Déployer Firewall Management Center Virtual sur Nutanix

Nutanix AHV est un hyperviseur système d'exploitation natif de type 1, une infrastructure hyperconvergée HCI offrant des fonctionnalités activées pour le nuage.

Ce chapitre décrit comment le Firewall Management Center Virtual 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.

Vous pouvez déployer le Firewall Management Center Virtual sur Nutanix AHV.

Configuration système requise

Nous vous recommandons de ne pas diminuer les paramètres par défaut : 32 Go de RAM pour la plupart des instances Firewall Management Center Virtual, 64 Go pour 300 (VMware uniquement). Pour améliorer les performances, vous pouvez augmenter la mémoire et le nombre de processeurs d'une appliance virtuelle, en fonction de vos ressources disponibles.

Exigences en mémoire et en ressources

- Vous pouvez exécuter plusieurs machines virtuelles avec des images de système d'exploitation non modifiées à l'aide de Nutanix AHV. Chaque machine virtuelle dispose d'un matériel virtualisé privé : une carte réseau, un disque, un adaptateur graphique, etc. Consultez les guide de compatibilité de Cisco Secure Firewall Threat Defense .
- Consultez les dernières notes de version pour savoir si une nouvelle version affecte votre environnement. Vous devrez peut-être augmenter les ressources pour déployer la dernière version.
- Le matériel spécifique utilisé pour les déploiements Firewall Management Center Virtual peut varier en fonction du nombre d'instances déployées et des exigences d'utilisation. Chaque appliance virtuelle que vous créez nécessite une allocation minimale de ressources (mémoire, nombre de CPU et espace disque) sur la machine hôte.

- La liste suivante répertorie les paramètres par défaut et recommandés pour l'appareil Firewall Management Center Virtual surNutanix AHV :
- Processeurs
  - Nécessite 4 vCPU
- Mémoire
  - Minimum requis de 28 Go/ conseillé (par défaut) 32 Go de RAM

Important La plateforme Firewall Management Center Virtual échoue si vous allouez moins de 28 Go de RAM à l'appliance virtuelle.

- Mise en réseau
  - Prend en charge les pilotes virtIO.
  - Prend en charge une interface de gestion
- Stockage de l'hôte par machine virtuelle
  - Le Firewall Management Center Virtual nécessite 250 Go
  - Prend en charge les périphériques Virtio Block et SCSI
- Console
  - Prend en charge un serveur terminal via Telnet.

Prérequis

Versions

Version du gestionnaire	Version de l'appareil
Firewall Device Manager 7.0	Firewall Threat Defense 7.0
On-Prem Firewall Management Center 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 Firewall Threat Defense Virtual.

Téléchargez le fichier qcow2 On-Prem Firewall Management Center à partir de Cisco.com et placez-le sur votre console Nutanix Prism Web :

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

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

Licences Firewall Management Center Virtual

- Configurez tous les droits de licence pour les services de sécurité à partir de la 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 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

Mode de déploiement – autonome

Fonctionnalités non prises en charge

Les périphériques Firewall Management Center Virtual n'ont pas de numéros de série. La page **System (Système** > **Configuration** affiche soit **None** (Aucun) soit **Not Specified** (Non précisé) selon la plateforme virtuelle.

- Les hyperviseurs imbriqués (Nutanix AHV s'exécutant sur ESXi) ne sont pas pris en charge. Seuls les déploiements de grappe autonome Nutanix sont pris en charge.
- La haute disponibilité n'est pas prise en charge.
- Nutanix AHV ne prend pas en charge SR-IOV ou DPDK-OVS.

Documentation associée

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

Déployer Firewall Management Center Virtual

Étape	Tâche	Autres renseignements
1	Passez en revue les conditions préalables.	Prérequis, à la page 2
2	Chargez le fichier qcow2 Firewall Management Center Virtual dans l'environnement Nutanix.	Charger le fichier QCOW2 Firewall Management Center Virtual dans Nutanix, à la page 4
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 5
4	Déployez Firewall Management Center Virtual dans l'environnement Nutanix.	Déployer Management Center Virtual sur Nutanix
5	(Facultatif) Si vous n'avez pas utilisé de fichier de configuration de jour 0 pour configurer Firewall Management Center Virtual, terminez la configuration en vous connectant à l'interface de ligne de commande.	Terminer l'assistant de Firewall Management Center Virtual, à la page 9

Charger le fichier QCOW2 Firewall Management Center Virtual dans Nutanix

Pour déployer Firewall Management Center Virtual dans l'environnement Nutanix, vous devez créer une image à partir du fichier disque qcow2 Firewall Management Center Virtual dans la console Web Prism.

Avant de commencer

Téléchargez le fichier disque qcow2 Firewall Management Center Virtual 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 Firewall Management Center Virtual.

   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 Firewall Management Center Virtual. 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 Firewall Management Center Virtual.
- Si vous déployez sans fichier de configuration de jour 0, vous devez configurer les paramètres requis par le système après le lancement; consultez Terminer l'assistant de Firewall Management Center Virtual, à la page 9 pour de plus amples renseignements.

Vous pouvez spécifier :

- 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.
- 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 : Notez que le texte est au format JSON. Vous pouvez valider le texte à l'aide d'un outil de validation avant de copier le texte.

Exemple :

```
#FMC
{
    "EULA": "accept",
    "Hostname": "FMC-Production",
    "AdminPassword": "Admin123",
    "DNS1": "10.1.1.5",
    "DNS2": "192.168.1.67",
    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.45",
    "IPv4Mask": "255.255.0.0",
```

```
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "disabled",
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
}
```

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 Firewall Management Center Virtual que vous souhaitez déployer.

Déployer le Firewall Management Center Virtual sur Nutanix

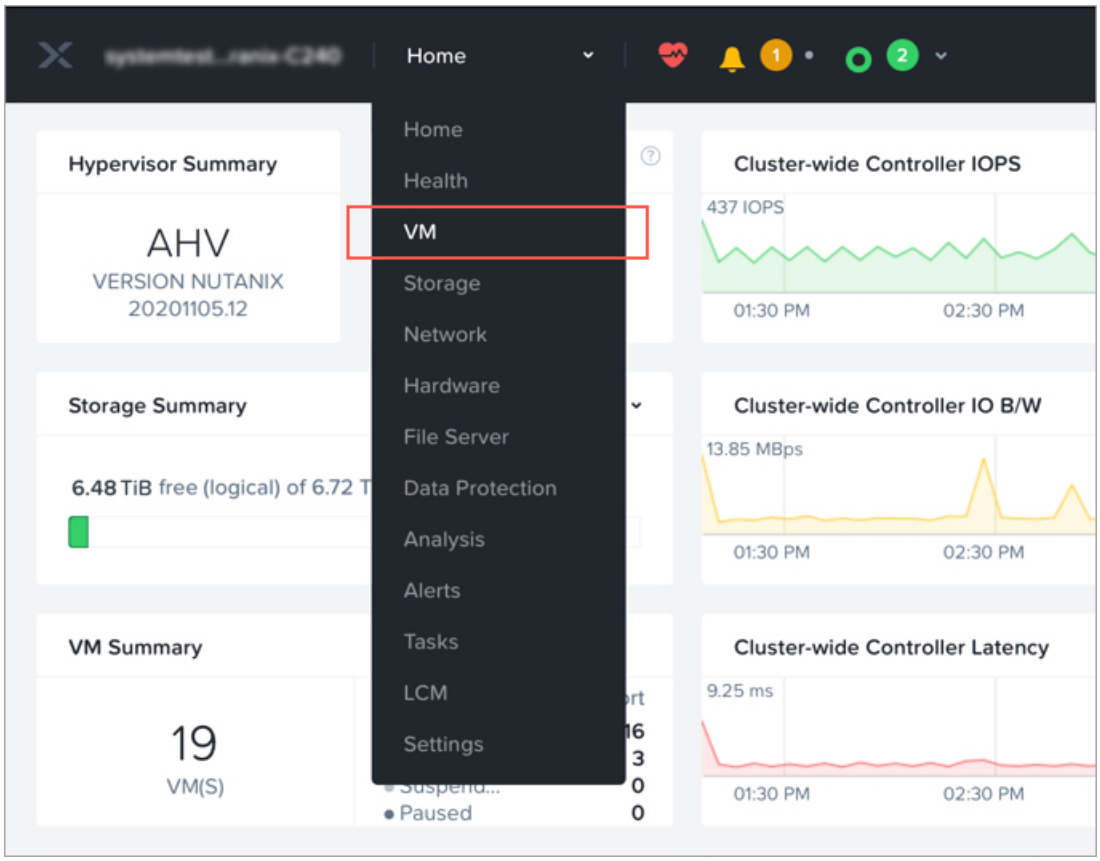
Avant de commencer

Assurez-vous que l'image de Firewall Management Center Virtual 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 Firewall Management Center Virtual.
2. Vous pouvez choisir de saisir une description pour l'instance Firewall Management Center Virtual.
3. Sélectionnez le fuseau horaire que vous souhaitez que l'instance Firewall Management Center Virtual utilise.

Étape 5 Entrez les détails du calcul.

1. Saisissez le nombre de CPU virtuels à allouer à l'instance Firewall Management Center Virtual.
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 Firewall Management Center Virtual.

Étape 6 Associez un disque à l'instance Firewall Management Center Virtual.

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 **SCSI**, **PCI**, ou **SATA**.

5. Dans la liste déroulante **Image**, choisissez l'image que vous souhaitez utiliser.
6. Cliquez sur **Add** (ajouter).

Étape 7 Sous **Network Adapters (NIC)**, cliquez sur **Add New NIC** (ajouter une nouvelle carte réseau), sélectionnez un réseau et cliquez sur **Add** (ajouter).

Étape 8 Configurez la politique d'affinité pour le Firewall Management Center Virtual.

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 Firewall Management Center Virtual 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 Firewall Management Center Virtual. L'instance Firewall Management Center Virtual apparaît dans la vue du tableau de la machine virtuelle.

Étape 11 Créez et associez un port série virtuel au Management Center Virtual. Pour le faire, connectez-vous à une machine virtuelle de contrôleur Nutanix (CVM) avec SSH et exécutez les commandes Acropolis CLI (aCLI) indiquées ci-dessous. Pour plus d'information sur aCLI, consultez Référence des commandes aCLI.

Commandes pour Nutanix AHV version 6.8 et antérieure :

vm.serial_port_create <*management-center-virtual-VM-name*> **type=kServer index=0**

vm.update <*management-center-virtual-VM-name*> **disable_branding=true**

vm.update <*management-center-virtual-VM-name*> **extra_flags="enable_hyperv_clock=False"**

Commandes pour Nutanix AHV version 6.8.1 et supérieure :

vm.serial_port_create <*management-center-virtual-VM-name*> **type=kServer index=0**

vm.update <*management-center-virtual-VM-name*> **disable_branding=true**

vm.update <*management-center-virtual-VM-name*> **disable_hyperv=True**

Étape 12 Allez dans la vue du tableau la machine virtuelle, sélectionnez l'instance Firewall Management Center Virtual nouvellement créée, et cliquez sur **Power On** (démarrer).

Étape 13 Une fois le Firewall Management Center Virtual activé, vérifiez l'état. Accédez à **Home > VM** (Accueil > VM) Firewall Management Center Virtual, sélectionnez la VM déployée et ouvrez une session.

Terminer l'assistant de Firewall Management Center Virtual

Pour tous les On-Prem Firewall Management Center, vous devez effectuer un processus de configuration qui permet à l'appareil de communiquer sur votre réseau de gestion. Si vous déployez sans fichier Day 0, la configuration du Firewall Management Center Virtualse fait en deux étapes :

Procédure

Étape 1 Après avoir initialisé Firewall Management Center Virtual, exécutez un script sur la console du périphérique qui vous aide à configurer celui-ci pour qu'il communique sur votre réseau de gestion.

Étape 2 Terminez ensuite le processus de configuration en utilisant un ordinateur de votre réseau de gestion pour accéder à l'interface Web de Firewall Management Center Virtual.

Étape 3 Terminez la configuration de Firewall Management Center Virtual à l'aide de l'interface de ligne de commande. Consultez Configurer les paramètres réseau à l'aide d'un script, à la page 9.

Étape 4 Terminez le processus de configuration en utilisant un ordinateur de votre réseau de gestion pour accéder à l'interface Web de Firewall Management Center Virtual. Consultez Effectuer la configuration initiale à l'aide de l'interface Web, à la page 10.

Configurer les paramètres réseau à l'aide d'un script

La procédure suivante décrit comment terminer la configuration initiale de Firewall Management Center Virtual à l'aide de l'interface de ligne de commande.

Procédure

Étape 1 À la console, connectez-vous à l'appareil Firewall Management Center Virtual. Utilisez le nom d'utilisateur **admin** et le mot de passe **Admin123**. Si vous utilisez la console Nutanix, le mot de passe par défaut est **Admin123**.

Si vous y êtes invité, réinitialisez le mot de passe.

Étape 2 À l'invite d'administration, exécutez le script suivant :

Exemple :

```
sudo /usr/local/sf/bin/configure-network
```

Lors de la première connexion au Firewall Management Center Virtual, vous êtes invité à effectuer la configuration après le démarrage.

Étape 3 Suivez les instructions du script.

Configurez (ou désactivez) d'abord . Si vous spécifiez manuellement les paramètres réseau, vous devez saisir l'adresse IPv4 .

Étape 4 Confirmez que vos paramètres sont corrects.

Étape 5 Déconnectez-vous du périphérique.

Prochaine étape

- Terminez le processus de configuration en utilisant un ordinateur de votre réseau de gestion pour accéder à l'interface Web de Firewall Management Center Virtual.

Effectuer la configuration initiale à l'aide de l'interface Web

La procédure suivante décrit comment terminer la configuration initiale de Firewall Management Center Virtual à l'aide de l'interface Web.

Procédure

Étape 1 Dirigez votre navigateur vers l'adresse IP par défaut de l'interface de gestion de Firewall Management Center Virtual :

Exemple :

```
https://192.168.45.45
```

Étape 2 Connectez-vous à l'appliance Firewall Management Center Virtual. Utilisez le nom d'utilisateur **admin** et le mot de passe **Admin123**. Si vous y êtes invité, réinitialisez le mot de passe.

La page de configuration s'affiche. Vous devez changer le mot de passe administrateur, préciser les paramètres réseau (si ce n'est pas déjà fait) et accepter le contrat de licence d'utilisateur final (CLUF).

Étape 3 Lorsque vous avez terminé, cliquez sur **Apply** (Appliquer). Le Firewall Management Center Virtual est configuré en fonction de vos sélections. Après l'affichage d'une page intermédiaire, vous êtes connecté à l'interface Web en tant qu'utilisateur admin, qui a le rôle d'administrateur.

Le Firewall Management Center Virtual est configuré en fonction de vos sélections. Après l'affichage d'une page intermédiaire, vous êtes connecté à l'interface Web en tant qu'utilisateur admin, qui a le rôle d'administrateur.

Prochaine étape

- Pour plus d'informations sur la configuration initiale de Firewall Management Center Virtual, consultez Configuration initiale Firewall Management Center Virtual.
- Pour un aperçu des prochaines étapes nécessaires à votre déploiement Firewall Management Center Virtual, consultez le chapitre Guide de démarrage de Cisco Secure Firewall Management Center Virtual (Cisco Secure Firewall Management Center Virtual Getting Started Guide)

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.