Guide de démarrage de Cisco Secure Firewall Management Center Virtual

Dernière modification : 2025-11-10

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

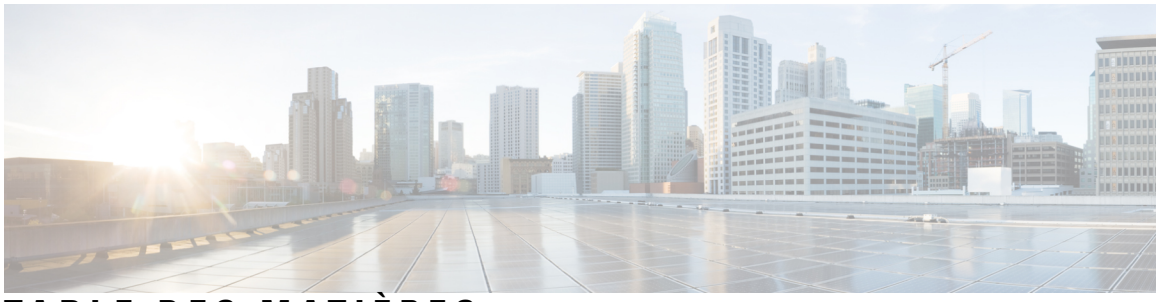
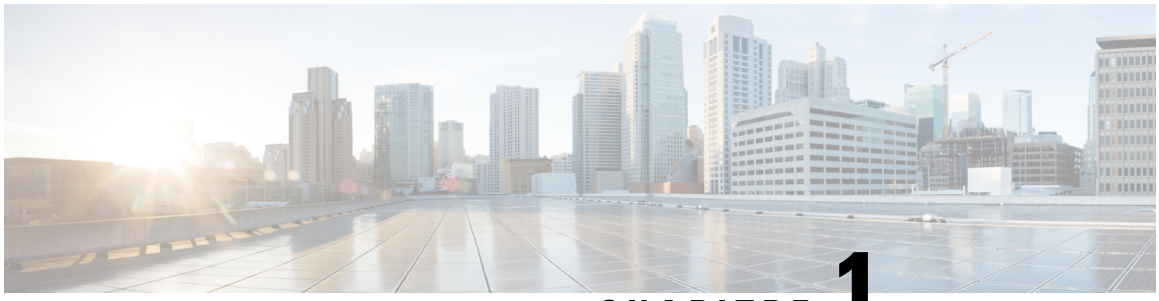


TABLE DES MATIÈRES



CHAPITRE 1

Introduction à Cisco Secure Firewall Management Center Virtual Appliance

L'Cisco Secure Firewall Management Center Virtual (anciennement Firepower Management Center Virtual) apporte la fonctionnalité complète de pare-feu aux environnements virtualisés afin de sécuriser le trafic des centres de données et les environnements multi-détenteurs. Le Firewall Management Center Virtual peut gérer l'appareil physique, et l'appareil Cisco Secure Firewall Threat Defense Virtual (anciennement Firepower Threat Defense Virtual) apporte des appareils complets, NGIPS et FirePOWER.

Plateformes et soutien pour le Firewall Management Center Virtual

Exigences en mémoire et en ressources

Chaque instance du Firewall Management Center Virtual nécessite une allocation minimale de ressources (quantité de mémoire, nombre de CPU et espace disque) sur la plateforme cible afin d'assurer un rendement optimal.

Important Lors de la mise à niveau du Firewall Management Center Virtual, consultez les notes de version les plus récentes pour savoir si la nouvelle version a une incidence sur votre environnement. Vous devrez peut-être augmenter les ressources pour déployer les dernières versions.

Lors de la mise à niveau, vous ajoutez les dernières fonctionnalités et correctifs qui permettent d'améliorer les capacités de sécurité et les performances de votre déploiement.

Firewall Management Center Virtual requiert 28 Go de mémoire vive pour la mise à niveau (6.6.0 ou versions ultérieures)

La plateforme Firewall Management Center Virtual a introduit une nouvelle vérification de la mémoire lors de la mise à niveau. Les mises à niveau de Firewall Management Center Virtual vers la version 6.6.0 ou les versions ultérieures échoueront si vous attribuez moins de 28 Go à l'appliance virtuelle.

Important 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 Firewall Management Center Virtual 300 (FMCv300). Pour améliorer les performances, vous pouvez augmenter la mémoire et le nombre de processeurs d'une appliance virtuelle, en fonction de vos ressources disponibles.

En raison de cette vérification de mémoire, nous ne pourrons pas prendre en charge les instances à mémoire limitée sur les plateformes prises en charge. Consultez À propos des performances des appliances virtuelles, à la page 5 pour obtenir des renseignements importants sur la mise à niveau de Firewall Management Center Virtual.

Configuration initiale Firewall Management Center Virtual (6.5.0 et ultérieures)

Avec la version 6.5, le Firewall Management Center Virtual offre une expérience de configuration initiale améliorée qui comprend les modifications et améliorations suivantes :

- **DHCP on Management** : le protocole DHCP est activé par défaut sur l'interface de gestion (eth0).

  L'interface de gestion Firewall Management Center Virtual est préconfigurée pour accepter une adresse IP4 attribuée par DHCP. Consultez votre administrateur système pour connaître l'adresse IP que le DHCP est configuré à attribuer au Firewall Management Center Virtual. Dans les scénarios où aucun DHCP n'est disponible, l'interface de gestion Cisco Secure Firewall Management Center (anciennement Cisco Firepower Management Center) utilise l'adresse IPv4 192.168.45.45 .

Remarque Si vous utilisez DHCP, vous devez utiliser la réservation DHCP, de sorte que l'adresse attribuée ne change pas. Si l'adresse DHCP change, l'enregistrement du périphérique échouera car la configuration réseau On-Prem Firewall Management Center n'est pas synchronisée. Pour récupérer après un changement d'adresse DHCP, connectez-vous à On-Prem Firewall Management Center (en utilisant le nom d'hôte ou la nouvelle adresse IP) et accédez à **System (Système)** > **Configuration** > **Management Interfaces (Interfaces de gestion)** afin de réinitialiser le réseau.

- **URL de l'interface Web** : l'URL par défaut de l'interface Web Firewall Management Center Virtual est passée à *https://<-IP>:<port>/ui/login*.
- **Réinitialisation du mot de passe** : pour assurer la sécurité et la confidentialité du système, la première fois que vous vous connectez à On-Prem Firewall Management Center, vous devez changer le mot de passe **admin**. Lorsque l'écran de l'assistant de modification du mot de passe s'affiche, vous avez deux options : saisirz un nouveau mot de passe dans les champs **New Password** (Nouveau mot de passe) et **Confirm Password** (Confirmer le mot de passe). Le mot de passe doit être conforme aux critères énumérés dans la boîte de dialogue.

- **Paramètres réseau** : le Firewall Management Center Virtual comprend désormais un assistant d'installation pour terminer la configuration initiale :
  - **Full Qualified Domain Name (Nom de domaine complet)** : acceptez la valeur par défaut, si une est affichée, ou saisissez un nom de domaine complet (syntaxe<hostname> .<domain>) ou le nom d'hôte.
  - **Protocole de démarrage pour la connexion IPV4** : choisissez DHCP ou Static/Manual (Statique/Manuel) comme méthode affectation d'adresses IP.
  - **Groupe DNS** : le groupe de Serveur de nom de domaine par défaut pour le Firewall Management Center Virtual est Cisco Umbrella DNS .
  - **Serveurs de groupes NTP** : le groupe de protocoles de temps de réseau par défaut est défini sur les pools NTP Sourcefire.
- **Exigences en matière de RAM** : la taille de la RAM recommandée est de 32 Go pour le Firewall Management Center Virtual.
- **FMCv300 pour VMware** : une nouvelle image évolutive Firewall Management Center Virtual est disponible sur la plateforme VMware. Elle prend en charge la gestion d'un maximum de 300 périphériques et affiche une capacité de disque plus élevée.

Plateformes prises en charge

Le Firewall Management Center Virtual peut être déployé sur les plateformes suivantes :

- **VMware vSphere Hypervisor (ESXi)** : vous pouvez déployer le Firewall Management Center Virtual en tant que machine virtuelle invitée sur VMware ESXi.
- **Kernel Virtualization Module (KVM)** : vous pouvez déployer le Firewall Management Center Virtual sur un serveur Linux qui exécute l' hyperviseur KVM.
- **Amazon Web Services (AWS)** : vous pouvez déployer le Firewall Management Center Virtual sur des instances EC2 dans le nuage AWS.
- **Microsoft Azure** : vous pouvez déployer leFirewall Management Center Virtual sur le nuage Microsoft Azure.
- **Google Cloud Platform (GCP)** : vous pouvez déployer le Firewall Management Center Virtual sur le GCP public.
- **Oracle Cloud Infrastructure (OCI)** : vous pouvez déployer le Firewall Management Center Virtual sur l'OCI.
- **OpenStack** : vous pouvez déployer le Firewall Management Center Virtual sur OpenStack. Ce déploiement utilise un hyperviseur KVM pour gérer les ressources virtuelles.
- **Cisco HyperFlex** : vous pouvez déployer le Firewall Management Center Virtual sur Cisco HyperFlex.
- **Nutanix** : vous pouvez déployer le Firewall Management Center Virtual sur l'environnement Nutanix avec hyperviseur AHV .
- **Alibaba Cloud** : vous pouvez déployer le Firewall Management Center Virtual sur le nuage Alibaba Cloud.

Remarque La configuration à haute disponibilité (HA) est prise en charge sur le déploiement Firewall Management Center Virtual sur VMware, AWS, Azure, KVM, OCI et HyperFlex. Consultez la section *Haute disponibilité* dans le Guide d'administration du centre de gestion pour en savoir plus sur les exigences du système pour la haute disponibilité.

Prise en charge des hyperviseurs et des versions

Pour la prise en charge des hyperviseur et des versions, consultez Compatibilité de Secure Firewall Threat Defense.

Licences Firewall Management Center Virtual

La licence Firewall Management Center Virtual est une licence de plateforme plutôt qu'une licence de fonctionnalité. La version de la licence virtuelle que vous achetez détermine le nombre de périphériques que vous pouvez gérer par l'intermédiaire de On-Prem Firewall Management Center. Par exemple, vous pouvez acheter des licences qui vous permettent de gérer deux périphériques, 10 périphériques, 25 périphériques ou 300 périphériques.

À propos des licences de fonctionnalités On-Prem Firewall Management Center

Vous pouvez obtenir des licences pour diverses fonctionnalités afin de créer un déploiement de système optimal pour votre organisation. Le On-Prem Firewall Management Center vous permet de gérer ces licences de fonctionnalités et de les attribuer à vos périphériques.

Remarque Le On-Prem Firewall Management Center gère les licences de fonctionnalités pour vos périphériques, mais vous n'avez pas besoin de licence de fonctionnalité pour utiliser le On-Prem Firewall Management Center.

Les licences de fonctionnalités du On-Prem Firewall Management Center dépendent du type de périphérique :

- Les licences Smart sont disponibles pour les appareils Firewall Threat Defense et Firewall Threat Defense Virtual.
- Les licences Classic sont disponibles pour les périphériques de la série 7000 et 8000, ASA FirePOWER et NGIPSv.

Les périphériques qui utilisent des licences Classic sont parfois appelés périphériques Classic. Un seul On-Prem Firewall Management Center peut gérer les licences Classic et Smart.

En plus des licences de fonctionnalités de « droit d'utilisation », de nombreuses fonctionnalités nécessitent un abonnement de service . Les licences de droit d'utilisation n'expirent pas, mais les abonnements aux services nécessitent un renouvellement périodique.

Pour des informations détaillées sur la plateforme de licences, consultez Licences dans le Guide d'administration de Secure Firewall Management Center.

Pour des réponses aux questions courantes sur les licences Smart, les licences Classic, les licences de droit d'utilisation et les abonnements de service, consultez la section Licences de fonctionnalité de Secure Firewall Management Center.

À propos des performances des appliances virtuelles

Il est impossible de prévoir avec précision le débit et la capacité de traitement des appliances virtuelles. Un certain nombre de facteurs influent fortement sur les performances, notamment les suivants :

- la quantité de mémoire et la capacité CPU de l'hôte
- le nombre total de machines virtuelles en exécution sur l'hôte
- la performance réseau, la vitesse des interfaces et le nombre d'interfaces d'analyse déployées
- la quantité de ressources attribuées à chaque appliance virtuelle
- le niveau d'activité des autres appliances virtuelles partageant l'hôte
- la complexité des politiques appliquées à un périphérique virtuel

Si le débit n'est pas satisfaisant, ajustez les ressources attribuées aux appliances virtuelles qui partagent l'hôte.

Chaque appliance virtuelle que vous créez nécessite une certaine quantité de mémoire, de CPU et d'espace disque dur sur l'hôte. Ne réduisez pas les paramètres par défaut, car il s'agit du minimum requis pour exécuter le logiciel système. Toutefois, pour améliorer la performance, vous pouvez augmenter la mémoire et le nombre de CPU d'une appliance virtuelle, selon les ressources disponibles.

Le tableau suivant présente les limites Firewall Management Center Virtual prises en charge.

Tableau 1 : Limites virtuelles de centre de gestion prises en charge

Composant	FMCv2/FMCv10/FMCv25	FMCv300
Processeur virtuel	8/4 vCPU	32 unités centrales de traitement virtuelles
Mémoire	32 Go	64 Go
Espace de stockage d'incidents	250 Go	2,2 To
Taille maximale de mappage réseau (hôtes - utilisateurs)	50 000 – 50 000	150 000 – 150 000
Fréquence maximale des événements (événements par seconde)	5 000	12 000 éps

Exigences par défaut et mémoire minimale Firewall Management Center Virtual

Toutes les implémentations de Firewall Management Center Virtual ont désormais les mêmes exigences en matière de mémoire vive : 32 Go recommandés, 28 Go requis (64 Go pour le FMCv 300). Les mises à niveau de vers la version 6.6 ou les versions ultérieures échoueront si vous attribuer moins de 28 Go à l'appliance virtuelle. Après la mise à niveau, le moniteur d'intégrité vous alertera si vous réduisez l'allocation de mémoire.

Ces nouvelles exigences en matière de mémoire imposent des exigences uniformes dans tous les environnements virtuels, améliorent les performances et vous permettent de tirer parti des nouvelles fonctionnalités. Nous vous recommandons de ne pas modifier à la baisse les paramètres par défaut. Pour améliorer les performances, vous pouvez augmenter la mémoire et le nombre de processeurs d'une appliance virtuelle, en fonction de vos ressources disponibles.

Important À partir de la version 6.6.0, les types d'instances à mémoire limitée pour les déploiements Firewall Management Center Virtual sur le nuage (AWS, Azure) sont entièrement abandonnés. Vous ne pouvez pas créer d'autres instances Firewall Management Center Virtual en les utilisant, même pour les versions antérieures. Vous pouvez continuer à exécuter les instances existantes.

Le tableau suivant récapitule les exigences préalables à la mise à niveau pour les déploiements Firewall Management Center Virtual à mémoire limitée.

Tableau 2 : Firewall Management Center Virtual Mémoire requise pour les mises à niveau de la version 6.6.0 et les versions ultérieures

Observations	Action préalable à la mise à niveau	Détails
VMware	Allouez 28 Go minimum/32 Go recommandés.	Éteignez d'abord la machine virtuelle. Pour obtenir des instructions, consultez la documentation de VMware.
KVM	Allouez 28 Go minimum/32 Go recommandés.	Pour obtenir des instructions, consultez la documentation de votre environnement KVM.
AWS	Redimensionner les instances : • **De** c3.xlarge **à** c3.4xlarge. • **De** c3.2.xlarge **à** c3.4xlarge. • **De** c4.xlarge **à** c4.4xlarge. • **De** c4.2xlarge **à** c4.4xlarge. Nous proposons également une instance c5.4xlarge pour les nouveaux déploiements.	Arrêtez l'instance avant de la redimensionner. Notez que lorsque vous faites cela, les données sur le volume du magasin d'instances sont perdues, donc procédez d'abord à la migration de votre instance sauvegardée par le magasin d'instances. En outre, si votre interface de gestion ne dispose pas d'une adresse IP élastique, son adresse IP publique est publiée. Pour obtenir des instructions, consultez la documentation sur la modification de votre type d'instance dans le guide de l'utilisateur AWS pour les instances Linux.
Azure	Redimensionner les instances : • **De** Standard_D3_v2 **à** Standard_D4_v2.	Utilisez le portail Azure ou PowerShell. Vous n'avez pas besoin d'arrêter l'instance avant de la redimensionner, mais l'arrêt peut révéler des tailles supplémentaires. Le redimensionnement redémarre une machine virtuelle en cours d'exécution. Pour obtenir des instructions, consultez la documentation d'Azure sur le redimensionnement d'une machine virtuelle Windows.

Observations	Action préalable à la mise à niveau	Détails
GCP	Allouez de la mémoire en fonction du type d'instance GCP.	Consultez la section Soutien pour les types de machines GCP pour de plus amples renseignements.
OCI	Allouez de la mémoire en fonction du type d'instance OCI.	Consultez la section Formes de calcul OCI pour de plus amples renseignements.
OpenStack	Allouez 28 Go minimum/32 Go recommandés.	Consultez la section Exigences en matière de mémoire et de ressources pour de plus amples renseignements.
Hyperflex	Allouez 28 Go minimum/32 Go recommandés.	Consultez la section Configuration requise pour le système hôte pour de plus amples renseignements.
Nutanix	Allouez 28 Go minimum/32 Go recommandés.	Consultez la section Configuration requise pour le système hôte pour de plus amples renseignements.

Télécharger le paquet de déploiement Firewall Management Center Virtual

Vous pouvez télécharger les paquets de déploiement Firewall Management Center Virtual à partir de Cisco.com, ou dans le cas de correctifs et de correctifs urgents, vous pouvez les télécharger à partir de On-Prem Firewall Management Center.

Pour télécharger le paquet de déploiement Firewall Management Center Virtual :

Procédure

Étape 1 Accédez à la page de téléchargement du logiciel Cisco.

Remarque
Un identifiant Cisco.com et un contrat de service Cisco sont nécessaires.

Étape 2 Cliquez sur **Browse all** (Parcourir tout) pour rechercher le paquet de déploiement Firewall Management Center Virtual.

Étape 3 Choisissez **Security** > **Firewalls** > **Firewall Management**et sélectionnez **Secure Firewall Management Center Virtual** .

Étape 4 Choisissez votre *modèle* > **FireSIGHT System Software (Logiciel système FireSIGHT** > *version*.

Ce tableau comprend les conventions de dénomination ainsi que des renseignements à propos du logiciel Firewall Management Center Virtual sur Cisco.com.

Modèle	Type de forfait	Nom du paquet
Firewall Management Center Virtual	Installateur de logiciel : VMware	Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-*version*.**tar.gz**
	Installateur de logiciel : KVM	Cisco_Secure_FW_Mgmt_Center_Virtual_KVM-*version*.**qcow2**
	Installateur de logiciel : AWS	Connectez-vous au service en nuage et déployez à partir du Marché.
	Installateur de logiciel : Azure	Connectez-vous au service en nuage et déployez à partir du Marché.

Étape 5 Localisez le paquet de déploiement et téléchargez-le sur un serveur ou sur votre ordinateur de gestion.

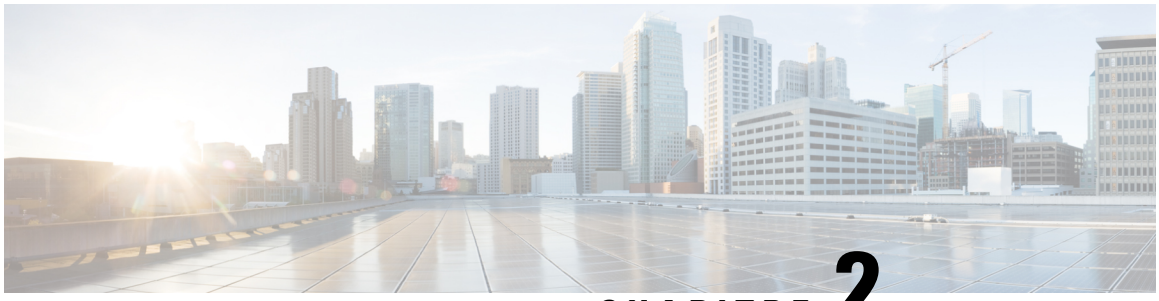
De nombreux noms de paquets se ressemblent, alors assurez-vous de télécharger le bon.

Procédez au téléchargement directement à partir du Site d'assistance et de téléchargement Cisco. Si vous transférez un paquet par e-mail, il peut se corrompre.

Prochaine étape

Consultez le chapitre qui s'applique à votre plateforme de déploiement :

- Pour déployer le Firewall Management Center Virtual en tant que machine virtuelle invitée sur VMware ESXi, consultez Déployer Firewall Management Center Virtual à l'aide de VMware, à la page 9.
- Pour déployer le Firewall Management Center Virtual sur un serveur Linux exécutant l' hyperviseur KVM, consultez Déployer Firewall Management Center Virtual à l'aide de KVM, à la page 25.
- Pour déployer le Firewall Management Center Virtual dans AWS, consultez Déployer Firewall Management Center Virtual sur AWS, à la page 35.
- Pour déployer le Firewall Management Center Virtual dans Azure, consultez Déployer Firewall Management Center Virtual sur Azure à partir du portail AWS., à la page 49.
- Pour déployer le Firewall Management Center Virtual dans la plateforme Google Cloud, consultez Déployer Management Center Virtual (Centre de gestion virtuel) sur la plateforme Google Cloud
- Pour déployer le Firewall Management Center Virtual dans l'infrastructure en nuage Oracle, consultez Déployer Management Center Virtual (Centre de gestion virtuel) sur l'infrastructure en nuage Oracle
- Pour déployer le Firewall Management Center Virtual en utilisant OpenStack, consultez Déployer Management Center Virtual (Centre de gestion virtuel) à l'aide d'OpenStack
- Pour déployer le Firewall Management Center Virtual en utilisant Cisco Hyperflex, consultez Déployer Management Center Virtual (Centre de gestion virtuel) à l'aide de Cisco Hyperflex
- Pour déployer le Firewall Management Center Virtual en utilisant Nutanix, consultez Déployer Management Center Virtual (Centre de gestion virtuel) à l'aide de Nutanix
- Pour déployer le Firewall Management Center Virtual sur Hyper-V, consultez Déployer le Firewall Management Center Virtual sur Hyper-V, à la page 115.



CHAPITRE 2

Déployer Firewall Management Center Virtual à l'aide de VMware

Vous pouvez déployer le FMCv avec VMware Firewall Management Center Virtual.

Prise en charge des fonctionnalités de VMware pour Firewall Management Center Virtual

Le tableau suivant énumère la prise en charge des fonctionnalités de VMware pour Firewall Management Center Virtual.

Tableau 3 : Prise en charge des fonctionnalités de VMware pour Firewall Management Center Virtual

Fonctionnalités	Description	Prise en charge (Oui/Non)	Commentaire
Clonage à froid	La machine virtuelle est hors tension pendant le clonage.	Non	–
Ajout à chaud	La machine virtuelle est en cours d'exécution pendant un ajout.	Non	–
Clonage à chaud	La machine virtuelle est en cours d'exécution pendant le clonage.	Non	–
Suppression à chaud	La machine virtuelle est en cours d'exécution pendant la suppression.	Non	–

Fonctionnalités	Description	Prise en charge (Oui/Non)	Commentaire
Instantanés	La machine virtuelle se bloque pendant quelques secondes.	Non	Il existe un risque de désynchronisation entre le FMC et les périphériques gérés. Voir la section Prise en charge des instantanés, à la page 15. .
Suspendre et reprendre	La machine virtuelle est suspendue, puis reprend.	Oui	–
vCloud Director	Autorise le déploiement automatique des machines virtuelles.	Non	–
Migration de machine virtuelle	La machine virtuelle est hors tension pendant la migration.	Oui	–
vMotion	Utilisé pour la migration en direct des machines virtuelles.	Oui	Utiliser le stockage partagé. Consultez Prise en charge de vMotion, à la page 15.
VMware FT	Utilisé pour la haute disponibilité sur les machines virtuelles.	Non	–
VMware haute disponibilité	Utilisé pour ESXi et les défaillances de serveur.	Oui	–
VMware haute accessibilité avec pulsations de machine virtuelle	Utilisé pour les défaillances de machine virtuelle.	Non	–
Client Windows autonome VMware vSphere	Utilisé pour déployer les machines virtuelles.	Oui	–
Client Web VMware vSphere	Utilisé pour déployer les machines virtuelles.	Oui	–

Configuration système requise

Firewall Management Center Virtual requiert 28 Go de mémoire vive pour la mise à niveau (6.6.0+)

La plateforme Firewall Management Center Virtual a introduit une nouvelle vérification de la mémoire lors de la mise à niveau. Les mises à niveau Firewall Management Center Virtual vers la version 6.6.0 ou les versions ultérieures échoueront si vous attribuez moins de 28 Go à l'appliance virtuelle.

Important 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 Firewall Management Center Virtual 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.

En raison de cette vérification de mémoire, nous ne pourrons pas prendre en charge les instances à mémoire limitée sur les plateformes prises en charge.

Exigences en mémoire et en ressources

Vous pouvez déployer Firewall Management Center Virtual à l'aide du provisionnement VMware vSphere hébergé sur les hyperviseurs VMware ESX et ESXi . Consultez les Guide de compatibilité de Cisco Secure Firewall Threat Defense .

Important Lors de la mise à niveau de Firewall Management Center Virtual, vérifiez 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.

La mise à niveau apporte les dernières fonctions et corrections qui améliorent la sécurité et les performances de votre déploiement.

Le matériel spécifique utilisé pour les déploiements d'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.

Nous vous recommandons fortement de réserver des ressources de CPU et de mémoire pour qu'elles correspondent à l'allocation de ressources. Le non-respect de cette consigne peut avoir une incidence considérable sur les performances et la stabilité Firewall Management Center Virtual.

Le tableau suivant répertorie les paramètres recommandés et par défaut de l'appareil Firewall Management Center Virtual.

Important Assurez-vous d'allouer suffisamment de mémoire pour assurer les performances optimales de votre Firewall Management Center Virtual. Si votre Firewall Management Center Virtual a une mémoire inférieure à 32 Go, des problèmes de déploiement de politiques peuvent survenir. Pour améliorer les performances, vous pouvez augmenter la mémoire et le nombre de processeurs d'une appliance virtuelle, en fonction de vos ressources disponibles. Ne réduisez pas les paramètres par défaut, car il s'agit du minimum requis pour exécuter le logiciel système.

Tableau 4 : Paramètres de l'appareil Firewall Management Center Virtual

Paramètres	Minimum	Par défaut	Recommandations	Paramètre réglable?
Mémoire	28 Go	32 Go	32 Go	Avec restrictions. **Important** La plateforme Firewall Management Center Virtual a introduit une nouvelle vérification de la mémoire lors de la mise à niveau. Les mises à niveau Firewall Management Center Virtual vers la version 6.6.0 ou les versions ultérieures échoueront si vous attribuez moins de 28 Go à l'appliance virtuelle.
Processeurs virtuels	4	4	16	Oui, jusqu'à 16
Taille provisionnée du disque dur	250 Go	250 Go	S.O.	Non

Tableau 5 : Paramètres de l'appliance virtuelle Firewall Management Center Virtual 300 (FMCv300)

Paramètres	Par défaut	Paramètre réglable?
Mémoire	64 Go	Oui
Processeurs virtuels	32	Non
Taille provisionnée du disque dur	2,2 To	Non

Une allocation insuffisante de RAM entraîne le redémarrage des processus en raison d'événements hors mémoire (Out Of Memory, OOM). Le redémarrage des processus de base de données peut également entraîner la corruption de cette dernière. Dans ce cas, assurez-vous de mettre à niveau la RAM jusqu'à l'allocation requise et de sauvegarder fréquemment la base de données pour éviter toute perturbation en raison d'une corruption de la base de données.

Les systèmes exécutant VMware vCenter Server et les instances ESXi doivent satisfaire à des exigences spécifiques en matière de matériel et de système d'exploitation. Pour obtenir la liste des plateformes prises en charge, consultez le Guide de compatibilité en ligne de VMware .

Prise en charge de la technologie de virtualisation

L'ordinateur qui sert d'hôte ESXi doit répondre aux exigences suivantes :

- Il doit avoir un processeur de 64 bits qui fournit une prise en charge de la virtualisation , soit la technologie de virtualisation Intel® (VT) ou la technologie AMD Virtualization™ (AMD-VTM).
- La virtualisation doit être activée dans les paramètres BIOS

Remarque Intel et AMD fournissent tous deux des utilitaires d'identification de processeur en ligne pour vous aider à identifier les CPU et à déterminer leurs capacités. La VT peut être désactivée par défaut sur de nombreux serveurs qui comprennent des CPU avec prise en charge de VT, vous devez donc l'activer manuellement. Consultez la documentation du fabricant pour obtenir des instructions sur la façon d'activer la prise en charge de la VT sur votre système.

- Si vos CPU prennent en charge la VT, mais que vous ne voyez pas cette option dans le BIOS, contactez votre fournisseur pour demander une version du BIOS qui vous permet d'activer la prise en charge de la VT.
- Pour héberger des périphériques virtuels, l'ordinateur doit avoir des interfaces réseau compatibles avec les pilotes Intel e1000 (comme les adaptateurs de serveur double port PRO 1000MT ou les adaptateurs de bureau PRO 1000GT).

Vérifier la prise en charge de la CPU

Vous pouvez utiliser la ligne de commande Linux pour obtenir des informations sur le matériel de la CPU. Par exemple, le fichier **/process/cpuinfo** contient des détails sur les cœurs de CPU individuels. Affiche son contenu avec **less** ou **cat**.z

Vous pouvez consulter la section des indicateurs pour obtenir les valeurs suivantes :

- vmx : extensions VT Intel
- svm : extensions AMD-V

Utilisez **grep** pour voir rapidement si l'une de ces valeurs existe dans le fichier en exécutant la commande suivante :

```
egrep "vmx|svm" /proc/cpuinfo
```

Si votre système prend en charge la VT ou SSSE3, vous devriez voir *vmx* ou *svm* dans la liste d'indicateurs.

Lignes directrices et limites relatives à la licence

Lignes directrices relatives aux fichiers OVF

Les appliances virtuelles utilisent l'emballage Open Virtual Format (OVF). Vous déployez une appliance virtuelle avec une infrastructures virtuelles (VI) ou un modèle OVF ESXi . La sélection du fichier OVF repose sur la cible de déploiement :

- Pour le déploiement sur vCenter —Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-**VI**-*X.X.X-xxx*.ovf
- Pour le déploiement sur ESXi (sans vCenter)—Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-**ESXi**-*X.X.X-xxx*.ovf

où *X.X.X-xxx* est la version et le numéro de version du logiciel du système que vous souhaitez déployer. Voir

- Si vous effectuez le déploiement avec un modèle VI OVF, le processus d'installation vous permet d'effectuer la configuration initiale complète de l'appareil Firewall Management Center Virtual. Vous pouvez préciser :
  - Un nouveau mot de passe du compte administrateur.
  - Paramètres réseau qui permettent à l'appareil de communiquer sur votre réseau de gestion.

Remarque Vous devez gérer cette appliance virtuelle à l'aide de VMware vCenter.

- Si vous effectuez un déploiement à l'aide d'un modèle OVF ESXi, vous devez configurer les paramètres requis par le système après l'installation. Vous pouvez gérer cette appliance virtuelle à l'aide de VMware vCenter ou l'utiliser comme appliance autonome.

Lorsque vous déployez un modèle OVF, vous fournissez les informations suivantes :

Tableau 6 : Paramètres du modèle OVF VMware

Paramètres	ESXi ou VI	Action
Importer/déployer le modèle OVF	Les deux	Accédez aux modèles OVF que vous avez téléchargés à partir de Cisco.com.
Détails du modèle OVF	Les deux	Confirmez le périphérique que vous installez (Firewall Management Center Virtual) et l'option de déploiement (VI ou ESXi).
Accepter le CLUF	VI seulement	Acceptez les conditions des licences incluses dans le modèle OVF.
Nom et emplacement	Les deux	Saisissez un nom unique et significatif pour votre appliance virtuelle et sélectionnez l'emplacement d'inventaire de votre appliance.

Paramètres	ESXi ou VI	Action
Hôte ou grappe	Les deux	Sélectionnez l'hôte ou la grappe dans lequel vous souhaitez déployer l'appliance virtuelle.
Pool de ressources	Les deux	Gérez vos ressources informatiques dans un hôte ou une grappe en les organisant dans une hiérarchie pertinente. Les machines virtuelles et les sous-groupes de ressources héritent des ressources du groupe parent.
Stockage	Les deux	Sélectionnez un magasin de données pour stocker tous les fichiers associés à la machine virtuelle.
Format de disque	Les deux	Sélectionnez le format de stockage des disques virtuels : thick provision lazy zeroed (provisionnement épais à mise à zéro différée), thick provision eager zeroed (provisionnement épais à mise à zéro immédiate) ou thin provision (provisionnement léger).
Mappage du réseau	Les deux	Sélectionnez l'interface de gestion pour l'appliance virtuelle.
Properties (propriétés)	VI seulement	Personnaliser la configuration initiale de la machine virtuelle.

Heure et synchronisation de l'heure

Utilisez un serveur NTP (Network Time Protocol) pour synchroniser l'horloge système sur le Firewall Management Center Virtual et tous les périphériques. Vous spécifiez généralement des serveurs NTP lors de la configuration initiale de Firewall Management Center Virtual ; consultez Configuration initiale Firewall Management Center Virtual, à la page 123 pour en savoir plus sur les serveurs NTP par défaut.

La synchronisation de l'horloge système sur votre Firewall Management Center Virtual et ses périphériques gérés est essentielle au bon fonctionnement de votre système. Vous pouvez prendre des mesures supplémentaires pour assurer la synchronisation de l'heure lorsque vous configurez le NTP sur le serveur VMware ESXi pour qu'il corresponde aux paramètres NTP de Firewall Management Center Virtual.

Vous pouvez utiliser le client vSphere pour configurer le protocole NTP sur les hôtes ESXi . Consultez la documentation de VMware pour obtenir des instructions précises. De plus, la VMware KO 2012069 décrit comment configurer le protocole NTP sur les hôtes ESX/ ESXi à l'aide du client vSphere .

Prise en charge de vMotion

Nous vous recommandons d'utiliser le stockage partagé uniquement si vous prévoyez utiliser vMotion. Pendant le déploiement, si vous avez une grappe d'hôtes, vous pouvez provisionner le stockage localement (sur un hôte précis) ou sur un hôte partagé. Cependant, si vous essayez d'utiliser Firewall Management Center Virtual vMotion vers un autre hôte, l'utilisation du stockage local produira une erreur.

Prise en charge des instantanés

Un instantané VMware est une copie du fichier disque de la machine virtuelle (VMDK) à un instant donné. Les instantanés fournissent un journal des modifications pour le disque virtuel et peuvent être utilisés pour restaurer une machine virtuelle à un moment particulier lorsqu'une défaillance ou une erreur de système se produit. Les instantanés ne fournissent pas de sauvegarde et ne doivent pas être utilisés comme sauvegarde.

Si vous avez besoin de sauvegardes de configuration , utilisez la fonction de sauvegarde et de restauration de On-Prem Firewall Management Center (**System (Système)** > **Tools (Outils)** > **Backup/Restore (Sauvegarde/Restauration)**).

La fonctionnalité d'instantanés de VMware sur ESXi peut épuiser la capacité de stockage de la machine virtuelle et avoir une incidence sur les performances de l'appliance virtuelle FMC. Consultez les articles suivants de la base de connaissances de VMware :

- Bonnes pratiques pour l'utilisation des instantanés dans l'environnement vSphere (VMware KO 1025279).
- Comprendre les instantanés de machine virtuelle dans ESXi (VMware KO 1015180).

La haute disponibilité (c) n'est pas prise en charge.

Vous pouvez établir la haute disponibilité (disponibilité) entre deux appareils Firewall Management Center Virtual sur VMware ESXi.

- Les deux Firewall Management Center Virtual d'une configuration à haute disponibilité doivent être du même modèle.
- Pour établir la haute disponibilité Firewall Management Center Virtual, Firewall Management Center Virtual nécessite un droit de licence supplémentaire Firewall Management Center Virtual pour chaque périphérique Cisco Secure Firewall Threat Defense (anciennement Firepower Threat Defense) qu'il gère dans la configuration HA . Cependant, le droit de licence requis pour la fonctionnalité Firewall Threat Defense pour chaque appareil de Firewall Threat Defense ne change pas, quelle que soit la configuration à haute disponibilité de Firewall Management Center Virtual. Consultez *les Exigences de licence pour les périphériques de défense contre les menaces dans une paire à haute accessibilité* dans le Guide de configuration des périphériques de Cisco Secure Firewall Management Center pour connaître les consignes à propos des licences.
- Si vous rompez la paire à haute disponibilité Firewall Management Center Virtual, le droit de licence supplémentaire Firewall Management Center Virtual est libéré et vous n'avez besoin que d'un seul droit pour chaque appareil Firewall Threat Defense.

Consultez la section *Établissement de la haute disponibilité du centre de gestion* dans le Guide d'administration de Cisco Secure Firewall Management Center pour connaître les consignes à propos de la haute disponibilité.

Symptôme des messages d'erreur de relecture INIT

Vous pouvez voir le message d'erreur suivant sur la console Firewall Management Center Virtual s'exécutant sur ESXi 6 et ESXi 6.5 :

```
"INIT: Id "fmcv" respawning too fast: disabled for 5 minutes"
```

Solution de contournement : modifiez les paramètres de la machine virtuelle dans vSphere pour ajouter un port série lorsque le périphérique est hors tension.

1. Faites un clic droit sur la machine virtuelle et sélectionnez **Edit Settings** (modifier les paramètres).
2. Sous l'onglet Virtual Hardware (matériel virtuel), sélectionnez **Serial port** (port série) dans le menu déroulant **New device** (nouveau périphérique), puis cliquez sur **Add** (ajouter).

   Le port série apparaît au bas de la liste des périphériques virtuels.
3. Sous l'onglet **Virtual Hardware** (matériel virtuel), développez **Serial port** (port série) et sélectionnez le type de connexion **Use physical serial port** (port série physique).

4. Décochez la case **Connect at power on** (connecter à l'alimentation).

   Cliquez sur **OK** pour enregistrer les paramètres.

Restrictions

Les limites suivantes existent lors du déploiement pour VMware :

- Les appliances Firewall Management Center Virtual n'ont pas de numéros de série. La page **System (Système** > **Configuration** affichera soit **None** (Aucun) soit **Not Specified** (Non précisé) selon la plateforme virtuelle.
- Le clonage d'une machine virtuelle n'est pas pris en charge.
- La restauration d'une machine virtuelle à partir d'un instantané n'est pas prise en charge.
- VMware Workstation, Player, Server et Fusion ne reconnaissent pas l'emballage OVF et ne sont pas pris en charge.

Configurez les interfaces VMXNET3

Important À partir de la version 6.4, Firewall Threat Defense Virtual et Firewall Management Center Virtual sur VMware utilisent les interfaces vmxnet3 lorsque vous créez un périphérique virtuel. Auparavant, la valeur par défaut était e1000. Si vous utilisez des interfaces e1000, nous vous **recommandons fortement** de changer. Les pilotes de périphérique vmxnet3 et le traitement réseau sont intégrés à l'hyperviseur ESXi. Ils utilisent donc moins de ressources et offrent de meilleures performances réseau.

Pour remplacer les interfaces e1000 par vmxnet3, vous devez supprimer TOUTES les interfaces et les réinstaller avec le pilote vmxnet3.

Bien que vous puissiez combiner des interfaces dans votre déploiement (p. ex. en déployant les interfaces e1000 sur On-Prem Firewall Management Center et les interfaces vmxnet3 sur son périphérique virtuel géré), vous ne pouvez pas mélanger des types d'interfaces sur la même appliance virtuelle. Toutes les interfaces de détection et de gestion de l'appliance virtuelle doivent être du même type.

Procédure

Étape 1 Mettez hors tension Firewall Threat Defense Virtual ou la machine Firewall Management Center Virtual.

Pour modifier les interfaces, vous devez éteindre l'appareil.

Étape 2 Faites un clic droit sur Firewall Threat Defense Virtual ou la machine Firewall Management Center Virtual dans l'inventaire et sélectionnez **Edit Settings** (modifier les paramètres).

Étape 3 Sélectionnez les adaptateurs de réseau applicables, puis sélectionnez **Remove** (supprimer).

Étape 4 Cliquez sur **Add** (ajouter) pour ouvrir **Add Hardware Wizard** (assistant d'ajout de matériel).

Étape 5 Sélectionnez **Ethernet adapter** (adaptateur Ethernet) et cliquez sur **Next** (suivant).

Étape 6 Sélectionnez l'adaptateur vmxnet3, puis choisissez l'étiquette du réseau.

Étape 7 Répétez l'opération pour toutes les interfaces sur Firewall Threat Defense Virtual.

Prochaine étape

- Démarrez Firewall Threat Defense Virtual ou Firewall Management Center Virtual à partir de la console VMware.

Télécharger le paquet d'installation

Cisco fournit des appliances virtuelles pour les environnements d'hôte VMware ESX et ESXi sur son site d'assistance sous forme de fichiers d'archive compressés (.tar.gz). Les appliances virtuelles Cisco sont regroupées en tant que machines virtuelles avec la version 7 du matériel virtuel. Chaque archive contient les modèles OVF et les fichiers manifestes pour une cible de déploiement ESXi ou VI, ainsi qu'un fichier de format de disque de machine virtuelle (vmdk).

Téléchargez le paquet d'installation Firewall Management Center Virtual depuis Cisco.com et enregistrez-le sur votre disque local. Cisco vous recommande de toujours utiliser le paquet le plus récent. Les paquets de dispositifs virtuels sont généralement associés aux versions majeures du logiciel système (par exemple, 6.1 ou 6.2).

Procédure

Étape 1 Accédez à la page de téléchargement du logiciel Cisco.

Remarque
Un identifiant Cisco.com et un contrat de service Cisco sont nécessaires.

Étape 2 Cliquez sur **Browse all** (Parcourir tout) pour rechercher le paquet de déploiement Firewall Management Center Virtual.

Étape 3 Choisissez **Security (Sécurité)** > **Firewalls (Pare-feux)** > **Firewall Management (Gestion du pare-feu)**et sélectionnez **Secure Firewall Management Center Virtual**.

Étape 4 Trouvez le paquet d'installation VMware que vous souhaitez télécharger pour l'appareil Firewall Management Center Virtual en utilisant la convention d'appellation suivante :

Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-X.X.X-xxx.tar.gz

où *X.X.X-xxx* est la version et le numéro de version du paquet à télécharger.

Étape 5 Cliquez sur le paquet d'installation que vous souhaitez télécharger.

Remarque
Lorsque vous êtes connecté au site de soutien, Cisco vous recommande de télécharger toutes les mises à jour disponibles pour les appliances virtuelles afin que, après l'installation d'une version majeure, vous puissiez mettre à jour le logiciel système. Vous devriez toujours exécuter la version la plus récente du logiciel système prise en charge par votre appliance. Pour le Firewall Management Center Virtual, vous devez également télécharger toutes les nouvelles règles d'intrusion et les mises à jour de la base de données de vulnérabilités (Vulnerability Database, VDB).

Étape 6 Copiez le paquet d'installation vers un emplacement accessible par la station de travail ou le serveur exécutant le vSphere Client.

Mise en garde
Ne transférez pas de fichiers d'archive par courriel ; les fichiers peuvent être corrompus.

Étape 7 Décompressez le fichier d'archive du paquet d'installation à l'aide de votre outil préféré et extrayez les fichiers d'installation. Pour le Firewall Management Center Virtual :

- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-X.X.X-xxx-disk1.vmdk
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-X.X.X-xxx.ovf
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-X.X.X-xxx.mf
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-X.X.X-xxx.ovf
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-X.X.X-xxx.mf

où *X.X.X-xxx* est la version et le numéro de version du fichier d'archive que vous avez téléchargé.

Remarque
Assurez-vous de conserver tous les fichiers dans le même répertoire.

Prochaine étape

- Déterminez votre cible de déploiement (VI ou ESXi) et continuez avec Déployer Firewall Management Center Virtual, à la page 19.

Déployer Firewall Management Center Virtual

Vous pouvez utiliser VMware vSphere vCenter, le client vSphere , le client Web vSphere ou l'hyperviseur ESXi (pour le déploiement autonome ESXi) pour déployer le Firewall Management Center Virtual. Vous pouvez déployer un modèle OVF VI ou ESXi :

- Si vous déployez à l'aide d'un modèle OVF VI, l'appareil doit être géré par VMware vCenter.
- Si vous déployez à l'aide d'un modèle OVF ESXi , l'appareil peut être géré par VMware vCenter ou déployé sur un hôte ESXi autonome. Dans tous les cas, vous devez configurer les paramètres requis par le système après l'installation.

Après avoir spécifié les paramètres sur chaque page de l' assistant, cliquez sur **Next** (Suivant) pour continuer. Pour votre commodité, la dernière page de l'assistant vous permet de confirmer vos paramètres avant de terminer la procédure.

Procédure

Étape 1 Depuis le client vSphere, choisissez **File (Fichier)** > **Deploy OVF Template (Déployer le modèle OVF)**.

Étape 2 Dans la liste déroulante, sélectionnez le modèle OVF que vous souhaitez utiliser pour déployer votre Firewall Management Center Virtual:

- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-*X.X.X-xxx*.ovf

- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-*X.X.X-xxx*.ovf
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-X.X.X-xxx-disk1.vmdk

où *X.X.X-xxx* est la version et le numéro de version du paquet d'installation téléchargé depuis Cisco.com.

Étape 3 Affichez la page **OVF Template Details** (Détails du gabarit OVF) et cliquez sur **Next** (Suivant).

Étape 4 Si les contrats de licence sont groupés avec le modèle OVF (modèles VI uniquement), la page **End User License Agreement** (Contrat de licence d'utilisateur final) s'affiche. Acceptez les modalités de la licence et cliquez sur **Next** (Suivant).

Étape 5 (Facultatif) Modifiez le nom et sélectionnez l'emplacement du dossier dans l'inventaire où résidera le Firewall Management Center Virtual, puis cliquez sur **Next** (Suivant).

Remarque
Lorsque le client vSphere est connecté directement à un hôte ESXi , l'option de sélection de l'emplacement du dossier ne s'affiche pas.

Étape 6 Sélectionnez l'hôte ou la grappe sur lequel vous souhaitez déployer le Firewall Management Center Virtual et cliquez sur Next (Suivant).

Étape 7 Accédez à et sélectionnez l'ensemble de ressources dans lequel vous souhaitez exécuter Firewall Management Center Virtual, puis cliquez sur **Next** (suivant).

Cette page s'affiche uniquement si la grappe contient un ensemble de ressources.

Étape 8 Sélectionnez un emplacement de stockage pour stocker les fichiers de la machine virtuelle, puis cliquez sur **Next** (Suivant).

Dans cette page, sélectionnez parmi les banques de données déjà configurées sur la grappe ou l'hôte de destination. Le fichier de configuration de la machine virtuelle et les fichiers de disque virtuel sont stockés dans la banque de données. Sélectionnez un magasin de données suffisamment grand pour contenir la machine virtuelle et tous ses fichiers de disque virtuel.

Étape 9 Sélectionnez le format de disque virtuel pour stocker les disques virtuels de la machine virtuelle, puis cliquez sur **Next**(Suivant).

Lorsque vous sélectionnez **Thick provisioned** (grand provisionnement), tout le stockage est immédiatement alloué. Lorsque vous sélectionnez **Thin provisioned** (provisionnement léger), le stockage est attribué à la demande, au fur et à mesure que les données sont écrites sur les disques virtuels.

Étape 10 Associez l'interface de gestion Firewall Management Center Virtual à un réseau VMware sur l'écran de mappage de réseau.

Sélectionnez un réseau en cliquant avec le bouton droit sur la colonne **Destination Networks** (Réseaux de destination) dans votre infrastructure pour configurer le mappage de réseau et cliquez sur **Next** (Suivant).

Étape 11 Si des propriétés configurables par l'utilisateur accompagnent le gabarit OVF (gabarits VI seulement), définissez-les et cliquez sur **Nex**t (Suivant).

Étape 12 Passez en revue et vérifiez les paramètres dans la fenêtre **Ready to Complete** (Prêt à terminer).

Étape 13 (Facultatif) cochez l'option **Power on after deployment** (Mise sous tension après le déploiement) pour démarrer la Firewall Management Center Virtual, puis cliquez sur **Finish** (Terminer).

Remarque : Si vous choisissez de ne pas s'activer après le déploiement, vous pouvez le faire plus tard à partir de la console VMware ; consultez Initialisation d'une appliance virtuelle.

Étape 14 Une fois que l'installation est terminée, fermez la fenêtre d'état.

Étape 15 Après avoir terminé l'assistant, le client web vSphere traite la VM; vous pouvez voir l'état « Initalize OVF Deployment » (Initier le déploiement OVF) dans le volet **Recent Tasks** (Tâches récentes) de la zone **Global Information** (Information globale).

Lorsqu'il a terminé, vous voyez l'état d'achèvement du déploiement du modèle OVF.

L'instance Firewall Management Center Virtual apparaît dans le centre de données spécifié dans l'inventaire. Le démarrage de la nouvelle machine virtuelle peut prendre jusqu'à 30 minutes.

Selon le modèle OVF utilisé, une image ISO **_ovfenv-<hostname>.iso** est montée sur VMware vSphere vCenter, le client vSphere , le client Web vSphere ou l' hyperviseur ESXi (pour le déploiement autonome ESXi) après le déploiement de Firewall Management Center Virtual. Cette image ISO comporte des variables d'environnement OVF telles que l'adresse IP, le masque réseau, les noms d'hôte, les rôles de haute disponibilité, etc. Ces variables sont générées par vSphere et utilisées lors du processus de démarrage.

Vous pouvez également démonter l'image après le démarrage de la machine virtuelle Firewall Management Center Virtual. Cependant, l'image sera montée chaque fois que Firewall Management Center Virtual sera sous tension ou éteint, même si **Connect at power on** (Connecter à la mise sous tension) dans **Network Adapter Configuration** VMware vSphere n'est pas coché.

Remarque
Pour enregistrer avec succès Firewall Management Center Virtual auprès de l'autorité de licence de Cisco, On-Prem Firewall Management Center nécessite un accès Internet. Vous devrez peut-être effectuer une configuration supplémentaire après le déploiement pour obtenir un accès Internet et un enregistrement de licence réussi.

Prochaine étape

- Confirmez que les paramètres matériel et de mémoire de l'appliance virtuelle répondent aux exigences de votre déploiement ; voir Vérifier les propriétés de la machine virtuelle, à la page 21.

Vérifier les propriétés de la machine virtuelle

Utilisez la boîte de dialogue VMware Virtual Machine Properties (Propriétés de la machine virtuelle VMware) pour ajuster l'allocation des ressources d'hôte pour la machine virtuelle sélectionnée. Vous pouvez modifier le processeur, la mémoire, le disque et les ressources avancées du processeur à partir de cet onglet. Vous pouvez également modifier le paramètre de connexion sous tension, l'adresse MAC et la connexion réseau pour la configuration de l'adaptateur Ethernet virtuel pour une machine virtuelle.

Procédure

Étape 1 Faites un clic droit sur le nom de votre nouvelle appliance virtuelle, puis choisissez **Edit Settings** (Modifier les paramètres) dans le menu contextuel, ou cliquez sur **Edit virtual machine settings** (Modifier les paramètres de la machine virtuelle) dans l'onglet **Getting Started** (Pour commencer dans la fenêtre principale.

Étape 2 Assurez-vous que les paramètres **Memory** (Mémoire, **CPU**et **Hard disk 1** (Disque dur 1 ne sont pas inférieurs aux valeurs par défaut, comme décrit dans Paramètres de l'appliance virtuelle par défaut, page 4.

Le paramètre de mémoire et le nombre de CPU virtuels pour l'appareil sont répertoriés dans le volet gauche. Pour voir la **Provisioned Size** (taille provisionnée)du disque, cliquez sur **Hard disk 1** (Disque dur 1).

Étape 3 Vous pouvez également augmenter la mémoire et le nombre de CPU virtuels en cliquant sur le paramètre approprié dans le côté gauche de la fenêtre, puis en effectuant des modifications dans le côté droit de la fenêtre.

Étape 4 Confirmez que les paramètres de **l'adaptateur réseau 1** sont les suivants, en les modifiant si nécessaire :

a) Sous **Device Status** (état dupériphérique), cochez la case **Connect at power on (connecter à la mise sous tension)**.

b) Sous **MAC Address** (adresse MAC), définissez manuellement l'adresse MAC de l'interface de gestion de votre appliance virtuelle.

Attribuez manuellement l'adresse MAC à votre appliance virtuelle afin d'éviter les changements ou conflits d'adresses provenant du bassin dynamique.

En outre, pour Firewall Management Center Virtual, définir l'adresse MAC manuellement vous évite de devoir redemander des licences à Cisco si vous devez réinitialiser l'appareil.

c) Sous **Network Connection** (Connexion réseau), définissez l' étiquette **Network** (réseau) au nom du réseau de gestion de votre appliance virtuelle.

Étape 5 Cliquez sur **OK**.

Prochaine étape

- Initialisez l'appliance virtuelle ; voir Mettre sous tension et initialiser l'appliance virtuelle, à la page 22.
- Vous pouvez également créer une interface de gestion supplémentaire avant de mettre le périphérique sous tension ; consultez le chapitre *Déployer le centre de gestion virtuel à l'aide de VMware du Guide de démarrage de Cisco Secure Firewall Management Center Virtual* pour plus d'informations.

Mettre sous tension et initialiser l'appliance virtuelle

Après avoir terminé le déploiement de l'appliance virtuelle, l'initialisation démarre automatiquement lorsque vous activez l'appliance virtuelle pour la première fois.

⚠

Mise en garde Le délai de démarrage dépend d'un certain nombre de facteurs, notamment la disponibilité des ressources du serveur. L'initialisation peut prendre entre sept et huit minutes. N'interrompez pas l'initialisation, sinon vous devrez peut-être supprimer l'appareil et recommencer.

Procédure

Étape 1 Mettez l'appareil sous tension.

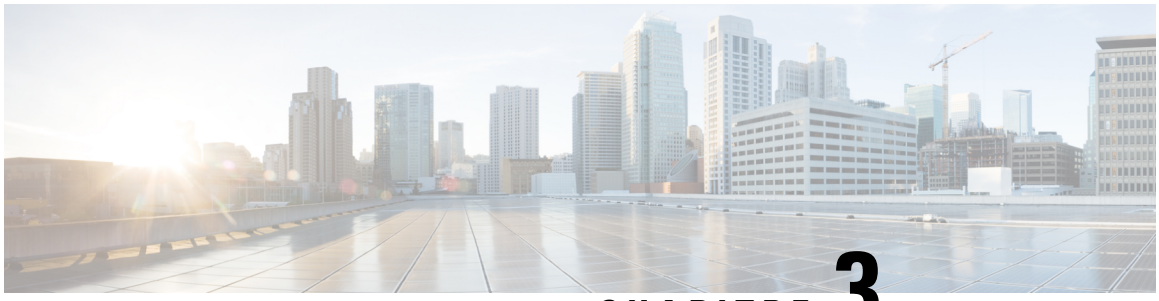
Dans le client vSphere , cliquez avec le bouton droit sur le nom de votre appliance virtuelle dans la liste d'inventaire, puis sélectionnez **Power (Mise sous tension)** > **Power On (Mettre sous tension)** dans le menu contextuel.

Étape 2 Surveillez l'initialisation sur l'onglet de la console VMware .

Prochaine étape

Après le déploiement du Firewall Management Center Virtual, vous devez terminer la configuration pour qu'il communique sur votre réseau de gestion de confiance. Si vous déployez un modèle OVF ESXi sur VMware, la configuration du Firewall Management Center Virtual se fait en deux étapes.

- Pour terminer la configuration initiale du Firewall Management Center Virtual, consultez Configuration initiale Firewall Management Center Virtual, à la page 123.
- Pour un aperçu des prochaines étapes nécessaires dans votre déploiement Firewall Management Center Virtual, consultez x.



CHAPITRE 3

Déployer Firewall Management Center Virtual à l'aide de KVM

Vous pouvez déployer Firewall Management Center Virtual sur KVM.

Aperçu

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.

Firewall Management Center Virtual Requiert 28 Go de mémoire vive pour la mise à niveau (6.6.0 et versions ultérieures)

La plateforme Firewall Management Center Virtual a introduit une nouvelle vérification de la mémoire lors de la mise à niveau. Les mises à niveau de Firewall Management Center Virtual vers la version 6.6 ou les versions ultérieures échoueront si vous attribuez moins de 28 Go de RAM à l'appliance virtuelle.

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

En raison de cette vérification de mémoire, nous ne pourrons pas prendre en charge les instances à mémoire limitée sur les plateformes prises en charge.

Exigences en mémoire et en ressources

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. Consultez les Guide de compatibilité de Cisco Secure Firewall Threat Defense .

Important Lors de la mise à niveau de Firewall Management Center Virtual, vérifiez 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.

La mise à niveau apporte les dernières fonctions et corrections qui améliorent la sécurité et les performances de votre déploiement.

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 sur KVM :

- Processeurs
  - Nécessite 4 vCPU
- Mémoire
  - Minimum requis de 28 Go/ conseillé (par défaut) 32 Go de RAM

Important La plateforme Firewall Management Center Virtual a introduit une nouvelle vérification de la mémoire lors de la mise à niveau. Les mises à niveau de Firewall Management Center Virtual vers la version 6.6 ou les versions ultérieures échoueront si vous attribuez 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

- 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

- Une connexion à Cisco.com et un contrat de service Cisco sont requis.
- Aux fins de l'exemple de déploiement présenté dans ce document, nous supposons que vous utilisez Ubuntu 18.04 LTS. Installez les paquets suivants sur l'hôte Ubuntu 18.04 LTS :
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager
  - virtinst
  - virsh tools
  - genisoimage
- Les performances sont affectées par l'hôte et sa configuration. Vous pouvez maximiser le débit sur KVM en réglant votre hôte. Pour les concepts génériques de réglage d'hôte, consultez l'information sur la virtualisation de la fonction réseau : qualité de service dans des serveurs d'accès à distance à large bande avec l'architecture Linux et Intel.
- Voici des optimisations utiles pour Ubuntu 18.04 LTS :
  - macvtap : pont Linux à haute performance; vous pouvez utiliser macvtap au lieu d'un pont Linux. Notez que vous devez configurer des paramètres précis pour utiliser macvtap au lieu du pont Linux.
  - Transparent Huge Pages : augmente la taille des pages de mémoire et est activé par défaut dans Ubuntu 18.04.
  - Hyperthread désactivé : réduit deux vCPU en un seul cœur.
  - txqueuelength : augmente la longueur de la file d'attente par défaut à 4 000 paquets et réduit le taux d'abandon.
  - épinglage : applique des processus qemu et vhost à des cœurs de CPU spécifiques; dans certaines conditions, l'épinglage augmente considérablement les performances.
- Pour en savoir plus sur l'optimisation d'une distribution basée sur RHEL, consultez le Guide de réglage et d'optimisation de la virtualisation Red Hat Enterprise Linux6.

Lignes directrices et limites relatives à la licence

- Les périphériques Firewall Management Center Virtual n'ont pas de numéros de série. La page **System** > **Configuration** > **(Configuration du système)** affichera soit **None** (Aucun) soit **Not Specified** (Non précisé) selon la plateforme virtuelle.
- Les hyperviseurs imbriqués (KVM s'exécutant sur VMware/ ESXi) ne sont pas pris en charge. Seuls les déploiements de KVM sans système d'exploitation sont pris en charge.
- Le clonage d'une machine virtuelle n'est pas pris en charge.

Préparer le fichier de configuration Day 0 (jour 0)

Vous pouvez préparer un fichier de configuration Day0 (Jour0) avant de lancer Firewall Management Center Virtual. La configuration Day 0 est un fichier texte qui contient les données de configuration initiale appliquées lors du déploiement d'une machine virtuelle. Cette configuration initiale est placée dans un fichier texte nommé « day0-config » dans un répertoire de travail que vous avez choisi, puis manipulée dans un fichier day0.iso qui est monté et lu lors du premier démarrage.

Remarque Le fichier day0.so doit être disponible lors du premier démarrage.

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. Vous pouvez préciser :

- Acceptation du CLUF
- Un nom d'hôte pour le système.
- Un nouveau mot de passe d'administrateur pour le compte admin.
- Des paramètres réseau permettant à l'appliance de communiquer sur votre réseau de gestion. Si vous déployez sans fichier Day 0, vous devez configurer les paramètres requis par le système après le lancement ; pour plus de renseignements, consultez Déployer sans utiliser le fichier de configuration Day 0 (jour 0), à la page 33.

Remarque Nous utilisons Linux dans cet exemple, mais il existe des utilitaires similaires pour Windows.

- Laissez les deux entrées DNS vides pour utiliser les serveurs DNS Cisco Umbrella par défaut. Pour fonctionner dans un environnement non DNS, définissez les deux entrées sur « None » (non sensible à la casse).

Procédure

Étape 1 Saisissez la configuration CLI pour des paramètres réseau Firewall Management Center Virtual dans un fichier texte appelé « day0-config ».

Exemple :

```
#FMC
{
    "EULA": "accept",
    "Hostname": "FMC-Production",
    "AdminPassword": "r2M$9^Uk69##",
    "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": "",
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
}
```

Étape 2 Générez le CD-ROM virtuel en convertissant le fichier texte en fichier ISO :

Exemple :

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

ou

Exemple :

```
/usr/bin/mkisofs -r -o day0.iso day0-config
```

Étape 3 Répétez les étapes pour créer des fichiers de configuration par défaut uniques pour chaque Firewall Management Center Virtual que vous souhaitez déployer.

Prochaine étape

- Si vous utilisez virt-install, ajoutez la ligne suivante à la commande virt-install :

  ```
  --disk path=/home/user/day0.iso,format=iso,device=cdrom \
  ```

- Si vous utilisez virt-manager, vous pouvez créer un CD-ROM virtuel à l'aide de l'interface graphique utilisateur virt-manager; voir Déployer Firewall Management Center Virtual, à la page 31.

Déployer Firewall Management Center Virtual

Vous pouvez lancer le Firewall Management Center Virtual sur KVM en utilisant les méthodes suivantes :

- Utiliser un script basé sur virt-install pour lancer le Firewall Management Center Virtual ; voir Lancer à l'aide d'un script de déploiement, à la page 30.
- Utiliser virtual Machine Manager : utilisez virt-manager, un outil graphique pour créer et gérer des machines virtuelles KVM, pour lancer le Firewall Management Center Virtual ; voir Déployer Firewall Management Center Virtual, à la page 31.

Vous pouvez également choisir de déployer le Firewall Management Center Virtual sans le fichier de configuration de Day 0. Cela vous oblige à terminer la configuration initiale à l'aide de l'interface de ligne de commande de l'appareil ou de l'interface Web.

Lancer à l'aide d'un script de déploiement

Vous pouvez utiliser un script de déploiement basé sur virt-install pour lancer le Firewall Management Center Virtual.

Avant de commencer

Sachez que vous pouvez optimiser les performances en sélectionnant le meilleur mode de mise en cache des invités pour votre environnement. Le mode de mise en cache utilisé aura une incidence sur la perte de données; il peut également influer sur les performances du disque.

Chaque interface de disque invité KVM peut avoir l'un des modes de cache suivants : *writethrough*, *writeback*, *none* (aucun), *directsync* (synchronisation directe) et *unsafe* (non sécurisé) Le mode *writethrough* fournit une mise en cache de lecture. *writeback* fournit une mise en cache de lecture et d'écriture ; *directsync* contourne le mise en cache de la page hôte ; *unsafe* peut mettre en cache tout le contenu et ignorer les demandes de purge de l'invité.

- Le mode *cache=writethrough* réduira la corruption de fichiers sur les machines invitées KVM lorsque l'hôte subit des pertes de puissance subites. Nous vous recommandons d'utiliser le mode writethrough.
- Cependant, *cache=writethrough* peut également influer sur les performances du disque en raison de plus grand nombre d'écritures d'E/S sur le disque que *cache=none*.
- Si vous supprimez le paramètre de mise en cache sur l'option *--disk*, la valeur par défaut est *writethrough*.
- Ne pas préciser d'option de mise en cache peut également réduire considérablement le temps nécessaire à la création de la machine virtuelle. Cela est causé par le fait que certains contrôleurs RAID plus anciens ont une mauvaise capacité de mise en cache de disque. Par conséquent, la désactivation de la mise en cache du disque (*cache=none*) et l'utilisation par défaut de l'écriture *writethrough* contribuent à l'intégrité des données.

Procédure

Étape 1 Créez un script virt-install appelé « virt_install_fmc.sh ».

Le nom de l'instance Firewall Management Center Virtual doit être unique pour toutes les autres machines virtuelles (VM) sur cet hôte KVM. Le Firewall Management Center Virtual peut prendre en charge 1 interface réseau. La carte réseau virtuelle doit être Virtio.

Exemple :

```
virt-install \
    --connect=qemu:///system \
    --network network=default,model=virtio \
    --name=fmcv \
    --arch=x86_64 \
    --cpu host \
    --vcpus=4 \
    --ram=28672 \
    --os-type=generic \
    --virt-type=kvm \
    --import \
    --watchdog i6300esb,action=reset \
    --disk path=<fmc_filename>.qcow2,format=qcow2,device=disk,bus=virtio,cache=writethrough \
    --disk path=<day0_filename>.iso,format=iso,device=cdrom \
    --console pty,target_type=serial \
    --serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \
    --force
```

Remarque
Dans le script de déploiement, veillez à définir la valeur du paramètre --os-type sur **générique** pour le processus de déploiement afin d'identifier correctement la plateforme sur laquelle l'instance virtuelle est déployée.

Étape 2 Exécutez le script virt_install :

Exemple :

```
/usr/bin/virt_install_fmc.sh
Starting install...
Creating domain...
```

Une fenêtre apparaît, affichant la console de la VM. Vous pouvez voir que la VM démarre. Le démarrage de la machine virtuelle prend quelques minutes. Une fois que la VM arrête de démarrer, vous pouvez exécuter des commandes de l'interface de ligne de commande à partir de l'écran de la console.

Déployer Firewall Management Center Virtual

Utilisez virt-manager, également appelé gestionnaire de machines virtuelles, pour lancer Firewall Management Center Virtual. Le gestionnaire virt-manager est un outil graphique pour créer et gérer des machines virtuelles d'invités.

Procédure

Étape 1 Démarrez virt-manager en accédant à la section du gestionnaire de machines virtuelles dans les outils de système **(Applications** > **System Tools** > **Virtual Machine Manager**).

Il se peut que vous deviez sélectionner l'hyperviseur ou saisir votre mot de passe racine.

Étape 2 Cliquez sur le bouton dans le coin supérieur gauche pour ouvrir l'assistant **New VM** (nouvelle machine virtuelle).

Étape 3 Saisissez les détails de la machine virtuelle :

a) Pour le système d'exploitation, sélectionnez **Import exist disk image** (Importer une image de disque existante).

Cette méthode vous permet d'importer une image de disque (contenant un système d'exploitation préinstallé et amorçable).

b) Cliquez sur **Forward** pour continuer.

Étape 4 Chargez l'image disque :

a) Cliquez sur **Browse...** (parcourir) pour sélectionner le fichier d'image.
b) Choisissez *Use Generic* (Générique) pour le **type de système d'exploitation**.
c) Cliquez sur **Forward** pour continuer.

Étape 5 Configurer les options de mémoire et de CPU :

a) Réglez la **mémoire (RAM)** à *28 672*.
b) Réglez les **CPU** à *4*.
c) Cliquez sur **Forward** pour continuer.

Étape 6 Cochez la case **Customize configuration before install**(personnaliser la configuration avant l'installation), précisez un **nom**, puis cliquez sur **Finish** (terminer).

Cela ouvre un autre assistant qui vous permet d'ajouter, de supprimer et de configurer les paramètres matériels de la machine virtuelle.

Étape 7 Modifier la configuration CPU

Dans le volet de gauche, sélectionnez **Processor** (processeur), puis sélectionnez **Configuration**Copy host CPU configuration (copier la configuration CPU de l'hôte).

Ainsi, le modèle et la configuration de CPU de l'hôte physique sont appliqués à votre machine virtuelle.

Étape 8 8. Configurer le disque virtuel :

a) Dans le volet de gauche, sélectionnez **Disk 1** (disque 1).
b) Sélectionnez **Advanced options** (options avancées).
c) Définissez **Disk bus** en choisissant *Virtio*.
d) Définissez le format de stockage (**Storage format**) pour *qcow2*.

Étape 9 Configurer une console série :

a) Dans le volet de gauche, sélectionnez **Console**.
b) Sélectionnez **Remove** pour supprimer la console par défaut.
c) Cliquez sur **Add Hardware** (ajouter du matériel) pour ajouter un périphérique série.
d) Pour **Device Type** (type de périphérique), sélectionnez *TCP net console (tcp)*.
e) Pour **Mode**, sélectionnez *Server mode (bind)*, soit le mode liaison pour le serveur.
f) Pour l'hôte (**Host**), saisissez **0.0.0.0** pour l'adresse IP, puis saisissez un numéro de **Port** unique.
g) Cochez la case **Use Telnet** (utiliser Telnet).
h) Configurer les paramètres de l'appareil

Étape 10 Configurez un périphérique de surveillance pour déclencher automatiquement une action lorsque l'invité KVM est suspendu ou planté :

a) Cliquez sur **Add Hardware** (ajouter du matériel) pour ajouter un périphérique de surveillance.

b) Pour **Model** (modèle), sélectionnez *default* (par défaut).
c) Pour **Action**, sélectionnez *Forcely reset the guest* (réinitialiser l'invité de manière forcée).

Étape 11 Configurez l'interface de réseau virtuel.

Choisissez **macvtap** ou indiquez un nom de périphérique partagé (utiliser un nom de pont).

Remarque
Par défaut, l'instance Firewall Management Center Virtual se lance avec une interface, que vous pouvez ensuite configurer.

Étape 12 Si vous déployez à l'aide d'un fichier de configuration de jour 0, créez un CD-ROM virtuel pour l'ISO :

a) Cliquez sur **Add Hardware** (ajouter du matériel).
b) Sélectionnez **Storage** (stockage).
c) Cliquez sur **Select managed or other existing storage** (sélectionner le stockage géré ou existant) et accédez à l'emplacement du fichier ISO.
d) Pour **Device type** (type d'appareil), sélectionnez *IDE CDROM*.

Étape 13 Après avoir configuré le matériel de la machine virtuelle, cliquez sur **Apply** (appliquer).

Étape 14 Cliquez sur **Begin installation** afin de commencer l'installation de virt-manager pour créer la machine virtuelle avec vos paramètres matériels précisés.

Déployer sans utiliser le fichier de configuration Day 0 (jour 0)

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 :

- 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.
- 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.

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**.

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) . 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 votre appareil Firewall Management Center Virtual. Utilisez le nom d'utilisateur **admin** et le mot de passe **Admin123**. La page de configuration s'affiche.

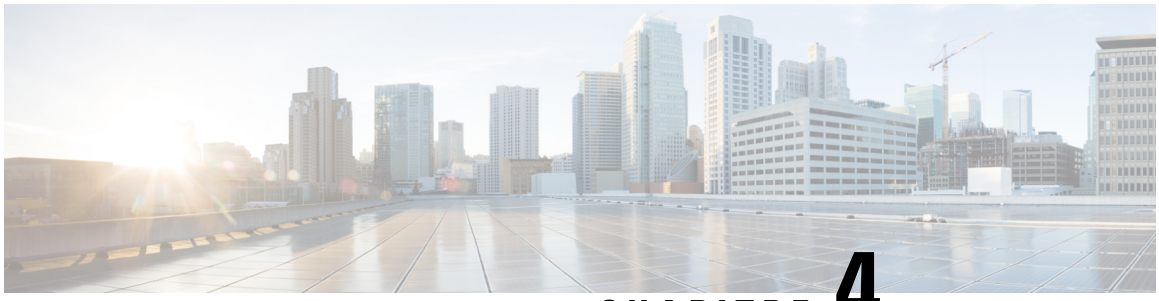
La page de configuration s'affiche. Vous devez changer le mot de passe administrateur, définir les paramètres réseau (au besoin) et accepter le CLUF.

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, à la page 123.
- Pour un aperçu des prochaines étapes nécessaires à votre déploiement Firewall Management Center Virtual, consultez le chapitre Firewall Management Center Virtual Administration et configuration initiale, à la page 133.



CHAPITRE 4

Déployer Firewall Management Center Virtual sur AWS

Amazon Virtual Private Cloud (Amazon VPC) vous permet de lancer des ressources Amazon Web Services (AWS) dans un réseau virtuel que vous définissez. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel qui pourrait fonctionner dans votre propre centre de données, avec les avantages de l'utilisation de l'infrastructure évolutive d'AWS.

Vous pouvez déployer Firewall Management Center Virtual sur le nuage AWS (AWS Cloud).

Aperçu

Firewall Management Center Virtual requiert 28 Go de mémoire vive pour la mise à niveau (6.6.0 ou versions ultérieures)

La plateforme Firewall Management Center Virtual a introduit une nouvelle vérification de la mémoire lors de la mise à niveau. Les mises à niveau de Firewall Management Center Virtual vers la version 6.6.0 ou les versions ultérieures échoueront si vous attribuez moins de 28 Go à l'appliance virtuelle.

Important À partir de la version 6.6.0, les types d'instances à mémoire limitée pour les déploiements Firewall Management Center Virtual sur le nuage (AWS, Azure) sont entièrement abandonnés. Vous ne pouvez pas créer d'autres instances Firewall Management Center Virtual en les utilisant, même pour les versions antérieures. Vous pouvez continuer à exécuter les instances existantes. Consultez Tableau 7 : Types d'instances pris en charge par AWS pour le Firewall Management Center Virtual, à la page 36.

En raison de cette vérification de mémoire, nous ne pourrons pas prendre en charge les instances à mémoire limitée sur les plateformes prises en charge.

Le tableau suivant résume les types d'instances AWS que Firewall Management Center Virtual prend en charge ; ceux que prennent en charge les versions 6.5.x et antérieures, et ceux que prennent en charge les version 6.6.0 et ultérieures.

Remarque La version 6.6 ajoute la prise en charge des types d'instances C5 affichés dans le tableau suivant. Les types d'instances plus importantes fournissent plus de ressources de CPU à vos VM AWS pour des performances accrues, et certains autorisent plus d'interfaces réseau.

Tableau 7 : Types d'instances pris en charge par AWS pour le Firewall Management Center Virtual

Observations	Versions 6.6.0 et ultérieures	vCPU	Mémoire (Go)	Nombre maximal d'interfaces	Versions 6.5 et antérieures	vCPU	Mémoire (Go)	Nombre maximal d'interfaces
Firewall Management Center Virtual	c3.4xlarge	16	30	8	c3.xlarge*	4	7.5	4
	c4.4xlarge	16	30	8	c3.2xlarge*	8	15	4
	c5.4xlarge	16	32	8	c3.4xlarge	16	30	8
	—	—	—	—	c4.xlarge*	4	7.5	4
					c4.2xlarge*	8	15	4
					c4.4xlarge	16	30	8
	* Notez que le Firewall Management Center Virtual ne prendra pas en charge ces types d'instances sur les versions 6.6.0 et supérieures. À partir de la version 6.6.0, vous devez déployer le Firewall Management Center Virtual (n'importe quelle version) en utilisant une instance avec au moins 28 Go de RAM. Consultez Types d'instances obsolètes et Redimensionnement des types d'instances, à la page 37 pour de plus amples renseignements.							

Tableau 8 : Types d'instances pris en charge par AWS pour le Firewall Management Center Virtual 300

Observations	Version 7.1.0 et ultérieures
Firewall Management Center Virtual 300 (FMCv300)	c5.9xlarge : 36 vCPU, 72 Go Stockage SSD : 2000 Go

Types d'instances obsolètes

Vous pouvez continuer à exécuter vos déploiements actuels de la version 6.5.x et antérieures Firewall Management Center Virtual, mais vous ne pourrez pas lancer les nouveaux déploiements Firewall Management Center Virtual (n'importe quelle version) en utilisant ces types d'instances :

- c3.xlarge : 4 vCPU de 7,5 Go (Désactivé pour le Firewall Management Center Virtual après les versions 6.6.0 et ultérieures)
- c3.2xlarge : 8 vCPU de 15 Go (Désactivé pour le Firewall Management Center Virtual après les versions 6.6.0 et ultérieures)
- c4.xlarge : 4 vCPU de 7,5 Go (Désactivé pour le Firewall Management Center Virtual après laes versions 6.6.0 et ultérieures)

- c4.2xlarge : 8 vCPU, 15 Go (Désactivé pour le Firewall Management Center Virtual après les versions 6.6.0 et ultérieures)

Redimensionnement des types d'instances

Étant donné que le chemin de mise à niveau de toute version antérieure de Firewall Management Center Virtual (6.2.x, 6.3.x, 6.4.x et 6.5.x) vers la version 6.6.0 comprend la vérification de la mémoire de 28 Go de RAM, vous devez redimensionner votre type d'instance actuel en un qui prend en charge la version 6.6.0 (voir Tableau 7 : Types d'instances pris en charge par AWS pour le Firewall Management Center Virtual, à la page 36).

Vous pouvez redimensionner une instance si le type d'instance actuel et le nouveau type d'instance que vous souhaitez sont compatibles. Pour les déploiements Firewall Management Center Virtual :

- Redimensionnez n'importe quelle instance c3.xlarge ou c3.2xlarge en type d'instance c3.4xlarge.
- Redimensionnez n'importe quelle instance c4.xlarge ou c4.2xlarge avec le type d'instance c4.4xlarge.

Gardez à l'esprit les éléments suivants avant de redimensionner votre instance :

- Vous devez arrêter votre instance avant de modifier les types d'instances.
- Vérifiez que votre type d'instance actuel est compatible avec le nouveau type d'instance que vous choisissez.
- Si cette instance a un volume de stockage d'instances, toutes les données qu'elle contient sont perdues lorsque l'instance est arrêtée. Migrez votre instance sauvegardée sur le magasin d'instances avant de la redimensionner.
- Si vous n'utilisez pas d'adresse IP Elastic, l'adresse IP publique est libérée lorsque vous arrêtez l'instance.

Pour des instructions sur la façon de redimensionner votre instance, consultez la documentation d'AWS « Changement du type d'instance » (https:docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-resize.html).

Aperçu de la solution AWS

AWS est un ensemble de services informatiques à distance proposés par Amazon.com, également appelés services Web, qui composent une plateforme de traitement en nuage. Ces services fonctionnent à partir de 11 régions géographiques partout au monde. De façon générale, familiarisez-vous avec les services AWS suivants lors du déploiement du Firewall Management Center Virtual :

- Amazon Elastic Compute Cloud (EC2) : un service Web qui vous permet de louer des ordinateurs virtuels pour lancer et gérer vos propres applications et services, comme un pare-feu, dans les centres de données d'Amazon.
- Amazon Virtual Private Cloud (VPC) : un service Web qui vous permet de configurer un réseau privé isolé qui existe dans le nuage public d'Amazon. Vous exécutez vos instances EC2 dans un VPC.
- Amazon Web Service (S3) : un service Web qui vous fournit une infrastructure de stockage de données.

Vous créez un compte sur AWS, configurez les composants VPC et EC2 (à l'aide des assistants AWS ou de la configuration manuelle), et choisissez une instance Amazon Machine Image (AMI). L'AMI est un modèle qui contient la configuration logicielle nécessaire pour lancer votre instance.

Remarque Les images d'AMI ne peuvent pas être téléchargées en dehors de l'environnement AWS.

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge (7.1.0 et versions ultérieures)

- **Management Center Virtual 300 (FMCv300) pour AWS** : une nouvelle image Firewall Management Center Virtual évolutive est disponible sur la plateforme AWS. Elle prend en charge la gestion d'un maximum de 300 périphériques et offre une capacité de disque plus élevée.
- La haute accessibilité (HA) Firewall Management Center Virtual est prise en charge.

Prérequis

Les conditions préalables suivantes concernent le Firewall Management Center Virtual sur AWS :

- Un compte Amazon. Vous pouvez en créer un à l' adresse aws.amazon.com.
- Un compte Cisco Smart. Vous pouvez en créer un sur le Centre des logiciels Cisco (https://software.cisco.com/).
- Obtenez une licence pour Firewall Management Center Virtual. Consultez Licences Firewall Management Center Virtual, à la page 4 pour connaître les directives générales sur les licences de plateforme virtuelle ; consultez la section « Licences du système » du *Guide de configuration de Cisco Secure Firewall Management Center* pour obtenir des renseignements plus détaillés sur la gestion des licences.
- Exigences de l'interface Firewall Management Center Virtual
  - Interface de gestion.
- Chemins de communication :
  - Adresses IP publiques et Elastic pour l'accès à Firewall Management Center Virtual.
- Pour la compatibilité de Firewall Management Center Virtual et du système, consultez le guide de compatibilité de Cisco Secure Firewall Threat Defense.

Directives

Les directives suivantes concernent le Firewall Management Center Virtual sur AWS :

- Déploiement dans le Cloud privé virtuel (VPC)
- Mise en réseau améliorée (SR-IOV) si disponible.
- Déploiement à partir du Marché Amazon
- Maximum de quatre vCPU par instance.
- Déploiement des utilisateurs des réseaux L3

Restrictions

Les limites suivantes concernent le Firewall Management Center Virtual sur AWS :

- Les périphériques Firewall Management Center Virtual n'ont pas de numéros de série. La page **System (Système** > **Configuration** affichera soit **None** (Aucun) soit **Not Specified** (Non précisé) selon la plateforme virtuelle.
- Toute configuration d'adresse IP (de l'interface de ligne de commande ou de On-Prem Firewall Management Center) doit correspondre à ce qui est créé dans la console AWS ; vous devez noter vos configurations pendant le déploiement.
- IPv6 n'est pas pris en charge pour le moment.
- Vous ne pouvez pas ajouter d'interfaces après le démarrage.
- Le clonage et les instantanés ne sont actuellement pas pris en charge.
- La découverte de l'identité du serveur TLS (Transport Layer Security) n'est pas prise en charge avec la configuration à Bras unique de Geneve sur AWS.

Configuration de l'environnement AWS

Pour déployer Firewall Management Center Virtual sur AWS, vous devez configurer un VPC Amazon avec vos exigences et vos paramètres de déploiement précis. Dans la plupart des situations, un assistant de configuration peut vous guider dans votre configuration. AWS fournit une documentation en ligne où vous pouvez trouver des informations utiles sur les services, des présentations aux fonctionnalités avancées. Consultez la section Mise en route d'AWS pour en savoir plus.

Pour vous aider à mieux contrôler votre configuration AWS, les sections suivantes proposent un guide de vos configurations VPC et EC2 avant de lancer les instances du Firewall Management Center Virtual :

- Créer le VPC, à la page 39
- Ajouter une passerelle Internet, à la page 40
- Ajoutez les sous-réseaux, à la page 41
- Ajouter une table de routage, à la page 42
- Créer un groupe de sécurité, à la page 42
- Créer des interfaces réseau, à la page 43
- Créer des adresses IP Elastic, à la page 44

Créer le VPC

Un Cloud privé virtuel (ou VPC) est un réseau virtuel dédié à votre compte AWS. Il est logiquement isolé des autres réseaux virtuels du Cloud AWS. Vous pouvez lancer vos ressources AWS, par exemple des instances Firewall Management Center Virtual, dans votre VPC. Vous pouvez configurer votre VPC; vous pouvez sélectionner sa plage d'adresses IP, créer des sous-réseaux et configurer les tables de routage, les passerelles réseau et les paramètres de sécurité.

Avant de commencer

- Créez votre compte AWS.
- Confirmez que des AMIs sont disponibles pour les instances Firewall Management Center Virtual.

Procédure

Étape 1 Connectez-vous à aws.amazon.com et choisissez votre région.

AWS 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 Cliquez sur **Services** > **VPC**.

Étape 3 Cliquez sur **VPC Dashboard** > **Your VPCs** > **(Tableau de bord VPC** > **Vos VPC)**.

Étape 4 Cliquez sur **Create VPC** (Créer un nuage privé virtuel).

Étape 5 Saisissez la commande suivante dans la boîte de dialogue **Create VPC** (Créer un VPC) :

a) Une **balise de nom** définie par l'utilisateur pour identifier le VPC.
b) Un **bloc CIDR** d'adresses IP. La notation CIDR (Classless Inter-Domain Routing) est une représentation compact d'une adresse IP et de son préfixe de routage associé. Par exemple, 10.0.0.0/24.
c) Un paramètre de localisation (**Tenancy setting**) par défaut pour s'assurer que les instances lancées dans ce VPC utilisent l'attribut de localisation précisé lors du lancement.

Étape 6 Cliquez sur **Yes, Create** pour créer votre VPC.

Prochaine étape

Ajoutez une passerelle Internet à votre VPC comme décrit dans la section suivante.

Ajouter une passerelle Internet

Vous pouvez ajouter une passerelle Internet pour connecter votre VPC à Internet. Vous pouvez acheminer le trafic pour les adresses IP en dehors de votre VPC vers la passerelle Internet.

Avant de commencer

- Créez un VPC pour vos instances Firewall Management Center Virtual.

Procédure

Étape 1 Cliquez sur **Services** > **VPC**.

Étape 2 Cliquez sur **VPC Dashboard (tableau de board VPC)** > **Internet Gateways (passerelles Internet)**, puis cliquez sur **Create Internet Gateway** (créer une passerelle Internet).

Étape 3 Saisissez une balise de nom (Name tag) définie par l'utilisateur pour définir la passerelle et cliquez sur Yes, Create pour créer la passerelle.

Étape 4 Sélectionnez la passerelle créée à l'étape précédente.

Étape 5 Cliquez sur **Attach to VPC** (associer au VPC)et sélectionnez le VPC que vous avez créé précédemment.

Étape 6 Cliquez sur **Yes, Attach (oui, associer)** pour associer la passerelle à votre VPC.

Par défaut, les instances lancées sur le VPC ne peuvent pas communiquer avec Internet tant qu'une passerelle n'est pas créée et liée au VPC.

Prochaine étape

Ajoutez des sous-réseaux à votre VPC, comme décrit dans la section suivante.

Ajoutez les sous-réseaux

Vous pouvez segmenter la plage d'adresses IP de votre VPC auquel les instances Firewall Management Center Virtual peuvent être associées. Vous pouvez créer des sous-réseaux pour regrouper les instances en fonction des besoins opérationnels et de sécurité. Pour Firewall Threat Defense Virtual, vous devez créer un sous-réseau pour la gestion, ainsi que des sous-réseaux pour le trafic.

Procédure

Étape 1 Cliquez sur **Services** > **VPC**.

Étape 2 Cliquez sur **VPC Dashboard (tableau de bord VPC)** > **Subnets (sous-réseaux)**, puis sur **Create Subnet** (créer un sous-réseau).

Étape 3 Saisissez les informations suivantes dans la boîte de dialogue **Create Subnet** (créer un sous-réseau) :

a) Une balise de nom (**Name tag**) définie par l'utilisateur pour identifier le sous-réseau.
b) Le **VPC** à utiliser pour ce sous-réseau.
c) La zone de disponibilité (**Availability Zone**) où ce sous-réseau résidera. Sélectionnez No Preference (aucune préférence) pour permettre à Amazon de sélectionner la zone.
d) Un **bloc CIDR** d'adresses IP. La plage d'adresses IP dans le sous-réseau doit être un sous-ensemble de la plage d'adresses IP dans le VPC. La taille des blocs doit être comprise entre un masque réseau/16 et un masque réseau/28. La taille du sous-réseau peut correspondre à la taille du VPC.

Étape 4 Cliquez sur **Yes, Create** pour créer votre sous-réseau.

Étape 5 Répétez l'opération pour tous les sous-réseaux requis. Créez un sous-réseau distinct pour le trafic de gestion et créez autant de sous-réseaux que nécessaire pour le trafic de données.

Prochaine étape

Ajoutez une table de routage à votre VPC comme décrit dans la section suivante.

Ajouter une table de routage

Vous pouvez associer une table de routage à la passerelle que vous avez configurée pour votre VPC. Vous pouvez également associer plusieurs sous-réseaux à une seule table de routage, mais un sous-réseau ne peut être associé qu'à une seule table de routage à la fois.

Procédure

Étape 1 Cliquez sur **Services** > **VPC**.

Étape 2 Cliquez sur **VPC Dashboard (tableau de bord VPC)** > **Route Tables (tables de routage)**, puis sur **Create Route Table** (créer une table de routage).

Étape 3 Saisissez une **Name tag (Balise de nom)** pour identifier la table de routage.

Étape 4 Sélectionnez le **VPC** dans la liste déroulante qui utilisera cette table de routage.

Étape 5 Cliquez sur **Yes, Create** (oui, créer) pour créer votre table de routage.

Étape 6 Sélectionnez la table de routage que vous avez créée.

Étape 7 Cliquez sur l'onglet **Routes** pour afficher les renseignements sur le routage dans le volet de détails.

Étape 8 Cliquez sur **Edit** (Modifier), puis sur **Add another route** (Ajouter une autre route).

a) Dans la colonne **Destination**, saisissez **0.0.0.0/0**.

b) Dans la colonne **Target** (cible), sélectionnez la passerelle Internet que vous avez créée ci-dessus.

Étape 9 Cliquez sur **Save** (enregistrer).

Étape 10 Cliquez sur l'onglet **Subnet Associations** (associations de sous-réseau), puis sur **Edit**(modifier).

Étape 11 Cochez la case à côté du sous-réseau à utiliser pour l'interface de gestion de Firewall Management Center Virtual et cliquez sur **Save** (Enregistrer).

Prochaine étape

Créez un groupe de sécurité comme décrit dans la section suivante.

Créer un groupe de sécurité

Vous pouvez créer un groupe de sécurité avec des règles précisant les protocoles autorisés, les ports et les plages d'adresses IP sources. Plusieurs groupes de sécurité peuvent être créés avec des règles différentes que vous pouvez attribuer à chaque instance. AWS dispose d'une documentation détaillée sur les Security Groups (Groupes de sécurité) si vous ne connaissez pas cette fonctionnalité.

Procédure

Étape 1 Cliquez sur **Services** > **EC2**.

Étape 2 Cliquez sur **ECS Dashboard (tableau de bord EC2)** > **Security Groups (groupes de sécurité)**.

Étape 3 Cliquez sur **Create Security Group** (Créer un groupe de sécurité).

Étape 4 Saisissez la commande suivante dans la boîte de dialogue **Create Security Group** (Créer un groupe de sécurité) :

a) Un **Security Group Name** (nom de groupe de sécurité) défini par l'utilisateur pour identifier le groupe de sécurité.
b) Une **Description** de ce groupe de sécurité.
c) Le **VPC** associé à ce groupe de sécurité.

Étape 5 Configurez les **Security Group Rules** (règles du groupe de sécurité) :

a) Cliquez sur **Create Security Group** (Créer un groupe de sécurité).
b) Dans la section **Inbound** (entrée), cliquez sur **Add Rule** (ajouter une règle).

Choisissez l'un des ports d'entrée suivants à ouvrir pour l'accès par Internet dans la liste déroulante **Type**. Par défaut, le type **All Traffic** (Tout le trafic) est sélectionné.

- SSH (22)
- TCP personnalisé (8305)
- HTTP (443)

Remarque
Les accès HTTPS et SSH sont requis pour gérer les Firewall Management Center Virtual à l'extérieur d'AWS. Vous devez préciser les adresses IP sources en conséquence. De plus, si vous configurez à la fois Firewall Management Center Virtual et Firewall Threat Defense Virtual dans le VPC AWS, vous devez autoriser l'accès au sous-réseau de gestion de l'IP privé.

c) Dans la section **Outbound** (trafic sortant), cliquez sur **Add Rule (Ajouter une règle)** pour ajouter une règle pour le trafic sortant, ou conservez les valeurs par défaut de **All traffic** (tout le trafic) (pour **Type**) et **Anywhere** (n'importe où) (pour **Destination**).

Étape 6 Cliquez sur **Create** (Créer) pour créer votre groupe de sécurité.

Prochaine étape

Créez des interfaces réseau comme décrit dans la section suivante.

Créer des interfaces réseau

Vous pouvez créer des interfaces réseau pour le Firewall Management Center Virtual en utilisant des adresses IP statiques. Créez des interfaces de réseau (externes et internes) selon les besoins de votre déploiement particulier.

Procédure

Étape 1 Cliquez sur **Services** > **EC2**.

Étape 2 Cliquez sur **EC2 Dashboard** > **(tableau de bord EC2)** > **Network Interfaces** > **(interfaces réseau)**.

Étape 3 Cliquez sur **Create Network Interface** (Créer une interface réseau).

Étape 4 Saisissez la commande suivante dans la boîte de dialogue **Create Network Interface** (créer une interface réseau) :

a) Une **description** facultative définie par l'utilisateur pour l'interface réseau.
b) Sélectionnez un **Subnet** (sous-réseau) dans la liste déroulante. Assurez-vous de sélectionner le sous-réseau du VPC dans lequel vous souhaitez créer l'instance .

c) Saisissez une adresse **IP privée**. Il est recommandé d'utiliser une adresse IP statique plutôt qu'une **attribution automatique**.
d) Sélectionnez un ou plusieurs **Security groups** (groupes de sécurité). Assurez-vous que tous les ports requis sont ouverts pour le groupe de sécurité.

Étape 5 Cliquez sur **Yes, Create** pour créer votre interface réseau.

Étape 6 Sélectionnez l'interface réseau que vous venez de créer.

Étape 7 Faites un clic droit et sélectionnez **Change Source/Dest pour modifier la source ou la destination. Cochez** .

Étape 8 Choisissez **Disabled** (Désactivé), puis cliquez sur **Save** (Enregistrer).

Répétez cette opération pour toutes les interfaces de réseau que vous créez.

Prochaine étape

Créez des adresses IP Elastic comme décrit dans la section suivante.

Créer des adresses IP Elastic

Lors de la création d'une instance, une adresse IP publique est associée à l'instance. Cette adresse IP publique change automatiquement lorsque vous arrêtez et démarrez l'instance. Pour résoudre ce problème, attribuez une adresse IP publique persistante à l'instance à l'aide de l'adressage IP élastique. Les adresses IP élastiques sont des adresses IP publiques réservées qui sont utilisées pour l'accès à distance au Firewall Management Center Virtual ainsi qu'à d'autres instances. AWS dispose d'une documentation détaillée sur les adresses IP Elastic si vous n'êtes pas familiarisé avec cette fonctionnalité.

Remarque Vous devez au minimum créer une adresse IP élastique pour Firewall Management Center Virtual et deux adresses IP élastiques pour les interfaces de gestion et de diagnostic Firewall Threat Defense Virtual.

Procédure

Étape 1 Cliquez sur **Services** > **EC2**.

Étape 2 Cliquez sur **EC2 Dashboard (Tableau de bord EC2)** > **Elastic IPs (Adresses IP élastiques)**.

Étape 3 Cliquez sur **Allocate New Address** (allouer une nouvelle adresse).

Répétez cette étape pour toutes les adresses IP élastiques ou publiques dont vous avez besoin.

Étape 4 Cliquez sur **Yes, Allocate** (oui, attribuer) pour créer votre adresse IP élastique.

Étape 5 Répétez l'opération pour toutes les adresses IP élastiques requises pour votre déploiement.

Prochaine étape

Déployez Firewall Management Center Virtual comme décrit dans la section suivante.

Déployer Firewall Management Center Virtual

Avant de commencer

- Configurez les éléments VPC AWS et EC2 comme décrit dans Configuring Your AWS Environment (Configuration de votre environnement AWS)
- Confirmez que l'AMI est disponible pour les instances Firewall Management Center Virtual.

Remarque Le mot de passe administrateur par défaut est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details (Détails avancés)** > **User Data (Données utilisateur)**) lors du déploiement initial.

Procédure

Étape 1 Accédez à https://aws.amazon.com/marketplace (Amazon Marketplace) et connectez-vous.

Étape 2 Une fois que vous êtes connecté à Amazon Marché, cliquez sur le lien fourni pour le Firewall Management Center Virtual.

Remarque
Si vous étiez déjà dans AWS, vous devrez peut-être vous déconnecter, puis vous reconnecter pour que le lien fonctionne.

Étape 3 Cliquez sur **Continue** (Continuer), puis cliquez sur l'onglet **Manual Launch** (Lancement manuel) .

Étape 4 Cliquez sur **Accept Terms** pour accepter les conditions.

Étape 5 Cliquez sur **Launch with EC2 Console** (lancer avec la console EC2) dans la région souhaitée

Étape 6 Choisissez un **type d'instance** pris en charge par le Firewall Management Center Virtual ; consultez About Deployment on the AWS Cloud (À propos du déploiement sur le nuage AWS) pour les types d'instances pris en charge.

Étape 7 Cliquez sur le bouton **Next: Configure Instance Details** (suivant; configurer les détails de l'instance au bas de l'écran) :

a) Modifiez le **réseau** pour qu'il corresponde à votre VPC précédemment créé.

b) Modifiez le **sous-réseau** pour qu'il corresponde à votre sous-réseau de gestion précédemment créé. Vous pouvez préciser une adresse IP ou utiliser la génération automatique.

c) Sous **Advanced Details** > **(Détails avancés)** > **User Data (Données utilisateur)**, ajoutez les renseignements de connexion par défaut.

Modifiez l'exemple ci-dessous pour qu'il corresponde à vos exigences en matière de nom d'appareil et de mot de passe.

Exemple de configuration de connexion :

```
#FMC
{
"AdminPassword": "<enter_your_password>",
"Hostname": "<Hostname-vFMC>"
}
```

Mise en garde
Utilisez uniquement du texte brut lors de la saisie des données dans le champ **Advanced Details** (Détails avancés). Si vous copiez ces informations à partir d'un éditeur de texte, assurez-vous de ne copier qu'en texte brut. Si vous copiez des données Unicode dans le champ **Advanced Details** (Détails avancés) , y compris un espace, l'instance peut être corrompue et vous devrez la résilier et la recréer.

Dans les versions 7.0 et ultérieures, le mot de passe administrateur par défaut est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details (Détails avancés)** > **User Data (Données utilisateur)**) lors du déploiement initial.

Dans les versions précédentes, le mot de passe admin par défaut était **Admin123**.

Étape 8 Cliquez sur **Next (Suivant) : Add Storage (Ajouter du stockage)** pour configurer les paramètres de votre périphérique de stockage.

Modifiez les paramètres du volume racine de sorte que la taille du volume (Go) soit de 250 Go. Moins de 250 Go limitera le stockage des événements et n'est pas pris en charge.

Étape 9 Cliquez sur **Next: Tag Instance** (suivant : étiquette d'instance).

Une balise est constituée d'une paire clé-valeur sensible à la casse. Par exemple, vous pouvez définir une balise avec **Key** = Name et **Value** = Management.

Étape 10 Sélectionnez **Next: Configure Security Group** (suivant : configurer le groupe de sécurité).

Étape 11 Cliquez sur **Select an existant Security Group (sélectionner un groupe de sécurité existant)** et choisissez le groupe de sécurité précédemment configuré, ou créez un nouveau groupe de sécurité. Consultez la documentation d'AWS pour de plus amples renseignements sur la création de groupes de sécurité.

Étape 12 Cliquez sur **Review and Launch** (vérifier et lancer).

Étape 13 Cliquez sur **Launch** (lancer).

Étape 14 Sélectionnez une paire de clés existante ou créez-en une nouvelle.

Remarque
Sélectionnez une paire de clés existante ou créez-en une nouvelle. La paire de clés se compose d'une clé publique qu'AWS stocke et d'un fichier de clé privée que l'utilisateur stocke. Ensemble, ils vous permettent de vous connecter à votre instance en toute sécurité. Assurez-vous d'enregistrer la paire de clés à un emplacement connu, car elle pourrait devoir se connecter à l'instance.

Étape 15 Cliquez sur **Launch Instances** (lancer les instances).

Étape 16 Cliquez sur **EC2 Dashboard** > **(Tableau de bord EC2)** > **Elastic IPs (Adresses IP Elastic)** et trouvez une adresse IP précédemment attribuée ou attribuez-en une nouvelle.

Étape 17 Sélectionnez l'adresse IP Elastic, cliquez avec le bouton droit et sélectionnez **Associate Address** (Associer l'adresse).

Localisez l'instance ou l'interface réseau à sélectionner, puis cliquez sur Associate (Associer).

Étape 18 Cliquez sur **EC2 Dashboard** > **(tableau de bord EC2)** > **Instances**.

Étape 19 L'état de l'instance Firewall Management Center Virtual affichera « running » (en cours d'exécution) et Status checks (Vérifications d'état) indiquera pass (réussite) pour « 2/2 checks » (2/2 vérifications) après quelques minutes seulement. Cependant, les processus de déploiement et de configuration initiale prendront entre 30 et 40 minutes. Pour consulter l'état, faites un clic droit sur l'instance, puis sélectionnez **Instance Settings (Paramètres de l'instance)** > **Get Instance Screenshot (Obtenir la capture d'écran de l'instance**.

Une fois la configuration terminée (après environ 30 à 40 minutes), la **capture d'écran de l'instance** doit afficher un message similaire à « Cisco Secure Firewall Management Center pour AWS vW.XY (build ZZ) » et peut-être suivi de lignes de sortie supplémentaires.

Vous devriez alors pouvoir vous connecter au nouveau Firewall Management Center Virtual à l'aide de SSH ou des HTTP. Les délais de déploiement réels peuvent varier en fonction de la charge AWS de votre région.

Vous pouvez accéder à Firewall Management Center Virtual à l'aide de SSH :

```
ssh -i <key_pair>.pem admin@<Public_Elastic_IP>
```

l'authentification SSH est gérée par une paire de clés. Aucun mot de passe n'est requis. Si vous êtes invité à saisir un mot de passe , la configuration est toujours en cours.

Vous pouvez également accéder au Firewall Management Center Virtual à l'aide de HTTPS :

```
https//<Public_Elastic_IP>
```

Remarque
Si vous voyez un message « system startup processes are still running » (les processus de démarrage du système s'exécutent toujours), cela signifie que la configuration n'est pas encore terminée.

Si vous n'obtenez aucune réponse via SSH ou HTTPS, vérifiez ces éléments :

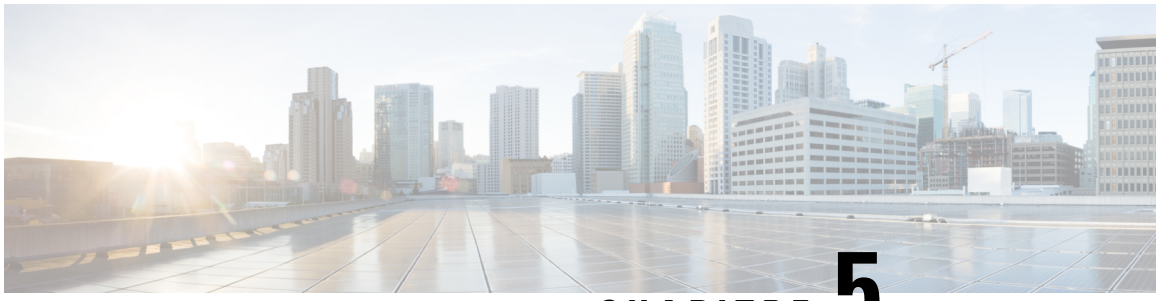
- Assurez-vous que le déploiement est terminé. La capture d'écran de l'instance de machine virtuelle Firewall Management Center Virtual doit afficher un message similaire à « Cisco Secure Firewall Management Center pour AWS vW.XY (build ZZ) » et peut-être suivi de lignes de sortie supplémentaires.
- Assurez-vous d'avoir une adresse IP Elastic associée à l'interface réseau de gestion (eni) du On-Prem Firewall Management Center et que vous vous connectez à cette adresse IP.
- Assurez-vous qu'une passerelle Internet (igw) est associée à votre VPC.
- Assurez-vous que votre sous-réseau de gestion est associé à une table de routage.
- Assurez-vous que la table de routage associé à votre sous-réseau de gestion comporte une route pour « 0.0.0.0/0 » qui pointe vers votre passerelle Internet (igw).
- Assurez-vous que votre groupe de sécurité autorise les SSH et/ou HTTPS entrants des adresses IP auxquelles vous vous connectez.

Prochaine étape

Configuration des politiques et des paramètres de l'appareil

Après avoir installé le Firewall Threat Defense Virtual et ajouté le périphérique au centre de gestion, vous pouvez utiliser l' interface utilisateur On-Prem Firewall Management Center pour configurer les paramètres de gestion des périphériques pour le Firewall Threat Defense Virtual s'exécutant sur AWS et pour configurer et appliquer les politiques de contrôle d'accès et autres politiques connexes pour gérer le trafic en utilisant votre périphérique Firewall Threat Defense Virtual. La politique de sécurité contrôle les services fournis par Firewall Threat Defense Virtual, tels que le filtrage IPS de nouvelle génération et le filtrage d'applications. Vous configurez la politique de sécurité sur Firewall Threat Defense Virtual à l'aide de On-Prem Firewall Management Center. Pour plus d'informations sur la configuration de la politique de sécurité, consultez le Guide de configuration de Cisco Secure Firewall ou l'aide en ligne du Centre de gestion.

-



CHAPITRE 5

Déployer Firewall Management Center Virtual sur Azure à partir du portail AWS.

Vous pouvez déployer le Firewall Management Center Virtual sur le nuage Microsoft Azure.

Important Le Firewall Management Center Virtual sur VMware prend en charge de la version logicielle Cisco 6.4 (ou ultérieure).

Aperçu

Vous déployez le Firewall Management Center Virtual dans Microsoft Azure à l'aide d'un modèle de solution disponible sur le Marché Azure. Lorsque vous déployez le Firewall Management Center Virtual depuis le portail Azure, vous pouvez utiliser un Resource Group (groupe de ressources) et un compte de stockage existants (ou en créer de nouveaux). Le modèle de solution vous guide dans un ensemble de paramètres de configuration qui fournissent la configuration initiale de votre Firewall Management Center Virtual, vous permettant de vous connecter à l'interface Web de Firewall Management Center Virtual après le premier démarrage.

Firewall Management Center Virtual Requiert 28 Go de mémoire vive pour la mise à niveau (6.6.0 ou versions ultérieures)

La plateforme Firewall Management Center Virtual a introduit une nouvelle vérification de la mémoire lors de la mise à niveau. Les mises à niveau de Firewall Management Center Virtual vers la version 6.6.0 ou les versions ultérieures échoueront si vous attribuez moins de 28 Go à l'appliance virtuelle.

Important À partir de la version 6.6.0, les types d'instances à mémoire limitée pour les déploiements Firewall Management Center Virtual sur le nuage (AWS, Azure) sont entièrement abandonnés. Vous ne pouvez plus créer de nouvelles instances Firewall Management Center Virtual en les utilisant, même pour les versions antérieures. Vous pouvez continuer à exécuter les tailles de VM existantes. Consultez Tableau 9 : Tailles de machine virtuelles prises en charge par Azure pour le Firewall Management Center Virtual, à la page 50.

En conséquence, nous ne pourrons pas prendre en charge les tailles de VM à plus faible mémoire sur les plateformes prises en charge.

Le Firewall Management Center Virtual sur Azure doit être déployé dans un réseau virtuel (Virtual Network, VNet) en utilisant le mode de déploiement Resource Manager. Vous pouvez déployer le Firewall Management Center Virtual dans l'environnement de nuage public Azure standard. Le Firewall Management Center Virtual dans le Marché Azure prend en charge le modèle BYOL (Bring Your Own License).

Le tableau suivant résume les tailles de machine virtuelle Azure que Firewall Management Center Virtual prend en charge ; celles prises en charge par les versions 6.5.x et antérieures, et celles prises en charge par les versions 6.6.0 et ultérieures.

Tableau 9 : Tailles de machine virtuelles prises en charge par Azure pour le Firewall Management Center Virtual

Observations	Versions 6.6.0 et ultérieures	Versions 6.5 et antérieures
Firewall Management Center Virtual	Standard_D4_v2 : 8 vCPU, 28 Go	Standard D3_v2 : 4 vCPU, 14 Go
	—	Standard_D4_v2 : 8 vCPU, 28 Go
	* Notez que le Firewall Management Center Virtual ne prendra plus en charge la taille de machine virtuelle Standard_D3_v2 après la sortie de la version 6.6.0. À partir de la version 6.6.0, vous devez déployer le Firewall Management Center Virtual (n'importe quelle version) en utilisant une taille de machine virtuelle avec au moins 28 Go de RAM. Consultez Redimensionnement de la machine virtuelle, à la page 50.	

Tailles de machine virtuelle obsolètes

Vous pouvez continuer à exécuter vos déploiements actuels de la version 6.5.x et les Firewall Management Center Virtual déploiements antérieurs à l'aide de Standard_D3_v2, mais vous ne pourrez pas lancer de nouveaux déploiements Firewall Management Center Virtual (n'importe quelle version) en utilisant cette taille de machine virtuelle.

Redimensionnement de la machine virtuelle

Étant donné que le chemin de mise à niveau de toute version antérieure de Firewall Management Center Virtual (6.2.x, 6.3.x, 6.4.x et 6.5.x) vers la version 6.6.0 comprend la vérification de la mémoire de 28 Go de RAM, si vous utilisez Standard_D3_v2, vous devez redimensionner votre machine virtuelle à Standard_D4_v2 (voir Tableau 9 : Tailles de machine virtuelles prises en charge par Azure pour le Firewall Management Center Virtual, à la page 50).

Vous pouvez utiliser le portail Azure ou PowerShell pour redimensionner votre machine virtuelle. Si la machine virtuelle est en cours d'exécution, la modification de sa taille entraînera son redémarrage. L'arrêt de la machine virtuelle peut révéler des tailles supplémentaires.

Pour des instructions sur la façon de redimensionner votre machine virtuelle, consultez la documentation d'Azure « Redimensionner une machine virtuelle Windows » (https:docs.microsoft.com/en-us/Azure/virtual-machines/Windows/resize-vm).

Prérequis

La prise en charge de Firewall Management Center Virtual sur Microsoft Azure est nouvelle avec la version de la version 6.4.0. Pour la compatibilité de Firewall Management Center Virtual et du système, consultez les Guide de compatibilité de Cisco Secure Firewall Threat Defense.

Vérifiez les éléments suivants avant de déployer le Firewall Management Center Virtual dans Azure :

- Créez un compte sur Azure.com.

  Après avoir créé un compte sur Microsoft Azure, vous pouvez vous connecter, choisir Firewall Management Center Virtual dans le Marché Microsoft Azure et déployer l'offre « On-Prem Firewall Management Center BYOL ».

- Un compte Cisco Smart. Vous pouvez en créer un sur le Centre des logiciels Cisco (https://software.cisco.com/).

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

- Tailles de machines virtuelles Azure prises en charge :
  - Standard_D3_v2 : 4 vCPU, mémoire de 14 Go, taille de disque de 250 Go
  - Standard_D4_v2 : 8 vCPU, mémoire de 28 Go, taille de disque de 400 Go

Licence

Le Firewall Management Center Virtual sur le Marché public Azure prend en charge le modèle Bring Your Own License (BYOL). Pour le Firewall Management Center Virtual, il s'agit d'une licence de plateforme plutôt que d'une licence de fonctionnalité. La version de la licence virtuelle que vous achetez détermine le nombre de périphériques que vous pouvez gérer par l'intermédiaire de Firewall Management Center Virtual. Par exemple, vous pouvez acheter des licences qui vous permettent de gérer deux périphériques, 10 périphériques ou 25 périphériques.

- Modes de licence :
  - Licence Smart uniquement.

Pour plus de détails sur les licences, consultez *Attribution de licence du système* dans le guide de configuration de Cisco Secure Firewall Management Center pour plus d'informations sur la gestion des licences ; Consultez la section Licences de fonctionnalité de Cisco Secure Firewall Management Center pour obtenir un aperçu des licences de fonctionnalités du système, y compris des liens utiles.

Arrêter et redémarrer le système

N'utilisez pas les contrôles **Restart** (Redémarrer) et **Stop** (Arrêter) sur la page de présentation de la machine virtuelle Azure pour démarrer la machine virtuelle Firewall Management Center Virtual. Il s'agit de mécanismes d'arrêt progressifs qui peuvent entraîner la corruption de la base de données.

Utilisez les options **System (Système)** > **Configuration** disponibles dans l'interface web du Firewall Management Center Virtual pour arrêter ou redémarrer l'appliance virtuelle.

Utilisez les commandes `shutdown` (arrêt) and `restart` (redémarrage) depuis l'interface en ligne de commande du Firewall Management Center Virtual pour arrêter ou redémarrer l'appliance.

Fonctionnalités non prises en charge

- Modes de licence :
  - Licence de paiement à l'utilisation (Pay As You Go, PAYG)
  - Réservation de licence permanente (Permanent License Reservation, PLR)
- Gestion
  - Fonction « reset password (réinitialiser le mot de passe) » du portail
  - Récupération de mot de passe sur la console; comme l'utilisateur n'a pas d'accès en temps réel à la console, la récupération du mot de passe est impossible. Il est impossible de démarrer l'image de récupération du mot de passe. Le seul recours est de déployer une nouvelle machine virtuelle Firewall Management Center Virtual.
- Importation/exportation de VM
- La HA n'est pas prise en charge avec Cisco Secure Firewall 7.4.1 et les versions antérieures.
- Génération de VM de 2e génération sur Azure
- Redimensionner la VM après le déploiement
- Migration ou mise à jour de l'UGS de stockage Azure pour le disque du système d'exploitation de la VM de l'UGS premium à l'UGS standard et inversement

Ressources créées lors du déploiement

Lorsque vous déployez Firewall Management Center Virtual dans Azure, les ressources suivantes sont créées :

- La machine Firewall Management Center Virtual avec une interface unique (nécessite un nouveau réseau virtuel ou un réseau virtuel existant avec 1 sous-réseau).
- Un groupe de ressources.

  Firewall Management Center Virtual est toujours déployé dans un nouveau groupe de ressources. Cependant, vous pouvez l'associer à un réseau virtuel existant dans un autre groupe de ressources.
- Un groupe de sécurité nommé *vm name*-mgmt-SecurityGroup

  Le groupe de sécurité sera associé à la Nic0 de la machine virtuelle.

Le groupe de sécurité comprend les règles qui autorisent SSH (port TCP 22) et le trafic de gestion pour l'interface On-Prem Firewall Management Center (port TCP 8305). Vous pourrez modifier ces valeurs après le déploiement.

- Une adresse IP publique (nommée en fonction de la valeur que vous avez choisie lors du déploiement).

  L'adresse IP publique est associée au Nic0 de la VM, lequel correspond à Management (Gestion).

Remarque Vous pouvez créer une nouvelle adresse IP publique ou en choisir une existante. Vous pouvez également choisir **NONE** (AUCUNE). Sans adresse IP publique, toute communication avec le Firewall Management Center Virtual doit provenir du réseau virtuel Azure

- Un tableau de routage pour le sous-réseau (mis à jour s'il existe déjà).
- Un fichier de diagnostic de démarrage dans le compte de stockage sélectionné.

  Le fichier de diagnostic de démarrage sera dans Blobs (objets binaires de grande taille).
- Deux fichiers dans le compte de stockage sélectionné sous Blobs et VHD (disques durs virtuels) de conteneur nommés *VM name*-disk.vhd et *VM name*-<uuid>.status.
- Un compte de stockage (sauf si vous avez choisi un compte de stockage existant).

Important Lorsque vous supprimez une machine virtuelle, vous devez supprimer chacune de ces ressources individuellement, à l'exception de celles que vous souhaitez conserver.

Déployer Firewall Management Center Virtual

Vous pouvez déployer Firewall Management Center Virtual dans Azure à l'aide de modèles. Cisco fournit deux types de modèles :

- **Modèle de solution sur la Place de marché Azure** : Utilisez le modèle de solution disponible sur la Place de marché Azure pour déployer Firewall Management Center Virtual à l'aide du portail Azure. Vous pouvez utiliser un groupe de ressources et un compte de stockage (ou en créer de nouveaux) pour déployer l'appliance virtuelle. Pour utiliser le modèle de solution, consultez Déployer à partir d'Azure Marketplace en utilisant le modèle de solution, à la page 54.
- **Modèles ARM dans le référentiel GitHub** : en plus du déploiement basé sur le Marché, Cisco fournit des modèles de Azure Resource Manager (ARM) dans le référentiel GitHub pour simplifier le processus de déploiement de Firewall Management Center Virtual sur Azure. À l'aide d'une image gérée et de deux fichiers JSON (un fichier de modèle et un fichier de paramètre), vous pouvez déployer et provisionner toutes les ressources du Firewall Management Center Virtual en une seule opération coordonnée.

Remarque Lors de la recherche d'offres Cisco sur le Marché, vous pouvez trouver deux offres différentes avec des noms similaires, mais des types d'offre différents (offre d'application et offre de machine virtuelle).

Pour les déploiements sur le Marché, utilisez UNIQUEMENT les offres d'application.

Offre de machine virtuelle (peut être visible) avec le plan de réservations de logiciels de machine virtuelle (Virtual Machine Software ReservationsVMSR) sur le Marché. Il s'agit de plans d'offre privée multiplateforme offerts pour le canal et la revente. Ils doivent être ignorés pour les déploiements réguliers.

Offres d'applications disponibles sur le Marché :

- Cisco Secure Firewall Management Center Virtual – BYOL
- Cisco Firepower Management Center 300 Virtual (FMCv300)

Déployer à partir d'Azure Marketplace en utilisant le modèle de solution

Déployez le Firewall Management Center Virtual depuis le portail Azure en utilisant le modèle de solution disponible dans Azure Marketplace. La procédure suivante est une liste de haut niveau des étapes à suivre pour configurer le Firewall Management Center Virtual dans Microsoft Azure. Pour connaître les étapes détaillées de la configuration d'Azure, consultez Mise en route d'Azure.

Lorsque vous déployez Firewall Management Center Virtual dans Azure, il génère automatiquement diverses configurations, telles que les ressources, les adresses IP publiques et les tables de routage. Vous pourrez gérer ces configurations après le déploiement. Par exemple, vous pouvez modifier la valeur du délai d'inactivité à partir de la valeur par défaut, qui est un délai d'expiration faible.

Procédure

Étape 1 Connectez-vous au portail Azure (https://portal.azure.com) à l'aide des informations d'authentification de votre compte Microsoft .

Le portail Azure affiche les éléments virtuels associés au compte et à l'abonnement actuels, quel que soit l'emplacement du centre de données.

Étape 2 Cliquez sur **Create a Resource** (Créer une ressource).

Étape 3 Recherchez le Marché pour « On-Prem Firewall Management Center », choisissez l'offre et cliquez sur **Create** (créer).

Étape 4 Configurez les paramètres sous **Basics** (de base).

a) Saisissez un nom pour la machine virtuelle dans le champ **FMC VM name in Azure** (nom de la machine virtuelle FMC dans Azure). Ce nom doit être unique dans votre abonnement Azure.

Attention
Assurez-vous de ne pas utiliser un nom existant, sinon le déploiement échouera.

b) (Facultatif) Choisissez la **version de logiciel FMC** dans la liste déroulante.

Il devrait s'agir de la dernière version disponible par défaut.

c) Saisissez un nom d'utilisateur pour l' administrateur du compte Azure dans le champ **Username for Primary Account** (nom d'utilisateur du compte principal).

Le nom « admin » est réservé dans Azure et ne peut pas être utilisé.

Attention
Le nom d'utilisateur saisi ici est pour le compte Azure, et non pour l'accès administrateur Firewall Management Center Virtual. N'utilisez pas ce nom d'utilisateur pour vous connecter au Firewall Management Center Virtual.

d) Choisissez un type d'authentification, **Password** (Mot de passe) ou **SSH public key** (Clé publique SSH).

Si vous choisissez **Password** (Mot de passe), saisissez un mot de passe et confirmez. Le mot de passe doit comporter entre 12 et 72 caractères ainsi que trois des éléments suivants : un caractère minuscule, un caractère majuscule, un chiffre et un caractère spécial qui n'est pas « \ » ou « - ».

Si vous choisissez une **clé SSH publique**, précisez la clé publique RSA de l'homologue distant.

e) Saisissez un **nom d'hôte FMC** pour le Firewall Management Center Virtual.

f) Entrez le **mot de passe administrateur**.

Voici le mot de passe que vous utiliserez lorsque vous vous connecterez à l'interface Web de Firewall Management Center Virtual en tant qu'administrateur pour configurer le Firewall Management Center Virtual.

g) Choisissez votre type d'**abonnement**.

Normalement, une seule option est répertoriée.

h) Créez un nouveau **Resource Group** (groupe de ressources).

Firewall Management Center Virtual doit être déployé dans un nouveau groupe de ressources. L'option de déploiement dans un groupe de ressources existant ne fonctionne que si ce groupe de ressources est vide.

Cependant, vous pouvez associer Firewall Management Center Virtual à un réseau virtuel existant dans un autre groupe de ressources lors de la configuration des options de réseau aux étapes ultérieures.

i) Sélectionner votre **emplacement** géographique.

Vous devez utiliser le même emplacement pour toutes les ressources utilisées dans ce déploiement. Le Firewall Management Center Virtual, le réseau, les comptes de stockage, etc. doivent tous utiliser le même emplacement.

j) Cliquez sur **OK**.

Étape 5 Ensuite, terminez la configuration initiale sous **Cisco FMCv Settings** (Paramètres Cisco FMCv) :

a) Confirmez la **taille de la machine virtuelle**sélectionnée ou cliquez sur le lien **Change size** (modifier la taille) pour afficher les options de taille de la machine virtuelle. Cliquez sur **Select** (Sélectionner) pour confirmer.

Seules les tailles de machine virtuelle prises en charge sont affichées.

b) Choisissez un **Storage account** (compte de stockage). Vous pouvez utiliser un compte de stockage existant ou en créer un nouveau.

- Saisissez un **nom** pour le compte de stockage, puis cliquez sur **OK**. Le nom du compte de stockage ne peut contenir que des lettres minuscules et des chiffres. Le nom ne peut pas contenir de caractères spéciaux.
- À partir de cette version, le Firewall Management Center Virtual ne prend en charge que le stockage de performance standard à usage général.

c) Choisissez une **adresse IP publique**. Vous pouvez utiliser une adresse IP existante ou en créer une nouvelle.

- Cliquez sur **Create new** (créer de nouveau) pour créer une nouvelle adresse IP publique. Saisissez une étiquette pour l'adresse IP dans le champ **Name** (nom), sélectionnez **Standard** pour l'option UGS , puis cliquez sur **OK**.

Remarque
Azure crée une adresse IP publique dynamique , quel que soit le choix dynamique/statique fait à cette étape. L'adresse IP publique peut changer lorsque la machine virtuelle est arrêtée et redémarrée. Si vous préférez une adresse IP fixe, vous pouvez modifier l'adresse IP publique et la faire passer d'une adresse dynamique à une adresse statique.

- Vous pouvez choisir **NONE** (Aucune) si vous ne souhaitez pas attribuer d'adresse IP publique au Firewall Management Center Virtual. Sans adresse IP publique, toute communication avec le Firewall Management Center Virtual doit provenir du réseau virtuel Azure.

d) Ajoutez une **étiquette DNS** qui correspond à l'étiquette de l'adresse IP publique.

Le nom de domaine complet sera votre étiquette DNS plus l'URL Azure : *<dnslabel>.<location>.cloudapp.azure.com*

e) Choisissez un **réseau virtuel** existant ou créez-en un nouveau, puis cliquez sur **OK**.
f) Configurez le sous-réseau de gestion pour le Firewall Management Center Virtual.

Définissez un **nom de sous-réseau de gestion** et passez en revue le **préfixe de sous-réseau de gestion**. Le nom de sous-réseau recommandé est « management ».

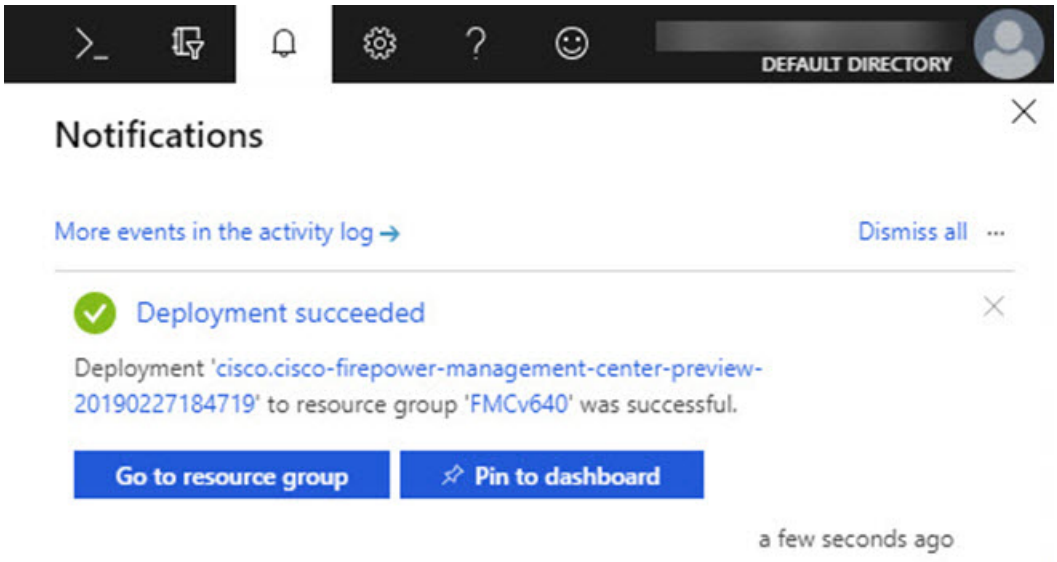
g) Cliquez sur **OK**.

Étape 6 Affichez le résumé de la configuration, puis cliquez sur **OK**.

Étape 7 Affichez les conditions d'utilisation, puis cliquez sur **Create** (Créer).

Étape 8 Sélectionnez **Notifications** (icône de cloche) en haut du portail pour afficher l'état du déploiement.

Illustration 1 : Notifications Azure



À partir de là, vous pouvez cliquer sur le déploiement pour afficher plus de détails ou accéder au groupe de ressources une fois le déploiement réussi. La durée totale jusqu'à ce que Firewall Management Center Virtual soit utilisé est d'environ 30 minutes. Les heures de déploiement varient dans Azure. Attendez qu'Azure signale que la machine virtuelle Firewall Management Center Virtual est en cours d'exécution.

Étape 9 (Facultatif) Azure fournit un certain nombre d'outils pour vous aider à surveiller l'état de votre machine virtuelle, notamment **les diagnostics de démarrage** et **la console de série**. Ces outils vous permettent de voir l'état de votre machine virtuelle lors du démarrage.

a) Dans le menu de gauche, sélectionnez **Virtual machines** (machines virtuelles).
b) Sélectionnez votre machine virtuelle Firewall Management Center Virtual dans la liste. La page de présentation de la machine virtuelle s'ouvre.
c) Faites défiler la section jusqu'à la section **Support + troubleshooting** (Assistance et dépannage) et sélectionnez **Boot diagnostics** (Diagnostics de démarrage) ou **Serial console** (console série). Un nouveau volet s'ouvre avec soit la **capture d'écran** des diagnostics de démarrage et le **journal série**, soit la **console série** en mode texte, et la connexion démarre.

   L'interface Web du Firewall Management Center Virtual est prête si l'invite de connexion s'affiche dans Boot diagnostics ou dans la console série.

   Exemple :

```
Cisco Secure Firewall Management Center for Azure v7.6.0 (build 44)
FMCv76East login:
```

Prochaine étape

- Assurez-vous de vérifier que votre déploiement Firewall Management Center Virtual a réussi. Le tableau de bord Azure répertorie les nouvelles machines virtuelles du Firewall Management Center Virtual sous Resource Groups (Groupes de ressources), ainsi que toutes les ressources connexes (stockage, réseau, table de routage, etc.).

Déployer à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressources

Vous pouvez créer vos propres images Firewall Management Center Virtual personnalisées en utilisant une image VHD compressée disponible auprès de Cisco. Pour déployer à l'aide d'une image de disque dur virtuel, vous devez charger l'image de disque dur virtuel dans votre compte de stockage Azure. Ensuite, vous pouvez créer une image gérée à l'aide de l'image disque chargée et d'un modèle d'Azure Resource Manager. Les modèles Azure sont des fichiers JSON qui contiennent des descriptions de ressources et des définitions de paramètres.

Avant de commencer

- Vous avez besoin du modèle JSON et du fichier de paramètres JSON correspondant pour votre déploiement de modèle Firewall Management Center Virtual. Vous pouvez télécharger ces fichiers à partir du référentiel GitHub.
- Cette procédure nécessite une machine virtuelle Linux existante dans Azure. Nous vous recommandons d'utiliser une machine virtuelle Linux temporaire (comme Ubuntu 16.04) pour charger l'image de disque dur virtuel compressée vers Azure. Cette image nécessite environ 50 Go de stockage lorsqu'elle est décompressée. De plus, vos délais de chargement vers le stockage Azure seront plus rapides à partir d'une machine virtuelle Linux dans Azure.

  Si vous devez créer une machine virtuelle, utilisez l'une des méthodes suivantes :

  - Créer une machine virtuelle Linux avec l'interface de ligne de commande Azure

- Créer une machine virtuelle Linux avec le portail Azure

- Dans votre abonnement Azure, vous devez avoir un compte de stockage disponible à l'emplacement dans lequel vous souhaitez déployer Firewall Management Center Virtual.

Procédure

Étape 1 Téléchargez l'image de disque dur virtuel compressée Firewall Management Center Virtual à partir de la page de téléchargement des logiciels Cisco :

a) Accédez à **Products (Produits)** > **Security (Sécurité)** > **Firewalls (Pare-feu)** > **Firewall Management (Gestion de pare-feu)** > **Secure Firewall Management Center Virtual**.

b) Cliquez sur **Firepower Management Center Software (Logiciel de centre de gestion Firepower)**.

Suivez les instructions pour télécharger l'image.

Par exemple, Cisco_Secure_FW_Mgmt_Center_Virtual_Azure-7.3.0-69.vhd.bz2

Étape 2 Copiez l'image de disque dur virtuel compressée sur votre machine virtuelle Linux dans Azure.

Il existe de nombreuses options que vous pouvez utiliser pour déplacer des fichiers vers Azure et à partir d'Azure. Cet exemple montre SCP ou copie sécurisée :

```
# scp /username@remotehost.com/dir/Cisco_Secure_FW_Mgmt_Center_Virtual_Azure-7.3.0-69.vhd.bz2
<linux-ip>
```

Étape 3 Connectez-vous à la machine virtuelle Linux dans Azure et accédez au répertoire où vous avez copié l'image de disque dur virtuel compressée.

Étape 4 Décompressez l'image de disque dur virtuel Firewall Management Center Virtual.

Il existe de nombreuses options que vous pouvez utiliser pour décompresser des fichiers. Cet exemple montre l'utilitaire Bzip2, mais des utilitaires basés sur Windows fonctionneraient également.

```
# bunzip2 Cisco_Secure_FW_Mgmt_Center_Virtual_Azure-7.3.0-69.vhd.bz2
```

Étape 5 Chargez le disque dur virtuel dans un conteneur dans votre compte de stockage Azure. Vous pouvez utiliser un compte de stockage existant ou en créer un nouveau. Le nom du compte de stockage ne peut contenir que des lettres minuscules et des chiffres.

Il existe de nombreuses options que vous pouvez utiliser pour téléverser un disque virtuel sur votre compte de stockage, notamment AntCopy, l'API de blocage de copie de stockage Azure, Azure Stockage Explorer, l'interface de ligne de commande Azure ou le portail Azure. Nous ne recommandons pas l'utilisation du portail Azure pour un fichier aussi volumineux que le disque dur virtuel Firewall Management Center Virtual.

L'exemple suivant montre la syntaxe à l'aide de l'interface de ligne virtuelle Azure :

```
azure storage blob upload \
       --file <unzipped vhd> \
       --account-name <azure storage account> \
       --account-key yX7txxxxxxxx1dnQ== \
       --container <container> \
       --blob <desired vhd name in azure> \
       --blobtype page
```

Étape 6 Créez une image gérée à partir du disque dur virtuel :

a) Dans le portail Azure, sélectionnez **Images**.

b) Cliquez sur **Add** (ajouter) pour créer une nouvelle image.
c) Fournir les renseignements suivants :

- **Subscription** (abonnement) : choisissez un abonnement dans la liste déroulante.
- **Resource group**(groupe de ressources) : choisissez un groupe de ressources existant ou créez-en.
- **Name** (nom) : saisissez un nom défini par l'utilisateur pour l'image gérée.
- **Region** (région) : choisissez la région dans laquelle la machine virtuelle est déployée.
- **OS type** (type de système d'exploitation) : choisissez **Linux** comme type de système d'exploitation.
- **VM genreation** (génération de la machine virtuelle) : choisissez **Gen 1**.

  Remarque
  Gen 2 n'est pas prise en charge.

- **Srorage blob** (objet biniare de stockage) : accédez au compte de stockage pour sélectionner le disque dur virtuel chargé.
- **Account type** (type de compte) : selon vos besoins, choisissez Standard HDD, Standard SSD ou Premium SSD dans la liste déroulante.

  Lorsque vous sélectionnez la taille de machine virtuelle planifiée pour le déploiement de cette image, assurez-vous que la taille de machine virtuelle prend en charge le type de compte sélectionné.
- **Host caching** (mise en mémoire cache de l'hôte) : choisissez Read/write (lecture/écriture) dans la liste déroulante.
- **Data disks**(disques de données) : laissez à la valeur par défaut; n'ajoutez pas de disque de données.

d) Cliquez sur **Create** (créer).

Attendez que le message **Successfully create image** (création d'image réussie) apparaisse sous l'onglet **Notifications**.

Remarque
Une fois que l'image gérée est créée, le disque dur virtuel chargé et le compte de stockage de charge peuvent être supprimés.

Étape 7 Obtenez l'ID de ressource de la nouvelle image gérée.

En interne, Azure associe chaque ressource à un ID de ressource. Vous aurez besoin de l'ID de ressource lorsque vous déployez de nouveaux pare-feu Firewall Management Center Virtual à partir d' de pare-feu de cette image gérée.

a) Dans le portail Azure, sélectionnez **Images**.
b) Sélectionnez l'image gérée créée à l'étape précédente.
c) Cliquez sur **Overview** (aperçu) pour afficher les propriétés de l'image.
d) Copier l'**ID de ressource** dans le presse-papiers.

L'ID de ressource (**Resource ID**) prend la forme de :

/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>

Étape 8 Créez des Firewall Management Center Virtualpare-feu en utilisant l'image gérée et un modèle de ressource :

a) Sélectionnez **New** (nouveau) et recherchez **Template Deployment** (déploiement de modèle) jusqu'à ce que vous puissiez le sélectionner dans les options.
b) Sélectionnez **Create** (créer).
c) Sélectionnez **Build your own template in the editor** (créer votre propre modèle dans l'éditeur).

   Vous avez un modèle vide qui peut être personnalisé. Consultez GitHub pour les fichiers de modèle.

d) Collez votre code de modèle JSON personnalisé dans la fenêtre, puis cliquez sur **Save** (enregistrer).
e) Choisissez un **Subscription** (abonnement) dans la liste déroulante.
f) Choisissez un **Resource group** (groupe de ressources) existant ou créez-en un nouveau.
g) Choisissez un **Location** (emplacement) dans la liste déroulante.
h) Collez l'**ID de ressource** d'image gérée de l'étape précédente dans le champ **Vm Managed Image ID** (ID de l'image gérée de machine virtuelle).

Étape 9 Cliquez sur **Edit Parameters** (Modifier les paramètres) en haut de la page **Custom Deployment** (Déploiement personnalisé). Un modèle de paramètres est disponible pour la personnalisation.

a) Cliquez sur **Load file** (charger le fichier) et accédez au fichier de paramètres Firewall Management Center Virtual personnalisé. Consultez GitHub pour les paramètres de modèle.
b) Collez votre code de paramètres JSON personnalisé dans la fenêtre, puis cliquez sur **Save** (enregistrer).

Étape 10 Passer en revue les détails du déploiement personnalisé. Assurez-vous que les informations dans **Bases** (bases) et **Settings** (paramètres) correspondent à la configuration de déploiement attendue, y compris l'**ID de ressource**.

Étape 11 Passez en revue les conditions générales et cochez la case **I agree to the terms and conditions stated above** (j'accepte les conditions générales énoncées ci-dessus).

Étape 12 Cliquez sur **Purchase** (acheter) pour déployer une de pare-feu Firewall Management Center Virtual à l'aide de l'image gérée et d'un modèle personnalisé.

S'il n'y a aucun conflit dans vos fichiers de modèle et de paramètres, le déploiement devrait avoir réussi.

L'image gérée est disponible pour plusieurs déploiements dans le même abonnement et la même région.

Prochaine étape

- Mettez à jour la configuration IP du Firewall Management Center Virtual dans Azure.

Déployer les offres Azure Marketplace dans l'environnement restreint Azure Private Marketplace

Cela s'applique uniquement aux utilisateurs d'Azure Private Marketplace (Marché privé Azure). Si vous utilisez Azure Private Marketplace, assurez-vous que les offres d'applications et les offres de machine virtuelle requises (masquées) sont activées pour l'utilisateur sur le Marché privé respectif.

Offres et forfaits de machines virtuelles (masqués) :

- ID éditeur : **cisco**
- Offres de machine Cisco Secure Firewall Management Center Virtual (utilisées pour les deux offres d'applications Cisco Secure Firewall Management Center Virtual)
  - ID de l'offre : **cisco-fmcv**

- ID du forfait BYOL : **fmcv-azure-byol**

- Cisco Firepower Management Center 300 Virtual
  - ID de l'offre : **cisco-fmcv300**
  - ID du forfait BYOL : **fmcv300-Azure-byol**

Lorsque l'utilisateur déploie l'offre d'application visible à partir du Marché, l'image correspondante du forfait d'offre de machine virtuelle est référencée et déployée.

Par conséquent, pour que le déploiement fonctionne, les offres d'application et de machine virtuelle doivent être activées/disponibles sur le Marché privé pour le détenteur/ l'abonnement Azure.

Consultez la documentation d'Azure pour activer ces offres d'applications et de machines virtuelles sur les marchés privés.

- Gouverner et contrôler à l'aide du Marché Azure privé
- Ajouter une offre à un Marché privé
- Set-AzMarketplacePrivateStoreOffer

Les offres d'applications sont facilement activées par l'intermédiaire de l'interface utilisateur d'Azure, car elles sont visibles sur le Marché.

Afin d'activer les offres de machines virtuelles masquées sur le Marché privé, vous devrez peut-être vous fier aux commandes de la CLI (au moment de la création de ce document, seule la méthode CLI est possible).

Exemple de commande :

Le forfait Cisco Secure Firewall Management Center Virtual BYOL peut être activé à l'aide de l'exemple de commande similaire donné ci-dessous :

```
$Params = @{
  privateStoreId = '<private-store-id>'
  offerId = '<publisher-id>.<vm-offer-id>'
  SpecificPlanIdsLimitation =@('<plan-id-under-vm-offer>')
}
Set-AzMarketplacePrivateStoreOffer @Params

$Params = @{
  privateStoreId = '<private-store-id>'
  offerId = 'cisco.cisco-fmcv'
  SpecificPlanIdsLimitation =@('fmcv-azure-byol')
}
Set-AzMarketplacePrivateStoreOffer @Params
```

Remarque L'exemple de commande est uniquement à titre de référence. Consultez la documentation d'Azure pour plus de détails.

Message d'erreur de référence

```
{
  "code": "MarketplacePurchaseEligibilityFailed",
  "details": [
    {
      "code": "BadRequest",
```

```
     "message": "Offer with PublisherId: 'cisco', OfferId: 'cisco-XXXX' cannot be purchased
 due to validation errors. For more information see details.
Correlation Id: 'XXXXX`
This plan is not available for purchase because it needs to be added to your tenant's Private
 Marketplace. Contact your admin to request adding the plan.
Link to plan: <URL>.
Plan: '<PLAN NAME>'(planId=<VM-OFFER-PLAN-ID>),
Offer: <OFFER_NAME>, Publisher: 'Cisco Systems, Inc.'(publisherId='cisco').
…
…
    }
  ],
  "message": "Marketplace purchase eligibilty check returned errors. See inner errors for
details. "
}
```

L'utilisateur peut rencontrer l'erreur ci-dessus lors du déploiement de l'offre de Marché. Pour résoudre ce problème, les offres d'application et de machine virtuelle doivent être activées/disponibles sur le détenteur/ l'abonnement Azure.

Vérifier le déploiement de Firewall Management Center Virtual

Après la création de la machine virtuelle Firewall Management Center Virtual, le tableau de bord Microsoft Azure répertorie la nouvelle machine virtuelle Firewall Management Center Virtual sous Groupes de ressources. Le compte de stockage et les ressources réseau correspondants sont également créés et répertoriés. Le tableau de bord fournit une vue unifiée de vos ressources Azure et permet d'évaluer d'un coup d'œil l'intégrité et la performance du Firewall Management Center Virtual.

Avant de commencer

La machine virtuelle Firewall Management Center Virtual est démarrée automatiquement. Pendant le déploiement, l'état est « Creating (Création) » pendant la création de la VM, puis « Running (En cours d'exécution) » une fois le déploiement terminé.

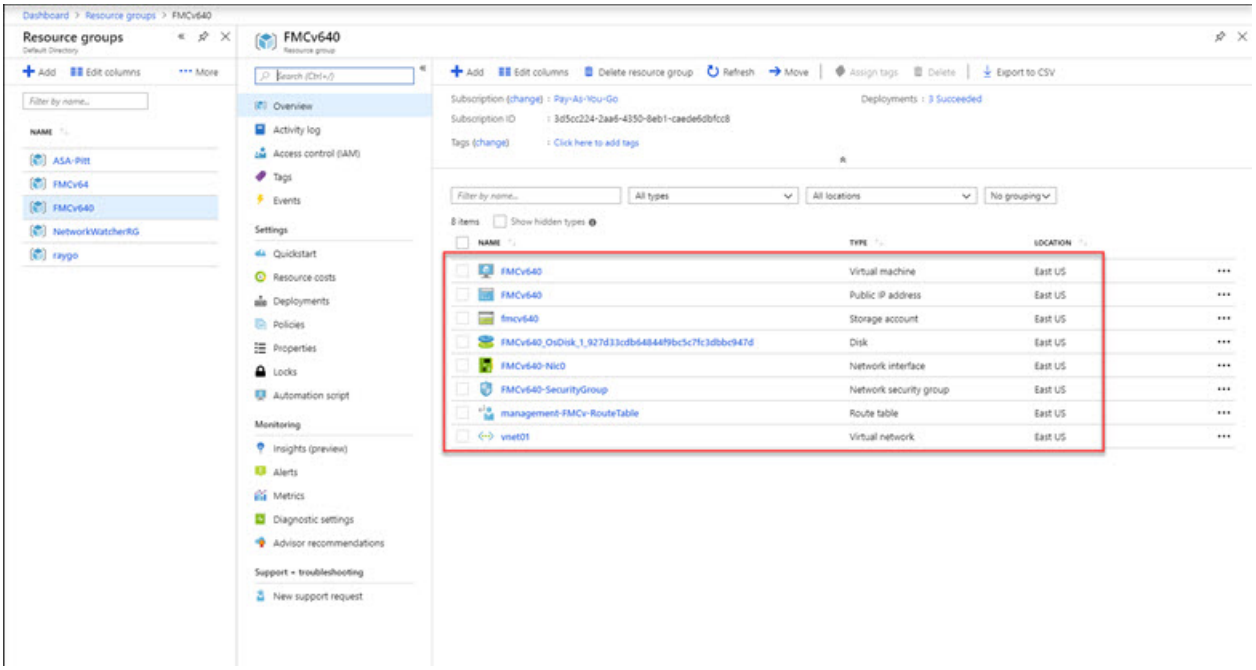
Remarque N'oubliez pas que les délais de déploiement varient dans Azure et que le temps total jusqu'à ce que Firewall Management Center Virtual soit utilisable est d'environ 30 minutes, même lorsque le tableau de bord Azure indique l'état de la machine virtuelle Firewall Management Center Virtual indique « Running » (En cours d'exécution).

Procédure

Étape 1 Pour afficher le groupe de ressources Firewall Management Center Virtual et ses éléments après le déploiement, cliquez sur **Resource groups** (Groupes de ressources) dans le menu de gauche.

La figure suivante montre un exemple de page de groupes de ressources dans le portail Microsoft Azure. Remarquez la machine virtuelle Firewall Management Center Virtual ainsi que ses ressources correspondantes (compte de stockage, ressources réseau, etc.).

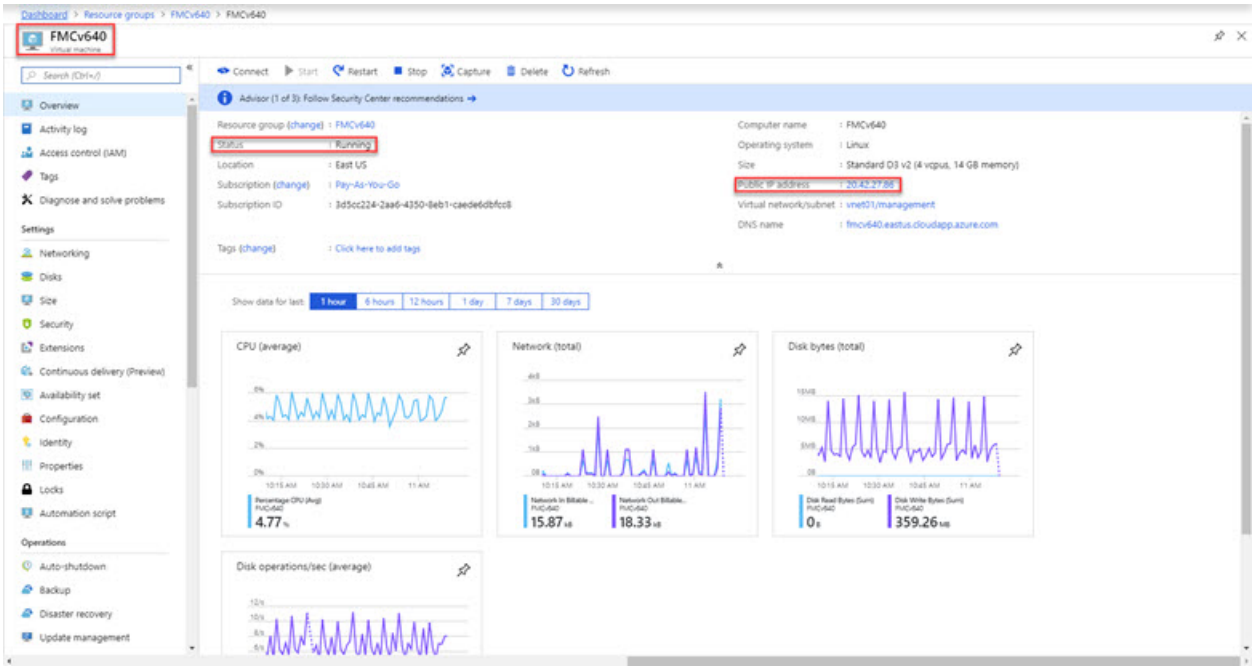
Illustration 2 : Page Azure Firewall Management Center Virtual Resource Group



Étape 2 Pour afficher les détails de la machine virtuelle Firewall Management Center Virtual associée au groupe de ressources, cliquez sur le nom de la machine virtuelle Firewall Management Center Virtual.

La figure suivante montre un exemple de la page de présentation de la **machine virtuelle** associée à la machine virtuelle Firewall Management Center Virtual. Vous accédez à cette présentation à partir de la page Groupes de ressources.

Illustration 3 : Présentation de la machine virtuelle



Notez que l'état est Running (En cours d'exécution). Vous pouvez arrêter, démarrer, redémarrer et supprimer la machine virtuelle Firewall Management Center Virtual à partir de la page de la **machine virtuelle** du portail Microsoft Azure. Notez que ces contrôles ne sont pas des mécanismes d'arrêt progressif pour Firewall Management Center Virtual; consultez Lignes directrices et limites relatives à la licence, à la page 51 pour obtenir des renseignements sur l'arrêt progressif.

Étape 3 Dans la page **Virtual machine** (machine virtuelle), trouvez l' **adresse IP publique** attribuée au Firewall Management Center Virtual.

Remarque
Vous pouvez survoler l'adresse IP et sélectionner **Click to copy** (Cliquez pour copier) pour copier l'adresse IP.

Étape 4 Dirigez votre navigateur vers **https:***public_ip/*, où *public_ip* est l'adresse IP attribuée à l'interface de gestion de Firewall Management Center Virtuallorsque vous avez déployé la machine virtuelle.

La page d'ouverture de session s'affiche.

Étape 5 Connectez-vous en utilisant **admin** comme nom d'utilisateur et le mot de passe du compte admin que vous avez spécifié lors du déploiement de la machine virtuelle.

Prochaine étape

- Nous vous recommandons d'effectuer certaines tâches administratives qui facilitent la gestion de votre déploiement, comme la création d'utilisateurs et l'examen des politiques d'intégrité et de système. Reportez-vous à Firewall Management Center Virtual Administration et configuration initiale, à la page 133 pour savoir comment commencer.
- Vous devez également vérifier les exigences d'enregistrement et de licence de votre périphérique.
- Pour démarrer la configuration de votre système, consultez le guide de configuration de Secure Firewall Management Center et le correspondant à votre version.

Surveillance et résolution des problèmes

Cette section comprend des directives générales en matière de surveillance et de dépannage pour l'appareil Firewall Management Center Virtual déployé dans Microsoft Azure. La surveillance et le dépannage peuvent être liés au déploiement de la machine virtuelle dans Azure ou à l'appareil Firewall Management Center Virtual lui-même.

Supervision Azure du déploiement de la machine virtuelle

Azure fournit un certain nombre d'outils dans le menu **Soutien + dépannage** qui vous permettent d'accéder rapidement aux outils et aux ressources pour vous aider à diagnostiquer et à résoudre les problèmes et à recevoir de l'aide supplémentaire. Voici deux éléments d'intérêt :

- **Boot diagnostics** (Diagnostics de démarrage) : vous permettent de voir l'état de votre machine virtuelle Firewall Management Center Virtual lors du démarrage. Les diagnostics de démarrage recueillent les informations de journal série de la machine virtuelle ainsi que les captures d'écran. Cela peut vous aider à diagnostiquer les problèmes de démarrage.

- **Serial console** (Console série): la console série de machine virtuelle dans le portail Azure permet d'accéder à une console de texte. Cette connexion série se rattache au port série COM1 de la machine virtuelle et offre un accès série et SSH (SSH) à l'interface en ligne de commande du Firewall Management Center Virtual en utilisant l'adresse IP publique attribuée au Firewall Management Center Virtual.

Supervision et connexion Firewall Management Center Virtual.

Les dépannages et les opérations générales de journalisation suivent les mêmes procédures que les modèles On-Prem Firewall Management Center et Firewall Management Center Virtual actuels. Consultez la section *System Monitoring and Troubleshooting* (Surveillance et dépannage du système) des guide de configuration de Cisco Secure Firewall Management Center pour votre version.

De plus, l'agent Microsoft Azure Linux (wanagent) gère le provisionnement Linux et l'interaction de la machine virtuelle avec le contrôleur de structure Azure. À ce titre, les journaux suivants sont importants pour le dépannage :

- **/var/log/wanagent.log** - Ce journal contiendra des erreurs du provisionnement de On-Prem Firewall Management Center avec Azure.
- **/var/log/firstboot.S07install_waagent** - Ce journal contiendra toute erreur liée à l'installation de waagent.

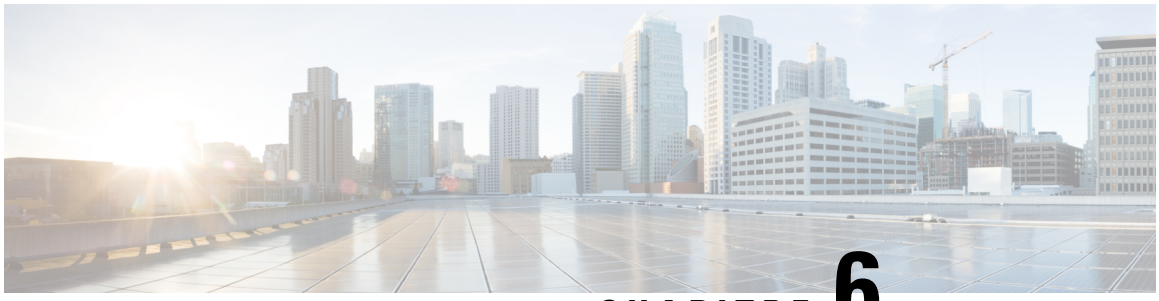
Échecs de provisionnement Azure

Les erreurs de provisionnement à l'aide du modèle de solution Azure Marketplace (Marché Azure) sont rares. Cependant, si vous rencontrez une erreur de provisionnement, tenez compte des points suivants :

- Azure dispose d'un délai d'expiration de 20 minutes pour que la machine virtuelle la provisionne avec le wanagent, auquel cas elle redémarre.
- Si On-Prem Firewall Management Center a des problèmes de provisionnement pour une raison quelconque, la minuterie de 20 minutes a tendance à se terminer au milieu de l'initialisation de la base de données On-Prem Firewall Management Center, ce qui entraîne probablement un échec du déploiement.
- Si On-Prem Firewall Management Center échoue au provisionnement en 20 minutes, nous vous recommandons de recommencer.
- Vous pouvez consulter le */var/log/wanagent.log* pour obtenir des renseignements de dépannage.
- Si vous voyez des erreurs de connexion HTTP dans la console série, cela signifie que l'agent ne peut pas communiquer avec la structure. Vous devez vérifier vos paramètres réseau lors du redéploiement.

Historique de la fonctionnalité

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Déployer le Firewall Management Center Virtual sur Microsoft Azure Cloud	6.4.0	Assistance initiale.



CHAPITRE 6

Déployer le Firewall Management Center Virtual sur GCP

Google Cloud Platform (GCP) est un service en nuage public fourni par Google qui vous permet de créer et d'héberger des applications de l'infrastructure évolutive de Google. Le nuage privé virtuel (VPC) de Google vous offre la possibilité d'évoluer et de contrôler la façon dont les charges de travail se connectent à l'échelle régionale et mondiale. GCP vous permet de créer vos propres VPC en plus de l'infrastructure publique de Google.

Vous pouvez déployer le Firewall Management Center Virtual sur le GCP.

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 le GCP public. Il peut ensuite être configuré pour gérer les périphériques virtuels et physiques.

Prise en charge des types de machines GCP

Firewall Management Center Virtual prend en charge les machines de calcul optimisé et les machines à usage général (types de machines standard, à mémoire élevée et à processeur élevé). Firewall Management Center Virtual prend en charge les types de machines GCP suivants :

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

Tableau 10 : Types de machines optimisées pour le calcul prises en charge

Types de machines optimisées pour le calcul	Attributs	
	vCPU	RAM (Go)
c2-standard-8	8	32 Go
c2-standard-16	16	64 Go

Tableau 11 : Types de machines générales prises en charge

Types de machines à usage général	Attributs	
	vCPU	RAM (Go)
n1-standard-8	8	30 Go
n1-standard-16	16	60 Go
n2-standard-8	8	32
n2-standard-16	16	64
n1-highcpu-32	32	28.8
n2-highcpu-32	32	32
n1-highmem-8	8	52
n1-highmem-16	16	104
n2-highmem-4	4	32
n2-highmem-8	8	64

Prérequis

- Créez un compte GCP à l'adresse https : //cloud.google.com.
- 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 de la On-Prem Firewall Management Center.
  - Consultez la section « Licence du système » dans le Guide de configuration On-Prem Firewall Management Center pour en savoir plus sur la gestion des licences.

- Exigences d'interface :
  - Interface de gestion : une interface utilisée pour connecter le périphérique au Firewall Threat Defense au On-Prem Firewall Management Center.
- Chemins de communication :
  - Adresse IP publique permettant l'accès administratif au On-Prem Firewall Management Center.
- 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

- Déploiement dans le moteur de traitement de GCP
- Maximum de 32 vCPU par instance (selon le type de machine GCP)
- Licences : Seul le protocole BYOL est pris en charge

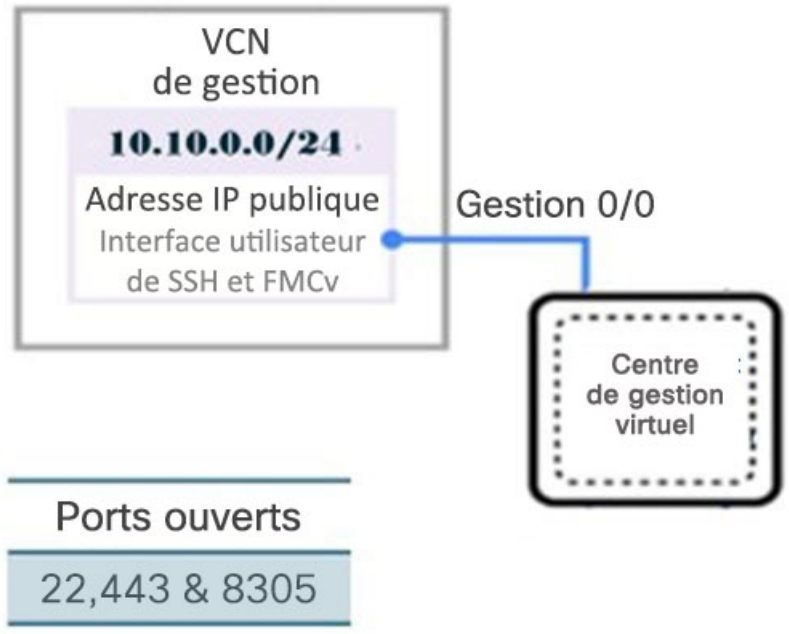
Fonctionnalités non prises en charge

- IPv6
- Haute accessibilité en natif Firewall Management Center Virtual
- Évolutivité automatique
- Modes transparent/en ligne/passif
- Mode multi-contexte

Exemple de topologie de réseau

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

Illustration 4 : Exemple de topologie pour le déploiement Firewall Management Center Virtual sur GCP



Déployer Firewall Management Center Virtual

Les procédures suivantes décrivent comment préparer votre environnement GCP et lancer l'instance Firewall Management Center Virtual.

Créer des réseaux vPC

Le déploiement Firewall Management Center Virtual nécessite le Management VPC (VPC de gestion) pour la gestion Firewall Management Center Virtual. Consultez la figure 1 à la page 3 comme guide.

Procédure

Étape 1 Dans la console GCP, choisissez **VPC networking** (réseaux VPC), puis cliquez sur **Create VPC Network** (créer un réseau VPC).

Étape 2 Dans le champ **Name** (nom), saisissez le nom descriptif de votre réseau VPC.

Étape 3 Dans le **Subnet creation mode** (mode de création de sous-réseau), cliquez sur **Custom** (personnalisé).

Étape 4 Dans le champ **Name** (Nom) sous **New subnet** (nouveau sous-réseau), saisissez le nom souhaité.

Étape 5 Dans la liste déroulante **Region** (région), sélectionnez la région appropriée pour votre déploiement.

Étape 6 Dans le champ **IP address range** (plage d'adresses IP), saisissez le sous-réseau du premier réseau au format CIDR, par exemple 10.10.0.0/24.

Étape 7 Acceptez les valeurs par défaut de tous les autres paramètres, puis cliquez sur **Create** (Créer).

Créer les règles de pare-feu

Chacun des réseaux VPC nécessite des règles de pare-feu pour autoriser SSH et le trafic. Créez les règles de pare-feu pour chaque réseau VPC.

Procédure

Étape 1 Dans la console GCP, choisissez **Networking (réseautage)** > **VPC network (réseau VPC)** > **Firewall (pare-feu)**, puis cliquez sur **Create Firewall Rule** (créer une règle de pare-feu).

Étape 2 Dans le champ **Name** (nom), saisissez un nom descriptif pour votre règle de pare-feu, par exemple, *vpc-asiasouth-mgmt-ssh*.

Étape 3 Dans la liste déroulante **Network** (réseau), sélectionnez le nom du réseau VPC pour lequel vous créez la règle de pare-feu, par exemple, *fmcv-south-mgmt*.

Étape 4 Dans la liste déroulante **Targets (** (cibles), sélectionnez l'option applicable à votre règle de pare-feu, par exemple, **All instances in the network** (toutes les instances du réseau).

Étape 5 Dans le champ **Source IP ranges** (plages IP sources), saisissez les plages d'adresses IP sources au format CIDR, par exemple, 0.0.0.0/0.

Le trafic n'est autorisé que par des sources comprises dans ces plages d'adresses IP.

Étape 6 Sous **Protocols and ports** (protocoles et ports), sélectionnez **Specified protocols and ports** (protocoles et ports spécifiés).

Étape 7 Ajoutez vos règles de sécurité :

a) Ajouter une règle pour autoriser SSH (TCP/22).

b) Ajoutez une règle pour autoriser le port TCP 443.

Vous accédez à l'UI Firewall Management Center Virtual qui exige l'ouverture du port 443 pour les connexions HTTPS.

Étape 8 Cliquez sur **Create** (créer).

Créer l'instance Firewall Management Center Virtual sur GCP

Vous pouvez suivre les étapes ci-dessous pour déployer l'instance Firewall Management Center Virtual à partir de la console GCP.

Procédure

Étape 1 Connectez-vous à la console GCP.

Étape 2 Cliquez sur **Navigation menu** > **(menu de navigation)** > **Marketplace** > **(Marché)**.

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

Étape 4 Cliquez sur **Launch** (lancer).

a) **Deployment name** (nom de déploiement) : Précisez un nom unique pour l'instance.

b) **Version de l'image** : sélectionnez la version dans la liste déroulante.

c) **Zone** : Sélectionnez la zone dans laquelle vous souhaitez déployer Firewall Management Center Virtual.

d) **Type de machine** : Choisissez le bon type de machine en fonction de Prise en charge des types de machines GCP, à la page 67.

e) **SSH key (clé SSH, facultatif)** : Collez la clé publique de la paire de clés SSH.

La paire de clés se compose d'une clé publique que GCP stocke et d'un fichier de clé privée que l'utilisateur stocke. Ensemble, ils vous permettent de vous connecter à votre instance en toute sécurité. Assurez-vous d'enregistrer la paire de clés à un emplacement connu, car elle devra se connecter à l'instance.

f) Choisissez d'autoriser ou de **bloquer les clés SSH à l'échelle du projet pour l'accès à cette instance**. Consultez la documentation de Google Autoriser ou bloquer les clés SSH publiques à l'échelle du projet à partir d'une instance Linux.

g) **Startup script** (Script de démarrage) : fournissez la configuration day0 (jour0) pour le Firewall Management Center Virtual.

L'exemple suivant montre une configuration day0 (jour0) que vous pouvez copier et coller dans le champ **Startup script** (Script de démarrage) :

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

Astuces
Pour éviter les erreurs d'exécution, vous devez valider votre configuration day0 à l'aide d'un programme de validation JSON.

h) Sélectionnez le **Boot disk type** (Type de disque de démarrage) dans la liste.

Par défaut, le **Standard Persistent Disk** (Disque persistant standard) est sélectionné. Cisco vous recommande d'utiliser le type de disque de démarrage par défaut.

i) La valeur par défaut **de la taille du disque de démarrage en Go** est de 250 Go. Cisco vous recommande de conserver la taille par défaut du disque de démarrage. Elle ne peut pas être inférieure à 250 Go.

j) Cliquez sur **Add network interface** (ajouter une interface de réseau) pour configurer l'interface de gestion (Management).

Remarque
Vous ne pouvez pas ajouter des interfaces à une instance après l'avoir créée. Si vous créez l'instance avec une configuration d'interface incorrecte, vous devez supprimer l'instance et la recréer avec la configuration d'interface appropriée.

- Dans la liste déroulante **Network** (réseau), sélectionnez un réseau VPC, par exemple, *vpc-branch-mgmt*.
- Dans la liste déroulante **External IP** (adresse IP externe), sélectionnez l'option appropriée.

  Pour l'interface de gestion, sélectionnez **External IP** (Adresse IP externe) à **Ephemeral** (Éphémère).
- Cliquez sur **Done (Terminé)**.

k) **Firewall** (pare-feu) : Appliquez les règles de pare-feu.

- Cochez la case **Allow TCP port 22 traffic from the Internet (SSH access)** (autoriser le trafic du port TCP 22 de l'Internet, accès SSH) pour autoriser SSH.
- Cochez la case **Allow HTTPS traffic from the Internet (FMC GUI)** (Autoriser le trafic HTTPS de l'Internet (interface FMC)) pour autoriser les connexions HTTPS.
- Cochez la case **Allow HTTPS traffic from the Internet** (SFTunnel comm.) (autoriser le trafic HTTPS de l'Internet (comm. SFTunnel) pour permettre au Firewall Management Center Virtual et aux périphériques gérés de communiquer à l'aide d'un canal de communication chiffré SSL bidirectionnel (SFTunnel).

l) Cliquez sur **More** (plus) pour développer l'affichage et assurez-vous que **IP Forwarding** (transfert IP) est défini sur **On** (activé).

Étape 5 Cliquez sur **Deploy** (déployer).

Remarque
Le délai de démarrage dépend d'un certain nombre de facteurs, notamment la disponibilité des ressources. L'initialisation peut prendre jusqu'à 35 minutes. N'interrompez pas l'initialisation, sinon vous devrez peut-être supprimer l'appareil et recommencer.

Prochaine étape

Affichez les détails de l'instance dans la page d'instance de VM de la console GCP. Vous trouverez l'adresse IP interne, l'adresse IP externe et les contrôles pour arrêter et démarrer l'instance. Vous devez arrêter l'instance si vous devez la modifier.

Accéder à l'instance Firewall Management Center Virtual sur GCP

Assurez-vous d'avoir déjà activé une règle de pare-feu pour autoriser les connexions SSH (TCP par le port 22) pendant le déploiement ; consultez Créer les règles de pare-feu, à la page 71 pour plus d'information.

Cette règle de pare-feu active l'accès à l'instance Firewall Management Center Virtual et vous permet de vous connecter à l'instance en utilisant les méthodes suivantes.

- External IP (IP externe)
  - Fenêtre du navigateur
  - Tout autre outil client SSH ou tiers
- Console de série
  - Ligne de commande Gcloud

Consultez la documentation de Google, Connexion aux instances pour en savoir plus.

Remarque Si vous choisissez de ne pas ajouter de configuration Day0, vous pouvez vous connecter à l'instance Firewall Management Center Virtual en utilisant les informations d'authentification par défaut. 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 la console de série

Procédure

Étape 1 Dans la console GCP, choisissez **Compute Engine (Moteur de calcul)** > **VM instances (Instances de VM)**.

Étape 2 Cliquez sur le nom de l'instance Firewall Management Center Virtual pour ouvrir la page des renseignements de l'instance de machine virtuelle (**VM instance details**).

Étape 3 Sous l'onglet **Details** (Détails), cliquez sur **Connect to serial console** (Se connecter à la console série).

Consultez la documentation de Google, Interagir avec la console série pour en savoir plus.

Se connecter à l'instance Firewall Management Center Virtual à l'aide d'une adresse IP externe

L'instance Firewall Management Center Virtual se voit attribuer une adresse IP interne et une adresse IP externe. Vous pouvez utiliser l'adresse IP externe pour accéder à l'instance Firewall Management Center Virtual.

Procédure

Étape 1 Dans la console GCP, choisissez **Compute Engine (Moteur de calcul)** > **VM instances (Instances de VM)**.

Étape 2 Cliquez sur le nom de l'instance Firewall Management Center Virtual pour ouvrir la page des renseignements de l'instance de machine virtuelle (**VM instance details**).

Étape 3 Sous l'onglet **Details** (Détails), cliquez sur le menu déroulant du champ **SSH**.

Étape 4 Sélectionnez l'option souhaitée dans le menu déroulant **SSH**.

Vous pouvez vous connecter à l'instance Firewall Management Center Virtual en utilisant la méthode suivante.

- Tout autre outil client SSH ou tiers : consultez l'information sur la connexion à l'aide d'outils tiers de la documentation de Google pour en savoir plus.

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

Procédure

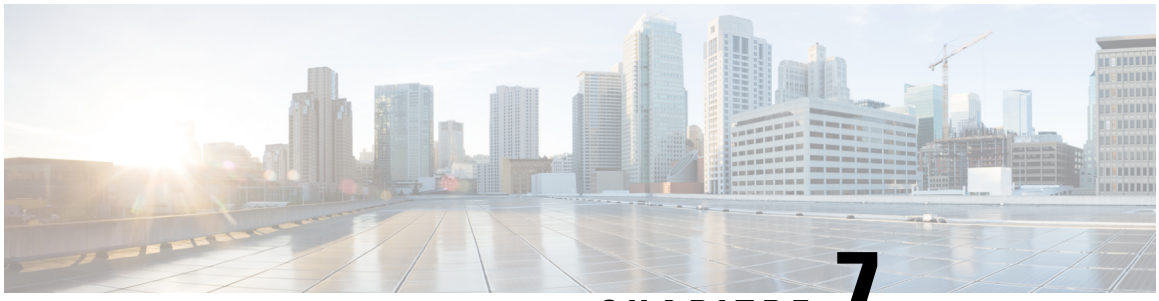
Étape 1 Dans la console GCP, choisissez **Compute Engine (Moteur de calcul)** > **VM instances (Instances de VM)**.

Étape 2 Cliquez sur le nom de l'instance Firewall Management Center Virtual pour ouvrir la page des renseignements de l'instance de machine virtuelle (**VM instance details**).

Étape 3 Sous l'onglet **Details** (Détails), cliquez sur le menu déroulant du champ **SSH**.

Étape 4 Cliquez sur **View gcloud command (Voir la commande gcloud)** > **Run in Cloud Shell (Exécuter dans Cloud Shell)**.

La fenêtre de terminal Cloud Shell s'ouvre. Consultez la documentation de Google, Présentation de l'outil de ligne de commande gcloudet Calcul gcloud ssh pour en savoir plus.



CHAPITRE 7

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

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 12 : 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 13 : 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.

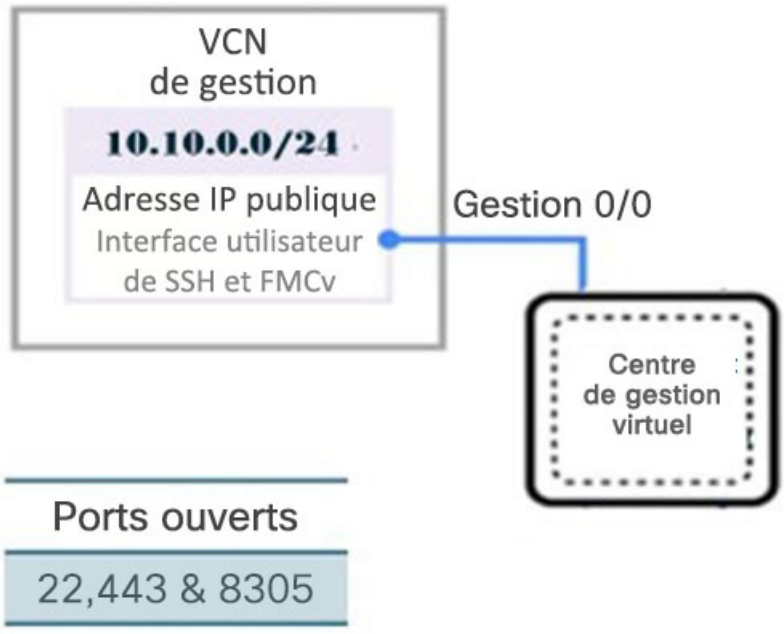
Fonctionnalités partiellement prises en charge

- 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 5 : 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).

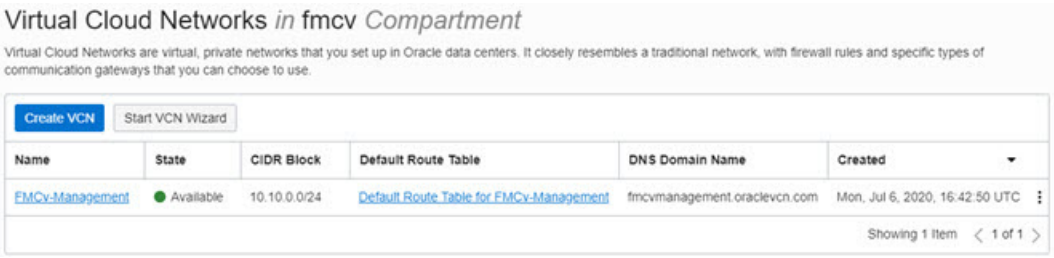
Étape 8 Sélectionnez une **Security List** (liste de sécurité) que vous avez créée précédemment.

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 6 : 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 77).

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 :

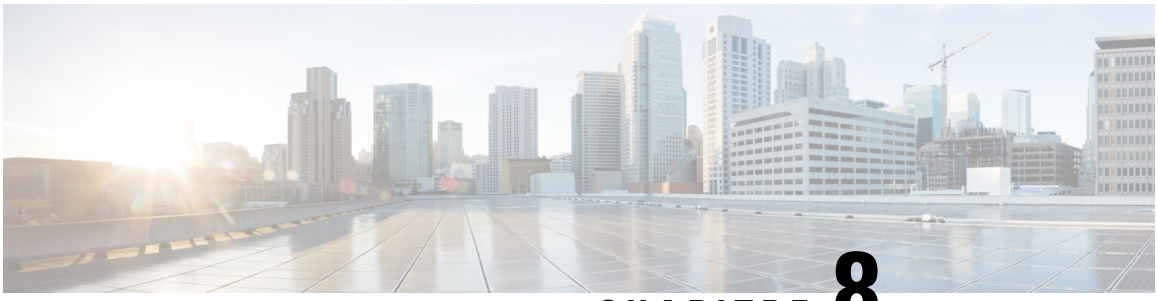
```
$ ssh –i <private_key> <username>@<public-ip-address>
```

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.



CHAPITRE 8

Déployer Firewall Management Center Virtual sur OpenStack

Vous pouvez déployer Firewall Management Center Virtual sur OpenStack.

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 91.
- 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 14 : 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/

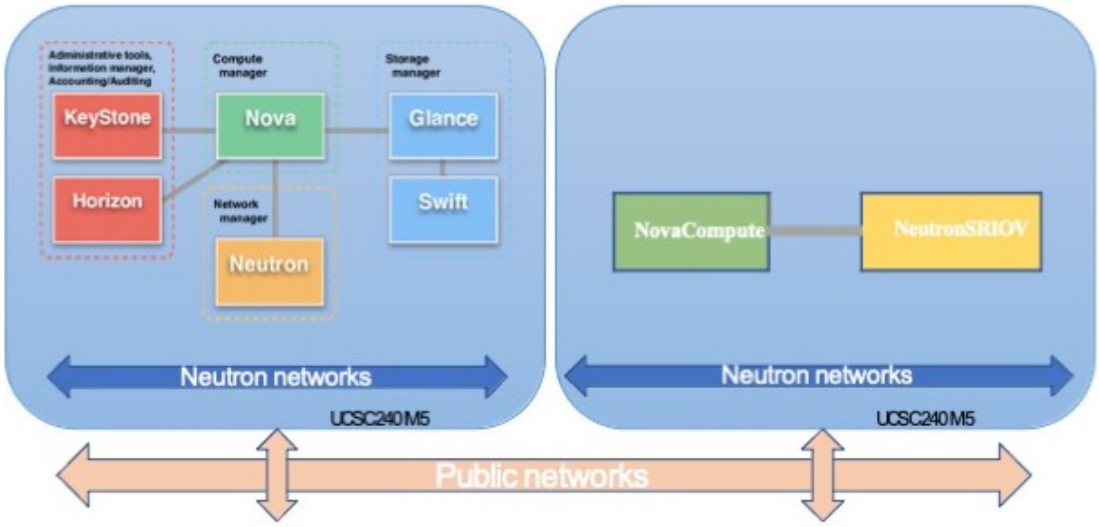
Tableau 15 : Configuration matérielle et logicielle requise pour Cisco VIM Managed OpenStack

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.

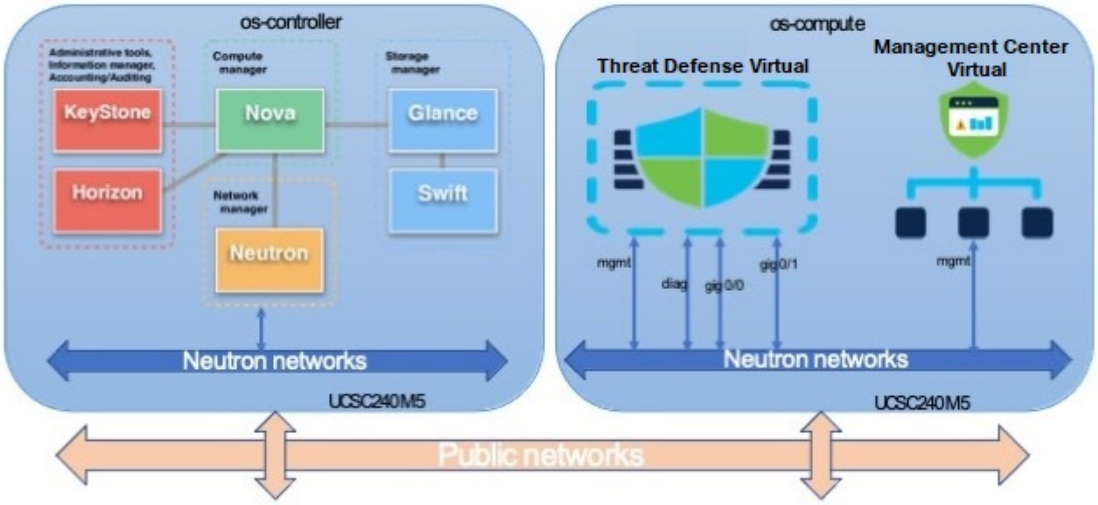
Illustration 7 : Topologie de la plateforme OpenStack



Exemple de topologie de réseau

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

Illustration 8 : 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 :

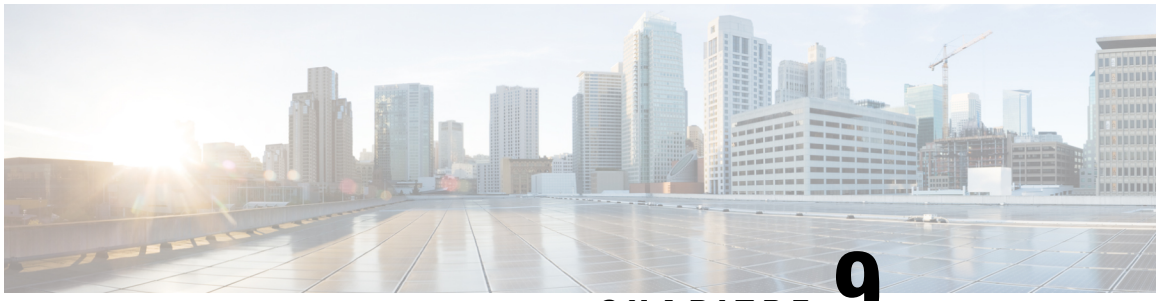
```
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| id                  | 96c8c126-107b-4733-8f6c-eb15a637219f |
| stack_name          | fmcv-stack                           |
| 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 |
+--------------------------------------+-------------+----------------------------------+----------------+
```



CHAPITRE 9

Déployer le Firewall Management Center Virtual sur Cisco HyperFlex

Les systèmes Cisco HyperFlex offrent une hyperconvergence pour toutes les applications et partout. Hyperflex, associé à la technologie Cisco Unified Computing System (Cisco UCS) gérée par la plateforme d'exploitation du nuage Cisco Intersight, peut propulser les applications et les données n'importe où, optimiser les opérations d'un centre de données central vers la périphérie et dans les nuages publics, et augmenter ainsi l'agilité en accélérant les pratiques DevOps.

Vous pouvez déployer Firewall Management Center Virtual sur Cisco HyperFlex.

Configuration système requise

Firewall Management Center Virtual nécessite 28 Go de RAM

Nous vous recommandons de ne pas diminuer les paramètres par défaut : 32 Go de RAM pour la plupart des instances Firewall Management Center Virtual, . 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 déployer le Firewall Management Center Virtual à l'aide du provisionnement de grappe HyperFlex hébergé sur les hyperviseurs HyperFlex ESX et ESXi . Consultez les Guide de compatibilité de Cisco Secure Firewall Threat Defense .
- Pour le Firewall Management Center Virtual, 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.

- Le tableau suivant répertorie les paramètres recommandés et par défaut de l'appareil Firewall Management Center Virtual.

Important Assurez-vous d'allouer suffisamment de mémoire pour assurer les performances optimales de votre Firewall Management Center Virtual. Si votre Firewall Management Center Virtual a une mémoire inférieure à 32 Go, des problèmes de déploiement de politiques peuvent survenir. Ne réduisez pas les paramètres par défaut, car il s'agit du minimum requis pour exécuter le logiciel système.

Tableau 16 : Paramètres de l'appliance virtuelle Firewall Management Center Virtual

Paramètres	Minimum	Par défaut	Recommandations	Paramètre réglable?
Mémoire	28 Go	32 Go	32 Go	Avec restrictions.
Processeurs virtuels	4	4	8	Oui, jusqu'à 8
Taille provisionnée du disque dur	250 Go	250 Go	S.O.	Non, selon la sélection du format de disque.

Tableau 17 : Paramètres de l'appliance virtuelle Firewall Management Center Virtual 300

Paramètres	Par défaut	Paramètre réglable?
Mémoire	64 Go	Oui
Processeurs virtuels	32	Non
Taille provisionnée du disque dur	2.2 To	Non, selon la sélection du format de disque.

Pour obtenir la liste des plateformes prises en charge et les exigences matérielles et logicielles détaillées, consultez le Guide de compatibilité.

Lignes directrices et limites relatives à la licence

Restrictions

Les limites suivantes existent lorsque vous déployez le Firewall Management Center Virtual pour Cisco HyperFlex :

- 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.
- Le clonage d'une machine virtuelle n'est pas pris en charge.

- La restauration d'une machine virtuelle à partir d'un instantané n'est pas prise en charge.
- VMware Workstation, Player, Server et Fusion ne reconnaissent pas l'emballage OVF et ne sont pas pris en charge.

Lignes directrices relatives aux fichiers OVF

Les appliances virtuelles utilisent l'emballage Open Virtual Format (OVF). Vous déployez une appliance virtuelle au moyen d'un modèle OVF d'infrastructure virtuelle (VI). Le choix du fichier OVF dépend de la cible de déploiement :

Pour le déploiement sur vCenter—Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-**VI**-*X.X.X-xxx*.ovf

où *X.X.X-xxx* est la version et le numéro de version du logiciel du système que vous souhaitez déployer. Le processus d'installation vous permet d'effectuer la configuration initiale complète de l'appareil Firewall Management Center Virtual. Vous pouvez préciser :

- Un nouveau mot de passe du compte administrateur.
- Paramètres réseau qui permettent à l'appareil de communiquer sur votre réseau de gestion.

Prise en charge de la haute disponibilité

Vous pouvez établir la haute disponibilité (haute disponibilité) entre deux appareils Firewall Management Center Virtual déployés sur l'hôte Hyperflex :

- Les deux appareils Firewall Management Center Virtual d'une configuration à haute disponibilité doivent être du même modèle.
- Pour établir la haute disponibilité Firewall Management Center Virtual, Firewall Management Center Virtual nécessite un droit de licence Firewall Management Center Virtual supplémentaire pour chaque appareil Firewall Threat Defense qu'il gère dans la configuration à haute disponibilité. Cependant, le droit de licence pour la fonctionnalité Firewall Threat Defense requise pour chaque appareil Firewall Threat Defense n'a pas de changement, quelle que soit la configuration à haute disponibilité Firewall Management Center Virtual. Voir *Exigences de licence pour les périphériques Threat Defense dans une paire à haute disponibilité*dans le Guide d'administration du Guide de configuration Cisco Secure Firewall Management Center Device pour les directives de licences.
- Si vous rompez la paire à haute disponibilité Firewall Management Center Virtual, le droit de licence supplémentaire Firewall Management Center Virtual est libéré et vous n'avez besoin que d'un seul droit pour l'appareil Firewall Threat Defense.

Consultez la section *Haute disponibilité* dans le Guide d'administration Cisco Secure Firewall Management Center pour connaître les directives de haute disponibilité.

Documents connexes

Notes de version pour la plateforme de données Cisco HX

Guides de configuration de la plateforme de données Cisco HX

Cisco HyperFlex 4.0 pour l'infrastructure de serveur virtuel avec VMware ESXi

Aperçu des solutions des systèmes HyperFlex de Cisco

La feuille de route de la documentation des systèmes Cisco HyperFlex

Déployer Firewall Management Center Virtual

Utilisez cette procédure pour déployer l'appareil Firewall Management Center Virtual sur Cisco HyperFlex sur un serveur vSphere vCenter Server.

Avant de commencer

- Assurez-vous d'avoir déployé Cisco HyperFlex et effectué toutes les tâches de configuration consécutives à l'installation. Pour en savoir plus, consultez la feuille de route de la documentation des systèmes Cisco HyperFlex.
- Vous devez avoir au moins un réseau configuré dans vSphere (pour la gestion) avant de déployer le Firewall Management Center Virtual.
- Téléchargez le fichier de modèle VI OVF Firewall Management Center Virtual à partir de Cisco.com : *Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-X.X.X-xxx.ovf*, où *X.X.X-xxx* est la version et le numéro de version.

Procédure

Étape 1 Connectez-vous au client web vSphere.

Étape 2 Sélectionnez la grappe HyperFlex dans laquelle vous souhaitez déployer le Firewall Management Center Virtual, et cliquez sur **ACTIONS** > **Deploy OVF Template (déployer le modèle OVF)**.

Étape 3 Parcourez votre système de fichiers à la recherche de l'emplacement de la source du modèle OVF, puis cliquez sur **Next** (suivant).

Sélectionnez le modèle VI OVF Firewall Management Center Virtual :

Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-X.X.X-xxx.ovf

où *X.X.X-xxx* est la version et le numéro de version du fichier d'archive que vous avez téléchargé.

Étape 4 Spécifiez un nom et un dossier pour le déploiement Firewall Management Center Virtual, puis cliquez sur **NEXT** (Suivant).

Étape 5 Sélectionnez une ressource de traitement informatique et attendez la vérification de compatibilité. Si la vérification de compatibilité réussit, cliquez sur **NEXT** (suivant).

Étape 6 Passez en revue les renseignements sur le modèle OVF (nom du produit, version, prestataire, taille de téléchargement, taille sur le disque et description), puis cliquez sur **NEXT** (suivant).

Étape 7 Passez en revue et acceptez le contrat de licence qui accompagne le modèle OVF (modèles VI uniquement), puis cliquez sur **NEXT** (suivant).

Étape 8 Sélectionnez un emplacement de stockage et un format de disque virtuel, puis cliquez sur **NEXT** (suivant).

Dans cette fenêtre, sélectionnez parmi les banques de données déjà configurées dans la grappe HyperFlex de destination. Le fichier de configuration de la machine virtuelle et les fichiers de disque virtuel sont stockés dans la banque de données. Sélectionnez un magasin de données suffisamment grand pour contenir la machine virtuelle et tous ses fichiers de disque virtuel.

Lorsque vous sélectionnez **Thick Provisioned** (grand provisionnement) comme format de disque virtuel, tout l'espace de stockage est immédiatement attribué. Lorsque vous sélectionnez**Thin Provisioned**(provisionnement léger) comme format de disque virtuel, le stockage est attribué à la demande, au fur et à mesure que les données sont écrites sur les

disques virtuels. Le provisionnement léger peut également réduire le temps nécessaire pour déployer l'appliance virtuelle.

Étape 9 Mappez les réseaux précisés dans le modèle OVF aux réseaux de votre inventaire, puis sélectionnez **NEXT** (suivant).

Étape 10 Définissez les propriétés configurables par l'utilisateur fournies avec le modèle OVF :

Remarque
Vous devez obligatoirement configurer toutes les personnalisations requises à cette étape.

a) **Mot de passe**

Définissez le mot de passe pour l'accès admin Firewall Management Center Virtual.

b) **Réseau**

Définissez les renseignements sur le réseau, notamment le nom de domaine complet (FQDN), le DNS, le domaine de recherche et le protocole de réseau (IPv4).

c) Cliquez sur **NEXT** (suivant).

Étape 11 Passez en revue et vérifiez les renseignements affichés. Pour commencer le déploiement avec ces paramètres, cliquez sur **FINISH** (terminer). Pour apporter des modifications, cliquez sur **BACK** (Retour) pour accéder aux écrans précédents.

Après avoir terminé la démarche guidée par l'assistant, le client Web vSphere gère la machine virtuelle; vous pouvez voir l'état « Initalize OVF Deployment » (initier le déploiement OVF) dans le volet des tâches récentes (**Recent Tasks**) de la zone d'information globale (**Global Information**).

Lorsqu'il a terminé, vous voyez l'état d'achèvement du déploiement du modèle OVF.

L'instance Firewall Management Center Virtual apparaît dans le centre de données spécifié dans l'inventaire. Le démarrage de la nouvelle machine virtuelle peut prendre jusqu'à 30 minutes.

Remarque
Pour enregistrer avec succès Firewall Management Center Virtual auprès de l'autorité de licence de Cisco, On-Prem Firewall Management Center nécessite un accès Internet. Vous devrez effectuer une configuration supplémentaire après le déploiement pour obtenir un accès Internet et un enregistrement de licence réussi. La configuration du serveur DNS est obligatoire pour l'enregistrement de la licence.

Prochaine étape

Pour initialiser l'appliance virtuelle ; voir Mettre sous tension et initialiser l'appliance virtuelle, à la page 22

Mettre sous tension et initialiser l'appliance virtuelle

Après avoir terminé le déploiement de l'appliance virtuelle, l'initialisation démarre automatiquement lorsque vous activez l'appliance virtuelle pour la première fois.

Mise en garde Le délai de démarrage dépend d'un certain nombre de facteurs, notamment la disponibilité des ressources du serveur. L'initialisation peut prendre entre sept et huit minutes. N'interrompez pas l'initialisation, sinon vous devrez peut-être supprimer l'appareil et recommencer.

Procédure

Étape 1 Mettez l'appareil sous tension.

Dans le client vSphere , cliquez avec le bouton droit sur le nom de votre appliance virtuelle dans la liste d'inventaire, puis sélectionnez **Power (Mise sous tension)** > **Power On (Mettre sous tension)** dans le menu contextuel.

Étape 2 Surveillez l'initialisation sur la console de machine virtuelle.

Prochaine étape

Après avoir déployé le Firewall Management Center Virtual, vous devez terminer un processus de configuration pour permettre au nouveau périphérique de communiquer sur votre réseau de gestion de confiance. Si vous déployez un modèle OVF VI sur Hyperflex, la configuration de Firewall Management Center Virtual est un processus en deux étapes.

- Pour terminer la configuration initiale de Firewall Management Center Virtual, consultez Configuration initiale Firewall Management Center Virtual, à la page 123.
- Pour un aperçu des prochaines étapes nécessaires à votre déploiement Firewall Management Center Virtual, consultez le guide de démarrage de Cisco Secure Firewall Management Center Virtual.

CHAPITRE 10

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 106
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 108
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 109
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 113

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 113 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

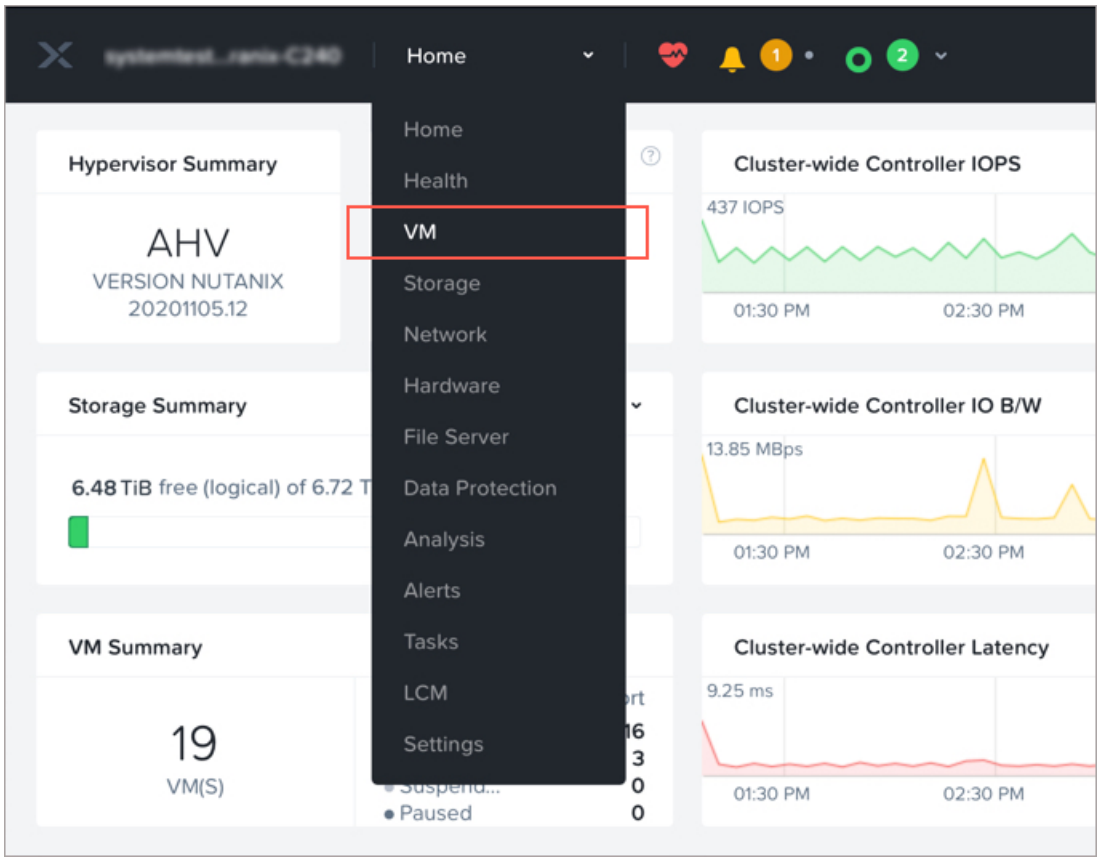
Avant de commencer

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 113.

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 114.

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, à la page 123.
- 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)

CHAPITRE 11

Déployer le Firewall Management Center Virtual sur Hyper-V

Microsoft Hyper-V est la plateforme de virtualisation matériel de Microsoft, également appelée *hyperviseur*. Hyper-V permet aux administrateurs de mieux utiliser le matériel en utilisant le même serveur physique pour exécuter plusieurs machines virtuelles.

Les machines virtuelles offrent plus de flexibilité, permettent d'économiser des coûts et constituent un moyen plus efficace d'utiliser le matériel que d'exécuter un seul système d'exploitation sur le matériel physique.

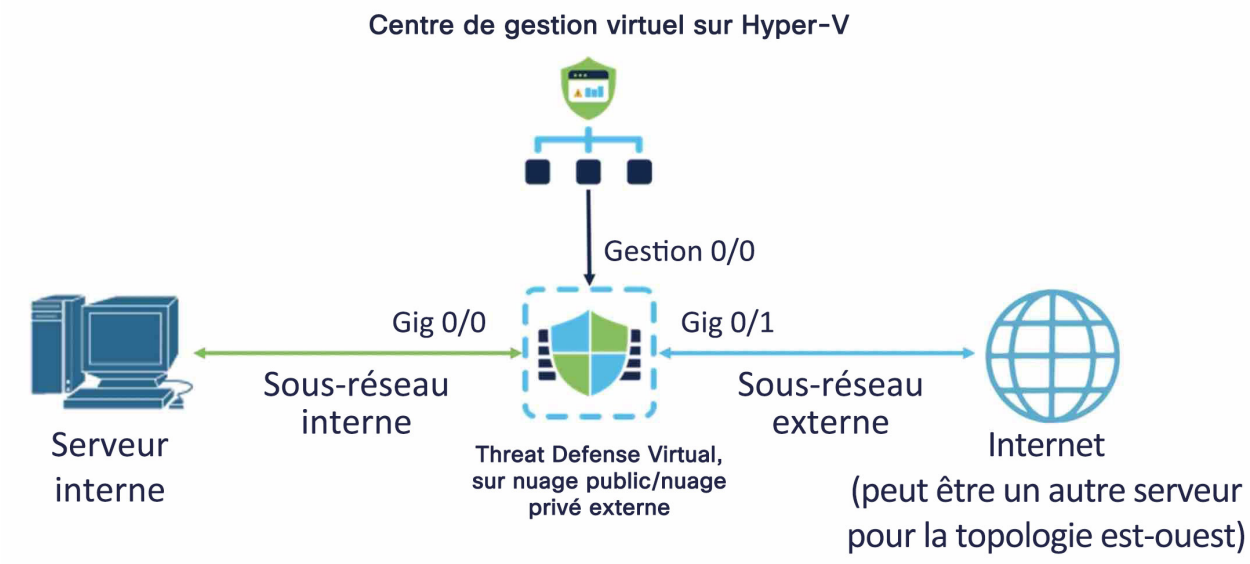
Le présent chapitre contient les sections suivantes :

Aperçu

Le centre virtuel est déployé sur Hyper-V à l'aide d'une image VHD disponible sur Cisco.com. Les fonctionnalités de contrôle de machine virtuelle de base telles que l'accès à la console, l'arrêt/redémarrage, la prise en charge d'IPv4 et d'IPv6 pour l'interface de gestion sont prises en charge. La configuration initiale est effectuée à l'aide d'un script de configuration day-0 . La haute disponibilité est prise en charge.

Exemple de topologie de Management Center Virtual (Centre de gestion virtuel) sur Hyper-V

Dans cet exemple de topologie, Management Center Virtual est connecté au port de gestion de Threat Defense Virtual déployé sur un nuage privé ou public externe. Threat Defense Virtual est connecté à Internet et à un serveur interne. Internet peut également être un autre serveur dans une topologie de flux de trafic est-ouest.



Serveur Windows pris en charge pour Management Center Virtual

Management Center Virtual 25 est pris en charge sur Windows Server 2019 Édition standard. Les exigences minimales en ressources pour Management Center Virtual sont indiquées ci-dessous :

- CPU : 4 vCPU
- RAM : 28 Go (32 Go recommandé)
- Stockage : 250 Go
- Nombre minimal d'interfaces : 1

Directives et limites du Management Center Virtual sur Hyper-V

- Le Management Center Virtual déployé sur Hyper-V peut être utilisé pour gérer des grappes virtuelles de défense contre les menaces qui sont déployées sur d'autres nuages publics ou privés. Cependant, pour gérer les grappes virtuelles de défense contre les menaces déployées sur le nuage public, vous devez

enregistrer manuellement la grappe avec le centre de gestion virtuel. Voir Ajouter la grappe au Management Center — déploiement manuel

- Le clonage n'est pas pris en charge.

Licences pour le déploiement de Management Center Virtual sur Hyper-V

Les types de licences suivants sont pris en charge :

- BYOL
  - Licence Smart
  - Réservation d'une licence spécifique (SLR)
  - Universal Permanent License Registration (PLR)
- Licence d'évaluation.

Préalables pour le déploiement de Management Center Virtual sur Hyper-V

- Microsoft Windows Server avec le rôle Hyper-V et le gestionnaire Hyper-V installés. Consultez Premiers pas avec Hyper-V sur le serveur Windows Server.
- Téléchargez l'image VHD compressée de Management Center Virtual depuis Cisco.com.
- Licence BYOL
- Nouveau commutateur virtuel (vSwitch) et nouvelle machine virtuelle (VM)

Déployer Management Center Virtual

Effectuez les procédures ci-dessous pour déployer le Management Center Virtual sur Hyper-V.

Télécharger l'image VHD du centre de gestion virtuelle

Téléchargez l'image VHD compressée de Management Center Virtual depuis la page Téléchargement de logiciels Cisco vers votre machine locale :

1. Accédez à **Products (Produits) > Security (Sécurité) > Firewalls (Pare-feu) > Firewall Management (Gestion des pare-feu) > Secure Firewall Management Center Virtual**.
2. Cliquez sur **Firepower Management Center Software** (Logiciel Firepower Management Center) et téléchargez l'image VHD requise. Par exemple, Cisco_Secure_FW_Mgmt_Center_Virtual_Azure-7.4.0-xxxx.vhd.tar.

Préparer le fichier de configuration Day 0 (jour 0)

Vous devez préparer un fichier de configuration Day-0 avant de lancer le Management Center Virtual (FMCv). Ce fichier est un fichier texte qui contient les données de configuration initiale appliquées lors du déploiement d'une machine virtuelle. Cette configuration initiale est placée dans un fichier texte nommé **day0-config** sur votre machine locale, puis convertie en fichier day0.iso qui est monté et lu au premier démarrage.

Remarque Le fichier day0.iso doit être disponible lors du premier démarrage.

Précisez les paramètres suivants dans le fichier de configuration de Day-0 :

- 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.

Remarque L'exemple ci-dessous utilise Linux, mais des utilitaires similaires existent pour Windows.

Procédure

Étape 1 Saisissez la configuration de la CLI pour Management Center Virtual dans un fichier texte appelé **day0-config**. Ajoutez les paramètres réseau et les informations nécessaires à la gestion du Management Center Virtual.

```
{
"EULA": "accept",
"Hostname": "virtual731265",
"AdminPassword": "r2M$9^Uk69##",
"DNS1": "208.67.222.222",
"DNS2": "208.67.222.222",
"IPv4Mode": "Manual",
"IPv4Addr": "10.10.0.92",
"IPv4Mask": "255.255.255.224",
"IPv4Gw": "10.10.0.65",
"IPv6Mode": "Manual",
"IPv6Addr": "2001:420:5440:2010:600:0:45:45",
"IPv6Mask": "112",
"IPv6Gw": "2001:420:5440:2010:600:0:45:1"
}
```

Étape 2 Générez le CD-ROM virtuel en convertissant le fichier texte en fichier ISO :

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

ou

```
/ usr/bin/mkisofs -r -o day0.iso day0-config
```

Créer un nouveau commutateur virtuel

Effectuez cette procédure pour créer un nouveau commutateur virtuel (vSwitch).

Procédure

Étape 1 Dans l'onglet Hyper-V Manager **Actions** du gestionnaire Hyper-V, cliquez sur **Virtual Switch Manager** (Gestionnaire de commutateur virtuel).

Étape 2 Cliquez sur **Virtual Switches > New virtual network switch** (commutateur virtuel > nouveau commutateur de réseau virtuel).

Étape 3 Dans la fenêtre **Create virtual Switch** (créer un commutateur virtuel), sélectionnez **External** (Externe).

Étape 4 Cliquez sur **Create Virtual Switch** (Créer un commutateur virtuel).

Étape 5 Dans la fenêtre **Virtual Switch Properties** (Propriétés de commutateur virtuel), saisissez un **nom** pour le commutateur virtuel.

Étape 6 Créez un vSwitch externe ou interne.

- Pour créer un vSwitch externe, sélectionnez **External network** (réseau externe) et l'adaptateur physique requis dans la liste déroulante.
- Pour créer un vSwitch interne, sélectionnez **Internal network** (Réseau interne) ou **Private network** (Réseau privé).

Étape 7 Sous **VLAN ID**, cochez la case située à côté de **Enable virtual LAN identification for management Operating system** (Activer l'identification du réseau local virtuel pour le système d'exploitation de gestion).

Étape 8 Cliquez sur **OK**.

Créer une nouvelle machine virtuelle

Exécutez cette procédure pour créer une nouvelle machine virtuelle.

Procédure

Étape 1 Sur le gestionnaire Hyper-V , cliquez sur **Action > New > Virtual Machine** (Action > Nouveau > Machine virtuelle).

Étape 2 Cliquez sur **Next** (Suivant) dans la boîte de dialogue **New Virtual Machine Wizard** (Assistant de nouvelle machine virtuelle).

Étape 3 Entrez un **nom** pour le modèle déployé et cliquez sur **Next** (Suivant).

Étape 4 Choisissez **Generation 1** (Génération 1) et cliquez sur **Next** (Suivant).

Étape 5 Précisez la quantité de **mémoire de démarrage** ou de RAM, en Mo, qui doit être allouée à la machine virtuelle (minimum : 28 672 Mo ; recommandé : 32 768 Mo)

Étape 6 Dans la liste déroulante, choisissez la **connexion** vSwitch requise.

Étape 7 Choisissez **Use an virtual hard disk** (Utilisation un disque dur virtuel existant) et cliquez sur **Browse** (Parcourir) pour choisir l'image VHD du centre de gestion virtuelle téléchargée.

Étape 8 Cliquez sur **Finish** (Terminer) pour créer la VM.

Étape 9 Après avoir créé la machine virtuelle, il est important d'augmenter le nombre de processeurs virtuels (vCPU) pour la machine virtuelle. Par défaut, sa valeur est fixée à *1*.

a) Dans le **gestionnaire Hyper-V**, faites un clic droit sur la machine virtuelle que vous avez créée et cliquez sur **Settings** (Paramètres).

La fenêtre des **paramètres** des machines virtuelles s'affiche.

b) Cliquez sur **Processor** (Processeur) sous **Hardware** (Matériel) dans le volet gauche.

La boîte de dialogue **Processor** (Processeur) s'affiche dans le volet de droite.

c) Dans le champ **Number of virtual processors** (Nombre de processeurs virtuels) : définissez la valeur sur **4**.

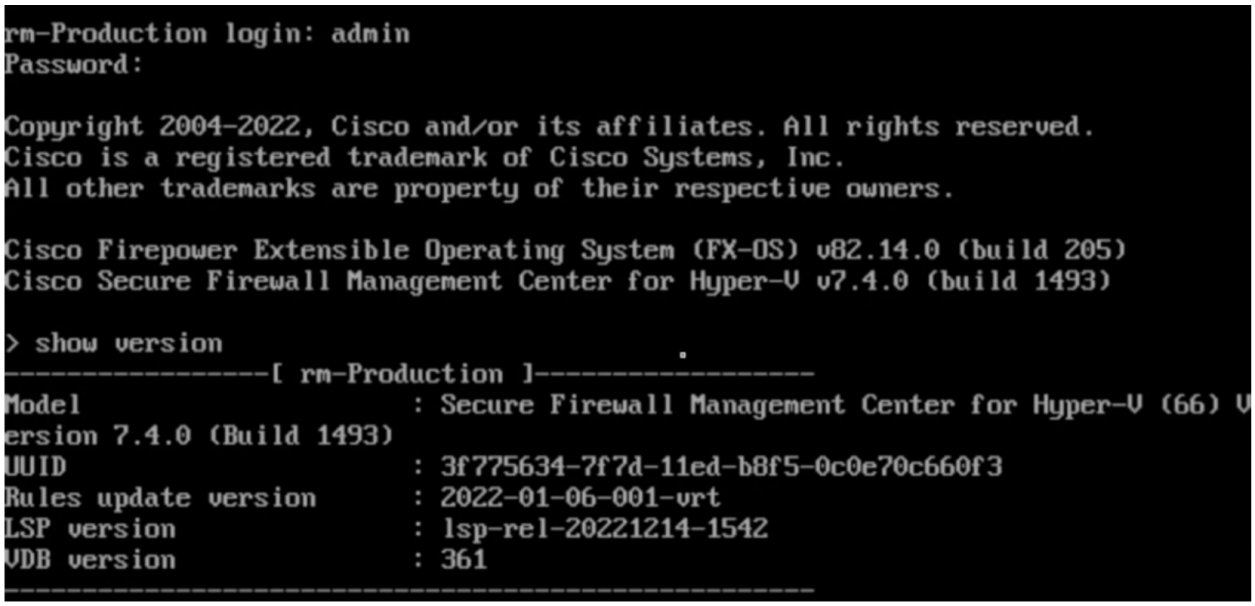
Remarque
Nous recommandons de définir la valeur des vCPU (processeurs virtuels) sur *8* pour des performances optimales. Notez qu'une machine virtuelle nécessite un minimum de *4* vCPU (processeurs virtuels).

Pour en savoir plus sur les exigences minimales en matière de ressources, consultez Serveur Windows pris en charge pour Management Center Virtual, à la page 116

d) Cliquez sur **OK**.

Vérifier le déploiement

Exécutez la commande **show version** sur la console série pour vous assurer que le centre de gestion virtuel est déployé sur Hyper-V.



Accéder aux journaux du premier démarrage

Pour accéder aux premiers journaux de démarrage, effectuez cette procédure avant de réactiver la machine virtuelle que vous avez créée sur le gestionnaire Hyper-V.

Procédure

Étape 1 Sur le gestionnaire Hyper-V , sélectionnez la nouvelle machine virtuelle et cliquez sur **Settings** (Paramètres) dans la section **Actions** du côté droit de la fenêtre.

Étape 2 Dans la section **Hardware** (Matériel), cliquez sur **COM1** et sélectionnez **Named Pipe** (Canal nommé).

Étape 3 Saisissez un **Pipe name** (Nom de canal). Par exemple, **virtual1**. Notez le **Named pipe path** (Chemin du canal nommé).

Étape 4 Cliquez sur **Apply** (Appliquer), puis sur **OK**.

Étape 5 Cliquez sur la machine virtuelle que vous avez créée, puis sur **Start** (Démarrer) dans la fenêtre **Actions** sur le côté droit de la fenêtre. L' **état** de la machine virtuelle devrait maintenant passer de **Starting** (Démarrage) à **Running** (En fonctionnement).

Étape 6 Vous devez maintenant connecter le canal nommé que vous avez créé à un client série, tel que **PuTTY**.

Étape 7 Accédez à votre hôte local et ouvrez la fenêtre **PuTTY**.

Étape 8 Saisissez le **chemin d'accès de canal nommé** que vous avez noté plus tôt dans le champ **de ligne de série**.

Par exemple, \\.*pipe**virtual1*.

Étape 9 Cliquez sur **Ouvrir** Vous pouvez maintenant voir les premiers journaux de démarrage sur la fenêtre **PuTTY**.

Arrêter Management Center Virtual

Dans le gestionnaire Hyper-V , faites un clic droit sur la machine virtuelle que vous souhaitez fermer, puis cliquez sur **Turn Off** (Désactiver).

Redémarrer Management Center Virtual

Exécutez la commande **sudo reboot** en mode **expert** sur la CLI de Management Center Virtual pour lancer un redémarrage progressif :

```
Cisco Firepower Extensible Operating System (FX-OS) v82.14.0
(build 205)
Cisco Secure Firewall Management Center for Hyper-V v7.4.0
(build 1493)
> expert
admin@hyperv-automation:~$ sudo reboot
```

Vous pouvez également accéder à Hyper-V Manager, cliquer avec le bouton droit sur la machine virtuelle que vous souhaitez fermer, puis cliquer sur **Turn Off** (Éteindre).

Supprimer Management Center Virtual (Centre de gestion virtuel)

Après l'arrêt de la machine virtuelle, cliquez avec le bouton droit sur celle-ci, puis cliquez sur **Delete** (Supprimer).

Remarque La suppression ne supprime pas le disque connecté à la machine virtuelle. Vous devez supprimer ce disque manuellement.

Dépannage

- Problème : impossible de démarrer la machine virtuelle, impossible d'initialiser la mémoire

  Scénario : ce problème se produit lorsque l'espace disque est insuffisant pour initialiser la machine virtuelle.

  Solution de contournement : libérez de l'espace sur le disque où se trouve le fichier VHD.

- Problème : impossible de provisionner ou de démarrer la machine virtuelle ; échec d'ouverture de la pièce jointe.

  Scénario : ce problème se produit lorsqu'une autre machine virtuelle utilise la même image que la nouvelle machine virtuelle

  Solution de contournement : supprimer l'ancienne machine virtuelle.

- Problème : échec du démarrage de la machine virtuelle, mémoire système insuffisante

  Scénario : ce problème se produit lorsque la RAM disponible sur le système d'exploitation hôte est insuffisante pour provisionner la mémoire configurée à la machine virtuelle.

  Solution de contournement : assurez-vous que la RAM requise est disponible sur le système d'exploitation hôte.

- Problème : impossible d'établir une connexion SSH au Management Center Virtual ou de charger l'IU du Management Center Virtual depuis un hôte externe.

  Solution de contournement : autorisez le port 22 (SSH), 443 (HTTPS), 80 (HTTP) dans les règles d'entrée et de sortie du pare-feu Windows .

- Problème : l'appareil ne peut pas accéder à Internet.

  Solution de contournement : si le périphérique utilise un vSwitch externe, assurez-vous que la passerelle du VLAN est correctement configurée.

CHAPITRE 12

Configuration initiale Firewall Management Center Virtual

Ce chapitre décrit le processus de configuration initiale que vous devez effectuer après avoir déployé l'appareil Firewall Management Center Virtual.

On-Prem Firewall Management Center Configuration initiale à l'aide de l'interface de ligne de commande pour les versions 6.5 et ultérieures

Après avoir déployé un Firewall Management Center Virtual, vous pouvez accéder à la console de l'appareil pour la configuration initiale.Vous pouvez effectuer la configuration initiale à l'aide de l'interface de ligne de commande au lieu d'utiliser l'interface Web. Vous devez effectuer un assistant de configuration initiale qui configure le nouveau périphérique pour qu'il communique sur votre réseau de gestion de confiance. L' assistant vous demande d'accepter le contrat de licence d'utilisateur final (CLUF) et de changer le mot de passe administrateur.

Avant de commencer

- Assurez-vous que les informations suivantes sont nécessaires pour que le Firewall Management Center Virtual communique sur votre réseau de gestion :
  - Une adresse IP de gestion IPv4 :

    L'interface On-Prem Firewall Management Center est préconfigurée pour accepter une adresse IP4 attribuée par DHCP. Consultez votre administrateur système pour connaître l'adresse IP que le DHCP attribue à l'adresse MAC On-Prem Firewall Management Center. Dans les scénarios où aucun DHCP n'est disponible, l'interface On-Prem Firewall Management Center utilise l'adresse IPv4 192.168.45.45.

  - Un masque réseau et une passerelle par défaut (si vous n'utilisez pas DHCP).

Procédure

Étape 1 Connectez-vous au Firewall Management Center Virtual sur la console en utilisant **admin** comme nom d'utilisateur et **Admin123** comme mot de passe pour le compte **admin**. Remarque : les mots de passe sont sensibles à la casse.

Étape 2 Lorsque vous y êtes invité, appuyez sur **Entrée** pour afficher le contrat de licence de l'utilisateur final (CLUF).

Étape 3 Passez en revue le CLUF. Lorsque vous y êtes invité, saisissez **`Yes (oui)`**, **`Yes (oui`**) ou appuyez sur **Enter** (Entrée) pour accepter le CLUF.

Important
Vous ne pouvez pas continuer sans accepter le CLUF. Si vous répondez par autre chose que **`Yes (oui)`**, **`Yes (oui`**) ou **Enter** (Entrée), le système vous déconnecte.

Étape 4 Pour assurer la sécurité et la confidentialité du système, la première fois que vous vous connectez à On-Prem Firewall Management Center, vous devez changer le mot de passe **admin**. Lorsque le système demande un nouveau mot de passe, saisissez un nouveau mot de passe conforme aux restrictions affichées, puis saisissez à nouveau le même mot de passe lorsque le système demande une confirmation.

Remarque
Le On-Prem Firewall Management Center compare votre mot de passe à un dictionnaire de craquage qui vérifie non seulement de nombreux mots du dictionnaire, mais aussi d'autres chaînes de caractères qui pourraient être facilement déchiffrées à l'aide de techniques courantes d'intrusion de mots de passe. Par exemple, le script de configuration initiale peut rejeter des mots de passe tels que « abcdefg » ou « passw0rd ».

Remarque
À l'achèvement du processus de configuration initiale, le système définit les mots de passe des deux comptes **d'administrateur** (un pour l'accès Web et l'autre pour l'accès à l'interface de ligne de commande) à la même valeur, conformément aux exigences relatives aux mot de passe sécurisés décrites dans le *Guide d'administration de Cisco Secure Firewall Management Center* pour votre version. Si vous modifiez les mots de passe de l'un ou l'autre des comptes **administrateurs** par la suite, ils ne seront plus identiques et l'exigence relative au mot de passe fort peut être supprimée du compte **administrateur** de l'interface Web.

Étape 5 Répondez aux invites pour configurer les paramètres réseau.

Lorsque vous suivez les invites, pour les questions à choix multiples, vos options sont répertoriées entre parenthèses, par exemple (**`o/n`**) pour oui ou non. Les valeurs par défaut sont indiquées entre crochets, par exemple [**`o`**]. Notez les éléments suivants lorsque vous répondez aux invites :

- Appuyez sur **Enter** (Entrée) à une invite pour accepter la valeur par défaut.
- Pour le nom d'hôte, indiquez un nom de domaine complet (`<hostname>.<domain>`) ou le nom d'hôte. Ce champ est obligatoire.
- Si vous utilisez DHCP, vous devez utiliser la réservation DHCP, de sorte que l'adresse attribuée ne change pas. Si l'adresse DHCP change, l'enregistrement du périphérique échouera car la configuration réseau On-Prem Firewall Management Center n'est pas synchronisée. Pour récupérer après un changement d'adresse DHCP, connectez-vous à On-Prem Firewall Management Center (en utilisant le nom d'hôte ou la nouvelle adresse IP) et accédez à **System (Système)** > **Configuration** > **Management Interfaces (Interfaces de gestion)**pour réinitialiser le réseau.
- Si vous choisissez de configurer IPv4 manuellement, le système vous demandera l'adresse IPv4, le masque réseau et la passerelle par défaut.

- La configuration d'un serveur DNS est facultative ; pour spécifier aucun serveur DNS, saisissez **None** (aucun). Sinon, spécifiez les adresses IPv4 pour un ou deux serveurs DNS. Si vous spécifiez deux adresses, séparez-les par une virgule. (Si vous spécifiez plus de deux serveurs DNS, le système ignore les entrées supplémentaires.) Si votre On-Prem Firewall Management Center n'a pas d'accès Internet, vous ne pouvez pas utiliser de DNS en dehors de votre réseau local.

  Remarque
  Si vous utilisez une licence d'évaluation, le fait de préciser que DNS est facultatif pour le moment, mais requis pour des licences permanentes.

- Vous devez saisir le nom de domaine complet ou l'adresse IP pour au moins un serveur NTP accessible à partir de votre réseau. (Vous ne pouvez pas préciser de noms de domaine complets pour les serveurs NTP si vous n'utilisez pas DHCP.) Vous pouvez définir deux serveurs (un principal et un secondaire) ; séparez les informations par une virgule. (Si vous spécifiez plus de deux serveurs DNS, le système ignore les entrées supplémentaires.) Si votre On-Prem Firewall Management Center n'a pas d'accès Internet, vous ne pouvez pas utiliser un serveur NTP en dehors de votre réseau local.

Exemple :

```
Enter a hostname or fully qualified domain name for this system [firepower]: fmc
Configure IPv4 via DHCP or manually? (dhcp/manual) [DHCP]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.0.66
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.224
Enter the IPv4 default gateway for the management interface [ ]: 10.10.0.65
Enter a comma-separated list of DNS servers or 'none' [CiscoUmbrella]: 208.67.222.222,208.67.220.220
Enter a comma-separated list of NTP servers [0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org]:
```

Étape 6 Le système affiche un résumé de vos sélections de configuration . Passez en revue les paramètres que vous avez saisis.

Exemple :

```
Hostname:                           fmc
IPv4 configured via:                manual configuration
Management interface IPv4 address:  10.10.0.66
Management interface IPv4 netmask:  255.255.255.224
Management interface IPv4 gateway:  10.10.0.65
DNS servers:                        208.67.222.222,208.67.220.220
NTP servers:                        0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org
```

Étape 7 La dernière invite vous donne la possibilité de confirmer les paramètres.

- Si les paramètres sont corrects, saisissez **o** et appuyez sur **Enter** (Entrée) pour accepter les paramètres et continuer.
- Si les paramètres sont incorrects, saisissez **n** et appuyez sur **Enter** (Entrée). Le système demande de nouveau les informations, en commençant par le nom d'hôte.

Exemple :

```
Are these settings correct? (y/n) y
If your networking information has changed, you will need to reconnect.

Updated network configuration.
```

Étape 8 Après avoir accepté les paramètres, vous pouvez saisir **exit** (sortie) pour quitter l'interface de ligne de commande On-Prem Firewall Management Center.

Prochaine étape

- Vous pouvez vous connecter à l'interface Web Firewall Management Center Virtual en utilisant les informations sur le réseau que vous venez de configurer.
- Passez en revue les activités de maintenance hebdomadaires que le On-Prem Firewall Management Center configure automatiquement dans le cadre du processus de configuration initial. Ces activités sont conçues pour maintenir votre système à jour et vos données sauvegardées. Voir Passer en revue la configuration initiale automatique pour les versions 6.5 et ultérieures, à la page 130 .

Effectuer la configuration initiale au niveau de l'interface Web pour les versions 6.5 et ultérieures

Après avoir déployé Firewall Management Center Virtual, vous pouvez effectuer la configuration initiale en utilisant HTTPS sur l'interface Web de l'appareil.

Lorsque vous vous connectez à l'interface Web On-Prem Firewall Management Center pour la première fois, le On-Prem Firewall Management Center présente un assistant de configuration initiale pour vous permettre de configurer rapidement et facilement les paramètres de base du périphérique. Cet assistant se compose de trois écrans et d'une boîte de dialogue contextuelle :

- Le premier écran vous force à modifier le mot de passe de l'utilisateur **admin** à partir de la valeur par défaut de **Admin123**.
- Le deuxième écran présente le contrat de licence d'utilisateur final (CLUF) que vous devez accepter avant d'utiliser l'appareil.
- Le troisième écran vous permet de modifier les paramètres réseau de l'interface de gestion des appareils. Cette page est préremplie avec les paramètres actuels, que vous pouvez modifier.
- L' assistant effectue la validation des valeurs que vous saisissez dans cet écran pour confirmer les éléments suivants :
  - Correction syntaxique
  - Compatibilité des valeurs saisies (par exemple, adresse IP et passerelle compatibles, ou DNS fourni lorsque les serveurs NTP sont précisés à l'aide de FQDN)
  - Connectivité réseau entre le Firewall Management Center Virtual et les serveurs DNS et NTP

  L' assistant affiche les résultats de ces tests en temps réel à l'écran, ce qui vous permet d'apporter des corrections et de tester la fiabilité de votre configuration avant de cliquer sur **Finish** (Terminer) au bas de l'écran. Les tests de connectivité NTP et DNS ne sont pas bloquants ; vous pouvez cliquer sur **Terminer** avant que l' assistant ne termine les tests de connectivité . Si le système signale un problème de connectivité après que vous ayez cliqué sur **Finish** (Terminer), vous ne pouvez pas modifier les paramètres dans l' assistant, mais vous pouvez configurer ces connexions à l'aide de l'interface Web après avoir terminé la configuration initiale.

  Le système n'effectue pas de tests de connectivité si vous saisissez des valeurs de configuration qui conduiraient à couper la connexion existante entre le Firewall Management Center Virtual et le navigateur. Dans ce cas, l' assistant n'affiche aucune information sur l'état de connectivité pour le DNS ou le NTP.

- Après avoir terminé les trois écrans, une boîte de dialogue contextuelle s'affiche et vous permet de configurer rapidement et facilement les licences Smart.

Lorsque vous avez terminé l'assistant de configuration initial et désactivé la boîte de dialogue de licences Smart, le système affiche la page de gestion des périphériques, décrite dans « Device Management » (gestion des périphériques) dans le Guide de configuration Cisco Secure Firewall Management Center Device pour votre version.

Avant de commencer

- Assurez-vous que les informations suivantes sont nécessaires pour que le On-Prem Firewall Management Center communique sur votre réseau de gestion :
  - Une adresse IP de gestion IPv4.

    L'interface On-Prem Firewall Management Center est préconfigurée pour accepter une adresse IP4 attribuée par DHCP. Consultez votre administrateur système pour déterminer l'IP attribuée par DHCP à l'adresse MAC On-Prem Firewall Management Center. Dans les scénarios où aucun DHCP n'est disponible, l'interface On-Prem Firewall Management Center utilise l'adresse IPv4 192.168.45.45.

  - Un masque réseau et une passerelle par défaut (si vous n'utilisez pas DHCP).
- Si vous n'utilisez pas DHCP, configurez un ordinateur local avec les paramètres réseau suivants :
  - Adresse IP : 192.168.45.2
  - Masque réseau : 255.255.255.0
  - La passerelle par défaut est 192.168.45.1.

  Désactivez toutes les autres connexions réseau sur cet ordinateur.

Procédure

Étape 1 À l'aide d'un navigateur, accédez à l'adresse IP du Firewall Management Center Virtual :*https://<Management Center-IP>*.

La page d'ouverture de session s'affiche.

Étape 2 Connectez-vous au Firewall Management Center Virtual en utilisant **admin** comme nom d'utilisateur et **Admin123** comme mot de passe pour le compte admin. (Les mots de passe sont sensibles à la casse.)

Étape 3 À l'écran **de modification du mot de passe** :

a) (Facultatif), cochez la case **Show password** (afficher le mot de passe) pour voir le mot de passe lorsque vous utilisez cette boîte de dialogue.

b) Cliquez sur **Generate Password** (générer un mot de passe) pour que le système crée un mot de passe conforme aux critères de la liste. (Les mots de passe générés ne sont pas mnémoniques ; prenez soin de noter le mot de passe si vous choisissez cette option.)

c) Pour définir le mot de passe de votre choix, saisissez un nouveau mot de passe dans les zones de texte **New Password** (Nouveau mot de passe) et **Confirm Password** (Confirmer le mot de passe).

Le mot de passe doit être conforme aux critères énumérés dans la boîte de dialogue.

Remarque
Le On-Prem Firewall Management Center vérifie les mots de passe à l'aide d'un dictionnaire spécial contenant non seulement de nombreux mots du dictionnaire, mais aussi d'autres chaînes de caractères qui pourraient être facilement déchiffrées à l'aide de techniques courantes d'intrusion de mots de passe. Par exemple, le script de configuration initiale peut rejeter des mots de passe tels que « abcdefg » ou « passw0rd ».

Remarque
À l'achèvement du processus de configuration initiale, le système définit les mots de passe des deux comptes d' **administrateur** (un pour l'accès Web et l'autre pour l'accès à l'interface de ligne de commande) à la même valeur. Le mot de passe doit être conforme aux exigences décrites dans le Guide d'administration Cisco Secure Firewall Management Center de votre version. Si vous modifiez les mots de passe de l'un ou l'autre des comptes **administrateurs** par la suite, ils ne seront plus identiques et l'exigence relative au mot de passe fort peut être supprimée du compte **administrateur** de l'interface Web.

d) Cliquez sur **Next** (suivant).

Une fois que vous avez cliqué sur **Next** (Suivant) sur l'écran **Change Password** (modifier le mot de passe) et que l'assistant a accepté le nouveau mot de passe **admin**, ce mot de passe est en vigueur pour l'interface Web et les comptes **admin** de l'interface de ligne de commande, même si vous ne terminez pas les activités restantes de l'assistant.

Étape 4 À l'écran du **contrat d'utilisateur**, lisez le CLUF et cliquez sur **Accept** (accepter) pour continuer.

Si vous cliquez sur **Decline** (Refuser), l'assistant vous déconnecte de Firewall Management Center Virtual.

Étape 5 Cliquez sur **Next** (suivant).

Étape 6 À l'écran **de modification des paramètres réseau** :

a) Saisissez un **nom de domaine complet (FQDN)**. Si la valeur par défaut s'affiche, vous pouvez l'utiliser si elle est compatible avec la configuration de votre réseau. Sinon, saisissez un nom de domaine complet (syntaxe `<hostname>.<domain>`) ou le nom d'hôte.

b) Choisissez le protocole de démarrage pour l'option **Configure IPv4** (Configuration IPv4), soit **à l'aide de DHCP**, soit **à l'aide de Static/Manual**.

Si vous utilisez DHCP, vous devez utiliser la réservation DHCP, de sorte que l'adresse attribuée ne change pas. Si l'adresse DHCP change, l'enregistrement du périphérique échouera car la configuration réseau On-Prem Firewall Management Center n'est pas synchronisée. Pour récupérer après un changement d'adresse DHCP, connectez-vous à On-Prem Firewall Management Center (en utilisant le nom d'hôte ou la nouvelle adresse IP) et accédez à **System (Système)** > **Configuration** > **Management Interfaces (Interfaces de gestion)**pour réinitialiser le réseau.

c) Acceptez la valeur affichée, si une est affichée, pour **l'adresse IPv4** ou saisissez une nouvelle valeur. Utilisez la forme décimale à points (par exemple, 192.168.45.45).

Remarque
Si vous modifiez l'adresse IP pendant la configuration initiale, vous devez vous reconnecter au On-Prem Firewall Management Center en utilisant les nouvelles informations réseau.

d) Acceptez la valeur affichée, le cas échéant, pour **le masque réseau** ou saisissez une nouvelle valeur. Utilisez la forme décimale à points (par exemple, 255.255.0.0).

Remarque
Si vous modifiez le masque réseau pendant la configuration initiale, vous devez vous reconnecter au On-Prem Firewall Management Center en utilisant les nouvelles informations réseau.

e) Vous pouvez accepter la valeur affichée, le cas échéant, pour **la passerelle** ou saisir une nouvelle passerelle par défaut. Utilisez la forme décimale à points (par exemple, 192.168.0.1).

Remarque
Si vous modifiez l'adresse de la passerelle pendant la configuration initiale, vous devrez peut-être vous reconnecter au On-Prem Firewall Management Center en utilisant les nouvelles informations réseau.

f) (Facultatif) Pour le **groupe DNS,** vous pouvez accepter la valeur par défaut, **Cisco Umbrella DNS**.

Pour modifier les paramètres DNS, choisissez **Custom DNS Servers** (serveurs DNS personnalisés) dans la liste déroulante et saisissez les adresses IPv4 pour le **DNS principal** et le **DNS secondaire**. Si votre On-Prem Firewall Management Center n'a pas d'accès Internet, vous ne pouvez pas utiliser de DNS en dehors de votre réseau local. Configurez le serveur DNS en sélectionnant **Custom DNS Servers** (serveurs DNS personnalisés) dans la liste déroulante et en supprimant les champs **Primary DNS** (DNS principal) et **Secondary DNS** (DNS secondaire).

Remarque
Si vous utilisez des noms de domaine complets plutôt que des adresses IP pour spécifier des serveurs NTP, vous devez préciser le DNS à ce moment. Si vous utilisez une licence d'évaluation, le DNS est facultatif, mais le DNS est requis pour utiliser des licences permanentes pour votre déploiement.

g) Pour les **serveurs de groupe NTP** vous pouvez accepter la valeur par défaut, **Default NTP Servers** (Serveurs NTP par défaut). Dans ce cas, le système utilise **0.sourcefire.pool.ntp.org** comme serveur NTP principal et **1.sourcefire.pool.ntp.org** comme serveur NTP secondaire.

Pour configurer d'autres serveurs NTP, choisissez **Custom NTP Group Servers** (serveurs de groupe NTP personnalisés) dans la liste déroulante et saisissez les noms de domaine complets ou les adresses IP d'un ou deux serveurs NTP accessibles à partir de votre réseau. Si votre On-Prem Firewall Management Center n'a pas d'accès Internet, vous ne pouvez pas utiliser un serveur NTP en dehors de votre réseau local.

Remarque
Si vous modifiez les paramètres réseau pendant la configuration initiale, vous devez vous reconnecter au On-Prem Firewall Management Center en utilisant les nouvelles informations réseau.

Étape 7 Cliquez sur **Finish** (terminer).

L' assistant effectue la validation des valeurs que vous saisissez sur cet écran pour confirmer l'exactitude syntaxique, la compatibilité des valeurs saisies et la connectivité réseau entre le On-Prem Firewall Management Center et les serveurs DNS et NTP. Si le système signale un problème de connectivité après que vous ayez cliqué sur **Finish** (Terminer), vous ne pouvez pas modifier les paramètres dans l' assistant, mais vous pouvez configurer ces connexions à l'aide de l'interface Web On-Prem Firewall Management Center après avoir terminé la configuration initiale.

Prochaine étape

- Le système affiche une fenêtre contextuelle qui vous permet de configurer rapidement et facilement les licences Smart. L'utilisation de cette boîte de dialogue est facultative; si votre Firewall Management Center Virtual gère des périphériques Cisco Firewall Threat Defense et que vous connaissez bien les licences Smart, utilisez cette boîte de dialogue. Sinon, ignorez cette boîte de dialogue et consultez la section « Licences » dans le Guide d'administration Cisco Secure Firewall Management Center de votre version.
- Passez en revue les activités de maintenance hebdomadaires que le On-Prem Firewall Management Center configure automatiquement dans le cadre du processus de configuration initial. Ces activités sont conçues pour maintenir votre système à jour et vos données sauvegardées. Voir Passer en revue la configuration initiale automatique pour les versions 6.5 et ultérieures, à la page 130 .

- Une fois que vous avez terminé l'assistant de configuration initial et désactivé la boîte de dialogue de licences Smart, le système affiche la page de gestion des périphériques, décrite dans le *Guide de configuration des périphériques de Cisco Secure Firewall Management Center*.

Passer en revue la configuration initiale automatique pour les versions 6.5 et ultérieures

Dans le cadre de la configuration initiale (qu'elle soit effectuée par l'intermédiaire de l'assistant de configuration initial ou de l'interface de ligne de commande), le On-Prem Firewall Management Center configure automatiquement les tâches de maintenance pour maintenir votre système à jour et vos données sauvegardées.

Ces tâches sont planifiées en UTC, ce qui signifie que le moment où elles se produisent *localement* dépend de la date et de votre emplacement spécifique. En outre, étant donné que les tâches sont planifiées en heure UTC, elles ne s'ajustent pas à l'heure avancée, à l'heure d'été, ni à tout autre ajustement saisonnier propre à votre emplacement. Si vous êtes concerné, les tâches planifiées se produisent une heure « ultérieurement » en été qu'en hiver, en fonction de l'heure locale.

Remarque Nous vous recommandons *fortement* de passer en revue les configurations de la planification automatique, de confirmer que On-Prem Firewall Management Center les a établies avec succès et de les ajuster si nécessaire.

- Mises à jour hebdomadaires de GeoDB

  Le On-Prem Firewall Management Center planifie automatiquement les mises à jour de la GeoDB chaque semaine, à une heure aléatoire déterminée. Vous pouvez observer l'état de cette mise à jour à l'aide de l'interface Web du centre de messages. Vous pouvez voir la configuration pour cette mise à jour automatique dans l'interface Web sous **Système** > **Mises à jour** > **Mises à jour de géolocalisation**>**RecurRING Geolocation Updates** (Mises à jour de géolocalisation récurrentes). Si le système ne parvient pas à configurer la mise à jour et que votre On-Prem Firewall Management Center a accès à Internet, nous vous recommandons de configurer des mises à jour régulières de GeoDB comme décrit dans le Guide d'administration Cisco Secure Firewall Management Center correspondant à votre version.

- Mises à jour logicielles On-Prem Firewall Management Center hebdomadaires

  Le On-Prem Firewall Management Centerplanifie automatiquement une tâche hebdomadaire pour télécharger la version logicielle la plus récente pour le On-Prem Firewall Management Center et ses périphériques gérés. Cette tâche est planifiée pour se produire entre 2 et 3 h, heure UTC, le dimanche matin. Selon la date et votre emplacement, cela peut correspondre du samedi après-midi au dimanche après-midi en heure locale. Vous pouvez observer l'état de cette tâche à l'aide de l'interface Web du centre de messages. Vous pouvez voir la configuration pour cette tâche dans l'interface Web sous **Système** > **Outils** > **Planification**. Si la planification des tâches échoue et que votre On-Prem Firewall Management Center a accès à Internet, nous vous recommandons de planifier une tâche récurrente pour le téléchargement des mises à jour logicielles, comme décrit dans le Guide d'administration Cisco Secure Firewall Management Center correspondant à votre version.

  Cette tâche télécharge uniquement les correctifs et mises à jour urgentes (hotfix) pour la version actuellement exécutée par vos appliances ; il vous revient d'installer les mises à jour téléchargées par cette tâche. Voir le *Guide de mise à niveau de Cisco On-Prem Firewall Management Center* pour obtenir plus d'information.

- Sauvegarde hebdomadaire de la configuration On-Prem Firewall Management Center

  Le On-Prem Firewall Management Center planifie automatiquement une tâche hebdomadaire pour effectuer une sauvegarde de la configuration uniquement stockée localement à 2 h UTC le lundi matin ; Selon la date et votre emplacement, cela peut se produire à tout moment, du samedi après-midi au dimanche après-midi à l'heure locale. Vous pouvez observer l'état de cette tâche à l'aide de l'interface Web du centre de messages. Vous pouvez voir la configuration pour cette tâche dans l'interface Web sous **Système** > **Outils** > **Planification**. Si la planification des tâches échoue, nous vous recommandons de planifier une tâche récurrente pour effectuer une sauvegarde, comme décrit dans le Guide d'administration Cisco Secure Firewall Management Center pour votre version.

- Mise à jour de la base de données de vulnérabilités

  Dans les versions 6.6 et ultérieures, le On-Prem Firewall Management Center télécharge et installe la dernière mise à jour de la base de données des vulnérabilités (VDB) à partir du site d'assistance de Cisco. Il s'agit d'une opération unique. Vous pouvez observer l'état de cette mise à jour à l'aide de l'interface Web du centre de messages. Pour maintenir votre système à jour, si votre On-Prem Firewall Management Center a accès à Internet, nous vous recommandons de planifier des tâches pour effectuer des téléchargements et des installations de mises à jour automatiques récurrentes de la VDB, comme décrit dans le Guide d'administration Cisco Secure Firewall Management Center pour votre version.

- Mise à jour quotidienne des règles d'intrusion

  Dans les versions 6.6 et ultérieures, le On-Prem Firewall Management Center configure une mise à jour quotidienne automatique des règles de prévention des intrusions à partir du site d'assistance de Cisco. La solution On-Prem Firewall Management Center déploie les mises à jour automatiques des règles d'intrusion sur les appareils gérés ciblés lors du prochain déploiement des politiques concernées. Vous pouvez observer l'état de cette tâche à l'aide de l'interface Web du centre de messages. Vous pouvez voir la configuration pour cette tâche dans l'interface Web sous **Système** > **Mises à jour** > **Mises à jour des règles**. Si la configuration de la mise à jour échoue et que votre On-Prem Firewall Management Center dispose d'un accès Internet, nous vous recommandons de configurer les mises à jour régulières des règles de prévention des intrusions comme décrit dans le Guide d'administration Cisco Secure Firewall Management Center pour votre version.

CHAPITRE 13

Firewall Management Center Virtual Administration et configuration initiale

Après avoir terminé le processus de configuration initiale de Firewall Management Center Virtual et vérifié sa réussite, nous vous recommandons d'effectuer diverses tâches administratives qui faciliteront la gestion de votre déploiement. Vous devez également effectuer toutes les tâches que vous avez ignorées lors de la configuration initiale, par exemple l'octroi de licences. Pour des informations détaillées sur l'une des tâches décrites dans les sections suivantes, ainsi que des renseignements sur la façon dont vous pouvez commencer à configurer votre déploiement, consultez les guides complets : Guide de configuration de Secure Firewall Management Center et pour votre version.

Comptes d'utilisateurs individuels

Après avoir terminé la configuration initiale, le seul utilisateur d'interface Web sur le système est l'utilisateur **admin**, qui a le rôle et l'accès administrateur. Les utilisateurs ayant ce rôle ont un accès complet au menu et à la configuration du système. Nous vous recommandons de limiter l'utilisation du compte **admin** (et du rôle d'administrateur) pour des raisons de sécurité et d'audit. Dans l'interface graphique Firewall Management Center Virtual, gérez les comptes utilisateur sur la page **System 'Système)** > **Users (Utilisateurs)** > **User (Utilisateur)**.

Remarque Les comptes **admin** permettant d'accéder à Firewall Management Center Virtual à l'aide de l'interface Shell et d'accéder à Firewall Management Center Virtual à l'aide de l'interface Web ne sont pas identiques et peuvent utiliser des mots de passe différents.

La création d'un compte distinct pour chaque personne qui utilise le système permet à votre organisation non seulement de vérifier les actions et les modifications effectuées par chaque utilisateur, mais aussi de limiter le rôle ou les rôles d'accès d'utilisateur associés à chaque personne. Cela est particulièrement important sur le Firewall Management Center Virtual, où vous effectuez la plupart de vos tâches de configuration et d'analyse.

Par exemple, un analyste a besoin d'accéder aux données d'événements pour analyser la sécurité de votre réseau, mais n'a peut-être pas besoin d'accéder aux fonctions d'administration du déploiement.

Le système inclut dix rôles utilisateur prédéfinis conçus pour divers administrateurs et analystes de l'interface Web. Vous pouvez également créer des rôles utilisateur personnalisés avec des privilèges d'accès spécialisés.

Enregistrement de l'appareil

Le On-Prem Firewall Management Center peut gérer n'importe quel périphérique, physique ou virtuel, actuellement pris en charge par le système :

- Firewall Threat Defense : fournit un pare-feu unifié de prochaine génération et un périphérique IPS de prochaine génération.
- Firewall Threat Defense Virtual : un périphérique virtuel de 64 bits conçu pour fonctionner dans plusieurs environnements hyperviseur, réduire les frais administratifs et accroître l'efficacité opérationnelle.
- Cisco Pare-feu ASA avec services FirePOWER (ou un module ASA FirePOWER) : fournit la politique système de première ligne et transmet le trafic au système pour la découverte et le contrôle d'accès. Cependant, vous ne pouvez pas utiliser l'interface Web On-Prem Firewall Management Center pour configurer les interfaces ASA FirePOWER. Cisco Pare-feu ASA avec services FirePOWER dispose d'un logiciel et d'une interface de ligne de commande uniques à la plateforme ASA que vous pouvez utiliser pour installer le système et effectuer d'autres tâches administratives spécifiques à la plateforme.
- Périphériques séries 7000 et 8000 : périphériques physiques conçus pour le système. Les périphériques séries 7000 et 8000 offrent une gamme de débits, tout en partageant la plupart des mêmes capacités. En général, les périphériques Série 8000 sont plus puissants que les périphériques Série 7000 ; ils prennent également en charge des fonctionnalités supplémentaires telles que les règles fastpath Série 8000, l'agrégation de liens et le stacking. Vous devez configurer la gestion à distance sur le périphérique avant de pouvoir l'enregistrer sur le On-Prem Firewall Management Center.
- NGIPSv : un périphérique virtuel de 64 bits déployé dans l'environnement VMware VSphere. Les périphériques NGIPSv ne prennent en charge aucune des fonctionnalités matérielles du système, comme la redondance et le partage des ressources, la commutation et le routage.

Pour enregistrer des périphériques gérés sur le On-Prem Firewall Management Center, utilisez la page **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** sur l'interface graphique utilisateur du On-Prem Firewall Management Center ; consultez les informations de gestion des périphériques dans le guide de configuration de Secure Firewall Management Center pour votre version.

Politiques d'intégrité et politiques système

Par défaut, tous les appareils ont une politique système initiale appliquée. La politique de système régit les paramètres susceptibles d'être similaires pour plusieurs périphériques d'un déploiement, tels que les préférences d'hôte de relais de messagerie et les paramètres de synchronisation de l'heure. Nous vous recommandons d'utiliser le On-Prem Firewall Management Center pour appliquer la même stratégie système à lui-même et à tous les périphériques qu'il gère.

Par défaut, le On-Prem Firewall Management Center dispose également d'une politique d'intégrité. Une politique d'intégrité, dans le cadre de la fonctionnalité de surveillance de l'intégrité, fournit les critères permettant au système de surveiller en permanence les performances des périphériques de votre déploiement.

Nous vous recommandons d'utiliser le On-Prem Firewall Management Center pour appliquer une stratégie d'intégrité à tous les périphériques qu'il gère.

Mises à jour logicielles et de base de données

Vous devez mettre à jour le logiciel système sur vos périphériques avant de commencer tout déploiement. Nous recommandons que tous les périphériques de votre déploiement exécutent la version la plus récente du système. Si vous les utilisez dans votre déploiement, vous devez également installer les dernières mises à jour des règles de prévention des intrusions, VDB et GeoDB.

Mise en garde Avant de mettre à jour une partie du système, vous devez lire les notes de version ou le texte d'avis qui accompagne la mise à jour. Les notes de version fournissent des informations importantes, notamment sur les plateformes prises en charge, la compatibilité, les conditions préalables, les avertissements, et les instructions d'installation et de désinstallation spécifiques.

Si votre On-Prem Firewall Management Center exécute les versions 6.5 et ultérieures :

Dans le cadre de la configuration , le On-Prem Firewall Management Center établit les activités suivantes pour maintenir votre système à jour et vos données sauvegardées :

- Mises à jour automatiques hebdomadaires de GeoDB
- Tâche hebdomadaire visant à télécharger les mises à jour logicielles pour le On-Prem Firewall Management Center et ses périphériques gérés.

Important Cette tâche ne télécharge que les mises à jour logicielles sur le On-Prem Firewall Management Center. Il est de votre responsabilité d'installer les mises à jour téléchargées par cette tâche. Voir le *Guide de mise à niveau de Cisco Secure Firewall Management Center* pour obtenir plus d'information.

- Une tâche hebdomadaire planifiée pour effectuer une sauvegarde de la configuration stockée uniquement localement de On-Prem Firewall Management Center.

Si votreOn-Prem Firewall Management Center exécute les versions 6.6 et ultérieures, dans le cadre de la configuration initiale, le On-Prem Firewall Management Center télécharge et installe la dernière mise à jour de la base de données des vulnérabilités (VDB) à partir du site d'assistance de Cisco. Il s'agit d'une opération unique.

Vous pouvez suivre l'état de ces activités à l'aide de l'interface Web du centre de messages. Si le système ne parvient pas à configurer l'une de ces activités et que votre On-Prem Firewall Management Center a accès à Internet, nous vous recommandons de configurer ces activités vous-même, comme décrit dans le *guide de configuration de Cisco Secure Firewall Management Center* pour votre version.

Dépannage

Cette section décrit des étapes de dépannage de base liées à votre déploiement du Firewall Management Center Virtual sur votre machine virtuelle.

Échec de connexion SSH

Le Firewall Management Center Virtual est entièrement opérationnel, l'interface utilisateur et la connexion à la console fonctionnent correctement, à l'exception de la connexion SSH . Dans certains cas, les fichiers clés d'hôte SSH peuvent être corrompus lors du démarrage initial de Firewall Management Center Virtual, ce qui entraîne des échecs de connexion SSH .

Vous pouvez vérifier les indicateurs suivants qui suggérent un échec de la connexion SSH :

1. Une erreur d'E/S de disque peut se produire lors du démarrage initial de Firewall Management Center Virtual, en particulier au démarrage du daemon SSH (sshd). Il en résulte que les fichiers clés SSH (fichiers ssh_host* générés par sshd) sont vides.

   ls -lrt /etc/ssh total 16

   ```
   -rw-r--r-- 1 root root 1746 Jan 17 23:31 ssh_config-openssh
   -rw-r--r-- 1 root root 6027 Jan 17 23:42 sshd_config
   -rw-r--r-- 1 root root 1293 Jan 17 23:42 ssh_config
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_dsa_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_dsa_key.pub
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ecdsa_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ecdsa_key.pub
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ed25519_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ed25519_key.pub
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_rsa_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_rsa_key.pub
   ```

2. Pour le problème d'E/S de disque, vous pouvez vérifier le fichier `/var/log/messages`, qui peut contenir des données erronées (indiquant une erreur d'E/S) près de l'horodatage de génération des clés.

Pour résoudre la défaillance SSH qui pourrait se produire lors du démarrage initial de Firewall Management Center Virtual, comme décrit ci-dessus, vous devez effectuer les étapes suivantes :

1. Connectez-vous à Firewall Management Center Virtual.
2. Exécutez la commande **sudo reboot** en mode **expert** sur l'interface de ligne de commande Firewall Management Center Virtual pour lancer un redémarrage progressif.
3. Exécutez la commande suivante pour supprimer les fichiers de clé SSH vides :

   ```
   cd /etc/ssh/
   rm ssh_host*
   ```

4. Exécutez la commande suivante pour redémarrer le service `sshd` afin de régénérer les fichiers de clé SSH correctement.

   ```
   /etc/rc.d/init.d/sshd stop
   /etc/rc.d/init.d/sshd start
   ```

Remarque Suivez les étapes de cette solution de contournement uniquement si vous êtes sûr que les fichiers de clé SSH sont vides. Si vous avez des doutes, il est conseillé de soumettre un dossier au TAC pour une enquête plus approfondie.

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.