

Identity Governance Service

Kern Datenmodell

Release 1.0.0

Identity Governance Service

Kern Datenmodell

Release 1.0.0

von Sophie Strecke und Dieter Steding

Inhaltsverzeichnis

Vorwort	1
Leserschaft	1
Vertraulichkeit	1
Typografische Konventionen	1
Konventionen Verzeichnisvariablen	1
Symbol Konventionen	2
Leitfaden für IAM	3
Warum ist IAM wichtig?	3
Installation des Datenbankschemas	4
Erstellen der Systemobjekte	4
Erstellen der Schemaobjekte	5
Datenmodell	6
User	6
Properties	6
Attribute	6
Constraints	6
Indexes	7
Foreign Keys	7
Role	7
Properties	7
Attributes	7
Constraints	7
Indexes	8
Foreign Keys	8
User Role	8
Properties	8
Attributes	8
Constraints	8
Indexes	8
Foreign Keys	8

Vorwort

Leserschaft

Dieser Leitfaden richtet sich an Administratoren von Ressourcen und Teams für die Integration von Zielsysteme.

Vertraulichkeit

Das in dieser Dokumentation enthaltene Material stellt geschützte, vertrauliche Informationen dar, die sich auf Produkte und Methoden von Oracle beziehen.

Die Leser stimmen zu, dass die Informationen in diesem Dokument nicht außerhalb von Oracle offengelegt und zu keinem anderen Zweck als zur Bewertung dieses Verfahrens vervielfältigt, verwendet oder offengelegt werden dürfen.

Typografische Konventionen

In diesem Dokument werden die folgenden typografische Konventionen verwendet.

Konvention	Bedeutung
fett	Fettschrift kennzeichnet Elemente der grafischen Benutzeroberfläche, die einer Aktion zugeordnet sind, oder Begriffe, die im Text oder im Glossar definiert sind.
<i>kursiv</i>	Kursivschrift kennzeichnet Buchtitel, Hervorhebungen oder Platzhaltervariablen, für die Sie bestimmte Werte angeben.
<code>monospace</code>	Monospace-Schrift kennzeichnet Befehle innerhalb eines Absatzes, URLs, Code in Beispielen, Text, der auf dem Bildschirm angezeigt wird, oder Text, den Sie eingeben.

Konventionen Verzeichnisvariablen

In diesem Dokument werden die folgenden Konventionen für Verzeichnisvariablen verwendet.

Variable	Bedeutung
<code>JAVA_HOME</code>	Der Speicherort, an dem das unterstützte Java Development Kit (JDK) installiert wurde.
<code>ORACLE_BASE</code>	Das Basisverzeichnis, unter dem Oracle-Produkte installiert sind.
<code>ORACLE_HOME</code>	Das Verzeichnis in dem gängige Dienstprogramme, Bibliotheken und andere Oracle Fusion Middleware-Produkte gespeichert sind.
<code>IGS_BASE</code>	Der Speicherort der <i>Identity Governance Service</i> . Für die Hostcomputer auf Anwendungsebene sollte es auf einem gemeinsam genutzten Datenträger gespeichert werden.

Symbol Konventionen

In diesem Dokument werden die folgenden Konventionen für Symbole verwendet.

Symbol	Bedeutung
[]	Enthält optionale Argumente und Befehlsoptionen.
{ }	Enthält eine Reihe von Auswahlmöglichkeiten 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.

Leitfaden für IAM

Identity und Access Management (IAM) ist ein Framework bestehend aus Geschäftsprozessen, Richtlinien und Technologien, der die Verwaltung elektronischer oder digitaler Identitäten erleichtert. Mit einem IAM-Framework können IT-Manager den Benutzerzugriff auf kritische Informationen in ihren Organisationen kontrollieren. Systeme, die für IAM verwendet werden, umfassen Single-Sign-On-Systeme, die während der Ausführung aufgetreten sind. [Zwei-Faktor Authentisierung](#), [Multi-Faktor Authentisierung](#) und [Verwaltung privilegierter Benutzerkonten](#). Diese Technologien bieten auch die Möglichkeit, Identitäts- und Profildaten sicher zu speichern, sowie Governance-Funktionen, um sicherzustellen, dass nur notwendige und relevante Daten geteilt werden.

IAM-Systeme können vor Ort, von einem Drittanbieter über ein Cloud-basiertes Abonnementmodell oder in einem Hybridmodell bereitgestellt werden.

Auf grundlegender Ebene umfasst IAM die folgenden Komponenten:

- wie Personen in einem System identifiziert werden (den Unterschied zwischen Identitätsmanagement und Authentifizierung verstehen)
- wie Rollen in einem System identifiziert und Personen zugeordnet werden
- Hinzufügen, Entfernen und Aktualisieren von Personen und deren Rollen in einem System
- Zuweisen von Zugriffsebenen zu Einzelpersonen oder Gruppen von Einzelpersonen
- Schutz der sensiblen Daten innerhalb des Systems und Sicherung des Systems selbst

Warum ist IAM wichtig?

Unternehmensleitungen und IT-Abteilungen stehen unter erhöhtem regulatorischem und organisatorischem Druck, den Zugriff auf Unternehmensressourcen zu schützen. Infolgedessen können sie sich nicht mehr auf manuelle und fehleranfällige Prozesse verlassen, um Benutzerrechte zuzuweisen und zu verfolgen. IAM automatisiert diese Aufgaben und ermöglicht eine granulare Zugriffskontrolle und Prüfung aller Unternehmensressourcen vor Ort und in der Cloud.

IAM, das über eine ständig wachsende Liste von Funktionen verfügt -- darunter Biometrie, Verhaltensanalyse und KI -- ist gut für die Anforderungen der neuen Sicherheitslandschaft geeignet. Beispielsweise entspricht die strenge Kontrolle des Ressourcenzugriffs durch IAM in stark verteilten und dynamischen Umgebungen dem Übergang der Branche von Firewalls zu Zero-Trust-Modellen und den Sicherheitsanforderungen von IoT.

Während IT-Experten denken mögen, dass IAM etwas für größere Organisationen mit größeren Budgets ist, ist die Technologie in Wirklichkeit für Unternehmen jeder Größe zugänglich.

Installation des Datenbankschemas

In diesem Kapitel wird beschrieben, wie die Objekte des Datenmodells der *Identity Governance Services* installiert werden.

In diesem Kapitel wird nicht beschrieben, wie eine Instanz der Zieldatenbank eingerichtet wird. Für die Erzeugung einer Instanz der Zieldatenbank ist die Dokumentation des jeweiligen Herstellers heranzuziehen.



Wichtig

Identity Governance Services unterstützt derzeit ausschließlich Oracle® als Zieldatenbank.

Um das für *Identity Governance Services* erforderliche Datenbankschema zu installieren, wird eine Reihe von Skripten mit vorbereiteten DDL-Anweisungen bereitgestellt. Diese Skripte erstellen die erforderlichen Tabellen und Standardindizes.

Um beliebige Objekte installieren zu können, benötigen Sie entweder lokal oder remote Zugriff auf die Oracle-Datenbank. Um die bereitgestellten Skripte ausführen zu können, ist eine Installation von *SQL*Plus* erforderlich.



Warnung

Für die Ausführung der Installation ist die Rolle **DBA** erforderlich.

Die Installation der Basisobjekte, die allgemein für jeden weiteren Modul innerhalb der *Identity Governance Services* notwendig sind, besteht aus:

- [Erstellen der Systemobjekte](#)
- [Erstellen der Schemaobjekte](#)

Erstellen der Systemobjekte

Das Erstellen des Systemobjekte führt zur Erzeugung eines Tablespace, sowie dem Eigentümer des Schemas mit den erforderlichen Rechten in der Datenbank.

Um die Systemobjekte zu installieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie eine Kommandozeile zu dem Betriebssystem, von dem aus der Zugriff auf die Datenbankinstanz möglich ist.
2. Suchen Sie das Verzeichnis der bereitgestellten Skripte und navigieren Sie dorthin:

```
cd <IGS_BASE>/governanceBackend/src/main/resources/igs
```

3. Erstellen Sie den Tablespace und den Eigentümer des Datenbankschemas *igd_igs* von *Identity Governance Services*, indem Sie den folgenden Befehl ausführen:

```
sqlplus / as sysdba @sys
```

Nach der Ausführung des Skripts zur Erstellung der Systemobjekte sollten die Protokolldateien auf Fehler, die während der Ausführung aufgetreten sein können, kontrolliert werden. Diese Protokolldateien befinden sich im gleichen Verzeichnis wie das zum Laden des Datenbankschemas verwendete Skript (siehe Punkt 3).

**Anmerkung**

Bei der erstmaligen Ausführung des Skripts ist es normal das Fehler wie *ORA-01918* auftreten.

Erstellen der Schemaobjekte

Um die Schemaobjekte zu erstellen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie eine Kommandozeile zu dem Betriebssystem, von dem aus der Zugriff auf die Datenbankinstanz möglich ist.
2. Suchen Sie das Verzeichnis der bereitgestellten Skripte und navigieren Sie dorthin:

```
cd <IGS_BASE>/governanceBackend/src/main/resources/igs
```

3. Laden Sie das Datenbankschema von *Identity Governance Services*, indem Sie den folgenden Befehl ausführen:

```
sqlplus / as sysdba @create
```

Nach der Ausführung des Skripts zur Erstellung der Schemaobjekte sollten die Protokolldateien auf Fehler, die während der Ausführung aufgetreten sein können, kontrolliert werden. Diese Protokolldateien befinden sich im gleichen Verzeichnis wie das zum Laden des Datenbankschemas verwendete Skript (siehe Schritt 3).

**Anmerkung**

Bei der erstmaligen Ausführung des Skripts ist es normal das Fehler wie *ORA-04080* oder *ORA-00942* auftreten.

Datenmodell

User

Properties

Eigenschaft	Wert
Verwendung	
Erstellt	11 März 2022 14:33:01
Geändert	11 März 2022 14:33:01

Attribute

Name	Datentyp	Länge	Skalierung	Nullfähigkeit	Standard
id	number	10	0	NOT NULL	
rowversion	varchar2	30		NOT NULL	
created_by	varchar2	30		NOT NULL	
created_on	date			NOT NULL	
updated_by	varchar2	30			
updated_on	date			NOT NULL	
active	number	1	0	NOT NULL	1
username	varchar2	36		NOT NULL	
lastname	varchar2	128		NOT NULL	
firstname	varchar2	128			
language	char	2		NOT NULL	
email	varchar2	512		NOT NULL	
phone	varchar2	64			
mobile	varchar2	64			

Constraints

Unique Constraints

Name	Spalte
igt_usr_uk1	username
igt_usr_uk2	email

Check Constraints

Name	Spalte	Bedingung
igt_usr_ck1	active	active IN (0, 1)
igt_usr_ck2	language	language IN ('ar', 'ca', 'cs', 'da', 'de', 'el', 'en', 'es', 'fi', 'fr', 'hi', 'hu', 'is', 'it', 'ja', 'ko', 'lb',

Name	Spalte	Bedingung
		'nl', 'no', 'pl', 'pt', 'ro', 'ru', 'sk', 'sr', 'sv', 'tr', 'zh')

Indexes

Name	Spalte	Typ	Eindeutig
igt_usr_pk	id		yes
igt_usr_uk1	username		yes
igt_usr_uk2	email		yes

Foreign Keys

Role

Properties

Eigenschaft	Wert
Verwendung	
Erstellt	11 März 2022 14:33:01
Geändert	11 März 2022 14:33:01

Attributes

Name	Datentyp	Länge	Skalierung	Nullfähigkeit	Standard
id	varchar2	30		NOT NULL	
rowversion	varchar2	30		NOT NULL	
created_by	varchar2	30		NOT NULL	
created_on	date			NOT NULL	
updated_by	varchar2	30			
updated_on	date			NOT NULL	
active	number	1	0	NOT NULL	1
display_name	varchar2	128		NOT NULL	
description	varchar2	512			

Constraints

Unique Constraints

Diese Tabelle hat keine zusätzlichen Unique Constraints.

Check Constraints

Name	Spalte	Bedingung
igt_rol_ck1	active	active IN (0, 1)

Indexes**Indexes**

Name	Spalte	Typ	Eindeutig
igt_rol_pk	id		yes

Foreign Keys**User Role****Properties**

Eigenschaft	Wert
Verwendung	
Erstellt	11 März 2022 14:33:01
Geändert	11 März 2022 14:33:01

Attributes

Name	Datentyp	Länge	Skalierung	Nullfähigkeit	Standard
usr_id	number	10	0	NOT NULL	
rol_id	varchar2	30		NOT NULL	
rowversion	varchar2	30		NOT NULL	
created_by	varchar2	30		NOT NULL	
created_on	date			NOT NULL	
updated_by	varchar2	30			
updated_on	date			NOT NULL	

Constraints**Unique Constraints**

Diese Tabelle hat keine zusätzlichen Unique Constraints.

Check Constraints

Diese Tabelle hat keine zusätzlichen Check Constraints.

Indexes

Name	Spalte	Typ	Eindeutig
igt_url_pk	usr_id, rol_id		yes
uit_url_usr_fk	usr_id		no
uit_url_rol_fk	rol_id		no

Foreign Keys