One Identity Manager 8.1.3

Administrationshandbuch für Active Roles Integration

Legende

WARNUNG: Das Symbol WARNUNG weist auf ein potenzielles Risiko von Körperverletzungen oder Sachschäden hin, für das Sicherheitsvorkehrungen nach Industriestandard empfohlen werden. Dieses Symbol ist oft verbunden mit elektrischen Gefahren bezüglich Hardware.

VORSICHT: Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.

One Identity Manager Administrationshandbuch für Active Roles Integration
Aktualisiert - Juni 2020
Version - 8.1.3

Inhalt

Integration mit Active Roles

Der One Identity Manager unterstützt die Anbindung von Active Directory-Umgebungen über einen integrierten Active Roles Konnektor. Zusätzliche Active Directory relevante Funktionalitäten, wie beispielsweise Microsoft Exchange, Office Communication Services oder Active Directory Lightweight Directory Service (AD LDS) werden über diesen Konnektor nicht unterstützt.

Der One Identity Manager ist in der Standardkonfiguration der Prozesse und des Synchronisationsverhaltens der Datenmaster und arbeitet ohne die Ansteuerung von Active Roles Arbeitsabläufen. Für das Standardverhalten wird ein administratives Benutzerkonto benötigt. Der integrierte Active Roles Konnektor erlaubt jedoch auch die Ansteuerung von Active Roles Arbeitsabläufen. Für diese Funktionalität müssen Sie gegebenenfalls die Prozesse im One Identity Manager benutzerdefiniert anpassen.

HINWEIS: Ausführliche Informationen zum Einsatz, Administration und Konfiguration eines Active Roles Servers entnehmen Sie Ihrer *One Identity Active Roles Dokumentation*.

HINWEIS: Dieses Handbuch geht nur auf die Besonderheiten bei der Verwendung des Active Roles Konnektors ein. Eine umfassende Dokumentation zur Verwaltung einer Active Directory-Umgebung mit dem One Identity Manager finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Active Directory-Umgebung*.

Architekturüberblick

Für die Verwaltung einer Active Directory-Umgebung mittels One Identity Manager und Active Roles spielen folgende Server eine Rolle:

- Active Roles Server

  Active Roles Server, der die Verbindung zum Active Directory Domänen-Controller herstellt. Der Synchronisationsserver verbindet sich gegen diesen Active Roles Server.

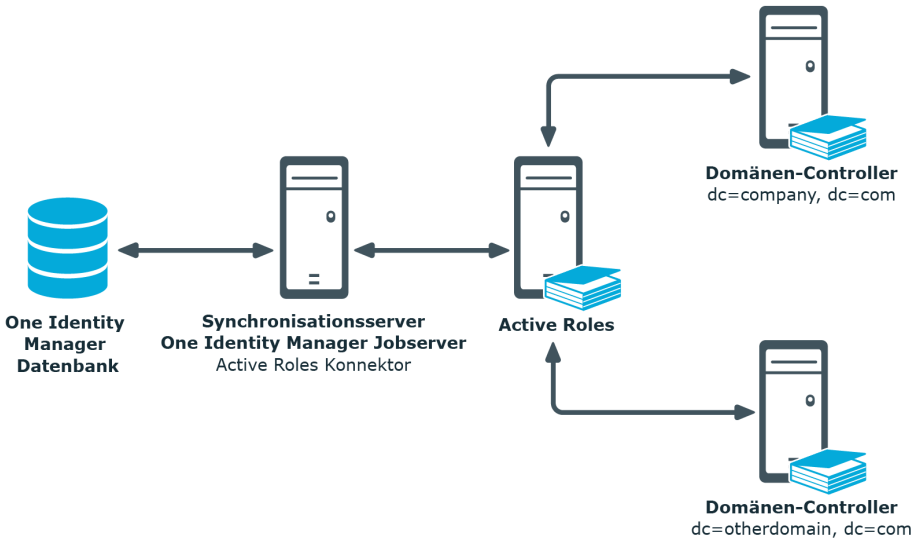
- Synchronisationsserver

  Vom Synchronisationsserver wird die Kommunikation des One Identity Manager Service mit Active Roles ausgeführt. Auf diesem Server ist der One Identity Manager Service mit dem Active Roles Konnektor installiert. Die für die Synchronisation und

Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet. Der Synchronisationsserver verbindet sich gegen den Active Roles Server.

Der Active Roles Konnektor des One Identity Manager verwendet das Active Roles ADSI Interface für die Kommunikation mit einer Active Roles Instanz. Der Active Roles Konnektor wird für die Synchronisation und Provisionierung der Active Directory-Umgebung eingesetzt. Der Active Roles Konnektor verbindet sich zu einer Active Roles Instanz, die dann die Verbindung zum Active Directory Domänen-Controller herstellt.

Abbildung 1: Architektur für die Synchronisation



Datenmigration zwischen One Identity Manager und Active Roles

Szenario

Eine mit Active Roles verwaltete Active Directory Domäne soll mit dem One Identity Manager verwaltet werden. Active Roles Self-Service Manager wird nicht eingesetzt.

Bei der Installation der One Identity Manager-Datenbank wählen Sie eine der folgenden Editionen:

- One Identity Manager Active Directory Edition
- One Identity Manager

Die initiale Synchronisation der Active Directory Domäne mit dem One Identity Manager muss mit dem Active Roles Konnektor erfolgen. Alle weiteren Synchronisationen erfolgen ebenfalls mit dem Active Roles Konnektor.

- Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt unter Verwendung der Standardprojektvorlage für Active Roles.

Szenario

Eine mit Active Roles verwaltete Active Directory Domäne soll mit dem One Identity Manager verwaltet werden. Active Roles Self-Service Manager wird eingesetzt. Die Funktionalität soll in den IT Shop des One Identity Manager überführt werden.

Bei der Installation der One Identity Manager-Datenbank wählen Sie eine der folgenden Editionen:

- One Identity Manager Active Directory Edition
- One Identity Manager

Mit der One Identity ManagerActive Directory Edition wird die Überführung der Funktionalität von Active Roles Self-Service Manager in den IT Shop des One Identity Manager direkt unterstützt. Wenn Sie die One Identity Manager Edition einsetzen, führen Sie vor der initialen Synchronisation zusätzlich folgende Schritte aus:

1. Aktivieren Sie im Designer den Konfigurationsparameter "QER\ITShop\GroupAutoPublish".
2. Aktivieren Sie im Designer den Konfigurationsparameter "QER\ITShop\GroupAutoPublish\ADSGroupExcludeList" und legen Sie die Active Directory Gruppen fest, die nicht automatisch in den IT Shop übernommen werden sollen.
3. Aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\ADS\ARS_SSM".
4. Kompilieren Sie die Datenbank.

Die Synchronisation der Active Directory Domäne mit dem One Identity Manager muss mit dem Active Roles Konnektor erfolgen. Alle weiteren Synchronisationen erfolgen ebenfalls mit dem Active Roles Konnektor.

- Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt unter Verwendung der Standardprojektvorlage für Active Roles.

Szenario

Eine mit dem One Identity Manager verwaltete Active Directory Domäne soll mit Active Roles verwaltet werden. Die Synchronisation der Active Directory Domäne erfolgt bisher mit dem Active Directory Konnektor.

Um die Active Directory Domäne mit One Identity Active Roles zu verwalten

1. Löschen Sie im Synchronization Editor das bestehende Synchronisationsprojekt.
2. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt unter Verwendung der Standardprojektvorlage für Active Roles.

Detaillierte Informationen zum Thema

- Einrichten der Synchronisation mit einer Active Directory-Umgebung über One Identity Active Roles auf Seite 9
- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 29

Einrichten der Synchronisation mit einer Active Directory-Umgebung über One Identity Active Roles

Der One Identity Manager unterstützt die Synchronisation mit Active Roles in den Versionen 6.9, 7.0, 7.2 und 7.3.1.

Um die Objekte einer Active Directory-Umgebung initial in die One Identity Manager-Datenbank einzulesen

1. Stellen Sie im Active Directory ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Die One Identity Manager Bestandteile für die Verwaltung von Active Directory-Umgebungen sind verfügbar, wenn der Konfigurationsparameter **TargetSystem | ADS** aktiviert ist.
    - Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.
    - Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.
3. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
4. Mit der One Identity Manager Active Directory Edition wird die Überführung der Funktionalität von Active Roles Self-Service Manager in den IT Shop des One Identity Manager direkt unterstützt. Wenn Sie die One Identity Manager Edition einsetzen, führen Sie vor der initialen Synchronisation zusätzlich folgende Schritte aus:
    a. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | GroupAutoPublish**.
    b. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | GroupAutoPublish | ADSGroupExcludeList** und legen Sie die Active Directory Gruppen fest, die nicht automatisch in den IT Shop übernommen werden sollen.

c. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | ADS | ARS_SSM**.

d. Kompilieren Sie die Datenbank.

5. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Detaillierte Informationen zum Thema

- Datenmigration zwischen One Identity Manager und Active Roles auf Seite 6
- Benötigte Rechte des One Identity Manager Service für die Synchronisation über Active Roles auf Seite 10
- Einrichten des Synchronisationsservers auf Seite 11
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Active Directory Domäne über Active Roles auf Seite 14
- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 29

Benötigte Rechte des One Identity Manager Service für die Synchronisation über Active Roles

Für die Verbindung zu einer Active Directory-Umgebung über Active Roles wird die Einrichtung eines eigenen Benutzerkontos für den One Identity Manager Service empfohlen. Zur Einrichtung verwenden Sie die Active Roles Zugriffsvorlagen. Über Zugriffsvorlagen delegieren Sie administrationsrelevanten Berechtigungen an ein Active Directory Benutzerkonto ohne jedoch diese Berechtigungen direkt im Active Directory zu erteilen. Weitere Informationen zu Active Roles Zugriffsvorlagen entnehmen Sie Ihrer One Identity Active Roles Dokumentation.

Folgende Zugriffsvorlagen werden für das Delegieren der Berechtigungen vorgeschlagen:

- All Objekts - Read All Properties
- All Objects - Full Control

Der One Identity Manager arbeitet ohne die Ansteuerung von Active Roles Arbeitsabläufen. Um eventuell vorhandene Active Roles Arbeitsabläufe zu umgehen, müssen Sie das Benutzerkonto in die Gruppe der Active Roles Administratoren aufnehmen. Diese Gruppe wird während der Installation des Active Roles erzeugt. Der Name der Gruppe ist in der Registrierungsdatenbank abgelegt unter:

- Registrierungsschüssel: HKEY_Local_Machine\Software\Aelita\Enterprise Directory Manager
- Wert: DSAdministrators

Verwandte Themen

- Interaktion mit Active Roles Arbeitsabläufen auf Seite 22

Einrichten des Synchronisationsservers

Für die Einrichtung der Synchronisation mit einer Active Directory-Umgebung muss ein Server zur Verfügung gestellt werden, auf dem die nachfolgend genannte Software installiert ist:

- Windows Betriebssystem

  Unterstützt werden die Versionen:

  - Windows Server 2008 R2 (nicht-Itanium 64-Bit) ab Service Pack 1
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
- Microsoft .NET Framework Version 4.7.2 oder höher

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.
- Windows Installer
- One Identity Active Roles Management Shell for Active Directory (x64)

  Auf 32-Bit Betriebssystemen ist das Active Roles Management Shell for Active Directory (x86) Paket zu verwenden.

  Die Anleitung zur Installation entnehmen Sie Ihrer One Identity Active Roles Dokumentation.
- One Identity Manager Service, Active Roles Konnektor

  - Installieren Sie die One Identity Manager Komponenten mit dem Installationsassistenten.

    1. Wählen Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen**.
    2. Wählen Sie die Maschinenrolle **Server | Jobserver | Active Directory**.

  HINWEIS: Für bestehende Active Roles Installationen:

  Der One Identity Manager Service kann auf einem Server mit Active Roles installiert werden.

Vom Synchronisationsserver werden alle Aktionen des One Identity Manager Service gegen die Zielsystemumgebung ausgeführt. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein.

Um den One Identity Manager Service zu installieren, nutzen Sie das Programm Server Installer. Das Programm führt folgende Schritte aus:

- Erstellen eines Jobservers.
- Festlegen der Maschinenrollen und Serverfunktionen für den Jobserver.
- Remote-Installation der One Identity Manager Service-Komponenten entsprechend der Maschinenrollen.
- Konfigurieren des One Identity Manager Service.
- Starten des One Identity Manager Service.

HINWEIS: Für die Generierung von Prozessen für die Jobserver werden der Provider, Verbindungsparameter und die Authentifizierungsdaten benötigt. Diese Informationen werden im Standardfall aus den Verbindungsdaten der Datenbank ermittelt. Arbeitet der Jobserver über einen Anwendungsserver müssen Sie zusätzliche Verbindungsinformationen im Designer konfigurieren. Ausführliche Informationen zum Einrichten des Jobservers finden Sie im *One Identity Manager Konfigurationshandbuch*.

HINWEIS: Das Programm führt eine Remote-Installation des One Identity Manager Service aus. Eine lokale Installation des Dienstes ist mit diesem Programm nicht möglich. Die Remote-Installation wird nur innerhalb einer Domäne oder in Domänen mit Vertrauensstellung unterstützt.

Für die Remote-Installation des One Identity Manager Service benötigen Sie eine administrative Arbeitsstation, auf der die One Identity Manager-Komponenten installiert sind. Ausführliche Informationen zur Installation einer Arbeitsstation finden Sie im *One Identity Manager Installationshandbuch*.

Um den One Identity Manager Service remote auf einem Server zu installieren und zu konfigurieren

1. Starten Sie das Programm Server Installer auf Ihrer administrativen Arbeitsstation.
2. Auf der Seite **Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.
3. Auf der Seite **Servereigenschaften** legen Sie fest, auf welchem Server der One Identity Manager Service installiert werden soll.
    a. Wählen Sie in der Auswahlliste **Server** einen Jobserver aus.

       - ODER -

       Um einen neuen Jobserver zur erstellen, klicken Sie **Hinzufügen**.
    b. Bearbeiten Sie folgende Informationen für den Jobserver.
        - **Server**: Bezeichnung des Jobservers.
        - **Queue**: Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue

angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.

- **Vollständiger Servername**: Vollständiger Servername gemäß DNS Syntax.

  Syntax:

  ```
  <Name des Servers>.<Vollqualifizierter Domänenname>
  ```

HINWEIS: Über die Option **Erweitert** können Sie weitere Eigenschaften für den Jobserver bearbeiten. Sie können die Eigenschaften auch zu einem späteren Zeitpunkt mit dem Designer bearbeiten.

4. Auf der Seite **Maschinenrollen** wählen Sie **Active Directory**.
5. Auf der Seite **Serverfunktionen** wählen Sie **Active Roles Konnektor**.
6. Auf der Seite **Dienstkonfiguration** erfassen Sie die Verbindungsinformationen und prüfen Sie die Konfiguration des One Identity Manager Service.

   HINWEIS: Die initiale Konfiguration des Dienstes ist bereits vordefiniert. Sollte eine erweiterte Konfiguration erforderlich sein, können Sie diese auch zu einem späteren Zeitpunkt mit dem Designer durchführen. Ausführliche Informationen zur Konfiguration des Dienstes finden Sie im *One Identity Manager Konfigurationshandbuch*.

   - Für eine direkte Verbindung zu Datenbank:
     a. Wählen Sie **Prozessabholung | sqlprovider**
     b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     c. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
   - Für eine Verbindung zum Anwendungsserver:
     a. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
     b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     c. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.
     d. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
     e. Wählen Sie das Authentifizierungsmodul. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
7. Zur Konfiguration der Remote-Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** wählen Sie das Verzeichnis mit den Installationsdateien.

10. Auf der Seite **Datenbankschlüsseldatei auswählen** wählen die Datei mit dem privaten Schlüssel.

    HINWEIS: Diese Seite wird nur angezeigt, wenn die Datenbank verschlüsselt ist.

11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
    - **Computer**: Name oder IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
    - **Dienstkonto**: Angaben zum Benutzerkonto des One Identity Manager Service.
      - Um den Dienst unter einem anderen Konto zu starten, deaktivieren Sie die Option **Lokales Systemkonto** und erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung.
    - **Installationskonto**: Angaben zum administrativen Benutzerkonto für die Installation des Dienstes.
      - Um das Benutzerkonto des angemeldeten Benutzers zu verwenden, aktivieren Sie die Option **Angemeldeter Benutzer**.
      - Um ein anderes Benutzerkonto zu verwenden, deaktivieren Sie die Option **Angemeldeter Benutzer** und geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.
    - Um das Installationsverzeichnis, den Namen, den Anzeigenamen oder die Beschreibung für den One Identity Manager Service zu ändern, nutzen Sie die weiteren Optionen.
12. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.

    Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.

13. Auf der letzten Seite des Server Installer klicken Sie **Fertig**.

    HINWEIS: In einer Standardinstallation wird der Dienst mit der Bezeichnung **One Identity Manager Service** in der Dienstverwaltung des Servers eingetragen.

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Active Directory Domäne über Active Roles

Verwenden Sie den Synchronization Editor, um die Synchronisation zwischen One Identity Manager-Datenbank und Active Directory-Umgebung einzurichten. Nachfolgend sind die Schritte für die initiale Einrichtung eines Synchronisationsprojektes beschrieben.

Nach der initialen Einrichtung können Sie innerhalb des Synchronisationsprojektes die Workflows anpassen und weitere Workflows konfigurieren. Nutzen Sie dazu den Workflow-

Assistenten im Synchronization Editor. Der Synchronization Editor bietet zusätzlich verschiedene Konfigurationsmöglichkeiten für ein Synchronisationsprojekt an.

Für die Einrichtung des Synchronisationsprojektes sollten Sie die folgenden Informationen bereit halten.

Tabelle 1: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Definierter Name der Domäne	Definierter LDAP Name der Domäne.
Benutzerkonto und Kennwort zur Anmeldung am Active Roles	Benutzerkonto und Kennwort zur Anmeldung am Active Roles. Stellen Sie ein Benutzerkonto mit ausreichend Berechtigungen bereit. Weitere Informationen finden Sie unter Benötigte Rechte des One Identity Manager Service für die Synchronisation über Active Roles auf Seite 10.
DNS Name oder IP Adresse des Active Roles Servers	Vollständiger Name oder IP Adresse des Active Roles Servers, gegen den sich der Synchronisationsserver verbindet. Beispiel: <Name des Servers>.<Vollqualifizierter Domänenname>
Synchronisationsserver für das Active Directory	Vom Synchronisationsserver werden alle Aktionen des One Identity Manager Service gegen die Zielsystemumgebung ausgeführt. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet. Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem Active Roles Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften. **Tabelle 2: Zusätzliche Eigenschaften für den Jobserver** Eigenschaft: Wert Serverfunktion: Active Roles Konnektor Maschinenrolle: Server/Jobserver/Active Directory Weitere Informationen finden Sie unter Einrichten des Synchronisationsservers auf Seite 11.

Angaben	Erläuterungen
Verbindungsdaten zur One Identity Manager-Datenbank	• Datenbankserver • Datenbank • SQL Server Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
Remoteverbindungsserver	Um die Synchronisation mit einem Zielsystem zu konfigurieren, muss der One Identity Manager Daten aus dem Zielsystem auslesen. Dabei kommuniziert der One Identity Manager direkt mit dem Zielsystem. Mitunter ist der direkte Zugriff von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, nicht möglich, beispielsweise aufgrund der Firewall-Konfiguration oder weil die Arbeitsstation nicht die notwendigen Hard- oder Softwarevoraussetzungen erfüllt. Wenn der direkte Zugriff von der Arbeitsstation nicht möglich ist, kann eine Remoteverbindung eingerichtet werden. Der Remoteverbindungsserver und die Arbeitsstation müssen in der selben Active Directory Domäne stehen. Konfiguration des Remoteverbindungsservers: • One Identity Manager Service ist gestartet • **RemoteConnectPlugin** ist installiert • Active Roles Konnektor ist installiert Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt. TIPP: Der Remoteverbindungsserver benötigt dieselbe Konfiguration (bezüglich der installierten Software sowie der Berechtigungen des Benutzerkontos) wie der Synchronisationsserver. Nutzen Sie den Synchronisationsserver gleichzeitig als Remoteverbindungsserver, indem Sie lediglich das `RemoteConnectPlugin` zusätzlich installieren. Ausführliche Informationen zum Herstellen einer Remoteverbindung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

HINWEIS: Der folgende Ablauf beschreibt die Einrichtung eines Synchronisationsprojekts, wenn der Synchronization Editor im Standardmodus

ausgeführt wird.

Wenn der Synchronization Editor im Expertenmodus ausgeführt wird, können zusätzliche Konfigurationseinstellungen vorgenommen werden. Folgen Sie in diesen Schritten den Anweisungen des Projektassistenten.

Um ein initiales Synchronisationsprojekt für eine Active Directory Domäne über Active Roles einzurichten

1. Starten Sie den Synchronization Editor und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie die Startseite. Klicken Sie **Mit einem neuen Synchronisationsprojekt beginnen**.

   Der Projektassistent wird gestartet.
3. Auf der Willkommensseite klicken Sie **Weiter**.
4. Auf der Seite **Zielsystem auswählen** wählen Sie **Active Roles Konnektor**.
5. Auf der Seite **Systemzugriff** legen Sie fest, wie der One Identity Manager auf das Zielsystem zugreifen kann.
   - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, möglich, nehmen Sie keine Einstellungen vor.
   - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, nicht möglich, können Sie eine Remoteverbindung herstellen.

     Aktivieren Sie die Option **Verbindung über einen Remoteverbindungsserver herstellen** und wählen Sie unter **Jobserver** den Server, über den die Verbindung hergestellt werden soll.
6. Auf der Seite **Zielserver** geben den Active Roles Server an, gegen den Sie sich verbinden möchten. Die möglichen Server werden, wenn möglich, automatisch ermittelt.
   - Wählen Sie unter **Hostname/IP Adresse** den Zielserver aus.
   - Kann der Server nicht automatisch ermittelt werden, tragen Sie unter **Hostname/IP Adresse** den DNS Namen oder die IP Adresse des Servers ein.
7. Auf der Seite **Anmeldeinformationen** geben Sie das Benutzerkonto und dass Kennwort für den Zugriff auf das Active Roles an.
8. Auf der Seite **Auswahl der Domäne/des Wurzeleintrages** wählen Sie die Domäne, die Sie synchronisieren möchten oder tragen Sie den definierten Namen des Wurzeleintrages ein.
9. Auf der Seite **One Identity Manager Verbindung** überprüfen Sie die Verbindungsdaten zur One Identity Manager-Datenbank. Die Daten werden aus der verbundenen Datenbank geladen. Geben Sie das Kennwort erneut ein.

   HINWEIS: Wenn Sie mit einer unverschlüsselten One Identity Manager-Datenbank arbeiten und noch kein Synchronisationsprojekt in der Datenbank gespeichert ist, erfassen Sie alle Verbindungsdaten neu. Wenn bereits ein Synchronisationsprojekt gespeichert ist, wird diese Seite nicht angezeigt.
10. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des

Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.

11. Auf der Seite **Zielsystemzugriff einschränken** legen Sie fest, wie der Systemzugriff erfolgen soll. Zur Auswahl stehen:

Tabelle 3: Zielsystemzugriff festlegen

Option	Bedeutung
Das Zielsystem soll nur eingelesen werden.	Angabe, ob nur ein Synchronisationsworkflow zum initialen Einlesen des Zielsystems in die One Identity Manager-Datenbank eingerichtet werden soll. Der Synchronisationsworkflow zeigt folgende Besonderheiten: • Die Synchronisationsrichtung ist **In den One Identity Manager**. • In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung **In den One Identity Manager** definiert.
Es sollen auch Änderungen im Zielsystem durchgeführt werden.	Angabe, ob zusätzlich zum Synchronisationsworkflow zum initialen Einlesen des Zielsystems ein Provisionierungsworkflow eingerichtet werden soll. Der Provisionierungsworkflow zeigt folgende Besonderheiten: • Die Synchronisationsrichtung ist **In das Zielsystem**. • In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung **In das Zielsystem** definiert. • Synchronisationsschritte werden nur für solche Schemaklassen erstellt, deren Schematypen schreibbar sind.

12. Auf der Seite **Synchronisationsserver** wählen Sie den Synchronisationsserver, der die Synchronisation ausführen soll.

    Wenn der Synchronisationsserver noch nicht als Jobserver in der One Identity Manager-Datenbank bekannt gegeben wurde, können Sie einen neuen Jobserver anlegen.

    a. Klicken Sie , um einen neuen Jobserver anzulegen.

    b. Erfassen Sie die Bezeichnung des Jobservers und den vollständigen Servernamen gemäß DNS-Syntax.

    c. Klicken Sie **OK**.

Der Synchronisationsserver wird als Jobserver für das Zielsystem in der One Identity Manager-Datenbank bekannt gegeben.

HINWEIS: Stellen Sie nach dem Speichern des Synchronisationsprojekts sicher, dass dieser Server als Synchronisationsserver eingerichtet ist.

13. Um den Projektassistenten zu beenden, klicken Sie **Fertig**.

    Es wird ein Standardzeitplan für regelmäßige Synchronisationen erstellt und zugeordnet. Aktivieren Sie den Zeitplan für die regelmäßige Synchronisation.

    Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

    HINWEIS:Beim Aktivieren wird eine Konsistenzprüfung durchgeführt. Wenn dabei Fehler auftreten, erscheint eine Meldung. Sie können entscheiden, ob das Synchronisationsprojekt dennoch aktiviert werden soll.

    Bevor Sie das Synchronisationsprojekt nutzen, prüfen Sie die Fehler. In der Ansicht **Allgemein** auf der Startseite des Synchronization Editor klicken Sie dafür **Projekt prüfen**.

    HINWEIS: Wenn das Synchronisationsprojekt nicht sofort aktiviert werden soll, deaktivieren Sie die Option **Synchronisationsprojekt speichern und sofort aktivieren**. In diesem Fall speichern Sie das Synchronisationsprojekt manuell vor dem Beenden des Synchronization Editor.

    HINWEIS: Die Verbindungsdaten zum Zielsystem werden in einem Variablenset gespeichert und können bei Bedarf im Synchronization Editor in der Kategorie **Konfiguration | Variablen** angepasst werden.

HINWEIS:

Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Personen erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für die Domäne bekannt, werden die Benutzerkonten mit den Personen verbunden. Es wird jedoch noch keine Kontendefinition zugewiesen. Die Benutzerkonten sind somit im Zustand **Linked** (verbunden).

Um die Benutzerkonten über Kontendefinitionen zu verwalten, weisen Sie diesen Benutzerkonten eine Kontendefinition und einen Automatisierungsgrad zu.

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie der Domäne die Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand **Linked** (verbunden) die Kontendefinition zu. Es wird der Standardautomatisierungsgrad der Kontendefinition für das Benutzerkonto übernommen.
    a. Wählen Sie im Manager die Kategorie **Active Directory | Benutzerkonten | Verbunden aber nicht konfiguriert | <Domäne>**.

       - ODER -

       Wählen Sie im Manager die Kategorie **Active Directory | Kontakte | Verbunden aber nicht konfiguriert | <Domäne>**.

b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.

c. Wählen Sie in der Auswahlliste **Kontendefinition** die Kontendefinition.

d. Wählen Sie die Benutzerkonten, die die Kontendefinition erhalten sollen.

e. Speichern Sie die Änderungen.

Verwandte Themen

- Einrichten des Synchronisationsservers auf Seite 11
- Benötigte Rechte des One Identity Manager Service für die Synchronisation über Active Roles auf Seite 10
- Standardprojektvorlage für Active Roles auf Seite 40

Beschleunigung der Provisionierung und Einzelobjektsynchronisation

Um Lastspitzen aufzufangen, kann die Verarbeitung der Prozesse zur Provisionierung und Einzelobjektsynchronisation auf mehrere Jobserver verteilt werden. Damit können die Provisionierung und Einzelobjektsynchronisation beschleunigt werden.

HINWEIS: Die Lastverteilung sollte nicht permanent für Provisionierungen oder Einzelobjektsynchronisationen eingesetzt werden. Durch die parallele Verarbeitung der Objekte kann es beispielsweise vorkommen, dass Abhängigkeiten nicht aufgelöst werden, da die referenzierten Objekte von einem anderen Jobserver noch nicht vollständig verarbeitet wurden.

Sobald die Lastverteilung nicht mehr benötigt wird, stellen Sie sicher, dass der Synchronisationsserver die Prozesse zur Provisionierung und Einzelobjektsynchronisation ausführt.

Um die Lastverteilung zu konfigurieren

1. Konfigurieren Sie die Server und geben Sie diese im One Identity Manager als Jobserver bekannt.
   - Weisen Sie diesen Jobservern die Serverfunktion **Active Roles Konnektor** zu.

   Alle Jobserver müssen auf die gleiche Active Directory Domäne zugreifen können, wie der Synchronisationsserver für das jeweilige Basisobjekt.
2. Weisen Sie im Synchronization Editor an das Basisobjekt eine kundendefinierte Serverfunktion zu.

   Über diese Serverfunktion werden alle Jobserver identifiziert, welche für die Lastverteilung genutzt werden sollen.

Wenn für das Basisobjekt noch keine kundendefinierte Serverfunktion vorhanden ist, erstellen Sie hier eine neue.

Ausführliche Informationen zur Bearbeitung von Basisobjekten finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

3. Weisen Sie diese Serverfunktion im Manager an alle Jobserver zu, welche die Prozesse zur Provisionierung und Einzelobjektsynchronisation für das Basisobjekt verarbeiten sollen.

   Wählen Sie nur die Jobserver, welche die gleiche Konfiguration wie der Synchronisationsserver des Basisobjekts haben.

   Ausführliche Informationen zur Bearbeitung von Servern finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Active Directory-Umgebung*.

Sobald alle Prozesse verarbeitet wurden, soll wieder der Synchronisationsserver die Provisionierung und Einzelobjektsynchronisation ausführen.

Um den Synchronisationsserver ohne Lastverteilung zu nutzen

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

Ausführliche Informationen zur Lastverteilung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

3

Interaktion mit Active Roles Arbeitsabläufen

In der Standardkonfiguration der Prozesse und des Synchronisationsverhaltens arbeitet der integrierte Active Roles Konnektor ohne die Ansteuerung von Active Roles Arbeitsabläufen. Änderungen werden sofort in die Active Directory-Umgebung publiziert. Für das Standardverhalten wird ein administratives Benutzerkonto benötigt, das Mitglied in der Gruppe der Active Roles Administratoren ist.

Der im One Identity Manager integrierte Active Roles Konnektor erlaubt jedoch auch die Ansteuerung von Active Roles Arbeitsabläufen. Das bedeutet, dass für jede Operation, in Active Roles die mit einem Arbeitsablauf verbunden ist, dieser Arbeitsablauf ausgelöst wird.

Wenn der Active Roles Konnektor Arbeitsabläufe auslösen soll, dann müssen Sie gegebenenfalls die Prozesse benutzerdefiniert so anpassen, dass die Prozesse auf die Ausführung der Arbeitsabläufe und somit die Ausführung der erwünschten Änderungen im Active Directory warten. Dies ist erforderlich, da die im One Identity Manager definierten Active Directory Prozesse synchron ausgeführt werden. Um Sie bei der Abfrage der möglichen Status der Arbeitsabläufe zu unterstützen, enthält der Active Roles Konnektor zusätzliche Funktionen.

Ob Arbeitsabläufe angesteuert werden, ist abhängig der Konfiguration der Domäne und den Berechtigungen des One Identity Manager Service Benutzerkontos.

> HINWEIS: Ist das Benutzerkonto des One Identity Manager Services Mitglied in der Gruppe der Active Roles Administratoren werden Arbeitsabläufe unabhängig von der Option immer umgangen.

Informationen zu Active Roles Arbeitsabläufen entnehmen Sie Ihrer One Identity Active Roles Dokumentation.

Die nachfolgende Tabelle zeigt die Zusammenhänge.

Tabelle 4: Zusammenhänge zur Ansteuerung von Active Roles Arbeitsabläufen

Das Benutzerkonto ist Mitglied der Active Roles Administratoren?	Die Option <Active Roles Arbeitsabläufe ausführen> ist gesetzt?	Die Operation ist mit Active Roles Arbeitsabläufen verbunden?	Ergebnis
Ja	Ja	Nein	Die Operation wird sofort ausgeführt.
Ja	Nein	Nein	Die Operation wird sofort ausgeführt.
Ja	Ja	Ja	Die Operation wird sofort ohne Ansteuerung der Arbeitsabläufe ausgeführt.
Ja	Nein	Ja	Die Operation wird sofort ohne Ansteuerung der Arbeitsabläufe ausgeführt.
Nein	Ja	Nein	Die Operation wird sofort ausgeführt.
Nein	Nein	Nein	Die Operation wird sofort ausgeführt.
Nein	Ja	Ja	Die Operation löst die Arbeitsabläufe aus und wird abhängig vom finalen Status ausgeführt.
Nein	Nein	Ja	Die Operation wird abgebrochen und eine Fehlermeldung ausgegeben.

Verwandte Themen

- Erweiterungen für die Verwendung von Active Roles Arbeitsabläufen auf Seite 24
- ID und Status einer Operation auf Seite 25
- Zusätzliche virtuelle Eigenschaften im Schema auf Seite 25
- Benötigte Rechte des One Identity Manager Service für die Synchronisation über Active Roles auf Seite 10

Erweiterungen für die Verwendung von Active Roles Arbeitsabläufen

HINWEIS: Die Einrichtung der Domänen in der One Identity Manager-Datenbank übernimmt der Synchronization Editor.

Um die Stammdaten einer Active Directory Domäne zu bearbeiten

1. Wählen Sie die Kategorie **Active Directory | Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Erfassen Sie auf dem Tabreiter **Active Roles** die folgenden Informationen für die Verwendung von Arbeitsabläufen.

   Tabelle 5: Erweiterte Eigenschaften für die Verwendung von Active Roles Arbeitsabläufen

Eigenschaft	Beschreibung
Active Roles Arbeitsabläufe ausführen	Angabe, ob Active Roles Arbeitsabläufe ausgeführt werden sollen. Informationen zu Active Roles Arbeitsabläufen entnehmen Sie Ihrer One Identity Active Roles Dokumentation. Ist diese Option gesetzt, erlaubt der integrierte Active Roles Konnektor die Ansteuerung von Active Roles Arbeitsabläufen. Gegebenenfalls müssen Sie die Prozesse im One Identity Manager benutzerdefiniert anpassen! Ist die Option nicht gesetzt, arbeitet der One Identity Manager ohne die Ansteuerung von Active Roles Arbeitsabläufen (Standardkonfiguration). Für das Standardverhalten wird ein administratives Benutzerkonto benötigt. HINWEIS: Ist das Benutzerkonto des One Identity Manager Service Mitglied in der Gruppe der Active Roles Administratoren werden Active Roles Arbeitsabläufe unabhängig von der Option immer umgangen.
Löschen von Benutzerkonten durch Active Roles Arbeitsabläufe	Angabe, ob Benutzerkonten über Deprovisionierungsabläufe im Active Roles gelöscht werden.
Löschen von Gruppen durch Active Roles Arbeitsabläufe	Angabe, ob Gruppen über Deprovisionierungsabläufe im Active Roles gelöscht werden.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Benötigte Rechte des One Identity Manager Service für die Synchronisation über Active Roles auf Seite 10
- Interaktion mit Active Roles Arbeitsabläufen auf Seite 22
- Deprovisionieren von Active Directory Benutzerkonten und Active Directory Gruppen auf Seite 33

ID und Status einer Operation

Bei jeder Änderungsoperation im Active Directory wird die vom Active Roles Konnektor übermittelte ID an den Ausgabeparameter "LastOperationID" zurückgegeben. Der vom Active Roles übermittelte Status der Operation wird an den Ausgabeparameter "LastOperationStatus" zurückgegeben. Wird kein Arbeitsablauf ausgelöst, dann wird bei erfolgreicher Ausführung der Operation der Status "Completed" zurückgegeben. Wird ein Arbeitsablauf ausgelöst, dann wird der Status "Pending" zurückgeliefert. Diese Ausgabeparameter können Sie in den Folgeprozessen verwenden, um auf die Ausführung der Arbeitsabläufe zu warten.

Zusätzliche virtuelle Eigenschaften im Schema

Für die Abfrage der aktuellen Status von Arbeitsabläufen enthält das Schema des Active Roles Konnektors zusätzliche virtuelle Eigenschaften.

> HINWEIS: Die virtuellen Eigenschaften erfordern keine Erweiterung des Active Directory Schemas. Active Roles verhält sich so, als ob diese Eigenschaften wirklich existieren würden.

Diese virtuellen Eigenschaften sind "nur lesend" definiert und an jedem Objekt vorhanden, werden jedoch in der Standardprojektvorlage nicht gemappt. Um diese Funktionalität zu nutzen, müssen Sie das Mapping kundenspezifisch anpassen.

Beim Lesen der Eigenschaften führt der Active Roles Konnektor einen "OperationSearchRequest"-Aufruf zum Active Roles aus. Um die Performance so wenig wie möglich zu beeinträchtigen, wird das Ergebnis gleicher Anfragen für 30 Sekunden im Cache gehalten.

Tabelle 6: Virtuelle Eigenschaften des Active Roles Konnektors

Eigenschaft	Beschreibung
vrtLastOperationID	ID der letzten Operation im Active Roles.

Eigenschaft	Beschreibung
vrtLastOperationStatus	Status der letzten Operation im Active Roles. Mögliche Status sind "Unknown", "Pending", "Completed", "Rejected", "Failed" und"Canceled".

Weitere Informationen entnehmen Sie Ihrer One Identity Active Roles Dokumentation.

4

Interaktion mit Active Roles Richtlinien

Bei der Definition von Bildungsregeln im One Identity Manager sollten Sie die im Active Roles definierte Richtlinien beachten. Werte, die der One Identity Manager generiert, werden ohne Prüfung auf Einhaltung der Active Roles Richtlinien an den Active Roles Konnektor übergeben. Verstoßen die übergebenen Werte gegen die Active Roles Richtlinien, wird der gesamte Prozess fehlschlagen. Um dies zu vermeiden, sollten Sie die One Identity Manager Bildungsregeln an die Active Roles anpassen.

Informationen zu Active Roles Richtlinien entnehmen Sie Ihrer One Identity Active Roles Dokumentation.

5

Verwalten der Active Directory Objekte

Im One Identity Manager können Sie organisatorische Einheiten in einer hierarchischen Containerstruktur einrichten. Organisatorische Einheiten (Geschäftsstellen oder Abteilungen) werden dazu genutzt, Objekte des Active Directory wie Benutzerkonten und Gruppen logisch zu organisieren und somit die Verwaltung der Objekte zu erleichtern.

HINWEIS: Nachfolgend wird auf Besonderheiten bei der Verwaltung von Active Directory Objekten über Active Roles eingegangen. Eine umfassende Dokumentation zur Verwaltung einer Active Directory-Umgebung mit dem One Identity Manager finden Sie im One Identity Manager Administrationshandbuch für die Anbindung einer Active Directory-Umgebung.

Detaillierte Informationen zum Thema

Active Directory Gruppen automatisch in den IT Shop aufnehmen

Tabelle 7: Konfigurationsparameter für die automatische Aufnahme von Gruppen in den IT Shop

Konfigurationsparameter	Beschreibung
QER | ITShop | GroupAutoPublish	Präprozessorrelevanter Konfigurationsparameter zur automatischen Übernahme von Gruppen in den IT Shop. Der Konfigurationsparameter legt fest, ob alle Gruppen der Zielsysteme Active Directory und SharePoint automatisch in den IT Shop übernommen werden. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.
QER | ITShop | GroupAutoPublish | ADSGroupExcludeList	Der Konfigurationsparameter enthält eine Auflistung aller Active Directory Gruppen, für die keine automatische Zuordnung zum IT Shop erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird. Beispiel: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS`
TargetSystem | ADS | ARS_SSM	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Überführung der Funktionalität von Active Roles Self-Service Manager in den One Identity ManagerIT Shop. Ist der Parameter aktiviert, sind die Bestandteile verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.

Mit der One Identity ManagerActive Directory Edition wird die Überführung der Funktionalität von Active Roles Self-Service Manager in den IT Shop des One Identity Manager direkt unterstützt. Wenn Sie die One Identity Manager Edition einsetzen, führen Sie vor der initialen Synchronisation zusätzlich folgende Schritte aus:

Um Gruppen automatisch in den IT Shop aufzunehmen

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER \| ITShop \| GroupAutoPublish**.
2. Aktivieren Sie im Designer den Konfigurationsparameter **QER \| ITShop \| GroupAutoPublish \| ADSGroupExcludeList** und legen Sie die Active Directory Gruppen fest, die nicht automatisch in den IT Shop übernommen werden sollen.
3. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem \| ADS \| ARS_SSM**.
4. Kompilieren Sie die Datenbank.

Die Gruppen werden ab diesem Zeitpunkt automatisch in den IT Shop aufgenommen.

- Die Synchronisation sorgt dafür, dass die Gruppen in den IT Shop aufgenommen werden. Bei Bedarf können Sie die Synchronisation im Synchronization Editor sofort starten.
- Gruppen, die im One Identity Manager neu erstellt werden, werden in den IT Shop aufgenommen.

Folgende Schritte werden bei der Aufnahme einer Gruppe in den IT Shop automatisch ausgeführt.

1. Es wird eine Leistungsposition für die Gruppe ermittelt.

   Für jede Gruppe wird die Leistungsposition geprüft und bei Bedarf angepasst. Die Bezeichnung der Leistungsposition entspricht der Gruppenbezeichnung. Die Leistungsposition wird einer der Standard-Servicekategorien zugeordnet.

   - Für Gruppen mit Leistungsposition wird die Leistungsposition angepasst.
   - Gruppen ohne Leitungsposition erhalten eine neue Leistungsposition.
   - Die Leistungsposition wird abhängig davon, ob die Gruppe im Active Roles Self-Service Manager veröffentlicht ist, aktiviert oder deaktiviert.

2. Es wird eine Anwendungsrolle für Produkteigner ermittelt und der Leistungsposition zugeordnet. Die Produkteigner können Bestellungen von Mitgliedschaften in diesen Gruppen genehmigen. Standardmäßig wird der Kontomanager einer Gruppe als Produkteigner ermittelt.

   HINWEIS: Die Anwendungsrolle für Produkteigner muss der Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner** untergeordnet sein.

   - Ist der Kontomanager der Gruppe bereits Mitglied einer Anwendungsrolle für Produkteigner, dann wird diese Anwendungsrolle der Leistungsposition zugewiesen. Alle Mitglieder dieser Anwendungsrolle werden dadurch Produkteigner der Gruppe.
   - Ist der Kontomanager der Gruppe noch kein Mitglied einer Anwendungsrolle für Produkteigner, dann wird eine neue Anwendungsrolle erzeugt. Die Bezeichnung der Anwendungsrolle entspricht der Bezeichnung des Kontomanagers.
     - Handelt es sich beim Kontomanager um ein Benutzerkonto oder einen Kontakt, wird die Person des Benutzerkontos oder des Kontaktes in die Anwendungsrolle aufgenommen.
     - Handelt es sich um eine Gruppe von Kontomanagern, werden die Personen aller Benutzerkonten dieser Gruppe in die Anwendungsrolle aufgenommen.
   - Besitzt die Gruppe keine Kontomanager wird die Standard-Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner | Ohne Eigentümer im AD** verwendet.

3. Die Gruppe wird mit der Option **IT Shop** gekennzeichnet und dem IT Shop Regal **Active Directory Gruppen** im Shop **Identity & Access Lifecycle** zugewiesen.

Anschließend können die Kunden des Shops Gruppenmitgliedschaften über das Web Portal bestellen.

HINWEIS: Wenn eine Gruppe endgültig aus der One Identity Manager-Datenbank gelöscht wird, wird auch die zugehörige Leistungsposition gelöscht.

Verwandte Themen

- Bestellen neuer Active Directory Gruppen über das Web Portal auf Seite 31
- Active Roles spezifische Erweiterungen für Active Directory Gruppen auf Seite 32
- One Identity Manager Administrationshandbuch für IT Shop

Bestellen neuer Active Directory Gruppen über das Web Portal

HINWEIS: Bei der Bestellung der Gruppenmitgliedschaft wird in der Standardinstallation der Entscheidungsworkflow "Entscheidung der Bestellungen von Mitgliedschaften in Active Directory Gruppen" wirksam.

Um eine neue Active Directory Gruppe zu bestellen

- Wählen Sie im Web Portal im Menü **Servicekatalog| Bestellung** die Servicekategorie "Active Directory Gruppen".
- Bestellen Sie die Active Directory Gruppe über die Produkte "Anlegen einer Active Directory Verteilerliste" oder "Anlegen einer Active Directory Sicherheitsgruppe".

Bei der Bestellung einer neuen Active Directory Gruppe werden automatisch die folgenden Schritte ausgeführt:

- Es wird ein Eintrag für die Active Directory Gruppe im One Identity Manager erzeugt.
- Die Active Directory Gruppe wird mit der Option **Gruppe ist im Self-Service Manager veröffentlicht** gekennzeichnet.
- Die Active Directory Gruppe wird mit der Option **IT Shop** gekennzeichnet.
- Es wird eine zugehörige Leistungsposition erzeugt. Es wird eine neue Anwendungsrolle erstellt, in welcher der Besteller Mitglied wird. Die Anwendungsrolle wird als Produkteigner der Leistungsposition eingetragen.

  Durch dieses Vorgehen ist der Besteller einer Active Directory Gruppe entscheidungsberechtigt bei der Bestellung von Mitgliedschaften in dieser Active Directory Gruppe.
- Die Active Directory Gruppe wird im Standardshop "Identity & Access Lifecycle" dem Regal "Active Directory Gruppen" zugewiesen.

Anschließend ist Mitgliedschaft in der Active Directory Gruppe für die Kunden des Shops über das Web Portal bestellbar.

HINWEIS: Wenn eine Active Directory Gruppe endgültig aus der One Identity Manager-Datenbank gelöscht wird, wird auch die zugehörige Leistungsposition gelöscht.

Verwandte Themen

- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 29
- Active Roles spezifische Erweiterungen für Active Directory Gruppen auf Seite 32
- One Identity Manager Anwenderhandbuch für das Web Portal
- One Identity Manager Administrationshandbuch für IT Shop

Active Roles spezifische Erweiterungen für Active Directory Gruppen

Um die aus dem Active Roles ermittelten Stammdaten einer Active Directory Gruppe anzuzeigen

1. Wählen Sie im Manager die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Active Roles**.

Die folgenden Eigenschaften werden abgebildet.

Tabelle 8: Active Roles-spezifische Eigenschaften einer Active Directory Gruppe

Eigenschaft	Beschreibung
Gruppe ist im Self-Service Manager veröffentlicht	Wenn eine Active Directory Gruppe veröffentlicht ist, kann diese Active Directory Gruppe nach der Synchronisation sofort das Web Portal bestellt werden. Die Angabe wird bei der Synchronisation aus dem Active Roles gelesen. Bei Anlage einer Active Directory Gruppe über das Web Portal wird diese Angabe publiziert, um bei Bedarf weitere Arbeitsabläufe in Active Roles zu starten.
Entscheidung durch die Besitzer der Gruppe	Angabe, ob die Entscheidung über die Gruppenmitgliedschaft durch den Besitzer (Kontomanager) der Active Directory Gruppe erfolgen muss. Die Angabe hat Auswirkung auf den Ablauf des Genehmigungsverfahrens im IT Shop.
Entscheidung durch einen zusätzlichen Besitzer der Gruppe	Angabe, ob die Entscheidung über die Gruppenmitgliedschaft durch die zusätzlichen Besitzer der Active Directory Gruppe erfolgen muss. Die Angabe hat Auswirkung auf den Ablauf des Genehmigungsverfahrens im IT Shop.
Zusätzliche Besitzer	Liste zusätzlicher Besitzer. Zulässig sind Active Directory Gruppen oder Active Directory Benutzerkonten.
Deprovisionierungsstatus	Status der Deprovisionierungsabläufe durch Active Roles

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td></td><td>beim Löschen des Objektes. Die Angabe wird bei der Synchronisation aus dem Active Roles gelesen.

<table><tr><th>Status</th><th>Beschreibung</th></tr><tr><td>Keine Deprovisionierung</td><td>Das Active Directory Objekt ist aktiv.</td></tr><tr><td>Deprovisionierung erfolgreich</td><td>Das Active Directory Objekt wurde erfolgreich deprovisioniert.</td></tr><tr><td>Deprovisionierung fehlerhaft</td><td>Bei der Deprovisionierung des Active Directory Objektes ist ein Fehler aufgetreten.</td></tr></table></td></tr>
<tr><td>Deprovisionierungsdatum</td><td>Datum der Deprovisionierungsabläufe durch Active Roles beim Löschen des Objektes. Die Angabe wird bei der Synchronisation aus Active Roles gelesen.</td></tr>
</table>

Verwandte Themen

- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 29
- Bestellen neuer Active Directory Gruppen über das Web Portal auf Seite 31
- Abbildung der Informationen zur Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen auf Seite 36

Deprovisionieren von Active Directory Benutzerkonten und Active Directory Gruppen

Der One Identity Manager unterstützt die Deprovisionierung über Active Roles. Anhand konfigurierter Deprovisionierungsrichtlinien im Active Roles wird ein Active Directory Objekt dabei so modifiziert, dass es temporär oder dauerhaft deaktiviert ist und gegebenenfalls erst nach dem Ablauf eines bestimmten Zeitraumes endgültig gelöscht wird. Detaillierte Informationen zur Active Roles Deprovisionierung entnehmen Sie Ihrer One Identity Active Roles Dokumentation.

HINWEIS: Die Konfiguration der Deprovisionierungsrichtlinien im Active Roles kann im Widerspruch zur Standardkonfiguration One Identity Manager stehen. Nehmen Sie in diesem Fall entsprechende kundenspezifische Anpassungen, beispielsweise an Bildungsregeln oder Prozessen, vor.

Zur Deprovisionierung der Active Directory Benutzerkonten und Active Directory Gruppen über den One Identity Manager werden folgenden Verfahren eingesetzt:

- Deprovisionieren statt Löschen
- Direktes Deprovisionieren

Detaillierte Informationen zum Thema

- Deprovisionieren statt Löschen auf Seite 34
- Direkte Deprovisionierung auf Seite 35
- Abbildung der Informationen zur Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen auf Seite 36
- Wiederherstellen deprovisionierter Active Directory Benutzerkonten und Active Directory Gruppen im One Identity Manager auf Seite 37
- Interaktion mit Active Roles Richtlinien auf Seite 27

Deprovisionieren statt Löschen

Um dieses Verfahren einzusetzen

- Aktivieren Sie für die Active Directory Domäne die Optionen **Löschen von Benutzerkonten durch Active Roles Arbeitsabläufe** und **Löschen von Gruppen durch Active Roles Arbeitsabläufe**.

Beim Löschen eines Active Directory Benutzerkonten oder einer Active Directory Gruppe im One Identity Manager wird anstelle der Standardprozesse zum Löschen ein Prozess zur Deprovisionierung im Active Roles erzeugt. Der Prozess stellt das Active Directory Objekt zur Deprovisionierung im Active Roles ein, setzt den Deprovisionierungsstatus und prüft den Deprovisionierungsverlauf. Abhängig davon erfolgt die Weiterbehandlung der Active Directory Objekte im One Identity Manager.

- Wurde das Active Directory Objekt im Active Roles sofort gelöscht, wird das Active Directory Objekt auch im One Identity Manager gelöscht.
- Wurde das Active Directory Objekt im Active Roles umbenannt oder in einen anderen Active Directory Container verschoben, dann erfolgt dies auch im One Identity Manager.

  Das Active Directory Objekt verbleibt in der One Identity Manager-Datenbank zunächst im Status „gelöscht".

Um ein Benutzerkonto zu löschen

1. Wählen Sie die Kategorie **Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Löschen Sie das Benutzerkonto.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Um eine Active Directory Gruppe zu löschen

1. Wählen Sie die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Löschen Sie die Gruppe über die Schaltfläche .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Verwandte Themen

- Erweiterungen für die Verwendung von Active Roles Arbeitsabläufen auf Seite 24
- Direkte Deprovisionierung auf Seite 35
- Abbildung der Informationen zur Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen auf Seite 36
- Deprovisionierung aufheben auf Seite 38
- Wiederherstellen gelöschter Objekte auf Seite 39

Direkte Deprovisionierung

Dieses Verfahren können Sie einsetzen, wenn die Active Directory Domäne nicht für die Deprovisionierung gekennzeichnet ist. Um einzelne Active Directory Benutzerkonten oder Active Directory Gruppen zu deprovisionieren, wird an diesen Objekten die Aufgabe **Deprovisionieren** angeboten.

Es wird ein Prozess zur Deprovisionierung im Active Roles erzeugt. Der Prozess stellt das Active Directory Objekt zur Deprovisionierung im Active Roles ein, setzt den Deprovisionierungsstatus und prüft den Deprovisionierungsverlauf. Abhängig davon erfolgt die Weiterbehandlung der Active Directory Objekte im One Identity Manager.

- Wurde das Active Directory Objekt im Active Roles sofort gelöscht, wird das Active Directory Objekt auch im One Identity Manager gelöscht.
- Wurde das Active Directory Objekt im Active Roles umbenannt oder in einen anderen Active Directory Container verschoben, dann erfolgt dies auch im One Identity Manager.

  Das Active Directory Objekt verbleibt in der One Identity Manager-Datenbank zunächst im Status "geändert". Durch die nächste Synchronisation werden alle Eigenschaften des Active Directory Objektes in die One Identity Manager-Datenbank eingelesen und der Status auf "publiziert" gesetzt.

Um ein Active Directory Benutzerkonto zu deprovisionieren

1. Wählen Sie die Kategorie **Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Deprovisionieren**.

4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Bestätigen Sie mit **OK**.

Um eine Active Directory Gruppe zu deprovisionieren

1. Wählen Sie die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Deprovisionieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Bestätigen Sie mit **OK**.

Verwandte Themen

- Deprovisionieren statt Löschen auf Seite 34
- Abbildung der Informationen zur Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen auf Seite 36
- Deprovisionierung aufheben auf Seite 38

Abbildung der Informationen zur Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen

Folgende Eigenschaften werden für die Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen abgebildet.

Tabelle 9: Informationen zur Deprovisionierung

Eigenschaft	Beschreibung
Deprovisionierungsstatus	Status der Deprovisionierungsabläufe durch Active Roles beim Löschen des Objektes. Die Angabe wird bei der Synchronisation aus dem Active Roles gelesen.

Status	Beschreibung
Keine Deprovisionierung	Das Active Directory Objekt ist aktiv.
Deprovisionierung	Das Active Directory Objekt wurde

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td></td><td>
<table>
<tr><th>Status</th><th>Beschreibung</th></tr>
<tr><td>erfolgreich</td><td>erfolgreich deprovisioniert.</td></tr>
<tr><td>Deprovisionierung fehlerhaft</td><td>Bei der Deprovisionierung des Active Directory Objektes ist ein Fehler aufgetreten.</td></tr>
</table>
</td></tr>
<tr><td>Deprovisionierungsdatum</td><td>Datum der Deprovisionierungsabläufe durch Active Roles beim Löschen des Objektes. Die Angabe wird bei der Synchronisation aus Active Roles gelesen.</td></tr>
</table>

Um die Stammdaten für die Deprovisionierung eines Active Directory Benutzerkontos anzuzeigen

1. Wählen Sie die Kategorie **Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Active Roles**.

Um die Stammdaten für die Deprovisionierung einer Active Directory Gruppe anzuzeigen

1. Wählen Sie die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Active Roles**.

Verwandte Themen

- Active Roles spezifische Erweiterungen für Active Directory Gruppen auf Seite 32

Wiederherstellen deprovisionierter Active Directory Benutzerkonten und Active Directory Gruppen im One Identity Manager

Deprovisionierte Active Directory Benutzerkonten und Active Directory Gruppen können Sie über den One Identity Manager bei Bedarf wiederherstellen. Dabei werden die folgenden Verfahren eingesetzt:

- Deprovisionierung aufheben
- Wiederherstellen gelöschter Objekte

Mit beiden Verfahren wird ein Prozess zur Deprovisionierung des Active Directory Objektes im Active Roles initiiert. Der Prozess ermittelt den Deprovisionierungsstatus, aktualisiert einige der Eigenschaften des Active Directory Objektes in der One Identity Manager-Datenbank, wie beispielsweise den Namen und den Active Directory Container, und setzt den Status des Active Directory Objektes auf "geändert". Durch die nächste Synchronisation werden alle Eigenschaften des Active Directory Objektes in die One Identity Manager-Datenbank eingelesen und der Status auf "publiziert" geändert.

Detaillierte Informationen zum Thema

- Deprovisionierung aufheben auf Seite 38
- Wiederherstellen gelöschter Objekte
- Deprovisionieren von Active Directory Benutzerkonten und Active Directory Gruppen auf Seite 33

Deprovisionierung aufheben

Mit diesem Verfahren heben Sie die Deprovisionierung der Active Directory Benutzerkonten und Active Directory Gruppen wieder auf. Das Verfahren können Sie unabhängig vom eingesetzten Deprovisionierungsverfahren nutzen.

Um die Deprovisionierung eines Active Directory Benutzerkonto aufzuheben

1. Wählen Sie die Kategorie **Active Directory | Benutzerkonten | Deprovisionierte Konten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Deprovisionierung aufheben**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Bestätigen Sie mit **OK**.

Um die Deprovisionierung einer Active Directory Gruppe aufzuheben

1. Wählen Sie die Kategorie **Active Directory | Gruppen | Deprovisionierte Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Deprovisionierung aufheben**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Bestätigen Sie mit **OK**.

Verwandte Themen

- Wiederherstellen gelöschter Objekte auf Seite 39
- Deprovisionieren von Active Directory Benutzerkonten und Active Directory Gruppen auf Seite 33

Wiederherstellen gelöschter Objekte

Dieses Verfahren können Sie alternativ auf die Active Directory Benutzerkonten und Active Directory Gruppen anwenden, die Sie über das Verfahren "Deprovisionieren statt Löschen" deprovisioniert haben. Das deprovisionierte Active Directory Objekt befindet sich in diesem Fall in der One Identity Manager-Datenbank im Status "gelöscht".

Um ein Benutzerkonto wiederherzustellen

1. Wählen Sie die Kategorie **Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste die Schaltfläche **Löschen rückgängig machen**.

Um eine Gruppe wiederherzustellen

1. Wählen Sie die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Klicken Sie in der Ergebnisliste die Schaltfläche **Löschen rückgängig machen**.

Verwandte Themen

- Deprovisionierung aufheben auf Seite 38
- Deprovisionieren von Active Directory Benutzerkonten und Active Directory Gruppen auf Seite 33

Anhang A

Standardprojektvorlage für Active Roles

Eine Standardprojektvorlage sorgt dafür, dass alle benötigten Informationen im One Identity Manager angelegt werden. Dazu gehören beispielsweise die Mappings, Workflows und das Basisobjekt der Synchronisation. Wenn Sie keine Standardprojektvorlage verwenden, müssen Sie das Basisobjekt der Synchronisation selbst im One Identity Manager bekannt geben.

Verwenden Sie eine Standardprojektvorlage für die initiale Einrichtung des Synchronisationsprojektes. Für kundenspezifische Implementierungen können Sie das Synchronisationsprojekt mit dem Synchronization Editor erweitern.

Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 10: Abbildung der Active Roles Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im Active Roles	Tabelle im One Identity Manager Schema
builtInDomain	ADSContainer
computer	ADSMachine
contact	ADSContact
container	ADSContainer
domainDNS	ADSDomain
group	ADSGroup
inetOrgPerson	ADSAccount
msDS-PasswordSettings	ADSPolicy
msExchSystemObjectsContainer	ADSContainer
oganization	ADSContainer
organizationalUnit	ADSContainer

Schematyp im Active Roles	Tabelle im One Identity Manager Schema
printQueue	ADSPrinter
rpcContainer	ADSContainer
user	ADSAccount

Über uns

One Identity Lösungen eliminieren die Komplexität und die zeitaufwendigen Prozesse, die häufig bei der Identity Governance, der Verwaltung privilegierter Konten und dem Zugriffsmanagement aufkommen. Unsere Lösungen fördern die Geschäftsagilität und bieten durch lokale, hybride und Cloud-Umgebungen eine Möglichkeit zur Bewältigung Ihrer Herausforderungen beim Identitäts- und Zugriffsmanagement.

Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen, wie Lizenzierungen, Support oder Support-Erneuerungen, besuchen Sie https://www.oneidentity.com/company/contact-us.aspx.

Technische Supportressourcen

Technische Unterstützung steht für One Identity Kunden mit einem gültigen Wartungsvertrag und Kunden mit Testversionen zur Verfügung. Sie können auf das Support Portal unter https://support.oneidentity.com/ zugreifen.

Das Support Portal bietet Selbsthilfe-Tools, die Sie verwenden können, um Probleme schnell und unabhängig zu lösen, 24 Stunden am Tag, 365 Tage im Jahr. Das Support Portal ermöglicht Ihnen:

- Senden und Verwalten von Serviceanfragen
- Anzeigen von Knowledge Base Artikeln
- Anmeldung für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Videos unter www.YouTube.com/OneIdentity
- Engagement in der One Identity Community
- Chat mit Support-Ingenieuren
- Anzeigen von Diensten, die Sie bei Ihrem Produkt unterstützen

Index