Déployer Défense contre les menaces virtuelles sur Nutanix

Ce chapitre décrit la marche à suivre pour déployer défense contre les menaces virtuelles dans un environnement Nutanix.

Aperçu

Cisco Cisco Secure Firewall Threat Defense Virtual (anciennement Firepower Threat Defense Virtual) apporte la fonctionnalité de pare-feu sécurisé de Cisco à des environnements virtualisés, ce qui permet à des politiques de sécurité cohérentes de faire le suivi des charges de travail dans vos environnements physiques, virtuels et en nuage, et entre les nuages.

Ce chapitre décrit comment le défense contre les menaces virtuelles fonctionne dans l'environnement Nutanix avec l'hyperviseur AHV, y compris la prise en charge des fonctionnalités, les exigences du système, les directives et les limites. Ce chapitre décrit également vos options pour la gestion de défense contre les menaces virtuelles.

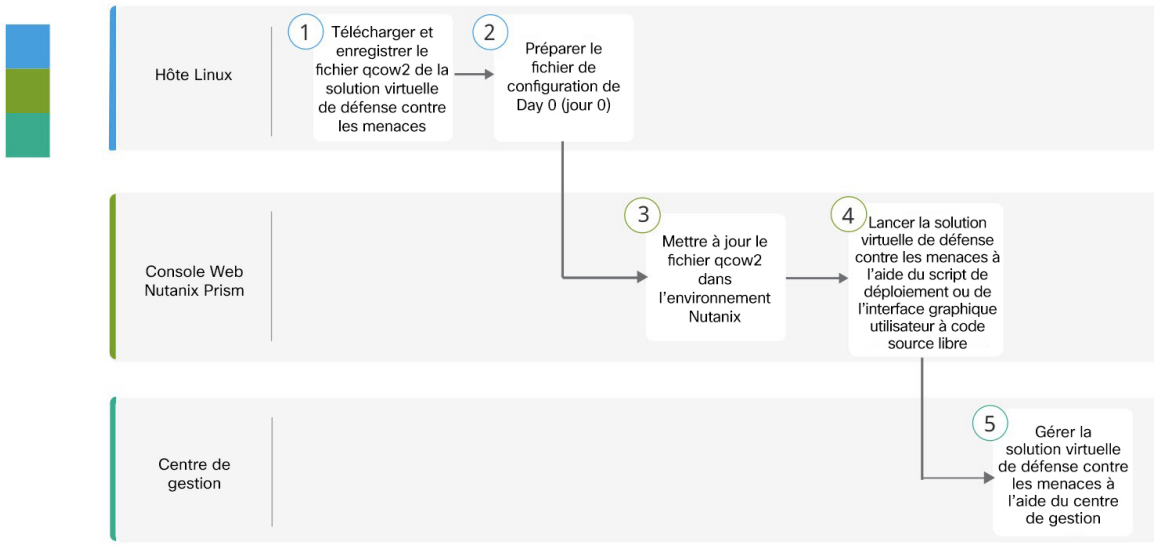
Il est important que vous compreniez vos options de gestion avant de commencer votre déploiement. Vous pouvez gérer et surveiller défense contre les menaces virtuelles à l'aide de Cisco Secure Firewall Management Center. (anciennement Cisco Firepower Management Center)

À propos du déploiement de Défense contre les menaces virtuelles sur Nutanix

La plateforme infonuagique de Nutanix Enterprise est un système convergé et évolutif de traitement informatique et de stockage conçu pour héberger et stocker des machines virtuelles. Vous pouvez exécuter plusieurs machines virtuelles avec des images de système d'exploitation non modifiées de défense contre les menaces virtuelles à l'aide de Nutanix AHV. Chaque machine virtuelle dispose d'un matériel virtualisé privé : une carte réseau, un disque, un adaptateur graphique, etc.

Procédure de bout en bout

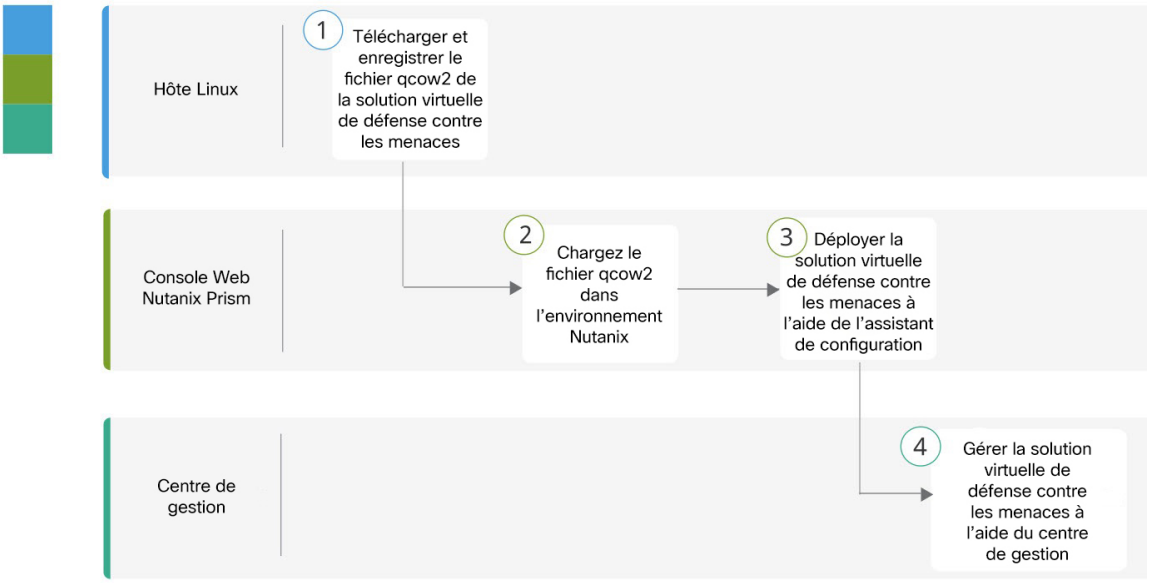
Le diagramme suivant illustre le flux de travail pour le déploiement de Threat Defense Virtual sur la plateforme Nutanix avec le fichier de configuration de Jour 0 (Day-0).



	Espace de travail	Étapes
1	Hôte Linux	Déployez Threat Defense Virtual sur Nutanix : téléchargez et enregistrez le fichier Threat Defense Virtual qcow2.
2	Hôte Linux	Déployez Threat Defense Virtual sur Nutanix : téléversez le fichier qcow2 dans l'environnement Nutanix.
3	Console Web Nutanix Prism	Déployez Threat Defense Virtual sur Nutanix: préparez le fichier de configuration de Jour 0 **fichier texte** > **Saisissez les détails de la configuration** > **Save as day0-config.txt**.
4	Console Web Nutanix Prism	Déployez le Threat Defense Virtual sur Nutanix : déployez le Threat Defense Virtual sur Nutanix.

	Espace de travail	Étapes
5	Centre de gestion	Gérer Threat Defense Virtual : • À l'aide du centre de gestion

Le diagramme suivant illustre le flux de travail pour le déploiement de Threat Defense Virtual sur la plateforme Nutanix sans le fichier de configuration de Jour 0 (Day-0).



	Espace de travail	Étapes
1	Hôte Linux	Déployez Threat Defense Virtual sur Nutanix : téléchargez et enregistrez le fichier Threat Defense Virtual qcow2.
2	Console Web Nutanix Prism	Déployez Threat Defense Virtual sur Nutanix : téléversez le fichier qcow2 dans l'environnement Nutanix.
3	Console Web Nutanix Prism	Déployez le Threat Defense Virtual sur Nutanix : déployez le Threat Defense Virtual sur Nutanix.
4	Centre de gestion	Gérer Threat Defense Virtual : • À l'aide du centre de gestion

Configuration système requise

Versions

Version du gestionnaire	Version de l'appareil
Centre de gestion 7.0	Défense contre les menaces 7.0

Consultez le guide de compatibilité de Cisco Secure Firewall Threat Defense pour obtenir les informations les plus récentes sur la prise en charge de l'hyperviseur pour défense contre les menaces virtuelles.

Défense contre les menaces virtuelles mémoire, vCPU et taille du disque

Le matériel spécifique utilisé pour les déploiements défense contre les menaces virtuelles peut varier en fonction du nombre d'instances déployées et des exigences d'utilisation. Chaque instance de défense contre les menaces virtuelles nécessite une allocation minimale de ressources (quantité de mémoire, nombre de CPU et espace disque) sur le serveur.

Paramètres	Valeur
Niveaux de performance	**Version 7.0 ou ultérieure** 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. • FTDv5 4vCPU/8Go (100 Mbit/s) • FTDv10 4 vCPU/8 Go (1 Gbit/s) • FTDv20 4vCPU/8 Go (3 Gbit/s) • FTDv30 8 vCPU/16 Go (5 Gbit/s) • FTDv50 12 vCPU/24 Go (10 Gbit/s) • FTDv100 16vCPU/32 Go (16 Gbit/s) Consultez le chapitre sur l'octroi de licences pour le système des documents *Configuration du centre de gestion Secure Firewall Management Center Configuration* et pour obtenir des instructions relatives à la licence de 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.
Stockage	50 Go (réglable) • Prend en charge les périphériques Virtio Block

Remarque Le nombre minimal de réseaux pour le défense contre les menaces virtuelles s'établit à quatre interfaces de données (gestion, diagnostic, externe et interne).

Licences Défense contre les menaces virtuelles

- Configurez tous les droits de licence pour les services de sécurité à partir de la centre de gestion.
- Pour en savoir plus sur la gestion des licences, consultez la section sur *les licences pour le système* du Guide de configuration du centre de gestion Cisco Secure Firewall Management Center.

Composants et versions de Nutanix

Composant	Version
Système d'exploitation Nutanix Acropolis (AOS)	5.15.5 LTS ou version ultérieure
Nutanix Cluster Check (NCC)	4.0.0.1
Nutanix AHV	20201105.12 et version ultérieure
Console Web Nutanix Prism	-

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

- Modes de déploiement : routage (autonome), routage (HA), dérivateur en ligne, En ligne, passif et transparent
- BYOL avec licence uniquement
- IPv6
- Haute accessibilité en natif Défense contre les menaces virtuelles
- Bâtis grand format
- virtio

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 Réglage et optimisation de la virtualisation sur Nutanix 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 Nutanix AHV ne prend pas en charge l'enfichage à chaud de l'interface. N'essayez pas d'ajouter ou de supprimer une interface lorsque le défense contre les menaces virtuelles est sous tension.
- Nutanix AHV ne prend pas en charge SR-IOV ou DPDK-OVS.

Remarque Nutanix AHV prend en charge DPDK sur invité à l'aide de VirtIO. Pour en savoir plus, consulter Prise en charge de DPDK sur AHV.

Lignes directrices générales

- Nécessite deux interfaces de gestion et deux interfaces de données pour le démarrage. Prend en charge un total de 11 interfaces.

Remarque

- La configuration par défaut défense contre les menaces virtuelles place l'interface de gestion, l'interface de dépistage et l'interface interne sur le même sous-réseau.
- Lorsque vous modifiez les interfaces réseau, vous devez désactiver le périphérique défense contre les menaces virtuelles.

- La configuration par défaut de défense contre les menaces virtuelles suppose que vous placiez les interfaces de gestion (gestion et de dépistage) et interne sur le **même sous-réseau** et que l'adresse de gestion utilise l'adresse interne comme passerelle vers Internet (en passant par l'interface externe).
- Le défense contre les menaces virtuelles doit être sous tension sur Firstboot avec au moins quatre interfaces. Votre système ne sera pas déployé sans quatre interfaces.
- Le défense contre les menaces virtuelles prend en charge un total de 10 interfaces : une interface de gestion, une interface de diagnostic et un maximum de 9 interfaces réseau pour le trafic de données. Les affectations interface-réseau doivent être ordonnées comme suit :
  1. Interface de gestion (obligatoire)
  2. Interface de diagnostic (obligatoire)

3. Interface externe (obligatoire)
4. Interface interne (obligatoire)
5. 5 à 11 interfaces de données (facultatives)

Remarque Le nombre minimal de réseaux pour le défense contre les menaces virtuelles est de quatre interfaces de données.

- Pour l'accès depuis la console, le serveur de terminaux est pris en charge par Telnet.
- Voici les paramètres de mémoire et de vCPU pris en charge :

CPU	Mémoire	Taille de la plateforme Défense contre les menaces virtuelles
4	8 Go	4vCPU/8 Go (par défaut)
8	16 Go	8vCPU/16 Go
12	24 Go	12vCPU/24 Go
16	32 Go	16vCPU/32 Go

- Consultez la concordance suivante concernant l'adaptateur réseau, les réseaux sources et les réseaux de destination pour les interfaces défense contre les menaces virtuelles :

Adaptateur réseau	Réseau source	Réseau de destination	Fonction
vnic0*	Gestion 0-0	Gestion 0/0	Gestion
vnic1	Diagnostic	Diagnostic	Diagnostic
vnic2*	GigabitEthernet 0-0	GigabitEthernet 0/0	Externe
vnic3*	GigabitEthernet 0-1	GigabitEthernet 0/1	Interne
*Rattacher au même sous-réseau.			

Documentation associée

- Notes de version Nutanix
- Guide d'installation de terrain Nutanix
- Support matériel sur Nutanix

Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual

Vous pouvez gérer votre appareil Cisco Secure Firewall Threat Defense Virtual en utilisant les éléments suivants :

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.

Conditions préalables au déploiement sur Nutanix

- Téléchargez le fichier disque qcow2 Défense contre les menaces virtuelles à partir de Cisco.com : https://software.cisco.com/download/navigator.html

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

- Passez en revue le chapitre Aperçu, à la page 1.
- Pour la compatibilité de Nutanix et du système, consultez le Guide de compatibilité de Cisco Secure Firewall Threat Defense .

Comment déployer Défense contre les menaces virtuelles sur Nutanix

Étape	Tâche	Autres renseignements
1	Passez en revue les conditions préalables.	Conditions préalables au déploiement sur Nutanix, à la page 8
2	Chargez le fichier qcow2 défense contre les menaces virtuelles dans l'environnement Nutanix.	Charger le fichier QCOW2 Défense contre les menaces virtuelles dans Nutanix, à la page 9
3	(Facultatif) Préparez un fichier de configuration Day 0 (jour 0) qui contient les données de configuration initiale qui sont appliquées au moment du déploiement d'une machine virtuelle.	Préparer le fichier de configuration Day 0 (jour 0), à la page 9
4	Déployez défense contre les menaces virtuelles dans l'environnement Nutanix.	Déployer Défense contre les menaces virtuelles, à la page 11

Étape	Tâche	Autres renseignements
5	(Facultatif) Si vous n'avez pas utilisé de fichier de configuration de jour 0 pour configurer défense contre les menaces virtuelles, terminez la configuration en vous connectant à l'interface de ligne de commande.	Terminez l'assistant de Défense contre les menaces virtuelles, à la page 13

Charger le fichier QCOW2 Défense contre les menaces virtuelles dans Nutanix

Pour déployer défense contre les menaces virtuelles dans l'environnement Nutanix, vous devez créer une image à partir du fichier disque qcow2 défense contre les menaces virtuelles dans la console Web Prism.

Avant de commencer

Téléchargez le fichier disque qcow2 défense contre les menaces virtuelles à partir de Cisco.com : https://software.cisco.com/download/navigator.html

Procédure

Étape 1 Connectez-vous à la console Web Nutanix Prism.

Étape 2 Cliquez sur l'icône en forme d'engrenage pour ouvrir la page **Settings** (paramètres).

Étape 3 Cliquez sur **Image Configuration** (configuration de l'image) dans le volet gauche.

Étape 4 Cliquez sur **Upload Image** (charger une image).

Étape 5 Créez l'image.

1. Saisissez un nom pour l'image.
2. Dans la liste déroulante **Image Type** (type d'image), sélectionnez **DISK** (disque).
3. Dans la liste déroulante **Storage Container** (conteneur de stockage), choisissez le conteneur souhaité.
4. Précisez l'emplacement du fichier disque qcow2 défense contre les menaces virtuelles.

   Vous pouvez soit préciser une URL (pour importer le fichier à partir d'un serveur Web), soit charger le fichier à partir de votre ordinateur.
5. Cliquez sur **Save** (enregistrer).

Étape 6 Attendez que la nouvelle image s'affiche dans la page **Image Configuration** (configuration d'image).

Préparer le fichier de configuration Day 0 (jour 0)

Vous pouvez préparer un fichier de configuration pour le jour 0 avant de déployer défense contre les menaces virtuelles. Ce fichier est un fichier texte qui contient les données de configuration initiale appliquées lors du déploiement d'une machine virtuelle.

À retenir :

- Si vous effectuez le déploiement avec un fichier de configuration Day0 (Jour0), le processus vous permet d'effectuer la configuration initiale complète de l'appareil défense contre les menaces virtuelles.
- Si vous déployez sans fichier de configuration de jour 0, vous devez configurer les paramètres requis par le système après le lancement; consultez Terminez l'assistant de Défense contre les menaces virtuelles, à la page 13 pour de plus amples renseignements.

Vous pouvez préciser :

- L'adhésion au Contrat de licence de l'utilisateur final (CLUF).
- Un nom d'hôte pour le système.
- Un nouveau mot de passe d'administrateur pour le compte admin.
- Le mode de pare-feu initial; définit le mode de pare-feu initial, **routed** (avec routage) ou **transparent**.

  Si vous prévoyez de gérer votre déploiement à l'aide du gestionnaire d'appareil local, vous ne pouvez saisir que **routed** (avec routage) pour le mode de pare-feu. Vous ne pouvez pas configurer des interfaces en mode pare-feu transparent à l'aide du gestionnaire d'appareil.
- Le mode de gestion; voir Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual.

  Saisissez les informations pour les champs centre de gestion (**FmcIp**, **FmcRegKey**et **FmcNatId**).
- Paramètres réseau qui permettent à l'appareil de communiquer sur votre réseau de gestion.

Procédure

Étape 1 Créez un nouveau fichier texte à l'aide d'un éditeur de texte de votre choix.

Étape 2 Saisissez les détails de la configuration dans le fichier texte, comme illustré dans l'exemple suivant :

Exemple :

```
#Firepower Threat Defense
{
    "EULA": "accept",
    "Hostname": "ftdv-production",
    "AdminPassword": "Admin123",
    "FirewallMode": "routed",
    "DNS1": "1.1.1.1",
    "DNS2": "1.1.1.2",
    "DNS3": "",
    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.44",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "disabled",
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
    "FmcIp": "",
    "FmcRegKey": "",
    "FmcNatId": "",
    "ManageLocally":"No"
}
```

Remarque
Le contenu du fichier de configuration Day0 (Jour 0) doit être au format JSON. Vous devez valider le texte à l'aide d'un outil de validation JSON.

Étape 3 Enregistrez le fichier sous le nom « **day0-config.txt** ».

Étape 4 Répétez les étapes 1 à 3 pour créer des fichiers de configuration par défaut uniques pour chaque défense contre les menaces virtuelles que vous souhaitez déployer.

Déployer Défense contre les menaces virtuelles

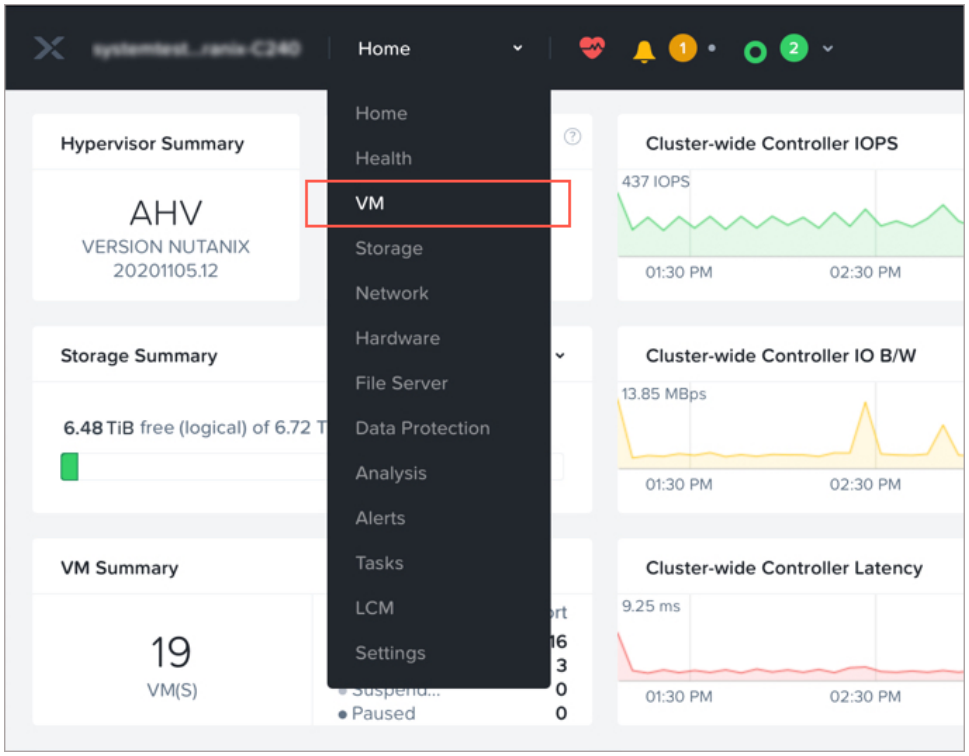
Avant de commencer

Assurez-vous que l'image de défense contre les menaces virtuelles que vous prévoyez de déployer apparaît sur la page **Image Configuration** (configuration de l'image).

Procédure

Étape 1 Connectez-vous à la console Web Nutanix Prism.

Étape 2 Dans la barre de menu principale, cliquez sur la liste déroulante d'affichage et sélectionnez **VM** (machine virtuelle).



Étape 3 Dans le tableau de bord de la VM, cliquez sur **Create VM** (créer une machine virtuelle).

Étape 4 Procédez comme suit :

1. Saisissez un nom pour l'instance défense contre les menaces virtuelles.
2. Vous pouvez choisir de saisir une description pour l'instance défense contre les menaces virtuelles.
3. Sélectionnez le fuseau horaire que vous souhaitez que l'instance défense contre les menaces virtuelles utilise.

Étape 5 Entrez les détails du calcul.

1. Saisissez le nombre de CPU virtuels à allouer à l'instance défense contre les menaces virtuelles.
2. Saisissez le nombre de cœurs qui doivent être affectés à chaque CPU virtuel.
3. Saisissez la quantité de mémoire (en Go) à allouer à l'instance défense contre les menaces virtuelles.

Étape 6 Associez un disque à l'instance défense contre les menaces virtuelles.

1. Sous **Disks** (disques), cliquez sur **Add New Disk** (ajouter un nouveau disque).
2. Dans la liste déroulante **Type**, choisissez **DISK** (DISQUE).
3. Dans la liste déroulante **Operation** (opération), choisissez **Clone from Image Service** (cloner à partir du service d'image).
4. Dans la liste déroulante **Bus Type** (Type de bus), choisissez **PCI** ou **SCSI**
5. Dans la liste déroulante **Image**, choisissez l'image que vous souhaitez utiliser.
6. Cliquez sur **Add** (ajouter).

Étape 7 Configurez au moins quatre interfaces de réseau virtuel.

Sous **Network Adapters (NIC)**, cliquez sur **Add New NIC** (ajouter une nouvelle carte réseau), sélectionnez un réseau et cliquez sur **Add** (ajouter).

Répétez ce processus pour ajouter d'autres interfaces réseau.

défense contre les menaces virtuelles sur Nutanix prend en charge un total de 11 interfaces : une interface de gestion, une interface de diagnostic et un maximum de neuf interfaces réseau pour le trafic de données. Les affectations interface-réseau doivent être ordonnées comme suit :

- vnic0 : interface de gestion (obligatoire)
- vNIC1 : interface de diagnostic (requise)
- vnic2 : interface externe (obligatoire)
- vnic3 : interface interne (obligatoire)
- vNIC4-10 : interfaces de données (facultatif)

Étape 8 Configurez la politique d'affinité pour le défense contre les menaces virtuelles.

Sous **VM Host Affinity** (affinité d'hôte VM), cliquez sur **Set Affinity** (définir l'affinité), sélectionnez les hôtes et cliquez sur **Save** (enregistrer).

Sélectionnez plusieurs hôtes pour vous assurer que défense contre les menaces virtuelles peut être exécuté même en cas de défaillance de nœud.

Étape 9 Si vous avez préparé un fichier de configuration Day 0 (Jour 0), procédez comme suit :

1. Sélectionnez **Custom Script** (script personnalisé).
2. Cliquez sur **Upload A File** (charger un fichier) et sélectionnez le fichier de configuration Day 0 (Jour 0) (**day0-config.txt**).

Remarque
Toutes les autres options de scripts personnalisés ne sont pas prises en charge dans la version.

Étape 10 Cliquez sur **Save** (Eeregistrer) pour déployer défense contre les menaces virtuelles. L'instance défense contre les menaces virtuelles apparaît dans la vue du tableau de la machine virtuelle.

Étape 11 Dans la vue du tableau la machine virtuelle, sélectionnez l'instance défense contre les menaces virtuelles nouvellement créée, et cliquez sur **Power On** (démarrer).

Prochaine étape

- Si vous avez utilisé un fichier de configuration de jour 0 pour configurer le défense contre les menaces virtuelles, vos prochaines étapes dépendent du mode de gestion que vous avez choisi.
  - Si vous avez choisi **No** (non) pour **ManageLocally**, vous utiliserez le centre de gestion pour gérer votre défense contre les menaces virtuelles; voir Gestion de Cisco Secure Firewall Threat Defense Virtual avec Cisco Secure Firewall Management Center.
- Si vous n'avez pas utilisé de fichier de configuration de jour 0 pour configurer défense contre les menaces virtuelles, terminez la configuration de défense contre les menaces virtuelles en vous connectant à l'interface de ligne de commande. Pour plus d'informations sur les instructions, consultez Terminez l'assistant de Défense contre les menaces virtuelles, à la page 13

Terminez l'assistant de Défense contre les menaces virtuelles

Étant donné que les appareils défense contre les menaces virtuelles n'ont pas d'interface Web , vous devez configurer un périphérique virtuel à l'aide de l'interface de ligne de commande si vous avez effectué un déploiement sans fichier de configuration Day 0 (jour 0).

Procédure

Étape 1 Établissez une connexion console avec défense contre les menaces virtuelles.

Étape 2 À l'invite **firepower login** (connexion à Firepower), connectez-vous avec les identifiants par défaut : *admin* comme **username** (nom d'utilisateur) et *Admin123* comme **password** (mot de passe).

Étape 3 Lorsque le système défense contre les menaces virtuelles démarre, un assistant de configuration vous demande les informations suivantes pour configurer le système :

- Accepter le CLUF
- Nouveau mot de passe de l'administrateur
- Configuration IPv4 ou IPv6
- Paramètres DHCP IPv4 ou IPv6

- Adresse IPv4 et filtre d'adresse locale du port de gestion, ou adresse et préfixe IPv6.
- Nom du système
- Passerelle par défaut
- Configuration DNS
- Proxy HTTP
- Mode gestion

Étape 4 Passez en revue les paramètres de l'assistant de configuration. Les valeurs par défaut ou les valeurs saisies précédemment apparaissent entre parenthèses. Pour accepter les valeurs saisies précédemment, appuyez sur la touche **Enter** (Entrée).

Étape 5 Terminez la configuration du système en suivant les invites.

Étape 6 Vérifiez que la configuration a été établie lorsque la console revient à l'invite #.

Étape 7 Fermez l'interface de ligne de commande.

Prochaine étape

Vos prochaines étapes dépendent du mode de gestion que vous avez choisi.

- Si vous avez sélectionné **No** (non) pour **Enable Local Manager** (activer le gestionnaire local), vous utiliserez centre de gestion pour gérer défense contre les menaces virtuelles; à ce sujet, consultez Gestion de Cisco Secure Firewall Threat Defense Virtual avec Cisco Secure Firewall Management Center.

Consultez Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual pour savoir comment choisir votre option de gestion.

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.