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 1 : Tailles de machine virtuelles prises en charge par Azure pour le Firewall Management Center Virtual, à la page 2.

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 1 : 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 2.	

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 1 : Tailles de machine virtuelles prises en charge par Azure pour le Firewall Management Center Virtual, à la page 2).

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 6.
- **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 ».

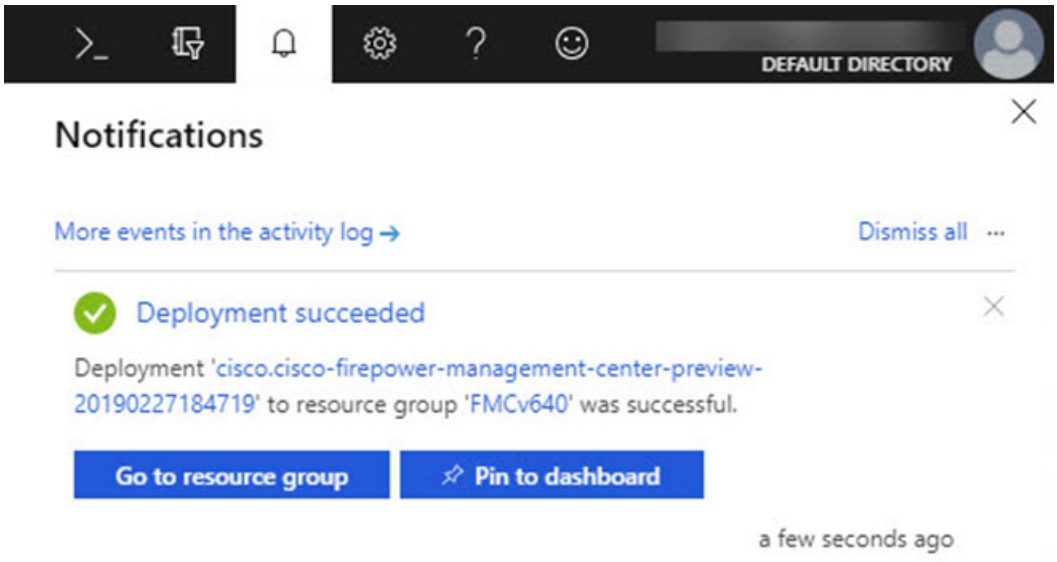
g) Cliquez sur **OK**.

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.

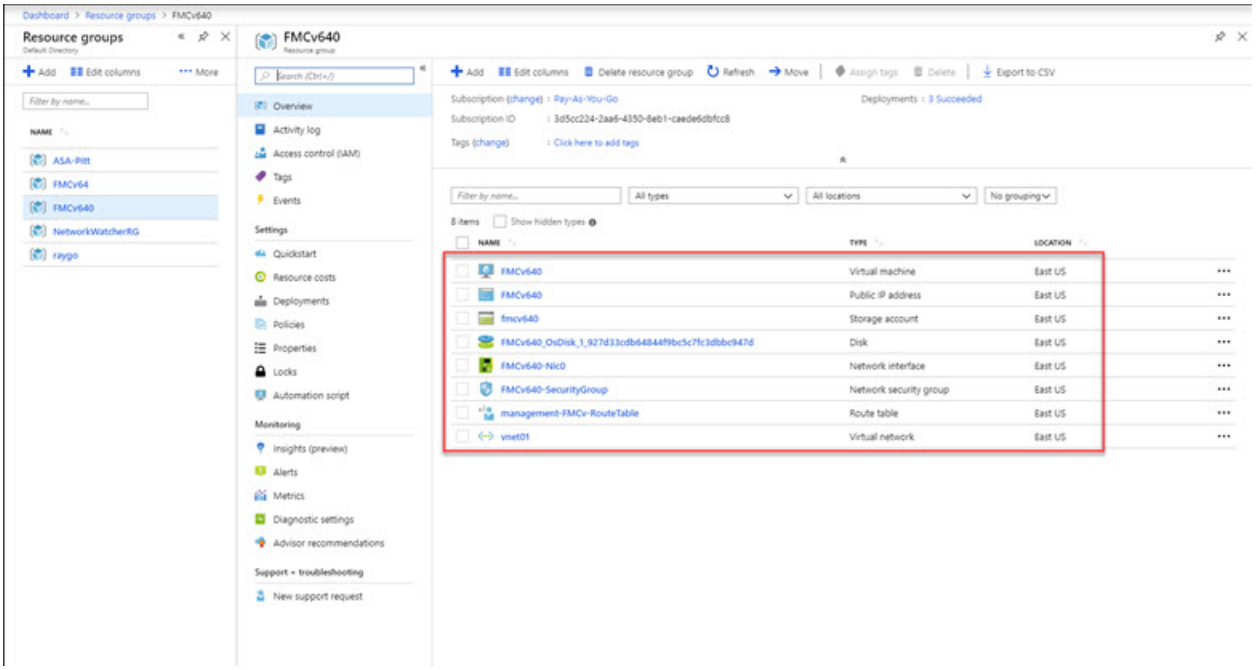
Remarque N'oubliez pas que les délais de déploiement varient dans Azure et que le temps total jusqu'à ce que Firewall Management Center Virtual soit utilisable est d'environ 30 minutes, même lorsque le tableau de bord Azure indique l'état de la machine virtuelle Firewall Management Center Virtual indique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

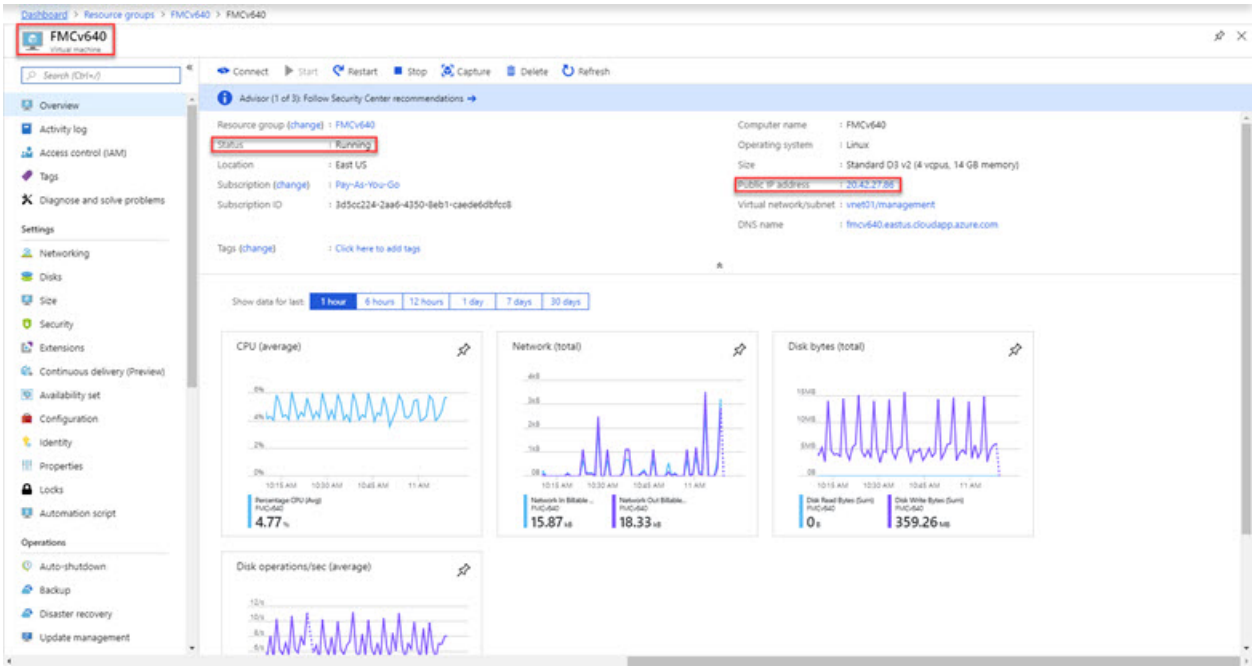
Illustration 2 : Page Azure Firewall Management Center Virtual Resource Group



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 3 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 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.

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.