

Déployer Firewall Management Center Virtual sur OCI

Oracle Cloud Infrastructure (OCI) est un service informatique en nuage public qui vous permet d'exécuter vos applications dans un environnement hautement disponible hébergé par Oracle. L'OCI offre une extensibilité en temps réel pour les applications d'entreprise en combinant les services autonomes, la sécurité intégrée et le traitement sans serveur d'Oracle.

Vous pouvez déployer le Firewall Management Center Virtual sur OCI

- Aperçu, à la page 1
- Prérequis, à la page 2
- Lignes directrices et limites relatives à la licence, à la page 3
- Exemple de topologie de réseau, à la page 3
- Déployer Firewall Management Center Virtual, à la page 4
- Accéder à l'instance Firewall Management Center Virtual sur OCI, à la page 8

Aperçu

Firewall Management Center Virtual exécute le même logiciel que les On-Prem Firewall Management Center physiques afin d'offrir des fonctionnalités de sécurité éprouvées dans un format virtuel. Firewall Management Center Virtual peut être déployé dans l'OCI public. Il peut ensuite être configuré pour gérer les périphériques virtuels et physiques.

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. Firewall Management Center Virtual prend en charge les types de formes OCI suivantes :

Tableau 1 : Calculer les formes prises en charge pour Firewall Management Center Virtual

Forme OCI	Version Firewall Management Center Virtual prise en charge	Attributs	
		oCPU	RAM (Go)
Intel VM.Standard 2.4	7.1.0 ou ultérieure	4	60

Tableau 2 : Modèles de traitement pris en charge pour Firewall Management Center Virtual 300 (FMCv300) dans les versions 7.1.0 et ultérieures

Forme OCI	Attributs	
	oCPU	RAM (Go)
VM.Standard2.16	16	240 GB Stockage SSD : 2 000 Go

Remarque Les types de formes pris en charge peuvent changer sans préavis.

- Dans OCI, 1 oCPU équivaut à 2 vCPU.
- Firewall Management Center Virtual requiert une interface.

Vous créez un compte sur OCI, lancez une instance de calcul à l'aide de l'offre de Firewall Management Center Virtual sur le Marché Oracle Cloud et choisissez une forme OCI.

Prérequis

- Créer 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/).
  - Configurez tous les droits de licence pour les services de sécurité à partir du On-Prem Firewall Management Center.
  - Consultez la section « Gestion des licences du système » dans le Guide de configuration On-Prem Firewall Management Center pour plus d'informations sur la gestion des licences.
- Exigences d'interface :
  - Interface de gestion : une interface utilisée pour connecter l'appareil Firewall Threat Defense au On-Prem Firewall Management Center.
- Chemins de communication :
  - IP public pour l'accès administratif au Firewall Management Center Virtual.
- Pour la compatibilité de Firewall Management Center Virtual et du système, consultez les 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
- Maximum de 8 vCPU par instance
- Mode routé (par défaut)
- Licences : Seul le protocole BYOL est pris en charge
- **Firewall Management Center Virtual 300 (FMCv300) pour OCI** : une nouvelle image évolutive Firewall Management Center Virtual est disponible sur la plateforme OCI. Elle prend en charge la gestion d'un maximum de 300 périphériques et affiche une capacité de disque plus élevée (7.1.0 et versions ultérieures).
- La haute accessibilité (HA) Firewall Management Center Virtual est prise en charge.

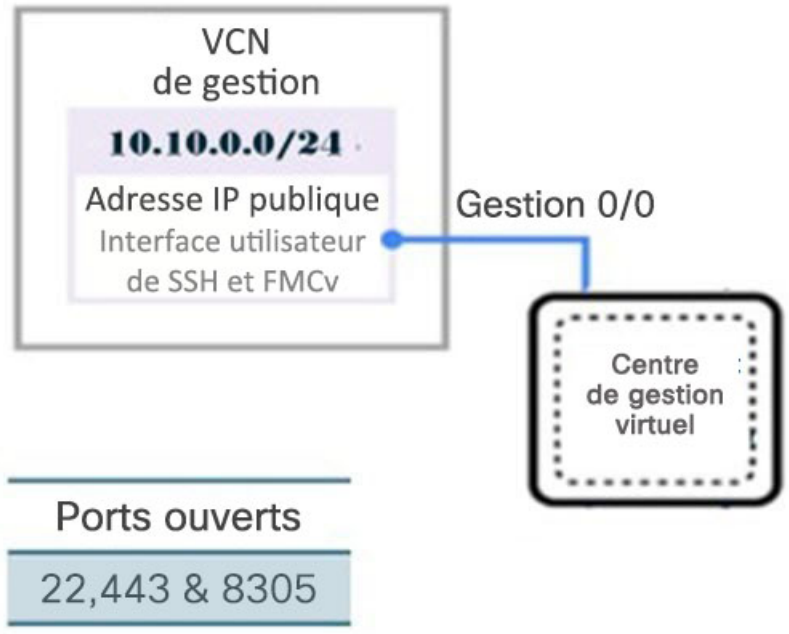
Fonctionnalités partiellement prises en charge

- IPv6

Exemple de topologie de réseau

La figure suivante illustre la topologie typique pour le Firewall Management Center Virtual avec un sous-réseau configuré dans l'OCI.

Illustration 1 : Exemple de topologie pour le déploiement Firewall Management Center Virtual sur OCI



Déployer Firewall Management Center Virtual

Configurer le réseau virtuel en nuage (VCN)

Vous configurez le réseau virtuel en nuage (VCN) pour votre déploiement de Firewall Management Center Virtual.

Avant de commencer

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 « Gestion des compartiments » pour en savoir plus.

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 *FMCv-Management*.

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

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

Prochaine étape

Vous pouvez poursuivre les procédures suivantes pour terminer le VCN de gestion.

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, *FMCv-Mgmt-Allow-22-443-8305*.

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

Le périphérique Firewall Management Center Virtual peut être géré par Firewall Management Center Virtual, ce qui nécessite l'ouverture du port 8305 pour les connexions HTTPS. Vous avez besoin du port 443 pour accéder au On-Prem Firewall Management Center lui-même.

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.

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).

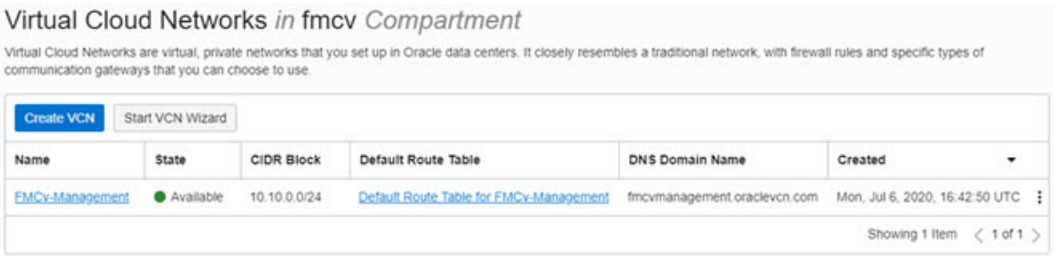
Étape 8 Sélectionnez une **Security List** (liste de sécurité) que vous avez créée précédemment.

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

Prochaine étape

Après avoir configuré votre VCN (Gestion), vous pouvez lancer le Firewall Management Center Virtual. Consultez le schéma suivant pour un exemple de configuration VCN Firewall Management Center Virtual.

Illustration 2 : Réseaux virtuels en nuage Firewall Management Center Virtual



Créer l'instance Firewall Management Center Virtual sur OCI

Vous déployez Firewall Management Center Virtual sur OCI par l'intermédiaire d'une instance de traitement en utilisant l'offre Firewall Management Center Virtual - BYOL sur le Marché Oracle Cloud. Vous 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. Assurez-vous que vous êtes dans la région prévue.

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

Étape 3 Effectuez une recherche sur le Marché pour « Firewall Management Center Virtual » et choisissez l'offre.

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, *Cisco-FMCv*.

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 Firewall Management Center Virtual; par exemple, VM.Standard2.4 (voir Formats de traitement OCI, à la page 1).

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 s'il n'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 le Firewall Management Center Virtual. La configuration day0 (jour 0) est appliquée lors du premier démarrage de Firewall Management Center Virtual.

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) :

```
{
"AdminPassword": "myPassword@123456",
"Hostname": "cisco-fmcv"
}
```

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

Prochaine étape

Surveillez l'instance Firewall Management Center Virtual, qui indique l'état Provisioning (Provisionnement) après avoir cliqué sur le bouton **Create** (Créer). Il est important de surveiller l'état. Recherchez l'instance Firewall Management Center Virtual qui passe de l'état Provisioning (Provisionnement) à l'état Running (En fonctionnement), ce qui indique que le démarrage Firewall Management Center Virtual est terminé.

Accéder à l'instance Firewall Management Center Virtual sur OCI

Vous pouvez vous connecter à une instance en cours d'exécution en utilisant une connexion Secure Shell (SSH).

- La plupart des systèmes de type UNIX incluent un client SSH par défaut.
- Les systèmes Windows 10 et Windows Server 2019 doivent inclure le client OpenSSH, dont vous aurez besoin si vous avez créé votre instance à l'aide des clés SSH générées par Oracle Cloud Infrastructure.
- Pour les autres versions de Windows, vous pouvez télécharger PuTTY, le client SSH gratuit depuis http://www.putty.org.

Prérequis

Vous aurez besoin des renseignements suivants pour vous connecter à l'instance :

- L'adresse IP publique de l'instance. Vous pouvez obtenir l'adresse à partir de la page Instance Details (Détails de l'instance) dans la console. Ouvrez le menu de navigation. Sous **Core Infrastructure** (Infrastructure principale), accédez à **Compute** (Informatique) et cliquez sur **Instances**. Ensuite, sélectionnez votre instance. Vous pouvez également utiliser les opérations ListVnicAttachments et GetVnic de l'API de services principaux.

- Le nom d'utilisateur et le mot de passe de votre instance.
- Le chemin complet vers la partie clé privée de la paire de clés SSH que vous avez utilisée lors du lancement de l'instance.

  Pour en savoir plus sur les paires de clés, consultez Gestion des paires de clés sur les instances Linux.



Remarque Si vous choisissez de ne pas ajouter de configuration Day0, vous pouvez vous connecter à l'instance Firewall Management Center Virtual à l'aide des informations d'authentification par défaut (admin/Admin123).

Vous êtes invité à définir le mot de passe lors de la première tentative de connexion.

Se connecter à l'instance Firewall Management Center Virtual à l'aide de PuTTY

Pour vous connecter à l'instance Firewall Management Center Virtual à l'aide de PuTTY depuis un système Windows :

Procédure

Étape 1 Ouvrez PuTTY.

Étape 2 Dans le volet **Category (catégorie)**, sélectionnez **Session (session)** et saisissez la commande suivante :

- **Host Name (or IP address) (nom d'hôte ou adresse IP non valide)** :

  `<username>@<public-ip-address>`

  Lieu :

  `<nom-utilisateur>` correspond au nom d'utilisateur de l'instance Firewall Management Center Virtual.

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

- **Port:** 22
- **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.

Étape 7 Cliquez sur **Open** (Ouvrir) pour démarrer 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.

Se connecter à l'instance Firewall Management Center Virtual à l'aide de SSH

Pour vous connecter à l'instance Firewall Management Center Virtual 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>
```

Lieu :

`<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 Firewall Management Center Virtual.

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

Se connecter à l'instance Firewall Management Center Virtual à l'aide d'OpenSSH

Pour vous connecter à l'instance Firewall Management Center Virtual 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 **Owner** (Propriétaire) 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>
```

Lieu :

`<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 Firewall Management Center Virtual.

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

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.