Déployer l'ASA virtuel sur Microsoft Azure Cloud

Vous pouvez déployer l'ASA virtuel sur le nuage Microsoft Azure.

Important À partir de la version 9.13(1), toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuel prise en charge. Cela permet aux ASA virtuel clients de fonctionner sur une grande variété de profils de ressources VM. Cela augmente également le nombre d'instances Azure prises en charge.

Aperçu

Sélectionnez le niveau et la taille de machine virtuelle Azure qui répondent à vos besoins ASA virtuel. Toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuelprise en charge. Cela vous permet d'exécuter l'ASA virtuel sur une grande variété de types d'instances Azure.

Tableau 1 : Types d'instances pris en charge par Azure

Instance	Attributs		Interfaces
	vCPU	Mémoire (Go)	
D3, D3_v2, DS3, DS3_v2	4	14	4
D4, D4_v2, DS4, DS4_v2	8	28	8

Instance	Attributs		Interfaces
	vCPU	Mémoire (Go)	
D5, D5_v2, DS5, DS5_v2	16	56	8
D8_v3	8	32	4
D16_v3	16	64	4
D8s_v3	8	32	4
D16s_v3	16	64	8
F4, F4s	4	8	4
F8, F8s	8	16	8
F16, F16s	16	32	8
F8s_v2	8	16	4
F16s_v2	16	32	8

Tableau 2 : ASA virtuel Limites des fonctionnalités sous licence en fonction des droits

Niveau de performance	Type d'instance (cœur/RAM)	Limite du débit	Limite de session RA VPN
ASAv5	D3_v2 4 cœurs/14 Go	100 Mbit/sec	50
ASAv10	D3_v2 4 cœurs/14 Go	1 Gbit/sec	250
ASAv30	D3_v2 4 cœurs/14 Go	2 Gbit/s	750
ASAv50	D4_v2 8 cœurs/28 Go	5,5 Gbit/s	10 000
ASAv100	D5_v2 16 cœurs/56 Go	11 Gbit/s	20 000

Vous pouvez déployer l'ASA virtuel sur Microsoft Azure :

- En tant que pare-feu autonome à l'aide d'Azure Resouce Manager sur le nuage public Azure standard et les environnements Azure pour le gouvernement
- En tant que solution partenaire intégrée à l'aide d'Azure Security Center
- En tant que paire à haute accessibilité à l'aide d'Azure Resource Manager sur le nuage public Azure standard et les environnements Azure pour le gouvernement.

Consultez Déployer l'ASA virtuel à partir d'Azure Resource Manager, à la page 11. Notez que vous pouvez déployer la configuration ASA virtuel à haute disponibilité sur le nuage public Azure standard et les environnements Azure pour le gouvernement.

Prérequis

- Créez un compte sur Azure.com.

  Après avoir créé un compte sur Microsoft Azure, vous pouvez vous connecter, choisir l'ASA virtuel dans le Marché Microsoft Azure et déployer l'ASA virtuel.

- Obtenez une licence pour l'ASA virtuel.

  Jusqu'à ce que vous obteniez une licence pour l'ASA virtuel, il fonctionnera en mode dégradé, ce qui n'autorisera que 100 connexions et un débit de 100 kbit/s. Consultez Obtention des licences logicielles Smart pour l'ASA virtuel.

Remarque L'ASA virtuel prend la valeur par défaut du droit à 2 Gbit/s lorsqu'il est déployé sur Azure. L'utilisation du droit à 100 Mbit/s et 1 Gbit/s est autorisée. Cependant, le niveau de débit doit être configuré explicitement pour utiliser le droit à 100 Mbit/s ou à 1 Gbit/s.

- Exigences d'interface :

  Vous devez déployer l'ASA virtuel avec quatre interfaces sur quatre réseaux. Vous pouvez attribuer une adresse IP publique à n'importe quelle interface. consultez Adresses IP publiques pour connaître les lignes directries d'Azure concernant les adresses IP publiques, y compris comment créer, modifier ou supprimer une adresse IP publique.

- Interface de gestion :

  Dans Azure, la première interface définie est toujours l'interface de gestion.

- Chemins de communication :

  - Interface de gestion : utilisée pour l'accès SSH et pour connecter l'ASA virtuel à l'ASDM.

Remarque La mise en réseau accélérée Azure n'est pas prise en charge sur l'interface de gestion.

  - Interface interne (requise) : utilisée pour connecter l'ASA virtuel aux hôtes internes.
  - Interface externe (requise) : utilisée pour connecter l'ASA virtuel au réseau public.
  - Interface DMZ (facultative) : utilisée pour connecter l'ASA virtuel au réseau DMZ lors de l'utilisation de l'interface Standard_D3.

- Pour en savoir plus sur l'hyperviseur ASA virtuel et la plateforme virtuelle, consultez compatibilité de Cisco Cisco Secure Firewall ASA.

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

- Déploiement à partir de Microsoft Azure Cloud
- Mise en réseau accélérée (AN) Azure
- Maximum de 16 vCPU, en fonction du type d'instance sélectionné

Remarque Azure ne fournit pas de capacité vSwitch configurable de couche 2.

- Adresse IP publique sur n'importe quelle interface

  Vous pouvez attribuer une adresse IP publique à n'importe quelle interface; consultez 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.

- Mode de pare-feu routé (par défaut)

Remarque En mode de pare-feu routé, l'ASA virtuel est une limite traditionnelle de couche 3 dans le réseau. Ce mode requiert une adresse IP pour chaque interface. Comme Azure ne prend pas en charge les interfaces balisées VLAN, les adresses IP doivent être configurées sur les interfaces non balisées et sans liaison.

Fonctionnalité Azure DDoS Protection

Azure DDoS Protection dans Microsoft Azure est une fonctionnalité supplémentaire implémentée à l'avant d'ASA virtuel. 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 Présentation de la norme Azure DDoS Protection.

Configuration du mot de passe

Assurez-vous que le mot de passe que vous définissez est conforme aux lignes directrices indiquées ci-dessous. Le mot de passe doit :

- être une chaîne alphanumérique avec un minimum de 12 caractères et un maximum de 72 caractères
- être composé de caractères minuscules et majuscules, de chiffres et de caractères spéciaux qui ne sont pas « \ » ou « - »
- ne pas comporter plus de 2 caractères ASCII répétés ou séquentiels
- ne pas être un mot que l'on peut trouver dans le dictionnaire

Si vous observez des problèmes de déploiement, tels que ceux énumérés ci-dessous, ou d'autres erreurs liées au mot de passe dans les journaux de démarrage, vous devez vérifier si votre mot de passe configuré est conforme aux lignes directrices en matière de complexité de mots de passe.

Erreurs de déploiement

- `OS Provisioning failed for VM 'TEST-CISCO-TDV-QC' due to an internal error. (Code: OSProvisioningInternal Error)`

- ```
  OS Provisioning failed for VM 'TEST-CISCO-ASAVM' due to an internal error.
  InternalDetail: RoleInstanceContainerProvisioningDetails:
  MediaStorageAccountName:ProvisionVmWithUpdate; MediaStorageHostName:ProvisionVmWithUpdate;
   MediaRelativeUrl:ProvisionVmWithUpdate;
  MediaTenantSecretId:00000000-0000-0000-0000-000000000000; ProvisioningResult:Failure;
  ProvisioningResultMessage:[ProtocolError] [CopyOvfEnv]
  Error mounting dvd: [OSUtilError] Failed to mount dvd device Inner error: [mount -o ro
   -t udf,iso9660 /dev/hdc /mnt/cdrom/secure] returned 32:
  mount: /mnt/cdrom/secure: no medium found on /dev/hdc
  ```

Vous pouvez examiner et reconfirmer ces erreurs liées au mot de passe en vous référant au journal de la console de série. Voici un exemple de détail d'erreur provenant d'un journal de console de série :

```
10150 bytes copied in 0.80 secs
Waagent - 2024-08-02T00:46:55.889400Z INFO Daemon Create user account if not exists
Waagent - 2024-08-02100:46:55.890685Z INFO Daemon Set user password.
ERROR: Password must contain:
ERROR: a value that has less than 3 repetitive or sequential ASCII characters.
Invalid Eg:aaaauser, user4321, aaabc789
Failed to add username "cisco"
ADD_USER reply indicates failure
```

Problèmes connus

Délai d'inactivité

L'ASA virtuel sur Azure a un *délai d'inactivité* configurable sur la VM. Le paramètre minimal est de 4 minutes et le paramètre maximal est de 30 minutes. Cependant, pour les sessions SSH, le paramètre minimal est de 5 minutes et le paramètre maximal est de 60 minutes.

Remarque Sachez que le délai d'inactivité de l'ASA virtuelremplace toujours le délai d'expiration SSH et déconnecte la session. Vous pouvez choisir de faire correspondre le délai d'inactivité de la VM au délai d'expiration SSH afin que la session n'expire pas de chaque côté.

Basculement de l'ASA virtuel principal à l'ASA virtuel de secours

Lorsqu'une mise à niveau Azure se produit sur un ASA virtuel haute disponibilité dans le déploiement Azure, un basculement peut se produire de l'ASA virtuel principal à l'ASA virtuelde secours. Une mise à niveau Azure fait entrer l'ASA virtuel principal dans un état de pause. L'ASA virtuel de secours ne reçoit pas de paquets Hello lorsque l'ASA virtuel principal est en pause. Si l'ASA virtuel de secours ne reçoit pas de paquets Hello au-delà du délai de rétention du basculement, un basculement vers l'ASA virtuel de secours se produit.

Il est également possible qu'un basculement se produise même si le délai de rétention du basculement n'a pas été dépassé. Imaginez un scénario dans lequel l'ASA virtuel principal reprend 19 secondes après être passé à l'état de pause. Le délai de rétention du basculement est de 30 secondes. Mais, l'ASA virtuel de secours ne reçoit pas les paquets Hello avec l'horodatage approprié, car l'horloge est synchronisée toutes les ~2 minutes. Cela entraîne un basculement de l'ASA virtuel principal vers l'ASA virtuelde secours.
```

Remarque Cette fonctionnalité prend uniquement en charge IPv4. L'ASA virtuel haute disponibilité n'est pas pris en charge pour la configuration IPv6.

Fonctionnalités non prises en charge

- Accès à la console (la gestion est effectuée à l'aide de SSH ou ASDM sur les interfaces réseau)
- Balisage du VLAN sur les interfaces d'instance d'utilisateur
- Bâtis grand format
- ARP de mandataire pour une adresse IP que l'appareil ne possède pas du point de vue d'Azure
- Mode promiscuité (pas de prise en charge du pare-feu en mode sniffer (analyseur réseau) ou transparent)

Remarque La politique Azure empêche l'ASA virtuel de fonctionner en mode de pare-feu transparent, car elle n'autorise pas les interfaces à fonctionner en mode promiscuité.

- Mode multi-contexte
- Mise en grappes
- ASA virtuel natif à haute disponibilité

Remarque Vous pouvez déployer l'ASA virtuel sur Azure dans une configuration active/de secours à haute disponibilité (HA) sans état.

- Importation/exportation de VM
- Par défaut, le mode FIPS n'est pas activé sur l'ASA virtuel exécuté dans le nuage Azure.

Remarque Si vous activez le mode FIPS, vous devez remplacer le groupe d'échange de clés Diffie-Helman par une clé plus renforcée à l'aide de la commande **ssh key-exchange group dh-group14-sha1**. Si vous ne modifiez pas le groupe Diffie-Helman, vous ne pourrez plus vous connecter à SSH avec l'ASA virtuel, et c'est la seule façon de gérer initialement l' ASA virtuel.

- IPv6
- Génération de VM de 2e génération sur Azure
- Redimensionner la VM après le déploiement
- Migration ou mise à jour de l'UGS de stockage Azure pour le disque du système d'exploitation de la VM de l'UGS premium à l'UGS standard et inversement

Ressources créées lors du déploiement

Lorsque vous déployez l'ASA virtuel dans Azure, les ressources suivantes sont créées :

- La machine ASA virtuel
- Un groupe de ressources (sauf si vous avez choisi un groupe de ressources existant)

  Le groupe de ressources ASA virtuel doit être le même groupe de ressources utilisé par le réseau virtuel et le compte de stockage.
- Quatre NIC nommés nom vm-Nic0, nom vm-Nic1, nom vm-Nic2, nom vm-Nic3

  Ces cartes réseau (NIC) correspondent aux interfaces ASA virtuel Management 0/0, GigabitEthernet 0/0, GigabitEthernet 0/1 et GigabitEthernet 0/2, respectivement.

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

- Un groupe de sécurité nommé nom vm-SSH-SecurityGroup

  Le groupe de sécurité sera associé à la Nic0 de la machine virtuelle, qui correspond à ASA virtuel Management 0/0.

  Le groupe de sécurité comprend des règles qui autorisent le protocole SSH, et les ports UDP 500 et UDP 4500 à des fins de réseau privé virtuel (VPN). 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 (IPv4 uniquement)

  à n'importe quelle interface. Consultez 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 avec quatre sous-réseaux (sauf si vous avez choisi un réseau existant)
- 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 ASA virtuel 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.

Routage Azure

Le routage dans un réseau virtuel Azure est déterminé par la table de routage effective du réseau virtuel. 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 L'ASA virtuel ne peut pas utiliser les protocoles de routage interne dynamique comme EIGRP et OSPF en raison de la nature du routage dans le nuage Azure. La table de routage effective détermine le saut suivant, que le client virtuel ait ou non une route statique/dynamique configurée.

Actuellement, vous ne pouvez pas afficher la table de routage effective ou la table de routage système.

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 spécifique l'emporte et est liée à la table de routage définie par l'utilisateur. La table de routage système comprend une route par défaut (0.0.0.0/0) pointant vers la passerelle Internet de réseau virtuel d'Azure. 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 l'ASA virtuel, le processus de déploiement d'ASA virtuel ajoute des routes sur chaque sous-réseau aux trois autres sous-réseaux en utilisant l'ASA virtuel comme saut suivant. Vous pouvez également ajouter une route par défaut (0.0.0.0/0) qui pointe vers l'interface ASA virtuel sur le sous-réseau. Cela enverra tout le trafic du sous-réseau par le biais d'ASA virtuel, ce qui peut exiger que des politiques ASA virtuel soient configurées à l'avance pour gérer ce trafic (éventuellement à l'aide de la NAT/PAT).

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 l'ASA virtuel 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 l'ASA virtuel.

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 ASA virtuel

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.

Remarque L'ASA virtuel ne peut pas utiliser les protocoles de routage interne dynamique comme EIGRP et OSPF en raison de la nature du routage dans le nuage Azure. La table de routage effective détermine le saut suivant, que le client virtuel ait ou non une route statique/dynamique configurée.

Adresses IP

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

- Vous devez utiliser DHCP pour définir les adresses IP des interfaces ASA virtuel.

  L'infrastructure Azure garantit que les interfaces de l'ASA virtuel reçoivent les adresses IP définies dans Azure.

- L'adresse IP privée de Management 0/0 se trouve dans le sous-réseau auquel il est associé.

  Une adresse IP publique peut être associée à cette adresse IP privée et la passerelle Internet Azure gérera les traductions NAT.

- Vous pouvez attribuer une adresse IP publique à n'importe quelle interface.
- Les adresses IP publiques qui sont dynamiques peuvent changer au cours d'un cycle d'arrêt/démarrage d'Azure. Cependant, elles sont persistantes pendant le redémarrage d'Azure et pendant le rechargement d'ASA virtuel.
- Les adresses IP publiques qui sont statiques ne changeront pas tant que vous ne les aurez pas modifiées dans Azure.

DNS

Tous les réseaux virtuels Azure ont accès à un serveur DNS intégré à l'adresse 168.63.129.16 que vous pouvez utiliser comme suit :

```
configure terminal
dns domain-lookup management
dns server-group DefaultDNS
 name-server 168.63.129.16
end
```

Vous pouvez utiliser cette configuration lorsque vous configurez les licences Smart et que vous n'avez pas configuré votre propre serveur DNS.

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 de l'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 Activer la mise en réseau accélérée sur les VM existantes. Redémarrez ensuite la VM.

Prise en charge du matériel Mellanox

Le nuage Microsoft Azure dispose de deux types de matériel qui prennent en charge la fonctionnalité AN : Mellanox 4 (MLX4) et Mellanox 5 (MLX5). L'ASA virtuel prend en charge AN pour le matériel Mellanox pour les instances suivantes de la version 9.15 :

- D3, D3_v2, DS3, DS3_v2
- D4, D4_v2, DS4, DS4_v2
- D5, D5_v2, DS5, DS5_v2
- D8_v3, D8s_v3
- D16_v3, D16s_v3
- F4, F4s
- F8, F8s, F8s_v2
- F16, F16s, F16s_v2

Remarque MLX4 (Mellanox 4) est également appelé connectx3 = cx3 et MLX5 (Mellanox 5) est également appelé connectx4 = cx4.

Vous ne pouvez pas spécifier quelle carte réseau Azure utilise MLX4 ou MLX5 pour votre déploiement de VM. Cisco vous recommande d'effectuer une mise à niveau vers la version 9.15 d'ASA virtuel ou une version ultérieure pour utiliser la fonctionnalité de mise en réseau accélérée.

Déployer l'ASA virtuel

Vous pouvez déployer l'ASA virtuel sur Microsoft Azure.

- Déployez l'ASA virtuel en tant que pare-feu autonome à l'aide d'Azure Resouce Manager sur le nuage public Azure standard et les environnements Azure pour le gouvernement. Consultez Déployer l'ASAv à partir d'Azure Resource Manager.

- Déployez l'ASA virtuel en tant que solution partenaire intégrée dans Azure à l'aide d'Azure Security Center. Les clients sensibles à la sécurité se voient proposer l'option ASA virtuel comme pare-feu pour protéger les charges de travail Azure. Les événements de sécurité et d'intégrité sont supervisés à partir d'un seul tableau de bord intégré. Consultez Déployer l'ASAv à partir d'Azure Security Center.
- Déployez une paire ASA virtuel à haute accessibilité à l'aide d'Azure Resource Manager. Pour assurer la redondance, vous pouvez déployer l'ASA virtuel dans une configuration active/de secours à haute accessibilité (HA). La haute accessibilité dans le nuage public met en œuvre une solution active/de secours sans état qui permet, en cas de défaillance de l'ASA virtuel actif, de déclencher un basculement automatique du système vers l'ASA virtuel de secours. Consultez Déployer l'ASA virtuel pour la haute disponibilité à partir d'Azure Resource Manager, à la page 15.
- Déployez la paire ASA virtuel ou ASA virtuel à haute accessibilité avec un modèle personnalisé à l'aide d'une image gérée à partir d'un disque dur virtuel (disponible sur cisco.com). Cisco fournit un disque dur virtuel (VHD) compressé que vous pouvez charger vers Azure pour simplifier le processus de déploiement de l'ASA virtuel. 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 l'ASA virtuel en une seule opération coordonnée. Pour utiliser le modèle personnalisé, consultez Déployer l'ASA virtuel à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressources, à la page 16.

Déployer l'ASA virtuel à partir d'Azure Resource Manager

La procédure suivante est une liste de haut niveau des étapes à suivre pour configurer Microsoft Azure sur l'ASA virtuel. Pour connaître les étapes détaillées de la configuration d'Azure, consultez Mise en route d'Azure.

Lorsque vous déployez l'ASA virtuel dans Azure, il génère automatiquement diverses configurations, telles que les ressources, les adresses IP publiques et les tables de routage. Vous pourrez gérer ces configurations après le déploiement. Par exemple, vous pouvez modifier la valeur du délai d'inactivité à partir de la valeur par défaut, qui est un délai d'expiration faible.

Procédure

Étape 1 Connectez-vous au portail Azure 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 Recherchez Cisco ASAv dans Marché, puis cliquez sur l'ASA virtuel que vous souhaitez déployer.

Étape 3 Configurez les paramètres de base.

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

Important
Si votre nom n'est pas unique et que vous réutilisez un nom existant, le déploiement échouera.

b) Entrez votre nom d'utilisateur.

c) Choisissez un type d'authentification, **Password** (Mot de passe) ou **SSH public key** (Clé publique SSH).

Si vous choisissez **Password** (Mot de passe), saisissez un mot de passe et confirmez. Consultez la section Configuration du mot de passe pour connaître les consignes de complexité des mots de passe.

d) Choisissez votre type d'abonnement.

e) Choisissez un **Resource group** (Groupe de ressources).

Le groupe de ressources doit être le même que le groupe de ressources du réseau virtuel.

f) Choisissez votre emplacement.

L'emplacement doit être le même que pour votre réseau et votre groupe de ressources.

g) Cliquez sur **OK**.

Étape 4 Configurez les paramètres d'ASA virtuel.

a) Choisissez la taille de la machine virtuelle.

b) Choisissez un compte de stockage.

Vous pouvez utiliser un compte de stockage existant ou en créer un nouveau. L'emplacement du compte de stockage doit être le même que pour le réseau et la machine virtuelle.

c) Demandez une adresse IP publique en saisissant une étiquette pour l'adresse IP dans le champ Name (Nom), puis cliquez sur **OK**.

Azure crée une adresse IP publique dynamique par défaut, qui peut changer lorsque la machine virtuelle est arrêtée et redémarrée. Si vous préférez une adresse IP fixe, vous pouvez ouvrir l'adresse IP publique dans le portail et le faire passer d'une adresse dynamique à une adresse statique.

d) Ajoutez une étiquette DNS si vous le souhaitez.

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

e) Choisissez un réseau virtuel existant ou créez-en un nouveau.

f) Configurez les quatre sous-réseaux sur lesquels l'ASA virtuel sera déployé, puis cliquez sur **OK**.

Important
Chaque interface doit être associée à un sous-réseau unique.

g) Cliquez sur **OK**.

Étape 5 Affichez le résumé de la configuration, puis cliquez sur **OK**.

Étape 6 Affichez les conditions d'utilisation, puis cliquez sur **Create** (Créer).

Prochaine étape

- Poursuivez la configuration à l'aide des commandes de l'interface de ligne de commande disponibles pour une entrée par le biais du protocole SSH ou utilisez ASDM. Consultez la section Démarrer ASDM pour obtenir des instructions concernant l'accès à ASDM.

Déployer l'ASA virtuel à partir d'Azure Security Center

Microsoft Azure Security Center est une solution de sécurité pour Azure qui permet aux clients de protéger, de détecter et d'atténuer les risques de sécurité pour leurs déploiements dans le cloud. À partir du tableau de bord du centre de sécurité, les clients peuvent définir des politiques de sécurité, surveiller les configurations de sécurité et afficher les alertes de sécurité.

Le centre de sécurité analyse l'état de sécurité des ressources Azure pour identifier les failles de sécurité potentielles. Une liste de recommandations guide les clients dans le processus de configuration des contrôles

nécessaires, qui peut inclure le déploiement d'ASA virtuel en tant que solution de pare-feu pour les clients Azure.

En tant que solution intégrée dans le centre de sécurité, vous pouvez déployer rapidement l'ASA virtuel en quelques clics, puis surveiller les événements de sécurité et d'intégrité à partir d'un seul tableau de bord. La procédure suivante est une liste de niveaux supérieurs des étapes pour déployer l'ASA virtuel à partir du centre de sécurité. Pour des renseignements plus détaillés, consultez Azure Security Center.

Procédure

Étape 1 Connectez-vous au portail Azure.

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 Dans le menu Microsoft Azure, choisissez **Security Center** (Centre de sécurité).

Si vous accédez au centre de sécurité pour la première fois, la lame **Welcome** (Bienvenue) s'ouvre. Choisissez **Yes! I want to Launch Azure Security Center** (Oui! Je souhaite lancer Azure Security Center) pour ouvrir la lame **Security Center** (Centre de sécurité) et activer la collecte de données.

Étape 3 Dans la lame **Security Center** (Centre de sécurité), choisissez la vignette **Policy** (Politique).

Étape 4 Dans la lame **Security policy** (Politique de sécurité), choisissez **Prevention policy** (Politique de prévention).

Étape 5 Dans la lame **Prevention policy** (Politique de prévention), activez les recommandations que vous souhaitez voir dans le cadre de votre politique de sécurité.

a) Définissez **Next generation firewall** (Pare-feu de nouvelle génération) sur **On** (Activé). Cela garantit que l'ASA virtuel est une solution recommandée dans le centre de sécurité.
b) Définissez d'autres recommandations selon vos besoins.

Étape 6 Revenez à la lame **Security Center** (Centre de sécurité) et à la vignette **Recommendations** (Recommandations).

Le centre de sécurité analyse périodiquement l'état de sécurité de vos ressources Azure. Lorsque le centre de sécurité identifie des failles de sécurité potentielles, il affiche les recommandations sur la lame **Recommendations** (Recommandations).

Étape 7 Sélectionnez la recommandation **Add a Next Generation Firewall** (Ajouter un pare-feu de nouvelle génération) dans la lame **Recommendations** (Recommandations) pour afficher plus de renseignements et/ou prendre des mesures pour résoudre le problème.

Étape 8 Choisissez **Create New** (Créer nouvelle) ou **Use existing solution** (Utiliser une solution existante), puis cliquez sur l'ASA virtuel que vous souhaitez déployer.

Étape 9 Configurez les paramètres de base.

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

Important
Si votre nom n'est pas unique et que vous réutilisez un nom existant, le déploiement échouera.

b) Entrez votre nom d'utilisateur.
c) Choisissez un type d'autorisation, mot de passe ou clé SSH.

Si vous choisissez mot de passe, saisissez un mot de passe et confirmez. Consultez la section Configuration du mot de passe pour connaître les consignes de complexité des mots de passe.

d) Choisissez votre type d'abonnement.

e) Choisissez un groupe de ressources.

Le groupe de ressources doit être le même que le groupe de ressources du réseau virtuel.

f) Choisissez votre emplacement.

L'emplacement doit être le même que pour votre réseau et votre groupe de ressources.

g) Cliquez sur **OK**.

Étape 10 Configurez les paramètres d'ASA virtuel.

a) Choisissez la taille de la machine virtuelle.

L'ASA virtuel prend en charge Standard D3 et Standard D3_v2.

b) Choisissez un compte de stockage.

Vous pouvez utiliser un compte de stockage existant ou en créer un nouveau. L'emplacement du compte de stockage doit être le même que pour le réseau et la machine virtuelle.

c) Demandez une adresse IP publique en saisissant une étiquette pour l'adresse IP dans le champ Name (Nom), puis cliquez sur **OK**.

Azure crée une adresse IP publique dynamique par défaut, qui peut changer lorsque la machine virtuelle est arrêtée et redémarrée. Si vous préférez une adresse IP fixe, vous pouvez ouvrir l'adresse IP publique dans le portail et le faire passer d'une adresse dynamique à une adresse statique.

d) Ajoutez une étiquette DNS si vous le souhaitez.

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

e) Choisissez un réseau virtuel existant ou créez-en un nouveau.

f) Configurez les quatre sous-réseaux sur lesquels l'ASA virtuel sera déployé, puis cliquez sur **OK**.

Important
Chaque interface doit être associée à un sous-réseau unique.

g) Cliquez sur **OK**.

Étape 11 Affichez le résumé de la configuration, puis cliquez sur **OK**.

Étape 12 Affichez les conditions d'utilisation, puis cliquez sur **Create** (Créer).

Prochaine étape

- Poursuivez la configuration à l'aide des commandes de l'interface de ligne de commande disponibles pour une entrée par le biais du protocole SSH ou utilisez ASDM. Consultez la section Démarrer ASDM pour obtenir des instructions concernant l'accès à ASDM.
- Si vous avez besoin d'en savoir plus sur la façon dont les recommandations du centre de sécurité vous aident à protéger vos ressources Azure, consultez la documentation disponible dans le centre de sécurité.

Déployer l'ASA virtuel pour la haute disponibilité à partir d'Azure Resource Manager

La procédure suivante est une liste de niveaux supérieurs des étapes pour configurer une paire ASA virtuel à haute accessibilité sur Microsoft Azure. Pour connaître les étapes détaillées de la configuration d'Azure, consultez Mise en route d'Azure.

L'ASA virtuel à haute disponibilité dans Azure déploie deux ASA virtuel dans un ensemble de disponibilité et génère automatiquement diverses configurations, telles que les ressources, les adresses IP publiques et les tables de routage. Vous pourrez gérer ces configurations après le déploiement.

Procédure

Étape 1 Connectez-vous au portail Azure.

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 Effectuez une recherche sur le Marché pour **Cisco ASAv**, puis cliquez sur **ASAv 4 NIC HA** (4 cartes réseau ASAv à haute disponibilité) pour déployer une configuration ASA virtuel de basculement.

Étape 3 Configurez les paramètres **Basics** (Base).

a) Saisissez un préfixe pour les noms de machine ASA virtuel. Les noms ASA virtuel auront le « préfixe »-A et le « préfixe »-B.

Important
Assurez-vous de ne pas utiliser un préfixe existant, sinon le déploiement échouera.

b) Saisissez un **nom d'utilisateur**.

Il s'agira du nom d'utilisateur administratif des deux machines virtuelles.

Important
L'**admin** du nom d'utilisateur n'est pas autorisé dans Azure.

c) Choisissez un type d'authentification pour les deux machines virtuelles, **Password** (Mot de passe) ou **SSH public key** (Clé publique SSH).

Si vous choisissez **Password** (Mot de passe), saisissez un mot de passe et confirmez. Consultez la section Configuration du mot de passe pour connaître les consignes de complexité des mots de passe.

d) Choisissez votre type d'abonnement.

e) Choisissez un **Resource group** (Groupe de ressources).

Choisissez **Create new (Créer nouveau)** pour créer un nouveau groupe de ressources, ou **Use exist** (Utiliser un groupe existant) pour sélectionner un groupe de ressources existant. Si vous utilisez un groupe de ressources existant, il doit être vide. Sinon, vous devez créer un nouveau groupe de ressources.

f) Choisissez votre **Location** (Emplacement).

L'emplacement doit être le même que pour votre réseau et votre groupe de ressources.

g) Cliquez sur **OK**.

Étape 4 Configurez les **Cisco ASAv settings** (Paramètres Cisco ASAv).

a) Choisissez la taille de la machine virtuelle.
b) Choisissez **Managed** (Géré) ou **Unmanaged OS disk** (Disque du système d'exploitation non géré) pour le stockage.

Important
Le mode haute disponibilité de l'ASA utilise toujours **Managed** (Géré).

Étape 5 Configurez les paramètres de l'**ASAv-A**.

a) (Facultatif) Choisissez **Create New** (Créer nouvelle) pour demander une adresse IP publique en saisissant une étiquette pour l'adresse IP dans le champ Name (Nom), puis cliquez sur **OK**. Choisissez **None** (Aucune) si vous ne souhaitez pas d'adresse IP publique.

Remarque
Azure crée une adresse IP publique dynamique par défaut, qui peut changer lorsque la machine virtuelle est arrêtée et redémarrée. Si vous préférez une adresse IP fixe, vous pouvez ouvrir l'adresse IP publique dans le portail et le faire passer d'une adresse dynamique à une adresse statique.

b) Ajoutez une étiquette DNS si vous le souhaitez.

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

c) Configurez les paramètres requis pour le compte de stockage pour les diagnostics de démarrage ASAv-A.

Étape 6 Répétez les étapes précédentes pour les paramètres **ASAv-B**.

Étape 7 Choisissez un réseau virtuel existant ou créez-en un nouveau.

a) Configurez les quatre sous-réseaux sur lesquels l'ASA virtuel sera déployé, puis cliquez sur **OK**.

Important
Chaque interface doit être associée à un sous-réseau unique.

b) Cliquez sur **OK**.

Étape 8 Affichez la configuration **Summary** (Résumé), puis cliquez sur **OK**.

Étape 9 Affichez les conditions d'utilisation, puis cliquez sur **Create** (Créer).

Prochaine étape

- Poursuivez la configuration à l'aide des commandes de l'interface de ligne de commande disponibles pour une entrée par le biais du protocole SSH ou utilisez ASDM. Consultez la section Démarrer ASDM pour obtenir des instructions concernant l'accès à ASDM.
- Consultez le chapitre « Basculement pour la haute disponibilité dans le nuage public » du Guide de configuration des opérations générales de la série ASA pour en savoir plus sur la configuration de l'ASA virtuel à haute disponibilité dans Azure.

Déployer l'ASA virtuel à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressources

Vous pouvez créer vos propres images ASA virtuel personnalisées en utilisant une image de disque dur virtuel 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 ASA virtuel. Vous pouvez télécharger des fichiers de modèles à partir du référentiel GitHub à l'adresse :

  https://github.com/CiscoDevNet/cisco-asav/tree/master/deployment-templates/azure

- Pour des instructions sur la création d'un modèle et d'un fichier de paramètres, consultez Annexe : Exemple de modèle de ressource Azure, à la page 20.
- 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 dans le portail Azure

- Dans votre abonnement Azure, vous devez avoir un compte de stockage disponible à l'emplacement dans lequel vous souhaitez déployer l'ASA virtuel.

Procédure

Étape 1 Téléchargez l'image de disque dur virtuel compressée ASA virtuel à partir de la page https://software.cisco.com/download/home :

a) Accédez à **Products (produits)** > **Security (sécurité)** > **Firewalls (pare-feu)** > **Adaptive Security Appliances (ASA) (appareils de sécurité adaptables (ASA))** > **Adaptive Securtiy Appliance (ASA) Software (logiciel d'appareil de sécurité adaptable (ASA))**.

b) Cliquez sur **Adaptive Security Virtual Appliance (ASAv)** (appareil virtuel de sécurité adaptable (ASAv)).

Suivez les instructions pour télécharger l'image.

Par exemple, asav9-14-1.vhd.bz2

Étape 2 Copiez l'image de disque dur virtuel compressée sur votre machine virtuelle Linux dans Azure.

Il existe de nombreuses options que vous pouvez utiliser pour déplacer des fichiers vers Azure et à partir d'Azure. Cet exemple montre SCP ou copie sécurisée :

```
# scp /username@remotehost.com/dir/asav9-14-1.vhd.bz2 <linux-ip>
```

Étape 3 Connectez-vous à la machine virtuelle Linux dans Azure et accédez au répertoire où vous avez copié l'image de disque dur virtuel compressée.

Étape 4 Décompressez l'image de disque dur virtuel d'ASA virtuel.

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

```
# bunzip2 asav9-14-1.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 charger un disque virtuel sur votre compte de stockage, notamment AzCopy, l'API pour le stockage d'objets blob Azure, l'explorateur de stockage Azure, 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 l'ASA virtuel.

L'exemple suivant montre la syntaxe en utilisant l'interface de ligne de commande Azure :

```
azure storage blob upload \
       --file <unzipped vhd> \
       --account-name <azure storage account> \
       --account-key yX7txxxxxxxx1dnQ== \
       --container <container> \
       --blob <desired vhd name in azure> \
       --blobtype page
```

Étape 6 Créez une image gérée à partir du disque dur virtuel :

a) Dans le portail Azure, sélectionnez **Images**.
b) Cliquez sur **Add** (ajouter) pour créer une nouvelle image.
c) Fournir les renseignements suivants :

- **Subscription** (abonnement) : choisissez un abonnement dans la liste déroulante.
- **Resource group**(groupe de ressources) : choisissez un groupe de ressources existant ou créez-en.
- **Name** (nom) : saisissez un nom défini par l'utilisateur pour l'image gérée.
- **Region** (région) : choisissez la région dans laquelle la machine virtuelle est déployée.
- **OS type** (type de système d'exploitation) : choisissez **Linux** comme type de système d'exploitation.
- **VM genreation** (génération de la machine virtuelle) : choisissez **Gen 1**.

  Remarque
  Gen 2 n'est pas prise en charge.

- **Srorage blob** (objet biniare de stockage) : accédez au compte de stockage pour sélectionner le disque dur virtuel chargé.
- **Account type** (type de compte) : selon vos besoins, choisissez Standard HDD, Standard SSD ou Premium SSD dans la liste déroulante.

  Lorsque vous sélectionnez la taille de machine virtuelle planifiée pour le déploiement de cette image, assurez-vous que la taille de machine virtuelle prend en charge le type de compte sélectionné.
- **Host caching** (mise en mémoire cache de l'hôte) : choisissez Read/write (lecture/écriture) dans la liste déroulante.
- **Data disks**(disques de données) : laissez à la valeur par défaut; n'ajoutez pas de disque de données.

d) Cliquez sur **Create** (créer).

Attendez que le message **Successfully create image** (création d'image réussie) apparaisse sous l'onglet **Notifications**.

Remarque
Une fois que l'image gérée est créée, le disque dur virtuel chargé et le compte de stockage de charge peuvent être supprimés.

Étape 7 Obtenez l'ID de ressource de la nouvelle image gérée.

En interne, Azure associe chaque ressource à un ID de ressource. Vous aurez besoin de l'ID de ressource lorsque vous déployez de nouveaux pare-feu ASA virtuel à partir de cette image gérée.

a) Dans le portail Azure, sélectionnez **Images**.
b) Sélectionnez l'image gérée créée à l'étape précédente.
c) Cliquez sur **Overview** (aperçu) pour afficher les propriétés de l'image.
d) Copier l'**ID de ressource** dans le presse-papiers.

L'**ID de ressource** prend la forme de :

/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>
/providers/Microsoft.Compute/<container>/ <vhdname>

Étape 8 Créez un pare-feu ASA virtuel 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 Créer un modèle de ressources, à la page 21 pour un exemple de création d'un modèle

d) Collez votre code de modèle JSON personnalisé dans la fenêtre, puis cliquez sur **Save** (enregistrer).
e) Choisissez un **Subscription** (abonnement) dans la liste déroulante.
f) Choisissez un **Resource group** (groupe de ressources) existant ou créez-en un nouveau.
g) Choisissez un **Location** (emplacement) dans la liste déroulante.
h) Collez l'**ID de ressource** d'image gérée de l'étape précédente dans le champ **Vm Managed Image ID** (ID de l'image gérée de machine virtuelle).

Étape 9 Cliquez sur **Edit Parameters** (modifier les paramètres) en haut de la page **Custom Deployment** (déploiement personnalisé). Un modèle de paramètres est disponible pour la personnalisation.

a) Cliquez sur **Load file** (charger le fichier) et accédez au fichier de paramètres ASA virtuel personnalisé. Consultez Créer un fichier de paramètres, à la page 30 pour un exemple de création d'un modèle de paramètres.
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 un pare-feu ASA virtuel 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

- Poursuivez la configuration à l'aide des commandes CLI disponibles pour une entrée par le biais du protocole SSH ou utilisez ASDM. Consultez Démarrer ASDM, page 87 pour obtenir des instructions concernant l'accès à ASDM.

Annexe : Exemple de modèle de ressource Azure

Cette section décrit la structure d'un modèle Azure Resource Manager que vous pouvez utiliser pour déployer l'ASA virtuel. Un modèle de ressource Azure est un fichier JSON. Pour simplifier le déploiement de toutes les ressources requises, cet exemple comprend deux fichiers JSON :

- **Fichier de modèle** : il s'agit du principal fichier de ressources qui déploie tous les composants du groupe de ressources.
- **Fichier de paramètres** : ce fichier comprend les paramètres requis pour déployer avec succès l'ASA virtuel. Il comprend des détails tels que les informations sur le sous-réseau, le niveau et la taille de la machine virtuelle, le nom d'utilisateur et le mot de passe pour l'ASA virtuel, le nom du conteneur de stockage, etc. Vous pouvez personnaliser ce fichier pour votre environnement de déploiement Azure Stack Hub.

Format du fichier du modèle

Cette section décrit la structure d'un fichier de modèle Azure Resource Manager. L'exemple suivant montre une vue réduite d'un fichier de modèle et présente les différentes sections d'un modèle.

Fichier de modèle JSON d'Azure Resource Manager

```
{
    "$schema":
"http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "",
    "parameters": { },
    "variables": { },
    "resources": [ ],
    "outputs": { }
}
```

Le modèle est composé de JSON et d'expressions que vous pouvez utiliser pour construire des valeurs pour votre déploiement ASA virtuel. Dans sa structure la plus simple, un modèle contient les éléments suivants :

Tableau 3 : Éléments définis du fichier de modèle JSON d'Azure Resource Manager

Élément	Obligatoire	Description
$schema	Oui	Emplacement du fichier de schéma JSON qui décrit la version de la langue du modèle. Utilisez l'URL indiquée dans le schéma précédent.

Élément	Obligatoire	Description
contentVersion	Oui	Version du modèle (comme 1.0.0.0). Vous pouvez fournir n'importe quelle valeur pour cet élément. Lors du déploiement de ressources à l'aide du modèle, cette valeur peut être utilisée pour s'assurer que le bon modèle est utilisé.
paramètres	Non	Valeurs fournies lors du déploiement pour personnaliser le déploiement des ressources. Les paramètres permettent de saisir des valeurs au moment du déploiement. Ils ne sont pas obligatoires, mais sans eux, le modèle JSON déploiera les ressources avec les mêmes paramètres à chaque fois.
variables	Non	Valeurs utilisées comme fragments JSON dans le modèle pour simplifier les expressions linguistiques du modèle.
Ressources	Oui	Types de ressources déployées ou mises à jour dans un groupe de ressources.
sorties	Non	Valeurs retournées après le déploiement.

Vous pouvez utiliser les modèles JSON pour non seulement déclarer les types de ressources à déployer, mais également leurs paramètres de configuration associés. L'exemple suivant montre un modèle qui déploie un nouveau ASA virtuel.

Créer un modèle de ressources

Vous pouvez utiliser l'exemple ci-dessous pour créer votre propre modèle de déploiement à l'aide d'un éditeur de texte.

Procédure

Étape 1 Copiez le texte dans l'exemple suivant.

Exemple :

```
{
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "type": "string",
            "defaultValue": "ngfw",
            "metadata": {
                "description": "Name of the NGFW VM"
            }
        },
        "vmManagedImageId": {
            "type": "string",
            "defaultValue":
"/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage",

            "metadata": {
                "description": "The ID of the managed image used for deployment.
```

```
/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage"

            }
        },
        "adminUsername": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Username for the Virtual Machine. admin, Administrator among other
 values are disallowed - see Azure docs"
            }
        },
        "adminPassword": {
            "type": "securestring",
            "defaultValue" : "",
            "metadata": {
                "description": "Password for the Virtual Machine. Passwords must be 12 to 72 chars
 and have at least 3 of the following: Lowercase, uppercase, numbers, special chars"
            }
        },
        "vmStorageAccount": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "A storage account name (boot diags require a storage account).
Between 3 and 24 characters. Lowercase letters and numbers only"
            }
        },
        "virtualNetworkResourceGroup": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Name of the virtual network's Resource Group"
            }
        },
        "virtualNetworkName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Name of the virtual network"
            }
        },
        "mgmtSubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv management interface will attach to this subnet"
            }
        },
        "mgmtSubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "NGFW IP on the mgmt interface (example: 192.168.0.10)"
            }
        },
        "diagSubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv diagnostic0/0 interface will attach to this subnet"
            }
        },
        "diagSubnetIP": {
```

```
                "type": "string",
                "defaultValue": "",
                "metadata": {
                    "description": "NGFW IP on the diag interface (example: 192.168.1.10)"
                }
            },
            "gig00SubnetName": {
                "type": "string",
                "defaultValue": "",
                "metadata": {
                    "description": "The FTDv Gigabit 0/0 interface will attach to this subnet"
                }
            },
            "gig00SubnetIP": {
                "type": "string",
                "defaultValue": "",
                "metadata": {
                    "description": "The IP on the Gigabit 0/0 interface (example: 192.168.2.10)"
                }
            },
            "gig01SubnetName": {
                "type": "string",
                "defaultValue": "",
                "metadata": {
                    "description": "The FTDv Gigabit 0/1 interface will attach to this subnet"
                }
            },
            "gig01SubnetIP": {
                "type": "string",
                "defaultValue": "",
                "metadata": {
                    "description": "The IP on the Gigabit 0/1 interface (example: 192.168.3.5)"
                }
            },
            "VmSize": {
                "type": "string",
                "defaultValue": "Standard_D3_v2",
                "allowedValues": [ "Standard_D3_v2" , "Standard_D3" ],
                "metadata": {
                    "description": "NGFW VM Size (Standard_D3_v2 or Standard_D3)"
                }
            }
        },
        "variables": {

            "virtualNetworkID":
"[resourceId(parameters('virtualNetworkResourceGroup'),'Microsoft.Network/virtualNetworks',
parameters('virtualNetworkName'))]",

            "vmNic0Name":"[concat(parameters('vmName'),'-nic0')]",
            "vmNic1Name":"[concat(parameters('vmName'),'-nic1')]",
            "vmNic2Name":"[concat(parameters('vmName'),'-nic2')]",
            "vmNic3Name":"[concat(parameters('vmName'),'-nic3')]",

            "vmNic0NsgName":"[concat(variables('vmNic0Name'),'-NSG')]",

            "vmMgmtPublicIPAddressName": "[concat(parameters('vmName'),'nic0-ip')]",
            "vmMgmtPublicIPAddressType": "Static",
            "vmMgmtPublicIPAddressDnsName": "[variables('vmMgmtPublicIPAddressName')]"
        },
        "resources": [
            {
                "apiVersion": "2017-03-01",
                "type": "Microsoft.Network/publicIPAddresses",
```

```
            "name": "[variables('vmMgmtPublicIPAddressName')]",
            "location": "[resourceGroup().location]",
            "properties": {
              "publicIPAllocationMethod": "[variables('vmMgmtPublicIpAddressType')]",
              "dnsSettings": {
                "domainNameLabel": "[variables('vmMgmtPublicIPAddressDnsName')]"
              }
            }
        },
        {
            "apiVersion": "2015-06-15",
            "type": "Microsoft.Network/networkSecurityGroups",
            "name": "[variables('vmNic0NsgName')]",
            "location": "[resourceGroup().location]",
            "properties": {
                "securityRules": [
                    {
                        "name": "SSH-Rule",
                        "properties": {
                            "description": "Allow SSH",
                            "protocol": "Tcp",
                            "sourcePortRange": "*",
                            "destinationPortRange": "22",
                            "sourceAddressPrefix": "Internet",
                            "destinationAddressPrefix": "*",
                            "access": "Allow",
                            "priority": 100,
                            "direction": "Inbound"
                        }
                    },
                    {
                        "name": "SFtunnel-Rule",
                        "properties": {
                            "description": "Allow tcp 8305",
                            "protocol": "Tcp",
                            "sourcePortRange": "*",
                            "destinationPortRange": "8305",
                            "sourceAddressPrefix": "Internet",
                            "destinationAddressPrefix": "*",
                            "access": "Allow",
                            "priority": 101,
                            "direction": "Inbound"
                        }
                    }
                ]
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic0Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
                "[concat('Microsoft.Network/networkSecurityGroups/',variables('vmNic0NsgName'))]",

                "[concat('Microsoft.Network/publicIPAddresses/',
variables('vmMgmtPublicIPAddressName'))]"
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
```

```
                            "privateIPAddress" : "[parameters('mgmtSubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('mgmtSubnetName'))]"
                            },
                            "publicIPAddress":{
                                "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('vmMgmtPublicIPAddressName'))]"
                            }
                        }
                    }
                ],
                "networkSecurityGroup": {
                    "id": "[resourceId('Microsoft.Network/networkSecurityGroups',
variables('vmNic0NsgName'))]"
                },
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic1Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('diagSubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('diagSubnetName'))]"
                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic2Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('gig00SubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('gig00SubnetName'))]"
                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
```

```
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic3Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('gig01SubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('gig01SubnetName'))]"

                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "type": "Microsoft.Storage/storageAccounts",
            "name": "[concat(parameters('vmStorageAccount'))]",
            "apiVersion": "2015-06-15",
            "location": "[resourceGroup().location]",
            "properties": {
              "accountType": "Standard_LRS"
            }
        },
        {
            "apiVersion": "2017-12-01",
            "type": "Microsoft.Compute/virtualMachines",
            "name": "[parameters('vmName')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
                "[concat('Microsoft.Storage/storageAccounts/', parameters('vmStorageAccount'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic0Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic1Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic2Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic3Name'))]"
            ],
            "properties": {
                "hardwareProfile": {
                    "vmSize": "[parameters('vmSize')]"
                },
                "osProfile": {
                    "computername": "[parameters('vmName')]",
                    "adminUsername": "[parameters('AdminUsername')]",
                    "adminPassword": "[parameters('AdminPassword')]"
                },
                "storageProfile": {
                    "imageReference": {
                        "id": "[parameters('vmManagedImageId')]"
                    },
                    "osDisk": {
                        "osType": "Linux",
                        "caching": "ReadWrite",
                        "createOption": "FromImage"
                    }
```

```
                },
                "networkProfile": {
                    "networkInterfaces": [
                        {
                            "properties": {
                                "primary": true
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic0Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic1Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic2Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic3Name'))]"
                        }
                    ]
                },
                "diagnosticsProfile": {
                    "bootDiagnostics": {
                        "enabled": true,
                        "storageUri":
"[concat('http://',parameters('vmStorageAccount'),'.blob.core.windows.net')]"
                    }
                }
            }
        }
    ],
    "outputs": {  }
}
```

Étape 2 Enregistrez le fichier localement en tant que fichier JSON; par exemple, **azureDeploy.json**.

Étape 3 Modifiez le fichier pour créer un modèle correspondant à vos paramètres de déploiement.

Étape 4 Utilisez ce modèle pour déployer l'ASA virtuel comme décrit dans Déployer l'ASA virtuel à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressources, à la page 16.

Format du fichier des paramètres

Lorsque vous démarrez un nouveau déploiement, des paramètres sont définis dans votre modèle de ressources. Ces derniers doivent être saisis avant que le déploiement puisse commencer. Vous pouvez saisir manuellement les paramètres que vous avez définis dans votre modèle de ressources, ou vous pouvez placer les paramètres dans un fichier JSON de paramètres de modèle.

Le fichier de paramètres contient une valeur pour chaque paramètre affiché dans l'exemple des paramètres dans Créer un fichier de paramètres, à la page 30. Ces valeurs sont automatiquement transmises au modèle lors du déploiement. Vous pouvez créer plusieurs fichiers de paramètres pour différents scénarios de déploiement.

Pour le modèle ASA virtuel de cet exemple, le fichier de paramètres doit comporter les paramètres définis suivants :

Tableau 4 : Définitions des paramètresASA virtuel

Champ	Description	Exemple
vmName	Le nom que la machine ASA virtuel aura dans Azure.	cisco-asav
vmManagedImageId	ID de l'image gérée utilisée pour le déploiement. En interne, Azure associe chaque ressource à un ID de ressource.	/subscriptions/73d2537e-ca44-46aa-beb2-74ff1dd61b41/ resourceGroups/ew ManagedImages-rg/providers/Microsoft .Compute/ images/ASAv910-Managed-I mage
adminUsername	Le nom d'utilisateur pour la connexion à l'ASA virtuel. Il ne peut pas s'agir du nom réservé « admin ».	jdoe
adminPassword	Le mot de passe de l'administrateur. Il doit comporter de 12 à 72 caractères et inclure trois des éléments suivants : 1 minuscule, 1 majuscule, 1 chiffre, 1 caractère spécial.	Pw0987654321
vmStorageAccount	Votre compte de stockage Azure. Vous pouvez utiliser un compte de stockage existant ou en créer un nouveau. Le nom du compte de stockage doit comporter de 3 à 24 caractères et ne peut contenir que des lettres minuscules et des chiffres.	ciscoasavstorage
virtualNetworkResourceGroup	Le nom du groupe de ressources du réseau virtuel. L'ASA virtuel est toujours déployé dans un nouveau groupe de ressources.	ew-west8-rg
virtualNetworkName	Le nom du réseau virtuel.	ew-west8-vnet

Champ	Description	Exemple
mgmtSubnetName	L'interface de gestion sera associée à ce sous-réseau. Cela mappe à Nic0, le premier sous-réseau. Veuillez noter que cela doit correspondre à un nom de sous-réseau existant si vous rejoignez un réseau existant.	mgmt
mgmtSubnetIP	L'adresse IP de l'interface de gestion	10.8.0.55
gig00SubnetName	L'interface GigabitEthernet 0/0 se connectera à ce sous-réseau. Cela mappe à Nic1, le deuxième sous-réseau. Veuillez noter que cela doit correspondre à un nom de sous-réseau existant si vous rejoignez un réseau existant.	interne
gig00SubnetIP	L'adresse IP de l'interface GigabitEthernet 0/0. Il s'agit de la première interface de données de l'ASA virtuel.	10.8.2.55
gig01SubnetName	L'interface GigabitEthernet 0/1 s'associera à ce sous-réseau. Cela mappe à Nic2, le troisième sous-réseau. Veuillez noter que cela doit correspondre à un nom de sous-réseau existant si vous rejoignez un réseau existant.	externe
gig01SubnetIP	L'adresse IP de l'interface GigabitEthernet 0/1. Il s'agit de la deuxième interface de données d'ASA virtuel.	10.8.3.55
gig02SubnetName	L'interface GigabitEthernet 0/2 sera associée à ce sous-réseau. Cela mappe à Nic3, le quatrième sous-réseau. Veuillez noter que cela doit correspondre à un nom de sous-réseau existant si vous rejoignez un réseau existant.	dmz
gig02SubnetIP	L'adresse IP de l'interface GigabitEthernet 0/2. Il s'agit de la troisième interface de données d'ASA virtuel.	10.8.4.55

Champ	Description	Exemple
vmSize	La taille de machine virtuelle à utiliser pour la machine virtuelle ASA virtuel. Standard_D3_V2 et Standard_D3 sont prises en charge. Standard_D3_V2 est la valeur par défaut.	Standard_D3_V2 ou Standard_D3

Créer un fichier de paramètres

Vous pouvez utiliser l'exemple ci-dessous pour créer votre propre fichier de paramètres à l'aide d'un éditeur de texte.

Remarque L'exemple suivant concerne uniquement IPV4.

Procédure

Étape 1 Copiez le texte dans l'exemple suivant.

Exemple :

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "vmName": {
      "value": "cisco-asav1"
    },
    "vmManagedImageId": {
      "value":
"/subscriptions/33d2517e-ca88-46aa-beb2-74ffldb61b41/resourceGroups/ewManagedImages-rg/providers/Microsoft.Compute/images/ASAv-9.10.1-81-Managed-Image"

    },
    "adminUsername": {
      "value": "jdoe"
    },
    "adminPassword": {
      "value": "Pw0987654321"
    },
    "vmStorageAccount": {
      "value": "ciscoasavstorage"
    },
    "virtualNetworkResourceGroup": {
      "value": "ew-west8-rg"
    },
    "virtualNetworkName": {
      "value": "ew-west8-vn"
    },
    "mgmtSubnetName": {
      "value": "mgmt"
    },
```

```
    "mgmtSubnetIP": {
      "value": "10.8.3.77"
    },
    "gig00SubnetName": {
      "value": "inside"
    },
    "gig00SubnetIP": {
      "value": "10.8.2.77"
    },
    "gig01SubnetName": {
      "value": "outside"
    },
    "gig01SubnetIP": {
      "value": "10.8.1.77"
    },
    "gig02SubnetName": {
      "value": "dmz"
    },
    "gig02SubnetIP": {
      "value": "10.8.0.77"
    },
    "VmSize": {
      "value": "Standard_D3_v2"
    }
  }
}
```

Étape 2 Enregistrez le fichier localement en tant que fichier JSON; par exemple, **azureParameters.json**.

Étape 3 Modifiez le fichier pour créer un modèle correspondant à vos paramètres de déploiement.

Étape 4 Utilisez ce modèle de paramètre pour déployer l'ASA virtuel comme décrit dans Déployer l'ASA virtuel à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressources, à la page 16.

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.