Déployer Défense contre les menaces virtuelles sur OCI

Vous pouvez déployer le défense contre les menaces virtuelles sur Oracle Cloud Infrastructure (OCI), un service informatique en nuage public qui vous permet d'exécuter vos applications dans un environnement hébergé hautement disponible offert par Oracle.

Les procédures suivantes décrivent comment préparer votre environnement OCI et lancer l'instance défense contre les menaces virtuelles. Vous vous connectez au portail OCI, recherchez dans le Marché OCI l'offre de pare-feu virtuel NGFW de Cisco Firepower (NGFWv) et lancez l'instance informatique. Après avoir lancé défense contre les menaces virtuelles, vous devez configurer les tables de routage pour diriger le trafic vers le pare-feu en fonction de la source et de la destination du trafic.

- Aperçu, à la page 2
- Procédure de bout en bout, à la page 2
- Prérequis, à la page 4
- Lignes directrices et limites relatives à la licence, à la page 4
- Exemple de topologie de réseau, à la page 6
- Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual, à la page 7
- Configurer l'environnement OCI, à la page 8
- Déployer Threat Defense Virtual sur OCI, à la page 11
- Associer les interfaces, à la page 13
- Ajouter des règles de routage pour les VNIC associées, à la page 13
- Déployer la solution d'évolutivité automatique, à la page 14
- Conditions préalables, à la page 15
- Chiffrer le mot de passe, à la page 23
- Préparation du fichier de configuration défense contre les menaces virtuelles, à la page 24
- Déployer la solution d'évolutivité automatique, à la page 30
- Valider le déploiement, à la page 35
- Mise à niveau, à la page 36
- Ensembles de systèmes principaux de l'équilibreur de charge, à la page 37
- Supprimer la configuration d'évolutivité automatique d'OCI, à la page 37
- Se connecter à l'instance Défense contre les menaces virtuelles à l'aide de SSH, à la page 40
- Se connecter à l'instance Défense contre les menaces virtuelles à l'aide d'OpenSSH, à la page 41
- Se connecter à l'instance Défense contre les menaces virtuelles à l'aide de PuTTY, à la page 42

Aperçu

Le Cisco Cisco Secure Firewall Threat Defense Virtual exécute le même logiciel que le Cisco Défense contre les menaces physique afin d'offrir des fonctionnalités de sécurité éprouvées dans un format virtuel. défense contre les menaces virtuelles peut être déployé dans l'OCI public. Il peut ensuite être configuré pour protéger les charges de travail des centres de données virtuels et physiques qui se développent, se contractent ou changent d'emplacement au fil du temps.

Formats de traitement OCI

Une forme est un modèle qui détermine le nombre de CPU, la quantité de mémoire et d'autres ressources qui sont allouées à une instance. Les défense contre les menaces virtuelles prennent en charge les types de formes OCI suivantes :

Tableau 1 : Calculer les formes prises en charge pour Défense contre les menaces virtuelles

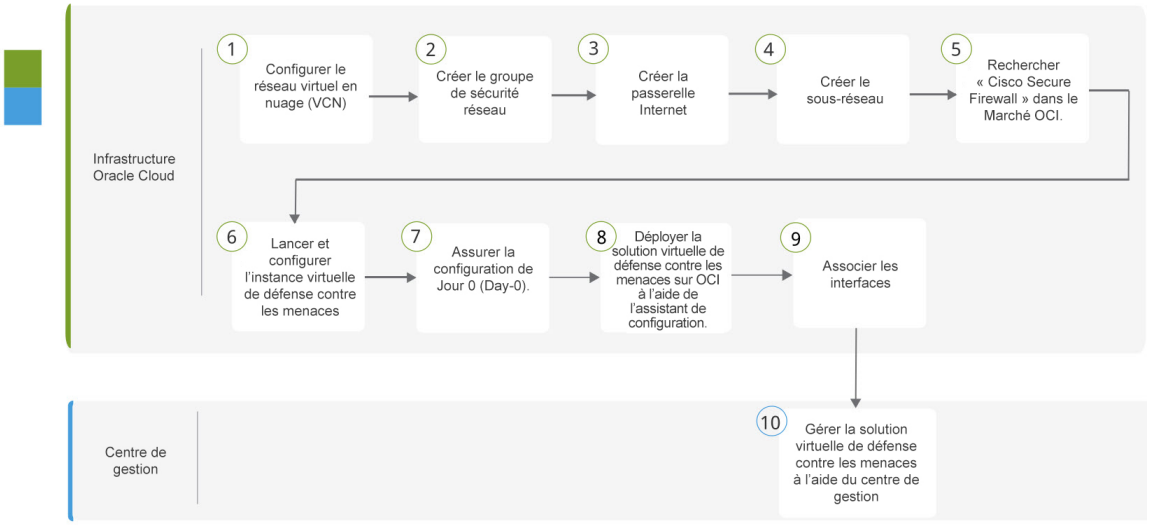
Forme OCI	Version de Threat Defense Virtual prise en charge	Attributs		Interfaces
		oCPU	RAM (Go)	
Intel VM.Standard 2.4	7.1, 7.2.x et 7.3.x	4	60	Minimum 4, Maximum 4
Intel VM.Standard2.8	7.1, 7.2.x et 7.3.x	8	120	Minimum 4, Maximum 8

- * Le mode SR-IOV est pris en charge avec les configurations Flex à partir de la version 7.4.x.
- Dans OCI, 1 oCPU équivaut à 2 vCPU.
- Le défense contre les menaces virtuelles nécessite un minimum de 4 interfaces.

Vous créez un compte sur OCI, lancez une instance de calcul à l'aide de l'offre de pare-feu virtuel Cisco Firepower NGFW (NGFWv) sur la place de marché en nuage d'Oracle et choisissez une forme OCI.

Procédure de bout en bout

Le diagramme suivant illustre le flux de travail pour le déploiement de Threat Defense Virtual sur Oracle Cloud Infrastructure.



	Espace de travail	Étapes
1	Infrastructure Oracle Cloud	Déployez la défense contre les menaces virtuelle sur OCI : Configurez le réseau en nuage virtuel (VCN) (**Networking** > **Virtual Cloud Networks** > **CIDR Block** > **Create VCN**).
2	Infrastructure Oracle Cloud	Déployer la solution virtuelle de défense contre les menaces sur OCI : Créez le groupe de sécurité réseau. (**Networking (mise en réseau)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > **Virtual Cloud Network Details (détails du réseau virtuel en nuage)** > **Network Security Groups (groupes de sécurité réseau)** et cliquez sur **Create Network Security Group** (créer un groupe de sécurité réseau).
3	Infrastructure Oracle Cloud	Déployer la solution virtuelle de défense contre les menaces sur OCI : Créez le groupe de sécurité réseau. **Networking (réseautage)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > **Virtual Cloud Network Details (détails de réseau virtuel en nuage)** > **Internet Gateways (passerelles Internet)** > **Create Internet Gateway (créer une passerelle Internet)**.
4	Infrastructure Oracle Cloud	Déployer la solution virtuelle de défense contre les menaces sur OCI : Créez le sous-réseau. **Networking (réseautage)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > **Virtual Cloud Network Details (détails du réseau virtuel en nuage)** > **Subnets (sous-réseaux)** > **Create Subnet (créer un sous-réseau)**.
5	Infrastructure Oracle Cloud	Déployer Threat Defense Virtual sur OCI, à la page 11 : Recherchez « Cisco Secure Firewall » dans le Marché OCI.
6	Infrastructure Oracle Cloud	Déployer Threat Defense Virtual sur OCI, à la page 11 : Lancez et configurez l'instance virtuelle de défense contre les menaces.
7	Infrastructure Oracle Cloud	Déployer Threat Defense Virtual sur OCI, à la page 11 : Assurez la configuration de Jour 0 (Day-0).

	Espace de travail	Étapes
8	Infrastructure Oracle Cloud	Déployer Threat Defense Virtual sur OCI, à la page 11 : Déployez la solution virtuelle de défense contre les menaces sur OCI à l'aide de l'assistant de configuration.
9	Infrastructure Oracle Cloud	Déployer la solution virtuelle de défense contre les menaces sur OCI : associez les interfaces.**Compute (traitement informatique)** > **Instances** > **Instance Details (renseignements)** > **Attached VNICs (VNICs associés)**
10	Centre de gestion	Gérez défense contre les menaces virtuelles à l'aide du centre de gestion

Prérequis

- Créez un compte OCI à https://www.oracle.com/cloud/.
- Un compte Cisco Smart. Vous pouvez en créer un sur le Centre des logiciels Cisco (https://software.cisco.com/).
- Obtenez une licence pour défense contre les menaces virtuelles.
  - Configurez tous les droits de licence pour les services de sécurité à partir de la centre de gestion.
  - Consultez la section « Licences » dans le *Guide d'administration de Cisco Secure Firewall Management Center* pour en savoir plus sur la gestion des licences.
- Exigences d'interface :
  - Interfaces de gestion (2) : une utilisée pour connecter défense contre les menaces virtuelles avec centre de gestion, la seconde utilisée pour les diagnostics; ne peut pas être utilisé pour le trafic de transit.
  - Interfaces de trafic (2) : utilisées pour connecter défense contre les menaces virtuelles aux hôtes internes et au réseau public.
- Chemins de communication :
  - Adresses IP publiques pour l'accès à défense contre les menaces virtuelles.
- Pour les configurations système de défense contre les menaces virtuelles, consultez le Guide de compatibilité de Cisco Secure Firewall Threat Defense.

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

- Déploiement dans le réseau virtuel en nuage (VCN) OCI
- Mode avec routage (par défaut)

- Licences : Seul le protocole BYOL est pris en charge
- Centre de gestion uniquement.
- Prise en charge de la virtualisation des E/S à racine unique (SR-IOV).

Niveaux de performance pour les licences Smart de FTDv

Le défense contre les menaces virtuelles prend en charge les licences par niveau de performance qui fournissent différents niveaux de débit et limites de connexion VPN en fonction des exigences de déploiement.

Tableau 2 : Défense contre les menaces virtuelles Limites des fonctionnalités sous licence en fonction des droits

Niveau de performance	Caractéristiques du périphérique (cœur/RAM)	Limite du débit	Limite de session RA VPN
FTDv5, 100 Mbit/s	4 cœurs/8 Go	100 Mbit/s	50
FTDv10, 1 Gbit/s	4 cœurs/8 Go	1 Gbit/s	250
FTDv20, 3 Gbit/s	4 cœurs/8 Go	3 Gbit/s	250
FTDv30, 5 Gbit/s	8 cœurs/16 Go	5 Gbit/s	250
FTDv50, 10 Gbit/s	12 cœurs/24 Go	10 Gbit/s	750
FTDv100, 16 Gbit/s	16 cœurs/32 Go	16 Gbit/s	10 000

Consultez le chapitre sur les licences du *Guide d'administration de Cisco Secure Firewall Management Center* pour connaître les consignes relatives à l'octroi de licences pour votre périphérique défense contre les menaces virtuelles.

Remarque Pour modifier les valeurs de vCPU/mémoire, vous devez d'abord éteindre le périphérique défense contre les menaces virtuelles.

Optimisation des performances

Pour obtenir les meilleures performances avec défense contre les menaces virtuelles, vous pouvez apporter des ajustements à la machine virtuelle et à l'hôte. Consultez la section sur le réglage et l'optimisation de la virtualisation sur OCI pour en savoir plus.

Receive Side Scaling (dimensionnement côté réception) : le défense contre les menaces virtuelles prend en charge Receive Côté Scaling (RSS), qui est une technologie utilisée par les adaptateurs réseau pour distribuer le trafic de réception réseau entre plusieurs cœurs de processeur. Pris en charge par les versions 7.0 et ultérieures. Consultez la section sur les files d'attente RX multiples pour le dimensionnement de la réception (RSS) pour en savoir plus.

Snort

- Si vous observez un comportement anormal comme un délai d'arrêt du Snort long, un ralentissement de la machine virtuelle en général ou l'exécution d'un processus spécifique, collectez les journaux de défense

contre les menaces virtuelles et de l'hôte VM. La collecte de l'utilisation globale du processeur, de la mémoire, de l'utilisation des E/S et de la vitesse de lecture/écriture vous aidera à résoudre les problèmes.

- Une utilisation élevée de la CPU et des E/S est observée lors de l'arrêt Snort. Si un certain nombre d'instances défense contre les menaces virtuelles ont été créées sur un seul hôte avec une mémoire insuffisante et aucun processeur dédié, Snort mettra beaucoup de temps à s'arrêter, ce qui entraînera la création de cœurs Snort.

Fonctionnalités non prises en charge

- Prise en charge de la gestion locale par l'intermédiaire de gestionnaire d'appareil.
- Haute accessibilité en natif Défense contre les menaces virtuelles
- Évolutivité automatique de la version 7.0 et les versions antérieures.
- Modes transparent/en ligne/passif
- Configuration de l'interface de données par DHCP
- IPv6

Limites

- Le déploiement de Défense contre les menaces virtuelles sur OCI ne prend pas en charge Mellanox 5 tant que vNIC en mode SR-IOV.
- Règles de routage distinctes requises pour Firewall Threat Defense Virtual pour la configuration statique et DHCP.

Exemple de topologie de réseau

La figure suivante montre la topologie recommandée pour défense contre les menaces virtuelles en mode pare-feu avec routage et avec quatre sous-réseaux configurés dans OCI pour défense contre les menaces virtuelles (gestion, diagnostic, interne et externe).

Illustration 1 : Modèle de Défense contre les menaces virtuelles sur le déploiement OCI avec des sous-réseaux dans quatre VCN

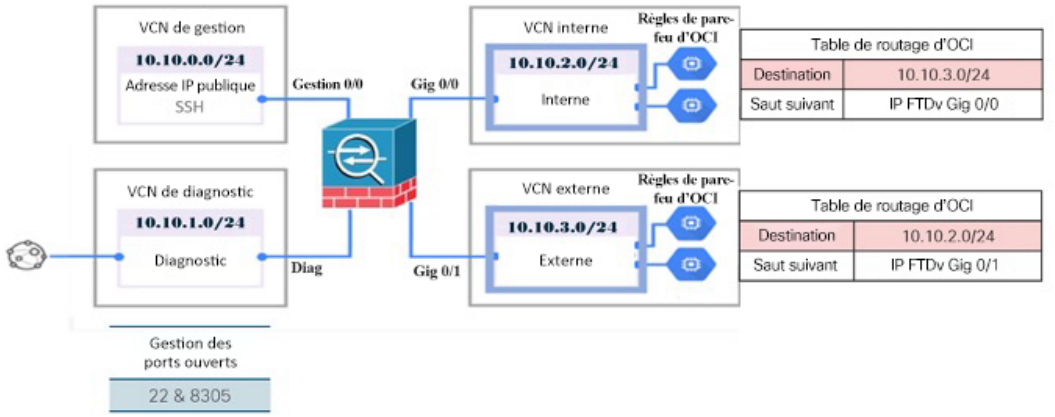
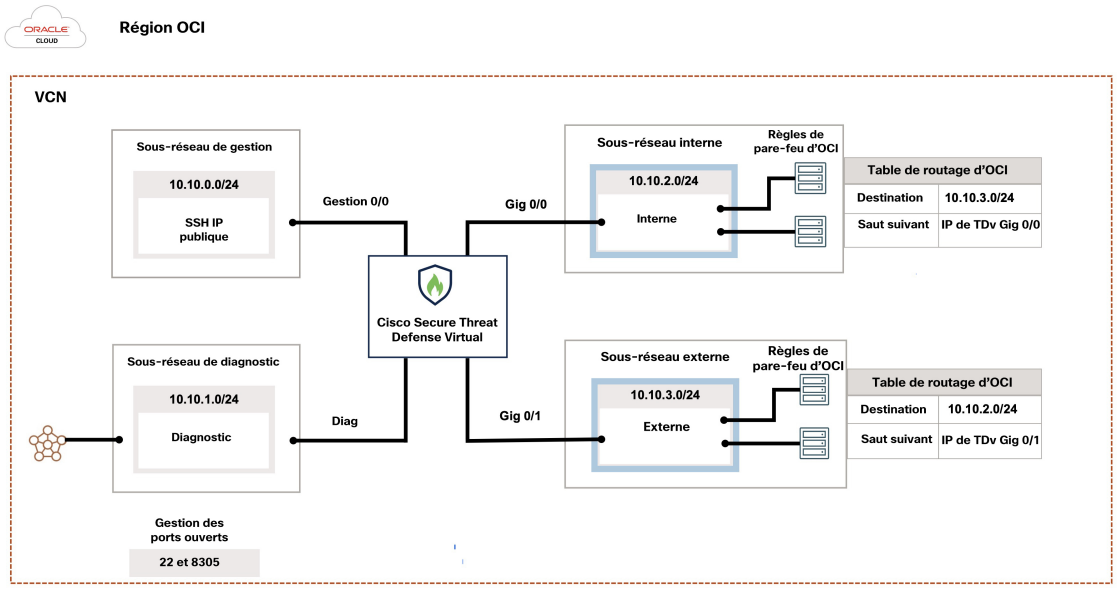


Illustration 2 : Modèle de Défense contre les menaces virtuelles sur le déploiement OCI avec quatre sous-réseaux dans un VCN



Remarque Lorsque vous utilisez quatre sous-réseaux dans un seul VCN, les chemins de routage spécifiques à un sous-réseau doivent être ajoutés au tableau de routage associé au sous-réseau.

Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual

Vous avez deux options pour gérer votre Cisco Secure Firewall Threat Defense Virtual.

Cisco Secure Firewall Management Center

Si vous gérez un grand nombre d'appareils, ou si vous voulez utiliser les fonctions et configurations plus complexes que permet défense contre les menaces, utilisez centre de gestion pour configurer vos appareils au lieu du gestionnaire d'appareil intégré.

Important Vous ne pouvez pas utiliser à la fois gestionnaire d'appareil et centre de gestion pour gérer l'appareil défense contre les menaces. Une fois que la gestion intégrée gestionnaire d'appareil est activée, il ne sera plus possible d'utiliser centre de gestion pour gérer le périphérique défense contre les menaces, à moins de désactiver la gestion locale et de reconfigurer la gestion pour utiliser centre de gestion. D'un autre côté, lorsque vous enregistrez le périphérique défense contre les menaces sur centre de gestion, le service de gestion intégrée gestionnaire d'appareil est désactivé.

Mise en garde Actuellement, Cisco n'offre pas la possibilité de migrer votre configuration gestionnaire d'appareil vers centre de gestion et vice versa. Tenez-en compte lorsque vous choisissez le type de gestion que vous configurez pour le périphérique défense contre les menaces.

Cisco Secure Firewall device manager

Le gestionnaire d'appareil est un gestionnaire intégré.

Le gestionnaire d'appareil est une interface de configuration Web incluse sur certains des périphériques défense contre les menaces. gestionnaire d'appareil vous permet de configurer les fonctions de base du logiciel qui sont le plus souvent utilisées pour les petits réseaux. Il est spécialement conçu pour les réseaux qui comprennent un seul périphérique ou quelques-uns, pour lesquels vous ne souhaitez pas utiliser un gestionnaire de périphériques multiples de grande puissance qui permet de contrôler un grand réseau contenant un grand nombre des périphériques défense contre les menaces.

Remarque Consultez Guide Cisco Secure Firewall Device Manager Configuration pour obtenir la liste des périphériques défense contre les menaces qui prennent en charge gestionnaire d'appareil.

Configurer l'environnement OCI

Vous pouvez configurer le réseau en nuage virtuel (VCN) pour votre déploiement de solution virtuelle de défense contre les menaces comme suit :

- **Plusieurs VCN** : au minimum, vous avez besoin de quatre VCN, un pour chaque interface de défense contre les menaces virtuelles. Cela permet une inspection du trafic isolé entre différents réseaux.
- **VCN unique avec sous-réseaux** : vous pouvez également configurer un VCN unique avec quatre sous-réseaux, un pour chaque interface virtuelle de défense contre les menaces. Dans cette configuration, le trafic entre les sous-réseaux du même réseau local virtuel peut être inspecté et contrôlé par le pare-feu à l'aide des tables de routage associées. Cela vous permet de gérer efficacement le trafic inter-sous-réseaux tout en utilisant un seul VCN.

Vous pouvez poursuivre les procédures suivantes pour terminer le VCN de gestion. Ensuite, revenez à **Networking** (mise en réseau) pour créer des VCN pour les interfaces de diagnostic, interne et externe.

Procédure

Étape 1 Connectez-vous à OCI et choisissez votre région.

OCI est divisé en plusieurs régions isolées les unes des autres. La région est affichée dans le coin supérieur droit de votre écran. Les ressources d'une région n'apparaissent pas dans une autre région. Vérifiez périodiquement que vous êtes dans la région prévue.

Étape 2 Sélectionnez **Networking (mise en réseau)** > **Virtual Cloud Networks (réseaux de nuage virtuel)** et cliquez sur **Create VCN** (créer des réseaux de nuage virtuel).

Étape 3 Saisissez un **Name** (Nom) descriptif pour votre réseau VCN, par exemple *FTDv-Management*.

Étape 4 Saisissez un **CIDR block** (bloc CIDR) pour votre VCN.

a) Un bloc CIDR IPv4 d'adresses IP. La notation CIDR (Classless Inter-Domain Routing) est une représentation compact d'une adresse IP et de son préfixe de routage associé. Par exemple, 10.0.0.0/24.

Remarque
Utiliser les noms de domaine DNS dans ce VCN.

Étape 5 Cliquez sur **Create VCN** (créer un VCN).

Prochaine étape

Poursuivez en suivant les procédures suivantes pour terminer le VCN de gestion. Lorsque vous terminerez le VCN de gestion, vous créerez des VCN pour les interfaces de diagnostic, interne et externe.

Remarque Après avoir sélectionné un service dans le menu de navigation, le menu de gauche comprend la liste des compartiments. Les compartiments vous aident à organiser des ressources pour faciliter le contrôle d'accès. Votre compartiment racine est créé pour vous par Oracle lorsque votre location est provisionnée. Un administrateur peut créer d'autres compartiments dans le compartiment racine, puis ajouter les règles d'accès pour contrôler quels utilisateurs peuvent voir et agir en leur nom. Consultez le document Oracle sur la gestion des compartiments pour en savoir plus.

Créer le groupe de sécurité réseau

Un groupe de sécurité réseau se compose d'un ensemble de vNIC et d'un ensemble de règles de sécurité qui s'appliquent à ces vNIC.

Procédure

Étape 1 Sélectionnez **Networking (mise en réseau)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > **Virtual Cloud Network Details (détails du réseau virtuel en nuage)** > **Network Security Groups (groupes de sécurité réseau)** et cliquez sur **Create Network Security Group** (créer un groupe de sécurité réseau).

Étape 2 Saisissez un **nom** de description pour votre groupe de sécurité réseau, par exemple, *FTDv-Mgmt-Allow-22-8305*.

Étape 3 Cliquez sur **Next** (suivant).

Étape 4 Ajoutez vos règles de sécurité :

a) Ajoutez une règle pour autoriser le port TCP 22 pour l'accès SSH.

b) Ajoutez une règle pour autoriser le port TCP 8305 pour l'accès HTTPS.

L'défense contre les menaces virtuelles peut être géré par centre de gestion, ce qui nécessite l'ouverture du port 8305 pour les connexions HTTPS.

Remarque
Vous appliquez ces règles de sécurité à l'interface de gestion/au VCN.

Étape 5 Cliquez sur **Create** (créer).

Créer la passerelle Internet

Une passerelle Internet est requise pour rendre votre sous-réseau de gestion accessible au public.

Procédure

Étape 1 Sélectionnez **Networking (réseautage)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > **Virtual Cloud Network Details (détails de réseau virtuel en nuage)** > **Internet Gateways (passerelles Internet)** et cliquez sur **Create Internet Gateway (créer une passerelle Internet)**.

Étape 2 Saisissez un **nom** descriptif pour votre passerelle Internet, par exemple, *FTDv-IG*.

Étape 3 Cliquez sur **Create Internet Gateway** (créer une passerelle Internet).

Étape 4 Ajouter le routeur à la passerelle Internet :

a) Choisissez **Networking (réseautage)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > **Virtual Cloud Network Details (détails du réseau virtuel en nuage)** > **Route Tables (tableaux de routage)**.
b) Cliquez sur le lien de votre tableau de routage par défaut pour ajouter des règles de routage.
c) Cliquez sur **Add Route Rules** (ajouter des règles de routage).
d) Dans la liste déroulante **Target Type** (type de cible), sélectionnez **Internet Gateway** (passerelle Internet).
e) Saisissez le bloc CIDR de l'IPv4 de destination, par exemple 0.0.0.0/0.
f) Dans la liste déroulante **Target Internet Gateway** (passerelle Internet cible), sélectionnez la passerelle que vous avez créée.
g) Cliquez sur **Add Route Rules** (ajouter des règles de routage).

Créer le sous-réseau

Chaque VCN aura au moins un sous-réseau. Vous créerez un sous-réseau de gestion pour le VCN de gestion. Vous aurez également besoin d'un sous-réseau de diagnostic pour le VCN de diagnostic, d'un sous-réseau interne pour le VCN interne et d'un sous-réseau externe pour le VCN externe.

Si vous utilisez un VCN, vous créerez un sous-réseau de gestion, un sous-réseau de diagnostic, un sous-réseau interne et un sous-réseau externe dans le VCN.

Procédure

Étape 1 Sélectionnez **Networking (réseautage)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > **Virtual Cloud Network Details (détails du réseau virtuel en nuage)** > **Subnets (sous-réseaux)**) et cliquez sur **Create Subnet (créer un sous-réseau)**.

Étape 2 Saisissez un **nom** descriptif pour votre sous-réseau, par exemple, *Gestion*.

Étape 3 Sélectionnez un **type de sous-réseau** (conservez la valeur par défaut recommandée de **Regional** [régional]).

Étape 4 Saisissez un **CIDR Block** (bloc CIDR), par exemple 10.10.0.0/24. L'adresse IP interne (non publique) du sous-réseau est extraite de ce bloc CIDR.

Étape 5 Sélectionnez l'un des tableaux de routage que vous avez créés précédemment dans la liste déroulante **Route Table** (tableau de routage).

Étape 6 Sélectionnez **Subnet Access** (accès au sous-réseau) pour votre sous-réseau.

Pour le sous-réseau de gestion, il doit s'agir de **Public Subnet** (sous-réseau public).

Étape 7 Sélectionnez **DHCP Option** (option DHCP).

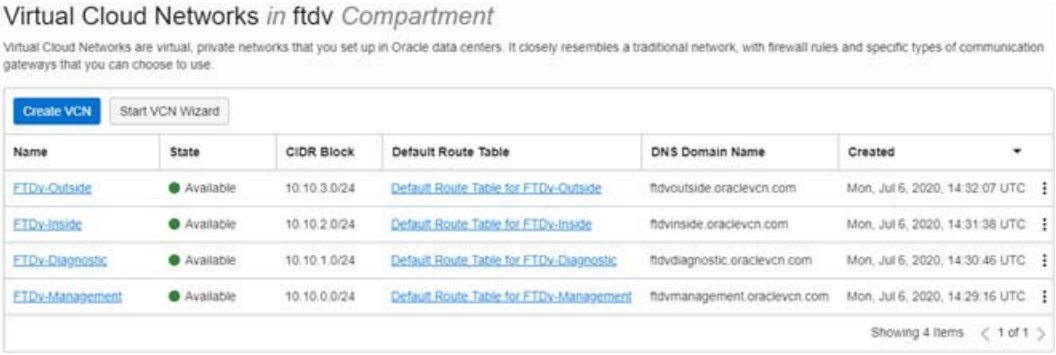
Étape 8 Sélectionnez une **Security List** (liste de sécurité) que vous avez créée précédemment.

Étape 9 Cliquez sur **Create Subnet** (créer un sous-réseau).

Prochaine étape

Après avoir configuré vos VCN (Gestion, Diagnostic, Interne, Externe), vous pouvez lancer défense contre les menaces virtuelles. Consultez le schéma suivant pour un exemple de configuration VCN défense contre les menaces virtuelles.

Illustration 3 : défense contre les menaces virtuelles Réseaux virtuels en nuage



Déployer Threat Defense Virtual sur OCI

Déployez défense contre les menaces virtuelles sur OCI par l'intermédiaire d'une instance de traitement en utilisant l'offre de pare-feu virtuel Cisco Firepower NGFW sur le Marché Oracle Cloud. Sélectionnez la forme de machine la plus appropriée en fonction de caractéristiques telles que le nombre de CPU, la quantité de mémoire et les ressources du réseau.

Procédure

Étape 1 Connectez-vous au portail OCI.

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

Étape 2 Choisissez **Marketplace (Marché)** > **Applications**.

Étape 3 Effectuez une recherche sur le Marché pour l'offre « Cisco Firepower NGFW virtual firewall (NGFWv) ».

Étape 4 Passez en revue les conditions générales et cochez la case **I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions.** (J'ai lu et j'accepte les conditions d'utilisation d'Oracle et les conditions générales des partenaires).

Étape 5 Cliquez sur **Launch Instance** (Lancer l'instance).

Étape 6 Saisissez un **Name** (nom) descriptif pour votre instance, par exemple, *FTDv-6-7*.

Étape 7 Cliquez sur **Change Shape** (modifier la forme) et sélectionnez la forme avec le nombre d'oCPU, la quantité de RAM et le nombre d'interfaces requises pour défense contre les menaces virtuelles; par exemple, VM.Standard2.4 (voir Aperçu, à la page 2).

Étape 8 Dans la liste déroulante **Virtual Cloud Network** (réseau en nuage virtuel), choisissez le VCN de gestion.

Étape 9 Dans la liste déroulante **Subnet** (sous-réseau), choisissez le sous-réseau de gestion si ce champ ne s'est pas rempli automatiquement.

Étape 10 Cochez la case **Use Network Security Groups to Control Traffic** (utiliser les groupes de sécurité réseau pour contrôler le trafic) et choisissez le groupe de sécurité que vous avez configuré pour le VCN de gestion.

Étape 11 Cliquez sur le bouton radio **Assign a Public Ip Address** (affecter une adresse IP publique).

Étape 12 Sous **Add SSH Keys** (ajouter des clés SSH), cliquez sur le bouton radio **Paste Public Keys** (coller des clés publiques) et collez la clé SSH.

Les instances basées sur Linux utilisent une paire de clés SSH au lieu d'un mot de passe pour authentifier les utilisateurs distants. Une paire de clés est composée d'une clé privée et d'une clé publique. Vous conservez la clé privée sur votre ordinateur et fournissez la clé publique lorsque vous créez une instance. Consultez la section Gestion des paires de clés sur les instances Linux pour obtenir des instructions.

Étape 13 Cliquez sur le lien **Show Advanced Options** (afficher les options avancées) pour développer les options.

Étape 14 Sous **Initialization Script** (Script d'initialisation), cliquez sur le bouton radio **Paste Cloud-Init Script** (Coller le script d'initialisation en nuage) pour fournir une configuration day0 (jour 0) pour votre défense contre les menaces virtuelles. La configuration day0 (jour 0) est appliquée lors du premier démarrage de défense contre les menaces virtuelles.

L'exemple suivant montre une configuration day0 (jour0) que vous pouvez copier et coller dans le champ **Cloud-Init Script** (script d'initialisation en nuage) :

```
{
"Hostname": "ftdv-oci",
"AdminPassword": "myPassword@123456",
"FirewallMode": "routed",
"IPv4Mode": "dhcp",
"ManageLocally":"No",
"FmcIp": "1.2.3.4",
"FmcRegKey": "cisco123reg",
"FmcNatId": "cisco123nat"
}
```

- **FmcRegKey** : Il s'agit d'une clé d'enregistrement à utilisation unique utilisée pour enregistrer l'enregistrement du périphérique sur centre de gestion. La clé d'enregistrement est toute valeur alphanumérique définie par l'utilisateur jusqu'à 37 caractères.
- **FmcNatId** : Il s'agit d'une chaîne à usage unique (définie par l'utilisateur). Si le périphérique et centre de gestion sont séparés par un périphérique de NAT, vous devez saisir un ID NAT unique, ainsi que la clé d'enregistrement unique.

Étape 15 Cliquez sur **Create** (créer).

Prochaine étape

Surveillez l'instance défense contre les menaces virtuelles, qui indique l'état Provisioning (provisionnement) après avoir cliqué sur le bouton **Create** (créer).

Important Il est important de surveiller l'état. Dès que l'instance défense contre les menaces virtuelles passe de l'état Provisioning (provisionnement) à l'état Running (en cours d'exécution), vous devez associer les VNIC comme nécessaire avant la fin du démarrage de défense contre les menaces virtuelles.

Associer les interfaces

défense contre les menaces virtuelles passe à l'état en cours d'exécution avec une VNIC associée (consultez **Compute (calculer)** > **Instances** > **Instance Details (détails de l'instance)** > **Attached VNICs (VNIC associées)**). C'est ce que l'on appelle la VNIC principale; elle mappe au VCN de gestion. Avant que défense contre les menaces virtuelles ne termine le premier démarrage, vous devez associer les VNIC pour les autres sous-réseaux VCN que vous avez créés précédemment (diagnostic, interne, externe) afin que les VNIC soient correctement détectées sur défense contre les menaces virtuelles.

Procédure

Étape 1 Sélectionnez votre nouvelle instance défense contre les menaces virtuelles.

Étape 2 Choisissez **Attached VNICs (VNIC associées)** > **Create VNIC (créer une VNIC)**).

Étape 3 Saisissez un **nom** descriptif pour votre VNIC, par exemple *Inside* (interne).

Étape 4 Sélectionnez le VCN dans la liste déroulante **Virtual Cloud Network** (réseau virtuel en nuage).

Étape 5 Sélectionnez votre sous-réseau dans le menu déroulant **Subnet (sous-réseau)**.

Étape 6 Cochez la case **Use Network Security Groups to Control Traffic (utiliser les groupes de sécurité réseau pour contrôler le trafic)** et choisissez le groupe de sécurité que vous avez configuré pour le VCN sélectionné.

Étape 7 Cochez la case **Skip Source Destination Check** (ignorer la vérification de la source de la destination) des groupes de sécurité réseau pour contrôler le trafic.

Étape 8 (Facultatif) Précisez une **Private IP Address** (adresse IP privée). C'est obligatoire uniquement si vous souhaitez choisir une adresse IP particulière pour la VNIC.

Si vous ne spécifiez pas d'adresse IP, le protocole OCI attribuera une adresse IP du bloc CIDR que vous avez attribué au sous-réseau.

Étape 9 Cliquez sur **Save Changes** (enregistrer les modifications) pour créer la carte VNIC.

Étape 10 Répétez cette procédure pour chaque VNIC requise par votre déploiement.

Ajouter des règles de routage pour les VNIC associées

Ajoutez des règles de tableau de routage aux tableaux de routage de diagnostic, interne et externe.

Procédure

Étape 1 Choisissez **Networking (réseautage)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** et cliquez sur le tableau de routage par défaut associé au VCN (interne ou externe).

Étape 2 Cliquez sur **Add Route Rules** (ajouter des règles de routage).

Étape 3 Dans la liste déroulante **Target Type** (type de cible), sélectionnez **Private IP** (adresse IP privée).

Étape 4 Dans la liste déroulante **Destination Type** (type de destination), sélectionnez **CIDR Block** (bloc CIDR).

Étape 5 Saisissez le **bloc CIDR de l'IPv4 de destination**, par exemple 0.0.0.0/0.

Étape 6 Saisissez l'adresse IP privée de la VNIC dans le champ **Target Selection** (sélection de cible).

Si vous n'avez pas explicitement attribué d'adresse IP à la VNIC, vous pouvez trouver l'adresse IP attribuée automatiquement à partir des détails de la VNIC (**Compute (calcul)** > **Instances** > **Instance Details (détails de l'instance)** > **Attached VNICs (VNIC associées)**).

Étape 7 Cliquez sur **Add Route Rules** (ajouter des règles de routage).

Étape 8 Répétez cette procédure pour chaque VNIC requise par votre déploiement.

Déployer la solution d'évolutivité automatique

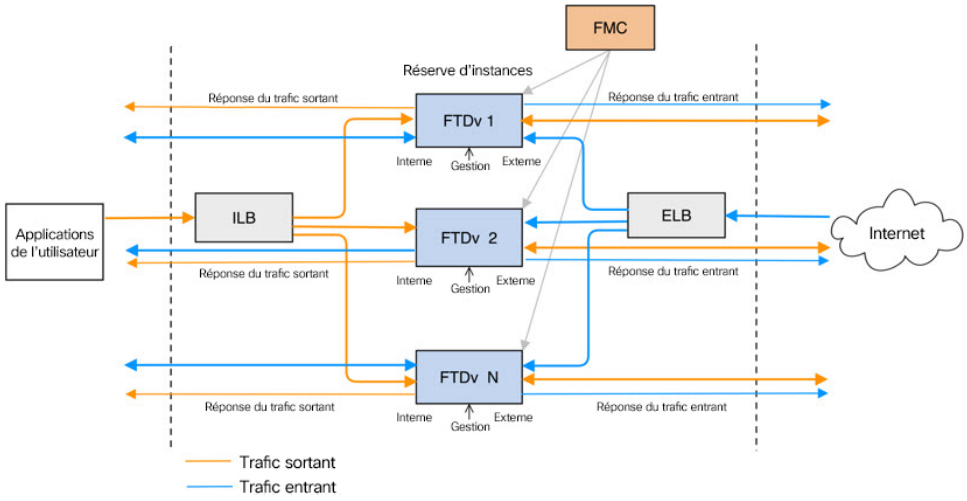
Les sections suivantes décrivent comment les composants de la solution d'évolutivité automatique fonctionnent pour défense contre les menaces virtuelles sur OCI.

Scénario d'évolutivité automatique

Le scénario de la solution d'évolutivité automatique défense contre les menaces virtuelles sur OCI est illustré dans la figure suivante. L'équilibreur de charges Internet a une adresse IP publique et des ports activés à l'aide d'une combinaison du point d'écoute et du groupe cible.

La bicurisation basée sur le port est possible pour le trafic et peut être réalisée en utilisant des règles de NAT. Cet exemple est expliqué dans les sections suivantes.

Illustration 4 : Diagramme de scénarios d'évolutivité automatique de Cisco Secure Firewall Threat Defense Virtual



Champ d'application

Ce document aborde les procédures détaillées pour déployer les composants sans serveur pour la solution défense contre les menaces virtuelles d'évolutivité automatique pour OCI.

Important

- Lisez le document entier avant de commencer le déploiement.
- Assurez-vous que les conditions préalables sont remplies avant de commencer le déploiement.
- Assurez-vous de suivre les étapes et l'ordre d'exécution décrits dans le présent document.

Conditions préalables

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)** > **Policies (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 sphère du détenteur
- Autoriser le groupe <*Group_Name*> à lire l'espace de nom du stockage d'objets dans la sphère du détenteur
- Autoriser le groupe <*Group_Name*> à gérer les référentiels dans la sphère du détenteur

Remarque Vous pouvez également créer des politiques au niveau de la sphère du détenteur. 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 :

   ```
   ALL {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)** > **Policies (politiques)** > **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

FTDv : 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 FTDv. 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 FTDv. Pour implémenter la solution selon ce scénario, l'instance FTDv nécessite quatre 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 FTDv et l'équilibreur de charges sur Internet. Assurez-vous que la passerelle de 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 de NAT/Internet.

Remarque Pour les sondes d'intégrité FTDv, 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 FTDv.

6. **Groupes de sécurité – Groupe de sécurité réseau pour l'instance FTDv**

   Configurez le groupe de sécurité pour les instances de FTDv qui permettent aux fonctions Oracle (dans le même VCN) d'effectuer des connexions SSH à l'adresse de gestion de FTDv.

7. **Object Storage Namespace** (espaces de nom du stockage d'objet)

   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 préauthentifiées pour le fichier configuration.txt. Cette URL préauthentifiée est utilisée lors du déploiement du modèle.

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

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

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

Conditions préalables Cisco Secure Firewall Management Center

Vous pouvez gérer les appareils défense contre les menaces virtuelles à l'aide de Cisco Secure Firewall Management Center, un gestionnaire multipériphérique complet. défense contre les menaces virtuelles s'enregistre et communique avec FMC sur l'interface de gestion que vous avez attribuée à la machine virtuelle défense contre les menaces virtuelles.

Créez tous les objets nécessaires à la configuration et à la gestion de défense contre les menaces virtuelles, y compris un groupe de périphériques, afin de pouvoir déployer des politiques et installer des mises à jour sur plusieurs périphériques. Toutes les configurations appliquées sur le groupe d'appareils transmises aux instances défense contre les menaces virtuelles.

Les sections suivantes donnent un bref aperçu des étapes de base pour préparer centre de gestion. Consultez le *Guide de configuration de Secure Firewall Management Center* et le pour des renseignements complets sur la marche à suivre. Lorsque vous préparez centre de gestion, assurez-vous de consigner les informations suivantes :

- Adresse IP publique Cisco Secure Firewall Management Center
- Nom d'utilisateur et mot de passe (si l'évolutivité basée sur la mémoire est activée, vous devez fournir deux identifiants d'utilisateur)
- Noms des zones de sécurité

- Cisco Secure Firewall Management Center Nom de la politique d'accès
- Cisco Secure Firewall Management Center Nom du protocole NAT
- Nom du groupe d'appareils

Créer un utilisateur dans Cisco Secure Firewall Management Center

Créez un nouvel utilisateur dans Cisco Secure Firewall Management Center avec des privilèges d'administrateur à utiliser uniquement par le gestionnaire d'évolutivité automatique.

Remarque Vous devez disposé d'un compte d'utilisateur Cisco Secure Firewall Management Center dédié à la solution d'évolutivité automatique défense contre les menaces virtuelles pour éviter les conflits avec d'autres sessions.

Procédure

Créez un nouvel utilisateur dans Cisco Secure Firewall Management Center avec des privilèges d'administrateur. Sélectionnez **System** > **Users (utilisateurs du système)** et cliquez sur **Create User** (créer un utilisateur). Le nom d'utilisateur doit être valide pour Linux :

- Au maximum, ils doivent comprendre 32 caractères alphanumériques (plus le tiret (-) et le trait de soulignement).
- Tous les caractères doivent être en minuscules.
- Ne doit pas commencer par un tiret (-); doit comporter des lettres; ne doit pas inclure de point (.), de signe @ ou de barre oblique (/)

Remplissez les options utilisateur selon les besoins de votre environnement. Consultez le *Guide de configuration de Secure Firewall Management Center* et le pour en savoir plus.

Créer un groupe d'appareils

Les groupes de périphériques vous permettent d'attribuer facilement des politiques et d'installer des mises à jour sur plusieurs périphériques. Un groupe de périphérique doit être créé et des règles doivent y être appliquées. Toutes les configurations appliquées sur le groupe d'appareils sont transmises aux instances défense contre les menaces virtuelles.

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 2 Dans le menu déroulant **Add** (ajouter), choisissez **Add Group** (ajouter un groupe).

Étape 3 Saisissez le nom du groupe d'appareils.

Étape 4 Cliquez sur **OK** pour ajouter le groupe de périphériques.

Créer des objets de réseau et des objets hôtes

Créez les objets suivants à utiliser pour la configuration défense contre les menaces virtuelles.

Procédure

Étape 1 Créez un hôte avec son nom *oci- metadata-server* et son adresse IP *169.254.169.254*.

Étape 2 Créez un port ayant son nom comme contrôle d'intégrité et sa valeur comme 8080 ou tout autre port selon les besoins.

Étape 3 Créez une interface interne, choisissez **Interface** > **Security Zone (zone de sécurité)**. Sélectionnez le type **Routed** (avec routage). Attribuez un nom à l'interface, par exemple, *inside-sz*.

Étape 4 Créez une interface externe, choisissez **Interface** > **Security Zone (zone de sécurité)**. Sélectionnez le type **Routed** (avec routage). Attribuez un nom à l'interface, par exemple, *outside-sz*.

Créer la politique de NAT

Créez une politique de traduction d'adresses réseau (NAT) et créez les règles de NAT nécessaires pour transférer le trafic de l'interface externe vers votre application, et associez cette politique au groupe d'appareils que vous avez créé pour l'évolutivité automatique.

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **NAT**.

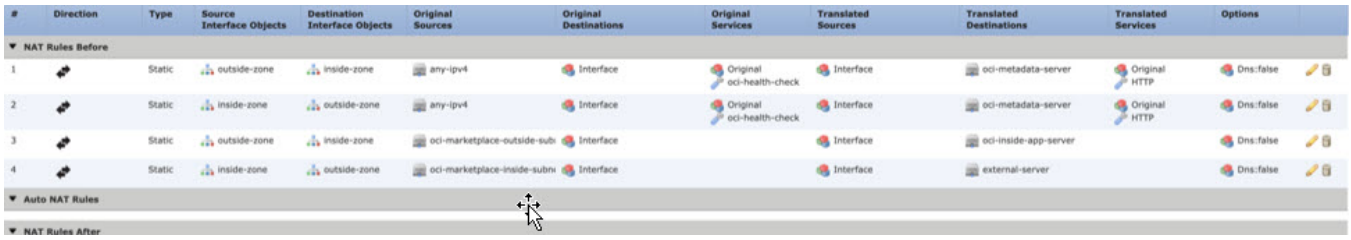
Étape 2 Dans la liste déroulante **New Policy** (nouvelle politique), choisissez **Threat Defense NAT** (traduction d'adresses réseau de défense contre les menaces).

Étape 3 Saisissez un nom unique dans le champ **Name**.

Étape 4 Vous pouvez également saisir une **Description**.

Étape 5 Configurez les règles de NAT. Reportez-vous à la section sur la configuration de la NAT pour Threat Defense dans le Guide de configuration des périphériques de Cisco Secure Firewall Management Center pour obtenir des instructions sur la création des règles de NAT et l'application des politiques de NAT. La figure suivante montre une approche de base pour la définition des règles.

Illustration 5 : Règles de NAT



Étape 6 Cliquez sur **Save** (enregistrer).

Créer des règles de NAT

Une règle de NAT typique convertit les adresses internes en un port sur l'adresse IP de l'interface externe. Ce type de règle NAT est appelé interface Port Address Translation (PAT). Consultez la section sur la configuration de la NAT dans la défense contre les menaces dans le Guide de configuration des périphériques de Cisco Secure Firewall Management Center pour obtenir de plus amples renseignements.

Configurez les deux règles obligatoires suivantes qui sont requises dans votre politique de NAT :

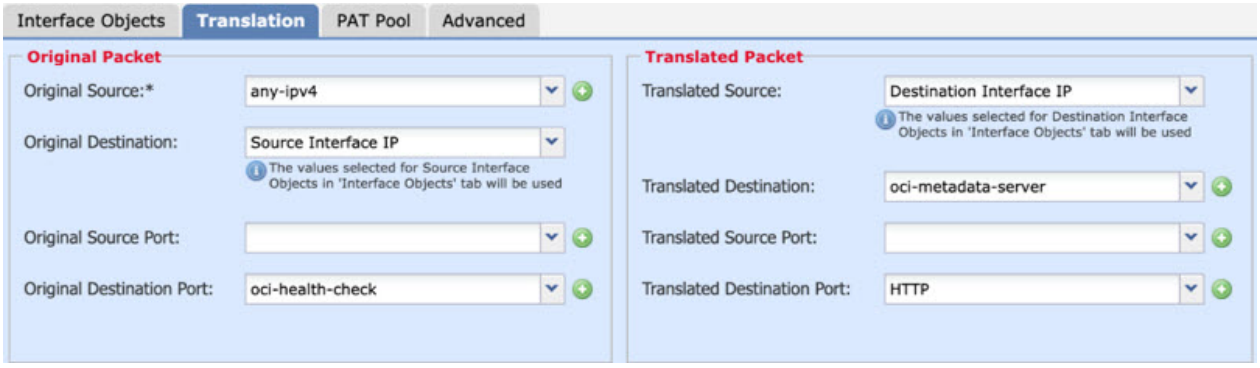
Procédure

Étape 1 Configurez la règle de NAT suivante pour la vérification de l'intégrité du trafic entrant :

- Zone source : zone externe
- Zone de destination : zone interne
- Sources originales : any-ipv4
- Destinations d'origine : IP d'interface source
- Port source d'origine : par défaut
- Original-destination-port: health-check-port
- Translated-sources: adresse IP de l'interface de destination
- Translated-destination: oci-metadata-server
- Port source traduite : par défaut
- Translated-destination-port: HTTP

La figure suivante montre la règle de NAT pour la vérification de l'intégrité du trafic entrant.

Illustration 6 : Règle de NAT d'intégrité entrante



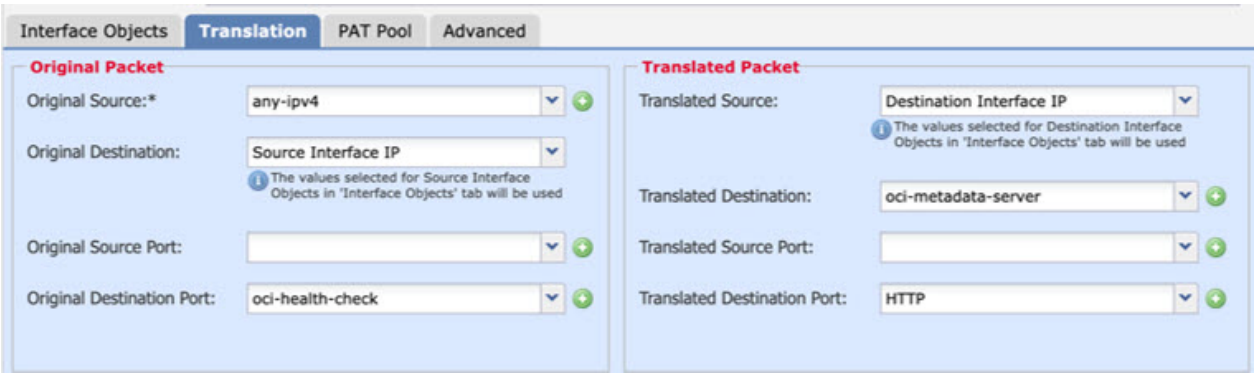
Étape 2 Configurez la règle de NAT suivante pour la vérification de l'intégrité sortante.

- Zone source : zone interne
- Zone de destination : zone externe
- Sources originales : any-ipv4

- Destinations d'origine : IP d'interface source
- Port source d'origine : par défaut
- Original-destination-port: health-check-port
- Translated-sources: adresse IP de l'interface de destination
- Translated-destination: oci-metadata-server
- Port source traduite : par défaut
- Translated-destination-port: HTTP

La figure suivante montre la règle de NAT pour la vérification de l'intégrité du trafic sortant.

Illustration 7 : Règle de NAT de la vérification de l'intégrité du trafic sortant



De même, toutes les règles NAT peuvent être ajoutées pour le trafic de données, et cette configuration les pousse vers les périphériques défense contre les menaces virtuelles.

Créer une politique d'accès

Configurez le contrôle d'accès pour autoriser le trafic de l'intérieur vers l'extérieur. Une stratégie d'accès avec toutes les stratégies requises peut être créée. L'objet de port d'intégrité doit être autorisé de sorte que le trafic sur ce port soit autorisé à atteindre l'appareil. Dans une politique de contrôle d'accès, les règles de contrôle d'accès précisent une méthode de gestion du trafic réseau sur plusieurs périphériques gérés. Une configuration et un séquencement appropriés des règles sont essentiels pour créer un déploiement efficace. Consultez les bonnes pratiques pour les règles de contrôle d'accès dans le Guide de configuration des périphériques de Cisco Secure Firewall Management Center.

Affectez le groupe de périphériques (créé dans le cadre des conditions préalables) à la politique d'accès à l'aide de l'attribution de politiques (**Policy Affectations**).

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.

Étape 2 Cliquez sur **New Policy** (nouvelle politique).

Étape 3 Saisissez un nom (Name) et, si vous le souhaitez, une description.

Étape 4 Configurez les paramètres de sécurité et les règles pour votre déploiement. Pour plus d'informations, voir la section sur le contrôle d'accès dans le Guide de configuration de dispositif du Cisco Secure Firewall Management Center.

Chiffrer le mot de passe

Remarque Pour en savoir plus sur cette procédure, consultez Create Vaults and Secrets (créer des vaults et des secrets).

Le mot de passe pour FTDv est utilisé pour configurer toutes les instances de FTDv utilisées lors de l'évolutivité automatique et il est utilisé pour créer des connexions pour les appels d'API Rest à des fins de configuration.

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.

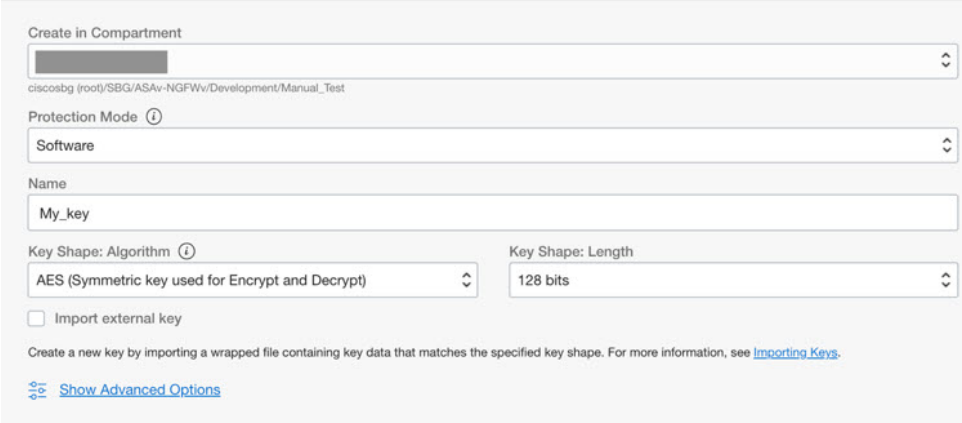
Une clé de chiffrement principale est nécessaire pour chiffrer le mot de passe en texte brut.

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 8 : 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 défense contre les menaces virtuelles

Il est prévu que l'application soit déployée ou que son plan de déploiement soit disponible.

Procédure

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

Paramètre	Type de données	Description
tenancy_ocid	Chaîne	OCID de la sphère à laquelle votre compte appartient. Pour savoir comment trouver l'OCID de la sphère du détenteur, consultez l'information ici. L'OCID de la sphère du détenteur ressemble à ceci : `ocid1.tenancy.oc1..<unique_ID>`
région	Chaîne	Identificateur unique de la région dans laquelle vous souhaitez que les ressources soient créées. Exemple : us-phoenix-1, us-ashburn-1
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
availability_domain	Chaîne	Exemple : Tpeb:PHX-AD-1, Tpeb:PHX-AD-2 **Remarque** Pour obtenir les noms de domaine de disponibilité, consultez l'information ici.
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.
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.
function_subnet_ocid	Chaîne	OCID du sous-réseau de fonction 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.
outside_nsg_ocid	Chaîne	OCID du groupe de sécurité réseau du sous-réseau externe qui doit être utilisé.

Paramètre	Type de données	Description
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 exécuter la vérification de l'intégrité. 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 »
livre_bs_politique	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'équilibreurs de charges, consultez l'information ici Valeurs prises en charge : « ROUND_ROBIN », « LEAST_CONNECTIONS », « IP_HASH »
image_name	Chaîne	Le nom de l'image de Marché à utiliser pour créer la configuration d'instance. Valeur par défaut : « Pare-feu virtuel Cisco Firepower NGFW (NGFWv) » **Remarque** Si l'utilisateur souhaite déployer une image personnalisée, il doit configurer le paramètre custom_image_ocid.
scaling_thresholds	Valeurs séparées par des virgules	Les seuils d'utilisation du CPU à utiliser pour l'évolutivité à la baisse ou à la hausse. Indiquez les valeurs de seuil d'évolutivité à la baisse et à la hausse séparées par une virgule. Exemple : 15,50 où 15 est le seuil d'évolutivité à la baisse et 50, le seuil d'évolutivité à la hausse.

Paramètre	Type de données	Description
compartment_id	Chaîne	L'OCID du compartiment dans lequel créer les ressources. Exemple : **locid1.compartment.oc1..**<ID_unique>
compartment_name	Chaîne	Nom du compartiment
custom_image_ocid	Chaîne	OCID de l'image personnalisée à utiliser pour créer la configuration de l'instance si l'image du Marché ne doit pas être utilisée. **Remarque** *custom_image_ocid est un paramètre facultatif*
ftdv_password	Chaîne	Le mot de passe pour défense contre les menaces virtuelles sous forme chiffrée, en utilisant le protocole SSH dans défense contre les menaces virtuelles pour la configuration. Utilisez le guide de configuration pour les instructions sur la façon de chiffrer le mot de passe ou consultez l'information ici.
ftdv_license_type	Chaîne	Type de licence défense contre les menaces virtuelles, BYOL ou PAYG. Actuellement, BYOL est pris en charge.
cryptographic_endpoint	Chaîne	Le terminal cryptographique est une URL utilisée pour déchiffrer le mot de passe. Il se trouve dans le Vault (le 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 (le centre de stockage). **Remarque** master_encryption_key_id et cryptographic_endpoint doivent appartenir au même centre de stockage.
fmc_ip	Chaîne	Adresse IP de Cisco Secure Firewall Management Center. Adresse IP du centre de gestion qui sera utilisée par le client pour gérer les instances de défense contre les menaces virtuelles. **Remarque** *L'adresse IP du centre de gestion ne peut être privée que si elle se trouve dans le même sous-réseau que défense contre les menaces virtuelles, sinon l'adresse IP publique doit être utilisée pour tous les autres cas.*
fmc_username	Chaîne	Nom d'utilisateur du compte centre de gestion. Ce nom d'utilisateur sera utilisé pour se connecter au centre de gestion afin de configurer chaque fois la nouvelle instance défense contre les menaces virtuelles.

Paramètre	Type de données	Description
fmc_password	Chaîne	Mot de passe chiffré du centre de gestion. Pour la procédure de chiffrement du mot de passe, consultez l'information ici.
fmc_device_group_name	Chaîne	Il doit y avoir un groupe d'appareils dans le centre de gestion; tous les défense contre les menaces virtuelles de cette solution d'évolutivité automatique seront ajoutés à ce groupe, de sorte que les mêmes politiques et la même configuration puissent être appliquées à tous.
enable_memory_based_scaling	Booléen	Publiez l'utilisation de la mémoire défense contre les menaces virtuelles à partir de Cisco Secure Firewall Management Center Virtual. En activant cet indicateur, l'évolutivité peut également se produire en fonction de l'utilisation de la mémoire. Par défaut, l'utilisation du processeur est adoptée.
fmc_metrics_username	Chaîne	Si vous optez pour l'utilisation de la mémoire en activant l'indicateur enable_memory_based_scaling, un compte d'utilisateur centre de gestion supplémentaire est nécessaire, car il sera utilisé en permanence pour extraire l'utilisation de la mémoire de toutes les instances défense contre les menaces virtuelles en cours d'exécution.
fmc_metrics_password	Chaîne	Mot de passe du compte centre de gestion supplémentaire sous forme chiffrée. Pour la procédure de chiffrement du mot de passe, consultez l'information ici.
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/ <user>@<mail>.com »
Object Storage Namespace (espace de nom du stockage d'objets)		Il s'agit d'un identifiant unique créé au moment de la création de l'espace de location. Accédez à **OCI** > **Administration** > **Tenancy Details (détails de la sphère du détenteur)**
Jeton d'autorisation		Il est utilisé comme mot de passe pour la connexion Docker, ce qui l'autorise à pousser les fonctions Oracle dans le registre de conteneur OCI. Accédez à **OCI** > **Identity** > **Users** > **User Details (soit aux détails de l'utilisateur, dans la section de l'identité sous OCI)** > **Auth Tokens (jetons d'authentification)** > **Generate Token (générer des jetons)**.

Étape 2 Créez le fichier *Configuration.json* avec le contenu suivant :

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],
  "performanceTier": "FTDv30",
  "fmcIpforDeviceReg": "DONTRESOLVE",
  "RegistrationId": "cisco",
  "NatId": "cisco",
  "fmcAccessPolicyName": "<autoscale-access-policy-name>",
  "fmcNatPolicyName": "<autoscale-nat-policy-name>",
  "fmcInsideNicName": "inside",
  "fmcOutsideNicName": "outside",
  "fmcInsideNic": "GigabitEthernet0/0",
  "fmcOutsideNic": "GigabitEthernet0/1",
  "fmcOutsideZone": "<outside-zone-name>",
  "fmcInsideZone": "<inside-zone-name>",
  "MetadataServerObjectName": "oci-metadata-server",
  "interfaceConfig": [
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "inside-zone"
      },
      "mode": "NONE",
      "ifname": "inside",
      "name": "GigabitEthernet0/0"
    },
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "outside-zone"
      },
      "mode": "NONE",
      "ifname": "outside",
      "name": "GigabitEthernet0/1"
    }
  ],
  "trafficRoutes": [
    {
      "interface": "outside",
      "network": "any-ipv4",
      "gateway": "",
      "metric": "2"
    },
    {
      "interface": "inside",
      "network": "oci-metadata-server",
      "gateway": "",
      "metric": "1"
    }
  ]
}
```

Étape 3 Mettez à jour le fichier *Configuration.json* avec les paramètres de configuration.

Étape 4 Chargez le fichier de configuration dans l'espace de stockage d'objets.

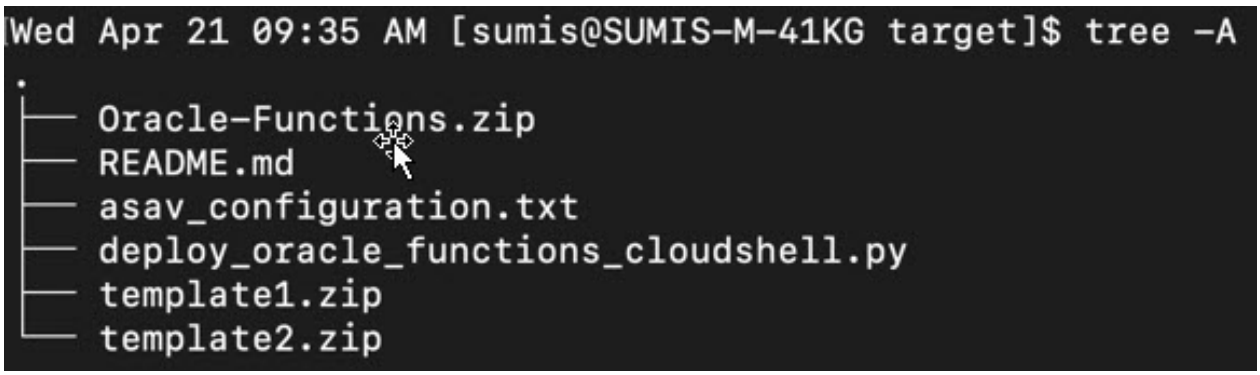
Le fichier *configuration.txt* doit être chargé dans l'espace de stockage d'objets créé par l'utilisateur, et la demande de préauthentification pour le fichier chargé doit être créée.

Remarque
Assurez-vous que l'URL de demande de préauthentification de configuration.txt est utilisée dans le déploiement de la pile.

Remarque
La période d'expiration doit être définie lors de la création d'une URL préauthentifiée dans OCI. Assurez-vous que cette période est suffisamment longue pour ne pas expirer pendant l'exécution de la solution.

Étape 5 Créez les 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.



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, déployer les fonctions Oracle, puis déployer Terraform Template-2.

Déployer la pile Terraform Template-1

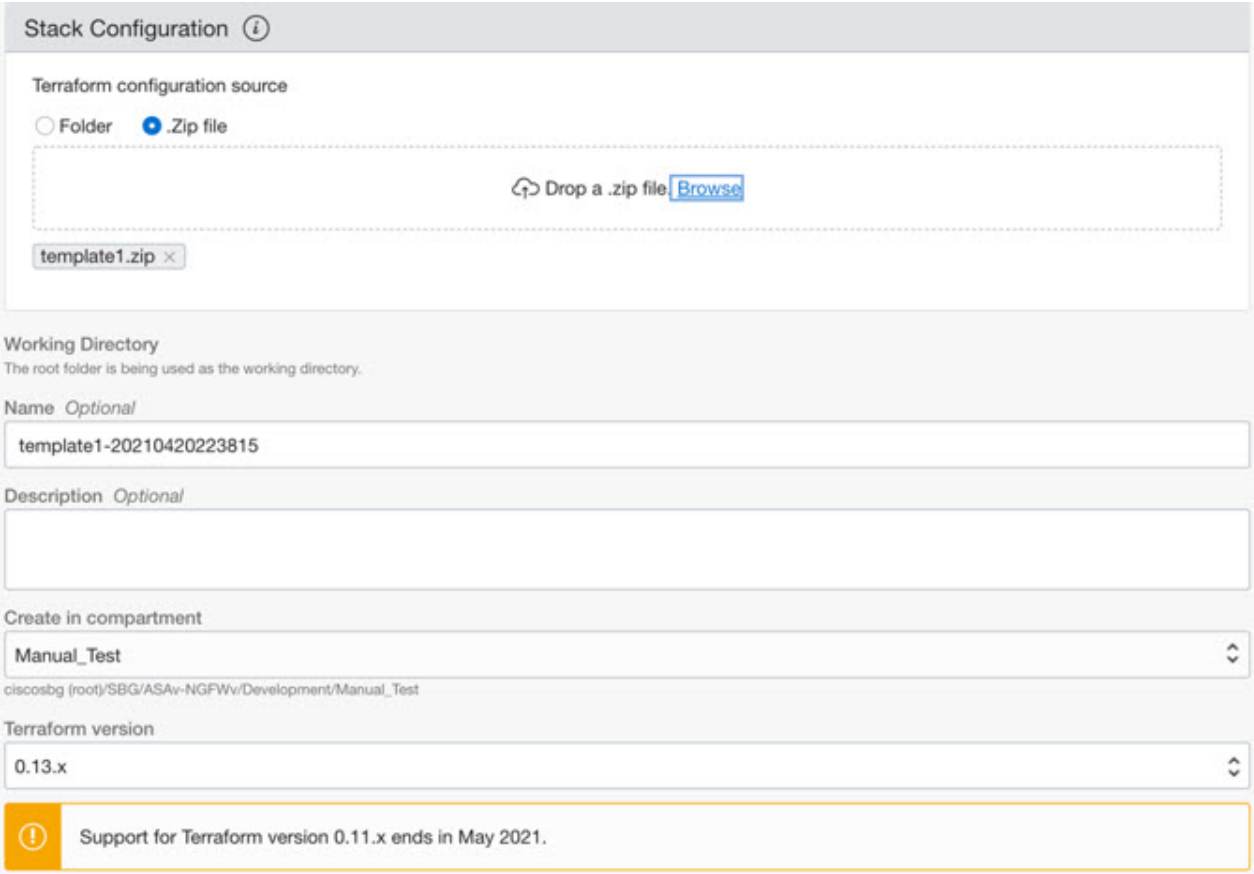
Procédure

Étape 1 Connectez-vous au portail OCI.

La région est affichée dans le coin supérieur droit de votre écran. Vérifiez 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.



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 Collection of Input Parameters (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** > **Apply pour appliquer les actions Terraform)**.

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

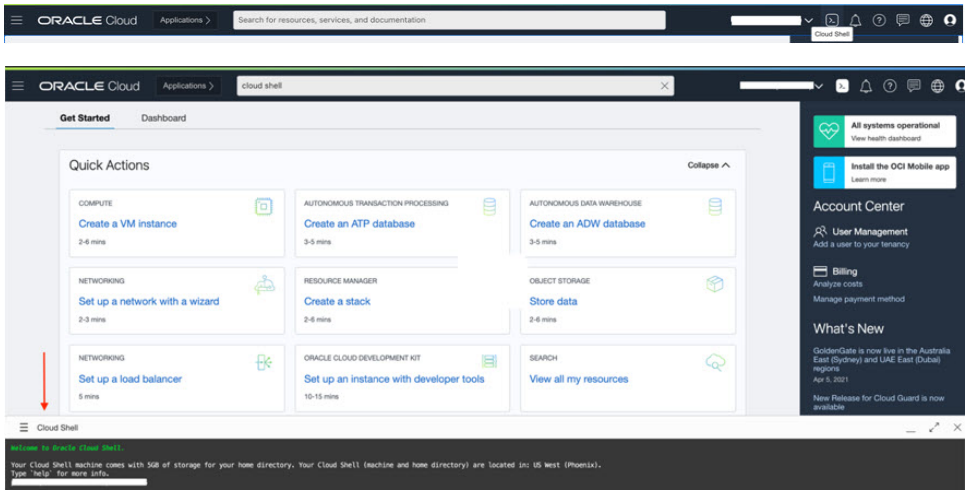
Déployer les fonctions Oracle

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

Dans OCI, les fonctions Oracle sont téléversées 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.

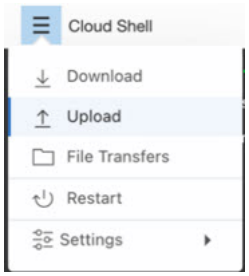
Procédure

Étape 1 Ouvrez OCI Cloud Shell.

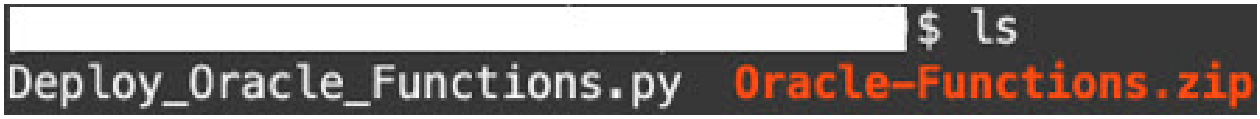


Étape 2 Téléversez *deploy_oracle_functions_cloudshell.py* et *Oracle-Functions.zip*.

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



Étape 3 Vérifiez les fichiers à l'aide de la commande **ls**.



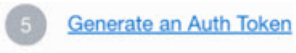
Étape 4 Exécutez `python3 Deploy_Oracle_Functions.py -h`. Le script `eploy_oracle_functions_cloudshell.py` nécessite certains paramètres d'entrée dont les détails peuvent être trouvés à l'aide de l'argument d'aide, comme illustré dans la figure ci-dessous.

```
                                $ 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, entrez les arguments suivants :

Tableau 3 : 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 modèle-1 et le suffixe **« _application ».**
Identifiant de région	L'identifiant de région est le mot de code de région fixe dans l'OCI pour différentes régions. Par exemple : « us-phoenix-1 » pour Phoenix ou « ap-telbourne-1 » pour Melbourne. Pour obtenir la liste de toutes les régions avec leurs identifiants de région, accédez à **OCI** > **Administration** > **Region Management (gestion des régions)**.
Nom de profil	Il s'agit du nom de profil de l'utilisateur simple dans le OCI. Exemple : *oracleidentitycloudservice/<user>@<mail>.com* Le nom se trouve dans la section du profil de l'utilisateur.
OCID du compartiment	Il s'agit de l'OCID (Oracle Cloud Identifier) du compartiment. OCID du compartiment où l'utilisateur dispose de l'application OCI. Accédez à **OCI** > **Identity** > **Compartment** > **Compartment Details** pour consulter les détails du compartiment.

Argument	Détails
Object Storage Namespace (espaces de nom du stockage d'objet)	Il s'agit d'un identifiant unique créé au moment de la création de l'espace de location. Accédez à **OCI** > **Administration** > **Tenancy Details (détails de la location)**.
Jeton d'autorisation	Il est utilisé comme mot de passe pour la connexion 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. Accédez à **OCI** > **Identity** > **Users** > **User Details (soit aux détails de l'utilisateur, dans la section de l'identité sous OCI)** > **Auth Tokens (jetons d'authentification)** > **Generate Token (générer des jetons)**. Si, pour quelque raison que ce soit, vous ne parvenez pas à afficher les détails de l'utilisateur (User Details), cliquez sur **Developer services** > **Functions** pour consulter les fonctions des services de développeur. 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. 

Étape 5 Exécutez la commande `pyth3 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. Vérifiez 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.

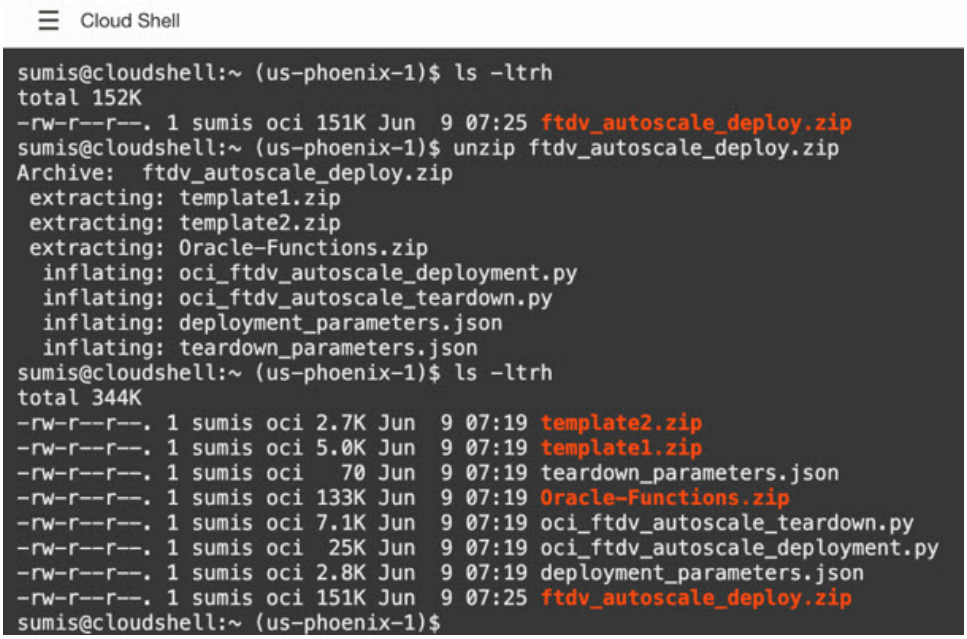
Étape 3 À l'étape suivante, cliquez sur **Terraform Actions (actions Terraform)** > **Apply (appliquer)**.

Déploiement à l'aide de CloudShell

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 *ftdv_autoscale_deploy.zip* dans le dossier cible de l'interface Cloud Shell et extrayez les fichiers.



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 le déploiement de la solution d'évolutivité automatique, exécutez la commande `python3 oci_ftdv_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

Vérifiez si toutes les ressources sont déployées et si 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 défense contre les menaces virtuelles.

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 défense contre les menaces virtuelles.

Remarque Précisez le nombre minimal d'instances défense contre les menaces virtuelles comme **protégées contre une évolutivité à la baisse** pour éviter qu'elles soient supprimées par la mise en œuvre des 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 Défense contre les menaces virtuelles

Aucune prise en charge de la mise à niveau des machines virtuelles défense contre les menaces virtuelles dans cette version. La pile doit être redéployée avec l'image défense contre les menaces virtuelles 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)** > **Function (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 ou la 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 ou 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 équilibreurs de charges, si défense contre les menaces virtuelles a une licence, elle sera perdue.

5. Pour certaines raisons, si l'instance défense contre les menaces virtuelles 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 défense contre les menaces virtuelles. 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 point d'écoute dans l'équilibreur de charges

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

Enregistrer un système principal dans l'ensemble principal

Afin d'enregistrer une instance défense contre les menaces virtuelles sur l'équilibreur de charges, l'adresse IP de l'interface externe de l'instance défense contre les menaces virtuelles 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 le point d'écoute.

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.

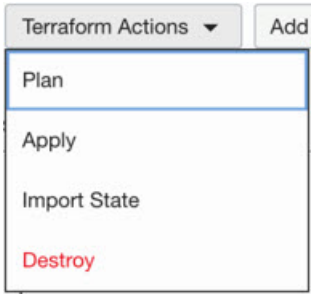
Procédure

Étape 1 Connectez-vous au portail OCI.

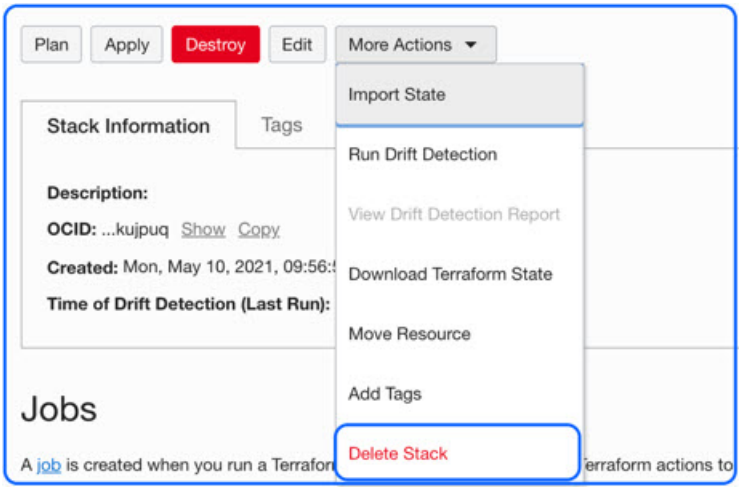
La région est affichée dans le coin supérieur droit de votre écran. Vérifiez que vous êtes dans la région prévue.

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. Vérifiez que vous êtes dans la région prévue.

Étape 2 Choisissez **Developer Services (services de développeur)** > **Functions (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

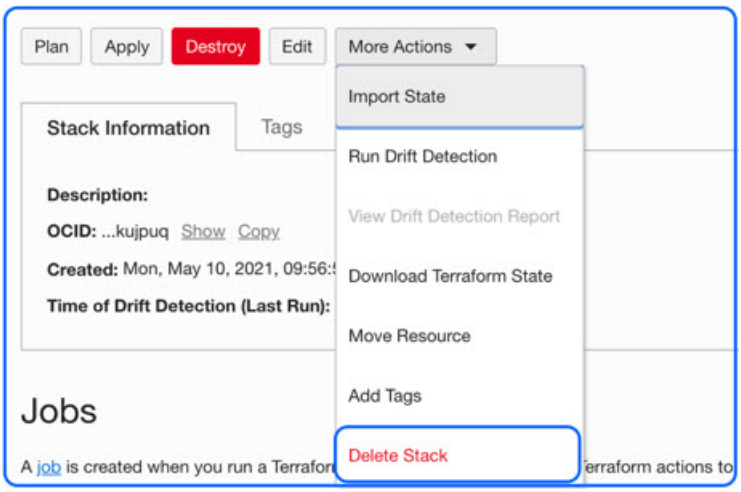
Étape 1 Connectez-vous au portail OCI.

La région est affichée dans le coin supérieur droit de votre écran. Vérifiez 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 la mise à l'échelle 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_ftdv_autoscale_teardown.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 *teardown_parameters.json*.

Se connecter à l'instance Défense contre les menaces virtuelles à l'aide de SSH

Pour vous connecter à l'instance défense contre les menaces virtuelles à partir d'un système de type Unix, connectez-vous à l'instance à l'aide de SSH.

Procédure

Étape 1 Utilisez la commande suivante pour définir les autorisations de fichier afin que seul vous puissiez lire le fichier :

```
$ chmod 400 <private_key>
```

Dans la chaîne ci-haut :

`<private_key>` est le chemin d'accès complet et le nom du fichier qui contient la clé privée associée à l'instance à laquelle vous souhaitez accéder.

Étape 2 Utilisez la commande SSH suivante pour accéder à l'instance :

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

<private_key> est le chemin d'accès complet et le nom du fichier qui contient la clé privée associée à l'instance à laquelle vous souhaitez accéder.

<nom-utilisateur> correspond au nom d'utilisateur de l'instance défense contre les menaces virtuelles.

<public-ip-address> correspond à l'adresse IP publique de votre instance que vous avez extraite de la console.

Se connecter à l'instance Défense contre les menaces virtuelles à l'aide d'OpenSSH

Pour vous connecter à l'instance défense contre les menaces virtuelles à partir d'un système Windows, connectez-vous à l'instance à l'aide d'OpenSSH.

Procédure

Étape 1 Si c'est la première fois que vous utilisez cette paire de clés, vous devez définir les autorisations de fichier de sorte que vous puissiez être le seul à lire le fichier.

Procédez comme suit :

a) Dans Windows Explorer, accédez au fichier de clé privée, cliquez avec le bouton droit sur le fichier, puis cliquez sur **Properties** (propriétés).
b) Dans l'onglet **Security** (sécurité), cliquez sur **Advanced** (avancé).
c) Assurez-vous que le propriétaire (**Owner**) est votre compte d'utilisateur.
d) Cliquez sur **Disable Inheritance** (désactiver l'hérédité), puis sélectionnez **Convert inherited permissions into explicit permissions on this object** (convertir les autorisations héritées en autorisations explicites sur cet objet).
e) Sélectionnez chaque entrée d'autorisation qui ne correspond pas à votre compte d'utilisateur et cliquez sur **Remove** (supprimer).
f) Assurez-vous que l'autorisation d'accès pour votre compte d'utilisateur est **Full control** (contrôle complet).
g) Enregistrez vos modifications.

Étape 2 Pour vous connecter à l'instance, ouvrez Windows PowerShell et exécutez la commande suivante :

```
$ ssh –i <private_key> <username>@<public-ip-address>
```

Dans la chaîne ci-haut :

<private_key> est le chemin d'accès complet et le nom du fichier qui contient la clé privée associée à l'instance à laquelle vous souhaitez accéder.

<nom-utilisateur> correspond au nom d'utilisateur de l'instance défense contre les menaces virtuelles.

<public-ip-address> correspond à l'adresse IP publique de votre instance que vous avez extraite de la console.

Se connecter à l'instance Défense contre les menaces virtuelles à l'aide de PuTTY

Pour vous connecter à l'instance défense contre les menaces virtuelles à l'aide de PuTTY depuis un système Windows :

Procédure

Étape 1 Ouvrez PuTTY.

Étape 2 Dans le volet **Category** (catégorie), sélectionnez **Session** et entrez les informations suivantes :

- **Le nom d'hôte ou l'adresse IP (« Host Name or IP address ») selon le modèle suivant :**

  `<nom-utilisateur>@<adresse-ip-publique>`

  Dans la chaîne ci-haut :

  `<nom-utilisateur>` correspond au nom d'utilisateur de l'instance défense contre les menaces virtuelles.

  `<adresse-ip-publique>` correspond à l'adresse IP publique d'instance que vous avez extraite de la console.

- **Port :** 22
- **Type de connexion (« Connection type ») :** SSH

Étape 3 Dans le volet **Category** (catégorie), développez **Window** (fenêtre), puis sélectionnez **Translation** (traduction).

Étape 4 Dans la liste déroulante **Remote character set** (jeu de caractères du système distant), sélectionnez **UTF-8**.

Sur les instances basées sur Linux, les paramètres régionaux par défaut sont définis pour UTF-8. PuTTY est configuré pour utiliser les mêmes paramètres régionaux.

Étape 5 Dans le volet **Category** (catégorie), développez la section **Connection** (connexion), puis la section **SSH**. Cliquez ensuite sur **Auth** (authentification).

Étape 6 Cliquez sur **Browse** (parcourir), puis sélectionnez votre clé privée (private key).

Étape 7 Cliquez sur **Open** (ouvrir) pour lancer la session.

S'il s'agit de votre première connexion à l'instance, un message indiquant que la clé d'hôte du serveur n'est pas mise en cache dans le registre pourrait s'afficher. Cliquez sur **Yes** (oui) pour poursuivre.

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.