

Déployer Firewall Management Center Virtual sur AWS

Amazon Virtual Private Cloud (Amazon VPC) vous permet de lancer des ressources Amazon Web Services (AWS) dans un réseau virtuel que vous définissez. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel qui pourrait fonctionner dans votre propre centre de données, avec les avantages de l'utilisation de l'infrastructure évolutive d'AWS.

Vous pouvez déployer Firewall Management Center Virtual sur le nuage AWS (AWS Cloud).

- Aperçu, à la page 1
- Lignes directrices et limites relatives à la licence, à la page 4
- Configuration de l'environnement AWS, à la page 5
- Déployer Firewall Management Center Virtual, à la page 11

Aperçu

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 pas créer d'autres instances Firewall Management Center Virtual en les utilisant, même pour les versions antérieures. Vous pouvez continuer à exécuter les instances existantes. Consultez Tableau 1 : Types d'instances pris en charge par AWS pour le Firewall Management Center Virtual, à la page 2.

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.

Le tableau suivant résume les types d'instances AWS que Firewall Management Center Virtual prend en charge ; ceux que prennent en charge les versions 6.5.x et antérieures, et ceux que prennent en charge les version 6.6.0 et ultérieures.

Remarque La version 6.6 ajoute la prise en charge des types d'instances C5 affichés dans le tableau suivant. Les types d'instances plus importantes fournissent plus de ressources de CPU à vos VM AWS pour des performances accrues, et certains autorisent plus d'interfaces réseau.

Tableau 1 : Types d'instances pris en charge par AWS pour le Firewall Management Center Virtual

Observations	Versions 6.6.0 et ultérieures	vCPU	Mémoire (Go)	Nombre maximal d'interfaces	Versions 6.5 et antérieures	vCPU	Mémoire (Go)	Nombre maximal d'interfaces
Firewall Management Center Virtual	c3.4xlarge	16	30	8	c3.xlarge*	4	7.5	4
	c4.4xlarge	16	30	8	c3.2xlarge*	8	15	4
	c5.4xlarge	16	32	8	c3.4xlarge	16	30	8
	—	—	—	—	c4.xlarge*	4	7.5	4
					c4.2xlarge*	8	15	4
					c4.4xlarge	16	30	8
	* Notez que le Firewall Management Center Virtual ne prendra pas en charge ces types d'instances sur les versions 6.6.0 et supérieures. À partir de la version 6.6.0, vous devez déployer le Firewall Management Center Virtual (n'importe quelle version) en utilisant une instance avec au moins 28 Go de RAM. Consultez Types d'instances obsolètes et Redimensionnement des types d'instances, à la page 3 pour de plus amples renseignements.							

Tableau 2 : Types d'instances pris en charge par AWS pour le Firewall Management Center Virtual 300

Observations	Version 7.1.0 et ultérieures
Firewall Management Center Virtual 300 (FMCv300)	c5.9xlarge : 36 vCPU, 72 Go Stockage SSD : 2000 Go

Types d'instances obsolètes

Vous pouvez continuer à exécuter vos déploiements actuels de la version 6.5.x et antérieures Firewall Management Center Virtual, mais vous ne pourrez pas lancer les nouveaux déploiements Firewall Management Center Virtual (n'importe quelle version) en utilisant ces types d'instances :

- c3.xlarge : 4 vCPU de 7,5 Go (Désactivé pour le Firewall Management Center Virtual après les versions 6.6.0 et ultérieures)
- c3.2xlarge : 8 vCPU de 15 Go (Désactivé pour le Firewall Management Center Virtual après les versions 6.6.0 et ultérieures)
- c4.xlarge : 4 vCPU de 7,5 Go (Désactivé pour le Firewall Management Center Virtual après laes versions 6.6.0 et ultérieures)

- c4.2xlarge : 8 vCPU, 15 Go (Désactivé pour le Firewall Management Center Virtual après les versions 6.6.0 et ultérieures)

Redimensionnement des types d'instances

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, vous devez redimensionner votre type d'instance actuel en un qui prend en charge la version 6.6.0 (voir Tableau 1 : Types d'instances pris en charge par AWS pour le Firewall Management Center Virtual, à la page 2).

Vous pouvez redimensionner une instance si le type d'instance actuel et le nouveau type d'instance que vous souhaitez sont compatibles. Pour les déploiements Firewall Management Center Virtual :

- Redimensionnez n'importe quelle instance c3.xlarge ou c3.2xlarge en type d'instance c3.4xlarge.
- Redimensionnez n'importe quelle instance c4.xlarge ou c4.2xlarge avec le type d'instance c4.4xlarge.

Gardez à l'esprit les éléments suivants avant de redimensionner votre instance :

- Vous devez arrêter votre instance avant de modifier les types d'instances.
- Vérifiez que votre type d'instance actuel est compatible avec le nouveau type d'instance que vous choisissez.
- Si cette instance a un volume de stockage d'instances, toutes les données qu'elle contient sont perdues lorsque l'instance est arrêtée. Migrez votre instance sauvegardée sur le magasin d'instances avant de la redimensionner.
- Si vous n'utilisez pas d'adresse IP Elastic, l'adresse IP publique est libérée lorsque vous arrêtez l'instance.

Pour des instructions sur la façon de redimensionner votre instance, consultez la documentation d'AWS « Changement du type d'instance » (https:docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-resize.html).

Aperçu de la solution AWS

AWS est un ensemble de services informatiques à distance proposés par Amazon.com, également appelés services Web, qui composent une plateforme de traitement en nuage. Ces services fonctionnent à partir de 11 régions géographiques partout au monde. De façon générale, familiarisez-vous avec les services AWS suivants lors du déploiement du Firewall Management Center Virtual :

- Amazon Elastic Compute Cloud (EC2) : un service Web qui vous permet de louer des ordinateurs virtuels pour lancer et gérer vos propres applications et services, comme un pare-feu, dans les centres de données d'Amazon.
- Amazon Virtual Private Cloud (VPC) : un service Web qui vous permet de configurer un réseau privé isolé qui existe dans le nuage public d'Amazon. Vous exécutez vos instances EC2 dans un VPC.
- Amazon Web Service (S3) : un service Web qui vous fournit une infrastructure de stockage de données.

Vous créez un compte sur AWS, configurez les composants VPC et EC2 (à l'aide des assistants AWS ou de la configuration manuelle), et choisissez une instance Amazon Machine Image (AMI). L'AMI est un modèle qui contient la configuration logicielle nécessaire pour lancer votre instance.

Remarque Les images d'AMI ne peuvent pas être téléchargées en dehors de l'environnement AWS.

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge (7.1.0 et versions ultérieures)

- **Management Center Virtual 300 (FMCv300) pour AWS** : une nouvelle image Firewall Management Center Virtual évolutive est disponible sur la plateforme AWS. Elle prend en charge la gestion d'un maximum de 300 périphériques et offre une capacité de disque plus élevée.
- La haute accessibilité (HA) Firewall Management Center Virtual est prise en charge.

Prérequis

Les conditions préalables suivantes concernent le Firewall Management Center Virtual sur AWS :

- Un compte Amazon. Vous pouvez en créer un à l' adresse aws.amazon.com.
- Un compte Cisco Smart. Vous pouvez en créer un sur le Centre des logiciels Cisco (https://software.cisco.com/).
- Obtenez une licence pour Firewall Management Center Virtual. Consultez Licences Firewall Management Center Virtual pour connaître les directives générales sur les licences de plateforme virtuelle ; consultez la section « Licences du système » du *Guide de configuration de Cisco Secure Firewall Management Center* pour obtenir des renseignements plus détaillés sur la gestion des licences.
- Exigences de l'interface Firewall Management Center Virtual
  - Interface de gestion.
- Chemins de communication :
  - Adresses IP publiques et Elastic pour l'accès à Firewall Management Center Virtual.
- Pour la compatibilité de Firewall Management Center Virtual et du système, consultez le guide de compatibilité de Cisco Secure Firewall Threat Defense.

Directives

Les directives suivantes concernent le Firewall Management Center Virtual sur AWS :

- Déploiement dans le Cloud privé virtuel (VPC)
- Mise en réseau améliorée (SR-IOV) si disponible.
- Déploiement à partir du Marché Amazon
- Maximum de quatre vCPU par instance.
- Déploiement des utilisateurs des réseaux L3

Restrictions

Les limites suivantes concernent le Firewall Management Center Virtual sur AWS :

- Les périphériques 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.
- Toute configuration d'adresse IP (de l'interface de ligne de commande ou de On-Prem Firewall Management Center) doit correspondre à ce qui est créé dans la console AWS ; vous devez noter vos configurations pendant le déploiement.
- IPv6 n'est pas pris en charge pour le moment.
- Vous ne pouvez pas ajouter d'interfaces après le démarrage.
- Le clonage et les instantanés ne sont actuellement pas pris en charge.
- La découverte de l'identité du serveur TLS (Transport Layer Security) n'est pas prise en charge avec la configuration à Bras unique de Geneve sur AWS.

Configuration de l'environnement AWS

Pour déployer Firewall Management Center Virtual sur AWS, vous devez configurer un VPC Amazon avec vos exigences et vos paramètres de déploiement précis. Dans la plupart des situations, un assistant de configuration peut vous guider dans votre configuration. AWS fournit une documentation en ligne où vous pouvez trouver des informations utiles sur les services, des présentations aux fonctionnalités avancées. Consultez la section Mise en route d'AWS pour en savoir plus.

Pour vous aider à mieux contrôler votre configuration AWS, les sections suivantes proposent un guide de vos configurations VPC et EC2 avant de lancer les instances du Firewall Management Center Virtual :

- Créer le VPC, à la page 5
- Ajouter une passerelle Internet, à la page 6
- Ajoutez les sous-réseaux, à la page 7
- Ajouter une table de routage, à la page 8
- Créer un groupe de sécurité, à la page 8
- Créer des interfaces réseau, à la page 9
- Créer des adresses IP Elastic, à la page 10

Créer le VPC

Un Cloud privé virtuel (ou VPC) est un réseau virtuel dédié à votre compte AWS. Il est logiquement isolé des autres réseaux virtuels du Cloud AWS. Vous pouvez lancer vos ressources AWS, par exemple des instances Firewall Management Center Virtual, dans votre VPC. Vous pouvez configurer votre VPC; vous pouvez sélectionner sa plage d'adresses IP, créer des sous-réseaux et configurer les tables de routage, les passerelles réseau et les paramètres de sécurité.

Avant de commencer

- Créez votre compte AWS.
- Confirmez que des AMIs sont disponibles pour les instances Firewall Management Center Virtual.

Procédure

Étape 1 Connectez-vous à aws.amazon.com et choisissez votre région.

AWS est divisé en plusieurs régions isolées les unes des autres. La région est affichée dans le coin supérieur droit de votre écran. Les ressources d'une région n'apparaissent pas dans une autre région. Vérifiez périodiquement que vous êtes dans la région prévue.

Étape 2 Cliquez sur **Services** > **VPC**.

Étape 3 Cliquez sur **VPC Dashboard** > **Your VPCs** > **(Tableau de bord VPC** > **Vos VPC)**.

Étape 4 Cliquez sur **Create VPC** (Créer un nuage privé virtuel).

Étape 5 Saisissez la commande suivante dans la boîte de dialogue **Create VPC** (Créer un VPC) :

a) Une **balise de nom** définie par l'utilisateur pour identifier le VPC.
b) Un **bloc CIDR** d'adresses IP. La notation CIDR (Classless Inter-Domain Routing) est une représentation compact d'une adresse IP et de son préfixe de routage associé. Par exemple, 10.0.0.0/24.
c) Un paramètre de localisation (**Tenancy setting**) par défaut pour s'assurer que les instances lancées dans ce VPC utilisent l'attribut de localisation précisé lors du lancement.

Étape 6 Cliquez sur **Yes, Create** pour créer votre VPC.

Prochaine étape

Ajoutez une passerelle Internet à votre VPC comme décrit dans la section suivante.

Ajouter une passerelle Internet

Vous pouvez ajouter une passerelle Internet pour connecter votre VPC à Internet. Vous pouvez acheminer le trafic pour les adresses IP en dehors de votre VPC vers la passerelle Internet.

Avant de commencer

- Créez un VPC pour vos instances Firewall Management Center Virtual.

Procédure

Étape 1 Cliquez sur **Services** > **VPC**.

Étape 2 Cliquez sur **VPC Dashboard (tableau de board VPC)** > **Internet Gateways (passerelles Internet)**, puis cliquez sur **Create Internet Gateway** (créer une passerelle Internet).

Étape 3 Saisissez une balise de nom (Name tag) définie par l'utilisateur pour définir la passerelle et cliquez sur Yes, Create pour créer la passerelle.

Étape 4 Sélectionnez la passerelle créée à l'étape précédente.

Étape 5 Cliquez sur **Attach to VPC** (associer au VPC)et sélectionnez le VPC que vous avez créé précédemment.

Étape 6 Cliquez sur **Yes, Attach (oui, associer)** pour associer la passerelle à votre VPC.

Par défaut, les instances lancées sur le VPC ne peuvent pas communiquer avec Internet tant qu'une passerelle n'est pas créée et liée au VPC.

Prochaine étape

Ajoutez des sous-réseaux à votre VPC, comme décrit dans la section suivante.

Ajoutez les sous-réseaux

Vous pouvez segmenter la plage d'adresses IP de votre VPC auquel les instances Firewall Management Center Virtual peuvent être associées. Vous pouvez créer des sous-réseaux pour regrouper les instances en fonction des besoins opérationnels et de sécurité. Pour Firewall Threat Defense Virtual, vous devez créer un sous-réseau pour la gestion, ainsi que des sous-réseaux pour le trafic.

Procédure

Étape 1 Cliquez sur **Services** > **VPC**.

Étape 2 Cliquez sur **VPC Dashboard (tableau de bord VPC)** > **Subnets (sous-réseaux)**, puis sur **Create Subnet** (créer un sous-réseau).

Étape 3 Saisissez les informations suivantes dans la boîte de dialogue **Create Subnet** (créer un sous-réseau) :

a) Une balise de nom (**Name tag**) définie par l'utilisateur pour identifier le sous-réseau.
b) Le **VPC** à utiliser pour ce sous-réseau.
c) La zone de disponibilité (**Availability Zone**) où ce sous-réseau résidera. Sélectionnez No Preference (aucune préférence) pour permettre à Amazon de sélectionner la zone.
d) Un **bloc CIDR** d'adresses IP. La plage d'adresses IP dans le sous-réseau doit être un sous-ensemble de la plage d'adresses IP dans le VPC. La taille des blocs doit être comprise entre un masque réseau/16 et un masque réseau/28. La taille du sous-réseau peut correspondre à la taille du VPC.

Étape 4 Cliquez sur **Yes, Create** pour créer votre sous-réseau.

Étape 5 Répétez l'opération pour tous les sous-réseaux requis. Créez un sous-réseau distinct pour le trafic de gestion et créez autant de sous-réseaux que nécessaire pour le trafic de données.

Prochaine étape

Ajoutez une table de routage à votre VPC comme décrit dans la section suivante.

Ajouter une table de routage

Vous pouvez associer une table de routage à la passerelle que vous avez configurée pour votre VPC. Vous pouvez également associer plusieurs sous-réseaux à une seule table de routage, mais un sous-réseau ne peut être associé qu'à une seule table de routage à la fois.

Procédure

Étape 1 Cliquez sur **Services** > **VPC**.

Étape 2 Cliquez sur **VPC Dashboard (tableau de bord VPC)** > **Route Tables (tables de routage)**, puis sur **Create Route Table** (créer une table de routage).

Étape 3 Saisissez une **Name tag (Balise de nom)** pour identifier la table de routage.

Étape 4 Sélectionnez le **VPC** dans la liste déroulante qui utilisera cette table de routage.

Étape 5 Cliquez sur **Yes, Create** (oui, créer) pour créer votre table de routage.

Étape 6 Sélectionnez la table de routage que vous avez créée.

Étape 7 Cliquez sur l'onglet **Routes** pour afficher les renseignements sur le routage dans le volet de détails.

Étape 8 Cliquez sur **Edit** (Modifier), puis sur **Add another route** (Ajouter une autre route).

a) Dans la colonne **Destination**, saisissez **0.0.0.0/0**.

b) Dans la colonne **Target** (cible), sélectionnez la passerelle Internet que vous avez créée ci-dessus.

Étape 9 Cliquez sur **Save** (enregistrer).

Étape 10 Cliquez sur l'onglet **Subnet Associations** (associations de sous-réseau), puis sur **Edit**(modifier).

Étape 11 Cochez la case à côté du sous-réseau à utiliser pour l'interface de gestion de Firewall Management Center Virtual et cliquez sur **Save** (Enregistrer).

Prochaine étape

Créez un groupe de sécurité comme décrit dans la section suivante.

Créer un groupe de sécurité

Vous pouvez créer un groupe de sécurité avec des règles précisant les protocoles autorisés, les ports et les plages d'adresses IP sources. Plusieurs groupes de sécurité peuvent être créés avec des règles différentes que vous pouvez attribuer à chaque instance. AWS dispose d'une documentation détaillée sur les Security Groups (Groupes de sécurité) si vous ne connaissez pas cette fonctionnalité.

Procédure

Étape 1 Cliquez sur **Services** > **EC2**.

Étape 2 Cliquez sur **ECS Dashboard (tableau de bord EC2)** > **Security Groups (groupes de sécurité)**.

Étape 3 Cliquez sur **Create Security Group** (Créer un groupe de sécurité).

Étape 4 Saisissez la commande suivante dans la boîte de dialogue **Create Security Group** (Créer un groupe de sécurité) :

a) Un **Security Group Name** (nom de groupe de sécurité) défini par l'utilisateur pour identifier le groupe de sécurité.
b) Une **Description** de ce groupe de sécurité.
c) Le **VPC** associé à ce groupe de sécurité.

Étape 5 Configurez les **Security Group Rules** (règles du groupe de sécurité) :

a) Cliquez sur **Create Security Group** (Créer un groupe de sécurité).
b) Dans la section **Inbound** (entrée), cliquez sur **Add Rule** (ajouter une règle).

Choisissez l'un des ports d'entrée suivants à ouvrir pour l'accès par Internet dans la liste déroulante **Type**. Par défaut, le type **All Traffic** (Tout le trafic) est sélectionné.

- SSH (22)
- TCP personnalisé (8305)
- HTTP (443)

Remarque
Les accès HTTPS et SSH sont requis pour gérer les Firewall Management Center Virtual à l'extérieur d'AWS. Vous devez préciser les adresses IP sources en conséquence. De plus, si vous configurez à la fois Firewall Management Center Virtual et Firewall Threat Defense Virtual dans le VPC AWS, vous devez autoriser l'accès au sous-réseau de gestion de l'IP privé.

c) Dans la section **Outbound** (trafic sortant), cliquez sur **Add Rule (Ajouter une règle)** pour ajouter une règle pour le trafic sortant, ou conservez les valeurs par défaut de **All traffic** (tout le trafic) (pour **Type**) et **Anywhere** (n'importe où) (pour **Destination**).

Étape 6 Cliquez sur **Create** (Créer) pour créer votre groupe de sécurité.

Prochaine étape

Créez des interfaces réseau comme décrit dans la section suivante.

Créer des interfaces réseau

Vous pouvez créer des interfaces réseau pour le Firewall Management Center Virtual en utilisant des adresses IP statiques. Créez des interfaces de réseau (externes et internes) selon les besoins de votre déploiement particulier.

Procédure

Étape 1 Cliquez sur **Services** > **EC2**.

Étape 2 Cliquez sur **EC2 Dashboard** > **(tableau de bord EC2)** > **Network Interfaces** > **(interfaces réseau)**.

Étape 3 Cliquez sur **Create Network Interface** (Créer une interface réseau).

Étape 4 Saisissez la commande suivante dans la boîte de dialogue **Create Network Interface** (créer une interface réseau) :

a) Une **description** facultative définie par l'utilisateur pour l'interface réseau.
b) Sélectionnez un **Subnet** (sous-réseau) dans la liste déroulante. Assurez-vous de sélectionner le sous-réseau du VPC dans lequel vous souhaitez créer l'instance .

c) Saisissez une adresse **IP privée**. Il est recommandé d'utiliser une adresse IP statique plutôt qu'une **attribution automatique**.
d) Sélectionnez un ou plusieurs **Security groups** (groupes de sécurité). Assurez-vous que tous les ports requis sont ouverts pour le groupe de sécurité.

Étape 5 Cliquez sur **Yes, Create** pour créer votre interface réseau.

Étape 6 Sélectionnez l'interface réseau que vous venez de créer.

Étape 7 Faites un clic droit et sélectionnez **Change Source/Dest pour modifier la source ou la destination. Cochez** .

Étape 8 Choisissez **Disabled** (Désactivé), puis cliquez sur **Save** (Enregistrer).

Répétez cette opération pour toutes les interfaces de réseau que vous créez.

Prochaine étape

Créez des adresses IP Elastic comme décrit dans la section suivante.

Créer des adresses IP Elastic

Lors de la création d'une instance, une adresse IP publique est associée à l'instance. Cette adresse IP publique change automatiquement lorsque vous arrêtez et démarrez l'instance. Pour résoudre ce problème, attribuez une adresse IP publique persistante à l'instance à l'aide de l'adressage IP élastique. Les adresses IP élastiques sont des adresses IP publiques réservées qui sont utilisées pour l'accès à distance au Firewall Management Center Virtual ainsi qu'à d'autres instances. AWS dispose d'une documentation détaillée sur les adresses IP Elastic si vous n'êtes pas familiarisé avec cette fonctionnalité.



Remarque Vous devez au minimum créer une adresse IP élastique pour Firewall Management Center Virtual et deux adresses IP élastiques pour les interfaces de gestion et de diagnostic Firewall Threat Defense Virtual.

Procédure

Étape 1 Cliquez sur **Services** > **EC2**.

Étape 2 Cliquez sur **EC2 Dashboard (Tableau de bord EC2)** > **Elastic IPs (Adresses IP élastiques)**.

Étape 3 Cliquez sur **Allocate New Address** (allouer une nouvelle adresse).

Répétez cette étape pour toutes les adresses IP élastiques ou publiques dont vous avez besoin.

Étape 4 Cliquez sur **Yes, Allocate** (oui, attribuer) pour créer votre adresse IP élastique.

Étape 5 Répétez l'opération pour toutes les adresses IP élastiques requises pour votre déploiement.

Prochaine étape

Déployez Firewall Management Center Virtual comme décrit dans la section suivante.

Déployer Firewall Management Center Virtual

Avant de commencer

- Configurez les éléments VPC AWS et EC2 comme décrit dans Configuring Your AWS Environment (Configuration de votre environnement AWS)
- Confirmez que l'AMI est disponible pour les instances Firewall Management Center Virtual.

Remarque Le mot de passe administrateur par défaut est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details (Détails avancés)** > **User Data (Données utilisateur)**) lors du déploiement initial.

Procédure

Étape 1 Accédez à https://aws.amazon.com/marketplace (Amazon Marketplace) et connectez-vous.

Étape 2 Une fois que vous êtes connecté à Amazon Marché, cliquez sur le lien fourni pour le Firewall Management Center Virtual.

Remarque
Si vous étiez déjà dans AWS, vous devrez peut-être vous déconnecter, puis vous reconnecter pour que le lien fonctionne.

Étape 3 Cliquez sur **Continue** (Continuer), puis cliquez sur l'onglet **Manual Launch** (Lancement manuel) .

Étape 4 Cliquez sur **Accept Terms** pour accepter les conditions.

Étape 5 Cliquez sur **Launch with EC2 Console** (lancer avec la console EC2) dans la région souhaitée

Étape 6 Choisissez un **type d'instance** pris en charge par le Firewall Management Center Virtual ; consultez About Deployment on the AWS Cloud (À propos du déploiement sur le nuage AWS) pour les types d'instances pris en charge.

Étape 7 Cliquez sur le bouton **Next: Configure Instance Details** (suivant; configurer les détails de l'instance au bas de l'écran) :

a) Modifiez le **réseau** pour qu'il corresponde à votre VPC précédemment créé.

b) Modifiez le **sous-réseau** pour qu'il corresponde à votre sous-réseau de gestion précédemment créé. Vous pouvez préciser une adresse IP ou utiliser la génération automatique.

c) Sous **Advanced Details** > **(Détails avancés)** > **User Data (Données utilisateur)**, ajoutez les renseignements de connexion par défaut.

Modifiez l'exemple ci-dessous pour qu'il corresponde à vos exigences en matière de nom d'appareil et de mot de passe.

Exemple de configuration de connexion :

```
#FMC
{
"AdminPassword": "<enter_your_password>",
"Hostname": "<Hostname-vFMC>"
}
```

Mise en garde
Utilisez uniquement du texte brut lors de la saisie des données dans le champ **Advanced Details** (Détails avancés). Si vous copiez ces informations à partir d'un éditeur de texte, assurez-vous de ne copier qu'en texte brut. Si vous copiez des données Unicode dans le champ **Advanced Details** (Détails avancés) , y compris un espace, l'instance peut être corrompue et vous devrez la résilier et la recréer.

Dans les versions 7.0 et ultérieures, le mot de passe administrateur par défaut est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details (Détails avancés)** > **User Data (Données utilisateur)**) lors du déploiement initial.

Dans les versions précédentes, le mot de passe admin par défaut était **Admin123**.

Étape 8 Cliquez sur **Next (Suivant) : Add Storage (Ajouter du stockage)** pour configurer les paramètres de votre périphérique de stockage.

Modifiez les paramètres du volume racine de sorte que la taille du volume (Go) soit de 250 Go. Moins de 250 Go limitera le stockage des événements et n'est pas pris en charge.

Étape 9 Cliquez sur **Next: Tag Instance** (suivant : étiquette d'instance).

Une balise est constituée d'une paire clé-valeur sensible à la casse. Par exemple, vous pouvez définir une balise avec **Key** = Name et **Value** = Management.

Étape 10 Sélectionnez **Next: Configure Security Group** (suivant : configurer le groupe de sécurité).

Étape 11 Cliquez sur **Select an existant Security Group (sélectionner un groupe de sécurité existant)** et choisissez le groupe de sécurité précédemment configuré, ou créez un nouveau groupe de sécurité. Consultez la documentation d'AWS pour de plus amples renseignements sur la création de groupes de sécurité.

Étape 12 Cliquez sur **Review and Launch** (vérifier et lancer).

Étape 13 Cliquez sur **Launch** (lancer).

Étape 14 Sélectionnez une paire de clés existante ou créez-en une nouvelle.

Remarque
Sélectionnez une paire de clés existante ou créez-en une nouvelle. La paire de clés se compose d'une clé publique qu'AWS stocke et d'un fichier de clé privée que l'utilisateur stocke. Ensemble, ils vous permettent de vous connecter à votre instance en toute sécurité. Assurez-vous d'enregistrer la paire de clés à un emplacement connu, car elle pourrait devoir se connecter à l'instance.

Étape 15 Cliquez sur **Launch Instances** (lancer les instances).

Étape 16 Cliquez sur **EC2 Dashboard** > **(Tableau de bord EC2)** > **Elastic IPs (Adresses IP Elastic)** et trouvez une adresse IP précédemment attribuée ou attribuez-en une nouvelle.

Étape 17 Sélectionnez l'adresse IP Elastic, cliquez avec le bouton droit et sélectionnez **Associate Address** (Associer l'adresse).

Localisez l'instance ou l'interface réseau à sélectionner, puis cliquez sur Associate (Associer).

Étape 18 Cliquez sur **EC2 Dashboard** > **(tableau de bord EC2)** > **Instances**.

Étape 19 L'état de l'instance Firewall Management Center Virtual affichera « running » (en cours d'exécution) et Status checks (Vérifications d'état) indiquera pass (réussite) pour « 2/2 checks » (2/2 vérifications) après quelques minutes seulement. Cependant, les processus de déploiement et de configuration initiale prendront entre 30 et 40 minutes. Pour consulter l'état, faites un clic droit sur l'instance, puis sélectionnez **Instance Settings (Paramètres de l'instance)** > **Get Instance Screenshot (Obtenir la capture d'écran de l'instance**.

Une fois la configuration terminée (après environ 30 à 40 minutes), la **capture d'écran de l'instance** doit afficher un message similaire à « Cisco Secure Firewall Management Center pour AWS vW.XY (build ZZ) » et peut-être suivi de lignes de sortie supplémentaires.

Vous devriez alors pouvoir vous connecter au nouveau Firewall Management Center Virtual à l'aide de SSH ou des HTTP. Les délais de déploiement réels peuvent varier en fonction de la charge AWS de votre région.

Vous pouvez accéder à Firewall Management Center Virtual à l'aide de SSH :

```
ssh -i <key_pair>.pem admin@<Public_Elastic_IP>
```

l'authentification SSH est gérée par une paire de clés. Aucun mot de passe n'est requis. Si vous êtes invité à saisir un mot de passe , la configuration est toujours en cours.

Vous pouvez également accéder au Firewall Management Center Virtual à l'aide de HTTPS :

```
https//<Public_Elastic_IP>
```

Remarque
Si vous voyez un message « system startup processes are still running » (les processus de démarrage du système s'exécutent toujours), cela signifie que la configuration n'est pas encore terminée.

Si vous n'obtenez aucune réponse via SSH ou HTTPS, vérifiez ces éléments :

- Assurez-vous que le déploiement est terminé. La capture d'écran de l'instance de machine virtuelle Firewall Management Center Virtual doit afficher un message similaire à « Cisco Secure Firewall Management Center pour AWS vW.XY (build ZZ) » et peut-être suivi de lignes de sortie supplémentaires.
- Assurez-vous d'avoir une adresse IP Elastic associée à l'interface réseau de gestion (eni) du On-Prem Firewall Management Center et que vous vous connectez à cette adresse IP.
- Assurez-vous qu'une passerelle Internet (igw) est associée à votre VPC.
- Assurez-vous que votre sous-réseau de gestion est associé à une table de routage.
- Assurez-vous que la table de routage associé à votre sous-réseau de gestion comporte une route pour « 0.0.0.0/0 » qui pointe vers votre passerelle Internet (igw).
- Assurez-vous que votre groupe de sécurité autorise les SSH et/ou HTTPS entrants des adresses IP auxquelles vous vous connectez.

Prochaine étape

Configuration des politiques et des paramètres de l'appareil

Après avoir installé le Firewall Threat Defense Virtual et ajouté le périphérique au centre de gestion, vous pouvez utiliser l' □interface utilisateur On-Prem Firewall Management Center pour configurer les paramètres de gestion des périphériques pour le Firewall Threat Defense Virtual s'exécutant sur AWS et pour configurer et appliquer les politiques de contrôle d'accès et autres politiques connexes pour gérer le trafic en utilisant votre périphérique Firewall Threat Defense Virtual. La politique de sécurité contrôle les services fournis par Firewall Threat Defense Virtual, tels que le filtrage IPS de nouvelle génération et le filtrage d'applications. Vous configurez la politique de sécurité sur Firewall Threat Defense Virtual à l'aide de On-Prem Firewall Management Center. Pour plus d'informations sur la configuration de la politique de sécurité, consultez le Guide de configuration de Cisco Secure Firewall ou l'aide en ligne du Centre de gestion.

-

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.