One Identity Manager 9.1

Anwenderhandbuch für den generischen Datenbankkonnektor zur Verbindung von Oracle Database

Copyright 2022 One Identity LLC.

ALLE RECHTE VORBEHALTEN.

Diese Anleitung enthält urheberrechtlich geschützte Informationen. Die in dieser Anleitung beschriebene Software wird unter einer Softwarelizenz oder einer Geheimhaltungsvereinbarung bereitgestellt. Diese Software darf nur in Übereinstimmung mit den Bestimmungen der geltenden Vereinbarung verwendet oder kopiert werden. Kein Teil dieser Anleitung darf ohne die schriftliche Erlaubnis von One Identity LLC in irgendeiner Form oder mit irgendwelchen Mitteln, elektronisch oder mechanisch reproduziert oder übertragen werden, einschließlich Fotokopien und Aufzeichnungen für irgendeinen anderen Zweck als den persönlichen Gebrauch des Erwerbers.

Die Informationen in diesem Dokument werden in Verbindung mit One Identity Produkten bereitgestellt. Durch dieses Dokument oder im Zusammenhang mit dem Verkauf von One Identity LLC Produkten wird keine Lizenz, weder ausdrücklich oder stillschweigend, noch durch Duldung oder anderweitig, an jeglichem geistigen Eigentumsrecht eingeräumt. MIT AUSNAHME DER IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT GENANNTEN BEDINGUNGEN ÜBERNIMMT ONE IDENTITY KEINERLEI HAFTUNG UND SCHLIESST JEGLICHE AUSDRÜCKLICHE, IMPLIZIERTE ODER GESETZLICHE GEWÄHRLEISTUNG ODER GARANTIE IN BEZUG AUF IHRE PRODUKTE AUS, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE IMPLIZITE GEWÄHRLEISTUNG DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET ONE IDENTITY FÜR JEGLICHE DIREKTE, INDIREKTE, FOLGE-, STÖRUNGS-, SPEZIELLE ODER ZUFÄLLIGE SCHÄDEN (EINSCHLIESSLICH, OHNE EINSCHRÄNKUNG, SCHÄDEN FÜR VERLUST VON GEWINNEN, GESCHÄFTSUNTERBRECHUNGEN ODER VERLUST VON INFORMATIONEN), DIE AUS DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DIESES DOKUMENTS RESULTIEREN, SELBST WENN ONE IDENTITY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN HAT. One Identity übernimmt keinerlei Zusicherungen oder Garantien hinsichtlich der Richtigkeit und Vollständigkeit des Inhalts dieses Dokuments und behält sich das Recht vor, Änderungen an Spezifikationen und Produktbeschreibungen jederzeit ohne vorherige Ankündigung vorzunehmen. One Identity verpflichtet sich nicht, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Wenn Sie Fragen zu Ihrer potenziellen Nutzung dieses Materials haben, wenden Sie sich bitte an:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Besuchen Sie unsere Website (http://www.OneIdentity.com) für regionale und internationale Büro-Adressen.

Patente

One Identity ist stolz auf seine fortschrittliche Technologie. Für dieses Produkt können Patente und anhängige Patente gelten. Für die aktuellsten Informationen über die geltenden Patente für dieses Produkt besuchen Sie bitte unsere Website unter http://www.OneIdentity.com/legal/patents.aspx.

Marken

One Identity und das One Identity Logo sind Marken und eingetragene Marken von One Identity LLC. in den USA und anderen Ländern. Für eine vollständige Liste der One Identity Marken, besuchen Sie bitte unsere Website unter www.OneIdentity.com/legal/trademark-information.aspx. Alle anderen Marken sind Eigentum der jeweiligen Besitzer.

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 Anwenderhandbuch für den generischen Datenbankkonnektor zur Verbindung von Oracle Database
Aktualisiert - 19. September 2022, 11:54 Uhr

Die aktuellsten Versionen der Produktdokumentation finden Sie unter One Identity Manager Dokumentation.

Inhalt

Generischer Datenbankkonnektor für Oracle Database ... 4
Benutzer und Berechtigungen für die Synchronisation ... 5
Benutzerspezifische Anwendungsrollen für die Synchronisation einrichten ... 9
Einrichten des Synchronisationsservers ... 11
Erstellen eines Synchronisationsprojektes ... 14
Synchronisationsprojekt erstellen ... 17
Systemverbindung zu einer Oracle Database herstellen ... 19
Schema aktualisieren ... 26
Synchronisation starten ... 28
Synchronisation auswerten ... 28
Nachbehandlung ausstehender Objekte ... 29
Zielsystemabgleich konfigurieren ... 30
Ausstehende Objekte nachbehandeln ... 32
Provisionierung von Mitgliedschaften konfigurieren ... 33
Einzelobjektsynchronisation konfigurieren ... 35
Datenfehler bei der Synchronisation ignorieren ... 36
Fehlerbehebung ... 38
Unterstützung bei der Analyse von Synchronisationsproblemen ... 38
Über uns ... 39
Kontaktieren Sie uns ... 40
Technische Supportressourcen ... 41
Index ... 42

Generischer Datenbankkonnektor für Oracle Database

Mit dem generischen Datenbankkonnektor können externe Datenbanken mit der One Identity Manager-Datenbank synchronisiert werden. Der One Identity Manager unterstützt unter anderem die Anbindung von Oracle Database.

Der generische Datenbankkonnektor kann nicht jede beliebige Datenkonfiguration des externen Datenbanksystems lesen. Beispielsweise werden kundendefinierte Datentypen und Spalten, die Wertelisten enthalten, derzeit nicht unterstützt.

Der generische Datenbankkonnektor stellt keine Projektvorlagen zum Einrichten der Synchronisation bereit. Die Komponenten der Synchronisationskonfiguration (Mappings, Workflows, Startkonfigurationen, ...) müssen nach dem Speichern des Synchronisationsprojekts manuell erstellt werden.

Im Synchronization Editor werden die Tabellen und Spalten der externen Datenbank als Schematypen und Schemaeigenschaften referenziert.

Um die Synchronisation mit einer Datenbank einzurichten

1. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
2. Statten Sie die One Identity Manager Benutzer mit den erforderlichen Berechtigungen für die Einrichtung der Synchronisation und die Nachbehandlung der Synchronisationsobjekte aus.
3. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Detaillierte Informationen zum Thema

- Einrichten des Synchronisationsservers auf Seite 11
- Benutzer und Berechtigungen für die Synchronisation auf Seite 5
- Erstellen eines Synchronisationsprojektes auf Seite 14

Benutzer und Berechtigungen für die Synchronisation

Bei der Synchronisation mit den Datenbankkonnektoren gibt es drei Anwendungsfälle für die Abbildung der Synchronisationsobjekte im Datenmodell des One Identity Manager.

1. Abbildung als kundendefiniertes Zielsystem
2. Abbildung in Standardtabellen (beispielsweise `Person`, `Department`)
3. Abbildung in kundendefinierten Tabellen

Für die nicht-rollenbasierte Anmeldung an den One Identity Manager-Werkzeugen genügt es in allen drei Anwendungsfällen, einen Systembenutzer in die Berechtigungsgruppen **DPR_EditRights_Methods** und **QBM_LaunchPad** aufzunehmen. Ausführliche Informationen zu Systembenutzern und Berechtigungsgruppen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Tabelle 1: Benutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung

Benutzer	Aufgaben
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne.
Systembenutzer in der Berechtigungsgruppe **DPR_EditRights_ Methods**	• Konfigurieren und starten die Synchronisation im Synchronization Editor. • Bearbeiten im Manager Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation.
Systembenutzer in der Berechtigungsgruppe **QBM_LaunchPad**	• Arbeiten mit dem Launchpad.

Für die rollenbasierte Anmeldung sind je nach Anwendungsfall unterschiedliche Schritte erforderlich, um One Identity Manager Benutzer mit den erforderlichen Berechtigungen für die Einrichtung der Synchronisation und die Nachbehandlung der Synchronisationsobjekte auszustatten.

Tabelle 2: Benutzer und Berechtigungsgruppen für die rollenbasierte Anmeldung: Abbildung als kundendefiniertes Zielsystem

Benutzer	Aufgaben
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne.
Zielsystemadministratoren	Die Zielsystemadministratoren müssen der Anwendungsrolle **Zielsysteme | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen. • Legen die Zielsystemverantwortlichen fest. • Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein. • Legen fest, welche Anwendungsrollen für Zielsystemverantwortliche sich ausschließen. • Berechtigen weitere Personen als Zielsystemadministratoren. • Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Kundendefinierte Zielsysteme** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Tabelle 3: Benutzer und Berechtigungsgruppen für die rollenbasierte Anmeldung: Abbildung von Standardtabellen

Benutzer	Aufgaben
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter.

Benutzer	Aufgaben
	• Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne.
Benutzerspezifische Anwendungsrolle	Benutzer mit dieser Anwendungsrolle: • Konfigurieren und starten die Synchronisation im Synchronization Editor. • Bearbeiten im Manager Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. Die Anwendungsrolle erhält ihre Berechtigungen über eine kundendefinierte Berechtigungsgruppe und die Berechtigungsgruppe **vi_4_SYNCPROJECT_ADMIN**.

Tabelle 4: Benutzer und Berechtigungsgruppen für die rollenbasierte Anmeldung: Abbildung in kundendefinierten Tabellen

Benutzer	Aufgaben
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne.
Administratoren für benutzerspezifische Aufgaben	Die Administratoren müssen der Anwendungsrolle **Benutzerspezifisch | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Administrieren die benutzerspezifischen Anwendungsrollen. • Richten bei Bedarf weitere Anwendungsrollen für Verantwortliche ein.

Benutzer	Aufgaben
Verantwortliche für benutzerspezifische Aufgaben	Die Verantwortlichen müssen der Anwendungsrolle **Benutzerspezifisch | Verantwortliche** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen unternehmensspezifisch definierte Aufgaben im One Identity Manager. • Konfigurieren und Starten die Synchronisation im Synchronization Editor. • Bearbeiten im Manager Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. Sie können diese Anwendungsrolle beispielsweise nutzen, um One Identity Manager Benutzern Berechtigungen auf kundenspezifische Tabellen oder Spalten zu gewähren. Alle Anwendungsrollen, die Sie hier definieren, müssen ihre Berechtigungen über kundendefinierte Berechtigungsgruppen erhalten. Die Anwendungsrolle erhält ihre Berechtigungen über eine kundendefinierte Berechtigungsgruppe und die Berechtigungsgruppe **vi_4_SYNCPROJECT_ADMIN**.

Um Synchronisationsprojekte und Zielsystemabgleich konfigurieren zu können (in den Anwendungsfällen 2 und 3)

1. Erstellen Sie eine kundendefinierte Berechtigungsgruppe mit allen Berechtigungen für die Konfiguration der Synchronisation und die Bearbeitung der Synchronisationsobjekte.
2. Ordnen Sie diese Berechtigungsgruppe einer benutzerspezifischen Anwendungsrolle zu.

Detaillierte Informationen zum Thema

- Benutzerspezifische Anwendungsrollen für die Synchronisation einrichten auf Seite 9

Benutzerspezifische Anwendungsrollen für die Synchronisation einrichten

Um bei rollenbasierter Anmeldung den One Identity Manager Benutzern die erforderlichen Berechtigungen für die Konfiguration der Synchronisation und die Bearbeitung ausstehender Objekte zu gewähren, erstellen Sie eine benutzerspezifische Anwendungsrolle. Diese Anwendungsrolle erhält die erforderlichen Berechtigungen über eine kundendefinierte Berechtigungsgruppe.

Um eine Anwendungsrolle für die Synchronisation einzurichten (Anwendungsfall 2)

1. Wählen Sie im Manager die Standardanwendungsrolle, mit der Sie die Objekte bearbeiten können, die Sie synchronisieren möchten.
   - Ermitteln Sie die Standardberechtigungsgruppe dieser Anwendungsrolle.

   Wenn Sie beispielsweise Personenstammdaten importieren wollen, wählen Sie die Anwendungsrolle **Identity Management | Personen | Administratoren**. Die Standardberechtigungsgruppe dieser Anwendungsrolle ist **vi_4_PERSONADMIN**.
2. Erstellen Sie im Designer eine neue Berechtigungsgruppe.
   - Aktivieren Sie die Option **Nur für rollenbasierte Anmeldung**.
3. Stellen Sie die Abhängigkeit der neuen Berechtigungsgruppe zur Berechtigungsgruppe **vi_4_SYNCPROJECT_ADMIN** her.

   Die Berechtigungsgruppe **vi_4_SYNCPROJECT_ADMIN** muss dabei als übergeordnete Berechtigungsgruppe zugeordnet werden. Damit vererbt sie ihre Eigenschaften an die neu definierte Berechtigungsgruppe.
4. Stellen Sie die Abhängigkeit der neuen Berechtigungsgruppe zur Standardberechtigungsgruppe der ausgewählten Standardanwendungsrolle her.

   Die Standardberechtigungsgruppe muss dabei als übergeordnete Berechtigungsgruppe zugeordnet werden. Damit vererbt sie ihre Eigenschaften an die neu definierte Berechtigungsgruppe.
5. Speichern Sie die Änderungen.
6. Erstellen Sie im Manager eine neue Anwendungsrolle.
   a. Ordnen Sie die ausgewählte Standardanwendungsrolle als übergeordnete Anwendungsrolle zu.
   b. Ordnen Sie die neu erstellte Berechtigungsgruppe zu.
7. Weisen Sie dieser Anwendungsrolle Personen zu.
8. Speichern Sie die Änderungen.

Um eine Anwendungsrolle für die Synchronisation einzurichten (Anwendungsfall 3)

1. Erstellen Sie im Designer eine neue Berechtigungsgruppe für die kundendefinierten Tabellen, die durch die Synchronisation befüllt werden.
   - Aktivieren Sie die Option **Nur für rollenbasierte Anmeldung**.
2. Gewähren Sie dieser Berechtigungsgruppe alle erforderlichen Berechtigungen auf die kundendefinierten Tabellen.
3. Erstellen Sie eine weitere Berechtigungsgruppe für die Synchronisation.
   - Aktivieren Sie die Option **Nur für rollenbasierte Anmeldung**.
4. Stellen Sie die Abhängigkeit der Berechtigungsgruppe für die Synchronisation zur Berechtigungsgruppe für die kundendefinierten Tabellen her.

Die Berechtigungsgruppe für die kundendefinierten Tabellen muss dabei als übergeordnete Berechtigungsgruppe zugeordnet werden. Damit vererbt sie ihre Eigenschaften an die Berechtigungsgruppe für die Synchronisation.

5. Stellen Sie die Abhängigkeit der Berechtigungsgruppe für die Synchronisation zur Berechtigungsgruppe **vi_4_SYNCPROJECT_ADMIN** her.

   Die Berechtigungsgruppe **vi_4_SYNCPROJECT_ADMIN** muss dabei als übergeordnete Berechtigungsgruppe zugeordnet werden. Damit vererbt sie ihre Eigenschaften an die Berechtigungsgruppe für die Synchronisation.
6. Speichern Sie die Änderungen.
7. Erstellen Sie im Manager eine neue Anwendungsrolle.
   a. Ordnen Sie die Anwendungsrolle **Benutzerspezifisch | Verantwortliche** als übergeordnete Anwendungsrolle zu.
   b. Ordnen Sie die Berechtigungsgruppe für die Synchronisation zu.
8. Weisen Sie dieser Anwendungsrolle Personen zu.
9. Speichern Sie die Änderungen.

Ausführliche Informationen zum Einrichten von Anwendungsrollen und Berechtigungsgruppen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Einrichten des Synchronisationsservers

Für die Einrichtung der Synchronisation muss ein Server zur Verfügung gestellt werden, auf dem die nachfolgend genannte Software installiert ist:

- One Identity Manager Service
  - 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 | Job Server**.

  Ausführliche Informationen zu den Systemanforderungen für die Installation des One Identity Manager Service finden Sie im *One Identity Manager Installationshandbuch*.

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: Das Programm führt eine Remote-Installation des One Identity Manager Service aus. Eine lokale Installation des Dienstes ist mit diesem Programm nicht möglich.

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*.

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*.

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 Jobserver 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 **Job Server**.
5. Auf der Seite **Serverfunktionen** wählen Sie **Generischer Datenbankkonnektor**.
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:
     1. Wählen Sie **Prozessabholung > sqlprovider**
     2. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     3. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
   - Für eine Verbindung zum Anwendungsserver:
     1. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
     2. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     3. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.
     4. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
     5. 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** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.
10. Wenn die Datenbank verschlüsselt ist, wählen Sie auf der Seite **Datenbankschlüsseldatei auswählen** die Datei mit dem privaten Schlüssel.
11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.

- **Computer**: Erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
- **Dienstkonto**: Erfassen Sie die Angaben zum Benutzerkonto unter dem der One Identity Manager Service läuft. Erfassen Sie das Benutzerkonto, das Kennwort zum Benutzerkonto und die Kennwortwiederholung.

Die Installation des Dienstes erfolgt mit dem Benutzerkonto, mit dem Sie an der administrativen Arbeitsstation angemeldet sind. Möchten Sie ein anderes Benutzerkonto für die Installation des Dienstes nutzen, können Sie dieses in den erweiterten Optionen eintragen. Angaben zum One Identity Manager Service können Sie ebenfalls über die erweiterten Optionen ändern, beispielsweise das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den One Identity Manager Service.

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

Ein Synchronisationsprojekt ist die Zusammenstellung aller Informationen, die für die Synchronisation der One Identity Manager-Datenbank mit einem Zielsystem benötigt werden. Dazu gehören die Verbindungsinformationen zum Zielsystem, Schematypen und -eigenschaften, Mappings und Synchronisationsworkflows.

Für die Einrichtung eines Synchronisationsprojekts für die Synchronisation mit dem generischen Datenbankkonnektor halten Sie die folgenden Informationen bereit.

Tabelle 5: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Synchronisationsserver	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. Installierte Komponenten: • One Identity Manager Service (gestartet)

Angaben	Erläuterungen
	Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt. Weitere Informationen finden Sie unter Einrichten des Synchronisationsservers auf Seite 11.
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 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*.
Synchronisationsworkflow	Wenn die Synchronisation Daten aus einem sekundären System importiert, aktivieren Sie in den Synchronisationsschritten die Option **Datenimport**. Ausführliche Informationen zur Synchronisation von Benutzerdaten mit verschiedenen Systemen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsys-*

Angaben	Erläuterungen
	temsynchronisation.
Basisobjekt	Für Synchronisationen mit den Datenbankkonnektoren kann meist kein konkretes Basisobjekt festgelegt werden. Hier genügt die Zuordnung einer Basistabelle und des Synchronisationsservers. • Wählen Sie aus der Auswahlliste **Basistabelle** die Tabelle, in welche die Objekte eingelesen werden sollen. Die Basistabelle kann genutzt werden, um nachgelagerte Prozesse für die Synchronisation zu definieren. Ausführliche Informationen zu nachgelagerten Prozessen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*. • In der Auswahlliste **Synchronisationsserver** werden alle Jobserver angezeigt, für welche die Serverfunktion **Generischer Datenbankkonnektor** aktiviert ist.
Variablenset	Wenn Sie spezialisierte Variablensets einsetzen, stellen Sie sicher, das die Startkonfiguration und das Basisobjekt das selbe Variablenset nutzen.

Um die Synchronisation mit dem generischen Datenbankkonnektor zu konfigurieren

1. Erstellen Sie ein neues Synchronisationsprojekt.
2. Legen Sie Mappings an. Definieren Sie Property-Mapping-Regeln und Object-Matching-Regeln.
3. Erstellen Sie Synchronisationsworkflows.
4. Erstellen Sie eine Startkonfiguration.
5. Definieren Sie den Scope der Synchronisation.
6. Legen Sie das Basisobjekt der Synchronisation fest.
7. Legen Sie den Umfang des Synchronisationsprotokolls fest.
8. Führen Sie eine Konsistenzprüfung durch.
9. Aktivieren Sie das Synchronisationsprojekt.
10. Speichern Sie das neu angelegt Synchronisationsprojekt in der Datenbank.

Detaillierte Informationen zum Thema

- Synchronisationsprojekt erstellen auf Seite 17

Synchronisationsprojekt erstellen

Beim Erstellen eines Synchronisationsprojekts unterstützt Sie ein Assistent. Dieser Assistent führt Sie durch alle Schritte, die zum initialen Einrichten der Synchronisation mit einem Zielsystem erforderlich sind. Wenn Sie alle erforderlichen Angaben für einen Schritt erfasst haben, klicken Sie **Weiter**.

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

- im Standardmodus ausgeführt wird und
- aus dem Launchpad gestartet wird.

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

Um das Synchronisationsprojekt einzurichten

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.

   HINWEIS: Wenn die Synchronisation über einen Anwendungsserver ausgeführt werden soll, stellen Sie die Datenbankverbindung über den Anwendungsserver her.

2. Wählen Sie den Eintrag **Generischer Datenbankkonnektor** und klicken Sie **Starten**.

   Der Projektassistent des Synchronization Editor wird gestartet.

3. 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.

   - Klicken Sie **Weiter** um den Systemverbindungsassistenten zur Erstellung der Verbindung zu einer externen Datenbank zu starten.

4. Auf der Seite **Datenbanksystem auswählen** wählen Sie das Datenbanksystem aus, für das Sie die Verbindung einrichten möchten.
   - Wählen Sie **Oracle Database**.

5. Konfigurieren Sie die Systemverbindung.

   Weitere Informationen finden Sie unter Systemverbindung zu einer Oracle Database herstellen auf Seite 19.

6. Auf der Seite **Konfiguration speichern** können Sie die aktuelle Konfiguration als Vorlage speichern. Diese Konfiguration können Sie bei einer erneuten Verbindung zu einem Datenbanksystem des selben Typs als Vorlage verwenden.
    - Klicken Sie 🗁 und erfassen Sie den Namen und Ablagepfad der Konfigurationsdatei.
7. Auf der letzten Seite des Systemverbindungsassistenten können Sie die Verbindungsdaten speichern.
    - Aktivieren Sie die Option **Verbindung lokal speichern**, um die Verbindungsdaten zu speichern. Diese können Sie bei der Einrichtung weiterer Synchronisationsprojekte nutzen.
    - Um den Systemverbindungsassistenten zu beenden und zum Projektassistenten zurückzukehren, klicken Sie **Fertig**.
8. 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.
9. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.
10. Auf der Seite **Projektvorlage auswählen** wählen Sie eine Projektvorlage, mit der die Synchronisationskonfiguration erstellt werden soll.

    HINWEIS: Der generische Datenbankkonnektor stellt keine Standard-Projektvorlage zum Einrichten der Synchronisation bereit. Wenn Sie eigene Projektvorlagen erstellt haben, können Sie diese auswählen, um das Synchronisationsprojekt zu konfigurieren. Andernfalls wählen Sie **Leeres Projekt erstellen**.
11. Auf der Seite **Allgemein** erfassen Sie die allgemeinen Einstellungen für das Synchronisationsprojekt.

Tabelle 6: Allgemeine Eigenschaften des Synchronisationsprojekts

Eigenschaft	Beschreibung
Anzeigename	Anzeigename für das Synchronisationsprojekt.
Skriptsprache	Sprache, in der Skripte in diesem Synchronisationsprojekt geschrieben werden. Skripte werden an verschiedenen Stellen in der Synchro-

Eigenschaft	Beschreibung
	nisationskonfiguration eingesetzt. Wenn Sie ein leeres Projekt erstellen, legen Sie die Skriptsprache fest. WICHTIG: Die Skriptsprache kann nach dem Speichern des Synchronisationsprojekts nicht mehr geändert werden! Wenn Sie eine Projektvorlage nutzen, wird die Skriptsprache der Projektvorlage übernommen.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

12. Um den Projektassistenten zu beenden, klicken Sie **Fertig**.
13. Speichern Sie das Synchronisationsprojekt in der Datenbank.

Systemverbindung zu einer Oracle Database herstellen

Tabelle 7: Benötigte Informationen für die Erstellung der Systemverbindung

Angaben	Erläuterungen
Datenquelle	• Verbindungsparameter (Connect Descriptor) zur Oracle Database in folgender Syntax: `(DESCRIPTION=(ADDRESS=(protocol_address_information))(CONNECT_DATA=(SERVICE_NAME=service_name)))` - ODER - • TNS-Alias-Name aus der Datei `tnsnames.ora`.
Benutzer und Kennwort	Benutzername und Kennwort, mit dem sich der generische Datenbankkonnektor an der externen Datenbank anmeldet. Stellen Sie einen Benutzer mit ausreichenden Berechtigungen bereit.

Um die Verbindung zu einer Oracle Database zu konfigurieren

1. Auf der Seite **Verbindung herstellen** erfassen Sie die Verbindungsparameter. Geben Sie alle Parameter an, die der generische Datenbankkonnektor benötigt, um eine Verbindung mit dem ausgewählten Datenbanksystem herzustellen.
   - Um zusätzliche systemspezifische Informationen zur Systemverbindung zu erfassen, klicken Sie **Erweitert**.

   Die Verbindung zum Datenbanksystem wird getestet, sobald Sie **Weiter** klicken.
2. Auf der Seite **Datenbank beschreiben** geben Sie der Datenbankverbindung einen Anzeigenamen und einen eindeutigen Bezeichner.

- **Anzeigename der Datenbank**: Anzeigename der Datenbank für die Anzeige in den One Identity Manager Werkzeugen.
- **Systembezeichner**: Eindeutiger Bezeichner der Datenbank.

  WICHTIG: Der Systembezeichner muss die Datenbank eindeutig beschreiben. Mit Hilfe dieses Bezeichners werden die Datenbanken unterschieden. Um Fehlverhalten und Datenverlust zu vermeiden, stellen Sie sicher, dass die Systembezeichner innerhalb einer One Identity Manager-Umgebung eindeutig sind.

  - Bezeichner dürfen nicht mehrfach vergeben werden.
  - Bezeichner dürfen nach dem Speichern der Verbindung nicht geändert werden.
- **Systemkategorie**: Kategorie zur weiteren Unterscheidung von Systemtypen. Für die Bezeichnung sind maximal 16 Zeichen, bestehend aus Ziffern und Buchstaben, zulässig.

  Verbindungen mit dem generischen Datenbankkonnektor werden üblicherweise mit dem Systemtyp **DB** gespeichert. Die Systemkategorie erlaubt eine weitere Klassifizierung in Subtypen. So können verschiedenen Datenbankverbindungen mit unterschiedlichem Inhalt unterschieden werden.

  Beispiele:

  Verbindung 1: Typ=**DB**, Subtyp=**Rights**

  Verbindung 2: Typ=**DB**, Subtyp=**PersonImport**

3. Auf der Seite **Konfiguration laden** können Sie eine Datei angeben, aus der die Verbindungskonfiguration geladen werden soll. Diese Daten werden in den weiteren Schritten des Verbindungsassistenten als Vorlage verwendet und können dort angepasst werden.
4. Auf der Seite **Zeitzonenauswahl** wählen Sie die Zeitzone für Zeitangaben in der Datenbank aus. Die Zeitzone wird benötigt, um Zeitangaben, die in der Datenbank gespeichert sind, in die lokale Zeit umrechnen zu können. In den One Identity Manager Werkzeugen wird die lokale Zeit angezeigt.
5. Auf der Seite **Initialisierung** können Sie zusätzliche Verbindungseinstellungen festlegen. Um beispielsweise Einstellungen für Zahlen- und Datumsformate, die Sprache oder die Datensortierung festzulegen, formulieren Sie ein Skript in der Syntax der Datenbank. Das Skript wird nach jedem Verbindungsaufbau ausgeführt.
6. Auf der Seite **Teilschemas auswählen** können Sie das Datenbankschema durch die Auswahl von Teilschemen reduzieren. Wenn die Datenbank mehrere Schemas enthält, legen Sie hier fest, welche Schemas in das Synchronisationsprojekt eingelesen werden sollen.
   - Aktivieren Sie in der Liste **Teilschemas/Besitzer** alle Schemas, die verarbeitet werden sollen.
7. Auf der Seite **Schema laden** wird das Datenbankschema geladen. Dabei versucht der One Identity Manager ein bekanntes Schema zu erkennen.

- Wenn ein One Identity Manager Schema erkannt wurde, wird die Option **Systembeschreibung vollständig ausfüllen** angezeigt. Wenn nur lesend auf die Datenbank zugegriffen werden soll, können Sie diese Option deaktivieren.

Wenn das Schema erfolgreich geladen wurde, kann der nächste Schritt im Verbindungsassistenten ausgeführt werden.

8. Auf der Seite **Schlüsselinformationen erweitern** legen Sie für jede Tabelle die Spalten fest, die als eindeutiger Schlüssel bei der Identifikation der Objekte genutzt werden.

   HINWEIS:

   - Diese Seite wird nur angezeigt, wenn im Schema der externen Datenbank Tabellen vorhanden sind, für die kein eindeutiger Schlüssel identifiziert werden kann.
   - Tabellen ohne eindeutigen Schlüssel werden in der Synchronisationskonfiguration nicht verwendet.

Tabelle 8: Eindeutige Schlüssel definieren

Eigenschaft	Beschreibung
Nicht konfigurierte Tabellen ausblenden	Gibt an, ob Tabellen ausgeblendet werden, für die keine Einstellungen vorgenommen wurden.
Schema	Tabellen, für die kein eindeutiger Schlüssel definiert ist.
Spalte ist Schlüssel	Gibt an, ob die Spalte einen eindeutigen Schlüssel enthält.
Spaltengruppe	Schaltflächen zum Bearbeiten von Spaltengruppen. Wenn ein eindeutiger Schlüssel nur aus der Kombination mehrerer Spalten gebildet werden kann, erstellen Sie eine Spaltengruppe. • Um eine Spaltengruppe zu erstellen, klicken Sie **Hinzufügen**. • Um eine bestehende Spaltengruppe zu bearbeiten oder zu entfernen, klicken Sie **Bearbeiten oder entfernen**.

Tabelle 9: Eigenschaften einer Spaltengruppe

Eigenschaft	Beschreibung
Name der Spaltengruppe	Bezeichnung der Spaltengruppe. Zulässige Zeichen sind Buchstaben und der Unterstrich. Aus der Spaltengruppe wird eine virtuelle Schemaeigenschaft mit dem Namen `vrtColumnGroup<Spaltengruppe>` gebildet.

Eigenschaft	Beschreibung
Spalten	Spalten, aus denen die Spaltengruppe gebildet wird. Markieren Sie alle Spalten, die gemeinsam den eindeutigen Schlüssel der Tabelle bilden. HINWEIS: Spalten mit dem Datentyp `Char` werden nicht unterstützt.

9. Auf der Seite **Datenrelationen definieren** können Sie Informationen über Objektbeziehungen erfassen.

Tabelle 10: Spaltenbeziehungen definieren

Eigenschaft	Beschreibung
Nicht konfigurierte Tabellen ausblenden	Gibt an, ob Tabellen ausgeblendet werden, für die keine Einstellungen vorgenommen wurden.
Schema	Tabellen des Datenbankschemas.
Ziel(e)	Spalten, auf welche die Referenz verweist. Geben Sie den Tabellen- und Spaltennamen in folgender Syntax an: `<Schema>.]<Tabellenname>.<Spaltenname>` Wenn eine Referenz auf mehrere Spalten verweist, geben Sie die Ziele als kommagetrennte Liste an. Die Zielspalten müssen als Schlüsselspalten gekennzeichnet sein. TIPP: Sie können den Spaltennamen einer referenzierten Spalte über den Kontextmenüeintrag **Vollqualifizierten Spaltennamen kopieren** kopieren und als Ziel einfügen.
Referentielle Integrität geprüft	Gibt an, ob die referenzielle Integrität der Daten in den Zieltabellen sichergestellt ist.

10. Auf der Seite **Schema vervollständigen** können Sie zusätzliche Schemainformationen angeben.

Tabelle 11: Zusätzliche Schemainformationen

Eigenschaft	Beschreibung
Nicht konfigurierte Tabellen ausblenden	Gibt an, ob Tabellen ausgeblendet werden, für die keine Einstellungen vorgenommen wurden.

Eigenschaft	Beschreibung
Schema	Tabellen und Spalten des Datenbankschemas.
Anzeigewert	Spalte, die im Anzeigemuster verwendet wird. • Um die Spalte im Anzeigemuster zu verwenden, klicken Sie **Aufnehmen**.
Bevorzugter Schlüssel	Gibt an, ob die Spalte primär bei der Identifikation der Objekte genutzt werden soll. Der bevorzugte Schlüssel kann festgelegt werden, wenn für eine Tabelle mehrere eindeutige Schlüssel definiert sind. Es können nur Spalten mit dem Datentyp **String** ausgewählt werden.
Enthält sensible Daten	Gibt an, ob die Spalte sensible Daten enthält.
Revisionszähler	Gibt an, ob die Spalte den Revisionszähler enthält. Die Daten dieser Spalte bilden den Vergleichswert für die Revisionsfilterung.
Sortierkriterium für Hierarchien	Gibt an, ob der Wert dieser Spalte den Pfad in einer Objekthierarchie abbildet. Wenn die Objekte dieser Tabelle nach dieser Spalte sortiert werden, ergibt sich eine hierarchisch sortierte Liste. Dadurch wird die Auflösung von Objektabhängigkeiten ermöglicht. Pro Tabelle kann nur eine Spalte als Sortierkriterium markiert werden. Ein Beispiel für eine solche Spalte ist `CanonicalName`.
Scopereferenz	Gibt an, ob die Spalte zur Bildung des Referenzscope genutzt werden kann. Je Schematyp darf maximal eine Spalte als Scopereferenz gekennzeichnet sein.
Hat Standardwert	Gibt an, ob Standardwerte in der Spalte automatisch erkannt werden.
Kompatible Null-Behandlung aktivieren	Gibt an, ob ein Null-Wert in der Spalte in einen Leerstring umgewandelt werden soll.

Tabelle 12: Tabelleneigenschaften

Eigenschaft	Beschreibung
Anzeigemuster	Anzeigemuster, mit dem die Objekte im Synchronization Editor angezeigt werden. Das Anzeigemuster wird beispielsweise in Fehlermeldungen oder in den Testergebnissen von Object-Matching-Regeln genutzt. Das Anzeigemuster kann aus mehreren Spalten und zusätzlichen Zeichen gebildet werden. Erfassen Sie für jede Tabelle ein Anzeigemuster.

Eigenschaft	Beschreibung
	• Um eine Spalte im Anzeigemuster zu verwenden, wählen Sie eine Spalte und klicken Sie **Aufnehmen**.

11. Auf der Seite **Datenoperationen definieren** können Sie spezielle Operationen für die Änderung von Daten in der externen Datenbank festlegen. Das ist nur erforderlich, wenn die Standardoperationen `INSERT`, `UPDATE` und `DELETE` im externen Datenbanksystem nicht genutzt werden können.

   VORSICHT: **Für die Implementierung von Datenoperationen sind fundierte Programmierkenntnisse erforderlich. Fehler in dieser Implementierung können zu Datenverlust führen.**

   Um eine Datenoperation zu definieren

   a. Wählen Sie eine Tabelle und markieren Sie die Operation, für die Sie eine Datenoperation definieren möchten.

   b. Wählen Sie eine Strategie.

   c. Erfassen Sie im Eingabefeld **Einstellungen** die auszuführende Datenoperation.

   Tabelle 13: Datenoperation definieren

Eigenschaft	Beschreibung
Nicht konfigurierte Tabellen ausblenden	Gibt an, ob Tabellen ausgeblendet werden, für die keine Einstellungen vorgenommen wurden.
Tabelle/Operation	Tabellen, für die Datenoperationen definiert werden sollen.
Strategie	Strategie, mit der die Datenoperation erstellt und ausgeführt wird. Für eine Datenoperationen kann eine einfache Prozedur aufgerufen oder ein Skript ausgeführt werden. Wählen Sie die Strategie, mit der Sie die Datenoperation definieren möchten. • **Musterbasiert**: Einfacher Prozeduraufruf, der die Operation ausführt. HINWEIS: Wenn Spaltennamen referenziert werden, die Sonderzeichen enthalten, dann ersetzten Sie die Sonderzeichen durch Unterstrich (_). Sonderzeichen sind alle Zeichen außer Buchstaben, Ziffern und Unterstrich. • **Skriptbasiert**: Skript, das eine komplexe Datenoperation ausführt.

Eigenschaft	Beschreibung
	Im Skript können kundenspezifische Code-Ausschnitte verwendet werden. Die Code-Ausschnitte müssen ein Keywords-Element mit dem Stichwort **DML** enthalten. Ausführliche Informationen zur Unterstützung bei der Eingabe von Skripten finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*. • Um eine Datenoperation zu löschen, klicken Sie 🗑.
Erforderliche Spalten	Liste der erforderlichen Schlüsselspalten in einer skriptbasierten Datenoperation. Die Spalten müssen angegeben werden, wenn sie nicht Bestandteil des Anzeigenamens sind.
Einstellungen	Definieren Sie die Datenoperation, die beim Einfügen, Aktualisieren oder Löschen von Objekten ausgeführt werden soll. Je nach gewählter Strategie erfassen Sie hier den Prozeduraufruf oder erstellen Sie ein Skript. Beispiel für eine musterbasierte Datenoperation: `begin CreateUser('%UID%', '%Firstname%', '%Lastname%'); end;` Das Eingabefeld besitzt einen erweiterten Bearbeitungsmodus, in dem zusätzliche Aktionen möglich sind. Ausführliche Informationen zur Unterstützung beim Erstellen von Skripten finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

12. Wenn Sie auf der Seite **Schema laden** die Option **Systembeschreibung vollständig ausfüllen** aktiviert oder auf der Seite **Datenoperationen definieren** Einstellungen vorgenommen haben, wird die Seite **Zielsystemschema erweitern** geöffnet. Hier können Sie das Zielsystemschema um virtuelle Schemaeigenschaften erweitern. Nutzen Sie virtuelle Schemaeigenschaften, um zusätzliche Daten für eine eigene DML-Behandlung bereitzustellen.

Tabelle 14: Virtuelle Schemaeigenschaften

Eigenschaft	Beschreibung
Nicht konfigurierte Tabellen ausblenden	Gibt an, ob Tabellen ausgeblendet werden, für die keine Einstellungen vorgenommen wurden.

Eigenschaft	Beschreibung
Schema	Tabellen im Zielsystemschema, für die virtuelle Schemaeigenschaften angelegt werden können oder angelegt sind.
Virtuelle Schemaeigenschaft	Schaltflächen zum Bearbeiten von virtuellen Schemaeigenschaften. • Um eine virtuelle Schemaeigenschaft anzulegen, klicken Sie **Hinzufügen**. • Um eine virtuelle Schemaeigenschaft zu bearbeiten oder zu löschen, klicken Sie **Bearbeiten oder löschen**.
Datentyp	Datentyp der Schemaeigenschaft.
Mehrwertig	Gibt an, ob die Schemaeigenschaft mehrwertig ist.
Pflichtfeld	Gibt an, ob die Schemaeigenschaft eine Pflichteigenschaft ist.
Sensibler Wert	Gibt an, ob der Wert der Schemaeigenschaft im Synchronization Editor oder in Protokollen, Berichten und Meldungen angezeigt werden darf. Wenn die Option aktiviert ist, wird der Wert nicht angezeigt.

Um eine virtuelle Schemaeigenschaft zu bearbeiten oder zu löschen

a. Öffnen Sie in der Spalte **Schema** den Knoten der Tabelle, deren Schemaeigenschaften Sie bearbeiten oder löschen möchten.

b. Klicken Sie **Bearbeiten oder löschen**.

c. Bearbeiten Sie die Eigenschaften der virtuellen Schemaeigenschaft.

   - ODER -

   Klicken Sie **Löschen**.

Verwandte Themen

- Synchronisationsprojekt erstellen auf Seite 17

Schema aktualisieren

Während ein Synchronisationsprojekt bearbeitet wird, stehen alle Schemadaten (Schematypen und Schemaeigenschaften) des Zielsystemschemas und des One Identity Manager Schemas zur Verfügung. Für eine Synchronisationskonfiguration wird jedoch nur ein Teil dieser Daten benötigt. Wenn ein Synchronisationsprojekt fertig gestellt wird, werden die Schemas komprimiert, um die nicht benötigten Daten aus dem Synchronisationsprojekt zu entfernen. Dadurch kann das Laden des Synchronisationsprojekts beschleunigt werden. Die entfernten Schemadaten können zu

einem späteren Zeitpunkt wieder in die Synchronisationskonfiguration aufgenommen werden.

Wenn sich das Zielsystemschema oder das One Identity Manager Schema geändert hat, müssen diese Änderungen ebenfalls in die Synchronisationskonfiguration aufgenommen werden. Anschließend können die Änderungen in das Mapping der Schemaeigenschaften eingearbeitet werden.

Um Schemadaten, die beim Komprimieren entfernt wurden, und Schemaänderungen in der Synchronisationskonfiguration berücksichtigen zu können, aktualisieren Sie das jeweilige Schema im Synchronisationsprojekt. Das kann erforderlich sein, wenn:

- ein Schema geändert wurde, durch:
  - Änderungen am Zielsystemschema
  - unternehmensspezifische Anpassungen des One Identity Manager Schemas
  - eine Update-Migration des One Identity Manager
- ein Schema im Synchronisationsprojekt komprimiert wurde, durch:
  - die Aktivierung des Synchronisationsprojekts
  - erstmaliges Speichern des Synchronisationsprojekts
  - Komprimieren eines Schemas

Um das Schema einer Systemverbindung zu aktualisieren

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.

   - ODER -

   Wählen Sie die Kategorie **Konfiguration > One Identity Manager Verbindung**.
3. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Die Schemadaten werden neu geladen.

Um ein Mapping zu bearbeiten

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Mappings**.
3. Wählen Sie in der Navigationsansicht das Mapping.

   Der Mappingeditor wird geöffnet. Ausführliche Informationen zum Bearbeiten von Mappings finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

HINWEIS: Wenn das Schema eines aktivierten Synchronisationsprojekts aktualisiert wird, wird das Synchronisationsprojekt deaktiviert. Damit Synchronisationen ausgeführt werden, aktivieren Sie das Synchronisationsprojekt erneut.

Synchronisation starten

Synchronisationen werden über zeitgesteuerter Prozessaufträge gestartet. Ein zeitgesteuerter Prozessauftrag wird angelegt, sobald einer Startkonfiguration ein Zeitplan zugeordnet wird. Zeitpläne legen die Ausführungszeiten für die Synchronisation fest.

HINWEIS: Eine Synchronisation kann nur gestartet werden, wenn das Synchronisationsprojekt aktiviert ist.

Um regelmäßige Synchronisationen auszuführen, konfigurieren und aktivieren Sie einen Zeitplan. Wenn kein Zeitplan aktiviert ist, können Sie die Synchronisation auch manuell starten.

WICHTIG: Solange eine Synchronisation ausgeführt wird, sollte keine weitere Synchronisation für dasselbe Zielsystem gestartet werden. Das gilt insbesondere, wenn dieselben Synchronisationsobjekte verarbeitet werden.

- Wenn eine weitere Synchronisation mit derselben Startkonfiguration gestartet wird, wird dieser Prozess gestoppt und erhält den Ausführungsstatus **Frozen**. Es wird eine Fehlermeldung in die Protokolldatei des One Identity Manager Service geschrieben.
    - Stellen Sie sicher, dass Startkonfigurationen, die in Startfolgen verwendet werden, nicht gleichzeitig einzeln gestartet werden. Weisen Sie den Startfolgen und Startkonfigurationen unterschiedliche Zeitpläne zu.
- Wenn eine weitere Synchronisation mit einer anderen Startkonfiguration gestartet wird, die dasselbe Zielsystem anspricht, kann das zu Synchronisationsfehlern oder Datenverlust führen. Legen Sie an den Startkonfigurationen fest, wie sich der One Identity Manager in diesem Fall verhalten soll.
    - Stellen Sie über den Zeitplan sicher, dass die Startkonfigurationen nacheinander ausgeführt werden.
    - Gruppieren Sie die Startkonfigurationen mit gleichem Startverhalten.

Wenn verschiedene Zielsysteme immer in einer vorher festgelegten Reihenfolge synchronisiert werden sollen, nutzen Sie Startfolgen, um die Synchronisation zu starten. In einer Startfolge können beliebige Startkonfigurationen aus verschiedenen Synchronisationsprojekten zusammengestellt und in eine Ausführungsreihenfolge gebracht werden. Ausführliche Informationen zu Startfolgen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Synchronisation auswerten

Die Ergebnisse der Synchronisation werden im Synchronisationsprotokoll zusammengefasst. Der Umfang des Synchronisationsprotokolls kann für jede Systemverbindung separat festgelegt werden. Der One Identity Manager stellt verschiedene Berichte bereit, in denen die Synchronisationsergebnisse nach verschiedenen Kriterien aufbereitet sind.

Um das Protokoll einer Synchronisation anzuzeigen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Protokolle**.
3. Klicken Sie in der Symbolleiste der Navigationsansicht .

   In der Navigationsansicht werden die Protokolle aller abgeschlossenen Synchronisationsläufe angezeigt.
4. Wählen Sie per Maus-Doppelklick das Protokoll, das angezeigt werden soll.

   Die Auswertung der Synchronisation wird als Bericht angezeigt. Sie können diesen Bericht speichern.

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

- Aktivieren Sie im Designer den Konfigurationsparameter **DPR | Journal | LifeTime** und tragen Sie die maximale Aufbewahrungszeit ein.

Nachbehandlung ausstehender Objekte

Objekte, die im Zielsystem nicht vorhanden sind, können bei der Synchronisation in den One Identity Manager als ausstehend gekennzeichnet werden. Damit kann verhindert werden, dass Objekte aufgrund einer fehlerhaften Datensituation oder einer fehlerhaften Synchronisationskonfiguration gelöscht werden.

Ausstehende Objekte

- können im One Identity Manager nicht bearbeitet werden,
- werden bei jeder weiteren Synchronisation ignoriert,
- werden bei der Vererbungsberechnung ignoriert.

Das heißt, sämtliche Mitgliedschaften und Zuweisungen bleiben solange erhalten, bis die ausstehenden Objekte nachbearbeitet wurden.

Führen Sie dafür einen Zielsystemabgleich durch.

Um die Nachbehandlung ausstehender Objekte zu ermöglichen

- Konfigurieren Sie den Zielsystemabgleich.

  Weitere Informationen finden Sie unter Zielsystemabgleich konfigurieren auf Seite 30.

Verwandte Themen

- Ausstehende Objekte nachbehandeln auf Seite 32
- Benutzer und Berechtigungen für die Synchronisation auf Seite 5

Zielsystemabgleich konfigurieren

Um ausstehende Objekte nachbehandeln zu können, erstellen Sie einen Zielsystemtyp. Weisen Sie die Tabellen, die durch die Synchronisation befüllt werden, diesem Zielsystemtyp zu. Legen Sie die Tabellen fest, für die ausstehende Objekte in der Nachbehandlung in das Zielsystem publiziert werden dürfen. Definieren Sie einen Prozess zum Publizieren der Objekte.

Um einen Zielsystemtyp zu erstellen

1. Wählen Sie im Manager die Kategorie **Datensynchronisation > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Zielsystemtyps.
4. Speichern Sie die Änderungen.

Für einen Zielsystemtyp erfassen Sie folgende Daten.

Tabelle 15: Stammdaten eines Zielsystemtyps

Eigenschaft	Beschreibung
Zielsystemtyp	Bezeichnung des Zielsystemtyps.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Anzeigename	Name des Zielsystemtyps zur Anzeige in den One Identity Manager-Werkzeugen.
Grenzüberschreitende Vererbung	Angabe zur Zuweisung und Vererbung von Gruppen und Systemberechtigungen an Benutzerkonten, wenn diese verschiedenen kundendefinierten Zielsystemen angehören. • Ist die Option aktiviert, können Gruppen und Systemberechtigungen an Benutzerkonten zugewiesen werden, die zum selben Zielsystem oder zu unterschiedlichen Zielsystemen gehören. Die Zielsysteme müssen zum selben Zielsystemtyp gehören. Für alle Zielsysteme eines Zielsystemtyps müssen die Einstellungen für die Spalte **Benutzerkonto enthält Mitgliedschaften** (`UNSRootB.UserContainsGroupList`) identisch sein. • Ist die Option deaktiviert, können Gruppen und Systemberechtigungen nur an Benutzerkonten desselben Zielsystems zugewiesen werden. HINWEIS: Ist die Option nicht gesetzt, kann der Zielsystemtyp zur einfachen Gruppierung der Zielsysteme verwendet werden.

Eigenschaft	Beschreibung
Anzeige im Regeleditor für Complianceregeln	Gibt an, ob der Zielsystemtyp im Regeleditor für Complianceregeln beim Erstellen von Regelbedingungen ausgewählt werden kann.
Textbaustein	Textbaustein, der zum Verketten der Texte im Regeleditor für Complianceregeln verwendet wird.
Alternative Konnektoren	Liste von Konnektoren, welche diesen Zielsystemtyp ebenfalls verarbeiten können.

Um Tabellen in den Zielsystemabgleich aufzunehmen

1. Wählen Sie im Manager die Kategorie **Datensynchronisation > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp.
3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Tabellen zu, für die Sie ausstehende Objekte behandeln möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die Tabellen, für die ausstehende Objekte in das Zielsystem publiziert werden dürfen und aktivieren Sie die Option **Publizierbar**.
8. Speichern Sie die Änderungen.

HINWEIS: Damit ausstehende Objekte in der Nachbehandlung publiziert werden können, muss der Konnektor schreibend auf das Zielsystem zugreifen können. Das heißt, an der Zielsystemverbindung ist die Option **Verbindung darf nur gelesen werden** deaktiviert.

Um ausstehende Objekte publizieren zu können

- Erstellen Sie für jede Tabelle, für die Sie ausstehende Objekte publizieren möchten, einen Prozess, der durch das Ereignis `HandleOutstanding` ausgelöst wird und der die Provisionierung der Objekte ausführt. Verwenden Sie die Prozessfunktion `AdHocProjection` der Prozesskomponente `ProjectorComponent`.

  Ausführliche Informationen zum Definieren von Prozessen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Ausstehende Objekte nachbehandeln

Um ausstehende Objekte nachzubearbeiten

1. Wählen Sie im Manager die Kategorie **Datensynchronisation > Zielsystemabgleich: <Zielsystemtyp>**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp zugewiesen sind.
2. Wählen Sie in der Navigationsansicht die Tabelle, für die Sie ausstehende Objekte nachbearbeiten möchten.

   Auf dem Formular werden alle Objekte angezeigt, die als ausstehend markiert sind.

   TIPP:

   Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

   1. Wählen Sie auf dem Formular für den Zielsystemabgleich das Objekt.
   2. Öffnen Sie das Kontextmenü und klicken Sie **Objekt anzeigen**.
3. Wählen Sie die Objekte, die Sie nachbearbeiten möchten. Mehrfachauswahl ist möglich.
4. Klicken Sie in der Formularsymbolleiste eins der folgenden Symbole, um die jeweilige Methode auszuführen.

Tabelle 16: Methoden zur Behandlung ausstehender Objekte

Symbol	Methode	Beschreibung
	Löschen	Das Objekt wird sofort in der One Identity Manager-Datenbank gelöscht. Eine Löschverzögerung wird nicht berücksichtigt. Indirekte Mitgliedschaften können nicht gelöscht werden.
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung **Ausstehend** wird für das Objekt entfernt. Es wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt. Voraussetzungen: • Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen. • Der Zielsystemkonnektor kann schreibend auf das Zielsystem zugreifen. • Ein kundenspezifischer Prozess zur

Symbol	Methode	Beschreibung
		Provisionierung der Objekte ist eingerichtet.
	Zurücksetzen	Die Markierung **Ausstehend** wird für das Objekt entfernt.

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

HINWEIS: Standardmäßig werden die ausgewählten Objekte parallel verarbeitet. Damit wird die Ausführung der ausgewählten Methode beschleunigt. Wenn bei der Verarbeitung ein Fehler auftritt, wird die Aktion abgebrochen und alle Änderungen werden rückgängig gemacht.

Um den Fehler zu lokalisieren, muss die Massenverarbeitung der Objekte deaktiviert werden. Die Objekte werden damit nacheinander verarbeitet. Das fehlerhafte Objekt wird in der Fehlermeldung benannt. Alle Änderungen, die bis zum Auftreten des Fehlers vorgenommen wurden, werden gespeichert.

Um die Massenverarbeitung zu deaktivieren

- Deaktivieren Sie in der Formularsymbolleiste das Symbol .

Verwandte Themen

- Zielsystemabgleich konfigurieren auf Seite 30
- Benutzer und Berechtigungen für die Synchronisation auf Seite 5

Provisionierung von Mitgliedschaften konfigurieren

Mitgliedschaften, beispielsweise von Benutzerkonten in Gruppen, werden in der One Identity Manager-Datenbank in Zuordnungstabellen gespeichert. Bei der Provisionierung von geänderten Mitgliedschaften werden möglicherweise Änderungen, die im Zielsystem vorgenommen wurden, überschrieben. Dieses Verhalten kann unter folgenden Bedingungen auftreten:

- Mitgliedschaften werden im Zielsystem in Form einer Liste als Eigenschaft eines Objekts gespeichert.

  Beispiele: Liste von Benutzerkonten in der Eigenschaft `Member` einer Gruppe - ODER - Liste von Profilen in der Eigenschaft `MemberOf` eines Benutzerkontos
- Änderungen von Mitgliedschaften sind in beiden verbundenen Systemen zulässig.
- Ein Provisionierungsworkflow und Provisionierungsprozesse sind eingerichtet.

Wird eine Mitgliedschaft im One Identity Manager geändert, wird standardmäßig die komplette Mitgliederliste in das Zielsystem übertragen. Mitgliedschaften, die zuvor im

Zielsystem hinzugefügt wurden, werden dabei entfernt; zuvor gelöschte Mitgliedschaften werden wieder eingefügt.

Um das zu verhindern, kann die Provisionierung so konfiguriert werden, dass nur die einzelne geänderte Mitgliedschaft in das Zielsystem provisioniert wird. Das entsprechende Verhalten wird für jede Zuordnungstabelle separat konfiguriert.

Um die Einzelprovisionierung von Mitgliedschaften zu ermöglichen

1. Wählen Sie im Manager die Kategorie **Datensynchronisation > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp.
3. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
4. Wählen Sie die Zuordnungstabellen, für die Sie die Einzelprovisionierung ermöglichen möchten. Mehrfachauswahl ist möglich.
5. Klicken Sie **Merge-Modus**.

   HINWEIS:

   - Die Option kann nur für Zuordnungstabellen aktiviert werden, deren Basistabelle eine Spalte `XDateSubItem` hat.
   - Zuordnungstabellen, die im Mapping in einer virtuellen Schemaeigenschaft zusammengefasst sind, müssen identisch markiert werden.

     Beispiel: `ADSAccountInADSGroup`, `ADSGroupInADSGroup` und `ADSMachineInADSGroup`
6. Speichern Sie die Änderungen.

Für jede Zuordnungstabelle, die so gekennzeichnet ist, werden Änderungen, die im One Identity Manager vorgenommen werden, in einer separaten Tabelle gespeichert. Dabei werden nur die neu eingefügten und gelöschten Zuordnungen verarbeitet. Bei der Provisionierung der Änderungen wird die Mitgliederliste im Zielsystem mit den Einträgen in dieser Tabelle abgeglichen. Damit wird nicht die gesamte Mitgliederliste überschrieben, sondern nur die einzelne geänderte Mitgliedschaft provisioniert.

HINWEIS: Bei einer Synchronisation wird immer die komplette Mitgliederliste aktualisiert. Dabei werden Objekte mit Änderungen, deren Provisionierung noch nicht abgeschlossen ist, nicht verarbeitet. Diese Objekte werden im Synchronisationsprotokoll aufgezeichnet.

Die Einzelprovisionierung von Mitgliedschaften kann durch eine Bedingung eingeschränkt werden. Wenn für eine Tabelle der Merge-Modus deaktiviert wird, dann wird auch die Bedingung gelöscht. Tabellen, bei denen die Bedingung bearbeitet oder gelöscht wurde, sind durch folgendes Symbol gekennzeichnet: . Die originale Bedingung kann jederzeit wiederhergestellt werden.

Um die originale Bedingung wiederherzustellen

1. Wählen Sie die Zuordnungstabelle, für welche Sie die Bedingung wiederherstellen möchten.

2. Klicken Sie mit der rechten Maustaste auf die gewählte Zeile und wählen Sie im Kontextmenü **Originalwerte wiederherstellen**.
3. Speichern Sie die Änderungen.

HINWEIS: Um in der Bedingung den Bezug zu den eingefügten oder gelöschten Zuordnungen herzustellen, nutzen Sie den Tabellenalias `i`.

Beispiel für eine Bedingung an der Zuordnungstabelle `UNSAccountBInUNSGroupB`:

```
exists (select top 1 1 from UNSGroupB g
     where g.UID_UNSGroupB = i.UID_UNSGroupB
     and <einschränkende Bedingung>)
```

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

Einzelobjektsynchronisation konfigurieren

Änderungen an einem einzelnen Objekt im Zielsystem können sofort in die One Identity Manager-Datenbank übertragen werden, ohne dass eine vollständige Synchronisation der Zielsystem-Umgebung gestartet werden muss. Die Einzelobjektsynchronisation kann nur für Objekte ausgeführt werden, die in der One Identity Manager-Datenbank bereits vorhanden sind. Es werden die Änderungen an den gemappten Objekteigenschaften übernommen. Ist das Objekt im Zielsystem nicht mehr vorhanden, wird es in der One Identity Manager-Datenbank gelöscht.

Voraussetzungen

- Es gibt einen Synchronisationsschritt, der die Änderungen am geänderten Objekt in den One Identity Manager einlesen kann.
- Die Tabelle, die das geänderte Objekt enthält, ist einem Zielsystemtyp zugeordnet.
- Für die Tabelle, die das geänderte Objekt enthält, ist der Pfad zum Basisobjekt der Synchronisation festgelegt.

Legen Sie die Tabellen fest, für welche Sie die Einzelobjektsynchronisation nutzen möchten, und konfigurieren Sie die Einzelobjektsynchronisation für diese Tabellen. Ausführliche Informationen dazu finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*, im Abschnitt *Kundenspezifische Tabellen in die Synchronisation einbeziehen*.

Um den Pfad zum Basisobjekt der Synchronisation für eine Tabelle festzulegen

1. Wählen Sie im Manager die Kategorie **Datensynchronisation > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp.

3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Tabelle zu, für die Sie die Einzelobjektsynchronisation nutzen möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die Tabelle und erfassen Sie den **Pfad zum Basisobjekt**.
    - Wenn für das Zielsystem ein konkretes Basisobjekt festgelegt ist, geben Sie den Pfad zum Basisobjekt in der ObjectWalker-Notation der VI.DB an.

      Beispiel: `FK(UID_GAPCustomer).XObjectKey`
    - Wenn für das Zielsystem kein konkretes Basisobjekt festgelegt ist, erfassen Sie den XOjectKey der Basistabelle.

      Beispiel: `<Key><T>DialogTable</T><P>RMB-T-Org</P></Key>`
8. Speichern Sie die Änderungen.

Datenfehler bei der Synchronisation ignorieren

Standardmäßig werden Objekte mit fehlerhaften Daten nicht synchronisiert. Beispielsweise wird ein Benutzerkonto nicht in die One Identity Manager-Datenbank eingelesen, wenn in der Benutzerkontentabelle das Formatierungskript einer Spalte, die eine E-Mail-Adresse enthält, ungültige Daten erkennt. Diese Objekte können synchronisiert werden, sobald die fehlerhaften Daten korrigiert wurden. In einzelnen Situationen kann es notwendig sein, solche Objekte dennoch zu synchronisieren und nur die fehlerhaften Objekteigenschaften zu ignorieren. Dieses Verhalten kann für die Synchronisation in den One Identity Manager konfiguriert werden.

Um Datenfehler bei der Synchronisation in den One Identity Manager zu ignorieren

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > One Identity Manager Verbindung**.
3. In der Ansicht **Allgemein** klicken Sie **Verbindung bearbeiten**.

   Der Systemverbindungsassistent wird gestartet.
4. Auf der Seite **Weitere Einstellungen** aktivieren Sie **Versuche Datenfehler zu ignorieren**.

   Diese Option ist nur wirksam, wenn am Synchronisationsworkflow **Bei Fehler fortsetzen** eingestellt ist.

   Fehler in Standardspalten, wie Primärschlüssel oder UID-Spalten, und Pflichteingabespalten können nicht ignoriert werden.
5. Speichern Sie die Änderungen.

WICHTIG: Wenn die Option aktiviert ist, versucht der One Identity Manager Speicherfehler zu ignorieren, die auf Datenfehler in einer einzelnen Spalte zurückgeführt werden können. Dabei wird die Datenänderung an der betroffenen Spalte verworfen und das Objekt anschließend neu gespeichert. Das beeinträchtigt die Performance und führt zu Datenverlust.

Aktivieren Sie die Option nur im Ausnahmefall, wenn eine Korrektur der fehlerhaften Daten vor der Synchronisation nicht möglich ist.

Fehlerbehebung

Ausführliche Informationen zur Fehlerbehebung bei der Synchronisation von Objekthierarchien finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Unterstützung bei der Analyse von Synchronisationsproblemen

Für die Analyse von Problemen während der Synchronisation, beispielsweise unzureichender Performance, kann ein Bericht erzeugt werden. Der Bericht enthält Informationen wie beispielsweise:

- Ergebnisse der Konsistenzprüfung
- Einstellungen zur Revisionsfilterung
- Verwendeter Scope
- Analyse des Synchronisationspuffers
- Zugriffszeiten auf die Objekte in der One Identity Manager-Datenbank und im Zielsystem

Um den Synchronisationsanalysebericht zu erstellen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie das Menü **Hilfe > Synchronisationsanalysebericht erstellen** und beantworten Sie die Sicherheitsabfrage mit **Ja**.

   Die Generierung des Berichts nimmt einige Zeit in Anspruch. Er wird in einem separaten Fenster angezeigt.
3. Drucken Sie den Bericht oder Speichern Sie ihn in einem der verschiedenen Ausgabeformate.

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

A

Anwendungsrolle 5

Anwendungsrolle für die Synchronisation 9

Ausstehendes Objekt 29

B

Basisobjekt 14, 35

D

Datenbankkonnektor
- generischer 4

E

Einzelobjektsynchronisation 35

J

Jobserver
- bearbeiten 11

M

Mitgliedschaft
- Änderung provisionieren 33

O

Objekt
- ausstehend 29, 32
- publizieren 32
- sofort löschen 32

P

Provisionierung
- Mitgliederliste 33

R

Remoteverbindungsserver 14

S

Schema
- aktualisieren 26
- Änderungen 26
- komprimieren 26

Synchronisation
- starten 28

Synchronisationsanalysebericht 38

Synchronisationskonfiguration 14, 17

Synchronisationsprotokoll 28

Synchronisationsserver 14
- installieren 11
- Jobserver 11
- konfigurieren 11

V

Variablenset 14

W

Workflow 14

Z

Zielsystemabgleich
    Tabellen zuweisen 30
Zielsystemtyp 30