Déployer Défense contre les menaces virtuelles sur OpenStack

Aperçu

Ce guide décrit comment déployer défense contre les menaces virtuelles 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.

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.

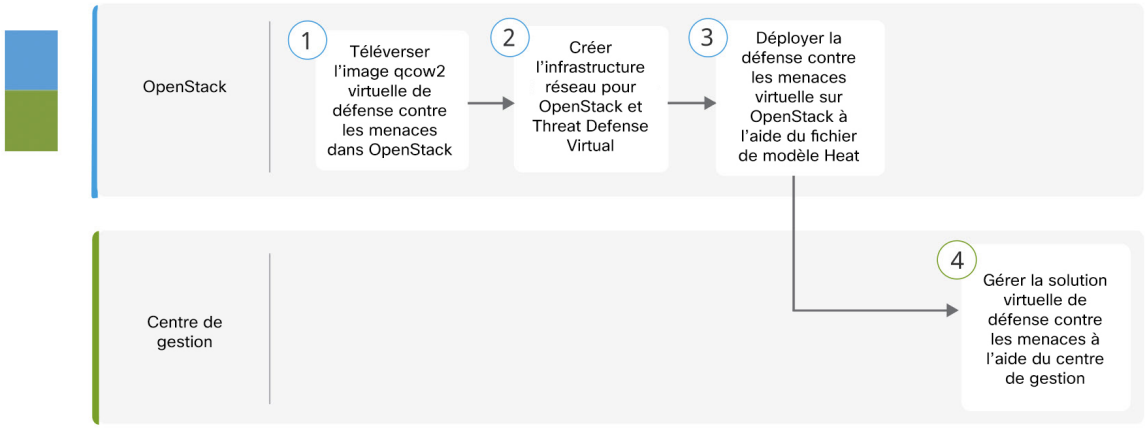
Vous pouvez exécuter plusieurs machines virtuelles avec des images de système d'exploitation non modifiées. Chaque machine virtuelle dispose d'un matériel virtualisé privé : une carte réseau, un disque, un adaptateur graphique, etc.

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.

Remarque Défense contre les menaces virtuelles sur OpenStack peut être installé dans n'importe quel environnement multi-nœuds optimisé.

Procédure de bout en bout

Le diagramme suivant illustre le flux de travail pour le déploiement de Threat Defense Virtual sur OpenStack.



	Espace de travail	Étapes
1	OpenStack	Deployer Threat Defense Virtual sur OpenStack : Téléversez l'image de la solution virtuelle de défense contre les menaces sur OpenStack.
2	OpenStack	Deployer Threat Defense Virtual sur OpenStack : Créez l'infrastructure de réseau pour OpenStack et la solution virtuelle de défense contre les menaces.
3	OpenStack	Déployer Threat Defense Virtual sur OpenStack : Déployez la solution virtuelle de défense contre les menaces sur OpenStack à l'aide du fichier de modèle virtuel Heat de défense contre les menaces.
4	Centre de gestion	Gérer la solution virtuelle de défense contre les menaces à l'aide du centre de gestion

Prérequis

- Obtenez l'image qcow2 défense contre les menaces virtuelles à partir de software.cisco.com.
- Défense contre les menaces virtuelles 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.

- Un compte Cisco Smart. Vous pouvez en créer un sur le Centre des logiciels Cisco.
- 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 sur les licences dans le *Cisco Secure Firewall Management Center Guide d'administration* pour plus d'informations 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 internes et externes : utilisées pour connecter défense contre les menaces virtuelles aux hôtes internes et au réseau public.
- Chemins de communication :
  - Adresses IP flottantes pour l'accès à défense contre les menaces virtuelles.
- Version défense contre les menaces virtuelles minimale prise en charge :
  - Version 7.0
- Pour les exigences d'OpenStack, consultez Configuration système requise, à la page 5.
- 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

défense contre les menaces virtuelles sur OpenStack prend en charge les fonctionnalités suivantes :

- Déploiement d'défense contre les menaces virtuelles sur l'hyperviseur KVM s'exécutant sur un nœud de traitement informatique de votre environnement OpenStack.
- Interface de ligne de commande OpenStack
- Déploiement basé sur un modèle Heat
- Tableau de bord OpenStack Horizon
- Licences : Seul le protocole BYOL est pris en charge
- Gestion de Défense contre les menaces virtuelles à l'aide de centre de gestion seulement.
- Pilotes : virtIO et SR-IOV

Niveaux de performance pour les Licences Smart Défense contre les menaces virtuelles

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 1 : 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	4 cœurs/8 Go	100 Mbit/s	50
FTDv10	4 cœurs/8 Go	1 Gbit/s	250
FTDv20	4 cœurs/8 Go	3 Gbit/s	250
FTDv30	8 cœurs/16 Go	5 Gbit/s	250
FTDv50	12 cœurs/24 Go	10 Gbit/s	750
FTDv100	16 cœurs/32 Go	16 Gbit/s	10 000

Consultez le chapitre sur les licences du *Cisco Secure Firewall Management Center Guide d'administration* pour connaître les consignes relatives à l'octroi de licences pour votre 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 OpenStack 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

défense contre les menaces virtuelles 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 2 : Exigences matérielles et logicielles pour le logiciel libre OpenStack

Type	Versions prises en charge	Notes
Matériel de 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.
Moteurs	VIRTIO, IXGBE et I40E	Voici les pilotes pris en charge.
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/

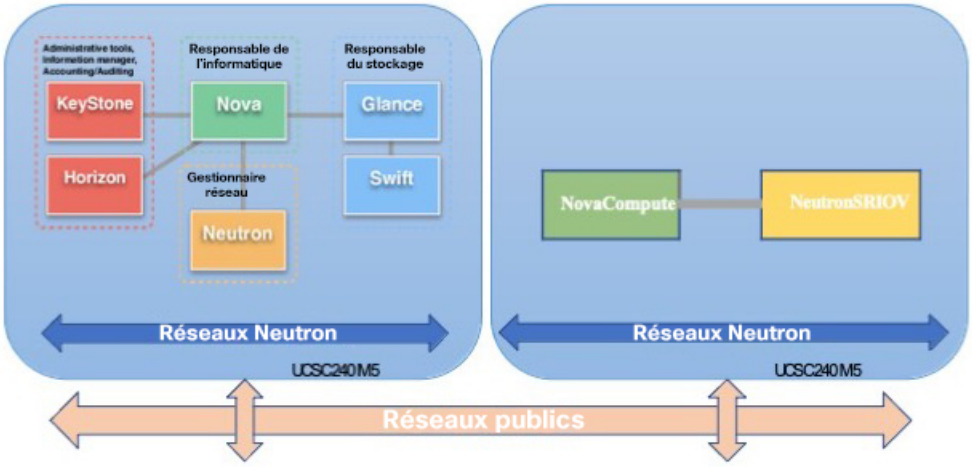
Tableau 3 : Configuration matérielle et logicielle requise pour Cisco VIM Managed OpenStack

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, IXGBE et I40E	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.

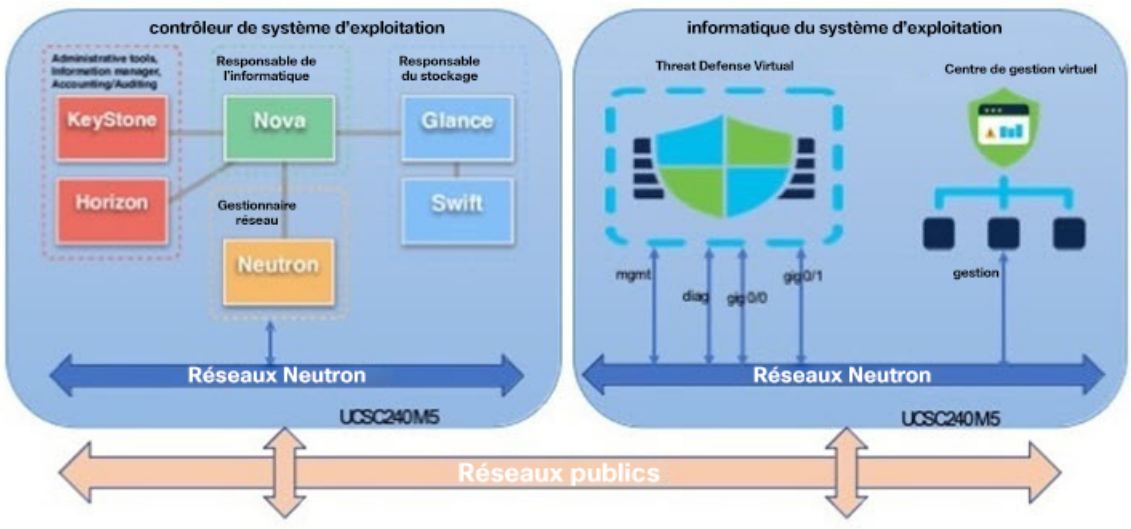
Illustration 1 : Topologie de la plateforme OpenStack



Exemple de topologie de réseau pour Défense contre les menaces virtuelles sur OpenStack

Voici un exemple de topologie de réseau pour défense contre les menaces virtuelles en mode pare-feu routé avec quatre sous-réseaux configurés dans OpenStack pour défense contre les menaces virtuelles (gestion, diagnostic, interne et externe).

Illustration 2 : Exemple de topologie avec Défense contre les menaces virtuelles et Centre de gestion virtuel sur OpenStack



Déployer Défense contre les menaces virtuelles

Cisco fournit des exemples de modèles Heat pour le déploiement de défense contre les menaces virtuelles. 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 défense contre les menaces virtuelles sont classées dans les sections suivantes.

- Chargez l'image défense contre les menaces virtuelles qcow2 vers le service OpenStack Glance.
- Créez l'infrastructure de réseau.
  - Réseau
  - Sous-réseaux
  - Interface du routeur
- Créez l'instance défense contre les menaces virtuelles.
  - Saveur
  - Groupes de sécurité
  - IP flottante
  - Instance

Vous pouvez déployer défense contre les menaces virtuelles sur OpenStack en utilisant les étapes suivantes.

Charger l'image Défense contre les menaces virtuelles dans OpenStack

Copiez l'image qcow2 défense contre les menaces virtuelles sur le nœud de contrôleur OpenStack, puis chargez l'image sur le service OpenStack Glance.

Avant de commencer

Téléchargez le fichier qcow2 défense contre les menaces virtuelles à partir de Cisco.com et placez-le sur votre hôte Linux :

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

Remarque Une connexion à Cisco.com et un contrat de service Cisco sont requis.

Procédure

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

Étape 2 Chargez l'image défense contre les menaces virtuelles sur le service OpenStack Glance.

```
root@ucs-os-controller:$ openstack image create <image_name> --public --disk-
format qcow2 --container-format bare --file ./<ftdv_qcow2_file>
```

Étape 3 Vérifiez si le chargement de l'image défense contre les menaces virtuelles est réussi.

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

Exemple :

```
root@ucs-os-controller:$ openstack image list
+--------------------------------------+-------------------+---------+
| ID                                   | Name              | Status |+
| 06dd7975-0b6e-45b8-810a-4ff98546a39d | ftdv-7-0-image    | active |+
```

L'image téléversée et son état s'affichent.

Prochaine étape

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

Créer l'infrastructure réseau pour OpenStack et Défense contre les menaces virtuelles

Avant de commencer

Les fichiers de modèle Heat sont nécessaires pour créer l'infrastructure réseau et les composants requis pour défense contre les menaces virtuelles, tels que la convivialité, les réseaux, les sous-réseaux, les interfaces de routeur et les règles de groupe de sécurité :

- `deploy_os_infra.yaml`
- `env.yaml`

Les modèles pour votre version défense contre les menaces virtuelles sont disponibles dans le référentiel GitHub sous FTDv 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. Consultez 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

Prochaine étape

Créez l'instance défense contre les menaces virtuelles sur OpenStack.

Déployer Défense contre les menaces virtuelles sur OpenStack

Utilisez l'exemple de modèle Heat défense contre les menaces virtuelles pour déployer défense contre les menaces virtuelles sur OpenStack.

Avant de commencer

Un modèle Heat est requis pour déployer défense contre les menaces virtuelles sur OpenStack :

- `deploy_ftdv.yaml`

Les modèles pour votre version défense contre les menaces virtuelles sont disponibles dans le référentiel GitHub sous FTDv 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. Consultez régulièrement GitHub pour connaître les mises à jour et les instructions ReadMe.

Procédure

Étape 1 Déployez le fichier de modèle Heat défense contre les menaces virtuelles (`deploy_ftdv.yaml`) pour créer l'instance défense contre les menaces virtuelles.

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

Exemple :

Déployer Défense contre les menaces virtuelles sur OpenStack

```
+---------------------+------------------------------+
| Field               | Value                        |
+---------------------+------------------------------+
| id                  | 14624af1-e5fa-4096-bd86-c453bc2928ae |
| stack_name          | ftdv-stack                   |
| description         | FTDvtemplate                 |
| updated_time        | None                         |
| stack_status        | CREATE_IN_PROGRESS           |
| stack_status_reason | Stack CREATE started         |
+---------------------+------------------------------+
```

Étape 2 Vérifiez que votre pile défense contre les menaces virtuelles est créée avec succès.

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

Exemple :

```
+--------------------------------------+-------------+----------------------------------+--------+
| ID                                   | Stack Name  | Project                          | Stack
Status    |
+--------------------------------------+-------------+----------------------------------+--------+
| 14624af1-e5fa-4096-bd86-c453bc2928ae | ftdv-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.