Déployer Défense contre les menaces virtuelles sur Azure à partir du portail AWS

Ce chapitre explique comment déployer Cisco Secure Firewall Threat Defense Virtual à partir du portail AWS.

Aperçu

Cisco Secure Firewall Threat Defense Virtual est intégré à la place de marché Microsoft Azure et prend en charge les types d'instances suivants :

- D3 standard : 4 CPU, 14 Go, 4 vNIC
- Standard D3_v2 : 4 CPU virtuelles, 14 Go, 4 vNIC
- D4_v2 standard : 8 CPU virtuelles, 28 Go, 8 VNIC **(nouveauté de la version 6.5**)
- Standard D5_v2 : 16 CPU virtuelles, 56 Go, 8 VNIC **(nouveauté de la version 6.5**)
- Standard_D8s_v3 : 8 CPU virtuelles, 32 Go, 4 vNIC (**nouveauté de la version 7.1**)

- Standard_D16s_v3 : 16 CPU virtuelles, 64 Go, 8vNIC (**nouveauté de la version 7.1**)
- Standard_F8s_v2 : 8 CPU virtuelles, 16 Go, 4vNIC (**nouveauté de la version 7.1**)
- Standard_F16s_v2 : 16 CPU virtuelles, 32 Go, 4 vNIC (**nouveauté de la version 7.1**)

Prérequis

- Un compte Microsoft Azure. Vous pouvez en créer un à https://azure.microsoft.com/en-us/.

  Après avoir créé un compte sur Azure, vous pouvez vous connecter, faire une recherche sur le marché pour Cisco Firepower Threat Defense et choisir l'offre « Cisco Firepower NGFW Virtual (NGFWv) ».
- Un compte Cisco Smart. Vous pouvez en créer un sur le Centre des logiciels Cisco.

  Licence pour défense contre les menaces virtuelles; consultez Licences de fonctionnalités de Cisco Secure Firewall Management Center pour obtenir un aperçu des licences de fonctionnalités du système de pare-feu, y compris des liens utiles.
- Pour la compatibilité de défense contre les menaces virtuelles et du système, consultez la section sur la compatibilité Défense contre les menaces virtuelles.

Chemins de communication

- Interface de gestion : utilisée pour connecter défense contre les menaces virtuelles avec Cisco Secure Firewall Management Center.

Remarque Dans la version 6.7 et ultérieure, vous pouvez éventuellement configurer une interface de données pour la gestion de centre de gestion au lieu de l'interface de gestion. L'interface de gestion est une condition préalable à la gestion de l'interface de données, vous devez donc toujours la configurer dans votre configuration initiale. Pour en savoir plus sur la configuration d'une interface de données pour l'accès centre de gestion, consultez la commande **configure network management-data-interface** dans Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

- Interface de diagnostic : utilisée pour les diagnostics et la création de rapports; ne peut pas être utilisée pour le trafic de transit.
- Interface interne (requise) : utilisée pour connecter défense contre les menaces virtuelles aux hôtes internes.
- Interface externe (requise) : utilisée pour connecter défense contre les menaces virtuelles au réseau public.

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

- Mode de pare-feu avec routage seulement
- Mise en réseau accélérée (AN) Azure
- Mode de gestion, l'un des deux choix suivants :
  - Vous pouvez utiliser Cisco Secure Firewall Management Center pour gérer votre défense contre les menaces virtuelles; voir Gestion de Cisco Secure Firewall Threat Defense Virtual avec Cisco Secure Firewall Management Center.
  - Vous pouvez utiliser Cisco Secure Firewall device manager intégré pour gérer votre défense contre les menaces virtuelles; voir Gestion de Cisco Secure Firewall Threat Defense Virtual avec Cisco Secure Firewall Device Manager.
- Adressage IP public : attribuez des adresses IP publiques à Gestion 0/0 et GigabitEthernet 0/0.

  Vous pouvez attribuer une adresse IP publique à d'autres interfaces au besoin; consultez la section sur les adresses IP publiques pour connaître les lignes directrices d'Azure concernant les adresses IP publiques, y compris comment créer, modifier ou supprimer une adresse IP publique.
- Interfaces :
  - Défense contre les menaces virtuelles déploie avec quatre vNIC par défaut.
  - Grâce à la prise en charge d'instances plus importantes, vous avez la possibilité de déployer défense contre les menaces virtuelles avec un maximum de 8 vNIC.
  - Pour ajouter des vNIC supplémentaires à votre déploiement défense contre les menaces virtuelles, consultez les informations fournies dans la section sur l'ajout des interfaces réseau à ou suppression des interfaces réseau des machines virtuelles.
  - Pour modifier la configuration des vNIC ou si le transfert IP est requis, consultez les renseignements fournis dans la section décrivant comment créer, modifier ou supprimer une interface de réseau.
  - Vous configurez vos interfaces défense contre les menaces virtuelles à l'aide de votre gestionnaire. Consultez le guide de configuration de votre plateforme de gestion, centre de gestion ou gestionnaire d'appareil, pour obtenir des renseignements complets sur la prise en charge et la configuration des interfaces.

Licence

- Le protocole BYOL (Bring Your Own License; apportez votre propre licence) est pris en charge.
- La licence PAYG (Pay As You Go) est un modèle de facturation basé sur l'utilisation qui permet au client d'exécuter défense contre les menaces virtuelles sans avoir à acheter des licences Cisco Smart. Toutes les fonctionnalités sous licence (Malware/Threat/URL Filtering/VPN, etc.) sont activées pour un appareil défense contre les menaces virtuelles selon le modèle PAYG. Les fonctionnalités sous licence ne peuvent pas être modifiées ou changées à partir de centre de gestion (version 6.5 ou ultérieure).

Remarque Les licences PAYG ne sont pas prises en charge sur les appareils défense contre les menaces virtuelles déployés en mode gestionnaire d'appareil.

Consultez le chapitre sur les licences du Guide d'administration de Cisco Secure Firewall Management Center pour connaître les consignes relatives à l'octroi de licences pour votre périphériquedéfense contre les menaces virtuelles.

Niveaux de performance pour les licences Smart Défense contre les menaces virtuelles

Le défense contre les menaces virtuelles prend en charge les licences par niveau de performance qui fournissent différents niveaux de débit et limites de connexion VPN en fonction des exigences de déploiement.

Tableau 1 : Défense contre les menaces virtuelles Limites des fonctionnalités sous licence en fonction des droits

Niveau de performance	Caractéristiques du périphérique (cœur/RAM)	Limite du débit	Limite de session RA VPN
FTDv5, 100 Mbit/s	4 cœurs/8 Go	100 Mbit/s	50
FTDv10, 1 Gbit/s	4 cœurs/8 Go	1 Gbit/s	250
FTDv20, 3 Gbit/s	4 cœurs/8 Go	3 Gbit/s	250
FTDv30, 5 Gbit/s	8 cœurs/16 Go	5 Gbit/s	250
FTDv50, 10 Gbit/s	12 cœurs/24 Go	10 Gbit/s	750
FTDv100, 16 Gbit/s	16 cœurs/34 Go	16 Gbit/s	10 000

Optimisation des performances

Pour obtenir les meilleures performances avec défense contre les menaces virtuelles, vous pouvez apporter des ajustements à la machine virtuelle et à l'hôte. Consultez la section sur le réglage et l'optimisation de la virtualisation sur Azure pour en savoir plus.

Receive Side Scaling (dimensionnement côté réception) : le défense contre les menaces virtuelles prend en charge Receive Côté Scaling (RSS), qui est une technologie utilisée par les adaptateurs réseau pour distribuer le trafic de réception réseau entre plusieurs cœurs de processeur. Pris en charge par les versions 7.0 et ultérieures. Consultez la section sur les files d'attente RX multiples pour le dimensionnement de la réception (RSS) pour en savoir plus.

Fonctionnalités non prises en charge

- Licences :
  - PLR (Permanent License Reservation; réservation de licence permanente)
  - PAYG (Pay As You Go; paiement graduel) (versions 6.4 et antérieures)
- Mise en réseau (nombre de ces limites sont des restrictions de Microsoft Azure) :
  - Bâtis grand format

- Réseaux VLAN 802.1Q
- Le mode transparent et d'autres fonctionnalités de couche 2; aucune diffusion, aucune multidiffusion.
- ARP de mandataire pour une adresse IP que l'appareil ne possède pas du point de vue d'Azure (a une incidence sur certaines fonctionnalités NAT);
- Mode de proximité (pas de capture de trafic de sous-réseau).
- Modes en ligne, mode passif.

Remarque La politique Azure empêche l'défense contre les menaces virtuelles de fonctionner en mode en ligne ou en mode pare-feu transparent, car elle n'autorise pas les interfaces à fonctionner en mode de proximité.

- ERSPAN (utilise le protocole GRE, qui n'est pas transféré dans Azure).

- Gestion :
  - Fonction de réinitialisation du mot de passe du portail Azure
  - 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 défense contre les menaces virtuelles.
- Haute accessibilité (actif/en veille)
- Mise en grappes
- IPv6
- Importation/exportation de VM
- 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
- Gestionnaire d'appareil interface utilisateur (versions 6.4 et antérieures)

Fonctionnalité Azure DDoS Protection

Azure DDoS Protection dans Microsoft Azure est une fonctionnalité supplémentaire implémentée à l'avant de défense contre les menaces virtuelles. Dans un réseau virtuel, lorsque cette fonctionnalité est activée, elle aide à défendre les applications contre les attaques courantes de couche de réseau en fonction du paquet par seconde du trafic attendu d'un réseau. Vous pouvez personnaliser cette fonctionnalité en fonction du modèle de trafic réseau.

Pour en savoir plus sur la fonctionnalité Azure DDoS Protection, consultez la présentation de la norme Azure DDoS Protection.

Snort

- Si vous observez un comportement anormal comme un délai d'arrêt du Snort long, un ralentissement de la machine virtuelle en général ou l'exécution d'un processus spécifique, collectez les journaux de défense contre les menaces virtuelles et de l'hôte VM. La collecte de l'utilisation globale du processeur, de la mémoire, de l'utilisation des E/S et de la vitesse de lecture/écriture vous aidera à résoudre les problèmes.
- Une utilisation élevée de la CPU et des E/S est observée lors de l'arrêt Snort. Si un certain nombre d'instances défense contre les menaces virtuelles ont été créées sur un seul hôte avec une mémoire insuffisante et aucun processeur dédié, Snort mettra beaucoup de temps à s'arrêter, ce qui entraînera la création de cœurs Snort.

Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual

Vous avez deux options pour gérer votre Cisco Secure Firewall Threat Defense Virtual.

Cisco Secure Firewall Management Center

Si vous gérez un grand nombre d'appareils, ou si vous voulez utiliser les fonctions et configurations plus complexes que permet défense contre les menaces, utilisez centre de gestion pour configurer vos appareils au lieu du gestionnaire d'appareil intégré.

Important Vous ne pouvez pas utiliser à la fois gestionnaire d'appareil et centre de gestion pour gérer l'appareil défense contre les menaces. Une fois que la gestion intégrée gestionnaire d'appareil est activée, il ne sera plus possible d'utiliser centre de gestion pour gérer le périphérique défense contre les menaces, à moins de désactiver la gestion locale et de reconfigurer la gestion pour utiliser centre de gestion. D'un autre côté, lorsque vous enregistrez le périphérique défense contre les menaces sur centre de gestion, le service de gestion intégrée gestionnaire d'appareil est désactivé.

Mise en garde Actuellement, Cisco n'offre pas la possibilité de migrer votre configuration gestionnaire d'appareil vers centre de gestion et vice versa. Tenez-en compte lorsque vous choisissez le type de gestion que vous configurez pour le périphérique défense contre les menaces.

Cisco Secure Firewall device manager

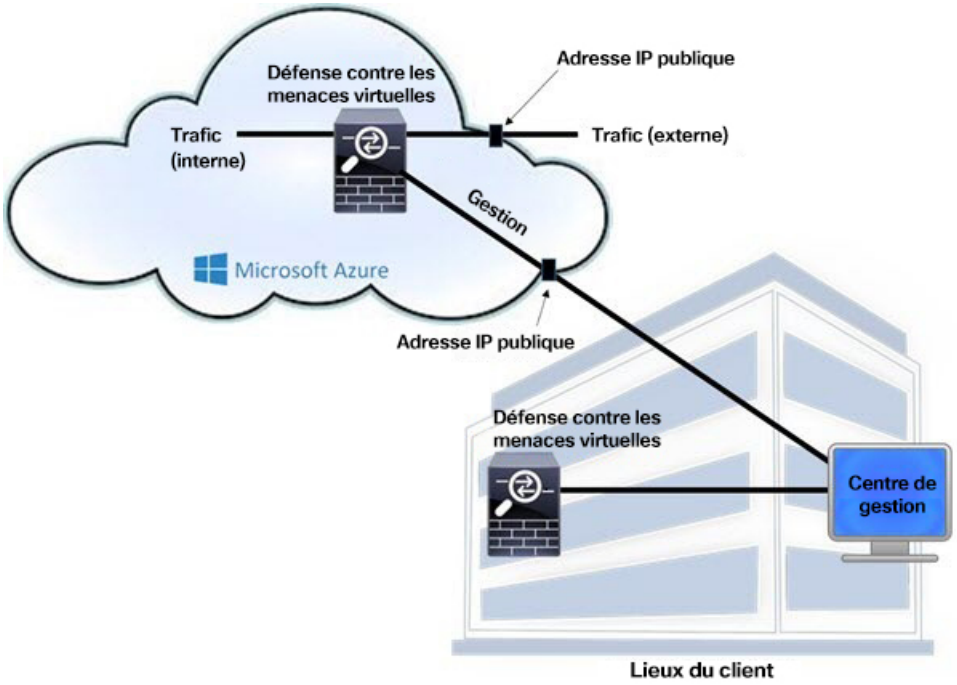
Le gestionnaire d'appareil est un gestionnaire intégré.

Le gestionnaire d'appareil est une interface de configuration Web incluse sur certains des périphériques défense contre les menaces. gestionnaire d'appareil vous permet de configurer les fonctions de base du logiciel qui sont le plus souvent utilisées pour les petits réseaux. Il est spécialement conçu pour les réseaux qui comprennent un seul périphérique ou quelques-uns, pour lesquels vous ne souhaitez pas utiliser un gestionnaire de périphériques multiples de grande puissance qui permet de contrôler un grand réseau contenant un grand nombre des périphériques défense contre les menaces.

Remarque Consultez Guide Cisco Secure Firewall Device Manager Configuration pour obtenir la liste des périphériques défense contre les menaces qui prennent en charge gestionnaire d'appareil.

Exemple de topologie de réseau pour Défense contre les menaces virtuelles sur Azure

La figure suivante montre la topologie typique pour défense contre les menaces virtuelles en mode de pare-feu avec routage. La première interface définie est toujours l'interface de gestion, et seules les interfaces Gestion 0/0 et GigabitEthernet 0/0 se voient attribuer des adresses IP publiques.



Ressources créées lors du déploiement

Lorsque vous déployez Cisco Secure Firewall Threat Defense Virtual dans Azure, les ressources suivantes sont créées :

- La machine défense contre les menaces virtuelles (VM)
- Un groupe de ressources
  - défense contre les menaces virtuelles 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.
- Quatre NICS nommées *vm name* -Nic0, *vm name* -Nic1, *vm name* -Nic2, *vm name* -Nic3

Remarque Selon les besoins, vous pouvez créer un réseau virtuel avec IPv4 uniquement.

Ces cartes réseau (NIC) correspondent aux interfaces défense contre les menaces virtuelles Gestion, Diagnostic 0/0, GigabitEthernet 0/0 et GigabitEthernet 0/1, respectivement.

- Un groupe de sécurité *vm name* -mgmt-SecurityGroup

  Le groupe de sécurité sera associé à la Nic0 de la machine virtuelle, qui correspond à l'interface de gestion défense contre les menaces virtuelles.

  Le groupe de sécurité comprend les règles qui autorisent SSH (port TCP 22) et le trafic de gestion pour l'interface centre de gestion (port TCP 8305). Vous pourrez modifier ces valeurs après le déploiement.

- Adresses IP publiques (nommées en fonction de la valeur que vous avez choisie lors du déploiement)

  Vous pouvez attribuer une adresse IP publique à n'importe quelle interface; consultez l'information sur les adresses IP publiques pour connaître les lignes directrices d'Azure concernant les adresses IP publiques, y compris comment créer, modifier ou supprimer une adresse IP publique.

- Un réseau virtuel de quatre sous-réseaux sera créé si vous choisissez l'option New Network (nouveau réseau).
- Un tableau de routage pour chaque sous-réseau (mis à jour s'il existe déjà)

  Les tableaux sont nommés *nom du sous-réseau*-ASAv-RouteTable.

  Chaque tableau de routage comprend les routes vers les trois autres sous-réseaux avec l'adresse IP défense contre les menaces virtuelles comme prochain saut. Vous pouvez choisir d'ajouter une route par défaut si le trafic doit atteindre d'autres sous-réseaux ou Internet.

- 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 *nom vm*-disk.vhd et *nom vm*-<uuid>.status
- Un compte de stockage (sauf si vous avez choisi un compte de stockage existant)

Remarque Lorsque vous supprimez une machine virtuelle, vous devez supprimer chacune de ces ressources individuellement, à l'exception de celles que vous souhaitez conserver.

Mise en réseau accélérée (AN)

La fonctionnalité de mise en réseau accélérée (AN) d'Azure permet la virtualisation d'E/S à racine unique (SR-IOV) sur une VM, ce qui accélère la mise en réseau en permettant aux cartes réseau de la VM de contourner l'hyperviseur et d'accéder directement à la carte PCIe en dessous. L'AN améliore considérablement les

performances de la VM en matière de débit et évolue également avec des cœurs supplémentaires (c.-à-d. des VM plus importantes).

L'AN est désactivée par défaut. Azure prend en charge l'activation d'AN sur les machines virtuelles préprovisionnées. Vous devez simplement arrêter la VM dans Azure et mettre à jour la propriété de la carte réseau pour définir le paramètre *enableAcceleratedNetworking* sur « true » (vrai). Consultez la documentation de Microsoft sur l'activation de la mise en réseau accélérée sur les machines virtuelles existantes. Redémarrez ensuite la VM.

Limites de l'utilisation des interfaces ixgbe-vf

Gardez à l'esprit des limites suivantes lors de l'utilisation des interfaces ixgbe-vf :

- La machine virtuelle (VM) invitée n'est pas autorisée à définir la VF en mode de proximité. Pour cette raison, le mode transparent n'est pas pris en charge lors de l'utilisation de ixgbe-vf.
- La VM invitée n'est pas autorisée à définir l'adresse MAC sur la VF. C'est pourquoi l'adresse MAC n'est pas transférée pendant la haute accessibilité, comme cela se fait sur d'autres plateformes défense contre les menaces virtuelles et avec d'autres types d'interfaces. Le basculement de la haute accessibilité fonctionne par le transfert de l'adresse IP du mode actif au mode en veille.

Remarque Cette limite s'applique également aux interfaces i40e-vf.

- Le serveur Cisco UCS-B ne prend pas en charge la vNIC ixgbe-vf.
- Dans une configuration de basculement, en cas de défaillance d'une défense contre les menaces virtuelles (unité principale) jumelée, l'unité en veille prend le rôle d'unité principale, et l'adresse IP de son interface est mise à jour avec la nouvelle adresse MAC de l'unité défense contre les menaces virtuelles en veille. Ensuite, défense contre les menaces virtuelles envoie une mise à jour spontanée du protocole ARP (Address Resolution Protocol) pour annoncer le changement d'adresse MAC de l'adresse IP de l'interface aux autres périphériques du même réseau. Cependant, en raison d'une incompatibilité avec ces types d'interfaces, la mise à jour spontanée du protocole ARP n'est pas envoyée à l'adresse IP globale qui est définie dans les instructions NAT ou PAT pour traduire l'adresse IP de l'interface en adresses IP globales.

Routeur Azure

Le routage dans un sous-réseau de réseau virtuel Azure est déterminé par la table de routage effective du sous-réseau. La table de routage effective est une combinaison d'une table de routage système existante et de la table de routage définie par l'utilisateur.

Remarque Vous pouvez afficher le tableau de routage effective sous les propriétés de NIC de la machine virtuelle.

Vous pouvez afficher et modifier la table de routage définie par l'utilisateur. Lorsque la table système et les tables définies par l'utilisateur sont combinées pour former la table de routage effective, la route la plus précise l'emporte et est liée à la table de routage définie par l'utilisateur. La table de routage système comprend également des routes spécifiques vers les autres sous-réseaux définis avec le prochain saut pointant vers la passerelle d'infrastructure de réseau virtuel d'Azure.

Pour acheminer le trafic par le biais de Azure Routing défense contre les menaces virtuelles, les routes doivent être ajoutées ou mises à jour dans le tableau de routage défini par l'utilisateur associé à chaque sous-réseau de données. Le trafic d'intérêt doit être acheminé en utilisant l'adresse IP défense contre les menaces virtuelles sur ce sous-réseau comme prochain saut.

En raison des routes spécifiques existantes dans la table de routage système, vous devez ajouter des routes spécifiques à la table de routage définie par l'utilisateur pour pointer vers défense contre les menaces virtuelles comme prochain saut. Sinon, une route par défaut dans la table définie par l'utilisateur perdrait sa route plus précise dans la table de routage système et le trafic contournerait défense contre les menaces virtuelles.

Configuration du routeur pour les machines virtuelles dans le réseau virtuel

Le routage dans Azure Virtual Network dépend du tableau de routage en vigueur et non des paramètres de passerelle particuliers sur les clients. Les clients s'exécutant dans un réseau virtuel peuvent recevoir des routages par DHCP qui sont l'adresse .1 sur leurs sous-réseaux respectifs. Il s'agit d'un espace réservé qui sert uniquement à transmettre le paquet à la passerelle virtuelle de l'infrastructure du réseau virtuel. Une fois qu'un paquet quitte la machine virtuelle, il est acheminé selon la table de routage effective (telle que modifiée par le tableau défini par l'utilisateur). La table de routage effective détermine le saut suivant, que le client virtuel ait ou non une passerelle configurée comme .1 ou comme adresse défense contre les menaces virtuelles

Les tableaux ARP de machine virtuelle Azure afficheront la même adresse MAC (1234.5678.9abc) pour tous les hôtes connus. Cela garantit que tous les paquets sortants d'une machine virtuelle Azure atteindront la passerelle Azure où la table de routage effective sera utilisée pour déterminer le chemin du paquet.

Adresses IP

Les informations suivantes s'appliquent aux adresses IP dans Azure :

- La première carte réseau sur défense contre les menaces virtuelles (qui assure le mappage avec l'interface de gestion) reçoit une adresse IP privée dans le sous-réseau auquel elle est associée.

  Une adresse IP publique peut être associée à cette adresse IP privée et la passerelle Internet Azure gérera les traductions d'adresses réseau (NAT).

- Les adresses IP publiques qui sont statiques ne changent pas tant que vous ne les avez pas modifiées dans Azure.

- Défense contre les menaces virtuelles interfaces peuvent utiliser DHCP pour définir les adresses IP. L'infrastructure Azure garantit que les interfaces défense contre les menaces virtuelles reçoivent les adresses IP définies dans Azure.

Déployer Défense contre les menaces virtuelles

Vous pouvez déployer défense contre les menaces virtuelles dans Azure à l'aide de modèles. Cisco fournit deux types de modèles :

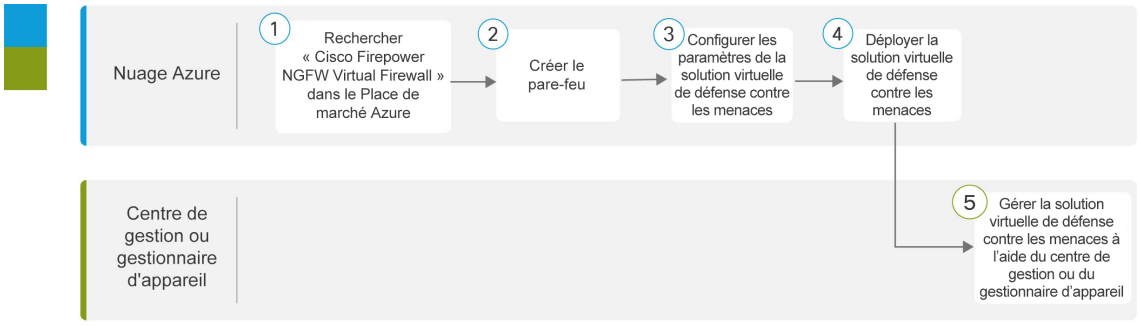
- **Modèle de solution sur la Place de marché Azure** : Utilisez le modèle de solution disponible sur la Place de marché Azure pour déployer défense contre les menaces virtuelles à l'aide du portail Azure.

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 de la Place de marché Azure à l'aide du modèle de solution, à la page 13.

- **Modèle personnalisé à l'aide d'une image gérée à partir d'un disque dur virtuel (disponible à partir de** https://software.cisco.com/download/home) : en plus du déploiement basé sur la Place de marché, Cisco fournit un disque dur virtuel compressé que vous pouvez télécharger sur Azure pour simplifier le processus de déploiement de défense contre les menaces virtuelles dans 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 pour défense contre les menaces virtuelles en une seule opération coordonnée. Pour utiliser le modèle personnalisé, consultez Déployer à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressources, à la page 15.

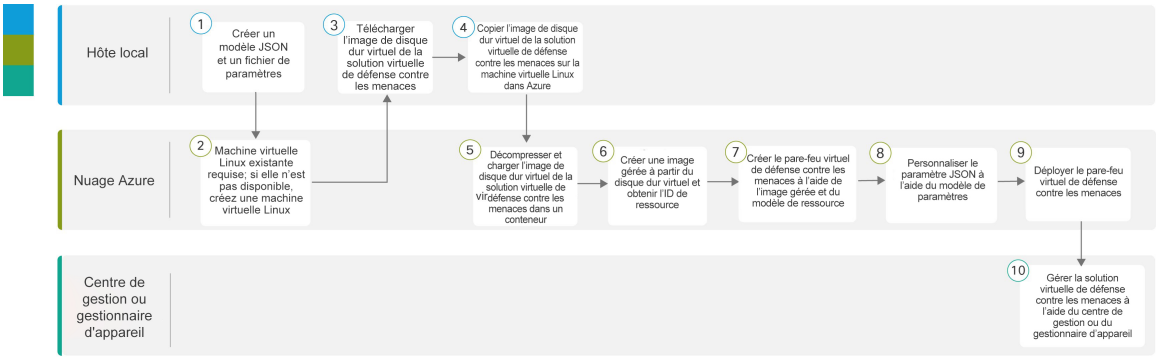
Procédure de bout en bout

Le diagramme suivant illustre le flux de travail pour le déploiement de défense contre les menaces virtuelles sur Microsoft Azure à l'aide du modèle de solution.



	Espace de travail	Étapes
1	Nuage Azure	Effectuer un déploiement à partir de la Place de marché Azure à l'aide du modèle de solution : Recherchez « Cisco Firepower NGFW Virtual Firewall » dans la Place de marché Azure.
2	Nuage Azure	Effectuer un déploiement à partir de la Place de marché Azure à l'aide du modèle de solution : Créer le pare-feu.
3	Nuage Azure	Effectuer un déploiement à partir de la Place de marché Azure à l'aide du modèle de solution : Configurer les paramètres défense contre les menaces virtuelles.
4	Nuage Azure	Effectuer un déploiement à partir de la Place de marché Azure à l'aide du modèle de solution : Déployer défense contre les menaces virtuelles.
5	Centre de gestion ou Gestionnaire d'appareil	Gérer défense contre les menaces virtuelles : • Gestion de Défense contre les menaces virtuelles avec Centre de gestion • Gestion de Défense contre les menaces virtuelles avec Gestionnaire d'appareil

Le diagramme suivant illustre le flux de travail pour le déploiement de défense contre les menaces virtuelles sur Microsoft Azure à l'aide du disque dur virtuel et du modèle de solution.



	Espace de travail	Étapes
1	Hôte local	Avant de commencer : Créez un modèle JSON et un fichier de paramètres.
2	Nuage Azure	Avant de commencer : machine virtuelle Linux existante requise - si elle n'est pas disponible, créez une machine virtuelle Linux : • Créer une machine virtuelle Linux avec l'interface de ligne de commande Azure • Créer une machine virtuelle Linux avec le portail Azure
3	Hôte local	Effectuez un déploiement à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressource : téléchargez l'image de disque dur virtuel de défense contre les menaces virtuelles de la page de téléchargement du logiciels Cisco.
4	Hôte local	Effectuez un déploiement à partir d'Azure à l'aide d'un de disque dur virtuel et d'un modèle de ressource : Copiez l'image de disque dur virtuel de défense contre les menaces virtuelles sur la machine virtuelle Linux dans Azure.
5	Nuage Azure	Effectuez un déploiement à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressource : Décompressez l'image de disque dur virtuel de défense contre les menaces virtuelles, puis téléversez-la dans un conteneur.
6	Nuage Azure	Effectuez un déploiement à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressource : Créez une image gérée à partir d'un disque dur virtuel et obtenez l'ID de ressource de cette image.
7	Nuage Azure	Effectuez un déploiement à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressource : Créez le pare-feu défense contre les menaces virtuelles à l'aide d'une image gérée et d'un modèle de ressource.
8	Nuage Azure	Effectuez un déploiement à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressource : Personnalisez les paramètres JSON à l'aide du modèle de paramètres.

	Espace de travail	Étapes
9	Nuage Azure	Effectuez un déploiement à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressource : Déployez le pare-feu défense contre les menaces virtuelles.
10	Centre de gestion ou Gestionnaire d'appareil	Gérer défense contre les menaces virtuelles : • Gestion de Défense contre les menaces virtuelles avec Centre de gestion • Gestion de Défense contre les menaces virtuelles avec Gestionnaire d'appareil

Déployer à partir de la Place de marché Azure à l'aide du modèle de solution

Les instructions suivantes vous montrent comment déployer le modèle de solution pour défense contre les menaces virtuelles qui est disponible sur la Place de marché Azure. Il s'agit d'une liste de niveaux supérieurs d'étapes pour configurer défense contre les menaces virtuelles dans l'environnement Microsoft Azure. Pour connaître les étapes détaillées de la configuration d'Azure, consultez la section sur la mise en route d'Azure.

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.

Remarque Pour utiliser les modèles ARM personnalisables disponibles dans le référentiel GitHub, consultez Déployer à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressources, à la page 15.

Procédure

Étape 1 Connectez-vous au portail Azure Resource Manager (ARM).

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 Choisissez **Azure Marketplace (Place de marché Azure)** > **Virtual Machines (machines virtuelles)**.

Étape 3 Recherchez sur place pour « Cisco Firepower NGFW Virtual (Défense contre les menaces virtuelles ») , choisissez l'offre et cliquez sur **Create** (créer).

Étape 4 Configurez les paramètres de base.

a) Entrez un nom pour la machine virtuelle. Ce nom doit être unique dans votre abonnement Azure.

Important
Si vous réutilisez un nom existant, le déploiement échouera.

b) Choisissez votre méthode de licence, **BYOL** ou **PAYG**.

Choisissez le protocole **BYOL** (Bring Your Own License; apportez votre propre licence) pour utiliser un compte de licence Cisco Smart.

Choisissez une licence **PAYG** (Pay As You Go) pour utiliser un modèle de facturation basé sur l'utilisation sans avoir à acheter de licences Cisco Smart.

Important
Vous ne pouvez utiliser **PAYG** que lorsque vous gérez le défense contre les menaces virtuelles à l'aide du centre de gestion.

c) Entrez un nom d'utilisateur pour l'administrateur défense contre les menaces virtuelles.

Remarque
Le nom « admin » est réservé dans Azure et ne peut pas être utilisé.

d) Choisissez un type d'authentification, soit un mot de passe ou une clé.

Si vous choisissez mot de passe, saisissez le mot de passe, puis confirmez-le.

Si vous choisissez une clé SSH, précisez la clé publique RSA de l'homologue distant.

e) Créez un mot de passe à utiliser avec le compte d'utilisateur **Admin** lorsque vous vous connectez pour configurer défense contre les menaces virtuelles.
f) Choisissez votre abonnement.
g) Créez un nouveau groupe de ressources (Resource Group).

défense contre les menaces virtuelles 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 défense contre les menaces virtuelles à un réseau virtuel existant dans un autre groupe de ressources lors de la configuration des options de réseau aux étapes ultérieures.

h) Sélectionner l'emplacement géographique. Il doit en être de même pour toutes les ressources utilisées dans ce déploiement (par exemple : Défense contre les menaces virtuelles, réseau, comptes de stockage).
i) Cliquez sur **OK**.

Étape 5 Configurez les paramètres défense contre les menaces virtuelles.

a) Choisissez la taille de la machine virtuelle.
b) Choisissez un compte de stockage.

Remarque
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.

c) Choisissez une adresse IP publique.

Vous pouvez choisir une adresse IP publique disponible pour l'abonnement et l'emplacement sélectionnés, ou cliquer sur **Create New** pour en créer une nouvelle.

Lorsque vous créez une nouvelle adresse IP publique, vous en obtenez une dans le bloc d'adresses IP que possède Microsoft, vous ne pouvez donc pas en choisir une en particulier. Le nombre maximal d'adresses IP publiques que vous pouvez attribuer à une interface est en fonction de votre abonnement Azure.

Important
Azure crée une adresse IP publique dynamique par défaut. L'adresse IP publique peut changer lorsque la machine virtuelle est arrêtée et redémarrée. Si vous préférez une adresse IP fixe, vous devez créer une adresse statique. Vous pouvez également modifier l'adresse IP publique après le déploiement et la faire passer d'une adresse dynamique à une adresse statique.

d) Ajoutez l'étiquette DNS.

Remarque
Le nom de domaine complet sera votre étiquette DNS plus l'URL Azure : <dnslabel>.<location>.cloudapp.azure.com

e) Choisissez un réseau virtuel.

Vous pouvez choisir un réseau virtuel Azure (VNet) existant ou en créer un nouveau et saisir l'espace d'adressage IP pour le réseau virtuel. Par défaut, l'adresse IP du routage inter-domaine sans classe (CIDR) est 10.0.0.0/16.

f) Configurez quatre sous-réseaux pour les interfaces de réseau défense contre les menaces virtuelles :

- L'interface de **gestion FTDv**, associée à Nic0 dans Azure, le « premier sous-réseau »;
- L'Interface de **diagnostic FTDv**, associée à Nic1 dans Azure, le « deuxième sous-réseau »;
- L'Interface **externe FTDv**, associée à Nic2 dans Azure, le « troisième sous-réseau »;
- L'interface **interne FTDv**, associée à Nic3 dans Azure, le « quatrième sous-réseau ».

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 **Purchase** (publier).

Les heures de déploiement varient dans Azure. Attendez qu'Azure signale que la machine virtuelle défense contre les menaces virtuelles est en cours d'exécution.

Prochaine étape

Vos prochaines étapes dépendent du mode de gestion que vous avez choisi.

- Si vous avez sélectionné **No** (non) pour **Enable Local Manager** (activer le gestionnaire local), vous utiliserez Cisco Secure Firewall Management Center pour gérer défense contre les menaces virtuelles; à ce sujet, consultez Gestion de Cisco Secure Firewall Threat Defense Virtual avec Cisco Secure Firewall Management Center.
- Si vous avez sélectionné **Yes** (oui) pour **Enable Local Manager** (activer le gestionnaire local), vous utiliserez Cisco Secure Firewall Device Manager pour gérer défense contre les menaces virtuelles; à ce sujet, consultez Gestion de Cisco Secure Firewall Threat Defense Virtual avec Cisco Secure Firewall Device Manager.

Consultez Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual pour savoir comment choisir votre option de gestion.

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 Défense contre les menaces virtuelles 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 Défense contre les menaces virtuelles. 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 Défense contre les menaces virtuelles.

Procédure

Étape 1 Téléchargez l'image de disque dur virtuel compressée Défense contre les menaces virtuelles à partir de la page de téléchargement des logiciels Cisco :

a) Accédez à **Products (produits)** > **Security (sécurité)** > **Firewalls (pare-feu)** > **Next-Generation Firewalls (NGFW) (pare-feu de nouvelle génération)** > **Secure Firewall Threat Defense Virtual**.

b) Cliquez sur **Firepower Threat Defense Software** (logiciel de défense contre les menacesFirepower) (logiciel de centre de gestion Firepower).

Suivez les instructions pour télécharger l'image.

Par exemple, Cisco_Secure_Firewall_Threat_Defense_Virtual-X.X.X-xxx.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 un client SCP ou une copie sécurisée :

```
# scp /username@remotehost.com/dir/Cisco_Secure_Firewall_Threat_Defense_Virtual-7.1.0-92.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 VHD compressée.

Étape 4 Décompressez l'image de disque dur virtuel Défense contre les menaces virtuelles.

Il existe de nombreuses options que vous pouvez utiliser pour décompresser des fichiers. Cet exemple montre l'utilitaire Bzip2, mais il existe également des utilitaires basés sur Windows qui fonctionneraient.

```
# bunzip2 Cisco_Firepower_Threat_Defense_Virtual-7.1.0-92.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 Défense contre les menaces virtuelles.

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
  Le génération 2 (**Gen 2**) n'est pas prise en charge.

- **Storage blob** (bloc de stockage) : accédez au compte de stockage pour sélectionner le disque dur téléchargé.
- **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 celle-ci prend en charge le type de compte sélectionné.
- **Host caching** (mise en cache de l'hôte) : choisissez Read/write (lecture/écriture) dans la liste déroulante.
- **Data disks** (disques de données) : laissez 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 Défense contre les menaces virtuelles à partir d'instances de 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 (**Resource ID**) 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 Défense contre les menaces virtuellesinstances de 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 (**Resource ID**) 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). Vous disposez d'un modèle de paramètres qui est disponible pour la personnalisation.

a) Cliquez sur **Load file** (charger le fichier) et accédez au fichier de paramètres Défense contre les menaces virtuelles 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 instance de Défense contre les menaces virtuelles 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 Défense contre les menaces virtuelles dans Azure.

Solution d'évolutivité automatique pour Threat Defense Virtual sur Azure

Aperçu

L'évolutivité automatique de défense contre les menaces virtuelles pour Azure est une implémentation complète sans serveur qui utilise l'infrastructure sans serveur fournie par Azure (application Logic, fonctions Azure, équilibreurs de charges, groupes de sécurité, ensemble d'évolutivité des machines virtuelles, etc.).

Certaines des fonctionnalités clés de l'évolutivité automatique de défense contre les menaces virtuelles pour la mise en œuvre d'Azure comprennent :

- Déploiement basé sur le modèle Azure Resource Manager (ARM).
- Prise en charge des mesures d'évolutivité en fonction du CPU et de la mémoire (RAM).

Remarque Consultez Logique d'évolutivité automatique, à la page 55 pour de plus amples renseignements.

- Prise en charge du déploiement d'défense contre les menaces virtuelles et des zones de multi-disponibilité.
- L'enregistrement et le désenregistrement d'instances défense contre les menaces virtuelles entièrement automatisés avec centre de gestion.
- La politique de NAT, la politique d'accès et les routes sont automatiquement appliquées aux instances défense contre les menaces virtuelles soumises à l'évolutivité à la hausse.
- Prise en charge des équilibreurs de charges et des zones de multi-disponibilité.
- Prise en charge de l'activation et de la désactivation de la fonction d'évolutivité automatique.
- Fonctionne uniquement avec centre de gestion; gestionnaire d'appareil n'est pas pris en charge.
- Prise en charge du déploiement de défense contre les menaces virtuelles avec le mode de licence PAYG ou BYOL. Le protocole PAYG s'applique uniquement aux logiciels défense contre les menaces virtuelles, versions 6.5 et ultérieures. Consultez Plateformes logicielles prises en charge, à la page 19.
- Cisco fournit un paquet de déploiement de l'évolutivité automatique pour Azure afin de faciliter le déploiement.

Plateformes logicielles prises en charge

La solution d'évolutivité automatique de défense contre les menaces virtuelles s'applique au défense contre les menaces virtuelles géré par le centre de gestion et ne dépend pas des versions logicielles. Le Guide de compatibilité Cisco Secure Firewall Threat Defense décrit la compatibilité matérielle et logicielle, y compris les exigences relatives au système d'exploitation et à l'environnement d'hébergement.

- Le tableau Centre de gestions : virtuel répertorie la compatibilité et les exigences de l'environnement d'hébergement virtuel pour centre de gestion virtuel.

- Le tableau Compatibilité de Défense contre les menaces virtuelles répertorie les exigences de compatibilité et d'environnement d'hébergement virtuel pour le défense contre les menaces virtuelles sur Azure.

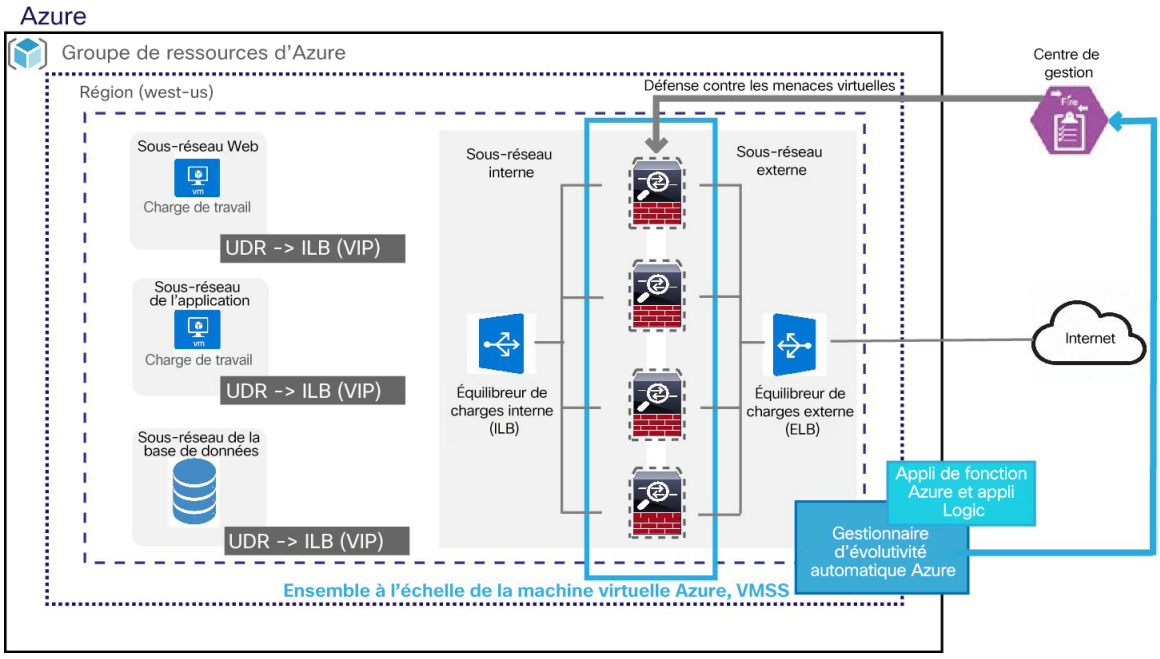
Remarque Aux fins de déploiement de la solution d'évolutivité automatique Azure, la version minimale prise en charge pour défense contre les menaces virtuelles sur Azure est la version 6.4.

Scénario d'évolutivité automatique

L'évolutivité automatique de défense contre les menaces virtuelles pour Azure est une solution d'évolutivité horizontale automatisée qui positionne ensemble d'évolutivité défense contre les menaces virtuelles pris en sandwich entre un équilibreur de charges interne (ILB) Azure et un équilibreur de charges externe (ELB) Azure.

- L'ELB distribue le trafic d'Internet aux instances défense contre les menaces virtuelles dans l'ensemble d'évolutivité; le pare-feu transfère ensuite le trafic à l'application.
- L'ILB distribue le trafic Internet sortant d'une application aux instances défense contre les menaces virtuelles dans l'ensemble d'évolutivité; le pare-feu transfère ensuite le trafic à Internet.
- Un paquet réseau ne traversera jamais les deux équilibreurs de charges (interne et externe) en une seule connexion.
- Le nombre d'instances défense contre les menaces virtuelles dans l'ensemble d'évolutivité se verra évoluer et sera configuré automatiquement en fonction des conditions de charge.

Illustration 1 : Diagramme des scénarios d'évolutivité automatique d'Défense contre les menaces virtuelles



Champ d'application

Ce document aborde les procédures détaillées pour déployer les composants sans serveur de l'évolutivité automatique de défense contre les menaces virtuelles de la solution Azure.

Important

- Lisez le document entier avant de commencer le déploiement.
- Assurez-vous que les conditions préalables sont remplies avant de commencer le déploiement.
- Assurez-vous de suivre les étapes et l'ordre d'exécution décrits dans le présent document.

Télécharger le paquet de déploiement

La solution d'évolutivité automatique de défense contre les menaces virtuelles pour Azure est un déploiement basé sur le modèle Azure Resource Manager (ARM) qui utilise l'infrastructure sans serveur fournie par Azure (application Logic, fonctions Azure, équilibreurs de charges, ensemble d'évolutivité des machines virtuelles, etc.).

Téléchargez les fichiers requis pour lancer la solution d'évolutivité automatique de défense contre les menaces virtuelles pour Azure. Les scripts et les modèles de déploiement pour votre version sont disponibles dans le référentiel GitHub.

Attention

Remarque : Les scripts et les modèles de déploiement fournis par Cisco pour l'évolutivité automatique sont présentés à titre d'exemples de code source libre et ne font pas l'objet de l'assistance technique du TAC dans sa portée normale. Consultez régulièrement GitHub pour connaître les mises à jour et les instructions ReadMe.

Consultez Créer des fonctions Azure à partir du code source, à la page 59 pour obtenir des instructions sur la façon de créer le paquet *ASM_Function.zip*.

Composants de la solution d'évolutivité automatique

Les composants suivants constituent la solution d'évolutivité automatique de défense contre les menaces virtuelles pour Azure.

Fonctions Azure (Function App)

Function App (appli de fonction) est un ensemble de fonctions Azure. Voici les fonctionnalités de base :

- Communiquez régulièrement avec les mesures d'Azure.
- Surveillez la charge de défense contre les menaces virtuelles et déclenchez les opérations d'évolutivité à la baisse/à la hausse.
- Enregistrez un nouveau défense contre les menaces virtuelles avec le centre de gestion.
- Configurez un nouveau défense contre les menaces virtuelles via centre de gestion.
- Annulez l'enregistrement (supprimez) un défense contre les menaces virtuelles faisant l'objet d'une évolutivité à la baisse de centre de gestion.

Ces fonctions sont fournies sous forme de paquets zip compressé (voir Créer le paquet d'applications Azure Function, à la page 24). Les fonctions sont aussi distinctes que possible pour effectuer des tâches spécifiques et peuvent être mises à niveau au besoin pour améliorer et prendre en charge les nouvelles versions.

Orchestrateur (application Logic)

L'application Logic d'évolutivité automatique est un flux de travail, c'est-à-dire un ensemble d'étapes dans une séquence. Les fonctions Azure sont des entités indépendantes et ne peuvent pas communiquer entre elles. Cet orchestrateur séquence l'exécution de ces fonctions et échange des renseignements entre elles.

- L'application Logic est utilisée pour orchestrer et transmettre des renseignements entre les fonctions Azure d'évolutivité automatique.
- Chaque étape représente une fonction Azure d'évolutivité automatique ou une logique standard intégrée.
- L'application Logic est fournie sous forme de fichier JSON.
- L'application Logic peut être personnalisée au moyen du fichier d'interface graphique ou JSON.

Ensemble d'évolutivité des machines virtuelles (VMSS)

Le VMSS est un ensemble de machines virtuelles homologues, telles que les appareils défense contre les menaces virtuelles.

- Le VMSS est capable d'ajouter de nouvelles machines virtuellles identiques à l'ensemble.
- Les nouvelles machines virtuelles ajoutées au VMSS sont automatiquement associées aux équilibreurs de charges, aux groupes de sécurité et aux interfaces réseau.
- Le VMSS a une fonctionnalité d'évolutivité automatique intégrée qui est désactivée pour défense contre les menaces virtuelles dans Azure.
- Vous ne devez pas ajouter ou supprimer des instances défense contre les menaces virtuelles dans le VMSS manuellement.

Modèle Azure Resource Manager (ARM)

Les modèles ARM sont utilisés pour déployer les ressources requises par l'évolutivité automatique de défense contre les menaces virtuelles pour la solution Azure.

Évolutivité automatique d' pour Azure : le modèle ARM **azure_ftdv_autoscale.json** fournit des entrées pour les composants du gestionnaire d'évolutivité automatique, notamment :

- Application de fonction Azure
- Application Azure Logic
- L'ensemble d'évolutivité des machines virtuelles (VMSS)
- Équilibreurs de charges internes et externes.
- Goupes de sécurité et autres composants divers nécessaires au déploiement.

Important Le modèle ARM a des limites en ce qui concerne la validation des entrées des utilisateurs. Il est donc de votre responsabilité de valider les entrées pendant le déploiement.

Conditions préalables

Ressources Azure

Groupe de ressources

Un groupe de ressources existant ou nouvellement créé est requis pour déployer tous les composants de cette solution.

Remarque Enregistrez le nom du groupe de ressources, la région dans laquelle il est créé et l'ID d'abonnement Azure pour une utilisation ultérieure.

Mise en réseau

Assurez-vous qu'un réseau virtuel est disponible ou créé. Un déploiement de l'évolutivité automatique ne crée, ne modifie ni ne gère de ressources réseau.

défense contre les menaces virtuelles nécessite quatre interfaces réseau. Par conséquent, votre réseau virtuel nécessite quatre sous-réseaux pour :

1. Le trafic de gestion
2. Le trafic de diagnostic
3. Le trafic interne
4. Le trafic externe

Les ports suivants doivent être ouverts dans le groupe de sécurité réseau auquel les sous-réseaux sont connectés :

- SSH (TCP/22)

  Requis pour la sonde d'intégrité entre l'équilibreur de charges et défense contre les menaces virtuelles.

  Requis pour la communication entre les fonctions sans serveur et défense contre les menaces virtuelles.

- TCP/8305

  Requis pour la communication entre défense contre les menaces virtuelles et centre de gestion.

- HTTPS (TCP/443)

  Requis pour la communication entre les composants sans serveur et centre de gestion.

- Protocole/ports spécifiques à l'application

  Requis pour toutes les applications des utilisateurs (par exemple, TCP/80, etc.).

Remarque Enregistrez le nom du réseau virtuel, le CIDR du réseau virtuel, les noms des 4 sous-réseaux et les adresses IP de passerelle des sous-réseaux externe et interne.

Créer le paquet d'applications Azure Function

La solution d'évolutivité automatique défense contre les menaces virtuelles nécessite que vous créiez un fichier d'archive : *ASM_Function.zip* qui fournit un ensemble de fonctions Azure distinctes sous la forme de paquet ZIP compressé.

Consultez Créer des fonctions Azure à partir du code source, à la page 59 pour obtenir des instructions sur la façon de créer le paquet *ASM_Function.zip*.

Ces fonctions sont aussi distinctes que possible pour effectuer des tâches spécifiques et peuvent être mises à niveau au besoin pour améliorer et prendre en charge les nouvelles versions.

Préparer Centre de gestion

Vous gérez défense contre les menaces virtuelles à l'aide du centre de gestion, un gestionnaire multipériphérique complet. défense contre les menaces virtuelles s'enregistre et communique avec centre de gestion sur l'interface de gestion que vous avez attribuée à la machine défense contre les menaces virtuelles.

Créez tous les objets nécessaires à la configuration et à la gestion de défense contre les menaces virtuelles, y compris un groupe de périphériques, afin de pouvoir déployer facilement des politiques et installer des mises à jour sur plusieurs périphériques. Toutes les configurations appliquées sur le groupe d'appareils transmises aux instances défense contre les menaces virtuelles.

Les sections suivantes donnent un bref aperçu des étapes de base pour préparer centre de gestion. Consultez en version intégrale le Guide de configuration de Secure Firewall Management Center pour en savoir plus. Lorsque vous préparez centre de gestion, assurez-vous de consigner les informations suivantes :

- L'adresse IP publique centre de gestion.
- Le nom d'utilisateur/mot de passe centre de gestion.
- Le nom de la politique de sécurité.
- Les noms d'objet de la zone de sécurité interne et externe.
- Le nom du groupe d'appareils.

Créer un nouvel utilisateur Centre de gestion

Créez un nouvel utilisateur dans centre de gestion avec des privilèges d'administrateur à utiliser uniquement par le gestionnaire d'évolutivité automatique.

Important Il est important que le compte d'utilisateur centre de gestion soit dédié à la solution d'évolutivité automatique défense contre les menaces virtuelles pour éviter les conflits avec d'autres sessions centre de gestion.

Procédure

Étape 1 Créez un nouvel utilisateur dans centre de gestion avec des privilèges d'administrateur. Sélectionnez **System** > **Users (utilisateurs du système)** et cliquez sur **Create User** (créer un utilisateur).

Le nom d'utilisateur doit être valide pour Linux :

- Au maximum, ils doivent comprendre 32 caractères alphanumériques (plus le tiret (-) et le trait de soulignement).

- Tous les caractères doivent être en minuscules.
- Il est impossible de commencer un nom d'utilisateur par un tiret (-). Un nom d'utilisateur ne peut pas se composer exclusivement de nombres. De plus, il ne peut pas inclure de point (.), de signe @ ou de barre oblique (/).

Étape 2 Remplissez les options utilisateur selon les besoins de votre environnement. Consultez Guide d'administration Cisco Secure Firewall Management Center pour obtenir des renseignements complets.

Configurer le contrôle d'accès

Configurez le contrôle d'accès pour autoriser le trafic de l'intérieur vers l'extérieur. Dans une politique de contrôle d'accès, les règles de contrôle d'accès précisent une méthode de gestion du trafic réseau sur plusieurs périphériques gérés. Il est essentiel de créer et de classer correctement les règles dans le bon ordre pour créer un déploiement efficace. Consultez les bonnes pratiques pour les règles de contrôle d'accès dans Guide de configuration Cisco Secure Firewall Management Center Device.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.

Étape 2 Cliquez sur **New Policy** (nouvelle politique).

Étape 3 Saisissez un **Name** (nom) et une **Description** facultative.

Étape 4 Consultez Guide de configuration Cisco Secure Firewall Management Center Device pour configurer les paramètres de sécurité et les règles pour votre déploiement.

Configurer les licences

Toutes les licences sont fournies au défense contre les menaces par centre de gestion. Vous pouvez également acheter les licences de fonctionnalités suivantes :

- **Secure Firewall Threat Defense IPS**—Security Intelligence (renseignements sur la sécurité) et Cisco Secure IPS
- **Cisco Secure Firewall Threat Defense Malware Defense**— Malware Defense (défense contre les programmes malveillants)
- **Filtrage URL Cisco Secure Firewall Threat Defense URL** — Filtrage URL
- **RA VPN** : AnyConnect Plus, AnyConnect Apex ou AnyConnect VPN Only.

Remarque Lorsque vous achetez une licence IPS, de défense contre les programmes malveillants ou de filtrage d'URL, vous avez également besoin d'une licence d'abonnement correspondante pour accéder aux mises à jour pendant 1, 3 ou 5 ans.

Avant de commencer

- Avoir un compte principal sur le gestionnaires de logiciels Cisco Smart Software Manager.

Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.

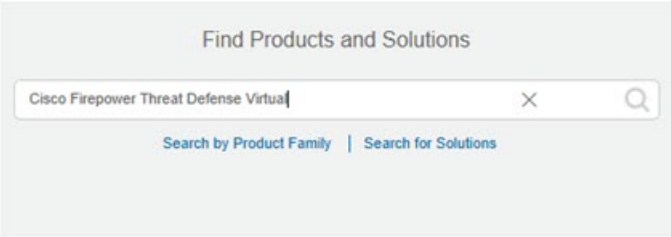
- Votre compte Cisco Smart Software Licensing doit être admissible à la licence de chiffrement renforcé (3DES/AES) pour utiliser certaines fonctionnalités (activées à l'aide de l'indicateur de conformité à l'exportation).

Procédure

Étape 1 Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin.

Lorsque vous avez acheté votre appareil auprès de Cisco ou d'un revendeur, vos licences doivent avoir été associées à votre compte de gestion des licences Smart Software. Cependant, si vous devez ajouter des licences vous-même, utilisez le champ de recherche de produits et de solutions (**Find Products and Solutions**) de Cisco Commerce Workspace. Recherchez les identifiants de produit (PID) de licences suivants :

Illustration 2 : Recherche de licences



Remarque
Si un PID est introuvable, vous pouvez l'ajouter manuellement à votre commande.

Étape 2 Si ce n'est pas déjà fait, enregistrez centre de gestion auprès du serveur de licences Smart.

Pour vous enregistrer, vous devez générer un jeton d'enregistrement dans Smart Software Manager. Consultez le Guide d'administration Cisco Secure Firewall Management Center pour des instructions détaillées.

Créer des objets de zone de sécurité

Créez des objets de zone de sécurité interne et externe pour votre déploiement.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

Étape 2 Sélectionnez **Interface** dans la liste des types d'objets.

Étape 3 Cliquez sur **Add** > **Security Zone** pour ajouter une zone de sécurité.

Étape 4 Saisissez un nom (**Name**; par exemple, *inside*, ou interne, et *outside*, ou externe).

Étape 5 Choisissez **Routed** (avec routage) comme type d'interface (**Interface Type**).

Étape 6 Cliquez sur **Save** (enregistrer).

Créer un groupe d'appareils

Les groupes de périphériques vous permettent d'attribuer facilement des politiques et d'installer des mises à jour sur plusieurs périphériques.

Procédure

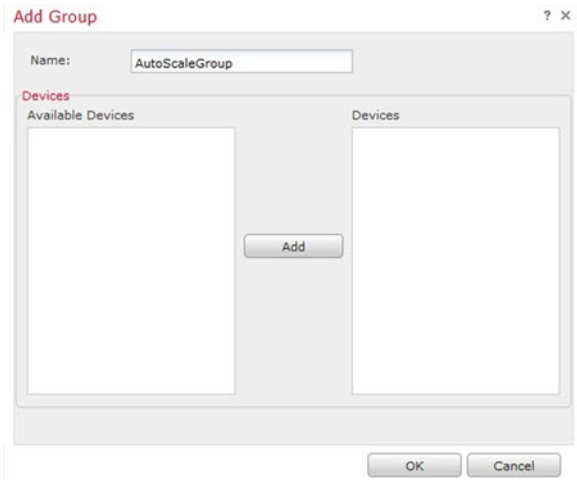
Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Illustration 3 : Gestion des périphériques

Étape 2 Dans le menu déroulant **Add** (ajouter), choisissez **Add Group** (ajouter un groupe).

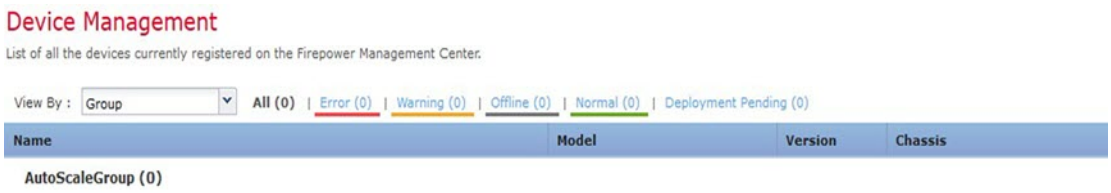
Étape 3 Saisissez un nom (**Name**). Par exemple, *AutoScaleGroup*.

Illustration 4 : Ajouter un groupe de périphériques



Étape 4 Cliquez sur **OK** pour ajouter le groupe de périphériques.

Illustration 5 : Groupe de périphériques ajouté



Configurer l'accès SSH

Les paramètres de plateforme pour les périphériques défense contre les menaces permettent de configurer une gamme de fonctionnalités indépendantes dont vous souhaitez peut-être partager les valeurs entre plusieurs périphériques. L'évolutivité automatique Défense contre les menaces virtuelles pour Azure nécessite une politique de paramètres de plateforme défense contre les menaces pour autoriser SSH sur les zones interne/externe et le groupe d'appareils créé pour le groupe d'évolutivité automatique. C'est nécessaire pour que les interfaces de données de défense contre les menaces virtuelles puissent répondre aux sondes d'intégrité des équilibreurs de charges.

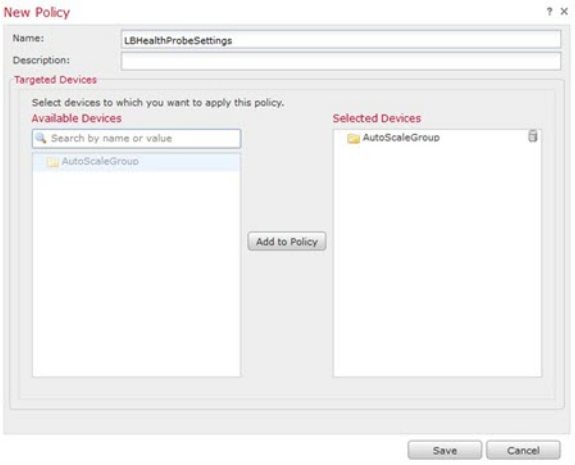
Avant de commencer

Vous avez besoin d'objets réseau qui définissent les hôtes ou les réseaux que vous autoriserez à établir des connexions SSH avec l'appareil. Vous pouvez ajouter des objets dans le cadre de la procédure, mais si vous souhaitez utiliser des groupes d'objets pour identifier un groupe d'adresses IP, assurez-vous que les groupes requis dans les règles existent déjà. Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)** pour configurer les objets. Par exemple, consultez l'objet *azure-utility-ip (168.63.129.16)* dans la procédure suivante.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Platform Settings (paramètres de la plateforme)** et créez ou modifiez une politique défense contre les menaces, par exemple *LBHealthProbeSettings*.

Illustration 6 : Stratégie des paramètres de la plateforme Défense contre les menaces



Étape 2 Sélectionnez **Secure Shell**.

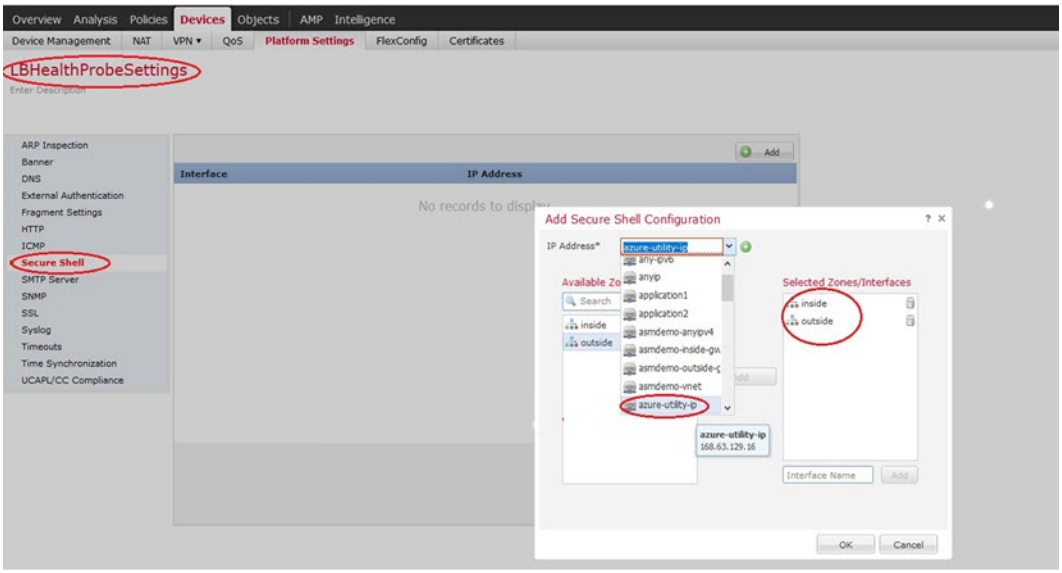
Étape 3 Déterminez les interfaces et les adresses IP qui permettent les connexions SSH.

a) Cliquez sur **Add** pour ajouter une nouvelle règle ou sur **Edit** pour modifier une règle existante.

b) Configurez les propriétés des règles :

- **IP Address** (adresse IP) : L'objet de réseau qui établit les hôtes ou les réseaux que vous autorisez à établir des connexions SSH (p. ex., *azure-utility-ip (168.63.129.16)*). Choisissez un objet dans le menu déroulant ou ajoutez un nouvel objet réseau en cliquant sur le signe plus (+).
- **Security Zones** (zones de sécurité) : Ajoutez les zones contenant les interfaces avec lesquelles vous autorisez les connexions SSH. Par exemple, vous pouvez affecter l'interface interne à la zone **interne**; et l'interface externe à la zone **externe**. Vous pouvez créer des zones de sécurité à partir de la page **Objects** (objets) de centre de gestion. Consultez Guide de configuration Cisco Secure Firewall Management Center Device pour obtenir des renseignements complets sur les zones de sécurité.
- Cliquez sur **OK**.

Illustration 7 : Accès SSH pour l'évolutivité automatique Défense contre les menaces virtuelles



Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Remarque
Vous pouvez également configurer le port TCP 443 pour la sonde d'intégrité au lieu d'utiliser **SSH Access** (accès SSH). Pour ce faire, accédez à **Devices > Platform Settings > HTTP Access** (paramètres de plateforme > accès HTTP), cochez la case **Enable HTTP Server** (activer le serveur HTTP) et saisissez **443** dans le champ **Port**. Associez ce paramètre aux interfaces interne et externe. Vous devez également modifier le port de sonde d'intégrité dans le modèle ARM en 443. Pour en savoir plus sur la configuration de l'accès HTTP, consultez la section sur la configuration de HTTP.

Configurer la traduction d'adresses réseau (NAT)

Créez une politique de traduction d'adresses réseau (NAT) et créez les règles de NAT nécessaires pour transférer le trafic de l'interface externe vers votre application, et associez cette politique au groupe d'appareils que vous avez créé pour l'évolutivité automatique.

Procédure

Étape 1 Choisissez **Périphériques** > **NAT**.

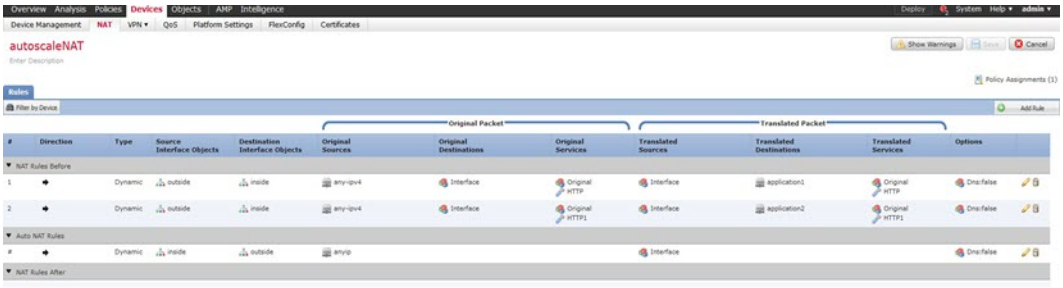
Étape 2 Dans la liste déroulante **New Policy** (nouvelle politique), choisissez **Threat Defense NAT** (traduction d'adresses réseau de défense contre les menaces).

Étape 3 Saisissez un nom unique dans le champ **Name**.

Étape 4 Vous pouvez également saisir une **Description**.

Étape 5 Configurez vos règles de NAT. Consultez la procédure sur la configuration de la NAT pour la défense contre les menaces dans Guide de configuration Cisco Secure Firewall Management Center Device pour obtenir des instructions sur la création de règles NAT et l'application des politiques de NAT. La figure suivante montre une approche de base.

Illustration 8 : Exemple de protocole de NAT



Remarque
Nous vous recommandons de garder vos règles aussi simples que possible pour éviter les problèmes de traduction et les situations de dépannage difficiles. Une planification rigoureuse avant de mettre en œuvre la NAT est essentielle.

Étape 6 Cliquez sur **Save** (enregistrer).

Paramètres d'entrée

Le tableau suivant définit les paramètres du modèle et fournit un exemple. Une fois que vous avez choisi ces valeurs, vous pouvez utiliser ces paramètres pour créer l'appareil défense contre les menaces virtuelles lorsque vous déployez le modèle ARM dans votre abonnement Azure. Consultez Déployer le modèle ARM d'évolutivité automatique, à la page 40.

Tableau 2 : Paramètres du modèle

Nom du paramètre	Type/valeurs autorisés	Description	Type de création de ressource
resourceNamePrefix	Chaîne* (3 à 10 caractères)	Toutes les ressources sont créées avec un nom contenant ce préfixe. Remarque : utilisez uniquement des lettres minuscules. Exemple : ftdv	New (Nouvelle)
virtualNetworkRg	Chaîne	Le nom du groupe de ressources du réseau virtuel. Exemple : cisco-virtualnet-rg	Existant
virtualNetworkName	Chaîne	Le nom du réseau virtuel (déjà créé). Exemple : cisco-virtualnet	Existant

Nom du paramètre	Type/valeurs autorisés	Description	Type de création de ressource
virtualNetworkCidr	Format CIDR x.x.x.x/y	CIDR du réseau virtuel (déjà créé)	Existant
mgmtSubnet	Chaîne	Le nom du sous-réseau de gestion (déjà créé). Exemple : cisco-mgmt-subnet	Existant
diagSubnet	Chaîne	Le nom du sous-réseau de diagnostic (déjà créé). Exemple : cisco-diag-subnet	Existant
insideSubnet	Chaîne	Le nom du sous-réseau interne (déjà créé). Exemple : cisco-inside-subnet	Existant
internalLbIp	Chaîne	L'adresse IP de l'équilibreur de charges interne pour le sous-réseau interne (déjà créé). Exemple : 1.2.3.4	Existant
insideNetworkGatewayIp	Chaîne	L'adresse IP de la passerelle du sous-réseau interne (déjà créé).	Existant
outsideSubnet	Chaîne	Le nom du sous-réseau externe (déjà créé). Exemple : cisco-outside-subnet	Existant
outsideNetworkGatewayIp	Chaîne	L'adresse IP de la passerelle du sous-réseau externe (déjà créé).	Existant
deviceGroupName	Chaîne	Groupe d'appareils dans centre de gestion (déjà créé)	Existant
insideZoneName	Chaîne	Nom de la zone interne dans centre de gestion (déjà créé)	Existant
outsideZoneName	Chaîne	Nom de la zone externe dans centre de gestion (déjà créé)	Existant
softwareVersion	Chaîne	La version défense contre les menaces virtuelles (sélectionnée dans la liste déroulante pendant le déploiement).	Existant
vmSize	Chaîne	Taille de l'instance défense contre les menaces virtuelles (sélectionné dans la liste déroulante pendant le déploiement).	S. O.

Nom du paramètre	Type/valeurs autorisés	Description	Type de création de ressource
ftdLicensingSku	Chaîne	Mode de licence de Défense contre les menaces virtuelles (PAYG/BYOL) Remarque : le protocole PAYG est pris en charge dans la version 6.5 et ultérieures.	S. O.
licenseCapability	Chaîne séparée par des virgules	BASE, PROGRAMME MALVEILLANT, FILTRAGE D'URL, MENACE	S. O.
ftdVmManagementUserName	Chaîne*	Le nom d'utilisateur de l'administrateur de gestion des machines virtuelles défense contre les menaces virtuelles. Cela **ne peut pas** être « admin ». Consultez Azure pour connaître les lignes directrices relatives au nom d'utilisateur de l'administrateur des VM.	New (Nouvelle)
ftdVmManagementUserPassword	Chaîne*	Mot de passe de l'utilisateur de l'administrateur de gestion des VM défense contre les menaces virtuelles. Les mots de passe doivent comporter de 12 à 72 caractères et doivent contenir : des minuscules, des majuscules, des chiffres et des caractères spéciaux; et ne doivent pas comporter plus de deux caractères répétés. **Remarque** Il n'y a pas de vérification de conformité pour cela dans le modèle.	New (Nouvelle)
fmcIpAddress	Chaîne x.x.x.x	L'adresse IP publique du centre de gestion (déjà créé)	Existant
fmcUserName	Chaîne	Nom d'utilisateur Centre de gestion, avec privilèges d'administrateur (déjà créé)	Existant

Nom du paramètre	Type/valeurs autorisés	Description	Type de création de ressource
fmcPassword	Chaîne	Mot de passe Centre de gestion pour le nom d'utilisateur centre de gestion ci-dessus (déjà créé)	Existant
policyName	Chaîne	Politique de sécurité créée dans le centre de gestion (déjà créé)	Existant
scalingPolicy	POLITIQUE-1 / POLITIQUE-2	**POLITIQUE-1** : l'évolutivité à la hausse sera déclenchée lorsque la charge moyenne de n'importe quel défense contre les menaces virtuelles dépassera le seuil d'évolutivité à la hausse pour la durée configurée. **POLITIQUE-2** : l'évolutivité à la hausse sera déclenchée lorsque la charge moyenne de tous les appareils défense contre les menaces virtuelles du groupe d'évolutivité automatique dépassera le seuil d'évolutivité à la hausse pour la durée configurée. Dans les deux cas, la logique d'évolutivité à la baisse reste la même : l'évolutivité à la baisse sera déclenchée lorsque la charge moyenne de tous les appareils défense contre les menaces virtuelles sera inférieure au seuil d'évolutivité à la baisse pour la durée configurée.	S. O.
scalingMetricsList	Chaîne	Mesures utilisées pour prendre la décision d'évolutivité. Autorisé : CPU CPU, MÉMOIRE Par défaut : CPU	S. O.

Nom du paramètre	Type/valeurs autorisés	Description	Type de création de ressource
cpuScaleInThreshold	Chaîne	Le seuil d'évolutivité à la baisse en pourcentage pour les mesures du CPU. Par défaut : 10 Lorsque la mesure défense contre les menaces virtuelles passe en dessous de cette valeur, l'évolutivité à la baisse est déclenchée. Consultez Logique d'évolutivité automatique, à la page 55.	S. O.
cpuScaleOutThreshold	Chaîne	Le seuil d'évolutivité à la hausse en pourcentage pour les mesures du CPU. Par défaut : 80 Lorsque la mesure défense contre les menaces virtuelles dépasse cette valeur, l'évolutivité à la hausse est déclenchée. La valeur « cpuScaleOutThreshold » doit toujours être **supérieure** à la valeur « cpuScaleInThreshold ». Consultez Logique d'évolutivité automatique, à la page 55.	S. O.
memoryScaleInThreshold	Chaîne	Le seuil d'évolutivité à la baisse en pourcentage pour les mesures de la mémoire. Par défaut : 0 Lorsque la mesure défense contre les menaces virtuelles passe en dessous de cette valeur, l'évolutivité à la baisse est déclenchée. Consultez Logique d'évolutivité automatique, à la page 55.	S. O.

Nom du paramètre	Type/valeurs autorisés	Description	Type de création de ressource
memoryScaleOutThreshold	Chaîne	Le seuil d'évolutivité à la hausse en pourcentage pour les mesures de la mémoire. Par défaut : 0 Lorsque la mesure défense contre les menaces virtuelles dépasse cette valeur, l'évolutivité à la hausse est déclenchée. La valeur « memoryScaleOutThreshold » doit toujours être **supérieure** à la valeur « memoryScaleInThreshold ». Consultez Logique d'évolutivité automatique, à la page 55.	S. O.
minFtdCount	Nombre entier	Le nombre minimal d'instances défense contre les menaces virtuelles disponibles dans l'ensemble d'évolutivité à tout moment. Exemple : 2	S. O.
maxFtdCount	Nombre entier	Le nombre maximal d'instances défense contre les menaces virtuelles autorisées dans l'ensemble d'évolutivité. Exemple : 10 **Remarque** Ce nombre est limité par la capacité de centre de gestion. La logique d'évolutivité automatique ne vérifiera pas la plage de cette variable. Remplacez donc cette variable avec soin.	S. O.

Nom du paramètre	Type/valeurs autorisés	Description	Type de création de ressource
metricsAverageDuration	Nombre entier	Sélectionnez une option dans la liste déroulante. Ce nombre représente la durée (en minutes) sur laquelle les mesures sont calculées en moyenne. Si la valeur de cette variable est 5 (c.-à-d. 5min), lorsque le gestionnaire d'évolutivité automatique est planifié, il vérifiera la moyenne des mesures des 5 dernières minutes et en fonction de cela, il prendra une décision en matière d'évolutivité. **Remarque** Seuls les chiffres 1, 5, 15 et 30 sont valides en raison des limites d'Azure.	S. O.

Nom du paramètre	Type/valeurs autorisés	Description	Type de création de ressource
initDeploymentMode	LOT/ÉTAPE		

Nom du paramètre	Type/valeurs autorisés	Description	Type de création de ressource
		Applicable principalement pour le premier déploiement ou lorsque l'ensemble d'évolutivité ne contient aucune instance défense contre les menaces virtuelles. BULK (LOT) : le gestionnaire d'évolutivité automatique tentera de déployer un nombre « minFtdCount » d'instances défense contre les menaces virtuelles en parallèle à la fois. **Remarque** Le lancement se fait en parallèle, mais l'enregistrement avec centre de gestion est séquentiel en raison des limites de centre de gestion. STEP (ÉTAPE) : le gestionnaire d'évolutivité automatique déploiera le nombre « minFtdCount » d'appareils défense contre les menaces virtuelles un par un à chaque intervalle planifié. **Remarque** L'option STEP (ÉTAPE) prendra longtemps pour que le nombre « minFtdCount » d'instances soit lancé et configuré avec centre de gestion et devienne opérationnel, mais utile pour le débogage. L'option BULK (LOT) prend le même temps pour lancer tous les nombres « minFtdCount' » de défense contre les menaces virtuelles qu'un lancement défense contre les menaces virtuelles (car il s'exécute en parallèle), mais l'enregistrement du centre de gestion est séquentiel. La durée totale du déploiement de « minFtdCount » est de défense contre les menaces virtuelles = (heure de lancement d'un défense contre les menaces virtuelles + heure d'enregistrement/configuration	

Nom du paramètre	Type/valeurs autorisés	Description	Type de création de ressource
		d'un défense contre les menaces virtuelles *minFtdCount).	
* Azure a des restrictions sur la convention de dénomination des nouvelles ressources. Vérifiez les limites ou utilisez simplement des minuscules. **N'utilisez pas d'espaces ni d'autres caractères spéciaux**.			

Déployer la solution d'évolutivité automatique

Télécharger le paquet de déploiement

La solution d'évolutivité automatique de défense contre les menaces virtuelles pour Azure est un déploiement basé sur le modèle Azure Resource Manager (ARM) qui utilise l'infrastructure sans serveur fournie par Azure (application Logic, fonctions Azure, équilibreurs de charges, ensemble d'évolutivité des machines virtuelles, etc.).

Téléchargez les fichiers requis pour lancer la solution d'évolutivité automatique de défense contre les menaces virtuelles pour Azure. Les scripts et les modèles de déploiement pour votre version sont disponibles dans le référentiel GitHub.

Attention Remarque : Les scripts et les modèles de déploiement fournis par Cisco pour l'évolutivité automatique sont présentés à titre d'exemples de code source libre et ne font pas l'objet de l'assistance technique du TAC dans sa portée normale. Consultez régulièrement GitHub pour connaître les mises à jour et les instructions ReadMe.

Consultez Créer des fonctions Azure à partir du code source, à la page 59 pour obtenir des instructions sur la façon de créer le paquet *ASM_Function.zip*.

Déployer le modèle ARM d'évolutivité automatique

Évolutivité automatique de Utilisez le modèle ARM **azure_ftdv_autoscale.json** pour déployer les ressources requises par l'évolutivité automatique dedéfense contre les menaces virtuelles pour Azure. Dans un groupe de ressources donné, le déploiement du modèle ARM crée les éléments suivants :

- Ensemble d'évolutivité des machines virtuelles (VMSS)
- Équilibreur de charges externe
- Équilibreur de charges interne
- Application de fonction Azure
- Application Logic
- Groupes de sécurité (pour les interfaces de données et de gestion)

Avant de commencer

- Téléchargez les modèles ARM à partir du référentiel GitHub (https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure).

Procédure

Étape 1 Si vous devez déployer les instances défense contre les menaces virtuelles dans plusieurs zones Azure, modifiez le modèle ARM en fonction des zones disponibles dans la région de déploiement.

Exemple :

```
"zones": [
    "1",
    "2",
    "3"
],
```

Cet exemple montre la région du centre des États-Unis qui comporte trois zones.

Étape 2 Modifiez les règles de trafic requises dans l'équilibreur de charges externe. Vous pouvez ajouter n'importe quel nombre de règles en étendant ce tableau « json ».

Exemple :

```
{
 "type": "Microsoft.Network/loadBalancers",
 "name": "[variables('elbName')]",
 "location": "[resourceGroup().location]",
 "apiVersion": "2018-06-01",
 "sku": {
   "name": "Standard"
 },
 "dependsOn": [
   "[concat('Microsoft.Network/publicIPAddresses/', variables('elbPublicIpName'))]"

 ],
 "properties": {
   "frontendIPConfigurations": [
     {
       "name": "LoadBalancerFrontEnd",
         "properties": {
           "publicIPAddress": {
             "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('elbPublicIpName'))]"
           }
         }
     }
   ],
   "backendAddressPools": [
     {
       "name": "backendPool"
     }
   ],
   "loadBalancingRules": [
     {
       "properties": {
         "frontendIPConfiguration": {
           "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
variables('elbName')), '/frontendIpConfigurations/LoadBalancerFrontend')]"
         },
         "backendAddressPool": {
           "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
```

```
variables('elbName')), '/backendAddressPools/BackendPool')]"
                },
                "probe": {
                  "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
variables('elbName')), '/probes/lbprobe')]"
                },
                "protocol": "TCP",
                "frontendPort": "80",
                "backendPort": "80",
                "idleTimeoutInMinutes": "[variables('idleTimeoutInMinutes')]"
              },
              "Name": "lbrule"
            }
          ],
```

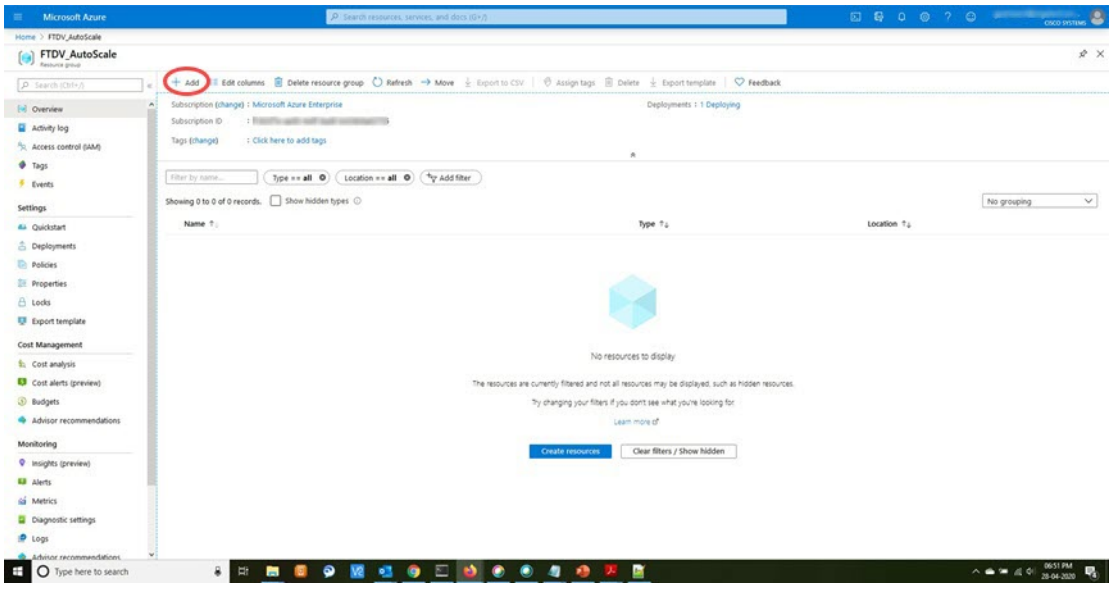
Remarque
Vous pouvez également le modifier à partir du portail Azure après le déploiement si vous préférez ne pas modifier ce fichier.

Étape 3 Connectez-vous au portail Microsoft Azure en utilisant le nom d'utilisateur et le mot de passe de votre compte Microsoft.

Étape 4 Cliquez sur **Resource groups** (groupes de ressources) dans le menu des services pour accéder à la lame Resource Groups (groupes de ressources). Vous verrez tous les groupes de ressources de votre abonnement répertoriés dans la lame.

Créez un nouveau groupe de ressources ou sélectionnez un groupe de ressources existant et vide; par exemple, *défense contre les menaces virtuelles_AutoScale*.

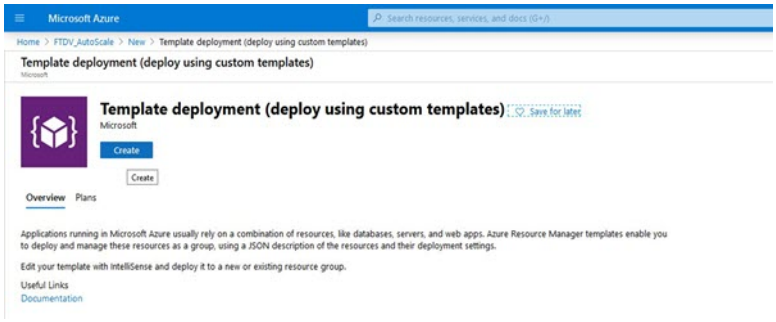
Illustration 9 : Portail Azure



Étape 5 Cliquez sur **Create a resource (+)** (créer une ressource (+)) pour créer une nouvelle ressource pour le déploiement du modèle. La lame Create Resource Group (créer un groupe de ressources) apparaît.

Étape 6 Dans **Search the Marketplace** (rechercher sur le Marché), tapez **Template deployment (deploy using custom templates)** (déploiement de modèles - déployez en utilisant des modèles personnalisés), puis appuyez sur **Enter** (Entrée).

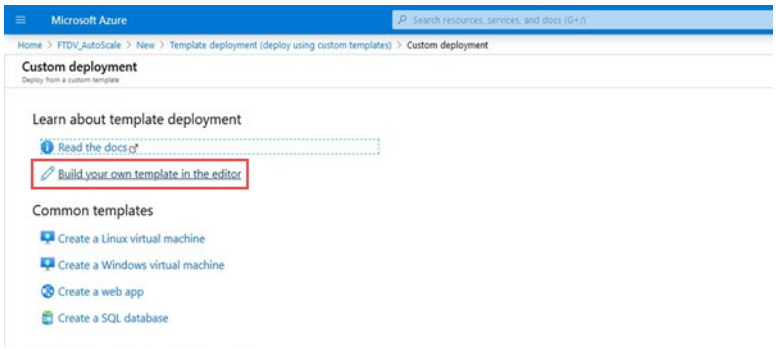
Illustration 10 : Déploiement du modèle personnalisé



Étape 7 Cliquez sur **Create** (créer).

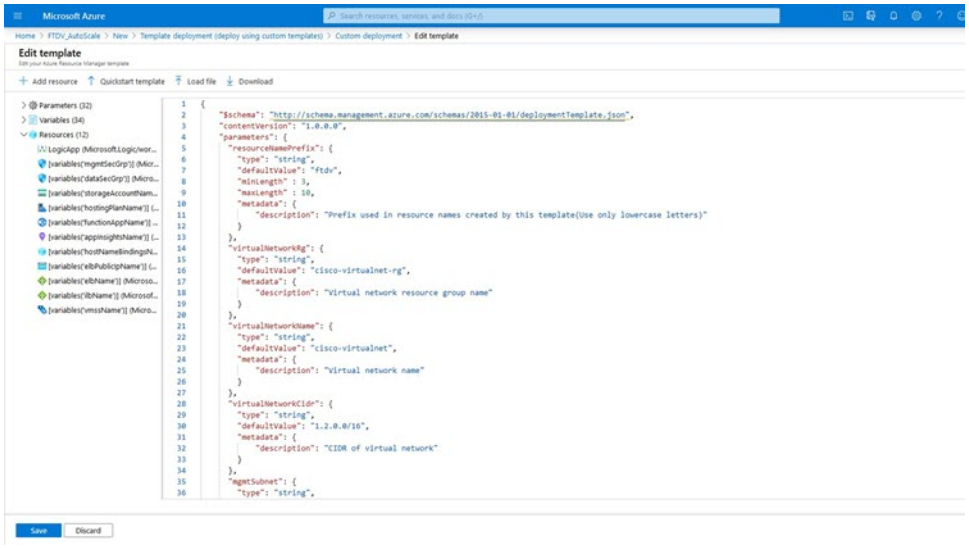
Étape 8 Il existe plusieurs options pour créer un modèle. Choisissez **Build your own template in editor** (créer votre propre modèle dans l'éditeur).

Illustration 11 : Créez votre propre modèle



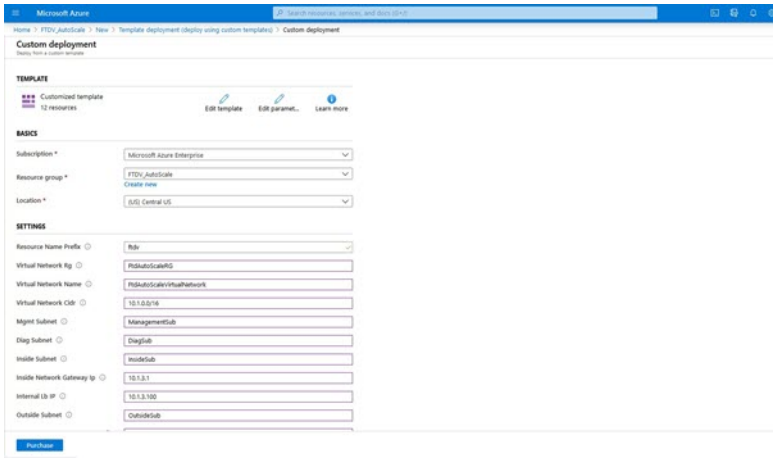
Étape 9 Dans la fenêtre **Edit template** (modifier le modèle), supprimez tout le contenu par défaut et copiez le contenu à partir du fichier *azure_ftdv et _autoscale.json* mis à jour, puis cliquez sur **Save** (enregistrer).

Illustration 12 : Modifier le modèle



Étape 10 Dans la section suivante, renseignez tous les paramètres. Reportez-vous à Paramètres d'entrée, à la page 31 pour en savoir plus sur chaque paramètre, puis cliquez sur **Purchase** (achat).

Illustration 13 : Paramètres du modèle ARM

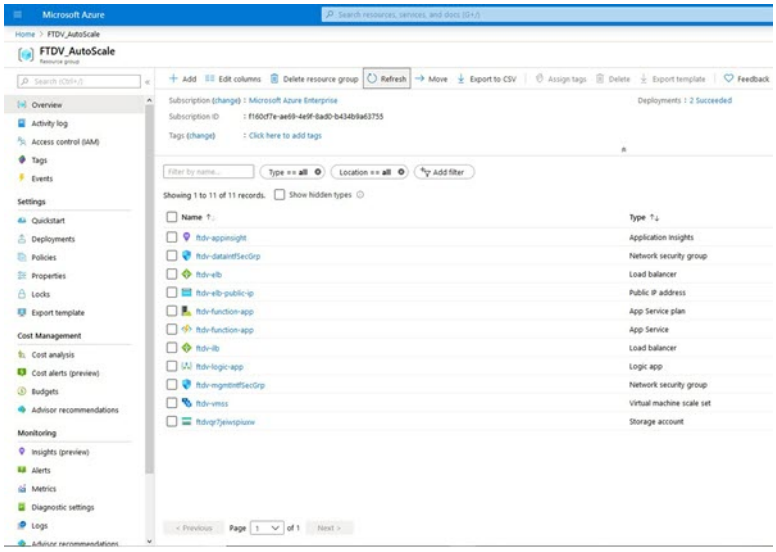


Remarque
Vous pouvez également cliquer sur **Edit Parameters** (modifier les paramètres) et modifier le fichier JSON ou charger le contenu prérempli.

Le modèle ARM a des capacités de validation d'entrée limitées. Il est donc de votre responsabilité de valider l'entrée.

Étape 11 Lorsqu'un déploiement de modèle est réussi, il crée toutes les ressources requises pour l'évolutivité automatique de défense contre les menaces virtuelles pour la solution Azure. Consultez les ressources dans la figure suivante. La colonne Type décrit chaque ressource, y compris l'application Logic, VMSS, les équilibreurs de charges, l'adresse IP publique, etc.

Illustration 14 : Threat Defense Virtual Déploiement du modèle d'évolutivité automatique



Déployer l'application de fonction Azure

Lorsque vous déployez le modèle ARM, Azure crée une application Function minimale, que vous devez ensuite mettre à jour et configurer manuellement avec les fonctions requises pour la logique du Auto Scale Manager (gestionnaire d'évolutivité automatique).

Avant de commencer

- Créez le paquet *ASM_Function.zip*. Consultez Créer des fonctions Azure à partir du code source, à la page 59.

Procédure

Étape 1 Accédez à l'application Function que vous avez créée lors du déploiement du modèle ARM et vérifiez qu'aucune fonction n'est présente. Dans un navigateur, accédez à cette URL :

https://<Function App Name>.scm.azurewebsites.net/DebugConsole

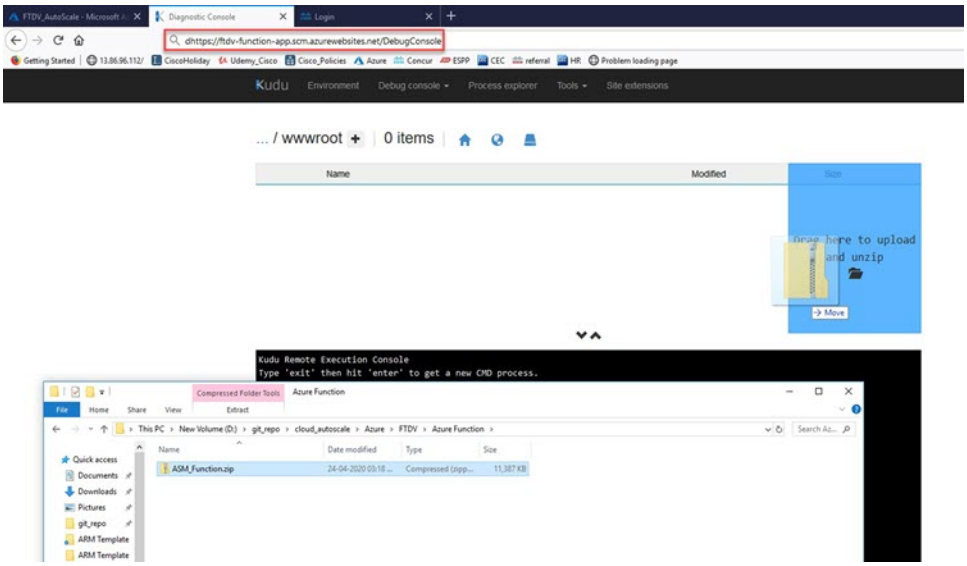
Par exemple dans Déployer le modèle ARM d'évolutivité automatique, à la page 40 :

https://ftdv-function-app.scm.azurewebsites.net/DebugConsole

Étape 2 Dans l'explorateur de fichiers, accédez à **site/wwwroot**.

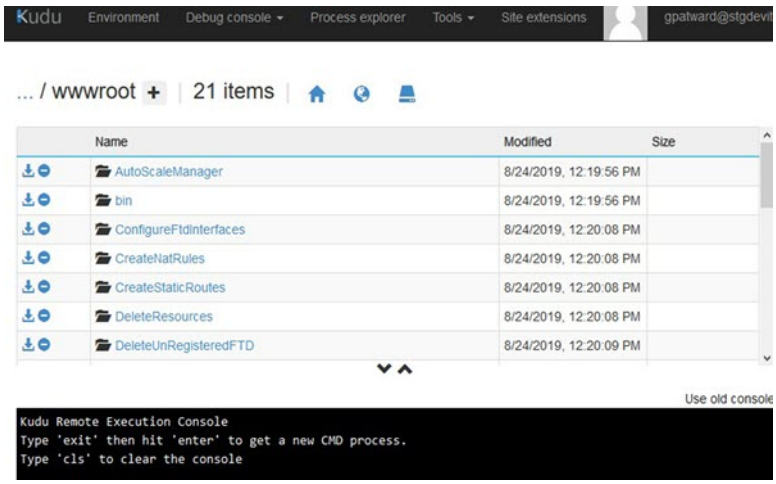
Étape 3 Glissez et déposez le fichier **ASM_Function.zip** dans le coin droit de l'explorateur de fichiers.

Illustration 15 : Charger les fonctions d'évolutivité automatique Threat Defense Virtual



Étape 4 Une fois le chargement réussi, toutes les fonctions sans serveur devraient apparaître.

Illustration 16 : Fonctions sans serveur Threat Defense Virtual

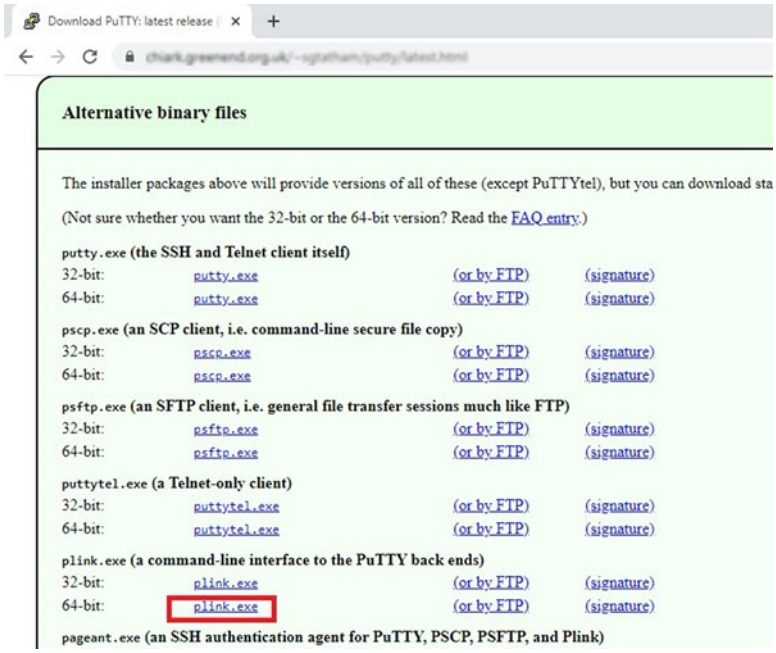


Étape 5 Téléchargez le client PuTTY SSH.

Les fonctions Azure doivent accéder à défense contre les menaces virtuelles par l'intermédiaire d'une connexion SSH. Cependant, les bibliothèques à code source libre utilisées dans le code sans serveur ne prennent pas en charge les algorithmes d'échange de clés SSH utilisés par défense contre les menaces virtuelles. Par conséquent, vous devez télécharger un client SSH préconçu.

Téléchargez l'interface CLI PuTTY sur le serveur principal PuTTY (*plink.exe*) à partir de www.putty.org.

Illustration 17 : Télécharger PuTTY



Étape 6 Renommez le fichier exécutable client SSH **plink.exe** en **ftdssh.exe**.

Étape 7 Glissez et déposez le fichier **ftdssh.exe** dans le coin droit de l'explorateur de fichiers, à l'emplacement où **ASM_Function.zip** a été chargé à l'étape précédente.

Étape 8 Vérifiez que le client SSH est présent avec l'application de fonction. Actualisez la page au besoin.

Mise au point de la configuration

Quelques configurations sont disponibles pour ajuster le gestionnaire d'évolutivité automatique ou utiliser pour le débogage. Ces options ne sont pas exposées dans le modèle ARM, mais vous pouvez les modifier dans Function App (appli de fonction).

Avant de commencer

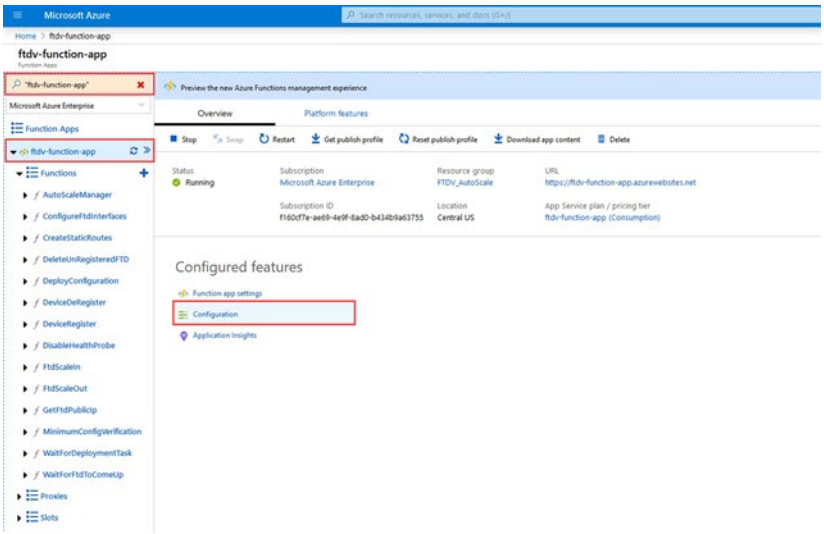
Remarque Cela peut être modifié à tout moment. Suivez cette marche à suivre pour modifier les configurations.

- Désactiver Function App (appli de fonction).
- Attendre la fin de la tâche planifiée.
- Modifier et enregistrer la configuration.
- Activer Function App (appli de fonction).

Procédure

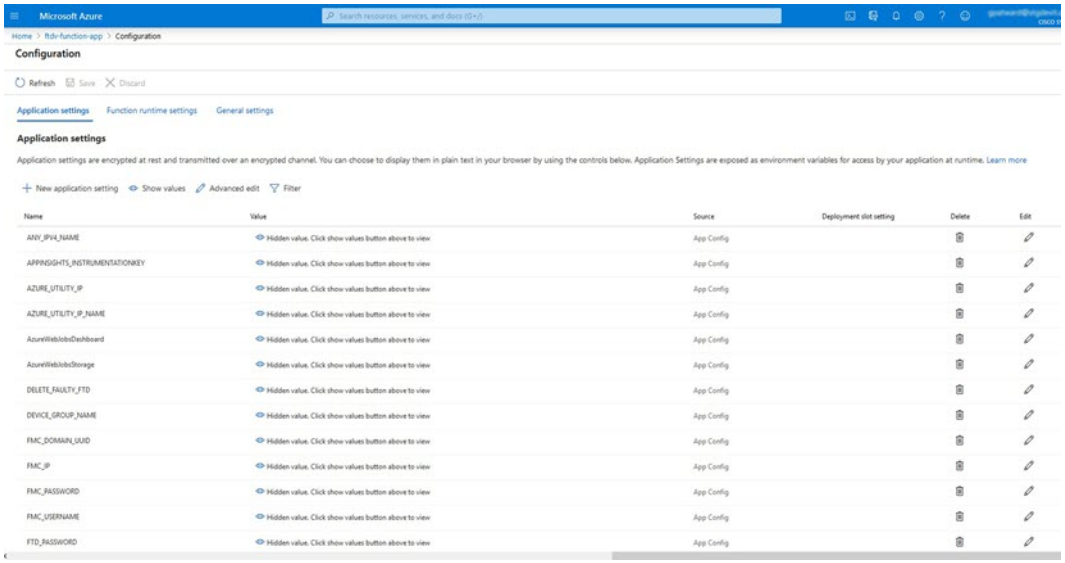
Étape 1 Dans le portail Azure, recherchez et sélectionnez l'application de fonction défense contre les menaces virtuelles.

Illustration 18 : Threat Defense VirtualFunction App (appli de fonction)



Étape 2 Les configurations transmises par le modèle ARM peuvent également être modifiées ici. Les noms des variables peuvent sembler différents de ceux du modèle ARM, mais vous pouvez facilement cerner le but de ces variables à partir de leur nom.

Illustration 19 : Paramètres de l'application



La plupart des options s'expliquent d'elles-mêmes à partir de leur nom. Par exemple :

- Nom de configuration : « DELETE_FAULTY_FTD » (valeur par défaut : OUI)

  Pendant l'évolutivité à la hausse, une nouvelle instance défense contre les menaces virtuelles est lancée et enregistrée avec l'centre de gestion. En cas d'échec de la configuration, en fonction de cette option, le gestionnaire d'évolutivité automatique décidera de conserver cette instance défense contre les menaces virtuelles ou de la supprimer. (OUI : supprimer défense contre les menaces virtuelles défectueux/NON : conserver l'instance défense contre les menaces virtuelles même si elle ne parvient pas à s'enregistrer auprès de l'centre de gestion).

- Dans les paramètres de Function App (appli de fonction), toutes les variables (y compris les variables contenant une chaîne sécurisée comme « password », soit mot de passe) peuvent être vues en texte clair par les utilisateurs qui ont accès à l'abonnement Azure.

  Si les utilisateurs rencontrent des problèmes de sécurité à ce sujet (par exemple, si un abonnement Azure est partagé entre des utilisateurs ayant des privilèges inférieurs au sein de l'organisation), un utilisateur peut utiliser le service *Key Vault* d'Azure pour protéger les mots de passe. Une fois cette configuration terminée, au lieu de fournir un « password » (mot de passe) en texte clair dans les paramètres de fonction, l'utilisateur doit fournir un identifiant sécurisé généré par le trousseau de clés où le mot de passe est stocké.

  Remarque
  Recherchez dans la documentation d'Azure pour trouver les bonnes pratiques pour sécuriser vos données d'application.

Configurer le rôle IAM dans l'ensemble de machines virtuelles évolutives

Azure Identity and Access Management (IAM) est utilisé dans le cadre de la sécurité et du contrôle d'accès Azure pour gérer et contrôler l'identité d'un utilisateur. Les identités gérées pour les ressources d'Azure fournissent aux services Azure une identité gérée automatiquement dans Azure Active Directory.

Cela permet à Function App (appli de fonction) de contrôler les ensembles d'évolutivité des machines virtuelles (VMSS) sans renseignements d'authentification explicites.

Procédure

Étape 1 Dans le portail Azure, accédez à VMSS.

Étape 2 Cliquez sur **Access control (IAM)** (contrôle d'accèas, IAM).

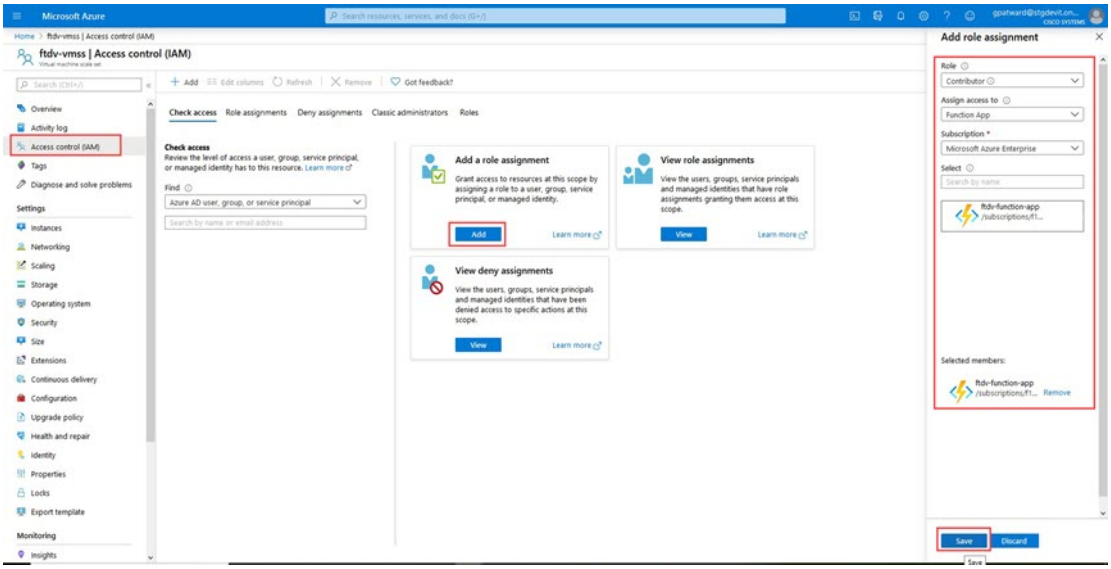
Étape 3 Cliquez sur **Add** (ajouter) pour ajouter une affectation de rôle

Étape 4 Dans la liste déroulante **Add Role Assignment** (ajouter une affectation de rôle), choisissez **Contributor** (contributeur).

Étape 5 Dans la liste déroulante **Assign access to** (affecter l'accès à), sélectionnez **Function App** (appli de fonction).

Étape 6 Sélectionnez l'application de fonction défense contre les menaces virtuelles.

Illustration 20 : Affectation du rôle AIM



Étape 7 Cliquez sur **Save** (enregistrer).

Remarque
Vous devez également vérifier qu'aucune instance défense contre les menaces virtuelles n'a encore été lancée.

Mettre à jour les groupes de sécurité

Le modèle ARM crée deux groupes de sécurité, l'un pour l'interface de gestion et l'autre pour les interfaces de données. Le groupe de sécurité de gestion autorisera uniquement le trafic requis pour les activités de gestion de défense contre les menaces virtuelles. Cependant, le groupe de sécurité de l'interface de données autorisera tout le trafic.

Procédure

Ajustez les règles des groupes de sécurité en fonction de la topologie et des besoins en application de vos déploiements.

Remarque
Le groupe de sécurité de l'interface de données doit autoriser au minimum le trafic SSH provenant des équilibreurs de charges.

Mettre à jour l'application Azure Logic

L'application Logic agit en tant qu'orchestrateur de la fonctionnalité d'évolutivité automatique. Le modèle ARM crée une application Logic minimale, que vous devez ensuite mettre à jour manuellement pour fournir les renseignements nécessaires à son fonctionnement en tant qu'orchestrateur de l'évolutivité automatique.

Procédure

Étape 1 À partir du référentiel, récupérez le fichier *LogicApp.txt* dans le système local et modifiez-le comme indiqué ci-dessous.

Important
Lisez et comprenez toutes ces étapes avant de continuer.

Ces étapes manuelles ne sont pas automatisées dans le modèle ARM afin que seule l'application Logic puisse être mise à niveau indépendamment plus tard.

a) Obligatoire : Recherchez et remplacez toutes les occurrences de « SUBSCRIPTION_ID » par les renseignements de votre ID d'abonnement.
b) Obligatoire : Recherchez et remplacez toutes les occurrences de « RG_NAME » par le nom de votre groupe de ressources.
c) Obligatoire : Recherchez et remplacez toutes les occurrences de « FUNCTIONAPPNAME » par le nom de votre application de fonction.

L'exemple suivant montre quelques-unes de ces lignes dans le fichier *LogicApp.txt* :

```
  "AutoScaleManager": {
      "inputs": {
          "function": {
              "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/AutoScaleManager"

          }
.
.
                      },
                      "Deploy_Changes_to_FTD": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeployConfiguration"

                              }
.
.
                      "DeviceDeRegister": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
```

```
                                    "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeviceDeRegister"

                                }
                            },
                            "runAfter": {
                                "Delay_For_connection_Draining": [
```

d) (Facultatif) Modifiez l'intervalle de déclenchement ou conservez la valeur par défaut (5). Il s'agit de l'intervalle de temps auquel la fonctionnalité d'évolutivité automatique est déclenchée périodiquement. L'exemple suivant montre ces lignes dans le fichier *LogicApp.txt* :

```
"triggers": {
    "Recurrence": {
        "conditions": [],
        "inputs": {},
        "recurrence": {
            "frequency": "Minute",
            "interval": 5
        },
```

e) (Facultatif) Modifiez le temps de purge ou conservez la valeur par défaut (5). Il s'agit de l'intervalle de temps pour purger les connexions existantes de défense contre les menaces virtuelles avant de supprimer le périphérique pendant l'opération d'évolutivité à la baisse. L'exemple suivant montre ces lignes dans le fichier *LogicApp.txt* :

```
"actions": {
     "Branch_based_on_Scale-In_or_Scale-Out_condition": {
         "actions": {
             "Delay_For_connection_Draining": {
                 "inputs": {
                     "interval": {
                         "count": 5,
                         "unit": "Minute"
                     }
```

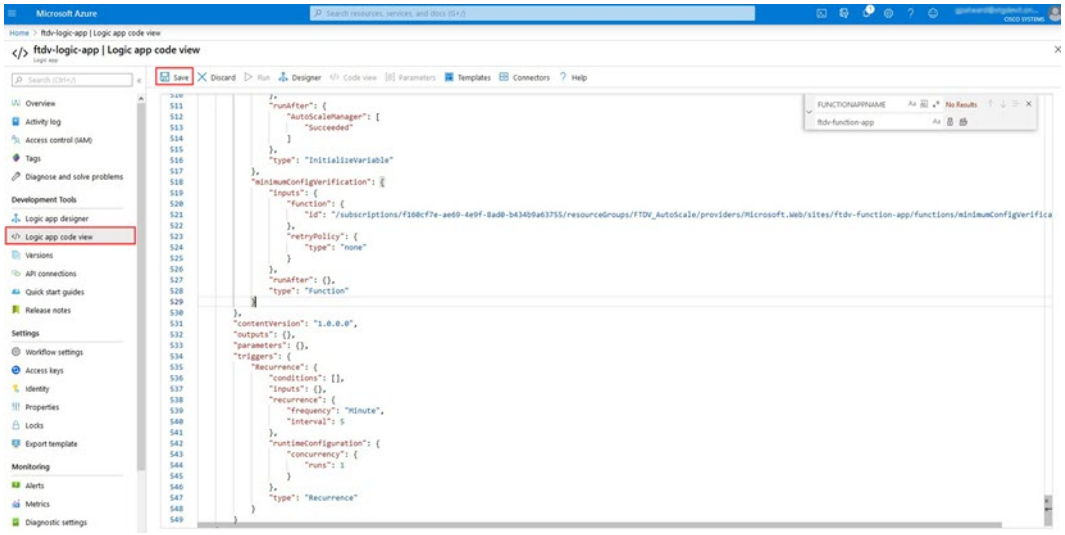
f) (Facultatif) Modifiez le temps de refroidissement ou conservez la valeur par défaut (10). C'est le moment d'effectuer NO ACTION (aucune action) une fois le processus d'évolutivité à la hausse terminé. L'exemple suivant montre ces lignes dans le fichier *LogicApp.txt* :

```
"actions": {
    "Branch_based_on_Scale-Out_or_Invalid_condition": {
        "actions": {
            "Cooldown_time": {
                "inputs": {
                    "interval": {
                        "count": 10,
                        "unit": "Second"
                    }
```

Remarque
Ces étapes peuvent également être effectuées à partir du portail Azure. Pour en savoir plus, consultez la documentation Azure.

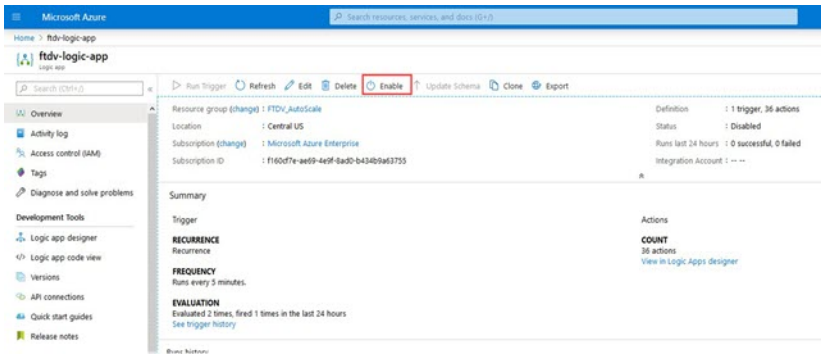
Étape 2 Accédez à **Logic App code view** (vue du code d'application Logic), supprimez le contenu par défaut et collez le contenu du fichier modifié *LogicApp.txt*, puis cliquez sur **Save** (enregistrer).

Illustration 21 : Affichage du code d'application Logic



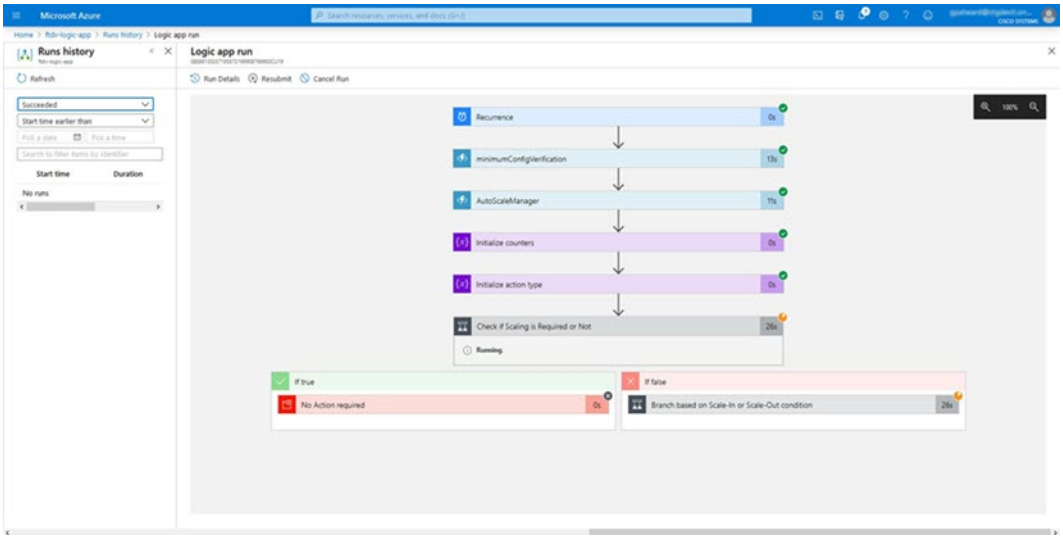
Étape 3 Lorsque vous enregistrez l'application Logic, elle est à l'état « Disabled » (désactivé). Cliquez sur **Enable** (activer) lorsque vous souhaitez démarrer le gestionnaire d'évolutivité automatique.

Illustration 22 : Activer l'application Logic



Étape 4 Une fois cette option activée, les tâches commencent à s'exécuter. Cliquez sur l'état « Running » (en cours d'exécution) pour voir l'activité.

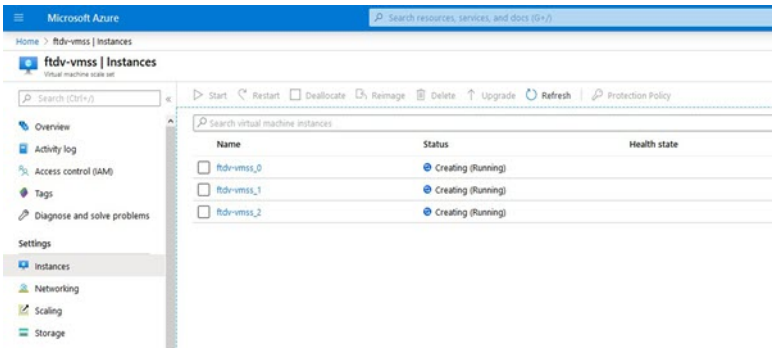
Illustration 23 : État en cours d'exécution de l'application Logic



Étape 5 Une fois que l'application Logic démarre, toutes les étapes liées au déploiement sont terminées.

Étape 6 Vérifiez dans le VMSS que des instances défense contre les menaces virtuelles sont créées.

Illustration 24 : Instances Threat Defense Virtual en cours d'exécution



Dans cet exemple, trois instances défense contre les menaces virtuelles sont lancées parce que « minFtdCount » a été défini sur « 3 » et « initDeploymentMode » a été défini sur « BULK » dans le déploiement du modèle ARM.

Mettre à niveau le défense contre les menaces virtuelles

La mise à niveau de défense contre les menaces virtuelles est prise en charge uniquement sous la forme d'une mise à niveau d'image de l'ensemble d'évolutivité des machines virtuelles (VMSS). Par conséquent, vous mettez à niveau défense contre les menaces virtuelles par l'intermédiaire de l'interface API REST d'Azure.

Remarque Vous pouvez utiliser n'importe quel client REST pour mettre à niveau défense contre les menaces virtuelles.

Avant de commencer

- Obtenez la nouvelle version de l'image défense contre les menaces virtuelles disponible sur le marché (p. ex. : 650.32.0).
- Obtenez l'UGS utilisée pour déployer l'ensemble d'évolutivité d'origine (p. ex. : ftdv-azure-byol).
- Obtenez le nom défini pour le groupe de ressources et l'ensemble d'évolutivité des machines virtuelles.

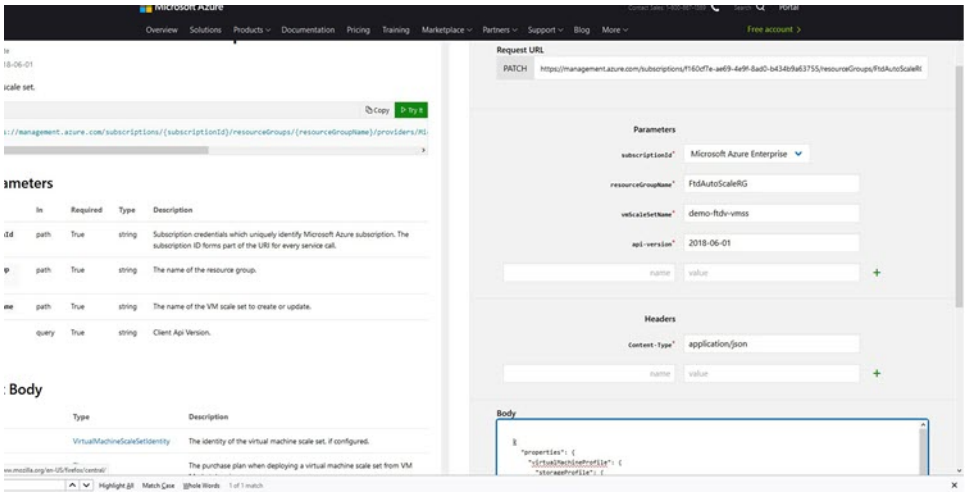
Procédure

Étape 1 Dans un navigateur, accédez à l'URL suivante :

https://docs.microsoft.com/en-us/rest/api/compute/virtualmachinescalesets/update#code-try-0

Étape 2 Saisissez les détails dans la section Parameters (paramètres).

Illustration 25 : Mettre à niveau le défense contre les menaces virtuelles



Étape 3 Saisissez l'entrée JSON contenant la nouvelle version d'image de défense contre les menaces virtuelles, l'UGS et le déclencheur d'exécution dans la section **Body** (corps).

```
{
 "properties": {
        "virtualMachineProfile": {
              "storageProfile": {
                      "imageReference": {
                           "publisher": "cisco",
                           "offer": "cisco-ftdv",
                           "sku": "ftdv-azure-byol",
                            "version": "650.32.0"
                      }
                 },
            }
      }
}
```

Étape 4 Une réponse réussie d'Azure signifie que le VMSS a accepté la modification.

La nouvelle image sera utilisée dans les nouvelles instances de défense contre les menaces virtuelles qui seront lancées dans le cadre de l'opération d'évolutivité à la hausse.

- Les instances de défense contre les menaces virtuelles existantes continueront d'utiliser l'ancienne image logicielle tant qu'elles existent dans un ensemble d'évolutivité.
- Vous pouvez remplacer le comportement ci-dessus et mettre à niveau les instances de défense contre les menaces virtuelles existantes manuellement. Pour ce faire, cliquez sur le bouton **Upgrade** (mettre à niveau) dans VMSS. Il redémarrera et mettra à niveau les instances de défense contre les menaces virtuelles sélectionnées. Vous devez réenregistrer et reconfigurer ces instances de défense contre les menaces virtuelles mises à niveau manuellement. **Notez que cette méthode n'est PAS recommandée.**

Logique d'évolutivité automatique

Mesure de l'évolutivité

Vous utilisez le modèle ARM pour déployer les ressources requises par la solution de mise à l'échelle automatique défense contre les menaces virtuelles. Lors du déploiement du modèle ARM, vous avez les options suivantes pour les mesures d'évolutivité :

- Processeur (CPU)
- CPU, mémoire (version 6.7+).

Remarque Les mesures du processeur sont recueillies auprès d'Azure; les mesures de la mémoire sont recueillies à partir du centre de gestion.

Logique d'évolutivité à la hausse

- **POLITIQUE-1** : le protocole d'évolutivité à la hausse sera déclenché lorsque la charge moyenne de **n'importe quel** défense contre les menaces virtuelles dépasse le seuil d'évolutivité à la hausse pour la durée configurée. Lorsque vous utilisez la mesure d'évolutivité « CPU, MEMORY » (CPU, mémoire), le seuil d'évolutivité à la hausse est l'utilisation moyenne du processeur**ou** de la mémoire de **tout** défense contre les menaces virtuelles de l'ensemble d'évolutivité.
- **POLITIQUE-2** : l'évolutivité à la hausse sera déclenchée lorsque la charge moyenne de **tous** les appareils défense contre les menaces virtuelles dépassera le seuil d'évolutivité à la hausse pour la durée configurée. Lorsque vous utilisez la mesure d'évolutivité « CPU, MEMORY » (CPU, mémoire), le seuil d'évolutivité à la hausse est l'utilisation moyenne du CPU **ou** de la mémoire de **tous** les appareils défense contre les menaces virtuelles de l'ensemble d'évolutivité.

Logique d'évolutivité à la baisse

- Si l'utilisation du processeur de **tous** les appareils défense contre les menaces virtuelles passe en dessous du seuil d'évolutivité à la baisse configuré pour la durée configurée. Lors de l'utilisation de la mesure d'évolutivité « CPU, MEMORY » (CPU, mémoire), si l'utilisation du processeur **et** de la mémoire de

tous les appareils défense contre les menaces virtuelles de l'ensemble d'évolutivité tombe en dessous du seuil d'évolutivité à la baisse configuré pour la durée configurée, le défense contre les menaces virtuelles avec le processeur le moins chargé sera abandonné.

Notes

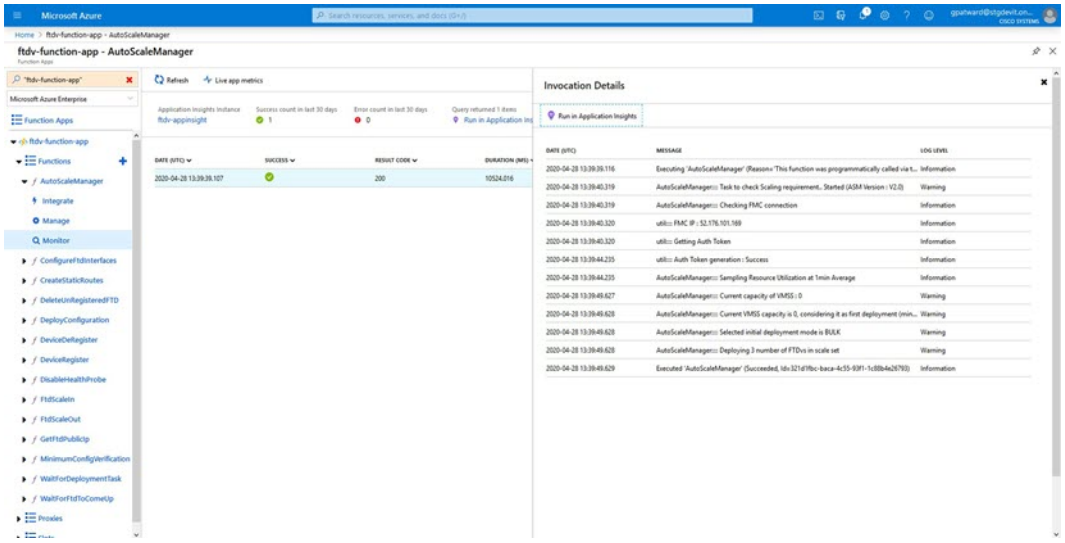
- L'évolutivité à la baisse ou à la hausse s'attache à un élément (c.-à-d. que seul 1 défense contre les menaces virtuelles sera ajouté ou abandonné à la fois).
- La mesure de l'utilisation de la mémoire reçue du centre de gestion n'est pas une valeur moyenne calculée au fil du temps, mais plutôt une valeur ponctuelle, établie selon un échantillon. Par conséquent, la mesure de la mémoire seule ne suffit pas à la prise de décisions en matière d'évolutivité. Vous n'avez pas la possibilité d'utiliser une mesure de mémoire uniquement lors du déploiement.

Journalisation et débogage de l'évolutivité automatique

Chaque composant du code sans serveur a son propre mécanisme de journalisation. En outre, des journaux sont publiés dans les données d'application.

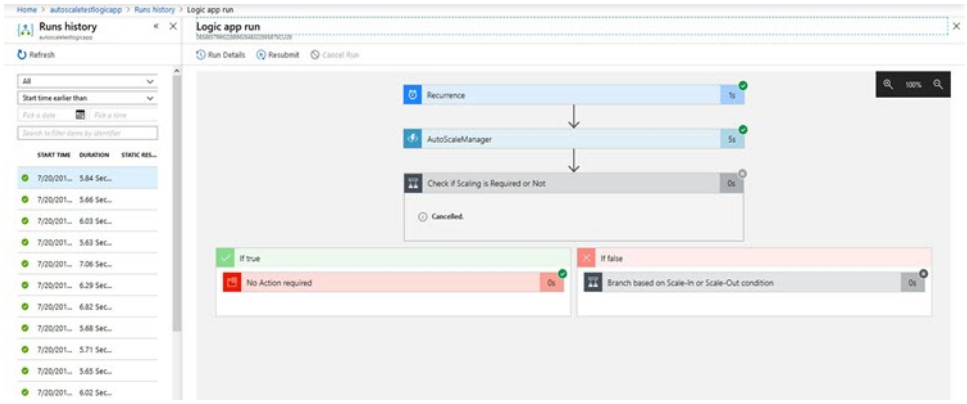
- Les journaux des fonctions Azure individuelles peuvent être consultés.

Illustration 26 : Journaux de fonction Azure



- Des journaux similaires pour chaque exécution de l'application Logic et de ses composants individuels peuvent être consultés.

Illustration 27 : Journaux d'exécution de l'application Logic



- Si nécessaire, toute tâche en cours dans l'application Logic peut être arrêtée ou terminée à tout moment. Cependant, les appareils défense contre les menaces virtuelles en cours d'exécution sont lancés ou terminés et seront dans un état incohérent.
- Le temps nécessaire à chaque exécution ou tâche individuelle peut être vu dans l'application Logic.
- L'application de fonction peut être mise à niveau à tout moment en chargeant un nouveau fichier zip. Arrêtez l'application Logic et attendez que toutes les tâches soient terminées avant de mettre à niveau l'application de fonction.

Lignes directrices et limites relatives à l'évolutivité automatique

Prenez connaissance des directives et des limites suivantes lors du déploiement de la mise à l'échelle automatique de défense contre les menaces virtuelles pour Azure :

- (Version 6.6 et antérieure) Les décisions d'évolutivité sont basées sur l'utilisation du processeur.
- (Version 6.7 ou ultérieure) Les décisions d'évolutivité peuvent se fonder sur l'utilisation du processeur (ou CPU) uniquement ou sur l'utilisation du processeur et de la mémoire.
- La gestion de Centre de gestion est requise. Gestionnaire d'appareil n'est pas pris en charge.
- Le centre de gestion doit avoir une adresse IP publique.
- L'interface de gestion défense contre les menaces virtuelles est configurée pour avoir une adresse IP publique.
- Seul IPv4 est pris en charge.
- L'évolutivité automatique de Défense contre les menaces virtuelles pour Azure prend uniquement en charge les configurations telles que les politiques d'accès, les politiques de traduction d'adresse réseau (NAT) et les paramètres de la plateforme, qui sont appliqués au groupe d'appareils et propagées aux instances de défense contre les menaces virtuelles soumises à l'évolutivité. Vous pouvez seulement modifier les configurations du groupe d'appareils à l'aide du centre de gestion. Les configurations spécifiques à l'appareil ne sont pas prises en charge.
- Le modèle ARM a des capacités de validation d'entrée limitées. Il est donc de votre responsabilité de prévoir une validation d'entrée appropriée.

- L'administrateur Azure peut voir des données sensibles (comme les informations d'authentification et les mots de passe de l'administrateur) en texte brut dans l'environnement d'application de fonction. Vous pouvez utiliser le service *Azure Key Vault* pour sécuriser des données sensibles.
- Toute modification de la configuration ne sera pas automatiquement reflétée sur les instances déjà en cours d'exécution. Ces modifications ne seront reflétées que sur les prochains périphériques intégrés. Toutes les modifications de ce type doivent être transférées manuellement vers les périphériques déjà en cours.
- Si vous rencontrez des problèmes lors de la mise à jour manuelle de la configuration sur les instances existantes, nous vous recommandons de supprimer ces instances du groupe d'évolutivité et de les remplacer par de nouvelles.

Dépannage

Voici des scénarios d'erreurs courants et des conseils de débogage pour l'évolutivité automatique de défense contre les menaces virtuelles pour Azure :

- Échec de la connexion à centre de gestion : vérifiez l'adresse IP et lles informations d'authentification de centre de gestion; vérifiez si centre de gestion est défectueux ou inaccessible.
- Impossible de connecter avec le protocole SSH à défense contre les menaces virtuelles : vérifiez si un mot de passe complexe est transmis à défense contre les menaces virtuelles au moyen du modèle; vérifiez si les groupes de sécurité autorisent les connexions SSH.
- Échec du contrôle de l'intégrité de l'équilibreur de charges : vérifiez si l'défense contre les menaces virtuelles répond à SSH sur les interfaces de données; vérifiez les paramètres du groupe de sécurité.
- Problèmes de trafic : vérifiez les règles de l'équilibreur de charges, les règles NAT ou les routes statiques configurées dans défense contre les menaces virtuelles; vérifiez les détails d'Azure Virtual Network, des sous-réseaux et de la passerelle fournis dans le modèle et les règles du groupe de sécurité.
- défense contre les menaces virtuelles n'a pas pu s'enregistrer auprès du centre de gestion : vérifiez la capacité de centre de gestion à accueillir de nouveaux appareils défense contre les menaces virtuelles; vérifiez les licences; vérifiez la compatibilité des versions défense contre les menaces virtuelles.
- L'application Logic n'a pas pu accéder à VMSS : vérifiez si la configuration du rôle IAM dans VMSS est correcte.
- L'application Logic fonctionne très longtemps : vérifiez l'accès SSH sur les appareils défense contre les menaces virtuelles qui évoluent à la hausse; vérifiez les problèmes d'enregistrement des appareils dans centre de gestion; vérifiez l'état des appareils défense contre les menaces virtuelles dans Azure VMSS.
- La fonction Azure lance une erreur liée à l'ID d'abonnement : vérifiez que vous avez un abonnement par défaut sélectionné dans votre compte.
- Échec de l'opération d'évolutivité à la baisse : parfois, Azure prend considérablement de temps pour supprimer une instance dans de telles situations. L'opération d'évolutivité à la baisse peut expirer et signaler une erreur; mais l'instance sera peut-être supprimée.
- Avant de modifier la configuration, assurez-vous de désactiver l'application Logic et d'attendre la fin de toutes les tâches en cours.

Créer des fonctions Azure à partir du code source

Configuration système requise

- Ordinateur de bureau/portable Microsoft Windows.
- Visual Studio (testé avec Visual Studio 2019 version 16.1.3)

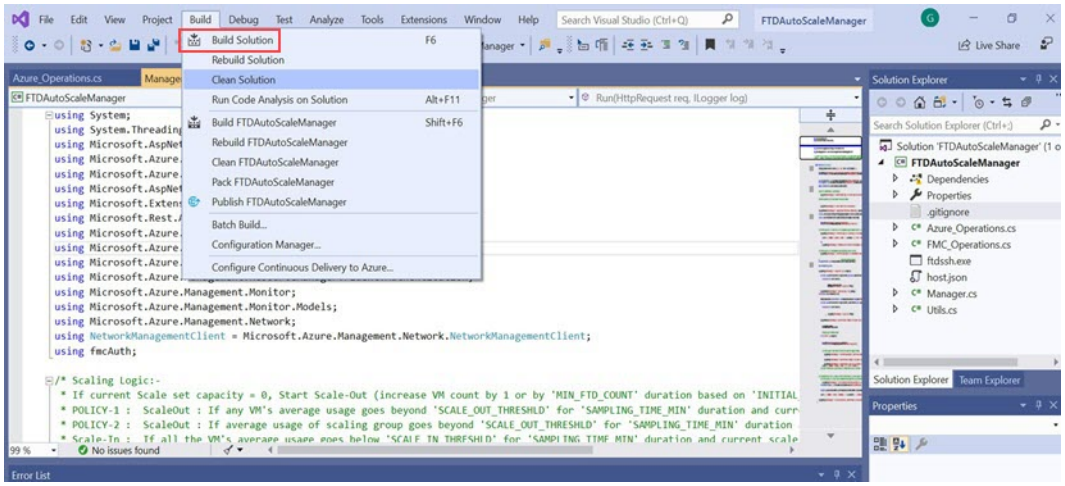
Remarque Les fonctions Azure sont écrites à l'aide de C#.

- La charge de travail « Azure Development » (développement Azure) doit être installée dans Visual Studio.

Créer avec Visual Studio

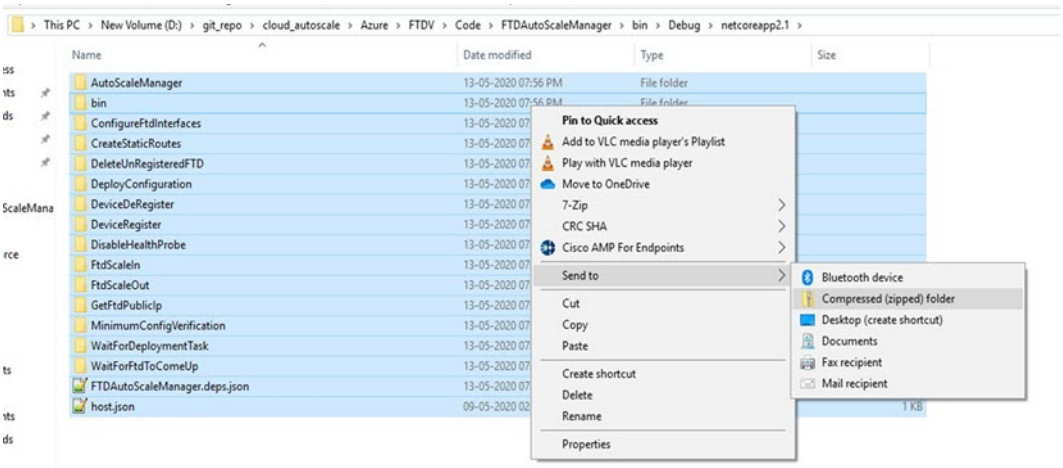
1. Téléchargez le dossier « code » sur la machine locale.
2. Accédez au dossier « FTDAutoScaleManager ».
3. Ouvrez le fichier de projet « FTDAutoScaleManager.csproj » dans Visual Studio.
4. Utilisez la procédure standard de Visual Studio pour nettoyer et créer.

Illustration 28 : Création dans Visual Studio



5. Une fois que la version est compilée avec succès, accédez au dossier **\bin\Release\netcoreapp2.1**.
6. Sélectionnez tout le contenu, cliquez sur **Send to (envoyer à)** > **Compressed (zipped) folder (dossier compressé (zip))**, et enregistrez le fichier ZIP sous le nom *ASM_Function.zip*.

Illustration 29 : Créer ASM_Function.zip



Défense contre les menaces virtuelles Instantané de l'image

Vous pouvez créer et déployer le défense contre les menaces virtuelles à l'aide d'une image d'instantané dans le portail Azure. L'instantané de l'image est une instance d'image défense contre les menaces virtuelles répliquée sans données sur l'état.

Défense contre les menaces virtuelles Survol de l'instantané

Le processus de création d'une image d'instantané de l'instance défense contre les menaces virtuelles permet de réduire au minimum le temps initial *de démarrage* du système en ignorant les procédures de premier démarrage effectuées pour défense contre les menaces virtuelles et FSIC. L'image d'instantané repose sur la base de données préremplie et le processus de démarrage initial défense contre les menaces virtuelles, qui permettent à l'image de régénérer des ID uniques (UUID, numéro de série) liés à l'identité du système dans centre de gestion ou dans tout autre centre de gestion. Ce processus permet d'accélérer le démarrage de défense contre les menaces virtuelles, ce qui est essentiel pour le déploiement de l'évolutivité automatique.

Créer l'image d'instantané Défense contre les menaces virtuelles à partir de l'image gérée

La création d'un instantané d'image Défense contre les menaces virtuelles est un processus de réplication d'une image gérée existante de l'instance défense contre les menaces virtuelles dans le portail Azure.

Avant de commencer

Vous devez avoir créé une image gérée de défense contre les menaces virtuelles version 7.2 ou ultérieure en téléversant l'image du disque dur virtuel redimensionnée dans un conteneur de votre compte de stockage Azure d'une machine virtuelle Linux dans le portail Azure. Pour en savoir plus sur la création d'images de disque sur virtuel redimensionnées, consultez Déployer à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressources, à la page 15.

Vous ne devez pas enregistrer l'instance défense contre les menaces virtuelles que vous préparez pour l'instantané d'image sur un gestionnaire tel que centre de gestion ou gestionnaire d'appareil.

Procédure

Étape 1 Accédez au portail Azure où vous avez créé l'image gérée de l'instance défense contre les menaces virtuelles.

Remarque
Assurez-vous que l'instance défense contre les menaces virtuelles que vous prévoyez de répliquer n'est pas enregistrée sur le centre de gestion ou configurée sur un autre gestionnaire local ou appliquée à une configuration.

Étape 2 Accédez au **groupe de ressources** et sélectionnez l'instance défense contre les menaces virtuelles.

Étape 3 Cliquez sur **Serial Console** (console de série) sur la page de navigation de l'instance défense contre les menaces virtuelles.

Étape 4 Utilisez les scripts suivants pour exécuter le processus de pré-instantané à partir de l'interface Shell expert :

```
> expert
admin@FTDvbaseimg:~$ Sudo su
root@firepower:/ngfw/var/common# prepare_snapshot
Do you want to continue [Y/N]:
```

Lorsque vous utilisez la commande `prepare_snapshot` dans le script, un message intermédiaire s'affiche pour demander la confirmation de l'exécution du script. Appuyez sur **Y** (oui) pour exécuter le script.

Vous pouvez également ajouter une commande `-f` à cette commande, par exemple `root@firepower:/ngfw/var/common# prepare_snapshot -f` pour ignorer le message de confirmation de l'utilisateur et exécuter directement le script.

Ce script supprime toutes les configurations de ligne, les politiques déployées, le gestionnaire configuré et les UUID associées à l'instance défense contre les menaces virtuelles. Une fois le traitement informatique terminé, l'instance défense contre les menaces virtuelles est fermée.

Étape 5 Cliquez **Capture**.

Étape 6 Dans la page **Create an image** (créer une image), choisissez un groupe de ressources existant ou créez-en un nouveau dans la liste déroulante **Resource Group** (groupe de ressources).

Étape 7 Cliquez sur **No, capture only a managed image** (non, saisir seulement une image gérée) dans la section **Instance Details** (détails de l'instance) pour créer uniquement une image gérée.

Étape 8 Saisissez le nom de l'image d'instantané que vous créez en utilisant l'image gérée de l'instance défense contre les menaces virtuelles.

Étape 9 Cliquez sur **Review+Create** (examiner et créer) pour créer une nouvelle image d'instantané de l'instance défense contre les menaces virtuelles.

Prochaine étape

Déployez l'instance défense contre les menaces virtuelles à l'aide de l'image de l'instantané. Consultez l'information sur le déploiement de Cisco Secure Firewall Threat Defense Virtual à l'aide de l'image d'instantané.

Déployer l'instance Défense contre les menaces virtuelles à l'aide de l'instantané de l'image

Avant de commencer

Cisco recommande ce qui suit :

- Confirmez qu'une image d'instantané est disponible pour l'instance défense contre les menaces virtuelles.

Procédure

Étape 1 Connectez-vous au portail Azure.

Étape 2 Copiez l'ID de ressource de l'image d'instantané nouvellement créée.

Remarque
Azure associe chaque ressource (image instantanée) à un ID de ressource. L'ID de ressource de l'image de l'instantané est requis pour le déploiement de la nouvelle instance défense contre les menaces virtuelles.

a) Dans le portail Azure, sélectionnez **Images**.
b) Sélectionnez l'image d'instantané que vous avez créée en utilisant une image gérée.
c) Cliquez sur **Overview** (aperçu) pour afficher les propriétés de l'image.
d) Copier l'ID de ressource (**Resource ID**) dans le presse-papiers. La syntaxe **de l'ID de ressource** est structurée comme suit :
/abonnements/<subscription-id>/groupesderessources/<resourceGroup>/fournisseurs/Microsoft.Compute/<conteneur>/<vhdname>

Étape 3 Poursuivez le déploiement de l'instance défense contre les menaces virtuelles à l'aide de l'image d'instantané. Consultez Déployer à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressources, à la page 15.

Remarque
Vous pouvez exécuter les commandes CLI **show version** et **show snapshot detail** à partir de la console défense contre les menaces virtuelles pour connaître la version et les détails de l'instance défense contre les menaces virtuelles nouvellement déployée.

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.