Déployer l'ASA virtuel sur AWS en nuage

Vous pouvez déployer l'ASA virtuel sur le nuage Amazon Web Services (AWS).

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 AWS prises en charge.

- Aperçu, à la page 1
- Prérequis, à la page 4
- Lignes directrices et limites relatives à la licence, à la page 4
- Migration de la configuration et authentification SSH, à la page 5
- Exemple de topologie de réseau, à la page 6
- Déploiement ASA virtuel, à la page 7
- Intégration du service Amazon GuardDuty et Défense contre les menaces virtuelles, à la page 10
- À propos de l'intégration d'Cisco Secure Firewall ASA virtuel et GuardDuty, à la page 10
- Plateformes logicielles prises en charge, à la page 13
- Lignes directrices et limites pour l'intégration d'Amazon GuardDuty et de Cisco Secure Firewall ASA Virtual, à la page 13
- Intégrer Amazon GuardDuty avec ASA virtuel, à la page 14
- Mettre à jour la configuration de déploiement de solution existante, à la page 26
- Réglage de la performance, à la page 27

Aperçu

L'ASA virtuel exécute le même logiciel que les ASA physiques pour fournir des fonctionnalités de sécurité éprouvées dans un format virtuel. L'ASA virtuel peut être déployé dans le nuage AWS public. Il peut ensuite être configuré pour protéger les charges de travail des centres de données virtuels et physiques qui se développent, se contractent ou changent d'emplacement au fil du temps.

L'ASA virtuel prend en charge les types d'instances AWS suivants.

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

Instance	Attributs		Nombre maximal d'interfaces
	vCPU	Mémoire (Go)	
c3.large	2	3,75	3
c3.xlarge	4	7,5	4
c3.2xlarge	8	15	4
c4.large	2	3,75	3
c4.xlarge	4	7,5	4
c4.2xlarge	8	15	4
c5.large	2	4	3
c5.xlarge	4	8	4
c5.2xlarge	8	16	4
c5.4xlarge	16	32	8
c5a.large	2	4	3
c5a.xlarge	4	8	4
c5a.2xlarge	8	16	4
c5a.4xlarge	16	32	8
c5ad.large	2	4	3
c5ad.xlarge	4	8	4
c5ad.2xlarge	8	16	4
c5ad.4xlarge	16	32	8
c5d.large	2	4	3
c5d.xlarge	4	8	4
c5d.2xlarge	8	16	4
c5d.4xlarge	16	32	8
c5n.large	2	5,3	3
c5n.xlarge	4	10,5	4
c5n.2xlarge	8	21	4
c5n.4xlarge	16	42	8

Instance	Attributs		Nombre maximal d'interfaces
	vCPU	Mémoire (Go)	
m4.large	2	8	2
m4.xlarge	4	16	4
m4.2xlarge	8	32	4
m5n.large	2	8	3
m5n.xlarge	4	16	4
m5n.2xlarge	8	32	4
m5n.4xlarge	16	64	8
m5zn.large	2	8	3
m5zn.xlarge	4	16	4
m5zn.2xlarge	8	32	4

Astuces Si vous utilisez le type d'instance M4 ou C4, nous vous recommandons de migrer vers le type d'instance M5 ou C5 qui utilise des pilotes d'interface pour l'hyperviseur Nitro et Elastic Network Adapter (ENA) pour améliorer les performances.

Astuces Si vous utilisez le type d'instance C4, nous vous recommandons de migrer vers le type d'instance C5 qui utilise l'hyperviseur Nitro et les pilotes d'interface Elastic Network Adapter (ENA) pour améliorer les performances.

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	c5.large 2 cœurs/4 Go	100 Mbit/sec	50
ASAv10	c5.large 2 cœurs/4 Go	1 Gbit/sec	250
ASAv30	c5.xlarge 4 cœurs/8 Go	2 Gbit/s	750
ASAv50	c5.2xlarge 8 cœurs/16 Go	10 Gbit/s	10 000

Niveau de performance	Type d'instance (cœur/RAM)	Limite du débit	Limite de session RA VPN
ASAv100	c5n.4xlarge 16 cœurs/42 Go	16 Gbit/s	20 000

Vous créez un compte sur AWS, configurez l'ASA virtuel à l'aide de l'assistant AWS et avez choisi une image de machine Amazon (AMI). L'AMI est un modèle qui contient la configuration logicielle nécessaire pour lancer votre instance.

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

Prérequis

- Créez un compte sur aws.amazon.com.
- 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 Gestion des licences pour l'ASA virtuel.
- Exigences d'interface :
  - Interface de gestion
  - Interfaces interne et externe
  - (Facultatif) Sous-réseau supplémentaire (DMZ)
- Chemins de communication :
  - Interface de gestion : utilisée pour connecter l'ASA virtuel à ASDM; ne peut pas être utilisée pour le trafic traversant.
  - 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 c3.xlarge.
- Pour les exigences du système ASA virtuel, consultez Compatibilité Cisco Cisco Secure Firewall ASA.

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

L'ASA virtuel sur AWS prend en charge les fonctionnalités suivantes :

- Prise en charge des instances Amazon EC2 C5, la prochaine génération de la famille d'instances de Calcul optimisé Amazon EC2.
- Déploiement dans le Cloud privé virtuel (VPC)
- Mise en réseau améliorée (SR-IOV), si disponible
- Déploiement à partir du Marché Amazon
- Déploiement des utilisateurs des réseaux L3
- Mode avec routeur (par défaut)
- Amazon CloudWatch

Fonctionnalités non prises en charge

L'ASA virtuel sur AWS ne prend pas en charge les éléments suivants :

- Accès à la console (la gestion est effectuée à l'aide de SSH ou ASDM sur les interfaces réseau)
- VLAN
- Mode promiscuité (pas de prise en charge de pare-feu en mode sniffer (analyseur de réseau) ou transparent)
- Mode contexte multiple
- Mise en grappes
- Haute disponibilité en natif ASA virtuel
- EtherChannel n'est pris en charge que sur les interfaces physiques directes
- Importation/exportation de machine virtuelle
- Package indépendant de l'hyperviseur
- VMware ESXi
- Messages de diffusion ou de multidiffusion

  Ces messages ne sont pas propagés dans AWS, de sorte que les protocoles de routage qui nécessitent la diffusion et la multidiffusion ne fonctionnent pas comme prévu dans AWS. VXLAN ne peut fonctionner qu'avec des homologues statiques.
- ARP Gratuitous et non sollicités

  Ces ARP ne sont pas acceptés dans AWS. Les configurations NAT qui nécessitent des ARP Gratuitous ou non sollicités ne fonctionnent pas comme prévu.
- IPv6

Migration de la configuration et authentification SSH

Incidence sur la mise à niveau lors de l'utilisation de l'authentification par clé publique SSH : en raison des mises à jour de l'authentification SSH, une configuration supplémentaire est requise pour activer l'authentification par clé publique SSH; par conséquent, les configurations SSH existantes utilisant

l'authentification par clé publique ne fonctionnent plus après la mise à niveau. L'authentification par clé publique est la valeur par défaut pour l'ASA virtuel sur Amazon Web Services (AWS), donc les utilisateurs AWS verront ce problème. Pour éviter la perte de connectivité SSH, vous pouvez mettre à jour votre configuration avant d'effectuer la mise à niveau. Vous pouvez également utiliser ASDM après la mise à niveau (si vous avez activé l'accès ASDM) pour corriger la configuration.

Voici un exemple de configuration d'origine pour un nom d'utilisateur « admin » :

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
  07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

Pour utiliser la commande **ssh authentication**, avant d'effectuer la mise à niveau, saisissez les commandes suivantes :

```
aaa authentication ssh console LOCAL
username admin password <password> privilege 15
```

Nous vous recommandons de définir un mot de passe pour le nom d'utilisateur plutôt que de conserver le mot clé **nopassword**, s'il est présent. Le mot clé **nopassword** signifie que tout mot de passe peut être saisi, et non qu'aucun mot de passe ne peut être saisi. Dans les versions antérieures à la version 9.6(2), la commande **aaa** n'était pas requise pour l'authentification par clé publique SSH, le mot clé **nopassword** n'était donc pas déclenché. Maintenant que la commande **aaa** est requise, elle permet également l'authentification par mot de passe normale pour un mot clé **username** si le mot clé **password** (ou **nopassword**) est présent.

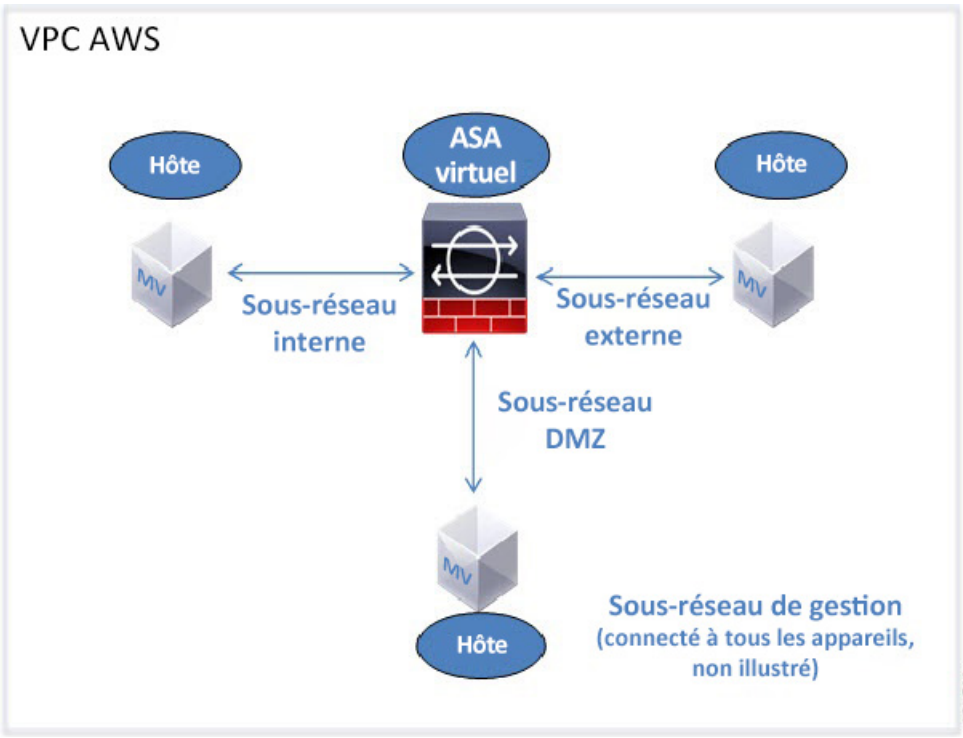
Après la mise à niveau, la commande **username** ne nécessite plus le mot clé **password** ou **nopassword**. Vous pouvez exiger qu'un utilisateur ne puisse pas saisir de mot de passe. Par conséquent, pour forcer l'authentification par clé publique uniquement, saisissez la commande **username** :

```
username admin privilege 15
```

Exemple de topologie de réseau

La figure suivante montre la topologie recommandée pour l'ASA virtuel en mode pare-feu routé avec quatre sous-réseaux configurés dans AWS pour l'ASA virtuel (gestion, interne, externe et DMZ).

Illustration 1 : Exemple d'ASA virtuel sur le déploiement AWS



Déploiement ASA virtuel

La procédure suivante fournit une liste de niveaux supérieurs des étapes pour configurer AWS sur l'ASA virtuel. Pour les étapes détaillées, consultez Mise en route d'AWS.

Procédure

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

Remarque
AWS est divisé en plusieurs régions isolées les unes des autres. Les régions sont affichées dans le coin supérieur droit de votre page. Les ressources disponibles dans une région n'apparaissent pas dans une autre région. Vérifiez périodiquement que vous êtes dans la région prévue.

Étape 2 Cliquez sur **My Account (Mon compte)** > **AWS Management Console (Console de gestion AWS)** et sous **Networking (Mise en réseau)**, cliquez sur **VPC** > **Start VPC Wizard (Démarrer l'assistant VPC)**, créez votre VPC en choisissant un seul sous-réseau public et configurez les éléments suivants (utilisez les paramètres par défaut, sauf indication contraire) :

- Sous-réseau interne et externe : saisissez un nom pour le VPC et les sous-réseaux.
- Passerelle Internet : saisissez le nom de la passerelle Internet. Elle permet la connectivité directe sur Internet.

- Table externe : ajoutez une entrée pour activer le trafic sortant vers Internet (ajoutez 0.0.0.0/0 à la passerelle Internet).

Étape 3 Cliquez sur **My Account (Mon compte)** > **AWS Management Console (Console de gestion AWS)** > **EC2**, puis sur **Create an Instance** (Créer une instance).

- Sélectionnez votre AMI, par exemple, le serveur Ubuntu 14.04 LTS.

  Utilisez l'AMI identifiée dans la notification de livraison de votre image.

- Choisissez le type d'instance pris en charge par l'ASA virtuel, par exemple, c3.large.
- Configurez l'instance (les CPU et la mémoire sont fixes).
- Développez la section **Advanced Details** (Détails avancés) et dans le champ **User data** (Données utilisateur) facultatif, vous pouvez saisir la configuration Day0 (Jour0), qui est le texte saisi contenant la configuration ASA virtuel appliquée lors du lancement d'ASA virtuel. Pour en savoir plus sur la configuration Day0 (Jour0), notamment sur les licences Smart, consultez la section Préparer le fichier de configuration Day0 (Jour0).
  - **Interface de gestion** : si vous choisissez de fournir les détails de la configuration Day0 (Jour0), vous *devez* fournir les détails de l'interface de gestion, qui doit être configurée pour utiliser DHCP.
  - **Interfaces de données** : les adresses IP des interfaces de données seront attribuées et configurées uniquement si vous fournissez ces renseignements dans le cadre de la configuration Day0 (Jour0). Les interfaces de données peuvent être configurées pour utiliser le protocole DHCP, ou si les interfaces réseau à associer sont déjà créées et les adresses IP connues, vous pouvez fournir les détails de l'adresse IP dans la configuration Day0 (Jour0).
  - **Sans configuration Day0 (Jour0)** : si vous déployez l'ASA virtuel *sans* fournir la configuration Day0 (Jour0), l'ASA virtuel applique la configuration ASA virtuel par défaut où il récupère les adresses IP des interfaces associées du serveur de métadonnées AWS et attribue les adresses IP (les interfaces de données obtiennent les adresses IP attribuées, mais les ENI seront inactifs). L'interface Management0/0 sera opérationnelle et obtiendra l'adresse IP configurée avec l'adresse DHCP. Consultez la section Adressage IP dans votre VPC pour en savoir plus sur Amazon EC2 et l'adressage IP d'Amazon VPC.

    Exemple de configuration Day0 (Jour0) -

```
! ASA Version 9.x.1.200
!
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute

no shutdown
!


crypto key generate rsa modulus 2048
ssh 0 0 management
ssh ::/0 management
ssh timeout 60
ssh version 2
username admin password Q1w2e3r4 privilege 15
username admin attributes
service-type admin
aaa authentication ssh console LOCAL
!
```

```
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list allow-all extended permit ip any any
access-list allow-all extended permit ip any6 any6
access-group allow-all global
!
interface G0/0
nameif outside
ip address dhcp setroute

no shutdown
!
interface G0/1
nameif inside
ip address dhcp

no shutdown
!
```

- Stockage : conservez les valeurs par défaut.
- Instance de balise : vous pouvez créer de nombreuses balises pour classer vos appareils. Attribuer un nom à vos appareils vous aide à les localiser facilement.
- Groupe de sécurité : créez un groupe de sécurité et nommez-le. Le groupe de sécurité est un pare-feu virtuel pour une instance permettant de contrôler le trafic entrant et sortant.

  Par défaut, le groupe de sécurité est ouvert à toutes les adresses. Modifiez les règles pour autoriser uniquement l'entrée SSH des adresses utilisées pour accéder à votre ASA virtuel.

  Pour savoir comment le groupe de sécurité contrôle le trafic, consultez la documentation d'AWS - Contrôler le trafic de vos ressources AWS à l'aide des groupes de sécurité.
- Développez la section **Advanced Details** (Détails avancés) et dans le champ **User data** (Données utilisateur), vous pouvez éventuellement saisir une configuration Day0 (Jour0), qui est le texte saisi contenant la configuration ASA virtuel appliquée lors du lancement d'ASA virtuel. Pour en savoir plus sur la façon de réaliser une configuration Day0 (Jour0), notamment sur les licences Smart, consultez la section Préparer le fichier de configuration Day0 (Jour0).
  - **Interface de gestion** : si vous choisissez de fournir une configuration Day0 (Jour0), vous **devez** fournir les détails de l'interface de gestion, qui doit être configurée pour utiliser DHCP.
  - **Interfaces de données** : les adresses IP des interfaces de données seront attribuées et configurées uniquement si vous fournissez ces renseignements dans le cadre de la configuration Day0 (Jour0). Les interfaces de données peuvent être configurées pour utiliser le protocole DHCP ou, si les interfaces réseau à associer sont déjà créées et que les adresses IP sont connues, vous pouvez fournir les détails de l'IP dans la configuration Day0 (Jour0).
  - **Sans configuration Day0 (Jour0)** : si vous déployez l'ASA virtuel **sans** fournir la configuration Day0 (Jour0), l'ASA virtuel applique la configuration ASA virtuel par défaut où il récupère les IP des interfaces associées du serveur de métadonnées AWS et attribue les IP (les interfaces de données obtiennent les IP attribuées, mais les ENI seront inactifs). L'interface Management0/0 sera opérationnelle et obtiendra l'IP configurée avec l'adresse DHCP. Consultez la section Adressage IP dans votre VPC pour en savoir plus sur Amazon EC2 et l'adressage IP d'Amazon VPC.
- Passez en revue votre configuration, puis cliquez sur **Launch** (Lancer).

Étape 4 Créez une paire de clés.

Mise en garde
Attribuez à la paire de clés un nom que vous reconnaîtrez et téléchargerez la clé en lieu sûr; la clé ne pourra jamais être téléchargée de nouveau. Si vous perdez la paire de clés, vous devez détruire vos instances et les redéployer.

Étape 5 Cliquez sur **Launch Instance** (Lancer l'instance) pour déployer votre ASA virtuel.

Étape 6 Cliquez sur **My Account (Mon compte)** > **AWS Management Console (Console de gestion AWS)** > **EC2** > **Launch an Instance (Lancer une instance)** > **My AMIs (Mes AMI)**.

Étape 7 Assurez-vous que la vérification de la source/destination est désactivée par interface pour l'ASA virtuel.

Les paramètres par défaut d'AWS permettent uniquement à une instance de recevoir le trafic pour son adresse IP (IPv4) et permettent uniquement à une instance d'envoyer le trafic de sa propre adresse IP (IPv4). Pour permettre à ASA virtuel d'agir comme un saut routé, vous devez désactiver la vérification de la source/destination sur chacune des interfaces de trafic d'ASA virtuel(interne, externe et DMZ).

Intégration du service Amazon GuardDuty et Défense contre les menaces virtuelles

Amazon GuardDuty est un service de supervision qui traite les données de diverses sources telles que les journaux VPC, les journaux des événements de gestion CloudTrail, les journaux des événements des données CloudTrail S3, les journaux DNS, etc. pour identifier les activités potentiellement non autorisées et malveillantes dans l'environnement AWS.

À propos de l'intégration d'Cisco Secure Firewall ASA virtuel et GuardDuty

Cisco propose une solution pour intégrer le service Amazon GuardDuty à Cisco Secure Firewall ASA virtuel à l'aide de l' interface de ligne de commande sur SSH.

Cette solution utilise les données ou les résultats d'analyse des menaces d'Amazon GuardDuty (adresses IP malveillantes générant des menaces, des attaques, etc.) et fournit ces informations (adresse IP malveillante) à l'Cisco Secure Firewall ASA virtuel pour protéger le réseau et les applications sous-jacentes contre les menaces futures provenant de ces sources (adresse IP malveillante).

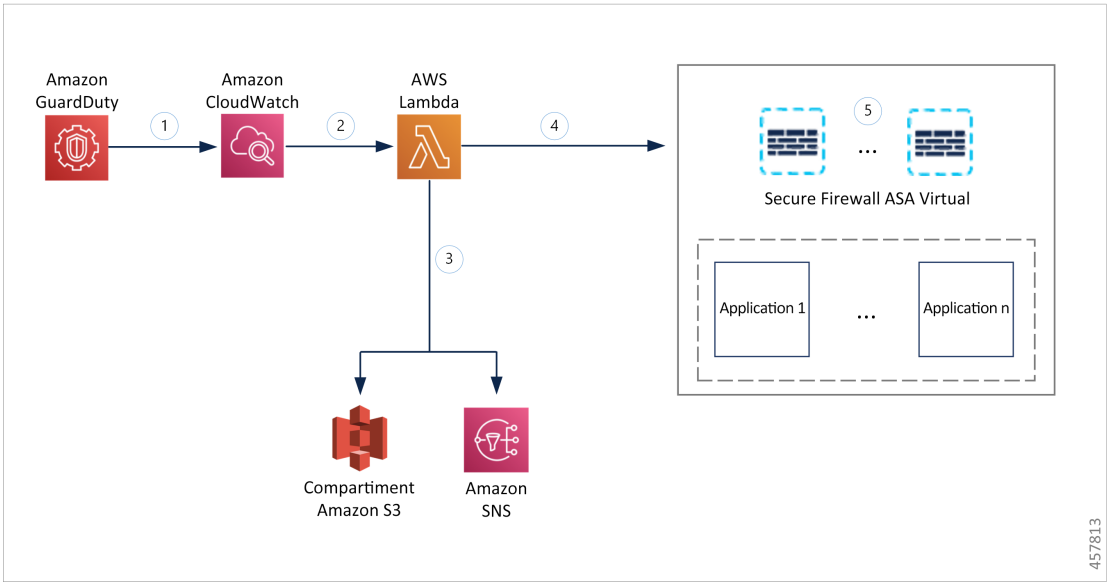
Procédure de bout en bout

Les solutions d'intégration suivantes avec des exemples de flux de travail vous aident à comprendre l'intégration d'Amazon GuardDuty avec Cisco Secure Firewall Threat Defense Virtual .

Le diagramme de flux de travail suivant montre la solution d'intégration d'Amazon GuardDuty avec ASA virtuel.

Intégration avec le Cisco Secure Firewall device manager à l'aide du groupe d'objets réseau

Le diagramme de flux de travail suivant montre la solution d'intégration d'Amazon GuardDuty avec le Cisco Secure Firewall device manager à l'aide du groupe d'objets réseau.



1	Le service GuardDuty envoie des résultats de menaces à CloudWatch lorsqu'il détecte une activité malveillante.
2	L'événement CloudWatch active la fonction Lambda d'AWS.
3	La fonction Lambda met à jour l'hôte malveillant dans le fichier de rapport dans le compartiment S3 et envoie une notification par SNS.
4	La fonction Lambda configure ou met à jour le groupe d'objets réseau avec l'adresse IP de l'hôte malveillant dans le Cisco Secure Firewall device manager.
5	La politique de contrôle d'accès du Cisco Secure Firewall device manager demande au périphérique géré de gérer le trafic en fonction des actions configurées, par exemple, bloquer le trafic des hôtes malveillants signalés par GuardDuty. Cette politique de contrôle d'accès utilise le groupe d'objets réseau avec l'adresse IP malveillante fournie par la fonction Lambda.

Composants clés de cette intégration

Composant	Description
Amazon GuardDuty	Un service Amazon responsable de la génération de résultats de menaces pour les diverses ressources AWS dans une région spécifique, comme EC2, S3, IAM, etc.

Amazon Simple Storage Service (S3)	Un service Amazon utilisé pour stocker divers artefacts associés à la solution : • Fichier zip de la fonction Lambda • Fichier zip de couche Lambda • Fichier d'entrée de la configuration (.ini) ASA virtuelde • Fichier de rapport de sortie (.txt) contenant une liste d'adresses IP malveillantes signalées par la fonction Lambda
Amazon CloudWatch	Un service Amazon utilisé pour : • Superviser le service GuardDuty pour détecter les résultats signalés et déclencher la fonction Lambda pour traiter les résultats. • Journalisation des activités liées à la fonction Lambda dans le groupe de journaux CloudWatch.
Amazon Simple Notification Service (SNS)	Un service Amazon utilisé pour envoyer des notifications par courriel. Ces notifications par courriel contiennent : • Les détails de résultat GuardDuty qui a été traité avec succès par la fonction Lambda. • Les détails des mises à jour effectuées sur les gestionnaires de Cisco Secure Firewall par la fonction Lambda. • Toutes les erreurs importantes rencontrées par la fonction Lambda.
Fonction AWS Lambda	Un service de traitement informatique sans serveur AWS qui exécute votre code en réponse aux événements et gère automatiquement les ressources de traitement sous-jacentes pour vous. La fonction Lambda est déclenchée par la règle d'événement CloudWatch en fonction des résultats de GuardDuty. Dans cette intégration, la fonction Lambda est responsable de : • Traitement des résultats de GuardDuty pour vérifier que tous les critères requis sont respectés, comme la gravité, le sens de la connexion, la présence d'adresses IP malveillantes, etc. • (Selon la configuration) Mise à jour du groupe d'objets réseau sur les gestionnaires de Cisco Secure Firewall avec l'adresse IP malveillante. • Mise à jour de l'adresse IP malveillante dans le fichier de rapport sur le compartiment S3. • Informer l'administrateur de Cisco Secure Firewall de différentes mises à jour de gestionnaire et de toute erreur.

Modèle CloudFormation	Utilisé pour déployer diverses ressources requises pour l'intégration dans AWS. Le modèle CloudFormation contient les ressources suivantes : • **AWS::SNS::Topic** : la rubrique SNS pour l'envoi de notifications par courriel. • **AWS::Lambda::Function, AWS::Lambda::LayerVersion** : la fonction Lambda et les fichiers de couche • **AWS::Events::Rule**: la règle d'événement CloudWatch pour déclencher la fonction Lambda en fonction de l'événement de résultats de GuardDuty. • **AWS::Lambda::Permission**: autorisation pour la règle d'événement CloudWatch de déclencher la fonction Lambda. • **AWS::IAM::Rôle, AWS::IAM::Policy** : le rôle et les ressources de politique IAM pour autoriser diverses autorisations d'accès à la fonction Lambda pour diverses ressources AWS. Ce modèle accepte les paramètres d'entrée des utilisateurs pour personnaliser le déploiement.

Plateformes logicielles prises en charge

- La solution d'intégration GuardDuty s'applique à Cisco Secure Firewall ASA virtuel géré à l'aide de l'interface de ligne de commande sur SSH.
- La fonction Lambda peut mettre à jour les groupes d'objets réseau dans le Cisco Secure Firewall ASA virtuel. Assurez-vous que la fonction Lambda peut se connecter à Cisco Secure Firewall ASA virtuel en utilisant des adresses IP publiques.

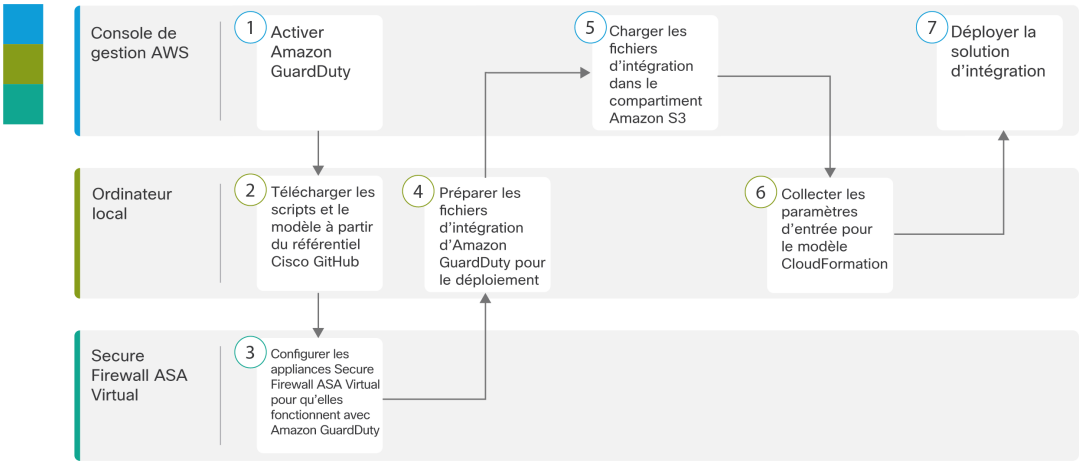
Lignes directrices et limites pour l'intégration d'Amazon GuardDuty et de Cisco Secure Firewall ASA Virtual

- La fonction Lambda est uniquement responsable de la mise à jour des groupes d'objets réseau avec les adresses IP malveillantes. Selon vos besoins, créez des règles d'accès et des politiques d'accès pour bloquer tout trafic non nécessaire.
- Les services AWS utilisés dans cette intégration sont propres à la région. Si vous souhaitez utiliser les résultats de GuardDuty de différentes régions, vous devez déployer des instances propres à la région.
- Vous pouvez configurer les mises à jour d'ASA virtuel à l'aide de l'interface de ligne de commande sur SSH. ASDM, CSM et CDO ne sont pas pris en charge.
- Vous pouvez uniquement utiliser la connexion par mot de passe. Aucune autre méthode d'authentification n'est prise en charge.
- Si vous utilisez des mots de passe chiffrés dans le fichier d'entrée, gardez à l'esprit que :
    - Seul le chiffrement à l'aide des clés KMS symétriques est pris en charge.

- Tous les mots de passe doivent être chiffrés à l'aide d'une clé KMS unique accessible à la fonction Lambda.

Intégrer Amazon GuardDuty avec ASA virtuel

Effectuer les tâches suivantes pour intégrer Amazon GuardDuty à ASA virtuel



	Espace de travail	Étapes
1	Console de gestion AWS	Activer le service Amazon GuardDuty sur AWS, à la page 14
2	Ordinateur local	Télécharger le Cisco Secure Firewall ASA virtuel et le modèle de solution Amazon GuardDuty, à la page 15
3	ASA virtuel	Configurer vos périphériques gérés pour qu'ils fonctionnent avec Amazon GuardDuty, à la page 16
4	Ordinateur local	Préparer les fichiers de ressources d'Amazon GuardDuty pour le déploiement, à la page 18
5	Console de gestion AWS	Charger des fichiers dans le service Amazon Simple Storage, à la page 21
6	Ordinateur local	Collecter les paramètres d'entrée pour le modèle CloudFormation, à la page 22
7	Console de gestion AWS	Déployer la pile, à la page 24

Activer le service Amazon GuardDuty sur AWS

Cette section décrit comment activer le service Amazon GuardDuty sur AWS.

Avant de commencer

Assurez-vous que toutes les ressources AWS se trouvent dans la même région.

Procédure

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

Étape 2 Choisissez **Services** > **GuardDuty**.

Étape 3 Cliquez sur **Get Started** (Mise en route) dans la page **GuardDuty**.

Étape 4 Cliquez sur **Enable GuardDuty** (Activer GuardDuty) pour activer le service Amazon GuardDuty.

Pour en savoir plus sur l'activation de GuardDuty, consultez la section Mise en route de GuardDuty dans la documentation d'AWS.

Prochaine étape

Téléchargez les fichiers de solution Amazon GuardDuty (modèles et scripts) à partir du référentiel Cisco GitHub. Consultez .Télécharger le Cisco Secure Firewall ASA virtuel et le modèle de solution Amazon GuardDuty, à la page 15

Télécharger le Cisco Secure Firewall ASA virtuel et le modèle de solution Amazon GuardDuty

Téléchargez les fichiers requis pour la solution Amazon GuardDuty. Les scripts et les modèles de déploiement pour votre version de Cisco Secure Firewall ASA virtuel sont disponibles dans le référentiel Cisco GitHub à l'adresse :

https://github.com/CiscoDevNet/cisco-asav

Voici une liste de ressources dans le référentiel Cisco GitHub :

Fichiers	Description
READ.MD	Fichier ReadMe
configuration/	Modèle de fichier de configuration d'Cisco Secure Firewall ASA virtuel.
images/	Il contient l'Cisco Secure Firewall ASA virtuel et des exemples de solutions d'intégration Amazon GuardDuty.
lambda/	Fichiers Python de fonction Lambda.
templates/	Modèle CloudFormation pour le déploiement.

Configurer vos périphériques gérés pour qu'ils fonctionnent avec Amazon GuardDuty

La fonction Lambda traite les résultats d'Amazon GuardDuty et identifie l'adresse IP malveillante qui a déclenché l'événement CloudWatch. Ensuite, la fonction Lambda met à jour le groupe d'objets réseau dans l'ASAv avec l'adresse IP malveillante. Vous pouvez ensuite configurer une stratégie de contrôle d'accès qui utilise ce groupe d'objets réseau pour gérer le trafic.

Créer un groupe d'objets réseau

Dans ASA virtuel, vous devez configurer ou créer un groupe d'objets réseau pour la fonction Lambda afin de mettre à jour l'adresse IP malveillante détectée par Amazon GuardDuty.

Si vous ne configurez pas de groupe d'objets réseau avec la fonction Lambda, un groupe d'objets réseau avec le nom par défaut **aws-gd-suspicious-hosts** est créé par la fonction Lambda pour mettre à jour l'adresse IP malveillante.

Créer un groupe d'objets réseau dans Cisco Secure Firewall ASA Virtual

Dans Cisco Secure Firewall ASA Virtual, vous devez créer un groupe d'objets réseau pour la fonction Lambda afin de mettre à jour l'adresse IP malveillante détectée par Amazon GuardDuty.

Si vous ne configurez pas de groupe d'objets réseau avec la fonction Lambda, un groupe d'objets réseau avec le nom par défaut *aws-gd-suspicious-hosts* est créé par la fonction Lambda pour mettre à jour l'adresse IP malveillante.

Initialement, pour utiliser le groupe d'objets réseau dans une règle ACL, vous devrez peut-être créer le groupe d'objets avec une adresse IP factice. Vous pouvez créer plusieurs groupes d'objets réseau sur un seul ASAv.

Pour en savoir plus sur le groupe d'objets réseau et la politique d'accès, consultez le guide de configuration de l'interface de ligne de commande des pare-feu de la série Cisco ASA.

Pour créer le groupe d'objets réseau, procédez comme suit :

Procédure

Étape 1 Connectez-vous à Cisco Secure Firewall ASA Virtual.

Étape 2 Créez un groupe d'objets réseau avec une description. Dans cet exemple, une adresse IP d'hôte factice 12.12.12.12 est ajoutée au groupe d'objets réseau créé.

Exemple :

```
hostname(config)# object-group network aws-gd-suspicious-hosts
hostname(config)# description Malicious Hosts reported by AWS GuardDuty
hostname(config)# network-object host 12.12.12.12
```

Étape 3 Créez ou mettez à jour la politique d'accès ou la règle de contrôle d'accès pour gérer le trafic à l'aide du groupe d'objets réseau. \

Astuces
Vous pouvez également créer ou mettre à jour la politique de contrôle d'accès ou la règle de contrôle d'accès après avoir vérifié que la fonction Lambda met à jour le groupe d'objets réseau avec l'adresse IP malveillante.

Exemple :

```
hostname(config)# access-list out-iface-access line 1 extended deny ip object-group
aws-gd-suspicious-hosts any
```

Création de comptes d'utilisateur dans ASAv pour l'accès à la fonction Lambda

La fonction Lambda nécessite un utilisateur dédié sur ASAv pour gérer les mises à jour de configuration. Un niveau de privilège de 15 garantit que l'utilisateur dispose de tous les privilèges.

Pour en savoir plus sur la création d'utilisateur, consultez le guide de configuration de l'interface de ligne de commande des pare-feu de la série Cisco ASA.

Procédure

Étape 1 Créez un utilisateur.

username *nom* [**password** *mot de passe*] **privilege** *niveau*

Exemple :

```
hostname(config)# username aws-gd password MyPassword@2021 privilege 15
```

Étape 2 Configurez les attributs de nom d'utilisateur.

username *nom d'utilisateur* **attributes**

Exemple :

```
hostname(config)# username aws-gd attributes
```

Étape 3 Fournissez à l'utilisateur un accès de niveau administrateur à tous les services.

service-type admin

Exemple :

```
hostname(config)# service-type admin
```

(Facultatif) Chiffrer les mots de passe

Au besoin, vous pouvez fournir des mots de passe chiffrés dans le fichier de configuration d'entrée. Vous pouvez également fournir des mots de passe en texte brut.

Chiffrez tous les mots de passe à l'aide d'une clé KMS unique accessible à la fonction Lambda. Utilisez la commande **aws kms encrypt --key-id** <*KMS-ARN*> **--plaintext** <*password*> pour générer le mot de passe chiffré. Vous devez installer et configurer l'interface de ligne de commande AWS pour exécuter cette commande.

Remarque Assurez-vous que les mots de passe sont chiffrés à l'aide de clés KMS symétriques.

Pour en savoir plus sur l'interface de ligne de commande AWS, consultez Interface de ligne de commande AWS. Pour en savoir plus sur les clés principales et le chiffrement, consultez le document AWS Création de clés et la Référence de commande de l'interface de ligne de commande AWS sur le chiffrement des mots de passe et KMS.

Exemple :

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext <password>
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
}
$
```

La valeur de la clé *CiphertextBlob* doit être utilisée comme mot de passe.

Préparer les fichiers de ressources d'Amazon GuardDuty pour le déploiement

Les fichiers de ressources de déploiement de la solution Amazon GuardDuty sont disponibles dans le référentiel Cisco GitHub.

Avant de déployer la solution Amazon GuardDuty sur AWS, vous devez préparer les fichiers suivants :

- Fichier d'entrée de configuration du gestionnaire Secure Firewall ASA virtuel
- Fichier zip de la fonction Lambda
- Fichier zip de la couche Lambda

Préparer le fichier d'entrée de la configuration

Dans le modèle de configuration, vous devez définir les détails de l'ASAv que vous intégrez à la solution Amazon GuardDuty.

Avant de commencer

- Assurez-vous d'authentifier et de vérifier le compte d'utilisateur du gestionnaire d'appareils avant de fournir les détails du compte d'utilisateur dans le fichier de configuration.
- Assurez-vous de configurer un seul ASAv dans le fichier de configuration. Si vous configurez plusieurs ASAv, la fonction Lambda peut mettre à jour simultanément tous les ASAv configurés dans le fichier, ce qui entraîne une situation de concurrence et un comportement déterministe.
- Vous devez avoir noté l'adresse IP et le nom de l'ASAv.
- Vous devez avoir créé un compte d'utilisateur disposant de privilèges d'administrateur pour la fonction Lambda afin d'accéder à ces groupes d'objets réseau dans l'ASAv et de les mettre à jour.

Procédure

Étape 1 Connectez-vous à la machine locale sur laquelle vous avez téléchargé les fichiers de ressources Amazon GuardDuty.

Étape 2 Accédez au dossier **asav-template** > **configuration**.

Étape 3 Ouvrez le fichier `asav-manager-config-input.ini` dans un éditeur de texte. Dans ce fichier, vous devez saisir les détails de l'ASAv sur lequel vous prévoyez d'intégrer et de déployer la solution Amazon GuardDuty.

Étape 4 Entrez les paramètres ASAv suivants :

Paramètres	Description
[asav-1]	Nom de la section : identifiant ASAv unique dans le fichier
public-ip	Adresse IP publique de l'ASAv
user name	Nom d'utilisateur pour se connecter à l'ASAv.
mot de passe	Mot de passe de connexion à l'ASAv. Le mot de passe peut être en texte brut ou une chaîne chiffrée qui a été chiffrée à l'aide de KMS.
enable-password	Activer le mot de passe de l'ASAv. Le mot de passe peut être en texte brut ou une chaîne chiffrée qui a été chiffrée à l'aide de KMS.
object-group-name	Nom de groupes d'objets réseau mis à jour avec l'adresse IP d'hôte malveillante par la fonction Lambda. Si vous saisissez plusieurs noms de groupes d'objets réseau, assurez-vous qu'il s'agit de valeurs séparées par des virgules.

Étape 5 Enregistrez et fermez le fichier `asav-manager-config-input.ini`.

Prochaine étape

Créez le fichier d'archive de la fonction Lambda.

Préparation du fichier d'archive de la fonction Lambda

Cette section décrit comment archiver les fichiers de fonction Lambda dans un environnement Linux.

Remarque Le processus d'archivage peut différer selon le système d'exploitation de la machine locale sur laquelle vous archivez les fichiers.

Avant de commencer

Assurez-vous que votre hôte Linux exécute Ubuntu version 18.04 avec Python version 3.6 ou ultérieure.

Procédure

Étape 1 Ouvrez la console d'interface en ligne de commande sur la machine locale sur laquelle vous avez téléchargé les ressources d'Amazon GuardDuty.

Étape 2 Accédez au dossier /lambda et archivez les fichiers. Voici un exemple de transcription à partir d'un hôte Linux.

```
$ cd lambda
$ zip asav-gd-lambda.zip *.py
adding: aws.py (deflated 71%)
adding: asav.py (deflated 79%)
adding: main.py (deflated 73%)
adding: utils.py (deflated 65%)
$
```

Le fichier zip `asav-gd-lambda.zip` est créé.

Étape 3 Quittez et fermez la console d'interface en line de commande.

Prochaine étape

Créez le fichier zip de couche Lambda à l'aide du fichier zip `asav-gd-lambda.zip`.

Préparer le fichier de la couche Lambda

Cette section décrit comment archiver le fichier de la couche Lambda dans un environnement Linux.

Remarque Le processus d'archivage peut différer selon le système d'exploitation de la machine locale sur laquelle vous archivez le fichier.

Procédure

Étape 1 Ouvrez la console d'interface en ligne de commande de la machine locale sur laquelle vous avez téléchargé les ressources d'Amazon GuardDuty.

Étape 2 Effectuez les actions suivantes dans votre console d'interface en ligne de commande.

Voici un exemple de transcription à partir d'un hôte Linux tel qu'Ubuntu 22.04 avec Python 3.9 installé.

```
$ mkdir -p layer
$ virtualenv -p /usr/bin/python3.9 ./layer/
$ source ./layer/bin/activate
$ pip3.9 install cffi==1.15.0
$ pip3.9 install cryptography==37.0.2
$ pip3.9 install paramiko==2.7.1
$ mkdir -p ./python/.libs_cffi_backend/
$ cp -r ./layer/lib/python3.9/site-packages/* ./python/
$ zip -r asav-gd-lambda-layer.zip ./python
```

Le fichier zip `asav-gd-lambda-layer.zip` est créé.

Notez que vous devez installer Python 3.9 et ses dépendances pour créer la couche Lambda.

Voici l'exemple de transcription pour l'installation de Python 3.9 sur un hôte Linux tel qu'Ubuntu 22.04.

```
$ sudo apt update
$ sudo apt install software-properties-common
$ sudo add-apt-repository ppa:deadsnakes/ppa
$ sudo apt install python3.9
$ sudo apt install python3-virtualenv
$ sudo apt install zip
$ sudo apt-get install python3.9-distutils
$ sudo apt-get install python3.9-dev
$ sudo apt-get install libffi-dev
```

Étape 3 Quittez et fermez la console d'interface en line de commande.

Prochaine étape

Dans le compartiment Amazon S3, vous devez charger le fichier de configuration Secure Firewall ASA virtuel, le fichier zip de la fonction Lambda et le fichier zip de la couche Lambda. Voir la section Charger des fichiers dans le service Amazon Simple Storage, à la page 21.

Charger des fichiers dans le service Amazon Simple Storage

Après avoir préparé tous les artefacts de solution Amazon GuardDuty, vous devez charger les fichiers dans un dossier de compartiment Amazon Simple Storage Service (S3) dans le portail AWS.

Procédure

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

Étape 2 Ouvrez la console Amazon S3.

Étape 3 Créez un compartiment Amazon S3 pour le chargement des artefacts Amazon GuardDuty. Consultez Création d'Amazon S3.

Étape 4 Chargez les artefacts Amazon GuardDuty suivants dans le compartiment Amazon S3.

- Fichier de configuration de Cisco Secure Firewall ASA virtuel : `asav-config-input.ini`

  Remarque
  Il n'est pas nécessaire de charger ce fichier lorsque vous utilisez la méthode Security Intelligence Network Feed (flux de réseau de renseignements de sécurité) pour le déploiement de la solution Amazon GuardDuty dans les centres de gestion.

- Fichier zip de la couche Lambda : `asav-gd-lambda-layer.zip`
- Fichier zip de la fonction Lambda : `asav-gd-lambda.zip`

Prochaine étape

Préparez le modèle CloudFormation utilisé pour le déploiement des ressources d'Amazon GuardDuty. Consultez Collecter les paramètres d'entrée pour le modèle CloudFormation, à la page 22.

Collecter les paramètres d'entrée pour le modèle CloudFormation

Cisco fournit le modèle CloudFormation utilisé pour déployer les ressources requises par la solution Amazon GuardDuty dans AWS. Collectez des valeurs pour les paramètres de modèle suivants avant le déploiement.

Procédure

Template Parameters

Paramètre	Description	Exemple
Nom du déploiement*	Le nom que vous saisissez dans ce paramètre est utilisé comme préfixe pour toutes les ressources créées par le modèle CloudFormation.	**cisco-asav-gd**
Niveau de gravité minimal de la recherche de GD*	Le niveau de gravité minimal des résultats d'Amazon GuardDuty à prendre en compte pour le traitement doit être compris entre **1,0** et **8,9**. Tout résultat signalé avec une gravité inférieure à la plage minimale est ignoré. La classification de la gravité est la suivante : • Faible : de 1,0 à 3,9 Moyenne : de 4,0 à 6,9 Élevée : de 7,0 à 8,9	**4,0**
ID d'e-mail de l'administrateur*	Adresse e-mail de l'administrateur pour recevoir des notifications sur Secure Firewall ASA virtuel au sujet des mises à jour effectuées par la fonction Lambda dans le Secure Firewall ASA virtuel.	**abc@xyz.com**
Nom du compartiment S3*	Nom du compartiment Amazon S3 contenant les fichiers d'artefacts Amazon GuardDuty (fichier zip de la fonction Lambda, fichier zip de la couche Lambda et fichiers de gestionnaire de configuration Secure Firewall ASA virtuel).	Par exemple : **asav-gd-bucket**

Paramètre	Description	Exemple
Préfixe de dossier/chemin d'accès au compartiment S3	Chemin d'accès au compartiment Amazon S3 ou nom du dossier dans lequel les fichiers de configuration sont stockés. S'il n'y a pas de dossier, laissez ce champ vide.	Par exemple : **« »** ou « **cisco/asav-gd/** »
Nom du fichier zip de la couche Lambda*	Nom du fichier zip de la couche Lambda.	Par exemple : `asav-gd-lambda-layer.zip`
Nom du fichier zip de la fonction Lambda*	Nom du fichier zip de la fonction Lambda.	Par exemple : `asav-gd-lambda.zip`
Secure Firewall ASA virtuel	Le fichier ***.ini** contenant les détails de configuration du gestionnaire Secure Firewall ASA virtuel. (Adresse IP publique, nom d'utilisateur, mot de passe, type d'appareil, noms de groupes d'objets réseau, etc.)	Par exemple : `asav-config-input.ini`
ARN de la clé KMS utilisée pour le chiffrement des mots de passe	ARN d'une clé KMS existante (clé KMS AWS utilisée pour le chiffrement des mots de passe). Vous pouvez laisser ce paramètre vide dans le cas où des mots de passe en texte brut sont fournis dans le fichier d'entrée de configuration de Secure Firewall ASA virtuel. Si vous le spécifiez, tous les mots de passe mentionnés dans le fichier d'entrée de la configuration de Secure Firewall ASA virtuel doivent être chiffrés. Les mots de passe doivent être chiffrés uniquement à l'aide de l'ARN spécifié. Génération de mots de passe chiffrés : aws kms encrypt --key-id <ARN KMS> --plaintext <password>	Par exemple : **arn:aws:kms:<region>:<awsaccountid>:key/<keyid>**
Activer/désactiver les journaux de débogage*	Activez ou désactivez les journaux de débogage de la fonction Lambda dans CloudWatch.	Par exemple : **activer** ou **désactiver**

* : Champ obligatoire

Prochaine étape

Déployez la pile à l'aide du modèle CloudFormation. Voir la section Déployer la pile, à la page 24.

Déployer la pile

Une fois que toutes les conditions préalables pour le déploiement de la solution Amazon GuardDuty sont terminées, créez la pile AWS CloudFormation. Utilisez le fichier de modèle dans le répertoire cible : `templates/cisco-asav-gd-integration.yaml`, et fournissez les paramètres collectés dans Collect Input Parameters for CloudFormation Template (Recueillir les paramètres d'entrée pour le modèle CloudFormation).

Procédure

Étape 1 Connectez-vous à la console AWS.

Étape 2 Accédez à Services > CloudFormation > Stacks (Piles) > Create stack (Créer une pile) (avec de nouvelles ressources) > Prepare template (Préparer le modèle) (le modèle est fourni dans le dossier) > Specify template (Spécifier le modèle) > Template source (Source du modèle) (chargez le fichier de modèle à partir du répertoire cible : `templates/cisco-asav-gd-integration.yaml`) > Create Stack (Créer une pile).

Pour en savoir plus sur le déploiement d'une pile sur AWS, consultez la documentation d'AWS.

Prochaine étape

Validez votre déploiement. Consultez Valider votre déploiement, à la page 25.

Abonnez-vous également pour recevoir des notifications par e-mail sur les mises à jour de détection des menaces signalées par Amazon GuardDuty. Consultez S'abonner aux notifications par courriel, à la page 24.

S'abonner aux notifications par courriel

Dans le modèle CloudFormation, un identifiant de courriel est configuré pour recevoir des notifications sur les mises à jour des résultats de GuardDuty effectuées par la fonction Lambda. Après avoir déployé le modèle CloudFormation sur AWS, une notification par courriel est envoyée à cet identifiant de courriel par le biais du service Amazon Web Notification Service (SNS) vous demandant de vous abonner pour recevoir les mises à jour de notification.

Procédure

Étape 1 Ouvrez la notification par courriel :

Étape 2 Cliquez sur le lien **Subscription** (abonnement) disponible dans la notification par courriel.

Prochaine étape

Validez votre déploiement. Consultez Valider votre déploiement, à la page 25.

Valider votre déploiement

Dans AWS, vous avez des options pour vérifier la solution Amazon GuardDuty, comme décrit dans cette section. Vous pouvez suivre ces instructions de validation du déploiement une fois le déploiement de CloudFormation terminé.

Avant de commencer

Assurez-vous d'avoir installé et configuré l'interface de ligne de commande (CLI) AWS pour exécuter des commandes de validation du déploiement. Pour en savoir plus sur la documentation relative à l'interface de ligne de commande AWS, consultez Interface de ligne de commande AWS.

Procédure

Étape 1 Connectez-vous à la console de gestion AWS.

Étape 2 Accédez à **Services > GuardDuty > Settings (Paramètres) > About GuardDuty (À propos de GuardDuty) > Detector ID (ID de détecteur)** pour noter l'ID de détecteur.

Cet ID de détecteur est requis pour générer des exemples de résultats dans Amazon GuardDuty.

Étape 3 Ouvrez la console d'interface en ligne de commande AWS pour générer l'exemple de résultat dans Amazon GuardDuty en exécutant les commandes suivantes :

```
aws guardduty create-sample-findings --detector-id <detector-id> --finding-types
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
```

```
aws guardduty create-sample-findings --detector-id <detector-id> --finding-types
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
```

Étape 4 Vérifiez l'exemple de résultat dans la liste des résultats sur la console Amazon GuardDuty.

Les exemples de résultats contiennent le préfixe **[sample]** (exemple). Vous pouvez vérifier les détails de l'exemple de résultat en affichant les attributs tels que le sens de connexion, l'adresse IP distante, etc.

Étape 5 Attendez que la fonction Lambda s'exécute.

Après le déclenchement de la fonction Lambda, vérifiez les éléments suivants :

- Une notification par e-mail avec les détails concernant les résultats d'Amazon GuardDuty reçus et les mises à jour de Secure Firewall ASA virtuel effectuées par la fonction Lambda.
- Vérifiez si le fichier de rapport est généré dans le compartiment Amazon S3. Il contient l'adresse IP malveillante signalée par l'exemple de résultat dans Amazon GuardDuty. Vous pouvez identifier le nom du fichier de rapport au format : `<deployment-name>-report.txt`.
- vérifiez que les groupes d'objets réseau sont mis à jour sur les gestionnaires configurés (Secure Firewall ASA virtuel) avec l'adresse IP malveillante mise à jour à partir de l'exemple de résultat.

Étape 6 Accédez à **AWS Console (Console AWS) > Services > CloudWatch > Logs (Journaux) > Log groups (Groupes de journaux) >** *select the log group (sélectionner le groupe de journaux)* pour vérifier les journaux Lambda dans la console CloudWatch. Vous pouvez identifier le nom du groupe de journaux CloudWatch au format : `<deployment-name>-lambda`.

Étape 7 Après avoir validé le déploiement, nous vous recommandons de nettoyer les données générées par l'exemple de résultat comme suit :

a) Accédez à **AWS Console (Console AWS) > Services > GuardDuty > Findings (Résultats) > Select the finding (Sélectionner le résultat) > Actions > Archive (Archiver)** pour afficher les exemples de données de résultat.
b) Supprimez les adresses IP malveillantes ajoutées dans le groupe d'objets réseau pour effacer les données mises en mémoire cache de Secure Firewall ASA virtuel.
c) Nettoyez le fichier de rapport dans le compartiment Amazon S3. Vous pouvez mettre à jour le fichier en supprimant les adresses IP malveillantes signalées par l'exemple de résultat.

Mettre à jour la configuration de déploiement de solution existante

Nous vous recommandons de ne pas mettre à jour le compartiment S3 ou les valeurs de préfixe de dossier et de chemin d'accès au compartiment S3 après le déploiement. Toutefois, si vous devez mettre à jour la configuration d'une solution qui a été déployée, utilisez l'option **`Update Stack`** (Mettre à jour la pile) sur la page CloudFormation dans la console AWS.

Vous pouvez mettre à jour n'importe lequel des paramètres ci-dessous.

Paramètre	Description
Nom du fichier de configuration du gestionnaire Secure Firewall ASA virtuel	Ajoutez ou mettez à jour le fichier de configuration dans le compartiment Amazon S3. Vous êtes autorisé à mettre à jour le fichier du même nom que le fichier précédent. Si le nom du fichier de configuration est modifié, vous pouvez mettre à jour ce paramètre en utilisant l'option **Update stack** (Mettre à jour la pile) dans la console AWS.
Niveau de gravité minimal de la recherche de GD*	Utilisez l'option **Update stack** (Mettre à jour la pile) dans la console AWS pour mettre à jour la valeur du paramètre.
ID d'e-mail de l'administrateur*	Mettez à jour la valeur du paramètre d'ID d'e-mail à l'aide de l'option **Update Stack** (Mettre à jour la pile) dans la console AWS. Vous pouvez également ajouter ou mettre à jour des abonnements par e-mail via la console de service SNS.
Nom du compartiment S3*	Mettez à jour le fichier zip dans le compartiment Amazon S3 avec un nouveau nom, puis mettez à jour le paramètre à l'aide de l'option **Update Stack** (Mettre à jour la pile) dans la console AWS.
Nom du fichier zip de la couche Lambda*	Mettez à jour le nom du fichier zip de la couche Lambda dans le compartiment Amazon S3 avec un nouveau nom, puis mettez à jour cette valeur de paramètre à l'aide de l'option **Update Stack** (Mettre à jour la pile) dans la console AWS.

Paramètre	Description
Nom du fichier zip de la fonction Lambda*	Mettez à jour le fichier zip de la fonction Lambda dans le compartiment Amazon S3 avec un nouveau nom, puis mettez à jour cette valeur de paramètre à l'aide de l'option **Update Stack** (Mettre à jour la pile) dans la console AWS.
ARN de la clé KMS utilisée pour le chiffrement des mots de passe	Utilisez l'option **Update stack** (Mettre à jour la pile) dans la console AWS pour mettre à jour la valeur du paramètre.
Activer/désactiver les journaux de débogage*	Utilisez l'option **Update stack** (Mettre à jour la pile) dans la console AWS pour mettre à jour la valeur du paramètre.

Procédure

Étape 1 Accédez à la console de gestion AWS.

Étape 2 Si nécessaire, créez le nouveau compartiment et le nouveau dossier.

Étape 3 Assurez-vous que les artefacts ci-dessous sont copiés de l'ancien compartiment au nouveau compartiment.

- Fichier de configuration de Cisco Secure Firewall ASA virtuel : `asav-config-input.ini`
- Fichier zip de la couche Lambda : `asav-gd-lambda-layer.zip`
- Fichier zip de la fonction Lambda : `asav-gd-lambda.zip`
- Fichier de rapport de sortie : `<deployment-name>-report.txt`

Étape 4 Pour mettre à jour les valeurs des paramètres, accédez à **Services > CloudFormation > Stacks > > Update (Update Stack) > Prepare template > Use current template > Next >** <*update parameters*>> **Update Stack**.

Réglage de la performance

Optimisation du réseau privé virtuel (VPN)

Les instances AWS c5 offrent des performances beaucoup plus élevées que les anciennes instances c3, c4 et m4. Le débit approximatif du VPN d'accès à distance (DTLS utilisant un trafic TCP de 450B avec le chiffrement AES-CBC) sur la famille d'instances c5 devrait être :

- 0,5 Gbit/s sur c5.large
- 1 Gbit/s sur c5.xlarge
- 2 Gbit/s sur c5.2xlarge

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.