One Identity Manager 8.2.1

Administrationshandbuch für die Anbindung von Cloud-Anwendungen

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. 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 Administrationshandbuch für die Anbindung von Cloud-Anwendungen
Aktualisiert - 27. April 2022, 03:24 Uhr
Version - 8.2.1

Inhalt

Abbilden von Cloud-Anwendungen im One Identity Manager 7

Architekturüberblick 8

One Identity Manager Benutzer für die Verwaltung von Cloud-Anwendungen 10

Synchronisieren von Cloud-Anwendungen über das Universal Cloud Interface 12

Einrichten der Initialsynchronisation mit einer Cloud-Anwendung 13

Benutzer und Berechtigungen für die Synchronisation mit einer Cloud-Anwendung 13

Einrichten des SCIM Synchronisationsservers 14

Systemanforderungen für den SCIM Synchronisationsserver 15

One Identity Manager Service mit SCIM Konnektor installieren 15

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Cloud-Anwendung 18

Benötigte Informationen für die Erstellung eines Synchronisationsprojektes 19

Initiales Synchronisationsprojekt für eine Cloud-Anwendung erstellen 21

Synchronisationsprotokoll konfigurieren 29

Anpassen einer Synchronisationskonfiguration 29

Synchronisation in die Cloud-Anwendung konfigurieren 31

Einstellungen der Systemverbindung zur Cloud-Anwendung ändern 31

Verbindungsparameter im Variablenset bearbeiten 32

Eigenschaften der Zielsystemverbindung bearbeiten 33

Schema aktualisieren 34

Beschleunigung der Synchronisation durch Revisionsfilterung 35

Provisionierung von Mitgliedschaften konfigurieren 36

Einzelobjektsynchronisation konfigurieren 38

Beschleunigung der Provisionierung und Einzelobjektsynchronisation 39

Synchronisation mit Überlagerungsdatei 40

Ausführen einer Synchronisation 42

Synchronisationen starten 42

Synchronisationsergebnisse anzeigen 43

Synchronisation deaktivieren 44

Einzelobjekte synchronisieren 45

Fehleranalyse 46
Datenfehler bei der Synchronisation ignorieren 47
Standardprofile an Benutzerkonten in Salesforce Anwendungen zuweisen 47

Provisionierung von Objektänderungen 49
Ablauf der Provisionierung 50
Anstehende Änderungen anzeigen 51
Aufbewahrungszeitraum für anstehende Änderungen 51
Manuelle Provisionierung konfigurieren 52

Verwalten von Provisionierungsvorgängen im Web Portal 54
Offene Provisionierungsvorgänge bearbeiten 55
Provisionierungsvorgänge einsehen und bearbeiten 56
Alle Provisionierungsvorgänge einsehen 56
Statistiken einsehen 57

Abbilden von Cloud-Objekten im One Identity Manager 58
Cloud-Anwendungen 58
Cloud-Anwendungen bearbeiten 59
Allgemeine Stammdaten für Cloud-Anwendungen 59
Alternative Spaltenbezeichnungen festlegen 61
Synchronisationsprojekt für eine Cloud-Anwendung bearbeiten 62
Containerstrukturen in Cloud-Anwendungen 62
Benutzerkonten in Cloud-Anwendungen 63
Benutzerkonten anzeigen 64
Allgemeine Stammdaten für Benutzerkonten in Cloud-Anwendungen 64
Logindaten für Benutzerkonten in Cloud-Anwendungen 65
Angaben zur Identifikation von Benutzerkonten in Cloud-Anwendungen 66
Kontaktinformationen für Benutzerkonten in Cloud-Anwendungen 66
Benutzerdefinierte Stammdaten für Benutzerkonten in Cloud-Anwendungen 67
Zugewiesene Gruppen und Systemberechtigungen anzeigen 67
Zugewiesene Berechtigungselemente anzeigen 68
Überblick über Benutzerkonten in Cloud-Anwendungen anzeigen 68
Gruppen und Systemberechtigungen in Cloud-Anwendungen 69
Typen von Systemberechtigungen in Cloud-Anwendungen 69
Gruppen in Cloud-Anwendungen 71
Allgemeine Stammdaten für Gruppen in Cloud-Anwendungen 72

Benutzerdefinierte Stammdaten für Gruppen in Cloud-Anwendungen 73
Zugewiesene Benutzerkonten anzeigen 73
Zugewiesene Gruppen anzeigen 73
Zugewiesene Berechtigungselemente anzeigen 74
Überblick über Gruppen in Cloud-Anwendungen anzeigen 74
Systemberechtigungen in Cloud-Anwendungen 75
Allgemeine Stammdaten für Systemberechtigungen in Cloud-Anwendungen 76
Benutzerdefinierte Stammdaten für Systemberechtigungen in Cloud-Anwendungen 77
Zugewiesene Benutzerkonten anzeigen 77
Zugewiesene Systemberechtigungen anzeigen 78
Überblick über Systemberechtigungen in Cloud-Anwendungen anzeigen 78
Berechtigungselemente in einer Cloud-Anwendung 79
Allgemeine Stammdaten für Berechtigungselemente in Cloud-Anwendungen 80
Benutzerdefinierte Stammdaten für Berechtigungselemente in Cloud-Anwendungen 80
Zugewiesene Benutzerkonten anzeigen 81
Zugewiesene Gruppen anzeigen 81
Überblick über Berechtigungselemente in Cloud-Anwendungen anzeigen 82

Basisdaten für die Verwaltung von Cloud-Anwendungen 83
Jobserver für cloud-spezifische Prozessverarbeitung 84
Jobserver für Cloud-Anwendungen bearbeiten 84
Allgemeine Stammdaten für Jobserver 85
Festlegen der Serverfunktionen 87
Cloud-Administratoren 88
Cloud-Operatoren 90
Cloud-Auditoren 92

Anhang: Standardprojektvorlage für Cloud-Anwendungen 94
Projektvorlage für SCIM-Umgebungen 94
Projektvorlage für One Identity Starling Connect-Umgebungen 95

Anhang: Verarbeitungsmethoden von Cloud-Systemobjekten 96

Anhang: Konfigurationsparameter für die Verwaltung von Cloud-Anwendungen 97

Über uns 98
Kontaktieren Sie uns 98

Technische Supportressourcen 98

Index **99**

Abbilden von Cloud-Anwendungen im One Identity Manager

Der One Identity Manager unterstützt die Umsetzung von Identity und Access Governance Anforderungen in IT-Umgebungen, die häufig eine Mischung aus traditionellen, intern gehosteten Applikationen und modernen Cloud-Anwendungen darstellen. Benutzer und Berechtigungen aus Cloud-Anwendungen können im One Identity Manager abgebildet werden.

Datenschutzrichtlinien, wie die Datenschutz-Grundverordnung, erfordern eine Abstimmung, welche Daten eines Mitarbeiters in Cloud-Anwendungen gespeichert werden dürfen. Bei entsprechender Konfiguration der Systemumgebung gewährleistet der One Identity Manager, dass Cloud-Anwendungen und deren verantwortliche Administratoren keinerlei Zugriff auf die Personenstammdaten sowie die Identity und Access Governance Prozesse erhalten. Aus diesem Grund werden Cloud-Anwendungen in zwei getrennten Modulen verwaltet, die bei Bedarf in getrennten Datenbanken installiert sein können.

Das Modul Universal Cloud Interface bildet die Schnittstelle, über die Benutzer und Berechtigungen aus Cloud-Anwendungen in eine One Identity Manager-Datenbank übertragen werden können. Hier wird die Synchronisation mit den Cloud-Anwendungen konfiguriert und ausgeführt. Jede Cloud-Anwendung wird als eigenes Basisobjekt im One Identity Manager abgebildet. Die Benutzerdaten werden als Benutzerkonten, Gruppen, Systemberechtigungen und Berechtigungselemente gespeichert und können in Containern organisiert werden. Sie können im One Identity Manager nicht bearbeitet werden. Eine Verbindung zu Identitäten (Personen) wird hier nicht hergestellt.

Im Modul Cloud Systems Management wird die Verbindung zu Identitäten hergestellt; Benutzerkonten, Gruppen, Systemberechtigungen und Berechtigungselemente können erstellt und bearbeitet werden. Per Synchronisation werden die Daten zwischen den Modulen Universal Cloud Interface und Cloud Systems Management ausgetauscht. Provisionierungsprozesse sorgen dafür, dass Änderungen an den Objekten aus dem Modul Cloud Systems Management in das Modul Universal Cloud Interface übertragen werden.

Für manche Cloud-Anwendungen kann (aus technischen Gründen) oder soll (aufgrund der zu geringen Änderungsmenge) keine automatisierte Schnittstelle zum Provisionieren von Änderungen aus dem Modul Universal Cloud Interface in die Cloud-Anwendung eingesetzt werden. In diesem Fall können die Änderungen manuell provisioniert werden.

Da im Modul Universal Cloud Interface nur die Daten gespeichert werden, die in den Cloud-Anwendungen verfügbar sein müssen, kann dieses Modul in einer separaten Datenbank

installiert werden. Diese Datenbank kann sich auch außerhalb der Unternehmensinfrastruktur befinden.

In Verbindung mit der Cloud-Lösung One Identity Starling Connect entsteht eine einfache und umfassende Lösung zur Integration von Cloud-Anwendungen und zur Abbildung der Anforderungen an hybride Lösungsszenarien.

Architekturüberblick

Für den Datenaustausch mit einer Cloud-Anwendung kennt der One Identity Manager zwei Vorgehen.

- Automatische Synchronisation und Provisionierung

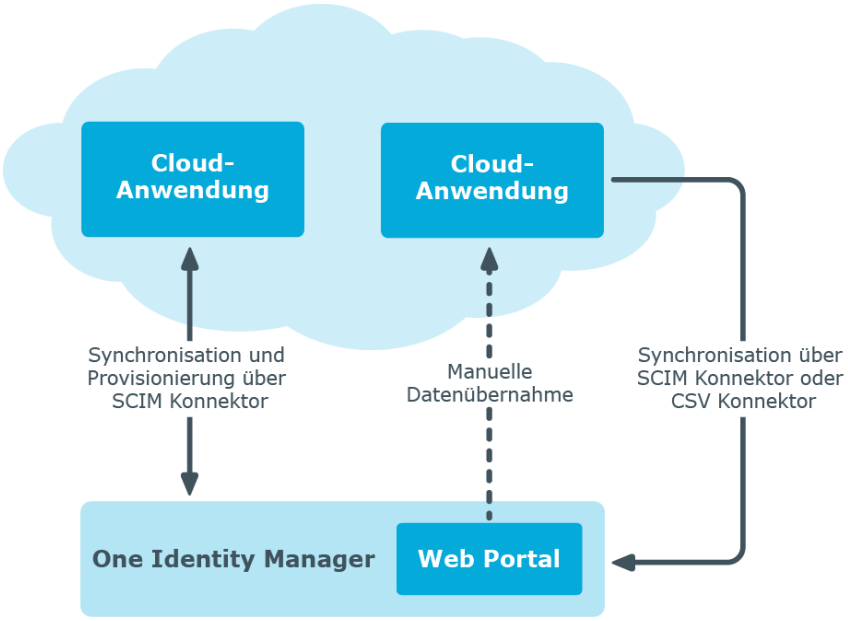
  Die Synchronisation einer Cloud-Anwendung mit der One Identity Manager-Datenbank und die Provisionierung von Objektänderungen aus der One Identity Manager-Datenbank in die Cloud-Anwendung übernimmt der SCIM Konnektor des One Identity Manager. Mit diesem Standardvorgehen ist sichergestellt, dass die Daten zwischen Zielsystem und Datenbank regelmäßig abgeglichen und damit konsistent gehalten werden.

- Manuelle Provisionierung

  Für manche Cloud-Anwendungen soll keine automatisierte Schnittstelle zum Provisionieren der Änderungen eingesetzt werden. Für solche Cloud-Anwendungen können die Änderungen manuell provisioniert werden. Für die Datenübernahme aus der Cloud-Anwendung in die One Identity Manager-Datenbank kann die Synchronisation mit dem SCIM Konnektor konfiguriert werden. Wenn der One Identity Manager auch keinen lesenden Zugriff auf die Cloud-Anwendung erhalten kann, können Sie den Datenaustausch beispielsweise über den CSV Konnektor einrichten.

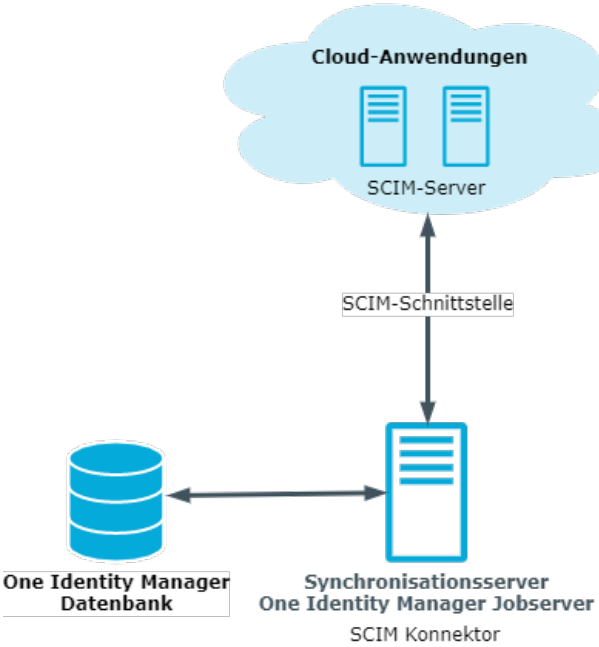
  Mit diesem Vorgehen tragen Sie das Risiko von inkonsistenten Daten und Datenverlust, wenn manuelle Prozesse nicht eingehalten werden. Dieses Vorgehen wird daher nicht empfohlen.

Abbildung 1: Architektur für die Synchronisation



Um auf die Cloud-Anwendungen zuzugreifen, wird auf einem Synchronisationsserver der SCIM Konnektor installiert. Der SCIM Konnektor kann mit Cloud-Anwendungen kommunizieren, welche die System for Cross-domain Identity Management (SCIM) Spezifikation verstehen. Der Synchronisationsserver sorgt für den Abgleich der Daten zwischen der One Identity Manager-Datenbank und der Cloud-Anwendung.

Abbildung 2: Topologie der Synchronisation



Detaillierte Informationen zum Thema

- Einrichten der Initialsynchronisation mit einer Cloud-Anwendung auf Seite 13
- Manuelle Provisionierung konfigurieren auf Seite 52

One Identity Manager Benutzer für die Verwaltung von Cloud-Anwendungen

In die Einrichtung und Verwaltung von Cloud-Anwendungen sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Cloud-Administratoren	Die Cloud-Administratoren müssen der Anwendungsrolle **Universal Cloud Interface | Administratoren** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Administrieren die Anwendungsrollen für das Universal Cloud Interface. • Richten bei Bedarf weitere Anwendungsrollen ein. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Cloud-Anwendung und One Identity Manager. • Bearbeiten im Manager die Cloud-Anwendungen. • Bearbeiten offene, manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken. • Erhalten im Web Portal und im Manager Informationen über die Cloud-Objekte.
Cloud-Operatoren	Die Cloud-Operatoren müssen der Anwendungsrolle **Universal Cloud Interface | Operatoren** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Bearbeiten offene manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken.
Cloud-Auditoren	Die Cloud-Auditoren müssen der Anwendungsrolle **Universal Cloud Interface | Auditoren** oder einer untergeordneten Anwendungsrolle zugewiesen sein.

Benutzer	Aufgaben
	Benutzer mit dieser Anwendungsrolle: • Sehen manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken.
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.

2

Synchronisieren von Cloud-Anwendungen über das Universal Cloud Interface

Der One Identity Manager unterstützt die Synchronisation mit Cloud-Anwendungen, welche die System for Cross-domain Identity Management (SCIM) Spezifikation in der Version 2.0 verstehen. Die Anforderungen von RFC 7643 (System for Cross-domain Identity Management: Core Schema) und RFC 7644 (System for Cross-domain Identity Management: Protocol) sind zu gewährleisten.

Informieren Sie sich hier:

- wie Sie die Synchronisation einrichten, um initial Daten aus einer Cloud-Anwendung in die One Identity Manager-Datenbank einzulesen,
- wie Sie eine Synchronisationskonfiguration anpassen, beispielsweise um verschiedene Cloud-Anwendungen mit ein und demselben Synchronisationsprojekt zu synchronisieren,
- wie Sie die Synchronisation starten und deaktivieren,
- wie Sie die Synchronisationsergebnisse auswerten.

TIPP: Bevor Sie die Synchronisation mit einer Cloud-Anwendung einrichten, machen Sie sich mit dem Synchronization Editor vertraut. Ausführliche Informationen über dieses Werkzeug finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Detaillierte Informationen zum Thema

- Einrichten der Initialsynchronisation mit einer Cloud-Anwendung auf Seite 13
- Anpassen einer Synchronisationskonfiguration auf Seite 29
- Ausführen einer Synchronisation auf Seite 42
- Fehleranalyse auf Seite 46
- Verarbeitungsmethoden von Cloud-Systemobjekten auf Seite 96

Einrichten der Initialsynchronisation mit einer Cloud-Anwendung

Der One Identity Manager stellt Projektvorlagen bereit, mit denen Sie die Synchronisation von Cloud-Anwendungen einrichten können. Nutzen Sie diese Projektvorlagen, um Synchronisationsprojekte zu erstellen, mit denen Sie Daten aus einer Cloud-Anwendung in Ihre One Identity Manager-Datenbank einlesen. Zusätzlich werden die notwendigen Prozesse angelegt, über die Änderungen an Zielsystemobjekten aus der One Identity Manager-Datenbank in das Zielsystem provisioniert werden.

Um die Objekte einer Cloud-Anwendung initial in die One Identity Manager-Datenbank einzulesen

1. Stellen Sie einen Benutzer für den Zugriff auf die Cloud-Anwendung mit ausreichenden Berechtigungen bereit.
2. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
3. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Detaillierte Informationen zum Thema

- Benutzer und Berechtigungen für die Synchronisation mit einer Cloud-Anwendung auf Seite 13
- Einrichten des SCIM Synchronisationsservers auf Seite 14
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Cloud-Anwendung auf Seite 18
- Standardprojektvorlage für Cloud-Anwendungen auf Seite 94

Benutzer und Berechtigungen für die Synchronisation mit einer Cloud-Anwendung

Bei der Synchronisation des One Identity Manager mit einer Cloud-Anwendung spielen folgende Benutzer eine Rolle.

Tabelle 2: Benutzer für die Synchronisation

Benutzer	Berechtigungen
Benutzerkonto des One Identity Manager Service	Das Benutzerkonto für den One Identity Manager Service benötigt die Benutzerrechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Verzeichnisse und Dateien anlegen und bearbeiten.

Benutzer	Berechtigungen
	Das Benutzerkonto muss der Gruppe **Domänen-Benutzer** angehören. Das Benutzerkonto benötigt das erweiterte Benutzerrecht **Anmelden als Dienst**. Das Benutzerkonto benötigt Berechtigungen für den internen Webservice. HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so können Sie die Berechtigungen für den internen Webservice über folgenden Kommandozeilenaufruf vergeben: `netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"` Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis. In der Standardinstallation wird der One Identity Manager installiert unter: • `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen) • `%ProgramFiles%\One Identity` (auf 64-Bit Betriebssystemen)
Sicherheitstoken oder Benutzer für den Zugriff auf die Cloud-Anwendung	Sicherheitstoken oder Benutzername und Kennwort, mit dem die Authentifizierung an der Cloud-Anwendung möglich ist.
Benutzer für den Zugriff auf die One Identity Manager-Datenbank	Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer **Synchronization** bereitgestellt.

Einrichten des SCIM Synchronisationsservers

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 SCIM Konnektor installiert werden.

Detaillierte Informationen zum Thema

- Systemanforderungen für den SCIM Synchronisationsserver auf Seite 15
- One Identity Manager Service mit SCIM Konnektor installieren auf Seite 15

Systemanforderungen für den SCIM Synchronisationsserver

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

- Windows Betriebssystem

  Unterstützt werden die Versionen:

  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
- Microsoft .NET Framework Version 4.7.2 oder höher

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.

One Identity Manager Service mit SCIM Konnektor installieren

Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem SCIM Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein.

Tabelle 3: Eigenschaften des Jobservers

Eigenschaft	Wert
Serverfunktion	SCIM Konnektor
Maschinenrolle	Server | Jobserver | SCIM

HINWEIS: Wenn mehrere gleichartige Zielsystemumgebungen über den selben Synchronisationsserver synchronisiert werden sollen, ist es aus Performancegründen günstig, für jedes einzelne Zielsystem einen eigenen Jobserver einzurichten. Dadurch wird ein unnötiger Wechsel der Verbindungen zum Zielsystem vermieden, da stets nur gleichartige Aufträge von einem Jobserver zu verarbeiten sind (Nachnutzung bestehender Verbindungen).

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 **SCIM**.
5. Auf der Seite **Serverfunktionen** wählen Sie **SCIM 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:
     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 für die initiale Synchronisation einer Cloud-Anwendung

Verwenden Sie den Synchronization Editor, um die Synchronisation zwischen One Identity Manager-Datenbank und Cloud-Anwendung einzurichten. Nachfolgend sind die Schritte für die initiale Einrichtung eines Synchronisationsprojektes beschrieben. Ausführliche Informationen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

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.

Detaillierte Informationen zum Thema

- Benötigte Informationen für die Erstellung eines Synchronisationsprojektes auf Seite 19
- Initiales Synchronisationsprojekt für eine Cloud-Anwendung erstellen auf Seite 21

Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

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

HINWEIS: Beachten Sie bei der Konfiguration, dass für Teile der URL gegebenenfalls die Groß-/Kleinschreibung beachtet werden muss.

Tabelle 4: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
URL des SCIM-Servers	URL, über die der Server erreicht werden kann, der die SCIM-Schnittstelle bereitstellt. Die URL muss das genutzte Übertragungsprotokoll enthalten.
Port	Port für den Zugriff auf die Cloud-Anwendung.
URI des Dienstes	URI, unter welchem der SCIM-Dienst erreichbar ist.
Authentifizierungsendpunkt/URL	URI, unter welchem die Authentifizierung möglich ist. Wird für die Authentifizierung ein anderer Server oder eine andere Basis-URL verwendet, ist hier die vollständige URL anzugeben.
Authentifizierungsart	Zulässige Authentifizierungsart für die Anmeldung an der Cloud-Anwendung.
Benutzername und Kennwort	Benutzername und Kennwort für die Anmeldung an der Cloud-Anwendung mit den Authentifizierungsarten **Basis-Authentifizierung**, **OAuth-Authentifizierung** und **Ausgehandelte Authentifizierung**.
Sicherheitstoken	Sicherheitstoken für die Anmeldung an der Cloud-Anwendung mit der Authentifizierungsart **OAuth-Authentifizierung**.
Applikations-/Client-ID	Applikations-/Client-ID mit der die Cloud-Anwendung beim Sicherheitstokendienst registriert ist. Wird für die Anmeldung mit der Authentifizierungsart **OAuth-Authentifizierung** benötigt.
Authentifizierungstoken	Authentifizierungstoken für die Anmeldung an der Cloud-Anwendung mit der Authentifizierungsart **Bearer-Authentifizierung**.
SCIM-Endpunkte	URIs oder URLs zu den Endpunkten für den Zugriff auf die Schemainformationen, Ressourceninformationen und Service-Provider-Informationen der Cloud-Anwendung.

Angaben	Erläuterungen
Zeitzone des SCIM Servers	Zeitzone, auf deren Basis der SCIM Provider Zeitinformationen bereitstellt.
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. Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem SCIM Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften. • Serverfunktion: **SCIM Konnektor** • Maschinenrolle: **Server/Jobserver/SCIM** Weitere Informationen finden Sie unter Systemanforderungen für den SCIM Synchronisationsserver auf Seite 15.
Verbindungsdaten zur One Identity Manager-Datenbank	• Datenbankserver • Name der Datenbank • SQL Server Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung verwendet wird Die Verwendung der integrierten Windows-Authentifizierung wird nicht empfohlen. Sollten Sie das 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

Angaben	Erläuterungen
	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 • SCIM Konnektor ist installiert Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt. Ausführliche Informationen zum Herstellen einer Remoteverbindung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Initiales Synchronisationsprojekt für eine Cloud-Anwendung erstellen

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.

HINWEIS: Pro Zielsystem und genutzter Standardprojektvorlage kann genau ein Synchronisationsprojekt erstellt werden.

Um ein initiales Synchronisationsprojekt für eine Cloud-Anwendung 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 **Zielsystemtyp SCIM Schnittstelle** und klicken Sie **Starten**.

   Der Projektassistent des Synchronization Editors 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.
4. Auf der Seite **Verbindungsdaten** erfassen Sie die Verbindungsparameter, die der SCIM Konnektor zur Anmeldung an der Cloud-Anwendung benötigt.

Tabelle 5: Serverparameter

Eigenschaft	Beschreibung
URL des Servers	URL, über die der Server erreicht werden kann. Geben Sie auch das genutzte Übertragungsprotokoll an.
Port	Port für den Zugriff auf die Cloud-Anwendung. Wenn Standardports (HTTP:80, HTTPS:443) verwendet werden, kann dieses Feld frei bleiben.
URI des Dienstes	URI, unter welchem der SCIM-Dienst erreichbar ist. Es wird nur der Teil der URL benötigt, der von allen aufzurufenden Endpunkten gemeinsam verwendet wird. Der SCIM Konnektor setzt die URL aus der Server-URL, dem Port und dem URI zusammen. Beispiel: Wenn die komplette URL https://identities.example.net:8080/scim/v2 lautet, dann ist hier als URI **scim/v2** einzugeben.

Tabelle 6: Authentifizierungsart

Eigenschaft	Beschreibung
Basis-Authentifizierung	Authentifizierung über Benutzername und Kennwort.
OAuth-Authentifizierung	Authentifizierung über das OAuth-Protokoll 2.0.
Ausgehandelte Authentifizierung (NTLM/Kerberos)	Authentifizierung mittels Windows Authentifizierungsmethoden wie NTLM oder Kerberos.
Clientzertifikat benutzen	Authentifizierung mittels Clientzertifikat.
Bearer-Authentifizierung	Authentifizierung über einen vorhandenen Bearer-Token.

Eigenschaft	Beschreibung
Authentifizierungsendpunkt/ URL	URI, unter welchem die Authentifizierung möglich ist. Es wird nur der Teil der URL benötigt, der dem gemeinsamen Teil hinzuzufügen ist, um den Authentifizierungsendpunkt zu erreichen. Wird für die Authentifizierung ein anderer Server oder eine andere Basis-URL verwendet, ist hier die vollständige URL anzugeben. Beispiel: Wenn der komplette URI https://identities.example.net:8080/scim/v2/auth/token lautet, dann ist hier **auth/token** einzugeben. Wenn die Basis-URL oder der Server verschieden zur Resourcen-URL ist, dann ist hier die komplette URL anzugeben, beispielsweise **https://authserver.example.net/token**. Bei allen Authentifizierungsverfahren, außer OAuth-Authentifizierung, wird diese URL nur zum Testen der Verbindung genutzt.

- Auf der Seite **Basis-Authentifizierung** erfassen Sie Benutzername und Kennwort für die Authentifizierungsart **Basis-Authentifizierung**.
- Auf der Seite **OAuth-Authentifizierung** geben Sie den Sicherheitstoken für die Authentifizierungsart **OAuth-Authentifizierung** an und wählen Sie den Zugangstyp.

Tabelle 7: Eigenschaften der OAuth-Authentifizierung

Eigenschaft	Beschreibung
Sicherheitstoken	Sicherheitstoken für die Anmeldung an der Cloud-Anwendung. Wenn der Sicherheitstoken nicht bekannt ist, erfassen Sie Benutzername und Kennwort.
Benutzername und Kennwort	Benutzername und Kennwort für die Anmeldung an der Cloud-Anwendung, wenn der Sicherheitstoken nicht bekannt ist.
Applikations-/Client-ID	Applikations-/Client-ID mit der die Cloud-Anwendung beim Sicherheitstokendienst registriert ist.
Zugangstyp	Zugangstyp für die Anmeldung an der Cloud-Anwendung mit der Authentifizierungsart **OAuth-Authentifizierung**. Aktivieren Sie **Client-Berechtigung** oder **Kennwort-Berechtigung**.

Eigenschaft	Beschreibung
Scope	Scope-Parameter, der für die Anmeldung am Zielsystem gültig ist. Wenn mehrere Parameter gültig sind, trennen Sie diese durch Leerzeichen. Ob ein Scope für die Anmeldung erforderlich ist und welche Scope-Parameter gültig sind, ist abhängig vom Service-Provider.

- Auf der Seite **Ausgehandelte Authentifizierung** erfassen Sie Benutzername und Kennwort für die Authentifizierungsart **Ausgehandelte Authentifizierung (NTLM/Kerberos)**.
- Auf der Seite **Clientzertifikat** wählen Sie das zu nutzende Zertifikat. Zertifikate können aus `*.CER` oder `*.PFX` - Dateien in den Zertifikatsspeicher des lokalen Computers importiert werden.
- Auf der Seite **Bearer-Authentifizierung** geben Sie das vom Zielsystem berechnete Bearer-Token an.

5. Auf der Seite **Verbindungseinstellungen prüfen** können Sie die erfassten Verbindungsdaten testen. Klicken Sie **Test**.

   Der One Identity Manager versucht eine Verbindung zur Cloud-Anwendung aufzubauen.

   > TIPP: Der One Identity Manager speichert das Testergebnis. Wenn die Seite erneut aufgerufen wird und die Verbindungsdaten nicht geändert wurden, wird das gespeicherte Testergebnis angezeigt. War dieser Test erfolgreich, müssen die Verbindungsdaten nicht erneut getestet werden.

6. Auf der Seite **Endpunktkonfiguration** erfassen Sie die URIs zu den SCIM-Endpunkten. Wenn keine URIs angegeben sind, wird der SCIM-Standard verwendet.

   Tabelle 8: Endpunktkonfiguration

Eigenschaft	Beschreibung
Schema	Endpunkt für den Zugriff auf die Schemainformationen der Cloud-Anwendung.
Ressourcen	Endpunkt für den Zugriff auf die Ressourceninformationen der Cloud-Anwendung, beispielsweise Gruppen oder Benutzerkonten.
Unterstützte Service-Optionen	Endpunkt für den Zugriff auf die Service-Provider-Informationen der Cloud-Anwendung.

   - Um die Verbindung zu den angegebenen Endpunkten zu testen, klicken Sie **Test**.

TIPP: Der One Identity Manager speichert das Testergebnis. Wenn die Seite erneut aufgerufen wird und die Endpunktkonfiguration nicht geändert wurde, wird das gespeicherte Testergebnis angezeigt.

7. Auf der Seite **Optimierungen** können Sie zusätzliche Einstellungen zur Optimierung der Synchronisationsperformance vornehmen.

Tabelle 9: Einstellungen zur Performanceoptimierung

Eigenschaft	Beschreibung
Lokalen Cache verwenden	Gibt an, ob der lokale Cache des SCIM Konnektors genutzt werden soll. Der lokale Cache wird genutzt, um die Synchronisation zu beschleunigen. Bei einer Vollsynchronisation werden die Zugriffe auf die Cloud-Anwendung minimiert. Bei der Provisionierung wird die Option ignoriert. Die Option ist standardmäßig aktiviert. Bei Synchronisationen mit Revisionsfilterung ist die Verwendung des Cache nicht sinnvoll. Wenn das Zielsystem die Revisionsfilterung unterstützt, deaktivieren Sie die Option nach der initialen Synchronisation.
Max. Anzahl paralleler Anfragen	Anzahl der Datenanfragen am Zielsystem, die maximal gleichzeitig ausgeführt werden können. Erfassen Sie einen Wert zwischen **1** und **32**.
HTTP Keep-Alive nutzen	Gibt an, ob HTTP-Verbindungen aufrecht erhalten werden sollen. Wenn die Option deaktiviert ist, werden Verbindungen sofort geschlossen und können nicht für weitere Anfragen genutzt werden.

8. Auf der Seite **Zeitzone des SCIM-Servers** geben Sie die Zeitzone an, auf deren Basis der SCIM-Provider Zeitinformationen bereitstellt.

   Wenn der SCIM-Provider Zeitangaben übermittelt, die keine Zeitzoneninformation enthalten, wird die hier angegebene Zeitzone verwendet.

9. Auf der Seite **Auswahl des Zielprodukts** kann das Verhalten des SCIM Konnektors auf die Eigenheiten spezieller Zielprodukte angepasst werden, beispielsweise auf HTTP-Request-Formate.

Tabelle 10: Zielprodukte

Eigenschaft	Beschreibung
SCIM Core V 2.0	Produkt für die Synchronisation einer Standard-SCIM-Umgebung.
One Identity Starling Connect	Produkt für die Synchronisation einer One Identity Starling Connect-Umgebung

10. Auf der Seite **Anzeigename** erfassen Sie einen eindeutigen Anzeigenamen für die Cloud-Anwendung.

    Über den Anzeigenamen können Sie die Cloud-Anwendungen in den One Identity Manager Werkzeugen unterscheiden. Er kann nachträglich nicht mehr geändert werden.

11. Auf der letzten Seite des Systemverbindungsassistenten können Sie die Verbindungsdaten lokal speichern und die Konfiguration der Systemverbindung abschließen.

    - Aktivieren Sie die Option **Verbindung auf dem Computer 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**.

12. 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.

13. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.

14. Auf der Seite **Projektvorlage auswählen** wählen Sie eine Projektvorlage, mit der die Synchronisationskonfiguration erstellt werden soll.

Tabelle 11: Standardprojektvorlagen

Projektvorlage	Beschreibung
SCIM Synchronisation	Verwenden Sie diese Projektvorlage für die initiale Einrichtung des Synchronisationsprojektes für die Synchronisation einer System for Cross-domain Identity Management-Umgebung.
Synchronisation einer One Identity Starling Connect-Umgebung	Verwenden Sie diese Projektvorlage für die initiale Einrichtung des Synchronisationsprojektes für die Synchronisation einer SCIM-Umgebung über die One Identity Starling Connect-Infrastruktur.

HINWEIS: 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.

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

Tabelle 12: Zielsystemzugriff festlegen

Option	Bedeutung
Das Zielsystem soll nur eingelesen werden.	Gibt an, 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.	Gibt an, 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.

16. 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.

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

17. 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**.

    - 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.

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

Detaillierte Informationen zum Thema

- Systemanforderungen für den SCIM Synchronisationsserver auf Seite 15
- Benutzer und Berechtigungen für die Synchronisation mit einer Cloud-Anwendung auf Seite 13
- Synchronisationsergebnisse anzeigen auf Seite 43
- Anpassen einer Synchronisationskonfiguration auf Seite 29
- Beschleunigung der Synchronisation durch Revisionsfilterung auf Seite 35
- Synchronisation mit Überlagerungsdatei auf Seite 40
- Standardprojektvorlage für Cloud-Anwendungen auf Seite 94

Synchronisationsprotokoll konfigurieren

Im Synchronisationsprotokoll werden alle Informationen, Hinweise, Warnungen und Fehler, die bei der Synchronisation auftreten, aufgezeichnet. Welche Informationen aufgezeichnet werden sollen, kann für jede Systemverbindung separat konfiguriert werden.

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

1. Um das Synchronisationsprotokoll für die Zielsystemverbindung zu konfigurieren, wählen Sie im Synchronization Editor die Kategorie **Konfiguration > Zielsystem**.

   - ODER -

   Um das Synchronisationsprotokoll für die Datenbankverbindung zu konfigurieren, wählen Sie im Synchronization Editor die Kategorie **Konfiguration > One Identity Manager Verbindung**.
2. Wählen Sie den Bereich **Allgemein** und klicken Sie **Konfigurieren**.
3. Wählen Sie den Bereich **Synchronisationsprotokoll** und aktivieren Sie **Synchronisationsprotokoll erstellen**.
4. Aktivieren Sie die zu protokollierenden Daten.

   HINWEIS: Einige Inhalte erzeugen besonders viele Protokolldaten. Das Synchronisationsprotokoll soll nur die für Fehleranalysen und weitere Auswertungen notwendigen Daten enthalten.
5. Klicken Sie **OK**.

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.

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 43

Anpassen einer Synchronisationskonfiguration

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation einer Cloud-Anwendung eingerichtet. Mit diesem Synchronisationsprojekt können Sie Objekte aus der Cloud-Anwendung in die One Identity Manager-Datenbank einlesen. Wenn Sie Benutzerkonten und ihre Berechtigungen mit dem One Identity Manager verwalten, werden Änderungen in die Cloud-Anwendung provisioniert.

Um die Datenbank und die Cloud-Anwendung regelmäßig abzugleichen und Änderungen zu synchronisieren, passen Sie die Synchronisationskonfiguration an.

- Um bei der Synchronisation den One Identity Manager als primäres System zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um festzulegen, welche Cloud-Objekte und Datenbankobjekte bei der Synchronisation behandelt werden, bearbeiten Sie den Scope der Zielsystemverbindung und der One Identity Manager-Datenbankverbindung. Um Dateninkonsistenzen zu vermeiden, definieren Sie in beiden Systemen den gleichen Scope. Ist kein Scope definiert, werden alle Objekte synchronisiert.
- Um allgemeingültige Synchronisationskonfigurationen zu erstellen, die erst beim Start der Synchronisation die notwendigen Informationen über die zu synchronisierenden Objekte erhalten, können Variablen eingesetzt werden. Variablen können beispielsweise in den Basisobjekten, den Schemaklassen oder den Verarbeitungsmethoden eingesetzt werden.
- Wenn sich das One Identity Manager Schema oder das Zielsystemschema geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.
- Um zusätzliche Schemaeigenschaften zu synchronisieren, aktualisieren Sie das Schema im Synchronisationsprojekt. Nehmen Sie die Schemaerweiterungen in das Mapping auf.
- Um Daten zu synchronisieren, für die keine Schematypen im Konnektorschema angelegt sind, legen Sie eigene Schematypen an. Nehmen Sie die Schemaerweiterungen in das Mapping auf.
- Wenn der SCIM Konnektor das Schema nicht ermitteln kann, übergeben Sie ihm die Schemainformationen mittels Überlagerungsdateien.
- Wenn das Schema der Cloud-Anwendung durch keine Standard-Projektvorlage ausreichend abgebildet werden kann, passen Sie die Synchronisationskonfiguration an. Definieren Sie dabei, wie die Systemberechtigungen im One Identity Manager Schema abgebildet werden. Stellen Sie sicher, dass bei der Einrichtung der Synchronisation das Basisobjekt für die Cloud-Anwendung (`UCIRoot`) in der Datenbank angelegt wird und die Eigenschaften **Typen der verwendeten Systemberechtigungen** (`GroupUsageMask`) und **Benutzerkonto enthält Mitgliedschaften** (`UserContainsGroupList`) korrekt gesetzt werden.

Ausführliche Informationen zum Konfigurieren einer Synchronisation finden Sie im One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation.

Detaillierte Informationen zum Thema

- Synchronisation in die Cloud-Anwendung konfigurieren auf Seite 31
- Einstellungen der Systemverbindung zur Cloud-Anwendung ändern auf Seite 31
- Schema aktualisieren auf Seite 34
- Synchronisation mit Überlagerungsdatei auf Seite 40
- Typen von Systemberechtigungen in Cloud-Anwendungen auf Seite 69

Synchronisation in die Cloud-Anwendung konfigurieren

Das Synchronisationsprojekt für die initiale Synchronisation stellt je einen Workflow zum initialen Einlesen der Zielsystemobjekte (Initial Synchronization) und für die Provisionierung von Objektänderungen aus der One Identity Manager-Datenbank in das Zielsystem (Provisioning) bereit. Das Synchronisationsprojekt für die initiale Synchronisation stellt je einen Workflow zum initialen Einlesen der Cloud-Objekte (Initial Synchronization) und für die Provisionierung von Objektänderungen aus der One Identity Manager-Datenbank in das Zielsystem (Provisioning) bereit. Um bei der Synchronisation den One Identity Manager als primäres System zu nutzen, benötigen Sie zusätzlich einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.

Um eine Synchronisationskonfiguration für die Synchronisation in die Cloud-Anwendung zu erstellen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Prüfen Sie, ob die bestehenden Mappings für die Synchronisation in die Cloud-Anwendung genutzt werden können. Erstellen Sie bei Bedarf neue Mappings.
3. Erstellen Sie mit dem Workflowassistenten einen neuen Workflow.

   Es wird ein Workflow mit der Synchronisationsrichtung **In das Zielsystem** angelegt.
4. Erstellen Sie eine neue Startkonfiguration. Nutzen Sie dabei den neu angelegten Workflow.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

Einstellungen der Systemverbindung zur Cloud-Anwendung ändern

Beim Einrichten der initialen Synchronisation werden für die Eigenschaften der Systemverbindung Standardwerte gesetzt. Diese Standardwerte können angepasst werden. Dafür gibt es zwei Wege:

a. Legen Sie ein spezialisiertes Variablenset an und ändern Sie die Werte der betroffenen Variablen.

   Die Standardwerte bleiben im Standardvariablenset erhalten. Die Variablen können jederzeit auf die Standardwerte zurückgesetzt werden. (Empfohlenes Vorgehen)

b. Bearbeiten Sie die Zielsystemverbindung mit dem Systemverbindungsassistenten und ändern Sie die betroffenen Werte.

Der Systemverbindungsassistent liefert zusätzliche Erläuterungen zu den Einstellungen. Die Standardwerte können nur unter bestimmten Voraussetzungen wiederhergestellt werden.

Detaillierte Informationen zum Thema

- Verbindungsparameter im Variablenset bearbeiten auf Seite 32
- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 33

Verbindungsparameter im Variablenset bearbeiten

Die Verbindungsparameter wurden beim Einrichten der Synchronisation als Variablen im Standardvariablenset gespeichert. Sie können die Werte dieser Variablen in einem spezialisierten Variablenset Ihren Erfordernissen anpassen und dieses Variablenset einer Startkonfiguration und einem Basisobjekt zuordnen. Damit haben Sie jederzeit die Möglichkeit, erneut die Standardwerte aus dem Standardvariablenset zu nutzen.

HINWEIS: Um die Datenkonsistenz in den angebundenen Zielsystemen zu bewahren, stellen Sie sicher, dass die Startkonfiguration für die Synchronisation und das Basisobjekt für die Provisionierung dasselbe Variablenset verwenden.

Um die Verbindungsparameter in einem spezialisierten Variablenset anzupassen

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

   Einige Verbindungsparameter können hier in Variablen umgewandelt werden. Für andere sind bereits Variablen angelegt.
4. Wählen Sie einen Parameter und klicken Sie **Umwandeln**.
5. Wählen Sie die Kategorie **Konfiguration > Variablen**.

   Im unteren Bereich der Dokumentenansicht werden alle spezialisierten Variablensets angezeigt.
6. Wählen Sie ein spezialisiertes Variablenset oder klicken Sie in der Symbolleiste der Variablensetansicht .
   - Um das Variablenset umzubenennen, markieren Sie das Variablenset und klicken Sie in der Symbolleiste der Variablensetansicht . Erfassen Sie einen Namen für das Variablenset.
7. Wählen Sie die zuvor angelegten Variablen und erfassen Sie neue Werte.
8. Wählen Sie die Kategorie **Konfiguration > Startkonfigurationen**.
9. Wählen Sie eine Startkonfiguration und klicken Sie **Bearbeiten**.

10. Wählen Sie den Tabreiter **Allgemein**.
11. Ordnen Sie im Eingabefeld **Variablenset** das spezialisierte Variablenset zu.
12. Wählen Sie die Kategorie **Konfiguration > Basisobjekte**.
13. Wählen Sie ein Basisobjekt und klicken Sie .

    - ODER -

    Klicken Sie , um ein neues Basisobjekt anzulegen.
14. Ordnen Sie im Eingabefeld **Variablenset** das spezialisierte Variablenset zu.
15. Speichern Sie die Änderungen.

Ausführliche Informationen zur Anwendung von Variablen und Variablensets, zum Wiederherstellen der Standardwerte und zum Anlegen von Basisobjekten finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 33

Eigenschaften der Zielsystemverbindung bearbeiten

Die Verbindungsparameter können auch mit dem Systemverbindungsassistenten geändert werden. Wenn für die Einstellungen Variablen definiert sind, werden die Änderungen in das aktive Variablenset übernommen.

HINWEIS: Unter folgenden Umständen können die Standardwerte nicht wiederhergestellt werden:

- Die Verbindungsparameter sind nicht als Variablen hinterlegt.
- Das Standardvariablenset ist als aktives Variablenset ausgewählt.

In beiden Fällen überschreibt der Systemverbindungsassistent die Standardwerte. Sie können später nicht wiederhergestellt werden.

Um die Verbindungsparameter mit dem Systemverbindungsassistenten zu bearbeiten

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie in der Symbolleiste das aktive Variablenset, das für die Verbindung zum Zielsystem verwendet werden soll.

   HINWEIS: Ist das Standardvariablenset ausgewählt, werden die Standardwerte überschrieben und können später nicht wiederhergestellt werden.
3. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
4. Klicken Sie **Verbindung bearbeiten**.

   Der Systemverbindungsassistent wird gestartet.

5. Folgen Sie den Anweisungen des Systemverbindungsassistenten und ändern Sie die gewünschten Eigenschaften.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Verbindungsparameter im Variablenset bearbeiten auf Seite 32

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.

Beschleunigung der Synchronisation durch Revisionsfilterung

Beim Start der Synchronisation werden alle zu synchronisierenden Objekte geladen. Ein Teil dieser Objekte wurde gegebenenfalls seit der letzten Synchronisation nicht geändert und muss daher bei der Synchronisation nicht verarbeitet werden. Indem nur solche Objekte geladen werden, die sich seit der letzten Synchronisation geändert haben, kann die Synchronisation beschleunigt werden. Zur Beschleunigung der Synchronisation nutzt der One Identity Manager die Revisionsfilterung.

Der SCIM Konnektor unterstützt die Revisionsfilterung. Als Revisionszähler wird das Datum der letzten Änderung der Cloud-Objekte genutzt. Jede Synchronisation speichert ihr letztes Ausführungsdatum als Revision in der One Identity Manager-Datenbank (Tabelle `DPRRevisionStore`, Spalte `Value`). Dieser Wert wird als Vergleichswert für die Revisionsfilterung bei der nächsten Synchronisation mit dem selben Workflow genutzt. Bei der Synchronisation mit diesem Workflow wird das Änderungsdatum der Cloud-Objekte mit der in der One Identity Manager-Datenbank gespeicherten Revision verglichen. Es werden nur noch die Objekte aus der Cloud-Anwendung gelesen, die sich seit diesem Datum verändert haben.

Die Revision wird zu Beginn einer Synchronisation ermittelt. Objekte, die durch die Synchronisation geändert werden, werden bei der nächsten Synchronisation nochmals geladen und überprüft. Die zweite Synchronisation nach der Initialsynchronisation ist daher noch nicht deutlich schneller.

Die Revisionsfilterung kann an den Workflows oder an den Startkonfigurationen zugelassen werden.

Um die Revisionsfilterung an einem Workflow zuzulassen

- Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
- Bearbeiten Sie die Eigenschaften des Workflows. Wählen Sie in der Auswahlliste **Revisionsfilterung** den Eintrag **Revisionsfilter nutzen**.

Um die Revisionsfilterung an einer Startkonfiguration zuzulassen

- Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
- Bearbeiten Sie die Eigenschaften der Startkonfiguration. Wählen Sie in der Auswahlliste **Revisionsfilterung** den Eintrag **Revisionsfilter nutzen**.

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

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 `members~value` einer Cloud Gruppe (`Group`) - ODER - Liste von Rollen in der Eigenschaft `roles~value` eines Benutzers `User`
- 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 **Universal Cloud Interface > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **SCIM Schnittstelle**.
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.
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 `UCIUserInGroup`:

```
exists (select top 1 1 from UCIGroup g
     where g.UID_UCIGroup = i.UID_UCIGroup
     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. Gehört zu diesen Objekteigenschaften eine Mitgliederliste, werden auch die Einträge in der Zuordnungstabelle aktualisiert. 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.
- Für die Tabelle, die das geänderte Objekt enthält, ist der Pfad zum Basisobjekt der Synchronisation festgelegt.

Für Synchronisationsprojekte, die mit der Standard-Projektvorlage erstellt wurden, ist die Einzelobjektsynchronisation vollständig konfiguriert. Wenn Sie kundenspezifische Tabellen in solch ein Synchronisationsprojekt einbeziehen möchten, müssen Sie die Einzelobjektsynchronisation für diese Tabellen konfigurieren. Ausführliche Informationen dazu finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Um den Pfad zum Basisobjekt der Synchronisation für eine kundenspezifische Tabelle festzulegen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **SCIM Schnittstelle**.
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**.

   Geben Sie den Pfad zum Basisobjekt in der ObjectWalker-Notation der VI.DB an.

   Beispiel: `FK(UID_UCIRoot).XObjectKey`
8. Speichern Sie die Änderungen.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 45

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.
   - Für Jobserver, die an der Lastverteilung teilnehmen, muss die Option **Keine Prozesszuteilung** deaktiviert sein.
   - Weisen Sie diesen Jobservern die Serverfunktion **SCIM Konnektor** zu.

   Alle Jobserver müssen auf die gleiche Cloud-Anwendung 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.

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*.

Detaillierte Informationen zum Thema

- Jobserver für cloud-spezifische Prozessverarbeitung auf Seite 84

Synchronisation mit Überlagerungsdatei

Beim Einrichten der Synchronisation mit einer Cloud-Anwendung nutzt der One Identity Manager das SCIM Schema, welches vom Server exportiert wird. Wenn der SCIM Konnektor das Schema nicht ermitteln kann, können Sie ihm die Schemainformationen mittels Überlagerungsdateien übergeben. Die Überlagerungsdateien enthalten eine vollständige Beschreibung des genutzten Schemas. Sie müssen der SCIM Core Schema Spezifikation (RFC 7643) entsprechen.

Um die Synchronisation mit Überlagerungsdateien zu konfigurieren

1. Starten Sie den Synchronization Editor.
2. Aktivieren Sie den Expertenmodus.
3. Erstellen Sie ein initiales Synchronisationsprojekt. Weitere Informationen finden Sie unter Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Cloud-Anwendung auf Seite 18. Es gelten folgende Besonderheiten:
    a. Auf der Seite **Experteneinstellungen** legen Sie fest, ob Sie zusätzliche Einstellungen vornehmen möchten. Aktivieren Sie **Schemaeinstellungen anzeigen**.
    b. Auf der Seite **Schemadefinition (manuell)** geben Sie den Pfad zu den Überlagerungsdateien an. Beide Dateien müssen vorhanden sein.
        - **Schemaüberlagerungsdatei**: Enthält die vollständige Schemadefinition der Cloud-Anwendung.
        - **Ressourcenkonfiguration-Überlagerungsdatei**: Enthält die vollständige Ressourcendefinition der Cloud-Anwendung.
    c. Um die Überlagerungsdateien auf Fehler zu überprüfen, klicken Sie **Prüfen**.

HINWEIS: Wenn in der Synchronisationskonfiguration Überlagerungsdateien angegeben sind, ersetzen diese eine auf dem Server vorhandene Schemadefinition.

Die Schemadefinitionen aus den Überlagerungsdateien werden als Verbindungsparameter (`DPRSystemConnection.ConnectionParameter`) gespeichert.

Änderungen am SCIM Schema müssen in den Überlagerungdateien gepflegt werden. Geänderte Überlagerungsdateien müssen erneut in das Synchronisationsprojekt eingelesen werden.

Um Schemaänderungen in das Synchronisationsprojekt zu übernehmen

1. Aktualisieren Sie die Schemadefinition in den Überlagerungsdateien.
2. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
3. Aktivieren Sie den Expertenmodus.
4. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
5. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Verbindung bearbeiten**.

   Der Systemverbindungsassistent wird gestartet.
6. Auf der Seite **Schemadefinition (manuell)** geben Sie den Pfad zu den Überlagerungsdateien an.
7. Beenden Sie den Systemverbindungsassistenten.

   Die Verbindungsparameter werden aktualisiert.
8. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
9. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
10. Speichern Sie die Änderungen.

Wenn, beispielsweise durch nachträgliche Anpassungen, der Server eine gültige Schemadefinition bereitstellt, muss die Schemadefinition der Überlagerungsdateien aus den Verbindungsparametern entfernt werden.

Um das Schema der Überlagerungsdateien zu entfernen und die Schemadefinition des Servers zu verwenden

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Aktivieren Sie den Expertenmodus.
3. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
4. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Verbindung bearbeiten**.

   Der Systemverbindungsassistent wird gestartet.
5. Wählen Sie die Seite **Endpunktkonfiguration** und erfassen Sie die URIs zu den SCIM-Endpunkten. Wenn keine URIs angegeben sind, wird das SCIM Basisschema verwendet.
6. Wählen Sie die Seite **Schemadefinition (manuell)** und klicken Sie **Vorhandene entfernen**, sowohl für die Schemaüberlagerungsdatei als auch für die Ressourcenkonfiguration-Überlagerungsdatei.
7. Beenden Sie den Systemverbindungsassistenten.
8. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
9. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
10. Speichern Sie die Änderungen.

Ausführen einer Synchronisation

Synchronisationen werden über zeitgesteuerte Prozessaufträge gestartet. Im Synchronization Editor ist es auch möglich, eine Synchronisation manuell zu starten. Zuvor können Sie die Synchronisation simulieren, um das Ergebnis der Synchronisation abzuschätzen und Fehler in der Synchronisationskonfiguration aufzudecken. Wenn eine Synchronisation irregulär abgebrochen wurde, müssen Sie die Startinformation zurücksetzen, um die Synchronisation erneut starten zu können.

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*.

Detaillierte Informationen zum Thema

- Synchronisationen starten auf Seite 42
- Synchronisation deaktivieren auf Seite 44
- Synchronisationsergebnisse anzeigen auf Seite 43
- Einzelobjekte synchronisieren auf Seite 45

Synchronisationen starten

Beim Einrichten des initialen Synchronisationsprojekts über das Launchpad werden Standardzeitpläne für regelmäßige Synchronisationen erstellt und zugeordnet. Um regelmäßige Synchronisationen auszuführen, aktivieren Sie diese Zeitpläne.

Um regelmäßige Synchronisationen auszuführen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Startkonfigurationen**.
3. Wählen Sie in der Dokumentenansicht eine Startkonfiguration aus und klicken Sie **Zeitplan bearbeiten**.
4. Bearbeiten Sie die Eigenschaften des Zeitplans.
5. Um den Zeitplan zu aktivieren, klicken Sie **Aktiviert**.
6. Klicken Sie **OK**.

Wenn kein Zeitplan aktiviert ist, können Sie die Synchronisation auch manuell starten.

Um die initiale Synchronisation manuell zu starten

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Startkonfigurationen**.
3. Wählen Sie in der Dokumentenansicht eine Startkonfiguration und klicken Sie **Ausführen**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

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.

Synchronisationsergebnisse anzeigen

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.

Um das Protokoll einer Provisionierung 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 Provisionierungsprozesse angezeigt.
4. Wählen Sie per Maus-Doppelklick das Protokoll, das angezeigt werden soll.

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

Die Protokolle sind in der Navigationsansicht farblich gekennzeichnet. Die Kennzeichnung gibt den Ausführungsstatus der Synchronisation/Provisionierung wieder.

TIPP: Die Protokolle werden auch im Manager unter der Kategorie **<Zielsystemtyp> > Synchronisationsprotokolle** angezeigt.

Verwandte Themen

- Synchronisationsprotokoll konfigurieren auf Seite 29
- Fehleranalyse auf Seite 46

Synchronisation deaktivieren

Regelmäßige Synchronisationen können nur gestartet werden, wenn das Synchronisationsprojekt und der Zeitplan aktiviert sind.

Um regelmäßige Synchronisationen zu verhindern

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Startkonfiguration und deaktivieren Sie den hinterlegten Zeitplan.

   Synchronisationen können nun nur noch manuell gestartet werden.

Ein aktiviertes Synchronisationsprojekt kann nur eingeschränkt bearbeitet werden. Sind Schemaänderungen notwendig, muss das Schema im Synchronisationsprojekt aktualisiert werden. Dabei wird das Synchronisationsprojekt deaktiviert und kann erneut bearbeitet werden.

Des Weiteren muss das Synchronisationsprojekt deaktiviert werden, wenn keinerlei Synchronisationen gestartet werden dürfen (auch nicht manuell).

Um das Synchronisationsprojekt zu deaktivieren

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie auf der Startseite die Ansicht **Allgemein**.
3. Klicken Sie **Projekt deaktivieren**.

Detaillierte Informationen zum Thema

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Cloud-Anwendung auf Seite 18

Einzelobjekte synchronisieren

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. Gehört zu diesen Objekteigenschaften eine Mitgliederliste, werden auch die Einträge in der Zuordnungstabelle aktualisiert.

HINWEIS: Ist das Objekt im Zielsystem nicht mehr vorhanden, wird es in der One Identity Manager-Datenbank gelöscht.

Um ein Einzelobjekt zu synchronisieren

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface**.
2. Wählen Sie in der Navigationsansicht den Objekttyp.
3. Wählen Sie in der Ergebnisliste das Objekt, das Sie synchronisieren möchten.
4. Wählen Sie die Aufgabe **Objekt synchronisieren**.

   Es wird ein Prozess zum Lesen dieses Objekts in die Jobqueue eingestellt.

Besonderheiten bei der Synchronisation von Mitgliederlisten

Wenn Sie Änderungen in der Mitgliederliste eines Objekts synchronisieren, führen Sie die Einzelobjektsynchronisation am Basisobjekt der Zuweisung aus. Die Basistabelle einer Zuordnung enthält eine Spalte `XDateSubItem` mit der Information über die letzte Änderung der Mitgliedschaften.

Beispiel:

Basisobjekt für die Zuweisung von Benutzerkonten an Gruppen ist die Gruppe.

Im Zielsystem wurde ein Benutzerkonto an eine Gruppe zugewiesen. Um diese Zuweisung zu synchronisieren, wählen Sie im Manager die Gruppe, der das

Benutzerkonto zugewiesen wurde, und führen Sie die Einzelobjektsynchronisation aus. Dabei werden alle Mitgliedschaften für diese Gruppe synchronisiert.

Das Benutzerkonto muss in der One Identity Manager-Datenbank bereits als Objekt vorhanden sein, damit die Zuweisung angelegt werden kann.

Detaillierte Informationen zum Thema

- Einzelobjektsynchronisation konfigurieren auf Seite 38

Fehleranalyse

Bei der Analyse und Behebung von Synchronisationsfehlern unterstützt Sie der Synchronization Editor auf verschiedene Weise.

- Synchronisation simulieren

  Die Simulation ermöglicht es, das Ergebnis einer Synchronisation abzuschätzen. Dadurch können beispielsweise Fehler in der Synchronisationskonfiguration aufgedeckt werden.

- Synchronisation analysieren

  Für die Analyse von Problemen während der Synchronisation, beispielsweise unzureichender Performance, kann der Synchronisationsanalysebericht erzeugt werden.

- Meldungen protokollieren

  Der One Identity Manager bietet verschiedene Möglichkeiten zur Protokollierung von Meldungen. Dazu gehören das Synchronisationsprotokoll, die Protokolldatei des One Identity Manager Service, die Protokollierung von Meldungen mittels NLog und weitere.

- Startinformation zurücksetzen

  Wenn eine Synchronisation irregulär abgebrochen wurde, beispielsweise weil ein Server nicht erreichbar war, muss die Startinformation manuell zurückgesetzt werden. Erst danach kann die Synchronisation erneut gestartet werden.

Ausführliche Informationen zu diesen Themen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 43

Datenfehler bei der Synchronisation ignorieren

Standardmäßig werden Objekte mit fehlerhaften Daten nicht synchronisiert. 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.

Standardprofile an Benutzerkonten in Salesforce Anwendungen zuweisen

Cloud-Anwendungen wie Salesforce erfordern, dass beim Anlegen neuer Benutzerkonten bereits eine Systemberechtigung mit einem bestimmten Typ zugewiesen ist. Für diesen Zweck wird an Cloud Benutzerkonten, die in One Identity Manager neu angelegt werden, automatisch ein Standardprofil zugewiesen.

Voraussetzungen

- Die Synchronisation einer Cloud-Anwendung mit dem SCIM Konnektor ist im Universal Cloud Interface eingerichtet. Beim Erstellen des Synchronisationsprojekts wurde das Zielprodukt One Identity Starling Connect ausgewählt und die Projektvorlage **Synchronisation einer One Identity Starling Connect-Umgebung** verwendet.
- Das Zielsystem wurde initial synchronisiert.
- Die Synchronisation der Cloud-Anwendung ist im Modul Cloud Systems Management eingerichtet.
- Das Cloud Zielsystem wurde initial synchronisiert.
- Im kanonischen Namen oder im Anzeigenamen des Cloud Zielsystems wird die Zeichenkette **Salesforce** verwendet.
- Es gibt eine Cloud Systemberechtigung 2, die als Standardprofil verwendet werden soll. Der Name der Systemberechtigung ist für diese Systemberechtigung erfasst (`CSMGroup2.GroupName`).

Um das Standardprofil für neue Benutzerkonten zu ändern

- Bearbeiten Sie im Designer den Wert des Konfigurationsparameters **TargetSystem | CSM | ApplicationType | Salesforce | DefaultProfileName** und tragen Sie den Namen der Systemberechtigung 2 ein, welche automatisch an alle neuen Benutzerkonten zugewiesen werden soll.

HINWEIS: Standardmäßig wird die Zuweisung im Universal Cloud Interface durch die Property-Mapping-Regel `vrtProfileFirst profiles~value` im Mapping **User** in die Cloud-Anwendung übertragen. Sollte das Standardprofil in der Cloud-Anwendung an einer anderen Schemaeigenschaft hinterlegt sein, passen Sie die Property-Mapping-Regel entsprechend an.

TIPP: Wenn kein Standardprofil automatisch an neue Benutzerkonten zugewiesen werden soll, deaktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | CSM | ApplicationType | Salesforce | DefaultProfileName**.

3

Provisionierung von Objektänderungen

Änderungen an Cloud-Objekten können nur im Modul Cloud Systems Management vorgenommen werden. Provisionierungsprozesse sorgen dafür, dass Objektänderungen aus dem Modul Cloud Systems Management in das Modul Universal Cloud Interface übertragen werden. Standardmäßig werden diese Objektänderungen anschließend durch automatische Provisionierungsprozesse in die Cloud-Anwendungen publiziert. Für manche Cloud-Anwendungen soll keine automatisierte Schnittstelle zum Provisionieren der Änderungen eingesetzt werden. Für solche Cloud-Anwendungen können die Änderungen manuell provisioniert werden. Über ein Web Portal werden die manuellen Provisionierungsvorgänge angezeigt. Operatoren können anhand dieser Übersicht die anstehenden Änderungen in die Cloud-Anwendungen übertragen.

Der One Identity Manager zeichnet die Objektänderungen als anstehende Änderungen in separaten Tabellen auf. Die Tabelle `QBMPendingChange` enthält die geänderten Objekte und deren Verarbeitungsstatus. In der Tabelle `QBMPendingChangeDetail` werden die Details der Änderungen, die auszuführenden Operationen, der Erstellungszeitpunkt und der Verarbeitungsstatus gespeichert. Bei der automatischen Provisionierung werden die anstehenden Änderungen in der Reihenfolge ihrer Erstellung verarbeitet. Für die manuelle Provisionierung werden die anstehenden Änderungen in der Reihenfolge ihrer Erstellung im Web Portal aufgelistet.

Der Verarbeitungsstatus für ein Objekt wird erst dann abschließend auf erfolgreich gesetzt, wenn alle zugehörigen Änderungen für dieses Objekt erfolgreich provisioniert wurden. Der Verarbeitungsstatus eines Objekts ist fehlgeschlagen, wenn alle zugehörigen Änderungen verarbeitet wurden und mindestens eine dieser Änderungen fehlgeschlagen ist.

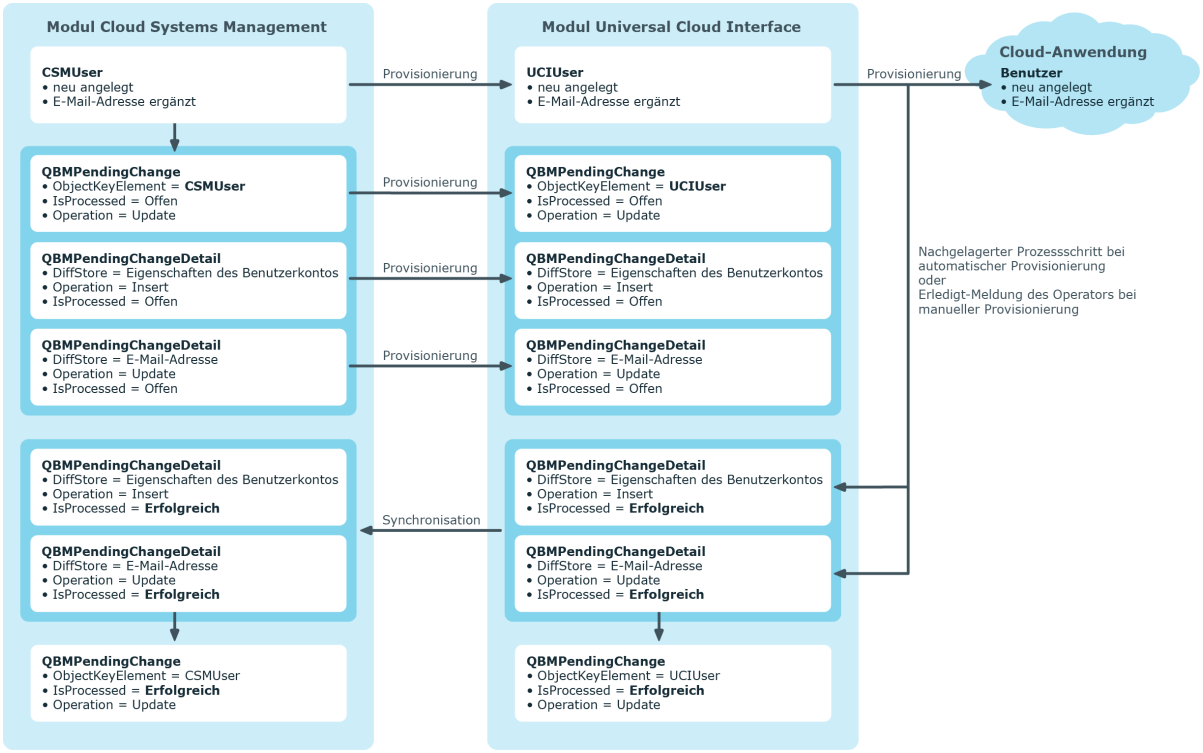
Detaillierte Informationen zum Thema

- Ablauf der Provisionierung auf Seite 50
- Manuelle Provisionierung konfigurieren auf Seite 52
- Aufbewahrungszeitraum für anstehende Änderungen auf Seite 51

Ablauf der Provisionierung

Folgende Grafik zeigt die Provisionierung von Objektänderungen und die zugehörige Verarbeitung der anstehenden Änderungen. Der Ablauf ist für automatische und manuelle Provisionierungsvorgänge identisch und ist unabhängig davon, ob die Module Cloud Systems Management und Universal Cloud Interface in der selben oder in separaten Datenbanken installiert sind.

Abbildung 3: Ablauf der Provisionierung von anstehenden Änderungen



Standardmäßig wird die Synchronisation zwischen den Modulen Cloud Systems Management und Universal Cloud Interface stündlich ausgeführt. Damit ist sichergestellt, dass der Verarbeitungsstatus für die anstehenden Änderungen zeitnah im Modul Cloud Systems Management bekannt ist.

Verwandte Themen

- Provisionierung von Objektänderungen auf Seite 49

Anstehende Änderungen anzeigen

Die anstehenden Änderungen können Sie auch im Manager einsehen. Hier werden sowohl die manuellen als auch die automatischen Provisionierungsvorgänge angezeigt.

Um anstehende Änderungen anzuzeigen

- Wählen Sie im Manager das Menü **Datenbank > Anstehende Änderungen**.

Tabelle 13: Bedeutung der Einträge in der Symbolleiste

Symbol	Bedeutung
	Ausgewähltes Objekt anzeigen.
	Ansicht aktualisieren.

Verwandte Themen

- Provisionierung von Objektänderungen auf Seite 49

Aufbewahrungszeitraum für anstehende Änderungen

Anstehende Änderungen werden für einen festgelegten Zeitraum gespeichert. Nach Ablauf der Frist werden die Einträge durch den DBQueue Prozessor aus den Tabellen `QBMPendingChange` und `QBMPendingChangeDetail` gelöscht. Der Aufbewahrungszeitraum ist vom Verarbeitungsstatus der Provisionierungsvorgänge abhängig und kann über Konfigurationsparameter konfiguriert werden. Die definierten Fristen gelten gleichermaßen für automatische als auch manuelle Provisionierungsvorgänge.

Um den Aufbewahrungszeitraum von anstehenden Änderungen zu konfigurieren

1. Um den Aufbewahrungszeitraum für erfolgreiche Provisionierungsvorgänge zu ändern, bearbeiten Sie im Designer den Wert des Konfigurationsparameters **QBM | PendingChange | LifeTimeSuccess**. Erfassen Sie den Aufbewahrungszeitraum in Tagen. Der Standardzeitraum beträgt **2** Tage.
2. Um den Aufbewahrungszeitraum für fehlgeschlagene Provisionierungsvorgänge zu konfigurieren, aktivieren Sie im Designer den Konfigurationsparameter **QBM | PendingChange | LifeTimeError** und erfassen Sie den Aufbewahrungszeitraum in Tagen. Der Standardzeitraum beträgt **30** Tage.
3. Um den Aufbewahrungszeitraum für offene Provisionierungsvorgänge zu konfigurieren, aktivieren Sie im Designer den Konfigurationsparameter **QBM | PendingChange | LifeTimeRunning** und erfassen Sie den Aufbewahrungszeitraum in Tagen. Der Standardzeitraum beträgt **60** Tage.

Verwandte Themen

- Provisionierung von Objektänderungen auf Seite 49

Manuelle Provisionierung konfigurieren

> ⚠ VORSICHT: **Datenverlust durch inkonsistente Daten!**
>
> Wenn Sie die manuelle Provisionierung wählen, müssen Sie durch geeignete manuelle Prozesse sicherstellen, dass die Änderungen aus der One Identity Manager-Datenbank zeitnah in die Cloud-Anwendung übertragen werden.
>
> Stellen Sie sicher, dass die Daten zwischen Cloud-Anwendung und One Identity Manager-Datenbank regelmäßig und zeitnah abgeglichen werden. Richten Sie dafür die Synchronisation über den SCIM Konnektor ein. Sollte das nicht möglich sein, können Sie die Synchronisation über den CSV Konnektor nutzen.

Ob eine manuelle Provisionierung zulässig ist, wird an den Cloud-Anwendungen konfiguriert. Über ein Web Portal werden die offenen manuellen Provisionierungsvorgänge für diese Cloud-Anwendungen angezeigt. Operatoren können anhand dieser Übersicht die anstehenden Änderungen in die Cloud-Anwendungen übertragen und danach als erledigt kennzeichnen. Auditoren können die offenen und die verarbeiteten Provisionierungsvorgänge im Web Portal prüfen.

Um die manuelle Provisionierung zu konfigurieren

1. Bearbeiten Sie die Stammdaten der Cloud-Anwendung.
    a. Aktivieren Sie die Option **Manuelle Provisionierung**.
    b. Ordnen Sie die Operatoren zu, welche die offenen Provisionierungsvorgänge im Web Portal bearbeiten dürfen.

        > TIPP: Sie können Operatoren auch für einzelne Container festlegen. Weitere Informationen finden Sie unter Containerstrukturen in Cloud-Anwendungen auf Seite 62.

2. Legen Sie die Auditoren fest, die manuelle Provisionierungsvorgänge im Web Portal prüfen dürfen.

Ausführliche Informationen zum Einrichten der Synchronisation mit dem CSV Konnektor finden Sie im *One Identity Manager Anwenderhandbuch für den CSV Konnektor*.

Detaillierte Informationen zum Thema

- Cloud-Anwendungen bearbeiten auf Seite 59
- Allgemeine Stammdaten für Cloud-Anwendungen auf Seite 59
- Cloud-Operatoren auf Seite 90
- Cloud-Auditoren auf Seite 92
- Offene Provisionierungsvorgänge bearbeiten auf Seite 55

- Alle Provisionierungsvorgänge einsehen auf Seite 56
- Einrichten der Initialsynchronisation mit einer Cloud-Anwendung auf Seite 13

4

Verwalten von Provisionierungsvorgängen im Web Portal

Über das Web Portal werden die offenen manuellen Provisionierungsvorgänge für Cloud-Anwendungen angezeigt. Operatoren können anhand dieser Übersicht die anstehenden Änderungen in die Cloud-Anwendungen übertragen und danach als erledigt kennzeichnen. Auditoren können die offenen und die verarbeiteten Provisionierungsvorgänge im Web Portal prüfen.

Abhängig davon, welche Anwendungsrolle der Benutzer besitzt, kann er entsprechend seiner Berechtigungen, Provisionierungsvorgänge im Web Portal einsehen oder verwalten. Weitere Informationen finden Sie unter One Identity Manager Benutzer für die Verwaltung von Cloud-Anwendungen auf Seite 10.

Um sich im Web Portal anzumelden

1. Öffnen Sie die Web Portal Seite, indem Sie in der Adressleiste des Webbrowsers die URL-Adresse der Web Portal Seite eingeben.

   Standardmäßig lautet die URL http://<Servername>/Applikationsname/, wobei <Servername> der Name des Servers ist, auf dem die Web Portal Anwendung installiert ist.
2. Erfassen Sie im Textfeld **Anmeldename** Ihren vollständigen Anmeldenamen.
3. Erfassen Sie im Textfeld **Kennwort** Ihr persönliches Kennwort.
4. Klicken Sie **Anmelden**.

Ausführliche Informationen zur Anmeldung am Web Portal finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.

Detaillierte Informationen zum Thema

- Provisionierung von Objektänderungen auf Seite 49
- Offene Provisionierungsvorgänge bearbeiten auf Seite 55
- Provisionierungsvorgänge einsehen und bearbeiten auf Seite 56
- Alle Provisionierungsvorgänge einsehen auf Seite 56

Offene Provisionierungsvorgänge bearbeiten

Als Operator bearbeiten Sie offene, manuelle Provisionierungsvorgänge im Web Portal. Ein Provisionierungsvorgang ist ein Arbeitsauftrag für den Operator, für den er eine Operation an einem Zielobjekt ausführt.

HINWEIS: Neben dem Operator kann auch ein Administrator offene Provisionierungsvorgänge bearbeiten.

In der Ansicht **Offene Cloud Operationen** werden Ihnen die Vorgänge absteigend sortiert nach Eingangsdatum mit Objektnamen und Beschreibung der Operation angezeigt. Die Operationsart sehen Sie im Anzeigefeld **Operation** in den Detailinformationen zum markierten Vorgang. Es gibt folgende Operationsarten.

Tabelle 14: Operationsarten

Neues Objekt	Erstellen Sie ein neues Objekt.
Änderung	Setzen Sie einen Wert im Zielsystem.
Löschung	Löschen Sie ein Objekt.

In den Detailinformationen wird zu jeder angeforderten Operation eine ausführliche Anweisung formuliert, die mit gekennzeichnet ist. Sind zu einem Zielobjekt mehrere offene Vorgänge vorhanden, arbeiten Sie die Vorgänge in der Reihenfolge ihres Eintreffens ab. Das heißt, der älteste Vorgang muss zuerst bearbeitet werden.

Um offene Provisionierungsvorgänge zu bearbeiten

1. Öffnen Sie auf der Startseite des Web Portals das Menü **Offene Cloud Operationen**.
2. Markieren Sie in der Ansicht **Offene Cloud Operationen** den gewünschten Provisionierungsvorgang.

   HINWEIS: Werden in den Detailinformationen zum markierten offenen Vorgang mehrere Operationen untereinander angezeigt, bearbeiten Sie die erste Operation.
3. Führen Sie die Anweisung aus.
4. Klicken Sie **Als erledigt markieren**.

   Ein ausgeführter Provisionierungsvorgang verschwindet aus der Ansicht **Offene Cloud Operationen**.

Provisionierungsvorgänge einsehen und bearbeiten

Als Administrator können Sie alle Provisionierungsvorgänge einsehen. Das heißt, Sie sehen offene und geschlossene Vorgänge. Offene Vorgänge können Sie bearbeiten. Fehlgeschlagene Provisionierungsvorgänge können nicht bearbeitet werden. Weitere Informationen finden Sie unter Offene Provisionierungsvorgänge bearbeiten auf Seite 55.

Um Provisionierungsvorgänge einzusehen

1. Öffnen Sie das Menü **Cloud Operationen**.

   Offene und geschlossene Provisionierungsvorgänge werden absteigend nach Eingangsdatum sortiert angezeigt.
2. Nehmen Sie eine der folgenden Aktionen vor:
   a. Markieren Sie den offenen Vorgang und führen Sie die Anweisung aus. Klicken Sie **Als erledigt markieren**.
   b. Markieren Sie den Vorgang und sehen Sie sich die relevanten Informationen in den Detailinformationen an.

Um sich nur offene Provisionierungsvorgänge anzusehen

1. Öffnen Sie das Menü **Offene Cloud Operationen**.
2. Bearbeiten Sie den Vorgang und klicken Sie **Als erledigt markieren**.

   Die bearbeiteten Vorgänge werden in die Ansicht **Cloud Operationen** verschoben.

Alle Provisionierungsvorgänge einsehen

Als Auditor können Sie alle Provisionierungsvorgänge im Web Portal einsehen. Das heißt, Sie können geschlossene und offene Provisionierungsvorgänge einsehen. Offene Provisionierungsvorgänge können Sie nicht bearbeiten.

Um Provisionierungsvorgänge einzusehen

1. Öffnen Sie das Menü **Cloud Operationen**.

   Offene und geschlossene Provisionierungsvorgänge werden absteigend nach Eingangsdatum sortiert angezeigt.
2. Markieren Sie den Vorgang und sehen Sie sich die relevanten Informationen in den Detailinformationen an.

Statistiken einsehen

Statistiken zu Provisionierungsvorgängen werden auf der Startseite des Web Portals angezeigt und sind für den Adminitstrator, Operator und Auditor sichtbar. In der Statistik wird die Anzahl der offenen Provisionierungsvorgänge in einem Zeitverlauf angezeigt. Der Zeitverlauf besteht aus Punkten, die jeweils ein Datum repräsentieren und angeklickt werden können. Wenn Sie die Maus über einen Punkt im Zeitverlauf bewegen, wird ein kleiner Text angezeigt, der Informationen zu den offenen Vorgängen an diesem Tag liefert.

Um sich die Statistiken anzusehen

1. Doppelklicken Sie in der grafischen Darstellung auf einen Punkt im Zeitverlauf.

   Ein Fenster mit einer vergrößerten grafischen Darstellung wird angezeigt. Die Daten zu den einzelnen Punkten im Zeitverlauf sind jetzt sichtbar.
2. Bewegen Sie die Maus an dem Datum über den Punkt, zu dem Sie sich informieren möchten.

   Zu dem Datum wird die Anzahl der Vorgänge angezeigt.
3. Lassen Sie sich alle Vorgänge mit Werten chronologisch absteigend anzeigen.
   a. Klicken Sie auf den Link **Hilfe**.
   b. Wählen Sie den Tabreiter **Quelldateien anzeigen**.

Abbilden von Cloud-Objekten im One Identity Manager

Mit dem One Identity Manager verwalten Sie die Benutzer und Berechtigungen von Cloud-Anwendungen. Jede Cloud-Anwendung wird als eigenes Basisobjekt im One Identity Manager abgebildet. Die Benutzerdaten werden als Benutzerkonten, Gruppen, Systemberechtigungen und Berechtigungselemente gespeichert und können in Containern organisiert werden.

Detaillierte Informationen zum Thema

- Cloud-Anwendungen bearbeiten auf Seite 59
- Containerstrukturen in Cloud-Anwendungen auf Seite 62
- Benutzerkonten in Cloud-Anwendungen auf Seite 63
- Gruppen in Cloud-Anwendungen auf Seite 71
- Berechtigungselemente in einer Cloud-Anwendung auf Seite 79
- Berichte über Objekte in Cloud Zielsystemen

Cloud-Anwendungen

Jede Cloud-Anwendung wird als eigenes Basisobjekt im One Identity Manager abgebildet. Die Stammdaten einer Cloud-Anwendung werden im Manager angezeigt. Hier können Sie die Operatoren zuordnen.

Für bestehende Cloud-Anwendungen werden deren Eigenschaften im Modul Cloud Systems Management an den Cloud Zielsystemen gepflegt und durch die Provisionierung in das Modul Universal Cloud Interface übernommen.

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

Detaillierte Informationen zum Thema

- Cloud-Anwendungen bearbeiten auf Seite 59

Cloud-Anwendungen bearbeiten

Die allgemeinen Stammdaten einer Cloud-Anwendung werden im Manager angezeigt. Hier können Sie die Operatoren zuordnen und alternative Spaltenbezeichnungen festlegen. Bei Bedarf kann eine Cloud-Anwendung auch im Manager neu angelegt werden.

Um die Stammdaten einer Cloud-Anwendung anzuzeigen und Operatoren zuzuordnen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > Basisdaten zur Konfiguration > Cloud-Anwendungen**.
2. Wählen Sie in der Ergebnisliste eine Cloud-Anwendung.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Um im Web Portal manuelle Provisionierungsvorgänge bearbeiten zu können, wählen Sie im Eingabefeld **Operator** eine Anwendungsrolle für Operatoren.
5. Speichern Sie die Änderungen.

TIPP: Die Eigenschaften einer Cloud-Anwendung können Sie auch in der Kategorie **Universal Cloud Interface | <Cloud-Anwendung>** anzeigen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Cloud-Anwendungen auf Seite 59
- Alternative Spaltenbezeichnungen festlegen auf Seite 61

Allgemeine Stammdaten für Cloud-Anwendungen

Für eine Cloud-Anwendung werden die folgenden allgemeinen Stammdaten angezeigt. Für die Bearbeitung manueller Provisionierungsvorgänge ordnen Sie eine Anwendungsrolle für Operatoren zu.

Tabelle 15: Allgemeine Stammdaten einer Cloud-Anwendung

Eigenschaft	Beschreibung
Cloud-Anwendung	Bezeichnung der Cloud-Anwendung.
Kanonischer Name	Vollständiger Name der Cloud-Anwendung. Der kanonische

Eigenschaft	Beschreibung
	Name setzt sich zusammen aus dem DNS-Namen des Servers beziehungsweise dessen URL, dem Port und der URI des Dienstes. Beispiel: `identities.example.net:8080/scim/v2`
Definierter Name	Definierter Name der Cloud-Anwendung. Der definierte Name wird zur Bildung der definierten Namen untergeordneter Objekte verwendet. Syntaxbeispiel: `DC = <Kanonischer Name>`
Anzeigename	Bezeichnung, unter der die Cloud-Anwendung in den Werkzeugen des One Identity Manager angezeigt wird.
Operator	Anwendungsrolle, in der die Cloud-Operatoren festgelegt sind. Die Operatoren bearbeiten manuelle Provisionierungsvorgänge für die Cloud-Anwendung, der sie zugewiesen sind. Jeder Cloud-Anwendung können andere Operatoren zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle, deren Mitglieder manuelle Provisionierungsvorgänge bearbeiten dürfen. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.
Typen der verwendeten Systemberechtigungen	Typen von Systemberechtigungen, denen in dieser Cloud-Anwendung Benutzerkonten zugewiesen werden können.
Benutzerkonto enthält Mitgliedschaften	Gibt an, für welche Typen von Systemberechtigungen die Zuweisungen an den Benutzerkonten gepflegt werden. Beispiel: Im Eingabefeld **Typen der verwendeten Systemberechtigungen** sind die Werte **Gruppe** und **Systemberechtigung 1** ausgewählt. Im Eingabefeld **Benutzerkonto enthält Mitgliedschaften** ist nur der Wert **Systemberechtigung 1** ausgewählt. Die Zuweisungen von Benutzerkonten zu Gruppen werden an den Gruppen gespeichert, die Zuweisungen von Benutzerkonten zu Systemberechtigungen 1 an den Benutzerkonten.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Manuelle Provisionierung	Gibt an, ob Änderungen an Cloud-Ojekten in der One Identity Manager-Datenbank automatisch in die Cloud-Anwendung provisioniert werden. Wenn die Option deaktiviert ist, sind die

Eigenschaft	Beschreibung
	Prozesse zur automatischen Provisionierung von Objektänderungen konfiguriert. Wenn Objektänderungen nicht automatisch in die Cloud-Anwendung publiziert werden dürfen, aktivieren Sie diese Option. Nutzen Sie das Web Portal, um die Änderungen in die Cloud-Anwendung zu übernehmen. WICHTIG: Wenn Sie die Option aktivieren, stellen Sie durch regelmäßige und häufige Synchronisationen sicher, dass die Daten zwischen der One Identity Manager-Datenbank und der Cloud-Anwendung konsistent gehalten werden!
Benutzerkonten löschen nicht erlaubt	Angabe, ob Benutzerkonten in der Cloud-Anwendung gelöscht werden dürfen. Wenn die Option aktiviert ist, können die Benutzerkonten lediglich deaktiviert werden.

Verwandte Themen

- Manuelle Provisionierung konfigurieren auf Seite 52
- Verwalten von Provisionierungsvorgängen im Web Portal auf Seite 54
- Typen von Systemberechtigungen in Cloud-Anwendungen auf Seite 69

Alternative Spaltenbezeichnungen festlegen

Wenn auf den Stammdatenformularen abweichende Bezeichnungen der Eingabefelder benötigt werden, können Sie für jeden Objekttyp die alternativ zu verwendenden Spaltenbezeichnungen sprachabhängig festlegen.

Um alternative Spaltenbezeichnungen festzulegen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > Basisdaten zur Konfiguration > Cloud-Anwendungen**.
2. Wählen Sie in der Ergebnisliste eine Cloud-Anwendung und wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wechseln Sie auf den Tabreiter **Alternative Spaltenbezeichnungen**.
4. Öffnen Sie den Mitgliederbaum der Tabelle, deren Spaltenbezeichnungen angepasst werden sollen.

   Es werden alle Spalten dieser Tabelle mit den Standard-Spaltenbezeichnungen aufgelistet.
5. Tragen Sie eine beliebige Benennung in der verwendeten Anmeldesprache ein.
6. Speichern Sie die Änderungen.

Synchronisationsprojekt für eine Cloud-Anwendung bearbeiten

Synchronisationsprojekte, in denen eine Cloud-Anwendung bereits als Basisobjekt verwendet wird, können auch über den Manager geöffnet werden. In diesem Modus können beispielsweise die Konfigurationseinstellungen überprüft oder die Synchronisationsprotokolle eingesehen werden. Der Synchronization Editor wird nicht mit seinem vollen Funktionsumfang gestartet. Verschiedene Funktionen, wie Simulieren oder Ausführen einer Synchronisation, Starten des Zielsystembrowsers und andere, können nicht ausgeführt werden.

HINWEIS: Der Manager ist währenddessen für die Bearbeitung gesperrt. Um Objekte im Manager bearbeiten zu können, schließen Sie den Synchronization Editor.

Um ein bestehendes Synchronisationsprojekt im Synchronization Editor zu öffnen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > Basisdaten zur Konfiguration > Cloud-Anwendungen**.
2. Wählen Sie in der Ergebnisliste die Cloud-Anwendung.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten...**.

Verwandte Themen

- Anpassen einer Synchronisationskonfiguration auf Seite 29

Containerstrukturen in Cloud-Anwendungen

Die Containerstruktur repräsentiert die Strukturelemente einer Cloud-Anwendung. Container werden in einer hierarchischen Baumstruktur dargestellt.

Um die Stammdaten eines Containers anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Containerstruktur**.
2. Wählen Sie in der Ergebnisliste den Container.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Zu einem Container erhalten Sie die folgenden Stammdaten. Für die Bearbeitung manueller Provisionierungsvorgänge ordnen Sie eine Anwendungsrolle für Operatoren zu.

Tabelle 16: Stammdaten eines Containers

Eigenschaft	Beschreibung
Bezeichnung	Name des Containers.
Definierter Name	Definierter Name des Containers.
Übergeordneter Container	Übergeordneter Container zur Abbildung einer hierarchischen Containerstruktur.
Cloud-Anwendung	Cloud-Anwendung des Containers.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Kontomanager	Verantwortlicher für den Container.
Operatoren	Anwendungsrolle, in der die Cloud-Operatoren festgelegt sind. Die Operatoren bearbeiten manuelle Provisionierungsvorgänge für den Container, dem sie zugewiesen sind. Jedem Container können andere Operatoren zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle, deren Mitglieder manuelle Provisionierungsvorgänge bearbeiten dürfen. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.

Verwandte Themen

- Cloud-Operatoren auf Seite 90

Benutzerkonten in Cloud-Anwendungen

Die Benutzerkonten repräsentieren die Authentifizierungsobjekte einer Cloud-Anwendung. Ein Benutzerkonto erhält über seine Mitgliedschaften in Gruppen, Systemberechtigungen und Berechtigungselementen die nötigen Berechtigungen zum Zugriff auf die Cloud-Ressourcen.

Verwandte Themen

- Benutzerkonten anzeigen auf Seite 64
- Zugewiesene Gruppen und Systemberechtigungen anzeigen auf Seite 67
- Zugewiesene Berechtigungselemente anzeigen auf Seite 68
- Überblick über Benutzerkonten in Cloud-Anwendungen anzeigen auf Seite 68

Benutzerkonten anzeigen

Um die Stammdaten eines Benutzerkontos anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten anzeigen**.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Benutzerkonten in Cloud-Anwendungen auf Seite 64
- Logindaten für Benutzerkonten in Cloud-Anwendungen auf Seite 65
- Angaben zur Identifikation von Benutzerkonten in Cloud-Anwendungen auf Seite 66
- Kontaktinformationen für Benutzerkonten in Cloud-Anwendungen auf Seite 66
- Benutzerdefinierte Stammdaten für Benutzerkonten in Cloud-Anwendungen auf Seite 67

Allgemeine Stammdaten für Benutzerkonten in Cloud-Anwendungen

Zu einem Benutzerkonto erhalten Sie die folgenden allgemeinen Stammdaten.

Tabelle 17: Allgemeine Stammdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Cloud-Anwendung	Cloud-Anwendung des Benutzerkontos.
Anrede	Anrede des Benutzers.
Vorname	Vorname des Benutzers.
Nachname	Nachname des Benutzers.
Vollständiger Name	Vollständiger Name des Benutzers.
Initialen	Initialen des Benutzers.
Berufsbezeichnung	Berufsbezeichnung des Benutzers.
Nickname	Zusätzliche Information zum Benutzerkonto.
Namenszusatz	Namenszusatz des Benutzers, beispielsweise "von" oder "zu".
Anzeigename	Anzeigename des Benutzerkontos.

Eigenschaft	Beschreibung
Alias	Alias des Benutzerkontos zur weiteren Identifizierung.
Bezeichnung	Bezeichnung des Benutzerkontos.
Container	Container des Benutzerkontos.
Erste primäre Gruppe	Primäre Gruppe des Benutzerkontos.
Zweite primäre Gruppe	Zusätzliche primäre Gruppe des Benutzerkontos. Wenn es in der Cloud-Anwendung Gruppen mit unterschiedlichen Gruppentypen gibt, kann hier eine weitere primäre Gruppe zugeordnet sein.
E-Mail-Adresse	E-Mail-Adresse des Benutzers.
E-Mail-Kodierung	Art der E-Mail-Kodierung.
Kontoverfallsdatum	Tag, bis zu welchem das Benutzerkonto zur Anmeldung genutzt werden darf.
Ressourcentyp	Typ der Ressource, beispielsweise `User`.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Anmeldename	Name, mit dem sich der Benutzer an der Cloud-Anwendung anmeldet.
Benutzerkonto ist deaktiviert	Angabe, ob das Benutzerkonto gesperrt ist.

Logindaten für Benutzerkonten in Cloud-Anwendungen

Auf dem Tabreiter **Login** erhalten Sie die folgenden Daten.

Tabelle 18: Logindaten eines Benutzerkontos

Eigenschaft	Beschreibung
Kennwort/Kennwortbestätigung	Kennwort für das Benutzerkonto.
Letzte Kennwortänderung	Datum der letzten Änderung des Kennwortes.
Letzte Anmeldung	Datum und Uhrzeit der letzten Anmeldung an der Cloud-Anwendung.

Angaben zur Identifikation von Benutzerkonten in Cloud-Anwendungen

Auf dem Tabreiter **Identifikation** erhalten Sie die Adressinformationen der Person, die dieses Benutzerkonto verwendet.

Tabelle 19: Identifikationsdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Straße	Straße.
Postfach	Postfach.
Ort	Ort.
Postleitzahl	Postleitzahl.
Bundesland	Bundesland.
Land	Land.
Adresse	Formatierte Postanschrift.
Sprachkultur	Bezeichnung der Sprachkultur.
Zeitzone	Bezeichnung der Zeitzone.
Raum	Raum.
Abteilung	Abteilung der Person.
Bereich	Bereich, zu dem das Benutzerkonto gehört.
Organisation	Organisation, zu der das Benutzerkonto gehört.
Personennummer	Nummer zur Kennzeichnung der Person, zusätzlich zur Personenkennung.
Art der Anstellung	Art der Anstellung.
Kontomanager	Verantwortlicher für das Benutzerkonto.

Kontaktinformationen für Benutzerkonten in Cloud-Anwendungen

Auf dem Tabreiter **Kontakt** erhalten Sie die Informationen zur Erreichbarkeit der Person, die dieses Benutzerkonto verwendet.

Tabelle 20: Kontaktdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Telefon	Nummer des Festnetztelefons.
Mobiltelefon	Nummer des Mobiltelefons.
Webseite	Webseite des Benutzers.

Benutzerdefinierte Stammdaten für Benutzerkonten in Cloud-Anwendungen

Auf dem Tabreiter **Benutzerdefiniert** erhalten Sie unternehmensspezifische Angaben zum Benutzerkonto.

Tabelle 21: Benutzerdefinierte Stammdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Freies Feld Nr. 01- Freies Feld Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freies Datum Nr. 01- Freies Datum Nr. 03	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freier Text Nr. 01- Freier Text Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freie Option Nr. 01 - Freie Option Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Zugewiesene Gruppen und Systemberechtigungen anzeigen

Über diese Aufgabe sehen Sie alle Gruppen und Systemberechtigungen, die dem Benutzerkonto zugewiesen sind.

Um zugewiesene Gruppen und Systemberechtigungen anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.

3. Wählen Sie die Aufgabe **Gruppen und Systemberechtigungen zuweisen**.
4. Wählen Sie den Tabreiter **Gruppen**, **Systemberechtigungen 1**, **Systemberechtigungen 2** oder **Systemberechtigungen 3**.

Verwandte Themen

- Gruppen in Cloud-Anwendungen auf Seite 71

Zugewiesene Berechtigungselemente anzeigen

Über diese Aufgabe sehen Sie alle Berechtigungselemente, die dem Benutzerkonto zugewiesen sind.

Um zugewiesene Berechtigungselemente anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Berechtigungselemente zuweisen**.

Verwandte Themen

- Berechtigungselemente in einer Cloud-Anwendung auf Seite 79

Überblick über Benutzerkonten in Cloud-Anwendungen anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einem Benutzerkonto.

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das Benutzerkonto**.

Gruppen und Systemberechtigungen in Cloud-Anwendungen

Gruppen und Systemberechtigungen bilden die Objekte ab, über die in der Cloud-Anwendung der Zugriff auf die Cloud-Ressourcen gesteuert wird. Ein Benutzerkonto erhält durch die Zuweisung zu Gruppen und Systemberechtigungen die nötigen Berechtigungen zum Zugriff auf die Cloud-Ressourcen.

Detaillierte Informationen zum Thema

- Typen von Systemberechtigungen in Cloud-Anwendungen auf Seite 69
- Gruppen in Cloud-Anwendungen auf Seite 71
- Systemberechtigungen in Cloud-Anwendungen auf Seite 75

Typen von Systemberechtigungen in Cloud-Anwendungen

Viele Cloud-Anwendungen nutzen verschiedene Berechtigungstypen, um Benutzerberechtigungen zu administrieren. Das können neben Gruppen beispielsweise auch Rollen oder Berechtigungssets sein. Über Synchronisationsprojekte, die mit der Projektvorlage **Synchronisation einer One Identity Starling Connect-Umgebung** erstellt wurden, werden die verschiedenen Typen folgendermaßen im One Identity Manager abgebildet.

Tabelle 22: Abbildung von Systemberechtigungen im One Identity Manager

Typ	Tabelle	Anzeigename
Group	UCIGroup	Gruppen
Role	UCIGroup1	Systemberechtigungen 1
Profile	UCIGroup2	Systemberechtigungen 2
Entitlement	UCIGroup3	Systemberechtigungen 3
Permissionset	UCIItem	Berechtigungselemente

HINWEIS: In Synchronisationsprojekten, die mit einer One Identity Manager Version älter als 8.2 erstellt wurden, sind Objekte vom Typ **Profile** ebenfalls in der Tabelle `UCIItem` abgebildet.

Ein Benutzerkonto erhält über seine Zuweisungen zu den Gruppen oder Systemberechtigungen die nötigen Berechtigungen zum Zugriff auf die Zielsystemressourcen. Abhängig vom Zielsystem werden die Zuweisungen entweder an

den Benutzerkonten (benutzerbasierte Zuweisung) oder an den Systemberechtigungen (berechtigungsbasierte Zuweisung) gepflegt. Beim Einrichten der Synchronisation mit der Projektvorlage **Synchronisation einer One Identity Starling Connect-Umgebung** ermittelt der SCIM Konnektor, an welchem Objekttyp die Zuweisungen gespeichert sind. Die Mitgliedschaften werden in den folgenden Tabellen abgebildet:

Tabelle 23: Benutzerbasierte Zuweisung

`UCIUserHasGroup`	**Gruppen: Zuweisungen zu Benutzerkonten**
`UCIUserHasGroup1`	**Systemberechtigungen 1: Zuweisungen zu Benutzerkonten**
`UCIUserHasGroup2`	**Systemberechtigungen 2: Zuweisungen zu Benutzerkonten**
`UCIUserHasGroup3`	**Systemberechtigungen 3: Zuweisungen zu Benutzerkonten**
`UCIUserHasItem`	**Benutzerkonten: Zuweisungen Berechtigungselemente**

Tabelle 24: Berechtigungsbasierte Zuweisung

`UCIUserInGroup`	**Benutzerkonten: Zuweisungen zu Gruppen**
`UCIUserInGroup1`	**Benutzerkonten: Zuweisungen zu Systemberechtigungen 1**
`UCIUserInGroup2`	**Benutzerkonten: Zuweisungen zu Systemberechtigungen 2**
`UCIUserInGroup3`	**Benutzerkonten: Zuweisungen zu Systemberechtigungen 3**

Zuweisungen für den Typ `Permissionset` sind immer benutzerbasiert.

Über Synchronisationsprojekte, die mit der Projektvorlage **SCIM Synchronisation** erstellt wurden, werden standardmäßig nur Gruppen abgebildet. Der SCIM Konnektor ermittelt, an welchem Objekttyp die Zuweisungen gespeichert sind und bildet diese entsprechend entweder in der Tabelle `UCIUserHasGroup` oder in der Tabelle `UCIUserInGroup` ab.

An den Cloud-Anwendungen ist hinterlegt, welche Typen von Systemberechtigungen verwendet werden und ob die Zuweisungen an den Benutzerkonten oder den Systemberechtigungen gespeichert werden.

Um die verwendeten Typen von Systemberechtigungen anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > Basisdaten zur Konfiguration > Cloud-Anwendungen**.
2. Wählen Sie in der Ergebnisliste eine Cloud-Anwendung und wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    - **Typen der verwendeten Systemberechtigungen**: Liste der in der Cloud-Anwendung verwendeten Typen von Systemberechtigungen.
    - **Benutzerkonto enthält Mitgliedschaften**: Liste der Typen von Systemberechtigungen mit benutzerbasierten Zuweisungen. Für Typen, die hier nicht aufgelistet sind, werden die Zuweisungen an den Systemberechtigungen gespeichert.

TIPP: Wenn das Schema der Cloud-Anwendung durch keine Standard-Projektvorlage ausreichend abgebildet werden kann, passen Sie die Synchronisationskonfiguration an. Definieren Sie dabei, wie die Systemberechtigungen im One Identity Manager Schema abgebildet werden. Stellen Sie sicher, dass bei der Einrichtung der Synchronisation das Basisobjekt für die Cloud-Anwendung (`UCIRoot`) in der Datenbank angelegt wird und die Eigenschaften **Typen der verwendeten Systemberechtigungen** (`GroupUsageMask`) und **Benutzerkonto enthält Mitgliedschaften** (`UserContainsGroupList`) korrekt gesetzt werden.

Verwandte Themen

- Allgemeine Stammdaten für Cloud-Anwendungen auf Seite 59

Gruppen in Cloud-Anwendungen

Gruppen und Systemberechtigungen bilden die Objekte ab, über die in der Cloud-Anwendung der Zugriff auf die Cloud-Ressourcen gesteuert wird. Ein Benutzerkonto erhält durch die Zuweisung zu Gruppen und Systemberechtigungen die nötigen Berechtigungen zum Zugriff auf die Cloud-Ressourcen.

Um die Stammdaten einer Gruppe anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Stammdaten anzeigen**.

Um die Stammdaten einer Systemberechtigung anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Wählen Sie die Aufgabe **Stammdaten anzeigen**.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Gruppen in Cloud-Anwendungen auf Seite 72
- Benutzerdefinierte Stammdaten für Gruppen in Cloud-Anwendungen auf Seite 73

- Zugewiesene Benutzerkonten anzeigen auf Seite 73
- Zugewiesene Gruppen anzeigen auf Seite 73
- Zugewiesene Berechtigungselemente anzeigen auf Seite 74

Verwandte Themen

- Systemberechtigungen in Cloud-Anwendungen auf Seite 75

Allgemeine Stammdaten für Gruppen in Cloud-Anwendungen

Zu einer Gruppe erhalten Sie die folgenden allgemeinen Stammdaten.

Tabelle 25: Allgemeine Stammdaten einer Gruppe

Eigenschaft	Beschreibung
Bezeichnung	Bezeichnung der Gruppe.
Container	Container der Gruppe.
Cloud-Anwendung	Cloud-Anwendung der Gruppe.
Definierter Name	Definierter Name der Gruppe.
Anzeigename	Anzeigename zur Anzeige der Gruppe in der Benutzeroberfläche der One Identity Manager Werkzeuge.
Name der Gruppe	Zusätzliche Bezeichnung der Gruppe.
E-Mail-Adresse	E-Mail-Adresse der Gruppe.
Kontomanager	Verantwortlicher der Gruppe.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Gruppentyp	Eindeutige Kennung des Gruppentyps, beispielsweise wenn über ein und denselben SCIM-Endpunkt Gruppen verschiedenen Typs geliefert werden.
Ressourcentyp	Bezeichnung des Ressourcentyps. Der Ressourcentyp entspricht einem SCIM-Endpunkt, beispielsweise `/Groups`.

Verwandte Themen

- Gruppen in Cloud-Anwendungen auf Seite 71

Benutzerdefinierte Stammdaten für Gruppen in Cloud-Anwendungen

Auf dem Tabreiter **Benutzerdefiniert** erhalten Sie unternehmensspezifische Angaben zur Gruppe.

Tabelle 26: Benutzerdefinierte Stammdaten einer Gruppe

Eigenschaft	Beschreibung
Freies Feld Nr. 01- Freies Feld Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freies Datum Nr. 01- Freies Datum Nr. 03	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freier Text Nr. 01- Freier Text Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freie Option Nr. 01 - Freie Option Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Zugewiesene Benutzerkonten anzeigen

Über diese Aufgabe sehen Sie alle Benutzerkonten, die der Gruppe zugewiesen sind.

Um zugewiesene Benutzerkonten anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.

Verwandte Themen

- Benutzerkonten in Cloud-Anwendungen auf Seite 63
- Gruppen in Cloud-Anwendungen auf Seite 71

Zugewiesene Gruppen anzeigen

Über diese Aufgabe sehen Sie alle Gruppen, die der Gruppe zugewiesen sind.

Um zugewiesene Gruppen anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Um alle Gruppen anzuzeigen, die in der gewählten Gruppe Mitglied sind, wählen Sie den Tabreiter **Hat Mitglieder**.
5. Um alle Gruppen anzuzeigen, in denen die gewählte Gruppe Mitglied ist, wählen Sie den Tabreiter **Ist Mitglied in**.

Verwandte Themen

- Gruppen in Cloud-Anwendungen auf Seite 71

Zugewiesene Berechtigungselemente anzeigen

Über diese Aufgabe sehen Sie alle Berechtigungselemente, die der Gruppe zugewiesen sind.

Um zugewiesene Berechtigungselemente anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Berechtigungselemente zuweisen**.

Verwandte Themen

- Berechtigungselemente in einer Cloud-Anwendung auf Seite 79
- Gruppen in Cloud-Anwendungen auf Seite 71
-

Überblick über Gruppen in Cloud-Anwendungen anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Gruppe.

Um einen Überblick über eine Gruppe zu erhalten

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die Gruppe**.

Verwandte Themen

- Gruppen in Cloud-Anwendungen auf Seite 71

Systemberechtigungen in Cloud-Anwendungen

Gruppen und Systemberechtigungen bilden die Objekte ab, über die in der Cloud-Anwendung der Zugriff auf die Cloud-Ressourcen gesteuert wird. Ein Benutzerkonto erhält durch die Zuweisung zu Gruppen und Systemberechtigungen die nötigen Berechtigungen zum Zugriff auf die Cloud-Ressourcen.

Um die Stammdaten einer Systemberechtigung anzuzeigen

Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 1**.

- ODER -

Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 2**.

- ODER -

Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 3**.

1. Wählen Sie in der Ergebnisliste die Systemberechtigung.
2. Wählen Sie die Aufgabe **Stammdaten anzeigen**.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Systemberechtigungen in Cloud-Anwendungen auf Seite 76
- Benutzerdefinierte Stammdaten für Systemberechtigungen in Cloud-Anwendungen auf Seite 77
- Zugewiesene Benutzerkonten anzeigen auf Seite 77
- Zugewiesene Systemberechtigungen anzeigen auf Seite 78
- Überblick über Systemberechtigungen in Cloud-Anwendungen anzeigen auf Seite 78

Verwandte Themen

- Gruppen in Cloud-Anwendungen auf Seite 71

Allgemeine Stammdaten für Systemberechtigungen in Cloud-Anwendungen

Zu einer Systemberechtigungen erhalten Sie die folgenden allgemeinen Stammdaten.

Tabelle 27: Allgemeine Stammdaten einer Systemberechtigungen

Eigenschaft	Beschreibung
Bezeichnung	Bezeichnung der Systemberechtigung.
Container	Container der Systemberechtigung.
Cloud-Anwendung	Cloud-Anwendung der Systemberechtigung.
Definierter Name	Definierter Name der Systemberechtigung.
Anzeigename	Anzeigename zur Anzeige der Systemberechtigung in der Benutzeroberfläche der One Identity Manager Werkzeuge.
Name der Systemberechtigung	Zusätzliche Bezeichnung der Systemberechtigung.
E-Mail-Adresse	E-Mail-Adresse der Systemberechtigung.
Kontomanager	Verantwortlicher der Systemberechtigung.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Typ der Systemberechtigung	Eindeutige Kennung des Typs der Systemberechtigung, beispielsweise wenn über ein und denselben SCIM-Endpunkt Systemberechtigungen verschiedenen Typs geliefert werden.
Ressourcentyp	Bezeichnung des Ressourcentyps. Der Ressourcentyp entspricht einem SCIM-Endpunkt, beispielsweise `/Roles`.

Verwandte Themen

- Systemberechtigungen in Cloud-Anwendungen auf Seite 75

Benutzerdefinierte Stammdaten für Systemberechtigungen in Cloud-Anwendungen

Auf dem Tabreiter **Benutzerdefiniert** erhalten Sie unternehmensspezifische Angaben zur Systemberechtigung.

Tabelle 28: Benutzerdefinierte Stammdaten einer Systemberechtigung

Eigenschaft	Beschreibung
Freies Feld Nr. 01- Freies Feld Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freies Datum Nr. 01- Freies Datum Nr. 03	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freier Text Nr. 01- Freier Text Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freie Option Nr. 01 - Freie Option Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Zugewiesene Benutzerkonten anzeigen

Über diese Aufgabe sehen Sie alle Benutzerkonten, die der Systemberechtigung zugewiesen sind.

Um zugewiesene Benutzerkonten anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.

Verwandte Themen

- Benutzerkonten in Cloud-Anwendungen auf Seite 63
- Systemberechtigungen in Cloud-Anwendungen auf Seite 75

Zugewiesene Systemberechtigungen anzeigen

Über diese Aufgabe sehen Sie alle Systemberechtigungen, die der Systemberechtigung zugewiesen sind.

Um zugewiesene Systemberechtigungen anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Passend zur gewählten Systemberechtigung, wählen Sie die Aufgabe **Systemberechtigungen 1 zuweisen**, **Systemberechtigungen 2 zuweisen** oder **Systemberechtigungen 3 zuweisen**.
4. Um alle Systemberechtigungen anzuzeigen, die in der gewählten Systemberechtigung Mitglied sind, wählen Sie den Tabreiter **Hat Mitglieder**.
5. Um alle Systemberechtigungen anzuzeigen, in denen die gewählte Systemberechtigung Mitglied ist, wählen Sie den Tabreiter **Ist Mitglied in**.

Verwandte Themen

- Systemberechtigungen in Cloud-Anwendungen auf Seite 75

Überblick über Systemberechtigungen in Cloud-Anwendungen anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Systemberechtigung.

Um einen Überblick über eine Systemberechtigung zu erhalten

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Passend zur gewählten Systemberechtigung, wählen Sie die Aufgabe **Überblick über Systemberechtigung 1**, **Überblick über Systemberechtigung 2** oder **Überblick über Systemberechtigung 3**.

Verwandte Themen

- Systemberechtigungen in Cloud-Anwendungen auf Seite 75

Berechtigungselemente in einer Cloud-Anwendung

Berechtigungselemente bilden entweder Systemberechtigungen vom Typ `Permissionset` oder beliebige weitere Objekte der Cloud-Anwendung ab.

Um die Stammdaten eines Berechtigungselements anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
3. Wählen Sie die Aufgabe **Stammdaten anzeigen**.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Berechtigungselemente in Cloud-Anwendungen auf Seite 80
- Benutzerdefinierte Stammdaten für Berechtigungselemente in Cloud-Anwendungen auf Seite 80
- Zugewiesene Benutzerkonten anzeigen auf Seite 81
- Zugewiesene Gruppen anzeigen auf Seite 81
- Überblick über Berechtigungselemente in Cloud-Anwendungen anzeigen auf Seite 82

Verwandte Themen

- Typen von Systemberechtigungen in Cloud-Anwendungen auf Seite 69
- Gruppen und Systemberechtigungen in Cloud-Anwendungen auf Seite 69

Allgemeine Stammdaten für Berechtigungselemente in Cloud-Anwendungen

Für ein Berechtigungselement erhalten Sie die folgenden Stammdaten.

Tabelle 29: Allgemeine Stammdaten eines Berechtigungselements

Eigenschaft	Beschreibung
Cloud-Anwendung	Cloud-Anwendung, in der das Berechtigungselement gültig ist.
Berechtigungselement	Bezeichnung des Berechtigungselements.
Kanonischer Name	Kanonischer Name des Berechtigungselements.
Definierter Name	Definierter Name des Berechtigungselements.
Berechtigungstyp	Typ des Berechtigungselements.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Verwandte Themen

- Berechtigungselemente in einer Cloud-Anwendung auf Seite 79

Benutzerdefinierte Stammdaten für Berechtigungselemente in Cloud-Anwendungen

Auf dem Tabreiter **Benutzerdefiniert** erhalten Sie unternehmensspezifische Angaben zu einem Berechtigungselement.

Tabelle 30: Benutzerdefinierte Stammdaten eines Berechtigungselements

Eigenschaft	Beschreibung
Freies Feld Nr. 01- Freies Feld	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder

Eigenschaft	Beschreibung
Nr. 05	können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freies Datum Nr. 01- Freies Datum Nr. 03	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freier Text Nr. 01- Freier Text Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freie Option Nr. 01 - Freie Option Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Zugewiesene Benutzerkonten anzeigen

Über diese Aufgabe sehen Sie alle Benutzerkonten, die dem Berechtigungselement zugewiesen sind.

Um zugewiesene Benutzerkonten anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.

Verwandte Themen

- Benutzerkonten in Cloud-Anwendungen auf Seite 63
- Berechtigungselemente in einer Cloud-Anwendung auf Seite 79

Zugewiesene Gruppen anzeigen

Über diese Aufgabe sehen Sie alle Gruppen, die dem Berechtigungselement zugewiesen sind.

Um zugewiesene Gruppen anzuzeigen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.

Verwandte Themen

- Gruppen in Cloud-Anwendungen auf Seite 71
- Berechtigungselemente in einer Cloud-Anwendung auf Seite 79

Überblick über Berechtigungselemente in Cloud-Anwendungen anzeigen

Auf dem Überblicksformular erhalten Sie auf einen Blick die wichtigsten Informationen zu einem Berechtigungselement.

Um einen Überblick über ein Berechtigungselement zu erhalten

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > <Cloud-Anwendung> > Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
3. Wählen Sie die Aufgabe **Überblick über das Berechtigungselement**.

6

Basisdaten für die Verwaltung von Cloud-Anwendungen

Für die Verwaltung einer Cloud-Anwendung im One Identity Manager sind folgende Basisdaten relevant.

- Zielsystemtypen

  An den Zielsystemtypen werden Einstellungen für die Provisionierung von Mitgliedschaften und die Einzelobjektsynchronisation vorgenommen. Zusätzlich dient der Zielsystemtyp zur Abbildung der Objekte im Unified Namespace.

  Weitere Informationen finden Sie unter Provisionierung von Mitgliedschaften konfigurieren auf Seite 36 und Einzelobjektsynchronisation konfigurieren auf Seite 38.

- Server

  Für die Verarbeitung der cloud-spezifischen Prozesse im One Identity Manager müssen die Server mit ihren Serverfunktionen bekannt sein. Dazu gehört beispielsweise der Synchronisationsserver.

  Weitere Informationen finden Sie unter Jobserver für cloud-spezifische Prozessverarbeitung auf Seite 84.

- Cloud-Administratoren

  Im One Identity Manager können Sie jeder Cloud-Anwendung Personen zuweisen, die die Synchronisation dieser Cloud-Anwendung mit dem One Identity Manager konfigurieren können. Im One Identity Manager ist eine Standardanwendungsrolle für die Cloud-Administratoren vorhanden. Weisen Sie dieser Anwendungsrolle die Personen zu, die berechtigt sind, Synchronisationen einzurichten und manuelle Provisionierungen durchzuführen. Bei Bedarf erstellen Sie weitere Anwendungsrollen.

  Weitere Informationen finden Sie unter Cloud-Administratoren auf Seite 88.

- Cloud-Operatoren

  Im One Identity Manager können Sie jeder Cloud-Anwendung Personen zuweisen, die manuelle Provisionierungen durchführen können. Im One Identity Manager ist eine Standardanwendungsrolle für die Cloud-Operatoren vorhanden. Bei Bedarf erstellen Sie weitere Anwendungsrollen.

Weitere Informationen finden Sie unter Cloud-Operatoren auf Seite 90.

- Cloud-Auditoren

  Im One Identity Manager können Sie jeder Cloud-Anwendung Personen zuweisen, die Provisionierungsvorgänge im Web Portal auditieren können. Im One Identity Manager ist eine Standardanwendungsrolle für die Cloud-Auditoren vorhanden. Bei Bedarf erstellen Sie weitere Anwendungsrollen.

  Weitere Informationen finden Sie unter Cloud-Auditoren auf Seite 92.

Jobserver für cloud-spezifische Prozessverarbeitung

Für die Verarbeitung der cloud-spezifischen Prozesse im One Identity Manager muss der Synchronisationsserver mit seinen Serverfunktionen bekannt sein. Um die Funktion eines Servers zu definieren, haben Sie mehrere Möglichkeiten:

- Erstellen Sie im Designer in der Kategorie **Basisdaten > Installationen > Jobserver** einen Eintrag für den Jobserver. Ausführliche Informationen dazu finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Wählen Sie im Manager in der Kategorie **Universal Cloud Interface > Basisdaten zur Konfiguration > Server** einen Eintrag für den Jobserver und bearbeiten Sie die Stammdaten des Jobservers.

  Nutzen Sie dieses Verfahren, wenn der Jobserver bereits im One Identity Manager bekannt ist und Sie für den Jobserver spezielle Funktionen konfigurieren möchten.

Verwandte Themen

- Systemanforderungen für den SCIM Synchronisationsserver auf Seite 15

Jobserver für Cloud-Anwendungen bearbeiten

HINWEIS: Damit ein Server seine Funktion im One Identity Manager Netzwerk ausführen kann, muss ein One Identity Manager Service installiert, konfiguriert und gestartet sein. Gehen Sie dazu wie im *One Identity Manager Installationshandbuch* beschrieben vor.

Um einen Jobserver und seine Funktionen zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface > Basisdaten zur Konfiguration > Server**.
2. Wählen Sie in der Ergebnisliste den Jobserver-Eintrag.

3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für den Jobserver.
5. Wählen Sie die Aufgabe **Serverfunktionen zuweisen** und legen Sie die Serverfunktionen fest.
6. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Jobserver auf Seite 85
- Festlegen der Serverfunktionen auf Seite 87

Allgemeine Stammdaten für Jobserver

HINWEIS: Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten > Installationen > Jobserver** zur Verfügung.

HINWEIS: Abhängig von den installierten Modulen können weitere Eigenschaften verfügbar sein.

Tabelle 31: Eigenschaften eines Jobservers

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS Syntax. Syntax: `<Name des Servers>.<Vollqualifizierter Domänenname>`
Zielsystem	Zielsystem des Computerkontos.
Sprachkultur	Sprache des Servers.
Server ist Cluster	Gibt an, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. HINWEIS: Die Eigenschaften **Server ist Cluster** und **Server gehört zu Cluster** schließen einander aus.
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.
IP-Adresse (IPv4)	Internet Protokoll Version 4 (IPv4)-Adresse des Servers.
Kopierverfahren (Quellserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Quelle einer Kopieraktion ist. Derzeit werden nur Kopierverfahren über die Programme `Robocopy` und `rsync` unterstützt.

Eigenschaft	Bedeutung
	Wird kein Verfahren angegeben, ermittelt der One Identity Manager Service zur Laufzeit das Betriebssystem des Servers, auf dem die Kopieraktion ausgeführt wird. Die Replikation erfolgt dann zwischen Servern mit einem Windows Betriebssystem mit dem Programm Robocopy und zwischen Servern mit einem Linux Betriebssystem mit dem Programm rsync. Unterscheiden sich die Betriebssysteme des Quellservers und des Zielservers, so ist für eine erfolgreiche Replikation die Angabe der zulässigen Kopierverfahren zwingend erforderlich. Es wird das Kopierverfahren eingesetzt, das beide Server unterstützen.
Kopierverfahren (Zielserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Ziel einer Kopieraktion ist.
Codierung	Codierung des Zeichensatzes mit der Dateien auf dem Server geschrieben werden.
Übergeordneter Jobserver	Bezeichnung des übergeordneten Jobservers.
Ausführender Server	Bezeichnung des ausführenden Servers. Eingetragen wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden. Diese Angabe wird bei der automatischen Aktualisierung des One Identity Manager Service ausgewertet. Verarbeitet ein Server mehrere Queues, wird mit der Auslieferung von Prozessschritten solange gewartet, bis alle Queues, die auf demselben Server abgearbeitet werden, die automatische Aktualisierung abgeschlossen haben.
Queue	Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Mit dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Serverbetriebssystem	Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte **Win32**, **Windows**, **Linux** und **Unix**. Ist die Angabe leer, wird **Win32** angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen.

Eigenschaft	Bedeutung
One Identity Manager Service installiert	Gibt an, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur QBM_PJobQueueLoad aktiviert, sobald die Queue das erste Mal angefragt wird. Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.
Stopp One Identity Manager Service	Gibt an, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten. Den Dienst können Sie mit entsprechenden administrativen Berechtigungen im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*.
Kein automatisches Softwareupdate	Gibt an, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.
Softwareupdate läuft	Gibt an, ob gerade eine Softwareaktualisierung ausgeführt wird.
Serverfunktion	Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

Verwandte Themen

- Festlegen der Serverfunktionen auf Seite 87

Festlegen der Serverfunktionen

HINWEIS: Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten > Installationen > Jobserver** zur Verfügung.

Die Serverfunktion definiert die Funktion eines Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

HINWEIS: Abhängig von den installierten Modulen können weitere Serverfunktionen verfügbar sein.

Tabelle 32: Zulässige Serverfunktionen

Serverfunktion	Anmerkungen
Aktualisierungsserver	Der Server führt die automatische Softwareaktualisierung aller anderen Server aus. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Der Server kann SQL Aufträge ausführen. Bei der initialen Schemainstallation wird der Server, auf dem die One Identity Manager-Datenbank installiert ist, mit dieser Serverfunktion gekennzeichnet.
SQL Ausführungsserver	Der Server kann SQL Aufträge ausführen. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Für eine Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.
CSV Skriptserver	Der Server kann CSV-Dateien per Prozesskomponente `ScriptComponent` verarbeiten.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
SMTP Host	Server, auf dem durch den One Identity Manager Service E-Mail Benachrichtigungen verschickt werden. Voraussetzung zum Versenden von Mails durch den One Identity Manager Service ist ein konfigurierter SMTP Host.
Standard Berichtserver	Server, auf dem die Berichte generiert werden.
SCIM Konnektor	Der Server kann sich mit einer Cloud-Anwendung verbinden.

Verwandte Themen

- Allgemeine Stammdaten für Jobserver auf Seite 85

Cloud-Administratoren

Im One Identity Manager können Sie jeder Cloud-Anwendung Personen zuweisen, die die Synchronisation dieser Cloud-Anwendung mit dem One Identity Manager konfigurieren können. Im One Identity Manager ist eine Standardanwendungsrolle für die Cloud-Administratoren vorhanden. Weisen Sie dieser Anwendungsrolle die Personen zu, die berechtigt sind, Synchronisationen einzurichten und manuelle Provisionierungen durchzuführen. Bei Bedarf erstellen Sie weitere Anwendungsrollen.

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

Inbetriebnahme der Anwendungsrolle für Cloud-Administratoren

1. Der One Identity Manager Administrator legt Personen als Administratoren für das Universal Cloud Interface fest.
2. Die Cloud-Administratoren nehmen die Personen in die Standardanwendungsrolle für Operatoren und Auditoren auf.

   Administratoren der Standardanwendungsrolle sind berechtigt alle Cloud-Anwendungen im One Identity Manager zu bearbeiten.
3. Administratoren können weitere Personen als Administratoren berechtigen und bei Bedarf untergeordnete Anwendungsrollen erstellen.

Tabelle 33: Standardanwendungsrolle für Cloud-Administratoren

Benutzer	Aufgaben
Cloud-Administratoren	Die Cloud-Administratoren müssen der Anwendungsrolle **Universal Cloud Interface | Administratoren** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Administrieren die Anwendungsrollen für das Universal Cloud Interface. • Richten bei Bedarf weitere Anwendungsrollen ein. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Cloud-Anwendung und One Identity Manager. • Bearbeiten im Manager die Cloud-Anwendungen. • Bearbeiten offene, manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken. • Erhalten im Web Portal und im Manager Informationen über die Cloud-Objekte.

Um eine Person initial als Cloud-Administrator festzulegen

1. Melden Sie sich als One Identity Manager Administrator (Anwendungsrolle **Basisrollen | Administratoren**) am Manager an.
2. Wählen Sie die Kategorie **One Identity Manager Administration > Universal Cloud Interface > Administratoren**.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Person zu und speichern Sie die Änderung.

Um weitere Personen als Cloud-Administratoren zu berechtigen

1. Melden Sie sich mit der Anwendungsrolle **Universal Cloud Interface | Administratoren** am Manager an.
2. Wählen Sie in der Kategorie **Universal Cloud Interface > Basisdaten zur Konfiguration > Universal Cloud Interface Verantwortliche > Administratoren** die Anwendungsrolle.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Person zu und speichern Sie die Änderung.

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung von Cloud-Anwendungen auf Seite 10
- Provisionierungsvorgänge einsehen und bearbeiten auf Seite 56

Cloud-Operatoren

Im One Identity Manager können Sie jeder Cloud-Anwendung Personen zuweisen, die manuelle Provisionierungen durchführen können. Im One Identity Manager ist eine Standardanwendungsrolle für die Cloud-Operatoren vorhanden. Bei Bedarf erstellen Sie weitere Anwendungsrollen.

Tabelle 34: Standardanwendungsrolle für Cloud-Operatoren

Benutzer	Aufgaben
Cloud-Operatoren	Die Cloud-Operatoren müssen der Anwendungsrolle **Universal Cloud Interface | Operatoren** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Bearbeiten offene manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken.

TIPP: Wenn Sie die Bearbeitungsberechtigungen der Cloud-Operatoren auf einzelne Cloud-Anwendungen einschränken wollen, definieren Sie untergeordnete Anwendungsrollen für diese Cloud-Anwendungen.

Um Cloud-Operatoren festzulegen

1. Melden Sie sich mit der Anwendungsrolle **Universal Cloud Interface | Administratoren** am Manager an.
2. Wählen Sie die Kategorie **Universal Cloud Interface > Basisdaten zur Konfiguration > Cloud-Anwendungen**.

3. Wählen Sie in der Ergebnisliste die Cloud-Anwendung.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Operatoren** die Anwendungsrolle.

   - ODER -

   Klicken Sie neben der Auswahlliste **Operatoren** auf , um eine neue Anwendungsrolle zu erstellen.

   - Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Universal Cloud Interface | Operatoren** zu.
   - Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.
6. Speichern Sie die Änderungen.
7. Weisen Sie der Anwendungsrolle die Personen zu, die berechtigt sind, Provisionierungsvorgänge für diese Cloud-Anwendung zu bearbeiten.

HINWEIS: Sie können Cloud-Operatoren auch für einzelne Container festlegen. Die Operatoren eines Containers sind berechtigt, die manuellen Provisionierungsvorgänge dieses Containers zu bearbeiten. Operatoren für Container legen Sie in der Kategorie **Universal Cloud Interface | <Cloud-Anwendung> | Containerstruktur** fest.

Um Personen in eine Anwendungsrolle aufzunehmen

1. Melden Sie sich mit der Anwendungsrolle **Universal Cloud Interface | Administratoren** am Manager an.
2. Wählen Sie in der Kategorie **Universal Cloud Interface > Basisdaten zur Konfiguration > Universal Cloud Interface Verantwortliche > Operatoren** die Anwendungsrolle.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Personen zu und speichern Sie die Änderungen.

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

Verwandte Themen

- Allgemeine Stammdaten für Cloud-Anwendungen auf Seite 59
- Containerstrukturen in Cloud-Anwendungen auf Seite 62
- Offene Provisionierungsvorgänge bearbeiten auf Seite 55
- One Identity Manager Benutzer für die Verwaltung von Cloud-Anwendungen auf Seite 10

Cloud-Auditoren

Im One Identity Manager können Sie jeder Cloud-Anwendung Personen zuweisen, die Provisionierungsvorgänge im Web Portal auditieren können. Im One Identity Manager ist eine Standardanwendungsrolle für die Cloud-Auditoren vorhanden. Bei Bedarf erstellen Sie weitere Anwendungsrollen.

Tabelle 35: Standardanwendungsrolle für Cloud-Auditoren

Benutzer	Aufgaben
Cloud-Auditoren	Die Cloud-Auditoren müssen der Anwendungsrolle **Universal Cloud Interface | Auditoren** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sehen manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken.

Um Personen als Cloud-Auditoren festzulegen

1. Melden Sie sich mit der Anwendungsrolle **Universal Cloud Interface \| Administratoren** am Manager an.
2. Wählen Sie die Kategorie **Universal Cloud Interface > Basisdaten zur Konfiguration > Universal Cloud Interface Verantwortliche > Auditoren**.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Personen zu und speichern Sie die Änderungen.

Um weitere Anwendungsrollen für Cloud-Auditoren zu erstellen

1. Melden Sie sich mit der Anwendungsrolle **Universal Cloud Interface \| Administratoren** am Manager an.
2. Wählen Sie die Kategorie **Universal Cloud Interface > Basisdaten zur Konfiguration > Universal Cloud Interface Verantwortliche > Auditoren**.
3. Klicken Sie in der Ergebnisliste .
4. Bearbeiten Sie die Stammdaten der Anwendungsrolle.
    - Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Universal Cloud Interface \| Auditoren** oder eine untergeordnete Anwendungsrolle zu.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Alle Provisionierungsvorgänge einsehen auf Seite 56
- One Identity Manager Benutzer für die Verwaltung von Cloud-Anwendungen auf Seite 10

Anhang A

Standardprojektvorlage für Cloud-Anwendungen

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.

Detaillierte Informationen zum Thema

- Projektvorlage für SCIM-Umgebungen auf Seite 94
- Projektvorlage für One Identity Starling Connect-Umgebungen auf Seite 95

Projektvorlage für SCIM-Umgebungen

Für die Synchronisation einer beliebigen System for Cross-domain Identity Management-Umgebung nutzen Sie die Projektvorlage **SCIM Synchronisation**. Die Projektvorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 36: Abbildung der SCIM Schematypen auf Tabellen im One Identity Manager Schema

SCIM Schematyp	Tabelle im One Identity Manager Schema
Group	UCIGroup
User	UCIUser

Projektvorlage für One Identity Starling Connect-Umgebungen

Für die Synchronisation einer SCIM-Umgebung über One Identity Starling Connect nutzen Sie die Projektvorlage **Synchronisation einer One Identity Starling Connect-Umgebung**. Die Projektvorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 37: Abbildung der One Identity Starling Connect Schematypen auf Tabellen im One Identity Manager Schema

SCIM Schematyp	Tabelle im One Identity Manager Schema
Group	UCIGroup
User	UCIUser
Permissionset	UCIItem
Role	UCIGroup1
Profile	UCIGroup2
Entitlement	UCIGroup3

Anhang B

Verarbeitungsmethoden von Cloud-Systemobjekten

Folgende Tabelle beschreibt die zulässigen Verarbeitungsmethoden für die SCIM Schematypen und benennt notwendige Einschränkungen bei der Verarbeitung der Systemobjekte. One Identity Manager lässt standardmäßig alle Verarbeitungsmethoden zu. Ob diese Verarbeitungsmethoden in der angebundenen Cloud-Anwendung genutzt werden können, ist von der Implementierung der Cloud-Anwendung abhängig.

Tabelle 38: Zulässige Verarbeitungsmethoden für SCIM Schematypen

Schematyp	Lesen	Einfügen	Löschen	Aktualisieren
Benutzerkonto (`User`)	ja	ja	ja	ja
Berechtigungselement (`UCIItem`)	ja	ja	ja	ja
Gruppe (`Group`)	ja	ja	ja	ja
Systemberechtigung 1 (`UCIGroup1`)	ja	ja	ja	ja
Systemberechtigung 2 (`UCIGroup2`)	ja	ja	ja	ja
Systemberechtigung 3 (`UCIGroup3`)	ja	ja	ja	ja

Anhang C

Konfigurationsparameter für die Verwaltung von Cloud-Anwendungen

Folgende Konfigurationsparameter werden benötigt.

Tabelle 39: Zusätzliche Konfigurationsparameter

Konfigurationsparameter	Bedeutung
QBM | PendingChange	Allgemeiner Konfigurationsparameter für die Konfiguration von anstehenden Änderungen.
QBM | PendingChange | LifeTimeError	Der Konfigurationsparameter legt den Aufbewahrungszeitraum (in Tagen) für fehlgeschlagene Provisionierungsvorgänge fest. Der Standardzeitraum beträgt **30** Tage.
QBM | PendingChange | LifeTimeRunning	Der Konfigurationsparameter legt den Aufbewahrungszeitraum (in Tagen) für offene Provisionierungsvorgänge fest. Der Standardzeitraum beträgt **60** Tage.
QBM | PendingChange | LifeTimeSuccess	Der Konfigurationsparameter legt den Aufbewahrungszeitraum (in Tagen) für erfolgreiche Provisionierungsvorgänge fest. Der Standardzeitraum beträgt **2** Tage.
TargetSystem | CSM | ApplicationType	Konfiguration der verschiedenen Cloud-Anwendungen.
TargetSystem | CSM | ApplicationType | Salesforce	Einstellungen für Salesforce Anwendungen.
TargetSystem | CSM | ApplicationType | Salesforce | DefaultProfileName	Name des Standardprofils, welches neuen Salesforce Benutzern zugewiesen wird.

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

Anstehende Änderung 49, 51
- Aufbewahrungszeitraum 51

Anwendungsrolle 10
- Cloud-Administrator 88
- Cloud-Auditor 92
- Cloud-Operator 90

Auditor 52

B

Basisobjekt 32, 38

Benutzerkonto (Cloud-Anwendung) 63
- Kontomanager 66
- Logindaten 65
- Stammdaten 64
- Überblicksformular 68
- zugewiesene Berechtigungselemente 68
- zugewiesene Gruppen 67
- zugewiesene Systemberechtigungen 67

Berechtigungselement (Cloud-Anwendung) 79
- Berechtigungstyp 80
- zugewiesene Benutzerkonten 81
- zugewiesene Gruppen 81

C

Cloud-Administrator 10, 88

Cloud-Anwendung 58
- alternative Spaltenbezeichnung 61
- anzeigen 59
- bearbeiten 59
- Benutzer 10
- Benutzerkonto löschen 59
- manuelle Provisionierung 59
- Operator 59
- Systemberechtigung 59

Cloud-Auditor 10, 92

Cloud-Operator 10, 90

Cloud Benutzerkonto
- Standardprofil 47

Container 62
- Kontomanager 62
- Operator 62

E

Einzelobjekt synchronisieren 45

Einzelobjektsynchronisation 38, 45
- beschleunigen 39

G

Gruppe (Cloud-Anwendung) 71
- Container 72
- Gruppentyp 72
- Kontomanager 72
- zugewiesene Benutzerkonten 73
- Zugewiesene Berechtigungslemente 74
- zugewiesene Gruppen 73

J

Jobserver 84
- bearbeiten 15
- Eigenschaften 85
- Lastverteilung 39

K

Konfigurationsparameter 97
Kontomanager 66

L

Lastverteilung 39
Lokaler Cache 21

M

Mitgliedschaft
- Änderung provisionieren 36

O

Operator 52

P

Projektvorlage 94
Provisionierung 49
- beschleunigen 39
- manuell 52
- Mitgliederliste 36

Provisionierungsvorgang 52
- anzeigen 51
- fehlgeschlagen 51
- löschen 51
- offen 51

R

Ressourcenkonfiguration 40
Revisionsfilter 35

S

Schema
- aktualisieren 34
- Änderungen 34
- komprimieren 34

Schemadefinition 40
Server 84
Serverfunktion 87
Startkonfiguration 32
Synchronisation
- Benutzer 13
- Berechtigungen 13
- beschleunigen 35
- Cache nutzen 21
- einrichten 13
- konfigurieren 21, 29
- nur Änderungen 35
- Scope 29
- starten 42
- Synchronisationsprojekt
  - erstellen 21
- Verbindungsparameter 21, 29
- verhindern 44
- Voraussetzung 12
- Workflow 21, 31
- Zeitplan 42

Synchronisationskonfiguration
- anpassen 29, 31

Synchronisationsprojekt
bearbeiten 62
deaktivieren 44
erstellen 21
Projektvorlage 94
Synchronisationsprotokoll 43
erstellen 29
Inhalt 29
Synchronisationsrichtung
In das Zielsystem 21, 31
In den One Identity Manager 21
Synchronisationsserver 14, 84
bearbeiten 84
installieren 15
Jobserver 15
konfigurieren 15
Serverfunktion 87
Systemanforderungen 15
Synchronisationsworkflow
erstellen 21, 31
Systemberechtigung
Typ 69
Zuweisung
benutzerbasiert 69
berechtigungsbasiert 69
speichern 69
Systemberechtigung (Cloud-Anwendung) 75
Systemberechtigung (Cloud-Anwendung)
Container 76
Gruppentyp 76
Kontomanager 76
zugewiesene Benutzerkonten 77
zugewiesene Systemberechtigungen 78
Systemverbindung
aktives Variablenset 33
ändern 31

U

Überlagerungsdatei 40

V

Variablenset 32
aktiv 33
Verbindungsparameter umwandeln 32

Z

Zeitplan 42
deaktivieren 44