

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, à la page 1
- Licences Firewall Management Center Virtual, à la page 4
- À propos des performances des appliances virtuelles, à la page 5
- Télécharger le paquet de déploiement Firewall Management Center Virtual, à la page 7

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.
- 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.
- Pour déployer le Firewall Management Center Virtual dans AWS, consultez Déployer Firewall Management Center Virtual sur AWS.
- Pour déployer le Firewall Management Center Virtual dans Azure, consultez Déployer Firewall Management Center Virtual sur Azure à partir du portail AWS..
- 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 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.