

Déployer Firewall Management Center Virtual sur OpenStack

Vous pouvez déployer Firewall Management Center Virtual sur OpenStack.

- Aperçu, à la page 1
- Prérequis, à la page 2
- Lignes directrices et limites relatives à la licence, à la page 3
- Configuration système requise, à la page 3
- Exemple de topologie de réseau, à la page 5
- Déployer Firewall Management Center Virtual, à la page 5

Aperçu

Ce guide décrit comment déployer Firewall Management Center Virtual dans un environnement OpenStack. OpenStack est une plateforme informatique en nuage standard ouverte et gratuite, déployée principalement comme infrastructure en tant que service (IaaS) dans des nuages publics et privés où des serveurs virtuels et d'autres ressources sont mis à la disposition des utilisateurs.

Le 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. Le Firewall Management Center Virtual peut être déployé sur OpenStack. Il peut ensuite être configuré pour gérer les périphériques virtuels et physiques.

Ce déploiement utilise un hyperviseur KVM pour gérer les ressources virtuelles. KVM est une solution de virtualisation complète pour Linux sur du matériel x86 contenant des extensions de virtualisation (comme Intel VT). Il se compose d'un module de noyau chargeable, kvm.ko, qui fournit l'infrastructure de virtualisation de base et d'un module propre au processeur, tel que kvm-intel.ko. Vous pouvez exécuter plusieurs machines virtuelles avec des images de système d'exploitation non modifiées. Chaque machine virtuelle dispose d'un matériel virtualisé privé : une carte réseau, un disque, un adaptateur graphique, etc.

Comme les périphériques sont déjà pris en charge sur l'hyperviseur KVM, aucun progiciel de noyau ou pilote supplémentaire n'est nécessaire pour activer la prise en charge d'OpenStack.

Prérequis

- Téléchargez le fichier qcow2 Firewall Management Center Virtual à partir de software.cisco.com et placez-le sur votre hôte Linux :

  https://software.cisco.com/download/navigator.html

- Un software.cisco.com et un contrat de service Cisco sont nécessaires.
- Firewall Management Center Virtual prend en charge le déploiement sur l'environnement OpenStack à code source libre et l'environnement OpenStack géré par Cisco VIM.

  Configurez l'environnement OpenStack en fonction des lignes directrices OpenStack.

  - Consultez le document OpenStack à code source libre :

    Version de Wallaby - https://docs.openstack.org/project-deploy-guide/openstack-ansible/wallaby/overview.html

  - Consultez le document OpenStack de Cisco Virtualized Infrastructure Manager (VIM) : Cisco Virtualized Infrastructure Manager Documentation, 4.4.3.

- Licences :
  - Vous configurez tous les droits de licence pour les services de sécurité à partir du On-Prem Firewall Management Center.
  - Pour en savoir plus sur la gestion des licences, consultez la section sur les licences pour le système des *Guide de configuration du Secure Firewall Management Center*.
- Exigences en mémoire et en ressources
  - Processeurs
    - Nécessite 4 vCPU ou 8 vCPU
  - Mémoire
    - Minimum requis de 28 Go/ conseillé (par défaut) 32 Go de RAM
  - Stockage de l'hôte par machine virtuelle
    - Firewall Management Center Virtual nécessite 250 Go

Remarque Vous pouvez modifier les valeurs de vCPU et de mémoire selon vos besoins.

- Exigences d'interface :
  - Interface de gestion : une interface utilisée pour connecter le périphérique au On-Prem Firewall Management Center.
- Chemins de communication :

- Adresses IP flottantes pour l'accès à Firewall Management Center Virtual.

- Version Firewall Management Center Virtual minimale prise en charge :
  - Version 7.0
- Pour les exigences d'OpenStack, consultez Configuration système requise, à la page 3.
- Pour la compatibilité de Firewall Management Center Virtual et du système, consultez le guide de compatibilité de Cisco Secure Firewall Threat Defense.

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

Firewall Management Center Virtual sur OpenStack prend en charge les fonctionnalités suivantes :

- Déployez Firewall Management Center Virtual sur l'hyperviseur KVM exécuté sur un nœud de calcul de votre environnement OpenStack.
- Interface de ligne de commande OpenStack
- Déploiement basé sur un modèle Heat
- Licences : seul le protocole BYOL est pris en charge
- Pilotes, VIRTIO

Fonctionnalités non prises en charge

Firewall Management Center Virtual sur OpenStack ne prend pas en charge les éléments suivants :

- Évolutivité automatique
- Grappe

Configuration système requise

L'environnement OpenStack doit être conforme aux exigences matérielles et logicielles prises en charge suivantes.

Tableau 1 : Configuration matérielle et logicielle requise

Type	Versions prises en charge	Notes
Serveur	UCS C240 M5	Il est recommandé de disposer de deux serveurs UCS, un pour le contrôleur OS et un pour le nœud de calcul OS.
Pilote	VIRTIO	Voici les pilotes pris en charge.

Type	Versions prises en charge	Notes
Système d'exploitation	Serveur Ubuntu 20.04	Il s'agit du système d'exploitation recommandé sur les serveurs UCS.
Version OpenStack	Version Wallaby	Des détails sur les différentes versions d'OpenStack sont disponibles à l'adresse suivante : https://releases.openstack.org/

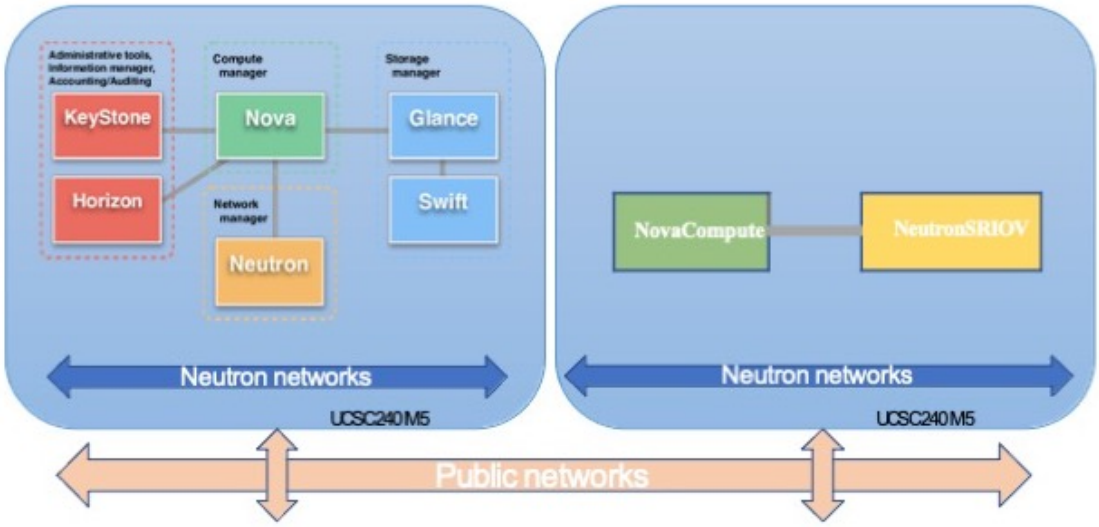
Tableau 2 : Configuration matérielle et logicielle requise pour Cisco VIM Managed OpenStack

Type	Versions prises en charge	Notes
Matériel de serveur	UCS C220-M5/UCS C240-M4	Il est recommandé d'utiliser cinq serveurs UCS, trois pour le contrôleur OS et deux ou plus pour le nœud de calcul du système d'exploitation.
Moteurs	VIRTIO	Voici les pilotes pris en charge.
Version de Cisco VIM	Cisco VIM 4.4.3 Pris en charge par : • Système d'exploitation – Red Hat Enterprise Linux 8.4 • Version d'OpenStack – OpenStack 16.2 (version Train)	Reportez-vous à la documentation de Cisco Virtualized Infrastructure Manager, 4.4.3, pour en savoir plus.

Topologie de la plateforme OpenStack

La figure suivante montre la topologie recommandée pour prendre en charge les déploiements dans OpenStack à l'aide de deux serveurs UCS.

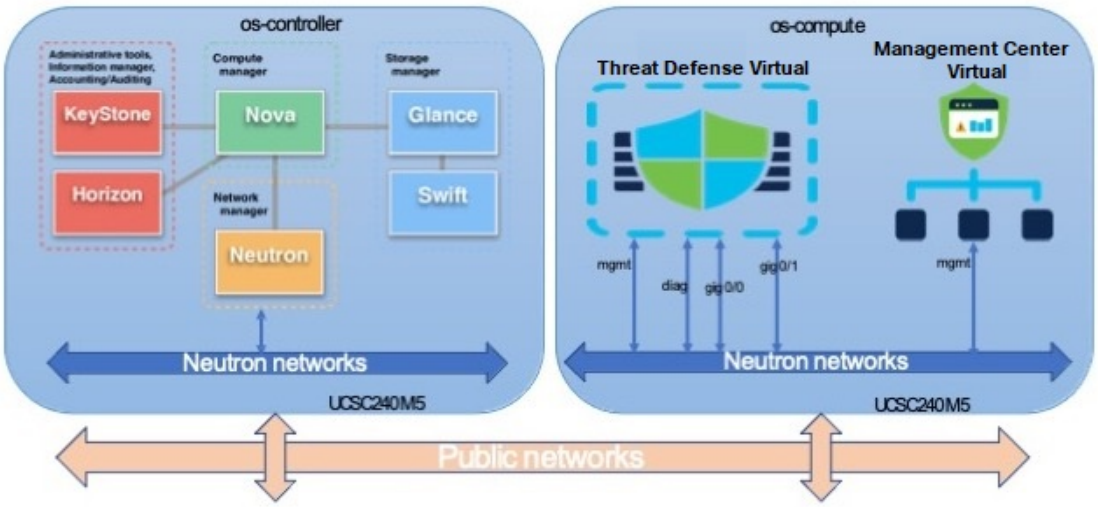
Illustration 1 : Topologie de la plateforme OpenStack



Exemple de topologie de réseau

La figure suivante montre un exemple de topologie du réseau pour le Firewall Management Center Virtual dans OpenStack.

Illustration 2 : Exemple de topologie avec le Firewall Management Center Virtual sur OpenStack



Déployer Firewall Management Center Virtual

Cisco fournit des exemples de modèles Heat pour le déploiement d'Firewall Management Center Virtual. Les étapes de création des ressources d'infrastructure OpenStack sont combinées dans un fichier de modèle Heat

(`deploy_os_infra.uaml`) pour créer des réseaux, des sous-réseaux et des interfaces de routeur. À un niveau supérieur, les étapes de déploiement de Firewall Management Center Virtual sont classées dans les sections suivantes.

- Chargez l'image Firewall Management Center Virtual qcow2 vers le service OpenStack Glance.
- Créez l'infrastructure de réseau.
  - Réseau
  - Sous-réseau
  - Interface du routeur
- Créez l'instance Firewall Management Center Virtual.
  - Saveur
  - Groupes de sécurité
  - IP flottante
  - Instance

Vous pouvez déployer Firewall Management Center Virtual sur OpenStack en utilisant les étapes suivantes.

Charger l'image Firewall Management Center Virtual dans OpenStack

Copiez l'image qcow2 Firewall Management Center Virtual sur le nœud de contrôleur OpenStack, puis chargez l'image sur le service OpenStack Glance.

Avant de commencer

- Téléchargez le fichier qcow2 Firewall Management Center Virtual à partir de Cisco.com et placez-le sur votre hôte Linux :

  https://software.cisco.com/download/navigator.html

Procédure

Étape 1 Copiez le fichier image qcow2 sur le nœud de contrôleur OpenStack.

Étape 2 Chargez l'image Firewall Management Center Virtual sur le service OpenStack Glance.

```
root@ucs-os-controller:$ openstack image create <fmcv_image> --public --disk-
format qcow2 --container-format bare --file ./<fmcv_qcow2_file>
```

Étape 3 Vérifiez si le chargement de l'image Firewall Management Center Virtual est réussi.

root@ucs-os-controller:$ openstack image list

Exemple :

```
root@ucs-os-controller:$ openstack image list
+--------------------------------------+-------------------+---------+
| ID                                   | Name              | Status |+
| b957b5f9-ed1b-4975-b226-4cddf5887991 | fmcv-7-0-image    | active |+
```

L'image chargée et son état sont affichés.

Prochaine étape

Créez l'infrastructure réseau à l'aide du modèle `deploy_os_infra.yaml`.

Créer l'infrastructure réseau pour OpenStack et Firewall Management Center Virtual

Déployez le modèle Heat d'infrastructure OpenStack pour créer l'infrastructure réseau.

Avant de commencer

Les fichiers de modèle Heat sont nécessaires pour créer l'infrastructure réseau et les composants requis pour Firewall Management Center Virtual, tels que la convivialité, les réseaux, les sous-réseaux, les interfaces de routeur et les règles de groupe de sécurité :

- `env.yam` : définit les ressources créées pour prendre en charge Firewall Management Center Virtual sur le noeud de traitement informatique, telles que le nom de l'image, les interfaces et les adresses IP.
- `deploy_os_infra.yml` : définit l'environnement pour le Firewall Management Center Virtual, comme le réseau et les sous-réseaux.

Les modèles pour votre version Firewall Management Center Virtual sont disponibles dans le référentiel GitHub sous FTDv OpenStack heat template (Modèle Heat OpenStack FMCv).



Important Notez que les modèles fournis par Cisco sont fournis à titre d'exemples à code source libre et ne sont pas couverts par la portée normale du centre d'assistance technique Cisco. Vérifiez régulièrement GitHub pour connaître les mises à jour et les instructions ReadMe.

Procédure

Étape 1 Déployez le fichier de modèle Heat d'infrastructure.

root@ucs-os-controller:$ opensstack stack create<stack-name> -e<environment files name> -t<deployment file name>

Exemple :

```
root@ucs-os-controller:$ openstack stack create infra-stack -e env.yaml -t deploy_os_infra.yaml
```

Étape 2 Vérifiez si la pile d'infrastructure est créée avec succès.

root@ucs-os-controller:$ openstack stack list

Exemple :

```
root@ucs-os-controller:$ openstack stack list
+--------------------------------------+------------+----------------------------------+-----------------+
| ID                                   | Stack Name | Project                          | Stack
```

```
Status    |
+--------------------------------------+-------------+----------------------------------+-----------------+
| b30d5875-ce3a-4258-a841-bf2d09275929 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
+--------------------------------------+-------------+----------------------------------+-----------------+
```

Prochaine étape

Créez l'instance Firewall Management Center Virtual sur OpenStack.

Créer l'instance Firewall Management Center Virtual sur OpenStack

Utilisez l'exemple de modèle Heat pour déployer Firewall Management Center Virtual sur OpenStack.

Avant de commencer

Un modèle Heat est requis pour déployer Firewall Management Center Virtual sur OpenStack :

- `deploy_fmcv.yml`

Les modèles pour votre version Firewall Management Center Virtual sont disponibles dans le référentiel GitHub sous FMCv OpenStack heat template.

Important Notez que les modèles fournis par Cisco sont fournis à titre d'exemples à code source libre et ne sont pas couverts par la portée normale du centre d'assistance technique Cisco. Vérifiez régulièrement GitHub pour connaître les mises à jour et les instructions ReadMe.

Procédure

Étape 1 Déployez le fichier de modèle Heat Firewall Management Center Virtual (`deploy_fmcv.yaml`) pour créer l'instance Firewall Management Center Virtual.

root@ucs-os-controller:$ openstack stack create fmcv-stack -e env.yaml-t deploy_fmcv.yaml

Exemple :

```
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| id                  | 96c8c126-107b-4733-8f6c-eb15a637219f |
| stack_name          | fmcv-stack                           |
| description         | FMCv template                        |
| updated_time        | None                                 |
| stack_status        | CREATE_IN_PROGRESS                   |
| stack_status_reason | Stack CREATE started                 |
+---------------------+--------------------------------------+
```

Étape 2 Vérifiez que votre pile Firewall Management Center Virtual est créée avec succès.

root@ucs-os-controller:$ openstack stack list

Exemple :

```
+--------------------------------------+-------------+----------------------------------+--------+
| ID                                   | Stack Name  | Project                          | Stack
Status    |
+--------------------------------------+-------------+----------------------------------+----------------+
| 14624af1-e5fa-4096-bd86-c453bc2928ae | fmcv-stack  | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
| 198336cb-1186-45ab-858f-15ccd3b909c8 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
+--------------------------------------+-------------+----------------------------------+----------------+
```

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.