ORACLE
Consulting

Connector Administration

Oracle® Identity Manager Connector Guide für Google Apigee Edge

Release 1.0.0

ORACLE

Connector Administration

Oracle® Identity Manager Connector Guide für Google Apigee Edge

Release 1.0.0

von Sophie Strecke, Dieter Steding und Sylvert Bernet

Inhaltsverzeichnis

Einführung

Dieses Handbuch beschreibt den Konnektor, der für das On-Boarding von Google Apige Edge Anwendungen in Oracle Identity Governance verwendet wird.

Leserkreis

Dieses Dokument wendet sich an Personen, die sich mit der Administration von Ressourcen, sowie Teams, die sich mit der Integration von Zielsystemen, in Oracle Identity Governance befassen.

Bezugsdokumente

Weitere Informationen zur Installation und Verwendung von Oracle Identity Governance 12.2.1.3.0 finden Sie auf der Oracle-Hilfeseite:

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

Weitere Informationen zur Dokumentation von Oracle Identity Governance Konnektoren 12.2.1.3.0 finden Sie auf der Oracle-Hilfeseite:

- *http://docs.oracle.com/cd/E52734_01/index.html*

Vertraulichkeit

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

Der Leserkreis erklärt sich damit einverstanden, dass die in dieser Dokumentation enthaltenen Informationen 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 in einem Absatz kennzeichnet Befehle, URLs, Code-Beispiele, Text, der auf dem Bildschirm angezeigt wird, oder Text, den Sie eingeben.

Google Apigee Edge Connector

Oracle® Identity Governance ist eine zentralisierte Lösung zu Verwaltung von Identitätsdaten, die Service-, Compliance-, Bereitstellungs- und Kennwortverwaltungsdienste für Anwendungen vor Ort oder in der Cloud bereitstellt. Oracle® Identity Governance-Konnektoren werden verwendet, um Oracle® Identity Governance in externe, identitätsbezogene Anwendungen zu integrieren.

Mit dem Konnektor für Google Apigee Edge können Sie dieses System als verwaltete (Ziel-) Quelle von Benutzerkonten erstellen und integrieren. Im Modus der Benutzerkontenverwaltung (Zielressource) des Konnektor werden die Daten für Benutzerkonten direkt im Zielsystem erstellt, geändert oder gelöscht. Änderungen die im Zielsystem an bestehende Benutzerkonten vorgenommen wurden, werden mit Oracle® Identity Governance abgeglichen. Diese so bereitgestellten bzw. abgeglichenen Daten werden verwendet, um neue Berechtigungen zuzuweisen, zu aktualisieren oder zu entziehen, die Identitäten in Oracle® Identity Governance zugewiesen wurden. Diese in Oracle® Identity Governance durchgeführten Bereitstellungsvorgänge werden durch den Konnektor in die Erstellung oder Aktualisierung von Zielsystemkonten übersetzt.

> **Anmerkung**
>
> In diesem Handbuch wird der Konnektor, der mit der Option **Anwendungen** auf der Registerkarte **Verwalten** die von Identity Self Service bereitgestellt wird, als **AOB-Anwendung** bezeichnet. Der Konnektor, der mit der Option **Manage Connector** in Oracle Identity System Administration bereitgestellt wird, wird als **CI-basierter Konnektor** (Connector Installer-based Connector) bezeichnet.

Seit Oracle® Identity Governance Version 12.2.1.3.0 wird die Bereitstellung von Konnektoren mithilfe der Funktion Anwendungs-Onboarding innerhalb von Oracle Identity Self Service vorgenommen. Diese Funktion ermöglicht es Endanwendern, Anwendungen mit minimalen Details und minimalem Aufwand zu integrieren. Das Installationspaket eines Konnektors enthält eine Zusammenstellung vordefinierter Vorlagen (XML-Dateien), die alle Informationen enthalten, die für die Provisionierung nach und den Datenabgleich aus einer bestimmten Anwendung oder einem bestimmten Zielsystem erforderlich sind. Diese Vorlagen enthalten auch grundlegende Verbindungs- und Konfigurationsdetails, die für Ihr Zielsystem spezifisch sind. Der Konnektor verwendet Informationen aus diesen vordefinierten Vorlagen, sodass Sie Ihre Anwendungen schnell und einfach über eine einzige und vereinfachte Benutzeroberfläche integrieren können.

Das **On-Boarding von Anwendungen** ist der Prozess der Registrierung oder Verknüpfung einer Anwendung mit Oracle Identity Governance und mach diese Anwendung für die Provisionierung und den Abgleich von Benutzerinformationen verfügbar.

Die folgenden Themen bieten einen allgemeinen Überblick über den Google Apigee Edge Konnektor.

> **Anmerkung**
>
> An einigen Stellen in diesem Handbuch wird Google Apigee Edge als **Zielsystem** bezeichnet.

Anforderungen des Konnektors

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 aktuellen 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)*

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
Connector Server	12.2.1.3.0
Connector Server JDK	JDK oder JRE 1.8 und höher
Zielsystem	Oracle® RDBMS 12c (12.2.0.1.0) oder höher

Erforderliche Patches

Komponente	Version
Oracle® Identity Governance	Patch 30735905 Oracle® Identity Governance Bundle Patch ID:200108.2108)

Nutzungsempfehlung

Dies sind die Empfehlungen für die Version des Google Apigee Edge Konnektors, die Sie je nach verwendeter Identity Governance Version installieren und verwenden können.

> **Anmerkung**
>
> Oracle® Identity Governance Version 11.1.x wird von diesem Konnektor nicht unterstützt.

Wenn Sie Oracle® Identity Governance 12c (12.2.1.3.0) verwenden, verwenden Sie die neueste 12.2.1.x-Version dieses Konnektors. Stellen Sie den Konnektor mithilfe der Option **Anwendungen** auf der Registerkarte **Verwalten** des Identity Self Service bereit oder mithilfe der Option **Manage Connector** der Identity System Administration bereit.

Sprachen

Der Konnektor unterstützt die folgenden Sprachen:

- Englisch
- Französich

- Deutsch

Unterstüzte Operationen

Dies ist die Liste der Operationen, die der Konnektor für Ihr Zielsystem unterstützt.

Benutzerverwaltung

Operation	Unterstützt?
Benutzerkonto erstellen	Ja
Benutzerkonto ändern	Ja
Benutzerkonto löschen	Ja
Benutzerkonto aktivieren	Nein
Benutzerkonto deaktivieren	Nein
Kennwort zurücksetzen	Ja

Organisationsverwaltung

Operation	Unterstützt?
Organisation erstellen	Nein
Organisation ändern	Nein
Organisation löschen	Nein

Rollenverwaltung

Operation	Unterstützt?
Gruppe erstellen	Nein
Gruppe ändern	Nein
Gruppe löschen	Nein

Berechtigungsverwaltung

Operation	Unterstützt?
Zu Organization hinzufügen	Ja
Aus Organization entfernen	Ja
Zu Rolle hinzufügen	Ja
Aus Rolle entfernen	Ja

Architektur des Konnektors

Mit dem Konnektor können Sie Benutzerkonten auf dem Zielsystem verwalten. Die Kontoverwaltung wird auch als Zielressourcenverwaltung bezeichnet. Die Verwaltung der Benutzerkonten umfasst die folgenden Prozesse:

- **Ressourcenprovisionierung**

  Die Provisionierung umfasst das Erstellen, Aktualisieren oder Löschen von Benutzerkonten auf dem Zielsystem über Oracle® Identity Governance.

Wenn Sie einer Identiät eine Google Apigee Edge-Ressource zuweisen (oder bereitstellen), führt der Vorgang zur Erstellung eines Kontos in Google Apigee Edge für diese Identität. Im Kontext von Oracle® Identity Governance umfasst der Begriff Provisionierung auch Aktualisierungen, die am Zielsystemkonto über Oracle® Identity Governance vorgenommen wurden. Diese Aktualisierungen umfassen auch die Aktivierung bzw. Deaktivierung von Benutzerkonten,

Bevor Sie Benutzerkonten für die erforderlichen Organisationen und Rollen auf dem Zielsystem zuweisen können, müssen Sie die Liste aller auf dem Zielsystem verfügbaren Organisationen und Rollen nach Oracle® Identity Governance synchronisieren. Dies wird erreicht durch Verwendung der Hintergrundprozesse für die Synchronisierung von Wertelisten erreicht.

- **Ressourcenabgleich**

  Beim Zielressourcenabgleich werden Daten zu im Zielsystem neu erstellten und geänderten Benutzerkonten abgeglichen und mit bestehenden Identitäten und provisionierten Ressourcen verknüpft. Für Zielressourcenabgleich werden Hintergrundprozess verwendet. Der Konnektor wendet Filter an, um abzugleichende Benutzerdaten auf dem Zielsystem zu finden, und ruft dann die Attributwerte dieser Benutzerkonten ab.

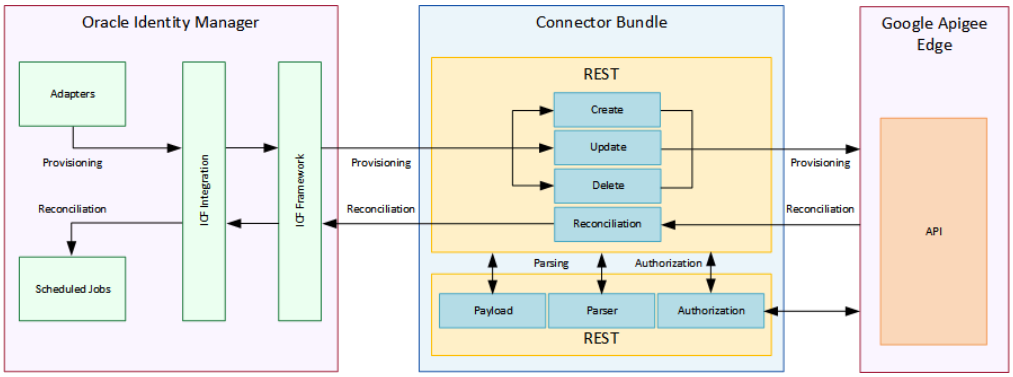

Abbildung 2.1. Google Apigee Edge Konnektor Architektur

Wie aus der Abbildung hervorgeht, ist der Google Apigee Edge Konnektor als Zielressource von Oracle® Identity Governance konfiguriert. Durch Provisionierung, die in Oracle® Identity Governance ausgeführt wird, werden Konten für Identitäten auf dem Zielsystem erstellt und aktualisiert. Durch den Abgleich werden Kontodaten, die direkt auf dem Zielsystem erstellt und aktualisiert werden, in Oracle® Identity Governance eingelesen und gegen die entsprechenden Identitäten gespeichert.

Der Google Apigee Edge Konnektor wird mithilfe des Identity Connector Framework (ICF) implementiert. ICF ist eine erforderliche Komponente, die grundlegende Abstimmungs- und Bereitstellungsvorgänge bietet, die allen Konnektoren in Oracle® Identity Governance gemeinsam sind. Darüber hinaus bietet ICF allgemeine Funktionen, die Entwickler sonst selbst implementieren müssten, z.B. Verbindungspooling, Pufferung, Zeitüberschreitungen und Filterung. ICF wird zusammen mit Oracle® Identity Governance ausgeliefert, daher müssen Sie ICF nicht konfigurieren oder anpassen.

Anmerkung

Der Google Apigee Edge Konnektor verwendet REST, um auf das Zielsystem zuzugreifen und unterstützt **ausschließlich** die Verwaltung von Benutzerkonten.

Matrix der unterstützten Funktionen

Die Liste der Funktionen bereit, die von der *AOB* Applikation und dem *CI*-basierter Konnektor unterstützt werden.

Funktion	AOB	CI
Vollständiger Abgleich Benutzerkonten	Ja	Ja
Inkrementeller Abgleich Benutzerkonten	Ja	Ja
Eingeschränkter Abgleich Benutzerkonten	Ja	Ja
Abgleich gelöschter Benutzerkonten	Ja	Ja
Abgleich Rollen	Ja	Ja
Abgleich Organizationen	Ja	Ja
Sichere Kommunikation	Ja	Ja
Connector Server	Ja	Ja
Verbindungstest	Ja	Nein

Funktionen des Konnektors

Zu den Funktionen des Konnektors gehören neben der Provisionierung von Benutzerkonten, der vollständige Abgleich von Benutzerkonten und der Abgleich von gelöschten Kontendaten:

- Authentisierung
- Vollständiger und inkrementeller Datenabgleich
- Eingeschränkter Datenabgleich
- Batch Datenabgleich
- Datenabgleich gelöschter Benutzerkonten
- Abgleich von Wertelisten mit dem Zielsystem
- Provisionierung von Benutzerkonten
- Unterstützung für Connector-Server
- Unterstützung von Pre- und Post-Aktions-Skripten
- Transformation von Kontodaten
- Sichere Kommunikation zum Zielsystem

Authentisierung

Standardmäßig unterstützt der Konnektor die HTTP-Basisauthentifizierung.

Wenn das Zielsystem nicht den vom Konnektor unterstützten Authentifizierungsmechanismus anbietet, kann mithilfe der von diesem Konnektor bereitgestellten Plug-In's eine eigene Implementierung für die Authentifizierung hinzugefügt werden.

Vollständiger und inkrementeller Datenabgleich

Der vollständige Abgleich umfasst den Abgleich aller vorhandenen Benutzerdatensätze aus dem Zielsystem mit Oracle® Identity Governance.

Beim inkrementellen Abgleich werden nur Datensätze durch Oracle® Identity Governance abgerufen, die nach dem letzten Abgleichslauf hinzugefügt oder geändert wurden.

Nachdem Sie die Anwendung erstellt haben, führen Sie zunächst einen vollständigen Datenbabgleich durch, um alle vorhandenen Benutzerkonten vom Zielsystem in Oracle® Identity Governance zu übertragen. Nach dem ersten vollständigen Abgleichslauf wird der inkrementelle Abgleich automatisch aktiviert. Beim inkrementellen Abgleich werden dann nur

noch die Benutzerkonten durch Oracle® Identity Governance abgerufen, die seit dem letzten Abgleichslauf hinzugefügt oder geändert wurden.

Eingeschränkter Datenabgleich

Sie können Datensätze von Benutzerkonten aus dem Zielsystem basierend auf festgelegten Filterkriterien abgleichen. Diese Filterkriterien bestimmen die Teilmenge der hinzugefügten und geänderten Zielsystemdatensätze, die während der Ausführung des Abgleichs von Oracle® Identity Governance abgerufen werden.

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.

Datenabgleich gelöschter Benutzerkonten

Sie können den Konnektor verwenden, um Benutzerdatensätze, die auf dem Zielsystem gelöscht wurden, mit Oracle® Identity Governance abzugleichen.

Weitere Informationen zu Hintergrundprozessen zum Datenabgleich dieser gelöschten Datensätze finden Sie in einem der folgenden Abschnitte:

<insert>link</insert>

Abgleich von Wertelisten mit dem Zielsystem

Während eines Provisionierungsvorgangs verwenden Sie in einem Formular Wertelisten, um einen einzelnen Wert aus einer Reihe von Werten anzugeben. Sie verwenden beispielsweise die Werteliste *Land* um ein Land aus der Liste von Länder im Formularfeld auszuwählen.

Wenn Sie den Konnektor bereitstellen, werden in Oracle® Identity Governance Definitionen von Wertelisten erstellt, die den Wertelistenfeldern auf dem Zielsystem entsprechen. Die Synchronisierung der Wertelisten umfasst das Kopieren von Ergänzungen oder Änderungen in die Wertelisten in Oracle® Identity Governance, die an den Wertelistenfeldern des Zielsystems vorgenommen wurden.

Weitere Informationen zu Hintergrundprozessen für den Abgleich von Wertelisten finden Sie in einem der folgenden Abschnitte:

<insert>link</insert>

Provisionierung von Benutzerkonten

Sie können den Konnektor verwenden, um Google Apigee Edge Benutzerkonten und Gruppenzuordnungen bereitzustellen. Sie können einen neuen Benutzer in Oracle Identity Manager mithilfe der Seite Benutzer erstellen.

Unterstützung für Connector-Server

Connector-Server ist eine der Funktionen von ICF. Durch die Verwendung von einem oder mehreren Connector-Server ermöglicht die Architektur Ihrer Anwendung die Kommunikation mit extern bereitgestellten Bundles.

Ein Java-Connector-Server ist hilfreich, wenn Sie kein Java-Connector-Bundle in derselben VM wie Ihre Anwendung ausführen möchten. Es kann von Vorteil sein, einen Konnektor auf einem anderen Host auszuführen, um die Leistung zu verbessern.

Informationen zum Installieren, Konfigurieren und Ausführen des Connector-Servers und zum anschließenden Installieren des Konnektors auf einem Connector-Server finden Sie unter *Using an Identity Connector Server* in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

Support for Running Pre and Post Action Scripts

Sie können Pre- und Post-Action-Skripts auf einem Computer ausführen, auf dem der Konnektor bereitgestellt wird. Diese Skripte können vom Typ SQL/StoredProc/Groovy sein. Sie können die Skripte so konfigurieren, dass sie vor oder nach dem Erstellen, Aktualisieren oder Löschen eines Benutzerkontos ausgeführt werden.

Weitere Informationen finden Sie unter, *Updating the Provisioning Configuration* in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Transformation von Kontodaten

Sie können die Umwandlung von Kontodaten konfigurieren, die während der Abgleichsvorgänge nach Oracle® Identity Governance übertragen und oder durch Provisionierungsvorgänge von dort gesendet werden, indem Sie beim Erstellen Ihrer Anwendung Groovy-Skripts einbinden.

Weitere Informationen finden Sie unter, *Validation and Transformation of Provisioning and Reconciliation Attributes* in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Sichere Kommunikation zum Zielsystem

Um eine sichere Kommunikation mit dem Zielsystem bereitzustellen, ist SSL erforderlich. Sie können SSL zwischen Oracle® Identity Governance und dem Connector-Server sowie zwischen dem Connector-Server und dem Zielsystem konfigurieren.

Wenn Sie SSL nicht konfigurieren, können Kennwörter im Klartext über das Netzwerk übertragen werden. Dieses Problem kann beispielsweise auftreten, wenn Sie einen Benutzerkonto erstellen oder das Kennwort eines Benutzerkontos ändern.

Weitere Informationen finden Sie unter Sichere Kommunikation konfigurieren.

Wertelisten

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

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

- Vorkonfigurierte Wertelisten
- Synchronisierte Wertelisten

Vorkonfigurierte Wertelisten

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

Innerhalb dieser Kategorie von Wertelisten wird wiederum unterschieden nach:

- Globale Wertelisten
- Lokale Wertelisten

Globale Wertelisten

Globale Wertelisten sind unabhängig von einem spezifischen Zielsystem.

Lokale Wertelisten

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

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 Konnektor 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 Konnektors werden in Oracle Identity Manager automatisch die folgenden Wertelisten erstellt, die als Quelle für Wertelisten verwendet werden:

- GAE.Role
- GAE.Tenant

Die Wertelisten GAE.Role und GAE.Tenant 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 und Organisationen werden mit Werten aus den Wertelisten GAE.Role bzw. GAE.Tenant gefüllt, die beim Bereitstellen des Konnectors 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 GAE.Role 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 zielsystemspezifische Identifier, der jedem Eintrag einer Werteliste zugewiesen ist. Dieser Wert wird basierend auf dem Attributnamen des Zielsystems ausgefüllt, der im Encode-Attribut des Hintergrundprozesses für

Wert	Format	Beschreibung
		die Synchronisierung von Wertelisten angegeben ist.
Decode	*<IT_RESOURCE>~<VALUE>*	*IT_RESOURCE* ist der Name, der IT-Ressource in Identity Manager.
		VALUE ist der zielsystemspezifische Bezeichner, 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.

Die nachfolgende Table zeigt beispielhafte Einträge in der Werteliste GAE.Role:

Encode	Decoded
Encode	Decoded

Bereitstellung des Konnektors

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

Die folgenden Themen enthalten Details zum Installieren und Konfigurieren Konnektors:

- Vorbereitung
- Installation
- Postinstallation

Vorbereitung

Die Vorbereitung für den Konnektor 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:

- Implementieren der benutzerdefinierten Authentifizierung
- Implementieren von benutzerdefiniertem Parsing

Implementieren der benutzerdefinierten Authentifizierung

Wenn das Zielsystem einen Authentifizierungsmechanismus verwendet, der von diesem Konnnektor nicht unterstützt wird, müssen Sie die vom Zielsystem verwendete Authentifizierung implementieren und sie dann mithilfe der von diesem Konnektor bereitgestellten Plug-In's an den Konnektor binden.

Die Implementierung einer benutzerdefinierten Authentifizierung umfasst:

- das Erstellen einer Java-Klasse
- das Überschreiben der Methode *getAuthHeaders(Map<String, Object> parameter)* von *Map<String, String>*, die den Autorisierungsheader in Form einer *Map* zurückgibt
- die Aktualisierung des Konnnektor-Installationsmediums, um die neue Java-Klasse.

Alle Konfigurations- und Authentifizierungsdetails des Zielsystems, die zum Abrufen des Berechtigungsheaders erforderlich sein können, werden über bestimmte Parameter der IT Ressource an die Methode *getAuthHeaders(Map<String, Object> parameter)* übergeben. Auf alle von diesem Konnektor bereitgestellten Konfigurationseigenschaften können innerhalb dieser Methode als Teil von *parameter*emphasis> zugegriffen werden.

Die Implementierung 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 sp#228;ter in diesem Handbuch beschrieben wird.
2.
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:

Implementieren von benutzerdefiniertem Parsing

Installation

Die folgenden Themen enthalten Details zur Installation des Connectors:

- Grundlagen der Installation
- Installation in Identity Manager
- Konfigurieren der IT-Ressource für das Zielsystem
- Informationen zu Kategorien von Parameter von IT-Ressourcen
- Parameter von IT-Ressourcen
- Angeben von Werten für Parameter einer IT-Ressource

Grundlagen der Installation

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

- Schritte zum Installieren des Konnektors
- Informationen zur lokalen und Remote-Installation des Konnektors

Schritte zum Installieren des Konnektors

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

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

1. Führen Sie das Konnektor-Installationsprogramm aus, um das Konnektor-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. Konfigurieren der IT-Ressource für das Zielsystem

Informationen zur lokalen und Remote-Installation des Konnektors

Installation in Identity Manager

Konfigurieren der IT-Ressource für das Zielsystem

Die IT Ressource für das Zielsystem wird nach der Installation des Konnektors 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 Konnektors kann in die folgenden Kategorien unterteilt werden:

- Verbindungsbezogene Parameter
- Authentifizierungsparameter
- Parser Parameter
- Zusätzliche Konfigurationsparameter

> **Anmerkung**
> 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 Konnektor 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:

Informationen zu Kategorien von Parameter von IT-Ressourcen

Parameter von IT-Ressourcen

Angeben von Werten für Parameter einer IT-Ressource

Postinstallation

Protokollierung

TBD