ORACLE
Consulting

Connector Administration

Guide du connecteurOracle® Identity Manager pour Google Apigee Edge

Release 1.0.0

ORACLE

Connector Administration

Guide du connecteurOracle® Identity Manager pour Google Apigee Edge

Release 1.0.0

par Sophie Strecke, Dieter Steding, et Sylvert Bernet

Table des matières

Préface

Ce guide décrit le connecteur utilisé pour intégrer Oracle Identity Manager à Google Apigee Edge.

Public

Ce guide est destiné aux administrateurs de ressources et aux équipes d'intégration de systèmes cibles.

Documents connexes

Pour plus d'informations sur l'installation et l'utilisation d'Oracle Identity and Access Management, consultez la page suivante du centre d'aide Oracle:

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

Pour plus d'informations sur la documentation d'Identity Manager Connector, consultez la page suivante du centre d'aide Oracle:

- *http://docs.oracle.com/cd/E22999_01/index.htm*

Confidentialité

Les éléments contenus dans cette documentation représentent des informations exclusives et confidentielles relatives aux produits et méthodes Oracle.

Le public accepte que les informations contenues dans cette documentation ne soient pas divulguées en dehors d'Oracle, et ne doivent pas être dupliquées, utilisées ou divulguées â d'autres fins que l'évaluation de cette procédure.

Conventions typographiques

Les conventions de texte suivantes sont utilisées dans ce document.

Convention	Sens
caractères gras	Les caractères gras indiquent les éléments de l'interface utilisateur graphique associés â une action, ou les termes définis dans le texte ou le glossaire.
italique	Le type italique indique les titres de livres, l'emphase ou les variables d'espace réservé pour lesquelles vous fournissez des valeurs particulières.
monospace	Le type â espacement fixe indique les commandes dans un paragraphe, les URL, le code dans les exemples, le texte qui apparaît â l'écran ou le texte que vous saisissez.

À propos du connecteur

L'Oracle® Identity Manager Connector pour Google Apigee Edge intègre Oracle Identity Manager â Google Apigee Edge.

Oracle® Identity Manager est une solution de gestion des identités centralisée qui fournit des services de libre-service, de conformité, de provisionnement et de gestion des mots de passe pour les applications résidant sur site ou sur le Cloud. Oracle Identity Manager connecte les utilisateurs aux ressources, révoque et restreint les accès non autorisés pour protéger les informations sensibles de l'entreprise.

Oracle® Les connecteurs Identity Manager sont utilisés pour intégrer Identity Manager â des applications externes prenant en compte l'identité. Ce guide décrit les procédures de déploiement et d'utilisation du connecteur, qui intègre Oracle® Gestionnaire d'identité avec Google Apigee Edge. Le connecteur utilise l'API de gestion REST.

Ce guide décrit les procédures de déploiement et d'utilisation du connecteur, qui intègre Identity Manager â Google Apigee Edge.

Dans le mode de gestion de compte (ressource cible) du connecteur, les informations sur les utilisateurs créés ou modifiés directement sur le système cible peuvent être réconciliées dans Identity Manager. En outre, vous pouvez utiliser Identity Manager pour effectuer des opérations de provisionnement sur le système cible.

Présentation du connecteur

Le connecteur Google Apigee Edge est une solution permettant d'intégrer Oracle Identity Manager â Google Apigee Edge. Google Apigee Edge expose ses API ou interfaces REST pour la gestion des identités.

> **Note**
> À certains endroits de ce guide, Google Apigee Edge est appelé **système cible**.

Le connecteur Google Apigee Edge fournit un système centralisé pour rationaliser la fourniture de services et d'actifs aux consommateurs de votre entreprise, et gérer ces services et actifs d'une manière simple, sécurisée et rentable en utilisant l'automatisation. Le connecteur Google Apigee Edge standardise les processus de service et implémente l'automatisation pour remplacer les tâches manuelles.

Afin de se connecter â un système cible Google Apigee Edge, le connecteur Google Apigee Edge prend en charge l'authentification de base HTTP. Ce connecteur ne prend pas en charge l'authentification auprès du système cible en utilisant le jeton d'accès et le jeton d'actualisation comme entrée de l'utilisateur.

Si votre système cible ne prend en charge aucun des types d'authentification pris en charge par ce connecteur, vous pouvez implémenter l'authentification personnalisée prise en charge par votre système cible. Vous pouvez connecter cette implémentation personnalisée au connecteur â l'aide des plug-ins exposés par ce connecteur.

The Google Apigee Edge connector synchronizes data between Oracle Identity Manager and target systems by performing reconciliation and provisioning operations that parse data in the JSON format. If your target system does not support request or response payload in JSON format, then you can create your own implementation for parsing data. You can connect this custom implementation to the connector by using the plug-ins exposed by this connector.

Le connecteur Google Apigee Edge synchronise les données entre Oracle Identity Manager et les systèmes cibles en effectuant des opérations de réconciliation et de provisionnement qui analysent les données au format JSON. Si votre système cible ne prend pas en charge la charge utile de demande ou de réponse au format JSON, vous pouvez créer votre propre

implémentation pour l'analyse des données. Vous pouvez connecter cette implémentation personnalisée au connecteur â l'aide des plug-ins exposés par ce connecteur.

Exigences du connecteur

Il s'agit des composants logiciels et de leurs versions nécessaires â l'intégration d'Oracle Identity Manager avec un connecteur Google Apigee Edge.

Required Versions

Composante	Version
Oracle Java Development Kit	JDK 1.8.0_131 or higher
Oracle Infrastruktur	Oracle® WebLogic 12c (12.2.1.3.0)
Oracle Database	Oracle® RDBMS 12c (12.2.0.1.0) or higher
Oracle Identity Governance	Oracle® Identity Governance 12c Release 12.2.1.3.0
Connector Server	Identity Connectore Server Release 12.2.1.3.0

Required Patches

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

Architecture du connecteur

Le connecteur Google Apigee Edge est mis en œuvre â l'aide d'Identity Connector Framework (ICF).

L'ICF est livré avec Oracle Identity Manager.

L'ICF est un composant qui fournit des opérations de rapprochement et d'approvisionnement de base communes â tous les connecteurs Oracle Identity Manager. In addition, ICF provides common features that developers would otherwise need to implement on their own, such as connection pooling, buffering, time outs, and filtering.

La figure 1-1 illustre l'intégration d'Oracle Identity Manager sur site avec le service Google Apigee Edge.

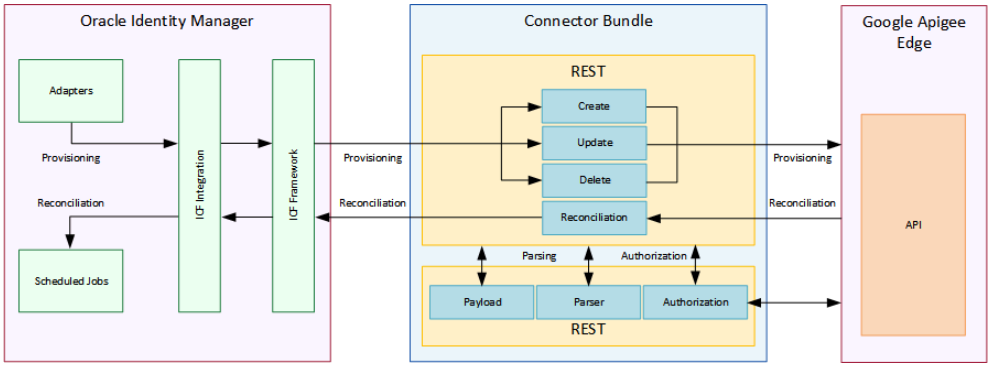

Figure 1-1: Architecture du connecteur Google Apigee Edge

Caractéristiques du connecteur

Les fonctionnalités du connecteur incluent la prise en charge de la réconciliation complète et incrémentielle, de la réconciliation limitée, de l'authentification personnalisée, de l'analyse personnalisée, de la charge utile personnalisée, de la gestion de plusieurs URL de point de terminaison et de la communication SSL.

Voici les caractéristiques du connecteur:

- Authentification
- Communication sécurisée
- Rapprochement complet et incrémentiel
- Rapprochement limité (filtré)

Authentication

Par défaut, le connecteur Google Apigee Edge prend en charge l'authentification de base HTTP.

Si votre système cible utilise les mécanismes d'authentification qui ne sont pas pris en charge par le connecteur, vous pouvez écrire votre propre implémentation pour l'authentification personnalisée â l'aide des plug-ins exposés par ce connecteur.

Communication sécurisée

Vous pouvez configurer la communication SSL entre Oracle Identity Manager et le système cible Google Apigee Edge.

Consultez la section Configuration SSL pour le connecteur Google Apigee Edge pour plus d'informations sur la configuration d'une communication sécurisée.

Rapprochement complet et incrémentiel

Après avoir créé le connecteur, vous pouvez effectuer une réconciliation complète pour transférer toutes les données utilisateur existantes du système cible vers Oracle Identity Manager. Après la première exécution de réconciliation complète, vous pouvez configurer votre connecteur pour une réconciliation incrémentielle. Dans la réconciliation incrémentielle, seuls les enregistrements ajoutés ou modifiés après la dernière exécution de réconciliation sont récupérés dans Oracle Identity Manager. Voir Implémentation de l'authentification personnalisée.

Vous pouvez effectuer un cycle de rapprochement complet â tout moment.

Rapprochement limité (filtré)

Vous pouvez rapprocher les enregistrements du système cible en fonction d'un critère de filtre spécifié. Pour limiter ou filtrer les enregistrements extraits dans Oracle Identity Manager lors d'une exécution de rapprochement, vous pouvez spécifier le sous-ensemble d'enregistrements du système cible ajoutés ou modifiés qui doivent être rapprochés.

Vous pouvez définir un filtre de rapprochement comme valeur de l'attribut Filtre des tâches planifiées. Ce filtre spécifie le sous-ensemble d'enregistrements du système cible nouvellement ajoutés et modifiés qui doivent être rapprochés. Voir Réconciliation limitée pour Google Apigee Edge Connector.

Déployer le connecteur

TBD

Enregistrement

TBD