Déployer la solution d'évolutivité automatique ASA virtuel sur AWS

Solution d'évolutivité automatique pour la Défense contre les menaces virtuelles ASA virtuel sur AWS

Les sections suivantes décrivent comment les composants de la solution d'évolutivité automatique fonctionnent pour l'ASA virtuel sur AWS.

Aperçu

Cisco fournit des modèles et des scripts CloudFormation pour le déploiement d'un groupe d'évolutivité automatique de pare-feu ASA virtuel à l'aide de plusieurs services AWS, notamment Lambda, les groupes d'évolutivité automatique, Elastic Load Balancing (ELB, équilibreur de charge élastique), les compartiments Amazon S3, SNS et CloudWatch.

L'évolutivité automatique de l'ASA virtuel dans AWS est une implémentation complète sans serveur (c.-à-d. aucune machine virtuelle d'assistant n'est impliquée dans l'automatisation de cette fonctionnalité) qui ajoute une capacité d'évolutivité automatique horizontale aux instances d'ASA virtuel dans l'environnement AWS. À partir de la version 6.4, la solution d'évolutivité automatique est prise en charge sur gérée par centre de gestion.

La solution d'évolutivité automatique ASA virtuel est un déploiement basé sur un modèle CloudFormation qui fournit :

- La configuration entièrement automatisée s'applique automatiquement aux instances ASA virtuel mises à l'échelle.
- Prise en charge des équilibreurs de charges et des zones de multi-disponibilité.

- Prise en charge de l'activation et de la désactivation de la fonction d'évolutivité automatique.

Scénario d'évolutivité automatique à l'aide de la topologie de Sandwich

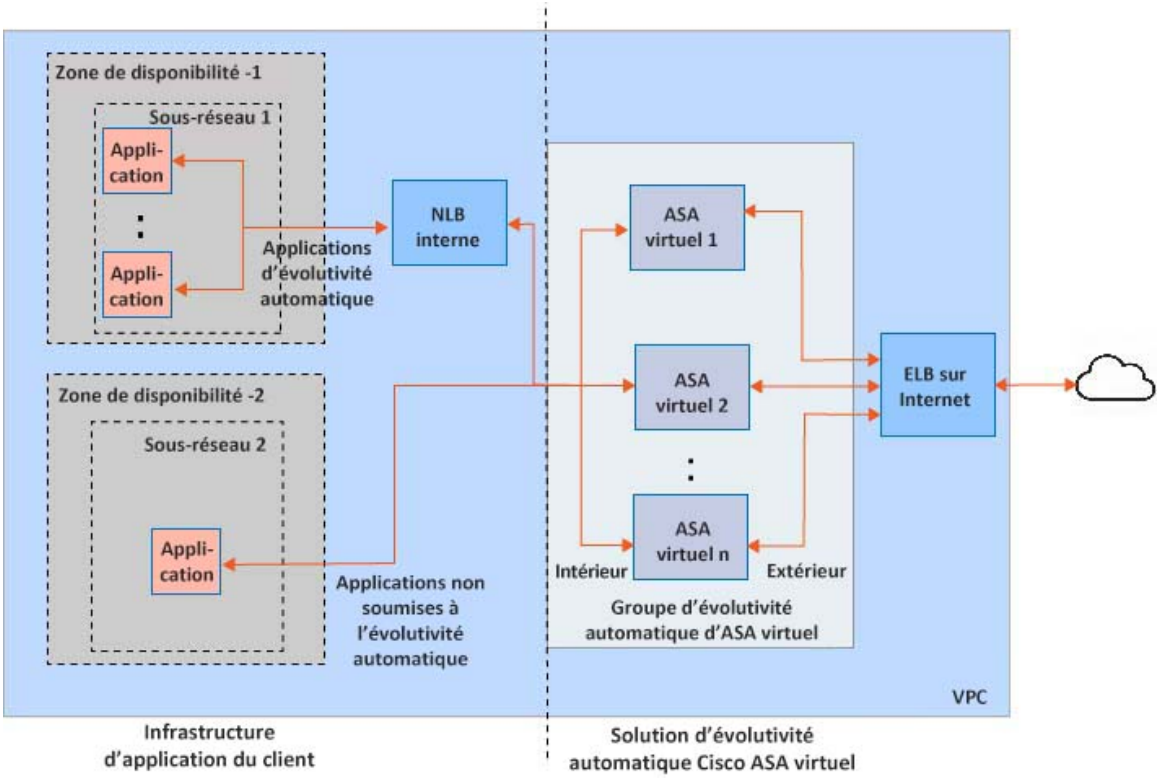
Le scénario de cette solution d'évolutivité automatique AWS ASA virtuel est illustré dans le diagramme des scénarios. Comme l'équilibreur de charges AWS autorise uniquement les connexions entrantes, seul le trafic externe est autorisé à passer à l'intérieur par le pare-feu ASA virtuel.

Remarque Les ports sécurisés ont besoin d'un certificat SSL/TLS, comme décrit dans Certificat de serveur SSL, à la page 7 dans les conditions préalables.

L'équilibreur de charges Internet peut être un équilibreur de charges réseau ou un équilibreur de charges d'application. Toutes les exigences et conditions d'AWS sont remplies dans tous les cas. Comme indiqué dans le diagramme des scénarios, le côté droit de la ligne pointillée est déployé par l'intermédiaire des modèles ASA virtuel. Le côté gauche est entièrement défini par l'utilisateur.

Remarque Le trafic sortant initié par l'application ne passera pas par l'ASA virtuel.

Illustration 1 : Diagramme des scénarios d'évolutivité automatique d'ASA virtuel à l'aide de la topologie de Sandwich



La bipolation du trafic basée sur le port est possible. Cela peut être possible en utilisant des règles NAT. Par exemple, le trafic DNS LB sur Internet, Port : 80 peut être acheminé vers Application-1; le trafic Port : 88 peut être acheminé vers Application-2.

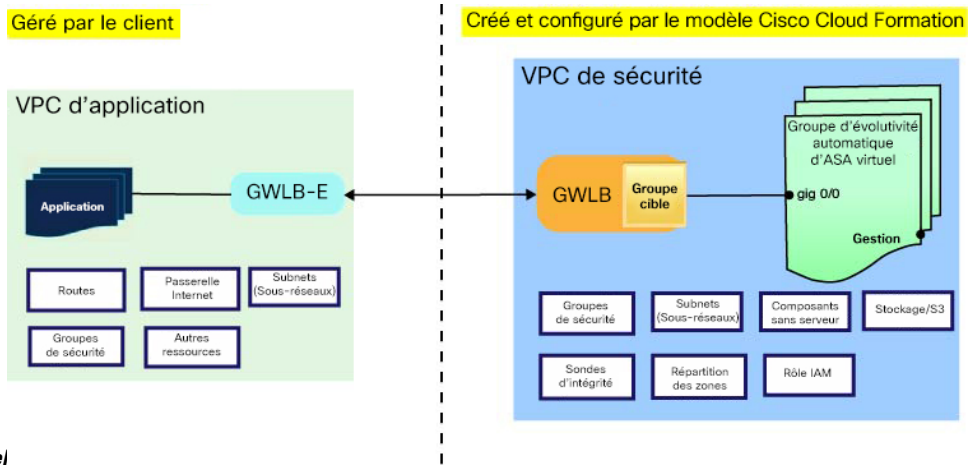
Scénario d'évolutivité automatique à l'aide de l'équilibreur de charges de la passerelle AWS

Le scénario de la solution d'évolutivité automatique de l'équilibreur de charges de la passerelle (GWLB) AWS d'ASA virtuel est illustré dans le diagramme de scénarios. La GWLB AWS permet les connexions entrantes et sortantes, de sorte que le trafic généré en interne et en externe est autorisé à passer à l'intérieur par le pare-feu Cisco ASA virtuel.

L'équilibreur de charges sur Internet peut être un terminal d'équilibreur de charges de passerelle (GWLBe) AWS. Le GWLBe envoie le trafic à la solution GWLB, puis à ASA virtuel pour inspection. Toutes les exigences et conditions d'AWS sont remplies dans tous les cas. Comme indiqué dans le diagramme de scénarios, le côté droit de la ligne pointillée représente la solution d'évolutivité automatique GWLB d'ASA virtuel déployée via les modèles ASA virtuel. Le côté gauche est entièrement défini par l'utilisateur.

Remarque Le trafic sortant initié par l'application ne passera pas par l'ASA virtuel.

Illustration 2 : Diagramme de scénarios d'évolutivité automatique de la solution GWLB AWS d'ASA



virtuel

Fonctionnement de la solution d'évolutivité automatique

Pour l'évolutivité à la baisse et à la hausse des instances ASA virtuel, une entité externe appelée Auto Scale Manager supervise les mesures, les commandes et le groupe d'évolutivité automatique pour ajouter ou supprimer les instances ASA virtuel, et configure les instances ASA virtuel.

Auto Scale Manager est implémenté en utilisant l'architecture sans serveur AWS et communique avec les ressources d'AWS et l'ASA virtuel. Nous fournissons des modèles CloudFormation pour automatiser le déploiement des composants d'Auto Scale Manager. Le modèle déploie également d'autres ressources nécessaires pour que la solution complète fonctionne.

Remarque Les scripts d'évolutivité automatique sans serveur ne sont appelés que par les événements CloudWatch. Ils ne s'exécutent donc que lorsqu'une instance est lancée.

Composants de la solution d'évolutivité automatique

Les composants suivants constituent la solution d'évolutivité automatique.

Modèle CloudFormation

Le modèle CloudFormation est utilisé pour déployer les ressources requises par la solution d'évolutivité automatique dans AWS. Le modèle comprend les éléments suivants :

- Groupe d'évolutivité automatique, équilibreur de charges, groupes de sécurité et autres composants divers.
- Le modèle prend en compte les données des utilisateurs pour personnaliser le déploiement.

Remarque Le modèle a des limites pour la validation des entrées des utilisateurs. Il est donc de la responsabilité de l'utilisateur de valider les entrées pendant le déploiement.

Fonctions Lambda

La solution d'évolutivité automatique est un ensemble de fonctions Lambda développées en Python, qui sont déclenchées à partir de crochets de cycle de vie, de SNS et d'événements/alarmes CloudWatch. Voici les fonctionnalités de base :

- Ajouter/Supprimer les interfaces Gig 0/0 et Gig 0/1 à l'instance.
- Enregistrez l'interface Gig 0/1 dans les groupes cibles de l'équilibreur de charges.
- Configurez et déployez un nouveau ASA virtuel avec le fichier de configuration ASA.

Les fonctions Lambda sont fournies au client sous la forme d'un progiciel Python.

Crochets de cycle de vie

- Les crochets de cycle de vie sont utilisés pour obtenir une notification de modification de cycle de vie d'une instance.
- Dans le cas du lancement d'une instance, un crochet de cycle de vie est utilisé pour déclencher une fonction Lambda qui peut ajouter des interfaces à une instance ASA virtuel et enregistrer les adresses IP d'interface externe aux groupes cibles.
- Dans le cas de la résiliation d'une instance, un crochet de cycle de vie est utilisé pour déclencher une fonction Lambda afin d'annuler l'enregistrement d'une instance ASA virtuel du groupe cible.

Service de notification simple (SNS)

- Le service de notification simple (SNS) d'AWS est utilisé pour générer des événements.
- En raison de la limitation liée à l'absence d'orchestrateur adapté aux fonctions Lambda sans serveur dans AWS, la solution utilise SNS comme type de chaînage de fonctions pour orchestrer les fonctions Lambda selon les événements.

Prérequis

Télécharger les fichiers de déploiement

Téléchargez les fichiers requis pour lancer l'évolutivité automatique ASA virtuel pour la solution AWS. Les scripts et les modèles de déploiement pour votre version ASA sont disponibles dans le référentiel GitHub.

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

Configuration de l'infrastructure

Dans un référentiel GitHub cloné/téléchargé, les fichiers **infrastructure.yaml** se trouvent dans le dossier de modèle. Ce CFT peut être utilisé pour déployer des VPC, des sous-réseaux, des routes, des ACL, des groupes de sécurité, des points terminaux VPC et des compartiments S3 avec des politiques de compartiment. Ce CFT peut être modifié selon vos besoins.

Les sections suivantes fournissent de plus amples renseignements sur ces ressources et leur utilisation dans l'évolutivité automatique. Vous pouvez déployer manuellement ces ressources et les utiliser pour l'évolutivité automatique.

Remarque Le modèle **infrastructure.yaml** déploie uniquement des VPC, des sous-réseaux, des ACL, des groupes de sécurité, des compartiments S3 et des points terminaux de VPC. Il ne crée pas le certificat SSL, la couche Lambda ou les ressources de clés KMS.

VPC

Vous devez créer le VPC selon les besoins de votre application. Il est prévu que le VPC ait une passerelle Internet avec au moins un sous-réseau associé à une route vers Internet. Consultez les sections appropriées pour connaître les exigences des groupes de sécurité, des sous-réseaux, etc.

Subnets (Sous-réseaux)

Des sous-réseaux peuvent être créés selon les besoins de l'application. La machine ASA virtuel nécessite 3 sous-réseaux pour fonctionner, comme illustré dans le scénario.

Remarque Si la prise en charge de plusieurs zones de disponibilité est nécessaire, des sous-réseaux sont nécessaires pour chaque zone, car les sous-réseaux sont des propriétés zonées dans le nuage AWS.

Sous-réseau externe

Le sous-réseau externe doit avoir une route par défaut avec « 0.0.0.0/0 » vers la passerelle Internet. Celui contiendra l'interface externe de l'ASA virtuel, et le NLB sur Internet se trouvera également dans ce sous-réseau.

Sous-réseau interne

Cela peut être similaire aux sous-réseaux d'application, avec ou sans passerelle NAT/Internet. Veuillez noter que pour les sondes d'intégrité de l'ASA virtuel, il devrait être possible d'atteindre le serveur de métadonnées AWS (169.254.169.254) par le port 80.

Remarque Dans cette solution d'évolutivité automatique, les sondes d'intégrité de l'équilibreur de charges sont redirigées vers le serveur de métadonnées AWS par l'intermédiaire de l'interface interne/Gig0/0. Cependant, vous pouvez le modifier en utilisant votre propre application pour assurer les connexions de sonde d'intégrité envoyées à l'ASA virtuel à partir de l'équilibreur de charges. Dans ce cas, vous devez remplacer l'objet du serveur de métadonnées AWS par l'adresse IP de l'application respective pour fournir la réponse des sondes d'intégrité.

Management Subnet (Sous-réseau de gestion)

Ce sous-réseau comprend l'interface de gestion de l'ASA virtuel. Il est facultatif d'avoir une route par défaut.

Sous-réseaux Lambda

La fonction AWS Lambda nécessite deux sous-réseaux ayant la passerelle NAT comme passerelle par défaut. Cela rend la fonction Lambda privée pour le VPC. Les sous-réseaux Lambda ne doivent pas être aussi larges que les autres sous-réseaux. Veuillez vous reporter à la documentation d'AWS pour connaître les bonnes pratiques sur les sous-réseaux Lambda.

Sous-réseaux d'application

Aucune restriction n'est imposée sur ce sous-réseau par la solution d'évolutivité automatique, mais si l'application a besoin de connexions sortantes en dehors du VPC, des routes respectives doivent être configurées sur le sous-réseau. En effet, le trafic initié vers la sortie ne passe pas par les équilibreurs de charges. Consultez le Guide de l'utilisateur de l'équilibrage de charges élastiques d'AWS.

Groupes de sécurité

Toutes les connexions sont autorisées dans le modèle de groupe d'évolutivité automatique fourni. Vous n'avez besoin que des connexions suivantes pour que la solution d'évolutivité automatique fonctionne.

Tableau 1 : Ports requis

Port	Usage	Sous-réseau
Port de sonde d'intégrité (par défaut : 8080)	Sondes d'intégrité de l'équilibreur de charges sur Internet	Sous-réseaux extérieur, intérieur
Ports d'application	Transit de données des applications	Sous-réseaux extérieur, intérieur

Compartiment Amazon S3

Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets qui offre une évolutivité, une disponibilité des données, une sécurité et des performances de pointe. Vous pouvez placer tous les fichiers requis pour le modèle de pare-feu et le modèle d'application dans le compartiment S3.

Lorsque des modèles sont déployés, des fonctions Lambda sont créées en référençant les fichiers zip dans le compartiment S3. Par conséquent, le compartiment S3 devrait être accessible au compte d'utilisateur.

Certificat de serveur SSL

Si l'équilibreur de charge Internet doit prendre en charge TLS/SSL, un ARN de certificat est requis. Consultez les liens suivants pour en savoir plus :

- Travailler avec des certificats de serveur
- Créer une clé privée et un certificat autosigné pour les tests
- Créer AWS ELB avec un certificat SSL autosigné (lien tiers)

Exemple d'ARN : arn:aws:iam::[Compte AWS]:server-certificate/[Nom du certificat]

Couche Lambda

Le fichier ***autoscale_layer.zip*** peut être créé dans un environnement Linux, comme Ubuntu 18.04 sur lequel Python 3.9 est installé.

```
#!/bin/bash
mkdir -p layer
virtualenv -p /usr/bin/python3.9 ./layer/
source ./layer/bin/activate
pip3 install cffi==1.15.1
pip3 install cryptography==2.9.1
pip3 install paramiko==2.7.1
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install jsonschema==3.2.0
pip3 install pycryptodome==3.15.0
echo "Copy from ./layer directory to ./python\n"
cp -r ./layer/lib/python3.9/site-packages/* ./python/
zip -r autoscale_layer.zip ./python
```

Le fichier ***autoscale_layer.zip*** résultant doit être copié dans le dossier *lambda-python-files*.

Clé principale de KMS

Cela est nécessaire si les mots de passe ASA virtuel sont dans un format chiffré. Sinon, ce composant n'est pas obligatoire. Les mots de passe doivent être chiffrés uniquement à l'aide du KMS fourni ici. Si l'ARN KMS est saisi sur CFT, les mots de passe doivent être chiffrés. Sinon, les mots de passe doivent être en texte brut.

Pour en savoir plus à propos des clés principales et du 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 'MyC0mplIc@tedProtect1oN'
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
}
$
```

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

Environnement Python 3

Un fichier ***make.py*** se trouve dans le répertoire supérieur du référentiel cloné. Cela compressera les fichiers python dans un fichier zip et les copiera dans un dossier cible. Afin d'effectuer ces tâches, l'environnement Python 3 doit être disponible.

Déployer la solution d'évolutivité automatique

Préparation

Il est attendu que l'application est déployée ou que son plan de déploiement est disponible.

Paramètres d'entrée

Les paramètres d'entrée suivants doivent être recueillis avant le déploiement.

Remarque Pour l'équilibreur de charges de passerelle AWS (GWLB), les paramètres **LoadBalancerType**, **LoadBalancerSG**, **LoadBalancerPort**et **SSLcertificate** ne sont pas applicables.

Tableau 2 : Paramètres d'entrée de l'évolutivité automatique

Paramètre	Valeurs/Type autorisés	Description
Numéro de module (PodNumber)	Chaîne Modèle autorisé : « ^\d{1,3}$ »	Voici le numéro de module (pod). Ce suffixe sera ajouté au nom du groupe d'évolutivité automatique (ASA virtuel-Nom-Groupe). Par exemple, si cette valeur est « 1 », le nom de groupe sera *ASA virtuel-Nom-Groupe-1*. Il doit comporter au moins 1 chiffre numérique, mais pas plus de 3 chiffres. Par défaut : 1
AutoscaleGRPNamePrefix	Chaîne	Il s'agit du préfixe du nom du groupe d'évolutivité automatique. Le numéro de module (pod) sera ajouté en tant que suffixe. Maximum : 18 caractères Exemple : Cisco-ASA virtuel-1
NotifyEmailID	Chaîne	Les événements de l'évolutivité automatique seront envoyés à cette adresse e-mail. Vous devez accepter une demande d'abonnement par e-mail. Exemple : admin@company.com
VpcId	Chaîne	L'ID du VPC dans lequel l'appareil doit être déployé. Il doit être configuré conformément aux exigences d'AWS. Type : AWS::EC2::VPC::Id Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.
LambdaSubnets	Liste	Les sous-réseaux dans lesquels les fonctions Lambda seront déployées. Type : Liste<AWS::EC2::Subnet::Id> Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.
LambdaSG	Liste	Les groupes de sécurité pour les fonctions Lambda. Type: List<AWS::EC2::SecurityGroup::Id> Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.

Paramètre	Valeurs/Type autorisés	Description
S3BktName	Chaîne	Le nom du compartiment S3 pour les fichiers. Il doit être configuré dans votre compte conformément aux exigences d'AWS. Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.
LoadBalancerType	Chaîne	Le type d'équilibreur de charges sur Internet, « application » ou « réseau ». Exemple : application
LoadBalancerSG	Chaîne	Les groupes de sécurité pour l'équilibreur de charges. Dans le cas d'un équilibreur de charges réseau, il ne sera pas utilisé. Mais vous devez fournir un ID de groupe de sécurité. Type: List<AWS::EC2::SecurityGroup::Id> Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.
LoadBalancerPort	Nombre entier	Le port de l'équilibreur de charges. Ce port sera ouvert sur LB avec le protocole HTTP/HTTPS ou TCP/TLS, en fonction du type d'équilibreur de charges choisi. Assurez-vous que le port est un port TCP valide, il sera utilisé pour créer l'écouteur de l'équilibreur de charges. Par défaut : 80
SSLcertificate	Chaîne	L'ARN du certificat SSL pour les connexions de port sécurisées. S'il n'est pas spécifié, un port ouvert sur l'équilibreur de charges sera TCP/HTTP. S'il est spécifié, un port ouvert sur l'équilibreur de charges sera TLS/HTTPS.
TgHealthPort	Nombre entier	Ce port est utilisé par le groupe cible pour les sondes d'intégrité. Les sondes d'intégrité provenant de ce port sur l'ASA virtuel seront acheminées vers le serveur de métadonnées AWS et ne devraient pas être utilisées pour le trafic. Il doit s'agir d'un port TCP valide. Si vous souhaitez que votre application réponde aux sondes d'intégrité, les règles NAT peuvent être modifiées en conséquence pour l'ASA virtuel. Dans ce cas, si l'application ne répond pas, l'ASA virtuel sera marqué comme non intègre et supprimé en raison de l'alarme de seuil d'instance Non intègre. Exemple : 8080

Paramètre	Valeurs/Type autorisés	Description
AssignPublicIP	Booléen	Si la valeur est sélectionnée comme « true » (vraie), une adresse IP publique sera attribuée. Dans le cas d'un ASA virtuel de type BYOL, vous devez vous connecter à https://tools.cisco.com. Exemple : TRUE (VRAI)
ASAvInstanceType	Chaîne	L'Amazon Machine Image (AMI) prend en charge différents types d'instances, qui déterminent la taille de l'instance et la quantité de mémoire requise. Seuls les types d'instances AMI qui prennent en charge l'ASA virtuel doivent être utilisés. Exemple : c4.2xlarge
ASAvLicenseType	Chaîne	Le type de licence ASA virtuel, BYOL ou PAYG. Assurez-vous que l'ID AMI associé est du même type de licence. Exemple : BYOL
ASAvAmiId	Chaîne	L'ID AMI d'ASA virtuel (un ID AMI de Cisco ASA virtuel valide). Type : AWS::EC2::Image::Id Veuillez choisir le bon ID AMI en fonction de la région et de la version souhaitée de l'image.
ConfigFileURL	Chaîne	L'URL HTTP pour les fichiers de configuration d'ASA virtuel. Les fichiers de configuration de chaque zone de disponibilité doivent être disponibles dans l'URL. La fonction Lambda se chargera de choisir le bon fichier. Vous pouvez déployer un serveur HTTP pour héberger des fichiers de configuration ou vous pouvez utiliser la fonction d'hébergement web statique d'AWS S3. **Remarque** Le dernier « / » est également nécessaire, car les noms des fichiers de configuration seront ajoutés à l'URL au moment de l'importation. Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur. Exemple : https://myserver/asavconfig/asaconfig .txt/

Paramètre	Valeurs/Type autorisés	Description
NoOfAZs	Nombre entier	Le nombre de zones de disponibilité que l'ASA virtuel doit traverser, entre 1 et 3. Dans le cas d'un déploiement ALB, la valeur minimale est de 2, comme l'exige AWS. Exemple : 2
ListOfAzs	Chaîne séparée par des virgules	Une liste de zones séparées par des virgules dans l'ordre. **Remarque** L'ordre dans lequel elles sont énumérées est important. Les listes de sous-réseaux doivent être données dans le même ordre. Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur. Exemple : us-east-1a, us-east-1b, us-east-1c
ASAvMgmtSubnetId	Liste séparée par des virgules	Une liste d'ID de sous-réseau de gestion séparés par des virgules. La liste doit être dans le même ordre que les zones de disponibilité correspondantes. Type: List<AWS::EC2::SecurityGroup::Id> Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.
ASAvInsideSubnetId	Liste séparée par des virgules	Une liste d'ID de sous-réseau interne/Gig0/0 séparés par des virgules. La liste doit être dans le même ordre que les zones de disponibilité correspondantes. Type: List<AWS::EC2::SecurityGroup::Id> Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.
ASAvOutsideSubnetId	Liste séparée par des virgules	Une liste d'ID de sous-réseau externe/Gig0/1 séparés par des virgules. La liste doit être dans le même ordre que les zones de disponibilité correspondantes. Type: List<AWS::EC2::SecurityGroup::Id> Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.

Paramètre	Valeurs/Type autorisés	Description
KmsArn	Chaîne	L'ARN d'un KMS existant (clé AWS KMS à chiffrer au repos). S'ils sont spécifiés, les mots de passe ASA virtuel doivent être chiffrés. Le chiffrement du mot de passe doit être effectué uniquement à l'aide de l'ARN spécifié. Exemple de génération de mot de passe chiffré : « aws kms encrypt --key-id <ARN KMS> --plaintext <password> ». Veuillez utiliser les mots de passe générés, comme indiqué. Exemple : arn:aws:kms:us-east-1:[Compte AWS]:key/7d586a25-5875-43b1-bb68-a452e2f6468e
CpuThresholds	Nombre entiers séparés par des virgules	Le seuil inférieur et le seuil supérieur pour le CPU. La valeur minimale est de 0 et la valeur maximale est de 99. Par défaut : 10, 70 Veuillez noter que le seuil inférieur doit être inférieur au seuil supérieur. Exemple : 30, 70

Mettre à jour les fichiers de configuration ASA

Vous préparez des fichiers de configuration ASA et vous les stockez dans un serveur http/https accessible par une instance ASA virtuel. Il s'agit d'un format de fichier de configuration ASA standard. Un ASA virtuel évolutif téléchargera un fichier de configuration et mettra à jour sa configuration.

Les sections suivantes fournissent des exemples sur la façon dont le fichier de configuration ASA peut être modifié pour la solution d'évolutivité automatique.

Objets, groupes de périphériques, règles NAT et politiques d'accès

Consultez les éléments suivants pour obtenir un exemple d'objets, de routes et de règles NAT pour les sondes d'intégrité de l'équilibreur de charges pour la configuration ASA virtuel.

```
! Load Balancer Health probe Configuration
object network aws-metadata-server
host 169.254.169.254
object service aws-health-port
service tcp destination eq 7777
object service aws-metadata-http-port
service tcp destination eq 80
route inside 169.254.169.254 255.255.255.255 10.0.100.1 1
nat (outside,inside) source static any interface destination static interface
aws-metadata-server service aws-health-port aws-metadata-http-port
!
```

Remarque Les connexions de sonde d'intégrité ci-dessus doivent être autorisées dans votre politique d'accès.

Consultez la section suivante pour obtenir un exemple de configuration du plan de données pour une configuration ASA virtuel.

```
! Data Plane Configuration
route inside 10.0.0.0 255.255.0.0 10.0.100.1 1
object network http-server-80
host 10.0.50.40
object network file-server-8000
host 10.0.51.27
object service http-server-80-port
service tcp destination eq 80
nat (outside,inside) source static any interface destination static interface http-server-80
 service http-server-80-port http-server-80-port
object service file-server-8000-port
service tcp destination eq 8000
nat (outside,inside) source static any interface destination static interface file-server-8000
 service file-server-8000-port file-server-8000-port
object service https-server-443-port
service tcp destination eq 443
nat (outside,inside) source static any interface destination static interface http-server-80
 service https-server-443-port http-server-80-port
!
```

Mises à jour des fichiers de configuration

La configuration ASA virtuel doit être mise à jour dans les fichiers *az1-configuration.txt*, *az2-configuration.txt*et *az3-configuration.txt*.

Remarque Avoir trois fichiers de configuration vous permet de modifier la configuration en fonction de la zone de disponibilité (AZ). Par exemple, la route statique vers le serveur aws- metadata-server aura une passerelle différente dans chaque zone de disponibilité.

Mises à jour du modèle

Le modèle *deploy_autoscale.yaml* doit être modifié avec soin. Vous devez modifier le champ *UserData* (données utilisateur) du ***LaunchTemplate*** (modèle de lancement). Le champ *UserData* (données utilisateur) peut être mis à jour au besoin. Le serveur de noms *name-server* doit être mis à jour en conséquence; par exemple, il peut s'agir de l'adresse IP DNS du VPC. Lorsque votre licence est BYOL, l'*idtoken* (jeton d'identité) de licence doit être partagé ici.

```
!
dns domain-lookup management
DNS server-group DefaultDNS
name-server <VPC DNS IP>
!
! License configuration
        call-home
        profile License
        destination transport-method http
        destination address http <url>
        license smart
        feature tier standard
        throughput level <entitlement>
        license smart register idtoken <token>
```

Charger des fichiers dans le service de stockage Amazon Simple Storage (S3)

Tous les fichiers du répertoire *cible* doivent être chargés dans le compartiment Amazon S3. Vous pouvez également utiliser l'interface de ligne de commande pour charger tous les fichiers du répertoire *cible* dans le compartiment Amazon S3.

```
$ cd ./target
$ aws s3 cp . s3://<bucket-name> --recursive
```

Déployer la pile

Une fois que toutes les conditions préalables pour le déploiement sont terminées, vous pouvez créer la pile AWS CloudFormation.

Utilisez le fichier *deploy_autoscale.yaml* dans le répertoire *target* (cible).

Utilisez le fichier *deploy_ngfw_autoscale_with_gwlb.yaml* dans le répertoire *target* (cible) pour Geneve Autoscale.

Remarque Avant de déployer le fichier *deploy_ngfw_autoscale_with_gwlb.yaml* , vous devez déployer le fichier **infrastructure_gwlb.yaml** pour la solution d'évolutivité automatique AWS GWLB.

Vous devez créer le point terminal de l'équilibreur de charge de passerelle (GWLB-E) en sélectionnant le GWLB qui est créée lors du déploiement du modèle *deploy_autoscale_with_gwlb.Yaml*. Après avoir créé le GWLBe, vous devez mettre à jour le routeur par défaut pour utiliser GWLBe pour le sous-réseau d'application et le tableau de routage par défaut.

Pour en savoir plus, consultez https://docs.amazonaws.cn/en_us/vpc/latest/privatelink/create-endpoint-service-gwlbe.html.

Fournissez les paramètres comme collectés dans Paramètres d'entrée, à la page 8.

Valider les déploiements

Une fois le déploiement du modèle réussi, vous devez valider que les fonctions Lambda et les événements CloudWatch sont créés. Par défaut, le groupe d'évolutivité automatique a le nombre minimal et maximal d'instances à zéro. Vous devez modifier le groupe d'évolutivité automatique dans la console AWS EC2 avec le nombre d'instances que vous souhaitez. Cela déclenchera les nouvelles instances ASA virtuel.

Nous vous recommandons de lancer une seule instance, de vérifier son flux de travail et de valider son comportement pour savoir si elle fonctionne comme prévu. Une fois que les exigences réelles de l'ASA virtuel peuvent être déployées, elle peuvent également vérifier le comportement. Le nombre minimal d'instances ASA virtuel peut être marqué comme protégé contre une évolutivité à la baisse pour éviter que ces dernières soient supprimées par les politiques d'évolutivité AWS.

Tâches de maintenance

Processus d'évolutivité

Cette rubrique explique comment suspendre puis reprendre un ou plusieurs des processus d'évolutivité pour votre groupe d'évolutivité automatique.

Actions de début et de fin d'évolutivité

Pour commencer et arrêter les actions d'évolutivité à la hausse/baisse, procédez comme suit.

- Pour l'évolutivité dynamique d'AWS, consultez le lien suivant pour obtenir des renseignements afin d'activer ou de désactiver les actions d'évolutivité à la hausse :

  Suspension et reprise des processus d'évolutivité

Moniteur d'intégrité

Toutes les 60 minutes, une tâche CloudWatch Cron déclenche le gestionnaire d'évolutivité automatique Lambda pour le module d'intégrité

- S'il y a des adresses IP non intègres qui appartiennent à une machine virtuelle ASA virtuel valide, cette instance est supprimée si ASA virtuel date de plus d'une heure.
- Si ces adresses IP ne proviennent pas d'une machine ASA virtuel valide, seules les adresses IP sont supprimées du groupe de cibles.

Désactiver le moniteur d'intégrité

Pour désactiver un moniteur d'intégrité, dans ***constant.py***, définissez la constante sur « True ».

Activer le moniteur d'intégrité

Pour activer un moniteur d'intégrité, dans ***constant.py***, définissez la constante sur « False ».

Désactiver les crochets de cycle de vie

Dans le cas peu probable où le crochet de cycle de vie doit être désactivé, s'il est désactivé, il n'ajoutera pas d'interfaces supplémentaires aux instances. Cela peut également entraîner une série d'échecs du déploiement des instances ASA virtuel.

Désactiver Auto Scale Manager

Pour désactiver le gestionnaire d'évolutivité automatique Auto Scale Manager, les événements CloudWatch Events « notify-instance-lancement » et « notify-instance-terminal » doivent être désactivés. Cette désactivation ne déclenchera pas Lambda pour de nouveaux événements. Mais l'exécution des actions Lambda se poursuivra déjà. Il n'y a pas d'arrêt brutal d'Auto Scale Manager. La tentative d'arrêt brut par la suppression de la pile ou la suppression des ressources peut entraîner un état indéfini.

Cibles de l'équilibreur de charge

Comme l'équilibreur de charge AWS n'autorise pas les cibles de type instance pour les instances ayant plusieurs interfaces réseau, l'adresse IP de l'interface Gigabit0/1 est configurée comme cible sur les groupes de cibles. Pour l'instant, cependant, les contrôles d'intégrité de l'évolutivité automatique d'AWS ne fonctionnent que pour les cibles de type d'instance, et non pour les adresses IP. En outre, ces adresses IP ne sont pas automatiquement ajoutées ou supprimées des groupes cibles. Par conséquent, notre solution d'évolutivité automatique gère ces deux tâches de manière programmatique. Mais dans le cas d'une maintenance ou d'un dépannage, il pourrait y avoir une situation nécessitant un effort manuel.

Enregistrer une cible dans un groupe de cibles

Pour enregistrer l'instance ASA virtuel sur l'équilibreur de charge, son adresse IP d'instance Gigabit0/1 (sous-réseau externe) doit être ajoutée en tant que cible dans le ou les groupes de cibles. Consultez Enregistrer ou annuler l'enregistrement des cibles par adresse IP.

Annuler l'enregistrement d'une cible d'un groupe de cibles

Pour annuler l'enregistrement de l'instance ASA virtuel de l'équilibreur de charge, son adresse IP d'instance Gigabit0/1 (sous-réseau externe) doit être supprimée en tant que cible dans le ou les groupes de cibles. Consultez Enregistrer ou annuler l'enregistrement des cibles par adresse IP.

Instance en attente

AWS n'autorise pas le redémarrage d'instance dans le groupe d'évolutivité automatique, mais il permet à un utilisateur de mettre une instance en veille et d'effectuer de telles actions. Cependant, cela fonctionne mieux lorsque les cibles de l'équilibreur de charges sont de type instance. Cependant, les machines ASA virtuel ne peuvent pas être configurées en tant que cibles de type instance, en raison de plusieurs interfaces réseau.

Mettre une instance en veille

Si une instance est mise en veille, son adresse IP dans les groupes de cibles continuera toujours d'être dans le même état jusqu'à ce que les sondes d'intégrité échouent. Pour cette raison, il est recommandé de désinscrire les adresses IP respectives du groupe cible avant de mettre l'instance en état de veille; consultez Annuler l'enregistrement d'une cible d'un groupe de cibles, à la page 17 pour en savoir plus.

Une fois les IP supprimées, consultez Supprimer temporairement les instances de votre groupe d'évolutivité automatique.

Supprimer une instance de la mise en veille

De même, vous pouvez déplacer une instance de l'état de veille à l'état d'exécution. Après sa suppression de l'état de veille, l'adresse IP de l'instance doit être enregistrée sur les cibles du groupe cible. Consultez Enregistrer une cible dans un groupe de cibles, à la page 17.

Pour en savoir plus sur la mise en veille des instances à des fins de dépannage ou de maintenance, consultez le blogue d'actualités AWS.

Supprimer/dissocier l'instance du groupe d'évolutivité automatique

Pour supprimer une instance du groupe d'évolutivité automatique, vous devez d'abord la mettre en mode veille. Consultez la section « Mettre des instances en veille ». Une fois que l'instance est en état de veille, elle

peut être supprimée ou dissociée. Consultez Dissocier les instances EC2 de votre groupe d'évolutivité automatique.

Mettre fin à une instance

Pour mettre fin à une instance, elle doit être mise en veille; voir Instance en attente, à la page 17. Une fois que l'instance est en veille, vous pouvez procéder à la résiliation.

Protection à l'échelle de l'instance

Pour éviter la suppression accidentelle d'une instance particulière du groupe d'évolutivité automatique, elle peut être protégée par l'évolutivité à la baisse. Si une instance est protégée par l'évolutivité à la baisse, elle ne sera pas résiliée en raison d'un événement d'évolutivité à la baisse.

Veuillez vous reporter au lien suivant pour mettre une instance en état protégé par l'évolutivité à la baisse.

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html

Important Il est recommandé de faire en sorte que le nombre minimal d'instances qui sont intègres (l'adresse IP cible doit être intègre, pas seulement l'instance EC2) soit protégé par l'évolutivité à la baisse.

Changements de configuration

Toute modification de la configuration ne sera pas automatiquement reflétée sur les instances déjà en cours d'exécution. Ces modifications ne seront reflétées que sur les prochains périphériques intégrés. Toutes les modifications de ce type doivent être transférées manuellement vers les périphériques existants.

Si vous rencontrez des problèmes lors de la mise à jour manuelle de la configuration sur les instances existantes, nous vous recommandons de supprimer ces instances du groupe d'évolutivité et de les remplacer par de nouvelles.

Modifier le mot de passe d'administrateur ASA Virtuel

Une modification du mot de passe ASA virtuel oblige l'utilisateur à le modifier sur chaque périphérique manuellement pour les instances en cours d'exécution. Pour les nouveaux périphériques ASA virtuel à intégrer, le mot de passe ASA virtuel sera tiré des variables d'environnement Lambda. Consultez la section sur l'utilisation des variables d'environnement AWS Lambda.

Modifications des ressources AWS

Vous pouvez modifier de nombreuses choses dans AWS après le déploiement, telles que le groupe d'évolutivité automatique, la configuration de lancement, les événements CloudWatch, les politiques d'évolutivité, etc. Vous pouvez importer vos ressources dans une pile CloudFormation ou créer une nouvelle pile à partir de vos ressources existantes.

Consultez la section sur l'importation de ressources existantes dans Cloud Formation Management pour en savoir plus sur la gestion des modifications effectuées sur les ressources d'AWS.

Récupérer et analyser les journaux CloudWatch

Afin d'exporter les journaux CloudWatch, consultez la section Exporter les données du journal vers Amazon S3 à l'aide de l'interface de ligne de commande d'AWS.

Dépannage et débogage

Console AWS CloudFormation

Vous pouvez vérifier les paramètres d'entrée de votre pile CloudFormation dans la console AWS CloudFormation, qui vous permet de créer, de superviser, de mettre à jour et de supprimer des piles directement à partir de votre navigateur Web.

Accédez à la pile requise et vérifiez l'onglet des paramètres. Vous pouvez également vérifier les entrées des fonctions Lambda sous l'onglet des variables d'environnement des fonctions Lambda.

Pour en savoir plus sur la console AWS CloudFormation, consultez le *Guide de l'utilisateur AWS CloudFormation*.

Journaux Amazon CloudWatch

Vous pouvez afficher les journaux des fonctions Lambda individuelles. AWS Lambda supervise automatiquement les fonctions Lambda en votre nom, en effectuant des rapports sur les mesures par l'entremise d'Amazon CloudWatch. Pour vous aider à dépanner les défaillances d'une fonction, Lambda consigne toutes les demandes gérées par votre fonction et stocke également automatiquement les journaux générés par votre code dans les journaux Amazon CloudWatch.

Vous pouvez afficher les journaux pour Lambda en utilisant la console Lambda, la console CloudWatch, l'interface CLI 'AWS ou l'API CloudWatch. Pour en savoir plus sur les groupes de journaux et y accéder par l'entremise de la console CloudWatch, consultez le système de supervision, l'application et les fichiers journaux personnalisés dans le *Guide de l'utilisateur Amazon CloudWatch*.

Échec de contrôle de l'intégrité de l'équilibreur de charges

Le contrôle de l'intégrité de l'équilibreur de charges contient des informations telles que le protocole, le port ping, le chemin ping, le délai d'expiration de réponse et l'intervalle de contrôle de l'intégrité. Une instance est considérée comme saine si elle renvoie un code de réponse de 200 dans l'intervalle de contrôle de l'intégrité.

Si l'état actuel de certaines ou de toutes vos instances est `Outofservice` et que le champ de description affiche le message que `Instance has failed at least the Unhealthy Threshold number of health checks consecutively` (l'instance a échoué au moins à un nombre limite de contrôles d'intégrité consécutifs), les instances ont échoué au contrôle de l'intégrité de l'équilibreur de charges.

Vous devez vérifier la règle NAT de la sonde d'intégrité dans la configuration ASA. Pour en savoir plus, consultez Dépannage d'un équilibreur de charges classique : contrôles d'intégrité.

Problèmes de trafic

Pour résoudre les problèmes de trafic pour vos instances ASA virtuel, vous devez vérifier les règles de l'équilibreur de charge, les règles NAT et les routes statiques configurées dans les instances ASA virtuel.

Vous devez également vérifier les détails du réseau virtuel AWS, des sous-réseaux et de la passerelle fournis dans le modèle de déploiement, y compris les règles de groupe de sécurité, etc. Vous pouvez également consulter la documentation AWS, par exemple, Dépannage des instances EC2.

Échec de la configuration de ASA virtuel

Si l'ASA virtuel ne parvient pas à se configurer, vous devez vérifier la connectivité à la configuration d'hébergement du serveur Web HTTP statique Amazon S3. Consultez Hébergement d'un site Web statique sur Amazon S3 pour en savoir plus.

Échec de la licence ASA virtuel

Si la licence ASA virtuel échoue, vous devez vérifier la connectivité au serveur CSSM, vérifiez la configuration du groupe de sécurité ASA virtuel et vérifiez les listes de contrôle d'accès.

Impossible d'inscrire le protocole SSH dans l'ASA virtuel

Si vous ne parvenez pas à inscrire le protocole SSH dans l'ASA virtuel, vérifiez si le mot de passe complexe a été transmis à l'ASA virtuel au moyen du modèle.

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.