

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, à la page 1
- Lignes directrices et limites relatives à la licence, à la page 2
- Déployer Firewall Management Center Virtual, à la page 4
- Mettre sous tension et initialiser l'appliance virtuelle, à la page 5

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 1 : 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 2 : 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

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.
- 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.

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.