ORACLE
Consulting

Konnektor Administration

Oracle® Identity Governance Connector Guide für openfire™ Datenbank Konnektor

Release 1.0.0

ORACLE

Konnektor Administration

Oracle® Identity Governance Connector Guide für openfire™ Datenbank Konnektor

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 openfire™ als 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*
- *https://docs.oracle.com/en/middleware/idm/suite/12.2.1.4/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.

Symbol Konventionen

In diesem Dokument werden die folgenden Konventionen für Symbole verwendet.

Symbol	Bedeutung
[ ]	Enthält optionale Argumente und Befehlsoptionen.
{ | }	Enthält eine Reihe von Auswahlm öglichkeiten für eine erforderliche Befehlsoption.
${ }	Referenziert eine Variable.
-	Verbindet gleichzeitig mehrere Tastenanschläge.
+	Verbindet mehrere aufeinanderfolgende Tastenanschläge.
>	Zeigt die Auswahl eines Menüpunkts in der grafischen Benutzeroberfläche an.

Über den openfire™ Datenbank Konnektor

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 Oracle® Identity Manager Connector können Sie openfire™ XMPP Server in Oracle® Identity Governance als Anwendungen erstellen und integrieren.

> **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 macht diese Anwendung für die Provisionierung und den Abgleich von Benutzerinformationen verfügbar.

Die folgenden Abschnitte bieten einen allgemeinen Überblick über den openfire™ Datenbank Konnektor:

- Komponenten
- Nutzungsempfehlung
- Sprachen
- Unterstüzte Operationen
- Architektur des Konnektors
- Matrix der unterstützten Funktionen
- Funktionen des Konnektors

> **Anmerkung**
> An einigen Stellen in diesem Handbuch wird openfire™ XMPP Server als **Zielsystem** bezeichnet.

Komponenten

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

Dies sind die Softwarekomponenten und deren Versionen, die für die Installation und Nutzung des Konnektors erforderlich sind.

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

Erforderliche Patches

Dies sind die Softwarekomponenten und deren Versionen, die für die Installation und Nutzung des Konnektors erforderlich sind.

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

Nutzungsempfehlung

Dies sind die Empfehlungen für die Version des openfire™ 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.
- Wenn Sie Oracle® Identity Governance 12c (12.2.1.3.0) verwenden, verwenden Sie die neueste 12.2.1.x-Version dieses Konnektors. Installieren Sie den Konnektor mithilfe der Option **Manage Connector** des Identity System Administration.

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

Gruppenverwaltung

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

Raumverwaltung

Operation	Unterstützt?
Raum erstellen	Nein
Raum ändern	Nein
Raum löschen	Nein

Berechtigungsverwaltung

Operation	Unterstützt?
Zu Gruppe hinzufügen	Ja
Aus Gruppe entfernen	Ja
Zu Raum hinzufügen	Ja
Aus Raum entfernen	

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 openfire™-Ressource zuweisen (oder bereitstellen), führt der Vorgang zur Erstellung eines Kontos in der Datenbank des openfire™ XMPP Servers 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 Gruppen oder Räume auf dem Zielsystem zuweisen können, müssen Sie die Liste aller auf dem Zielsystem verwendeten Gruppen und Räume nach Oracle® Identity Governance synchronisieren. Dies wird erreicht durch Verwendung der Hintergrundprozesse für die Synchronisierung von Wertelisten erreicht.
- **Ressourcenabgleich**

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

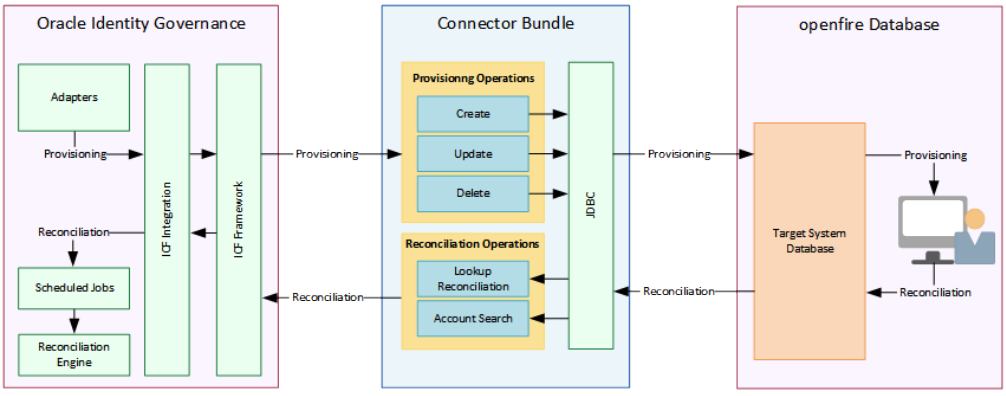

Abbildung 2.1. Connector Architekture

Wie in dieser Abbildung gezeigt, ist die Datenbank des openfire™ XMPP Server 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 geholt und gegen die entsprechenden Identitäten gespeichert. Der openfire™ XMPP Server-Connector wird mithilfe des Identity Connector Framework (ICF) implementiert. ICF ist eine Komponente, die erforderlich

ist, um Identity Connectors zu verwenden und 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.

Der openfire™ Database Connector verwendet JDBC, um auf das Zielsystem zuzugreifen.

Dieser Konnektor unterstützt nur Zieldie 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 Gruppen	Ja	Ja
Abgleich Räume	Ja	Ja
Sichere Kommunikation	Ja	Ja
Connector Server	Ja	Ja
Verbindungstest	Ja	Nein

Funktionen des Konnektors

Zu den Funktionen des Konnektors gehören die Unterstützung für Connector-Server, Unterstützung für die Hochverfügbarkeitskonfiguration des Zielsystems, Verbindungspooling, Abgleich gelöschter Benutzerdatensätze, Unterstützung für Groovy-Skripts und so weiter.

- Vollständiger und inkrementeller Datenabgleich
- Eingeschränkter Datenabgleich
- Datenabgleich gelöschter Benutzerkonten
- Batch Datenabgleich
- 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
- Verbindungspool
- Unterstützung für die Hochverfügbarkeitskonfiguration des Zielsystems

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 ein neues Benutzerkonto einschließlich der Gruppen- und Raumzuordnungen durch Oracle® Identity Governance mithilfe der Seite **Benutzer** im Zielsystem erstellen.

Sie können den Konnektor verwenden, um Benutzerkonten, Gruppenzuordnungen und Raumzuordnungen durch Oracle® Identity Governance im Zielsystem zu ändern.

Sie können den Konnektor verwenden, um Benutzerkonten, Gruppenzuordnungen und Raumzuordnungen durch Oracle® Identity Governance im Zielsystem zu löschen.

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*.

Unterstützung von Pre- und Post-Aktions-Skripten

Sie können Pre- und Post-Aktions-Skripte 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 TLS/SSL erforderlich. Sie können TLS/SSL zwischen Oracle® Identity Governance und dem Connector-Server sowie zwischen dem Connector-Server und dem Zielsystem konfigurieren.

Wenn Sie TLS/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.

Verbindungspool

Ein Verbindungspool ist ein Cache von Objekten, die physische Verbindungen zum Zielsystem darstellen. Konnektoren von Oracle® Identity Governance können diese Verbindungen verwenden, um mit Zielsystemen zu kommunizieren.

Zur Laufzeit fordert die Anwendung eine Verbindung vom Pool an. Wenn eine Verbindung verfügbar ist, verwendet der Konnektor sie und gibt sie dann an den Pool zurück. Eine an den Pool zurückgegebene Verbindung kann erneut für den Konnektor angefordert und von diesem für eine andere Operation verwendet werden. Durch die Aktivierung der Wiederverwendung von Verbindungen trägt der Verbindungspool dazu bei, den Aufwand für die Verbindungserstellung wie Netzwerklatenz, Speicherzuweisung und Authentifizierung zu reduzieren.

Für jede Basiskonfiguration, den Sie beim Erstellen einer Anwendung angeben, wird ein Verbindungspool erstellt. Wenn Sie beispielsweise drei Anwendungen für drei Installationen des Zielsystems haben, werden drei Verbindungspools erstellt, einer für jede Zielsysteminstallation.

Weitere Informationen zu den Parametern, die Sie für das Verbindungspooling konfigurieren können, finden Sie unter:

<insert>link</insert>

Unterstützung für die Hochverfügbarkeitskonfiguration des Zielsystems

Sie können den Konnektor für die Anforderung nach Hochverfügbarkeit der Umgebung des Zielsystems konfigurieren.

Der Konnektor kann Informationen zu Backup-Zielsystemhosts aus dem Failover-Parameter der Basiskonfiguration lesen und diese Informationen anwenden, wenn er keine Verbindung zum primären Host herstellen kann.

Weitere Informationen zum Failover-Parameter finden Sie unter
<insert>link</insert>

Datenmodell openfire™ Server Connector

Übersicht

Nachfolgende Abbildung zeigt eine Übersicht des Datenmodells des Connectors.

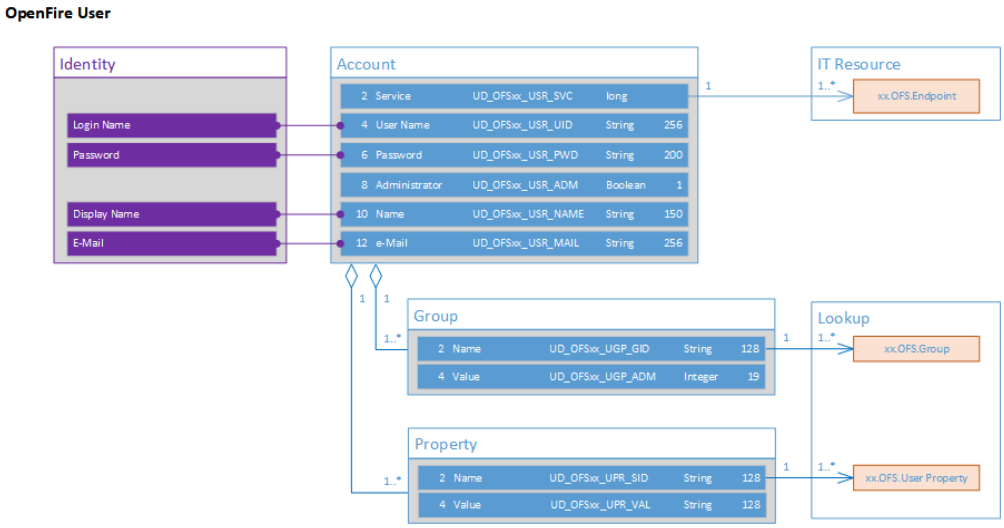

Abbildung 3.1. Datenmodell openfire™ Server Connector

Das Datenmodell des Connectors unterstützt neben den von einem openfire™ Server benötigten Kontodaten die Speicherung von Gruppen und kontospezifischen Eigenschaften.

- Gruppen
- Eigenschaften

Benutzerkonto

Die Kontodaten werden im Formular UD_OFS_USR gespeichert.

Attribute

Label	Name	Type	Length
Service	UD_OFS_USR_SVC	Long	
User Name	UD_OFS_USR_UID	String	256
Password	UD_OFS_PWD	String	200
Administrator	UD_OFS_USR_ADM	Boolean	
Name	UD_OFS_USR_NAME	String	150
e-Mail	UD_OFS_USR_MAIL	String	256

Account Prepopulation

Für einige der oben beschriebenen Attribute sind Regeln implementiert, die Werte für ein solches Attribut aus dem Profil einer Identität ableiten, zu der das Konto gehört.

Die nachfolgenden Abschnitte beschreiben die Adapter-Konfiguration für:

- User Name
- Password
- Name
- E-Mail

User Name

Eigenschaft	Wert	Beschreibung
Adapter	OCS PrePopulate Required String Converted	Der logische Adapter, der zur Vorbelegung des Wertes für das Attribut angewendet wird.
profileValue	User Login	Die Quelle für den Wert des Attributs im Benutzerkonto, der aus dem Profile der Identität abgeleitet wird.
convertRule	lower	Der Hinweis für den Adapter, den aus dem Identitätsprofil abgeleiteten Wert in Kleinbuchstaben umzuwandeln.

Password

Eigenschaft	Wert	Beschreibung
Adapter	OCS PrePopulate Required String	Der logische Adapter, der zur Vorbelegung des Wertes für das Attribut angewendet wird.
profileValue	Password	Die Quelle für den Wert des Attributs im Benutzerkonto, der aus dem Profile der Identität abgeleitet wird.

Name

Eigenschaft	Wert	Beschreibung
Adapter	OCS PrePopulate Conditional	Der logische Adapter, der zur Vorbelegung des Wertes für das Attribut angewendet wird.
profileValue1	Initials	Die primäre Quelle für den Wert des Attributs im Benutzerkonto, der aus dem Profile der Identität abgeleitet wird.
profileValue2	Display Name	Die secundäre Quelle für den Wert des Attributs im Benutzerkonto, der aus dem Profile der Identität abgeleitet wird.

E-Mail

Eigenschaft	Wert	Beschreibung
Adapter	OCS PrePopulate Required String	Der logische Adapter, der zur Vorbelegung des Wertes für das Attribut angewendet wird.
profileValue	Email Address	Die Quelle für den Wert des Attributs im Benutzerkonto, der aus dem Profile der Identität abgeleitet wird.

Gruppen

Die einem Benutzerkonto zugewiesenen Gruppen werden im Formular UD_OFS_UGP gespeichert.

Attribute

Label	Name	Type	Length
Name	UD_OFS_UGP_GID	String	128
Administrator	UD_OFS_UGP_ADM	Integer	19

Prepopulation

Das Formular unterliegt keinen Regeln für die Vorbelegung von Werten.

Property

Die einem Benutzerkonto zugewiesenen Gruppen werden im Formular UD_OFS_UPR gespeichert.

Attribute

Label	Name	Type	Length
Name	UD_OFS_UPR_SID	String	128
Administrator	UD_OFS_UPR_VAL	String	128

Prepopulation

Das Formular unterliegt keinen Regeln für die Vorbelegung von Werten.

Probleme und deren Umgehungen

These ...

Administratoren

Problem

Wird ein zuvor als Administrator markiert Benutzerkonto im Server-UI gelöscht wird, verbleibt dieses Konto als markiert Administrator in der Tabelle der Systemeigenschaften (ofProperty), sofern diese Berechtigung nicht zuvor entzogen und gespeichert wurde.

Workaround

Zur Zeit kein Workaround vorhanden.

Kennwortverschlüsselung

Problem

Kennwörter werden mit dem Blowfish Block Cipher verschlüsselt.

Die Initialisierung eines solchen Ciphers ist eine kostspielige Operation. Um den Block Cipher zu initialisieren, ist ein vereinbartes Geheimnis (Key Material) notwendig, welches zu diesem Zweck aus der Datenbank geladen werden muss.

Um zu diesen Vorgang nicht jedesmal, wenn ein neues Benutzerkonto erzeugt oder für ein bestehendes Benutzerkonto eine Änderung des Kennworts vorgenommen wird, durchführen zu müssen, ist der gesamte Ciper nach seiner Initialisierung gecachet. Allerdings ist dabei zu beachten, dass wenn sich der Wert in der Datenbank ändert, der Cipher des Server und der im Cache des Konnektors befindliche Cipher ab diesem Zeitpunkt verschiedenen Werte für die Verschlüsselung verwenden. Dies ist aber ein generelles Problem des Servers, da die vorhandenen Kennwörter nach der Änderung nicht automatisch neu berechnet werden und sich somit kein Benutzerkonto mehr am Server anmelden kann.

Workaround

Ein Workaround ist, dass Identity Governance durchgestartet wird, und danach somit den geänderten Wert für die Kennwortverschlüsselung verwendet. Damit kann erreicht werden, dass sich neu angelegte Benutzerkonten und die Benutzerkonten, für die nach diesem Neustart das Kennwort zurückgesetzt wurde, wieder am Server anmelden können.

Wenn zu befürchten ist, dass dieses Verfahren zu große Auswirkungen auf die Benutzer von Identity Governance hat, sollte der Connector auf einem externen Connector-Server bereitgestellt werden. In dieser Architektur, muss lediglich der Connector Server neu gestartet werden.

Status eine Benutzerkontos

Problem

Der Status eines Benutzerkontos in openfire™ wird als Flag mit einer Gültigkeitsdauer definiert. Identity Governance betrachtet andererseits den Status eines Benutzerkontos wiederum als globale Eigenschaft.

> **Anmerkung**
> Es gibt zu einem gewissen Zeitpunkt immer nur genau eine oder keine Statusinformation in openfire™ zu einem bestimmten Benutzerkonto.

Workaround

Als Workaround wird der Status eines Benutzerkontos bei Deaktivierung des Kontos mit dem aktuellem Datum als Startzeitpunkt der Deaktivierung gesetzt. Das Ablaufdatum der Deaktivierung wird auf unbestimmte Dauer gesetzt. Die Aktivierung des betreffenden Benutzerkontos löscht die Status Informationen.

Gesperrte Benutzerkonten

Problem

Wird ein Benutzerkonto geperrt ist eine Anmeldung in openfire™ Admin Console und das Eröffnen einer XMPP Session nicht mehr möglich. Diese Verhalten ist so gewollt.

Wenn das Benutzerkonto nun durch den Konnector entsperrt, ist ein Login in openfire™ Admin Console oder das Öffnen einer XMPP-Sitzung ist weiterhin nicht möglich.

Ursache

openfire™ setzt sehr stark auf Caching. Da der Connector direkt auf der Datenbank arbeitet, bleiben die Caches in der Middleware unberührt und können somit einen anderen Status für ein Benutzerkonto anzeigen (Split Brain).

Ein gerade entsperrter Benutzer muss warten, bis diese maximale Lebensdauer abgelaufen ist, bevor er sich erneut anmelden kann.

Workaround

Ein Adminstrator setzt folgende Caches manuell zurück.

- Locked Out Accounts
- User