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 1 : 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 7. .
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 7.
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 2 : 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 3 : 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 4 : 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 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 11.

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 13.

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 14.
- 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.
- Pour un aperçu des prochaines étapes nécessaires dans votre déploiement Firewall Management Center Virtual, consultez x.

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.