



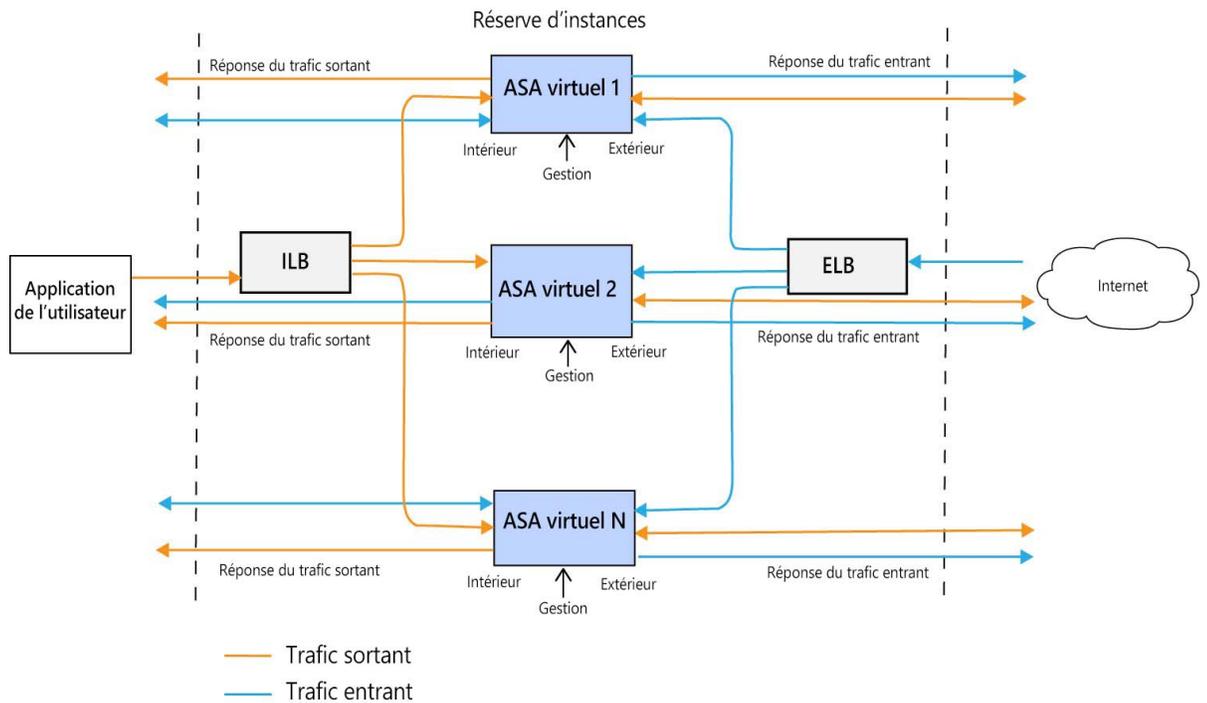
Déployer la solution d'évolutivité automatique ASA virtuel sur OCI

- [Scénario](#) , à la page 1
- [Prérequis](#), à la page 2
- [Préparation du fichier de configuration ASA](#), à la page 8
- [Déployer la solution d'évolutivité automatique](#), à la page 14
- [Valider le déploiement](#), à la page 19
- [Mise à niveau](#), à la page 20
- [Supprimer la configuration d'évolutivité automatique d'OCI](#), à la page 21

Scénario

Le scénario pour cet ASA virtuel : la solution d'évolutivité automatique OCI est illustrée dans le diagramme des scénarios. L'équilibreur de charges Internet a une adresse IP publique et des ports activés à l'aide d'une combinaison de l'écouteur et du groupe cible.

Illustration 1 : Diagramme de scénario



Le partage basé sur le port peut être mis en œuvre pour le trafic réseau. Cela peut être réalisé en utilisant des règles NAT. Cet exemple de configuration est expliqué dans les sections suivantes.

Prérequis

Autorisations et politiques

Voici les autorisations et les politiques OCI dont vous avez besoin pour implémenter la solution :

1. Utilisateurs et groupe



Remarque Vous devez être un utilisateur OCI ou un administrateur de location pour créer les utilisateurs et les groupes.

Créez des comptes d'utilisateurs Oracle Cloud Infrastructure et un groupe auquel ces comptes d'utilisateurs appartiennent. Si le groupe approprié avec les comptes d'utilisateurs existe, vous n'avez pas besoin de les créer. Pour obtenir des instructions sur la création des utilisateurs et des groupes, consultez [Création de groupes et d'utilisateurs](#).

2. Politiques de groupe

Vous devez créer les politiques, puis les mapper au groupe. Pour créer les politiques, accédez à **OCI > Identity & Security (Identité et sécurité) > Politiques (Politiques) > Create Policy (Créer une politique)**. Créez et ajoutez les politiques suivantes au groupe souhaité :

- Autoriser le groupe `<Group_Name>` à utiliser les mesures dans le compartiment `<Compartment_Name>`
- Autoriser le groupe `<Group_Name>` à gérer les alarmes dans le compartiment `<Compartment_Name>`
- Autoriser le groupe `<Group_Name>` à gérer les sujets pertinents dans le compartiment `<Compartment_Name>`
- Autoriser le groupe `<Group_Name>` à inspecter les mesures dans le compartiment `<Compartment_Name>`
- Autoriser le groupe `<Group_Name>` à lire les mesures dans le compartiment `<Compartment_Name>`
- Autoriser le groupe `<Group_Name>` à utiliser des espaces de noms de balises dans le compartiment `<Compartment_Name>`
- Autoriser le groupe `<Group_Name>` à lire les groupes de journaux dans le compartiment `<Compartment_Name>`
- Autoriser le groupe `<Group_Name>` à utiliser le compartiment de regroupement d'instances `<Compartment_Name>`
- Autoriser le groupe `<Group_Name>` à utiliser Cloud Shell dans la location
- Autoriser le groupe `<Group_Name>` à lire l'espace de nom du stockage d'objets dans la location
- Autoriser le groupe `<Group_Name>` à gérer les référentiels dans la location

**Remarque**

Vous pouvez également créer des politiques au niveau de la location. Vous êtes libre de décider comment vous souhaitez accorder toutes les autorisations.

3. Autorisation pour les fonctions Oracle

Pour permettre à une fonction Oracle d'accéder à une autre ressource d'Oracle Cloud Infrastructure, incluez la fonction dans un groupe dynamique, puis créez une politique pour accorder l'accès du groupe dynamique à cette ressource.

4. Créer un groupe dynamique

Pour créer des groupes dynamiques, accédez à **OCI > Identity & Security (Identité et sécurité) > Dynamic Group (Groupe dynamique) > Create Dynamic Group (Créer un groupe dynamique)**

Précisez la règle suivante lors de la création du groupe dynamique :

```
TOUS {resource.type = « fnfunc », resource.compartment.id = « <Your_Compartment_OCID> »}
```

Pour en savoir plus sur les groupes dynamiques, consultez :

- <https://docs.oracle.com/en-us/iaas/Content/Functions/Tasks/functionsaccessingociresources.htm>
- <https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm>

5. Créer une politique pour un groupe dynamique

Pour ajouter une politique, accédez à **OCI > Identity & Security (Identité et sécurité) > Politiques (Policies) > Create Policy (Créer une politique)**. Ajoutez la politique suivante au groupe :

Autoriser le groupe dynamique `<Dynamic_Group_Name>` à gérer toutes les ressources dans le compartiment `<Compartment_OCID>`

Téléchargez les fichiers à partir de GitHub

ASA virtuel : la solution d'évolutivité automatique OCI est fournie en tant que référentiel [GitHub](#). Vous pouvez extraire ou télécharger les fichiers du référentiel.

Environnement Python 3

Un fichier `make.py` se trouve dans le référentiel cloné. Ce programme compresse les fonctions oracle et les fichiers de modèle dans un fichier Zip; copiez-les dans un dossier cible. Afin d'effectuer ces tâches, l'environnement Python 3 doit être configuré.



Remarque Ce script Python ne peut être utilisé que dans l'environnement Linux.

Configuration de l'infrastructure

Les éléments suivants doivent être configurés :

1. VCN

Créez le VCN selon les besoins de votre application ASA virtuel. Créez le VCN avec la passerelle Internet ayant au moins un sous-réseau associé à une route vers Internet.

Pour en savoir plus sur la création du VCN, consultez <https://docs.oracle.com/en-us/iaas/Content/GSG/Tasks/creatingnetwork.htm>.

2. Sous-réseaux d'application

Créez des sous-réseaux selon les besoins de votre application ASA virtuel. Pour implémenter la solution selon ce scénario, l'instance ASA virtuel nécessite trois sous-réseaux pour fonctionner.

Pour en savoir plus sur la création d'un sous-réseau, consultez https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingVCNs_topic-Overview_of_VCNs_and_Subnets.htm#.

3. Sous-réseau externe

Le sous-réseau doit avoir une route avec « 0.0.0.0/0 » vers la passerelle Internet. Ce sous-réseau contient l'interface externe de Cisco ASA virtuel et l'équilibreur de charges sur Internet. Assurez-vous que la passerelle NAT est ajoutée pour le trafic sortant.

Pour en savoir plus, consultez les documents suivants :

- <https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingIGs.htm>
- https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/NATgateway.htm#To_create_a_NAT_gateway

4. Sous-réseau interne

Ceci est similaire aux sous-réseaux d'application, avec ou sans passerelle NAT/Internet.



Remarque Pour les sondes d'intégrité ASA virtuel, vous pouvez atteindre le serveur de métadonnées (169.254.169.254) par le port 80.

5. Management Subnet (Sous-réseau de gestion)

Le sous-réseau de gestion doit être public afin de prendre en charge l'accessibilité SSH avec ASA virtuel.

6. Groupes de sécurité – Groupe de sécurité réseau pour l'instance ASA virtuel

Configurez le groupe de sécurité pour les instances ASA virtuel qui répondent aux exigences suivantes :

- Les fonctions Oracle (dans le même VCN) établissent des connexions SSH à l'adresse de gestion de ASA virtuel.
- Les hôtes d'administration peuvent avoir besoin d'un accès SSH aux instances d'ASA virtuel.
- L'ASA virtuel initie la communication avec les serveurs CSSM/satellite pour les licences.

7. Espace de nom du stockage d'objets

Cet espace de nom du stockage d'objets est utilisé pour l'hébergement d'un site Web statique, ayant le fichier configuration.txt. Vous devez créer des demandes préauthenticées pour le fichier configuration.txt. Cette URL préauthenticée est utilisée lors du déploiement du modèle.



Remarque Assurez-vous que les configurations suivantes qui sont chargées sont accessibles par les instances de ASA virtuel par l'intermédiaire de l'URL HTTP.

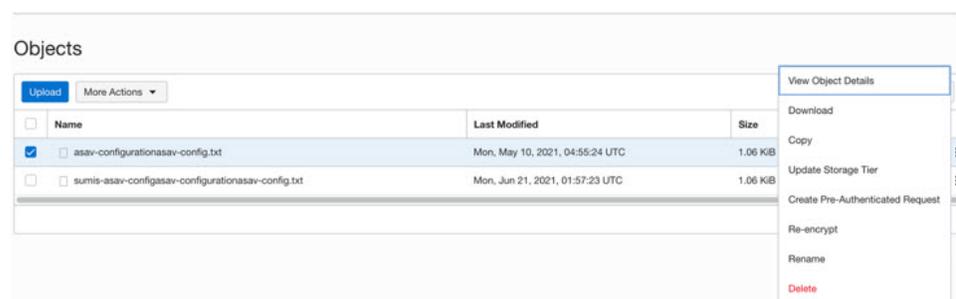
Lorsque ASA virtuel est démarré, il exécute la commande suivante `$ copy /noconfirm <URL de demande préauthenticée du fichier configuration.txt > disk0:Configuration.txt`

Cette commande permet de configurer le lancement de ASA virtuel avec le fichier configuration.txt.

8. Charger le fichier configuration.txt

Pour créer une URL de demande préauthenticée du fichier de configuration ASA virtuel :

1. Cliquez sur **Buckets (Compartiments) > Create Bucket (Créer un compartiment)**.
2. Cliquez sur **Upload (Charger)**.
3. Lorsque le fichier de configuration est chargé, choisissez **Create Pre-Authenticated Request (Créer une demande préauthenticée)** comme illustré dans la figure ci-dessous.





Remarque Le fichier de configuration devrait maintenant être accessible à partir de la fonction oracle.

Configuration du réseau

1. Trafic entrant

Assurez-vous que l'adresse *<IP de la VM d'application>* est correcte dans configuration.txt, comme mentionné dans [Configuration des objets, des licences, des règles NAT et des politiques d'accès](#).

2. Trafic sortant

- Assurez-vous que l'adresse *<IP du serveur externe>* est correcte dans configuration.txt, comme mentionné dans [Configuration des objets, des licences, des règles NAT et des politiques d'accès](#).
- Assurez-vous qu'il y a une passerelle NAT dans votre VCN externe.
- Assurez-vous d'ajouter la même adresse *<IP du serveur externe>* dans la table de routage de votre VCN externe, à destination de la passerelle NAT, comme illustré dans l'exemple ci-dessous :

<input type="checkbox"/>	Destination	Target Type	Target
<input type="checkbox"/>	0.0.0.0/0	Internet Gateway	outside-ig
<input type="checkbox"/>	8.8.8.8/32	NAT Gateway	nat-gw

Chiffrer le mot de passe



Remarque Pour en savoir plus sur cette procédure, consultez [Créer des vaults et des secrets](#).

Le mot de passe pour ASA virtuel est utilisé pour configurer toutes les instances de ASA virtuel utilisées lors de l'évolutivité automatique et il est utilisé pour récupérer les données d'utilisation du processeur (CPU) des instances ASA virtuel.

Par conséquent, vous devez enregistrer le mot de passe et le réinitialiser de temps en temps. En raison des modifications courantes et de la vulnérabilité, la modification ou l'enregistrement du mot de passe en texte brut n'est pas autorisée. Le mot de passe doit être en format chiffré uniquement.

Pour obtenir le mot de passe chiffré :

Procédure

Étape 1

Créez un vault.

OCI Vault fournit des services pour créer et enregistrer des clés de chiffrement principales en toute sécurité, et des méthodes de chiffrement et de déchiffrement pour leur utilisation. Vault doit donc être créé (si ce n'est déjà fait) dans le même compartiment que le reste de la solution d'évolutivité automatique.

Accédez à **OCI > Identity & Security (identité et sécurité) > Vault > Choose or Create a new Vault (choisir ou créer un nouveau vault)**

Étape 2

Créez une clé de chiffrement principale.

Une clé de chiffrement principale est nécessaire pour chiffrer le mot de passe en texte brut.

Accédez à **OCI > Identity & Security (identité et sécurité) > Vault > Choose or Create Key (choisir ou créer une clé)**

Choisissez l'une des clés de l'algorithme donné avec n'importe quel bit de longueur.

1. AES – 128, 192, 256
2. RSA – 2048, 3072, 4096
3. ECDSA – 256, 384, 521

Illustration 2 : Créer une clé

Étape 3

Créez un mot de passe chiffré.

1. Accédez à **OCI > Open CloudShell (OCI Cloud Terminal)** (ouvrir CloudShell (terminal OCI Cloud)).
2. Exécutez la commande suivante en remplaçant *<Password>* par votre mot de passe.

```
echo -n '<Password>' | base64
```

3. À partir du Vault sélectionné, copiez le terminal cryptographique et l'OCID de la clé de chiffrement principale. Remplacez les valeurs suivantes, puis exécutez la commande de chiffrement :
 - KEY_OCID avec l'OCID de votre clé
 - Cryptographic_Endpoint_URL avec l'URL du terminal cryptographique de votre Vault
 - Password avec votre mot de passe

Commande de chiffrement

```
oci kms crypto encrypt --key-id Key_OCID --endpoint
Cryptographic_Endpoint_URL --plaintext <base64-value-of-password>
```

4. Copiez le texte chiffré à partir de la sortie de la commande ci-dessus et utilisez-le selon vos besoins.

Préparation du fichier de configuration ASA

Assurez-vous que l'application est déployée ou que son plan de déploiement est disponible.

Procédure

Étape 1 Collectez les paramètres d'entrée suivants avant le déploiement :

Paramètre	Type de données	Description
tenancy_ocid	Chaîne	OCID de la location à laquelle votre compte appartient. Pour savoir comment trouver votre OCID de location, consultez ici . L'OCID de location ressemble à ceci : <code>ocid1.tenancy.oc1..<ID_unique></code>
compartment_id	Chaîne	L'OCID du compartiment dans lequel créer les ressources. Exemple : <code>locid1.compartment.oc1..<ID_unique></code>
compartment_name	Chaîne	Nom du compartiment
région	Chaîne	Identificateur unique de la région dans laquelle vous souhaitez que les ressources soient créées. Exemple : <code>us-phoenix-1, us-ashburn-1</code>
lb_size	Chaîne	Un modèle qui détermine la bande passante préprovisionnée totale (entrée plus sortie) de l'équilibreur de charges externe et interne. Valeurs prises en charge : 100 Mbit/s, 10 Mbit/s, 10 Mbit/s-Micro, 400 Mbit/s, 8 000 Mbit/s Exemple : 100 Mbit/s

Paramètre	Type de données	Description
availability_domain	Valeurs séparées par des virgules	Exemple : Tpeb:PHX-AD-1 Remarque Exécutez la commande oci iam availability-domain list dans Cloud Shell pour obtenir les noms de domaine de disponibilité.
min_and_max_instance_count	Valeurs séparées par des virgules	Le nombre minimal et maximal d'instances que vous souhaitez conserver dans le groupe d'instances. Exemple : 1,5
autoscale_group_prefix	Chaîne	Le préfixe à utiliser pour nommer toutes les ressources créées à l'aide du modèle. Par exemple, si le préfixe de ressource est « autoscale », toutes les ressources sont nommées comme suit : autoscale_resource1, autoscale_resource2, etc.
asav_config_file_url	URL	L'URL du fichier de configuration chargé dans le stockage d'objets à utiliser pour configurer l'ASA virtuel. Remarque L'URL de demande préauthentification du fichier de configuration doit être donnée. Exemple : https://objectstorage.<nom-region>.oraclecloud.com/<nom-objet-stockage>/oci-asav-configuration.txt
mgmt_subnet_ocid	Chaîne	OCID du sous-réseau de gestion qui doit être utilisé.
inside_subnet_OCID	Chaîne	OCID du sous-réseau interne qui doit être utilisé.
outside_subnet_ocid	Chaîne	OCID du sous-réseau externe qui doit être utilisé.
mgmt_nsg_ocid	Chaîne	OCID du groupe de sécurité réseau du sous-réseau de gestion qui doit être utilisé.
inside_nsg_ocid	Chaîne	OCID du groupe de sécurité réseau du sous-réseau interne qui doit être utilisé.

Paramètre	Type de données	Description
outside_nsg_ocid	Chaîne	OCID du groupe de sécurité réseau du sous-réseau externe qui doit être utilisé.
elb_listener_port	Valeurs séparées par des virgules	Liste des ports de communication pour l'écouteur de l'équilibreur de charges externe. Exemple : 80
ilb_listener_port	Valeurs séparées par des virgules	Liste des ports de communication pour l'écouteur de l'équilibreur de charges interne. Exemple : 80
health_check_port	Chaîne	Le port du serveur principal de l'équilibreur de charges par rapport auquel la vérification d'intégrité est exécutée. Exemple : 8080
instance_shape	Chaîne	La forme de l'instance à créer. La forme détermine le nombre de CPU, la quantité de mémoire et d'autres ressources qui sont allouées à l'instance. Formes prises en charge : « VM.Standard2.4 » et « VM.Standard2.8 »
lb_bs_policy	Chaîne	La politique d'équilibreur de charges à utiliser pour l'ensemble principal de l'équilibreur de charges interne et externe. Pour en savoir plus sur le fonctionnement des politiques d'équilibreur de charges, consultez ce lien . Valeurs prises en charge : « ROUND_ROBIN », « LEAST_CONNECTIONS », « IP_HASH »

Paramètre	Type de données	Description
image_name	Chaîne	<p>Le nom de l'image de Marché à utiliser pour créer la configuration d'instance.</p> <p>Valeur par défaut : « Cisco ASA virtual firewall (ASAv) » (pare-feu virtuel Cisco ASA (ASAv))</p> <p>Remarque Si l'utilisateur souhaite déployer une image personnalisée, il doit configurer le paramètre custom_image_ocid.</p>
image_version	Chaîne	<p>La version de l'image ASA virtuel disponible dans le Marché OCI à utiliser. Actuellement, les versions 9.15.1.15 et 9.16.1 sont disponibles.</p> <p>Valeur par défaut : « Cisco ASA virtual firewall (ASAv) » (pare-feu virtuel Cisco ASA (ASAv))</p>
scaling_thresholds	Valeurs séparées par des virgules	<p>Les seuils d'utilisation du CPU à utiliser pour l'évolutivité à la baisse ou à la hausse. Précisez les valeurs de seuil d'évolutivité à la baisse et à la hausse séparées par des virgules.</p> <p>Exemple : 15,50</p> <p>où 15 est le seuil d'évolutivité à la baisse et 50 est le seuil d'évolutivité à la hausse.</p>
custom_image_ocid	Chaîne	<p>OCID de l'image personnalisée à utiliser pour créer la configuration de l'instance si l'image du Marché ne doit pas être utilisée.</p> <p>Remarque custom_image_ocid est un paramètre facultatif</p>
asav_password	Chaîne	<p>Le mot de passe pour ASA virtuel sous forme chiffrée, en utilisant le protocole SSH dans l'ASA virtuel pour la configuration. Utilisez le guide de configuration pour les instructions sur la façon de chiffrer le mot de passe ou consultez ce lien.</p>

Paramètre	Type de données	Description
cryptographic_endpoint	Chaîne	Le terminal cryptographique est une URL utilisée pour déchiffrer le mot de passe. Il se trouve dans le Vault (centre de stockage).
master_encryption_key_id	Chaîne	L'OCID de la clé avec laquelle le mot de passe a été chiffré. Il se trouve dans le Vault (centre de stockage).
Profile Name (Nom de profil)		Il s'agit du nom de profil de l'utilisateur dans OCI. Il se trouve dans la section du profil de l'utilisateur. Exemple : oracleidentitycloudservice/<utilisateur>@<mail>.com
Object Storage Namespace (espaces de nom du stockage d'objet)		Il s'agit d'un identifiant unique créé au moment de la création de la location. Vous pouvez trouver cette valeur dans OCI > Administration > Tenancy Details (détails de la location)
Jeton d'autorisation		Il est utilisé comme mot de passe pour la connexion au docker, qui autorise l'envoi d'Oracle-Functions dans le registre de conteneur OCI. Pour se procurer le jeton, accédez à OCI > Identity (identité) > Users (utilisateurs) > User Details (détails de l'utilisateur >) Auth Tokens (jetons d'autorisation) > Generate Token (générer un jeton) .

Étape 2

Configurez les objets, les licences, la règle NAT pour les sondes d'intégrité de l'équilibreur de charges et les politiques d'accès.

```
! Default route via outside
route outside 0.0.0.0 0.0.0.0 <Outside Subnet gateway> 2

! Health Check Configuration
object network metadata-server
host 169.254.169.254
object service health-check-port
service tcp destination eq <health-check-port>
object service http-port
service tcp destination eq <traffic port>
route inside 169.254.169.254 255.255.255.255 <Inside Subnet GW> 1

! Health check NAT
nat (outside,inside) source static any interface destination static interface metadata-server service
health-check-port http-port
nat (inside,outside) source static any interface destination static interface metadata-server service
health-check-port http-port
```

```

! Outbound NAT
object network inside-subnet
subnet <Inside Subnet> <Inside Subnet Gateway>
object network external-server
host <External Server IP>
nat (inside,outside) source static inside-subnet interface destination static interface
external-server

! Inbound NAT
object network outside-subnet
subnet <Outside Subnet> <Outside Subnet GW>
object network http-server-80
host <Application VM IP>
nat (outside,inside) source static outside-subnet interface destination static interface
http-server-80

!
dns domain-lookup outside
DNS server-group DefaultDNS

! License Configuration
call-home
profile license
destination transport-method http
destination address http <URL>
debug menu license 25 production
license smart
feature tier standard
throughput level <Entitlement>
licence smart register idtoken <License token> force
!

```

Ces connexions de sonde d'intégrité et cette configuration de plan de données doivent être autorisées sur la politique d'accès.

Étape 3 Mettez à jour le fichier *configuration.txt* avec les détails de la configuration.

Étape 4 Chargez le fichier *configuration.txt* dans l'espace de stockage d'objets créé par l'utilisateur et créez la demande de préauthenticatifion pour le fichier chargé.

Remarque

Assurez-vous que l'URL de demande de préauthenticatifion du fichier *configuration.txt* est utilisée dans le déploiement de la pile.

Étape 5 Créez des fichiers zip.

Un fichier *make.py* se trouve dans le référentiel cloné. Exécutez la commande `python3 make.py build` pour créer les fichiers zip. Le dossier cible contient les fichiers suivants.

```

Tue Jun 08 07:46 AM [sumis@SUMIS-M-41KG target]$ tree -A
.
├── Oracle-Functions.zip
├── asav_autoscale_deploy.zip
├── asav_configuration.txt
├── deploy_oracle_functions_cloudshell.py
├── template1.zip
└── template2.zip

0 directories, 6 files
Tue Jun 08 07:46 AM [sumis@SUMIS-M-41KG target]$

```

Remarque

Si vous déployez la solution d'évolutivité automatique à l'aide de Cloud Shell, mettez à jour le fichier *easy_deploy/deployment_parameters.json* avant d'exécuter la commande `python3 make.py build`. Pour la mise à jour, reportez-vous à [Collecte des paramètres d'entrée](#) et [Déploiement des fonctions Oracle](#).

Déployer la solution d'évolutivité automatique

Après avoir effectué les étapes préalables au déploiement, commencez à créer la pile OCI. Vous pouvez effectuer un [déploiement manuel](#) ou effectuer un [déploiement à l'aide de Cloud Shell](#). Les scripts et les modèles de déploiement pour votre version sont disponibles dans le référentiel [GitHub](#).

Déploiement manuel

Le déploiement de la solution d'évolutivité automatique de bout en bout comprend trois étapes : [déployer la pile Terraform Template-1](#), [déploier les fonctions Oracle](#), puis [déploier Terraform Template-2](#).

Déployer la pile Terraform Template-1

Procédure

- Étape 1** Connectez-vous au portail [OCI](#).
- La région est affichée dans le coin supérieur droit de votre écran. Assurez-vous que vous êtes dans la région prévue.
- Étape 2** Choisissez **Developer Service (Service de développeur)** > **Resource Manager (Gestionnaire de ressources)** > **Stack (Pile)** > **Create Stack (Créer une pile)**.
- Choisissez **My Configuration** (Ma configuration), puis sélectionnez le fichier *Terraform template1.zip* dans le dossier cible en tant que source de configuration Terraform, comme illustré dans la figure ci-dessous.

Stack Configuration ⓘ

Terraform configuration source

Folder .Zip file

📁 Drop a .zip file [Browse](#)

template1.zip ×

Working Directory
The root folder is being used as the working directory.

Name *Optional*

template1-20210420223815

Description *Optional*

Create in compartment

Manual_Test ⌵

ciscosbg (root)/SBG/ASAv-NGFWv/Development/Manual_Test

Terraform version

0.13.x ⌵

ⓘ Support for Terraform version 0.11.x ends in May 2021.

Étape 3 Dans la liste déroulante **Transform version** (Version de Transform), sélectionnez 0.13.x ou 0.14.x.

Étape 4 À l'étape suivante, saisissez tous les détails recueillis dans [Collecte des paramètres d'entrée](#).

Remarque

Saisissez des paramètres d'entrée valides, sans quoi le déploiement de la pile pourrait échouer à d'autres étapes.

Étape 5 À l'étape suivante, choisissez **Terraform Actions (Actions Terraform) > Apply (Appliquer)**.

Une fois le déploiement réussi, procédez au déploiement des fonctions Oracle.

Déployer les fonctions Oracle

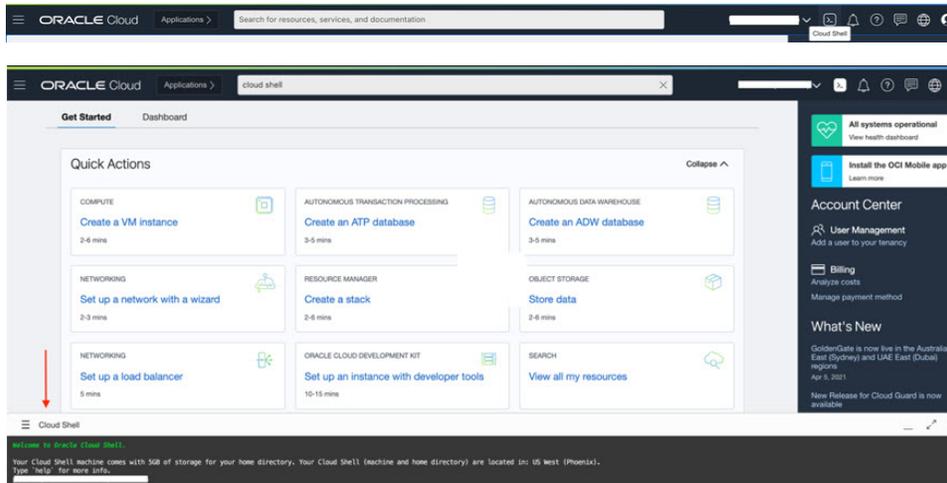


Remarque Cette étape doit être effectuée uniquement après le déploiement réussi de Terraform Template-1.

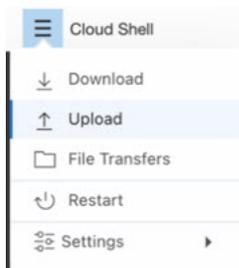
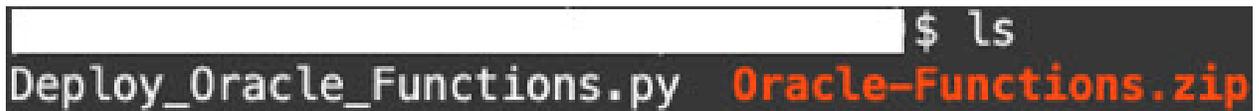
Dans OCI, les fonctions Oracle sont chargées en tant qu'images Docker, qui sont enregistrées dans le registre de conteneur OCI. Les fonctions Oracle doivent être poussées dans l'une des applications OCI (créées dans Terraform Template-1) au moment du déploiement.

Procédure

Étape 1 Ouvrez OCI Cloud Shell.

Étape 2 Chargez `deploy_oracle_functions_cloudshell.py` et `Oracle-Functions.zip`.

Dans le menu contextuel de Cloud Shell, choisissez **Upload** (Charger).

Étape 3 Vérifiez les fichiers à l'aide de la commande `ls`.Étape 4 Exécutez `python3 Deploy_Oracle_Functions.py -h`. Le script `deploy_oracle_functions_cloudshell.py` nécessite certains paramètres d'entrée dont les détails peuvent être trouvés à l'aide de l'argument d'aide, comme illustré dans la figure ci-dessous.

```

$ python3 Deploy_Oracle_Functions.py -h
usage: Deploy_Oracle_Functions.py [-h] -a -r -p -c -o -t

*** Script to deploy Oracle Function for OCI ASAv Autoscale Solution ***

Instruction to find values of required arguments:
Application Name: Name of Application created by first Terraform Template
Region Identifier: OCI -> Administration -> Region Management
Profile Name: OCI -> Profile
Compartment OCID: OCI -> Identity -> Compartment -> Compartment Details
Object Storage Namespace: OCI -> Administration -> Tenancy Details
Authorization Token: OCI -> Identity -> Users -> User Details -> Auth Tokens -> Generate Token

optional arguments:
-h, --help  show this help message and exit
-a          Name of Application in OCI to which functions will be deployed
-r          Region Identifier
-p          Profile Name of User
-c          Compartment OCID
-o          Object Storage Namespace
-t          Authorization Token for Docker Login (*Please Put in Quotes)

```

Pour exécuter le script, transmettez les arguments suivants :

Tableau 1 : Arguments et détails

Argument	Détails
Nom de l'application	Il s'agit du nom de l'application OCI créée par le déploiement de Terraform Template-1. Sa valeur est obtenue en combinant « autoscale_group_prefix » dans le Template-1 et le suffixe « _application ».
Identifiant de région	L'identifiant de région est le mot de code de région fixé dans OCI pour différentes régions. Par exemple : « us-phoenix-1 » pour Phoenix ou « ap-melbourne-1 » pour Melbourne. Pour obtenir la liste de toutes les régions avec leurs identifiants de région, accédez à OCI > Administration > Region Management (Gestion de la région) .
Nom de profil	Il s'agit du nom de profil de l'utilisateur simple dans OCI. Exemple : <i>oracleidentitycloudservice/<user>@<mail>.com</i> Le nom se trouve dans la section du profil de l'utilisateur.
OCID du compartiment	Il s'agit de l'OCID (Oracle Cloud Identifiant) du compartiment. OCID du compartiment où l'utilisateur dispose de l'application OCI. Accédez à OCI > Identity (Identité) > Compartment (Compartiment) > Compartment Details (Détails du compartiment) .
Espace de nom du stockage d'objets	Il s'agit d'un identifiant unique créé au moment de la création de la location. Accédez à OCI > Administration > Tenancy Details (Détails de la location) .

Argument	Détails
Jeton d'autorisation	<p>Il est utilisé comme mot de passe pour la connexion au docker, ce qui l'autorise à pousser les fonctions Oracle dans le registre de conteneur OCI. Précisez le jeton entre guillemets dans le script de déploiement.</p> <p>Accédez à OCI > Identity (Identité) > Users (Utilisateurs) > User Details (Détails de l'utilisateur) > Auth Tokens (Jetons d'autorisation) > Generate Token (Générer un jeton).</p> <p>Si, pour quelque raison que ce soit, vous ne parvenez pas à afficher les détails de l'utilisateur, cliquez sur Developer services (Services de développeur) > Functions (Fonctions). Accédez à l'application créée par Terraform Template-1. Cliquez sur Getting Started (Mise en route) et choisissez Cloud Shell Setup (Configuration de Cloud Shell). Parmi les étapes, vous trouverez le lien pour générer un jeton d'authentification, comme illustré ci-dessous.</p> 

Étape 5 Exécutez la commande `python3 Deploy_Oracle_Functions.py` en transmettant des arguments d'entrée valides. Le déploiement de toutes les fonctions prendra un certain temps. Vous pouvez ensuite supprimer le fichier et fermer Cloud Shell.

Déployer Terraform Template-2

Template 2 déploie les ressources liées à la création d'alarmes, y compris les alarmes et les sujets ONS pour la fonction d'appel. Le déploiement de Template 2 est similaire au déploiement de Terraform Template-1.

Procédure

- Étape 1** Connectez-vous au portail [OCI](#).
- La région est affichée dans le coin supérieur droit de votre écran. Assurez-vous que vous êtes dans la région prévue.
- Étape 2** Choisissez **Developer Service (service de développeur) > Resource Manager (gestionnaire de ressources) > Stack (pile) > Create Stack (créer une pile)**.
- Sélectionnez *Terraform template template2.zip* dans le dossier cible comme source de la configuration de Terraform.
- Étape 3** À l'étape suivante, cliquez sur **Terraform Actions (actions Terraform) > Apply (appliquer)**.

Déployer l'évolutivité automatique à l'aide de Cloud Shell

Pour éviter les frais généraux de déploiement, vous pouvez invoquer le script de déploiement de bout en bout facile pour déployer la solution d'évolutivité automatique (fonctions Terraform `template1`, `template2` et `oracle`).

Procédure

Étape 1 Chargez le fichier `asav_autoscale_deploy.zip` dans le dossier cible de l'interface Cloud Shell et extrayez les fichiers.

```
Cloud Shell

sumis@cloudshell:~ (us-phoenix-1)$ ls -ltrh
total 52K
-rw-r--r--. 1 sumis oci 51K Jun  8 02:43 asav_autoscale_deploy.zip
sumis@cloudshell:~ (us-phoenix-1)$ unzip asav_autoscale_deploy.zip
Archive:  asav_autoscale_deploy.zip
  extracting: template1.zip
  extracting: template2.zip
  extracting: Oracle-Functions.zip
  inflating: oci_asav_autoscale_deployment.py
  inflating: oci_asav_autoscale_tearardown.py
  inflating: deployment_parameters.json
  inflating: tearardown_parameters.json
sumis@cloudshell:~ (us-phoenix-1)$ ls -ltrh
total 140K
-rw-r--r--. 1 sumis oci 2.5K Jun  8 02:16 template2.zip
-rw-r--r--. 1 sumis oci 4.6K Jun  8 02:16 template1.zip
-rw-r--r--. 1 sumis oci  70 Jun  8 02:16 tearardown_parameters.json
-rw-r--r--. 1 sumis oci 35K Jun  8 02:16 Oracle-Functions.zip
-rw-r--r--. 1 sumis oci 7.1K Jun  8 02:16 oci_asav_autoscale_tearardown.py
-rw-r--r--. 1 sumis oci 22K Jun  8 02:16 oci_asav_autoscale_deployment.py
-rw-r--r--. 1 sumis oci 1.9K Jun  8 02:16 deployment_parameters.json
-rw-r--r--. 1 sumis oci 51K Jun  8 02:43 asav_autoscale_deploy.zip
sumis@cloudshell:~ (us-phoenix-1)$
```

Étape 2 Assurez-vous d'avoir mis à jour les paramètres d'entrée dans le `deployment_parameters.json` avant d'exécuter la commande `python3 make.py`.

Étape 3 Pour commencer à déployer la solution d'évolutivité automatique, exécutez la commande `python3 oci_asav_autoscale_deployment.py` sur l'interface Cloud Shell.

Le déploiement de la solution prendra environ 10 à 15 minutes.

Si une erreur survient pendant le déploiement de la solution, le journal des erreurs est enregistré.

Valider le déploiement

Validez si toutes les ressources sont déployées et que les fonctions Oracle sont connectées avec des alarmes et des événements. Par défaut, le regroupement d'instances a un nombre minimal et maximal d'instances à zéro. Vous pouvez modifier le regroupement d'instances dans l'interface utilisateur d'OCI avec le nombre minimal et maximal que vous souhaitez. Cela déclenchera de nouvelles instances ASA virtuel.

Nous vous recommandons de lancer une seule instance, de vérifier son flux de travail et de valider son comportement pour vous assurer qu'elle fonctionne comme prévu. Après cette validation, vous pouvez déployer les exigences réelles de ASA virtuel.



Remarque Précisez le nombre minimal d'instances ASA virtuel comme **protégé contre une évolutivité à la baisse** pour éviter qu'elles soient supprimées par les politiques d'évolutivité d'OCI.

Mise à niveau

Mettre à niveau la pile d'évolutivité automatique

Aucune prise en charge de la mise à niveau dans cette version. Les piles doivent être redéployées.

Mettre à niveau les machines virtuelles ASA virtuel

Aucune prise en charge de la mise à niveau des machines virtuelles ASA virtuel dans cette version. La pile doit être redéployée avec l'image ASA virtuel requise.

Réserve d'instances

1. Pour modifier le nombre minimum et maximum d'instances dans le groupe d'instances :

Cliquez sur **Developer Services (Services de développeurs) > Fonction (Fonction) > Application Name (Nom de l'application) (créé par Terraform Template 1) > Configuration**.

Modifiez respectivement `min_instance_count` et `max_instance_count`.

2. La suppression/résiliation de l'instance n'est pas l'équivalent d'une évolutivité à la baisse. Si une instance de la réserve d'instances est supprimée/résiliée en raison d'une action externe et non d'une action d'évolutivité à la baisse, la réserve d'instances lance automatiquement une nouvelle instance à récupérer.
3. `Max_instance_count` définit la limite de seuil pour l'action d'évolutivité à la hausse, mais elle peut être dépassée en modifiant le nombre d'instances de la réserve d'instances à l'aide de l'interface utilisateur. Assurez-vous que le nombre d'instances de l'interface utilisateur est inférieur au `max_instance_count` défini dans l'application OCI. Sinon, augmentez le seuil en conséquence.
4. La réduction du nombre d'instances dans la réserve d'instances directement à partir de l'application n'effectue pas les actions de nettoyage définies par programmation. En raison de quoi les systèmes dorsaux ne seront pas purgés et supprimés des deux équilibrateurs de charges, si ASA virtuel a une licence, elle sera perdue.
5. Pour certaines raisons, si l'instance ASA virtuel n'est pas intègre, ne répond pas et est inaccessible par SSH pendant une période définie, l'instance est supprimée de la réserve d'instances avec force, et des licences peuvent être perdues.

Fonctions Oracle

- Les fonctions Oracle sont en fait des images de Docker. Ces images sont enregistrées dans le répertoire racine du registre de conteneur OCI. Ces images ne doivent pas être supprimées, car cela supprimera également la fonction utilisée dans la solution d'évolutivité automatique.
- L'application OCI créée par Terraform template-1 contient des variables environnementales essentielles, qui sont requises par les fonctions Oracle pour fonctionner correctement. Ni la valeur ni le format de ces

variables d'environnement ne doivent être modifiés, sauf si cela est obligatoire. Toutes les modifications apportées sont reflétées dans les nouvelles instances uniquement.

Ensembles de systèmes principaux de l'équilibreur de charge

Dans OCI, la connexion de l'équilibreur de charges au groupe d'instances n'est prise en charge que par l'utilisation de l'interface principale configurée comme interface de gestion dans ASA virtuel. Par conséquent, l'interface interne est connectée à l'ensemble principal de l'équilibreur de charges interne; l'interface externe est connectée à l'ensemble principal de l'équilibreur de charges externe. Ces adresses IP ne sont pas automatiquement ajoutées ou supprimées de l'ensemble principal. La solution d'évolutivité automatique gère ces deux tâches de manière programmatique. Mais dans le cas d'une action, d'une maintenance ou d'un dépannage externe, il pourrait y avoir une situation nécessitant un effort manuel pour les utiliser.

Selon les besoins, d'autres ports peuvent être ouverts sur l'équilibreur de charges à l'aide d'un écouteur et d'ensembles principaux. Les adresses IP des instances à venir sont automatiquement ajoutées à l'ensemble principal, mais les adresses IP des instances existantes doivent être ajoutées manuellement.

Ajout d'un écouteur dans l'équilibreur de charges

Pour ajouter un port en tant qu'écouteur dans l'équilibreur de charges, accédez à **OCI > Networking (réseautage) > Load Balancer (équilibreur de charges) > Listener (écouteur) > Create Listener (créer un écouteur)**.

Enregistrer un système principal dans l'ensemble principal

Afin d'enregistrer une instance ASA virtuel sur l'équilibreur de charges, l'adresse IP de l'interface externe de l'instance ASA virtuel doit être configurée en tant que système principal dans l'ensemble principal de l'équilibreur de charges externe. L'adresse IP de l'interface interne doit être configurée comme système principal dans l'ensemble principal de l'équilibreur de charges interne. Assurez-vous que le port que vous utilisez a été ajouté dans l'écouteur.

Supprimer la configuration d'évolutivité automatique d'OCI

Les piles déployées à l'aide de Terraform peuvent être supprimées de la même manière, à l'aide du gestionnaire de ressources dans OCI. La suppression de la pile supprime toutes les ressources créées par celle-ci et tous les renseignements associés à ces ressources sont supprimés définitivement.



Remarque

En cas de suppression de pile, il est recommandé de faire en sorte que le nombre minimal d'instances dans le groupe d'instances soit de 0 et d'attendre la fin des instances. Cela facilitera la suppression de toutes les instances et ne laissera aucune trace.

Vous pouvez effectuer une [suppression manuelle](#) ou utiliser [Cloud Shell](#).

Suppression manuelle

La suppression de la solution d'évolutivité automatique de bout en bout se déroule en trois étapes : [supprimer la pile Terraform Template-2](#), [supprimer les fonctions Oracle](#), puis [supprimer la pile Terraform Template-1](#).

Supprimer la pile Terraform Template-2

Pour supprimer la configuration de l'évolutivité automatique, vous devez commencer par supprimer la pile Terraform Template-2.

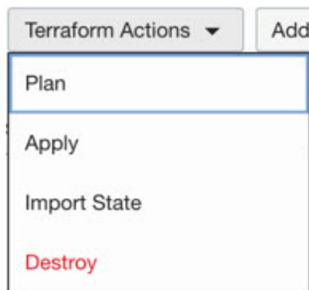
Procédure

Étape 1 Connectez-vous au portail [OCI](#).

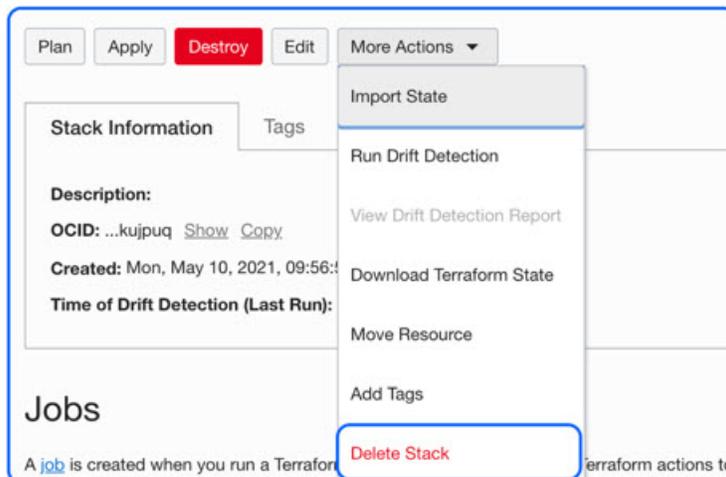
La région est affichée dans le coin supérieur droit de votre écran. Assurez-vous que vous êtes dans la région prévue.

Étape 2 Choisissez **Developer Services (Services de développeur)** > **Resource Manager (Gestionnaire de ressources)** > **Stack (Pile)**.

Étape 3 Sélectionnez la pile créée par Terraform Template-2, puis sélectionnez **Destroy** (Détruire) dans le menu déroulant **Terraform Actions** (Actions Terraform) comme illustré dans la figure ci-dessous :



La tâche de destruction est créée, ce qui prend un certain temps pour supprimer des ressources les unes après les autres. Vous pouvez supprimer la pile une fois la tâche de destruction terminée, comme illustré dans la figure ci-dessous :



Étape 4 Procédez à la suppression des fonctions Oracle.

Supprimer les fonctions Oracle

Le déploiement des fonctions Oracle ne fait pas partie du déploiement de la pile Terraform Template, il est chargé séparément à l'aide de Cloud Shell. Par conséquent, sa suppression n'est pas non plus prise en charge par la suppression de la pile Terraform. Vous devez supprimer toutes les fonctions Oracle dans l'application OCI créée par Terraform Template-1.

Procédure

-
- Étape 1** Connectez-vous au portail [OCI](#).
La région est affichée dans le coin supérieur droit de votre écran. Assurez-vous que vous êtes dans la région prévue.
- Étape 2** Choisissez **Developer Services (Services de développeur) > Fonctions (Fonctions)**. Choisissez le nom de l'application qui a été créée dans la pile Template-1.
- Étape 3** Dans cette application, visitez chaque fonction et supprimez-le.
-

Supprimer la pile Terraform Template-1

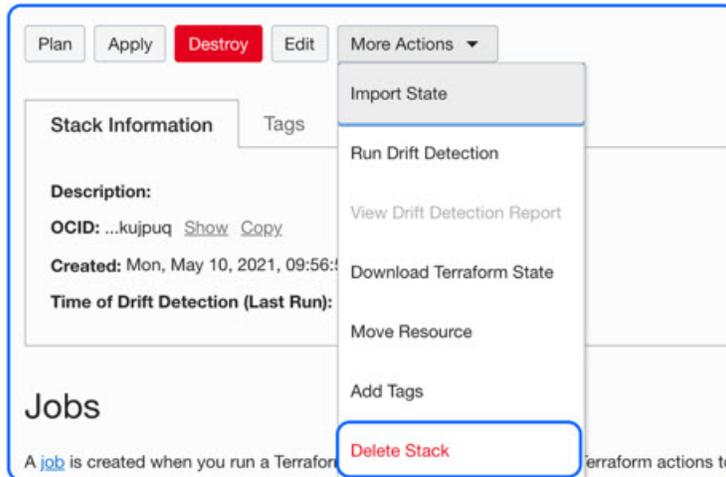


Remarque La suppression de la pile Template-1 de la pile ne réussira qu'après avoir supprimé toutes les fonctions Oracle.

Identique à la suppression de Terraform Template-2.

Procédure

-
- Étape 1** Connectez-vous au portail [OCI](#).
La région est affichée dans le coin supérieur droit de votre écran. Assurez-vous que vous êtes dans la région prévue.
- Étape 2** Choisissez **Developer Services (Services de développeur) > Resource Manager (Gestionnaire de ressources) > Stack (Pile)**.
- Étape 3** Sélectionnez la pile créée par Terraform Template-2, puis cliquez sur **Destroy (Détruire)** dans le menu déroulant **Terraform Actions (Actions Terraform)**. La tâche de destruction sera créée, ce qui prendra un certain temps pour supprimer les ressources les unes après les autres.
- Étape 4** Une fois la tâche de destruction terminée, vous pouvez supprimer la pile du menu déroulant **More Actions (Plus d'actions)**, comme illustré dans la figure ci-dessous.



Après la suppression réussie de la pile Terraform Template-1, vous devez vérifier si toutes les ressources sont supprimées et qu'il n'y a aucun reste.

Supprimer l'évolutivité automatique à l'aide de Cloud Shell

L'utilisateur peut utiliser le script pour supprimer les piles et les fonctions Oracle en exécutant la commande `python3 oci_asav_autoscale_takedown.py` dans l'interface Cloud Shell. Si les piles sont déployées manuellement, mettez à jour l'identifiant de pile de `stack1` et `stack2`, ainsi que l'identifiant de l'application dans le fichier `takedown_parameters.json`.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.