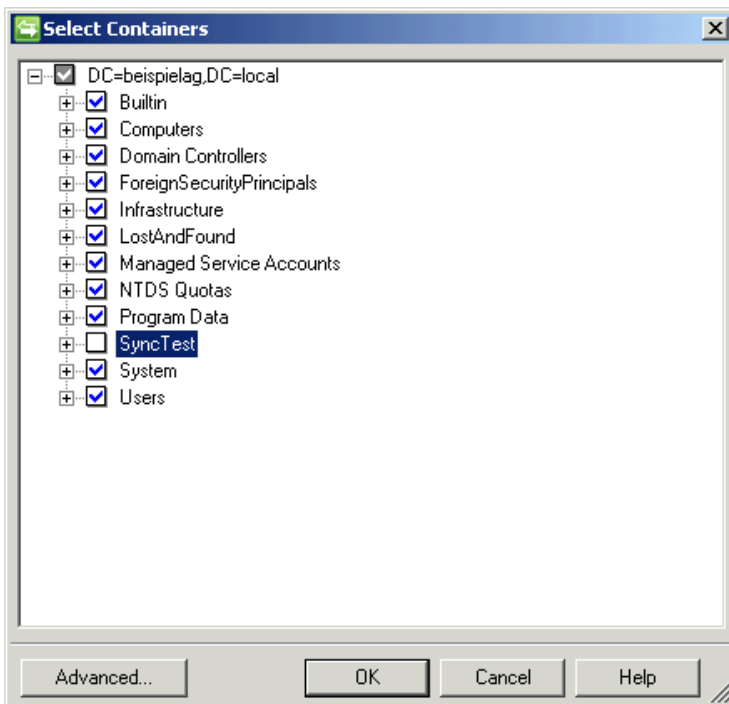


Abbildung 1.3: Container-Auswahl

8. Schließen Sie alle Fenster mit OK.
9. Öffnen Sie das Kontextmenü der Zeile SOURCEAD und wählen den Befehl RUN.
10. Markieren Sie das RUN PROFILE mit dem Namen FULL IMPORT FULL SYNC und klicken auf OK.
11. Warten Sie bis der STATE der Zeile SOURCEAD auf IDLE steht.

Die Änderungen werden dann beim nächsten Synchronisierungsintervall berücksichtigt. Möchten Sie direkt die Synchronisierung durchführen, gehen Sie wie folgt vor:

1. Öffnen Sie den Installationsordner des Verzeichnissynchronisierungstools (standardmäßig *C:\Program Files\Microsoft Office Directory Sync*).
2. Doppelklicken Sie das Skript *DirSyncConfigShell.psc1*.
3. Führen Sie folgendes Cmdlet aus, um die Synchronisierung zu starten:

`Start-OnlineCoexistenceSync`

Listing 1.1: Start der Verzeichnissynchronisierung

Nicht mehr synchronisierte Benutzerkonten

Benutzerkonten, die nun nicht mehr synchronisiert werden, markiert das Synchronisierungstool automatisch als gelöscht. Damit sind sie und die Daten, beispielsweise das Postfach, aber noch nicht endgültig verloren: In

der Benutzerverwaltung des Office 365-Portals finden Sie den Bereich GELÖSCHT (siehe Abbildung 1.4).

Benutzer

Aktiv | Gelöscht

Diese Benutzerkonten wurden deaktiviert. Die Konten und Daten sind nach Ablauf von 30 Tagen nach Löschung nicht mehr wiederherstellbar.

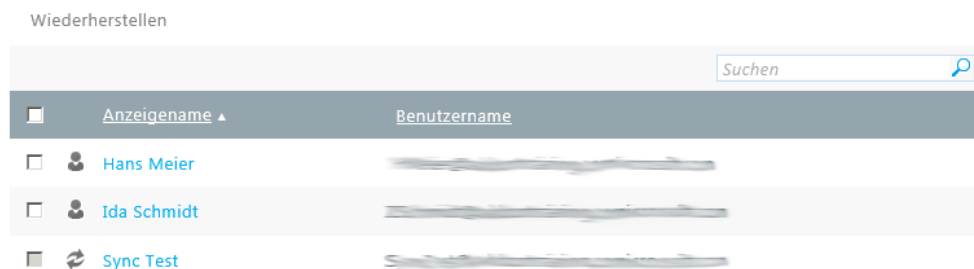


Abbildung 1.4: Gelöschte Benutzerkonten

Die URL zur Benutzerverwaltung lautet:

<https://portal.microsoftonline.com/UserManagement/UserManager.aspx>

In diesem Bereich aufgeführte Benutzerkonten können bis zum Ablauf von 30 Tagen wiederhergestellt werden. Allerdings können Sie Benutzer, die vom Verzeichnissynchronisierungstool angelegt und gelöscht wurden, hier nicht manuell wiederherstellen. In Abbildung 1.4 betrifft das beispielsweise den Benutzer mit dem Anzeigenamen SYNC TEST. Sie müssen die Filtereinstellungen so konfigurieren, dass der zu wiederherstellende Benutzer wieder synchronisiert wird. Nach dem nächsten Synchronisierungslauf ist er dann – samt seinem eventuell vorhandenen Postfach – wieder hergestellt.

1.1.2 Domänen filtern

Der Vorgang zur Auswahl der zu synchronisierenden Domänen ist sehr ähnlich wie bei der Auswahl von Organisationseinheiten. Wählen Sie lediglich in Abbildung 1.2 die gewünschten Domänen aus. Domänen, die dort nicht mit einem Häkchen markiert sind, werden auch nicht synchronisiert.

1.1.3 Eigenschaftsbasierte Filterung

Den Ausschluss von Objekten aus der Synchronisierung können Sie auch über eine eigenschaftsbasierte Filterung konfigurieren, um damit beispielsweise alle Benutzerkonten mit bestimmten Eigenschaften von der Synchronisierung auszuschließen. Gehen Sie dazu wie folgt vor:

1. Starten Sie wie in Abschnitt 1.1.1, „Organisationseinheiten filtern“ die Verwaltungskonsole des Forefront Identity Managers.

2. Wechseln Sie zum Bereich MANAGEMENT AGENTS.
3. Klicken Sie doppelt auf die Zeile SOURCEAD.
4. Wählen Sie den Bereich CONFIGURE CONNECTOR FILTER (siehe Abbildung 1.5).

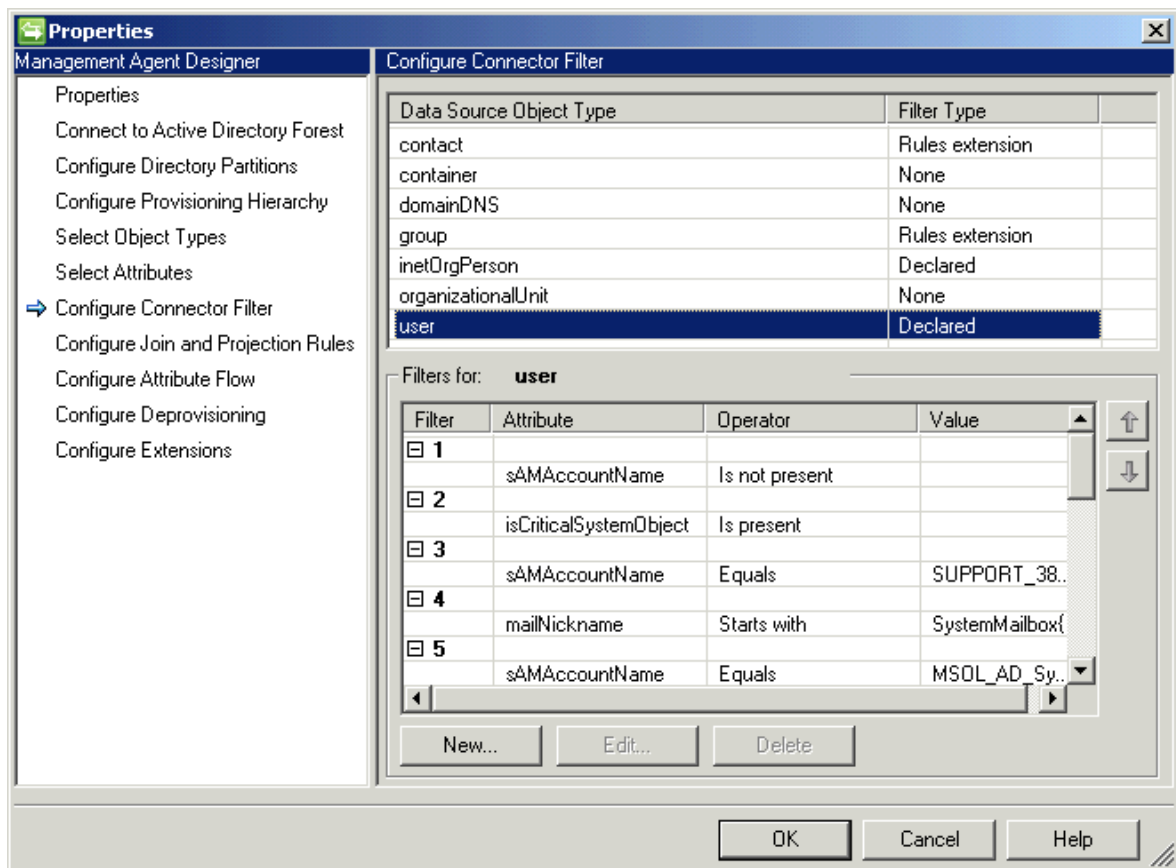


Abbildung 1.5: Filter-Eigenschaften

5. Markieren Sie in der Liste die Objektart, für Benutzerkonten beispielsweise USER.
6. Klicken Sie auf die Schaltfläche New, um einen Filter anzulegen. In Abbildung 1.6 werden beispielsweise alle Benutzerkonten nicht synchronisiert, die als Wohnort BERLIN eingetragen haben.

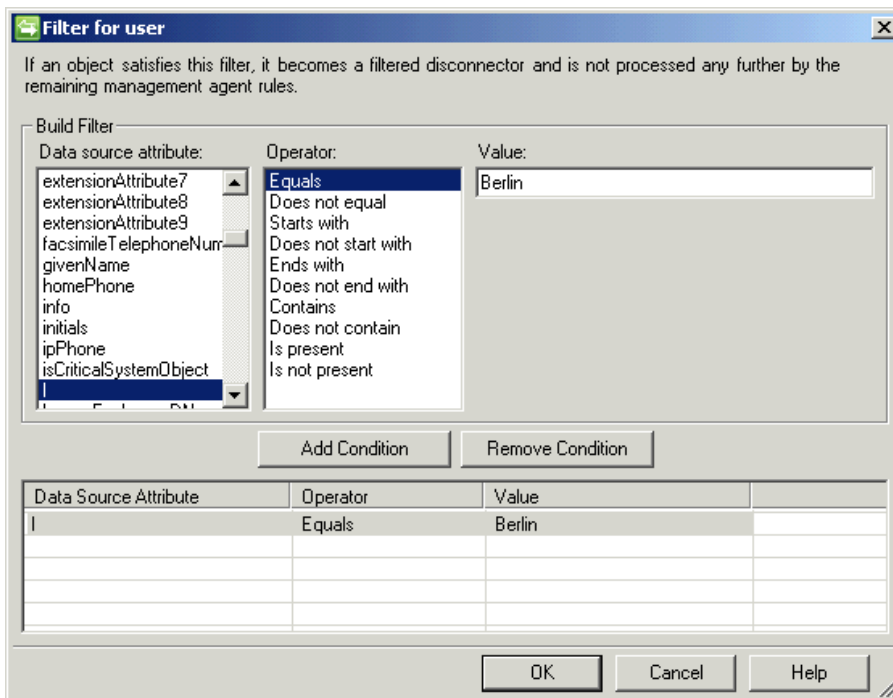


Abbildung 1.6: Anlegen eines neuen Filters

7. Schließen Sie alle Fenster mit OK.
8. Öffnen Sie das Kontextmenü der Zeile SOURCEAD und wählen den Befehl RUN.
9. Markieren Sie das RUN PROFILE mit dem Namen FULL IMPORT FULL SYNC und klicken auf OK.
10. Warten Sie bis der STATE der Zeile SOURCEAD auf IDLE steht.
11. Starten Sie gegebenenfalls wie in Abschnitt 1.1.1, „Organisationseinheiten filtern“ direkt einen Synchronisierungsvorgang mit Hilfe der PowerShell.

1.2 Weitere Informationen

Viele weitere Informationen und PowerShell-Beispiele zur Konfiguration Ihres Office 365-Kontos finden Sie in meinem Buch:

Microsoft Office 365

Administration, Konfiguration, Integration

Markus Widl

Galileo Computing

752 S., 2012, geb., mit Poster

49,90 Euro, ISBN 978-3-8362-1800-9

<http://office365buch.de>



Abbildung 1.7: Office 365-Buch