OCI Cloud Guardrails - FR

Oracle OCI Cloud Guardrails Francais

Ludovic Dessemon Enterprise Cloud Strategist at Oracle

Description

Prowler est un outil de ligne de commande pour OCI Cloud Guardrails, initialement développé par Toni de la Fuente (https://github.com/toniblyx/prowler)

OCI Prowler est une adaptation pour Oracle Cloud Infrastructure, développé par Ludovic Dessemon, Enterprise Cloud Strategist (Oracle Canada) - Juillet 2020

Exigences et installation

Ce script a été écrit en bash et Python en utilisant le Python SDK pour Oracle Cloud Infrastructure, Oracle Identity Cloud Service REST APIs, et OCI CLI.

Oracle Identity Cloud Service REST APIs

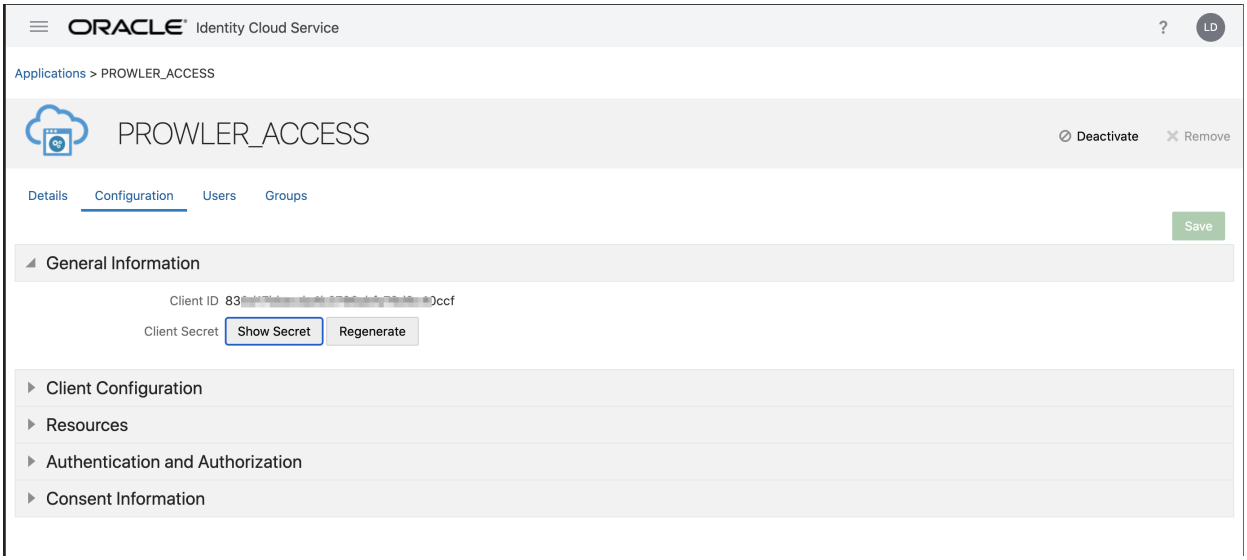
Les API REST d'Oracle Identity Cloud Service prennent en charge les points de terminaison compatibles SCIM 2.0 avec les schémas principaux SCIM 2.0 standard et les extensions de schéma Oracle pour gérer par programme les utilisateurs, les groupes, les applications et les fonctions d'identité, telles que la gestion des mots de passe et les tâches administratives. Pour effectuer des appels d'API REST vers votre environnement Oracle Identity Cloud Service, vous avez besoin d'un jeton d'accès OAuth2 à utiliser pour l'autorisation. Le jeton d'accès fournit une session (avec étendue et expiration), que votre application cliente peut utiliser pour effectuer des tâches dans Oracle Identity Cloud Service.

Les sections suivantes vous expliquent les étapes requises pour utiliser le Prowler OCI avec les API REST d'Oracle Identity Cloud Service:

Enregistrer une application confidentielle dans Oracle Identity Cloud Service

- Accédez à votre instance Oracle Identity Cloud Service (par exemple: https: // tenant-base-url / ui / v1 / adminconsole) et connectez-vous avec vos informations d'identification d'administrateur de domaine d'identité.
- Cliquez sur **Applications**, puis **Add**
- Choisir **Confidential Application** comme type d'application.
- Saisir un **nom d'application** (eg. ProwlerAccess) et une description, puis cliquer sur **Next**.
- Sur la page Autorisation, définissez les éléments suivants:
  - Choisir l'option **Configure this application as a client now**.
  - Choisir **Client Credentials** depuis la section **Allowed Grant Type**.
  - Au bas de la page cochez la case **Grant the client access to Identity Cloud Service Admin APIs** .
  - Cliquez sur votre curseur dans la zone qui apparaît sous la case à cocher, puis sélectionnez le type d'accès pour les API REST. Par exemple, choisir **Identity Domain**

Administrator. Vos informations d'identification et toutes les tâches disponibles pour l'administrateur du domaine d'identité vous seront accessibles.
    - Cliquez **Next**, puis **Finish**.
    - Prenez note (à l'aide de votre utilitaire de notes préféré) de l'ID client et du secret client qui apparaissent dans la fenêtre de confirmation, puis cliquez sur **Close**.
- Cliquez **Activate** dans la section supérieure droite de la page pour activer l'application.



Oracle OCI CLI

Aperçu

L'outil CLI est un outil à faible encombrement que vous pouvez utiliser seul ou avec la console pour terminer les tâches d'Oracle Cloud Infrastructure. L'interface de ligne de commande fournit les mêmes fonctionnalités de base que la console, ainsi que des commandes supplémentaires. Certains d'entre eux, comme la possibilité d'exécuter des scripts, étendent les fonctionnalités de la console.
Ce script utilise OCI CLI.

Installation

Linux

- Ouvrir un terminal
- Pour exécuter le script du programme d'installation, exécutez la commande suivante.

```
bash -c "$(curl -L https://raw.githubusercontent.com/oracle/oci-cli/master/scripts/install/install.sh)"
```

- Répondez aux invites du script d'installation.

Si vous utilisez Oracle Linux 7, vous pouvez utiliser yum pour installer CLI.

```
sudo yum install python36-oci-cli
```

Mac OS X

Vous pouvez utiliser Homebrew pour installer, mettre à niveau et désinstaller CLI sous Mac OS.

Pour installer CLI sur Mac OS X avec Homebrew:

```
brew update && brew install oci-cli
```

Pour mettre à niveau votre installation CLI sur Mac OS X à l'aide de Homebrew:

```
brew update && brew upgrade oci-cli
```

Pour désinstaller CLI sur Mac OS X à l'aide de Homebrew:

```
brew uninstall oci-cli
```

Windows

- Ouvrez la console PowerShell à l'aide de l'option Exécuter en tant qu'administrateur.
- Le programme d'installation active la saisie semi-automatique en installant et en exécutant un script. Pour autoriser ce script à s'exécuter, vous devez activer la stratégie d'exécution RemoteSigned.
  Pour configurer la stratégie d'exécution à distance pour PowerShell, exécutez la commande suivante.

```
Set-ExecutionPolicy RemoteSigned
```

- Téléchargez le script d'installation:

```
Invoke-WebRequest https://raw.githubusercontent.com/oracle/oci-cli/maste
r/scripts/install/install.ps1 -OutFile install.ps1
```

- Exécutez le script du programme d'installation avec ou sans invites:

```
iex ((New-ObjectSystem.Net.WebClient).DownloadString('https://raw.githubu
sercontent.com/oracle/oci-cli/master/scripts/install/install.ps1'))
```

Invites de script d'installation

Le script d'installation vous demande les informations suivantes.

- Si vous n'avez pas de version compatible de Python installée:
  - Windows et Linux: vous êtes invité à fournir un emplacement pour l'installation des binaires et des exécutables. Le script installera Python pour vous.
  - MacOS: vous êtes averti que votre version de Python est incompatible. Vous devez mettre à niveau avant de pouvoir procéder à l'installation. Le script n'installera pas Python pour vous.
- Lorsque vous êtes invité à mettre à niveau CLI vers la dernière version, répondez par Y pour écraser une installation existante.
- Lorsque vous êtes invité à mettre à jour votre PATH, répondez par Y pour pouvoir appeler CLI sans fournir le chemin complet de l'exécutable. Cela ajoutera oci.exe à votre PATH.

Configuration du fichier de configuration

Avant d'utiliser l'interface de ligne de commande, vous devez créer un fichier de configuration contenant les informations d'identification requises pour travailler avec Oracle Cloud Infrastructure. Vous pouvez créer ce fichier à l'aide d'une boîte de dialogue de configuration ou manuellement à l'aide d'un éditeur de texte.

```
vi ~/.oci/config
```

Pour que CLI vous guide tout au long du processus de configuration initiale, utilisez la commande oci setup config. La commande vous demande les informations requises pour le fichier de configuration et les clés publiques / privées de l'API. La boîte de dialogue de configuration génère une paire de clés API et crée le fichier de configuration.

Si vous souhaitez configurer vous-même les clés publiques / privées de l'API et écrire votre propre fichier de configuration, cf SDK and Tool Configuration.

OCI SDK pour Python

Il est fortement recommandé d'utiliser un environnement virtuel Python lors de l'installation d'oci. Veuillez consulter le guide Installing packages using pip and virtualenv de la Python Software Foundation pour plus d'informations sur les environnements virtuels.

Voir le guide d'installation pour le dépannage de l'installation et les méthodes d'installation alternatives.
Une fois votre environnement virtuel actif, oci peut être installé à l'aide de pip.

```
pip install oci
```

Usage

1. Exécutez la commande `prowler` sans options (elle utilisera les informations d'identification de la variable d'environnement si elles existent ou utilisera par défaut le fichier `~/.oci/config` et exécutera les vérifications):

```
./prowler
```

Utilisez `-l` pour lister tous les contrôles disponibles et les groupes (sections) qui les référencent

2. Pour un contrôle unique, utilisez l'option `-c` :

```
./prowler -c check310
```

ou plusieurs contrôles séparés par une virgule:

```
./prowler -c check310,check722
```

ou tous les contrôles mais certains d'entre eux:

```
./prowler -E check42,check43
```

ou pour un profil personnalisé:

```
./prowler -p custom-profile -c check11
```

ou pour un groupe de contrôles, utilisez le nom du groupe:

```
./prowler -g group1
```

ou exclure certains contrôles du groupe:

```
./prowler -g group4 -E check42,check43
```

Sauvegardez vos rapports

1. Si vous souhaitez enregistrer votre rapport pour une analyse ultérieure, il existe différentes manières, nativement (texte pris en charge, mono, csv, json, json-asff et junit-xml, voir la note ci-dessous pour plus d'informations):

```
./prowler -M csv
```

ou avec plusieurs formats en même temps:

```
./prowler -M csv,json,json-asff
```

ou tout simplement un groupe de contrôles dans plusieurs formats:

```
./prowler -g gdpr -M csv,json,json-asff
```

Maintenant, `-M` crée un fichier dans le répertoire racine du rôdeur nommé 'ociprowler-output - YYYYMMDDHHMMSS.format`. Vous n'avez rien à spécifier d'autre, pas de tuyaux, pas de redirections.

ou simplement enregistrer la sortie dans un fichier comme ci-dessous:

```
./prowler -M mono > prowler-report.txt
```

ou si vous voulez un rapport HTML coloré, faites:

```
pip install ansi2html
./prowler | ansi2html -la > report.html
```

Pour générer des fichiers de rapport JUnit, incluez le format junit-xml. Cela peut être combiné avec n'importe quel autre format. Les fichiers sont écrits dans un répertoire racine de prowler nommé `junit-reports` :

```
./prowler -M text,junit-xml
```

> Remarque sur les formats de sortie à utiliser avec `-M` :" text "est celui par défaut avec les couleurs, "mono" est comme celui par défaut mais monochrome, "csv" est des valeurs séparées par des virgules, "json" json basique simple (sans virgule entre lignes) .

2. Si vous voulez exécuter Prowler pour vérifier plusieurs comptes OCI en parallèle (jusqu'à 4 simultanément `-P 4`):

```
grep -E '^\[([0-9A-Aa-z_-]+)\]'  ~/.oci/config | tr -d '][' | shuf |
 \
xargs -n 1 -L 1 -I @ -r -P 4 ./prowler -p @ -M csv  2> /dev/null  >> a
ll-accounts.csv
```

3. Pour obtenir de l'aide:

```
./prowler -h
```

Utilisation avancée

Dossier personnalisé pour les contrôles personnalisés

L'indicateur `-x /my/own/checks` inclura toute vérification dans ce répertoire particulier.

Afficher ou enregistrer uniquement les échecs

Afin de supprimer le bruit et de n'obtenir que les résultats d'échec, il existe un indicateur `-q` qui oblige Prowler à n'afficher et à enregistrer que les échecs. Il peut être combiné avec n'importe quelle autre option.

```
./prowler -q -M csv -b
```

Exécuter Prowler

export OCI_CONFIG=/Users/ludovicdessemon/.oci/config
export PATH=**OCI_CLI_Path**/bin:$PATH

Ajouter des contrôles personnalisés

Afin d'ajouter un nouveau contrôle, n'hésitez pas à créer un nouveau contrôle supplémentaire dans le groupe extras ou dans un autre groupe. Pour ce faire, vous devrez suivre ces étapes:

1. Suivez la structure du fichier `checks/check_sample`
2. Nommez votre contrôle avec un numéro faisant partie d'un groupe existant ou d'un nouveau
3. Enregistrez les modifications et exécutez-le sous `./prowler -c extraNN`

Ajouter des groupes personnalisés

1. Suivez la structure dans le fichier `groups/groupN_sample`
2. Nommez votre groupe avec un numéro inexistant
3. Enregistrez les modifications et exécutez-le sous `./prowler -g extraNN`
    - Vous pouvez également créer un groupe avec uniquement les contrôles que vous souhaitez effectuer dans votre entreprise, par exemple un groupe nommé `group9_mycompany` avec uniquement la liste des contrôles qui vous intéressent ou votre conformité particulière s'applique.

Licence