

Déployer Firewall Management Center Virtual à l'aide de KVM

Vous pouvez déployer Firewall Management Center Virtual sur KVM.

- Aperçu, à la page 1
- Prérequis, à la page 3
- Lignes directrices et limites relatives à la licence, à la page 4
- Préparer le fichier de configuration Day 0 (jour 0), à la page 4
- Déployer Firewall Management Center Virtual, à la page 6
- Déployer sans utiliser le fichier de configuration Day 0 (jour 0), à la page 9

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 9.

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 7.

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 6.
- 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 7.

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.
- 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 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.