Connector Administration

Connector Guide für Pivotal Cloud Foundry Connector Release 1.0.0

Autor: Dieter Steding  
 Sophie Strecke

Erstelldatum: 27-11-2019

Letzte Änderung: 30-10-2020

Kontrollnummer: OC\_DE/300516442/DO.081/0024

Version: 1.0

**Freigabe:**

|  |  |
| --- | --- |
| Bundeskriminalamt |  |
| Oracle Consulting |  |

logored Kopie-Nr. \_\_\_\_\_

## Dokumentenkontrolle

### Änderungshistorie

| Date | Autor | Version | | Änderungsreferenz |
| --- | --- | --- | --- | --- |
|  |  |  |  | |
| 27-11-19 | Dieter Steding | 1.0 | Kein vorheriges Dokument | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |

### Reviewer

| Name | Position |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Inhalt

[Dokumentenkontrolle ii](#_Toc55044610)

[Änderungshistorie ii](#_Toc55044611)

[Reviewer ii](#_Toc55044612)

[Einführung 1](#_Toc55044613)

[Leserkreis 1](#_Toc55044614)

[Bezugsdokumente 1](#_Toc55044615)

[Vertraulichkeit 1](#_Toc55044616)

[Typografische Konventionen 1](#_Toc55044617)

[Pivotal Cloud Foundry Foundation Connector 2](#_Toc55044618)

[Hardware und Software Zertifizierung 2](#_Toc55044619)

[Erforderliche Komponentenversionen 2](#_Toc55044620)

[Erforderliche Patches 3](#_Toc55044621)

[Architektur 3](#_Toc55044622)

[Funktionen 3](#_Toc55044623)

[Authentisierung 3](#_Toc55044624)

[Sichere Kommunikation 4](#_Toc55044625)

[Provisionierung von Benutzerkonten 4](#_Toc55044626)

[Vollständiger und inkrementeller Datenabgleich 4](#_Toc55044627)

[Eingeschränkter Datenabgleich 4](#_Toc55044628)

[Batch Datenabgleich 4](#_Toc55044629)

[Wertelisten 4](#_Toc55044630)

[Vorkonfigurierte Wertelisten 5](#_Toc55044631)

[Synchronisierte Wertelisten 6](#_Toc55044632)

[Bereitstellen des Pivotal Cloud Foundry Foundation Connector 8](#_Toc55044633)

[Vorbereitung 8](#_Toc55044634)

[Implementieren der benutzerdefinierten Authentifizierung 8](#_Toc55044635)

[Implementieren von benutzerdefiniertem Parsing 9](#_Toc55044636)

[Installation 10](#_Toc55044637)

[Grundlagen der Installation 10](#_Toc55044638)

[Installation in Identity Manager 10](#_Toc55044639)

[Konfigurieren der IT-Ressource für das Zielsystem 10](#_Toc55044640)

[Informationen zu Kategorien von Parameter von IT-Ressourcen 11](#_Toc55044641)

[Parameter von IT-Ressourcen 12](#_Toc55044642)

[Angeben von Werten für Parameter einer IT-Ressource 13](#_Toc55044643)

[Postinstallation 13](#_Toc55044644)

[Konfiguration Identity Manager 13](#_Toc55044645)

[Löschen von Inhalten aus dem Server-Cache 14](#_Toc55044646)

[Verwalten der Protokollierung 15](#_Toc55044647)

[Konfigurieren von SSL für den Connector 16](#_Toc55044648)

[Verwenden des Pivotal Cloud Foundry Foundation Connector 18](#_Toc55044649)

[Verwendung von Wertelisten 18](#_Toc55044650)

[Vorkonfigurierte Wertelisten 18](#_Toc55044651)

[Synchronisierte Wertelisten 19](#_Toc55044652)

[Abgleichsvorgänge konfigurieren 20](#_Toc55044653)

[Regeln für den Datenabgleich 20](#_Toc55044654)

[Vollständiger und inkrementeller Datenabgleich 20](#_Toc55044655)

[Eingeschränkter Datenabgleich 20](#_Toc55044656)

[Hintergrundprozess 21](#_Toc55044657)

[Synchronisierung von Wertelisten 21](#_Toc55044658)

[Abgleich von Benutzerdatensätzen 21](#_Toc55044659)

[Abgleich gelöschter Benutzerdatensätze 22](#_Toc55044660)

[Hintergrundprozesse konfigurieren 22](#_Toc55044661)

[Provisionierungsvorgänge ausführen 23](#_Toc55044662)

[Deinstallation des Connectors 23](#_Toc55044663)

[Limitierungen des Pivotal Cloud Foundry Foundation Connector 24](#_Toc55044664)

[Zuweisung von Rollen in Spaces 24](#_Toc55044665)

[Entzug von Rollen in Organisationen 24](#_Toc55044666)

## Einführung

### Leserkreis

Dieses Dokument wendet sich an Personen, die sich mit der Installation der Oracle Identity und Access Management Infrastruktur befassen

### Bezugsdokumente

Informationen zur Installation und Verwendung von Oracle Identity und Access Management finden Sie auf der folgenden Oracle-Hilfeseite:

* https://docs.oracle.com/en/middleware/idm/suite/12.2.1.3/index.html

### Vertraulichkeit

Das in dieser Dokumentation enthaltene Material enthält geschützte, vertrauliche Informationen zu Oracle-Produkten und –Methoden.

Die Leserschaft erklärt sich damit einverstanden, dass die Informationen in dieser Dokumentation nicht nach außerhalb weitergegeben und nicht für andere Zwecke als zur Bewertung dieses Verfahrens vervielfältigt, verwendet oder weitergegeben werden.

### Typografische Konventionen

Die folgenden typografischen Konventionen werden in diesem Dokument verwendet.

|  |  |
| --- | --- |
| **Konvention** | **Bedeutung** |
| **Fettdruck** | Fettdruck kennzeichnet Elemente der grafischen Benutzeroberfläche, die einer Aktion zugeordnet sind, oder Begriffe, die im Text oder im Glossar definiert sind. |
| *kursiv* | Kursivschrift kennzeichnet Buchtitel, Hervorhebungen oder Platzhalter, für die Sie bestimmte Werte angeben. |
| monospace | Monospace kennzeichnet in einem Absatz Befehle, URLs, Code-Beispiele, Text, der auf dem Bildschirm angezeigt wird, oder Text, den Sie eingeben.. |

## Pivotal Cloud Foundry Foundation Connector

Der Pivotal Cloud Foundry Foundation Connector integriert Oracle Identity Manager (OIM) in Pivotal Cloud Foundry Foundation. Oracle Identity Manager ist eine zentralisierte Identitätsverwaltungslösung, die sich selbst für Service-, Compliance-, Bereitstellungs- und Kennwortverwaltungsdienste für Anwendungen vor Ort oder in der Cloud bereitstellt. Oracle Identity Manager-Konnektoren werden verwendet, um Oracle Identity Manager in externe, identitätsbezogene Anwendungen zu integrieren. Mit dem Pivotal Cloud Foundry Foundation Connector können Sie Pivotal Cloud Foundry Foundation Service als verwaltete (Ziel-) Ressource in Oracle Identity Manager verwenden.

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| In diesem Handbuch wird der Begriff Zielsystem manchmal für Pivotal Cloud Foundry Foundation Service verwendet. |

Die folgenden Themen bieten einen allgemeinen Überblick über den Pivotal Cloud Foundry Foundation Connector:

Einführung in den Pivotal Cloud Foundry Foundation Connector

Mit dem Pivotal Cloud Foundry Foundation Connector können Sie den Pivotal Cloud Foundry Foundation Service als verwaltete (Ziel-) Quelle von Identitätsdaten für Oracle Identity Manager verwenden. Im Modus der Benutzerkontenverwaltung (Zielressource) des Connectors werden die Daten zu den Benutzern die direkt auf dem Zielsystem erstellt oder geändert mit Oracle Identity Manager abgeglichen. Diese Daten werden verwendet, um neue Ressourcen bereitzustellen (zuzuweisen) oder Ressourcen zu aktualisieren, die Identitäten in Oracle Identity Manager bereits zugewiesen wurden. Sie können Oracle Identity Manager auch zum Bereitstellen oder Aktualisieren von Pivotal Cloud Foundry Foundation-Ressourcen (Benutzerkonten) verwenden, die Identitäten in Oracle Identity Manager zugewiesen sind. Diese in Oracle Identity Manager durchgeführten Bereitstellungsvorgänge werden in die Erstellung oder Aktualisierung von Zielsystemkonten übersetzt.

### Hardware und Software Zertifizierung

Die plattformspezifischen Anforderungen an Hardware und Software, die in diesem Dokument aufgeführt werden, sind gültig für den Zeitpunkt zu dem, dieses Dokument erstellt wurde. Da neue Plattformen und Betriebssysteme zertifiziert werden können, nachdem dieses Dokument veröffentlicht wurde, wird empfohlen die Zertifizierungsmatrix auf Oracle Technology Network heranzuziehen. Dort befinden sich die aktuellsten Aussagen zu zertifizierten Plattformen und Betriebssystemen.

Die jeweilige Zertifizierungsmatrix für Produkte der Oracle Identity und Access Management Suite sind unter folgenden URLs verfügbar:

[Oracle® Fusion Middleware 12c (12.2.1.3.0)](https://www.oracle.com/technetwork/middleware/fmw-122130-certmatrix-3867828.xlsx)

#### Erforderliche Komponentenversionen

| **Komponente** | **Version** |
| --- | --- |
| **Oracle Java Development Kit** | JDK 1.8.0\_131 oder höher |
| **Oracle Infrastruktur** | Oracle® WebLogic 12c (12.2.1.3.0) |
| **Oracle Datenbank** | Oracle® RDBMS 12c (12.2.0.1.0 oder höher |
| **Oracle Identity Governance** | Oracle® Identity Governance 12c Release 12.2.1.3.0 |

#### Erforderliche Patches

| **Komponente** | **Patch** |
| --- | --- |
| **Oracle Identity Governance** | Patch 30735905 (Oracle® Identity Governance Bundle Patch ID:200108.2108) |

### Architektur

Der Pivotal Cloud Foundry Foundation Service Connector wird mithilfe des Identity Connector Framework (ICF) implementiert. Die ICF ist eine Komponente, die grundlegende Abstimmungs- und Bereitstellungsvorgänge bietet, die allen Oracle Identity Manager-Connectors gemeinsam sind. Darüber hinaus bietet ICF allgemeine Funktionen, die Entwickler sonst selbst implementieren müssten, z. B. Verbindungspooling, Pufferung, Zeitüberschreitungen und Filterung. Die ICF wird zusammen mit Oracle Identity Manager ausgeliefert.

Abbildung 1–1 zeigt die Integration von Oracle Identity Manager on-premise in den Pivotal Cloud Foundry Foundation Service. Der Pivotal Cloud Foundry Foundation Service Connector folgt einem hybriden Datenverwaltungssystem, das Möglichkeiten für Unternehmen bietet, die in Oracle Identity Manager invertiert haben, jedoch auf das Oracle Pivotal Cloud Foundry Foundation Service-Framework migrieren möchten. Wie aus dem Diagramm hervorgeht, kann der Pivotal Cloud Foundry Foundation Service-Connector Bereitstellungs- und Abgleichsvorgänge für Pivotal Cloud Foundry Foundation Service ausführen. In der Abbildung ist das Connector-Bundle für die Interaktion mit Pivotal Cloud Foundry Foundation Service verantwortlich, einem SCIM-kompatiblen Ziel. Daher verwendet das Connector-Paket das generische SCIM-Bundle. Das Parsen und Autorisieren erfolgt über das gemeinsame REST-Bundle, das Teil des generischen SCIM-Bundles ist. Standardmäßig unterstützt es die OAuth 2.0-Kennwortauthentifizierung für Ressourcenbesitzer.



### Funktionen

Zu den Funktionen des Connectors gehören neben der Provisionierung von Benutzerkonten, der vollständige, inkrementelle und eingeschränkte Abgleich von Benutzerkonten und der Abgleich von gelöschten Kontendaten.

#### Authentisierung

Standardmäßig unterstützt der Connector die HTTP-Basisauthentifizierung und die OAuth 2.0-Authentifizierungsmechanismen. Die unterstützten Grant-Typen für den OAuth 2.0-Authentifizierungsmechanismus sind

1. Java WebToken (JWT)
2. Client Credentials
3. Resource Owner Password.

Wenn das Zielsystem einen der vom Connector nicht unterstützten Authentifizierungsmechanismen verwendet, kann mithilfe der von diesem Connector bereitgestellten Plug-Ins eine eigene Implementierung für die benutzerdefinierte Authentifizierung hinzugefügt werden.

#### Sichere Kommunikation

Die Kommunikation zwischen Identity Manager und dem Zielsystem kann konfiguriert werden.

Informationen zum Konfigurieren der sicheren Kommunikation finden Sie unter Konfigurieren von SSL für den Connector.

#### Provisionierung von Benutzerkonten

Sie können den Connector verwenden, um Pivotal Cloud Foundry Benutzerkonten und Gruppenzuordnungen bereitzustellen. Sie können einen neuen Benutzer in Oracle Identity Manager mithilfe der Seite Benutzer erstellen.

#### Vollständiger und inkrementeller Datenabgleich

Bei einem vollständigen Datenabgleich werden alle Datensätze vom Zielsystem durch Oracle Identity Manager abgerufen. Nachdem Sie den Connector bereitgestellt haben, können Sie einen vollständigen Datenabgleich durchführen, um alle Benutzerdaten vom Zielsystem nach Oracle Identity Manager zu übertragen. Nach dem ersten vollständigen Abgleich wird der inkrementelle Abgleich automatisch aktiviert. Bei einem inkrementellen Abgleich werden Benutzerkonten, die seit der letzten Ausführung des Abgleichs hinzugefügt oder geändert wurden, durch Oracle Identity Manager abgerufen. Sie können jederzeit einen vollständigen Datenabgleich durchführen.

#### Eingeschränkter Datenabgleich

Sie können Datensätze von Benutzerkonten aus dem Zielsystem basierend auf festgelegten Filterkriterien abgleichen. Um die Datensätze einzuschränken oder zu filtern, die während der Ausführung des Abgleichs von Oracle Identity Manager abgerufen werden, können Sie die Teilmenge der hinzugefügten oder geänderten Zielsystemdatensätze angeben, die abgeglichen werden müssen.

#### Batch Datenabgleich

Abhängig von der Anzahl der Datensätze, die abgeglichen werden sollen, kann eine Aufteilung in Stapel (Batches) konfiguriert werden. Sie können die Ausführung eines Abgleichs in Stapel aufteilen, indem Sie die Anzahl der Datensätze angeben, die in jedem Stapel enthalten sein müssen.

### Wertelisten

Wertelisten die während des Datenabgleichs und Provisionierung verwendet werden, sind entweder vorkonfiguriert oder werden mit dem Zielsystem synchronisiert.

Wertelisten, die während Connector Operationen verwendet werden, können wie folgt kategorisiert werden:

1. Vorkonfigurierte Wertelisten
2. Synchronisierte Wertelisten

#### Vorkonfigurierte Wertelisten

Vorkonfigurierte Wertelisten werden in Oracle Identity Manager erstellt, wenn Sie den Connector bereitstellen. Diese Wertelisten sind entweder mit Werten vorab ausgefüllt oder müssen nach der Bereitstellung des Connectors manuell eingegeben werden.

Innerhalb dieser Kategorie von Wertelisten wird wiederum unterschieden nach:

1. Globale Wertelisten
2. Lokale Wertelisten

##### Globale Wertelisten

Globale Wertelisten sind unabhängig von einem spezifischen Zielsystem.

1. PCF.UAA.Origin

###### PCF.UAA.Origin

| **Encode** | **Decoded** | **Beschreibung** |
| --- | --- | --- |
| **unknown** | Unknown |  |
| **uaa** | Internal |  |
| **saml** | External |  |
| **oauth2.0** | Oauth 2.0 |  |
| **oidc1.0** | OpenID Connect |  |
| **ldap** | Directory Service |  |
| **keystone** | Keystone Login |  |
| **login-server** | Login Server |  |

###### PCF.ORL.Scope

| **Encode** | **Decoded** | **Beschreibung** |
| --- | --- | --- |
| **users** | User |  |
| **managers** | Manager |  |
| **auditors** | Auditor |  |
| **billing\_managers** | Billing Manager |  |

###### PCF.SRL.Scope

| **Encode** | **Decoded** | **Beschreibung** |
| --- | --- | --- |
| **managers** | Manager |  |
| **auditors** | Auditor |  |
| **developers** | Developer |  |

##### Lokale Wertelisten

Lokale Wertelisten sind nur innerhalb eines spezifischen Zielsystems (Stage) verfügbar.

1. PCF. IDP.<Stage>

###### PCF. IDP.<Stage>

| **Encode** | **Decoded** | **Beschreibung** |
| --- | --- | --- |
| **uaa** | Internal |  |

#### Synchronisierte Wertelisten

Während eines Bereitstellungsvorgangs verwenden Sie eine Werteliste im Prozessformular, um einen einzelnen Wert aus einer Reihe von Werten auszuwählen. Beispielsweise möchten Sie möglicherweise eine Gruppe aus dem Suchfeld Gruppen auswählen, um die Gruppe anzugeben, die dem Benutzer zugewiesen wird. Wenn Sie den Connector bereitstellen, werden in Oracle Identity Manager Wertelisten erstellt, die den Wertelisten des Zielsystems entsprechen. Bei der Synchronisierung von Wertelisten werden Ergänzungen oder Änderungen, die an bestimmten Feldern im Zielsystem vorgenommen wurden, in die Wertelisten in Oracle Identity Manager kopiert. Nach der Bereitstellung des Connectors werden in Oracle Identity Manager automatisch die folgenden Wertelisten erstellt, die als Quelle für Wertelisten verwendet werden:

1. PCF.UGP.<Stage>
2. PCF.ORL.<Stage>
3. PCF.SRL.<Stage>

Die Wertelisten PCF.UGP.<Stage>, PCF.ORL.<Stage> und PCF.SRL.<Stage> werden mit Werten gefüllt, die von den Hintergrundprozessen für die Wertelisten-Synchronisation aus dem Zielsystem abgerufen werden. Während eines Vorgangs zur Provisionierung eines Benutzerkontos verwenden Sie das Feld Name in der Registerkarte Gruppe im Prozessformular, um eine Gruppe dem entsprechenden Benutzerkonto zuzuweisen. Die Wertelisten für Gruppen, Organisationen und Spaces werden mit Werten aus den Wertelisten PCF.UGP.<Stage>, PCF.OSC.<Stage> und PCF.SSC.<Stage> gefüllt, die beim Bereitstellen des Connectors automatisch in Oracle Identity Manager erstellt werden.

Standardmäßig sind diese Wertelisten leer. Sie werden mit Werten gefüllt, die vom Zielsystem abgerufen werden, wenn Sie den Hintergrundprozess für die Synchronisierung von Wertelisten ausführen. Wenn Sie beispielsweise den Hintergrundprozess ausführen, werden alle Gruppen auf dem Zielsystem von Oracle Identity Manager abgerufen und in die Werteliste PCF.UGP.<Stage> eingetragen.

Nach der Synchronisierung werden die Daten in jeder der Wertelisten im folgenden Format gespeichert:

| **Wert** | **Format** | **Beschreibung** |
| --- | --- | --- |
| **Encode** | <IT\_RESOURCE\_KEY>~< ID> | IT\_RESOURCE\_KEY ist der numerische Code, der jeder IT-Ressource in Identity Manager zugewiesen wird.  ID ist der Zielsystemcode, der jedem Eintrag einer Werteliste zugewiesen ist. Dieser Wert wird basierend auf dem Attributnamen des Zielsystems ausgefüllt, der im Encode-Attribut des Hintergrundprozesses für die Synchronisierung von Wertelisten angegeben ist. |
| **Decode** | <IT\_RESOURCE\_NAME>~<VALUE> | IT\_RESOURCE\_NAME ist der Name der IT-Ressource in Identity Manager.  VALUE ist der Zielsystemcode, der jedem Eintrag einer Werteliste zugewiesen ist. Dieser Wert wird basierend auf dem Attributnamen des Zielsystems ausgefüllt, der im Decode-Attribut des geplanten Jobs für die Synchronisierung von Suchfeldern angegeben ist. |

Die nachfolgende Table zeigt beispielhafte Einträge in der Werteliste PCF.UGP.<Stage>:

| **Encode** | **Decoded** |
| --- | --- |
| **43~0001db3b-6da5-4658-9e3b-ca0169cde493** | PCF.Endpoint.<Stage>~scim.me |
| **43~1a4a9faa-c327-4946-84dc-2d94852be1f6** | PCF.Endpoint.<Stage>~clients.read |
| **43~1a4a9faa-c327-4946-84dc-2d94852be1f6** | PCF.Endpoint.<Stage>~clients.read |

## Bereitstellen des Pivotal Cloud Foundry Foundation Connector

Sie müssen den Connector in Identity Manager installieren. Bei Bedarf können Sie den Connector auch auf einem Connector-Server bereitstellen.

Die folgenden Themen enthalten Details zum Installieren und Konfigurieren Connectors:

1. Vorbereitung
2. Installation
3. Postinstallation

### Vorbereitung

Die Vorbereitung für den Connector umfasst die Implementierung einer benutzerdefinierten Authentifizierung und die Implementierung eines benutzerdefinierten Parsers. Für den Connector werden diese Schritte vor der Metadatengenerierung ausgeführt.

Die Vorbereitung umfasst die folgenden optionalen Verfahren:

1. Implementieren der benutzerdefinierten Authentifizierung
2. Implementieren von benutzerdefiniertem Parsing

#### Implementieren der benutzerdefinierten Authentifizierung

Wenn das Zielsystem einen Authentifizierungsmechanismus verwendet, der von diesem Connector nicht unterstützt wird, müssen Sie die vom Zielsystem verwendete Authentifizierung implementieren und sie dann mithilfe der von diesem Connector bereitgestellten Plug-Ins an den Connector binden. Das Implementieren einer benutzerdefinierten Authentifizierung umfasst:

1. das Erstellen einer Java-Klasse
2. das Überschreiben der Methode getAuthHeaders (Map <String, Object> authParams) von Map <String, String>, die den Autorisierungsheader in Form einer Map zurückgibt
3. die Aktualisierung des Connector-Installationsmediums, um die neue Java-Klasse.

Alle Konfigurations- und Authentifizierungsdetails des Zielsystems, die zum Abrufen des Berechtigungsheaders erforderlich sein können, werden über bestimmte IT‑Ressourcenparameter an die Methode Map <String, String> getAuthHeaders (Map <String, Object> authParams) übergeben. Auf alle von diesem Connector bereitgestellten Konfigurationseigenschaften kann innerhalb dieser Methode als Teil von "authParams" zugegriffen werden.

Das Implementieren einer benutzerdefinierten Authentifizierung erfolgt folgendermaßen:

1. Erstellen Sie eine Java-Klasse zum Implementieren der benutzerdefinierten Authentifizierung. Diese Klasse muss die Schnittstelle org.identityconnectors.scimcommon.auth.spi.AuthenticationPlugin implementieren.  
     
   Notieren Sie sich den Namen dieser Java-Klasse. Sie geben den Namen der Java-Klasse an, während Sie die IT‑Ressource für das Zielsystem konfigurieren, die später in diesem Handbuch beschrieben wird.
2. Überschreiben Sie die **Map <String, String> getAuthHeaders-Methode (Map <String, Object> authParams)** in der benutzerdefinierten Java-Klasse.  
     
   Diese Methode muss die benutzerdefinierte Authentifizierungslogik implementieren, die den Autorisierungsheader in Form einer Zuordnung zurückgibt.  
     
   Beispiel: {Authorization = Bearer XXXXXXXXXX}.  
     
   Der Autorisierungsheader enthält das vom Ziel empfangene Zugriffstoken.
3. Packen Sie die Java-Klasse, die die benutzerdefinierte Authentifizierung implementiert, in eine JAR-Datei.
4. Packen Sie die JAR-Datei mit der benutzerdefinierten Authentifizierungsimplementierung wie folgt in die JAR des Connector-Bundles:

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Stellen Sie sicher, dass alle JARs für andere benutzerdefinierte Implementierungen gepackt sind. |

* 1. Extrahieren Sie den Inhalt der Datei gws.identity.connector.bundle-12.2.1.3.jar in ein temporäres Verzeichnis.
  2. Kopieren Sie die JAR-Datei mit der benutzerdefinierten Authentifizierung (ab Schritt 3) in das lib-Verzeichnis.
  3. Generieren Sie das Connector-Bundle (gws.identity.connector.bundle-12.2.1.3.jar) neu, indem Sie den folgenden Befehl ausführen:

|  | **Kommando** |
| --- | --- |
| jar -cvfm gws.identity.connector.bundle-12.2.1.3.jar META-INF/MANIFEST.MF \* |

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Stellen Sie beim Aktualisieren des Connector-Bundles sicher, dass die Datei META-INF\MANIFEST.MF unverändert bleibt. |

1. Führen Sie das Dienstprogramm Oracle Identity Manager Delete JARs aus, um vorhandene JARs in der Oracle Identity Manager-Datenbank zu löschen, bevor Sie das neu generierte Connector-Bundle hochladen. Dieses Dienstprogramm wird bei der Installation von Oracle Identity Manager an den folgenden Speicherort kopiert:  
     
   Wenn Sie das Dienstprogramm ausführen, werden Sie aufgefordert, die Anmeldeinformationen des Identity Manager-Administrators, die URL des Identity Manager-Hostcomputers, den Wert der Kontext‑Factory, den Typ der zu löschenden JAR-Datei und den Speicherort der zu löschenden JAR-Datei einzugeben.  
     
   Geben Sie 4 (ICF-Bundle) als Wert des JAR-Typs an.

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Bevor Sie dieses Dienstprogramm verwenden, stellen Sie sicher, dass die Umgebungsvariable WL\_HOME auf das Verzeichnis festgelegt ist, in dem Oracle WebLogic Server installiert ist. |

1. Starten Sie Oracle Identity Manager neu.

#### Implementieren von benutzerdefiniertem Parsing

Standardmäßig unterstützt der Connector nur JSON als Format während der Abstimmungsläufe. Wenn die Abstimmungsdaten von Ihrem Zielsystem nicht im JSON-Format vorliegen, müssen Sie eine benutzerdefinierte Parser-Implementierung für Ihr Datenformat schreiben.

### Installation

Sie müssen den Connector in Identity Manager installieren.

Bei Bedarf können Sie den Connector auch auf einem Connector-Server bereitstellen.

Die folgenden Themen enthalten Details zur Installation des Connectors:

1. Grundlagen der Installation
2. Installation in Identity Manager
3. Konfigurieren der IT-Ressource für das Zielsystem

#### Grundlagen der Installation

Das Verfahren zum Verständnis der Installation des Connectors ist in zwei Phasen unterteilt:

1. Schritte zum Installieren des Connectors
2. Informationen zur lokalen und Remote-Installation des generischen SCIM-Connectors

##### Schritte zum Installieren des Connectors

Für die Installation dieses Connectors müssen Sie das im Installationsmedium enthaltene Connector-Bundle installieren und anschließend das Connector-Bundle (spezifisch für Ihr Zielsystem) installieren.

Im Folgenden finden Sie eine Zusammenfassung der Schritte zum Installieren des Connectors:

1. Führen Sie das Connector-Installationsprogramm aus, um das Connector‑Bundle (spezifisch für Ihr Zielsystem) zu installieren.  
   Die Vorgehensweise zum Installieren des Connector-Pakets wird später in diesem Handbuch beschrieben.
2. Konfigurieren Sie die IT-Ressource.  
   Siehe Konfigurieren der IT-Ressource für das Zielsystem.

##### Informationen zur lokalen und Remote-Installation des generischen SCIM-Connectors

#### Installation in Identity Manager

#### Konfigurieren der IT-Ressource für das Zielsystem

Die IT‑Ressource für das Zielsystem wird nach der Installation des Connectors erstellt. Eine IT‑Ressource besteht aus Parametern, in denen die Verbindung und andere allgemeine Informationen zu einem Zielsystem gespeichert sind. Identity Manager verwendet diese Informationen, um eine Verbindung zu einer bestimmten Installation oder Instanz des Zielsystems herzustellen und Abgleichs- und Bereitstellungsvorgänge durchzuführen.

Die Liste der Parameter der IT‑Ressource des Connectors kann in die folgenden Kategorien unterteilt werden:

1. Verbindungsbezogene Parameter
2. Authentifizierungsparameter
3. Parser-Parameter
4. Zusätzliche Konfigurationsparameter

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Sie können die Liste der Parameter der IT-Ressourcen jederzeit aktualisieren, indem Sie die Definition des IT-Ressourcentyps mithilfe der Identity Manager Design Console ändern. Es ist nicht erforderlich, den Connector neu zu erstellen und zu installieren, wenn Sie die Definition des IT-Ressourcentyps aktualisieren. |

In diesem Abschnitt werden die folgenden Themen im Zusammenhang mit der Konfiguration von IT‑Ressourcen behandelt:

1. Informationen zu Kategorien von Parameter von IT-Ressourcen
2. Parameter von IT-Ressourcen
3. Angeben von Werten für Parameter einer IT-Ressource

#### Informationen zu Kategorien von Parameter von IT-Ressourcen

Eine IT-Ressource besteht aus Parametern, in denen die Verbindung und andere allgemeine Informationen zu einem Zielsystem gespeichert sind. Identity Manager verwendet diese Informationen, um eine Verbindung zu einer bestimmten Installation oder Instanz des Zielsystems herzustellen.

Die Liste der IT-Ressourcenparameter für diesen Connector kann in die folgenden Kategorien unterteilt werden:

1. Verbindungsbezogene Parameter
2. Authentifizierungsparameter
3. Parser-Parameter
4. Konfigurationsparameter

##### Verbindungsbezogene Parameter

Verbindungsparameter werden vom Connector verwendet, um eine Verbindung zwischen Identity Manager und dem Zielsystem für den Austausch von Identitätsinformationen herzustellen.

##### Authentifizierungsparameter

Authentifizierungsparameter werden vom Zielsystem zur Authentifizierung der Anwendung verwendet. Die Parameter der IT-Ressource für die Authentifizierung variieren je nach Wert des Parameters *Authentication Scheme*. Der Parameter *Authentication Scheme* enthält den Authentifizierungstyp, der vom Zielsystem verwendet wird. Standardmäßig unterstützt der Connector die folgenden Authentifizierungstypen:

| **Wert** | **Bedeutung** |
| --- | --- |
| **basic** |  |
| **authorization code** | Authorization Code Grant Flow  Der Berechtigungstyp Authorization Code Grant wird von vertraulichen und öffentlichen Clients verwendet, um einen Autorisierungscode gegen ein Zugriffstoken auszutauschen. |
| **password** | Resource Owner Password Credential Grant  Die *Resource Owner Password Credential* (d.h. Benutzername und Kennwort) können direkt als Berechtigungsgewährung verwendet werden, um ein Zugriffstoken zu erhalten. Die Anmeldeinformationen werden verwendet, wenn zwischen dem Besitzer der Ressource und dem Client ein hohes Maß an Vertrauen besteht (z. B. wenn der Client Teil des Gerätebetriebssystems oder einer hochprivilegierten Anwendung ist). |
| **client\_credentials** | Client Credentials Flow  Die Anmeldeinformationen des Clients (oder andere Formen der Client-Authentifizierung) können als Authorization Grant verwendet werden, wenn der Autorisierungsbereich auf die geschützten Ressourcen unter der Kontrolle des Clients oder auf geschützte Ressourcen beschränkt ist, die zuvor mit dem Autorisierungsserver vereinbart wurden. Die Anmeldeinformationen des Clients werden in der Regel als Authorization Grant verwendet, wenn der Client in eigenem Namen handelt (der Client ist auch der Besitzer der Ressource) oder auf der Grundlage einer zuvor mit dem Autorisierungsserver vereinbarten Autorisierung Zugriff auf geschützte Ressourcen anfordert. |

Abgesehen von den aufgeführten Authentifizierungstypen müssen Sie, wenn das Zielsystem einen anderen Authentifizierungstyp verwendet, eine eigene Implementierung schreiben, die Entwicklungsaufwand erfordert. Folgende Werte sind für diesen Parameter möglich:

##### Parser-Parameter

Standardmäßig unterstützt der Connector nur JSON Formate während der Abgleichläufe. Wenn die Abgleichdaten vom Zielsystem nicht im JSON-Format vorliegen, muss eine benutzerdefinierte Parser-Implementierung für das Datenformat bereitgestellt werden. Wenn die Daten des Zielsystems im JSON-Format vorliegen, verwendet der Connector einen JSON-Parser und Sie müssen einen Wert für den erweiterten Parameter json-resource-tags angeben. Der Parameter json-resource-tags muss den Wert des json-Tags enthalten, der während der Abstimmung zum Parsen mehrerer Einträge in einer einzelnen Antwort verwendet wird.

##### Konfigurationsparameter

Alle zusätzlichen Konfigurationsparameter sind zielsystemspezifisch.

#### Parameter von IT-Ressourcen

Die IT-Ressource für das Zielsystem enthält Verbindungsinformationen zum Zielsystem. Identity Manager verwendet diese Informationen während der Provisionierung und Abgleich.

##### Verbindungsbezogene Parameter

| **Parameter** | **Bedeutung** |
| --- | --- |
| **Accept Type** | Dieser Parameter enthält den vom Zielsystem erwarteten Akzeptanztyp im Header.  Default: application/json |
| **Connector Server** |  |
| **Content Type** | Dieser Parameter enthält den vom Zielsystem erwarteten Inhaltstyp im Header.  Default: application/json |
| **Locale Country** |  |
| **Locale Language** |  |
| **Locale TimeZone** |  |
| **Secure Socket** |  |
| **Service Domain** |  |
| **Service Port** |  |
| **Server Feature** |  |

##### Authentifizierungsparameter

| **Parameter** | **Bedeutung** |
| --- | --- |
| **Authentication Scheme** | Gibt den Typ der zu verwendenden Autorisierung an.  Beispiel: password |
| **Client Identifier** | Geben Sie die Client-ID (eine eindeutige Zeichenfolge) ein, die der Autorisierungsserver während des Registrierungsvorgangs an den Client ausgegeben hat.  Default: cf |
| **Client Secret** | Geben Sie das Geheimnis ein, mit dem die Identität von Identity Manager authentifiziert wird. |
| **Connector Server** |  |
| **Principal Name** | Name des Benutzerkontos, das Identity Manager verwenden muss, um eine Verbindung zum Zielsystem herzustellen und auf dieses zuzugreifen.  Beispiel: admin |
| **Principal Password** | Kennwort des Benutzerkontos, das Identity Manager verwenden muss, um eine Verbindung zum Zielsystem herzustellen und auf dieses zuzugreifen.  Beispiel: admin |
| **Resource Username** | Geben Sie den Benutzernamen oder die Benutzer-ID des Besitzers der Ressource ein. |
| **Resource Password** | Geben Sie das Kennwort des Besitzers der Ressource ein. |

#### Angeben von Werten für Parameter einer IT-Ressource

Die IT-Ressource für das Zielsystem enthält Verbindungsinformationen zum Zielsystem. Identity Manager verwendet diese Informationen während der Provisionierung und Abgleich.

### Postinstallation

#### Konfiguration Identity Manager

Sie müssen ein UI-Formular und eine Anwendungsinstanz für die Ressource erstellen, für die Sie die Provisionierungs‑ und Abgleichprozesse ausführen möchten. Darüber hinaus müssen Sie die Hintergrundprozesse der Berechtigungs- und Katalogsynchronisierung ausführen.

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Führen Sie die in diesem Abschnitt beschriebenen Verfahren nur aus, wenn Sie den Connector im als Zielressource verwenden. |

Diese Verfahren werden in den folgenden Abschnitten beschrieben:

##### Erstellen und Aktivieren einer Sandbox

Sie müssen eine Sandbox erstellen und aktivieren, um die Funktionen für die UI Anpassung und Formularverwaltung nutzen zu können. Anschließend können Sie die Sandbox veröffentlichen, um die Anpassungen anderen Benutzern zur Verfügung zu stellen.

Siehe [Erstellen einer Sandbox](http://www.oracle.com/pls/topic/lookup?ctx=E22999-01&id=OMDEV4798) und [Aktivieren und Deaktivieren einer Sandbox](http://www.oracle.com/pls/topic/lookup?ctx=E22999-01&id=OMDEV4799) in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

##### Erstellen eines neuen UI-Formulars

Anweisungen zum Erstellen eines neuen UI-Formulars finden Sie unter [Erstellen von Formularen mithilfe des Formular-Designers](http://www.oracle.com/pls/topic/lookup?ctx=E22999-01&id=OMADM4796) in *Oracle Fusion Middleware Administering Oracle Identity Manager*. Stellen Sie beim Erstellen des UI-Formulars sicher, dass Sie das Ressourcenobjekt auswählen, das dem Connector entspricht, dem Sie das Formular zuordnen möchten. Aktivieren Sie außerdem das Kontrollkästchen **Berechtigungsformulare generieren**.

##### Verknüpfen des Formulars mit der Anwendungsinstanz

##### Veröffentlichen der Sandbox

Führen Sie vor dem Veröffentlichen einer Sandbox das folgende Verfahren als bewährte Methode aus, um alle bis zu diesem Zeitpunkt vorgenommenen Sandbox-Änderungen zu überprüfen, da es schwierig ist, Änderungen nach dem Veröffentlichen einer Sandbox rückgängig zu machen:

1. Deaktivieren Sie in der Systemadministration die Sandbox.  
   Melden Sie sich von der Systemadministration ab.
2. Melden Sie sich mit den Benutzeranmeldeinformationen von xelsysadm beim Self Service an und aktivieren Sie die Sandbox, die Sie in Schritt 1 deaktiviert haben.
3. Stellen Sie im Katalog sicher, dass das Formular der Anwendungsinstanz mit den richtigen Feldern angezeigt wird.
4. Veröffentlichen Sie die Sandbox. Siehe [Veröffentlichen einer Sandbox](http://www.oracle.com/pls/topic/lookup?ctx=E22999-01&id=OMDEV4802) in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

##### Synchronisation des Katalogs und von Berechtigungen

Den Katalog und die Berechtigungen synchronisieren Sie wie folgt:

Führen Sie den Hintergrundprozess für die Synchronisierung der Wertelisten des Connectors aus, die unter Hintergrundprozess für die Wertelisten beschrieben werden.

Führen Sie den Hintergrundprozess „E*ntitlement List*“ aus, um das Schema der Zuweisung von Berechtigungen aus der untergeordneten Prozessformularen zu füllen.

Führen Sie den Hintergrundprozess für die Katalogsynchronisierung „*Catalog Synchronization*“ aus.

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| [Vordefinierte Hintergrundprozess](http://www.oracle.com/pls/topic/lookup?ctx=E22999-01&id=OMADM743)e in *Oracle Fusion Middleware Administering Oracle Identity Manager*. |

#### Löschen von Inhalten aus dem Server-Cache

Wenn Sie den Connector bereitstellen, werden die Connector-Bundle aus dem Ressourcenverzeichnis auf dem Installationsmedium in die Identity Manager-Datenbank kopiert. Wenn Sie dem Verzeichnis *connectorResources* ein neues Connector-Bundle hinzufügen oder Änderungen an einem vorhandenen Connector-Bundle vornehmen, müssen Sie den Inhalt der Connector-Ressourcenpakete aus dem Server-Cache löschen.

Um Inhalte der Connector-Bundle aus dem Server-Cache zu löschen, können Sie entweder Identity Manager neu starten oder das Dienstprogramm *PurgeCache* ausführen. Im Folgenden wird beschrieben, wie Sie den Server-Cache durch Ausführen des *PurgeCache*-Dienstprogramms löschen:

1. Wechseln Sie in einem Befehlsfenster in das Verzeichnis *OIM\_HOME*/ server/bin.
2. Geben Sie einen der folgenden Befehle ein:  
     
    Unter Microsoft Windows: PurgeCache.bat All  
    Unter UNIX: PurgeCache.sh All  
     
   Wenn Sie dazu aufgefordert werden, geben Sie den Benutzernamen und das Kennwort eines Benutzerkontos ein, das zur Gruppe SYSTEM ADMINISTRATORS gehört. Darüber hinaus werden Sie aufgefordert, die Service-URL im folgenden Format einzugeben:  
     
    t3: // OIM\_HOST\_NAME: OIM\_PORT\_NUMBER  
     
   In diesem Format:  
     
    Ersetzen Sie OIM\_HOST\_NAME durch den Hostnamen oder die IP-Adresse des Oracle Identity Manager-Hostcomputers.  
    Ersetzen Sie OIM\_PORT\_NUMBER durch den Port, den Oracle Identity Manager überwacht.

Mit dem Dienstprogramm PurgeCache können Sie den Cache für jede Inhaltskategorie löschen.

#### Verwalten der Protokollierung

Identity Manager verwendet den Protokollierungsdienst Oracle Diagnostic Logging (ODL) zum Aufzeichnen aller Arten von Ereignissen, die den Connector betreffen.

Die folgenden Themen enthalten detaillierte Informationen zur Protokollierung:

1. Grundlegendes zu Ebenen der Protokollierung
2. Aktivieren der Protokollierung

##### Grundlegendes zu Ebenen der Protokollierung

Wenn Sie die Protokollierung aktivieren, speichert Identity Manager automatisch Informationen zu Ereignissen in einer Protokolldatei, die während der Bereitstellungs- und Abstimmungsvorgänge auftreten.

Identity Manager verwendet Oracle Java Diagnostic Logging (OJDL) für die Protokollierung. OJDL basiert auf java.util.logger. Um den Ereignistyp anzugeben, für den die Protokollierung stattfinden soll, können Sie die Protokolle auf eine der folgenden verfügbaren Ebenen festlegen:

| **Ebene** | **Bedeutung** |
| --- | --- |
| **SEVERE.intValue()+100** | Diese Ebene ermöglicht die Protokollierung von Informationen über schwerwiegende Fehler. |
| **SEVERE** | Diese Ebene ermöglicht die Protokollierung von Informationen zu Fehlern, die es Identity Manager ermöglichen könnten, weiter ausgeführt zu werden. |
| **WARNING** | Diese Ebene ermöglicht die Protokollierung von Informationen über potenziell schädliche Situationen. |
| **INFO** | Diese Ebene ermöglicht die Protokollierung von Nachrichten, die den Fortschritt der Anwendung hervorheben. |
| **CONFIG** | Diese Ebene ermöglicht die Protokollierung von Informationen zu detaillierten Ereignissen, die für das Debuggen hilfreich sind. |
| **FINE, FINER, FINEST** | Diese Ebenen ermöglichen die Protokollierung von Informationen zu detaillierten Ereignissen, wobei FINEST Informationen zu allen Ereignissen protokolliert. |

Diese Protokollebenen werden den Kombinationen aus ODL-Nachrichtentyp und -Ebene zugeordnet:

| **Ebene** | **Bedeutung** |
| --- | --- |
| **SEVERE.intValue()+100** | INCIDENT\_ERROR:1. |
| **SEVERE** | ERROR:1 |
| **WARNING** | WARNING:1 |
| **INFO** | NOTIFICATION:1 |
| **CONFIG** | NOTIFICATION:16. |
| **FINE** | TRACE:1. |
| **FINER** | TRACE:16 |
| **FINEST** | TRACE:32 |

Die Konfigurationsdatei für OJDL lautet logging.xml und befindet sich unter folgendem Pfad:  
  
 *DOMAIN\_HOME*/config/fmwconfig/servers/*OIM\_SERVER*/logging.xml

Hier sind *DOMAIN\_HOME* und *OIM\_SERVER* der Domänenname und der Servername, die während der Installation von Identity Manager angegeben wurden.

##### Aktivieren der Protokollierung

#### Konfigurieren von SSL für den Connector

Konfigurieren Sie SSL, um die Kommunikation zwischen Identity Manager und dem Zielsystem zu sichern.

Beziehen Sie das SSL-Zertifikat für den öffentlichen Schlüssel für das Zielsystem.

Kopieren Sie das Zertifikat mit dem öffentlichen Schlüssel des Zielsystems auf den Computer, auf dem Identity Manager gehostet wird.

Führen Sie den Befehl keytool aus, um das Zertifikat in den Oracle WebLogic Server-Keystore zu importieren:

|  | **Kommando** |
| --- | --- |
| keytool -import -keystore KEYSTORE\_NAME -storepass PASSWORD -file CERT\_FILE\_NAME -alias |

In diesem Kommando

| **Platzhalter** | **Bedeutung** |
| --- | --- |
| **KEYSTORE\_NAME** | Der vollständige Pfad einschließlich des Namens zum DemoTrust Keystore des WebLogic Servers. |
| **PASSWORD** | Das Kennwort für den Keystore |
| **CERT\_FILE\_NAME** | Der vollständige Pfad einschließlich des Namens zum Zertifikat des Zielsystems. |
| **ALIAS** | Der Aliasname für das Zertifikat des Zielsystems. |

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Ändern Sie die an den Befehl keytool übergebenen Parameterwerte entsprechend Ihren Anforderungen. Stellen Sie sicher, dass die keytool-Argumente keinen Zeilenumbruch enthalten.  Stellen Sie sicher, dass das Systemdatum für Identity Manager mit dem Gültigkeitsdatum des Zertifikats synchronisiert ist, um Fehler während der abgesicherten Kommunikation zu vermeiden. |

## Verwenden des Pivotal Cloud Foundry Foundation Connector

Sie können den Connector zum Ausführen von Provisionierungs- und Abgleichsvorgängen verwenden, nachdem Sie ihn so konfiguriert haben, dass er Ihren Anforderungen entspricht.

In diesem Abschnitt werden die folgenden Themen behandelt:

1. Verwendung von Wertelisten
2. Abgleichsvorgänge konfigurieren
3. Hintergrundprozess
4. Provisionierungsvorgänge ausführen
5. Deinstallation des Connectors

### Verwendung von Wertelisten

Wertelisten, die während der des Datenabgleichs‑ und der Provisionierung verwendet werden, sind entweder vorkonfiguriert oder können mit dem Zielsystem synchronisiert werden.

Die folgenden Kategorien von Wertelisten werden in diesem Abschnitt erläutert:

1. Vorkonfigurierte Wertelisten
2. Synchronisierte Wertelisten

#### Vorkonfigurierte Wertelisten

Vorkonfigurierte Wertelisten sind die anderen Wertelisten, die in Identity Manager erstellt werden, wenn Sie den Connector bereitstellen. Diese Wertelisten sind entweder mit Werten vorab ausgefüllt oder müssen nach der Bereitstellung des Connectors manuell eingegeben werden.

Die vordefinierten Wertelisten sind:

1. PCF.UAA.Origin
2. PCF.ORL.Scope
3. PCF.SRL.Scope

##### PCF.UAA.Origin

Die Werteliste PCF.UAA.Origin enthält Connector-Konfigurationseinträge, die während der Datenabgleichs- (sowohl vertrauenswürdige Quell- als auch Zielressource) und Provisionierungsvorgänge verwendet werden.

| **Encode** | **Decoded** | **Beschreibung** |
| --- | --- | --- |
| **unknown** | Unknown |  |
| **uaa** | Internal |  |
| **saml** | External |  |
| **oauth2.0** | Oauth 2.0 |  |
| **oidc1.0** | OpenID Connect |  |
| **ldap** | Directory Service |  |
| **keystone** | Keystone Login |  |
| **login-server** | Login Server |  |

##### PCF.ORL.Scope

Die Werteliste PCF.ORL. enthält Connector-Konfigurationseinträge, die während der Datenabgleichs- (sowohl vertrauenswürdige Quell- als auch Zielressource) und Provisionierungsvorgänge verwendet werden.

| **Encode** | **Decoded** | **Beschreibung** |
| --- | --- | --- |
| **organizations** | User |  |
| **managed\_organizations** | Manager |  |
| **auditored\_organizations** | Auditor |  |
| **billing\_managed\_organizations** | Billing Manager |  |

##### PCF.SRL.Scope

Die Werteliste PCF.SRL.Scope enthält Connector-Konfigurationseinträge, die während der Datenabgleichs- (sowohl vertrauenswürdige Quell- als auch Zielressource) und Provisionierungsvorgänge verwendet werden.

| **Encode** | **Decoded** | **Beschreibung** |
| --- | --- | --- |
| **spaces** | Developer |  |
| **managered\_spaces** | Manager |  |
| **auditored\_spaces** | Auditor |  |

#### Synchronisierte Wertelisten

Bei der Synchronisierung von Wertelisten werden Ergänzungen oder Änderungen an bestimmten Feldern im Zielsystem in Wertelisten in Identity Manager kopiert.

Während eines Provisionierungsvorgangs verwenden Sie eine Werteliste im Prozessformular, um einen einzelnen Wert aus einer Reihe von Werten anzugeben. Beispielsweise möchten Sie möglicherweise eine Gruppe aus einer Werteliste auswählen (mit einer Reihe von Gruppen), um die dem Benutzer zuzuweisende Gruppe anzugeben.

Bei der Synchronisierung von Wertelisten werden Ergänzungen oder Änderungen an den Zielsystemattributen in entsprechende Wertelisten (die als Eingabequelle für Suchfelder verwendet werden) in Identity Manager kopiert. Dies wird erreicht, indem Hintergrundprozesse für die Synchronisierung von Wertelisten ausgeführt werden.

Nach der Synchronisierung werden die Daten in jeder der Wertelisten im folgenden Format gespeichert:

| **Wert** | **Format** | **Beschreibung** |
| --- | --- | --- |
| **Encode** | <*IT\_RESOURCE\_KEY*>~< ID> | IT\_RESOURCE\_KEY ist der numerische Code, der jeder IT-Ressource in Identity Manager zugewiesen wird.  ID ist der Zielsystemcode, der jedem Eintrag einer Werteliste zugewiesen ist. Dieser Wert wird basierend auf dem Attributnamen des Zielsystems ausgefüllt, der im Decode-Attribut des Hintergrundprozesses für die Synchronisierung von Wertelisten angegeben ist. |
| **Decode** | <*IT\_RESOURCE\_NAME*>~<VALUE> | IT\_RESOURCE\_NAME ist der Name der IT-Ressource in Identity Manager.  VALUE ist der Zielsystemcode, der jedem Eintrag einer Werteliste zugewiesen ist. Dieser Wert wird basierend auf dem Attributnamen des Zielsystems ausgefüllt, der im Decode-Attribut des geplanten Jobs für die Synchronisierung von Suchfeldern angegeben ist. |

| D:\tt\icon-note-16.png | **Siehe auch** |
| --- | --- |
|  |

### Abgleichsvorgänge konfigurieren

#### Regeln für den Datenabgleich

Regeln für den Datenabgleich werden automatisch erstellt, wenn Sie den Connector bereitstellen.

Das folgende ist das Format des Regelelements:

User Login Equals NameAttribute

In diesem Regelelement bedeutet:

| **Element** | **Bedeutung** |
| --- | --- |
| **User Login** | Das Feld Benutzer-ID im Identity Manager-Benutzerformular.. |
| **NameAttribute** | Der Wert des Kontoqualifizierers. |

#### Vollständiger und inkrementeller Datenabgleich

Bei einem vollständigen Abgleich werden alle vorhandenen Benutzerdatensätze des Zielsystems in Identity Manager abgeglichen.

Bei einem inkrementellen Abgleich werden nur Datensätze für den Abgleich berücksichtigt, die nach dem letzten Datum oder Zeitstempel erstellt oder geändert wurden, zu dem der erfolgreiche letzte Abgleich durchgeführt wurde.

Nachdem Sie den Connector bereitgestellt haben, müssen Sie zunächst einen vollständigen Abgleich durchführen.

#### Eingeschränkter Datenabgleich

Bei dem eingeschränkten oder gefilterten Abgleich wird die Anzahl der Datensätze begrenzt, die basierend auf festgelegten Filterkriterien abgeglichen werden.

Standardmäßig werden alle Zielsystemdatensätze, die nach dem letzten Abgleichsvorgang hinzugefügt oder geändert wurden, während des aktuellen Abgleichsvorgang abgeglichen. Sie können diesen Prozess anpassen, indem Sie die Teilmenge der hinzugefügten oder geänderten Zielsystemdatensätze angeben, die abgeglichen werden müssen. Dazu erstellen Sie Filter für das Abgleichsmodul.

Sie können einen eingeschränkten Abgleich durchführen, indem Sie Filter erstellen, die Ihr Zielsystem unterstützt. Dieser Connector bietet das Filterattribut, mit dem Sie eines oder mehrere der Attribute des Zielsystems zum Filtern von Zielsystemdatensätzen verwenden können.

### Hintergrundprozess

Wenn Sie den Installationsvorgang des Connectors ausführen, werden automatisch Hintergrundprozess in Identity Manager erstellt. Sie müssen diese Hintergrundprozesse entsprechend Ihren Anforderungen konfigurieren, indem Sie Werte für ihre Attribute angeben.

Die Hintergrundprozesse, die Sie für den Datenabgleich konfigurieren können, werden in den folgenden Abschnitten erläutert:

1. Synchronisierung von Wertelisten
2. Abgleich von Benutzerdatensätzen
3. Abgleich gelöschter Benutzerdatensätze
4. Hintergrundprozesse konfigurieren

#### Synchronisierung von Wertelisten

Hintergrundprozesse für die Synchronisierung aktualisieren die Wertelisten in Identity Manager basierend auf den neuesten Werte aus bestimmten Feldern im Zielsystem. Diese Wertelisten werden als Eingabequelle für Attribute in Oracle Identity Manager verwendet.

| **Attribute** | **Bedeutung** |
| --- | --- |
| **Batch Size** |  |
| **Decoded Value** | Geben Sie den Namen des Attributs ein, das zum Auffüllen der Decode-Spalte der Lookup-Definition verwendet wird (angegeben als Wert des Attributs Lookup Name). |
| **Dependent Job** |  |
| **Encoded Value** | Geben Sie den Namen des Attributs ein, das zum Auffüllen der Spalte Codeschlüssel der Werteliste verwendet wird (angegeben als Wert des Attributs "Reconciliation Object"). |
| **Entitlement Prefix Required** |  |
| **IT Resource** | Name der IT-Ressource für die Zielsysteminstallation, von der Sie Datensätze abgleichen möchten. |
| **Last Reconciled** |  |
| **Reconciliation Object** | Name der Werteliste in Identity Manager, die mit Werten gefüllt werden muss, die vom Zielsystem abgerufen werden. |
| **Reconciliation Operation** |  |
| **Reconciliation Source** | Geben Sie den Objekttyp ein, den Sie abgleichen möchten. |

#### Abgleich von Benutzerdatensätzen

Hintergrundprozesse für den Abgleich der Benutzerdaten des Zielsystems mit Identity Manager wurden während der Installation des Connectors in Identity Manager automatisch erstellt.

| **Attribute** | **Bedeutung** |
| --- | --- |
| **Batch Size** |  |
|  |  |
| **Dependent Job** |  |
|  |  |
|  |  |
| **IT Resource** |  |
| **Last Reconciled** |  |
| **Reconciliation Object** | Name des Ressourcenobjekts, das für den Abgleich verwendet wird. |
|  |  |
|  |  |

#### Abgleich gelöschter Benutzerdatensätze

Hintergrundprozesse für den Abgleich der gelöschten Benutzerdaten des Zielsystems mit Identity Manager wurden während der Installation des Connectors in Identity Manager automatisch erstellt.

| **Attribute** | **Bedeutung** |
| --- | --- |
| **Batch Size** |  |
|  |  |
| **Dependent Job** |  |
|  |  |
|  |  |
| **IT Resource** |  |
| **Last Reconciled** |  |
| **Reconciliation Object** | Name des Ressourcenobjekts, das für den Abgleich verwendet wird. |
|  |  |
|  |  |

#### Hintergrundprozesse konfigurieren

Konfigurieren Sie Hintergrundprozess für Abgleichsvorgänge, die regelmäßig nach neuen Informationen auf Ihrem Zielsystem suchen und die Daten in Identity Manager replizieren.

So konfigurieren Sie einen Hintergrundprozess:

1. Melden Sie sich bei Oracle Identity System Administration an.
2. Klicken Sie im linken Bereich unter Systemverwaltung auf Scheduler.
3. Suchen und öffnen Sie den Hintergrundprozess wie folgt:
   1. Geben Sie im linken Bereich im Feld Suchen den Namen des Hintergrundprozesses als Suchkriterium ein. Alternativ können Sie auf Erweiterte Suche klicken und das Suchkriterium angeben.
   2. Klicken Sie in der Ergebnistabelle im linken Bereich auf den Hintergrundprozess in der Spalte Jobname.
4. Auf der Registerkarte Jobdetails können Sie die folgenden Parameter ändern:  
     
   **Wiederholungen**:  
   Geben Sie in dieses Feld einen ganzzahligen Wert ein. Diese Zahl gibt an, wie oft der Scheduler versucht, den Job zu starten, bevor er dem Job den Status Gestoppt zuweist.  
     
   **Zeitplantyp**:  
   Wählen Sie abhängig von der Häufigkeit, mit der der Job ausgeführt werden soll, den entsprechenden Zeitplantyp aus.  
     
   Zusätzlich zum Ändern der Jobdetails können Sie einen Job aktivieren oder deaktivieren.
5. Geben Sie auf der Registerkarte Auftragsdetails im Bereich Parameter Werte für die Attribute des Hintergrundprozesses an.

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Attributwerte sind in der von Ihnen importierten Connector-XML-Datei vordefiniert. Geben Sie nur Werte für die Attribute an, die Sie ändern möchten. |

1. Klicken Sie auf Übernehmen, um die Änderungen zu speichern.

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Auf der Seite "Scheduler-Status" in der Identity System Administration können Sie den Scheduler entweder starten, stoppen oder neu initialisieren. |

### Provisionierungsvorgänge ausführen

Sie erstellen einen neuen Benutzer in Oracle Identity Self Service auf der Seite Benutzer erstellen. Sie stellen Konten auf der Registerkarte Konten der Seite Benutzerdetails bereit oder fordern sie an.

So führen Sie Provisionierungsvorgänge in Identity Manager aus:

### Deinstallation des Connectors

Durch die Deinstallation des Connectors werden alle kontobezogenen Daten gelöscht, die den Ressourcenobjekten des Connectors zugeordnet sind. Mit dem Dienstprogramm "Connectors deinstallieren" können Sie einen Connector deinstallieren.

Wenn Sie den Connector aus irgendeinem Grund deinstallieren möchten, lesen Sie [Uninstalling Connectors](http://www.oracle.com/pls/topic/lookup?ctx=E22999-01&id=OMADM4346) in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

## Limitierungen des Pivotal Cloud Foundry Foundation Connector

### Zuweisung von Rollen in Spaces

Um einem Benutzerkonto in einem Space eine Rolle zu zuweisen, muss dem entsprechenden Benutzer zuvor in der Organisation dem der Space angehört die Rolle *User* zugeordnet sein.

### Entzug von Rollen in Organisationen

Um einem Benutzerkonto die Rolle User in einer Organisation zu entziehen, sind zuvor alle Zuordnungen von Rollen zu den der Organisation angehörigen Spaces zu entziehen.